THE BIG LIST OF INFOSEC RESOURCES

Awesome Infosec
==========

[![Awesome](https://cdn.rawgit.com/sindresorhus/awesome/d7305f38d29fed78fa85652e3a63e154dd8e8829/media/badge.svg)](https://github.com/sindresorhus/awesome)

A curated list of awesome information security resources, inspired by the awesome-* trend on GitHub.

Those resources and tools are intended only for cybersecurity professional and educational use in a controlled environment.

Table of Contents
==========

Massive Online Open Courses
==========

Stanford University - Computer Security
In this class you will learn how to design secure systems and write secure code. You will learn how to find vulnerabilities in code and how to design software systems that limit the impact of security vulnerabilities. We will focus on principles for building secure systems and give many real world examples.

- [Stanford University - Computer Security](https://www.coursera.org/learn/security)

Stanford University - Cryptography I
This course explains the inner workings of cryptographic primitives and how to correctly use them. Students will learn how to reason about the security of cryptographic constructions and how to apply

this knowledge to real-world applications. The course begins with a detailed discussion of how two parties who have a shared secret key can communicate securely when a powerful adversary eavesdrops and tampers with traffic. We will examine many deployed protocols and analyze mistakes in existing systems. The second half of the course discusses public-key techniques that let two or more parties generate a shared secret key. We will cover the relevant number theory and discuss public-key encryption and basic key-exchange. Throughout the course students will be exposed to many exciting open problems in the field.

- [Stanford University - Cryptography I](https://www.coursera.org/learn/crypto)

Stanford University - Cryptography II
This course is a continuation of Crypto I and explains the inner workings of public-key systems and cryptographic protocols. Students will learn how to reason about the security of cryptographic constructions and how to apply this knowledge to real-world applications. The course begins with constructions for digital signatures and their applications. We will then discuss protocols for user authentication and zero-knowledge protocols. Next we will turn to privacy applications of cryptography supporting anonymous credentials and private database lookup. We will conclude with more advanced topics including multi-party computation and elliptic curve cryptography.

- [Stanford University - Cryptography II](https://www.coursera.org/learn/crypto2)

University of Maryland - Usable Security
This course focuses on how to design and build secure systems with a human-centric focus. We will look at basic principles of human-computer interaction, and apply these insights to the design of secure systems with the goal of developing security measures that respect human performance and their goals within a system.

- [University of Maryland - Usable Security](https://www.coursera.org/learn/usablesec)

University of Maryland - Software Security
This course we will explore the foundations of software security. We will consider important software vulnerabilities and attacks that exploit them -- such as buffer overflows, SQL injection, and session hijacking -- and we will consider defenses that prevent or mitigate these attacks, including advanced testing and program analysis techniques. Importantly, we take a "build security in" mentality, considering techniques at each phase of the development cycle that can be used to strengthen the security of software systems.

- [University of Maryland - Software Security](https://www.coursera.org/learn/softwaresec)

University of Maryland - Cryptography
This course will introduce you to the foundations of modern cryptography, with an eye toward practical applications. We will learn the importance of carefully defining security; of relying on a set of well-studied "hardness assumptions" (e.g., the hardness of factoring large numbers); and of the possibility of proving security of complicated constructions based on low-level primitives. We will not only cover these ideas in theory, but will also explore their real-world impact. You will learn about cryptographic primitives in wide use today, and see how these can be combined to develop modern protocols for secure communication.

- [University of Maryland - Cryptography](https://www.coursera.org/learn/cryptography)

University of Maryland - Hardware Security
This course will introduce you to the foundations of modern cryptography, with an eye toward practical applications. We will learn the importance of carefully defining security; of relying on a set of well-studied “hardness assumptions” (e.g., the hardness of factoring large numbers); and of the possibility of proving security of complicated constructions based on low-level primitives. We will not only cover these ideas in theory, but will also explore their real-world impact. You will learn about cryptographic primitives in wide use today, and see how these can be combined to develop modern protocols for secure communication.

- [University of Maryland - Hardware Security](https://www.coursera.org/learn/hardwaresec)

Academic Courses
==========

NYU Tandon School of Engineering - OSIRIS Lab's Hack Night

Developed from the materials of NYU Tandon's old Penetration Testing and Vulnerability Analysis course, Hack Night is a sobering introduction to offensive security. A lot of complex technical content is covered very quickly as students are introduced to a wide variety of complex and immersive topics over thirteen weeks.

- [NYU Tandon's OSIRIS Lab's Hack Night](https://github.com/isislab/Hack-Night)

Florida State University's - Offensive Computer Security
The primary incentive for an attacker to exploit a vulnerability, or series of vulnerabilities is to achieve a return on an investment (his/her time usually). This return need not be strictly monetary, an attacker may be interested in obtaining access to data, identities, or some other commodity that is valuable to them. The field of penetration testing involves authorized auditing and exploitation of systems to assess actual system security in order to protect against attackers. This requires thorough knowledge of vulnerabilities and how to exploit them. Thus, this course provides an introductory but comprehensive coverage of the fundamental methodologies, skills, legal issues, and tools used in white hat penetration testing and secure system administration.

* [Offensive Computer Security - Spring 2014](http://www.cs.fsu.edu/~redwood/OffensiveComputerSecurity)
* [Offensive Computer Security - Spring 2013](http://www.cs.fsu.edu/~redwood/OffensiveSecurity)

Florida State University's - Offensive Network Security
This class allows students to look deep into know protocols (i.e. IP, TCP, UDP) to see how an attacker can utilize these protocols to their advantage and how to spot issues in a network via captured network traffic.
The first half of this course focuses on know protocols while the second half of the class focuses on reverse engineering unknown protocols. This class will utilize captured traffic to allow students to reverse the protocol by using known techniques such as incorporating bioinformatics introduced by Marshall Beddoe. This class will also cover fuzzing protocols to see if the server or client have

vulnerabilities. Overall, a student finishing this class will have a better understanding of the network layers, protocols, and network communication and their interaction in computer networks.

* [Offensive Network Security](http://www.cs.fsu.edu/~lawrence/OffNetSec/)

Rensselaer Polytechnic Institute - Malware Analysis

This course will introduce students to modern malware analysis techniques through readings and hands-on interactive analysis of real-world samples. After taking this course students will be equipped with the skills to analyze advanced contemporary malware using both static and dynamic analysis.

- [CSCI 4976 - Fall '15 Malware Analysis](https://github.com/RPISEC/Malware)

Rensselaer Polytechnic Institute - Modern Binary Exploitation
This course will start off by covering basic x86 reverse engineering, vulnerability analysis, and classical forms of Linux-based userland binary exploitation. It will then transition into protections found on modern systems (Canaries, DEP, ASLR, RELRO, Fortify Source, etc) and the techniques used to defeat them. Time permitting, the course will also cover other subjects in exploitation including kernel-land and Windows based exploitation.

* [CSCI 4968 - Spring '15 Modern Binary Exploitation](https://github.com/RPISEC/MBE)

Rensselaer Polytechnic Institute - Hardware Reverse Engineering
Reverse engineering techniques for semiconductor devices and their applications to competitive analysis, IP litigation, security testing, supply chain verification, and failure analysis. IC packaging technologies and sample preparation techniques for die recovery and live analysis. Deprocessing and staining methods for revealing features bellow top passivation. Memory technologies and appropriate extraction techniques for each. Study contemporary anti-tamper/anti-RE methods and their effectiveness at protecting designs from attackers. Programmable logic microarchitecture and the issues involved with reverse engineering programmable logic.

- [CSCI 4974/6974 - Spring '14 Hardware Reverse Engineering](http://security.cs.rpi.edu/courses/hwre-spring2014/)

City College of San Francisco - Sam Bowne Class

- [CNIT 40: DNS Security](https://samsclass.info/40/40_F16.shtml)
DNS is crucial for all Internet transactions, but it is subject to numerous security risks, including phishing, hijacking, packet amplification, spoofing, snooping, poisoning, and more. Learn how to configure secure DNS servers, and to detect malicious activity with DNS monitoring. We will also cover DNSSEC principles and deployment. Students will perform hands-on projects deploying secure DNS servers on both Windows and Linux platforms.

- [CNIT 120 - Network Security](https://samsclass.info/120/120_S15.shtml)
Knowledge and skills required for Network Administrators and Information Technology professionals to be aware of security vulnerabilities, to implement security measures, to analyze an existing network environment in consideration of known security threats or risks, to defend against attacks or viruses, and to ensure data privacy and integrity. Terminology and procedures for implementation and

configuration of security, including access control, authorization, encryption, packet filters, firewalls, and Virtual Private Networks (VPNs).

- [CNIT 121 - Computer Forensics](https://samsclass.info/121/121_F16.shtml)
The class covers forensics tools, methods, and procedures used for investigation of computers, techniques of data recovery and evidence collection, protection of evidence, expert witness skills, and computer crime investigation techniques. Includes analysis of various file systems and specialized diagnostic software used to retrieve data. Prepares for part of the industry standard certification exam, Security+, and also maps to the Computer Investigation Specialists exam.

- [CNIT 123 - Ethical Hacking and Network Defense](https://samsclass.info/123/123_S17.shtml)
Students learn how hackers attack computers and networks, and how to protect systems from such attacks, using both Windows and Linux systems. Students will learn legal restrictions and ethical guidelines, and will be required to obey them. Students will perform many hands-on labs, both attacking and defending, using port scans, footprinting, exploiting Windows and Linux vulnerabilities, buffer overflow exploits, SQL injection, privilege escalation, Trojans, and backdoors.

- [CNIT 124 - Advanced Ethical Hacking](https://samsclass.info/124/124_F15.shtml)
Advanced techniques of defeating computer security, and countermeasures to protect Windows and Unix/Linux systems. Hands-on labs include Google hacking, automated footprinting, sophisticated ping and port scans, privilege escalation, attacks against telephone and Voice over Internet Protocol (VoIP) systems, routers, firewalls, wireless devices, Web servers, and Denial of Service attacks.

- [CNIT 126 - Practical Malware Analysis](https://samsclass.info/126/126_S16.shtml)
Learn how to analyze malware, including computer viruses, trojans, and rootkits, using disassemblers, debuggers, static and dynamic analysis, using IDA Pro, OllyDbg and other tools.

- [CNIT 127 - Exploit Development](https://samsclass.info/127/127_S17.shtml)
Learn how to find vulnerabilities and exploit them to gain control of target systems, including Linux, Windows, Mac, and Cisco. This class covers how to write tools, not just how to use them; essential skills for advanced penetration testers and software security professionals.

- [CNIT 128 - Hacking Mobile Devices](https://samsclass.info/128/128_S17.shtml)
Mobile devices such as smartphones and tablets are now used for making purchases, emails, social networking, and many other risky activities. These devices run specialized operating systems have many security problems. This class will cover how mobile operating systems and apps work, how to find and exploit vulnerabilities in them, and how to defend them. Topics will include phone call, voicemail, and SMS intrusion, jailbreaking, rooting, NFC attacks, malware, browser exploitation, and application vulnerabilities. Hands-on projects will include as many of these activities as are practical and legal.

- [CNIT 129S: Securing Web Applications](https://samsclass.info/129S/129S_F16.shtml)
Techniques used by attackers to breach Web applications, and how to protect them. How to secure authentication, access, databases, and back-end components. How to protect users from each other. How to find common vulnerabilities in compiled code and source code.

- [CNIT 140: IT Security Practices](https://samsclass.info/140/140_F16.shtml)
Training students for cybersecurity competitions, including CTF events and the [Collegiate Cyberdefense Competition (CCDC)](http://www.nationalccdc.org/). This training will prepare students for employment

as security professionals, and if our team does well in the competitions, the competitors will gain recognition and respect which should lead to more and better job offers.

- [Violent Python and Exploit Development](https://samsclass.info/127/127_WWC_2014.shtml)
In the exploit development section, students will take over vulnerable systems with simple Python scripts.

Open Security Training
OpenSecurityTraining.info is dedicated to sharing training material for computer security classes, on any topic, that are at least one day long.

Beginner Classes

- [Android Forensics & Security Testing]
(http://opensecuritytraining.info/AndroidForensics.html)
This class serves as a foundation for mobile digital forensics, forensics of Android operating systems, and penetration testing of Android applications.

- [Certified Information Systems Security Professional (CISSP)
Common Body of Knowledge (CBK)® Review](
http://opensecuritytraining.info/CISSP-Main.html)
The CISSP CBK Review course is uniquely designed for federal agency information assurance (IA) professionals in meeting [NSTISSI-4011](http://www.cnss.gov/Assets/pdf/nstissi_4011.pdf), National Training Standard for Information Systems Security Professionals, as required by [DoD 8570.01-M](http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf), Information Assurance Workforce Improvement Program.

- [Flow Analysis & Network Hunting](http://opensecuritytraining.info/Flow.html)
This course focuses on network analysis and hunting of malicious activity from a security operations center perspective. We will dive into the netflow strengths, operational limitations of netflow, recommended sensor placement, netflow tools, visualization of network data, analytic trade craft for network situational awareness and networking hunting scenarios.

- [Hacking Techniques and Intrusion Detection](http://opensecuritytraining.info/HTID.html)
The course is designed to help students gain a detailed insight into the practical and theoretical aspects of advanced topics in hacking techniques and intrusion detection.

- [Introductory Intel x86: Architecture, Assembly, Applications, &
Alliteration](http://opensecuritytraining.info/IntroX86.html)
This class serves as a foundation for the follow on Intermediate level x86 class. It teaches the basic concepts and describes the hardware that assembly code deals with. It also goes over many of the most common assembly instructions. Although x86 has hundreds of special purpose instructions, students will be shown it is possible to read most programs by knowing only around 20-30 instructions and their variations.

- [Introductory Intel x86-64: Architecture, Assembly, Applications, &
Alliteration](http://opensecuritytraining.info/IntroX86-64.html)

This class serves as a foundation for the follow on Intermediate level x86 class. It teaches the basic concepts and describes the hardware that assembly code deals with. It also goes over many of the most common assembly instructions. Although x86 has hundreds of special purpose instructions, students will be shown it is possible to read most programs by knowing only around 20-30 instructions and their variations.

- [Introduction to ARM](http://opensecuritytraining.info/IntroARM.html)
This class builds on the Intro to x86 class and tries to provide parallels and differences between the two processor architectures wherever possible while focusing on the ARM instruction set, some of the ARM processor features, and how software works and runs on the ARM processor.

- [Introduction to Cellular Security](http://opensecuritytraining.info/IntroCellSec.html)
This course is intended to demonstrate the core concepts of cellular network security. Although the course discusses GSM, UMTS, and LTE - it is heavily focused on LTE. The course first introduces important cellular concepts and then follows the evolution of GSM to LTE.

- [Introduction to Network Forensics](http://opensecuritytraining.info/NetworkForensics.html)
This is a mainly lecture based class giving an introduction to common network monitoring and forensic techniques.

- [Introduction to Secure Coding](http://opensecuritytraining.info/IntroSecureCoding.html)
This course provides a look at some of the most prevalent security related coding mistakes made in industry today. Each type of issue is explained in depth including how a malicious user may attack the code, and strategies for avoiding the issues are then reviewed.

- [Introduction to Vulnerability Assessment](http://opensecuritytraining.info/IntroductionToVulnerabilityAssessment.html)
This is a lecture and lab based class giving an introduction to vulnerability assessment of some common common computing technologies. Instructor-led lab exercises are used to demonstrate specific tools and technologies.

- [Introduction to Trusted Computing](http://opensecuritytraining.info/IntroToTrustedComputing.html)
This course is an introduction to the fundamental technologies behind Trusted Computing. You will learn what Trusted Platform Modules (TPMs) are and what capabilities they can provide both at an in-depth technical level and in an enterprise context. You will also learn about how other technologies such as the Dynamic Root of Trust for Measurement (DRTM) and virtualization can both take advantage of TPMs and be used to enhance the TPM's capabilities.

- [Offensive, Defensive, and Forensic Techniques for Determining Web User Identity](http://opensecuritytraining.info/WebIdentity.html)
This course looks at web users from a few different perspectives. First, we look at identifying techniques to determine web user identities from a server perspective. Second, we will look at obfuscating techniques from a user whom seeks to be anonymous. Finally, we look at forensic techniques, which, when given a hard drive or similar media, we identify users who accessed that server.

- [Pcap Analysis & Network Hunting](http://opensecuritytraining.info/Pcap.html)
Introduction to Packet Capture (PCAP) explains the fundamentals of how, where, and why to capture network traffic and what to do with it. This class covers open-source tools like tcpdump, Wireshark, and

ChopShop in several lab exercises that reinforce the material. Some of the topics include capturing packets with tcpdump, mining DNS resolutions using only command-line tools, and busting obfuscated protocols. This class will prepare students to tackle common problems and help them begin developing the skills to handle more advanced networking challenges.

- [Malware Dynamic Analysis](http://opensecuritytraining.info/MalwareDynamicAnalysis.html)
This introductory malware dynamic analysis class is dedicated to people who are starting to work on malware analysis or who want to know what kinds of artifacts left by malware can be detected via various tools. The class will be a hands-on class where students can use various tools to look for how malware is: Persisting, Communicating, and Hiding

- [Secure Code Review](http://opensecuritytraining.info/SecureCodeReview.html)
The course briefly talks about the development lifecycle and the importance of peer reviews in delivering a quality product. How to perform this review is discussed and how to keep secure coding a priority during the review is stressed. A variety of hands-on exercises will address common coding mistakes, what to focus on during a review, and how to manage limited time.

- [Smart Cards](http://opensecuritytraining.info/SmartCards.html)
This course shows how smart cards are different compared to other type of cards.
It is explained how smart cards can be used to realize confidentiality and integrity of information.

- [The Life of Binaries](http://opensecuritytraining.info/LifeOfBinaries.html)
Along the way we discuss the relevance of security at different stages of a binary's life, from the tricks that can be played by a malicious compiler, to how viruses really work, to the way which malware "packers" duplicate OS process execution functionality, to the benefit of a security-enhanced OS loader which implements address space layout randomization (ASLR).

- [Understanding Cryptology: Core Concepts](http://opensecuritytraining.info/CryptoCore.html)
This is an introduction to cryptology with a focus on applied cryptology. It was designed to be accessible to a wide audience, and therefore does not include a rigorous mathematical foundation (this will be covered in later classes).

- [Understanding Cryptology: Cryptanalysis](http://opensecuritytraining.info/Cryptanalysis.html)
A class for those who want to stop learning about building cryptographic systems and want to attack them. This course is a mixture of lecture designed to introduce students to a variety of code-breaking techniques and python labs to solidify those concepts. Unlike its sister class, [Core Concepts](http://opensecuritytraining.info/CryptoCore.html), math is necessary for this topic.

Intermediate Classes

- [Exploits 1: Introduction to Software Exploits](http://opensecuritytraining.info/Exploits1.html)
Software vulnerabilities are flaws in program logic that can be leveraged by an attacker to execute arbitrary code on a target system. This class will cover both the identification of software vulnerabilities and the techniques attackers use to exploit them. In addition, current techniques that attempt to remediate the threat of software vulnerability exploitation will be discussed.

- [Exploits 2: Exploitation in the Windows Environment (http://opensecuritytraining.info/Exploits2.html)
This course covers the exploitation of stack corruption vulnerabilities in the Windows environment. Stack overflows are programming flaws that often times allow an attacker to execute arbitrary code in the context of a vulnerable program. There are many nuances involved with exploiting these vulnerabilities in Windows. Window's exploit mitigations such as DEP, ASLR, SafeSEH, and SEHOP, makes leveraging these programming bugs more difficult, but not impossible. The course highlights the features and weaknesses of many the exploit mitigation techniques deployed in Windows operating systems. Also covered are labs that describe the process of finding bugs in Windows applications with mutation based fuzzing, and then developing exploits that target those bugs.

- [Intermediate Intel x86: Architecture, Assembly, Applications, & Alliteration](http://opensecuritytraining.info/IntermediateX86.html)
Building upon the Introductory Intel x86 class, this class goes into more depth on topics already learned, and introduces more advanced topics that dive deeper into how Intel-based systems work.

Advanced Classes

- [Advanced x86: Virtualization with Intel VT-x](http://opensecuritytraining.info/AdvancedX86-VTX.html)
The purpose of this course is to provide a hands on introduction to Intel hardware support for virtualization. The first part will motivate the challenges of virtualization in the absence of dedicated hardware. This is followed by a deep dive on the Intel virtualization "API" and labs to begin implementing a blue pill / hyperjacking attack made famous by researchers like Joanna Rutkowska and Dino Dai Zovi et al. Finally a discussion of virtualization detection techniques.

- [Advanced x86: Introduction to BIOS & SMM](http://opensecuritytraining.info/IntroBIOS.html)
We will cover why the BIOS is critical to the security of the platform. This course will also show you what capabilities and opportunities are provided to an attacker when BIOSes are not properly secured. We will also provide you tools for performing vulnerability analysis on firmware, as well as firmware forensics. This class will take people with existing reverse engineering skills and teach them to analyze UEFI firmware. This can be used either for vulnerability hunting, or to analyze suspected implants found in a BIOS, without having to rely on anyone else.

- [Introduction to Reverse Engineering Software](http://opensecuritytraining.info/IntroductionToReverseEngineering.html)
Throughout the history of invention curious minds have sought to understand the inner workings of their gadgets. Whether investigating a broken watch, or improving an engine, these people have broken down their goods into their elemental parts to understand how they work. This is Reverse Engineering (RE), and it is done every day from recreating outdated and incompatible software, understanding malicious code, or exploiting weaknesses in software.

- [Reverse Engineering Malware](http://opensecuritytraining.info/ReverseEngineeringMalware.html)
This class picks up where the [Introduction to Reverse Engineering Software](http://opensecuritytraining.info/IntroductionToReverseEngineering.html) course left off, exploring how static reverse engineering techniques can be used to understand what a piece of malware does and how it can be removed.

- [Rootkits: What they are, and how to find them](http://opensecuritytraining.info/Rootkits.html)

Rootkits are a class of malware which are dedicated to hiding the attacker's presence on a compromised system. This class will focus on understanding how rootkits work, and what tools can be used to help find them.

- [The Adventures of a Keystroke: An in-depth look into keylogging on Windows](http://opensecuritytraining.info/Keylogging.html)
Keyloggers are one of the most widely used components in malware. Keyboard and mouse are the devices nearly all of the PCs are controlled by, this makes them an important target of malware authors. If someone can record your keystrokes then he can control your whole PC without you noticing.

Cybrary - Online Cyber Security Training

- [CompTIA A+](https://www.cybrary.it/course/comptia-aplus)
This course covers the fundamentals of computer technology, basic networking, installation and configuration of PCs, laptops and related hardware, as well as configuring common features for mobile operation systems Android and Apple iOS.

- [CompTIA Linux+](https://www.cybrary.it/course/comptia-linux-plus)
Our free, self-paced online Linux+ training prepares students with the knowledge to become a certified Linux+ expert, spanning a curriculum that covers Linux maintenance tasks, user assistance and installation and configuration.

- [CompTIA Cloud+](https://www.cybrary.it/course/comptia-cloud-plus)
Our free, online Cloud+ training addresses the essential knowledge for implementing, managing and maintaining cloud technologies as securely as possible. It covers cloud concepts and models, virtualization, and infrastructure in the cloud.

- [CompTIA Network+](https://www.cybrary.it/course/comptia-network-plus)
In addition to building one's networking skill set, this course is also designed to prepare an individual for the Network+ certification exam, a distinction that can open a myriad of job opportunities from major companies

- [CompTIA Advanced Security Practitioner](https://www.cybrary.it/course/comptia-casp)
In our free online CompTIA CASP training, you'll learn how to integrate advanced authentication, how to manage risk in the enterprise, how to conduct vulnerability assessments and how to analyze network security concepts and components.

- [CompTIA Security+](https://www.cybrary.it/course/comptia-security-plus)
Learn about general security concepts, basics of cryptography, communications security and operational and organizational security. With the increase of major security breaches that are occurring, security experts are needed now more than ever.

- [ITIL Foundation](https://www.cybrary.it/course/itil)
Our online ITIL Foundation training course provides baseline knowledge for IT service management best practices: how to reduce costs, increase enhancements in processes, improve IT productivity and overall customer satisfaction.

- [Cryptography](https://www.cybrary.it/course/cryptography)
In this online course we will be examining how cryptography is the cornerstone of security technologies, and how through its use of different encryption methods you can protect private or sensitive information from unauthorized access.

- [Cisco CCNA](https://www.cybrary.it/course/cisco-ccna)
Our free, online, self-paced CCNA training teaches students to install, configure, troubleshoot and operate LAN, WAN and dial access services for medium-sized networks. You'll also learn how to describe the operation of data networks.

- [Virtualization Management](https://www.cybrary.it/course/virtualization-management)
Our free, self-paced online Virtualization Management training class focuses on installing, configuring and managing virtualization software. You'll learn how to work your way around the cloud and how to build the infrastructure for it.

- [Penetration Testing and Ethical Hacking](https://www.cybrary.it/course/ethical-hacking)
If the idea of hacking as a career excites you, you'll benefit greatly from completing this training here on Cybrary. You'll learn how to exploit networks in the manner of an attacker, in order to find out how protect the system from them.

- [Computer and Hacking Forensics](https://www.cybrary.it/course/computer-hacking-forensics-analyst)
Love the idea of digital forensics investigation? That's what computer forensics is all about. You'll learn how to; determine potential online criminal activity at its inception, legally gather evidence, search and investigate wireless attacks.

- [Web Application Penetration Testing](https://www.cybrary.it/course/web-application-pen-testing)
In this course, SME, Raymond Evans, takes you on a wild and fascinating journey into the cyber security discipline of web application pentesting. This is a very hands-on course that will require you to set up your own pentesting environment.

- [CISA - Certified Information Systems Auditor](https://www.cybrary.it/course/cisa)
In order to face the dynamic requirements of meeting enterprise vulnerability management challenges, this course covers the auditing process to ensure that you have the ability to analyze the state of your organization and make changes where needed.

- [Secure Coding](https://www.cybrary.it/course/secure-coding)
Join industry leader Sunny Wear as she discusses secure coding guidelines and how secure coding is important when it comes to lowering risk and vulnerabilities. Learn about XSS, Direct Object Reference, Data Exposure, Buffer Overflows, & Resource Management.

- [NIST 800-171 Controlled Unclassified Information Course](https://www.cybrary.it/course/nist-800-171-controlled-unclassified-information-course)
The Cybrary NIST 800-171 course covers the 14 domains of safeguarding controlled unclassified information in non-federal agencies. Basic and derived requirements are presented for each security domain as defined in the NIST 800-171 special publication.

- [Advanced Penetration Testing](https://www.cybrary.it/course/advanced-penetration-testing)
This course covers how to attack from the web using cross-site scripting, SQL injection attacks, remote and local file inclusion and how to understand the defender of the network you're breaking into to. You'll also learn tricks for exploiting a network.

- [Intro to Malware Analysis and Reverse Engineering](https://www.cybrary.it/course/malware-analysis)
In this course you'll learn how to perform dynamic and static analysis on all major files types, how to carve malicious executables from documents and how to recognize common malware tactics and debug and disassemble malicious binaries.

- [Social Engineering and Manipulation](https://www.cybrary.it/course/social-engineering)
In this online, self-paced Social Engineering and Manipulation training class, you will learn how some of the most elegant social engineering attacks take place. Learn to perform these scenarios and what is done during each step of the attack.

- [Post Exploitation Hacking](https://www.cybrary.it/course/post-exploitation-hacking)
In this free self-paced online training course, you'll cover three main topics: Information Gathering, Backdooring and Covering Steps, how to use system specific tools to get general information, listener shells, metasploit and meterpreter scripting.

- [Python for Security Professionals](https://www.cybrary.it/course/python)
This course will take you from basic concepts to advanced scripts in just over 10 hours of material, with a focus on networking and security.

- [Metasploit](https://www.cybrary.it/course/metasploit)
This free Metasploit training class will teach you to utilize the deep capabilities of Metasploit for penetration testing and help you to prepare to run vulnerability assessments for organizations of any size.

- [ISC2 CCSP - Certified Cloud Security Professional](https://www.cybrary.it/course/isc2-certified-cloud-security-professional-ccsp)
The reality is that attackers never rest, and along with the traditional threats targeting internal networks and systems, an entirely new variety specifically targeting the cloud has emerged.

Executive

- [CISSP - Certified Information Systems Security Professional](https://www.cybrary.it/course/cissp)
Our free online CISSP (8 domains) training covers topics ranging from operations security, telecommunications, network and internet security, access control systems and methodology and business continuity planning.

- [CISM - Certified Information Security Manager](https://www.cybrary.it/course/cism)
Cybrary's Certified Information Security Manager (CISM) course is a great fit for IT professionals looking to move up in their organization and advance their careers and/or current CISMs looking to learn about the latest trends in the IT industry.

- [PMP - Project Management Professional](https://www.cybrary.it/course/project-management-professional)
Our free online PMP training course educates on how to initiate, plan and manage a project, as well as the process behind analyzing risk, monitoring and controlling project contracts and how to develop schedules and budgets.

- [CRISC - Certified in Risk and Information Systems Control](https://www.cybrary.it/course/crisc)
Certified in Risk and Information Systems Control is for IT and business professionals who develop and maintain information system controls, and whose job revolves around security operations and compliance.

- [Risk Management Framework](https://www.cybrary.it/course/risk-management-framework)
The National Institute of Standards and Technology (NIST) established the Risk Management Framework (RMF) as a set of operational and procedural standards or guidelines that a US government agency must follow to ensure the compliance of its data systems.

- [ISC2 CSSLP - Certified Secure Software Life-cycle Professional](https://www.cybrary.it/course/csslp-training)
This course helps professionals in the industry build their credentials to advance within their organization, allowing them to learn valuable managerial skills as well as how to apply the best practices to keep organizations systems running well.

- [COBIT - Control Objectives for Information and Related Technologies](https://www.cybrary.it/course/cobit)
Cybrary’s online COBIT certification program offers an opportunity to learn about all the components of the COBIT 5 framework, covering everything from the business end-to-end to strategies in how effectively managing and governing enterprise IT.

- [Corporate Cybersecurity Management](https://www.cybrary.it/course/corporate-cybersecurity-management)
Cyber risk, legal considerations and insurance are often overlooked by businesses and this sets them up for major financial devastation should an incident occur.

Laboratories
============

Syracuse University's SEED

Hands-on Labs for Security Education

Started in 2002, funded by a total of 1.3 million dollars from NSF, and now used by hundreds of educational institutes worldwide, the SEED project's objective is to develop hands-on laboratory exercises (called SEED labs) for computer and information security education and help instructors adopt these labs in their curricula.

Software Security Labs

These labs cover some of the most common vulnerabilities in general software. The labs show students how attacks work in exploiting these vulnerabilities.

- [Buffer-Overflow Vulnerability Lab](http://www.cis.syr.edu/~wedu/seed/Labs_12.04/Software/Buffer_Overflow)
Launching attack to exploit the buffer-overflow vulnerability using shellcode. Conducting experiments with several countermeasures.

- [Return-to-libc Attack Lab](http://www.cis.syr.edu/~wedu/seed/Labs_12.04/Software/Return_to_libc)
Using the return-to-libc technique to defeat the "non-executable stack" countermeasure of the buffer-overflow attack.

- [Environment Variable and Set-UID Lab](http://www.cis.syr.edu/~wedu/seed/Labs_12.04/Software/Environment_Variable_and_SetUID)
This is a redesign of the Set-UID lab (see below).

- [Set-UID Program Vulnerability Lab](http://www.cis.syr.edu/~wedu/seed/Labs_12.04/Software/Set-UID)
Launching attacks on privileged Set-UID root program. Risks of environment variables. Side effects of system().

- [Race-Condition Vulnerability Lab](http://www.cis.syr.edu/~wedu/seed/Labs_12.04/Software/Race_Condition)
Exploiting the race condition vulnerability in privileged program. Conducting experiments with various countermeasures.

- [Format-String Vulnerability Lab](http://www.cis.syr.edu/~wedu/seed/Labs_12.04/Software/Format_String)
Exploiting the format string vulnerability to crash a program, steal sensitive information, or modify critical data.

- [Shellshock Attack Lab](http://www.cis.syr.edu/~wedu/seed/Labs_12.04/Software/Shellshock)
Launch attack to exploit the Shellshock vulnerability that is discovered in late 2014.

Network Security Labs

These labs cover topics on network security, ranging from attacks on TCP/IP and DNS to various network security technologies (Firewall, VPN, and IPSec).

- [TCP/IP Attack Lab](http://www.cis.syr.edu/~wedu/seed/Labs_12.04/Networking/TCPIP)
Launching attacks to exploit the vulnerabilities of the TCP/IP protocol, including session hijacking, SYN flooding, TCP reset attacks, etc.

- [Heartbleed Attack Lab](http://www.cis.syr.edu/~wedu/seed/Labs_12.04/Networking/Heartbleed)

Using the heartbleed attack to steal secrets from a remote server.

- [Local DNS Attack Lab](http://www.cis.syr.edu/~wedu/seed/Labs_12.04/Networking/DNS_Local)
Using several methods to conduct DNS pharming attacks on computers in a LAN environment.

- [Remote DNS Attack
Lab](http://www.cis.syr.edu/~wedu/seed/Labs_12.04/Networking/DNS_Remote)
Using the Kaminsky method to launch DNS cache poisoning attacks on remote DNS servers.

- [Packet Sniffing and Spoofing
Lab](http://www.cis.syr.edu/~wedu/seed/Labs_12.04/Networking/Sniffing_Spoofing)
Writing programs to sniff packets sent over the local network; writing programs to spoof various types of packets.

- [Linux Firewall Exploration
Lab](http://www.cis.syr.edu/~wedu/seed/Labs_12.04/Networking/Firewall_Linux)
Writing a simple packet-filter firewall; playing with Linux's built-in firewall software and web-proxy firewall; experimenting with ways to evade firewalls.

- [Firewall-VPN Lab: Bypassing Firewalls using
VPN](http://www.cis.syr.edu/~wedu/seed/Labs_12.04/Networking/Firewall_VPN)
Implement a simple vpn program (client/server), and use it to bypass firewalls.

- [Virtual Private Network (VPN)
Lab](http://www.cis.syr.edu/~wedu/seed/Labs_12.04/Networking/VPN)
Design and implement a transport-layer VPN system for Linux, using the TUN/TAP technologies. This project requires at least a month of time to finish, so it is good for final project.

- [Minix IPSec Lab](http://www.cis.syr.edu/~wedu/seed/Labs_12.04/Networking/IPSec)
Implement the IPSec protocol in the Minix operating system and use it to set up Virtual Private Networks.

- [Minix Firewall Lab](http://www.cis.syr.edu/~wedu/seed/Labs_12.04/Networking/Firewall_Minix)
Implementing a simple firewall in Minix operating system.

Web Security Labs
These labs cover some of the most common vulnerabilities in web applications. The labs show students how attacks work in exploiting these vulnerabilities.

Elgg-Based Labs
Elgg is an open-source social-network system. We have modified it for our labs.

- [Cross-Site Scripting Attack
Lab](http://www.cis.syr.edu/~wedu/seed/Labs_12.04/Web/Web_XSS_Elgg)
Launching the cross-site scripting attack on a vulnerable web application. Conducting experiments with several countermeasures.

- [Cross-Site Request Forgery Attack Lab](http://www.cis.syr.edu/~wedu/seed/Labs_12.04/Web/Web_CSRF_Elgg)
Launching the cross-site request forgery attack on a vulnerable web application. Conducting experiments with several countermeasures.

- [Web Tracking Lab](http://www.cis.syr.edu/~wedu/seed/Labs_12.04/Web/Web_Tracking_Elgg)
Experimenting with the web tracking technology to see how users can be checked when they browse the web.

- [SQL Injection Attack Lab](http://www.cis.syr.edu/~wedu/seed/Labs_12.04/Web/Web_SQL_Injection)
Launching the SQL-injection attack on a vulnerable web application. Conducting experiments with several countermeasures.

Collabtive-Based Labs
Collabtive is an open-source web-based project management system. We have modified it for our labs.

- [Cross-site Scripting Attack Lab](http://www.cis.syr.edu/~wedu/seed/Labs/Web/XSS_Collabtive)
Launching the cross-site scripting attack on a vulnerable web application. Conducting experiments with several countermeasures.

- [Cross-site Request Forgery Attack Lab](http://www.cis.syr.edu/~wedu/seed/Labs/Web/CSRF_Collabtive)
Launching the cross-site request forgery attack on a vulnerable web application. Conducting experiments with several countermeasures.

- [SQL Injection Lab](http://www.cis.syr.edu/~wedu/seed/Labs/Web/SQL_Injection_Collabtive)
Launching the SQL-injection attack on a vulnerable web application. Conducting experiments with several countermeasures.

- [Web Browser Access Control Lab](http://www.cis.syr.edu/~wedu/seed/Labs/Web/Web_SOP_Collabtive)
Exploring browser's access control system to understand its security policies.

PhpBB-Based Labs
PhpBB is an open-source web-based message board system, allowing users to post messages. We have modified it for our labs.

- [Cross-site Scripting Attack Lab](http://www.cis.syr.edu/~wedu/seed/Labs/Attacks_XSS)
Launching the cross-site scripting attack on a vulnerable web application. Conducting experiments with several countermeasures.

- [Cross-site Request Forgery Attack Lab](http://www.cis.syr.edu/~wedu/seed/Labs/Attacks_CSRF)
Launching the cross-site request forgery attack on a vulnerable web application. Conducting experiments with several countermeasures.

- [SQL Injection Lab](http://www.cis.syr.edu/~wedu/seed/Labs/Attacks_SQL_Injection)

Launching the SQL-injection attack on a vulnerable web application. Conducting experiments with several countermeasures.

- [ClickJacking Attack Lab](http://www.cis.syr.edu/~wedu/seed/Labs/Vulnerability/ClickJacking)
Launching the ClickJacking attack on a vulnerable web site. Conducting experiments with several countermeasures.

System Security Labs
These labs cover the security mechanisms in operating system, mostly focusing on access control mechanisms in Linux.

- [Linux Capability Exploration
Lab](http://www.cis.syr.edu/~wedu/seed/Labs_12.04/System/Capability_Exploration)
Exploring the POSIX 1.e capability system in Linux to see how privileges can be divided into smaller pieces to ensure the compliance with the Least Privilege principle.

- [Role-Based Access Control (RBAC)
Lab](http://www.cis.syr.edu/~wedu/seed/Labs_12.04/System/RBAC_Cap)
Designing and implementing an integrated access control system for Minix that uses both capability-based and role-based access control mechanisms. Students need to modify the Minix kernel.

- [Encrypted File System Lab](http://www.cis.syr.edu/~wedu/seed/Labs_12.04/System/EFS)
Designing and implementing an encrypted file system for Minix. Students need to modify the Minix kernel.

Cryptography Labs
These labs cover three essential concepts in cryptography, including secrete-key encryption, one-way hash function, and public-key encryption and PKI.

- [Secret Key Encryption
Lab](http://www.cis.syr.edu/~wedu/seed/Labs_12.04/Crypto/Crypto_Encryption)
Exploring the secret-key encryption and its applications using OpenSSL.

- [One-Way Hash Function
Lab](http://www.cis.syr.edu/~wedu/seed/Labs_12.04/Crypto/Crypto_Hash)
Exploring one-way hash function and its applications using OpenSSL.

- [Public-Key Cryptography and PKI
Lab](http://www.cis.syr.edu/~wedu/seed/Labs_12.04/Crypto/Crypto_PublicKey)
Exploring public-key cryptography, digital signature, certificate, and PKI using OpenSSL.

Mobile Security Labs
These labs focus on the smartphone security, covering the most common vulnerabilities and attacks on mobile devices. An Android VM is provided for these labs.

- [Android Repackaging
Lab](http://www.cis.syr.edu/~wedu/seed/Labs_Android5.1/Android_Repackaging)
Insert malicious code inside an existing Android app, and repackage it.

- [Android Device Rooting Lab](http://www.cis.syr.edu/~wedu/seed/Labs_Android5.1/Android_Rooting)
Develop an OTA (Over-The-Air) package from scratch to root an Android device.

Pentester Lab
There is only one way to properly learn web penetration testing: by getting your hands dirty. We teach how to manually find and exploit vulnerabilities. You will understand the root cause of the problems and the methods that can be used to exploit them. Our exercises are based on common vulnerabilities found in different systems. The issues are not emulated. We provide you real systems with real vulnerabilities.

- [From SQL Injection to Shell](https://pentesterlab.com/exercises/from_sqli_to_shell)
This exercise explains how you can, from a SQL injection, gain access to the administration console. Then in the administration console, how you can run commands on the system.

- [From SQL Injection to Shell II](https://pentesterlab.com/exercises/from_sqli_to_shell_II)
This exercise explains how you can, from a blind SQL injection, gain access to the administration console. Then in the administration console, how you can run commands on the system.

- [From SQL Injection to Shell: PostgreSQL edition](https://pentesterlab.com/exercises/from_sqli_to_shell_pg_edition)
This exercise explains how you can from a SQL injection gain access to the administration console. Then in the administration console, how you can run commands on the system.

- [Web for Pentester](https://pentesterlab.com/exercises/web_for_pentester)
This exercise is a set of the most common web vulnerabilities.

- [Web for Pentester II](https://pentesterlab.com/exercises/web_for_pentester_II)
This exercise is a set of the most common web vulnerabilities.

- [PHP Include And Post Exploitation](https://pentesterlab.com/exercises/php_include_and_post_exploitation)
This exercice describes the exploitation of a local file include with limited access. Once code execution is gained, you will see some post exploitation tricks.

- [Linux Host Review](https://pentesterlab.com/exercises/linux_host_review)
This exercice explains how to perform a Linux host review, what and how you can check the configuration of a Linux server to ensure it is securely configured. The reviewed system is a traditional Linux-Apache-Mysql-PHP (LAMP) server used to host a blog.

- [Electronic Code Book](https://pentesterlab.com/exercises/ecb)
This exercise explains how you can tamper with an encrypted cookies to access another user's account.

- [Rack Cookies and Commands injection](https://pentesterlab.com/exercises/rack_cookies_and_commands_injection)
After a short brute force introduction, this exercice explains the tampering of rack cookie and how you can even manage to modify a signed cookie (if the secret is trivial). Using this issue, you will be able to escalate your privileges and gain commands execution.

- [Padding Oracle](https://pentesterlab.com/exercises/padding_oracle)
This course details the exploitation of a weakness in the authentication of a PHP website. The website uses Cipher Block Chaining (CBC) to encrypt information provided by users and use this information to ensure authentication. The application also leaks if the padding is valid when decrypting the information. We will see how this behavior can impact the authentication and how it can be exploited.

- [XSS and MySQL FILE](https://pentesterlab.com/exercises/xss_and_mysql_file)
This exercise explains how you can use a Cross-Site Scripting vulnerability to get access to an administrator's cookies. Then how you can use his/her session to gain access to the administration to find a SQL injection and gain code execution using it.

- [Axis2 Web service and Tomcat Manager](https://pentesterlab.com/exercises/axis2_and_tomcat_manager)
This exercice explains the interactions between Tomcat and Apache, then it will show you how to call and attack an Axis2 Web service. Using information retrieved from this attack, you will be able to gain access to the Tomcat Manager and deploy a WebShell to gain commands execution.

- [Play Session Injection](https://pentesterlab.com/exercises/play_session_injection)
This exercise covers the exploitation of a session injection in the Play framework. This issue can be used to tamper with the content of the session while bypassing the signing mechanism.

- [Play XML Entities](https://pentesterlab.com/exercises/play_xxe)
This exercise covers the exploitation of a XML entities in the Play framework.

- [CVE-2007-1860: mod_jk double-decoding](https://pentesterlab.com/exercises/cve-2007-1860)
This exercise covers the exploitation of CVE-2007-1860. This vulnerability allows an attacker to gain access to unaccessible pages using crafted requests. This is a common trick that a lot of testers miss.

- [CVE-2008-1930: Wordpress 2.5 Cookie Integrity Protection Vulnerability](https://pentesterlab.com/exercises/cve-2008-1930)
This exercise explains how you can exploit CVE-2008-1930 to gain access to the administration interface of a Wordpress installation.

- [CVE-2012-1823: PHP CGI](https://pentesterlab.com/exercises/cve-2012-1823)
This exercise explains how you can exploit CVE-2012-1823 to retrieve the source code of an application and gain code execution.

- [CVE-2012-2661: ActiveRecord SQL injection](https://pentesterlab.com/exercises/cve-2012-2661)
This exercise explains how you can exploit CVE-2012-2661 to retrieve information from a database.

- [CVE-2012-6081: MoinMoin code execution](https://pentesterlab.com/exercises/cve-2012-6081)
This exercise explains how you can exploit CVE-2012-6081 to gain code execution. This vulnerability was exploited to compromise Debian's wiki and Python documentation website.

- [CVE-2014-6271/Shellshock](https://pentesterlab.com/exercises/cve-2014-6271)
This exercise covers the exploitation of a Bash vulnerability through a CGI.

Dr. Thorsten Schneider's Binary Auditing
Learn the fundamentals of Binary Auditing. Know how HLL mapping works, get more inner file understanding than ever. Learn how to find and analyse software vulnerability. Dig inside Buffer Overflows and learn how exploits can be prevented. Start to analyse your first viruses and malware the safe way. Learn about simple tricks and how viruses look like using real life examples.

- [Binary Auditing](http://www.binary-auditing.com/)

Damn Vulnerable Web Application (DVWA)
Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

- [Damn Vulnerable Web Application (DVWA)](https://github.com/ethicalhack3r/DVWA)

Damn Vulnerable Web Services
Damn Vulnerable Web Services is an insecure web application with multiple vulnerable web service components that can be used to learn real world web service vulnerabilities. The aim of this project is to help security professionals learn about Web Application Security through the use of a practical lab environment.

- [Damn Vulnerable Web Services](https://github.com/snoopysecurity/dvws)

NOWASP (Mutillidae)
OWASP Mutillidae II is a free, open source, deliberately vulnerable web-application providing a target for web-security enthusiest. With dozens of vulns and hints to help the user; this is an easy-to-use web hacking environment designed for labs, security enthusiast, classrooms, CTF, and vulnerability assessment tool targets. Mutillidae has been used in graduate security courses, corporate web sec training courses, and as an "assess the assessor" target for vulnerability assessment software.

- [OWASP Mutillidae](http://sourceforge.net/projects/mutillidae/files/)

OWASP Broken Web Applications Project
Open Web Application Security Project (OWASP) Broken Web Applications Project, a collection of vulnerable web applications that is distributed on a Virtual Machine in VMware format compatible with their no-cost and commercial VMware products.

- [OWASP Broken Web Applications Project](https://sourceforge.net/projects/owaspbwa/files/1.2/)

OWASP Bricks
Bricks is a web application security learning platform built on PHP and MySQL. The project focuses on variations of commonly seen application security issues. Each 'Brick' has some sort of security issue which can be leveraged manually or using automated software tools. The mission is to 'Break the Bricks' and thus learn the various aspects of web application security.

