

# Conducting Passive Reconnaissance

- Gather Background Information
- Prepare Background Findings for Next Steps

# Information Gathering



The process of identifying, discovering, and obtaining information that may have relevance to the pen test.

- Covers a variety of tasks, goals, and outcomes.
- Crucial to the success of most pen tests.
- Provides tester with potentially actionable data.
  - Data may shape specific attacks or prompt rethinking of overall strategy.
- Attacking target without gathering info will lead to issues achieving objectives.
  - Can even lead to outright failure.
- Not all gathered info will be useful.
  - Hard to predict what will be relevant.
  - You'll need to identify what data is and is not useful to the test.

# OSINT



**Open source intelligence:** Actionable information that has been gathered from freely and publicly available sources.

- Not something that can be kept private.
- Anyone can obtain this info without breaking laws.
- Valuable to preliminary pen test phases.
  - Skilled attackers want to be as discreet as possible.
- Example sources: Whois registration information; target organization's public site; additional related sites; social media profiles of organization/people; public job postings; Google search results; online blogs, news articles, etc.; and info gathered from DNS, mail records, and SSL/TLS certs.

# Whois (Slide 1 of 2)



A protocol that supports querying of data related to entities who register public domains and other Internet resources.

- Info is available to anyone who queries databases.
- Query can be executed at command line or through a web app.
- Queries typically conducted on public domains to reveal info about them.
- Info such as: Name of registrant; name of organization; mailing address, phone number, email, etc., of organization; administrative and technical contact info; registrar info; domain status; and name servers used by domain.
- A great tool for identifying details about target organization.
  - Use info to take more targeted actions against organization.

# Whois (Slide 2 of 2)

## Contact Information

### Registrant Contact

Name: Sys Admin  
Organization: CompTIA  
Mailing Address: 3500 LACEY Rd  
#100, Downers Grove Illinois  
60515 US  
Phone: +1.6306788300  
Ext:  
Fax:  
Fax Ext:  
Email: Administrator@comptia.org

### Admin Contact

Name: Sys Admin  
Organization: COMPTIA  
Mailing Address: 3500 Lacey Rd  
#100, Downers Grove Illinois  
60515 US  
Phone: +1.6306788304  
Ext:  
Fax:  
Fax Ext:  
Email: administrator@comptia.org

### Tech Contact

Name: Sys Admin  
Organization: COMPTIA  
Mailing Address: 3500 Lacey Rd  
#100, Downers Grove Illinois  
60515 US  
Phone: +1.8886429675  
Ext:  
Fax: +1.5714344620  
Fax Ext:  
Email: administrator@comptia.org

## Registrar

WHOIS Server: whois.godaddy.com  
URL: <http://www.godaddy.com>  
Registrar: GoDaddy.com, LLC  
IANA ID: 146  
Abuse Contact Email: [abuse@godaddy.com](mailto:abuse@godaddy.com)  
Abuse Contact Phone: +1.4806242505

