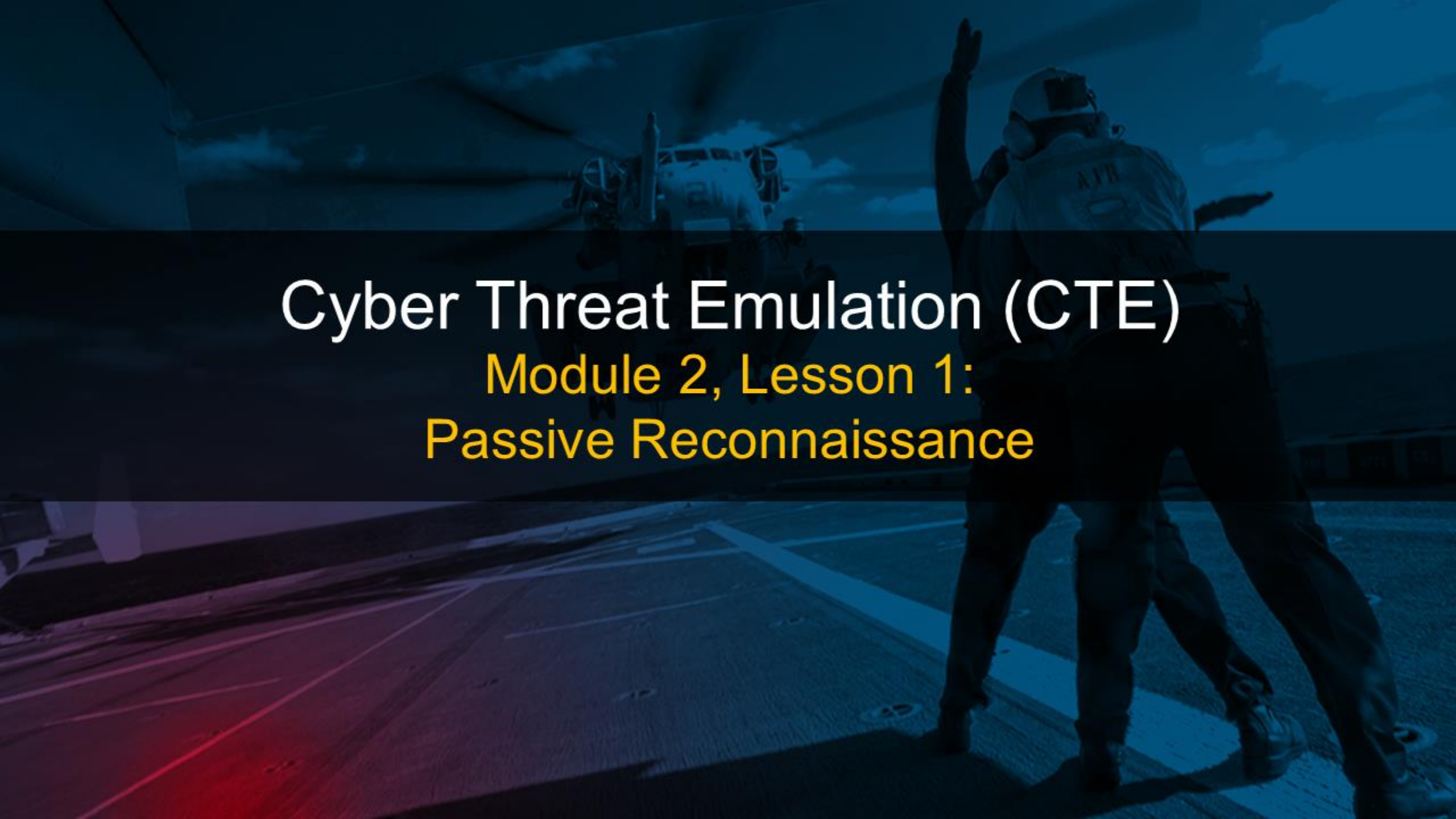


Cyber Threat Emulation (CTE)

Module 2, Lesson 1:
Passive Reconnaissance

Course Objectives

After completing this course, students will be able to:

- Summarize the CTE squad's responsibilities, objectives, and deliverables from each CPT stage
- Analyze threat information
- Develop a Threat Emulation Plan (TEP)
- Generate mitigative and preemptive recommendations for local defenders
- Develop mission reporting
- Conduct participative operations
- Conduct reconnaissance
- Analyze network logs for offensive and defensive measures

Course Objectives (Continued)

Students will also be able to:

- Analyze network traffic and tunneling protocols for offensive and defensive measures
- Plan non-participative operations using commonly used tools, techniques and procedures (TTPs)

Module 2: Threat Emulation (Objectives)

- Conduct reconnaissance
- Generate mission reports from non-participative operations
- Plan a non-participative operation using social engineering
- Plan a non-participative operation using Metasploit
- Analyze network logs for offensive and defensive measures
- Analyze network traffic and tunneling protocols for offensive and defensive measures
- Plan a non-participative operation using Python
- Develop fuzzing scripts
- Develop buffer overflow exploits

Module 2 – Lesson 1: Reconnaissance (Objectives)

- Recognize the difference between passive and semi-passive information gathering
- Identify open source reconnaissance tools
- Use open source reconnaissance tools for data gathering
- Develop a mission report from results of passive reconnaissance

Lesson Overview – Reconnaissance

Recon Types

- Passive
- Semi-passive
- Active

Recon Categories

- Infrastructure
- People
- Organization

Recon Tools

- Native OS Tools
- Robtex
- Shodan
- Maltego
- Metagoofil
- theHarvester
- Recon-ng
- ThreatMiner

Reconnaissance… and The Art of War

Take advantage of the enemy's unreadiness, make your way by unexpected routes, and attack unguarded spots.

—Sun Tzu

Reconnaissance: Gathering Information

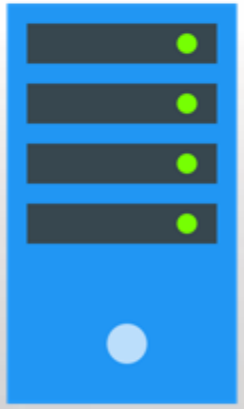
- Gather as much as possible
- Find publicly available information (Open Source)
- Avoid detection
- Avoid triggering alerts on Intrusion Detection Systems (IDS)
- Avoid creating any log entries on target systems
- Keep detailed notes

Passive Reconnaissance

- Never send any traffic (packets) to target organization
- Collection activities must never be detected by the target
- Only gather archived or stored information
- Gathered information could be inaccurate and out of date – some may be collected by a third party

Open Source Intelligence (OSINT)

- Another name for passive reconnaissance
- Information related to the target from publicly available sources
- Discover potential vectors or entry points into an organization



PHYSICAL
Server Room

ELECTRONIC
Internet

HUMAN
Personnel

Semi-passive Reconnaissance

- Profile the target with methods that appear like normal Internet traffic and behavior

Avoid drawing attention, meaning…

- No in-depth reverse lookups
- No brute force DNS requests
- No searching for hidden content – "unpublished" servers or directories
- No port scans or crawlers on target network

- Only metadata found in published documents and files

Active Reconnaissance

- Actively mapping network infrastructure through port scans
- Actively enumerating and/or vulnerability scanning for open services
- Actively seeking unpublished directories, files, and servers
- Should be detected by the target as suspicious or malicious behavior