- [OWASP Bricks](http://sechow.com/bricks/download.html)

OWASP Hackademic Challenges Project
The Hackademic Challenges implement realistic scenarios with known vulnerabilities in a safe and controllable environment. Users can attempt to discover and exploit these vulnerabilities in order to learn important concepts of information security through an attacker's perspective.

- [OWASP Hackademic Challenges project](https://github.com/Hackademic/hackademic/)

Web Attack and Exploitation Distro (WAED)
The Web Attack and Exploitation Distro (WAED) is a lightweight virtual machine based on Debian Distribution. WAED is pre-configured with various real-world vulnerable web applications in a sandboxed environment. It includes pentesting tools that aid in finding web application vulnerabilities. The main motivation behind this project is to provide a practical environment to learn about web application's vulnerabilities without the hassle of dealing with complex configurations. Currently, there are around 18 vulnerable applications installed in WAED.

- [Web Attack and Exploitation Distro (WAED)](http://www.waed.info/)

Xtreme Vulnerable Web Application (XVWA)
XVWA is a badly coded web application written in PHP/MySQL that helps security enthusiasts to learn application security. It’s not advisable to host this application online as it is designed to be “Xtremely Vulnerable”. We recommend hosting this application in local/controlled environment and sharpening your application security ninja skills with any tools of your own choice. It’s totally legal to break or hack into this. The idea is to evangelize web application security to the community in possibly the easiest and fundamental way. Learn and acquire these skills for good purpose. How you use these skills and knowledge base is not our responsibility.

- [Xtreme Vulnerable Web Application (XVWA)](https://github.com/s4n7h0/xvwa)

WebGoat: A deliberately insecure Web Application
WebGoat is a deliberately insecure web application maintained by OWASP designed to teach web application security lessons.

- [WebGoat](https://github.com/WebGoat/WebGoat)

Audi-1's SQLi-LABS
SQLi-LABS is a comprehensive test bed to Learn and understand nitti gritty of SQL injections and thereby helps professionals understand how to protect.
- [SQLi-LABS](https://github.com/Audi-1/sqli-labs)
- [SQLi-LABS Videos](http://www.securitytube.net/user/Audi)

Capture the Flag
==========

Hack The Box

This pentester training platform/lab is full of machines (boxes) to hack on the different difficulty level. Majority of the content generated by the community and released on the website after the staff's

approval. Besides boxes users also can pick static challenges or work on advanced tasks like Fortress or Endgame.

- [Hack The Box link](https://www.hackthebox.eu/)

Vulnhub
We all learn in different ways: in a group, by yourself, reading books, watching/listening to other people, making notes or things out for yourself. Learning the basics & understanding them is essential; this knowledge can be enforced by then putting it into practice.

Over the years people have been creating these resources and a lot of time has been put into them, creating 'hidden gems' of training material. However, unless you know of them, its hard to discover them.

So VulnHub was born to cover as many as possible, creating a catalogue of 'stuff' that is (legally) 'breakable, hackable & exploitable' - allowing you to learn in a safe environment and practice 'stuff' out. When something is added to VulnHub's database it will be indexed as best as possible, to try and give you the best match possible for what you're wishing to learn or experiment with.

- [Vulnhub Repository](https://www.vulnhub.com/)

CTF Write Ups
- [CTF Resources](https://ctfs.github.io/resources)
  A general collection of information, tools, and tips regarding CTFs and similar security competitions.

- [CTF write-ups 2016](https://github.com/ctfs/write-ups-2016)
Wiki-like CTF write-ups repository, maintained by the community. (2015)

- [CTF write-ups 2015](https://github.com/ctfs/write-ups-2015)
Wiki-like CTF write-ups repository, maintained by the community. (2015)

- [CTF write-ups 2014](https://github.com/ctfs/write-ups-2014)
Wiki-like CTF write-ups repository, maintained by the community. (2014)

- [CTF write-ups 2013](https://github.com/ctfs/write-ups-2013)
Wiki-like CTF write-ups repository, maintained by the community. (2013)

CTF Repos

- [captf](http://captf.com)
This site is primarily the work of psifertex since he needed a dump site for a variety of CTF material and since many other public sites documenting the art and sport of Hacking Capture the Flag events have come and gone over the years.

- [shell-storm](http://shell-storm.org/repo/CTF)
The Jonathan Salwan's little corner.

SecurityTube Playlists

==========

Security Tube hosts a large range of video tutorials on IT security including penetration testing , exploit development and reverse engineering.

* [SecurityTube Metasploit Framework Expert (SMFE)](http://www.securitytube.net/groups?operation=view&groupId=10)
This video series covers basics of Metasploit Framework. We will look at why to use metasploit then go on to how to exploit vulnerbilities with help of metasploit and post exploitation techniques with meterpreter.

* [Wireless LAN Security and Penetration Testing Megaprimer](http://www.securitytube.net/groups?operation=view&groupId=9)
This video series will take you through a journey in wireless LAN (in)security and penetration testing. We will start from the very basics of how WLANs work, graduate to packet sniffing and injection attacks, move on to audit infrastructure vulnerabilities, learn to break into WLAN clients and finally look at advanced hybrid attacks involving wireless and applications.

* [Exploit Research Megaprimer](http://www.securitytube.net/groups?operation=view&groupId=7)
In this video series, we will learn how to program exploits for various vulnerabilities published online. We will also look at how to use various tools and techniques to find Zero Day vulnerabilities in both open and closed source software.

* [Buffer Overflow Exploitation Megaprimer for Linux](http://www.securitytube.net/groups?operation=view&groupId=4)
In this video series, we will understand the basic of buffer overflows and understand how to exploit them on linux based systems. In later videos, we will also look at how to apply the same principles to Windows and other selected operating systems.

Open Security Books
==========

Crypto 101 - lvh
Comes with everything you need to understand complete systems such as SSL/TLS: block ciphers, stream ciphers, hash functions, message authentication codes, public key encryption, key agreement protocols, and signature algorithms. Learn how to exploit common cryptographic flaws, armed with nothing but a little time and your favorite programming language. Forge administrator cookies, recover passwords, and even backdoor your own random number generator.

- [Crypto101](https://www.crypto101.io/)
- [LaTeX Source](https://github.com/crypto101/book)

A Graduate Course in Applied Cryptography - Dan Boneh & Victor Shoup
This book is about constructing practical cruptosystems for which we can argue security under plausible assumptions. The book covers many constructions for different tasks in cryptography. For each task we define the required goal. To analyze the constructions, we develop a unified framework for doing cryptographic proofs. A reader who masters this framework will capable of applying it to new constructions that may not be covered in this book. We describe common mistakes to avoid as well as

attacks on real-world systems that illustratre the importance of rigor in cryptography. We end every chapter with a fund application that applies the ideas in the chapter in some unexpected way.

- [A Graduate Course in Applied Cryptography](https://crypto.stanford.edu/~dabo/cryptobook/)

Security Engineering, A Guide to Building Dependable Distributed Systems - Ross Anderson
The world has changed radically since the first edition of this book was published in 2001. Spammers, virus writers, phishermen, money launderers, and spies now trade busily with each other in a lively online criminal economy and as they specialize, they get better. In this indispensable, fully updated guide, Ross Anderson reveals how to build systems that stay dependable whether faced with error or malice. Here?s straight talk on critical topics such as technical engineering basics, types of attack, specialized protection mechanisms, security psychology, policy, and more.

- [Security Engineering, Second Edition](https://www.cl.cam.ac.uk/~rja14/book.html)

Reverse Engineering for Beginners - Dennis Yurichev
This book offers a primer on reverse-engineering, delving into disassembly code-level reverse engineering and explaining how to decipher assembly language for those beginners who would like to learn to understand x86 (which accounts for almost all executable software in the world) and ARM code created by C/C++ compilers.

- [Reverse Engineering for Beginners](http://beginners.re/)
- [LaTeX Source](https://github.com/dennis714/RE-for-beginners)

CTF Field Guide - Trail of Bits
The focus areas that CTF competitions tend to measure are vulnerability discovery, exploit creation, toolkit creation, and operational tradecraft.. Whether you want to succeed at CTF, or as a computer security professional, you'll need to become an expert in at least one of these disciplines. Ideally in all of them.

- [CTF Field Guide](https://trailofbits.github.io/ctf/)
- [Markdown Source](https://github.com/trailofbits/ctf)

Challenges

- [Reverse Engineering Challenges](https://challenges.re/)

- [Matasano Crypto Challenges](http://cryptopals.com/)

Documentation

OWASP - Open Web Application Security Project
The Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software. Our mission is to make software security visible, so that individuals and organizations worldwide can make informed decisions about true software security risks.

- [Open Web Application Security Project](https://www.owasp.org/index.php/Main_Page)

Applied Crypto Hardening - bettercrypto.org
This guide arose out of the need for system administrators to have an updated, solid, well re-searched and thought-through guide for configuring SSL, PGP,SSH and other cryptographic tools in the post-Snowdenage. Triggered by the NSA leaks in the summer of 2013, many system administrators and IT security officers saw the need to strengthen their encryption settings.This guide is specifically written for these system administrators.

- [Applied Crypto Hardening](https://bettercrypto.org/static/applied-crypto-hardening.pdf)
- [LaTeX Source](https://github.com/BetterCrypto/Applied-Crypto-Hardening)

PTES - Penetration Testing Execution Standard
The penetration testing execution standard cover everything related to a penetration test - from the initial communication and reasoning behind a pentest, through the intelligence gathering and threat modeling phases where testers are working behind the scenes in order to get a better understanding of the tested organization, through vulnerability research, exploitation and post exploitation, where the technical security expertise of the testers come to play and combine with the business understanding of the engagement, and finally to the reporting, which captures the entire process, in a manner that makes sense to the customer and provides the most value to it.

- [Penetration Testing Execution Standard](http://www.pentest-standard.org/index.php/Main_Page)

Related Awesome Lists

- [Awesome Pentest](https://github.com/enaqx/awesome-pentest)
A collection of awesome penetration testing resources, tools and other shiny things.

- [Awesome Appsec](https://github.com/paragonie/awesome-appsec)
A curated list of resources for learning about application security.

- [Awesome Malware Analysis](https://github.com/rshipp/awesome-malware-analysis)
A curated list of awesome malware analysis tools and resources.

- [Android Security Awesome](https://github.com/ashishb/android-security-awesome)
A collection of android security related resources.

- [Awesome CTF](https://github.com/apsdehal/awesome-ctf)
A curated list of CTF frameworks, libraries, resources and softwares.

- [Awesome Security](https://github.com/sbilly/awesome-security)
A collection of awesome software, libraries, documents, books, resources and cools stuffs about security.

- [Awesome Honeypots](https://github.com/paralax/awesome-honeypots)

A curated list of awesome honeypots, tools, components and much more.

- [Awesome Incident Response](https://github.com/meirwah/awesome-incident-response)
A curated list of tools and resources for security incident response, aimed to help security analysts and DFIR teams.

- [Awesome Threat Intelligence](https://github.com/hslatman/awesome-threat-intelligence)
A curated list of awesome Threat Intelligence resources.

- [Awesome PCAP Tools](https://github.com/caesar0301/awesome-pcaptools)
A collection of tools developed by other researchers in the Computer Science area to process network traces.

- [Awesome Forensics](https://github.com/Cugu/awesome-forensics)
A curated list of awesome forensic analysis tools and resources.

- [Awesome Hacking](https://github.com/carpedm20/awesome-hacking)
A curated list of awesome Hacking tutorials, tools and resources.

- [Awesome Industrial Control System Security](https://github.com/hslatman/awesome-industrial-control-system-security)
A curated list of resources related to Industrial Control System (ICS) security.

- [Awesome Web Hacking](https://github.com/infoslack/awesome-web-hacking)
This list is for anyone wishing to learn about web application security but do not have a starting point.

- [Awesome Sec Talks](https://github.com/PaulSec/awesome-sec-talks)
A curated list of awesome Security talks.

- [Awesome YARA](https://github.com/InQuest/awesome-yara)
A curated list of awesome YARA rules, tools, and people.

- [Sec Lists](https://github.com/danielmiessler/SecLists)
SecLists is the security tester's companion. It is a collection of multiple types of lists used during security assessments. List types include usernames, passwords, URLs, sensitive data grep strings, fuzzing payloads, and many more.

[Contributing](https://github.com/onlurking/awesome-infosec/blob/master/contributing.md)
==========

Awesome Penetration Testing
[![Awesome](https://cdn.rawgit.com/sindresorhus/awesome/d7305f38d29fed78fa85652e3a63e154dd8e8829/media/badge.svg)](https://github.com/sindresorhus/awesome)

> A collection of awesome penetration testing resources.

[This project is supported by Netsparker Web Application Security Scanner](https://www.netsparker.com/?utm_source=github.com&utm_content=awesome+penetration+testing&utm_medium=referral&utm_campaign=generic+advert)

[Penetration testing](https://en.wikipedia.org/wiki/Penetration_test) is the practice of launching authorized, simulated attacks against computer systems and their physical infrastructure to expose potential security weaknesses and vulnerabilities.

Your contributions and suggestions are heartily ❤ welcome. (✿◕‿◕). Please check the [Contributing Guidelines](CONTRIBUTING.md) for more details.

Contents

Online Resources

Penetration Testing Resources

* [Metasploit Unleashed](https://www.offensive-security.com/metasploit-unleashed/) - Free Offensive Security Metasploit course.
* [Penetration Testing Execution Standard (PTES)](http://www.pentest-standard.org/) - Documentation designed to provide a common language and scope for performing and reporting the results of a penetration test.
* [Open Web Application Security Project (OWASP)](https://www.owasp.org/index.php/Main_Page) - Worldwide not-for-profit charitable organization focused on improving the security of especially Web-based and Application-layer software.
* [PENTEST-WIKI](https://github.com/nixawk/pentest-wiki) - Free online security knowledge library for pentesters and researchers.
* [Penetration Testing Framework (PTF)](http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html) - Outline for performing penetration tests compiled as a general framework usable by vulnerability analysts and penetration testers alike.
* [XSS-Payloads](http://www.xss-payloads.com) - Ultimate resource for all things cross-site including payloads, tools, games and documentation.
* [MITRE's Adversarial Tactics, Techniques & Common Knowledge (ATT&CK)](https://attack.mitre.org/) - Curated knowledge base and model for cyber adversary behavior.
* [InfoSec Institute](http://resources.infosecinstitute.com) - IT and security bootcamps.

Exploit Development

* [Shellcode Tutorial](http://www.vividmachines.com/shellcode/shellcode.html) - Tutorial on how to write shellcode.
* [Shellcode Examples](http://shell-storm.org/shellcode/) - Shellcodes database.
* [Exploit Writing Tutorials](https://www.corelan.be/index.php/2009/07/19/exploit-writing-tutorial-part-1-stack-based-overflows/) - Tutorials on how to develop exploits.

Open Sources Intelligence (OSINT) Resources

* [OSINT Framework](http://osintframework.com/) - Collection of various OSINT tools broken out by category.
* [Intel Techniques](https://inteltechniques.com/menu.html) - Collection of OSINT tools. Menu on the left can be used to navigate through the categories.
* [NetBootcamp OSINT Tools](http://netbootcamp.org/osinttools/) - Collection of OSINT links and custom Web interfaces to other services.
* [WiGLE.net](https://wigle.net/) - Information about wireless networks world-wide, with user-friendly desktop and web applications.
* [CertGraph](https://github.com/lanrat/certgraph) - Crawls a domain's SSL/TLS certificates for its certificate alternative names.

Social Engineering Resources

* [Social Engineering Framework](http://www.social-engineer.org/framework/general-discussion/) - Information resource for social engineers.

Lock Picking Resources

* [Schuyler Towne channel](https://www.youtube.com/user/SchuylerTowne/) - Lockpicking videos and security talks.
* [bosnianbill](https://www.youtube.com/user/bosnianbill) - More lockpicking videos.
* [/r/lockpicking](https://www.reddit.com/r/lockpicking) - Resources for learning lockpicking, equipment recommendations.

Operating Systems

* [Security related Operating Systems @ Rawsec](http://list.rawsec.ml/operating_systems.html) - Complete list of security related operating systems.
* [Security @ Distrowatch](http://distrowatch.com/search.php?category=Security) - Website dedicated to talking about, reviewing, and keeping up to date with open source operating systems.
* [cuckoo](https://github.com/cuckoosandbox/cuckoo) - Open source automated malware analysis system.
* [Digital Evidence & Forensics Toolkit (DEFT)](http://www.deftlinux.net/) - Live CD for forensic analysis runnable without tampering or corrupting connected devices where the boot process takes place.
* [SIFT](https://digital-forensics.sans.org/community/downloads) - Forensic workstation made by SANS.
* [Tails](https://tails.boum.org/) - Live OS aimed at preserving privacy and anonymity.
* [Qubes OS](https://www.qubes-os.org) - High-security Operating System providing strict application isolation.

Tools

Penetration Testing Distributions

* [Kali](https://www.kali.org/) - GNU/Linux distribution designed for digital forensics and penetration testing.
* [ArchStrike](https://archstrike.org/) - Arch GNU/Linux repository for security professionals and enthusiasts.
* [BlackArch](https://www.blackarch.org/) - Arch GNU/Linux-based distribution for penetration testers and security researchers.
* [Network Security Toolkit (NST)](http://networksecuritytoolkit.org/) - Fedora-based bootable live operating system designed to provide easy access to best-of-breed open source network security applications.
* [BackBox](https://backbox.org/) - Ubuntu-based distribution for penetration tests and security assessments.
* [Parrot](https://www.parrotsec.org/) - Distribution similar to Kali, with multiple architecture.
* [Buscador](https://inteltechniques.com/buscador/) - GNU/Linux virtual machine that is pre-configured for online investigators.
* [The Pentesters Framework](https://github.com/trustedsec/ptf) - Distro organized around the Penetration Testing Execution Standard (PTES), providing a curated collection of utilities that eliminates often unused toolchains.
* [AttifyOS](https://github.com/adi0x90/attifyos) - GNU/Linux distribution focused on tools useful during Internet of Things (IoT) security assessments.
* [PentestBox](https://pentestbox.org/) - Opensource pre-configured portable penetration testing environment for Windows OS.
* [Android Tamer](https://androidtamer.com/) - OS for Android Security Professionals. Includes all the tools required for Android security testing.

Docker for Penetration Testing

* `docker pull kalilinux/kali-linux-docker` - [Official Kali Linux](https://hub.docker.com/r/kalilinux/kali-linux-docker/).
* `docker pull owasp/zap2docker-stable` - [Official OWASP ZAP](https://github.com/zaproxy/zaproxy).
* `docker pull wpscanteam/wpscan` - [Official WPScan](https://hub.docker.com/r/wpscanteam/wpscan/).
* `docker pull citizenstig/dvwa` - [Damn Vulnerable Web Application (DVWA)](https://hub.docker.com/r/citizenstig/dvwa/).
* `docker pull wpscanteam/vulnerablewordpress` - [Vulnerable WordPress Installation](https://hub.docker.com/r/wpscanteam/vulnerablewordpress/).
* `docker pull hmlio/vaas-cve-2014-6271` - [Vulnerability as a service: Shellshock](https://hub.docker.com/r/hmlio/vaas-cve-2014-6271/).
* `docker pull hmlio/vaas-cve-2014-0160` - [Vulnerability as a service: Heartbleed](https://hub.docker.com/r/hmlio/vaas-cve-2014-0160/).
* `docker pull vulnerables/cve-2017-7494` - [Vulnerability as a service: SambaCry](https://hub.docker.com/r/vulnerables/cve-2017-7494/).
* `docker pull opendns/security-ninjas` - [Security Ninjas](https://hub.docker.com/r/opendns/security-ninjas/).

* `docker pull diogomonica/docker-bench-security` - [Docker Bench for Security](https://hub.docker.com/r/diogomonica/docker-bench-security/).
* `docker pull ismisepaul/securityshepherd` - [OWASP Security Shepherd](https://hub.docker.com/r/ismisepaul/securityshepherd/).
* `docker pull webgoat/webgoat-7.1` - [OWASP WebGoat Project 7.1 docker image](https://hub.docker.com/r/webgoat/webgoat-7.1/).
* `docker pull webgoat/webgoat-8.0` - [OWASP WebGoat Project 8.0 docker image](https://hub.docker.com/r/webgoat/webgoat-8.0/).
* `docker-compose build && docker-compose up` - [OWASP NodeGoat](https://github.com/owasp/nodegoat#option-3---run-nodegoat-on-docker).
* `docker pull citizenstig/nowasp` - [OWASP Mutillidae II Web Pen-Test Practice Application](https://hub.docker.com/r/citizenstig/nowasp/).
* `docker pull bkimminich/juice-shop` - [OWASP Juice Shop](https://github.com/bkimminich/juice-shop#docker-container--).
* `docker pull phocean/msf` - [docker-metasploit](https://hub.docker.com/r/phocean/msf/).

Multi-paradigm Frameworks

* [Metasploit](https://www.metasploit.com/) - Software for offensive security teams to help verify vulnerabilities and manage security assessments.
* [Armitage](http://fastandeasyhacking.com/) - Java-based GUI front-end for the Metasploit Framework.
* [Faraday](https://github.com/infobyte/faraday) - Multiuser integrated pentesting environment for red teams performing cooperative penetration tests, security audits, and risk assessments.
* [ExploitPack](https://github.com/juansacco/exploitpack) - Graphical tool for automating penetration tests that ships with many pre-packaged exploits.
* [Pupy](https://github.com/n1nj4sec/pupy) - Cross-platform (Windows, Linux, macOS, Android) remote administration and post-exploitation tool.
* [AutoSploit](https://github.com/NullArray/AutoSploit) - Automated mass exploiter, which collects target by employing the Shodan.io API and programmatically chooses Metasploit exploit modules based on the Shodan query.
* [Decker](https://github.com/stevenaldinger/decker) - Penetration testing orchestration and automation framework, which allows writing declarative, reusable configurations capable of ingesting variables and using outputs of tools it has run as inputs to others.

Network vulnerability scanners

* [Netsparker Application Security Scanner](https://www.netsparker.com/) - Application security scanner to automatically find security flaws.
* [Nexpose](https://www.rapid7.com/products/nexpose/) - Commercial vulnerability and risk management assessment engine that integrates with Metasploit, sold by Rapid7.
* [Nessus](https://www.tenable.com/products/nessus-vulnerability-scanner) - Commercial vulnerability management, configuration, and compliance assessment platform, sold by Tenable.
* [OpenVAS](http://www.openvas.org/) - Free software implementation of the popular Nessus vulnerability assessment system.
* [Vuls](https://github.com/future-architect/vuls) - Agentless vulnerability scanner for GNU/Linux and FreeBSD, written in Go.

Static Analyzers

* [Brakeman](https://github.com/presidentbeef/brakeman) - Static analysis security vulnerability scanner for Ruby on Rails applications.
* [cppcheck](http://cppcheck.sourceforge.net/) - Extensible C/C++ static analyzer focused on finding bugs.
* [FindBugs](http://findbugs.sourceforge.net/) - Free software static analyzer to look for bugs in Java code.
* [sobelow](https://github.com/nccgroup/sobelow) - Security-focused static analysis for the Phoenix Framework.
* [bandit](https://pypi.python.org/pypi/bandit/) - Security oriented static analyser for python code.
* [Progpilot](https://github.com/designsecurity/progpilot) - Static security analysis tool for PHP code.
* [RegEx-DoS](https://github.com/jagracey/RegEx-DoS) - Analyzes source code for Regular Expressions susceptible to Denial of Service attacks.

Web Vulnerability Scanners

* [Netsparker Application Security Scanner](https://www.netsparker.com/) - Application security scanner to automatically find security flaws.
* [Nikto](https://cirt.net/nikto2) - Noisy but fast black box web server and web application vulnerability scanner.
* [Arachni](http://www.arachni-scanner.com/) - Scriptable framework for evaluating the security of web applications.
* [w3af](https://github.com/andresriancho/w3af) - Web application attack and audit framework.
* [Wapiti](http://wapiti.sourceforge.net/) - Black box web application vulnerability scanner with built-in fuzzer.
* [SecApps](https://secapps.com/) - In-browser web application security testing suite.
* [WebReaver](https://www.webreaver.com/) - Commercial, graphical web application vulnerability scanner designed for macOS.
* [WPScan](https://wpscan.org/) - Black box WordPress vulnerability scanner.
* [cms-explorer](https://code.google.com/archive/p/cms-explorer/) - Reveal the specific modules, plugins, components and themes that various websites powered by content management systems are running.
*
[joomscan](https://www.owasp.org/index.php/Category:OWASP_Joomla_Vulnerability_Scanner_Project) - Joomla vulnerability scanner.
* [ACSTIS](https://github.com/tijme/angularjs-csti-scanner) - Automated client-side template injection (sandbox escape/bypass) detection for AngularJS.
* [SQLmate](https://github.com/UltimateHackers/sqlmate) - A friend of sqlmap that identifies sqli vulnerabilities based on a given dork and website (optional).
* [JCS](https://github.com/TheM4hd1/JCS) - Joomla Vulnerability Component Scanner with automatic database updater from exploitdb and packetstorm.

Network Tools

* [pig](https://github.com/rafael-santiago/pig) - GNU/Linux packet crafting tool.
* [Network-Tools.com](http://network-tools.com/) - Website offering an interface to numerous basic network utilities like `ping`, `traceroute`, `whois`, and more.

* [Intercepter-NG](http://sniff.su/) - Multifunctional network toolkit.
* [SPARTA](https://sparta.secforce.com/) - Graphical interface offering scriptable, configurable access to existing network infrastructure scanning and enumeration tools.
* [Zarp](https://github.com/hatRiot/zarp) - Network attack tool centered around the exploitation of local networks.
* [dsniff](https://www.monkey.org/~dugsong/dsniff/) - Collection of tools for network auditing and pentesting.
* [scapy](https://github.com/secdev/scapy) - Python-based interactive packet manipulation program & library.
* [Printer Exploitation Toolkit (PRET)](https://github.com/RUB-NDS/PRET) - Tool for printer security testing capable of IP and USB connectivity, fuzzing, and exploitation of PostScript, PJL, and PCL printer language features.
* [Praeda](http://h.foofus.net/?page_id=218) - Automated multi-function printer data harvester for gathering usable data during security assessments.
* [routersploit](https://github.com/reverse-shell/routersploit) - Open source exploitation framework similar to Metasploit but dedicated to embedded devices.
* [CrackMapExec](https://github.com/byt3bl33d3r/CrackMapExec) - Swiss army knife for pentesting networks.
* [impacket](https://github.com/CoreSecurity/impacket) - Collection of Python classes for working with network protocols.
* [dnstwist](https://github.com/elceef/dnstwist) - Domain name permutation engine for detecting typo squatting, phishing and corporate espionage.
* [THC Hydra](https://github.com/vanhauser-thc/thc-hydra) - Online password cracking tool with built-in support for many network protocols, including HTTP, SMB, FTP, telnet, ICQ, MySQL, LDAP, IMAP, VNC, and more.
* [IKEForce](https://github.com/SpiderLabs/ikeforce) - Command line IPSEC VPN brute forcing tool for Linux that allows group name/ID enumeration and XAUTH brute forcing capabilities.
* [hping3](https://github.com/antirez/hping) - Network tool able to send custom TCP/IP packets.
* [rshijack](https://github.com/kpcyrd/rshijack) - TCP connection hijacker, Rust rewrite of `shijack`.

Exfiltration Tools

* [DET](https://github.com/sensepost/DET) - Proof of concept to perform data exfiltration using either single or multiple channel(s) at the same time.
* [pwnat](https://github.com/samyk/pwnat) - Punches holes in firewalls and NATs.
* [tgcd](http://tgcd.sourceforge.net/) - Simple Unix network utility to extend the accessibility of TCP/IP based network services beyond firewalls.
* [Iodine](https://code.kryo.se/iodine/) - Tunnel IPv4 data through a DNS server; useful for exfiltration from networks where Internet access is firewalled, but DNS queries are allowed.

Network Reconnaissance Tools

* [zmap](https://zmap.io/) - Open source network scanner that enables researchers to easily perform Internet-wide network studies.
* [nmap](https://nmap.org/) - Free security scanner for network exploration & security audits.
* [scanless](https://github.com/vesche/scanless) - Utility for using websites to perform port scans on your behalf so as not to reveal your own IP.
* [DNSDumpster](https://dnsdumpster.com/) - Online DNS recon and search service.

* [CloudFail](https://github.com/m0rtem/CloudFail) - Unmask server IP addresses hidden behind Cloudflare by searching old database records and detecting misconfigured DNS.
* [dnsenum](https://github.com/fwaeytens/dnsenum/) - Perl script that enumerates DNS information from a domain, attempts zone transfers, performs a brute force dictionary style attack, and then performs reverse look-ups on the results.
* [dnsmap](https://github.com/makefu/dnsmap/) - Passive DNS network mapper.
* [dnsrecon](https://github.com/darkoperator/dnsrecon/) - DNS enumeration script.
* [dnstracer](http://www.mavetju.org/unix/dnstracer.php) - Determines where a given DNS server gets its information from, and follows the chain of DNS servers.
* [passivedns-client](https://github.com/chrislee35/passivedns-client) - Library and query tool for querying several passive DNS providers.
* [passivedns](https://github.com/gamelinux/passivedns) - Network sniffer that logs all DNS server replies for use in a passive DNS setup.
* [Mass Scan](https://github.com/robertdavidgraham/masscan) - TCP port scanner, spews SYN packets asynchronously, scanning entire Internet in under 5 minutes.
* [smbmap](https://github.com/ShawnDEvans/smbmap) - Handy SMB enumeration tool.
* [XRay](https://github.com/evilsocket/xray) - Network (sub)domain discovery and reconnaissance automation tool.
* [ACLight](https://github.com/cyberark/ACLight) - Script for advanced discovery of sensitive Privileged Accounts - includes Shadow Admins.
* [ScanCannon](https://github.com/johnnyxmas/ScanCannon) - Python script to quickly enumerate large networks by calling `masscan` to quickly identify open ports and then `nmap` to gain details on the systems/services on those ports.
* [fierce](https://github.com/mschwager/fierce) - Python3 port of the original `fierce.pl` DNS reconnaissance tool for locating non-contiguous IP space.

Protocol Analyzers and Sniffers

* [tcpdump/libpcap](http://www.tcpdump.org/) - Common packet analyzer that runs under the command line.
* [Wireshark](https://www.wireshark.org/) - Widely-used graphical, cross-platform network protocol analyzer.
* [netsniff-ng](https://github.com/netsniff-ng/netsniff-ng) - Swiss army knife for for network sniffing.
* [Dshell](https://github.com/USArmyResearchLab/Dshell) - Network forensic analysis framework.
* [Debookee](http://www.iwaxx.com/debookee/) - Simple and powerful network traffic analyzer for macOS.
* [Dripcap](https://github.com/dripcap/dripcap) - Caffeinated packet analyzer.
* [Netzob](https://github.com/netzob/netzob) - Reverse engineering, traffic generation and fuzzing of communication protocols.
* [sniffglue](https://github.com/kpcyrd/sniffglue) - Secure multithreaded packet sniffer.

Proxies and MITM Tools

* [dnschef](https://github.com/iphelix/dnschef) - Highly configurable DNS proxy for pentesters.
* [mitmproxy](https://github.com/mitmproxy/mitmproxy) - Interactive TLS-capable intercepting HTTP proxy for penetration testers and software developers.
* [Morpheus](https://github.com/r00t-3xp10it/morpheus) - Automated ettercap TCP/IP Hijacking tool.
* [mallory](https://github.com/justmao945/mallory) - HTTP/HTTPS proxy over SSH.

* [SSH MITM](https://github.com/jtesta/ssh-mitm) - Intercept SSH connections with a proxy; all plaintext passwords and sessions are logged to disk.
* [evilgrade](https://github.com/infobyte/evilgrade) - Modular framework to take advantage of poor upgrade implementations by injecting fake updates.
* [Ettercap](http://www.ettercap-project.org) - Comprehensive, mature suite for machine-in-the-middle attacks.
* [BetterCAP](https://www.bettercap.org/) - Modular, portable and easily extensible MITM framework.
* [MITMf](https://github.com/byt3bl33d3r/MITMf) - Framework for Man-In-The-Middle attacks.

Wireless Network Tools

* [Aircrack-ng](http://www.aircrack-ng.org/) - Set of tools for auditing wireless networks.
* [Kismet](https://kismetwireless.net/) - Wireless network detector, sniffer, and IDS.
* [Reaver](https://code.google.com/archive/p/reaver-wps) - Brute force attack against WiFi Protected Setup.
* [Wifite](https://github.com/derv82/wifite) - Automated wireless attack tool.
* [Fluxion](https://github.com/FluxionNetwork/fluxion) - Suite of automated social engineering based WPA attacks.
* [Airgeddon](https://github.com/v1s1t0r1sh3r3/airgeddon) - Multi-use bash script for Linux systems to audit wireless networks.
* [Cowpatty](https://github.com/joswr1ght/cowpatty) - Brute-force dictionary attack against WPA-PSK.
* [BoopSuite](https://github.com/MisterBianco/BoopSuite) - Suite of tools written in Python for wireless auditing.
* [Bully](http://git.kali.org/gitweb/?p=packages/bully.git;a=summary) - Implementation of the WPS brute force attack, written in C.
* [infernal-twin](https://github.com/entropy1337/infernal-twin) - Automated wireless hacking tool.
* [krackattacks-scripts](https://github.com/vanhoefm/krackattacks-scripts) - WPA2 Krack attack scripts.
* [KRACK Detector](https://github.com/securingsam/krackdetector) - Detect and prevent KRACK attacks in your network.
* [wifi-arsenal](https://github.com/0x90/wifi-arsenal) - Resources for Wi-Fi Pentesting.
* [WiFi-Pumpkin](https://github.com/P0cL4bs/WiFi-Pumpkin) - Framework for rogue Wi-Fi access point attack.

Transport Layer Security Tools

* [SSLyze](https://github.com/nabla-c0d3/sslyze) - Fast and comprehensive TLS/SSL configuration analyzer to help identify security mis-configurations.
* [tls_prober](https://github.com/WestpointLtd/tls_prober) - Fingerprint a server's SSL/TLS implementation.
* [testssl.sh](https://github.com/drwetter/testssl.sh) - Command line tool which checks a server's service on any port for the support of TLS/SSL ciphers, protocols as well as some cryptographic flaws.
* [crackpkcs12](https://github.com/crackpkcs12/crackpkcs12) - Multithreaded program to crack PKCS#12 files (`.p12` and `.pfx` extensions), such as TLS/SSL certificates.

Web Exploitation

* [OWASP Zed Attack Proxy (ZAP)](https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project) - Feature-rich, scriptable HTTP intercepting proxy and fuzzer for penetration testing web applications.
* [Fiddler](https://www.telerik.com/fiddler) - Free cross-platform web debugging proxy with user-friendly companion tools.
* [Burp Suite](https://portswigger.net/burp/) - Integrated platform for performing security testing of web applications.
* [autochrome](https://www.nccgroup.trust/us/about-us/newsroom-and-events/blog/2017/march/autochrome/) - Easy to install a test browser with all the appropriate setting needed for web application testing with native Burp support, from NCCGroup.
* [Browser Exploitation Framework (BeEF)](https://github.com/beefproject/beef) - Command and control server for delivering exploits to commandeered Web browsers.
* [Offensive Web Testing Framework (OWTF)](https://www.owasp.org/index.php/OWASP_OWTF) - Python-based framework for pentesting Web applications based on the OWASP Testing Guide.
* [Wordpress Exploit Framework](https://github.com/rastating/wordpress-exploit-framework) - Ruby framework for developing and using modules which aid in the penetration testing of WordPress powered websites and systems.
* [WPSploit](https://github.com/espreto/wpsploit) - Exploit WordPress-powered websites with Metasploit.
* [SQLmap](http://sqlmap.org/) - Automatic SQL injection and database takeover tool.
* [tplmap](https://github.com/epinna/tplmap) - Automatic server-side template injection and Web server takeover tool.
* [weevely3](https://github.com/epinna/weevely3) - Weaponized web shell.
* [Wappalyzer](https://www.wappalyzer.com/) - Wappalyzer uncovers the technologies used on websites.
* [WhatWeb](https://github.com/urbanadventurer/WhatWeb) - Website fingerprinter.
* [BlindElephant](http://blindelephant.sourceforge.net/) - Web application fingerprinter.
* [wafw00f](https://github.com/EnableSecurity/wafw00f) - Identifies and fingerprints Web Application Firewall (WAF) products.
* [fimap](https://github.com/kurobeats/fimap) - Find, prepare, audit, exploit and even Google automatically for LFI/RFI bugs.
* [Kadabra](https://github.com/D35m0nd142/Kadabra) - Automatic LFI exploiter and scanner.
* [Kadimus](https://github.com/P0cL4bs/Kadimus) - LFI scan and exploit tool.
* [liffy](https://github.com/hvqzao/liffy) - LFI exploitation tool.
* [Commix](https://github.com/commixproject/commix) - Automated all-in-one operating system command injection and exploitation tool.
* [DVCS Ripper](https://github.com/kost/dvcs-ripper) - Rip web accessible (distributed) version control systems: SVN/GIT/HG/BZR.
* [GitTools](https://github.com/internetwache/GitTools) - Automatically find and download Web-accessible `.git` repositories.
* [sslstrip](https://www.thoughtcrime.org/software/sslstrip/) - Demonstration of the HTTPS stripping attacks.
* [sslstrip2](https://github.com/LeonardoNve/sslstrip2) - SSLStrip version to defeat HSTS.
* [NoSQLmap](https://github.com/codingo/NoSQLMap) - Automatic NoSQL injection and database takeover tool.
* [VHostScan](https://github.com/codingo/VHostScan) - A virtual host scanner that performs reverse lookups, can be used with pivot tools, detect catch-all scenarios, aliases and dynamic default pages.

* [FuzzDB](https://github.com/fuzzdb-project/fuzzdb) - Dictionary of attack patterns and primitives for black-box application fault injection and resource discovery.
* [EyeWitness](https://github.com/ChrisTruncer/EyeWitness) - Tool to take screenshots of websites, provide some server header info, and identify default credentials if possible.
* [webscreenshot](https://github.com/maaaaz/webscreenshot) - A simple script to take screenshots of list of websites.
* [recursebuster](https://github.com/c-sto/recursebuster) - Content discovery tool to perform directory and file bruteforcing.
* [Raccoon](https://github.com/evyatarmeged/Raccoon) - High performance offensive security tool for reconnaissance and vulnerability scanning.
* [WhatWaf](https://github.com/Ekultek/WhatWaf) - Detect and bypass web application firewalls and protection systems.
* [badtouch](https://github.com/kpcyrd/badtouch) - Scriptable network authentication cracker.

Hex Editors

* [HexEdit.js](https://hexed.it) - Browser-based hex editing.
* [Hexinator](https://hexinator.com/) - World's finest (proprietary, commercial) Hex Editor.
* [Frhed](http://frhed.sourceforge.net/) - Binary file editor for Windows.
* [0xED](http://www.suavetech.com/0xed/0xed.html) - Native macOS hex editor that supports plug-ins to display custom data types.
* [Hex Fiend](http://ridiculousfish.com/hexfiend/) - Fast, open source, hex editor for macOS with support for viewing binary diffs.
* [Bless](https://github.com/bwrsandman/Bless) - High quality, full featured, cross-platform graphical hex editor written in Gtk#.
* [wxHexEditor](http://www.wxhexeditor.org/) - Free GUI hex editor for GNU/Linux, macOS, and Windows.
* [`hexedit`](https://github.com/pixel/hexedit) - Simple, fast, console-based hex editor.

File Format Analysis Tools

* [Kaitai Struct](http://kaitai.io/) - File formats and network protocols dissection language and web IDE, generating parsers in C++, C#, Java, JavaScript, Perl, PHP, Python, Ruby.
* [Veles](https://codisec.com/veles/) - Binary data visualization and analysis tool.
* [Hachoir](https://hachoir.readthedocs.io/) - Python library to view and edit a binary stream as tree of fields and tools for metadata extraction.

Anti-virus Evasion Tools

* [Veil](https://www.veil-framework.com/) - Generate metasploit payloads that bypass common anti-virus solutions.
* [shellsploit](https://github.com/Exploit-install/shellsploit-framework) - Generates custom shellcode, backdoors, injectors, optionally obfuscates every byte via encoders.
* [Hyperion](http://nullsecurity.net/tools/binary.html) - Runtime encryptor for 32-bit portable executables ("PE `.exe`s").
* [AntiVirus Evasion Tool (AVET)](https://github.com/govolution/avet) - Post-process exploits containing executable files targeted for Windows machines to avoid being recognized by antivirus software.

* [peCloak.py](https://www.securitysift.com/pecloak-py-an-experiment-in-av-evasion/) - Automates the process of hiding a malicious Windows executable from antivirus (AV) detection.
* [peCloakCapstone](https://github.com/v-p-b/peCloakCapstone) - Multi-platform fork of the peCloak.py automated malware antivirus evasion tool.
* [UniByAv](https://github.com/Mr-Un1k0d3r/UniByAv) - Simple obfuscator that takes raw shellcode and generates Anti-Virus friendly executables by using a brute-forcable, 32-bit XOR key.
* [Shellter](https://www.shellterproject.com/) - Dynamic shellcode injection tool, and the first truly dynamic PE infector ever created.

Hash Cracking Tools

* [John the Ripper](http://www.openwall.com/john/) - Fast password cracker.
* [Hashcat](http://hashcat.net/hashcat/) - The more fast hash cracker.
* [CeWL](https://digi.ninja/projects/cewl.php) - Generates custom wordlists by spidering a target's website and collecting unique words.
* [JWT Cracker](https://github.com/lmammino/jwt-cracker) - Simple HS256 JWT token brute force cracker.
* [Rar Crack](http://rarcrack.sourceforge.net) - RAR bruteforce cracker.
* [BruteForce Wallet](https://github.com/glv2/bruteforce-wallet) - Find the password of an encrypted wallet file (i.e. `wallet.dat`).
* [StegCracker](https://github.com/Paradoxis/StegCracker) - Steganography brute-force utility to uncover hidden data inside files.

Windows Utilities

* [Sysinternals Suite](https://technet.microsoft.com/en-us/sysinternals/bb842062) - The Sysinternals Troubleshooting Utilities.
* [Windows Credentials Editor](https://www.ampliasecurity.com/research/windows-credentials-editor/) - Inspect logon sessions and add, change, list, and delete associated credentials, including Kerberos tickets.
* [mimikatz](http://blog.gentilkiwi.com/mimikatz) - Credentials extraction tool for Windows operating system.
* [PowerSploit](https://github.com/PowerShellMafia/PowerSploit) - PowerShell Post-Exploitation Framework.
* [Windows Exploit Suggester](https://github.com/GDSSecurity/Windows-Exploit-Suggester) - Detects potential missing patches on the target.
* [Responder](https://github.com/SpiderLabs/Responder) - Link-Local Multicast Name Resolution (LLMNR), NBT-NS, and mDNS poisoner.
* [Bloodhound](https://github.com/adaptivethreat/Bloodhound/wiki) - Graphical Active Directory trust relationship explorer.
* [Empire](https://www.powershellempire.com/) - Pure PowerShell post-exploitation agent.
* [Fibratus](https://github.com/rabbitstack/fibratus) - Tool for exploration and tracing of the Windows kernel.
* [wePWNise](https://labs.mwrinfosecurity.com/tools/wepwnise/) - Generates architecture independent VBA code to be used in Office documents or templates and automates bypassing application control and exploit mitigation software.
* [redsnarf](https://github.com/nccgroup/redsnarf) - Post-exploitation tool for retrieving password hashes and credentials from Windows workstations, servers, and domain controllers.

* [Magic Unicorn](https://github.com/trustedsec/unicorn) - Shellcode generator for numerous attack vectors, including Microsoft Office macros, PowerShell, HTML applications (HTA), or `certutil` (using fake certificates).
* [DeathStar](https://github.com/byt3bl33d3r/DeathStar) - Python script that uses Empire's RESTful API to automate gaining Domain Admin rights in Active Directory environments.
* [RID_ENUM](https://github.com/trustedsec/ridenum) - Python script that can enumerate all users from a Windows Domain Controller and crack those user's passwords using brute-force.
* [MailSniper](https://github.com/dafthack/MailSniper) - Modular tool for searching through email in a Microsoft Exchange environment, gathering the Global Address List from Outlook Web Access (OWA) and Exchange Web Services (EWS), and more.
* [Ruler](https://github.com/sensepost/ruler) - Abuses client-side Outlook features to gain a remote shell on a Microsoft Exchange server.
* [SCOMDecrypt](https://github.com/nccgroup/SCOMDecrypt) - Retrieve and decrypt RunAs credentials stored within Microsoft System Center Operations Manager (SCOM) databases.
* [LaZagne](https://github.com/AlessandroZ/LaZagne) - Credentials recovery project.
* [Active Directory and Privilege Escalation (ADAPE)](https://github.com/hausec/ADAPE-Script) - Umbrella script that automates numerous useful PowerShell modules to discover security misconfigurations and attempt privilege escalation against Active Directory.

GNU/Linux Utilities

* [Linux Exploit Suggester](https://github.com/PenturaLabs/Linux_Exploit_Suggester) - Heuristic reporting on potentially viable exploits for a given GNU/Linux system.
* [Lynis](https://cisofy.com/lynis/) - Auditing tool for UNIX-based systems.
* [unix-privesc-check](https://github.com/pentestmonkey/unix-privesc-check) - Shell script to check for simple privilege escalation vectors on UNIX systems.
* [Hwacha](https://github.com/n00py/Hwacha) - Post-exploitation tool to quickly execute payloads via SSH on one or more Linux systems simultaneously.

macOS Utilities

* [Bella](https://github.com/kdaoudieh/Bella) - Pure Python post-exploitation data mining and remote administration tool for macOS.
* [EvilOSX](https://github.com/Marten4n6/EvilOSX) - Modular RAT that uses numerous evasion and exfiltration techniques out-of-the-box.

DDoS Tools

* [LOIC](https://github.com/NewEraCracker/LOIC/) - Open source network stress tool for Windows.
* [JS LOIC](http://metacortexsecurity.com/tools/anon/LOIC/LOICv1.html) - JavaScript in-browser version of LOIC.
* [SlowLoris](https://github.com/gkbrk/slowloris) - DoS tool that uses low bandwidth on the attacking side.
* [HOIC](https://sourceforge.net/projects/high-orbit-ion-cannon/) - Updated version of Low Orbit Ion Cannon, has 'boosters' to get around common counter measures.
* [T50](https://gitlab.com/fredericopissarra/t50/) - Faster network stress tool.