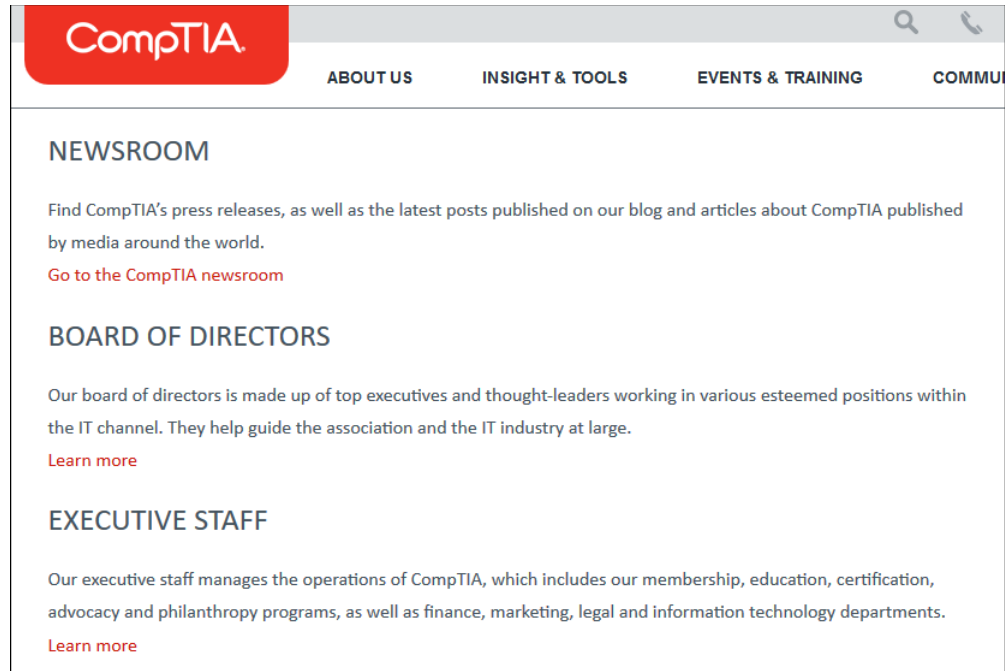
## Status

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>

# The Organization's Website (Slide 1 of 2)

- Marketing sites have the potential to be OSINT.
- Most sites have an "About" page.
  - Reveals purpose, goals, and nature of organization.
  - Even without this page, such info is usually on the site somewhere else.
  - May reveal key info about organization that is useful to pen test.
- Marketing sites provide the following useful info: Executive or other high-profile personnel; upcoming events; forms to fill out for more info; user forums; additional contact info; and links to social media profiles.
- Sites can also be storefronts, informational, etc.
  - Depends on the organization you're targeting.
- Don't expect to learn everything there is from one site.

# The Organization's Website (Slide 2 of 2)





# Related Websites (Slide 1 of 2)

- Other sites can contribute to your OSINT gathering:
  - Secondary sites meant for specific purposes, like B2B operations.
  - Subdomains of primary site, like admin portals.
  - Sites owned/operated by partner organizations.
  - Sites of target's subsidiaries or parent organization.
  - Social media profiles used extensively by target.
- May provide details beyond primary site.
  - Partner site might reveal info about relationship with target.
  - Example: 2014 breach of Target enabled through third-party HVAC supplier.




## Related Websites (Slide 2 of 2)


Logical Operations


SELECT LANGUAGE  MENU  [Schedule Consultation](#)

Training is where we help you soar.  
**Courseware. Certifications. CHOICE LMS.**  
Let the learning begin.

[CORPORATE SOLUTIONS](#) [LEARNING CENTER](#) [CERTIFICATIONS](#)



 Get CyberSAFE!  
Securing Assets for End-users →

 CFR is now U.S.  
DoD-8570  
[Read the press release](#) →

# Social Media (Slide 1 of 2)

- Most organizations have some presence on social media.
  - Used as a marketing channel to reach certain audiences in novel ways.
  - Can reveal more about the organization than its primary site.
- Also a rich source of info on individuals.
  - Everyone from executives to rank-and-file employees may have a presence.
  - May be linked to main company profile.
  - May have separate profiles for personal vs. professional life.
  - Can reveal interests, habits, behavior, relationships, etc.
- Examples of useful sites: Twitter, Facebook, LinkedIn, YouTube, Instagram, and Reddit.

# Social Media (Slide 2 of 2)

The screenshot shows the Twitter profile of CompTIA (@CompTIA). The header includes the CompTIA logo and statistics: 18.4K Tweets, 1,173 Following, 34K Followers, 3,276 Likes, and 18 Lists. A 'Follow' button is in the top right. The profile bio states: 'The world's leading technology association, CompTIA is building the foundation for technology's future.' It also lists the location as Illinois, USA, the website as comptia.org, and the join date as July 2008. Below the bio are links to broadcasts and a photo/video gallery showing 3,431 items. The main tweet area shows a tweet from 50 minutes ago about a workforce report, with a link to bit.ly/2IO15cD. The tweet features a graphic with two panels: an orange panel with a magnifying glass over '40%' and the text 'of U.S. IT firms are ACTIVELY RECRUITING', and a purple panel with a money bag icon and '\$112,890'. The right sidebar contains a 'New to Twitter?' sign-up prompt and a 'You may also like' section with recommendations for Professor Messer, CompTIA EMEA, and Creating IT Futures.

**CompTIA**

@CompTIA

The world's leading technology association, CompTIA is building the foundation for technology's future.

📍 Illinois, USA

🌐 [comptia.org](https://comptia.org)

📺 [View broadcasts](#)

📅 Joined July 2008

🖼️ 3,431 Photos and videos

**Tweets** **Tweets & replies** **Media**

**CompTIA** @CompTIA · 50m

In the digital age, one of the most critical resources is talent. Check out how there is a growing demand for tech talent through our workforce report. #NAWDConf [bit.ly/2IO15cD](https://bit.ly/2IO15cD)

**40%**  
of U.S. IT firms are  
ACTIVELY RECRUITING

**\$112,890**

**New to Twitter?**  
Sign up now to get your own personalized timeline!

**Sign up**

**You may also like** · Refresh

**Professor Messer**  
@ProfessorMesser

**CompTIA EMEA**  
@CompTIA\_EMEA

**Creating IT Futures**  
@createITfutures

# Job Boards (Slide 1 of 2)

- Job posts may reveal info about personnel structure, technical environments, etc.
- Employer needs to entice and provide enough info to prospective applicants.
- Amount and type of info given is dependent on industry and job.
  - Network admin position for a tech company might reveal more than a sales associate.
- Actionable info found on job boards:
  - Personnel makeup of departments/teams.
  - Lack of qualified personnel in crucial roles.
  - Level of technical sophistication.
  - Software architecture used.
  - Programming languages used.
  - Hardware used.
  - Network and security system used.