Personnel / Organizational Reconnaissance

- Create personnel and organizational profiles from customer's web presence
- Identify possible vulnerabilities found in relevant open source information
- Create persona and website (callback) profiles (malware)
- Harvest email addresses
- Social engineering opportunities
- Metadata for files, if found (data about data)
- Lack of individual internet presence

Infrastructure Reconnaissance

- Discover all networks owned by the target
- Identify presence in other countries
- Discover top level domains (TLD)
- Build a network diagram

Facebook.com - Robtex

QUICK INFO

facebook.com quick info

General	
FQDN	facebook.com
Host Name	
Domain Name	facebook.com
Registry	com
TLD	com
DNS	
IP numbers	*2a03:2880:f101:83:face:b00c::25de* *2a03:2880:f105:283:face:b00c::25de* *2a03:2880:f10d:183:face:b00c::25de* *2a03:2880:f10f:83:face:b00c::25de* *2a03:2880:f111:83:face:b00c::25de* *2a03:2880:f12d:83:face:b00c::25de* *2a03:2880:f134:183:face:b00c::25de* *31.13.65.36* *31.13.82.36* *31.13.93.35* *157.240.3.35* *157.240.11.35* *157.240.12.35* *185.60.216.35*
Name servers	*a.ns.**facebook**.com* *b.ns.**facebook**.com*
Mail servers	*msgin.vvv.**facebook**.com*

Reconnaissance Tools

- Native OS Tools (whois, nslookup, dig)
- Robtex
- Kali Open Source Tools
  - Shodan
  - Maltego
  - Metagoofil
  - theHarvester
  - Recon-ng
  - ThreatMiner

whois

Identifies:

- Registry Info
- Creation Date
- Update Date
- Domain Status
- DNS Servers
- Contacts

```
admin@kali:~$ whois hack.me
Domain Name: HACK.ME
Registry Domain ID: D108500000000003559-AGRS
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2018-04-30T15:06:34Z
Creation Date: 2008-04-29T18:00:32Z
Registry Expiry Date: 2021-04-29T18:00:32Z
Registrar Registration Expiration Date:
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Reseller:
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Registrant Organization: Domains By Proxy, LLC
Registrant State/Province: Arizona
Registrant Country: US
Name Server: NS5.DNSMADEEASY.COM
Name Server: NS6.DNSMADEEASY.COM
Name Server: NS7.DNSMADEEASY.COM
Name Server: NS4.HACK.ME
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form  https://www.icann.org/wicf/)
>>> Last update of WHOIS database: 2018-11-27T15:07:48Z <<<

For more information on Whois status codes, please visit https://icann.org/epp
```

nslookup

Identifies:

- Local DNS server
- Non-authoritative DNS server
- Mail servers (mx)
- DNS servers (ns)
- Start of Authority (soa)
- Pointer (ptr)
- A record (a)
- AAAA record (aaaa)

```
admin@kali:~$ nslookup
> hack.me
Server:         192.168.0.2
Address:        192.168.0.2#53

Non-authoritative answer:
Name:   hack.me
Address: 74.50.111.244
> set type=mx
> hack.me
Server:         192.168.0.2
Address:        192.168.0.2#53

Non-authoritative answer:
hack.me mail exchanger = 5 alt2.aspmx.l.google.com.
hack.me mail exchanger = 10 alt3.aspmx.l.google.com.
hack.me mail exchanger = 10 alt4.aspmx.l.google.com.
hack.me mail exchanger = 1 aspmx.l.google.com.
hack.me mail exchanger = 5 alt1.aspmx.l.google.com.

Authoritative answers can be found from:
> set type=ns
> hack.me
Server:         192.168.0.2
Address:        192.168.0.2#53

Non-authoritative answer:
hack.me nameserver = ns6.dnsmadeeasy.com.
hack.me nameserver = ns7.dnsmadeeasy.com.
hack.me nameserver = ns4.hack.me.
hack.me nameserver = ns5.dnsmadeeasy.com.
```

dig

Identifies:

- Local DNS server
- Non-authoritative DNS server
- Mail servers (mx)
- DNS servers (ns)
- Start of Authority (soa)
- Pointer (ptr)
- A record (a)
- AAAA record (aaaa)

```
admin@kali:~$ dig hack.me ns

; <<>> DiG 9.10.3-P4-Debian <<>> hack.me ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8452
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;hack.me.                       IN      NS

;; ANSWER SECTION:
hack.me.                60      IN      NS      ns6.dnsmadeeasy.com.
hack.me.                60      IN      NS      ns7.dnsmadeeasy.com.
hack.me.                60      IN      NS      ns4.hack.me.
hack.me.                60      IN      NS      ns5.dnsmadeeasy.com.

;; Query time: 28 msec
;; SERVER: 192.168.0.2#53(192.168.0.2)
;; WHEN: Tue Nov 27 15:15:26 UTC 2018
;; MSG SIZE  rcvd: 123
```

host

Identifies:

- Mail servers (mx)
- DNS servers (ns)
- Start of authority (soa)
- Pointer (ptr)
- A record (a)
- AAAA record (aaaa)

```
admin@kali:~$ host -t mx hack.me
hack.me mail is handled by 5 alt2.aspmx.l.google.com.
hack.me mail is handled by 10 alt3.aspmx.l.google.com.
hack.me mail is handled by 10 alt4.aspmx.l.google.com.
hack.me mail is handled by 1 aspmx.l.google.com.
hack.me mail is handled by 5 alt1.aspmx.l.google.com.
admin@kali:~$ host -t ns hack.me
hack.me name server ns7.dnsmadeeasy.com.
hack.me name server ns4.hack.me.
hack.me name server ns5.dnsmadeeasy.com.
hack.me name server ns6.dnsmadeeasy.com.
admin@kali:~$ host -t soa hack.me
hack.me has SOA record ns4.hack.me. hostmaster. 187 900 600 86400 3600
admin@kali:~$ host -t ptr hack.me
hack.me has no PTR record
admin@kali:~$ host hack.me
hack.me has address 74.50.111.244
hack.me mail is handled by 5 alt1.aspmx.l.google.com.
hack.me mail is handled by 5 alt2.aspmx.l.google.com.
hack.me mail is handled by 10 alt3.aspmx.l.google.com.
hack.me mail is handled by 10 alt4.aspmx.l.google.com.
hack.me mail is handled by 1 aspmx.l.google.com.
admin@kali:~$ host -t a hack.me
hack.me has address 74.50.111.244
admin@kali:~$ host -t aaaa hack.me
hack.me has no AAAA record
```

Differences Between host, dig and nslookup

nslookup	host	dig
• First tool for querying DNS • CLI for interacting with the DNS • Difficult to script	• Does the domain exist or resolve to an address? • Searching for simple DNS record type	• Used for probing the DNS • Produces multi-line output • More comprehensive answer than host

