



# DAY 1

## Instructors:


Omar Santos

Joseph Mlodzianowski

# DISCLAIMER/ WARNING

---

- The information provided on this training is **for educational purposes only**. The **authors**, O'Reilly, or any other entity **is in no way responsible for any misuse of the information**.
- Some of the tools and technologies that you will learn in this training class may be illegal depending on where you reside. Please check with your local laws.
- Please practice and use all the tools that are shown in this training in a lab that is not connected to the Internet or any other network.



Do not hack your neighbor





# Pre-requisites

---

- You must be familiar with virtualization technology (i.e., Virtual Box, VMWare, etc.)
- You must be familiar with basic Linux commands, basic networking, and basic cybersecurity concepts.





Learning Path: <https://h4cker.org/learning-path>



# Hands-on Bug Hunting Active and Passive Reconnaissance and Dark Web Research

Live training by Joseph Mlodzianowski and Omar Santos

**DARKNETRECON**

<https://darknetrecon.com>

**TRAINING INFO AND COURSE SETUP**

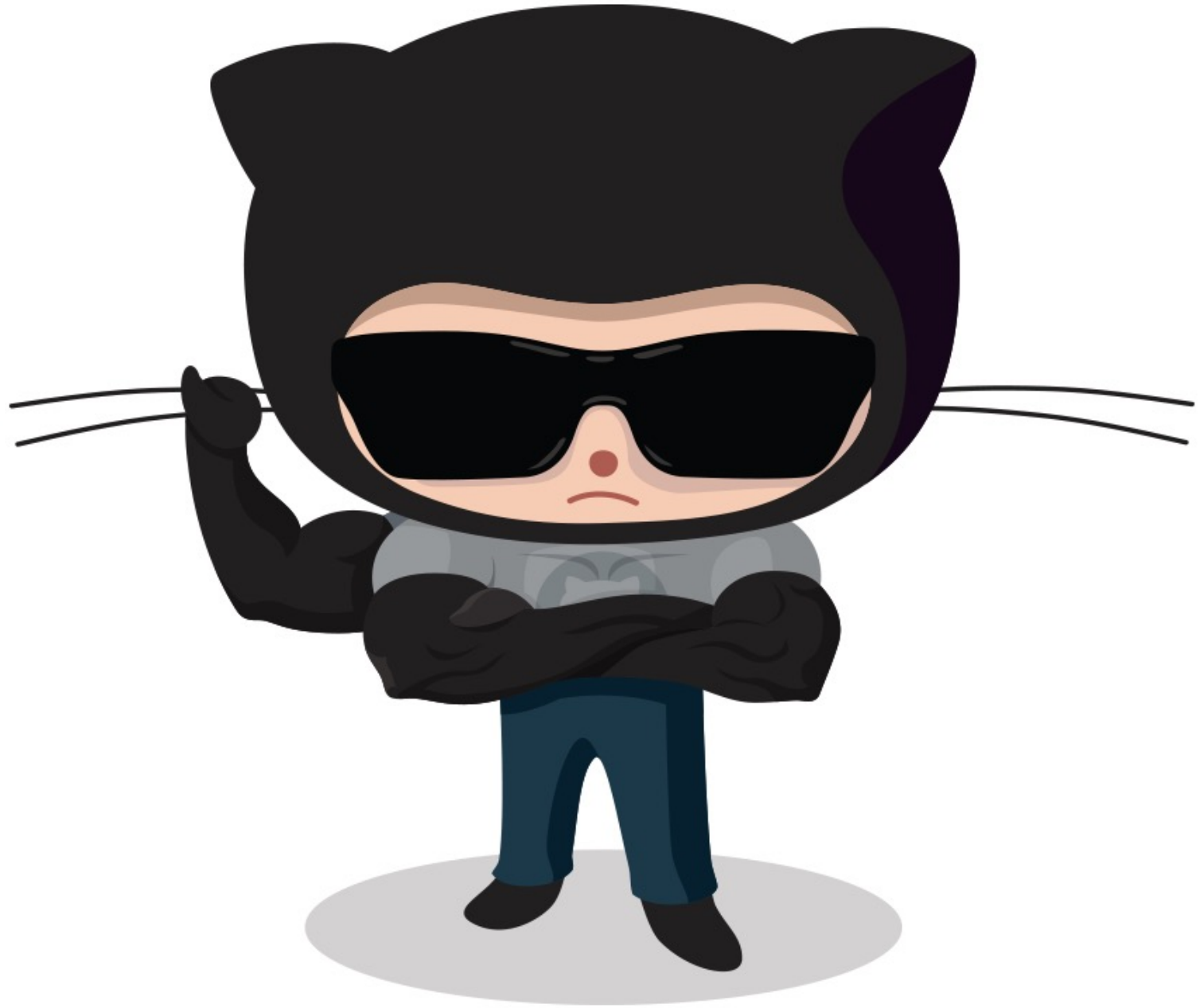


<https://websploit.org>



# GitHub Repo

<https://h4cker.org/github>





# This is an Extensive Hands-On Class

---

Most of the training will be led by demonstrations, "whiteboard sessions", and hands-on exercises.





# Lab Guide

- Each day you will get access to a lab guide.
- Most of the material is in the lab guide. The slides are here only to provide a little structure to the conversations.



# Hacker

**H4CKER.ORG**

Tons of additional Cybersecurity resources, on-demand videos (free with your subscription), and more!

# Day 1 - Agenda

- **Introduction to Passive Recon and OSINT**
- **Using Recon-NG and SpiderFoot**
- **Using Shodan and the Shodan API**
- **Using Maltego and the Harvester**
- **Introduction to Active Recon**
- **Port and Vulnerability Scanning**
- **Subdomain Enumeration**
- **Directory Enumeration**
- **Account Enumeration**



## Day 2 - Agenda

- **The Deep Web vs. the Dark Web**
- **Introduction to Tor**
- **Using the Tor Browser**
- **Using Proxies and Proxy Chains**
- **Creating Your Own VPN Server in the Cloud**
- **Staying Safe when Performing Dark Web Research**
- **Performing Dark Web Reconnaissance**



# Introduction to Passive Recon and OSINT



## What is Recon?

- Reconnaissance is always the initial step in a cyber attack.
- An attacker must first gather information about the target in order to be successful.



## Passive vs. Active Recon

- Passive:
  - You do not send any packets to the victim/target.
  - The attacker gathers information from public sources on the Internet, including but not limited to: DNS records, public records, social media, company websites, acquisitions, whois, shodan, etc.
- Active:
  - You actively probe the targeted systems and network using scanners, fuzzers, and other tools.

# What is Open Source Intelligence?

- Before compromising a victim, adversaries may search freely available technical databases for information about victims that can be used during targeting.
- Information about victims may be available in online databases and repositories, such as registrations of domains/certificates as well as public collections of network data/artifacts gathered from traffic and/or scans

attack.mitre.org/tactics/TA0043/

MITRE | ATT&CK®

MatricesTacticsTechniquesMitigationsGroupsSoftwareResourcesBlogContributeSearch

TACTICS

Enterprise

Reconnaissance

Resource Development

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Command and Control

Exfiltration

Impact

Mobile

Home > Tactics > Enterprise > Reconnaissance

Reconnaissance

The adversary is trying to gather information they can use to plan future operations.

Reconnaissance consists of techniques that involve adversaries actively or passively gathering information that can be used to support targeting. Such information may include details of the victim organization, infrastructure, or staff/personnel. This information can be leveraged by the adversary to aid in other phases of the adversary lifecycle, such as using gathered information to plan and execute Initial Access, to scope and prioritize post-compromise objectives, or to drive and lead further Reconnaissance efforts.