# Job Boards (Slide 2 of 2)

The screenshot displays a job board interface. At the top, there are filter tabs: 'Title', 'Location', 'Date posted', 'Type', 'Company type', and 'Employer'. Below these, a row of job category buttons includes 'All', 'Program analyst', 'Manager', 'Technical operations', 'Mechanical engineer', 'Operations', 'Operations analyst', 'Program coordinator', 'Instructor', 'Management analyst', 'Network engineer', and 'System administrator'. The 'All' button is selected.

On the left side, a list of job postings is shown. The first three are for 'Technical Operations Intern' at 'CompTIA, Inc.' in 'Downers Grove, IL', posted '6 days ago' via 'Glassdoor'. The fourth is for 'Technical Operations Intern' at 'CompTIA' in 'Downers Grove, IL', posted '5 days ago' via 'LinkedIn' and marked as an 'Internship'. The fifth is for 'Technical Operations Intern' at 'CompTIA, Inc.' in 'Downers Grove, IL', posted '5 days ago' via 'ZipRecruiter' and marked as an 'Internship'. The sixth is for 'Manager, Marketing' at 'CompTIA, Inc.' in 'Downers Grove, IL', posted '5 days ago' via 'Glassdoor'.

The right side shows a detailed view of the 'Technical Operations Intern' position. It includes the company logo and name, a 'SAVE' button, and an 'Apply' section with buttons for 'Glassdoor' and 'CareerBuilder'. Below this, it states '6 days ago' and provides a description: 'CompTIA is currently recruiting for a Technical Operations Intern. This position provides technical support and assists the Sr. Technical Operations Manager with issues related to CompTIA Learning products.' It also lists 'Essential Duties and Responsibilities' with two bullet points: 'Provides technical support of CompTIA Learning platforms.' and 'Provides tier 2 technical support of the learning platform and escalates issues to learning platform vendor or Sr. Technical Operations Manager as necessary.'

# Google Hacking (Slide 1 of 2)



The process of using the Google search engine to identify potential security weaknesses in publicly available sources.

- Not "hacking" in the strictest sense.
- Enables you to extract more info than from a typical search.
- Typically includes special search operators to provide more focused results.

Operator	Searches	Example
<b>site</b>	A specific site.	<code>site:comptia.org report</code>
<b>link</b>	For pages that link to the specified page.	<code>link:comptia.org report</code>
<b>filetype</b>	For specific file types.	<code>filetype:pdf report</code>
<b>intitle</b>	For page titles.	<code>intitle:Certification report</code>
<b>inurl</b>	For URLs.	<code>inurl:Certification report</code>
<b>inanchor</b>	For anchor text.	<code>inanchor:Certification report</code>

# Google Hacking (Slide 2 of 2)

- True power of Google hacking comes in combining operations.
- Example:
  - `site:comptia.org filetype:pdf OR filetype:docx intitle:Certification report`
    - Searches CompTIA website for PDF/DOCX files with title "Certification" and whose contents include "report".
- Enables you to focus search on exact info you're looking for.
  - Helps you avoid manually separating the signal from the noise.

# Online Articles and News (Slide 1 of 2)

- Can provide insight into target organization.
- Larger businesses are featured by mainstream news outlets.
  - News might report on new major services.
  - Financial publications may focus on fiscal performance.
  - News may report on unethical practices.
- Smaller businesses issue press releases.
  - Can be published on own website or on PR-specialized sites.
  - Can reveal how business changes and what this means for operations.
  - Example: PR on acquisitions that affects people, products, and technology.
- Won't always reveal everything you need to know.
- Should be used in conjunction with other OSINT.
  - Helps to fill in the bigger picture.



# Online Articles and News (Slide 2 of 2)

## CompTIA Sets Out to Create New Paradigms in Tech Training



Acquires award-winning learning resources firm gtslearning

Purchases comprehensive CompTIA certification content portfolio from Logical Operations

Launches CompTIA Official Content strategy

NEWS PROVIDED BY

CompTIA →

Mar 29, 2018, 09:15 ET

SHARE THIS ARTICLE



DOWNERS GROVE, Ill., March 29, 2018 /PRNewswire-USNewswire/ -- [CompTIA](#), the leading trade association for the information technology (IT) industry, today announced the completion of two acquisitions to expand its commitment to the high-tech workforce by providing new cutting-edge skills training, learning content and resources, assessments, and verification solutions.

# DNS Querying (Slide 1 of 2)

- Queries for name resolution info can reveal target's network structure.
- Standard queries identify IP address associated with domain name.
  - Might be a useful entry point or vector for more recon.
- Advanced queries retrieve additional DNS records.
  - MX, NS, TXT, etc.
  - Can reveal additional targets.
  - Example: Services revealed through SRV records.
- Querying tools include several web apps, `nslookup` and `dig` (Linux).
- Tools can also perform reverse lookups.
- Zone transfer can reveal even more info.
  - Improperly configured servers enable transfer to untrusted domains.
  - Can enumerate which hosts are accessible from the Internet.

