CompTIA

CompTIA PenTest+

Exam PT0-002

CompTIA PenTest+ Exam PT0-002

Lesson 3

Footprinting and Gathering Intelligence

Objectives

- Given a scenario, perform passive reconnaissance.
- Given a scenario, perform active reconnaissance.
- Given a scenario, analyze the results of a reconnaissance exercise.
- Explain use cases of the following tools during the phases of a penetration test.

Lesson 3

Topic 3A

Discover the Target

Gather Information

- Footprinting and reconnaissance involves identifying and obtaining information that is essential to the success of the PenTest
  - Search for key contacts, information, and technical data by combing through sources that includes online articles, social media, and press releases
- The details can provide a better understanding of the business operations and reputation of the target organization.
- Once obtained, the findings will help the team to better assess the target and evaluate possible attack vectors.

Record the Findings

- To preserve the data, the team can create a spreadsheet:
  - Include details such as asset, test, along with findings and results

Start	Asset	Test	Findings	Next Test
Whois	Greencityphysicians.com IP address	Nmap scan	TCP ports 80 and 443 open	Vuln scan
Email harvesting	List of email addresses	Phishing campaign	Several user credentials harvested	
Google hacking	BXB public website potential weakness	Windows Server vuln scan	Windows Server 2016 running: IIS, FTP, Telnet POP3	Arachni web app scan

Identify Organizational Details

- Scraping social media can be a rich resource of data about an employee's interests, behavior, relationships, and other PII.
- Public job boards such as CareerBuilder and Monster give the candidate information on open positions.
  - The description can reveal information about the organization

Examine DNS Information

- An organization’s IP address might be useful as an entry point into the network, or as a vector for performing more reconnaissance.
- An advanced DNS query can retrieve more information than just an IP address.
- For example, you can also identify individual DNS records for a particular domain, such as the following:
  - **Mail Exchange (MX)** record
  - **Nameserver (NS)** record
  - **Service (SRV)** record

Review Activity: Discover the Target

- Outline ways footprinting and reconnaissance can reveal information about the target
- List sites that can provide information on the company
- Describe how public job boards can reveal information about the organization
- Discuss how DNS information can provide additional information on the target

Lesson 3

Topic 3B

Gather Essential Data

Use Public Source Code Repositories

- There are dozens of source code repository hosts available for code sharing and collaboration:
  - GitHub, Bitbucket and SourceForge
- Along with the convenience of the repositories, comes risks.
  - Developers can upload private files, screenshots or comments that can contain useful intelligence and information
  - In addition, exposed code can be modified which can lead to an infrastructure attack or shut down systems

Google Hacking

- Uses Google search engines to identify security weaknesses in publicly available sources, such as an organization's website.
- Queries include a special search operator to focus on specific types of desired information that include:
  - **site** - A specific site
  - **filetype** - Specific file types.
  - **inurl** - Uniform resource locator (URL)
- The true power of Google hacking is in combining multiple operations into a single query.

Unearthing Archived Websites

- Webpages are updated, moved, or deleted
  - Information you found before might not be available.
- To obtain older website information, you can use a couple of different methods:
  1. Use a standard cache search on a site to see a recent view of the website.
  2. Do an archived search using the Wayback Machine
  3. Use a web cache viewer browser extension

Searching for Images and Interesting Data

- Searching images is another avenue the team can use when scouting the target to see if there is any actionable intel.
  - Sites that offer reverse image search include TinEye, Google and Bing.
- All image search engines work in a similar manner:
  - Either enter a URL or upload an image, and the search engine will hunt for all similar images and then present the results.
- Another option the team can use is Google Alerts.
  - Google will monitor the web for new content, and notify you if found

Review Activity: Gather Essential Data

- Explain the risks of using public source code repositories
- List ways the team can use Google search engines to identify security weaknesses in publicly available sources
- Discuss ways the team can obtain older website information during reconnaissance
- Describe how to search for images and interesting data

Lesson 3

Topic 3C

Compile Website Information

Evaluating the Website

- The goal is to identify vulnerabilities to launch various attacks:
  - Cross site scripting (XSS), SQL Injection (SQLi) , Web caching poisoning
- Numerous tools and techniques are available
  - Tools include browsers, Nmap, Metasploit, and DirBuster.
  - Techniques such as forced browsing and OSINT tools such as Maltego
- Identifying the type of technology as well as version information, will better prepare the team to exploit specific scenarios.