- Both **dig** and **host** created to facilitate scripting and ease of use

DNS Resource Records

Types of DNS Records

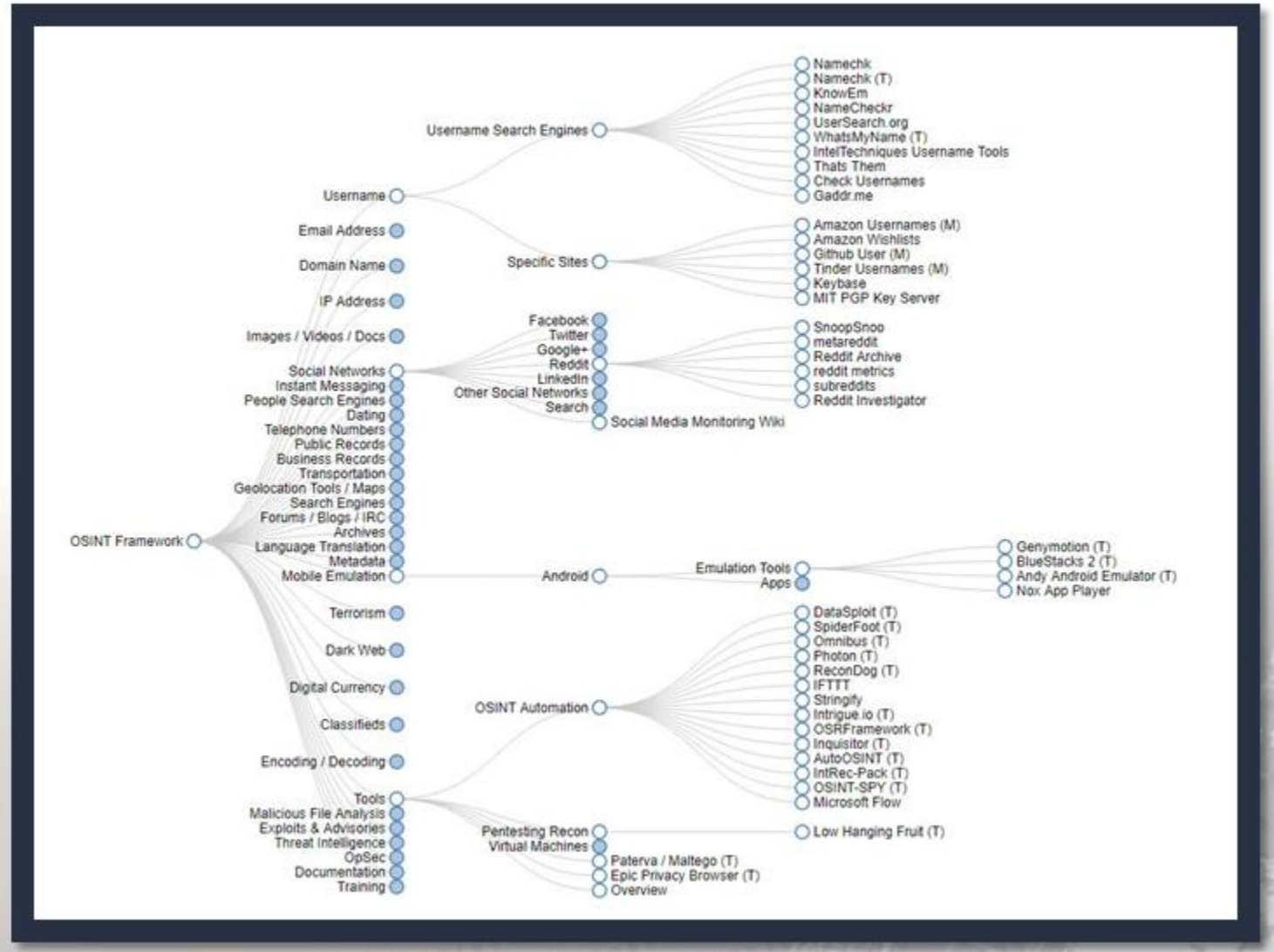
- Start of Authority (SOA)
- IP addresses (A and AAAA)
- SMTP mail exchangers (MX)
- Name servers (NS)
- Pointers for reverse DNS lookups (PTR)
- Domain name aliases (CNAME)
- DNS Security Extensions (DNSSEC)
- Responsible Person (RP)
- Real-time Blackhole List (RBL)

OSINT Framework

https://osintframework.com/

https://github.com/lockfale/osint-framework

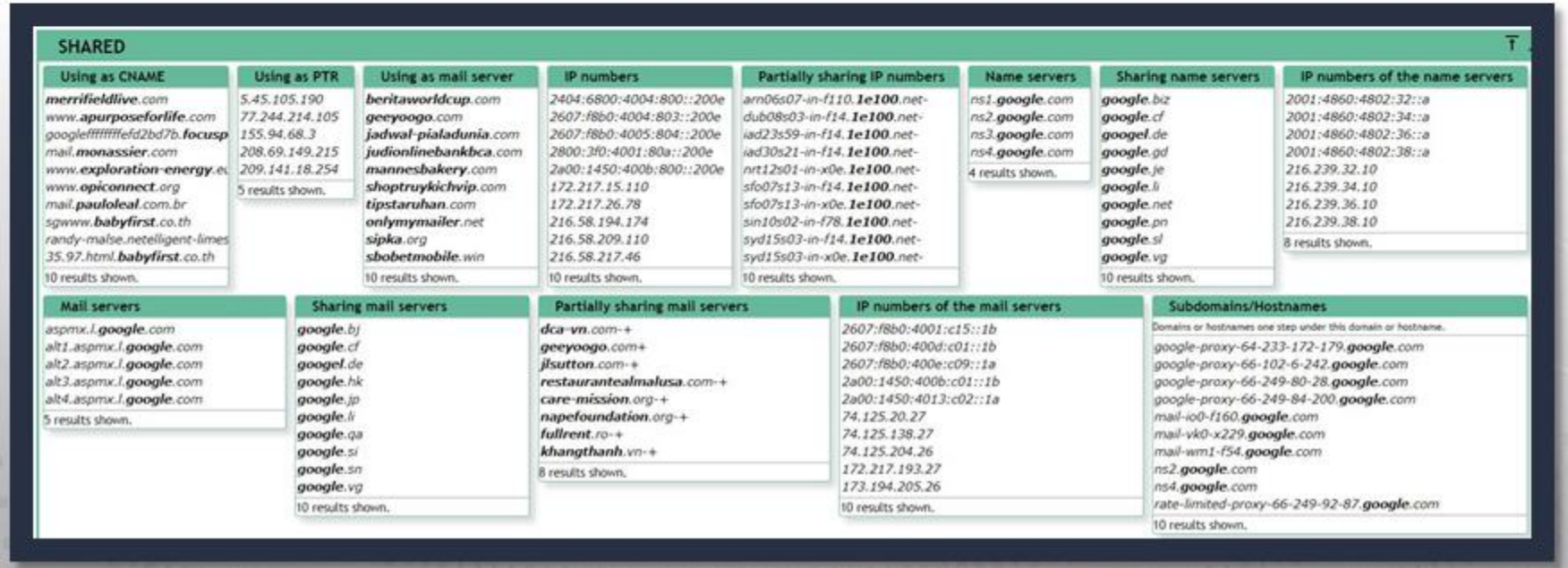
- Navigate options for information gathering
- Highlights tools or resources for OSINT