* [UFONet](https://github.com/epsylon/ufonet) - Abuses OSI layer 7 HTTP to create/manage 'zombies' and to conduct different attacks using; `GET`/`POST`, multithreading, proxies, origin spoofing methods, cache evasion techniques, etc.
* [Memcrashed](https://github.com/649/Memcrashed-DDoS-Exploit) - DDoS attack tool for sending forged UDP packets to vulnerable Memcached servers obtained using Shodan API.

Social Engineering Tools

* [Social Engineer Toolkit (SET)](https://github.com/trustedsec/social-engineer-toolkit) - Open source pentesting framework designed for social engineering featuring a number of custom attack vectors to make believable attacks quickly.
* [King Phisher](https://github.com/securestate/king-phisher) - Phishing campaign toolkit used for creating and managing multiple simultaneous phishing attacks with custom email and server content.
* [Evilginx](https://github.com/kgretzky/evilginx) - MITM attack framework used for phishing credentials and session cookies from any Web service.
* [Evilginx2](https://github.com/kgretzky/evilginx2) - Standalone man-in-the-middle attack framework.
* [wifiphisher](https://github.com/sophron/wifiphisher) - Automated phishing attacks against WiFi networks.
* [Catphish](https://github.com/ring0lab/catphish) - Tool for phishing and corporate espionage written in Ruby.
* [Beelogger](https://github.com/4w4k3/BeeLogger) - Tool for generating keylooger.
* [FiercePhish](https://github.com/Raikia/FiercePhish) - Full-fledged phishing framework to manage all phishing engagements.
* [SocialFish](https://github.com/UndeadSec/SocialFish) - Social media phishing framework that can run on an Android phone or in a Docker container.
* [ShellPhish](https://github.com/thelinuxchoice/shellphish) - Social media site cloner and phishing tool built atop SocialFish.
* [Gophish](https://getgophish.com) - Open-source phishing framework.
* [phishery](https://github.com/ryhanson/phishery) - TLS/SSL enabled Basic Auth credential harvester.
* [ReelPhish](https://github.com/fireeye/ReelPhish) - Real-time two-factor phishing tool.
* [Modlishka](https://github.com/drk1wi/Modlishka) - Flexible and powerful reverse proxy with real-time two-factor authentication.

OSINT Tools

* [Maltego](http://www.paterva.com/web7/) - Proprietary software for open source intelligence and forensics, from Paterva.
* [theHarvester](https://github.com/laramies/theHarvester) - E-mail, subdomain and people names harvester.
* [SimplyEmail](https://github.com/SimplySecurity/SimplyEmail) - Email recon made fast and easy.
* [creepy](https://github.com/ilektrojohn/creepy) - Geolocation OSINT tool.
* [metagoofil](https://github.com/laramies/metagoofil) - Metadata harvester.
* [Google Hacking Database](https://www.exploit-db.com/google-hacking-database/) - Database of Google dorks; can be used for recon.
* [GooDork](https://github.com/k3170makan/GooDork) - Command line Google dorking tool.
* [dork-cli](https://github.com/jgor/dork-cli) - Command line Google dork tool.
* [Censys](https://www.censys.io/) - Collects data on hosts and websites through daily ZMap and ZGrab scans.

* [Shodan](https://www.shodan.io/) - World's first search engine for Internet-connected devices.
* [recon-ng](https://bitbucket.org/LaNMaSteR53/recon-ng) - Full-featured Web Reconnaissance framework written in Python.
* [sn0int](https://github.com/kpcyrd/sn0int) - Semi-automatic OSINT framework and package manager.
* [github-dorks](https://github.com/techgaun/github-dorks) - CLI tool to scan GitHub repos/organizations for potential sensitive information leaks.
* [vcsmap](https://github.com/melvinsh/vcsmap) - Plugin-based tool to scan public version control systems for sensitive information.
* [Spiderfoot](http://www.spiderfoot.net/) - Multi-source OSINT automation tool with a Web UI and report visualizations.
* [BinGoo](https://github.com/Hood3dRob1n/BinGoo) - GNU/Linux bash based Bing and Google Dorking Tool.
* [fast-recon](https://github.com/DanMcInerney/fast-recon) - Perform Google dorks against a domain.
* [snitch](https://github.com/Smaash/snitch) - Information gathering via dorks.
* [Sn1per](https://github.com/1N3/Sn1per) - Automated Pentest Recon Scanner.
* [Threat Crowd](https://www.threatcrowd.org/) - Search engine for threats.
* [Virus Total](https://www.virustotal.com/) - Free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.
* [PacketTotal](https://packettotal.com/) - Simple, free, high-quality packet capture file analysis facilitating the quick detection of network-borne malware (using Bro and Suricata IDS signatures under the hood).
* [DataSploit](https://github.com/upgoingstar/datasploit) - OSINT visualizer utilizing Shodan, Censys, Clearbit, EmailHunter, FullContact, and Zoomeye behind the scenes.
* [AQUATONE](https://github.com/michenriksen/aquatone) - Subdomain discovery tool utilizing various open sources producing a report that can be used as input to other tools.
* [Intrigue](http://intrigue.io) - Automated OSINT & Attack Surface discovery framework with powerful API, UI and CLI.
* [ZoomEye](https://www.zoomeye.org/) - Search engine for cyberspace that lets the user find specific network components.
* [gOSINT](https://github.com/Nhoya/gOSINT) - OSINT tool with multiple modules and a telegram scraper.
* [OWASP Amass](https://github.com/OWASP/Amass) - Subdomain enumeration via scraping, web archives, brute forcing, permutations, reverse DNS sweeping, TLS certificates, passive DNS data sources, etc.
* [Hunter.io](https://hunter.io/) - Data broker providing a Web search interface for discovering the email addresses and other organizational details of a company.
* [FOCA (Fingerprinting Organizations with Collected Archives)](https://www.elevenpaths.com/labstools/foca/) - Automated document harvester that searches Google, Bing, and DuckDuckGo to find and extrapolate internal company organizational structures.
* [dorks](https://github.com/USSCltd/dorks) - Google hack database automation tool.
* [image-match](https://github.com/ascribe/image-match) - Quickly search over billions of images.
* [OSINT-SPY](https://github.com/SharadKumar97/OSINT-SPY) - Performs OSINT scan on email addresses, domain names, IP addresses, or organizations.
* [pagodo](https://github.com/opsdisk/pagodo) - Automate Google Hacking Database scraping.
* [surfraw](https://github.com/kisom/surfraw) - Fast UNIX command line interface to a variety of popular WWW search engines.

* [GyoiThon](https://github.com/gyoisamurai/GyoiThon) - GyoiThon is an Intelligence Gathering tool using Machine Learning.

Anonymity Tools

* [Tor](https://www.torproject.org/) - Free software and onion routed overlay network that helps you defend against traffic analysis.
* [OnionScan](https://onionscan.org/) - Tool for investigating the Dark Web by finding operational security issues introduced by Tor hidden service operators.
* [I2P](https://geti2p.net/) - The Invisible Internet Project.
* [Nipe](https://github.com/GouveaHeitor/nipe) - Script to redirect all traffic from the machine to the Tor network.
* [What Every Browser Knows About You](http://webkay.robinlinus.com/) - Comprehensive detection page to test your own Web browser's configuration for privacy and identity leaks.
* [dos-over-tor](https://github.com/zacscott/dos-over-tor) - Proof of concept denial of service over Tor stress test tool.
* [oregano](https://github.com/nametoolong/oregano) - Python module that runs as a machine-in-the-middle (MITM) accepting Tor client requests.
* [kalitorify](https://github.com/brainfuckSec/kalitorify) - Transparent proxy through Tor for Kali Linux OS.

Reverse Engineering Tools

* [Interactive Disassembler (IDA Pro)](https://www.hex-rays.com/products/ida/) - Proprietary multi-processor disassembler and debugger for Windows, GNU/Linux, or macOS; also has a free version, [IDA Free](https://www.hex-rays.com/products/ida/support/download_freeware.shtml).
* [WDK/WinDbg](https://msdn.microsoft.com/en-us/windows/hardware/hh852365.aspx) - Windows Driver Kit and WinDbg.
* [OllyDbg](http://www.ollydbg.de/) - x86 debugger for Windows binaries that emphasizes binary code analysis.
* [Radare2](http://rada.re/r/index.html) - Open source, crossplatform reverse engineering framework.
* [x64dbg](http://x64dbg.com/) - Open source x64/x32 debugger for windows.
* [Immunity Debugger](http://debugger.immunityinc.com/) - Powerful way to write exploits and analyze malware.
* [Evan's Debugger](http://www.codef00.com/projects#debugger) - OllyDbg-like debugger for GNU/Linux.
* [Medusa](https://github.com/wisk/medusa) - Open source, cross-platform interactive disassembler.
* [plasma](https://github.com/joelpx/plasma) - Interactive disassembler for x86/ARM/MIPS. Generates indented pseudo-code with colored syntax code.
* [peda](https://github.com/longld/peda) - Python Exploit Development Assistance for GDB.
* [dnSpy](https://github.com/0xd4d/dnSpy) - Tool to reverse engineer .NET assemblies.
* [binwalk](https://github.com/devttys0/binwalk) - Fast, easy to use tool for analyzing, reverse engineering, and extracting firmware images.
* [PyREBox](https://github.com/Cisco-Talos/pyrebox) - Python scriptable Reverse Engineering sandbox by Cisco-Talos.
* [Voltron](https://github.com/snare/voltron) - Extensible debugger UI toolkit written in Python.
* [Capstone](http://www.capstone-engine.org/) - Lightweight multi-platform, multi-architecture disassembly framework.

* [rVMI](https://github.com/fireeye/rVMI) - Debugger on steroids; inspect userspace processes, kernel drivers, and preboot environments in a single tool.
* [Frida](https://www.frida.re/) - Dynamic instrumentation toolkit for developers, reverse-engineers, and security researchers.
* [boxxy](https://github.com/kpcyrd/boxxy-rs) - Linkable sandbox explorer.

Physical Access Tools

* [LAN Turtle](https://lanturtle.com/) - Covert "USB Ethernet Adapter" that provides remote access, network intelligence gathering, and MITM capabilities when installed in a local network.
* [USB Rubber Ducky](http://usbrubberducky.com/) - Customizable keystroke injection attack platform masquerading as a USB thumbdrive.
* [Poisontap](https://samy.pl/poisontap/) - Siphons cookies, exposes internal (LAN-side) router and installs web backdoor on locked computers.
* [WiFi Pineapple](https://www.wifipineapple.com/) - Wireless auditing and penetration testing platform.
* [Proxmark3](https://proxmark3.com/) - RFID/NFC cloning, replay, and spoofing toolkit often used for analyzing and attacking proximity cards/readers, wireless keys/keyfobs, and more.
* [PCILeech](https://github.com/ufrisk/pcileech) - Uses PCIe hardware devices to read and write from the target system memory via Direct Memory Access (DMA) over PCIe.
* [AT Commands](https://atcommands.org/) - Use AT commands over an Android device's USB port to rewrite device firmware, bypass security mechanisms, exfiltrate sensitive information, perform screen unlocks, and inject touch events.
* [Bash Bunny](https://www.hak5.org/gear/bash-bunny) - Local exploit delivery tool in the form of a USB thumbdrive in which you write payloads in a DSL called BunnyScript.
* [Packet Squirrel](https://www.hak5.org/gear/packet-squirrel) - Ethernet multi-tool designed to enable covert remote access, painless packet captures, and secure VPN connections with the flip of a switch.

Industrial Control and SCADA Systems

* [Industrial Exploitation Framework (ISF)](https://github.com/dark-lbp/isf) - Metasploit-like exploit framework based on routersploit designed to target Industrial Control Systems (ICS), SCADA devices, PLC firmware, and more.
* [s7scan](https://github.com/klsecservices/s7scan) - Scanner for enumerating Siemens S7 PLCs on a TCP/IP or LLC network.

Side-channel Tools

* [ChipWhisperer](http://chipwhisperer.com) - Complete open-source toolchain for side-channel power analysis and glitching attacks.

CTF Tools

* [ctf-tools](https://github.com/zardus/ctf-tools) - Collection of setup scripts to install various security research tools easily and quickly deployable to new machines.
* [Pwntools](https://github.com/Gallopsled/pwntools) - Rapid exploit development framework built for use in CTFs.

* [RsaCtfTool](https://github.com/sourcekris/RsaCtfTool) - Decrypt data enciphered using weak RSA keys, and recover private keys from public keys using a variety of automated attacks.
* [shellpop](https://github.com/0x00-0x00/shellpop) - Easily generate sophisticated reverse or bind shell commands to help you save time during penetration tests.

Penetration Testing Report Templates

* [Public Pentesting Reports](https://github.com/juliocesarfort/public-pentesting-reports) - Curated list of public penetration test reports released by several consulting firms and academic security groups.
* [T&VS Pentesting Report Template](https://www.testandverification.com/wp-content/uploads/template-penetration-testing-report-v03.pdf) - Pentest report template provided by Test and Verification Services, Ltd.
* [Web Application Security Assessment Report Template](http://lucideus.com/pdf/stw.pdf) - Sample Web application security assessment reporting template provided by Lucideus.

Code examples for Penetration Testing

* [goHackTools](https://github.com/dreddsa5dies/goHackTools) - Hacker tools on Go (Golang).

Books

Penetration Testing Books

* [The Art of Exploitation by Jon Erickson, 2008](https://www.nostarch.com/hacking2.htm)
* [Metasploit: The Penetration Tester's Guide by David Kennedy et al., 2011](https://www.nostarch.com/metasploit)
* [Penetration Testing: A Hands-On Introduction to Hacking by Georgia Weidman, 2014](https://www.nostarch.com/pentesting)
* [Rtfm: Red Team Field Manual by Ben Clark, 2014](http://www.amazon.com/Rtfm-Red-Team-Field-Manual/dp/1494295504/)
* [Btfm: Blue Team Field Manual by Alan J White & Ben Clark, 2017](https://www.amazon.de/Blue-Team-Field-Manual-BTFM/dp/154101636X)
* [The Hacker Playbook by Peter Kim, 2014](http://www.amazon.com/The-Hacker-Playbook-Practical-Penetration/dp/1494932636/)
* [The Basics of Hacking and Penetration Testing by Patrick Engebretson, 2013](https://www.elsevier.com/books/the-basics-of-hacking-and-penetration-testing/engebretson/978-1-59749-655-1)
* [Professional Penetration Testing by Thomas Wilhelm, 2013](https://www.elsevier.com/books/professional-penetration-testing/wilhelm/978-1-59749-993-4)
* [Advanced Penetration Testing for Highly-Secured Environments by Lee Allen, 2012](http://www.packtpub.com/networking-and-servers/advanced-penetration-testing-highly-secured-environments-ultimate-security-gu)
* [Violent Python by TJ O'Connor, 2012](https://www.elsevier.com/books/violent-python/unknown/978-1-59749-957-6)
* [Fuzzing: Brute Force Vulnerability Discovery by Michael Sutton et al., 2007](http://www.fuzzing.org/)
* [Black Hat Python: Python Programming for Hackers and Pentesters by Justin Seitz, 2014](http://www.amazon.com/Black-Hat-Python-Programming-Pentesters/dp/1593275900)

* [Penetration Testing: Procedures & Methodologies by EC-Council, 2010](http://www.amazon.com/Penetration-Testing-Procedures-Methodologies-EC-Council/dp/1435483677)
* [Unauthorised Access: Physical Penetration Testing For IT Security Teams by Wil Allsopp, 2010](http://www.amazon.com/Unauthorised-Access-Physical-Penetration-Security-ebook/dp/B005DIAPKE)
* [Advanced Persistent Threat Hacking: The Art and Science of Hacking Any Organization by Tyler Wrightson, 2014](http://www.amazon.com/Advanced-Persistent-Threat-Hacking-Organization/dp/0071828362)
* [Bug Hunter's Diary by Tobias Klein, 2011](https://www.nostarch.com/bughunter)
* [Advanced Penetration Testing by Wil Allsopp, 2017](https://www.amazon.com/Advanced-Penetration-Testing-Hacking-Networks/dp/1119367689/)

Hackers Handbook Series

* [The Database Hacker's Handbook, David Litchfield et al., 2005](http://www.wiley.com/WileyCDA/WileyTitle/productCd-0764578014.html)
* [The Shellcoders Handbook by Chris Anley et al., 2007](http://www.wiley.com/WileyCDA/WileyTitle/productCd-047008023X.html)
* [The Mac Hacker's Handbook by Charlie Miller & Dino Dai Zovi, 2009](http://www.wiley.com/WileyCDA/WileyTitle/productCd-0470395362.html)
* [The Web Application Hackers Handbook by D. Stuttard, M. Pinto, 2011](http://www.wiley.com/WileyCDA/WileyTitle/productCd-1118026470.html)
* [iOS Hackers Handbook by Charlie Miller et al., 2012](http://www.wiley.com/WileyCDA/WileyTitle/productCd-1118204123.html)
* [Android Hackers Handbook by Joshua J. Drake et al., 2014](http://www.wiley.com/WileyCDA/WileyTitle/productCd-111860864X.html)
* [The Browser Hackers Handbook by Wade Alcorn et al., 2014](http://www.wiley.com/WileyCDA/WileyTitle/productCd-1118662091.html)
* [The Mobile Application Hackers Handbook by Dominic Chell et al., 2015](http://www.wiley.com/WileyCDA/WileyTitle/productCd-1118958500.html)
* [Car Hacker's Handbook by Craig Smith, 2016](https://www.nostarch.com/carhacking)

Defensive Development

* [Holistic Info-Sec for Web Developers (Fascicle 0)](https://leanpub.com/holistic-infosec-for-web-developers)
* [Holistic Info-Sec for Web Developers (Fascicle 1)](https://leanpub.com/holistic-infosec-for-web-developers-fascicle1-vps-network-cloud-webapplications)

Network Analysis Books

* [Nmap Network Scanning by Gordon Fyodor Lyon, 2009](https://nmap.org/book/)
* [Practical Packet Analysis by Chris Sanders, 2011](https://www.nostarch.com/packet2.htm)
* [Wireshark Network Analysis by by Laura Chappell & Gerald Combs, 2012](https://www.amazon.com/Wireshark-Network-Analysis-Second-Certified/dp/1893939944)

* [Network Forensics: Tracking Hackers through Cyberspace by Sherri Davidoff & Jonathan Ham, 2012](http://www.amazon.com/Network-Forensics-Tracking-Hackers-Cyberspace-ebook/dp/B008CG8CYU/)

Reverse Engineering Books

* [Reverse Engineering for Beginners by Dennis Yurichev](http://beginners.re/)
* [Hacking the Xbox by Andrew Huang, 2003](https://www.nostarch.com/xbox.htm)
* [The IDA Pro Book by Chris Eagle, 2011](https://www.nostarch.com/idapro2.htm)
* [Practical Reverse Engineering by Bruce Dang et al., 2014](http://www.wiley.com/WileyCDA/WileyTitle/productCd-1118787315.html)
* [Gray Hat Hacking The Ethical Hacker's Handbook by Daniel Regalado et al., 2015](http://www.amazon.com/Hacking-Ethical-Hackers-Handbook-Edition/dp/0071832386)

Malware Analysis Books

* [Practical Malware Analysis by Michael Sikorski & Andrew Honig, 2012](https://www.nostarch.com/malware)
* [The Art of Memory Forensics by Michael Hale Ligh et al., 2014](http://www.wiley.com/WileyCDA/WileyTitle/productCd-1118825098.html)
* [Malware Analyst's Cookbook and DVD by Michael Hale Ligh et al., 2010](http://www.wiley.com/WileyCDA/WileyTitle/productCd-0470613033.html)

Windows Books

* [Windows Internals by Mark Russinovich et al., 2012](http://www.amazon.com/Windows-Internals-Part-Developer-Reference/dp/0735648735/)
* [Troubleshooting with the Windows Sysinternals Tools by Mark Russinovich & Aaron Margosis, 2016](https://www.amazon.com/Troubleshooting-Windows-Sysinternals-Tools-2nd/dp/0735684448/)

Social Engineering Books

* [The Art of Deception by Kevin D. Mitnick & William L. Simon, 2002](http://www.wiley.com/WileyCDA/WileyTitle/productCd-0471237124.html)
* [The Art of Intrusion by Kevin D. Mitnick & William L. Simon, 2005](http://www.wiley.com/WileyCDA/WileyTitle/productCd-0764569597.html)
* [Ghost in the Wires by Kevin D. Mitnick & William L. Simon, 2011](http://www.hachettebookgroup.com/titles/kevin-mitnick/ghost-in-the-wires/9780316134477/)
* [No Tech Hacking by Johnny Long & Jack Wiles, 2008](https://www.elsevier.com/books/no-tech-hacking/mitnick/978-1-59749-215-7)
* [Unmasking the Social Engineer: The Human Element of Security by Christopher Hadnagy, 2014](http://www.wiley.com/WileyCDA/WileyTitle/productCd-1118608577.html)
* [Social Engineering in IT Security: Tools, Tactics, and Techniques by Sharon Conheady, 2014](https://www.mhprofessional.com/9780071818469-usa-social-engineering-in-it-security-tools-tactics-and-techniques-group)

Lock Picking Books

* [Practical Lock Picking by Deviant Ollam, 2012](https://www.elsevier.com/books/practical-lock-picking/ollam/978-1-59749-989-7)
* [Keys to the Kingdom by Deviant Ollam, 2012](https://www.elsevier.com/books/keys-to-the-kingdom/ollam/978-1-59749-983-5)
* [Lock Picking: Detail Overkill by Solomon](https://www.dropbox.com/s/y39ix9u9qpqffct/Lockpicking%20Detail%20Overkill.pdf?dl=0)
* [Eddie the Wire books](https://www.dropbox.com/sh/k3z4dm4vyyojp3o/AAAIXQuwMmNuCch_StLPUYm-a?dl=0)

Defcon Suggested Reading

* [Defcon Suggested Reading](https://www.defcon.org/html/links/book-list.html)

Vulnerability Databases

* [Common Vulnerabilities and Exposures (CVE)](https://cve.mitre.org/) - Dictionary of common names (i.e., CVE Identifiers) for publicly known security vulnerabilities.
* [National Vulnerability Database (NVD)](https://nvd.nist.gov/) - United States government's National Vulnerability Database provides additional meta-data (CPE, CVSS scoring) of the standard CVE List along with a fine-grained search engine.
* [US-CERT Vulnerability Notes Database](https://www.kb.cert.org/vuls/) - Summaries, technical details, remediation information, and lists of vendors affected by software vulnerabilities, aggregated by the United States Computer Emergency Response Team (US-CERT).
* [Full-Disclosure](http://seclists.org/fulldisclosure/) - Public, vendor-neutral forum for detailed discussion of vulnerabilities, often publishes details before many other sources.
* [Bugtraq (BID)](http://www.securityfocus.com/bid/) - Software security bug identification database compiled from submissions to the SecurityFocus mailing list and other sources, operated by Symantec, Inc.
* [Exploit-DB](https://www.exploit-db.com/) - Non-profit project hosting exploits for software vulnerabilities, provided as a public service by Offensive Security.
* [Microsoft Security Bulletins](https://technet.microsoft.com/en-us/security/bulletins#sec_search) - Announcements of security issues discovered in Microsoft software, published by the Microsoft Security Response Center (MSRC).
* [Microsoft Security Advisories](https://technet.microsoft.com/en-us/security/advisories#APUMA) - Archive of security advisories impacting Microsoft software.
* [Mozilla Foundation Security Advisories](https://www.mozilla.org/security/advisories/) - Archive of security advisories impacting Mozilla software, including the Firefox Web Browser.
* [Packet Storm](https://packetstormsecurity.com/files/) - Compendium of exploits, advisories, tools, and other security-related resources aggregated from across the industry.
* [CXSecurity](https://cxsecurity.com/) - Archive of published CVE and Bugtraq software vulnerabilities cross-referenced with a Google dork database for discovering the listed vulnerability.
* [SecuriTeam](http://www.securiteam.com/) - Independent source of software vulnerability information.
* [Vulnerability Lab](https://www.vulnerability-lab.com/) - Open forum for security advisories organized by category of exploit target.
* [Zero Day Initiative](http://zerodayinitiative.com/advisories/published/) - Bug bounty program with publicly accessible archive of published security advisories, operated by TippingPoint.
* [Vulners](https://vulners.com/) - Security database of software vulnerabilities.

* [Inj3ct0r](https://www.0day.today/) - Exploit marketplace and vulnerability information aggregator. ([Onion service](http://mvfjfugdwgc5uwho.onion/).)
* [HPI-VDB](https://hpi-vdb.de/) - Aggregator of cross-referenced software vulnerabilities offering free-of-charge API access, provided by the Hasso-Plattner Institute, Potsdam.
* [China National Vulnerability Database (CNNVD)](http://www.cnnvd.org.cn/) - Chinese government-run vulnerability database analoguous to the United States's CVE database hosted by Mitre Corporation.
* [Distributed Weakness Filing (DWF)](https://distributedweaknessfiling.org/) - Federated CNA (CVE Number Authority) mirroring MITRE's CVE database and offering additional CVE-equivalent numbers to otherwise out-of-scope vulnerability disclosures.

Security Courses

* [Offensive Security Training](https://www.offensive-security.com/information-security-training/) - Training from BackTrack/Kali developers.
* [SANS Security Training](http://www.sans.org/) - Computer Security Training & Certification.
* [Open Security Training](http://opensecuritytraining.info/) - Training material for computer security classes.
* [CTF Field Guide](https://trailofbits.github.io/ctf/) - Everything you need to win your next CTF competition.
* [ARIZONA CYBER WARFARE RANGE](http://azcwr.org/) - 24x7 live fire exercises for beginners through real world operations; capability for upward progression into the real world of cyber warfare.
* [Cybrary](http://cybrary.it) - Free courses in ethical hacking and advanced penetration testing. Advanced penetration testing courses are based on the book 'Penetration Testing for Highly Secured Environments'.
* [Computer Security Student](http://computersecuritystudent.com) - Many free tutorials, great for beginners, $10/mo membership unlocks all content.
* [European Union Agency for Network and Information Security](https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material) - ENISA Cyber Security Training material.

Information Security Conferences

* [DEF CON](https://www.defcon.org/) - Annual hacker convention in Las Vegas.
* [Black Hat](http://www.blackhat.com/) - Annual security conference in Las Vegas.
* [BSides](http://www.securitybsides.com/) - Framework for organising and holding security conferences.
* [CCC](https://events.ccc.de/congress/) - Annual meeting of the international hacker scene in Germany.
* [DerbyCon](https://www.derbycon.com/) - Annual hacker conference based in Louisville.
* [PhreakNIC](http://phreaknic.info/) - Technology conference held annually in middle Tennessee.
* [ShmooCon](http://shmoocon.org/) - Annual US East coast hacker convention.
* [CarolinaCon](http://www.carolinacon.org/) - Infosec conference, held annually in North Carolina.
* [CHCon](https://2016.chcon.nz/) - Christchurch Hacker Con, Only South Island of New Zealand hacker con.
* [SummerCon](http://www.summercon.org/) - One of the oldest hacker conventions, held during Summer.
* [Hack.lu](https://2016.hack.lu/) - Annual conference held in Luxembourg.
* [Hackfest](https://hackfest.ca) - Largest hacking conference in Canada.

* [HITB](https://conference.hitb.org/) - Deep-knowledge security conference held in Malaysia and The Netherlands.
* [Troopers](https://www.troopers.de) - Annual international IT Security event with workshops held in Heidelberg, Germany.
* [ThotCon](http://thotcon.org/) - Annual US hacker conference held in Chicago.
* [LayerOne](http://www.layerone.org/) - Annual US security conference held every spring in Los Angeles.
* [DeepSec](https://deepsec.net/) - Security Conference in Vienna, Austria.
* [SkyDogCon](http://www.skydogcon.com/) - Technology conference in Nashville.
* [SECUINSIDE](http://secuinside.com) - Security Conference in [Seoul](https://en.wikipedia.org/wiki/Seoul).
* [DefCamp](http://def.camp/) - Largest Security Conference in Eastern Europe, held annually in Bucharest, Romania.
* [AppSecUSA](https://appsecusa.org/) - Annual conference organized by OWASP.
* [BruCON](http://brucon.org) - Annual security conference in Belgium.
* [Infosecurity Europe](http://www.infosecurityeurope.com/) - Europe's number one information security event, held in London, UK.
* [Nullcon](http://nullcon.net/website/) - Annual conference in Delhi and Goa, India.
* [RSA Conference USA](https://www.rsaconference.com/) - Annual security conference in San Francisco, California, USA.
* [Swiss Cyber Storm](https://www.swisscyberstorm.com/) - Annual security conference in Lucerne, Switzerland.
* [Virus Bulletin Conference](https://www.virusbulletin.com/conference/index) - Annual conference going to be held in Denver, USA for 2016.
* [Ekoparty](http://www.ekoparty.org) - Largest Security Conference in Latin America, held annually in Buenos Aires, Argentina.
* [44Con](https://44con.com/) - Annual Security Conference held in London.
* [BalCCon](https://www.balccon.org) - Balkan Computer Congress, annually held in Novi Sad, Serbia.
* [FSec](http://fsec.foi.hr) - FSec - Croatian Information Security Gathering in Varaždin, Croatia.

Information Security Magazines

* [2600: The Hacker Quarterly](https://www.2600.com/Magazine/DigitalEditions) - American publication about technology and computer "underground."
* [Phrack Magazine](http://www.phrack.org/) - By far the longest running hacker zine.

Awesome Lists

* [Kali Linux Tools](http://tools.kali.org/tools-listing) - List of tools present in Kali Linux.
* [SecTools](http://sectools.org/) - Top 125 Network Security Tools.
* [Pentest Cheat Sheets](https://github.com/coreb1t/awesome-pentest-cheat-sheets) - Awesome Pentest Cheat Sheets.
* [C/C++ Programming](https://github.com/fffaraz/awesome-cpp) - One of the main language for open source security tools.
* [.NET Programming](https://github.com/quozd/awesome-dotnet) - Software framework for Microsoft Windows platform development.
* [Shell Scripting](https://github.com/alebcay/awesome-shell) - Command line frameworks, toolkits, guides and gizmos.

* [Ruby Programming by @dreikanter](https://github.com/dreikanter/ruby-bookmarks) - The de-facto language for writing exploits.
* [Ruby Programming by @markets](https://github.com/markets/awesome-ruby) - The de-facto language for writing exploits.
* [Ruby Programming by @Sdogruyol](https://github.com/Sdogruyol/awesome-ruby) - The de-facto language for writing exploits.
* [JavaScript Programming](https://github.com/sorrycc/awesome-javascript) - In-browser development and scripting.
* [Node.js Programming by @sindresorhus](https://github.com/sindresorhus/awesome-nodejs) - Curated list of delightful Node.js packages and resources.
* [Python tools for penetration testers](https://github.com/dloss/python-pentest-tools) - Lots of pentesting tools are written in Python.
* [Python Programming by @svaksha](https://github.com/svaksha/pythonidae) - General Python programming.
* [Python Programming by @vinta](https://github.com/vinta/awesome-python) - General Python programming.
* [Android Security](https://github.com/ashishb/android-security-awesome) - Collection of Android security related resources.
* [Awesome Awesomness](https://github.com/bayandin/awesome-awesomeness) - The List of the Lists.
* [AppSec](https://github.com/paragonie/awesome-appsec) - Resources for learning about application security.
* [CTFs](https://github.com/apsdehal/awesome-ctf) - Capture The Flag frameworks, libraries, etc.
* [InfoSec § Hacking challenges](https://github.com/AnarchoTechNYC/meta/wiki/InfoSec#hacking-challenges) - Comprehensive directory of CTFs, wargames, hacking challenge websites, pentest practice lab exercises, and more.
* [Hacking](https://github.com/carpedm20/awesome-hacking) - Tutorials, tools, and resources.
* [Honeypots](https://github.com/paralax/awesome-honeypots) - Honeypots, tools, components, and more.
* [Infosec](https://github.com/onlurking/awesome-infosec) - Information security resources for pentesting, forensics, and more.
* [Forensics](https://github.com/Cugu/awesome-forensics) - Free (mostly open source) forensic analysis tools and resources.
* [Malware Analysis](https://github.com/rshipp/awesome-malware-analysis) - Tools and resources for analysts.
* [PCAP Tools](https://github.com/caesar0301/awesome-pcaptools) - Tools for processing network traffic.
* [Security](https://github.com/sbilly/awesome-security) - Software, libraries, documents, and other resources.
* [Awesome Lockpicking](https://github.com/meitar/awesome-lockpicking) - Awesome guides, tools, and other resources about the security and compromise of locks, safes, and keys.
* [SecLists](https://github.com/danielmiessler/SecLists) - Collection of multiple types of lists used during security assessments.
* [Security Talks](https://github.com/PaulSec/awesome-sec-talks) - Curated list of security conferences.
* [OSINT](https://github.com/jivoi/awesome-osint) - Awesome OSINT list containing great resources.
* [YARA](https://github.com/InQuest/awesome-yara) - YARA rules, tools, and people.
* [Blue Team](https://github.com/meitar/awesome-cybersecurity-blueteam) - Awesome resources, tools, and other shiny things for cybersecurity blue teams.

* [Android Exploits](https://github.com/sundaysec/Android-Exploits) - Guide on Android Exploitation and Hacks.

License

Awesome Red Teaming

List of Awesome Red Team / Red Teaming Resources

This list is for anyone wishing to learn about Red Teaming but do not have a starting point.

Anyway, this is a living resources and will update regularly with latest Adversarial Tactics and Techniques based on [Mitre ATT&CK](https://attack.mitre.org/wiki/Main_Page)

You can help by sending Pull Requests to add more information.

Table of Contents
=================

[↑](#table-of-contents) Initial Access

* [How To: Empire’s Cross Platform Office Macro](https://www.blackhillsinfosec.com/empires-cross-platform-office-macro/)
* [Phishing with PowerPoint](https://www.blackhillsinfosec.com/phishing-with-powerpoint/)
* [PHISHING WITH EMPIRE](https://enigma0x3.net/2016/03/15/phishing-with-empire/)
* [Bash Bunny](https://hakshop.com/products/bash-bunny)
* [OWASP Presentation of Social Engineering - OWASP](https://www.owasp.org/images/5/54/Presentation_Social_Engineering.pdf)
* [USB Drop Attacks: The Danger of “Lost And Found” Thumb Drives](https://www.redteamsecure.com/usb-drop-attacks-the-danger-of-lost-and-found-thumb-drives/)
* [Weaponizing data science for social engineering: Automated E2E spear phishing on Twitter - Defcon 23](https://media.defcon.org/DEF%20CON%2024/DEF%20CON%2024%20presentations/DEFCON-24-Seymour-Tully-Weaponizing-Data-Science-For-Social-Engineering-WP.pdf)
* [Cobalt Strike - Spear Phishing documentation](https://www.cobaltstrike.com/help-spear-phish)
* [Cobalt Strike Blog - What's the go-to phishing technique or exploit?](https://blog.cobaltstrike.com/2014/12/17/whats-the-go-to-phishing-technique-or-exploit/)
* [Spear phishing with Cobalt Strike - Raphael Mudge](https://www.youtube.com/watch?v=V7UJjVcq2Ao)
* [EMAIL RECONNAISSANCE AND PHISHING TEMPLATE GENERATION MADE SIMPLE](https://cybersyndicates.com/2016/05/email-reconnaissance-phishing-template-generation-made-simple/)
* [Phishing for access](http://www.rvrsh3ll.net/blog/phishing/phishing-for-access/)
* [Excel macros with PowerShell](https://4sysops.com/archives/excel-macros-with-powershell/)
* [PowerPoint and Custom Actions](https://phishme.com/powerpoint-and-custom-actions/)
* [Macro-less Code Exec in MSWord](https://sensepost.com/blog/2017/macro-less-code-exec-in-msword/)
* [Multi-Platform Macro Phishing Payloads](https://medium.com/@malcomvetter/multi-platform-macro-phishing-payloads-3b688e8eff68)
* [Abusing Microsoft Word Features for Phishing: “subDoc”](https://rhinosecuritylabs.com/research/abusing-microsoft-word-features-phishing-subdoc/)
* [Phishing Against Protected View](https://enigma0x3.net/2017/07/13/phishing-against-protected-view/)
* [POWERSHELL EMPIRE STAGERS 1: PHISHING WITH AN OFFICE MACRO AND EVADING AVS](https://fzuckerman.wordpress.com/2016/10/06/powershell-empire-stagers-1-phishing-with-an-office-macro-and-evading-avs/)
* [The PlugBot: Hardware Botnet Research Project](https://www.redteamsecure.com/the-plugbot-hardware-botnet-research-project/)
* [Luckystrike: An Evil Office Document Generator](https://www.shellntel.com/blog/2016/9/13/luckystrike-a-database-backed-evil-macro-generator)
* [The Absurdly Underestimated Dangers of CSV Injection](http://georgemauer.net/2017/10/07/csv-injection.html)
* [Macroless DOC malware that avoids detection with Yara rule](https://furoner.wordpress.com/2017/10/17/macroless-malware-that-avoids-detection-with-yara-rule/amp/)
* [Phishing between the app whitelists](https://medium.com/@vivami/phishing-between-the-app-whitelists-1b7dcdab4279)

* [Executing Metasploit & Empire Payloads from MS Office Document Properties (part 1 of 2)](https://stealingthe.network/executing-metasploit-empire-payloads-from-ms-office-document-properties-part-1-of-2/)
* [Executing Metasploit & Empire Payloads from MS Office Document Properties (part 2 of 2)](https://stealingthe.network/executing-metasploit-empire-payloads-from-ms-office-document-properties-part-2-of-2/)
* [Social Engineer Portal](https://www.social-engineer.org/)
* [7 Best social Engineering attack](http://www.darkreading.com/the-7-best-social-engineering-attacks-ever/d/d-id/1319411)
* [Using Social Engineering Tactics For Big Data Espionage - RSA Conference Europe 2012](https://www.rsaconference.com/writable/presentations/file_upload/das-301_williams_rader.pdf)
* [USING THE DDE ATTACK WITH POWERSHELL EMPIRE](https://1337red.wordpress.com/using-the-dde-attack-with-powershell-empire/)
* [Phishing on Twitter - POT](https://www.kitploit.com/2018/02/pot-phishing-on-twitter.html)
* [Microsoft Office – NTLM Hashes via Frameset](https://pentestlab.blog/2017/12/18/microsoft-office-ntlm-hashes-via-frameset/)
* [Defense-In-Depth write-up](https://oddvar.moe/2017/09/13/defense-in-depth-writeup/)
* [Spear Phishing 101](https://blog.inspired-sec.com/archive/2017/05/07/Phishing.html)

[↑](#table-of-contents) Execution
* [Research on CMSTP.exe,](https://msitpros.com/?p=3960)
* [Windows oneliners to download remote payload and execute arbitrary code](https://arno0x0x.wordpress.com/2017/11/20/windows-oneliners-to-download-remote-payload-and-execute-arbitrary-code/)
* [Executing Commands and Bypassing AppLocker with PowerShell Diagnostic Scripts](https://bohops.com/2017/12/02/clickonce-twice-or-thrice-a-technique-for-social-engineering-and-untrusted-command-execution/)
* [WSH Injection: A Case Study](https://posts.specterops.io/wsh-injection-a-case-study-fd35f79d29dd)
* [Gscript Dropper](http://lockboxx.blogspot.com/2018/02/intro-to-using-gscript-for-red-teams.html)

[↑](#table-of-contents) Persistence
* [A View of Persistence](https://rastamouse.me/2018/03/a-view-of-persistence/)
* [hiding registry keys with psreflect](https://posts.specterops.io/hiding-registry-keys-with-psreflect-b18ec5ac8353)
* [Persistence using RunOnceEx – Hidden from Autoruns.exe](https://oddvar.moe/2018/03/21/persistence-using-runonceex-hidden-from-autoruns-exe/)
* [Persistence using GlobalFlags in Image File Execution Options – Hidden from Autoruns.exe](https://oddvar.moe/2018/04/10/persistence-using-globalflags-in-image-file-execution-options-hidden-from-autoruns-exe/)
* [Putting data in Alternate data streams and how to execute it – part 2](https://oddvar.moe/2018/04/11/putting-data-in-alternate-data-streams-and-how-to-execute-it-part-2/)
* [WMI Persistence with Cobalt Strike](https://blog.inspired-sec.com/archive/2017/01/20/WMI-Persistence.html)

* [Leveraging INF-SCT Fetch & Execute Techniques For Bypass, Evasion, & Persistence](https://bohops.com/2018/02/26/leveraging-inf-sct-fetch-execute-techniques-for-bypass-evasion-persistence/)
* [Leveraging INF-SCT Fetch & Execute Techniques For Bypass, Evasion, & Persistence (Part 2)](https://bohops.com/2018/03/10/leveraging-inf-sct-fetch-execute-techniques-for-bypass-evasion-persistence-part-2/)
* [Vshadow: Abusing the Volume Shadow Service for Evasion, Persistence, and Active Directory Database Extraction](https://bohops.com/2018/02/10/vshadow-abusing-the-volume-shadow-service-for-evasion-persistence-and-active-directory-database-extraction/)

[↑](#table-of-contents) Privilege Escalation

User Account Control Bypass
* [First entry: Welcome and fileless UAC bypass,](https://winscripting.blog/2017/05/12/first-entry-welcome-and-uac-bypass/)
* [Exploiting Environment Variables in Scheduled Tasks for UAC Bypass,](https://tyranidslair.blogspot.ru/2017/05/exploiting-environment-variables-in.html)
* Reading Your Way Around UAC in 3 parts:
  [Part 1.](https://tyranidslair.blogspot.ru/2017/05/reading-your-way-around-uac-part-1.html)
  [Part 2.](https://tyranidslair.blogspot.ru/2017/05/reading-your-way-around-uac-part-2.html)
  [Part 3.](https://tyranidslair.blogspot.ru/2017/05/reading-your-way-around-uac-part-3.html)
* [Bypassing UAC using App Paths,](https://enigma0x3.net/2017/03/14/bypassing-uac-using-app-paths/)
* ["Fileless" UAC Bypass using sdclt.exe,](https://enigma0x3.net/2017/03/17/fileless-uac-bypass-using-sdclt-exe/)
* [UAC Bypass or story about three escalations,](https://habrahabr.ru/company/pm/blog/328008/)
* ["Fileless" UAC Bypass Using eventvwr.exe and Registry Hijacking,](https://enigma0x3.net/2016/08/15/fileless-uac-bypass-using-eventvwr-exe-and-registry-hijacking/)
* [Bypassing UAC on Windows 10 using Disk Cleanup,](https://enigma0x3.net/2016/07/22/bypassing-uac-on-windows-10-using-disk-cleanup/)
* [Using IARPUninstallStringLauncher COM interface to bypass UAC,](http://www.freebuf.com/articles/system/116611.html)
* [Fileless UAC Bypass using sdclt](https://posts.specterops.io/fileless-uac-bypass-using-sdclt-exe-3e9f9ad4e2b3)
* [Eventvwr File-less UAC Bypass CNA](https://www.mdsec.co.uk/2016/12/cna-eventvwr-uac-bypass/)
* [Windows 7 UAC whitelist](http://www.pretentiousname.com/misc/win7_uac_whitelist2.html)

Escalation
* [Windows Privilege Escalation Checklist](https://github.com/netbiosX/Checklists/blob/master/Windows-Privilege-Escalation.md)
* [From Patch Tuesday to DA](https://blog.inspired-sec.com/archive/2017/03/17/COM-Moniker-Privesc.html)
* [A Path for Privilege Escalation](https://blog.cobaltstrike.com/2016/12/08/cobalt-strike-3-6-a-path-for-privilege-escalation/)

[↑](#table-of-contents) Defense Evasion
* [Window 10 Device Guard Bypass](https://github.com/tyranid/DeviceGuardBypasses)

* [App Locker ByPass List](https://github.com/api0cradle/UltimateAppLockerByPassList)
* [Window Signed Binary](https://github.com/vysec/Windows-SignedBinary)
* [Bypass Application Whitelisting Script Protections - Regsvr32.exe & COM Scriptlets (.sct files)](http://subt0x10.blogspot.sg/2017/04/bypass-application-whitelisting-script.html)
* [Bypassing Application Whitelisting using MSBuild.exe - Device Guard Example and Mitigations](http://subt0x10.blogspot.sg/2017/04/bypassing-application-whitelisting.html)
* [Empire without powershell](https://bneg.io/2017/07/26/empire-without-powershell-exe/)
* [Powershell without Powershell to bypass app whitelist](https://www.blackhillsinfosec.com/powershell-without-powershell-how-to-bypass-application-whitelisting-environment-restrictions-av/)
* [MS Signed mimikatz in just 3 steps](https://github.com/secretsquirrel/SigThief)
* [Hiding your process from sysinternals](https://riscybusiness.wordpress.com/2017/10/07/hiding-your-process-from-sysinternals/)
* [code signing certificate cloning attacks and defenses](https://posts.specterops.io/code-signing-certificate-cloning-attacks-and-defenses-6f98657fc6ec)
* [userland api monitoring and code injection detection](https://0x00sec.org/t/userland-api-monitoring-and-code-injection-detection/5565)
* [In memory evasion](https://blog.cobaltstrike.com/2018/02/08/in-memory-evasion/)
* [Bypassing AMSI via COM Server Hijacking](https://posts.specterops.io/bypassing-amsi-via-com-server-hijacking-b8a3354d1aff)
* [process doppelganging](https://hshrzd.wordpress.com/2017/12/18/process-doppelganging-a-new-way-to-impersonate-a-process/)
* [Week of Evading Microsoft ATA - Announcement and Day 1 to Day 5](http://www.labofapenetrationtester.com/2017/08/week-of-evading-microsoft-ata-day1.html)
* [VEIL-EVASION AES ENCRYPTED HTTPKEY REQUEST: SAND-BOX EVASION](https://cybersyndicates.com/2015/06/veil-evasion-aes-encrypted-httpkey-request-module/)
* [Putting data in Alternate data streams and how to execute it](https://oddvar.moe/2018/01/14/putting-data-in-alternate-data-streams-and-how-to-execute-it/)
* [AppLocker – Case study – How insecure is it really? – Part 1](https://oddvar.moe/2017/12/13/applocker-case-study-how-insecure-is-it-really-part-1/)
* [AppLocker – Case study – How insecure is it really? – Part 2](https://oddvar.moe/2017/12/21/applocker-case-study-how-insecure-is-it-really-part-2/)
* [Harden Windows with AppLocker – based on Case study part 2](https://oddvar.moe/2017/12/13/harden-windows-with-applocker-based-on-case-study-part-1/)
* [Harden Windows with AppLocker – based on Case study part 2](https://oddvar.moe/2017/12/21/harden-windows-with-applocker-based-on-case-study-part-2/)
* [Office 365 Safe links bypass](https://oddvar.moe/2018/01/03/office-365-safe-links-bypass/)
* [Windows Defender Attack Surface Reduction Rules bypass](https://oddvar.moe/2018/03/15/windows-defender-attack-surface-reduction-rules-bypass/)
* [Bypassing Device guard UMCI using CHM – CVE-2017-8625](https://oddvar.moe/2017/08/13/bypassing-device-guard-umci-using-chm-cve-2017-8625/)
* [Bypassing Application Whitelisting with BGInfo](https://oddvar.moe/2017/05/18/bypassing-application-whitelisting-with-bginfo/)
* [Cloning and Hosting Evil Captive Portals using a Wifi PineApple](https://blog.inspired-sec.com/archive/2017/01/10/cloning-captive-portals.html)
* https://bohops.com/2018/01/23/loading-alternate-data-stream-ads-dll-cpl-binaries-to-bypass-applocker/

