

# 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)

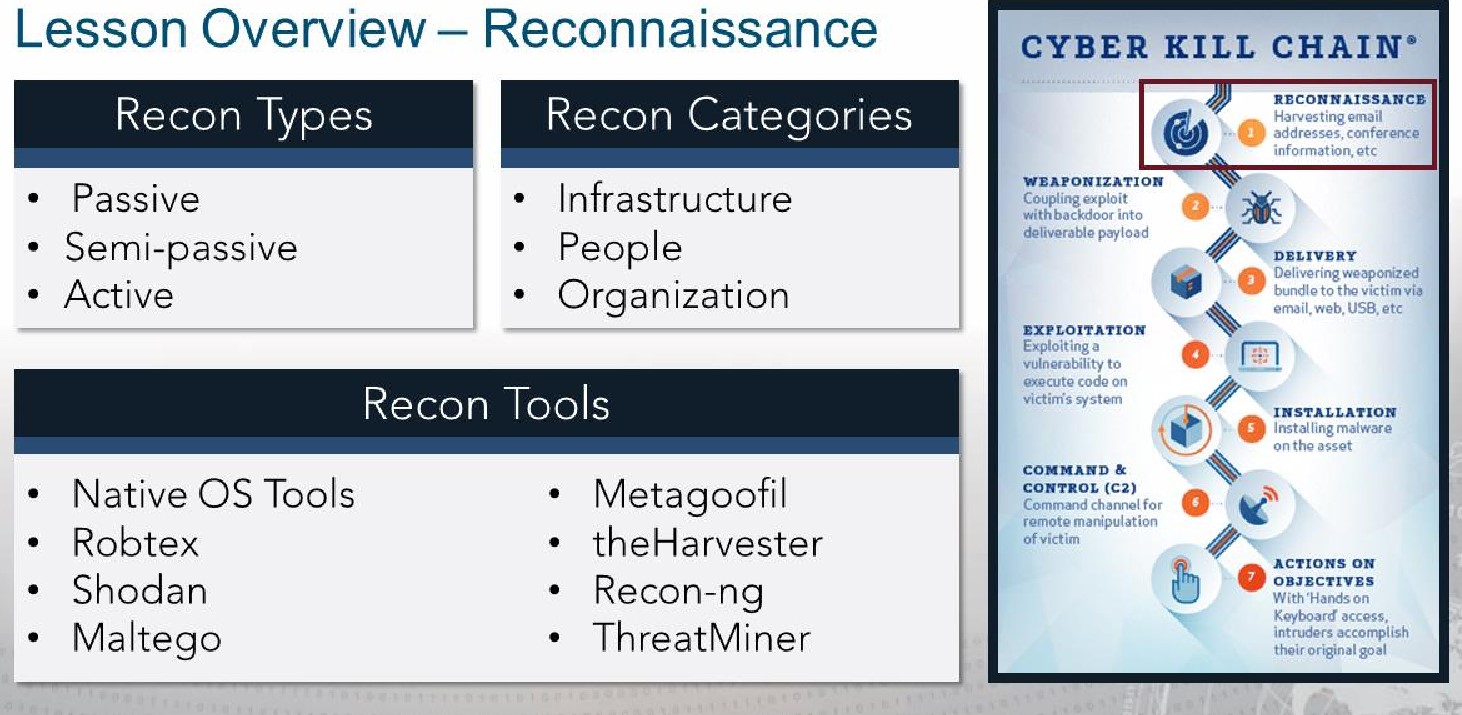
# Module 2: Threat Emulation (Objectives)

* 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)