# DNS Querying (Slide 2 of 2)

## A records

	Name	Address	Type	Class	TTL
#1	comptia.org	198.134.5.6	A	IN	60 (1 min)

## MX records

	Preference	Exchange	Name	Type	Class	TTL
#1	10	comptia-org.mail.protection.outlook.com	comptia.org	MX	IN	60 (1 min)

## NS records

	Nsd name	Name	Type	Class	TTL
#1	ns1.comptia.org	comptia.org	NS	IN	60 (1 min)
#2	ns2.comptia.org	comptia.org	NS	IN	60 (1 min)

# Email

- One of the most useful elements of contact info.
- The main point of contact for most organizations.
- Often a vector for soliciting info or conducting social engineering.
- Email addresses are also commonly used as account names.
  - Focus on gaining access.
- Enumerating email-based DNS records is also useful.
- MX records identify which server handles incoming mail.
  - Compromising server means compromising lines of communication.
- SPF validates incoming mail from a domain is coming from trusted IP address.
  - Mitigates email spoofing in spam, phishing, etc.
  - Presence of SPF may prompt you to adjust your tactics.

```
;; ANSWER SECTION:
comptia.org.      59      IN      TXT      "3EcCv2jIS7drI/TCUMslTod5prhLauj
8f4QUoGGtMYpAoR1fzs298ejgJptHnKnJdjKTdg4mxDFnc3ZyXGpvw=="
comptia.org.      59      IN      TXT      "MS=ms77029986"
comptia.org.      59      IN      TXT      "v=spf1 a mx ptr ip4:198.134.5.0
/24 ms=ms77029986 3eccv2jis7dri/tcumsltod5prhlauj8f4quoggtmypaoor1fzs298ejgjpthn
knjdjkt dg4mxd fnc3zyxg pvw== include:mail.zendesk.com include:informz.net ?all"
```

# SSL/TLS Certificates (Slide 1 of 2)

- Certs used in SSL/TLS can inform your pen test actions.
- SANs can identify specific subdomains the cert applies to.
  - Can also identify other domains, IP addresses, and email addresses.
  - Alleviates need to purchase/use multiple certs.
  - Can provide you with new targets.
- Some certs use a wildcard (\*) to denote all subdomains.
  - Can make it harder to identify specific subdomains.
- CT framework publishes CA issuer logs.
  - Contain info about domains/subdomains certs apply to.
  - Can help you discover subdomains covered by cert in the past.
  - Example: Organization used to have SANs, but now uses wildcard.

# SSL/TLS Certificates (Slide 2 of 2)

Subject	Issuer	# DNS names	Valid from	Valid to	# CT logs	
*.comptia.org	Go Daddy Secure Certificate Authority - G2	2	Aug 11, 2015	Aug 11, 2018	5	<a href="#">See details</a>
accessedge.dr.comptia.org	DigiCert SHA2 Secure Server CA	19	Jan 19, 2016	Jan 24, 2019	1	<a href="#">See details</a>
augusta.comptia.org	DigiCert SHA2 Secure Server CA	19	Jan 19, 2016	Jan 24, 2019	6	<a href="#">See details</a>
*.comptia.org	RapidSSL SHA256 CA	2	Jul 18, 2016	Jul 19, 2019	5	<a href="#">See details</a>
accessedge.comptia.org	DigiCert SHA2 Secure Server CA	19	Jan 19, 2016	Jan 24, 2019	1	<a href="#">See details</a>
*.comptia.org	RapidSSL SHA256 CA	2	Jul 18, 2016	Jul 19, 2019	4	<a href="#">See details</a>
*.comptia.org	DigiCert SHA2 Secure Server CA	2	Nov 15, 2017	Jan 23, 2020	1	<a href="#">See details</a>
*.comptia.org	RapidSSL RSA CA 2018	2	Jan 2, 2018	Jan 3, 2020	3	<a href="#">See details</a>