ID: TA0043

Created: 02 October 2020

Last Modified: 18 October 2020

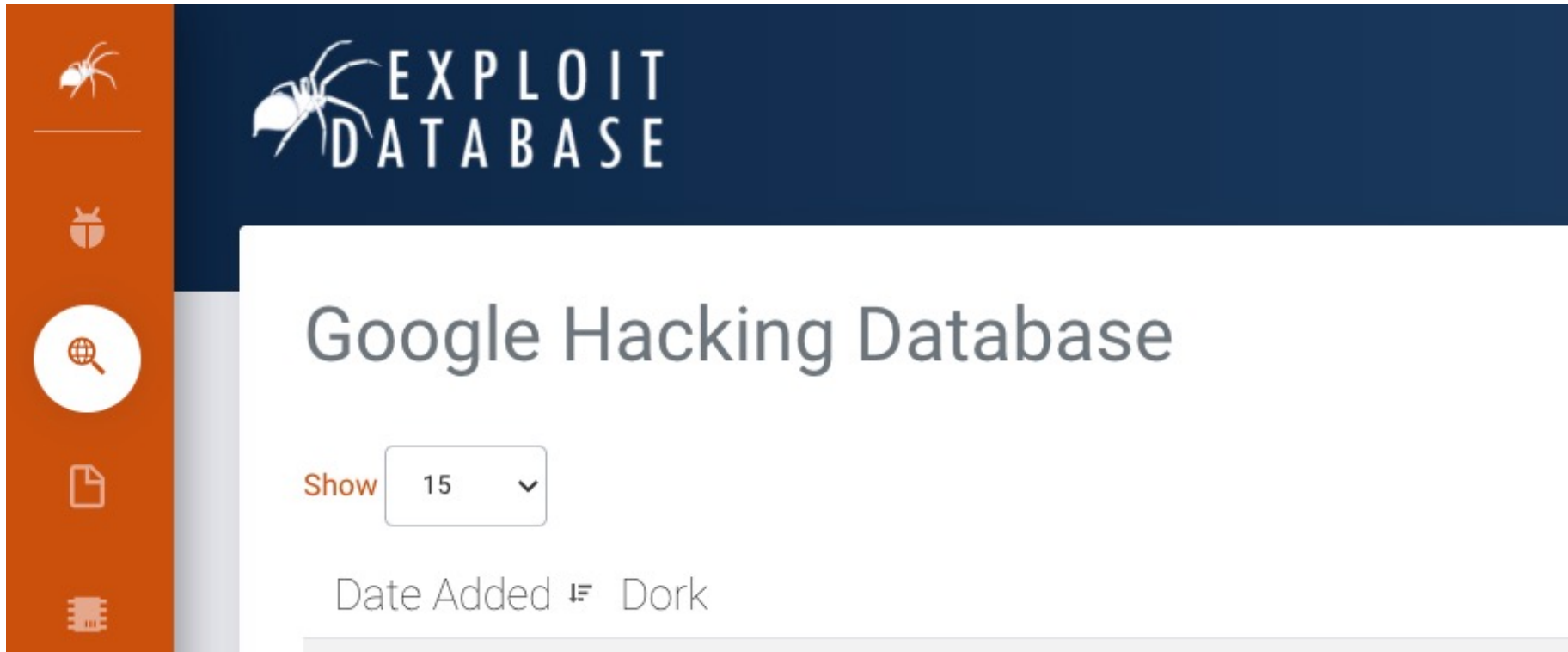
Version Permalink

Techniques: 10

ID	Name	Description
T1595	Active Scanning	Before compromising a victim, adversaries may execute active reconnaissance scans to gather information that can be used during targeting. Active scans are those where the adversary probes victim infrastructure via network traffic, as opposed to other forms of reconnaissance that do not involve direct interaction.
.001	Scanning IP Blocks	Before compromising a victim, adversaries may scan victim IP blocks to gather information that can be used during targeting. Public IP addresses may be allocated to organizations by block, or a range of sequential addresses.
.002	Vulnerability Scanning	Before compromising a victim, adversaries may scan victims for vulnerabilities that can be used during targeting. Vulnerability scans typically check if the configuration of a target host/application (ex: software and version) potentially aligns with the target of a specific exploit the adversary may seek to use.
T1592	Gather Victim Host Information	Before compromising a victim, adversaries may gather information about the victim's hosts that can be used during targeting. Information about hosts may include a variety of details, including administrative data (ex: name, assigned IP, functionality, etc.) as well as specifics regarding its configuration (ex: operating system, language, etc.).

<https://attack.mitre.org/tactics/TA0043/>

MITRE | ATT&CK®



Google Hacking Database

# Related Resources from my GitHub Repo

- OSINT:

<https://github.com/The-Art-of-Hacking/h4cker/tree/master/osint>

- Recon:

<https://github.com/The-Art-of-Hacking/h4cker/tree/master/recon>





# OSINT Tools for the Dark Web

- Ahmia Search Engine
  - [ahmia.fi](https://ahmia.fi)
  - <https://github.com/ahmia/ahmia-site>
- DarkSearch
  - <https://darksearch.io>
  - <https://github.com/thehappydinoa/DarkSearch>
- Katana:
  - <https://github.com/adnane-X-tebbaa/Katana>
- OnionSearch:
  - <https://github.com/megadose/OnionSearch>



# Tools to Obtain Information of .onion Links

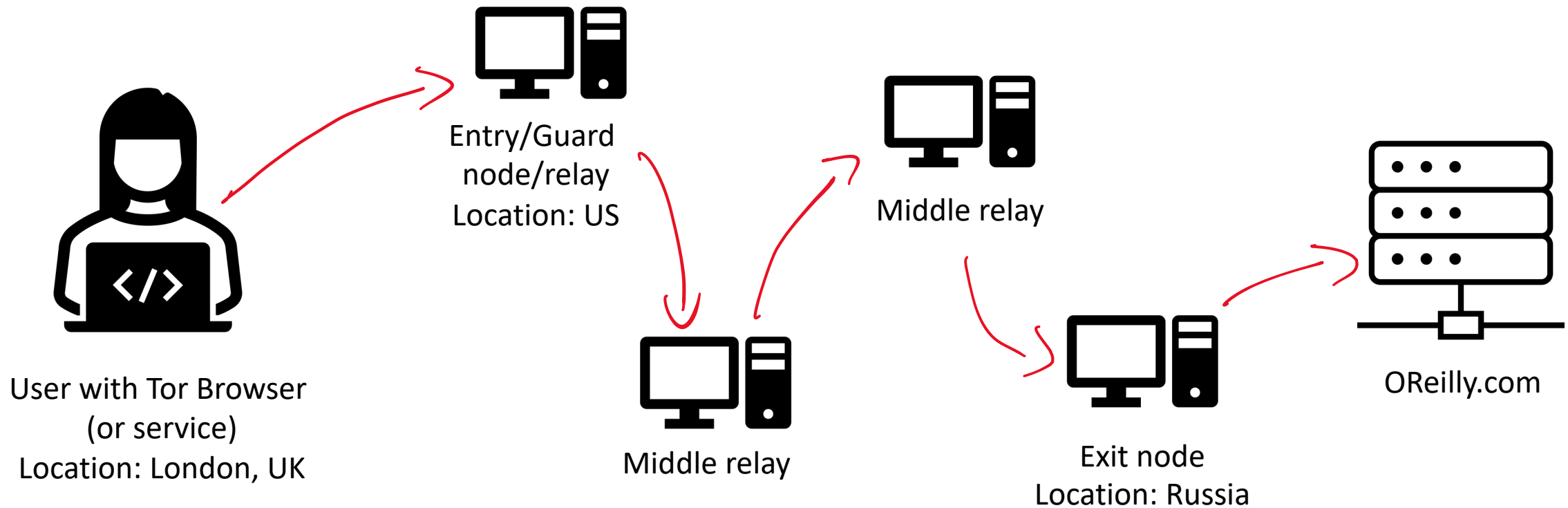
- [H-Indexer](#)
- [Hunchly](#)
- [Tor66 Fresh Onions](#)



# What is Tor?

- Technology originally created by the U.S. Navy.
- The Tor Project, Inc, became a 501(c)3 nonprofit in 2006, but the idea of "onion routing" began in the mid 1990s.
- “The goal of onion routing was to have a way to use the internet with as much privacy as possible, and the idea was to route traffic through multiple servers and encrypt it each step of the way.”
- Website: <https://www.torproject.org>

# How does Tor work?





# Tor Related Projects





# Onionoo

---

- <https://metrics.torproject.org/onionoo.html>
- “Onionoo is a web-based protocol to learn about currently running Tor relays and bridges.
- Onionoo provides the data for other applications and websites which in turn present Tor network status information to humans.
- RESTful web service
- Examples:  
<https://metrics.torproject.org/onionoo.html#examples>

← Orbot

## Log

```
Circuit (1) BUILT: pipeepgeorgia
NOTICE: Bootstrapped 90%: Establishing
Tor circuit
Set background service to FOREGROUND
Circuit (3) BUILT: pipeepgeorgia >
CatRelay > vitellius
NOTICE: Tor has successfully opened a
circuit. Looks like client functiona
is working.
NOTICE: Bootstrapped 100%: Done
Circuit (2) BUILT: pipeepgeorgia >
TangeNLV > Quintex17
Circuit (4) BUILT: pipeepgeorgia >
saisamon > tobrien
167.114.29.114 Canada (OVH SAS)
Circuit (5) BUILT: pipeepgeorgia > kbtr
> pldtor
209.133.66.214 United States (Abovenet
Communications, Inc)
199.249.223.66 United States (Mayfield
Paper Company, Inc.)
138.201.130.32 Germany (Hetzner Online
GmbH)
5.196.58.96 France (OVH SAS)
Circuit (6) BUILT: pipeepgeorgia >
madmanonsteroids > capespinymouse
Circuit (7) BUILT: pipeepgeorgia >
biotuxRelay > EecsUmichExit
138.197.129.153 Canada (Digital Ocean,
Inc.)
35.0.127.52 United States (University of
Michigan)
NOTICE: Rate limiting NEWNYM request:
```

# Orbot Proxy App

Orbot



NOTICE: Tor has successfully opened a circuit. Looks...