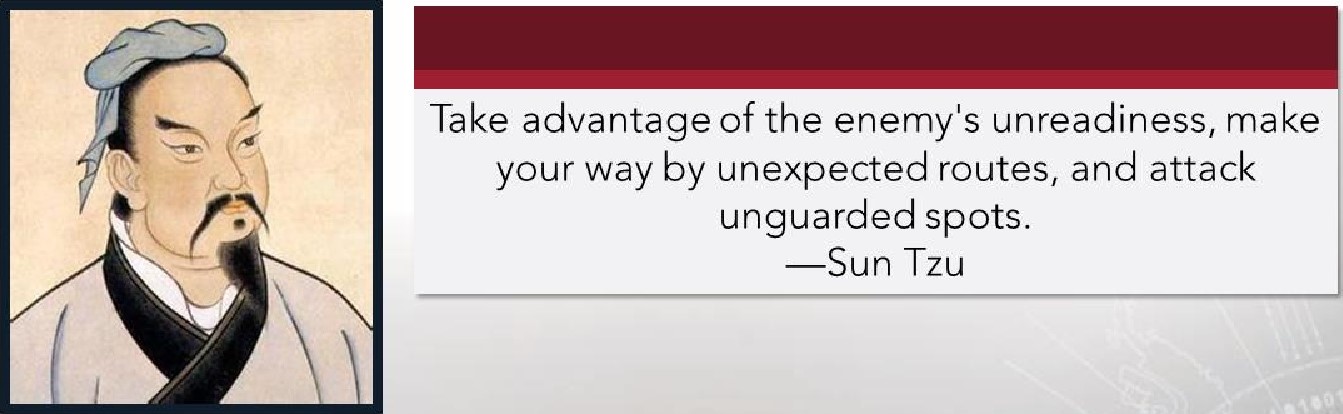
* Recognize the difference between passive and semi-passive information gathering
* Identify open source reconnaissance tools
* Use open source reconnaissance tools for data gathering
* Develop a mission report from results of passive reconnaissance

Cyber



I

# Reconnaissance. and The Art of War



## 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 ELECTRONIC HUMAN

Server Room Internet 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



|  |
| --- |
| UICK INFO |
| FQDN fac&ok.com  Host Name  Domain Name faceb00k.com  Registry  DNS  IP numbers  31.13.65.36  31.13.82.36  31.13.93.35  Robtex 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 server-s msgin. facebook.com |

### 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 -

# Reconnaissance Tools

* Native OS Tools (whois, nslookup, dig)
* Robtex
* Kali Open Source Tools

|  |  |
| --- | --- |
| • Shodan | • theHarvester |
| • Maltego | • Recon-ng |
| • Metagoofil | • ThreatMiner |

WhOiS hack. me

Domain Name: HACK. ME

Registry Domain ID: DlØ85UØOOO€ØO@3559-AGRS whois Registrar WHOIS Server: whois . godaddy . com

Registrar URL: http://www.godaddy . com Updated Date: 2018-04-36T15 Identifies: Creation Date:

Registry Expiry Date:

Registrar Registration Expiration Date:

* Registry Info Registrar: GODaddY , com, LLC

Registrar IANA ID: 146

* Creation Date Registrar Registrar Abuse Abuse Contact Contact Email; Phone: abuse@00daddy.com+1.4806242505

Reseller;

* Update Date Domain Status: clientDe1eteProhibited https://icann.org/epp#ctientDeteteProhibited Domain Status; clientRenewProhibited https://icann.orq/epp#cLientRenewProhibited

Domain Status: clientTransferProhibited https://icann.org/epp#cIientTransferProhibited

* Domain Status Domain Status: clientUPdatePrOhibited https://icann.org/epp#clientupdateprohibited

Registrant Organization: Domains By Proxy, LLC

* DNS Servers Registrant Registrant State/Province: Country: US Arizona

Name Server: . DNSMADEEASY.COM

* Contacts Name Server: NS6.DNSMADEEASY.COM Name Server: NS7. DNSMADEEASY.COM

Name Server: NS4 , HACK. ME

DNSSEC: unsigned

URL of the ICANN Wh0iS Inaccuracy Complatnt Form https://www.jcann.org/wtcf/) Last update of WHOIS database:

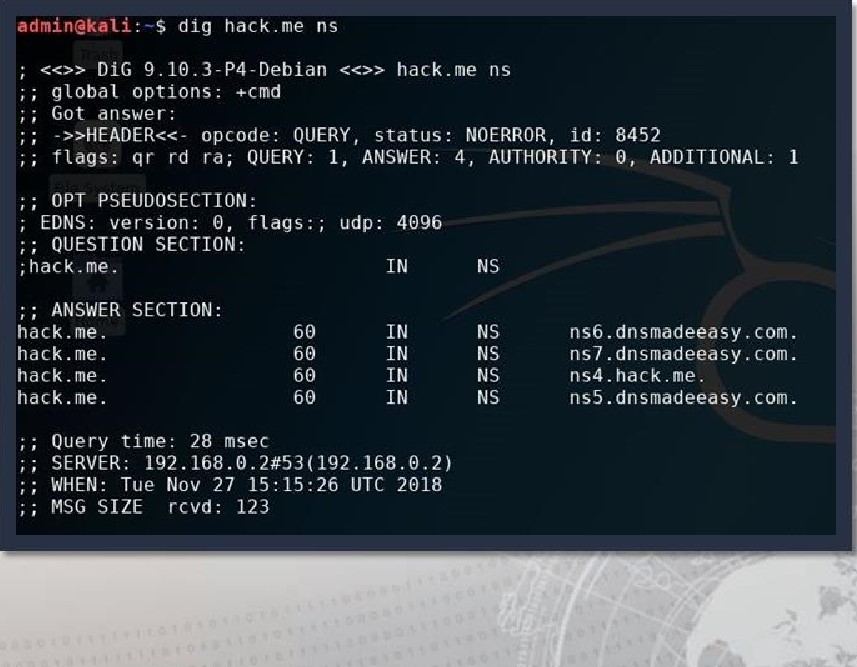
For more information on Whois status codes, please visit https://icann.org/epp

## 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)

## dig

Identifies:

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

## host

Identifies:

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

### • AAAA record (aaaa)

admin€kati.-$ host -t mx hack.me hack.me mail is handled by 5 alt2. aspmx.l . google.com. hack.me mail is handled by 19 alt3.aspmx.l.google. com. hack.me mail is handled by 19 alt4.aspmx.l.google. com. hack.me mail l is handled by 1 aspmx.l .gooqle. com.

hack.me mail is handled by 5 altl. aspmx. l . google.com, 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 nane server ns6. dnsmadeeasy. com host -t soa hack.me hack.me has SOA record ns4.hack.me. hostmaster. 181 86409 3690 host -t ptr hack.me hack.me has no PTR record admin@kali.-$ host hack.me hack.me has address 14.59. 111. 244 hack,me mail is handled by 5 altl. aspmx.l . google.com. hack.me mail is handled by 5 alt2. aspmx. l . google.com. hack.me mail is handled by 19 alt3.aspmx.l.google. com. hack.me mail is handled by 19 alt4.aspmx.l.gooqle. com. hack.me mail is handled by 1 aspmx.l.google. com. host -t a hack.me hack.me has address 74.59. 111. 244 admin€kati.-$ host -t aaaa hack.me hack.me has no AAAA record

## Differences Between host, dig and nslookup



# nslookup

* First tool for querying DNS • CLI for interacting with the DNS
* Difficult to script

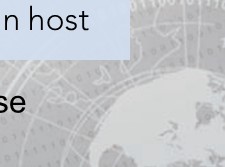
host



* Does the domain exist or resolve to an address? • Searching for simple DNS record type

# dig

## • Used for probing the DNS

* Produces multiline output  More comprehensive answer than host
* Both dig and host created to facilitate scripting and ease of use