* [Executing Commands and Bypassing AppLocker with PowerShell Diagnostic Scripts](https://bohops.com/2018/01/07/executing-commands-and-bypassing-applocker-with-powershell-diagnostic-scripts/)
* [mavinject.exe Functionality Deconstructed](https://posts.specterops.io/mavinject-exe-functionality-deconstructed-c29ab2cf5c0e)

[↑](#table-of-contents) Credential Access
* [Windows Access Tokens and Alternate credentials](https://blog.cobaltstrike.com/2015/12/16/windows-access-tokens-and-alternate-credentials/)
* [Bringing the hashes home with reGeorg & Empire](https://sensepost.com/blog/2016/bringing-the-hashes-home-with-regeorg-empire/)
* [Intercepting passwords with Empire and winning](https://sensepost.com/blog/2016/intercepting-passwords-with-empire-and-winning/)
* [Local Administrator Password Solution (LAPS) Part 1](https://rastamouse.me/2018/03/laps---part-1/)
* [Local Administrator Password Solution (LAPS) Part 2](https://rastamouse.me/2018/03/laps---part-2/)
* [USING A SCF FILE TO GATHER HASHES](https://1337red.wordpress.com/using-a-scf-file-to-gather-hashes/)
* [Remote Hash Extraction On Demand Via Host Security Descriptor Modification](https://www.harmj0y.net/blog/)
* [Offensive Encrypted Data Storage](https://www.harmj0y.net/blog/redteaming/offensive-encrypted-data-storage/)
* [Practical guide to NTLM Relaying](https://byt3bl33d3r.github.io/practical-guide-to-ntlm-relaying-in-2017-aka-getting-a-foothold-in-under-5-minutes.html)
* [Dump Clear-Text Passwords for All Admins in the Domain Using Mimikatz DCSync](https://adsecurity.org/?p=2053)
* [Dumping Domain Password Hashes](https://pentestlab.blog/2018/07/04/dumping-domain-password-hashes/)

[↑](#table-of-contents) Discovery
* [Red Team Operating in a Modern Environment](https://www.owasp.org/images/4/4b/Red_Team_Operating_in_a_Modern_Environment.pdf)
* [My First Go with BloodHound](https://blog.cobaltstrike.com/2016/12/14/my-first-go-with-bloodhound/)
* [Introducing BloodHound](https://wald0.com/?p=68)
* [A Red Teamer’s Guide to GPOs and OUs](https://wald0.com/?p=179)
* [Automated Derivative Administrator Search](https://wald0.com/?p=14)
* [A Pentester’s Guide to Group Scoping](https://www.harmj0y.net/blog/activedirectory/a-pentesters-guide-to-group-scoping/)
* [Local Group Enumeration](https://www.harmj0y.net/blog/redteaming/local-group-enumeration/)
* [The PowerView PowerUsage Series #1 - Mass User Profile Enumeration](http://www.harmj0y.net/blog/powershell/the-powerview-powerusage-series-1/)
* [The PowerView PowerUsage Series #2 – Mapping Computer Shortnames With the Global Catalog](http://www.harmj0y.net/blog/powershell/the-powerview-powerusage-series-2/)
* [The PowerView PowerUsage Series #3 – Enumerating GPO edit rights in a foreign domain](http://www.harmj0y.net/blog/powershell/the-powerview-powerusage-series-3/)

* [The PowerView PowerUsage Series #4 – Finding cross-trust ACEs](http://www.harmj0y.net/blog/powershell/the-powerview-powerusage-series-3/)
* [Aggressor PowerView](http://threat.tevora.com/aggressor-powerview/)
* [Lay of the Land with BloodHound](http://threat.tevora.com/lay-of-the-land-with-bloodhound/)
* [Scanning for Active Directory Privileges & Privileged Accounts](https://adsecurity.org/?p=3658)
* [Microsoft LAPS Security & Active Directory LAPS Configuration Recon](https://adsecurity.org/?p=3164)
* [Trust Direction: An Enabler for Active Directory Enumeration and Trust Exploitation](https://bohops.com/2017/12/02/trust-direction-an-enabler-for-active-directory-enumeration-and-trust-exploitation/)
* [SPN Discovery](https://pentestlab.blog/2018/06/04/spn-discovery/)

[↑](#table-of-contents) Lateral Movement

* [A Citrix Story](https://rastamouse.me/2017/05/a-citrix-story/)
* [Jumping Network Segregation with RDP](https://rastamouse.me/2017/08/jumping-network-segregation-with-rdp/)
* [Pass hash pass ticket no pain](http://resources.infosecinstitute.com/pass-hash-pass-ticket-no-pain/)
* [Abusing DNSAdmins privilege for escalation in Active Directory](http://www.labofapenetrationtester.com/2017/05/abusing-dnsadmins-privilege-for-escalation-in-active-directory.html)
* [Using SQL Server for attacking a Forest Trust](http://www.labofapenetrationtester.com/2017/03/using-sql-server-for-attacking-forest-trust.html)
* [Extending BloodHound for Red Teamers](https://www.youtube.com/watch?v=Pn7GWRXfgeI)
* [OPSEC Considerations for beacon commands](https://blog.cobaltstrike.com/2017/06/23/opsec-considerations-for-beacon-commands/)
* [My First Go with BloodHound](https://blog.cobaltstrike.com/2016/12/14/my-first-go-with-bloodhound/)
* [Kerberos Party Tricks: Weaponizing Kerberos Protocol Flaws](http://www.exumbraops.com/blog/2016/6/1/kerberos-party-tricks-weaponizing-kerberos-protocol-flaws)
* [Lateral movement using excel application and dcom](https://enigma0x3.net/2017/09/11/lateral-movement-using-excel-application-and-dcom/)
* [Lay of the Land with BloodHound](http://threat.tevora.com/lay-of-the-land-with-bloodhound/)
* [The Most Dangerous User Right You (Probably) Have Never Heard Of](https://www.harmj0y.net/blog/activedirectory/the-most-dangerous-user-right-you-probably-have-never-heard-of/)
* [Agentless Post Exploitation](https://blog.cobaltstrike.com/2016/11/03/agentless-post-exploitation/)
* [A Guide to Attacking Domain Trusts](https://www.harmj0y.net/blog/redteaming/a-guide-to-attacking-domain-trusts/)
* [Pass-the-Hash Is Dead: Long Live LocalAccountTokenFilterPolicy](https://www.harmj0y.net/blog/redteaming/pass-the-hash-is-dead-long-live-localaccounttokenfilterpolicy/)
* [Targeted Kerberoasting](https://www.harmj0y.net/blog/activedirectory/targeted-kerberoasting/)
* [Kerberoasting Without Mimikatz](https://www.harmj0y.net/blog/powershell/kerberoasting-without-mimikatz/)
* [Abusing GPO Permissions](https://www.harmj0y.net/blog/redteaming/abusing-gpo-permissions/)

* [Abusing Active Directory Permissions with PowerView](https://www.harmj0y.net/blog/redteaming/abusing-active-directory-permissions-with-powerview/)
* [Roasting AS-REPs](https://www.harmj0y.net/blog/activedirectory/roasting-as-reps/)
* [Getting the goods with CrackMapExec: Part 1](https://byt3bl33d3r.github.io/getting-the-goods-with-crackmapexec-part-1.html)
* [Getting the goods with CrackMapExec: Part 2](https://byt3bl33d3r.github.io/getting-the-goods-with-crackmapexec-part-2.html)
* [DiskShadow: The Return of VSS Evasion, Persistence, and Active Directory Database Extraction](https://bohops.com/2018/03/26/diskshadow-the-return-of-vss-evasion-persistence-and-active-directory-database-extraction/)
* [Abusing Exported Functions and Exposed DCOM Interfaces for Pass-Thru Command Execution and Lateral Movement](https://bohops.com/2018/03/17/abusing-exported-functions-and-exposed-dcom-interfaces-for-pass-thru-command-execution-and-lateral-movement/)
* [a guide to attacking domain trusts](https://posts.specterops.io/a-guide-to-attacking-domain-trusts-971e52cb2944)
* [Outlook Home Page – Another Ruler Vector](https://sensepost.com/blog/2017/outlook-home-page-another-ruler-vector/)
* [Outlook Forms and Shells](https://sensepost.com/blog/2017/outlook-forms-and-shells/)
* [Abusing the COM Registry Structure: CLSID, LocalServer32, & InprocServer32](https://bohops.com/2018/06/28/abusing-com-registry-structure-clsid-localserver32-inprocserver32/)
* [LethalHTA - A new lateral movement technique using DCOM and HTA](https://codewhitesec.blogspot.com/2018/07/lethalhta.html)
* [Abusing DCOM For Yet Another Lateral Movement Technique](https://bohops.com/2018/04/28/abusing-dcom-for-yet-another-lateral-movement-technique/)

[↑](#table-of-contents) Collection
* [Accessing clipboard from the lock screen in Windows 10 Part 1](https://oddvar.moe/2017/01/24/accessing-clipboard-from-the-lock-screen-in-windows-10/)
* [Accessing clipboard from the lock screen in Windows 10 Part 2](https://oddvar.moe/2017/01/27/access-clipboard-from-lock-screen-in-windows-10-2/)

[↑](#table-of-contents) Exfiltration
* [DNS Data exfiltration — What is this and How to use?](https://blog.fosec.vn/dns-data-exfiltration-what-is-this-and-how-to-use-2f6c69998822)
* [DNS Tunnelling](http://resources.infosecinstitute.com/dns-tunnelling/)
* [sg1: swiss army knife for data encryption, exfiltration & covert communication](https://securityonline.info/sg1-swiss-army-knife-for-data-encryption-exfiltration-covert-communication/?utm_source=ReviveOldPost&utm_medium=social&utm_campaign=ReviveOldPost)
* [Data Exfiltration over DNS Request Covert Channel: DNSExfiltrator](https://n0where.net/data-exfiltration-over-dns-request-covert-channel-dnsexfiltrator)
* [DET (extensible) Data Exfiltration Toolkit](https://github.com/PaulSec/DET)

* [Data Exfiltration via Formula Injection Part1](https://www.notsosecure.com/data-exfiltration-formula-injection/)

[↑](#table-of-contents) Command and Control

Domain Fronting
* [Empre Domain Fronting](https://www.xorrior.com/Empire-Domain-Fronting/)
* [Escape and Evasion Egressing Restricted Networks - Tom Steele and Chris Patten](https://www.optiv.com/blog/escape-and-evasion-egressing-restricted-networks)
* [Finding Frontable Domain](https://github.com/rvrsh3ll/FindFrontableDomains)
* [TOR Fronting – Utilising Hidden Services for Privacy](https://www.mdsec.co.uk/2017/02/tor-fronting-utilising-hidden-services-for-privacy/)
* [Simple domain fronting PoC with GAE C2 server](https://www.securityartwork.es/2017/01/31/simple-domain-fronting-poc-with-gae-c2-server/)
* [Domain Fronting Via Cloudfront Alternate Domains](https://www.mdsec.co.uk/2017/02/domain-fronting-via-cloudfront-alternate-domains/)
* [Finding Domain frontable Azure domains - thoth / Fionnbharr (@a_profligate)](https://theobsidiantower.com/2017/07/24/d0a7cfceedc42bdf3a36f2926bd52863ef28befc.html)
* [Google Groups: Blog post on finding 2000+ Azure domains using Censys](https://groups.google.com/forum/#!topic/traffic-obf/7ygIXCPebwQ)
* [Red Team Insights on HTTPS Domain Fronting Google Hosts Using Cobalt Strike](https://www.cyberark.com/threat-research-blog/red-team-insights-https-domain-fronting-google-hosts-using-cobalt-strike/)
* [SSL Domain Fronting 101](http://www.rvrsh3ll.net/blog/offensive/ssl-domain-fronting-101/)
* [How I Identified 93k Domain-Frontable CloudFront Domains](https://www.peew.pw/blog/2018/2/22/how-i-identified-93k-domain-frontable-cloudfront-domains)
* [Validated CloudFront SSL Domains](https://medium.com/@vysec.private/validated-cloudfront-ssl-domains-27895822cea3)
* [CloudFront Hijacking](https://www.mindpointgroup.com/blog/pen-test/cloudfront-hijacking/)
* [CloudFrunt GitHub Repo](https://github.com/MindPointGroup/cloudfrunt)

Connection Proxy
* [Redirecting Cobalt Strike DNS Beacons](http://www.rvrsh3ll.net/blog/offensive/redirecting-cobalt-strike-dns-beacons/)
* [Apache2Mod Rewrite Setup](https://github.com/n0pe-sled/Apache2-Mod-Rewrite-Setup)
* [Cobalt Strike HTTP C2 Redirectors with Apache mod_rewrite](https://bluescreenofjeff.com/2016-06-28-cobalt-strike-http-c2-redirectors-with-apache-mod_rewrite/)
* [High-reputation Redirectors and Domain Fronting](https://blog.cobaltstrike.com/2017/02/06/high-reputation-redirectors-and-domain-fronting/)
* [Cloud-based Redirectors for Distributed Hacking](https://blog.cobaltstrike.com/2014/01/14/cloud-based-redirectors-for-distributed-hacking/)
* [Combatting Incident Responders with Apache mod_rewrite](https://bluescreenofjeff.com/2016-04-12-combatting-incident-responders-with-apache-mod_rewrite/)
* [Operating System Based Redirection with Apache mod_rewrite](https://bluescreenofjeff.com/2016-04-05-operating-system-based-redirection-with-apache-mod_rewrite/)

* [Invalid URI Redirection with Apache mod_rewrite](https://bluescreenofjeff.com/2016-03-29-invalid-uri-redirection-with-apache-mod_rewrite/)
* [Strengthen Your Phishing with Apache mod_rewrite and Mobile User Redirection](https://bluescreenofjeff.com/2016-03-22-strengthen-your-phishing-with-apache-mod_rewrite-and-mobile-user-redirection/)
* [mod_rewrite rule to evade vendor sandboxes](https://gist.github.com/curi0usJack/971385e8334e189d93a6cb4671238b10)
* [Expire Phishing Links with Apache RewriteMap](https://bluescreenofjeff.com/2016-04-19-expire-phishing-links-with-apache-rewritemap/)
* [Serving random payloads with NGINX](https://gist.github.com/jivoi/a33ace2e25515a31aa2ffbae246d98c9)
* [Mod_Rewrite Automatic Setup](https://blog.inspired-sec.com/archive/2017/04/17/Mod-Rewrite-Automatic-Setup.html)
* [Hybrid Cobalt Strike Redirectors](https://zachgrace.com/2018/02/20/cobalt_strike_redirectors.html)
* [Expand Your Horizon Red Team – Modern SAAS C2](https://cybersyndicates.com/2017/04/expand-your-horizon-red-team/)
* [RTOps: Automating Redirector Deployment With Ansible](http://threat.tevora.com/automating-redirector-deployment-with-ansible/)

Web Services
* [C2 with Dropbox](https://pentestlab.blog/2017/08/29/command-and-control-dropbox/)
* [C2 with gmail](https://pentestlab.blog/2017/08/03/command-and-control-gmail/)
* [C2 with twitter](https://pentestlab.blog/2017/09/26/command-and-control-twitter/)
* [Office 365 for Cobalt Strike C2](https://labs.mwrinfosecurity.com/blog/tasking-office-365-for-cobalt-strike-c2/)
* [Red Team Insights on HTTPS Domain Fronting Google Hosts Using Cobalt Strike](https://www.cyberark.com/threat-research-blog/red-team-insights-https-domain-fronting-google-hosts-using-cobalt-strike/)
* [A stealthy Python based Windows backdoor that uses Github as a C&C server](http://securityblog.gr/4434/a-stealthy-python-based-windows-backdoor-that-uses-github-as-a-cc-server/)
* [External C2 (Third-Party Command and Control)](https://www.cobaltstrike.com/help-externalc2)
* [Cobalt Strike over external C2 – beacon home in the most obscure ways](https://outflank.nl/blog/2017/09/17/blogpost-cobalt-strike-over-external-c2-beacon-home-in-the-most-obscure-ways/)
* [External C2 for Cobalt Strike](https://github.com/ryhanson/ExternalC2/)
* [External C2 framework for Cobalt Strike](http://www.insomniacsecurity.com/2018/01/11/externalc2.html)
* [External C2 framework - GitHub Repo](https://github.com/Und3rf10w/external_c2_framework)
* [Hiding in the Cloud: Cobalt Strike Beacon C2 using Amazon APIs](https://github.com/Und3rf10w/external_c2_framework)
* [Exploring Cobalt Strike's ExternalC2 framework](https://blog.xpnsec.com/exploring-cobalt-strikes-externalc2-framework/)

Application Layer Protocol
* [C2 WebSocket](https://pentestlab.blog/2017/12/06/command-and-control-websocket/)
* [C2 WMI](https://pentestlab.blog/2017/11/20/command-and-control-wmi/)
* [C2 Website](https://pentestlab.blog/2017/11/14/command-and-control-website/)

* [C2 Image](https://pentestlab.blog/2018/01/02/command-and-control-images/)
* [C2 Javascript](https://pentestlab.blog/2018/01/08/command-and-control-javascript/)
* [C2 WebInterface](https://pentestlab.blog/2018/01/03/command-and-control-web-interface/)
* [C2 with DNS](https://pentestlab.blog/2017/09/06/command-and-control-dns/)
* [C2 with https](https://pentestlab.blog/2017/10/04/command-and-control-https/)
* [C2 with webdav](https://pentestlab.blog/2017/09/12/command-and-control-webdav/)
* [Introducing Merlin — A cross-platform post-exploitation HTTP/2 Command & Control Tool](https://medium.com/@Ne0nd0g/introducing-merlin-645da3c635a)
* [InternetExplorer.Application for C2](https://adapt-and-attack.com/2017/12/19/internetexplorer-application-for-c2/)

Infrastructure
* [Automated Red Team Infrastructure Deployment with Terraform - Part 1](https://rastamouse.me/2017/08/automated-red-team-infrastructure-deployment-with-terraform---part-1/)
* [Automated Red Team Infrastructure Deployment with Terraform - Part 2](https://rastamouse.me/2017/09/automated-red-team-infrastructure-deployment-with-terraform---part-2/)
* [Red Team Infrastructure - AWS Encrypted EBS](https://rastamouse.me/2018/02/red-team-infrastructure---aws-encrypted-ebs/)
* [6 RED TEAM INFRASTRUCTURE TIPS](https://cybersyndicates.com/2016/11/top-red-team-tips/)
* [How to Build a C2 Infrastructure with Digital Ocean – Part 1](https://www.blackhillsinfosec.com/build-c2-infrastructure-digital-ocean-part-1/)
* [Infrastructure for Ongoing Red Team Operations](https://blog.cobaltstrike.com/2014/09/09/infrastructure-for-ongoing-red-team-operations/)
* [Attack Infrastructure Log Aggregation and Monitoring](https://posts.specterops.io/attack-infrastructure-log-aggregation-and-monitoring-345e4173044e)
* [Randomized Malleable C2 Profiles Made Easy](https://bluescreenofjeff.com/2017-08-30-randomized-malleable-c2-profiles-made-easy/)
* [Migrating Your infrastructure](https://blog.cobaltstrike.com/2015/10/21/migrating-your-infrastructure/)
* [ICMP C2](https://pentestlab.blog/2017/07/28/command-and-control-icmp/)
* [Using WebDAV features as a covert channel](https://arno0x0x.wordpress.com/2017/09/07/using-webdav-features-as-a-covert-channel/)
* [Safe Red Team Infrastructure](https://medium.com/@malcomvetter/safe-red-team-infrastructure-c5d6a0f13fac)
* [EGRESSING BLUECOAT WITH COBALTSTIKE & LET'S ENCRYPT](https://cybersyndicates.com/2016/12/egressing-bluecoat-with-cobaltstike-letsencrypt/)
* [Command and Control Using Active Directory](http://www.harmj0y.net/blog/powershell/command-and-control-using-active-directory/)
* [A Vision for Distributed Red Team Operations](https://blog.cobaltstrike.com/2013/02/12/a-vision-for-distributed-red-team-operations/)
* [Designing Effective Covert Red Team Attack Infrastructure](https://bluescreenofjeff.com/2017-12-05-designing-effective-covert-red-team-attack-infrastructure/)
* [Serving Random Payloads with Apache mod_rewrite](https://bluescreenofjeff.com/2017-06-13-serving-random-payloads-with-apache-mod_rewrite/)
* [Mail Servers Made Easy](https://blog.inspired-sec.com/archive/2017/02/14/Mail-Server-Setup.html)

* [Securing your Empire C2 with Apache mod_rewrite](https://thevivi.net/2017/11/03/securing-your-empire-c2-with-apache-mod_rewrite/)
* [Automating Gophish Releases With Ansible and Docker](https://jordan-wright.com/blog/post/2018-02-04-automating-gophish-releases/)
* [How to Write Malleable C2 Profiles for Cobalt Strike](https://bluescreenofjeff.com/2017-01-24-how-to-write-malleable-c2-profiles-for-cobalt-strike/)
* [How to Make Communication Profiles for Empire](https://bluescreenofjeff.com/2017-03-01-how-to-make-communication-profiles-for-empire/)
* [A Brave New World: Malleable C2](http://www.harmj0y.net/blog/redteaming/a-brave-new-world-malleable-c2/)
* [Malleable Command and Control](https://www.cobaltstrike.com/help-malleable-c2)

[↑](#table-of-contents) Embedded and Peripheral Devices Hacking
* [Gettting in with the Proxmark3 & ProxBrute](https://www.trustwave.com/Resources/SpiderLabs-Blog/Getting-in-with-the-Proxmark-3-and-ProxBrute/)
* [Practical Guide to RFID Badge copying](https://blog.nviso.be/2017/01/11/a-practical-guide-to-rfid-badge-copying/)
* [Contents of a Physical Pentester Backpack](https://www.tunnelsup.com/contents-of-a-physical-pen-testers-backpack/)
* [MagSpoof - credit card/magstripe spoofer](https://github.com/samyk/magspoof)
* [Wireless Keyboard Sniffer](https://samy.pl/keysweeper/)
* [RFID Hacking with The Proxmark 3](https://blog.kchung.co/rfid-hacking-with-the-proxmark-3/)
* [Swiss Army Knife for RFID](https://www.cs.bham.ac.uk/~garciaf/publications/Tutorial_Proxmark_the_Swiss_Army_Knife_for_RFID_Security_Research-RFIDSec12.pdf)
* [Exploring NFC Attack Surface](https://media.blackhat.com/bh-us-12/Briefings/C_Miller/BH_US_12_Miller_NFC_attack_surface_WP.pdf)
* [Outsmarting smartcards](http://gerhard.dekoninggans.nl/documents/publications/dekoninggans.phd.thesis.pdf)
* [Reverse engineering HID iClass Master keys](https://blog.kchung.co/reverse-engineering-hid-iclass-master-keys/)
* [Android Open Pwn Project (AOPP)](https://www.pwnieexpress.com/aopp)

[↑](#table-of-contents) Misc
* [Red Tips of Vysec](https://github.com/vysec/RedTips)
* [Cobalt Strike Tips for 2016 ccde red teams](https://blog.cobaltstrike.com/2016/02/23/cobalt-strike-tips-for-2016-ccdc-red-teams/)
* [Models for Red Team Operations](https://blog.cobaltstrike.com/2015/07/09/models-for-red-team-operations/)
* [Planning a Red Team exercise](https://github.com/magoo/redteam-plan)
* [Raphael Mudge - Dirty Red Team tricks](https://www.youtube.com/watch?v=oclbbqvawQg)
* [introducing the adversary resilience methodology part 1](https://posts.specterops.io/introducing-the-adversary-resilience-methodology-part-one-e38e06ffd604)
* [introducing the adversary resilience methodology part 2](https://posts.specterops.io/introducing-the-adversary-resilience-methodology-part-two-279a1ed7863d)
* [Responsible red team](https://medium.com/@malcomvetter/responsible-red-teams-1c6209fd43cc)

* [Red Teaming for Pacific Rim CCDC 2017](https://bluescreenofjeff.com/2017-05-02-red-teaming-for-pacific-rim-ccdc-2017/)
* [How I Prepared to Red Team at PRCCDC 2015](https://bluescreenofjeff.com/2015-04-15-how-i-prepared-to-red-team-at-prccdc-2015/)
* [Red Teaming for Pacific Rim CCDC 2016](https://bluescreenofjeff.com/2016-05-24-pacific-rim-ccdc_2016/)
* [Responsible Red Teams](https://medium.com/@malcomvetter/responsible-red-teams-1c6209fd43cc)

[↑](#table-of-contents) RedTeam Gadgets
Network Implants
* [LAN Tap Pro](https://hackerwarehouse.com/product/lan-tap-pro/)
* [LAN Turtle](https://hakshop.com/collections/network-implants/products/lan-turtle)
* [Bash Bunny](https://hakshop.com/collections/physical-access/products/bash-bunny)
* [Packet Squirrel](https://hakshop.com/products/packet-squirrel)
Wifi Auditing
* [WiFi Pineapple](https://hakshop.com/products/wifi-pineapple)
* [Alpha Long range Wireless USB](https://hackerwarehouse.com/product/alfa-802-11bgn-long-range-usb-wireless-adapter/)
* [Wifi-Deauth Monster](https://www.tindie.com/products/lspoplove/dstike-wifi-deauther-monster/)
* [Crazy PA](https://www.amazon.com/gp/product/B00VYA3A2U/ref=as_li_tl)
IoT
* [BLE Key](https://hackerwarehouse.com/product/blekey/)
* [Proxmark3](https://hackerwarehouse.com/product/proxmark3-kit/)
* [Zigbee Sniffer](https://www.attify-store.com/products/zigbee-sniffing-tool-atmel-rzraven)
* [Attify IoT Exploit kit](https://www.attify-store.com/collections/frontpage/products/jtag-exploitation-kit-with-lab-manual)
Software Defined Radio - SDR
* [HackRF One Bundle](https://hackerwarehouse.com/product/hackrf-one-kit/)
* [RTL-SDR](https://hackerwarehouse.com/product/rtlsdr/)
* [YARD stick one Bundle](https://hackerwarehouse.com/product/yard-stick-one-kit/)
* [Ubertooth](https://hackerwarehouse.com/product/ubertooth-one/)
Misc
* [Key Grabber](https://hackerwarehouse.com/product/keygrabber/)
* [Magspoof](https://store.ryscc.com/products/magspoof%20)
* [Poison tap](https://samy.pl/poisontap/)
* [keysweeper](https://samy.pl/keysweeper/)
* [USB Rubber Ducky](https://hakshop.com/collections/physical-access/products/usb-rubber-ducky-deluxe)

[↑](#table-of-contents) Ebooks
* [Next Generation Red Teaming](https://www.amazon.com/Next-Generation-Teaming-Henry-Dalziel/dp/0128041714)
* [Targeted Cyber Attack](https://www.amazon.com/Targeted-Cyber-Attacks-Multi-staged-Exploits/dp/0128006048)
* [Advanced Penetration Testing: Hacking the World's Most Secure Networks](https://www.amazon.com/Advanced-Penetration-Testing-Hacking-Networks/dp/1119367689)

* [Social Engineers' Playbook Practical Pretexting](https://www.amazon.com/Social-Engineers-Playbook-Practical-Pretexting/dp/0692306617/)

[↑](#table-of-contents) Training (Free)
* [Tradecraft - a course on red team operations](https://www.youtube.com/watch?v=IRpS7oZ3z0o&list=PL9HO6M_MU2nesxSmhJjEvwLhUoHPHmXvz)
* [Advanced Threat Tactics Course & Notes](https://blog.cobaltstrike.com/2015/09/30/advanced-threat-tactics-course-and-notes/)
* [FireEye - a whiteboard session on red team operations](https://www.fireeye.com/services/red-team-assessments/red-team-operations-video-training.html)

[↑](#table-of-contents) Certification
* [CREST Certified Simulated Attack Specialist](http://www.crest-approved.org/examination/certified-simulated-attack-specialist/)
* [CREST Certified Simulated Attack Manager](http://www.crest-approved.org/examination/certified-simulated-attack-manager/)
* [SEC564: Red Team Operations and Threat Emulation](https://www.sans.org/course/red-team-operations-and-threat-emulation)
* [ELearn Security Penetration Testing eXtreme](https://www.elearnsecurity.com/course/penetration_testing_extreme/)

awesome-web-hacking
This list is for anyone wishing to learn about web application security but do not have a starting point.

You can help by sending Pull Requests to add more information.

If you're not inclined to make PRs you can tweet me at `@infoslack`

Table of Contents
==========

Books

* http://www.amazon.com/The-Web-Application-Hackers-Handbook/dp/8126533404/ The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws
* http://www.amazon.com/Hacking-Web-Apps-Preventing-Application/dp/159749951X/ Hacking Web Apps: Detecting and Preventing Web Application Security Problems
* http://www.amazon.com/Hacking-Exposed-Web-Applications-Third/dp/0071740643/ Hacking Exposed Web Applications
* http://www.amazon.com/SQL-Injection-Attacks-Defense-Second/dp/1597499633/ SQL Injection Attacks and Defense
* http://www.amazon.com/Tangled-Web-Securing-Modern-Applications/dp/1593273886/ The Tangled WEB: A Guide to Securing Modern Web Applications
* http://www.amazon.com/Web-Application-Obfuscation-Evasion-Filters/dp/1597496049/ Web Application Obfuscation: '-/WAFs..Evasion..Filters//alert(/Obfuscation/)-'
* http://www.amazon.com/XSS-Attacks-Scripting-Exploits-Defense/dp/1597491543/ XSS Attacks: Cross Site Scripting Exploits and Defense
* http://www.amazon.com/Browser-Hackers-Handbook-Wade-Alcorn/dp/1118662091/ The Browser Hacker's Handbook
* http://www.amazon.com/Basics-Web-Hacking-Techniques-Attack/dp/0124166008/ The Basics of Web Hacking: Tools and Techniques to Attack the Web
* http://www.amazon.com/Web-Penetration-Testing-Kali-Linux/dp/1782163166/ Web Penetration Testing with Kali Linux
* http://www.amazon.com/Web-Application-Security-Beginners-Guide/dp/0071776168/ Web Application Security, A Beginner's Guide
* https://www.crypto101.io/ - Crypto 101 is an introductory course on cryptography
* http://www.offensive-security.com/metasploit-unleashed/ - Metasploit Unleashed
* http://www.cl.cam.ac.uk/~rja14/book.html - Security Engineering
* https://www.feistyduck.com/library/openssl-cookbook/ - OpenSSL Cookbook

Documentation

* https://www.owasp.org/ - Open Web Application Security Project
* http://www.pentest-standard.org/ - Penetration Testing Execution Standard
* http://www.binary-auditing.com/ - Dr. Thorsten Schneider's Binary Auditing
* https://appsecwiki.com/ - Application Security Wiki is an initiative to provide all Application security related resources to Security Researchers and developers at one place.

Tools

* http://www.metasploit.com/ - World's most used penetration testing software
* http://www.arachni-scanner.com/ - Web Application Security Scanner Framework
* https://github.com/sullo/nikto - Nikto web server scanner
* http://www.tenable.com/products/nessus-vulnerability-scanner - Nessus Vulnerability Scanner
* http://www.portswigger.net/burp/intruder.html - Burp Intruder is a tool for automating customized attacks against web apps.
* http://www.openvas.org/ - The world's most advanced Open Source vulnerability scanner and manager.
* https://github.com/iSECPartners/Scout2 - Security auditing tool for AWS environments
* https://www.owasp.org/index.php/Category:OWASP_DirBuster_Project - Is a multi threaded java application designed to brute force directories and files names on web/application servers.

* https://www.owasp.org/index.php/ZAP - The Zed Attack Proxy is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.
* https://github.com/tecknicaltom/dsniff - dsniff is a collection of tools for network auditing and penetration testing.
* https://github.com/WangYihang/Webshell-Sniper - Manage your webshell via terminal.
* https://github.com/DanMcInerney/dnsspoof - DNS spoofer. Drops DNS responses from the router and replaces it with the spoofed DNS response
* https://github.com/trustedsec/social-engineer-toolkit - The Social-Engineer Toolkit (SET) repository from TrustedSec
* https://github.com/sqlmapproject/sqlmap - Automatic SQL injection and database takeover tool
* https://github.com/beefproject/beef - The Browser Exploitation Framework Project
* http://w3af.org/ - w3af is a Web Application Attack and Audit Framework
* https://github.com/espreto/wpsploit - WPSploit, Exploiting Wordpress With Metasploit
* https://github.com/WangYihang/Reverse-Shell-Manager - Reverse shell manager via terminal.
* https://github.com/RUB-NDS/WS-Attacker - WS-Attacker is a modular framework for web services penetration testing
* https://github.com/wpscanteam/wpscan - WPScan is a black box WordPress vulnerability scanner
* http://sourceforge.net/projects/paros/ Paros proxy
* https://www.owasp.org/index.php/Category:OWASP_WebScarab_Project Web Scarab proxy
* https://code.google.com/p/skipfish/ Skipfish, an active web application security reconnaissance tool
* http://www.acunetix.com/vulnerability-scanner/ Acunetix Web Vulnerability Scanner
* https://cystack.net/ CyStack Web Security Platform
* http://www-03.ibm.com/software/products/en/appscan IBM Security AppScan
* https://www.netsparker.com/web-vulnerability-scanner/ Netsparker web vulnerability scanner
* http://www8.hp.com/us/en/software-solutions/webinspect-dynamic-analysis-dast/index.html HP Web Inspect
* https://github.com/sensepost/wikto Wikto - Nikto for Windows with some extra features
* http://samurai.inguardians.com Samurai Web Testing Framework
* https://code.google.com/p/ratproxy/ Ratproxy
* http://www.websecurify.com Websecurify
* http://sourceforge.net/projects/grendel/ Grendel-scan
* https://www.owasp.org/index.php/Category:OWASP_DirBuster_Project DirBuster
* http://www.edge-security.com/wfuzz.php Wfuzz
* http://wapiti.sourceforge.net wapiti
* https://github.com/neuroo/grabber Grabber
* https://subgraph.com/vega/ Vega
* http://websecuritytool.codeplex.com Watcher passive web scanner
* http://xss.codeplex.com x5s XSS and Unicode transformations security testing assistant
* http://www.beyondsecurity.com/avds AVDS Vulnerability Assessment and Management
* http://www.golismero.com Golismero
* http://www.ikare-monitoring.com IKare
* http://www.nstalker.com N-Stalker X
* https://www.rapid7.com/products/nexpose/index.jsp Nexpose
* http://www.rapid7.com/products/appspider/ App Spider
* http://www.milescan.com ParosPro
* https://www.qualys.com/enterprises/qualysguard/web-application-scanning/ Qualys Web Application Scanning
* http://www.beyondtrust.com/Products/RetinaNetworkSecurityScanner/ Retina

* https://www.owasp.org/index.php/OWASP_Xenotix_XSS_Exploit_Framework Xenotix XSS Exploit Framework
* https://github.com/future-architect/vuls Vulnerability scanner for Linux, agentless, written in golang.
* https://github.com/rastating/wordpress-exploit-framework A Ruby framework for developing and using modules which aid in the penetration testing of WordPress powered websites and systems.
* http://www.xss-payloads.com/ XSS Payloads to leverage XSS vulnerabilities, build custom payloads, practice penetration testing skills.
* https://github.com/joaomatosf/jexboss JBoss (and others Java Deserialization Vulnerabilities) verify and EXploitation Tool
* https://github.com/commixproject/commix Automated All-in-One OS command injection and exploitation tool
* https://github.com/pathetiq/BurpSmartBuster A Burp Suite content discovery plugin that add the smart into the Buster!
* https://github.com/GoSecure/csp-auditor Burp and ZAP plugin to analyze CSP headers
* https://github.com/ffleming/timing_attack Perform timing attacks against web applications
* https://github.com/lalithr95/fuzzapi Fuzzapi is a tool used for REST API pentesting
* https://github.com/owtf/owtf Offensive Web Testing Framework (OWTF)
* https://github.com/nccgroup/wssip Application for capturing, modifying and sending custom WebSocket data from client to server and vice versa.
* https://github.com/tijme/angularjs-csti-scanner Automated client-side template injection (sandbox escape/bypass) detection for AngularJS (ACSTIS).
* https://reshift.softwaresecured.com A source code analysis tool for detecting and managing Java security vulnerabilities.

Cheat Sheets

* http://n0p.net/penguicon/php_app_sec/mirror/xss.html - XSS cheatsheet
* https://highon.coffee/blog/lfi-cheat-sheet/ - LFI Cheat Sheet
* https://highon.coffee/blog/reverse-shell-cheat-sheet/ - Reverse Shell Cheat Sheet
* https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/ - SQL Injection Cheat Sheet
* https://www.gracefulsecurity.com/path-traversal-cheat-sheet-windows/ - Path Traversal Cheat Sheet: Windows

Docker images for Penetration Testing

* `docker pull kalilinux/kali-linux-docker` [official Kali Linux](https://hub.docker.com/r/kalilinux/kali-linux-docker/)
* `docker pull owasp/zap2docker-stable` - [official OWASP ZAP](https://github.com/zaproxy/zaproxy)
* `docker pull wpscanteam/wpscan` - [official WPScan](https://hub.docker.com/r/wpscanteam/wpscan/)
* `docker pull pandrew/metasploit` - [docker-metasploit](https://hub.docker.com/r/pandrew/metasploit/)
* `docker pull citizenstig/dvwa` - [Damn Vulnerable Web Application (DVWA)](https://hub.docker.com/r/citizenstig/dvwa/)
* `docker pull wpscanteam/vulnerablewordpress` - [Vulnerable WordPress Installation](https://hub.docker.com/r/wpscanteam/vulnerablewordpress/)

* `docker pull hmlio/vaas-cve-2014-6271` - [Vulnerability as a service: Shellshock](https://hub.docker.com/r/hmlio/vaas-cve-2014-6271/)
* `docker pull hmlio/vaas-cve-2014-0160` - [Vulnerability as a service: Heartbleed](https://hub.docker.com/r/hmlio/vaas-cve-2014-0160/)
* `docker pull opendns/security-ninjas` - [Security Ninjas](https://hub.docker.com/r/opendns/security-ninjas/)
* `docker pull usertaken/archlinux-pentest-lxde` - [Arch Linux Penetration Tester](https://hub.docker.com/r/usertaken/archlinux-pentest-lxde/)
* `docker pull diogomonica/docker-bench-security` - [Docker Bench for Security](https://hub.docker.com/r/diogomonica/docker-bench-security/)
* `docker pull ismisepaul/securityshepherd` - [OWASP Security Shepherd](https://hub.docker.com/r/ismisepaul/securityshepherd/)
* `docker pull danmx/docker-owasp-webgoat` - [OWASP WebGoat Project docker image](https://hub.docker.com/r/danmx/docker-owasp-webgoat/)
* `docker pull citizenstig/nowasp` - [OWASP Mutillidae II Web Pen-Test Practice Application](https://hub.docker.com/r/citizenstig/nowasp/)

Vulnerabilities

* http://cve.mitre.org/ - Common Vulnerabilities and Exposures. The Standard for Information Security Vulnerability Names
* https://www.exploit-db.com/ - The Exploit Database – ultimate archive of Exploits, Shellcode, and Security Papers.
* http://0day.today/ - Inj3ct0r is the ultimate database of exploits and vulnerabilities and a great resource for vulnerability researchers and security professionals.
* http://osvdb.org/ - OSVDB's goal is to provide accurate, detailed, current, and unbiased technical security information.
* http://www.securityfocus.com/ - Since its inception in 1999, SecurityFocus has been a mainstay in the security community.
* http://packetstormsecurity.com/ - Global Security Resource
* https://wpvulndb.com/ - WPScan Vulnerability Database

Courses

* https://www.elearnsecurity.com/course/web_application_penetration_testing/ eLearnSecurity Web Application Penetration Testing
* https://www.elearnsecurity.com/course/web_application_penetration_testing_extreme/ eLearnSecurity Web Application Penetration Testing eXtreme
* https://www.offensive-security.com/information-security-training/advanced-web-attack-and-exploitation/ Offensive Security Advanced Web Attacks and Exploitation (live)
* https://www.sans.org/course/web-app-penetration-testing-ethical-hacking Sans SEC542: Web App Penetration Testing and Ethical Hacking
* https://www.sans.org/course/advanced-web-app-penetration-testing-ethical-hacking Sans SEC642: Advanced Web App Penetration Testing and Ethical Hacking * http://opensecuritytraining.info/ - Open Security Training
* http://securitytrainings.net/security-trainings/ - Security Exploded Training
* http://www.cs.fsu.edu/~redwood/OffensiveComputerSecurity/ - FSU - Offensive Computer Security
* http://www.cs.fsu.edu/~lawrence/OffNetSec/ - FSU - Offensive Network Security

* http://www.securitytube.net/ - World's largest Infosec and Hacking Portal.
* https://www.hacker101.com/ - Free class for web security by [Hackerone](https://www.hackerone.com)

Online Hacking Demonstration Sites

* http://testasp.vulnweb.com/ - Acunetix ASP test and demonstration site
* http://testaspnet.vulnweb.com/ - Acunetix ASP.Net test and demonstration site
* http://testphp.vulnweb.com/ - Acunetix PHP test and demonstration site
* http://crackme.cenzic.com/kelev/view/home.php - Crack Me Bank
* http://zero.webappsecurity.com/ - Zero Bank
* http://demo.testfire.net/ - Altoro Mutual

Labs

* http://www.cis.syr.edu/~wedu/seed/all_labs.html - Developing Instructional Laboratories for Computer SEcurity EDucation
* https://www.vulnhub.com/ - Virtual Machines for Localhost Penetration Testing.
* https://pentesterlab.com/ - PentesterLab is an easy and great way to learn penetration testing.
* https://github.com/jerryhoff/WebGoat.NET - This web application is a learning platform about common web security flaws.
* http://www.dvwa.co.uk/ - Damn Vulnerable Web Application (DVWA)
* http://sourceforge.net/projects/lampsecurity/ - LAMPSecurity Training
* https://github.com/Audi-1/sqli-labs - SQLI labs to test error based, Blind boolean based, Time based.
* https://github.com/paralax/lfi-labs - small set of PHP scripts to practice exploiting LFI, RFI and CMD injection vulns
* https://hack.me/ - Build, host and share vulnerable web apps in a sandboxed environment for free
* http://azcwr.org/az-cyber-warfare-ranges - Free live fire Capture the Flag, blue team, red team Cyber Warfare Range for beginners through advanced users. Must use a cell phone to send a text message requesting access to the range.
* https://github.com/adamdoupe/WackoPicko - WackoPicko is a vulnerable web application used to test web application vulnerability scanners.
* https://github.com/rapid7/hackazon - Hackazon is a free, vulnerable test site that is an online storefront built with the same technologies used in today's rich client and mobile applications.
* https://github.com/RhinoSecurityLabs/cloudgoat - Rhino Security Labs' "Vulnerable by Design" AWS infrastructure setup tool
* https://www.hackthebox.eu/ - Hack The Box is an online platform allowing you to test and advance your skills in cyber security.

SSL

* https://www.ssllabs.com/ssltest/index.html - This service performs a deep analysis of the configuration of any SSL web server on the public Internet.
* https://raymii.org/s/tutorials/Strong_SSL_Security_On_nginx.html - Strong SSL Security on nginx
* https://weakdh.org/ - Weak Diffie-Hellman and the Logjam Attack
* https://letsencrypt.org/ - Let's Encrypt is a new Certificate Authority: It's free, automated, and open.
* https://filippo.io/Heartbleed/ - A checker (site and tool) for CVE-2014-0160 (Heartbleed).

Security Ruby on Rails

* http://brakemanscanner.org/ - A static analysis security vulnerability scanner for Ruby on Rails applications.
* https://github.com/rubysec/ruby-advisory-db - A database of vulnerable Ruby Gems
* https://github.com/rubysec/bundler-audit - Patch-level verification for Bundler
* https://github.com/hakirisec/hakiri_toolbelt - Hakiri Toolbelt is a command line interface for the Hakiri platform.
* https://hakiri.io/facets - Scan Gemfile.lock for vulnerabilities.
* http://rails-sqli.org/ - This page lists many query methods and options in ActiveRecord which do not sanitize raw SQL arguments and are not intended to be called with unsafe user input.
* https://github.com/0xsauby/yasuo - A ruby script that scans for vulnerable & exploitable 3rd-party web applications on a network

Awesome Hacking Tools

A collection of awesome lists for hackers, pentesters & security researchers.

A curated list of awesome Hacking Tools. Your contributions are always welcome !

Awesome Repositories
Repository	Description
[Awesome Malware Analysis](https://github.com/rshipp/awesome-malware-analysis)	A curated list of awesome malware analysis tools and resources
[Awesome-Hacking](https://github.com/Hack-with-Github/Awesome-Hacking)	A collection of various awesome lists for hackers, pentesters and security researchers
[Awesome-osint](https://github.com/jivoi/awesome-osint)	A curated list of amazingly awesome OSINT
[fuzzdb](https://github.com/fuzzdb-project/fuzzdb)	Dictionary of attack patterns and primitives for black-box application fault injection and resource discovery.
[HUNT Proxy Extension](https://github.com/bugcrowd/HUNT)	Identify common parameters vulnerable to certain vulnerability classes (HUNT Scanner, availible for Burp Suite PRO and ZAProxy). Organize testing methodologies (currently avalible only inside of Burp Suite).
[List of Sec talks/videos](https://github.com/PaulSec/awesome-sec-talks)	A curated list of awesome Security talks
[Scanners-Box](https://github.com/We5ter/Scanners-Box)	The toolbox of open source scanners
[SecLists](https://github.com/danielmiessler/SecLists)	It is a collection of multiple types of lists used during security assessments
[Xerosploit](https://github.com/LionSec/xerosploit)	Efficient and advanced man in the middle framework
[ctf-tools](https://github.com/zardus/ctf-tools)	Some setup scripts for security research tools.
[PENTEST-WIKI](https://github.com/nixawk/pentest-wiki)	PENTEST-WIKI is a free online security knowledge library for pentesters / researchers. If you have a good idea, please share it with others.

Awesome custom projects / Scripts

Name	Description
[mimikatz](https://github.com/gentilkiwi/mimikatz)	A useful tool to play with Windows security including extracting plaintext passwords, kerberos tickets, etc.
[LAZY script v2.1.3](https://github.com/arismelachroinos/lscript)	The LAZY script will make your life easier, and of course faster.
[XSStrike](https://github.com/UltimateHackers/XSStrike)	XSStrike is a program which can fuzz and bruteforce parameters for XSS. It can also detect and bypass WAFs.