Extending Your Reach

- In addition to testing the main site, the team may be tasked to examine the target's partners, consultants, and contractors’ sites
  - This can reveal serous vulnerabilities within the supply chain.
- Other potential sites that might reveal actionable information:
  - Subdomains of primary sites that aren't directly linked or easily visible
  - Websites owned and/or operated by partner organizations
  - Websites of the target organization's subsidiaries; or, conversely, the target's parent organization.

Evaluating the robots.txt File

- Web crawlers search source code on a webpage to learn about the structure, and possibly find interesting information.

- One way to control *where* they search and more importantly, where NOT to search, is by using a robots.txt file

- If not written properly, the robots.txt can be a security risk.

- The team should examine the structure of the robots.txt file, to ensure that it has proper encoding to restrict access when searching

Recognizing Certificate Flaws

- SSL/TLS uses digital certificates to validate the identity of the web server and exchange cryptographic keys.

- Certificates used in SSL/TLS communications are another public resource that can aid in the PenTest process.

  - Vulnerability scanners can gather and validate certificate information to see if they are properly signed and secure.

  - Discovering out-of-date certificates often point to other administrative or support issues that can be exploited.

Discovering Certificate Details

- One of the more useful fields in a digital certificate is the SAN
  - Can identify specific subdomains that can be covered by the certificate.
- If found, any SANs listed can then be evaluated by the team:
  - **Common name**: *.comptia.org
  - **SANs:** *.comptia.org, comptia.org
- Some certificates simply use a wildcard (*) character to denote that all subdomains of the parent domain are covered by the certificate.
  - If used, you might not be able to identify any specific resources.

Using the Certificate Transparency Framework

- Logs of public CAs are published for anyone to access.
  - Contain information about the certificates for domains and subdomains issued by a CA.
- The framework can enable you to discover subdomains no longer covered by the certificate yet still exist.
- For example, an organization might have used a specific SAN in the past but later moved to a wildcard.
  - The past domain might still be listed in the CT logs

Revoking the Certificate

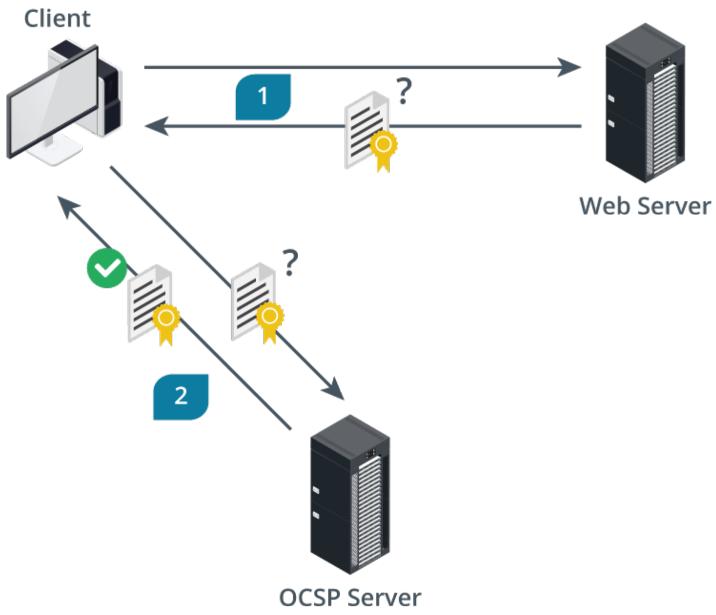
- All web browsers have a list of CAs and information on whether a certificate is valid, invalidated or revoked.
- When beginning a transaction, the status of the certificate is checked by using one of two methods:
  - The **Certification Revocation List** (**CRL**) - a list of certificates that in some way have been deemed invalid.
  - The **Online Certificate Status Protocol** (**OCSP**) newer way to check the validity of the certificate.