## DNS Resource Records

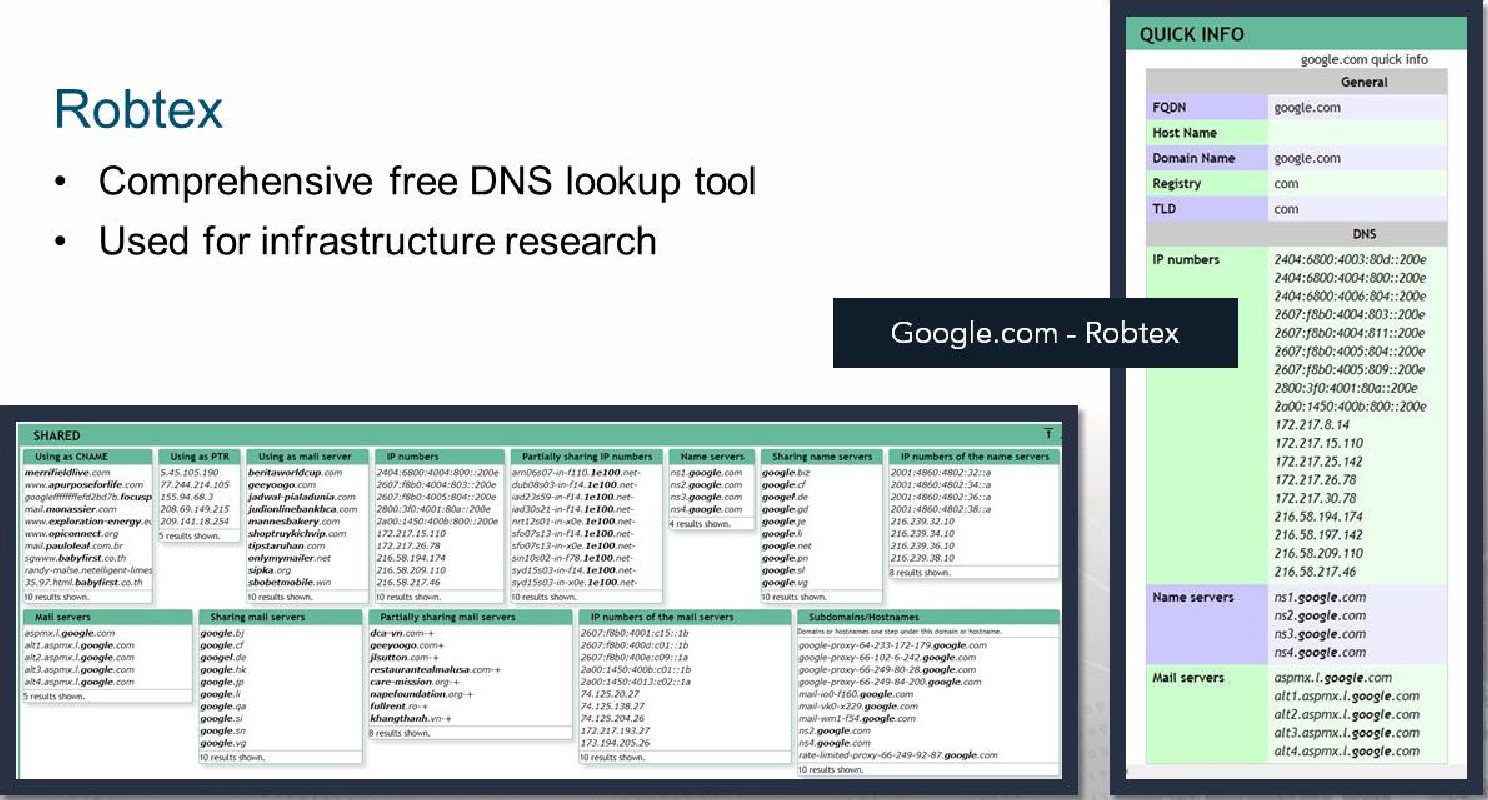
|  |  |
| --- | --- |
|  | Types of DNS Records |
|
|  | |
| * Start of Authority (SOA) Domain name aliases * IP addresses (A and AAAA) (CNAME) * SMTP mail exchangers (MX) DNS Security Extensions * Name servers (NS) (DNSSEC) * Pointers for reverse DNS Responsible Person (RP) lookups (PTR) Real-time Blackhole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