Global (Auto)

VPN Mode

Download 0kbps / 11MB

Upload 0kbps / 5MB

Trouble connecting? Use Bridges

Tor-Enabled Apps



<https://guardianproject.info/apps/org.torproject.android/>



# Shadow

- Network simulator and emulator
- Supports Tor and Bitcoin simulation
- <https://shadow.github.io>



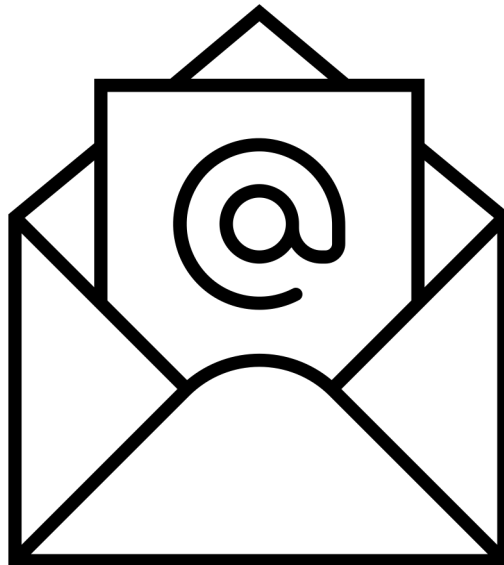
# Stem

```
[x]-[omar@websploit]-[~]  
$ sudo apt install python3-stem  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following packages will be upgraded:  
  python3-stem  
1 upgraded, 0 newly installed, 0 to remove and 2043 not upgraded.  
Need to get 310 kB of archives.  
After this operation, 0 B of additional disk space will be used.  
Get:1 https://ftp.osuosl.org/pub/parrotos/rolling/main amd64 python3-stem all 1.8.0-3 [310 kB]  
Fetched 310 kB in 2s (150 kB/s)  
Reading changelogs... Done  
(Reading database ... 430653 files and directories currently installed.)  
Preparing to unpack .../python3-stem_1.8.0-3_all.deb ...  
Unpacking python3-stem (1.8.0-3) over (1.8.0-2) ...  
Setting up python3-stem (1.8.0-3) ...  
Processing triggers for man-db (2.9.3-2) ...  
Scanning application launchers  
Removing duplicate launchers from Debian  
Launchers are updated  
[omar@websploit]-[~]  
$
```

- Python controller library for Tor
- <https://stem.torproject.org>
- Easy install:  
**sudo apt-get install python3-stem**

# TorBirdy

TorBirdy is an extension for [Mozilla Thunderbird](#) that configures it to make connections over the Tor network.





# txtorcon

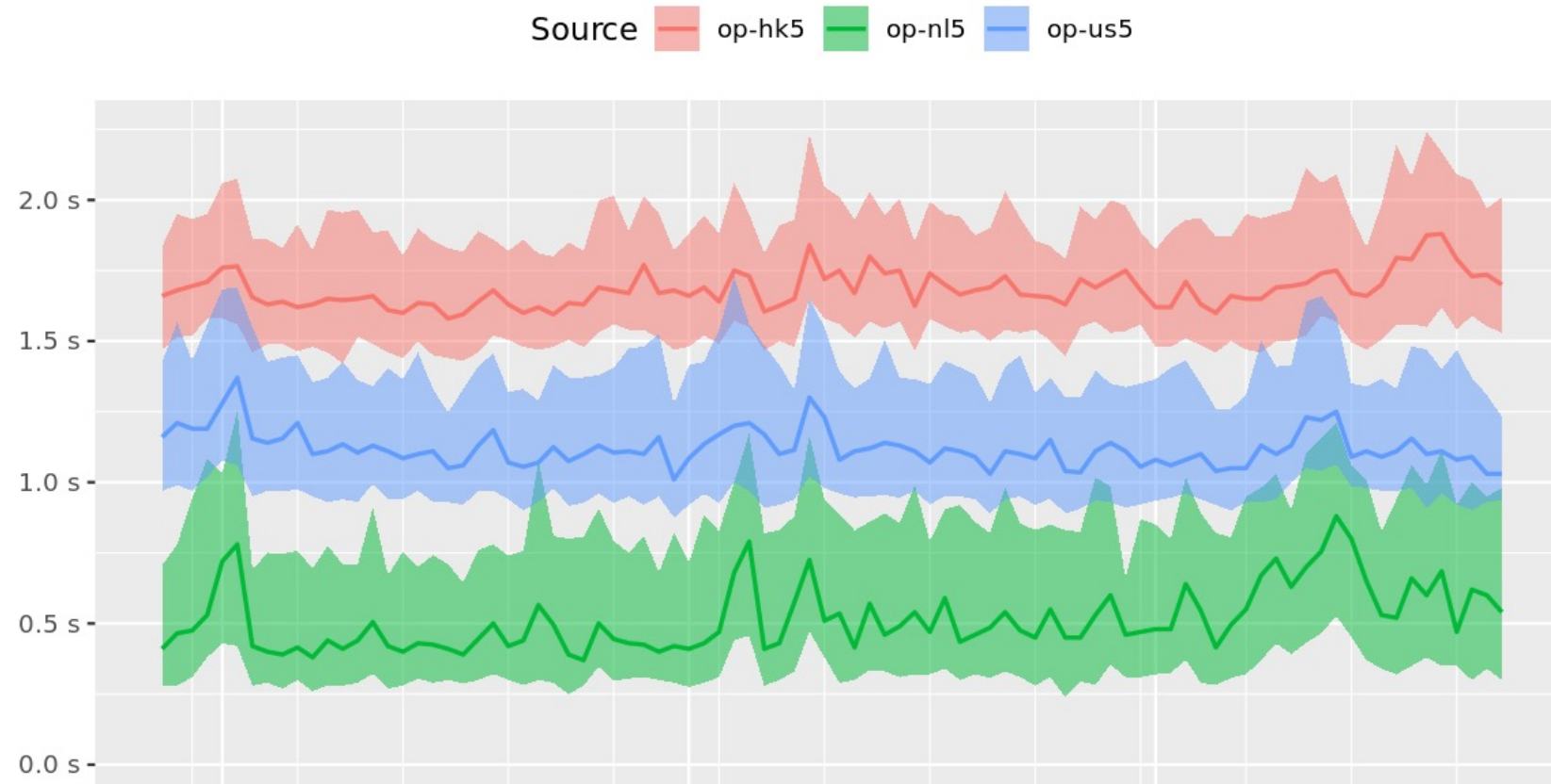
txtorcon is an implementation of the [control-spec](#) for [Tor](#) using the [Twisted](#) networking library for [Python](#) (*supports Py2, PyPy and Py3*).



<https://txtorcon.readthedocs.io/en/latest/>



## Time to complete 50 KiB request to public server



- <https://metrics.torproject.org>

arm - odin (Linux 2.6.28-18-generic) Tor 0.2.1.19 (unknown)  
caerSidi - 76.104.132.98:9001, Control Port (password): 9051  
flags: **Fast**, **HSDir**, **Named**, **Running**, **Stable**, **Valid**

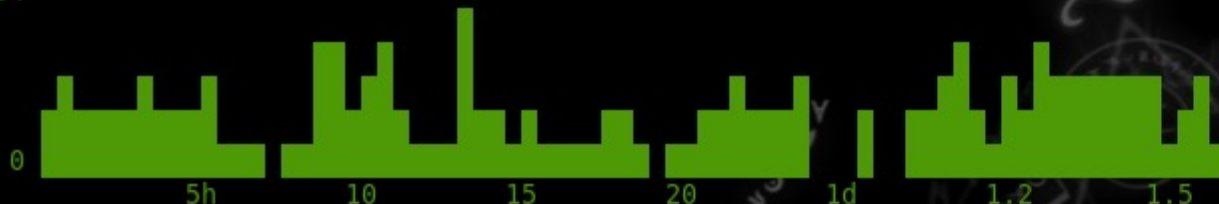
cpu: 0.6% mem: 49 MB (1.2%) pid: 4714 uptime: 10-22:26:36  
fingerprint: A7569A83B5706AB1B1A9CB52EFF7D2D32E4553EB  
exit policy: **reject** \*:\*

page 1 / 3 - q: quit, p: pause, h: page help

Bandwidth (cap: 40 KB, burst: 100 KB):

Downloaded (586 bytes/sec - avg: 13.2 KB/sec, total: 11.8 GB):

34



Uploaded (586 bytes/sec - avg: 13.3 KB/sec, total: 11.9 GB):

34



Accounting (awake)