Standard OCSP Process

- When a client goes to a web server to initiate a transaction, the following occurs:

1. The web server sends the client the certificate.

2. The *client* goes to the OCSP server to check the validity of the certificate.

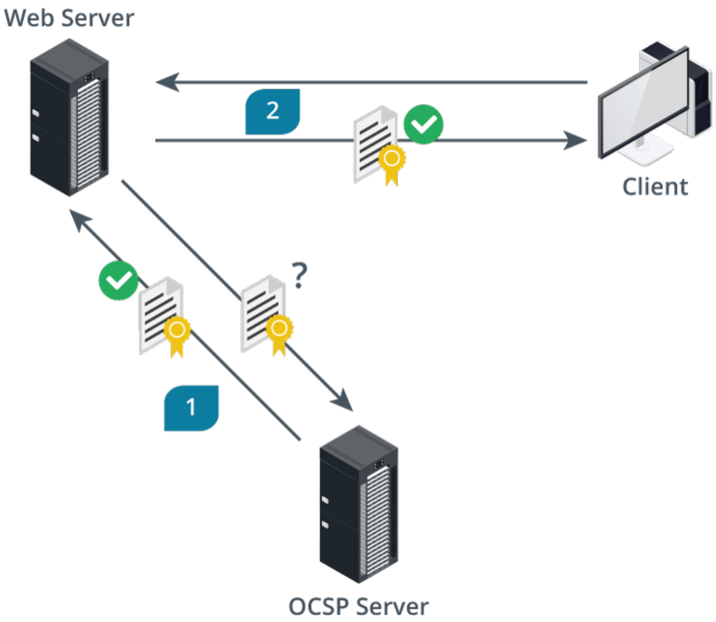


Stapling the Certificate

- Stapling reverses this burden, so the web server validates the certificate

  1. The *web server* goes to the OCSP server to check the validity of the certificate

  2. The web server then sends the validated certificate to the client.



Review Activity: Compile Website Information

- Explain the value of enumerating a website
- Describe why the team may be asked to examine the target's partners, consultants, and contractors’ sites
- Explain the significance of the robots.txt file
- Describe the importance of testing the SSL/TLS certificate
- Explain how the team can use the CT Framework
- Compare the standard OCSP process with stapling the certificate

Lab Activity

Assisted Lab: Exploring the Domain Tools: Nslookup, Dig and Whois

- Lab types
  - Assisted labs guide you step-by-step through tasks
  - Applied labs set goals with limited guidance
- Complete lab
  - Submit all items for grading and check each progress box
  - Select “Grade Lab” from final page
- Save lab
  - Select the hamburger menu and select “Save”
  - Save up to two labs in progress for up to 7 days
- Cancel lab without grading
  - Select the hamburger menu and select “End”

Lesson 3

Topic 3D

Discover Open-Source Intelligence Tools

Open-source Intelligence Tools (OSINT)

- Using OSINT is critical to the preliminary phases of a PenTest
- Used during the reconnaissance phase to gather information from freely and publicly available sources, for a more targeted discovery.
- Allows the team to discreetly gather information on the target without signaling any flags.

Searching Metadata

- Metadata is information stored or recorded as a property of an object, state of a system, or transaction.
    - Metadata entries can expose sensitive information.
- Two tools that aid in the discovery of metadata are Metagoofil and Fingerprinting Organizations with Collected Archives (FOCA).

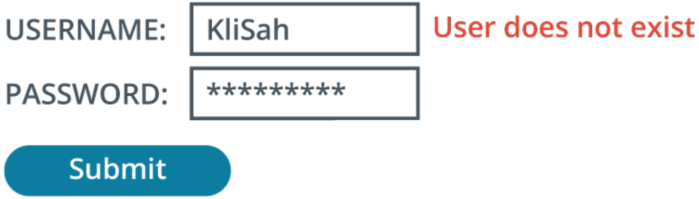
Searching Metadata with Metagoofil

- Metagoofil scrapes metadata, such as the author, company, title, and subject, from public documents on the target website(s)
- The output is then displayed in a standard browser using HTML
- When searching, commands will control the type of data:
  - Using **-d comptia.org** will scan for documents on Comptia.org
  - Using **-t pdf** will scan for pdf documents
  - Using **-l 75** will search for 75 documents