Exploitation tools
Name	Description
[BeEF](http://beefproject.com/)	Browser Exploitation Framework (Beef)
[Core Impact](https://www.coresecurity.com/core-impact)	Core Impact provides vulnerability assessment and penetration security testing throughout your organization.
[Metasploit](https://www.metasploit.com/)	The world's most used penetration testing framework

Linux Security Tools
Name	Description
[DefenseMatrix](https://github.com/K4YT3X/DefenseMatrix)	Full security solution for Linux Servers
[Kernelpop](https://github.com/spencerdodd/kernelpop)	kernel privilege escalation enumeration and exploitation framework
[Lynis](https://github.com/CISOfy/lynis)	Security auditing tool for Linux, macOS, and UNIX-based systems.
[linux-explorer](https://github.com/intezer/linux-explorer)	Easy-to-use live forensics toolbox for Linux endpoints

Exploit Databases
Name	Description
[0day](http://0day.today/)	Inj3ct0r is the ultimate database of exploits and vulnerabilities and a great resource for vulnerability researchers and security professionals.
[cxsecurity](http://cxsecurity.com/exploit)	Exploit Database
[exploit-db](https://www.exploit-db.com/)	Exploits Database by Offensive Security
[iedb](http://iedb.ir/)	Iranian Exploit DataBase
[rapid7](https://rapid7.com/db)	Vulnerability & Exploit Database - Rapid7

MITM tools
Name	Description
[BetterCAP](https://www.bettercap.org/)	MITM attacks against a network, manipulate HTTP, HTTPS and TCP traffic in realtime, sniff for credentials and much more.
[Burp Suite](https://portswigger.net/burp)	GUI based tool for testing Web application security.
[Ettercap](https://ettercap.github.io/ettercap/)	Ettercap is a comprehensive suite for man in the middle attacks
[Evilginx](https://github.com/kgretzky/evilginx)	Man-in-the-middle attack framework used for phishing credentials and session cookies of any web service.

[MITMf](https://github.com/byt3bl33d3r/MITMf) | Framework for Man-In-The-Middle attacks
[mitmproxy](https://mitmproxy.org/) | An interactive console program that allows traffic flows to be intercepted, inspected, modified and replayed

SQL Injection
Name	Description
[SQLmap](http://sqlmap.org/)	Automatic SQL injection and database takeover tool
[SQLninja](http://sqlninja.sourceforge.net/)	SQL Server injection & takeover tool
[SQLiv](https://github.com/Hadesy2k/sqliv)	Massive SQL injection scanner

Post explotation
Name	Description
[Portia](https://github.com/SpiderLabs/portia)	Portia aims to automate a number of techniques commonly performed on internal network penetration tests after a low privileged account has been compromised.
[RSPET](https://github.com/panagiks/RSPET)	RSPET (Reverse Shell and Post Exploitation Tool) is a Python based reverse shell equipped with functionalities that assist in a post exploitation scenario.

Search Engine for Penetration Tester
Name	Description
[Censys](https://www.censys.io/)	Censys continually monitors every reachable server and device on the Internet, so you can search for and analyze them in real time
[Shodan](http://shodan.io/)	Shodan is the world's first search engine for Internet-connected devices.
[WiGLE](https://wigle.net/index)	Maps and database of 802.11 wireless networks, with statistics, submitted by wardrivers, netstumblers, and net huggers.
[Zoomeye](https://www.zoomeye.org/)	search engine for cyberspace that lets the user find specific network components(ip, services, etc.)
Security Information and Event Management (SIEM)
Name	Description
[OSSIM](https://www.alienvault.com/products/ossim)	AlienVault’s Open Source Security Information and Event Management (SIEM) product

Network Scanning Tools
Name	Description
[NMAP](https://nmap.org/)	The industry standard in network/port scanning. Widely used.
[Wireshark](https://www.wireshark.org/)	A versatile and feature-packed packet sniffing/analysis tool.

Source Code Analysis Tools
Name	Description
[pyup](https://pyup.io/)	Automated Security and Dependency Updates
[RIPS](https://www.ripstech.com/)	PHP Security Analysis

[Retire.js](http://retirejs.github.io/retire.js/) | detecting the use of JavaScript libraries with known vulnerabilities
[Snyk](https://snyk.io/) | find & fix vulnerabilities in dependencies, supports various languages

Binary Analysis Tools
Name	Description
[BinNavi](https://github.com/google/binnavi)	BinNavi is a binary analysis IDE that allows to inspect, navigate, edit and annotate control flow graphs and call graphs of disassembled code
[Radare2](https://github.com/radare/radare2)	Radare2 is a reverse engineering suite which includes a complete toolkit for reverse enigneering needs.

Collaboration tools
Name	Description
[Dradis](https://dradisframework.com/ce/)	Open-source reporting and collaboration tool for InfoSec professionals

Linux privilege escalation
- https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/
- https://www.kernel-exploits.com/
- https://github.com/rebootuser/LinEnum
- https://github.com/PenturaLabs/Linux_Exploit_Suggester
- https://www.securitysift.com/download/linuxprivchecker.py
- http://pentestmonkey.net/tools/audit/unix-privesc-check
- https://github.com/mzet-/linux-exploit-suggester
- http://www.darknet.org.uk/2015/06/unix-privesc-check-unixlinux-user-privilege-escalation-scanner/
- https://www.youtube.com/watch?v=dk2wsyFiosg
- http://resources.infosecinstitute.com/privilege-escalation-linux-live-examples/\#gref
- https://www.rebootuser.com/?p=1758

My OSCP-prep collection_

[exam tips](https://github.com/ex16x41/OSCP-prep/blob/master/exam-tips.md)

[kali commands](https://github.com/Eva-Prokofiev/OSCP-prep/blob/master/Other/Kali-Env)

[scanning/enum](https://github.com/ex16x41/OSCP-prep/blob/master/methodology-notes.md)

[backdoors/shells](https://github.com/ex16x41/OSCP-prep/blob/master/Other/Backdoors-Web%20Shells.md)

[modifying exploits](https://github.com/ex16x41/OSCP-prep/blob/master/modifying-exploits.md)

[privesc-linux(&& shell escape)](https://github.com/ex16x41/OSCP-prep/blob/master/linux-privesc.md)

[privesc-windows](https://github.com/ex16x41/OSCP-prep/blob/master/win-privesc.md)

[post-exploitation(linux+win)](https://github.com/Eva-Prokofiev/OSCP-prep/blob/master/Other/post-exploitation.py)

[cross-compiling](https://github.com/ex16x41/OSCP-prep/blob/master/Other/Cross-compiling.md)

[file transfer](https://github.com/Eva-Prokofiev/OSCP-prep/blob/master/Other/File%20Transfer.txt)

[pivoting guides](https://github.com/Eva-Prokofiev/OSCP-prep/blob/master/Other/Pivoting.txt)

[practice & write-ups](https://github.com/ex16x41/OSCP-prep/blob/master/practice-sources)

CTF / WARGAMES / OTHERS..

very nice for web app tests > https://www.hacksplaining.com/

https://lab.pentestit.ru/pentestlabs/3
https://trailofbits.github.io/ctf/
http://smashthestack.org/
Google Gruyere
http://google-gruyere.appspot.com/
Hack This Site
http://www.hackthissite.org/
HackThis
http://www.hackthis.co.uk/
Hacking-Lab
https://www.hacking-lab.com
Hacker Test
http://www.hackertest.net/
Hax.Tor
http://hax.tor.hu/
OverTheWire
http://www.overthewire.org/wargames/
DEF CON CTF Archive
https://www.defcon.org/html/links/dc-ctf.html

A few Vulnhub VMs that are lookalike the oscp machines

- Kioptrix: Level 1 (#1)
- Kioptrix: Level 1.1 (#2)
- Kioptrix: Level 1.2 (#3)
- Kioptrix: Level 1.3 (#4)
- FristiLeaks: 1.3
- Stapler: 1
- PwnLab: init
- Tr0ll: 1

Tr0ll: 2
Kioptrix: 2014
Lord Of The Root: 1.0.1
Stapler: 1
Mr-Robot: 1
HackLAB: Vulnix
VulnOS: 2
SickOs: 1.2
pWnOS: 2.0

Other people's exp and journey to OSCP and some of my favorite

https://medium.com/@hakluke/haklukes-ultimate-oscp-guide-part-1-is-oscp-for-you-b57cbcce7440?source=user_profile---------13----------
https://medium.com/@hakluke/haklukes-ultimate-oscp-guide-part-2-workflow-and-documentation-tips-9dd335204a48
https://medium.com/@cosmin.ciobanu/the-only-oscp-advice-you-will-need-ae141060b87c
https://0x00sec.org/t/rains-pwk-oscp-write-up-and-ama/8164
https://scriptdotsh.com/index.php/2018/04/17/31-days-of-oscp-experience/
https://www.lewisecurity.com/i-am-finally-an-oscp/
https://prasannakumar.in/infosec/my-walk-towards-cracking-oscp/

Watch all IPPSEC videos
https://www.youtube.com/channel/UCa6eh7gCkpPo5XXUDfygQQA

Buffer Overflows

#EIP OVERWRITE
http://www.primalsecurity.net/0x0-exploit-tutorial-buffer-overflow-vanilla-eip-overwrite-2/

#Exploiting "Vulnerable Server" for Windows 7
https://samsclass.info/127/proj/vuln-server.htm

#Manually checking for Bad Characters
http://www.bulbsecurity.com/finding-bad-characters-with-immunity-debugger-and-mona-py/

#Nice BOF write-ups
Vulnhub VM:https://www.vulnhub.com/entry/brainpan-1,51/
Write-up:https://blog.vonhewitt.com/2017/11/brainpan1/
Youtube:https://www.youtube.com/watch?v=ohCY8CD6mSs (3 part series)

#SANS training -BOF
https://www.sans.org/reading-room/whitepapers/threats/paper/481

To Do

- Properly categorise everything

- Figure out what categories to actually use!
  - Binary hacking / web app testing / infrastructure pentesting etc. are all pretty big areas, use these as main categories?
  - Method: Keep finding and adding stuff until it becomes unmaintainable without categories.

- Work on the process document, making things gradually more automated!

- Add the following links:

http://pwnable.kr/

https://microcorruption.com/login

https://www.hackthis.co.uk/

https://www.sabrefilms.co.uk/revolutionelite/

https://www.wechall.net/

https://cryptopals.com/

https://holidayhackchallenge.com/past-challenges/

OSCP Links
24x7x365 SUPPORT http://www.captiongenerator.com/320492/Offsec-Student-Admins

https://natesubra.com/go/oscp

OSCP Syllabus:
https://www.offensive-security.com/information-security-training/penetration-testing-training-kali-linux/

Windows Privilege Escalation:
http://www.fuzzysecurity.com/tutorials/16.html
https://pentest.blog/windows-privilege-escalation-methods-for-pentesters/
http://it-ovid.blogspot.com/2012/02/windows-privilege-escalation.html
https://toshellandback.com/2015/11/24/ms-priv-esc/

Windows Post Exploitation:
http://www.handgrep.se/repository/cheatsheets/postexploitation/WindowsPost-Exploitation.pdf

Mubix: https://docs.google.com/document/d/1U10isynOpQtrIK6ChuReu-K1WHTJm4fgG3joiuz43rw/edit?hl=en_US

Linux Privilege Escalation:
https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/
https://speakerdeck.com/knaps/escape-from-shellcatraz-breaking-out-of-restricted-unix-shells

Linux Post Exploitation:
https://n0where.net/linux-post-exploitation/
Mubix: https://docs.google.com/document/d/1ObQB6hmVvRPCgPTRZM5NMH034VDM-1N-EWPRz2770K4/edit?hl=en_US#

Metasploit
https://www.offensive-security.com/metasploit-unleashed/
http://www.securitytube.net/groups?operation=view&groupId=8
Postex:
https://docs.google.com/document/d/1ZrDJMQkrp_YbU_9Ni9wMNF2m3nIPEA_kekqqqA2Ywto/edit

Pivoting:
https://pentest.blog/explore-hidden-networks-with-double-pivoting/
http://nerderati.com/2011/03/17/simplify-your-life-with-an-ssh-config-file/

OSCP Reviews:
https://localhost.exposed/path-to-oscp/
http://www.en-lightn.com/?p=941
http://www.securitysift.com/offsec-pwb-oscp/
https://blog.g0tmi1k.com/2011/07/pentesting-with-backtrack-pwb/
http://www.jasonbernier.com/oscp-review/
https://n3ko1.github.io/certification/2015/05/27/oscp---offensive-security-certified-professional/

Precompiled Exploits:
https://github.com/offensive-security/exploit-database-bin-sploits
https://www.kernel-exploits.com/

MSFVenom:
http://netsec.ws/?p=331
http://www.securityunlocked.com/2016/01/02/network-security-pentesting/most-useful-msfvenom-payloads/

Shellcode:
http://www.primalsecurity.net/0x0-shellcoding-tutorial-introduction-to-asm/
https://paraschetal.in/writing-your-own-shellcode
http://althing.cs.dartmouth.edu/local/shellcode.html
https://www.exploit-db.com/docs/17065.pdf

Rev/Web Shells:
http://tools.kali.org/maintaining-access/webshells
http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

https://github.com/stasinopoulos/commix/wiki/Upload-shells
https://highon.coffee/blog/reverse-shell-cheat-sheet/
https://github.com/JohnTroony/php-webshells

Spawn TTY Shell:
http://netsec.ws/?p=337

Tools
http://tools.kali.org/tools-listing
http://tools.kali.org/password-attacks/patator
http://tools.kali.org/web-applications/dirb
http://tools.kali.org/web-applications/dirbuster
http://tools.kali.org/web-applications/gobuster
http://tools.kali.org/web-applications/wpscan
http://tools.kali.org/web-applications/joomscan
http://tools.kali.org/vulnerability-analysis/sqlmap
http://tools.kali.org/exploitation-tools/commix
http://tools.kali.org/maintaining-access/weevely
http://tools.kali.org/password-attacks/ncrack
http://tools.kali.org/password-attacks/cewl
http://tools.kali.org/information-gathering/dotdotpwn
http://tools.kali.org/exploitation-tools/shellnoob

Wordlists
http://tools.kali.org/password-attacks/wordlists
https://github.com/danielmiessler/SecLists
https://github.com/govolution/betterdefaultpasslist

Pen Test Cheat Sheets:
https://github.com/Hack-with-Github/Awesome-Hacking
https://jivoi.github.io/2015/07/01/pentest-tips-and-tricks/
http://pwnwiki.io/
https://github.com/enaqx/awesome-pentest

Red-Team-Curation-List
A list to discover red team tooling and methodology for penetration testing and security assessment

Feel free to add any red team related entries to this list.

[Red Team Infrastructure Wiki](https://github.com/bluscreenofjeff/Red-Team-Infrastructure-Wiki)

[Awesome Penetration Testing](https://github.com/enaqx/awesome-pentest)

[Awesome Hacking](https://github.com/Hack-with-Github/Awesome-Hacking)

[Awesome Pentest Cheat Sheets](https://github.com/coreb1t/awesome-pentest-cheat-sheets)

[Mobile Application Penetration Testing Cheat Sheet](https://github.com/tanprathan/MobileApp-Pentest-Cheatsheet)

[Android Security Awesome Tools](https://github.com/ashishb/android-security-awesome#tools)

[Most usable tools for iOS penetration testing](https://github.com/ansjdnakjdnajkd/iOS)

[iOS Malware Samples](https://github.com/ashishb/ios-malware)

[Curated list of public penetration test reports released by several consulting firms and academic security groups](https://github.com/juliocesarfort/public-pentesting-reports)

[Awesome Static Analysis](https://github.com/mre/awesome-static-analysis)

[Awesome Web Hacking](https://github.com/infoslack/awesome-web-hacking)

[Awesome CTF](https://github.com/We5ter/Awesome-Platforms/blob/master/CTF-Platforms.md)

This wiki is intended to provide a resource for setting up a resilient Red Team infrastructure. It was made to complement Steve Borosh ([@424f424f](https://twitter.com/424f424f)) and Jeff Dimmock's ([@bluscreenofjeff](https://twitter.com/bluscreenofjeff)) BSides NoVa 2017 talk "Doomsday Preppers: Fortifying Your Red Team Infrastructure" ([slides](https://speakerdeck.com/rvrsh3ll/doomsday-preppers-fortifying-your-red-team-infrastructure))

If you have an addition you'd like to make, please submit a Pull Request or file an issue on the repo.

THANK YOU to all of the authors of the content referenced in this wiki and to all who [contributed](#thanks-to-contributors)!

Table of Contents

Design Considerations

Functional Segregation
When designing a red team infrastructure that needs to stand up to an active response or last for a long-term engagement (weeks, months, years), it's important to segregate each asset based on function. This provides resilience and agility against the Blue Team when campaign assets start getting detected. For example, if an assessment's phishing email is identified, the Red Team would only need to create a new SMTP server and payload hosting server, rather than a whole team server setup.

Consider segregating these functions on different assets:
* Phishing SMTP
* Phishing payloads
* Long-term command and control (C2)
* Short-term C2

Each of these functions will likely be required for each social engineering campaign. Since active incident response is typical in a Red Team assessment, a new set of infrastructure should be implemented for each campaign.

Using Redirectors
To further resilience and concealment, every back-end asset (i.e. team server) should have a redirector placed in front of it. The goal is to always have a host between our target and our backend servers.

Setting up the infrastructure in this manner makes rolling fresh infrastructure much quicker and easier - no need to stand up a new team server, migrate sessions, and reconnect non-burned assets on the backend.

Common redirector types:
* SMTP
* Payloads
* Web Traffic
* C2 (HTTP(S), DNS, etc)

Each redirector type has multiple implementation options that best fit different scenarios. These options are discussed in further detail in the [Redirectors](#redirectors) section of the wiki. Redirectors can be VPS hosts, dedicated servers, or even apps running on a Platform-as-a-Service instance.

Sample Design
Here is a sample design, keeping functional segregation and redirector usage in mind:

![Sample Infrastructure Setup](./images/sample-setup.png)

Further Resources

* [A Vision for Distributed Red Team Operations - Raphael Mudge (@armitagehacker)](https://blog.cobaltstrike.com/2013/02/12/a-vision-for-distributed-red-team-operations/)

* [Infrastructure for Ongoing Red Team Operations - Raphael Mudge](https://blog.cobaltstrike.com/2014/09/09/infrastructure-for-ongoing-red-team-operations/)

* [Advanced Threat Tactics (2 of 9): Infrastructure - Raphael Mudge](https://www.youtube.com/watch?v=3gBJOJb8Oi0)

* [Cloud-based Redirectors for Distributed Hacking - Raphael Mudge](https://blog.cobaltstrike.com/2014/01/14/cloud-based-redirectors-for-distributed-hacking/)

* [6 Red Team Infrastructure Tips - Alex Rymdeko-Harvey (@killswitch-gui)](https://cybersyndicates.com/2016/11/top-red-team-tips/)

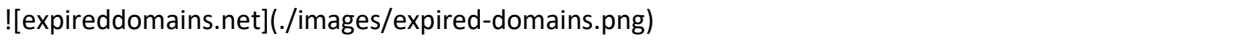
* [How to Build a C2 Infrastructure with Digital Ocean – Part 1 - Lee Kagan (@invokethreatguy)](https://www.blackhillsinfosec.com/build-c2-infrastructure-digital-ocean-part-1/)

* [Automated Red Team Infrastructure Deployment with Terraform - Part 1 - Rasta Mouse (@_RastaMouse)](https://rastamouse.me/2017/08/automated-red-team-infrastructure-deployment-with-terraform---part-1/)

Domains
Perceived domain reputation will vary greatly depending on the products your target is using, as well as their configuration. As such, choosing a domain that will work on your target is not an exact science.

Open source intelligence gathering (OSINT) will be critical in helping make a best guess at the state of controls and which resources to check domains against. Luckily, online advertisers face the same problems and have created some solutions we can leverage.

expireddomains.net is a search engine for recently expired or dropped domains. It provides search and advanced filtering, such as age of expiration, number of backlinks, number of Archive.org snapshots, [SimilarWeb](https://www.similarweb.com/) score. Using the site, we can register pre-used domains, which will come with domain age, that look similar to our target, look similar to our impersonation, or simply are likely to blend in on our target's network.



When choosing a domain for C2 or data exfiltration, consider choosing a domain categorized as Finance or Healthcare. Many organizations will not perform SSL middling on those categories due to the possibility of legal or data sensitivity issues. It is also important to ensure your chosen domain is not associated with any previous malware or phishing campaigns.

The tool [CatMyFish](https://github.com/Mr-Un1k0d3r/CatMyFish) by Charles Hamilton([@MrUn1k0d3r](https://twitter.com/mrun1k0d3r)) automates searches and web categorization checking with expireddomains.net and BlueCoat. It can be modified to apply more filters to searches or even perform long term monitoring of assets you register.

Another tool, [DomainHunter](https://github.com/minisllc/domainhunter) by Joe Vest ([@joevest](https://twitter.com/joevest)) & Andrew Chiles ([@andrewchiles](https://twitter.com/andrewchiles)), returns BlueCoat/WebPulse, IBM X-Force, and Cisco Talos categorization, domain age, alternate available TLDs, Archive.org links, and an HTML report. Additionally, it performs checks for use in known malware and phishing campaigns using Malwaredomains.com and MXToolBox. This tool also includes OCR support for bypassing the BlueCoat/WebPulse captchas. Check out the [blog post](http://threatexpress.com/2017/03/leveraging-expired-domains-for-red-team-engagements/) about the tool's initial release for more details.

Yet another tool, [AIRMASTER](https://github.com/t94j0/AIRMASTER) by [Max Harley (@Max_68)](https://twitter.com/@Max_68) uses expireddomains.net and Bluecoat to find categorized domains. This tool uses OCR to bypass the BlueCoat captcha, increasing the search speed.

If a previously-registered domain isn't available or you would prefer a self-registered domain, it's possible to categorize domains yourself. Using the direct links below or a tool like [Chameleon](https://github.com/mdsecactivebreach/Chameleon) by Dominic Chell ([@domchell](https://twitter.com/domchell)). Most categorization products will overlook redirects or cloned content when determining the domain's categorization. For more information about Chameleon usage, check out Dominic's post [Categorisation is not a security boundary](https://www.mdsec.co.uk/2017/07/categorisation-is-not-a-security-boundary/).

Finally, make sure your DNS settings have propogated correctly.
* [DNS Propogation Checker](https://dnschecker.org/)

Categorization and Blacklist Checking Resources
* [McAfee](https://trustedsource.org/en/feedback/url?action=checksingle)

* [Fortiguard](http://www.fortiguard.com/iprep)
* [Symantec + BlueCoat](http://sitereview.bluecoat.com/sitereview.jsp)
* [Checkpoint (requires free account)](https://www.checkpoint.com/urlcat/main.htm)
* [Palo Alto](https://urlfiltering.paloaltonetworks.com/)
* [Sophos (submission only; no checking)](https://secure2.sophos.com/en-us/support/contact-support.aspx) - Click Submit a Sample -> Web Address
* [TrendMicro](https://global.sitesafety.trendmicro.com/)
* [Brightcloud](http://www.brightcloud.com/tools/url-ip-lookup.php)
* [Websense (Forcepoint)](http://csi.websense.com/)
* [Lightspeed Systems](https://archive.lightspeedsystems.com/)
* [Chameleon](https://github.com/mdsecactivebreach/Chameleon)
* [SenderBase](https://www.senderbase.org/)
* [MultiBL](http://multirbl.valli.org/)
* [MXToolBox - Blacklists](https://mxtoolbox.com/blacklists.aspx)

Phishing Setup

Easy Web-Based Phishing
The words easy and phishing never really seem to go together. Setting up a proper phishing infrastructure can be a real pain. The following tutorial will provide you with the knowledge and tools to quickly setup a phishing server that passes "most" spam filters to-date and provides you with a RoundCube interface for an easy phishing experience including two-way communications with your target. There are many setup's and posts out there regarding phishing. This is just one method.

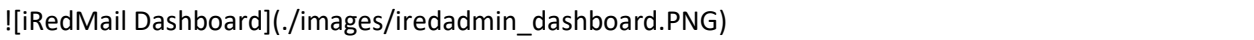
Once you have a domain that passes the proper checks listed in the previous section and have your phishing server spun-up, you'll need to create a couple "A" records for your domain as pictured.

Next, ssh into your phishing server and make sure you have a proper FQDN hostname listed in your /etc/hosts.
Example "127.0.0.1 email.yourphishingserver.com email localhost"

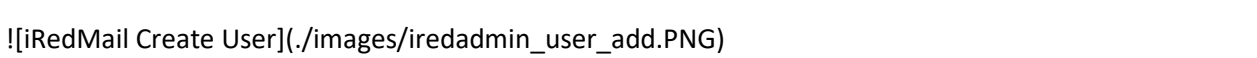
Now, you're going to install the web front-end to phish from in just a few easy steps. Start by downloading the latest "BETA" version of [iRedMail](http://www.iredmail.org/download.html) onto your phishing server. Easy way is to right click the download button, copy the link address, use wget to download directly onto your phishing server. Next, untar it "tar -xvf iRedMail-0.9.8-beta2.tar.bz2". Navigate into the unpacked folder and make the iRedMail.sh script executable (chmod +x iRedMail.sh). Execute the script as root, follow the prompts, and you'll need to reboot to finish everything.

You'll want to make sure you have all the proper DNS records ponting to your mail server. (https://docs.iredmail.org/setup.dns.html). For DKIM, the new command should be "amavisd-new showkeys" to list your DKIM key.

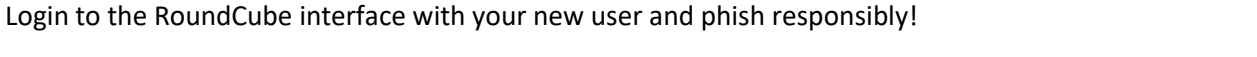
For DMARC we can use (https://www.unlocktheinbox.com/dmarcwizard/) to generate our dmarc entry.

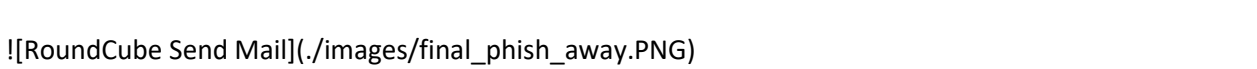


Now, create a user to phish with.

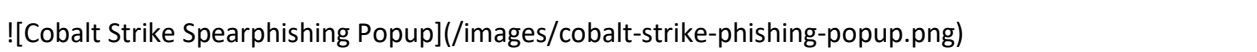


Login to the RoundCube interface with your new user and phish responsibly!





Cobalt Strike Phishing
Cobalt Strike provides customizable spearphishing functionality to support pentest or red team email phishing. It supports templates in HTML and/or plaintext formats, attachments, a bounceback address, URL embedding, remote SMTP server usage, and per-message send delays. Another interesting feature is the ability to add a unique token to each user's embedded URL for click tracking.



For more detailed information, check out these resources:

* [Cobalt Strike - Spear Phishing documentation](https://www.cobaltstrike.com/help-spear-phish)
* [Cobalt Strike Blog - What's the go-to phishing technique or exploit?](https://blog.cobaltstrike.com/2014/12/17/whats-the-go-to-phishing-technique-or-exploit/)
* [Spear phishing with Cobalt Strike - Raphael Mudge](https://www.youtube.com/watch?v=V7UJjVcq2Ao)
* [Advanced Threat Tactics (3 of 9) - Targeted Attacks - Raphael Mudge](https://www.youtube.com/watch?v=CxQfWtqpwRs)

Phishing Frameworks

Beyond rolling your own phishing setup or using a pentest or red teaming fraework, like Cobalt Strike, there are numerous tools and frameworks dedicated to email phishing. While this wiki won't go into detail about each framework, a few resources for each are collected below:

Gophish
* [Gophish Official Site](https://getgophish.com/)
* [Gophish GitHub Repo](https://github.com/gophish/gophish)
* [Gophish User Guide](https://www.gitbook.com/book/gophish/user-guide/details)

Phishing Frenzy

* [Phishing Frenzy Official Site](https://www.phishingfrenzy.com/)
* [Phishing Frenzy GitHub Repo](https://github.com/pentestgeek/phishing-frenzy)
* [Introducing Phishing Frenzy - Brandon McCann (@zeknox)](https://www.pentestgeek.com/phishing/introducing-phishing-frenzy)

The Social-Engineer Toolkit

* [The Social-Engineer Toolkit GitHub Repo](https://github.com/trustedsec/social-engineer-toolkit)
* [The Social-Engineer Toolkit User Manual](https://github.com/trustedsec/social-engineer-toolkit/raw/master/readme/User_Manual.pdf)

FiercePhish (formerly FirePhish)
* [FiercePhish GitHub Repo](https://github.com/Raikia/FiercePhish)
* [FiercePhish Wiki](https://github.com/Raikia/FiercePhish/wiki)

Redirectors

SMTP
“Redirector” may not be the best word to describe what we’re going to accomplish, but the goal is the same as with our other redirection. We want to remove any traces of our phishing origination from the final email headers and provide a buffer between the victim and our backend server. Ideally, the SMTP redirector will be quick to setup and easy to decommission.

There are two key actions we want to configure an SMTP redirector to perform:

Sendmail

Remove previous server headers
Add the following line to the end of `/etc/mail/sendmail.mc`:

```bash
define(`confRECEIVED_HEADER',`by $j ($v/$Z)$?r with $r$. id $i; $b')dnl
```

Add to the end of `/etc/mail/access`:

```bash
IP-to-Team-Server *TAB* RELAY
Phish-Domain *TAB* RELAY
```

[Removing Sender’s IP Address From Email’s Received From Header](https://www.devside.net/wamp-server/removing-senders-ip-address-from-emails-received-from-header)

[Removing Headers from Postfix setup](https://major.io/2013/04/14/remove-sensitive-information-from-email-headers-with-postfix/)

Configure a catch-all address
This will relay any email received to *@phishdomain.com to a chosen email address. This is highly useful to receive any responses or bounce-backs to a phishing email.

```bash
echo PHISH-DOMAIN >> /etc/mail/local-host-names
```

Add the following line right before `//Mailer Definitions//` (towards the end) of `/etc/mail/sendmail.mc`:

```bash
FEATURE(`virtusertable', `hash -o /etc/mail/virtusertable.db')dnl
```

Add the following line to the end of `/etc/mail/virtusertable`:

```bash
@phishdomain.com  external-relay-address
```

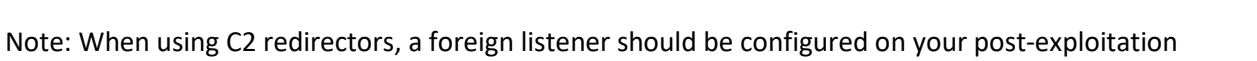
Note: The two fields should be tab-separated

Postfix

Postfix provides an easier alternative to sendmail with wider compatiblity. Postfix also offers full IMAP support with Dovecot. This allows testers to correspond in real-time with phishing targets who respond to the original message, rather than relying on the catch-all address and having to create a new message using your phishing tool.

A full guide to setting up a Postfix mail server for phishing is available in Julian Catrambone's ([@n0pe_sled](https://twitter.com/n0pe_sled)) post [Mail Servers Made Easy](https://blog.inspired-sec.com/archive/2017/02/14/Mail-Server-Setup.html).

DNS



Note: When using C2 redirectors, a foreign listener should be configured on your post-exploitation framework to send staging traffic through the redirector domain. This will cause the compromised host to stage through the redirector like the C2 traffic itself.

socat for DNS
socat can be used to redirect incoming DNS packets on port 53 to our team server. While this method works, some user's have reported staging issues with Cobalt Strike and or latency issues using this method.
Edit 4/21/2017:
The following socat command seems to work well thanks to testing from @xorrior:
```
socat udp4-recvfrom:53,reuseaddr,fork udp4-sendto:<IPADDRESS>; echo -ne
```

[Redirecting Cobalt Strike DNS Beacons - Steve Borosh](https://medium.com/rvrsh3ll/redirecting-cobalt-strike-dns-beacons-e3dcdb5a8b9b)

iptables for DNS
iptables DNS forwarding rules have been found to work well with Cobalt Strike. There does not seem to be any of the issues that socat has handling this type of traffic.

An example DNS redirector rule-set is below.

```bash
iptables -I INPUT -p udp -m udp --dport 53 -j ACCEPT
iptables -t nat -A PREROUTING -p udp --dport 53 -j DNAT --to-destination <IP-GOES-HERE>:53
iptables -t nat -A POSTROUTING -j MASQUERADE
iptables -I FORWARD -j ACCEPT
iptables -P FORWARD ACCEPT
sysctl net.ipv4.ip_forward=1
```

Also, change "FORWARD" chain policy to "ACCEPT"

DNS redirection can also be done behind NAT
Some may have the requirement or need to host a c2 server on an internal network. Using a combination of IPTABLES, SOCAT, and reverse ssh tunnels, we can certainly achieve this in the following manner.

In this scenario we have our volitile redirector using IPTables to forward all DNS traffic using the rule example described earlier in this section. Next, we create an SSH reverse port forward tunnel from our internal c2 server, to our main redirector. This will forward any traffic the main redirector receives on port 6667 to the internal c2 server on port 6667. Now, start socat on our team server to fork any of the incoming TCP traffic on port 6667 to UDP port 53 which, is what our DNS c2 needs to listen on. Finally, we similarly setup a socat instance on the main redirector to redirect any incoming UDP port 53 traffic into our SSH tunnel on port 6667.

HTTP(S)

Note: When using C2 redirectors, a foreign listener should be configured on your post-exploitation framework to send staging traffic through the redirector domain. This will cause the compromised host to stage through the redirector like the C2 traffic itself.

socat vs mod_rewrite
socat provides a ‘dumb pipe’ redirection. Any request socat receives on the specified source interface/port is redirected to the destination IP/port. There is no filtering or conditional redirecting. Apache mod_rewrite, on the other hand, provides a number of methods to strengthen your phishing and increase the resilience of your testing infrastructure. mod_rewrite has the ability to perform conditional redirection based on request attributes, such as URI, user agent, query string, operating system, and IP. Apache mod_rewrite uses htaccess files to configure rulesets for how Apache should handle each incoming request. Using these rules, you could, for instance, redirect requests to your server with the default wget user agent to a legitimate page on your target's website.

In short, if your redirector needs to perform conditional redirection or advanced filtering, use Apache mod_rewrite. Otherwise, socat redirection with optional iptables filtering will suffice.

socat for HTTP

socat can be used to redirect any incoming TCP packets on a specified port to our team server.

The basic syntax to redirect TCP port 80 on localhost to port 80 on another host is:

```
socat TCP4-LISTEN:80,fork TCP4:<REMOTE-HOST-IP-ADDRESS>:80
```

If your redirector is configured with more than one network interface, socat can be bound to a specific interface, by IP address, with the following syntax:

```
socat TCP4-LISTEN:80,bind=10.0.0.2,fork TCP4:1.2.3.4:80
```
In this example, 10.0.0.2 is one of the redirector's local IP addresses and 1.2.3.4 is the remote team server's IP address.

iptables for HTTP

In addition to socat, iptables can perform 'dumb pipe' redirection via NAT. To forward the redirector's local port 80 to a remote host, use the following syntax:

```
iptables -I INPUT -p tcp -m tcp --dport 80 -j ACCEPT
iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination <REMOTE-HOST-IP-ADDRESS>:80
iptables -t nat -A POSTROUTING -j MASQUERADE
iptables -I FORWARD -j ACCEPT
iptables -P FORWARD ACCEPT
sysctl net.ipv4.ip_forward=1
```

SSH for HTTP

We have previously covered using SSH for DNS tunnels. SSH works as a solid, and robust means to break through NAT and obtain a way for the implant to connect to a redirector and into your server environment. Before setting up an SSH redirector, you must add the following lines to `/etc/ssh/sshd_config`:

```text
# Allow the SSH client to specify which hosts may connect
GatewayPorts yes
```

```
# Allow both local and remote port forwards
AllowTcpForwarding yes
```

To forward the redirector's local port 80 to your internal teamsrver, use the following syntax on the internal server:

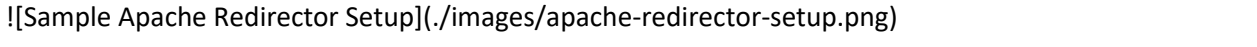
```
tmux new -S redir80
ssh <redirector> -R *:80:localhost:80
Ctrl+B, D
```

You can also forward more than one port, for example if you want 443 and 80 to be open all at once:

```
tmux new -S redir80443
ssh <redirector> -R *:80:localhost:80 -R *:443:localhost:443
Ctrl+B, D
```

Payloads and Web Redirection

When serving payload and web resources, we want to minimize the ability for incident responders to review files and increase the chances of successfully executing the payload, whether to establish C2 or gather intelligence.



Apache Mod_Rewrite usage and examples by Jeff Dimmock:
* [Strengthen Your Phishing with Apache mod_rewrite](https://bluescreenofjeff.com/2016-03-22-strengthen-your-phishing-with-apache-mod_rewrite-and-mobile-user-redirection/)
* [Invalid URI Redirection with Apache mod_rewrite](https://bluescreenofjeff.com/2016-03-29-invalid-uri-redirection-with-apache-mod_rewrite/)
* [Operating System Based Redirection with Apache mod_rewrite](https://bluescreenofjeff.com/2016-04-05-operating-system-based-redirection-with-apache-mod_rewrite/)
* [Combatting Incident Responders with Apache mod_rewrite](https://bluescreenofjeff.com/2016-04-12-combatting-incident-responders-with-apache-mod_rewrite/)
* [Expire Phishing Links with Apache RewriteMap](https://bluescreenofjeff.com/2016-04-19-expire-phishing-links-with-apache-rewritemap/)
* [Apache mod_rewrite Grab Bag](https://bluescreenofjeff.com/2016-12-23-apache_mod_rewrite_grab_bag/)
* [Serving Random Payloads with Apache mod_rewrite](https://bluescreenofjeff.com/2017-06-13-serving-random-payloads-with-apache-mod_rewrite/)

Other Apache mod_rewrite usage and examples:

* [mod_rewrite rule to evade vendor sandboxes from Jason Lang @curi0usjack](https://gist.github.com/curi0usJack/971385e8334e189d93a6cb4671238b10)

* [Serving random payloads with NGINX - Gist by jivoi](https://gist.github.com/jivoi/a33ace2e25515a31aa2ffbae246d98c9)

To automatically set up Apache Mod_Rewrite on a redirector server, check out Julain Catrambone's ([@n0pe_sled](https://twitter.com/n0pe_sled)) blog post [Mod_Rewrite Automatic Setup](https://blog.inspired-sec.com/archive/2017/04/17/Mod-Rewrite-Automatic-Setup.html) and the [accompanying tool](https://github.com/n0pe-sled/Apache2-Mod-Rewrite-Setup).

C2 Redirection

The intention behind redirecting C2 traffic is twofold: obscure the backend team server and appear to be a legitimate website if browsed to by an incident responder. Through the use of Apache mod_rewrite and [customized C2 profiles](#modifying-c2-traffic) or other proxying (such as with Flask), we can reliably filter the real C2 traffic from investigative traffic.

* [Cobalt Strike HTTP C2 Redirectors with Apache mod_rewrite - Jeff Dimmock](https://bluescreenofjeff.com/2016-06-28-cobalt-strike-http-c2-redirectors-with-apache-mod_rewrite/)
* [Securing your Empire C2 with Apache mod_rewrite - Gabriel Mathenge (@_theVIVI)](https://thevivi.net/2017/11/03/securing-your-empire-c2-with-apache-mod_rewrite/)
* [Expand Your Horizon Red Team – Modern SAAS C2 - Alex Rymdeko-Harvey (@killswitch-gui)](https://cybersyndicates.com/2017/04/expand-your-horizon-red-team/)
* [Hybrid Cobalt Strike Redirectors](https://zachgrace.com/2018/02/20/cobalt_strike_redirectors.html) - [Zach Grace (@ztgrace)](https://twitter.com/ztgrace) and [@m0ther_](https://twitter.com/m0ther_)

C2 Redirection with HTTPS

Building on "C2 Redirection" above, another method is to have your redirecting server use Apache's SSL Proxy Engine to accept inbound SSL requests, and proxy those to requests to a reverse-HTTPS listener. Encryption is used at all stages, and you can rotate SSL certificates on your redirector as needed.

To make this work with your mod_rewrite rules, you need to place your rules in **"/etc/apache2/sites-available/000-default-le-ssl.conf"** assuming you've used LetsEncrypt (aka CertBot) to install your certificate. Also, to enable the SSL ProxyPass engine, you'll need the following lines in that same config file:

```bash
# Enable the Proxy Engine
SSLProxyEngine On

# Tell the Proxy Engine where to forward your requests
ProxyPass / https://DESTINATION_C2_URL:443/
ProxyPassReverse / https://DESTINATION_C2_URL:443/

# Disable Cert checking, useful if you're using a self-signed cert
```

SSLProxyCheckPeerCN off
SSLProxyCheckPeerName off
SSLProxyCheckPeerExpire off
```

### Other Apache mod_rewrite Resources
* [Automating Apache mod_rewrite and Cobalt Strike Profiles](https://posts.specterops.io/automating-apache-mod-rewrite-and-cobalt-strike-malleable-c2-profiles-d45266ca642)
* [mod-rewrite-cheatsheet.com](http://mod-rewrite-cheatsheet.com/)
* [Official Apache 2.4 mod_rewrite Documentation](http://httpd.apache.org/docs/current/rewrite/)
* [Apache mod_rewrite Introduction](https://httpd.apache.org/docs/2.4/en/rewrite/intro.html)
* [An In-Depth Guide to mod_rewrite for Apache](http://code.tutsplus.com/tutorials/an-in-depth-guide-to-mod_rewrite-for-apache--net-6708)
* [Mod_Rewrite/.htaccess Syntax Checker](http://www.htaccesscheck.com/)

# Modifying C2 Traffic

## Cobalt Strike
Cobalt Strike modifies its traffic with Malleable C2 profiles. Profiles provide highly-customizable options for modifying how your server's C2 traffic will look on the wire. Malleable C2 profiles can be used to strengthen incident response evasion, impersonate known adversaries, or masquerade as legitimate internal applications used by the target.

* [Official Malleable C2 Profiles - GitHub](https://github.com/rsmudge/Malleable-C2-Profiles)
* [Malleable Command and Control Documentation - cobaltstrike.com](https://www.cobaltstrike.com/help-malleable-c2)
* [Cobalt Strike 2.0 - Malleable Command and Control - Raphael Mudge](http://blog.cobaltstrike.com/2014/07/16/malleable-command-and-control/)
* [Cobalt Strike 3.6 - A Path for Privilege Escalation - Raphael Mudge](http://blog.cobaltstrike.com/2016/12/08/cobalt-strike-3-6-a-path-for-privilege-escalation/)
* [A Brave New World: Malleable C2 - Will Schroeder (@harmj0y)](http://www.harmj0y.net/blog/redteaming/a-brave-new-world-malleable-c2/)
* [How to Write Malleable C2 Profiles for Cobalt Strike - Jeff Dimmock](https://bluescreenofjeff.com/2017-01-24-how-to-write-malleable-c2-profiles-for-cobalt-strike/)
* [In-Memory Evasion (Video series) - Raphael Mudge](https://www.youtube.com/watch?v=lz2ARbZ_5tE&list=PL9HO6M_MU2nc5Q31qd2CwpZ8J4KFMhgnK)

As you begin creating or modifying Malleable C2 profiles, it's important to keep data size limits for the Beacon info placement. For example, configuring the profile to send large amounts of data in a URL parameter will require many requests. For more information about this, check out Raphael Mudge's blog post [Beware of Slow Downloads](https://blog.cobaltstrike.com/2018/03/09/beware-of-slow-downloads/).

If you encounter issues with your Malleable C2 profile and notice the teamserver console outputting errors, refer to Raphael Mudge's blog post [Broken Promises and Malleable C2
```

Profiles](https://blog.cobaltstrike.com/2018/06/04/broken-promises-and-malleable-c2-profiles/) for troubleshooting tips.

Empire
Empire uses Communication Profiles, which provide customization options for the GET request URIs, user agent, and headers. The profile consists of each element, separated by the pipe character, and set with the `set DefaultProfile` option in the `listeners` context menu.

Here is a sample default profile:

```bash
"/CWoNaJLBo/VTNeWw11212/|Mozilla/4.0 (compatible; MSIE 6.0;Windows NT 5.1)|Accept:image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*|Accept-Language:en-en"
```

Alternatively, the DefaultProfile value can be set by modifying the file `/setup/setup_database.py` before Empire's initial setup. This will change the default Communication Profile that Empire will use.

In addition to the Communication Profile, consider customizing the Empire server's staging URIs, server headers, and defaut webpage content by following the steps presented in Joe Vest's ([@joevest](https://twitter.com/joevest)) post [Empire - Modifying Server C2 Indicators](http://threatexpress.com/2017/05/empire-modifying-server-c2-indicators/).

* [Default Empire Communication Profiles (in Empire GitHub repo)](https://github.com/EmpireProject/Empire/tree/master/data/profiles)
* [How to Make Communication Profiles for Empire - Jeff Dimmock](https://bluescreenofjeff.com/2017-03-01-how-to-make-communication-profiles-for-empire/)

Third-Party C2 Channels
Leveraging trusted, legitimate web services for C2 can provide a valuable leg-up over using domains and infrastructure you've configured yourself. Configuration time and complexity varies based on the technique and service being used. A popular example of leveraging third-party services for C2 redirection is Domain Fronting.

Domain Fronting

Domain Fronting is a technique used by censorship evasion services and apps to route traffic through legitimate and highly-trusted domains. Popular services that support Domain Fronting include [Google App Engine](https://cloud.google.com/appengine/), [Amazon CloudFront](https://aws.amazon.com/cloudfront/), and [Microsoft Azure](https://azure.microsoft.com/). It's important to note that many providers, like [Google](https://arstechnica.com/information-technology/2018/04/google-disables-domain-fronting-capability-used-to-evade-censors/) and [Amazon](https://aws.amazon.com/blogs/security/enhanced-domain-protections-for-amazon-cloudfront-requests/) have implemented mitigations against Domain Fronting, so some linked resources or information provided in this wiki may be outdated by the time you try to use it.

In a nutshell, traffic uses the DNS and SNI name of the trusted service provider, Google is used in the example below. When the traffic is received by the Edge Server (ex: located at gmail.com), the packet is forwarded to the Origin Server (ex: phish.appspot.com) specified in the packet's Host header. Depending on the service provider, the Origin Server will either directly forward traffic to a specified domain, which we'll point to our team server, or a proxy app will be required to perform the final hop forwarding.