16 GB / 30 GB

Time to reset: 150:10:02

16 GB / 30 GB

# Tor Nyx

<https://nyx.torproject.org>

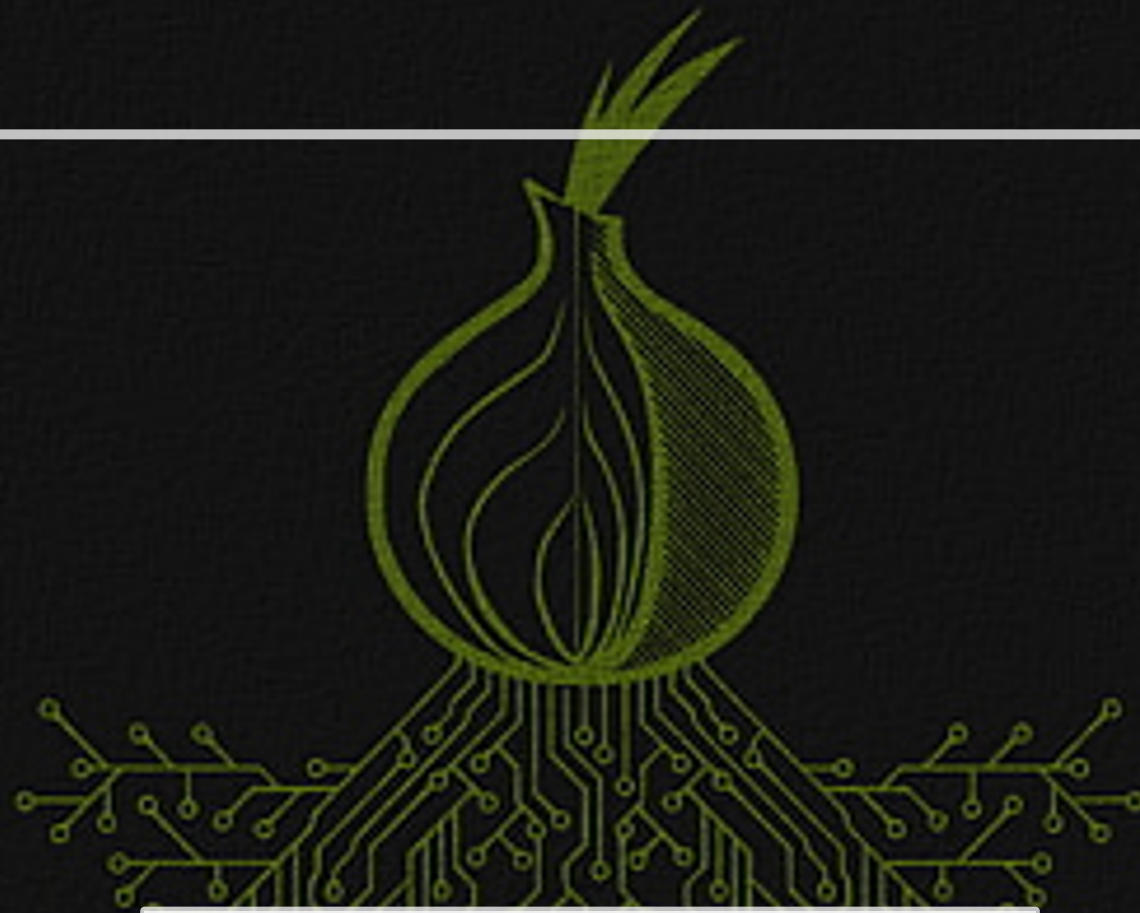
```
18:49:55 [BW] READ: 0, WRITTEN: 1758
18:49:54 [BW] READ: 1172, WRITTEN: 0
18:49:53 [BW] READ: 0, WRITTEN: 0
18:49:52 [INFO] router_pick_published_address(): Could not determine our address locally. Checking if directory headers provide any hints.
18:49:52 [INFO] resolve_my_address(): Address 'odin' resolves to private IP address '127.0.1.1'. Tor servers that use the default DirServers must have public IP addresses.
18:49:52 [INFO] resolve_my_address(): Interface IP address '192.168.1.20' is a private address too. Ignoring.
18:49:52 [INFO] resolve_my_address(): Guessed local hostname 'odin' resolves to a private IP address (127.0.1.1). Trying something else.
18:49:52 [BW] READ: 586, WRITTEN: 0
18:49:51 [BW] READ: 1172, WRITTEN: 1758
18:49:51 [INFO] circuit_n_conn_done(): or_conn failed. Closing circ.
18:49:50 [BW] READ: 1172, WRITTEN: 1172
18:49:49 [BW] READ: 1758, WRITTEN: 1758
18:49:48 [INFO] run_connection_housekeeping(): Expiring non-used OR connection to fd 104 (213.79.103.146:443) [Not in clique mode].
18:49:48 [BW] READ: 1172, WRITTEN: 2930
18:49:47 [BW] READ: 586, WRITTEN: 0
18:49:47 [INFO] resolve_my_address(): Could not determine our address locally. Checking if directory headers provide any hints.
```

# Tails



<https://tails.boum.org>





What are .onion sites?  
How can I create one?



```
## The port on which Tor will listen for local connections from Tor
## controller applications, as documented in control-spec.txt.
#ControlPort 9051
## If you enable the controlport, be sure to enable one of these
## authentication methods, to prevent attackers from accessing it.
#HashedControlPassword 16:872860B76453A77D60CA2BB8C1A7042072093276A3D701AD684053EC4C
#CookieAuthentication 1
```

```
##### This section is just for location-hidden services #####
```

```
# Once you have a configured hidden service, you can link it to the
# contents of the file ".../hidden_service/hostname" for the address
# to tell people.
##
## HiddenServicePort x y:z says to redirect requests to the
## address y:z.
```

```
HiddenServiceDir /var/lib/tor/hidden_service/
HiddenServicePort 80 127.0.0.1:1337
```

```
#HiddenServiceDir /var/lib/tor/other_hidden_service/
#HiddenServicePort 80 127.0.0.1:80
#HiddenServicePort 22 127.0.0.1:22
```

```
##### This section is just for relays #####
#
## See https://www.torproject.org/docs/tor-doc-relay for details.
```

# Tools to scan .onion links

- [Onioff](#)
- [Onion-nmap](#)
- [Onionscan](#)

<https://github.com/The-Art-of-Hacking/h4cker/blob/master/osint/README.md#dark-web-osint-tools>



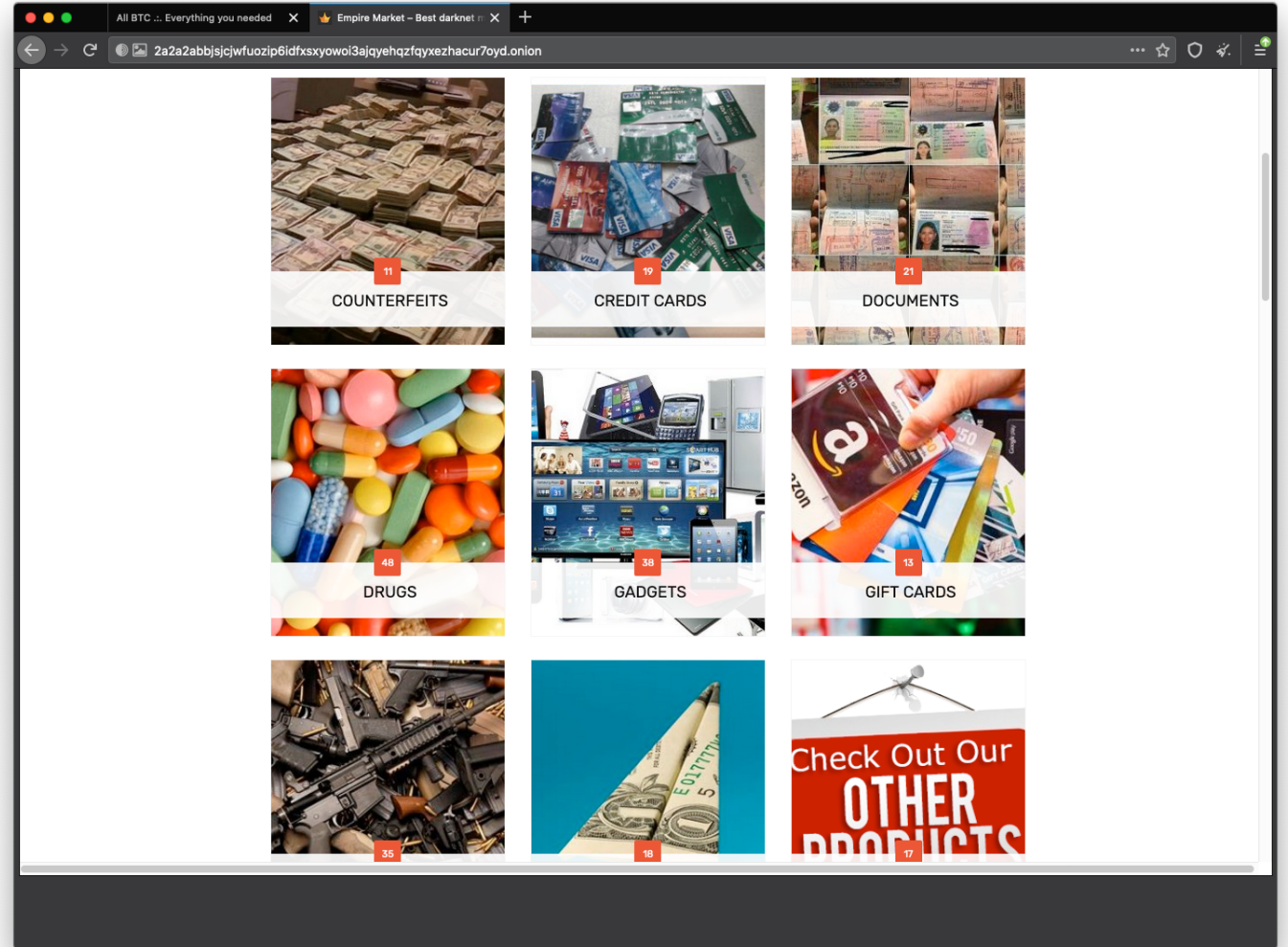
# Tools to Crawl Dark Web Data

- [TorBot](#)
- [TorCrawl](#)
- [OnionIngestor](#)

<https://github.com/The-Art-of-Hacking/h4cker/blob/master/osint/README.md#dark-web-osint-tools>



BE SUPER  
CAREFUL!