### OSINT Framework

#### https://osintframework.com/

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

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



## Shodan

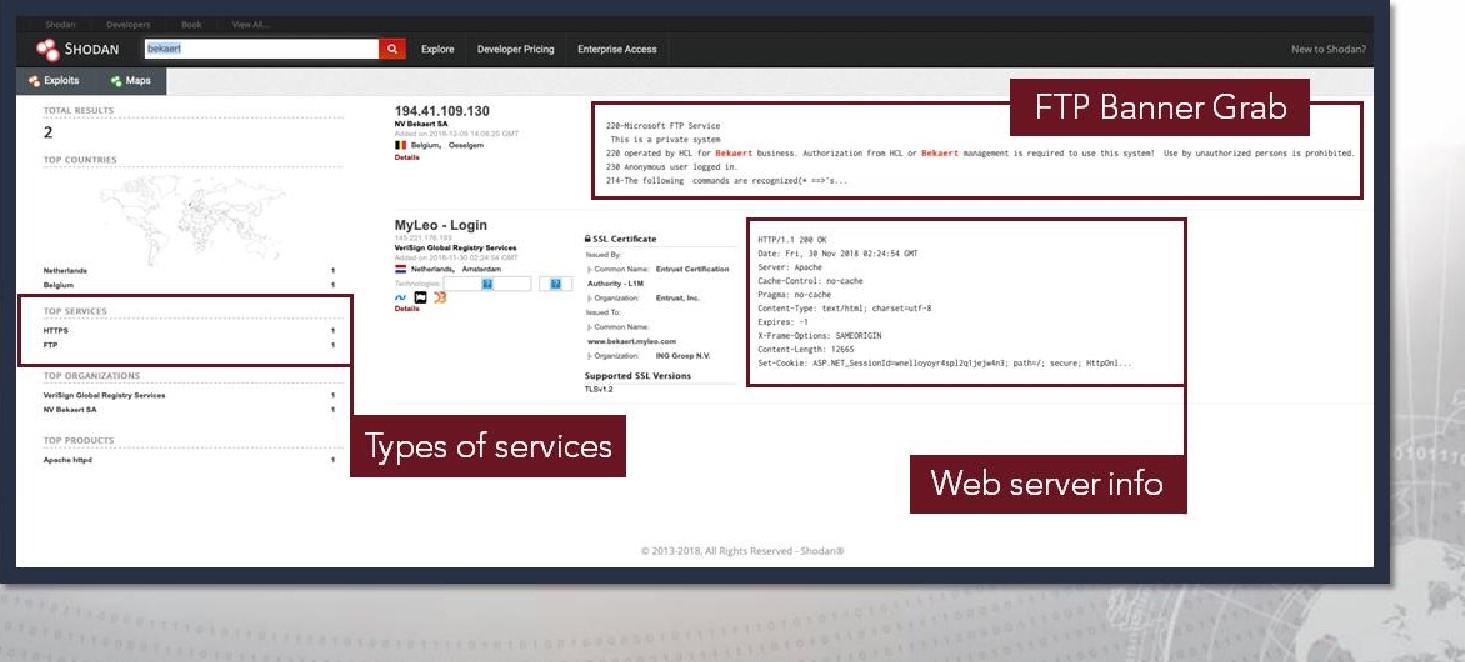
* Shodan crawls the Internet 24/7 to provide the latest Internet intelligence
* Shodan can integrate with Nmap, Metasploit,