Robtex

- Comprehensive free DNS lookup tool
- Used for infrastructure research

Google.com - Robtex



SHARED

Using as CNAME	Using as PTR	Using as mail server	IP numbers	Partially sharing IP numbers	Name servers	Sharing name servers	IP numbers of the name servers
merrifieldlive.com	5.45.105.190	beritaworldcup.com	2404:6800:4004:800::200e	arn06s07-in-f110.1e100.net-	ns1.google.com	google.biz	2001:4860:4802:32::a
www.apurposeforlife.com	77.244.214.105	geeyoogo.com	2607:f8b0:4004:803::200e	dub08s03-in-f14.1e100.net-	ns2.google.com	google.cf	2001:4860:4802:34::a
googlefffffffffefd2bd7b.focusp	155.94.68.3	jadwal-pialadunia.com	2607:f8b0:4005:804::200e	iad23s59-in-f14.1e100.net-	ns3.google.com	googel.de	2001:4860:4802:36::a
mail.monassier.com	208.69.149.215	judionlinebankbca.com	2800:3f0:4001:80a::200e	iad30s21-in-f14.1e100.net-	ns4.google.com	google.gd	2001:4860:4802:38::a
www.exploration-energy.e	209.141.18.254	mannesbakery.com	2a00:1450:400b:800::200e	nrt12s01-in-x0e.1e100.net-	4 results shown.	google.je	216.239.32.10
www.opiconnect.org	5 results shown.	shoptruykichvip.com	172.217.15.110	sfo07s13-in-f14.1e100.net-		google.li	216.239.34.10
mail.pauloleal.com.br		tipstaruhan.com	172.217.26.78	sfo07s13-in-x0e.1e100.net-		google.net	216.239.36.10
sgwww.babyfirst.co.th		onlymymailer.net	216.58.194.174	sin10s02-in-f78.1e100.net-		google.pn	216.239.38.10
randy-malse.netelligent-limes		sipka.org	216.58.209.110	syd15s03-in-f14.1e100.net-		google.sl	8 results shown.
35.97.html.babyfirst.co.th		sbobetmobile.win	216.58.217.46	syd15s03-in-x0e.1e100.net-		google.vg	
10 results shown.		10 results shown.	10 results shown.	10 results shown.		10 results shown.	

Mail servers	Sharing mail servers	Partially sharing mail servers	IP numbers of the mail servers	Subdomains/Hostnames
aspmx.l.google.com	google.bj	dca-vn.com-+	2607:f8b0:4001:c15::1b	Domains or hostnames one step under this domain or hostname.
alt1.aspmx.l.google.com	google.cf	geeyoogo.com+	2607:f8b0:400d:c01::1b	google-proxy-64-233-172-179.google.com
alt2.aspmx.l.google.com	googel.de	jlsutton.com-+	2607:f8b0:400e:c09::1a	google-proxy-66-102-6-242.google.com
alt3.aspmx.l.google.com	google.hk	restaurantealmalusa.com-+	2a00:1450:400b:c01::1b	google-proxy-66-249-80-28.google.com
alt4.aspmx.l.google.com	google.jp	care-mission.org-+	2a00:1450:4013:c02::1a	google-proxy-66-249-84-200.google.com
5 results shown.	google.li	napefoundation.org-+	74.125.20.27	mail-io0-f160.google.com
	google.qa	fullrent.ro-+	74.125.138.27	mail-vk0-x229.google.com
	google.si	khangthanh.vn-+	74.125.204.26	mail-wm1-f54.google.com
	google.sn	8 results shown.	172.217.193.27	ns2.google.com
	google.vg		173.194.205.26	ns4.google.com
	10 results shown.		10 results shown.	rate-limited-proxy-66-249-92-87.google.com
				10 results shown.

QUICK INFO

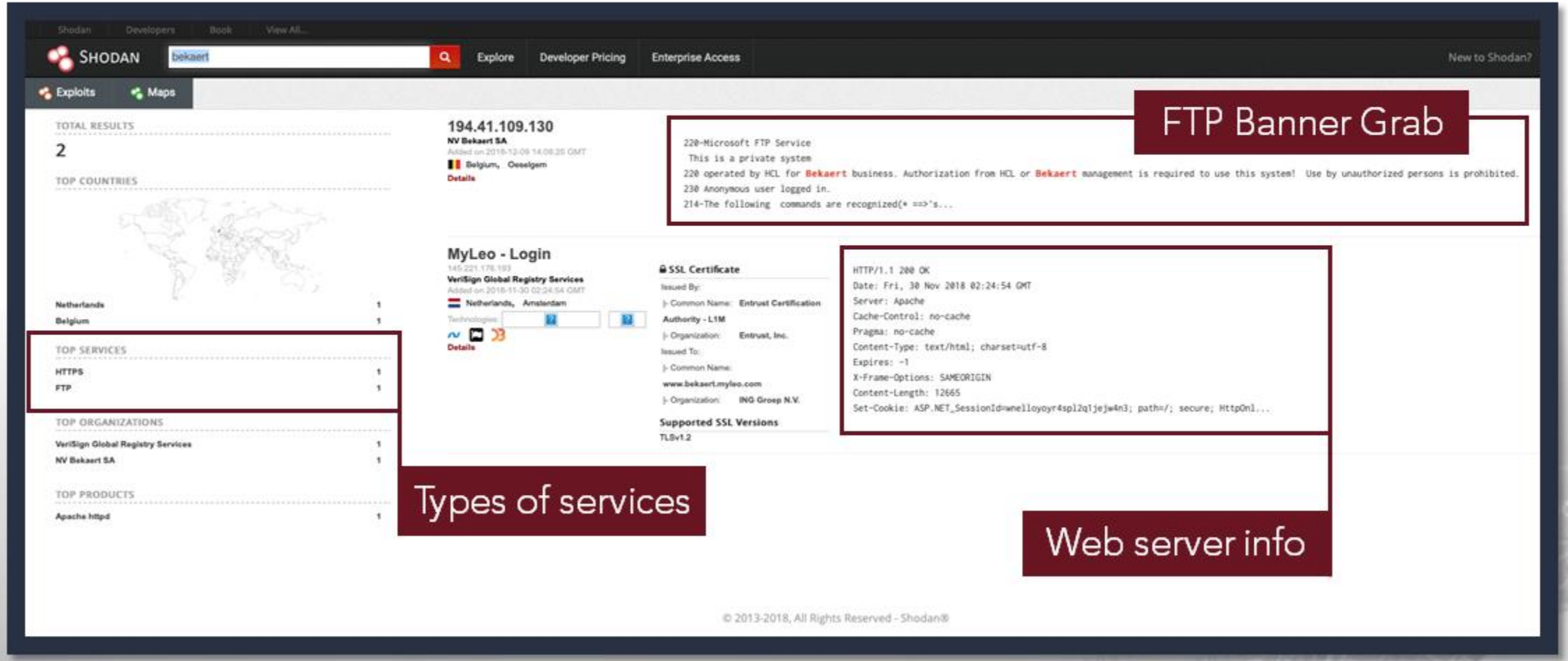
google.com quick info

	General
FQDN	google.com
Host Name	
Domain Name	google.com
Registry	com
TLD	com
	DNS
IP numbers	2404:6800:4003:80d::200e 2404:6800:4004:800::200e 2404:6800:4006:804::200e 2607:f8b0:4004:803::200e 2607:f8b0:4004:811::200e 2607:f8b0:4005:804::200e 2607:f8b0:4005:809::200e 2800:3f0:4001:80a::200e 2a00:1450:400b:800::200e 172.217.8.14 172.217.15.110 172.217.25.142 172.217.26.78 172.217.30.78 216.58.194.174 216.58.197.142 216.58.209.110 216.58.217.46
Name servers	ns1.google.com ns2.google.com ns3.google.com ns4.google.com
Mail servers	aspmx.l.google.com alt1.aspmx.l.google.com alt2.aspmx.l.google.com alt3.aspmx.l.google.com alt4.aspmx.l.google.com