For more detailed information about how Domain Fronting works, see the whitepaper [Blocking-resistant communication through domain fronting](https://www.bamsoftware.com/papers/fronting/) and the TOR Project's [meek documentation](https://trac.torproject.org/projects/tor/wiki/doc/meek)

In addition to the standard frontable domains, such as any google.com domain, it's possible to leverage other legitimate domains for fronting.

For more information about hunting frontable domains, check out:
* [Domain Fronting via Cloudfront Alternate Domains - Vincent Yiu (@vysecurity)](https://www.mdsec.co.uk/2017/02/domain-fronting-via-cloudfront-alternate-domains/)
* [Finding Domain frontable Azure domains - thoth / Fionnbharr (@a_profligate)](https://theobsidiantower.com/2017/07/24/d0a7cfceedc42bdf3a36f2926bd52863ef28befc.html)
* [Google Groups: Blog post on finding 2000+ Azure domains using Censys](https://groups.google.com/forum/#!topic/traffic-obf/7ygIXCPebwQ)
* [FindFrontableDomains tool - Steve Borosh (@rvrsh3ll)](https://github.com/rvrsh3ll/FindFrontableDomains)

Further Resources on Domain Fronting
* [Simplifying Domain Fronting - Tim Malcomvetter (@malcomvetter)](https://medium.com/@malcomvetter/simplifying-domain-fronting-8d23dcb694a0)
* [High-reputation Redirectors and Domain Fronting - Raphael Mudge](https://blog.cobaltstrike.com/2017/02/06/high-reputation-redirectors-and-domain-fronting/)
* [Empire Domain Fronting - Chris Ross (@xorrior)](https://www.xorrior.com/Empire-Domain-Fronting/)
* [Escape and Evasion Egressing Restricted Networks - Tom Steele (@_tomsteele) and Chris Patten](https://www.optiv.com/blog/escape-and-evasion-egressing-restricted-networks)
* [Red Team Insights on HTTPS Domain Fronting Google Hosts Using Cobalt Strike](https://www.cyberark.com/threat-research-blog/red-team-insights-https-domain-fronting-google-hosts-using-cobalt-strike/) - [Will Vandevanter and Shay Nahari of CyberArk](https://www.cyberark.com)
* [SSL Domain Fronting 101 - Steve Borosh (@424f424f)](https://medium.com/rvrsh3ll/ssl-domain-fronting-101-4348d410c56f)
* [How I Identified 93k Domain-Frontable CloudFront Domains - Chris Myers (@SWIZZLEZ_) and Barrett Adams (@PEEWPW)](https://www.peew.pw/blog/2018/2/22/how-i-identified-93k-domain-frontable-cloudfront-domains)
* [Domain Fronting: Who Am I? - Vincent Yiu (@vysecurity)](https://medium.com/@vysec.private/domain-fronting-who-am-i-3c982ccd52e6)

* [Validated CloudFront SSL Domains - Vincent Yiu (@vysecurity)](https://medium.com/@vysec.private/validated-cloudfront-ssl-domains-27895822cea3)
* [CloudFront Hijacking](https://www.mindpointgroup.com/blog/pen-test/cloudfront-hijacking/) - [Matt Westfall (@disloops)](https://twitter.com/disloops)
* [CloudFrunt GitHub Repo](https://github.com/MindPointGroup/cloudfrunt) - [MindPointGroup](https://github.com/MindPointGroup)
* [Metasploit Domain Fronting With Microsoft Azure (@ch1gg1ns)](https://chigstuff.com/blog/metasploit-domain-fronting-with-microsoft-azure/)
* [Alibaba CDN Domain Fronting - Vincent Yiu (@vysecurity)](https://medium.com/@vysec.private/alibaba-cdn-domain-fronting-1c0754fa0142)
* [CloudFlare Domain Fronting: an easy way to reach (and hide) a malware C&C - @theMiddle (Medium)](https://medium.com/@themiddleblue/cloudflare-domain-fronting-an-easy-way-to-reach-and-hide-a-malware-c-c-786255f0f437)

PaaS Redirectors
Many PaaS and SaaS providers provide a static subdomain or URL for use with a provisioned instance. If the associated domain is generally highly trusted, the instances could provide extra trust to your C2 infrastructure over a purchased domain and VPS.

To set the redirection up, you will need to identify a service that issues a static subdomain or URL as part of an instance. Then, either the instance will need to be configured with network or application-based redirection. The instance will act as a proxy, similar to the other redirectors discussed on this wiki.

Specific implementation can vary greatly based on the service; however, for an example using Heroku, check out the blog post [Expand Your Horizon Red Team – Modern SaaS C2](https://cybersyndicates.com/2017/04/expand-your-horizon-red-team/) by [Alex Rymdeko-Harvey (@Killswitch_GUI)](https://twitter.com/Killswitch_GUI).

Another interesting technique that merits further research is the use of overly-permissive Amazon S3 buckets for C2. Check out the post [S3 Buckets for Good and Evil](https://pentestarmoury.com/2017/07/19/s3-buckets-for-good-and-evil/) by [Andrew Luke (@Sw4mp_f0x)](https://twitter.com/Sw4mp_f0x) for more details on how S3 buckets could be used for C2. This technique could be combined with the third-party C2 capabilities of Empire to use the target's legitimate S3 buckets against them.

For another example of using PaaS for C2, check out [Databases and Clouds: SQL Server as a C2](https://blog.netspi.com/databases-and-clouds-sql-server-as-a-c2/) by Scott Sutherland ([@_nullbind](https://twitter.com/_nullbind)).

Other Third-Party C2
Other third-party services have been used in the wild for C2 in the past. Leveraging third-party websites that allow for the rapid posting or modification of user-generated content can help you evade reputation-based controls, especially if the third-party site is generally trusted.

Check out these resources for other third-party C2 options:
* [canisrufus (GitHub Repo)](https://github.com/maldevel/canisrufus) - [maldevel](https://github.com/maldevel)

* [External C2 (Third-Party Command and Control) - Cobalt Strike Documentation](https://www.cobaltstrike.com/help-externalc2)
* [Cobalt Strike over external C2 – beacon home in the most obscure ways](https://outflank.nl/blog/2017/09/17/blogpost-cobalt-strike-over-external-c2-beacon-home-in-the-most-obscure-ways/) - [Mark Bergman at outflank.nl](https://outflank.nl/blog/author/mark/)
* [“Tasking” Office 365 for Cobalt Strike C2](https://labs.mwrinfosecurity.com/blog/tasking-office-365-for-cobalt-strike-c2) - [William Knowles (@william_knows)](https://twitter.com/william_knows)
* [External C2 for Cobalt Strike](https://github.com/ryhanson/ExternalC2/) - [Ryan Hanson (@ryhanson)](https://twitter.com/ryhanson)
* [External C2 framework for Cobalt Strike](http://www.insomniacsecurity.com/2018/01/11/externalc2.html) - [Jonathan Echavarria (@Und3rf10w)](https://twitter.com/und3rf10w)
* [External C2 framework (GitHub Repo)](https://github.com/Und3rf10w/external_c2_framework) - [Jonathan Echavarria (@Und3rf10w)](https://twitter.com/und3rf10w)
* [Hiding in the Cloud: Cobalt Strike Beacon C2 using Amazon APIs](https://rhinosecuritylabs.com/aws/hiding-cloudcobalt-strike-beacon-c2-using-amazon-apis/) - [Rhino Security Labs](https://rhinosecuritylabs.com)
* [Exploring Cobalt Strike's ExternalC2 framework](https://blog.xpnsec.com/exploring-cobalt-strikes-externalc2-framework/) - [Adam (@_xpn_)](https://twitter.com/_xpn_)

Obscuring Infrastructure

Attack infrastructure is often easy to identify, appearing like a shell of a legitimate server. We will need to take additional steps with our infrastructure to increase the likelihood of blending in with real servers amongst either the target organization or services the target may conceivably use.

[Redirectors](#redirectors) can help blend in by [redirecting invalid URIs](https://bluescreenofjeff.com/2016-03-29-invalid-uri-redirection-with-apache-mod_rewrite/), [expiring phishing payload links](https://bluescreenofjeff.com/2016-04-19-expire-phishing-links-with-apache-rewritemap/), or [blocking common incident responder techniques](https://bluescreenofjeff.com/2016-04-12-combatting-incident-responders-with-apache-mod_rewrite/); however, attention should also be paid to the underlying host and its indicators.

For example, in the post [Fall of an Empire](http://securesql.info/hacks/2017/4/5/fall-of-an-empire), John Menerick ([@Lord_SQL](https://twitter.com/Lord_SQL)) covers methods to detect Empire servers on the internet.

To combat these and similar indicators, it's a good idea to [modify C2 traffic patterns](#modifying-c2-traffic), modify server landing pages, restrict open ports, and modify default response headers.

For more details about how to do these and other tactics for multiple attack frameworks, check out these posts:
* [Empire – Modifying Server C2 Indicators](http://threatexpress.com/2017/05/empire-modifying-server-c2-indicators/) - [Andrew Chiles](https://twitter.com/andrewchiles)
* [Hunting Red Team Empire C2 Infrastructure](http://www.chokepoint.net/2017/04/hunting-red-team-empire-c2.html) - [chokepoint.net](http://www.chokepoint.net/)
* [Hunting Red Team Meterpreter C2 Infrastructure](http://www.chokepoint.net/2017/04/hunting-red-team-meterpreter-c2.html) - [chokepoint.net](http://www.chokepoint.net/)

* [Identifying Empire HTTP Listeners (Tenable Blog)](https://www.tenable.com/blog/identifying-empire-http-listeners) - [Jacob Baines](https://www.tenable.com/profile/jacob-baines)
* [Host Header Manipulation - Vincent Yiu (@vysecurity)](https://vincentyiu.co.uk/host-header-manipulation/)

Securing Infrastructure
Attack infrastructure can be attacked just the same as any other internet-connected host, and it should be considered HIGHLY sensitive due to the data in use and connections into target environments.

In 2016, remote code execution vulnerabilities were disclosed on the most common attack tools:

* [2016 Metasploit RCE Static Key Deserialization](https://github.com/justinsteven/advisories/blob/master/2016_metasploit_rce_static_key_deserialization.md)
* [2017 Metasploit Meterpreter Dir Traversal Bugs](https://github.com/justinsteven/advisories/blob/master/2017_metasploit_meterpreter_dir_traversal_bugs.md)
* [Empire Fails - Will Schroeder](http://www.harmj0y.net/blog/empire/empire-fails/)
* [Cobalt Strike 3.5.1 Important Security Update - Raphael Mudge](http://blog.cobaltstrike.com/2016/10/03/cobalt-strike-3-5-1-important-security-update/)

iptables should be used to filter unwanted traffic and restrict traffic between required infrastructure elements. For example, if a Cobalt Strike team server will only serve assets to an Apache redirector, iptables rules should only allow port 80 from the redirector's source IP. This is especially important for any management interfaces, such as SSH or Cobalt Strike's default port 50050. Also consider blocking non-target country IPs. As an alternative, consider using hypervisor firewalls provided by your VPS providers. For example, Digital Ocean offers [Cloud Firewalls](https://www.digitalocean.com/community/tutorials/an-introduction-to-digitalocean-cloud-firewalls) that can protect one or multiple droplets.

chattr can be used on team servers to prevent cron directories from being modified. Using chattr, you can restrict any user, including root, from modifying a file until the chattr attribute is removed.

SSH should be limited to public-key authentication only and configured to use limited-rights users for initial login. For added security, consider adding multi-factor authentication to SSH.

Update! No securing list is complete without a reminder to regularly update systems and apply hot-fixes as needed to remediate vulnerabilities.

Of course, this list is not exhaustive of what you can do to secure a team server. Follow common hardening practices on all infrastructure:

* [Red Hat Enterprise Linux 6 Security Guide](https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/pdf/Security_Guide/Red_Hat_Enterprise_Linux-6-Security_Guide-en-US.pdf)
* [Debian Documentation on Hardening](https://wiki.debian.org/Hardening)
* [Securing Debian Manual](https://www.debian.org/doc/manuals/securing-debian-howto/)

* [20 Linux Server Hardening Security Tips - nixCraft](https://www.cyberciti.biz/tips/linux-security.html)
* [SANS Linux Security Checklists](https://www.sans.org/score/checklists/linux)
* [Docker Your Command & Control (C2)](https://blog.obscuritylabs.com/docker-command-controll-c2/)
- [Alex Rymdeko-Harvey (@killswitch_gui)](https://twitter.com/killswitch_gui)

Specific Hardening Resources
There are a number of resources available online discussing the secure setup and design of infrastructures. Not every design consideration will be appropriate for every attack infrastructure, but it's useful to know what options are available and what other testers are doing.

Here are some of those resoources:

* [Responsible Red Teams - Tim MalcomVetter (@malcomvetter)](https://medium.com/@malcomvetter/responsible-red-teams-1c6209fd43cc)
* [Safe Red Team Infrastructure - Tim MalcomVetter (@malcomvetter)](https://medium.com/@malcomvetter/safe-red-team-infrastructure-c5d6a0f13fac)
* [Red Team Infrastructure - AWS Encrypted EBS - @_rastamouse](https://rastamouse.me/2018/02/red-team-infrastructure---aws-encrypted-ebs/)
* [Attack Infrastructure Logging (4-part series) - Gabriel Mathenge (@_theVIVI)](https://thevivi.net/category/infrastructure/)

Automating Deployments
The topics covered in this wiki strengthen attack infrastrctures, but generally require a good deal of time to design and implement. Automation can be used to greatly reduce deployment times, allowing you to deploy more complex setups in less time.

Check out these resources about attack infrastructure automation:
* [Automated Red Team Infrastructure Deployment with Terraform - Part 1](https://rastamouse.me/2017/08/automated-red-team-infrastructure-deployment-with-terraform---part-1/) - [@_RastaMouse](https://twitter.com/_RastaMouse)
* [Automated Red Team Infrastructure Deployment with Terraform - Part 2](https://rastamouse.me/2017/09/automated-red-team-infrastructure-deployment-with-terraform---part-2/) - [@_RastaMouse](https://twitter.com/_RastaMouse)
* [Mod_Rewrite Automatic Setup](https://blog.inspired-sec.com/archive/2017/04/17/Mod-Rewrite-Automatic-Setup.html) - [Julian Catrambone (@n0pe_sled)](https://twitter.com/n0pe_sled)
* [Automated Empire Infrastructure](https://bneg.io/2017/11/06/automated-empire-infrastructure/) - [Jeremy Johnson (@beyondnegative)](https://twitter.com/beyondnegative)
* [RTOps: Automating Redirector Deployment With Ansible](http://threat.tevora.com/automating-redirector-deployment-with-ansible/) - [Kevin Dick](http://threat.tevora.com/author/e0x70i/)
* [Automating Gophish Releases With Ansible and Docker](https://jordan-wright.com/blog/post/2018-02-04-automating-gophish-releases/) - [Jordan Wright (@jw_sec)](https://twitter.com/jw_sec)
* [Red Baron GitHub Repo](https://github.com/Coalfire-Research/Red-Baron) - [Marcello (@byt3bl33d3r)](https://twitter.com/byt3bl33d3r)
* [Automating Apache mod_rewrite and Cobalt Strike Malleable C2 for Intelligent Redirection](http://threatexpress.com/2018/02/automating-cobalt-strike-profiles-apache-mod_rewrite-htaccess-files-intelligent-c2-redirection/) - [Joe Vest (@joevest)](https://twitter.com/joevest)
* [Modular Infrastructure with Terraform](https://blog.smallsec.ca/2018/05/17/modular-infrastructure-with-terraform/) - [Liam Somerville (@liamsomerville)](https://twitter.com/liamsomerville)

General Tips
* **Document everything** - Running a complex Red Team infrastructure means many moving parts. Be sure to document each asset's function and where its traffic is sent.

* **Split assets among different service providers and regions** - Infrastructure assets should be spread across multiple service providers and geographic regions. Blue Team members may raise monitoring thresholds against providers identified as actively performing an attack and may even outright block a given service provider. Note: keep international privacy laws in mind if sending encrypted or sensitive data across borders.

* **Don't go overboard** - It's easy to get excited about advanced techniques and want to throw the kitchen sink at a target. If you are emulating a specific adversarial threat, only leverage techniques the real threat actor used or techniques within the skillset of the threat actor. If your red team testing will attack the same target long-term, consider starting "easy" and working through the more advanced tradecraft as your assessments go on. Evolving the red team's technique alongside the blue team's will consistenly push the organization forward, whereas hitting the blue team with everything at once may overwhelm the blue team and slow the learning process.

* **Monitor logs** - All logs should be monitored throughout the engagement: SMTP logs, Apache logs, tcpdump on socat redirectors, iptables logs (specific to traffic forwarding or targeted filtering), weblogs, Cobalt Strike/Empire/MSF logs. Forward logs to a central location, such as with [rsyslog](https://bluescreenofjeff.com/2017-08-08-attack-infrastructure-log-aggregation-and-monitoring/), for easier monitoring. Operator terminal data retention may come in handy for going over an historical command useage during an operation. @Killswitch_GUI created an easy-to-use program named lTerm that will log all bash terminal commands to a central location. [Log all terminal output with lTerm](https://github.com/killswitch-GUI/lterm). Check out Vincent Yiu's post [CobaltSplunk](https://vincentyiu.co.uk/cobaltsplunk/) for an example of how to send Cobalt Strike logs to Splunk for advanced infrastructure monitoring and analysis.

* **Implement high-value event alerting** - Configure the attack infrastructure to generate alerts for high-value events, such as new C2 sessions or credential capture hits. One popular way of implementing alerting is via a chat platform's API, such as Slack. Check out the following posts about Slack alerting: [Slack Shell Bot - Russel Van Tuyl (@Ne0nd0g)](https://www.swordshield.com/2016/11/slackshellbot/), [Slack Notifications for Cobalt Strike - Andrew Chiles (@AndrewChiles)](http://threatexpress.com/2016/12/slack-notifications-for-cobalt-strike/), [Slack Bots for Trolls and Work - Jeff Dimmock (@bluscreenfojeff)](http://bluescreenofjeff.com/2017-04-11-slack-bots-for-trolls-and-work/)

* **Fingerprint incident response** - If possible, try to passively or actively fingerprint IR actions before the assessment starts. For example, send a mediocre phishing email to the target (using unrelated infrastructure) and monitor traffic that infrastructure receives. IR team investigations can disclose a good deal of information about how the team operates and what infrastructure they use. If this can be determined ahead of the assessment, it can be filtered or redirected outright.

Thanks to Contributors

A BIG THANK YOU to all the following people (listed alphabetically) who contributed tools, tips, or links to include in the wiki, and another THANK YOU to anyone who wrote a tool or post referenced in this wiki!

* [@andrewchiles - Andrew Chiles](https://twitter.com/andrewchiles)
* [@armitagehacker - Raphael Mudge](https://twitter.com/armitagehacker)
* [@beyondnegative - Jeremy Johnson](https://twitter.com/beyondnegative)
* [@bspence7337](https://twitter.com/bspence7337)
* [@domchell - Dominic Chell](https://twitter.com/domchell)
* [@jivoi - EK](https://twitter.com/jivoi)
* [@joevest - Joe Vest](https://twitter.com/joevest)
* [@killswitch_gui - Alex Rymdeko-Harvey](https://twitter.com/killswitch_gui)
* [@ne0nd0g - Russel Van Tuyl](https://twitter.com/ne0nd0g)
* [@n0pe_sled - Julian Catrambone](https://twitter.com/n0pe_sled)
* [@_RastaMouse](https://twitter.com/_RastaMouse)
* [@tifkin_ - Lee Christensen](https://twitter.com/tifkin_)
* [@Und3rf10w - Jonathan Echavarria](https://twitter.com/und3rf10w)
* [@vysecurity - Vincent Yiu](https://twitter.com/vysecurity)
* [@xorrior - Chris Ross](https://twitter.com/xorrior)

Awesome Resources For Learning Hacking & Pentesting
[![Awesome](https://cdn.rawgit.com/sindresorhus/awesome/d7305f38d29fed78fa85652e3a63e154dd8e8829/media/badge.svg)](https://github.com/sindresorhus/awesome)

Basically What I'm sharing here is a Collection of some best resources about Penetration Testing & Reverse Engineering That I want to Share with you all.., Along with Some Blogs Links, & YouTube Channels :)

Contribution
Your contributions and suggestions are heartily welcome. Please check the [Contributing Guidelines](.github/CONTRIBUTING.md) for more details.

Books

1. The Hacker Playbook 2: Practical Guide To Penetration Testing
2. The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy
3. Breaking into Information Security: Learning the Ropes 101
4. Penetration Testing: A Hands-On Introduction to Hacking
5. Social Engineering: The Art of Human Hacking
6. Hacking: The Art of Exploitation, 2nd Edition
7. Web Hacking 101
8. OWASP Testing Guide (A must read for web application developers and penetration testers)

Learning Platforms

Online
* [Hack The Box :: Penetration Testing Labs](https://www.hackthebox.eu)
* [OWASP Vulnerable Web Applications Directory Project (Online)](https://www.owasp.org/index.php/OWASP_Vulnerable_Web_Applications_Directory_Project#tab=On-Line_apps) - List of online available vulnerable applications for learning purposes
* [Pentestit labs](https://lab.pentestit.ru) - Hands-on Pentesting Labs (OSCP style)
* [Root-me.org](https://www.root-me.org) - Hundreds of challenges are available to train yourself in different and not simulated environments
* [Vulnhub.com](https://www.vulnhub.com) - Vulnerable By Design VMs for practical 'hands-on' experience in digital security

* [Infosecinstitute.com](http://resources.infosecinstitute.com/)
* [PentesterLab.com](https://pentesterlab.com/)
* [Complete Penetration Testing Tutorials by OWASP](https://www.owasp.org/index.php/Web_Application_Penetration_Testing)
* [Silesia Security Lab](https://silesiasecuritylab.com/blog/)
* [Rafay Hacking Articles, a great blog](http://www.rafayhackingarticles.net/)
* [Troyhunt](https://www.troyhunt.com/)

Off-Line
* [Damn Vulnerable Xebia Training Environment](https://github.com/davevs/dvxte) - Docker Container including several vurnerable web applications (DVWA,DVWServices, DVWSockets, WebGoat, Juiceshop, Railsgoat, django.NV, Buggy Bank, Mutilidae II and more)
* [OWASP Vulnerable Web Applications Directory Project (Offline)](https://www.owasp.org/index.php/OWASP_Vulnerable_Web_Applications_Directory_Project#tab=Off-Line_apps) - List of offline available vulnerable applications for learning purposes

Vulnerable Machines/Websites

1. [FiringRange](https://public-firing-range.appspot.com/)

Courses

1. [Computer Systems Security, MIT](http://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-858-computer-systems-security-fall-2014/video-lectures/)

For those who want to do CEH, the following links are for you.
2. [CBT Nuggets CEH Training](http://goo.gl/JuW85U)
3. [CEH Books](https://goo.gl/gjCBLK)
4. [Guide to Binary Exploitation](https://github.com/r0hi7/binexp)

Workshops/Playlists

1. [Web Hacking](https://www.youtube.com/playlist?list=PLJM73L2pQRd4lXBZjsHAmeEqsn5pENXxN)
2. [Ethical Hacking, A Comprehensive Playlist covering almost everything](https://www.youtube.com/playlist?list=PLkRo97mCIn9lgvE7AskNsmwJVOlJX2zaI)

Security Talks and Conferences

1. [InfoCon - Hacking Conference Archive](https://infocon.org/cons/)
2. [Curated list of Security Talks and Videos](https://github.com/PaulSec/awesome-sec-talks)
3. [Blackhat](https://www.youtube.com/user/BlackHatOfficialYT)
4. [Defcon](https://www.youtube.com/user/DEFCONConference)
5. [Security Tube](http://www.securitytube.net/)
6. [Kevin Mitnick: Live Hack at CeBIT](https://www.youtube.com/watch?v=Q7G3kKRdUl4)
7. [Ghost in the Cloud, Kevin Mitnick](https://www.youtube.com/watch?v=76yrWGzScgI)
8. [Kevin Mitnick | Talks at Google](https://www.youtube.com/watch?v=aUqes9QdLQ4)
9. [Complete Free Hacking Course: Go from Beginner to Expert Hacker Today](https://www.youtube.com/watch?v=7nF2BAfWUEg)

YouTube Channels

Now let's get Towards YouTube Channel Links... These Channels are Shared By Hackers where They Upload their Video POCs.. Watching them u can actually understand how to demonstrate these type of attacks...

1. [SecurityIdiots](https://www.youtube.com/channel/UCPPAYs04kwfXcHnerm_ueFw)
2. [Black Hat](https://www.youtube.com/channel/UCJ6q9Ie29ajGqKApbLqfBOg)
3. [Injector Pca](https://www.youtube.com/channel/UCRFG_j0cgLWtJOG6fl_-rxQ)
4. [Hisham Mir](https://www.youtube.com/channel/UCYTK8lk8oLLaA330rqd0qgA)
5. [Devil Killer](https://www.youtube.com/channel/UCwfYw-C2xqemqrXq0IKF_Mg)
6. [Suleman Malik](https://www.youtube.com/channel/UC59IHQcCmgNw4GIvsXeLnDQ)
7. [Dem0n](https://www.youtube.com/channel/UC_jNs1biBixcQeSUoJxvNLw)
8. [Frans Rosén](https://www.youtube.com/channel/UCV89UhUtxqwP0j4o9tMipsA)
9. [HackerOne](https://www.youtube.com/channel/UCsgzmECky2Q9lQMWzDwMhYw)
10. [ak1t4 machine](https://www.youtube.com/channel/UCaftcKRiJJW0AJHmR1E5MAQ)
11. [Shawar Khan](https://www.youtube.com/channel/UCPxJLZCoIRJHs1VebWeaByA)
12. [vulnerability0lab](https://www.youtube.com/channel/UC4QJ7X4nnkAYXsnFQpdytcA)
13. [Bugcrowd](https://www.youtube.com/channel/UCo1NHk_bgbAbDBc4JinrXww)
14. [Vijay Kumar](https://www.youtube.com/channel/UCs2NmJGRecw_huNzvQNf2_A)
15. [Web Development Tutorials](https://www.youtube.com/channel/UCS0y5e-AMsZO8GEFtKBAzkA)
16. [Jan Wikholm](https://www.youtube.com/channel/UCOQtLXVJduZ4-YUFOi5EzIA)
17. [Bhargav Tandel](https://www.youtube.com/channel/UCh5MTJLt3LYr_rkwcOQJNWg)
18. [ErrOr SquaD](https://www.youtube.com/channel/UCou-7r8Mk4oQcBmazxp5uwg)
19. [Hussnain Fareed](https://www.youtube.com/channel/UCbq5fgcqUz-PlMs3RCOUrXw)
20. [Penetration Testing in Linux](https://www.youtube.com/channel/UC286ntgASMskhPIJQebJVvA)

Any Channel Link Missing? Kindly add it in Comments

NOTE:
All references taken from Internet and shared on internet xD Thanks to those who shared their opinion before that helped me learn 😉
if you have any questions, please ask in the comments. If you know about any good resource for beginners, please share it.

For more articles on hacking you can follow me on Medium:
medium.com/@hussnainfareed

List of Top Platforms (Open/Public)

- ## Hackerone (H1)
- ## BugCrowd (BC)
- ## Intigriti
- ## BountyGraph (Software dependencies) [Closing on 12th December, 2018]
- ## BountyFactory
- ## OpenBugBounty (OBB) [Limited to XSSi and other non-intrusive type vulnerabilities]

List of Top (Closed/Invite-only) Platforms

- ## Synack
- ## Cobalt
- ## Zerocopter
- ## Detectify

Upcoming Platforms
Have an insider edge over the newer platforms, be the first to join them!
- ## PlugBounty (Vulnerabilities in Plugins)
- ## BugsBounty (Indian origin)

Misc. Other Platforms (Open)

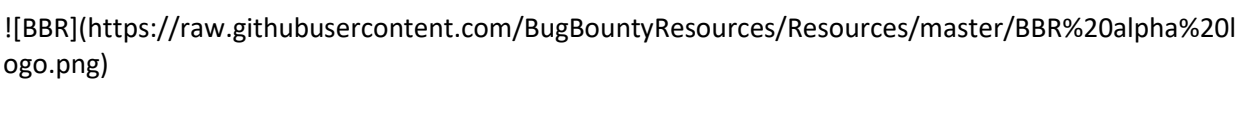
- ## Hackenproof
- ## BugBountyjp (dubious - Payment Delays, Unresponsive)
- ## BugsBounty (Upcoming Platform, currently running Internally and exclusively)
- ## CESPPA
- ## Hackrfi
- ## Safehats (Indian origin, although registration is open, goes through validation)
- ## Hacktrophy

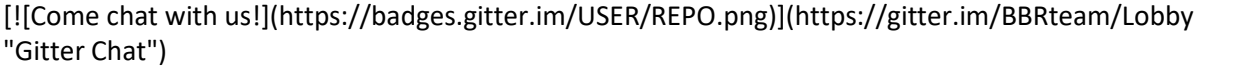
- ## Cyberarmy.id (Indonesian Origin)
- ## FireBounty (collection/list of bug bounty programs on different platforms like hackerone, bugcrowd, etc.)

Misc. other (Invite-only/closed) Platforms

- ## BugBountyZone
- ## Federacy
- ## Yogosha
- ## Vulnscope
- ## Antihack (dubious/infamous for non-payments, and other issues)

A word of caution goes here, we don't endorse or, opine about any platforms and the comments about them in parentheses merely reflect unbiased information which we gathered from the community and other credible sources. Platforms marked dubious, have payment delays and issues, so care should be taken while working on them.



[

](https://gitter.im/BBRteam/Lobby "Gitter Chat")

Bug Bounty Resources

Storehouse of resources related to Bug Bounty Hunting collected from different sources. Watch and Star this repo for all latest guides, tools, methodology, platforms tips, and tricks curated by us.

Getting Started (in Bug Hunting and More...)

Coming Soon, till then, just keep watching or, ✨ (starring) us! Thanks for your patience.

URL: https://nairuzabulhul.github.io/RoadMap/

General Courses

- [Volume I : The Complete Cyber Security Course by Nathan House](https://www.udemy.com/the-complete-internet-security-privacy-course-volume-1/) __Intermediate Level__

- [Volume II: The Complete Cyber Security Course by Nathan House](https://www.udemy.com/network-security-course/) --> __Intermediate Level__

- [Volume III: The Complete Cyber Security Course by Nathan House](https://www.udemy.com/the-complete-cyber-security-course-anonymous-browsing/) --> __Intermediate Level__

- [Volume IV: The Complete Cyber Security Course by Nathan House](https://www.udemy.com/network-security-course/)

- [System Security: Basic to advance level course by infySEC UK (5 starts for the delivery of the concepts)](https://www.udemy.com/sys-hacking/) --> __Basic Level__

- [Malware and Security course by infySEC UK (5 starts for the delivery of the concepts)](https://www.udemy.com/malwares/) --> __Intermediate Level__

- [CompTIA Security + Courses by PluralSight](https://www.pluralsight.com/paths/comptia-security-plus) __good for general concetps__

- [Web Application Penetration Testing Fundamentals by Mike Woolard](https://app.pluralsight.com/library/courses/web-app-pentesting-fundamentals/table-of-contents) __pluralsight__ __(90% Theory, 10% hands-on)__

- [Ethical Hacking: Hacking Web Applications by Troy Hunt](https://app.pluralsight.com/library/courses/ethical-hacking-web-applications/table-of-contents) __Pluralsight - Theory__

Pentesting Courses

- [Penetration Testing Student by elearningSecurity](https://www.elearnsecurity.com/course/penetration_testing_student/)

- [Penetration Testing Professional by eLearningSecuirty PTPv4](https://www.elearnsecurity.com/course/penetration_testing/)

`OSCP Roadmap:`

[![C9_T0_NLi_W0_AAmq_T9.jpg](https://s33.postimg.org/bwtkwie8v/C9_T0_NLi_W0_AAmq_T9.jpg)](https://postimg.org/image/fgfimbgyj/)

Level 1 :

General Terminology:

- [100 Top Computer Security Questions and Answers](https://github.com/nairuzabulhul/.CodeBits/blob/master/Security/100%20Security%20Questions.md) <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"> <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"> <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"> <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"> <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">

- [100 Top Networking Questions and Answers](https://github.com/nairuzabulhul/Algorithms_in_Python/blob/master/InterviewQuestions/Top%20100%20Networking%20Interview%20Questions%20%26%20Answers.md) <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"> <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"> <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"> <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"> <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">

- [10 things InfoSec professionals need to know about networking](https://artplusmarketing.com/10-things-infosec-professionals-need-to-know-about-networking-d159946efc93) <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"> <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"> <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"> <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"> <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">

Books :

- [Volient Python](https://www.amazon.com/Violent-Python-Cookbook-Penetration-Engineers/dp/1597499579/ref=pd_sim_14_1?_encoding=UTF8&pd_rd_i=1597499579&pd_rd_r=5C5E512J452R8PW2PE6H&pd_rd_w=LhlpR&pd_rd_wg=KSEN0&psc=1&refRID=5C5E512J452R8PW2PE6H)

- [Black Hat Python](https://www.amazon.com/Black-Hat-Python-Programming-Pentesters/dp/1593275900/ref=sr_1_1?ie=UTF8&qid=1480898714&sr=8-1&keywords=black+hat+Python) __Intermediate Python__ <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"> <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"> <img

src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"> <img
src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">

- [Wireshark Essentials by James Baxter](https://www.amazon.com/Wireshark-Essentials-James-H-Baxter/dp/1783554630) <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"> <img
src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"> <img
src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">

- [Kali Linux: Wireless Penetration Testing Beginner's Guide by Vivek Ramachandran (Author), Cameron Buchanan](https://www.amazon.com/Kali-Linux-Wireless-Penetration-Beginners/dp/1783280417/ref=sr_1_1?s=books&ie=UTF8&qid=1503563753&sr=1-1&keywords=wireless+by+vivek) __Beginners__ <img
src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"> <img
src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"> <img
src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"> <img
src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"> <img
src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">

Online Courses

- [Volume I : The Complete Cyber Security Course by Nathan House](https://www.udemy.com/the-complete-internet-security-privacy-course-volume-1/) __Intermediate Level__ <img
src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"> <img
src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"> <img
src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"> <img
src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"> <img
src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">

- [Volume II: The Complete Cyber Security Course by Nathan House](https://www.udemy.com/network-security-course/) --> __Intermediate Level__ <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">

- [Volume III: The Complete Cyber Security Course by Nathan House](https://www.udemy.com/the-complete-cyber-security-course-anonymous-browsing/) --> __Intermediate Level__ <img
src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">

- [Volume IV: The Complete Cyber Security Course by Nathan House](https://www.udemy.com/network-security-course/)

- [System Security: Basic to advance level course by infySEC UK (5 starts for the delivery of the concepts)](https://www.udemy.com/sys-hacking/) --> __Basic Level__

- [Malware and Security course by infySEC UK (5 starts for the delivery of the concepts)](https://www.udemy.com/malwares/) --> __Intermediate Level__

- [CompTIA Security + Courses by PluralSight](https://www.pluralsight.com/paths/comptia-security-plus) __good for general concetps__ [1-6]

  - 1 DONE

 - [Web Application Penetration Testing Fundamentals by Mike Woolard](https://app.pluralsight.com/library/courses/web-app-pentesting-fundamentals/table-of-contents) __pluralsight__ __(90% Theory, 10% hands-on)__

- [Ethical Hacking: Hacking Web Applications by Troy Hunt](https://app.pluralsight.com/library/courses/ethical-hacking-web-applications/table-of-contents) __Pluralsight - Theory__

OS Commands:

__Linux__:

- [100 Common Linux Commands](https://github.com/nairuzabulhul/.CodeBits/blob/master/Linux/100%20Common%20Linux%20Commands.md)

__Windows__:

- [Common Windows Commands]()

Git Commands

- [Basic Git Commands](https://github.com/quinnliu/gitCommands)
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">

Programming & Scripting

__Python__

- [Import Python](http://importpython.com/books/) - A collection of Python books from novice to expert <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">

- Python for Beginners by Alex Bowers <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">

- Complete Python BootCamp by Jose Portilla :

- Ultimate Python Programming Tutorial by Infinite Skills
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">

- Introduction to Python for beginners
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">

- [Python Tutorials by Code Academy](https://www.codecademy.com/learn/python)

<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">

- [Treehouse Django Tutorials](https://teamtreehouse.com/tracks/learn-django)
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">

- [Django Tutorials for Beginners by NewBoston](https://www.youtube.com/watch?v=qgGIqRFvFFk&list=PL6gx4Cwl9DGBlmzzFcLgDhKTTfNLfX1IK)
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">

- [Django Tutorial: Build your first Fast & Free by BlueApple](https://www.udemy.com/create-your-first-django-website-fast-free/)
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">

- [Python for Security](https://www.udemy.com/python-for-offensive-security-practical-course/?start=0)

- [Python Developer Career Path](https://www.packtpub.com/mapt/skill-plans/programmer/python-developer)

__JavaScript__

- [Free Code Camp](https://www.freecodecamp.com/) <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">

- [Web Development BootCamp by Colt Steele (Udemy online Course)](https://www.udemy.com/the-web-developer-bootcamp/) <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">

<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">

- [Ultimate Web Designer and Developer Course by Brad Hussey](https://www.udemy.com/web-developer-course/) <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">

- The Compelete Web Developer Course- Build 14 website v1.0 by Rob Percival <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">

- [JavaScript from Beginner to Expert by Arkadiusz Włodarczyk](https://www.udemy.com/javascript-from-beginner-to-expert-bring-life-to-your-site/) <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">

- [Projects in JavaScript & jQuery by Edonix](https://www.udemy.com/projects-in-javascript-jquery/) <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">

- [The Complete BootStrap: Master Class Course Build 4 projects by Joe Parys](https://www.udemy.com/bootstrapcourse/) <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">

__C Programming:__

- [C programming Tutorials by NewBoston](https://www.youtube.com/playlist?list=PL6gx4CwI9DGAKIXv8Yr6nhGJ9Vlcjyymq)
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">

- [Computer Systems programming in C by q Liu](https://www.youtube.com/playlist?list=PLPXsMt57rLtjNzxZBDg9xJB7KT83WStBO)
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">

- [C Programming in Linux Tutorial by ShellWaveX](https://www.youtube.com/playlist?list=PLypxmOPCOkHXbJhUgjRaV2pD9MJkIArhg)

- [C Programming Tutorials by the Bad Tutorials](https://www.youtube.com/playlist?list=PL_RGaFnxSHWoGzOXqtKeM71OLpvZbuU0P)

Youtube:

- [NMap 101 byHAK5](https://www.youtube.com/playlist?list=PLW5y1tjAOzI0ZLv7YfQtToQmc0yVDfkKO) --> __Basic Level__<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"> <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"> <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"><img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"> <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">

- [Netcat by HAK5](https://www.youtube.com/playlist?list=PLW5y1tjAOzI1v-RQ8rAftvqKawXQR87eL) -->__Basic Level__<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"> <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"> <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"><img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"> <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">

Projects:

- [Open Gate](https://github.com/nairuzabulhul/OpenGate)

- [KeyPlexer](https://github.com/nairuzabulhul/KeyPlexer)

- [Firewall Rules](https://github.com/nairuzabulhul/Firewall_Rules)

Level 2:

Books:

- [Effective Python for Penetration Testing by Rejah Rehim](https://www.amazon.com/Effective-Python-Penetration-Testing-Rejah/dp/1785280694)

  - [Chapter9 : Automation of tools]()

- [Linux Bible](https://github.com/nairuzabulhul/E-Books/blob/master/Linux/Linux%20Bible%2C%209th%20Edition.pdf)

- [Google Dorks](http://shop.oreilly.com/product/9780128029640.do)

  - [Chapter2: Advanced Operators](https://github.com/nairuzabulhul/RoadMap/blob/master/BooksNotes/Google%20Dorks/gooDorks.md)

Online Courses

- [PTS]() <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"> <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"> <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"><img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"> <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">__Hands-on Courses__

 Notes:

  - [Networking](https://github.com/nairuzabulhul/RoadMap/blob/master/PTS/Networking.md)
  - [Web Application](https://github.com/nairuzabulhul/RoadMap/blob/master/PTS/Web%20Application.md)
  - [Pentesting](https://github.com/nairuzabulhul/RoadMap/blob/master/PTS/Pentesting.md)
  - [Vulnerability Assessment](https://github.com/nairuzabulhul/RoadMap/blob/master/PTS/Vulnerability%20Assessement.md)

    - [Metasploit Commands](https://github.com/nairuzabulhul/RoadMap/blob/master/Commands/Metasploit.md)

  - Web Attacks:
    - [Introduction](https://github.com/nairuzabulhul/RoadMap/blob/master/PTS/Web%20Attacks%20_introduction.md)

- [System Attacks]()

- [Network Attacks]()

- [SQL Injection by Cybrary](https://www.cybrary.it/skill-certification-course/sql-injection-certification-training-course) <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"> <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"> <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10"> __Quick general overview about SQL injection[Not deep]__

Tools &Commands :

- [General Commands](https://github.com/nairuzabulhul/RoadMap/blob/master/Commands/Commands.md)

- [Nmap]()

- [Ncat]()

- [fping]()

- [Telnet]()

- [Open_SSL]()

- [Dirbuster]()

- [Nessus]()

- [BurpSuite]()

- [OWASP ZAP]()

- [Wireshark]()

- [Sysinternal whois]()

- [p0f]()

- [Nexpose]

- [sQLmap]

- [Firebug]

- [OpenVas]

Level 3

[PTP Roadmap by eLearningSecurity](https://www.elearnsecurity.com/course/penetration_testing)
:

- [__Web Security__](https://github.com/nairuzabulhul/RoadMap#web-security-)

- __Network Security__

- __System Security__

- __Wifi Security__

- __Ruby & Metasploit__

Web Security :

Books:

- [The Web Application Hacker's Handbook Finding and Exploiting Security Flaws Kindle Edition by Dafydd Stuttard - 2011](https://github.com/nairuzabulhul/E-Books/blob/master/Security/%5BThe%20Web%20Application%20Hacker's%20Handbook%20Finding%20and%20Exploiting%20Security%20Flaws%20Kindle%20Edition%20by%20Dafydd%20Stuttard%20-%202011%5D.pdf) __Level: Intermediate__ <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">

  - [Chapter 9 Notes for SQL](https://github.com/nairuzabulhul/RoadMap/blob/master/PTP/Web_Security/SQL_NOTES.md)

  - [Chapter 12 Noted for XSS](https://github.com/nairuzabulhul/RoadMap/blob/master/PTP/Web_Security/XSS%20CheatSheet.md)

Courses:

- [PTP NOTES](https://github.com/nairuzabulhul/RoadMap/tree/master/PTP/Web_Security)

  - [General Notes from PTP](https://github.com/nairuzabulhul/RoadMap/blob/master/PTP/Web_Security/Web%20Security%20Notes.md)

  - [SQL Notes:](https://github.com/nairuzabulhul/RoadMap/blob/master/PTP/Web_Security/SQL_NOTES.md)

  - [XSS Notes:](https://github.com/nairuzabulhul/RoadMap/blob/master/PTP/Web_Security/XSS%20Notes.md)

- [Learning Website Pentesting from scratch by Zaid Sabih](https://www.udemy.com/learn-website-hacking-penetration-testing-from-scratch/learn/v4/t/lecture/5878098?start=0) __Udemy__ __Level: Beginners -- Intermediate__ <img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">
<img src="https://s11.postimg.org/4xe7kokxf/star.pngg" width="10">

- [Web Application Penetration Testing with Burp Suite By Sunny Wear](https://www.pluralsight.com/courses/web-application-penetrationtesting-with-burp-suite) __PluralSight__

- [CEH Web Security Section by]()

- [SQL Injection by Tron Hunt](https://www.pluralsight.com/courses/ethical-hacking-sql-injection) __PluralSight__

Hands-on:

- [Pentesterlab]()

- [Over The Wire - Natas](http://overthewire.org/wargames/natas/)

CheatSheet:

- [XSS Payloads](https://github.com/nairuzabulhul/RoadMap/blob/master/PTP/Web_Security/CheatSheets/XSS.md)

- [SQLInjections](https://github.com/nairuzabulhul/RoadMap/blob/master/PTP/Web_Security/CheatSheets/SQL.md)

- [Extra Resources: Shell Uploads](http://www.securityidiots.com/Web-Pentest/hacking-website-by-shell-uploading.html)

- [Extra Resources: Shell uploads](https://xapax.gitbooks.io/security/content/bypass_image_upload.html)

Network Security:

Courses:

- PTP
- [CompTIA SY0-401 Security+ Certification by Professor Messer](https://www.youtube.com/watch?v=dv7I0SkF6P8&list=PLG49S3nxzAnkcKd71N4OjSv4cUXNhoPlQ)

Hands-on:

- [Network Analysis By CyberSkyline (Cybrary)]()

- [Log Analysis by CyberSkyline (Cybrary)]()

Books:

- [The Network Security Test Lab: A Step-by-Step Guide](https://www.amazon.com/Network-Security-Test-Step-Step-ebook/dp/B013SX649G/ref=sr_1_3?ie=UTF8&qid=1508269868&sr=8-3&keywords=Network+security)

- [The Web Application Hacker's Handbook Finding and Exploiting Security Flaws Kindle Edition by Dafydd Stuttard](https://github.com/nairuzabulhul/E-Books/blob/master/Web%20Development/%5BThe%20Web%20Application%20Hacker's%20Handbook

%20Finding%20and%20Exploiting%20Security%20Flaws%20Kindle%20Edition%20by%20Dafydd%20Stuttard%20-%202011%5D.pdf)

- [Burp Suite Essentials](https://github.com/nairuzabulhul/E-Books/blob/master/Web%20Development/Burp%20Suite%20Essentials.pdf)

- [Nmap 6 Cookbook: The Fat Free Guide to Network Security Scanning](https://www.amazon.com/Nmap-Cookbook-Network-Security-Scanning/dp/1507781385/ref=sr_1_1?s=books&ie=UTF8&qid=1504015056&sr=1-1&keywords=nmap+6)

- [Coding for Penetration Testers, Second Edition: Building Better Tools 2nd Edition](https://www.amazon.com/Coding-Penetration-Testers-Second-Building/dp/0128054727/ref=dp_ob_title_bk)

Extra Courses:

- [Play by Play: Exploring the Internet of Vulnerabilities](https://www.pluralsight.com/courses/play-by-play-exploring-internet-of-vulnerabilities)

- [Debugging the Web with FireBug, WebDeveloper, and Fiddler By Shawn Wildermuth](https://www.pluralsight.com/courses/web-debug) __PluralSight__

- [Pentester Academy]()

- [eCPPT Review](https://www.doyler.net/security-not-included/ecppt-exam)

- [eCPPT Review](https://www.rcesecurity.com/2012/03/ecppt-course-and-exam-review/)

- [BREAKING INTO INFOSEC: A BEGINNERS CURRICULUM](https://s3ctur.wordpress.com/2017/06/19/breaking-into-infosec-a-beginners-curriculum/)

Level 4

Reviews:

- [Offensive Security Certified Professional (OSCP) Review by Jim Wilbur](https://www.jimwilbur.com/2017/07/oscp-review/)

- [My experience with the OSCP certification Daniel Tomescu](https://securitycafe.ro/2016/03/17/my-experience-with-the-oscp-certification/)

- [OSCP-prep](https://github.com/ibr2/OSCP-Prep/blob/master/Practicing%20CTF)

- [OSCP Survival Guide](https://github.com/frizb/OSCP-Survival-Guide)

- [OSCP by John Kennedy](https://www.nebraskacert.org/csf/CSF-Oct2016.pdf)

- [Abatchy Blog](http://www.abatchy.com/2017/03/how-to-prepare-for-pwkoscp-noob.html)

- [OSCP by techexam](http://www.techexams.net/forums/security-certifications/127950-oscp-prep.html)

- [OSCP Review](http://www.hackingtutorials.org/hacking-courses/offensive-security-certified-professional-oscp/)

- [OSCP Prep](https://github.com/ihack4falafel/OSCP)

- [Infosec Review](http://www.pentest.guru/index.php/2016/04/07/cracking-infosec-interview-not-suck/)

- [oscp Review](https://www.rcesecurity.com/2013/05/oscp-course-and-exam-review/)

- [A Detailed Guide on OSCP Preparation – From Newbie to OSCP](http://niiconsulting.com/checkmate/2017/06/a-detail-guide-on-oscp-preparation-from-newbie-to-oscp/)

OpenSSL:

- [21 OpenSSL Examples to Help You in Real-World](https://geekflare.com/openssl-commands-certificates/)

Nmap

- [7 Nmap NSE Scripts for Recon](https://hackertarget.com/7-nmap-nse-scripts-recon/)

- [SANS Institute InfoSec Reading Room](https://www.sans.org/reading-room/whitepapers/testing/scanning-windows-deeper-nmap-scanning-engine-33138)

- [SOLDIERX.COM](https://www.soldierx.com/tutorials)

Linux

Pentest

- [Penetration Testing Tools Cheat Sheet](https://highon.coffee/blog/penetration-testing-tools-cheat-sheet/)

- [Top 5 Security Tools —August 2017](https://medium.com/hack-with-github/top-5-security-tools-august-2017-bbae4e155c59)

Bash Scripting:

- [BASH Programming - Introduction HOW-TO](http://tldp.org/HOWTO/Bash-Prog-Intro-HOWTO.html)

Exploit Development:

- [Best books, tutorials and courses to learn about exploit development](http://www.pentest.guru/index.php/2016/01/28/best-books-tutorials-and-courses-to-learn-about-exploit-development/)

Wireshark:

- [WIRESHARK DISPLAY FILTERS](http://hacktress.com/wp-content/uploads/2016/02/Wireshark_Display_Filters-1.pdf)

Life Cycle :

- [Information Gathering]()
- [Fingerprinting & Scanning]()
- [Vlunerability Assessment]()
- [Exploitation]()
- [Reporting]()

Information Gathering :

__General List__

- WHOIS
- DNS Information

- Check live hosts by their IP
- Check if one or more webites using the same IP
- Services runnign on the network
- Open ports
- OS running on hosts or servers

- Checking Items:
    - Emails
    - Phone numbers
    - websites
    - Addresses
    - Social Media : LinkedIn, Facebook, Twitter, CrunchBase,

Whoeis:
- use the command whois in Linux and OSX to find the general information about a domain
  Ex: whois www.apple.com

- For Windows, Sysinternal Whois

__Web Applicaiton__:

- Domain
- Sub Domain
- Page (website crawling)
- Technologies
- Langauges
- Frameworks and Content Managewment Systems
- Web Application Testing

Fingerprinting & Scanning

__OS Fingerprinting:__

- Fingerprinting OS helps narrow down the range of vulnerabilities and exploitation
- Finding an approximate version of the OS
- Level of patching

__Port Scanning:__

- Open ports
- Type of services on the ports
- Knowing the running service can infer:
    - OS
    - IP address inference (server IP or Client IP)
    - Types of servers --> Databases, Web, Email

__General Items__

- Routers
- Firewalls
- Hosts
- Services
- Printers
- Ports

>> You can perform the fingerprinting passively (through analyzing wireshark stored pcap file) or Actively unsing POF

__Port status__:

- if packets are flaged with RST means that the port is __closed__
- if packets compeleted the handshake, then sent RST flag means the port is __open__
- Every TCP connection (__full handshake__)is logged into the system and can be detectable
- __TCP syn__ is a stealthy way to scan the ports. Sending Syn packets to the target and analyze the results
  >>> The TCP-SYN sends a SYN packet to the target, if it gets RST, it means that the port is closed.