# Katana-DS

- Katana-ds (ds for dork\_scanner) is a simple python tool that automates Google Hacking/Dorking and supports Tor. It becomes a more powerful in combination with [GHDB](https://github.com/adnane-X-tebbaa/GHDB)



<https://github.com/adnane-X-tebbaa/Katana>

# Katana-DS Demo

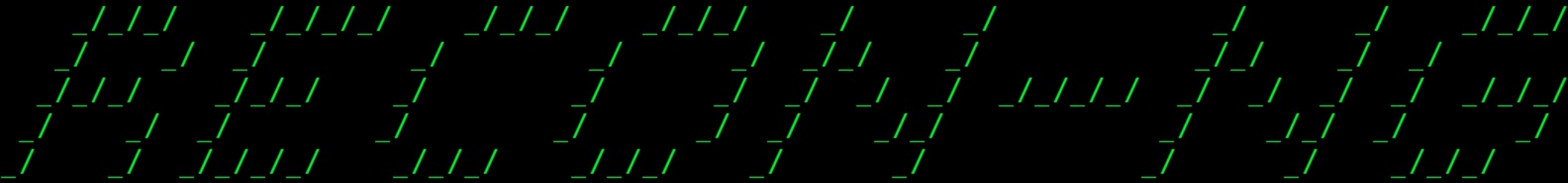
```

[+] Found > https://pastebin.com/SmUzJx19
[+] Found > https://pastebin.com/XfYZS1Rv
[+] Found > https://pastebin.com/5FXrG4tr
[+] Found > https://pastebin.com/Acq692xj
[+] Found > https://pastebin.com/gTi4S3Zi
[+] Found > https://pastebin.com/wn5j3CgB
[+] Found > https://pastebin.com/2LymS60C
[+] Found > https://pastebin.com/uMaCJSwQ
[+] Found > https://pastebin.com/DUEFwCG0

```

# Using Recon-NG and SpiderFoot

#recon-ng  
[\*] Version check disabled.



Sponsored by...



BLACK HILLS  
www.blackhillinfosec.com



www.practisec.com

[recon-ng v5.1.1, Tim Tomes (@lanmaster53)]

[\*] No modules enabled/installed.

[recon-ng][default] >

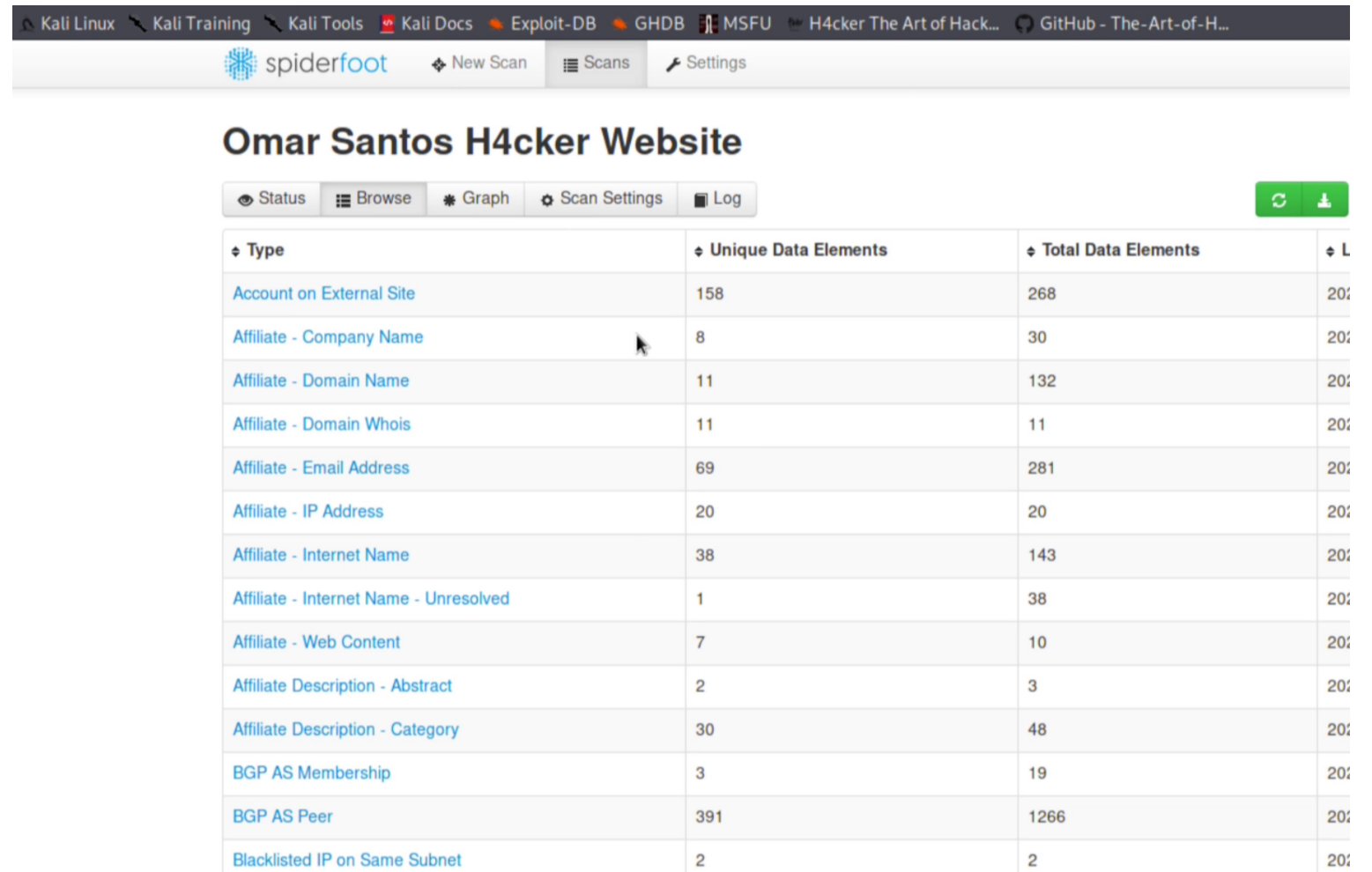


# Complete Exercise 1: Recon-NG

We will do a demo/walkthrough after the break...  
Everything is documented in your Lab Guide!



# SpiderFoot



The screenshot displays the SpiderFoot web interface. At the top, a navigation bar includes links to Kali Linux, Kali Training, Kali Tools, Kali Docs, Exploit-DB, GHDB, MSFU, H4cker The Art of Hack..., and GitHub - The-Art-of-H... Below this, the SpiderFoot logo and navigation tabs (New Scan, Scans, Settings) are visible. The main heading is 'Omar Santos H4cker Website'. Below the heading is a sub-navigation bar with tabs: Status, Browse, Graph, Scan Settings, and Log. To the right of these tabs are two green buttons: a refresh button and a download button. The main content area is a table with four columns: Type, Unique Data Elements, Total Data Elements, and a partially visible column labeled 'L'. The table lists various data types and their corresponding counts.

Type	Unique Data Elements	Total Data Elements	L
Account on External Site	158	268	20:
Affiliate - Company Name	8	30	20:
Affiliate - Domain Name	11	132	20:
Affiliate - Domain Whois	11	11	20:
Affiliate - Email Address	69	281	20:
Affiliate - IP Address	20	20	20:
Affiliate - Internet Name	38	143	20:
Affiliate - Internet Name - Unresolved	1	38	20:
Affiliate - Web Content	7	10	20:
Affiliate Description - Abstract	2	3	20:
Affiliate Description - Category	30	48	20:
BGP AS Membership	3	19	20:
BGP AS Peer	391	1266	20:
Blacklisted IP on Same Subnet	2	2	20:

# Complete Exercise 2: SpiderFoot

We will do a demo/walkthrough after the break...  
Everything is documented in your Lab Guide!