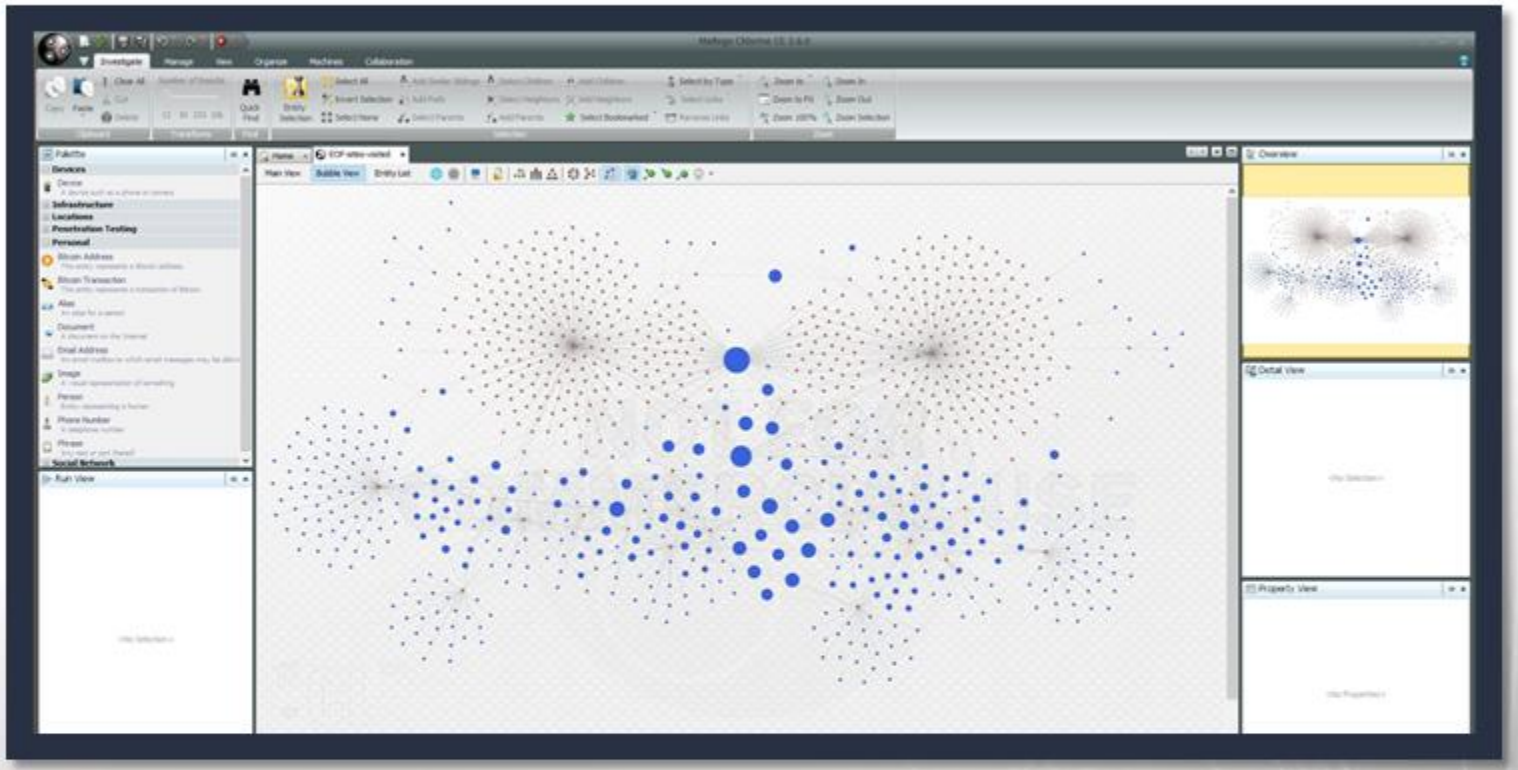
Shodan

- Shodan crawls the Internet 24/7 to provide the latest Internet intelligence
- Shodan can integrate with Nmap, Metasploit, FOCA, Chrome, Firefox and other tools
- Shodan collects information on public facing IPs

Shodan


SHODAN
bekaert
Explore
Developer Pricing
Enterprise Access
New to Shodan?
Exploits
Maps
TOTAL RESULTS
2
TOP COUNTRIES
Netherlands 1
Belgium 1
TOP SERVICES
HTTPS 1
FTP 1
TOP ORGANIZATIONS
VeriSign Global Registry Services 1
NV Bekaert SA 1
TOP PRODUCTS
Apache httpd 1
194.41.109.130
NV Bekaert SA
Belgium, Oosolgem
Details
220-Microsoft FTP Service
This is a private system
220 operated by HCL for Bekaert business. Authorization from HCL or Bekaert management is required to use this system! Use by unauthorized persons is prohibited.
230 Anonymous user logged in.
214-The following commands are recognized(* ==>'s...
FTP Banner Grab
MyLeo - Login
VeriSign Global Registry Services
Netherlands, Amsterdam
Details
SSL Certificate
Issued By:
Common Name: Entrust Certification Authority - L1M
Organization: Entrust, Inc.
Issued To:
Common Name: www.bekaert.myleo.com
Organization: ING Groep N.V.
Supported SSL Versions
TLSv1.2
HTTP/1.1 200 OK
Date: Fri, 30 Nov 2018 02:24:54 GMT
Server: Apache
Cache-Control: no-cache
Pragma: no-cache
Content-Type: text/html; charset=utf-8
Expires: -1
X-Frame-Options: SAMEORIGIN
Content-Length: 12665
Set-Cookie: ASP.NET_SessionId=wnelloyoyr4spl2q1jejw4n3; path=/; secure; HttpOnl...
Types of services
Web server info
© 2013-2018, All Rights Reserved - Shodan®