# Shodan (Slide 1 of 2)

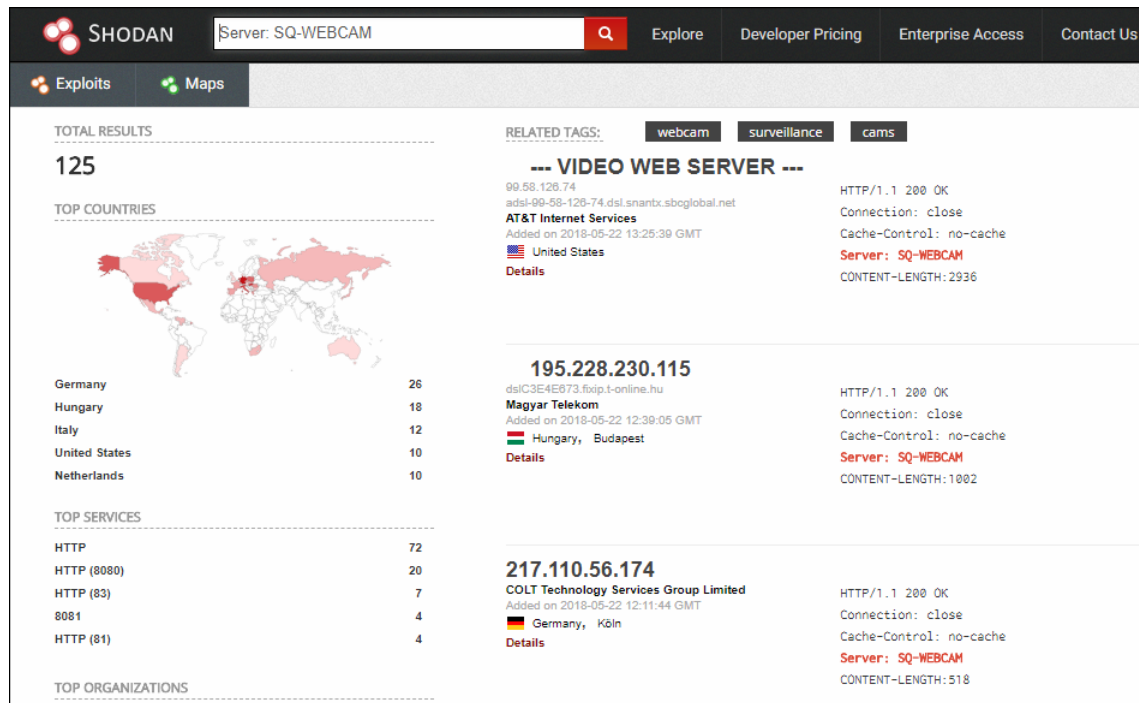


A search engine that enables anyone to connect to public or improperly secured devices that allow remote access through the Internet.

- Example: Zoo sets up an IP camera for anyone to watch the animals.
- Shodan indexes the connection and allows anyone to search for it.
  - Does this by banner grabbing through ports.
- Most devices are improperly secured, or not secured at all.
  - Exposes them to the wider world.
  - User may not even be aware.
  - Example: IP camera has default credentials and is connected to the Internet.

# Shodan (Slide 2 of 2)

- Can also index ICSs, traffic lights, and many more IoT devices.
  - IoT devices are notoriously insecure.
  - Some systems allow full remote access.
- Can be useful to a pen tester in numerous ways.
  - Example: Live feed of office's premises to inform a physical test.
  - Example: Finding accessible HVAC controllers.





# theHarvester (Slide 1 of 2)



An open source OSINT tool that gathers several different types of background information on a target.

- Gathers subdomain names, employee names, email addresses, PGP key entries, and open ports and service banners.
- Uses general search engines like Google and Bing.
- Uses Comodo cert search.
- Searches social media sites like Twitter and LinkedIn.
- Uses Shodan for service banners.
- Tool is simple, yet effective for automating OSINT gathering.

## theHarvester (Slide 2 of 2)

```
root@kali00:~# theharvester -d compitia.org -b linkedin

*****
*                                                                 *
* | |_|_|_|_|_/_/_/_/\_/_\_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_\_*
* | |_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_*
* | |_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_*
* \_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_*
*                                                                 *
* TheHarvester Ver. 2.7                                         *
* Coded by Christian Martorella                                 *
* Edge-Security Research                                        *
* cmartorella@edge-security.com                                *
*****

[-] Searching in Linkedin..
    Searching 100 results..
Users from Linkedin:
=====
R [REDACTED]
J [REDACTED]
J [REDACTED]
T [REDACTED] - Instructor - [REDACTED]
```

# Recon-ng



A command-line open source tool for gathering OSINT data.

- Similar in function to theHarvester, but more robust.
- Includes dozens of modules.
  - Each module runs a specific type of query.
  - You can set options for each query.
- Example modules:
  - Whois query
  - Email address search in HIBP
  - PGP key search
  - Social media profiles
  - File crawler
  - DNS record enumerator

```
-----
COMPTIA.ORG
-----
[*] URL: http://whois.arin.net/rest/pocs;domain=comptia.org
[*] URL: http://whois.arin.net/rest/poc/COMPT34-ARIN
[*] [contact] <blank> COMPTIA Administrator (administrator@comptia.org) - Whois
contact
[*] URL: http://whois.arin.net/rest/poc/[redacted]-ARIN
[*] [contact] [redacted] ([redacted]@comptia.org) - Whois contact
[*] URL: http://whois.arin.net/rest/poc/[redacted]-ARIN
[*] [contact] [redacted] ([redacted]@comptia.org) - Whois contact
[*] URL: http://whois.arin.net/rest/poc/[redacted]-ARIN
[*] [contact] [redacted] ([redacted]@comptia.org) - Whois contact
-----
SUMMARY
-----
[*] 4 total (4 new) contacts found.
```