FOCA, Chrome, Firefox and other tools

* Shodan collects information on public facing IPS



## Shodan



### Maltego

* Data Mining Tool
* Relationships based on public (Open

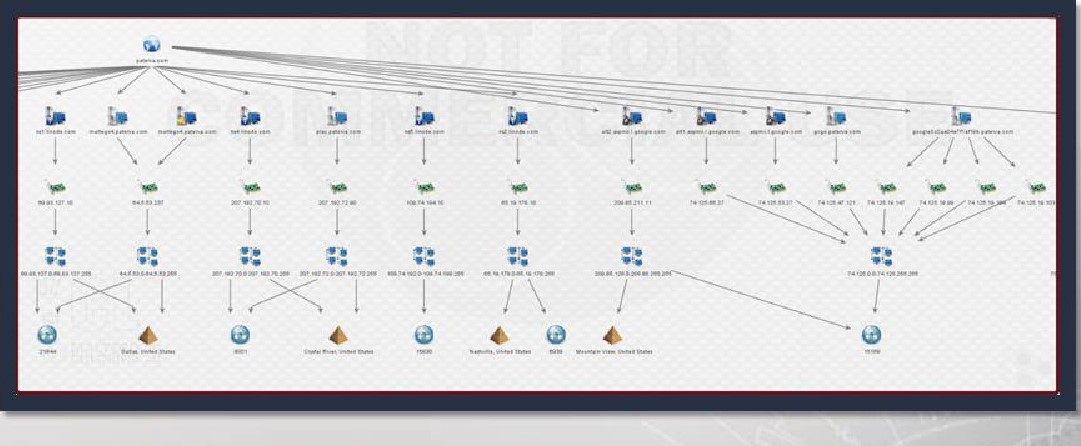
Source) information

* 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

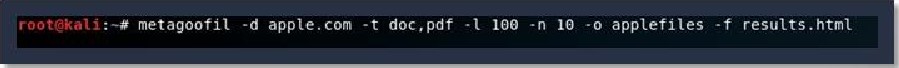
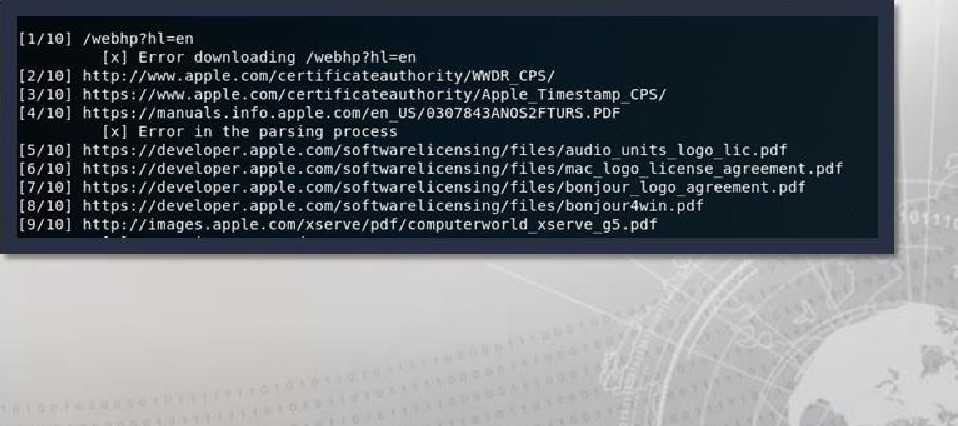
Infrastructure of the Paterva.com:

* 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

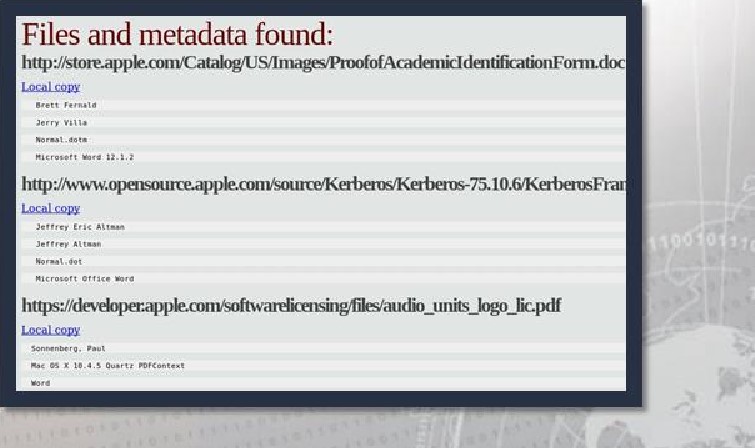
### Maltego

* "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

### 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: Donain to search Cornpany name

-b: data source: baidu, bing, bingapi, dog-pile, google, googleCSE googleplus, geog le- profiles. linkedin, pgp. twitter. "host, virustotölr threatcrowd, ertsh. nettraft, yahoo.