Maltego

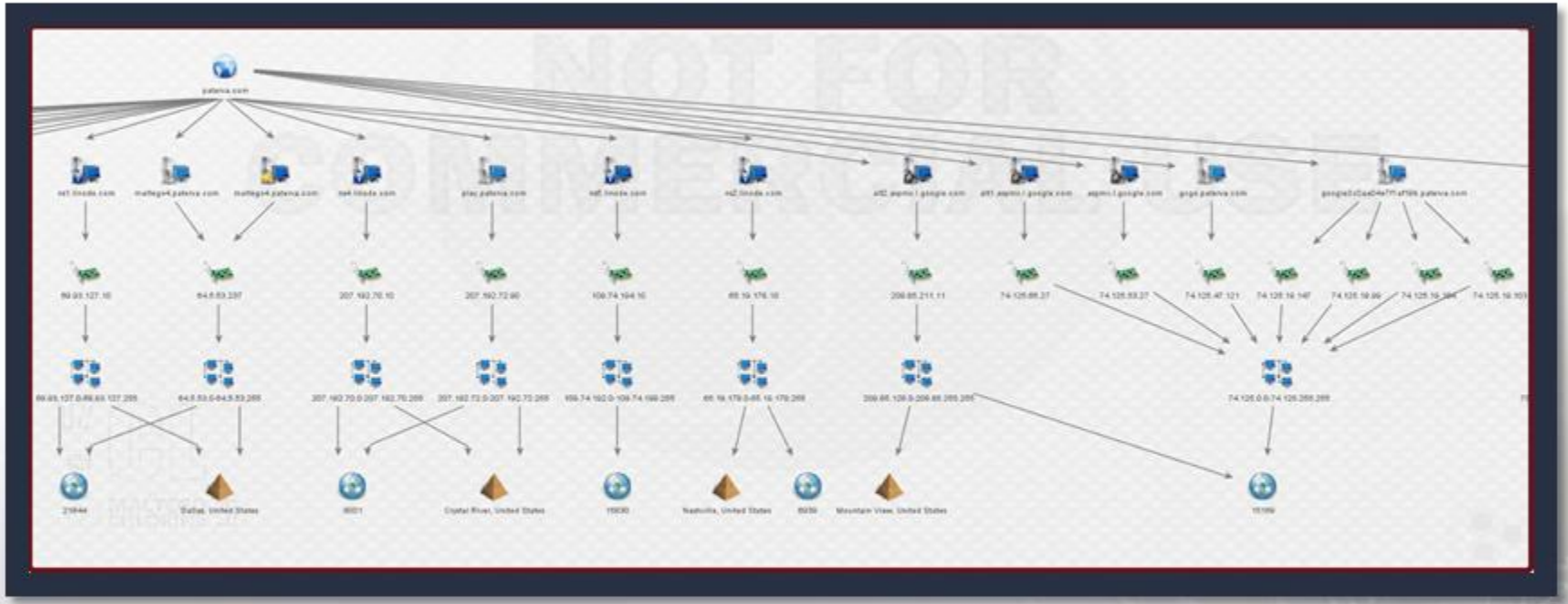


- Data Mining Tool
- Relationships based on public (Open Source) information
- Queries DNS, WHOIS, search engines, social media, etc.
- Visual representation of links
- Easily loaded onto Kali Linux
- Requires account registration
- APIs are required for full functionality

Maltego

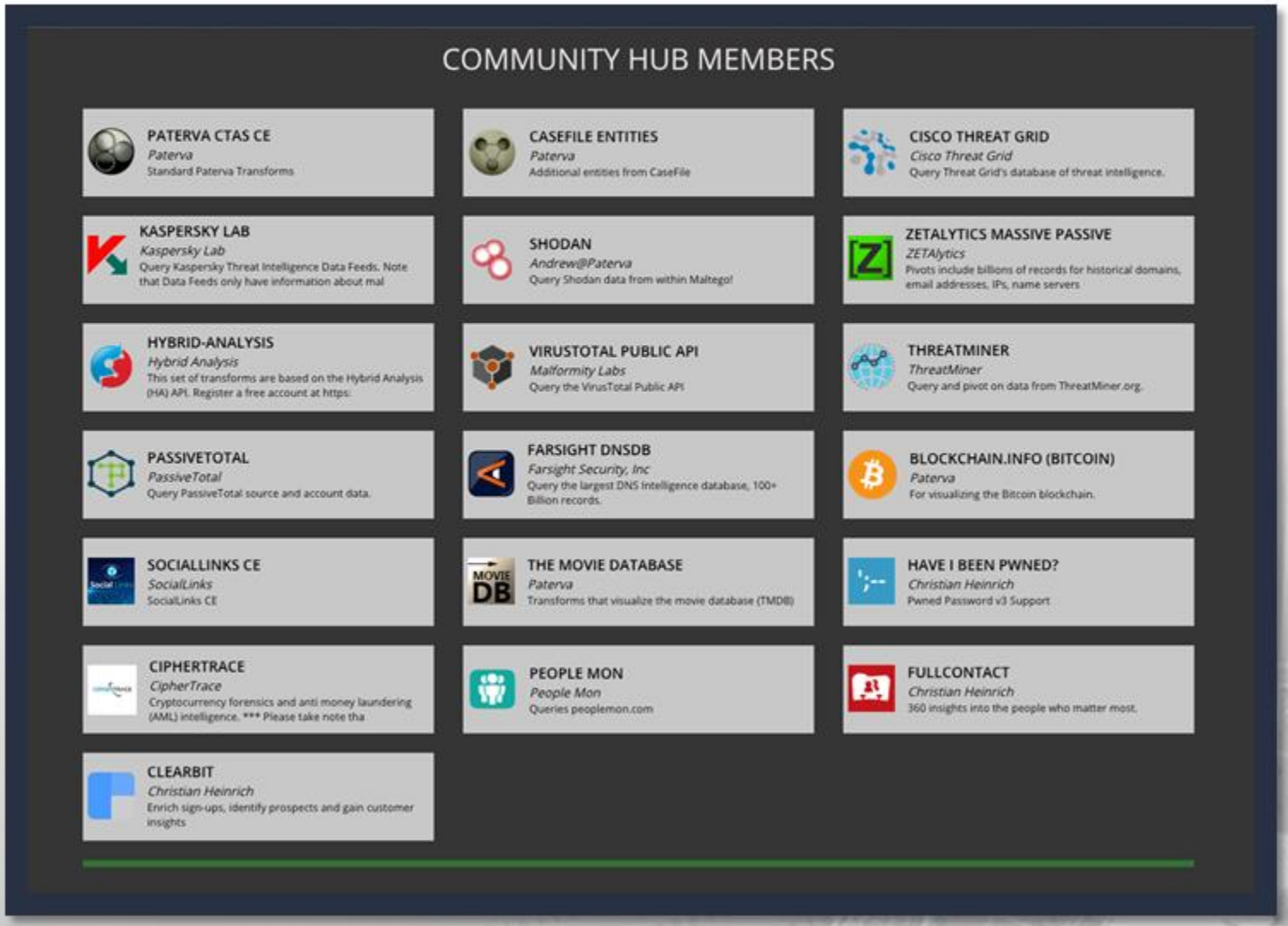
Infrastructure of the Paterva.com:

- Starts with the domain and then gets hostnames for the zone
- Hostnames resolve to IP addresses
- IPs taken to netblocks
- Netblocks to Autonomous Systems (AS)
- Locations



Maltego

- "Transforms" link to data sources, such as Shodan, VirusTotal, ThreatMiner, and others.
- Transform Input data (IPs, domain names, etc.) and return Output data (domain names, IPs, etc.).
- Output data then becomes Input data



Metagoofil

- First, performs a Google search to identify and download documents from a target to local disk
- Next, extracts file metadata with different libraries, such as Hachoir, PdfMiner and others


```
root@kali:~# metagoofil -d apple.com -t doc,pdf -l 100 -n 10 -o applefiles -f results.html
```

```
[1/10] /webhp?hl=en
        [x] Error downloading /webhp?hl=en
[2/10] http://www.apple.com/certificateauthority/WWDR_CPS/
[3/10] https://www.apple.com/certificateauthority/Apple_Timestamp_CPS/
[4/10] https://manuals.info.apple.com/en_US/0307843ANOS2FTURS.PDF
        [x] Error in the parsing process
[5/10] https://developer.apple.com/softwarelicensing/files/audio_units_logo_lic.pdf
[6/10] https://developer.apple.com/softwarelicensing/files/mac_logo_license_agreement.pdf
[7/10] https://developer.apple.com/softwarelicensing/files/bonjour_logo_agreement.pdf
[8/10] https://developer.apple.com/softwarelicensing/files/bonjour4win.pdf
[9/10] http://images.apple.com/xserve/pdf/computerworld_xserve_g5.pdf
```