# Sublister

```
exploit)-[~/Sublister  
list3r.py -v -d h4cker.org
```

```
Sublister
```

```
# Coded By Ahmed Aboul-Ela - @at
```

```
g subdomains now for h4cker.org  
is enabled, will show the subdomains  
now in Baidu..  
now in Yahoo..  
now in Google..  
now in Bing..  
now in Ask..  
now in Netcraft..  
now in DNSdumpster..  
now in Virustotal..  
now in ThreatCrowd..  
now in SSL Certificates..  
now in PassiveDNS..  
ustotal probably now is blockin  
.h4cker.org  
h4cker.org  
t.h4cker.org  
er.org  
ker.org  
.h4cker.org  
o.h4cker.org
```



# Complete Exercise 3: Sublister

We will do a demo/walkthrough after the break...  
Everything is documented in your Lab Guide!





# Using Shodan and the Shodan API



# The search engine for the Web

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account

Getting Started



## Explore the Internet of Things

Use Shodan to discover what's connected to the Internet.



## See the Big Picture

Websites are just one part of the Internet. There are power plants, cameras, and much more that can be found with Shodan.

# Shodan

<https://shodan.io>



# The Shodan API



# Using Maltego and TheHarvester

# Initial Activation

### Configure Maltego

#### STEPS

- License Agreement
- Login
- Login Result
- Install Transforms
- Help Improve Maltego
- Web Browser Options
- Privacy Mode Options
- Ready


LOGIN: Please log in to use the free online version of Maltego.

Enter your details below to log in to the Maltego Community Server  
Or if you have not done so yet, [register here](#)

Login

\* Email Address

Password



\* Solve captcha

< Back

Next >

Finish

Cancel


### Product Selection

Please select how you want to use Maltego.

Please choose how you want to use Maltego:

Compare Products

Activate without Internet




Maltego One

Activate with key

Purchase

Maltego One is the new unified solution to access and activate Maltego plans for Professionals and Enterprises.




Maltego XL

Activate with key

Purchase

Maltego eXtra Large is Paterva's premium solution to visualise large data sets and allows for more than 10 000 entities in a single graph.




Maltego Classic

Activate with key

Purchase


Maltego Classic is a commercial version of Maltego which allows users to visualize up to 10 000 entities in a graph.



Maltego CE (Free)

Run

In Maltego CE (Community Edition) the community transforms will be installed and can be run to generate graphs, but the features are limited and the resulting graphs may not be used for commercial purposes.



Maltego CaseFile (Free)

Run

In Maltego CaseFile graphs can only be created manually, no transforms may be run. More types of entities will be installed and the resulting graphs may be used for commercial purposes.

<https://docs.maltego.com/support/solutions/articles/15000008715-initial-activation>

# Maltego Concepts and Glossary of Terms

- **Entity**
  - An Entity is a piece of information shown as a node on the graph. Different Entity types are used to differentiate between the different pieces of information that can be represented in Maltego.
  - Entities can be anything from a DNS name, Person name, Phone number, etc. The Maltego Client comes with about 20 Entities targeted for use in online investigations, however, you can create your own custom Entities.
- **Transform**
  - A Transform is a piece of code that searches for information related to an Entity on the graph. Transforms allow you to query an API or database to show related info on the graph.
  - The idea is that we are "transforming" one type of information into another type. For example we could have the website "[www.maltego.com](http://www.maltego.com)" and transform it into the IP address "104.248.60.43".
  - By default Maltego has Transforms that can query information from data sources like DNS servers, search engines, social networks, WHOIS information, etc.
- **Machine**
  - Machines are the Maltego equivalent of macros. Machines allow you to chain together multiple Transforms, filters and actions in order to automate common and tedious tasks.
- **Hub Item**
  - Transforms and the Entity types that they query need to be stored on a server that can be accessed by the Maltego Client.
  - Hub items allow Maltego users to install combinations of Transforms, Entities and Machines from a server. By default, Maltego installs the Hub item called **Standard Transforms** which contains the Transforms, Entities and Machines that are developed and maintained by the developers of Maltego.
  - Additional Hub items can be installed to get 3rd party functionality built by the community.

# Transform Hub

**Maltego Community Edition 4.2.12**

**Maltego Transform Hub**  
Maltego Community Edition - Not licensed

[REFRESH] [UPDATE]  
58 Hub items total | 1 Hub items installed (159 Transforms)

**FILTER** [RESET]

**Data Categories**

- ☐ ALL
- ☐ Blockchain
- ☐ Breaches and Leaks
- ☐ Company Data
- ☐ Cybersecurity
- ☐ Deep and Dark Web
- ☐ Financial Data
- ☐ Geospatial
- ☐ Image Data
- ☐ Infrastructure
- ☐ Malware
- ☐ NLP
- ☐ Person of Interest
- ☐ Phishing
- ☐ Social Media
- ☐ Threat Intelligence
- ☐ Vulnerabilities
- ☐ Web Content

**Pricing**

- ☐ ALL
- ☐ Bring your own key
- ☐ Data bundle
- ☐ Free
- ☐ Free trial
- ☐ Paid connector

**Useful for Teams**

- ☐ ALL
- ☐ Anti-terrorism
- ☐ CERT
- ☐ Compliance
- ☐ Cryptocurrency Fraud
- ☐ Cyber and Digital Forensics
- ☐ Cybercrime
- ☐ Financial Crime
- ☐ Fraud Investigations
- ☐ Incident Response
- ☐ Investigative Journalists
- ☐ KYC and Corporate Investigations
- ☐ Procurement
- ☐ Red Team / Pentesters
- ☐ SOC
- ☐ Trust and Safety