-s: Start in result number X IdefauLt: e)

-v: verify host natne Via dns resolution and search for Virtual hosts Save the results into an i•ifMt\_ and XML file (both) perform a ONS reverse query on all ranges discovered Perform a DNS brute force for the domain name

Perform' a DNS VLD expansion discovery

•e: use this DNS server

-t: Litnlt the nuttiber Of results to work With(bång goes from 50 tö 50 results, google to 196, and pgp doesn't use this option) -h: use SHODAN database to query discovered hosts

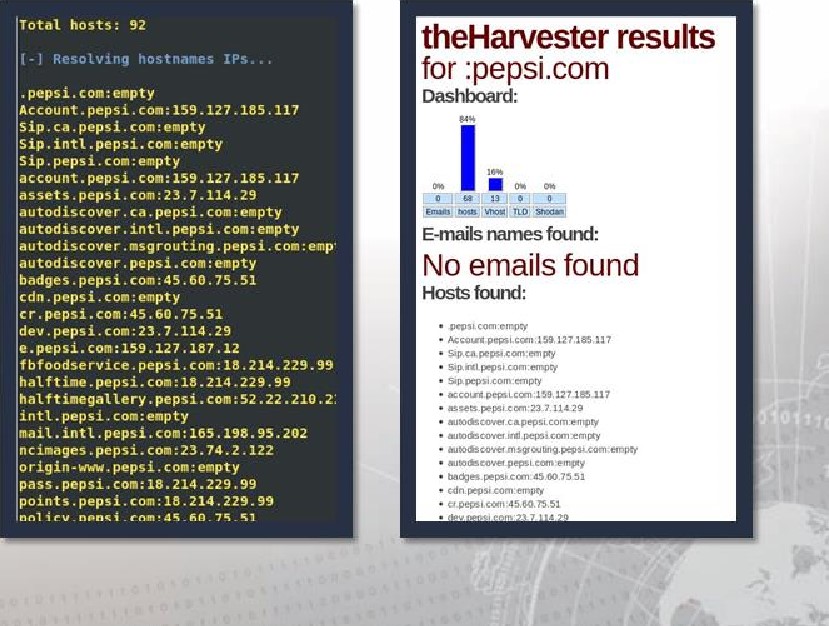
Examples :

-e microsoft.com -1 500 -b google myresutts.html

thehat•vester -d microsoft.com •b pgp theharvester -d microsoft •t 200 •b linkedin theha -d apple . com -b googvecsE -1 590 -s

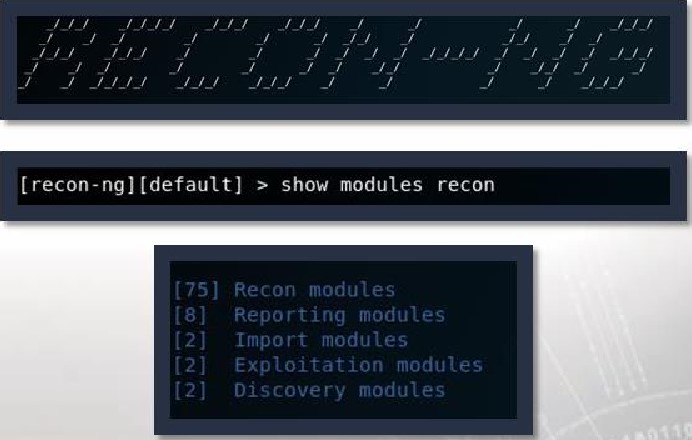
rootv@ka : •d

### theHarvester

Results for Pepsi.com

* 92 total hosts found in search engines
* 68 hosts with IP's
* 13 virtual hosts
* 1 1 'empty' (no IP's)
* 0 emails

### 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

• 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 | Hashes.org |
| • | BuiltWith | IP Info Database |
|  | Censys | Jigsaw |
|  | FliCkr | Shodan |
|  | FullContact | AmlPwned |
|  | Github | Twitter |

* Google (CSE)

### Recon-ng

Use 'search google' for a tool, such as google-related modules: googl and google\_site web

[recon•ng] [detaultl seat-eh google Searching for .