Metagoofil

- Metagoofil downloads local copies of the target's documents and their source locations
- With the results, Metagoofil generates a report with:
  - usernames
  - emails
  - software versions and servers
  - machine names

theHarvester

- Both Active and Passive Tool
- Gathers
  - Email addresses
  - Virtual hosts
  - Subdomain names
  - Open ports and banners
  - Employee names
  - Open Source

```
Usage: theharvester options

       -d: Domain to search or company name
       -b: data source: baidu, bing, bingapi, dogpile, google, googleCSE,
                        googleplus, google-profiles, linkedin, pgp, twitter, vhost,
                        virustotal, threatcrowd, crtsh, netcraft, yahoo, all

       -s: Start in result number X (default: 0)
       -v: Verify host name via dns resolution and search for virtual hosts
       -f: Save the results into an HTML and XML file (both)
       -n: Perform a DNS reverse query on all ranges discovered
       -c: Perform a DNS brute force for the domain name
       -t: Perform a DNS TLD expansion discovery
       -e: Use this DNS server
       -l: Limit the number of results to work with(bing goes from 50 to 50 results,
           google 100 to 100, and pgp doesn't use this option)
       -h: use SHODAN database to query discovered hosts

Examples:
       theharvester -d microsoft.com -l 500 -b google -h myresults.html
       theharvester -d microsoft.com -b pgp
       theharvester -d microsoft -l 200 -b linkedin
       theharvester -d apple.com -b googleCSE -l 500 -s 300

root@kali:~#
```

theHarvester

Results for Pepsi.com

- 92 total hosts found in search engines
- 68 hosts with IP's
- 13 virtual hosts
- 11 'empty' (no IP's)
- 0 emails

```
root@kali:~# theharvester -d pepsi.com -v -l 50 -b all -f myresults.html
```

```
Total hosts: 92

[-] Resolving hostnames IPs...

.pepsi.com:empty
Account.pepsi.com:159.127.185.117
Sip.ca.pepsi.com:empty
Sip.intl.pepsi.com:empty
Sip.pepsi.com:empty
account.pepsi.com:159.127.185.117
assets.pepsi.com:23.7.114.29
autodiscover.ca.pepsi.com:empty
autodiscover.intl.pepsi.com:empty
autodiscover.msgrouting.pepsi.com:emp
autodiscover.pepsi.com:empty
badges.pepsi.com:45.60.75.51
cdn.pepsi.com:empty
cr.pepsi.com:45.60.75.51
dev.pepsi.com:23.7.114.29
e.pepsi.com:159.127.187.12
fbfoodservice.pepsi.com:18.214.229.99
halftime.pepsi.com:18.214.229.99
halftimegallery.pepsi.com:52.22.210.2
intl.pepsi.com:empty
mail.intl.pepsi.com:165.198.95.202
ncimages.pepsi.com:23.74.2.122
origin-www.pepsi.com:empty
pass.pepsi.com:18.214.229.99
points.pepsi.com:18.214.229.99
policy.pepsi.com:45.60.75.51
```

Recon-ng

- Designed to facilitate web-based open source reconnaissance
- Modeled on Metasploit as far as look, feel and basic functionality
- Built around modules and a database as information is gathered
- Scrapes information from websites such as Google, Bing and others
- Python-based

```
[recon-ng][default] > show modules recon
```

```
[75] Recon modules
[8]  Reporting modules
[2]  Import modules
[2]  Exploitation modules
[2]  Discovery modules
```

Recon-ng

- Use `help` to list basic commands
  - `?` can also be used
- Use `keys list` to list all APIs that can be entered
- For full-functionality, load APIs for databases relevant to search:
  - Bing
  - BuiltWith
  - Censys
  - Flickr
  - FullContact
  - Github
  - Google (CSE)
  - Hashes.org
  - IP Info Database
  - Jigsaw
  - Shodan
  - AmIPwned
  - Twitter

```
[recon-ng][default] > help
```

```
[recon-ng][default] > keys list

  +-------------------------+
  |       Name              | Value |
  +-------------------------+
  | bing_api                |       |
  | builtwith_api           |       |
  | censysio_id             |       |
  | censysio_secret         |       |
  | flickr_api              |       |
  | fullcontact_api         |       |
  | github_api              |       |
  | google_api              |       |
  | google_cse              |       |
  | hashes_api              |       |
  | ipinfodb_api            |       |
  | jigsaw_api              |       |
  | jigsaw_password         |       |
  | jigsaw_username         |       |
  | pwnedlist_api           |       |
  | pwnedlist_iv            |       |
  | pwnedlist_secret        |       |
  | shodan_api              |       |
  | twitter_api             |       |
  | twitter_secret          |       |
  +-------------------------+
```

Recon-ng

1 Use 'search google' for a tool, such as google-related modules: google_site_api and google_site_web

```
[recon-ng][default][google_site_api] > search google
[*] Searching for 'google'...
```

2 Use the 'recon/hosts-hosts/bing_ip' module to find several additional IP's

```
-------------
172.217.192.26
-------------
[*] Searching Bing API for: ip:172.217.192.26
[*] No additional hosts discovered at '172.217.192.26'.

-------------
74.125.193.26
-------------
[*] Searching Bing API for: ip:74.125.193.26
[*] No additional hosts discovered at '74.125.193.26'.

-------------
173.194.76.26
-------------
[*] Searching Bing API for: ip:173.194.76.26
[*] No additional hosts discovered at '173.194.76.26'.

-------------
74.125.128.26
-------------
[*] Searching Bing API for: ip:74.125.128.26
[*] No additional hosts discovered at '74.125.128.26'.

-------------
209.85.232.26
-------------
[*] Searching Bing API for: ip:209.85.232.26
[*] No additional hosts discovered at '209.85.232.26'.

-------
SUMMARY
-------
[*] 3 total (1 new) hosts found.
```