  >>> if the packets are returned with ACK flags mean that the port is open. Therefore, in this case the scanner send RST packet to force close the connection and not compelete the connection.

- Since there was NO complete handshake, no logs were recorded on the system.

__Daemon__:

>> is a service running on a server with specific port.
Port scanning helps discover daemon service on the network.

>> When running port scanning, if the daemon is not running or running on different ports, TCP packets are sent with RST flag

__Figuring out the scope of address__:

- 16 bit long netmask means 65536 hosts
- To detemine which IP addresses are assigned to hosts, use __ping sweep__

- __Ping Sweep Tool__:
  - Fping is a Linux tool

    Ex: fping -a -g IPRANGE

- a for returning live hosts
- g for peforeming ping sweeps instead of regular pings
EX:
fping -a -g 10.54.12/24

- Fping also return offline hosts despite the option -a on LAN, to weed out offline hosts while performing the ping sweep use /dev/null

EX: fping -a -g 192.136.82.0 192.168.82.66 2>/dev/null

__Tools__:

- P0f:
- Nmap
- Zmap [Nmap GUI]

Vulnerability Assessment :

- Can be manually or automatically using automted tools
- Tools can include Scanners, Fuzzers

Exploitation :

>> is the last stage after gathering information and enumerating the systems multiple times

OSCP Course Review
==========

- Offensive Security's PWB and OSCP — My Experience
[*http://www.securitysift.com/offsec-pwb-oscp/*](http://www.securitysift.com/offsec-pwb-oscp/)

- OSCP Journey
[*https://scriptkidd1e.wordpress.com/oscp-journey/*](https://scriptkidd1e.wordpress.com/oscp-journey/)

- Down with OSCP
[*http://ch3rn0byl.com/down-with-oscp-yea-you-know-me/*](http://ch3rn0byl.com/down-with-oscp-yea-you-know-me/)

- Jolly Frogs - Tech Exams (Very thorough)

[*http://www.techexams.net/forums/security-certifications/110760-oscp-jollyfrogs-tale.html*](http://www.techexams.net/forums/security-certifications/110760-oscp-jollyfrogs-tale.html)

OSCP Inspired VMs and Walkthroughs
==========

- https://www.hackthebox.eu/

- https://www.root-me.org/

- [*https://www.vulnhub.com/*](https://www.vulnhub.com/)

- Walk through of Tr0ll-1 - Inspired by on the Trolling found in the OSCP exam
  [*https://highon.coffee/blog/tr0ll-1-walkthrough/*](https://highon.coffee/blog/tr0ll-1-walkthrough/)
  Another walk through for Tr0ll-1
  [*https://null-byte.wonderhowto.com/how-to/use-nmap-7-discover-vulnerabilities-launch-dos-attacks-and-more-0168788/*](https://null-byte.wonderhowto.com/how-to/use-nmap-7-discover-vulnerabilities-launch-dos-attacks-and-more-0168788/)
  Taming the troll - walkthrough
  [*https://leonjza.github.io/blog/2014/08/15/taming-the-troll/*](https://leonjza.github.io/blog/2014/08/15/taming-the-troll/)
  Troll download on Vuln Hub
  [*https://www.vulnhub.com/entry/tr0ll-1,100/*](https://www.vulnhub.com/entry/tr0ll-1,100/)

- Sickos - Walkthrough:
  [*https://highon.coffee/blog/sickos-1-walkthrough/*](https://highon.coffee/blog/sickos-1-walkthrough/)
  Sickos - Inspired by Labs in OSCP

[*https://www.vulnhub.com/series/*](https://www.vulnhub.com/series/sickos,70/)[sickos](https://www.vulnhub.com/series/sickos,70/)[*,70/*](https://www.vulnhub.com/series/sickos,70/)

- Lord of the Root Walk Through
  [*https://highon.coffee/blog/lord-of-the-root-walkthrough/*](https://highon.coffee/blog/lord-of-the-root-walkthrough/)
  Lord Of The Root: 1.0.1 - Inspired by OSCP
  [*https://www.vulnhub.com/series/lord-of-the-root,67/*](https://www.vulnhub.com/series/lord-of-the-root,67/)

- Tr0ll-2 Walk Through
  [*https://leonjza.github.io/blog/2014/10/10/another-troll-tamed-solving-troll-2/*](https://leonjza.github.io/blog/2014/10/10/another-troll-tamed-solving-troll-2/)
  Tr0ll-2
  [*https://www.vulnhub.com/entry/tr0ll-2,107/*](https://www.vulnhub.com/entry/tr0ll-2,107/)

Cheat Sheets
==========

- Penetration Tools Cheat Sheet
  [*https://highon.coffee/blog/penetration-testing-tools-cheat-sheet/*](https://highon.coffee/blog/penetration-testing-tools-cheat-sheet/)

- Pen Testing Bookmarks
  [*https://github.com/kurobeats/pentest-bookmarks/blob/master/BookmarksList.md*](https://github.com/kurobeats/pentest-bookmarks/blob/master/BookmarksList.md)

- OSCP Cheatsheets
  [*https://github.com/slyth11907/Cheatsheets*](https://github.com/slyth11907/Cheatsheets)

- CEH Cheatsheet
  [*https://scadahacker.com/library/Documents/Cheat_Sheets/Hacking%20-%20CEH%20Cheat%20Sheet%20Exercises.pdf*](https://scadahacker.com/library/Documents/Cheat_Sheets/Hacking%20-%20CEH%20Cheat%20Sheet%20Exercises.pdf)

- Net Bios Scan Cheat Sheet
  [*https://highon.coffee/blog/nbtscan-cheat-sheet/*](https://highon.coffee/blog/nbtscan-cheat-sheet/)

- Reverse Shell Cheat Sheet
  [*https://highon.coffee/blog/reverse-shell-cheat-sheet/*](https://highon.coffee/blog/reverse-shell-cheat-sheet/)

- NMap Cheat Sheet
  [*https://highon.coffee/blog/nmap-cheat-sheet/*](https://highon.coffee/blog/nmap-cheat-sheet/)

- Linux Commands Cheat Sheet
  [*https://highon.coffee/blog/linux-commands-cheat-sheet/*](https://highon.coffee/blog/linux-commands-cheat-sheet/)

- Security Hardening CentO 7
  [*https://highon.coffee/blog/security-harden-centos-7/*](https://highon.coffee/blog/security-harden-centos-7/)

- MetaSploit Cheatsheet
  [*https://www.sans.org/security-resources/sec560/misc_tools_sheet_v1.pdf*](https://www.sans.org/security-resources/sec560/misc_tools_sheet_v1.pdf)

- Google Hacking Database:

[*https://www.exploit-db.com/google-hacking-database/*](https://www.exploit-db.com/google-hacking-database/)

- Windows Assembly Language Mega Primer

[*http://www.securitytube.net/groups?operation=view&groupId=6*](http://www.securitytube.net/groups?operation=view&groupId=6)

- Linux Assembly Language Mega Primer

[*http://www.securitytube.net/groups?operation=view&groupId=5*](http://www.securitytube.net/groups?operation=view&groupId=5)

- Metasploit Cheat Sheet
[*https://www.sans.org/security-resources/sec560/misc_tools_sheet_v1.pdf*](https://www.sans.org/security-resources/sec560/misc_tools_sheet_v1.pdf)

- A bit dated but most is still relevant

[*http://hackingandsecurity.blogspot.com/2016/04/oscp-related-notes.html*](http://hackingandsecurity.blogspot.com/2016/04/oscp-related-notes.html)

- NetCat

- [*http://www.sans.org/security-resources/sec560/netcat_cheat_sheet_v1.pdf*](http://www.sans.org/security-resources/sec560/netcat_cheat_sheet_v1.pdf)

- [*http://www.secguru.com/files/cheatsheet/nessusNMAPcheatSheet.pdf*](http://www.secguru.com/files/cheatsheet/nessusNMAPcheatSheet.pdf)

- [*http://sbdtools.googlecode.com/files/hping3_cheatsheet_v1.0-ENG.pdf*](http://sbdtools.googlecode.com/files/hping3_cheatsheet_v1.0-ENG.pdf)

- [*http://sbdtools.googlecode.com/files/Nmap5%20cheatsheet%20eng%20v1.pdf*](http://sbdtools.googlecode.com/files/Nmap5%20cheatsheet%20eng%20v1.pdf)

- [*http://www.sans.org/security-resources/sec560/misc_tools_sheet_v1.pdf*](http://www.sans.org/security-resources/sec560/misc_tools_sheet_v1.pdf)

- [*http://rmccurdy.com/scripts/Metasploit%20meterpreter%20cheat%20sheet%20reference.html*](http://rmccurdy.com/scripts/Metasploit%20meterpreter%20cheat%20sheet%20reference.html)

- [*http://h.ackack.net/cheat-sheets/netcat*](http://h.ackack.net/cheat-sheets/netcat)

Essentials
==========

- Exploit-db
  [*https://www.exploit-db.com/*](https://www.exploit-db.com/)

- SecurityFocus - Vulnerability database
  [*http://www.securityfocus.com/*](http://www.securityfocus.com/)

- Vuln Hub - Vulnerable by design
  [*https://www.vulnhub.com/*](https://www.vulnhub.com/)

- Exploit Exercises
  [*https://exploit-exercises.com/*](https://exploit-exercises.com/)

- SecLists - collection of multiple types of lists used during
  security assessments. List types include usernames, passwords, URLs,
  sensitive data grep strings, fuzzing payloads
  [*https://github.com/danielmiessler/SecLists*](https://github.com/danielmiessler/SecLists)

- Security Tube
  [*http://www.securitytube.net/*](http://www.securitytube.net/)

- Metasploit Unleashed - free course on how to use Metasploit
  [*https://www.offensive-security.com/metasploit-unleashed*](https://www.offensive-security.com/metasploit-unleashed/)*/*

- 0Day Security Enumeration Guide
  [*http://www.0daysecurity.com/penetration-testing/enumeration.html*](http://www.0daysecurity.com/penetration-testing/enumeration.html)

- Github IO Book - Pen Testing Methodology
  [*https://monkeysm8.gitbooks.io/pentesting-methodology/*](https://monkeysm8.gitbooks.io/pentesting-methodology/)

Windows Privledge Escalation
==========

- Fuzzy Security

[*http://www.fuzzysecurity.com/tutorials/16.html*](http://www.fuzzysecurity.com/tutorials/16.html)

- accesschk.exe
  https://technet.microsoft.com/en-us/sysinternals/bb664922

- Windows Priv Escalation For Pen Testers
  https://pentest.blog/windows-privilege-escalation-methods-for-pentesters/

- Elevating Privileges to Admin and Further
  https://hackmag.com/security/elevating-privileges-to-administrative-and-further/

- Transfer files to windows machines
  https://blog.netspi.com/15-ways-to-download-a-file/

- Windows-Privesc/windows privesc sectalks BNE0x19.pdf
  https://github.com/codingo/Windows-Privesc/blob/master/windows%20privesc%20sectalks%20BNE0x19.pdf

CTF Challenges

- [A few HBH Updates](http://hellboundhackers.org)
- [A site to test and learn about web hacking](http://hackertest.net)
- [Backdoor](https://backdoor.sdslabs.co)
- [CTFLearn](http://ctflearn.com) (a new CTF based learning platform with user-contributed challenges)
- [CTFs · GitHub](https://github.com/ctfs)
- [Embedded Security CTF](https://microcorruption.com/login) (one of the best interfaces, a good difficulty curve and introduction to low-level reverse engineering, specifically on an MSP430)
- [Exploit Exercises](http://exploit-exercises.com)
- [Go ahead and ScanMe!](http://scanme.nmap.org)
- [Hacker Challenges](http://counterhack.net/Counter_Hack/Challenges.html)
- [Hacking Challenges](http://hax.tor.hu)
- [RingZer0](http://ringzer0team.com)
- [Mod](http://mod-x.co.uk/main.php)
- [Net](http://net-force.nl)
- [Reversing.Kr](http://reversing.kr)
- [Roothack.org](http://roothack.org)
- [SmashTheStack Wargaming Network](http://smashthestack.org/wargames.html)
- [TheBlacksheep at www.bright](http://bright-shadows.net)
- [Wargames](http://overthewire.org/wargames)
- [World Wide Web Challenges](https://w3challs.com)
- [Xtreme Vulnerable Web Application (XVWA)](http://vulnhub.com)
- http://intruded.net
- http://pwnable.kr one of the most popular recent wargamming sets of challenges
- https://pwn0.com
- io.netgarage.org
- [picoCTF 2017](https://picoctf.com)Designed for high school students while the event is usually new every year, it's left online and has a great - difficulty progression
- [plateforme d'apprentissage dédiée au Hacking et à la Sécurité de l'Information](https://root-me.org)

<!DOCTYPE NETSCAPE-Bookmark-file-1>
<!-- This is an automatically generated file.
    It will be read and overwritten.
    DO NOT EDIT! -->
<META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=UTF-8">
<TITLE>Bookmarks</TITLE>
<H1>Bookmarks Menu</H1>

<DL><p>
  <DT><A HREF="place:type=6&sort=14&maxResults=10" ADD_DATE="1508869838"
LAST_MODIFIED="1508869838">Recent Tags</A>
  <HR> <DT><H3 ADD_DATE="1508869838" LAST_MODIFIED="1508869838">Mozilla Firefox</H3>
  <DL><p>
    <DT><A HREF="https://www.mozilla.org/en-US/firefox/help/" ADD_DATE="1508869838"
LAST_MODIFIED="1508869838" ICON_URI="http://www.mozilla.org/2005/made-up-favicon/1-
1508869838651"
ICON="
QA/wD/AP+gvaeTAAAACXBIWXMAAAsTAAALEwEAmpwYAAAAB3RJTUUH3gwMDAsTBZbkNwAAAB1pVF
h0Q29tbWVudAAAAAAAQ3JlYXRlZCB3aXRoIEdJTVBkLmUHAAABNElEQVQ4y8WSsU0DURBE3yyWIaAJaq
AAN4DPSL6AlIACKIEOyJEgRsIgOOkiInJqgAKowNg7BHdn7MOksNl+zZ//dvbDf5cAiklp22BdVtXdeTEpDYDB
9m1VzU6OJuVp2NdEQCaI96fH2YHG4+mDduKYNMYINTcjcGbXzQVDEAphG0k48zUsajIbnAiMIXThpW8EIC
E0RAK4dvoKg9NIcTiQ589otyHOZLnwqK5nLwBFUZ4igc3iM0d1ff8CMC6mZ6Ihiaqq3gi1aUAnArD00SW1fq
5OLBg0ymYmSZsR2/t4e/rGyCLW0sbp3oq+yTYqVgytQWui2FS7XYF7GFprY921T4CNQt8zr47dNzCkIX7y/jB
tH+v+RGMQrc828W8pApnZbmEVQp/Ae7BlOy2ttib81/UFc+WRWEbjckIAAAAASUVORK5CYII=">Help and
Tutorials</A>
    <DT><A HREF="https://www.mozilla.org/en-US/firefox/customize/" ADD_DATE="1508869838"
LAST_MODIFIED="1508869838" ICON_URI="http://www.mozilla.org/2005/made-up-favicon/2-
1508869838653"
ICON="
QA/wD/AP+gvaeTAAAACXBIWXMAAAsTAAALEwEAmpwYAAAAB3RJTUUH3gwMDAsTBZbkNwAAAB1pVF
h0Q29tbWVudAAAAAAAQ3JlYXRlZCB3aXRoIEdJTVBkLmUHAAABNElEQVQ4y8WSsU0DURBE3yyWIaAJaq
AAN4DPSL6AlIACKIEOyJEgRsIgOOkiInJqgAKowNg7BHdn7MOksNl+zZ//dvbDf5cAiklp22BdVtXdeTEpDYDB
9m1VzU6OJuVp2NdEQCaI96fH2YHG4+mDduKYNMYINTcjcGbXzQVDEAphG0k48zUsajIbnAiMIXThpW8EIC
E0RAK4dvoKg9NIcTiQ589otyHOZLnwqK5nLwBFUZ4igc3iM0d1ff8CMC6mZ6Ihiaqq3gi1aUAnArD00SW1fq
5OLBg0ymYmSZsR2/t4e/rGyCLW0sbp3oq+yTYqVgytQWui2FS7XYF7GFprY921T4CNQt8zr47dNzCkIX7y/jB
tH+v+RGMQrc828W8pApnZbmEVQp/Ae7BlOy2ttib81/UFc+WRWEbjckIAAAAASUVORK5CYII=">Customiz
e Firefox</A>
    <DT><A HREF="https://www.mozilla.org/en-US/contribute/" ADD_DATE="1508869838"
LAST_MODIFIED="1508869838" ICON_URI="http://www.mozilla.org/2005/made-up-favicon/3-
1508869838655"
ICON="
QA/wD/AP+gvaeTAAAACXBIWXMAAAsTAAALEwEAmpwYAAAAB3RJTUUH3gwMDAsTBZbkNwAAAB1pVF
h0Q29tbWVudAAAAAAAQ3JlYXRlZCB3aXRoIEdJTVBkLmUHAAABNElEQVQ4y8WSsU0DURBE3yyWIaAJaq
AAN4DPSL6AlIACKIEOyJEgRsIgOOkiInJqgAKowNg7BHdn7MOksNl+zZ//dvbDf5cAiklp22BdVtXdeTEpDYDB
9m1VzU6OJuVp2NdEQCaI96fH2YHG4+mDduKYNMYINTcjcGbXzQVDEAphG0k48zUsajIbnAiMIXThpW8EIC
E0RAK4dvoKg9NIcTiQ589otyHOZLnwqK5nLwBFUZ4igc3iM0d1ff8CMC6mZ6Ihiaqq3gi1aUAnArD00SW1fq
5OLBg0ymYmSZsR2/t4e/rGyCLW0sbp3oq+yTYqVgytQWui2FS7XYF7GFprY921T4CNQt8zr47dNzCkIX7y/jB

tH+v+RGMQrc828W8pApnZbmEVQp/Ae7BlOy2ttib81/UFc+WRWEbjckIAAAAASUVORK5CYII=">Get Involved</A>
<DT><A HREF="https://www.mozilla.org/en-US/about/" ADD_DATE="1508869838" LAST_MODIFIED="1508869838" ICON_URI="http://www.mozilla.org/2005/made-up-favicon/4-1508869838657"
ICON="">About Us</A>
</DL><p>
<DT><H3 ADD_DATE="1508869837" LAST_MODIFIED="1511893322" PERSONAL_TOOLBAR_FOLDER="true">Bookmarks Toolbar</H3>
<DD>Add bookmarks to this folder to see them displayed on the Bookmarks Toolbar
<DL><p>
<DT><A HREF="https://forums.offensive-security.com/" ADD_DATE="1508871047" LAST_MODIFIED="1508871055" ICON_URI="https://forums.offensive-security.com/favicon.ico"
ICON="" LAST_CHARSET="windows-1252">Forums</A>
<DD>Offensive Security Training student forums
<DT><A HREF="https://support.offensive-security.com/#!index.md" ADD_DATE="1508871074" LAST_MODIFIED="1508871079" ICON_URI="https://support.offensive-security.com/favicon.png"
ICON="

wCH0Om3Ofn/NF8+e0263ubq84OdvT7h8+55mu01/uAPW8e56gkuShO3tbTpJggUc0HQGEcFaS13XhBDQ
usaXKwpV3vsaj5DmOa7X7fLx7i79bhcnQiRCWBUYY0iShOlsxmw2I6wqqmWBL0uqNKX0nrL2uGKxYHZ7i5Y
lESDeQ7WEoOzt7ZFlGa1WjNYVYVXixRAEUBACrsxzrssl87FgQ8Cpsr3ZQjVweHjIeDwmjmMMYIJirGLFoMa
AOFyStLEiGB+gqrDB46wDhP39fa4uLwGhNxjwpBKIItQ58mpFvlrhBr0+3a1NbFBur6+RqiJuNRGB0WhEVdc
ANJtNHo1GEEUEY8jyHElT3CJNwXtMCMzXW9DtoKo455hMJnjvWdzfk2YrgrWYRoN8uSSbz3HTyYS5yMOA
VpUoshhjiOMYay1lWVKvlvxz9Ra1lkqVYAxFVeHwHl0fwwICPN1/Stzp8+bNK4bDIReXV3z5/Cv+/OMvaoV6/
YVKFSOAWYMCOGf57uVLrIu4ubmhKApUlW9+/ImNRgMNAUL4z1Ux/4cFGOz0Ofr+B7Is4+zsjOl0ynQ6Zf/r
Ez55svuQM2v9C0CsUuXnmrqxAAAAAElFTkSuQmCC" LAST_CHARSET="UTF-8">Support</A>
<DD>
<DT><A HREF="https://www.offensive-security.com/offsec-irc-guide/" ADD_DATE="1508871099"
LAST_MODIFIED="1508871106" ICON_URI="https://www.offensive-security.com/favicon.ico"
ICON="
AAAAQAAAAAAAAAAAAAAAAAAAAAAAAAACH/AAAi/wAAJf8AACj/FhpC/9PY4P/p6en/Pz8//zY2Nv+8vLz/
5uns/yMpUf8AACj/AAAl/wAAIv8AAB7/AAAf/wAAIf8AACT/AAAn/wMELv+Lk6n/9fX1/4mJif9ISEj/zs7O/6y
zw/8ICTP/AAAn/wAAJP8AACD/AAAc/wAAHv8AAB//AAAj/wAAJv8AACr/OUFm//Dx8v+enp7/UVFR/8/Pz/
9faIb/AgMs/wICKP8CAiT/AgIh/wEBHP8DAx7/BAQg/wQEJf8BASb/AAAp/xQYQf/d4un/wcHB/zo6Ov/v8PH
/KzNZ/w0NNP8QEDP/Dw8u/xERLP8MDCP/Ghow/yQkO/8iIj3/CQkr/wICKv8REzz/2+Dn/7i4uP83Nzf/9vf4/
zM5Xf8tLU//MDBN/zY2T/8uLkT/Hh4x/ycnO/80NUz/MzNP/x0dO/8YGDz/ICNI/9zh6P+0tLT/Tk5O//n6+/9
BR2j/Pj5c/0NDXP9FRVr/OztO/y4uPf8UFSf/FRYq/xMTLP8ODiz/Cwwv/xcZP//c4Of/nJyc/1JSU//5+vv/OT9g
/yYmR/8rK0f/Ly9G/ykqPP8jJDL/CQkb/wsMHv8MDCT/Cgon/wkJK/8TFjv/2+Dn/3Nzc/8nJyf/+Pr7/yUrTv8E
BCf/Bgcj/wgJIP8KChz/CwsY/xMTIv8lJTT/MjJE/zIySf8vL0r/JypK/93h6P9AQED/ExMT/+/x8v8lK0z/BQYl/wc
HIf8HCB3/BwcY/wUGEv8eHiv/OTlF/0pKWP9LS1z/TExh/0NGX//e4+j/Hx8f/w4ODf/m5+j/Ki9N/wwMJ/8O
DST/DQ0f/woKGP8HBhH/DQ0Z/x0dKf8pKTj/KSk7/ykpP/8rLUf/3OHm/xMTE/8XFxf/9/j5/y81T/8VFCz/Gh
ou/yIjMv8jIy//GRki/wEBDf8EBBD/BgYV/wYGGf8HBh3/EhUv/9vg5f8QEBD/Gxsb//n6+/8zOVD/Gxsv/yYm
N/88PUr/QEBK/ykqMP8cHCb/Kys1/yoqN/8eHy7/FhYp/x4hNv/4NjT/42Njf/5+vv/KjBG/w0NH/8VFST
/Jycy/ygoMf8eHiP/Kysz/0dHTv8/QEn/Kys5/xgYKP8gIjX/3OHm/5eXl//BwcH/+Pr7/yMpPf8CAhP/BQUS/ws
LFf8LCxL/CQkN/xQUH/8dHSX/Ghok/w0NGv8BARH/DA8g/9XZ3f/r6+v/9PT0//f4+f8aHzD/AAAO/wEBDP8
BAQr/AQEH/wAABP8AAA7/AQEM/wEBDv8AAA7/AAAP/wMEFf8zPE7/SFRn/0hUZv88RRlf/CAkY/wAAC/8A
AAn/AAAG/wAABP8AAAL/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA==" LAST_CHARSET="UTF-8">IRC</A>
<DD>
<DT><A HREF="https://support.offensive-security.com/#!pwk-reporting.md"
ADD_DATE="1508871119" LAST_MODIFIED="1508871127" ICON_URI="https://support.offensive-
security.com/favicon.png"
ICON="
Q4jU2TTWsbVxiFn/feO7JGGlvWRyy1Dm1MCcUuhYCbOjaULkqhULoJ9F967V0Xoau0XhS66Cq2G2gU2Y4k
e0YzGs3c+3ZRYbo4nM15zuLAkS3QIIIBUEWAhrMcv3jGR6NHKHB3n/Hq13PSYkkAPBDWkk8HA23EMeo9e
ZpSZBmdrTa//Paard4OcRwTOcvR559x8fc7gshDiVfFDYZDdh8/piqXzG9umX34wGarSdzc4PT0lIODA06Oj9h
sxUTGoNZiGw08UIWAS+/uGANGlWKRISEgGgBYLBacn59zcvyCeGODpN0majbZ6vVQEe7zHNkUUWstkTE4
wCH0Om3Ofn/NF8+e0263ubq84OdvT7h8+55mu01/uAPW8e56gkuShO3tbTpJggUc0HQGEcFaS13XhBDQ
usaXKwpV3vsaj5DmOa7X7fLx7i79bhcnQiRCWBUYY0iShOlsxmw2I6wqqmWBL0uqNKX0nrL2uGKxYHZ7i5Y
lESDeQ7WEoOzt7ZFlGa1WjNYVYVXixRAEUBACrsxzrssl87FgQ8Cpsr3ZQjVweHjIeDwmjmMMYIJirGLFoMa
AOFyStLEiGB+gqrDB46wDhP39fa4uLwGhNxjwpBKIItQ58mpFvlrhBr0+3a1NbFBur6+RqiJuNRGB0WhEVdc
ANJtNHo1GEEUEY8jyHElT3CJNwXtMCMzXW9DtoKo455hMJnjvWdzfk2YrgrWYRoN8uSSbz3HTyYS5yMOA
VpUoshhjiOMYay1lWVKvlvxz9Ra1lkqVYAxFVeHwHl0fwwICPN1/Stzp8+bNK4bDIReXV3z5/Cv+/OMvaoV6/
YVKFSOAWYMCOGf57uVLrIu4ubmhKApUlW9+/ImNRgMNAUL4z1Ux/4cFGOz0Ofr+B7Is4+zsjOl0ynQ6Zf/r
Ez55svuQM2v9C0CsUuXnmrqxAAAAAElFTkSuQmCC" LAST_CHARSET="UTF-8">Reporting</A>
<DD>

<DT><A HREF="https://10.70.70.70/oscpanel/labcpanel.php?md=37cef9a07d3b830f8da29f5d8be375fe&pid=337949&servers=0" ADD_DATE="1508871203" LAST_MODIFIED="1508871210" LAST_CHARSET="UTF-8">Control Panel</A>
<DD>
<DT><A HREF="https://www.exploit-db.com/" ADD_DATE="1508875012" LAST_MODIFIED="1508875019" ICON_URI="https://www.exploit-db.com/wp-content/uploads/2016/10/searchsploit.png" ICON="" LAST_CHARSET="UTF-8">Exploitdb</A>
<DD>The Exploit Database - Exploits, Shellcode, 0days, Remote Exploits, Local Exploits, Web Apps, Vulnerability Reports, Security Articles, Tutorials and more.
<DT><H3 ADD_DATE="1509116962" LAST_MODIFIED="1511965315">Resources</H3>
<DL><p>
<DT><H3 ADD_DATE="1511893347" LAST_MODIFIED="1511893374">General Cheatsheets</H3>

<DL><p>
<DT><A HREF="https://remram44.github.io/regex-cheatsheet/regex.html" ADD_DATE="1511366848" LAST_MODIFIED="1511366848" LAST_CHARSET="UTF-8">Regex cheatsheet</A>
<DD>
<DT><A HREF="https://tldr.ostera.io/" ADD_DATE="1511533161" LAST_MODIFIED="1511533173" LAST_CHARSET="UTF-8">TL;DR Pages</A>
<DD>Simplified, community-driven man pages!
<DT><A HREF="https://github.com/adam-p/markdown-here/wiki/Markdown-Cheatsheet" ADD_DATE="1509117015" LAST_MODIFIED="1509117022" ICON_URI="https://assets-cdn.github.com/favicon.ico"
ICON="
RYhb2Wv2tUQRDHv9Fwefdul535zp7GRrGz9RcoiEIK/wdBjBhFOwsVxMI/wMbSQrSyiWKwE0t/NHbRIoURJ
dqI2iRBBZVocxeez93L5XI68Jo3M/v5zuzOvgf0b9F7P2Uid8zsZTRb3tpu/9rabv+KZstm9tJE7njvpwDEdazb28
qy3E1y2sgfXeBaj5E/SE6XZbl7YLCqBpI3jVzpF5wQskLypqqGdVcdyTeDgutPJN/03Q3n3ISRi8OCV7qx6Jyb6A
kPIez9F/CqiBDC3hxcjXxbS5gz8v4gooxc7OTO1d6/DSHoXwKMvF1fRFWPd9xj3vupaPahOnYUeUyRx9WxjG
YfOqM4BgCqejwh7nb90O1LVVGW5Z5qnKqGRqOxC8CmRBM3NRqNXfUTX5blnsza+6rVz2SC9vc8NH1YW
Zb7M1s0040ZN/JnKkhEJjcqQEQmMwJ+AhiHOnc2FdAm3wPgRgUAIMl3KYY6dxYkp1NO7/2pIcABAN77Uy
kGyWnUx6TbnnVfnz1MVUNqm42cQzT7+pfDbGFY8K6Z2UKdE82+ItWaaDY/bAHR7HWKlRRg5NKwBRi5lB
SQdQBbhsjfki00isxm7oATw6KLyInkVovMguStjPMFgNEh8EejyIvMGN6CtlrHUs5OwPWN0klez62vrdYxAPD
R7EsuyMh7AMYHYG8z8l5u3Wj2BYAHAKjqjVVVqtecc0co8qQi4nubvMsQznS+YpsTwFHfbB5U584ZOWPk9
xy8w7mxmqmq26PZtw5shSIXAIwZ+TzRkRkAIwkBIybyoBe0Uv03Vd3+R7aIXK0GNZvNA0VR7Kx/SFT1UK7n
zrnD/QgQkaup/FGSzyqVPupq895PqeqVVqt1NNP+rrXXgpN8hh7TNV69MkXkfA9YymSN1r/GWge6KIod0
Wx+NSnGpxrCJe/9SVW9DKAYREA0my+KYke/lZDkw8wVLesVQPIhBvi5GWEIp6PZx0EFRPITQziD9NT0bY4i
F8zslZGf0fndztiYkZ/N7BVDuAjAbQT8X+w36KQvZccCoxkAAAAASUVORK5CYII=" LAST_CHARSET="UTF-8">Markdown Cheatsheet</A>
<DD>markdown-here - Google Chrome, Firefox, and Thunderbird extension that lets you write email in Markdown and render it before sending.
</DL><p>
<DT><H3 ADD_DATE="1511893330" LAST_MODIFIED="1511893343">Discover Vulnerabilities</H3>
<DL><p>
<DT><A HREF="http://www.cvedetails.com/product/585/Openbsd-Openssh.html?vendor_id=97" ADD_DATE="1511285752" LAST_MODIFIED="1511285764" LAST_CHARSET="UTF-8">CVEDetails</A>
<DD>Openbsd Openssh security vulnerabilities, exploits, metasploit modules, vulnerability statistics and list of versions
</DL><p>
<DT><H3 ADD_DATE="1511893301" LAST_MODIFIED="1511895308">Privilege Escalation</H3>
<DL><p>
<DT><A HREF="http://www.fuzzysecurity.com/tutorials/16.html" ADD_DATE="1511878894" LAST_MODIFIED="1511878894" ICON_URI="http://www.fuzzysecurity.com/images/favicon/favicon.ico"
ICON="
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACycnLS0dISFNKy4wdFZdX4t
FTE9qBQUFMAAAABEAAAABAAAAAAAAAAAAAAAAAAAAAAAAAAAAABUVKTGqeqq3YfYeJ53V
/g+7C0tn9k6Cl9T9ERtRpcnWsMTc3XAAAAAcAAAAAAAAAAAAAAAAAAAAAAAAAAAJmcHOEytrf/cT
U2f6xwsj+y93j/77P1v+isLX9zd7k/oOPk8caGiMdAAAAAAAAAAAAAAAAAAAAAAAAAADbnZ6lLnJzv
28zNL/sMHH/73O1f+zxMr/vc7U/8fY3v+WpKfNLi4uFgAAAAAAAAAAAAAAAAAAAAAAATFVZP5mmq9

PD1Nv/tcXL/3qFiv+LmZ//hpOY/7bHzf++0Nb/kqCk4iktMUMAAAAAAAAAAAAAAAAAAAAOUFBH6KxtrHI
2N7+xdXa/8TU2f+ap6v/k6Gm/5OgpP+5yc7/y9zi/7zM0v52f4SqGhoaEwAAAAAAAAAAAAAAAYCLjXOxv8X
6mqWo/n2Gie+Mlpn5xNTZ/8rc4v+uvMH+foaI+Jqlqf68y9H/oKyy8l9kZ1sAAAAAAAAADVDQxOap6u7kJu
g/mBmZ6o3Oz5SQ0lLgKSxuPXC1Nv+f4qOvjg6PHZfZWeyho+T/aWxtv58h4qmLi4uCwAAAABia3A0orC152
Boa98xNTU5AAAAAExVVR6vvsbTwNLZ+3J9gXgAAAABHBwcJFpgYbGMlZn+ipSYyTxISBUAAAAAa3Z6R6Szu
PNRWFq/EhISDgAAAABdYmY0ucrQ4Mze5fuJlZl+AAAAAQAAAAA6Ojxxc3p9+oaQlM41Pz8YAAAAGtzd0C
quL7we4aJzzc8PDNJSVAmm6mulcvd5P3X6vH/p7a9xmx0eERBQUcnU1pclYSPk/x+hoq0JycnDQAAAABJUF
cmnaux1rzO1P60wsjTucjN1Mvc4/zc8Pb/3/L5/9Tm7f6/zdPkucfL27LCx/qtvsT8ZnF1fAAAAAIAAAAAAAAA
A4qZnX26y9L31Obt/9vu9f/h9Pr/6fr9/+r6/f/f8vn/1urx/9Pm7f/I3OP/kJ+l4zo+Qj0AAAAAAAAAAAAAAAtL
S0RlKKmhLLBx+nU5u3+4fP5/+z7/v/x/v7/5/j8/9vu9f/Q5Ov/n7C182dydnsAAAAEAAAAAAAAAAAAAAAA
AAAAAAAAAdud31Roa+1p7vL0eXP4eb73O3y/tjq7/7B0tn8mamv2WRscXUXFxcLAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAADo6Og1mb283e4eMbYaSl5R6hImeXGRofDxAQDcAAAACAAAAAAAAAAAAAA
AAA/38AAPgPAADwBwAA8AcAAPAHAADgAwAA4AMAAMQhAADOcQAAznkAAMwxAADAAwAA4AMAA
OAHAAD4DwAA/z8AAA==">FuzzySecurity | Windows Privilege Escalation Fundamentals</A>
<DT><A
HREF="https://xapax.gitbooks.io/security/content/privilege_escalation_windows.html"
ADD_DATE="1511895308" LAST_MODIFIED="1511895308"
ICON_URI="https://xapax.gitbooks.io/security/content/gitbook/images/favicon.ico"
ICON="
RYhd3XT0gjVxwH8LBQKLSwbKHtoRehh21La6F3oShNJvPebybRGSXRBkLDoJYePCiGGDVIQ06ebKUhF5Wq
HQ/BY3updIgB0YOoBEQtoQWlLqIkWYPVfPeyhJg/ZhLUQn/wO8ybee/7GZhJ3lgs/3UJgtBqtVo/tdvtH1qt1v
csFsuTB4x7whh7JghCiyAIz+12+ycWSZJQ2pzzayL6m3P+BxH9yDnvZ4x93GiS1Wr9iDH2DRH9wDn/nYjSRPR
veV4FoFYTUZpzPnMXRhTFzxhj00SUNruuaUAJpEBEv5ZCbDbbF0T0W6NrVQU4HI6XJiGXjLHvGGMhzvmN
mTlOp/Oq/NoKAABcXl4inU5jfX0di4uLClVC6OnpMX1XiqIgEAhgfn4ehmHg6OgIuVwOAKCq6j91AdXq+voa
W1tbiEQikGW5avDExAQSiQTy+XzNdZoGlNbh4SFkWb71RG9ubpqa2xDAMAwEAgGMj49XBJQ/K9ls9n4BG
xsbkGUZ0WgUMzMzcDgcSKVSpgD5fB7xeByzs7NIJBLNAaanpzE1NVU89vv9iMVidQGFQgGjo6Po7u7GyMg
IZFnGyspK44BYLIb+/n7kcjlcXFzA6/VC1/W6gP39fUiShL29PQCAruvo7e1tHHB6egqv1wtVVaEoCgYGBpDJZ
OoCUqkUJEnCwcEBAGB1dRUul6txAACsra0Vxw3DuHWuFuDm5gZDQ0PweDwIh8Po6urCwsJCc4BkMlkcT
yaTpgAAkMlk4PV60dfXh3A4jEKh8LiAk5OT4ng0Gr0171EAc3NzxfGmX8NmALlcDrquF3+qfT4frq6uHgcQiU
SgKErxuLOzE7u7uyivBwOUtsfjwfb2dkX4gwM0TcPy8vKd/wt1AW63Gz6fD36/H5OTk6YBOzs7t1638/NzGIa
BWCyGYDAITdPgdrtBRIU7AbV6cHAQS0tLOD4+rgrIZrM4OztDPB7H8PBwzT1DeTe8J5RlGcFgsGI/MDY2lnc
6nQ2t1RTgvtuiadobqqo+bW9v/8Bms30uiuJXr/fz3xNRnDH2Z7OLM8YOJEnSGWMhURS/5px/KQjC87a2tn
dbWlreNP2R0dHR8b4oii7O+c9ElK0VyDl/SUS/iKLoev2Vdf+lqurbnPNvOed/lQS/4JwPq6r69EFCq1Vra+tbRP
STJEm6zWZ759GC/3f1CoP65RqJ0nM1AAAAAElFTkSuQmCC">Privilege Escalation - Windows · Security -
My notepad</A>
</DL><p>
<DT><A HREF="https://github.com/frizb/OSCP-Survival-Guide" ADD_DATE="1509116955"
LAST_MODIFIED="1509116984" ICON_URI="https://assets-cdn.github.com/favicon.ico"
ICON="
RYhb2Wv2tUQRDHv9FwefdUl535zp7GRrGz9RcoiEIK/wdBjBhFOwsVxMI/wMbSQrSyiWKwE0t/NHbRIoURJ
dqI2iRBBZVocxeez93L5XI68Jo3M/v5zuzOvgf0b9F7P2Uid8zsZTRb3tpu/9rabv+KZstm9tJE7njvpwDEdazb28
qy3E1y2sgfXeBaj5E/SE6XZbl7YLCqBpI3jVzpF5wQskLypqqGdVcdyTeDgutPJN/03Q3n3ISRi8OCV7qx6Jyb6A
kPIez9F/CqiBDC3hxcjXxbS5gz8v4gooxc7OTO1d6/DSHoXwKMvF1fRFWPd9xj3vupaPahOnYUeUyRx9WxjG
YfOqM4BgCqejwh7nb90O1LVVGW5Z5qnKqGRqOxC8CmRBM3NRqNXfUTX5blnsza+6rVz2SC9vc8NH1YW
Zb7M1s0040ZN/JnKkhEJjcqQEQmMwJ+AhiHOnc2FdAm3wPgRgUAIMl3KYY6dxYkp1NO7/2pIcABAN77Uy
kGyWnUx6TbnnVfnz1MVUNqm42cQzT7+pfDbGFY8K6Z2UKdE82+ItWaaDY/bAHR7HWKlRRg5NKwBRi5lB
SQdQBbhsjfki00isxm7oATw6KLyInkVovMguStjPMFgNEh8EejyIvMGN6CtlrHUs5OwPWN0klez62vrdYxAPD
R7EsuyMh7AMYHYG8z8l5u3Wj2BYAHAKjqjVVVqtecc0co8qQi4nubvMsQznS+YpsTwFHfbB5U584ZOWPk9

xy8w7mxmqmq26PZtw5shSIXAIwZ+TzRkRkAIwkBIybyoBe0Uv03Vd3+R7aIXK0GNZvNA0VR7Kx/SFT1UK7n
zrnD/QgQkaup/FGSzyqVPupq895PqeqVVqt1NNP+rrXXgpN8hh7TNV69MkXkfA9YymSN1r/GWge6KIod0
Wx+NSnGpxrCJe/9SVW9DKAYREA0my+KYke/lZDkw8wVLesVQPIhBvi5GWEIp6PZx0EFRPITQziD9NT0bY4i
F8zslZGf0fndztiYkZ/N7BVDuAjAbQT8X+w36KQvZccCoxkAAAAASUVORK5CYII=" LAST_CHARSET="UTF-
8">OSCP Survival Guide</A>

<DD>OSCP-Survival-Guide - Kali Linux Offensive Security Certified Professional Survival Exam Guide

<DT><A HREF="https://github.com/danielmiessler/SecLists" ADD_DATE="1509116997" LAST_MODIFIED="1509117001" ICON_URI="https://assets-cdn.github.com/favicon.ico" ICON="
RYhb2Wv2tUQRDHv9FwefduI535zp7GRrGz9RcoiEIK/wdBjBhFOwsVxMI/wMbSQrSyiWKwE0t/NHbRIoURJ
dqI2iRBBZVocxeez93L5XI68Jo3M/v5zuzOvgf0b9F7P2Uid8zsZTRb3tpu/9rabv+KZstm9tJE7njvpwDEdazb28
qy3E1y2sgfXeBaj5E/SE6XZbl7YLCqBpI3jVzpF5wQskLypqqGdVcdyTeDgutPJN/03Q3n3ISRi8OCV7qx6Jyb6A
kPIez9F/CqiBDC3hxcjXxbS5gz8v4gooxc7OTO1d6/DSHoXwKMvF1fRFWPd9xj3vupaPahOnYUeUyRx9WxjG
YfOqM4BgCqejwh7nb90O1LVVGW5Z5qnKqGRqOxC8CmRBM3NRqNXfUTX5blnsza+6rVz2SC9vc8NH1YW
Zb7M1s0040ZN/JnKkhEJjcqQEQmMwJ+AhiHOnc2FdAm3wPgRgUAIMl3KYY6dxYkp1NO7/2pIcABAN77Uy
kGyWnUx6TbnnVfnz1MVUNqm42cQzT7+pfDbGFY8K6Z2UKdE82+ItWaaDY/bAHR7HWKlRRg5NKwBRi5lB
SQdQBbhsjfki00isxm7oATw6KLyInkVovMguStjPMFgNEh8EejyIvMGN6CtlrHUs5OwPWN0klez62vrdYxAPD
R7EsuyMh7AMYHYG8z8l5u3Wj2BYAHAKjqjVVVqtecc0co8qQi4nubvMsQznS+YpsTwFHfbB5U584ZOWPk9
xy8w7mxmqmq26PZtw5shSIXAIwZ+TzRkRkAIwkBIybyoBe0Uv03Vd3+R7aIXK0GNZvNA0VR7Kx/SFT1UK7n
zrnD/QgQkaup/FGSzyqVPupq895PqeqVVqt1NNP+rrXXgpN8hh7TNV69MkXkfA9YymSN1r/GWge6KIod0
Wx+NSnGpxrCJe/9SVW9DKAYREA0my+KYke/lZDkw8wVLesVQPIhBvi5GWEIp6PZx0EFRPITQziD9NT0bY4i
F8zslZGf0fndztiYkZ/N7BVDuAjAbQT8X+w36KQvZccCoxkAAAAASUVORK5CYII=" LAST_CHARSET="UTF-
8">SecLists</A>

<DD>SecLists is the security tester's companion. It is a collection of multiple types of lists used during security assessments. List types include usernames, passwords, URLs, sensitive data grep strings, fuzzing payloads, and many more.