# Maltego (Slide 1 of 3)



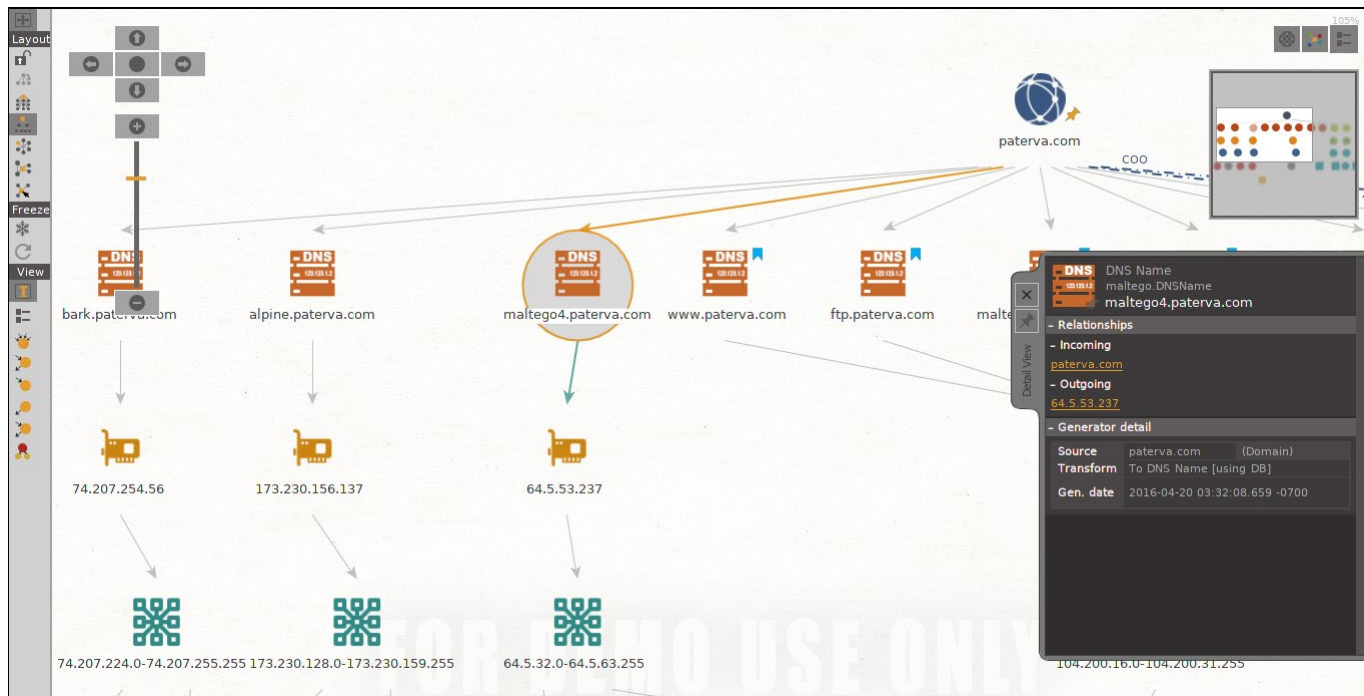
A graphical OSINT tool that can gather a wide variety of information on public resources.

- Features OSINT objects graphically and with links to other objects.
- Helps you visualize OSINT relationships; includes transforms that automate querying.
- Example transform enumeration:
  - People/company names, numbers, and addresses
  - Network blocks
  - Email addresses
  - External links
  - DNS records
  - Subdomains
  - Downloadable files
  - Social media profiles

## Maltego (Slide 2 of 3)

- Query results are placed in node graphs with links between nodes.
- Example: Running transform on a domain.
  - Domain is placed at top of tree hierarchy.
  - Several branching links to resources under domain; e.g., subdomains.
  - More resources branch out from these; e.g., IP addresses.
  - People-oriented transforms show contact info as branches.
- More than just hierarchical layouts.
  - Circular, block, organic, etc.
- Proprietary software with several editions.
- Maltego CE is free.
  - Requires registration to access limited subset of transforms.

# Maltego (Slide 3 of 3)



# FOCA (Slide 1 of 2)



**Fingerprinting Organizations with Collected Archives:** A GUI OSINT tool that discovers metadata that may be hidden within documents.

- Documents typically downloaded from the web.
- Can work with a variety of document types like Office, OpenDocument, etc.
- Can work with PDFs and some graphical design types like SVGs.
- Uses search engines like Google to identify files.
  - You can also provide your own local files.
- Extracts useful metadata like:
  - Names
  - Software/OS versions
  - Printer info
  - Plaintext passwords

# FOCA (Slide 2 of 2)

- Functionality has expanded to include general OSINT queries like DNS/IP address.
- Has a plugin architecture to extend functionality.
- Windows only.