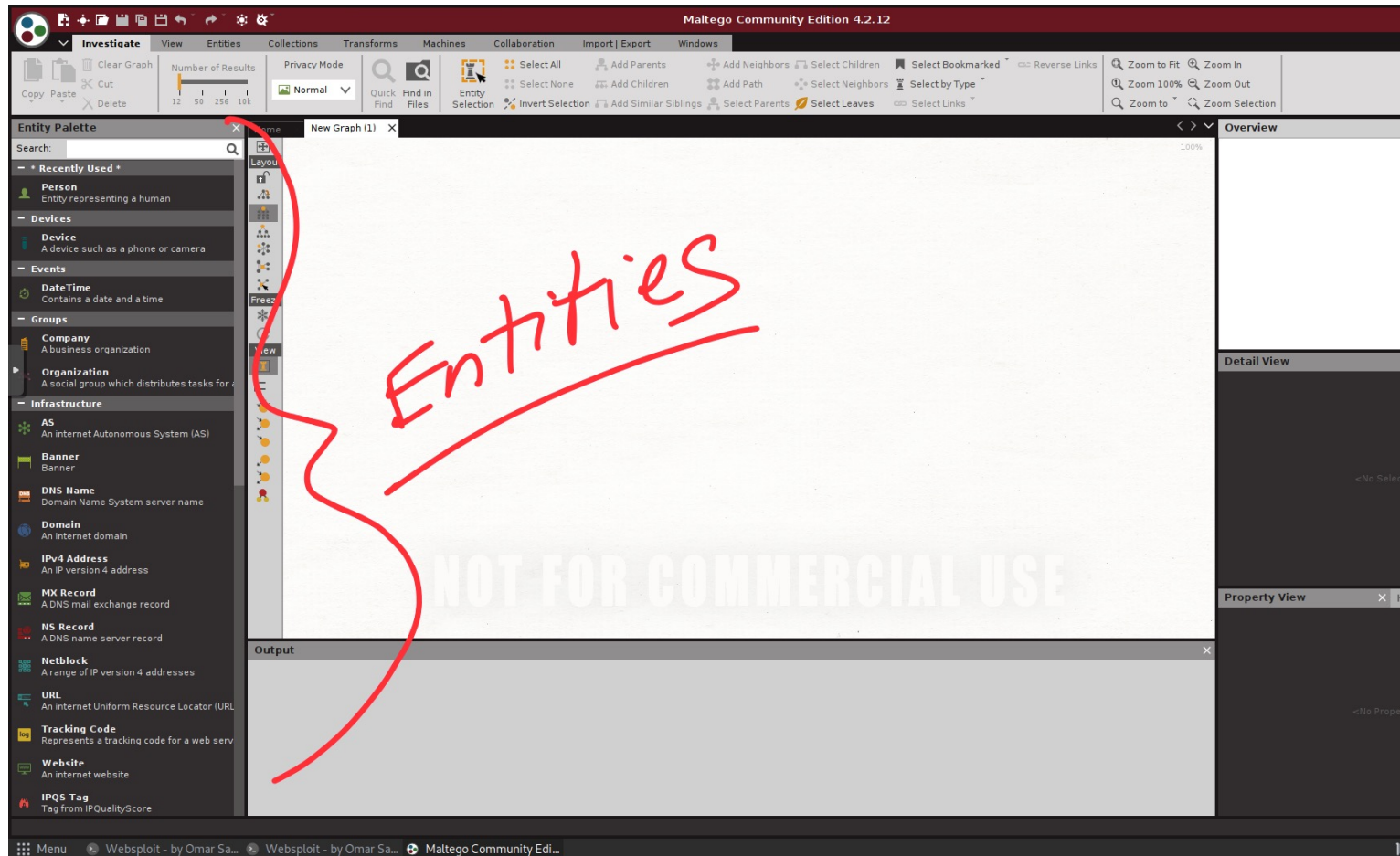
**TRANSFORM HUB PARTNERS** 58/58 shown

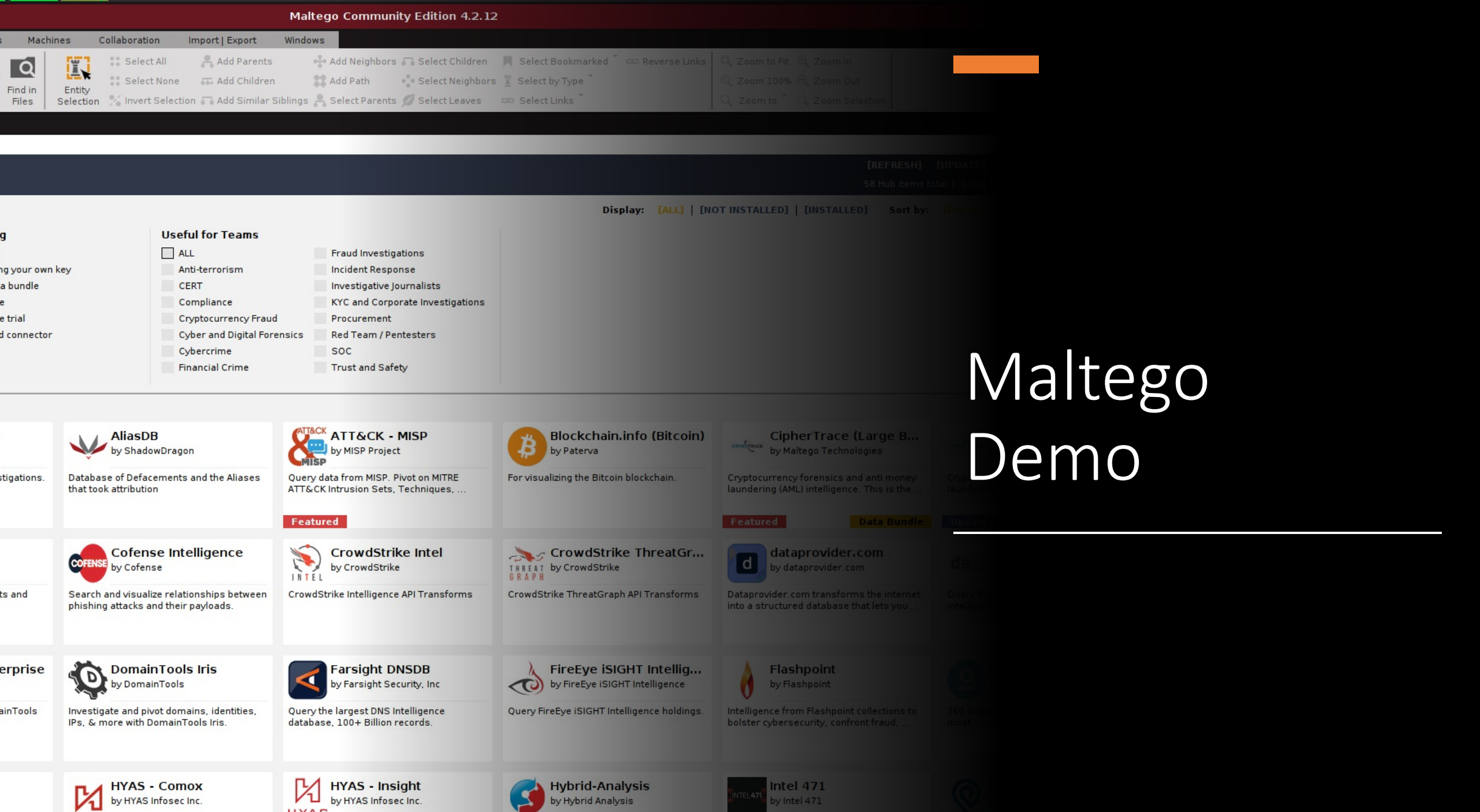
- Standard Transforms ...** by Maltego Technologies  
Free Standard OSINT Transforms  
**New**
- CaseFile Entities** by Paterva  
Useful entities for modeling investigations.
- AliasDB** by ShadowDragon  
Database of Defacements and the Aliases that took attribution
- ATT&CK - MISP** by MISP Project  
Query data from MISP. Pivot on MITRE ATT&CK Intrusion Sets, Techniques, ...  
**Featured**
- Blockchain.info (Bitcoin)** by Paterva  
For visualizing the Bitcoin blockchain.
- CipherTrace (Large B...)** by Maltego Technologies  
Cryptocurrency forensics and anti money laundering (AML) intelligence. This is the ...  
**Featured** **Data Bundle**
- CipherTrace** by Maltego Technologies  
CipherTrace provides powerful and easy-to-use cryptocurrency tracing for investigators and ...  
[DETAILS] [INSTALL]
- Cisco Threat Grid** by Cisco Threat Grid  
Query Threat Grid's database of threat intelligence.
- Clearbit** by Christian Heinrich  
Enrich sign-ups, identify prospects and gain customer insights
- Cofense Intelligence** by Cofense  
Search and visualize relationships between phishing attacks and their payloads.
- CrowdStrike Intel** by CrowdStrike  
CrowdStrike Intelligence API Transforms
- CrowdStrike ThreatGr...** by CrowdStrike  
CrowdStrike ThreatGraph API Transforms
- dataprovider.com** by dataprovider.com  
Dataprovider.com transforms the internet into a structured database that lets you ...
- Digital Shadows** by Digital Shadows  
Query the Digital Shadows cyber threat intelligence database.
- Discogs** by Maltego Technologies  
Visualize your favorite Artists using Discogs!  
**New**
- DomainTools Enterprise** by DomainTools  
Investigate cybercrime with DomainTools historic and reverse datasets.
- DomainTools Iris** by DomainTools  
Investigate and pivot domains, identities, IPs, & more with DomainTools Iris.
- Farsight DNSDB** by Farsight Security, Inc.  
Query the largest DNS Intelligence database, 100+ Billion records.
- FireEye ISIGHT Intellig...** by FireEye ISIGHT Intelligence  
Query FireEye ISIGHT intelligence holdings.
- Flashpoint** by Flashpoint  
Intelligence from Flashpoint collections to bolster cybersecurity, confront fraud, ...
- FullContact** by Christian Heinrich  
360 insights into the people who matter most.
- Have I Been Pwned?** by Christian Heinrich
- Host.io** by Christian Heinrich
- HYAS - Comox** by HYAS Infosec Inc.
- HYAS - Insight** by HYAS Infosec Inc.
- Hybrid-Analysis** by Hybrid Analysis
- Intel 471** by Intel 471
- IPInfo** by Christian Heinrich

Menu | Websploit - by Omar Sa... | Websploit - by Omar Sa... | Maltego Community Edi...



# Entities







# Looking for Names and Usernames


```
[X]-[root@parrot]-[/WhatsMyName]
#python3 web_accounts_list_checker.py -u johndoe
- 286 sites found in file.
> Looking up https://www.7cups.com/@johndoe
> Looking up https://learn.acloud.guru/profile/johndoe
> Looking up https://asciinema.org/~johndoe
> Looking up https://audiojungle.net/user/johndoe
> Looking up https://www.biggerpockets.com/users/johndoe
> Looking up https://www.bookcrossing.com/mybookshelf/johndoe
> Looking up https://www.buymeacoffee.com/johndoe
> Looking up https://www.championat.com/user/johndoe/
> Looking up https://community.cloudflare.com/u/johndoe
> Looking up https://www.cnet.com/profiles/johndoe/
> Looking up https://www.coroflot.com/johndoe
> Looking up https://www.codewars.com/users/johndoe
> Looking up https://coderwall.com/johndoe/
> Looking up https://johndoe.crevado.com/
> Looking up https://dating.ru/johndoe/
> Looking up https://www.designspiration.com/johndoe/
> Looking up https://dev.to/johndoe
> Looking up https://ello.co/johndoe
> Looking up https://www.eyem.com/u/johndoe
> Looking up https://fancy.com/johndoe
> Looking up https://www.gamepedia.com/members/johndoe
```




# Public Financial Transactions!!

← → ↺ 🏠 venmo.com/Lin [redacted]

**venmo** [Sign Up](#) [Log In](#)




Lir [redacted] paid Jamie [redacted]  
**Sweatshirt**  
4 hours ago - Comments (0)



Lir [redacted] paid Kayl [redacted]  
**Thank you!!**  
on Wednesday at 09:47PM - Comments (0)




Lir [redacted] paid Ja [redacted]  
**Thank you!**  
on February 6, 2021 at 07:52PM - Comments (0)



Lir [redacted] paid Eli [redacted]  
**Thank you!!**  
on February 3, 2021 at 07:18PM - Comments (0)



Pe [redacted] paid Lind [redacted]  
**Aspen school**  
on January 29, 2021 at 07:28PM - Comments (0)



Lir [redacted]  
Pr [redacted]  
Venmoing since July 2015.