Fingerprinting with FOCA

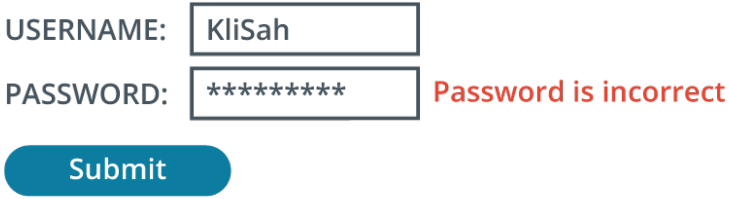
- A GUI tool used to discover metadata that may be hidden within documents, typically those downloaded from the web.
- Can work with a variety of document types
    - MS Office along with the OpenDocument format
    - PDFs and graphical design file types (SVG)
- Some of the useful metadata FOCA can extract includes:
    - User and people names, software and OS version information, printer information, and plaintext passwords

Monitoring Responses on a Login Page



USERNAME: KliSah User does not exist

PASSWORD: *********



USERNAME: KliSah

PASSWORD: ********* Password is incorrect

If prompt returns "User does not exist," this verifies the username is not in the database

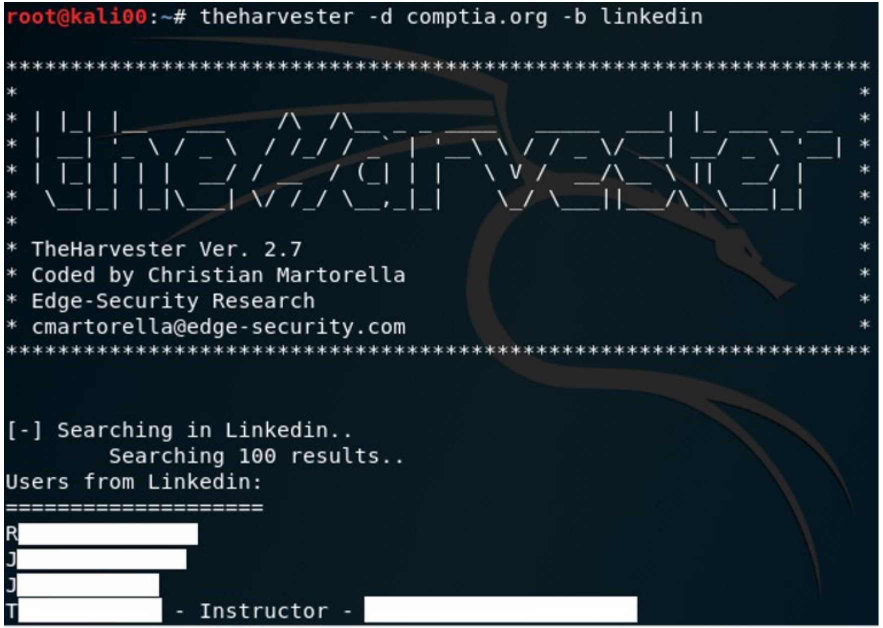
If prompt returns "Password is incorrect," this verifies the username is in the database

Collecting Data with theHarvester

- Can automate the information gathering tasks by using:
  - Google and Bing to gather information from public data sources.
  - Comodo's certificate search engine to obtain certificate information.
  - Social media sites like Twitter and LinkedIn.
  - Banner grabbing functionality using Shodan.
- theHarvester gathers information on the following:
  - Subdomain names, Employee names, Email addresses
  - PGP key entries, Open ports and service banners

Gathering Data

- When using theHarvester, enter the target domain and the data source.
- The data can be used in an exploit, such as a Spearphishing attack.