My Project - FOCA Open Source 3.4

Project Plugins Options TaskList About

My Project

- Network
  - Clients (0)
  - Servers (0)
  - Unlocated Servers
- Domains
  - Metadata
- Documents (7/131)
  - doc (2)
  - pdf (3)
    - eams-senate-letter2a7d24c
    - fedvtetraining-v5.pdf
    - impact-of-comptia-certifi
  - ppbx (1)
  - Unknown (1)
- Metadata Summary
- Users (5)
- Folders (0)
- Printers (0)
- Software (0)
- Emails (0)
- Operating Systems (0)
- Passwords (0)

Search engines: ☒ Google ☐ Bing ☐ Duck Duck

Extensions: ☒ doc ☒ xls ☒ ppt ☒ docx ☒ pps ☒ pptx

Search All

Id	Type	URL	Download	Download Date	Size	Analy
7		http://staging-www.comptia.org/communities/resources/...	✗	-	-	✗
8	docx	http://staging-certification.comptia.org/docs/default-sour...	✗	-	-	✗
9	docx	http://staging-certification.comptia.org/docs/default-sour...	✗	-	-	✗
10	docx	https://www.comptia.org/docs/default-source/sitedocu...	✗	-	-	✗
11	docx	https://www.comptia.org/docs/default-source/event-do...	✗	-	-	✗
12	docx	http://staging-www.comptia.org/docs/default-source/ev...	✗	-	-	✗
13	docx	http://staging-www.comptia.org/docs/default-source/ev...	✗	-	-	✗
14	docx	http://get.certification.comptia.org/rs/112-HIL-492/imag...	✗	-	-	✗
15		https://www.comptia.org/communities/resources/teleco...	•	05/22/2018 13:23:55	8.4 MB	•
16	ppbx	https://partners.comptia.org/docs/default-source/events...	•	05/22/2018 13:22:26	7.42 MB	•
17	ppbx	http://staging-www.comptia.org/docs/default-source/co...	✗	-	-	✗

Time	Source	Severity	Message

Conf Deactivate AutoScroll Clear Save log to File



# Guidelines for Gathering Background Information

## (Slide 1 of 2)

- Understand that not all gathered info will be useful.
- Understand the difference between OSINT and closed-source intelligence.
- Recognize which sources provide OSINT and which do not.
- Perform Whois queries to obtain registration info.
- Examine organization's main site for personnel and business info.
- Look for related sites to corroborate or expand your OSINT.
- Look over social media profiles for revealing info.
- Search job boards for personnel issues or technology info.
- Conduct Google hacking to run advanced queries on websites.
- Examine news articles to stay up-to-date on target's business operations.

# Guidelines for Gathering Background Information

## (Slide 2 of 2)

- Query DNS to obtain domain/subdomain info and additional network info.
- Leverage improperly configured servers for zone transfer.
- Identify email addresses that may be used as account logins.
- Identify domain's use of MX/SPF records.
- Identify SANs in certs to discover subdomains.
- Search through CT logs for past cert issuances.
- Use Shodan to discover IoT and similar devices.
- Use theHarvester/Recon-ng to perform OSINT techniques from the command line.
- Use Maltego to visualize connections between OSINT objects.
- Use FOCA to extract metadata from downloadable files.

# Findings Analysis and Weaponization



**Weaponization:** The process of turning passive recon results into directions or launch points for active recon and preliminary attacks.

- Ensures more overt phases are influenced by previous actions.
  - Prevents them from being isolated and missing out on key info.
  - Can enhance their effectiveness.
- Analyze findings for content of interest.
  - Depends on context like test scope and target's business.
  - Consider findings in a bigger picture, not a vacuum.
  - Combine info and consider how it pertains to the environment.
- Separate signal from the noise.
  - Determine what results are useful and what should be discarded.
  - Failure may impede the test or lead your weaponization astray.

# Content of Interest

- IP addresses and subdomains.
- External and third-party domains/sites.
- Key personnel and contact info.
- Info that facilitates social engineering tests.
- Info that reveals specific technologies.

# IP Addresses and Subdomains (Slide 1 of 2)

- IP addresses gained from OSINT will usually be public ranges.
  - Used by organizations to communicate to outside world.
- You can leverage public IP addresses through active scanning.
  - Discover services, ports, OS info, etc.
- Most hosts accessible through public addresses are meant to be public facing.
  - Web servers, FTP servers, mail servers, etc.
  - Doesn't include domain controllers and other private resources.
- Also leverage public IP addresses as entry points into the private network.

# IP Addresses and Subdomains (Slide 2 of 2)

- OSINT may also expose private IP addresses.
  - Example: Leaked network documents published on a site.
  - Helps you focus later scans on specific addresses.
- You can also focus on subdomains.
  - Example: **intranet.example.tld** should be further investigated.
  - Also tie IP addresses to subdomains.

# External and Third-Party Sites

- Perform OSINT on partner, contractor, or other related sites.
  - Can expand knowledge of target organization.
- How you proceed will depend on scope and actionable info.
  - You may be prohibited from taking next steps against a third party.
  - Not necessarily in scope, as they have not agreed to take part.
  - Even if authorized, the info may not be actionable.
- Many other types of third-party sites.
  - Any site not owned by target organization.
- Example: Glassdoor.com.
  - Employees review companies and management.
  - Reviews may reveal info about people, processes, and technology.
  - Organization has no control over site, yet it can still aid the pen test.