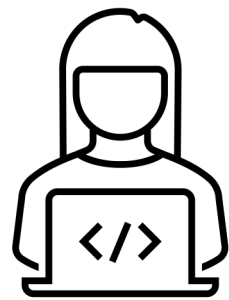
Join Lir [redacted] on Venmo

# Introduction to Active Recon



# Port and Vulnerability Scanning

# Port Scanning



Scanner



Victim/Target



# Port Scanning vs. Vulnerability Scanning



# Vulnerability Scanning Tools



[https://owasp.org/www-community/Vulnerability Scanning Tools](https://owasp.org/www-community/Vulnerability_Scanning_Tools)

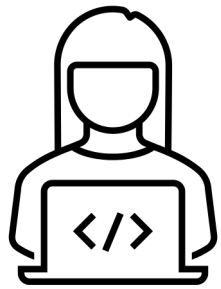
# Authenticated vs. Non-Authenticated Scans

# Nmap Cheat Sheet

<https://h4cker.org/nmap>



# What is Fuzzing?



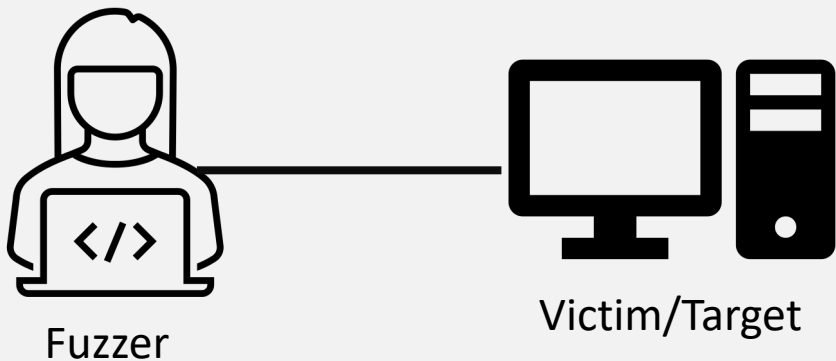
Fuzzer



Target/Victim



# Fuzzing Techniques



- **Mutation-Based:** craft a sample data format to create new test data. This is a very simple and straightforward approach. It starts with valid samples of protocol and keeps mangling every byte or file.
- **Generation-Based:** define new data based on the input of the model. It starts generating input from scratch based on the specification.
- **Protocol-based:** the fuzzer has detailed knowledge of protocol format being tested. It involves writing an array of the specification into the tool then by using model-based test generation technique go through the specification and add irregularity in the data contents, sequence, etc. This is also known as syntax testing, grammar testing, robustness testing, etc. Fuzzer can generate test cases from an existing one, or they can use valid or invalid inputs.

# Examples of Fuzzers

[https://github.com/The-Art-of-Hacking/h4cker/tree/master/fuzzing\\_resources](https://github.com/The-Art-of-Hacking/h4cker/tree/master/fuzzing_resources)



# Directory Enumeration



# Web Hacking "Fuzzing"?

```
root@websploit:~# ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://127.0.0.1:8888/FUZZ -c -v
```

The path to the wordlist

The URL of the web app

Put the FUZZ  
keyword wherever  
you want to fuzz

-c = colored output  
-v = verbose

# Gobuster

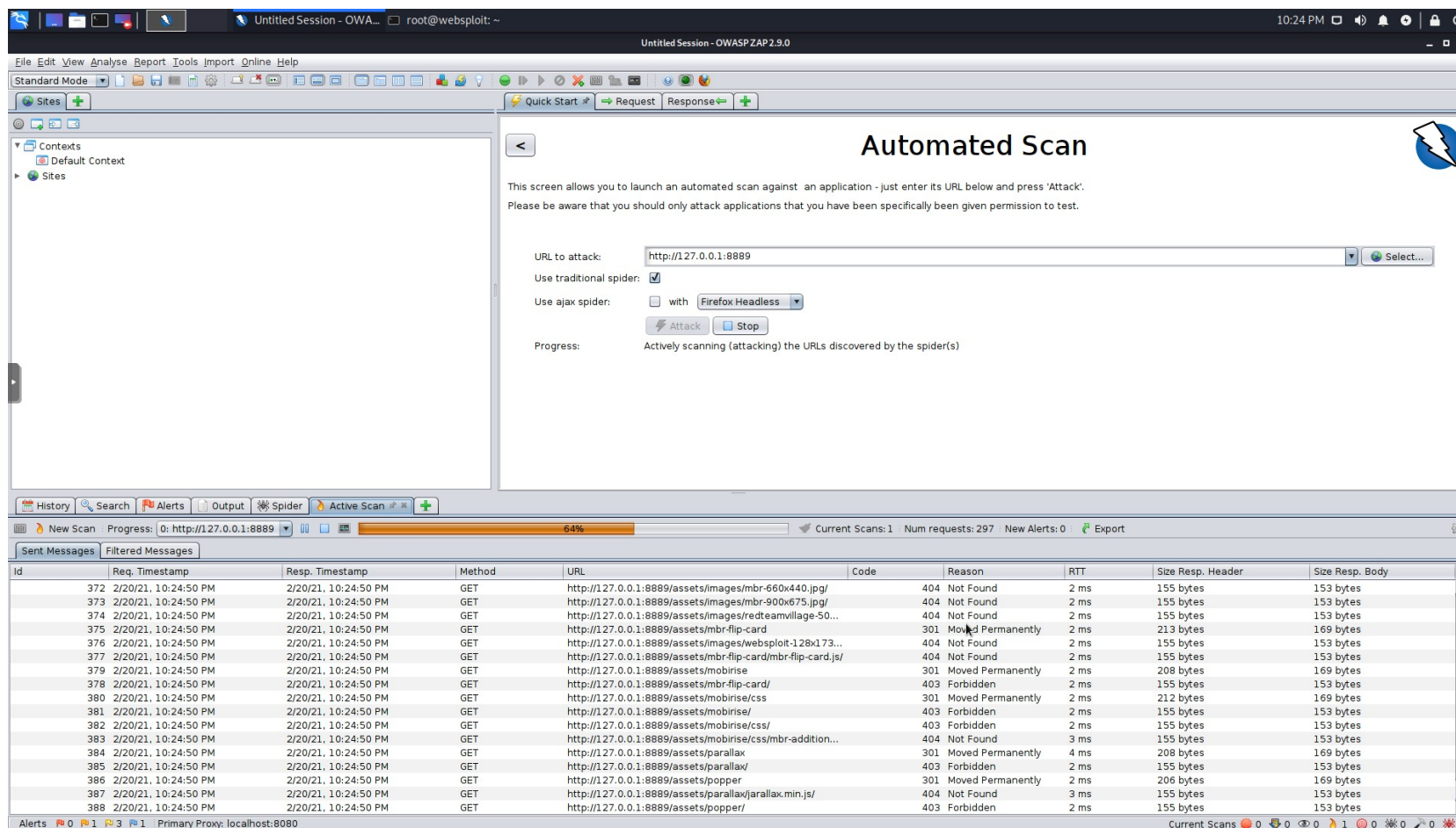
```
(root@websploit) - [~]
# gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://127.0.0.1:8889
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://127.0.0.1:8889
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:    gobuster/3.0.1
[+] Timeout:      10s
=====
2021/02/20 22:22:36 Starting gobuster
=====
/s (Status: 301)
/admin (Status: 301)
/assets (Status: 301)
/wp-login (Status: 301)
/wp-admin (Status: 301)
```

# Nikto

```
(root@webexploit) - [~]  
# nikto -h http://127.0.0.1:8889  
- Nikto v2.1.6  
-----  
+ Target IP: 127.0.0.1  
+ Target Hostname: 127.0.0.1  
+ Target Port: 8889  
+ Start Time: 2021-02-20 22:23:43 (GMT-5)  
-----  
+ Server: nginx/1.17.2  
+ The anti-clickjacking X-Frame-Options header is not present.  
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS  
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type  
+ No CGI Directories found (use '-C all' to force check all possible dirs)  
+ OSVDB-3092: /admin/: This might be interesting...  
+ /admin/index.html: Admin login page/section found.  
+ /wp-admin/: Admin login page/section found.  
+ /wp-login/: Admin login page/section found.  
+ 7892 requests: 0 error(s) and 7 item(s) reported on remote host  
+ End Time: 2021-02-20 22:23:52 (GMT-5) (9 seconds)  
-----  
+ 1 host(s) tested
```

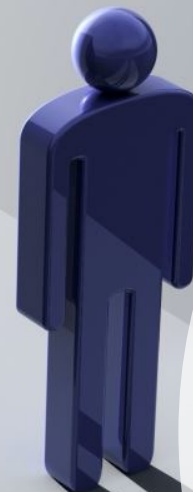
1 x

# OWASP Zed Attack Proxy (ZAP)





# Account Enumeration



# Complete Exercise 11

---

The lab guide will guide you through all  
the different examples and options.

Thank you! See you tomorrow!