Use the recon/hostshosts/bing\_ip' module to find several additional IP's

172. 217. 192. 26

Searching Bing for: 192 \_26

NO additional hosts discovered at

74.125.192,2'

searching Bing API 'or: .193.26 No additional hosts discovered at

searching Ging API for: ip:1ji.194.76.äo

No additional hosts discovered at .76.26

74.125.12B .26

Searching Bing for: ip:74.125 .128.26

NO additional hosts discovered

-209. as-an , 26

Searching Bing API for: 85.232.20

No addLtLonaL hosts discovered '299.85 .232. 26

total (1 new) hosts found.

|  |  |
| --- | --- |
|  | Use 'show hosts' to display additional IPS found between Bing & Google searches. |
|  |
|  |

[recon-ng] [default] I bing\_ip] > show hosts

|  |  |
| --- | --- |
| host | ip\_address |
| dcita edu | 1 52,95. 144-5 |
| Lea rn.dcita.edu | 144.202. 134. 162 | |
| dcita edu isd .  , dc edu | 52, 92,253-5 |
| pm.delta.edu | 69.195. 247. 154 |
| train , dci ta , edu | 54 , 228 .28 |

login. dcita.edu devlogin. dcita, edu lea rn . dcita . edu 144.292. 134. 162 | ops . dcita.edu 69. 195. 247 .152 dev . dcita.edu 69,195.247. 151 ouot

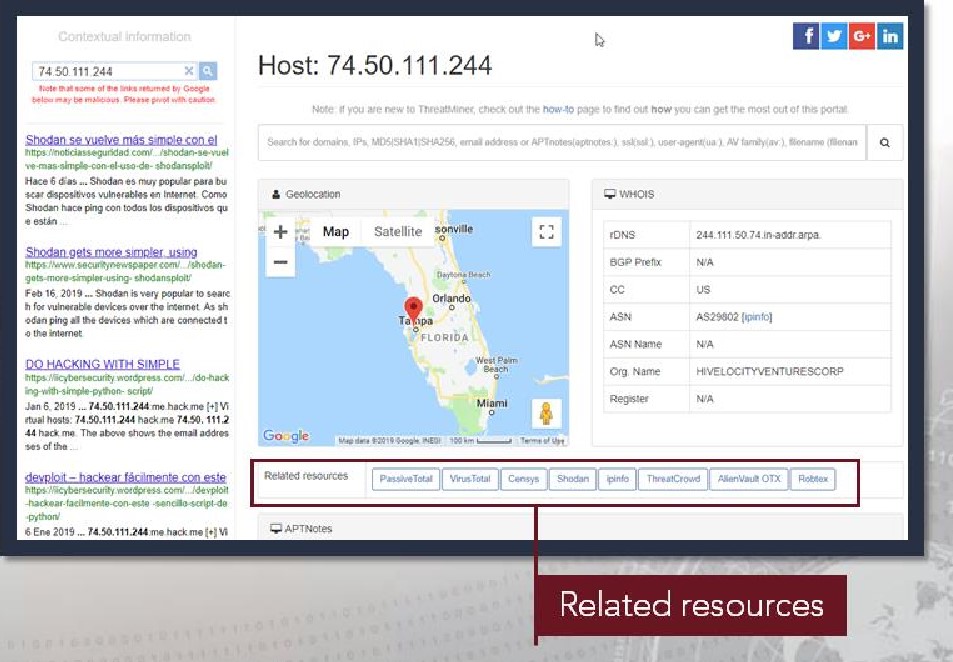
I ALTI.ASPMX.L.GOOCLE.COM I . 217 . 192.26

ALT2. ASPMX.L. GOOGLE . com 74.125. 193.26

ALT3. ASPMX.L. GOOGLE.COM I 173. 194. 76 .26

ALT4. ASPMX.L. GOOGLE . com 74. 125. 128 .26 I ASPMX.L.GOOGLE.COM | 209.85.232.26 wv.•w. dcita edu | 52, 92.253-5

#### ThreatMiner

Pivot directly from an open source research report to:

* PassiveTotal
* VirusTotal
* Censys
* Shodan
* Ipinfo
* ThreatCrowd
* AlientVault O TX
* 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?

Gathering

### Lesson Summary Attack

In this lesson we learned about:

#### • The phases of reconnaissance

* Categories of information
* People
* Infrastructure

#### Open source reconnaissance tools

* Native OS Tools • Metagoofil
* Robtex • theHarvester

##### • Shodan • Recon-ng

• Maltego • ThreatMiner

|  |
| --- |
| End of Module 2, Lesson 1 |