<DT><A HREF="https://forums.offensive-security.com/showthread.php?t=4689" ADD_DATE="1510161831" LAST_MODIFIED="1510161845" ICON_URI="https://forums.offensive-security.com/favicon.ico" ICON="
AAAAAAAABMLAAATCwAAAAAAAAAAAABkTCH/ZEwh/2RMIf9kTCH/ZEwh/2RMIf9kTCH/ZEwh/2RMIf9kTC
H/ZEwh/2RMIf9kTCH/ZEwh/2RMIf9kTCH/ZEwh/2RMIf9kTCH/ZEwh/2RMIf9kTCH/ZEwh/2NLIP9jSyD/ZEw
h/2RMIf9kTCH/ZEwh/2RMIf9kTCH/ZEwh/2RMIf9kTCH/ZEwh/2VNIu5nTyTaZ08l3WhRJ9ZoUSfbZEwh/mR
MIf9kTCH/ZEwh/2RMIf9kTCH/ZEwh/2RMIf9jSyD/aFAm/Yd0UkMAAAAAaFAlAwAAAABtVy4dZU0i8WRMI
f9kTCH/ZEwh/2RMIf9kTCH/ZEwh/2RMIf9iSh//blcu3oh1VA0AAAAAAAAAAAAAABrUyoFaFAmxmRLIP9k
TCH/ZEwh/2RMIf9kTCH/ZEwh/2RMIf9fRhr/hXJRlAAAAAAAAAAAAAAAAAAAAAAAAAAAAa1QrhWNKH/9kT
CH/ZEwh/2RMIf9kTCH/ZEwh/2NLIP9lTSL/j39fWQAAAAAAAAAoJJ4FqmbhA8AAAAAbFUsU2VNIv9kTCH/
ZEwh/2RMIf9kTCH/ZEwh/2NKH/9qUyrtlYZpFQAAAACekHUCkoFjmbGlkCoAAAAAdV84FWVNIuxkSyD/ZE
wh/2RMIf9kTCH/ZEwh/2BIHP9/a0eyAAAAAAAAAABrVCsYdF84139sSBcAAAAAe2dBAXBaMbtiSh//ZEwh/
2RMIf9kTCEzZEwhOF5FGTuPfV4cAAAAAAAAAACXiGsdb1kx2X5pRRcAAAAAAAAAAHReN31iSR7/ZEwh/2R
MIf8AAAAAAAAAAAAAAAAAAAAAAAAAAAAACXhmpTbVcu+KqdhS4AAAAAAAAAH9qRkZmTiT+Y0sg/
2RMIf8AAAAAAAAAAAAAAAAAAAAAAAAAAAAABvWTF7aVIo/499XmAAAAAAAAAAIRwThBnTyXoY0
sg/2RMIf9kTCHQZEwh1GRMIdpkTCHbZEwh22NLINhiSh7tY0sf/39rR3wAAAAAAAAAAAAAAB3YjytYUkd/
2RMIf9kTCH/ZEwh/2RMIf9kTCH/X0YZ/4l3VpsAAAAAAAAAAAAAAB4ZD54Ykoe/2R
MIf9kTCH/ZEwh/2RMIf9kTCH/YUgc/31pRdOZim4JAAAAAAAAAACOfF06Z1Am/2RMIf
9kTCH/ZEwh/2RMIf9kTCH/ZEwh/2xVLNtzXTcQAAAAAAAAACMe1oNa1Qq2WRMIf8

AAAAAAAAAAAAAAACgAAAA4AAAAfAAAAGQAAABEAAAAxAAAAMYAAA/GAAAPxgAAAAcAAAAHAAAA
AwAAAAMAIA" LAST_CHARSET="windows-1252">Guide to Alpha</A>
<DD>Welcome to Offensive Security's complete guide to "Alpha".

Warning. This thread contains spoilers.
Please note that Alpha cannot be included in your Lab Report

Table of Contents:

<DT><A HREF="https://github.com/rapid7/ssh-badkeys" ADD_DATE="1511287263"
LAST_MODIFIED="1511287275" ICON_URI="https://assets-cdn.github.com/favicon.ico"
ICON="
RYhb2Wv2tUQRDHv9Fwefdul535zp7GRrGz9RcoiEIK/wdBjBhFOwsVxMI/wMbSQrSyiWKwE0t/NHbRIoURJ
dqI2iRBBZVocxeez93L5XI68Jo3M/v5zuzOvgf0b9F7P2Uid8zsZTRb3tpu/9rabv+KZstm9tJE7njvpwDEdazb28
qy3E1y2sgfXeBaj5E/SE6XZbl7YLCqBpI3jVzpF5wQskLypqqGdVcdyTeDgutPJN/03Q3n3ISRi8OCV7qx6Jyb6A
kPIez9F/CqiBDC3hxcjXxbS5gz8v4gooxc7OTO1d6/DSHoXwKMvF1fRFWPd9xj3vupaPahOnYUeUyRx9WxjG
YfOqM4BgCqejwh7nb90O1LVVGW5Z5qnKqGRqOxC8CmRBM3NRqNXfUTX5blnsza+6rVz2SC9vc8NH1YW
Zb7M1s0040ZN/JnKkhEJjcqQEQmMwJ+AhiHOnc2FdAm3wPgRgUAIMl3KYY6dxYkp1NO7/2pIcABAN77Uy
kGyWnUx6TbnnVfnz1MVUNqm42cQzT7+pfDbGFY8K6Z2UKdE82+ItWaaDY/bAHR7HWKlRRg5NKwBRi5lB
SQdQBbhsjfki00isxm7oATw6KLyInkVovMguStjPMFgNEh8EejyIvMGN6CtlrHUs5OwPWN0klez62vrdYxAPD
R7EsuyMh7AMYHYG8z8l5u3Wj2BYAHAKjqjVVVqtecc0co8qQi4nubvMsQznS+YpsTwFHfbB5U584ZOWPk9
xy8w7mxmqmq26PZtw5shSIXAIwZ+TzRkRkAIwkBIybyoBe0Uv03Vd3+R7aIXK0GNZvNA0VR7Kx/SFT1UK7n
zrnD/QgQkaup/FGSzyqVPupq895PqeqVVqt1NNP+rrXXgpN8hh7TNV69MkXkfA9YymSN1r/GWge6KIod0
Wx+NSnGpxrCJe/9SVW9DKAYREA0my+KYke/lZDkw8wVLesVQPIhBvi5GWEIp6PZx0EFRPITQziD9NT0bY4i
F8zslZGf0fndztiYkZ/N7BVDuAjAbQT8X+w36KQvZccCoxkAAAAASUVORK5CYII=" LAST_CHARSET="UTF-
8">SSH Bad Keys</A>
<DD>ssh-badkeys - A collection of static SSH keys (public and private) that have made their way
into software and hardware products.
<DT><A HREF="https://monkeysm8.gitbooks.io/pentesting-
methodology/common_portsservices_and_how_to_use_them/port_135_-_msrpc.html"
ADD_DATE="1511965315" LAST_MODIFIED="1511965315"
ICON_URI="https://monkeysm8.gitbooks.io/pentesting-methodology/gitbook/images/favicon.ico"
ICON="
RYhd3XT0gjVxwH8LBQKLSwbKHtoRehh21La6F3oShNJvPebybRGSXRBkLDoJYePCiGGDVIQ06ebKUhF5Wq
HQ/BY3updIgB0YOoBEQtoQWlLqIkWYPVfPeyhJg/ZhLUQn/wO8ybee/7GZhJ3lgs/3UJgtBqtVo/tdvtH1qt1v
csFsuTB4x7whh7JghCiyAIz+12+ycWSZJQ2pzzayL6m3P+BxH9yDnvZ4x93GiS1Wr9iDH2DRH9wDn/nYjSRPR
veV4FoFYTUZpzPnMXRhTFzxhj00SUNruuaUAJpEBEv5ZCbDbbF0T0W6NrVQU4HI6XJiGXjLHvGGMhzvmN
mTlOp/Oq/NoKAABcXl4inU5jfX0di4uLCIVC6OnpMX1XiqIgEAhgfn4ehmHg6OgIuVwOAKCq6j91AdXq+voa
W1tbiEQikGW5avDExAQSiQTy+XzNdZoGlNbh4SFkWb71RG9ubpqa2xDAMAwEAgGMj49XBJQ/K9ls9n4BG
xsbkGUZ0WgUMzMzcDgcSKVSpgD5fB7xeByzs7NIJBLNAaanpzE1NVU89vv9iMVidQGFQgGjo6Po7u7GyMg
lZFnGyspK44BYLIb+/n7kcjlcXFzA6/VC1/W6gP39fUiShL29PQCAruvo7e1tHHB6egqv1wtVVaEoCgYGBpDJZ
OoCUqkUJEnCwcEBAGB1dRUul6txAACsra0Vxw3DuHWuFuDm5gZDQ0PweDwlh8Po6urCwsJCc4BkMlkcT
yaTpgAAkMlk4PV60dfXh3A4jEKh8LiAk5OT4ng0Gr0171EAc3NzxfGmX8NmALlcDrquF3+qfT4frq6uHgcQiU
SgKErxuLOzE7u7uyivBwOUtsfjwfb2dkX4gwM0TcPy8vKd/wt1AW63Gz6fD36/H5OTk6YBOzs7t1638/NzGIa
BWCyGYDAITdPgdrtBRIU7AbV6cHAQS0tLOD4+rgrIZrM4OztDPB7H8PBwzT1DeTe8J5RlGcFgsGI/MDY2lnc

6nQ2t1RTgvtuiadobqqo+bW9v/8Bms30uiuJXr/fz3xNRnDH2Z7OLM8YOJEnSGWMhURS/5px/KQjC87a2tn
dbWlreNP2R0dHR8b4oii7O+c9ElK0VyDl/SUS/iKLoev2Vdf+lqurbnPNvOed/lQS/4JwPq6r69EFCq1Vra+tbRP
STJEm6zWZ759GC/3f1CoP65RqJ0nM1AAAAAElFTkSuQmCC">Port 135 - MSRPC · Pentesting
Methodology</A>
</DL><p>
<DT><A HREF="http://pentestmonkey.net/blog/post-exploitation-without-a-tty"
ADD_DATE="1511791202" LAST_MODIFIED="1511791202">Internet Security by Zscaler</A>
</DL><p>
</DL>

https://github.com/frizb

Jim Wilbur's Blog
OSCP Links
This is a list of links I used while studying for the Offensive Security Certified Professional (OSCP) exam.
Reverse Shell Cheat Sheet – http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet
Offensive Security's Exploit Database Archive – https://www.exploit-db.com/
OSCP resource gold mine – https://backdoorshell.gitbooks.io/oscp-useful-links/content/
0x0 Exploit Tutorial: Buffer Overflow – Vanilla EIP Overwrite – http://www.primalsecurity.net/0x0-exploit-tutorial-buffer-overflow-vanilla-eip-overwrite-2/
Basic Linux Privilege Escalation – https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation
Vulnerable by Design – https://vulnhub.com
Elevating privileges by exploiting weak folder permissions – www.greyhathacker.net/?p=738/
NSEDoc Reference – https://nmap.org/nsedoc/
Encyclopaedia Of Windows Privilege Escalation – Brett Moore – www.youtube.com/watch?v=kMG8IsCohHA
Windows Privilege Escalation Fundamentals – http://www.fuzzysecurity.com/tutorials/16.html
0daysecurity Enumeration – http://0daysecurity.com/penetration-testing/enumeration.html
Free Password Hash Cracker – https://crackstation.net/
LinEnum – https://github.com/rebootuser/LinEnum
Linux_Exploit_Suggester – https://github.com/PenturaLabs/Linux_Exploit_Suggester
Windows-Exploit-Suggester – https://github.com/GDSSecurity/Windows-Exploit-Suggester
Windows Privilege Escalation – a cheatsheet – http://it-ovid.blogspot.com/2012/02/windows-privilege-escalation.html
unix-privesc-check – http://pentestmonkey.net/tools/audit/unix-privesc-check
windows-privesc-check – http://pentestmonkey.net/tools/windows-privesc-check
John The Ripper Hash Formats – http://pentestmonkey.net/cheat-sheet/john-the-ripper-hash-formats
Microsoft Privilege Escalation – www.toshellandback.com/2015/11/24/ms-priv-esc/
Kali linux Commands Complete List from A to Z – https://geekviews.tech/kali-linux-commands-complete-list/

Resources:
Some resources I used for this challenge:
http://www.fuzzysecurity.com/tutorials/16.html
http://pentestmonkey.net/category/cheat-sheet/shell

https://github.com/GDSSecurity/Windows-Exploit-Suggester
https://github.com/PenturaLabs/Linux_Exploit_Suggester
https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/
http://www.offensive-security.com/metasploit-unleashed/Main_Page
I also read the hackers playbook, the Metasploit unleashed book, and the Penetration Testing book by Georgia Weidman.
These are all very good resources.

- [Web Application Security on Fire - PHP Developers Cheat Sheet Version]
(https://speakerdeck.com/symbiansymoh/web-application-security-on-fire-php-developers-cheat-sheet-version)

OSCP-Archives

During my journey to getting the OSCP, I always come across many articles, Git repo, videos, and other types of sources of great and valuable information that helps me during my studies. While having all of these in a bookmark folder is great, I wanted to also build a curated list of the resources that I've collected overtime, all in one area for everyone to access.

This list will continue to grow over time as I come across new resources. If you know more resources or want me to add yours, please let me know and I'll add it in.

PS. A VERY big **thank you** to all the authors of these resources, for taking the time and energy putting this invaluable information together.

Enjoy!

~ Official Exam Guide ~

[`OSCP Certification Exam Guide`](https://support.offensive-security.com/#!oscp-exam-guide.md) - **Offensive Security**

~ Reviews and Experiences ~

[`31 Days of OSCP Experience`](https://scriptdotsh.com/index.php/2018/04/17/31-days-of-oscp-experience/) - **[ParanoidNinja](https://twitter.com/ninjaparanoid)**

[`Detailed Guide on OSCP Prep – From Newbie to OSCP`](http://niiconsulting.com/checkmate/2017/06/a-detail-guide-on-oscp-preparation-from-newbie-to-oscp/) - **Ramkisan Mohan**

[`Offensive Security Certified Professional – Lab and Exam Review`](https://theslickgeek.com/oscp/) - **[theslickgeek](https://twitter.com/theslickgeek)**

[`Passing The OSCP`](https://pinkysplanet.net/reflection-on-passing-the-oscp/amp/?__twitter_impression=true) - **[Pink_Panther](https://twitter.com/Pink_P4nther)**

[`OSCP Experience and the first torture!`](https://www.peerlyst.com/posts/oscp-experience-and-the-first-torture-nitesh-shilpkar-osce-oscp-oswp-ceh-crest) - **Nitesh Shilpkar**

~ Helpful VMs for Practice ~

[`Kioptrix`](https://sushant747.gitbooks.io/total-oscp-guide/content/) - **[loneferret](https://twitter.com/loneferret)**

[`OSCP-like Vulnhub VMs`](https://www.abatchy.com/2017/02/oscp-like-vulnhub-vms.html) - **[abatchy](https://twitter.com/abatchy17)**

[`OSCP Training VM's hosted on Vulnhub.com`](https://medium.com/@andr3w_hilton/oscp-training-vms-hosted-on-vulnhub-com-22fa061bf6a1) - **Andrew Hilton**

[`Pinky's Palace CTFs`](https://pinkysplanet.net/tag/ctf/) - **[Pink_Panther](https://twitter.com/Pink_P4nther)**

~ CTF Walkthroughs & Educational Videos ~

[`Hack The Box CTFs`](https://www.youtube.com/ippsec) - **[ippsec](https://twitter.com/ippsec)**

[`Hack The Box, Over The Wire, Other CTFs`](https://www.youtube.com/derekrook) - **[derekrook](https://twitter.com/derekrook)**

[`VunHub Walkthroughs`](https://highon.coffee/blog/walkthroughs/) - **[Arr0way](https://twitter.com/Arr0way)**

~ OSCP Prep, Tools, Cheatsheets, Guides, etc. ~

[`Metasploit Unleashed`](https://www.offensive-security.com/metasploit-unleashed/) - **Offensive Security**

[`15 Ways to Download a File`](https://blog.netspi.com/15-ways-to-download-a-file/) - **[NetSPI](https://twitter.com/NetSPI)**

[`Explain Shell - Great at explaining Linux Commands in Detail`](https://www.explainshell.com/) - **Idan Kamara**

[`Mixed Archives`](https://blog.g0tmi1k.com/archives/) - **[g0tmi1k](https://twitter.com/g0tmi1k)**

[`OWASP Testing Guide v4 Table of Contents`](https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents) - **[owasp](https://twitter.com/owasp)**

[`Penetration Testing Tools Cheat Sheet`](https://highon.coffee/blog/penetration-testing-tools-cheat-sheet/) - **[Arr0way](https://twitter.com/Arr0way)**

[`Reverse Shell Cheat Sheet`](https://highon.coffee/blog/reverse-shell-cheat-sheet/) - **[Arr0way](https://twitter.com/Arr0way)**

[`Linux Commands Cheat Sheet`](https://highon.coffee/blog/linux-commands-cheat-sheet/) - **[Arr0way](https://twitter.com/Arr0way)**

[`Reverse Shell Cheat Sheet`](http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet) - **Pentest Monkey**

[`Black Room Sec - CTFs, Guides, Tools`](https://www.blackroomsec.com/) - **[blackroomsec](https://twitter.com/blackroomsec)**

[`Dostoevskylabs's PenTest Notes`](https://dostoevskylabs.gitbooks.io/dostoevskylabs-pentest-notes/content/) - **Dostoevskylabs**

[`Pentest Compilation`](https://github.com/adon90/pentest_compilation) - **adon90**

[`SecLists`](https://github.com/danielmiessler/SecLists) - **danielmiessler**

[`OSCP-Prep`](https://github.com/burntmybagel/OSCP-Prep) - **burntmybagel**

[`OSCP-Prep`](https://github.com/rhodejo/OSCP-Prep) - **rhodejo**

[`OSCP Scripts`](https://github.com/garyhooks/oscp) - **garyhooks**

[`OSCP Scripts & Documents`](https://github.com/ihack4falafel/OSCP) - **ihack4falafel**

[`OSCP Recon Script`](https://github.com/xapax/oscp) - **xapax**

[`Cheatsheet-God`](https://github.com/OlivierLaflamme/Cheatsheet-God) - **OlivierLaflamme**

[`OSCP-Repo`](https://github.com/rewardone/OSCPRepo) - **rewardone**

[`Cheatsheets`](https://github.com/slyth11907/Cheatsheets) - **slyth11907**

[`OSCP tricks`](https://hackingandsecurity.blogspot.com/2017/09/oscp-tricks.html) - **WarLord**

[`Go-For-OSCP`](https://hackingandsecurity.blogspot.com/2017/08/go-for-oscp.html) - **WarLord**

[`How to prepare for the OSCP ? A STUDY PLAN`](https://www.peerlyst.com/posts/how-to-prepare-for-the-oscp-a-study-plan-magda-chelly-ph-d?utm_source=LinkedIn&utm_medium=Application_Share&utm_content=peerlyst_post&utm_campaign=peerlyst_shared_post) - **Magda CHELLY, CISSP, Ph.D**

[`OSCP useful Links`](https://backdoorshell.gitbooks.io/oscp-useful-links/content/) - **backdoorshell**

[`Total OSCP Guide`](https://sushant747.gitbooks.io/total-oscp-guide/content/) - **sushant747**

[`OSCP Course & Exam Preparation`](https://411hall.github.io/OSCP-Preparation/) - **[411Hall](https://twitter.com/411Hall)**

[`OSCP Journey: Python Code Challenges`](https://www.peerlyst.com/posts/oscp-journey-python-code-challenges-elias-ibrahim-cissp?utm_source=linkedin&utm_medium=social&utm_content=peerlyst_post&utm_campaign=peerlyst_shared_post) - **Elias Ibrahim**

[`SMB Enumeration Checklist`](https://0xdf.gitlab.io/2018/12/02/pwk-notes-smb-enumeration-checklist-update1.html) - **[0xdf](https://twitter.com/0xdf_)**

[`Tunneling and Pivoting`](https://0xdf.gitlab.io/2018/11/02/pwk-notes-tunneling.html) - **[0xdf](https://twitter.com/0xdf_)**

[`Post-Exploitation Windows File Transfers with SMB`](https://0xdf.gitlab.io/2018/10/11/pwk-notes-post-exploitation-windows-file-transfers.html) - **[0xdf](https://twitter.com/0xdf_)**

[`Multiple Ways to Exploit Tomcat Manager`](https://www.hackingarticles.in/multiple-ways-to-exploit-tomcat-manager/) - **[Raj Chande](https://twitter.com/rajchandel)**

~ SQL Injection ~

[`Preliminary SQL Injection Part 1`](https://jtnydv.xyz/2018/12/25/preliminary-sql-injection-part-1/) - **Jatin Yadav**

[`Preliminary SQL Injection Part 2`](https://jtnydv.xyz/2018/12/27/preliminary-sql-injection-part-2/) - **Jatin Yadav**

[`Informix SQL Injection Cheat Sheet`](http://pentestmonkey.net/cheat-sheet/sql-injection/informix-sql-injection-cheat-sheet) - **pentestmonkey**

[`MSSQL Injection Cheat Sheet`](http://pentestmonkey.net/cheat-sheet/sql-injection/mssql-sql-injection-cheat-sheet) - **pentestmonkey**

[`Oracle SQL Injection Cheat Sheet`](http://pentestmonkey.net/cheat-sheet/sql-injection/oracle-sql-injection-cheat-sheet) - **pentestmonkey**

[`MySQL SQL Injection Cheat Sheet`](http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet) - **pentestmonkey**

[`Postgres SQL Injection Cheat Sheet`](http://pentestmonkey.net/cheat-sheet/sql-injection/postgres-sql-injection-cheat-sheet) - **pentestmonkey**

[`DB2 SQL Injection Cheat Sheet`](http://pentestmonkey.net/cheat-sheet/sql-injection/db2-sql-injection-cheat-sheet) - **pentestmonkey**

[`Ingres SQL Injection Cheat Sheet`](http://pentestmonkey.net/cheat-sheet/sql-injection/ingres-sql-injection-cheat-sheet) - **pentestmonkey**

[`SQL Injection Reference Library & Techniques`](http://www.sqlinjection.net/what-is/) - **SQLINjection**

~ Linux Privilege Escalation ~

[`OSCP - Linux Priviledge Escalation`](https://hackingandsecurity.blogspot.com/2017/09/oscp-linux-priviledge-escalation.html?m=1) - **WarLord**

[`Basic Linux Privilege Escalation`](https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/) - **[g0tmi1k](https://twitter.com/g0tmi1k)**

~ Windows Privilege Escalation ~

[`OSCP - Windows Priviledge Escalation`](https://hackingandsecurity.blogspot.com/2017/09/oscp-windows-priviledge-escalation.html) - **WarLord**

[`Awesome-Windows-Exploitation`](https://github.com/enddo/awesome-windows-exploitation) - **enddo**

[`Windows Priv escalation`](https://github.com/kyawthiha7/oscp_notes/blob/master/windows_priv_escalation.md) - **kyawthiha7**

[`Windows Privilege Escalation Fundamentals`](http://www.fuzzysecurity.com/tutorials/16.html) - **[FuzzySec (b33f)](https://twitter.com/FuzzySec)**

~ LFI & RFI ~

[`PHP Local and Remote File Inclusion (LFI, RFI) Attacks`](https://hackingandsecurity.blogspot.com/2017/09/php-local-and-remote-file-inclusion-lfi.html) - **WarLord**

[`LFI Cheat Sheet`](https://highon.coffee/blog/lfi-cheat-sheet/) - **[Arr0way](https://twitter.com/Arr0way)**

~ Exploits & Exploit Developtment, Tutorials ~

[`Windows & Linux Exploit Development`](http://www.fuzzysecurity.com/tutorials.html) - **[FuzzySec (b33f)](https://twitter.com/FuzzySec)**

[`Exploit DB`](https://www.exploit-db.com/) - **Offensive Security**

[`Exploit Development - Starting from Part 1`](https://www.corelan.be/index.php/2009/07/19/exploit-writing-tutorial-part-1-stack-based-overflows/) - **Corelan Team**

[`Over The Wire - Wargames`](http://overthewire.org/wargames/) - **OverTheWire**

[SecuritySift](https://twitter.com/SecuritySift)

[`Windows Exploit Development – Part 1: The Basics`](https://www.securitysift.com/windows-exploit-development-part-1-basics/)

[`Windows Exploit Development – Part 2: Intro-Stack-Overflow`](https://www.securitysift.com/windows-exploit-development-part-2-intro-stack-overflow/)

[`Windows Exploit Development – Part 3: Changing-Offsets-and-Rebased-Modules`](https://www.securitysift.com/windows-exploit-development-part-3-changing-offsets-and-rebased-modules/)

[`Windows Exploit Development – Part 4: Locating-Shellcode-Jumps`](https://www.securitysift.com/windows-exploit-development-part-4-locating-shellcode-jumps/)

[`Windows Exploit Development – Part 5: Locating-Shellcode-Egghunting`](https://www.securitysift.com/windows-exploit-development-part-5-locating-shellcode-egghunting/)

[`Windows Exploit Development – Part 6: Seh-Exploits`](https://www.securitysift.com/windows-exploit-development-part-6-seh-exploits/)

[`Windows Exploit Development – Part 7: Unicode-Buffer-Overflows`](https://www.securitysift.com/windows-exploit-development-part-7-unicode-buffer-overflows/)

[shogun_lab](https://twitter.com/shogun_lab)

[`Zero Day Zen Garden: Windows Exploit Development - Part 0 [Dev Setup & Advice]`](http://www.shogunlab.com/blog/2017/08/11/zdzg-windows-exploit-0.html)

[`Zero Day Zen Garden: Windows Exploit Development - Part 1 [Stack Buffer Overflow Intro]`](http://www.shogunlab.com/blog/2017/08/19/zdzg-windows-exploit-1.html)

[`Zero Day Zen Garden: Windows Exploit Development - Part 2 [JMP to Locate Shellcode]`](http://www.shogunlab.com/blog/2017/08/26/zdzg-windows-exploit-2.html)

[`Zero Day Zen Garden: Windows Exploit Development - Part 3 [Egghunter to Locate Shellcode]`](http://www.shogunlab.com/blog/2017/09/02/zdzg-windows-exploit-3.html)

[`Zero Day Zen Garden: Windows Exploit Development - Part 4 [Overwriting SEH with Buffer Overflows]`](http://www.shogunlab.com/blog/2017/11/06/zdzg-windows-exploit-4.html)

[`Zero Day Zen Garden: Windows Exploit Development - Part 5 [Return Oriented Programming Chains]`](http://www.shogunlab.com/blog/2018/02/11/zdzg-windows-exploit-5.html)

Infosec Learning Materials

Resource for developing infosec skills for upcoming OSCP exam

OSCP Rules & Documents

[Exam Guide](https://support.offensive-security.com/#!oscp-exam-guide.md)

Practice

[Exploit Exercises](https://exploit-exercises.com/)

[OverTheWire - Wargames](https://overthewire.org/wargames/)

[Hack This Site](https://www.hackthissite.org/)

[Flare-On](http://www.flare-on.com/)

[Reverse Engineering Challenges](https://challenges.re/)

[CTF Learn](https://ctflearn.com/)

[Mystery Twister - Crypto Challenges](https://www.mysterytwisterc3.org/en/)

Buffer Overflows

[Buffer Overflow Practice](https://www.vortex.id.au/2017/05/pwkoscp-stack-buffer-overflow-practice/)

[Fuzzy Security - Windows Exploit Development](http://www.fuzzysecurity.com/tutorials.html)

[dostackbufferoverflowgood - easy to read](https://github.com/justinsteven/dostackbufferoverflowgood)

[Exploit Exercises](https://exploit-exercises.com/)

[Corelan's exploit writing tutorial](https://www.corelan.be/index.php/2009/07/19/exploit-writing-tutorial-part-1-stack-based-overflows/)

[Live Overflow's Binary Hacking Videos](https://www.youtube.com/watch?v=iyAyN3GFM7A&list=PLhixgUqwRTjxglIswKp9mpkfPNfHkzyeN)

[Introduction to 32-bit Windows Buffer Overflows](https://www.veteransec.com/blog/introduction-to-32-bit-windows-buffer-overflows)

[Getting Started with x86 Linux Buffer Overflows](https://scriptdotsh.com/index.php/2018/05/14/getting-started-with-linux-buffer-overflows-part-1-introduction/)

Binary Exploitation

[Binary Exploitation ELI5](https://medium.com/@danielabloom/binary-exploitation-eli5-part-1-9bc23855a3d8)

[Exploit Development Roadmap](https://www.reddit.com/r/ExploitDev/comments/7zdrzc/exploit_development_learning_roadmap/)

General OSCP Guides/Resources

[Real Useful OSCP Journey](https://infosecuritygeek.com/my-oscp-journey/)

[Tulpa PWK Prep](https://tulpa-security.com/2016/09/19/prep-guide-for-offsecs-pwk/)

[Tulpa PWK Prep PDF](https://tulpasecurity.files.wordpress.com/2016/09/tulpa-pwk-prep-guide1.pdf)

[Abatchy's Guide (apparently pretty good!)](https://www.abatchy.com/2017/03/how-to-prepare-for-pwkoscp-noob.html)

[Real good guide with many an info](https://www.securitysift.com/offsec-pwb-oscp/)

Infosec News / Publications

[Security Affairs](http://securityaffairs.co/wordpress/)

[The Register](https://www.theregister.co.uk/security/)

[Risky Biz](https://risky.biz/)

[Vectra](https://blog.vectra.ai/blog)

Infosec Blogs

[Nii Consulting](https://niiconsulting.com/checkmate/)

[Guido Vranken](https://guidovranken.com)

[SecJuice](https://medium.com/secjuice/)

OSCP Reviews/Writeups

~~[Process Focused Review](https://occultsec.com/2018/04/27/the-oscp-a-process-focused-review/) ~~

~~[Full marks in 90 days](https://coffeegist.com/security/my-oscp-experience/)

[Zero to OSCP in 292 days (still somewhat relevant)](https://blog.mallardlabs.com/zero-to-oscp-in-292-days-or-how-i-accidentally-the-whole-thing-part-2/)

[31-Day OSCP - with some useful info](https://scriptdotsh.com/index.php/2018/04/17/31-days-of-oscp-experience/)

Fuzzing

[Fuzzing Adobe Reader](https://kciredor.com/fuzzing-adobe-reader-for-exploitable-vulns-fun-not-profit.html)

Reverse Engineering

[Reverse Engineering x64 for Beginners](http://niiconsulting.com/checkmate/2018/04/reverse-engineering-x64-for-beginners-linux/)

[Backdoor - Reverse Engineering CTFs](https://backdoor.sdslabs.co/)

[Begin Reverse Engineering: workshop](https://www.begin.re/)

Pivoting

[The Red Teamer's Guide to Pivoting](https://artkond.com/2017/03/23/pivoting-guide/)

Github Disovered OSCP Tools/Resources

[Lots of OSCP Materials](https://gist.github.com/natesubra/5117959c660296e12d3ac5df491da395)

[Collection of things made during OSCP journey](https://github.com/ihack4falafel/OSCP)

[Notes from Study Plan](https://github.com/ferreirasc/oscp)

[Resource List - not overly thorough](https://github.com/secman-pl/oscp)

[Personal Notes for OSCP & Course](https://github.com/generaldespair/OSCP)

[Buffer Overflow Practice](https://github.com/mikaelkall/vuln)

[OSCP Cheat Sheet](https://github.com/mikaelkall/OSCP-cheat-sheet)

[Bunch of interesting 1-liners and notes](https://github.com/gajos112/OSCP)

[How to teach yourself infosec](https://github.com/thngkaiyuan/how-to-self-learn-infosec)

Non-Preinstalled Kali Tools

[Doubletap - loud/fast scanner](https://github.com/benrau87/doubletap)

[Reconnoitre - recon for OSCP](https://github.com/codingo/Reconnoitre)

[Pandora's Box - bunch of tools](https://github.com/paranoidninja/Pandoras-Box)

[SleuthQL - SQLi Discovery Tool](https://github.com/RhinoSecurityLabs/SleuthQL)

[Commix - Command Injection Exploiter](https://github.com/commixproject/commix)

Source Code Review / Analysis

[Static Analysis Tools](https://github.com/mre/awesome-static-analysis)

Malware Analysis

[Malware Analysis for Hedgehogs
(YouTube)](https://www.youtube.com/channel/UCVFXrUwuWxNlm6UNZtBLJ-A)

Misc

[Windows Kernel Exploitation](https://rootkits.xyz/blog/2017/06/kernel-setting-up/)

[Bunch of interesting tools/commands](https://github.com/adon90/pentest_compilation)

[Forensics Field Guide](https://trailofbits.github.io/ctf/forensics/)

[Bug Bounty Hunter's Methodology](https://github.com/jhaddix/tbhm)

[**Fantastic** lecture resource for learning assembly](https://www.youtube.com/watch?v=H4Z0S9ZbC0g)

[Awesome WAF bypass/command execution filter bypass](https://medium.com/secjuice/waf-evasion-techniques-718026d693d8)

CTF Resources - Pen-Test links

Webserver / http fingerprinting

An Introduction to HTTP fingerprinting
http://www.net-square.com/httprint_paper.html

Web Application finger printing
https://anantshri.info/articles/web_app_finger_printing.html

Metasploit

Scanner HTTP Auxiliary Modules
https://www.offensive-security.com/metasploit-unleashed/scanner-http-auxiliary-modules/

Creating Metasploit Payloads
https://netsec.ws/?p=331

Converting Metasploit Module to Stand Alone
https://netsec.ws/?p=262

Pen-test Cli command pages

https://jivoi.github.io/2015/07/01/pentest-tips-and-tricks/
https://jivoi.github.io/2015/08/21/pentest-tips-and-tricks-number-2/

>Privilege Escalation

Windows
Windows Privilege Escalation Methods for Pentesters
https://pentest.blog/windows-privilege-escalation-methods-for-pentesters/

Common Windows Privilege Escalation Vectors
https://www.toshellandback.com/2015/11/24/ms-priv-esc/

Linux

Basic Linux Privilege Escalation
https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/

Reach the root!
https://hackmag.com/security/reach-the-root/

Upgrading simple shells to fully interactive TTYs
https://blog.ropnop.com/upgrading-simple-shells-to-fully-interactive-ttys/

Post-Exploitation Without A TTY
http://pentestmonkey.net/blog/post-exploitation-without-a-tty

No Root Squash: NFS, no_root_squash and SUID - Basic NFS Security
http://fullyautolinux.blogspot.dk/2015/11/nfs-norootsquash-and-suid-basic-nfs.html?m=1

Escaping Linux Jail

Escape From SHELLcatraz - Breaking Out of Restricted Unix Shells
https://speakerdeck.com/knaps/escape-from-shellcatraz-breaking-out-of-restricted-unix-shells

Escaping Linux CHROOT jail
https://securitytraning.com/escaping-linux-chroot-jail/
https://www.cybrary.it/0p3n/escaping-linux-chroot-jail/

Escaping a chroot jail/1
https://filippo.io/escaping-a-chroot-jail-slash-1/

Exploit Dev

PEDA - Python Exploit Development Assistance for GDB
http://security.cs.pub.ro/hexcellents/wiki/kb/toolset/peda

Complex Calc Writeup (elf)
https://sploitfun.wordpress.com/

Simple Buffer Overflows</h3> (BOF 101)
https://netsec.ws/?p=180

Exploit writing tutorial part 1 : Stack Based Overflows
https://www.corelan.be/index.php/2009/07/19/exploit-writing-tutorial-part-1-stack-based-overflows/

Buffer Overflows and You!

(See all Vulnserver)
https://t0w3ntum.com/2016/08/05/buffer-overflows-and-you/

Vulnserver

Category: VulnServer
http://sh3llc0d3r.com/category/vulnserver/

Vulnserver – Fuzzing with Spike
http://sh3llc0d3r.com/vulnserver-fuzzing-with-spike/

Vulnserver – TRUN command buffer overflow exploit
http://sh3llc0d3r.com/vulnserver-trun-command-buffer-overflow-exploit/

Walktrough / Guides

Hackthebox reddit spoilers
https://www.reddit.com/r/hackthebox/?count=26&before=t3_6evskv

Web

Unrestricted File Upload Testing
https://www.aptive.co.uk/blog/unrestricted-file-upload-testing/

Shells

Php revere shell - Pentestmonkey (2011)
http://pentestmonkey.net/tools/web-shells/php-reverse-shell

Upgrading simple shells to fully interactive TTYs
https://blog.ropnop.com/upgrading-simple-shells-to-fully-interactive-ttys/

>Pivoting
A Red Teamer's guide to pivoting
https://artkond.com/2017/03/23/pivoting-guide/

Passive Info Web links

https://dnsdumpster.com/
https://www.yougetsignal.com/tools/web-sites-on-web-server/
https://www.whois.net/

https://builtwith.com/
https://whatcms.org/

https://github.com/PenturaLabs/Linux_Exploit_Suggester

https://github.com/GDSSecurity/Windows-Exploit-Suggester

Free Security eBooks
[![Build Status](https://travis-ci.org/Hack-with-Github/Free-Security-eBooks.svg?branch=master)](https://travis-ci.org/Hack-with-Github/Free-Security-eBooks)

A curated list of free Security and Pentesting related E-Books available on the Internet.

If you want to contribute to this list (please do), send a pull request. All contributors will be recognized and appreciated.

Disclaimer: The contributor(s) cannot be held responsible for any misuse of the data. This repository is just a collection of URLs to download eBooks for free. Download the eBooks at your own risks.

DMCA takedown cannot be possible as we are not republishing the books/infringement of code, but we are just hosting the links to 3rd party websites where these books can be downloaded. To know more on DMCA takedown policy [here](https://help.github.com/articles/dmca-takedown-policy/).

The topics include:

- [Android & iOS](#android--ios)
- [Cloud Security](#cloud-security)
- [Defensive Security](#defensive-security)
- [IoT](#iot)
- [Malware Analysis & Forensics](#malware-analysis--forensics)
- [Network Pentesting](#network-pentesting)
- [Offensive Security](#offensive-security)
- [Programming Languages](#programming-languages)
- [Reverse Engineering](#reverse-engineering)
- [SysAdmin](#sysadmin)
- [Virus Botnet and Malware](#virus-botnet-and-malware)
- [Wireless Network Pentesting](#wireless-network-pentesting)
- [Misc](#misc)

Network Pentesting

- [Wireshark Essentilals](https://github.com/cyberh3x/books/blob/master/9781783554638-WIRESHARK_ESSENTIALS.pdf)

- [Mastering Wireshark](https://github.com/cyberh3x/books/blob/master/9781783989522-MASTERING_WIRESHARK.pdf)

Defensive Security
- [Holistic Info-Sec for Web Developers - Fascicle 0](https://f0.holisticinfosecforwebdevelopers.com/)
- [Holistic Info-Sec for Web Developers - Fascicle 1](https://f1.holisticinfosecforwebdevelopers.com/)
- [OWASP Hacking Tutorials and Web App Protection](https://www.owasp.org/images/d/d0/Web_Services_Hacking_and_Hardening.pdf)

- [Threat Modeling - Designing for Security](https://news.asis.io/sites/default/files/Threat%20Modeling.pdf)

Offensive Security

- **Backtrack**
  - [Hack your Friend using Backtrack](http://hackerspace.cs.rutgers.edu/library/bt5tutorials/HackYourFriend.pdf)

- **Kali Linux**
  - [Kali Linux Revealed Book](https://kali.training/)

  - [Windows Pentesting with Kali Linux v2](https://github.com/cyberh3x/books/blob/master/9781782168492-KALI_LINUX_2_WINDOWS_PENETRATION_TESTING.pdf)

- **Hacking**
  - [Advanced SQL Injection Hacking and Guide](https://defcon.org/images/defcon-17/dc-17-presentations/defcon-17-joseph_mccray-adv_sql_injection.pdf)

  - [A Beginners Guide To Hacking Computer Systems](http://www.mediafire.com/download/dyewn6f3r3olnuw/A+Beginners+Guide+To+Hacking+Computer+Systems.zip)

  - [Blind SQL Injection Discovery & Exploitation](http://blueinfy.com/wp/blindsql.pdf)
  - [CEH – Hacking Database Secrets and Exploit](http://repo.thehackademy.net/depot_cehv6/)

  - [Ethical Hacking Complete E-book for Beginners](http://pdf.textfiles.com/security/palmer.pdf)

  - [Hackers High School 13 Complete Hacking Ebooks](http://www.mediafire.com/download/u2akquvibe6ia13/Hackers+High+School+13+Complete+Hacking+E-books.rar)

- [Hacking attacks and Examples Test](http://www.mediafire.com/download/dpysbzboord42lo/Hacking+attacks+and+Examples+Test.zip)

- [Hacking into Computer Systems](http://www.academia.edu/1153769/Hacking_into_computer_systems_-_a_beginners_guide)
- [Hackers' Secrets](http://www.onlinepot.org/security/HackersSecrets.pdf)

- **Operating Systems**
  - **Windows**
    - [Modern Windows Exploit Development](https://userscloud.com/9ifscj08wllu)

- **Web & WebApp**
  - [501 Website Hacking Secrets](http://www.mediafire.com/download/da8nhq8oh5iddae/501+Website+Hacking+Secrets.zip)
  - [Cross Site Scripting and Hacking Websites](http://www.objectif-securite.ch/research/xss_security_days.pdf)

- [Dangerous Google Hacking Database and Attacks](http://www.mediafire.com/download/s3535s2yg1w26u7/Dangerours+Google+Hacking+Database+and+Attacks.zip)

- [Hack any Website, Complete Web App Hacking](https://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Gentil/dc-11-gentil.pdf)

- [Hacking Website Database and owning systems](http://www.blackhat.com/presentations/bh-europe-07/Cerrudo/Whitepaper/bh-eu-07-cerrudo-WP-up.pdf)

- [Internet Advanced Denial of Service (DDOS) Attack](http://www.mediafire.com/download/b4jmyl022rh48c0/Internet+Advanced+Denial+of+Service+%28DDOS%29+Attack.zip)
- [Internet Security Technology and Hacking](http://www.mediafire.com/download/7tk860o8n777iqa/Internet+Security+Technology+and+Hacking.zip)

- [The Web Application Hacker's Handbook](https://leaksource.files.wordpress.com/2014/08/the-web-application-hackers-handbook.pdf)

- [Vulnerability Exploit & website Hacking for Dummies](http://www.mediafire.com/download/j8cvosmvcb4vpw9/Vulnerability+Exploitation+%26+website+Hacking+for+Dummies.rar)

- [Web App Hacking (Hackers Handbook)](http://www.mediafire.com/download/c7b18vtpc77sysi/Web+App+Hacking+%28Hackers+Handbook%29.zip)

- [XSS, Vulnerability Exploitation & Website Hacking](http://www.cis.syr.edu/~wedu/seed/Labs/Attacks_XSS/XSS.pdf)

Programming Languages
- **Python**
  - [Violent Python : A Cookbook for Hackers (2013)](https://github.com/reconSF/python/blob/master/Syngress.Violent.Python.a.Cookbook.for.Hackers.2013.pdf)

Reverse Engineering
- [Reverse Engineering Hacking and Cracking](https://media.blackhat.com/bh-dc-11/Grand/BlackHat_DC_2011_Grand-Workshop.pdf)

- [Reverse Engineering for Beginners](http://www.t-gr.com/fotis/books/re.pdf)

Virus Botnet and Malware
- [Black Book of Viruses and Hacking](http://www.mediafire.com/download/c8ilcobmyiqooyp/Black+Book+of+Viruses+and+Hacking.zip)

- [Computer Hacking & Malware Attacks for Dummies](http://www.mediafire.com/download/8derf9dueyq64i5/Computer+Viruses%2C+Hacking+and+Malware+attacks+for+Dummies.zip)

Miscellaneous:

- [Computer Hacking - Cyber Laws Harvard](https://cyber.harvard.edu/sites/cyber.law.harvard.edu/files/ComputerHacking.pdf)

- [Ethical Hacking Value and Penetration testing](https://www.certconf.org/presentations/2003/Wed/WM4.pdf)
- [Secrets of Super and Professional Hackers](http://www.mediafire.com/download/2sspb36u5gymd23/Secrets+of+Super+and+Professional+Hackers.zip)

- [Hackers High School 13Complete Hacking E-books](http://www.mediafire.com/download/u2akquvibe6ia13/Hackers+High+School+13+Complete+Hacking+E-books.rar)

- [Network Hacking and Shadows Hacking Attacks](http://www.mediafire.com/download/utp50jqd25ngw3q/Network_Hacking_and_Shadows_Hacking_Attacks.zip)