3 Use 'show hosts' to display additional IPs found between Bing & Google searches.

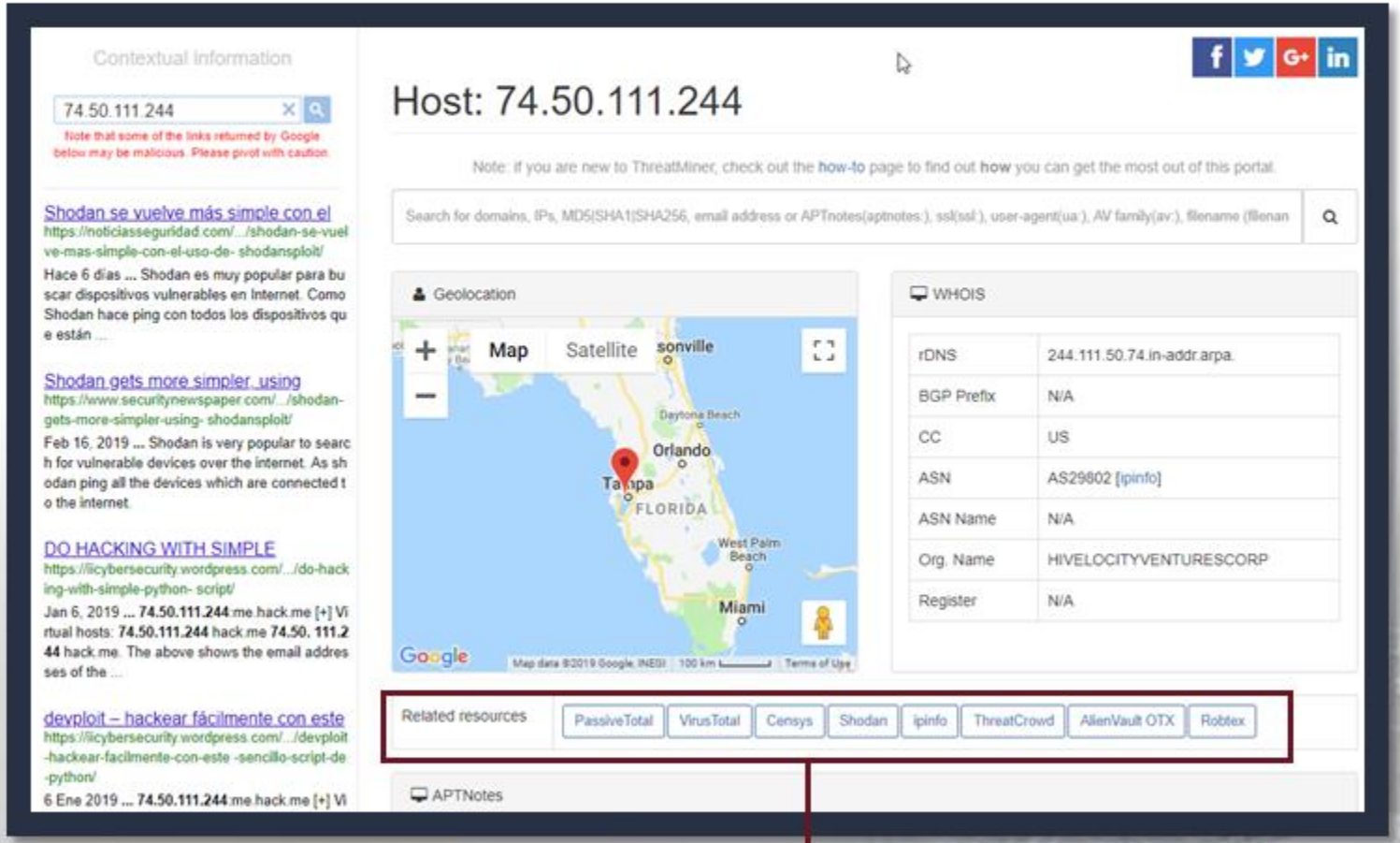
```
[recon-ng][default][bing_ip] > show hosts
```

host	ip_address
www.dcita.edu	52.95.144.5
learn.dcita.edu	144.202.134.162
dcita.edu	52.92.253.5
isd.dcita.edu	69.195.247.157
mail.dcita.edu	144.202.134.162
pm.dcita.edu	69.195.247.154
train.dcita.edu	54.71.228.28
login.dcita.edu	144.202.134.162
devlogin.dcita.edu	69.195.247.153
learn.dcita.edu	144.202.134.162
ops.dcita.edu	69.195.247.152
dev.dcita.edu	69.195.247.151
ALT1.ASPMX.L.GOOGLE.COM	172.217.192.26
ALT2.ASPMX.L.GOOGLE.COM	74.125.193.26
ALT3.ASPMX.L.GOOGLE.COM	173.194.76.26
ALT4.ASPMX.L.GOOGLE.COM	74.125.128.26
ASPMX.L.GOOGLE.COM	209.85.232.26
www.dcita.edu	52.92.253.5

ThreatMiner

Pivot directly from an open source research report to:

- PassiveTotal
- VirusTotal
- Censys
- Shodan
- Ipinfo
- ThreatCrowd
- AlientVault OTX
- Robtex



Exercise: Conducting Passive Reconnaissance

Objectives

After completing this exercise, students will be able to:

- Recognize the difference between passive and semi-passive information gathering
- Identify open source reconnaissance tools
- Use open source reconnaissance tools for data gathering
- Develop a Threat Emulation Assessment Report (TEAR) for the customer stakeholder

Duration

This exercise will take approximately **3** hours to complete.

Debrief

General Questions

- How did you feel about this procedure?
- Were there any areas in particular where you had difficulty?
- Do you understand how this relates to the work you will be doing?

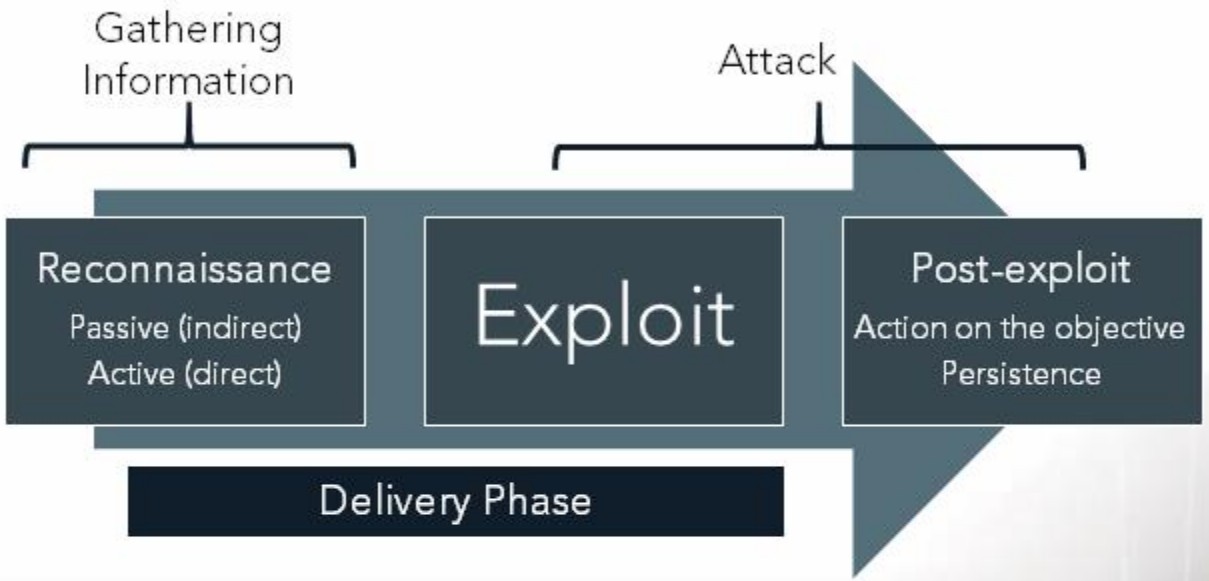
Specific Questions

- What tools did you use to conduct your passive reconnaissance?
- What tools could you use to help build an organizational chart?

Lesson Summary

In this lesson we learned about:

- The phases of reconnaissance
- Categories of information
  - People
  - Infrastructure
- Open source reconnaissance tools
  - Native OS Tools
  - Robtex
  - Shodan
  - Maltego
  - Metagoofil
  - theHarvester
  - Recon-ng
  - ThreatMiner



End of Module 2, Lesson 1