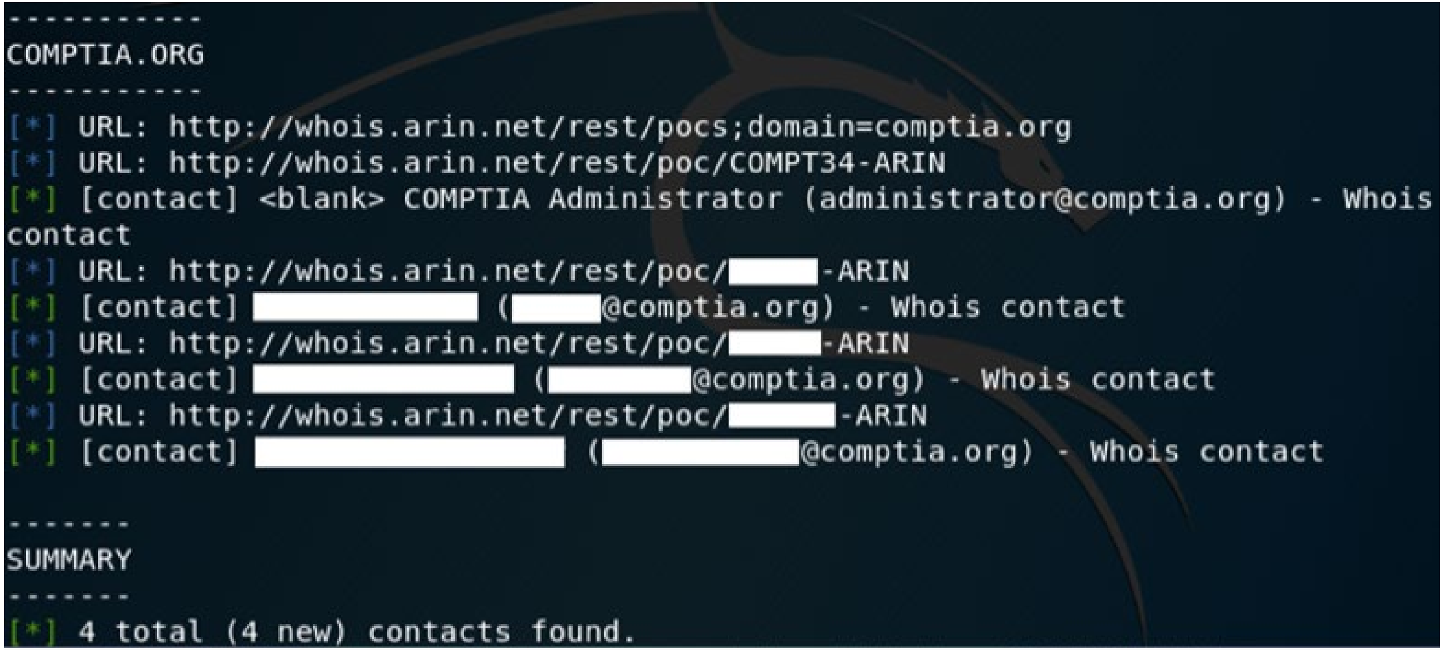
```
root@kali00:~# theharvester -d comptia.org -b linkedin

*******************************************************************
*                                                                 *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __| '_ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* 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]
```

Gathering with Recon-ng

- Recon-ng uses various modules to customize the search:
  - Whois query to identify points of contact
  - PGP key search
  - File crawler.
  - Social media profile associations.
  - DNS record enumerator
  - Check if the account has been associated with a breach.

Presenting the Information

- Enter the query and Recon-ng will then display the information:

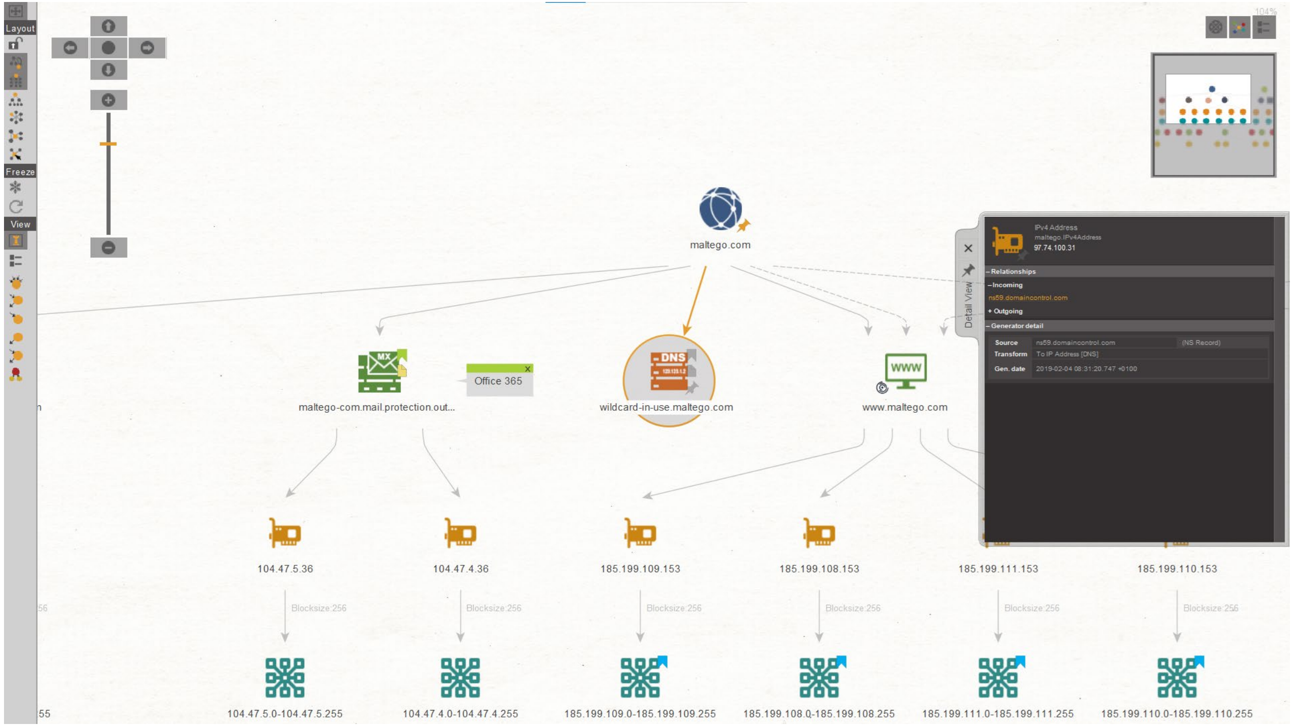


```
-----------
COMPTIA.ORG
-----------
[*] URL: http://whois.arin.net/rest/pocs;domain=comptia.org
[*] URL: http://whois.arin.net/rest/poc/COMPT34-ARIN
[*] [contact] <blank> COMPTIA Administrator (administrator@comptia.org) - Whois
contact
[*] URL: http://whois.arin.net/rest/poc/[redacted]-ARIN
[*]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

Transforming Data with Maltego

- Maltego is an OSINT tool that can gather a wide variety of information on public resources.
    - Uses a GUI to help users visualize the gathered information using an extensive library of "transforms"
    - Gathers Individual's names and physical addresses, phone numbers and email addresses and external links
    - Compares the data with other sets of information to provide commonalities among the sources.
- The results of the query are then placed in node graphs, and then links are established between each node.

Viewing a Maltego Graph



IPv4 Address
maltego.IPv4Address
97.74.100.31

– Relationships

–Incoming

ns59.domaincontrol.com

+ Outgoing

– Generator detail

Source	ns59.domaincontrol.com	(NS Record)
Transform	To IP Address [DNS]	
Gen. date	2019-02-04 08:31:20.747 +0100	

Searching with Shodan

- Shodan is a search engine designed to locate and index IoT devices that are connected to the Internet.
- Traffic lights, industrial control systems (ICSs), and other devices that have Internet connectivity and are part of the IoT.
- Shodan can be useful to the PenTest reconnaissance phase :
  - The team can locate the feed of a security camera outside the target organization’s office to get a better picture of the premises and its defenses.
  - If the target organization employs control systems, the team may be able to manipulate these remotely as part of the attack phase.

Review Activity: Discover Open-Source Intelligence Tools

- Recall how the team can use OSINT tools during the PenTest
- Explain how the team can use Metagoofil and FOCA
- List ways theHarvester can automate information gathering
- Review how Recon-ng uses modules to customize a search
- Outline the benefits of using Maltego to gather information on public resources.
- Describe how Shodan can locate and index IoT devices

Lab Activity

Assisted Lab: Navigating Open-Source Intelligence Tools

- Lab types
  - Assisted labs guide you step-by-step through tasks
  - Applied labs set goals with limited guidance
- Complete lab
  - Submit all items for grading and check each progress box
  - Select “Grade Lab” from final page
- Save lab
  - Select the hamburger menu and select “Save”
  - Save up to two labs in progress for up to 7 days
- Cancel lab without grading
  - Select the hamburger menu and select “End”

Lesson 3

Summary