# People (Slide 1 of 2)

- How you leverage people info depends on several factors:
  - Role they play in the organization.
  - Day-to-day responsibilities.
  - Teams and departments they work with.
  - Business identification details like email addresses and phone numbers.
  - Technical aptitude.
  - Mindsets and perspectives.



# People (Slide 2 of 2)

- Example scenarios:
  - Gathering info on an executive from organization's website.
    - Prepare info to use in a spear phishing attack.
  - Discovering social media profiles with personal details of a financial employee.
    - Use this in your password cracking wordlist.
  - Discovering disgruntled Facebook posts about network admin's negligent employees.
    - Focus your tests on finding weaknesses that exist because of negligence.
- Some people useful to the pen test may not work with the organization.
  - Friends, family, customers, etc.

# Social Engineering (Slide 1 of 2)



The practice of deceiving people into giving away access to unauthorized parties or enabling those parties to compromise sensitive assets.

- Targets are unaware of the trick.
- Commonly used by attackers because of how effective it can be.
  - People naturally trust others.
  - Attackers exploit this trust.
- Next logical step after gathering people-based OSINT.
  - Data says a lot about a person's life.
  - Why launch a technical attack when you can trick someone to get the same result?
  - Saves on time, effort, and risk.

# Social Engineering (Slide 2 of 2)

- Targets many different people and job roles.
  - Financial personnel are common targets.
  - Executives/managers are also common targets.
- Test scope may prohibit social engineering.
  - Raises ethical issues.

# Technologies

- OSINT tools can reveal technologies an organization is built with.
- Technology info can prepare you to exploit specific scenarios.
- A web server running Apache may prompt you to focus on Linux as a target.
- Some technologies indicate a reliance on a particular vendor.
  - Public resources use that vendor; why not its private resources as well?
  - Web server running on IIS might indicate the presence of an AD environment.
- Leveraging technology info requires research into vulnerabilities.
  - Vendors often issue alerts for security issues with products.
  - Use to hone your later scans.
- Technology info can also indicate strong defenses.
  - Up-to-date technology may prompt you to rule it out as a target or vector.
  - Focus instead on other, less well-protected technology.

# Preparation for Next Steps (Slide 1 of 2)

- Record your findings and conclusions in a document.
- Refer back to this document whenever necessary.
- Choose whichever document format you're most comfortable with.
  - Example: Spreadsheet with rows for each finding and columns for next steps.
- Make sure to define what "next steps" means to your test.
  - Could dive straight into active recon like port scanning and enumeration.
  - Could decide to start social engineering instead.
  - Could also decide to conduct physical pen tests.
- Direction you take depends on:
  - The test's scope.
  - Your findings.
  - Your own personal assessment of the situation.

# Preparation for Next Steps (Slide 2 of 2)

13					
14	Start	Asset	Test	Findings/Results	Next Test
15					
16	Whois	greenecityphysicians.com IP address	nmap scan	TCP ports 80 and 443 open	Vuln scan
				Discovery of restricted area Successfully cloned RFID badge Discovery of Wi-Fi SSID Discovery of networked medical devices with OS and default credentials	Try badge after hours
17	Google Maps/Google Earth	physical site information	physical reconnaissance		
18	Social media/job board	GCPG IT skills weakness			
19	Email harvesting	list of email addresses	phishing campaign	several user credentials harvested	
				Windows Server 2016 192.168.1.50 is running: IIS, FTP, Telnet, SMB, RPC, POP3, IMAP, SMTP	Arachni web app scan
20	Google hacking	BxB public website potential weakness	Windows Server vuln scan		
		Unaware users			
21	GCPG IT skills weakness	Reduced IT resources	USB booting	Ported documents to internal user computers	

# Guidelines for Preparing Background Findings for Next Steps (Slide 1 of 2)

- Clearly determine what "next steps" means for your test.
- Analyze findings to determine how to weaponize them in the future.
- Consider findings within a bigger picture, not in a vacuum.
- Discard irrelevant findings and focus on actionable findings.
- Determine how public IP addresses map to public resources you can target.
- Consider how public IP addresses might be useful as entry points.
- Determine which subdomains may be worth targeting.

# Guidelines for Preparing Background Findings for Next Steps (Slide 2 of 2)

- Leverage info from third-party sites about an organization and its people.
- Consider how people info can shape later testing.
- Leverage people info in conducting social engineering.
- Use gathered technology info to identify potential vulnerabilities.
- Consider that a target organization might rely on a specific technology vendor.
- Record findings and next steps in a document for easy reference.



# Reflective Questions

1. What types of OSINT do you believe would be the most valuable to your pen tests?
2. What types of OSINT tools do you or would you prefer to use, and why?

