Certified Ethical Hacker

Cybersecurity

Certification Prep Day 3

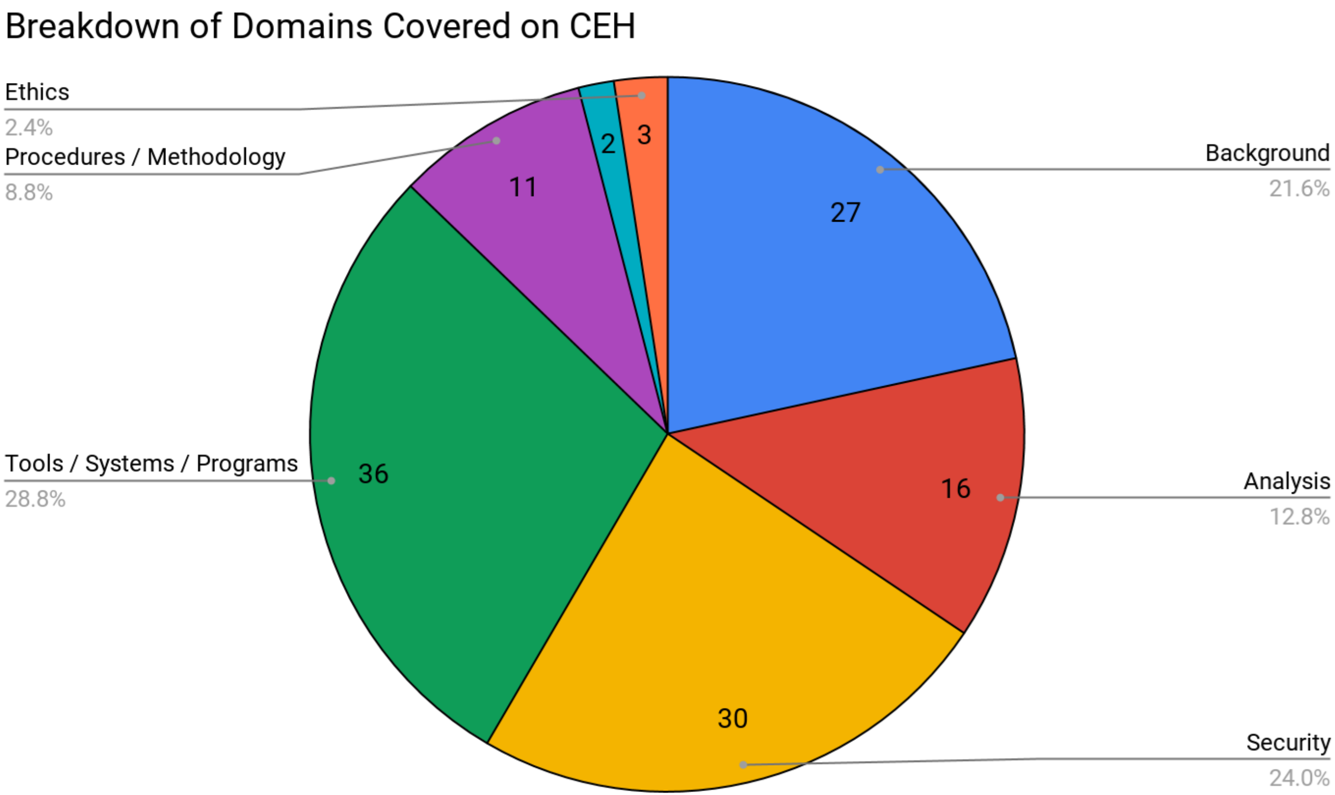
Class Objectives

By the end of class today, students will be able to:

- □ Describe the themes and topics covered in the CEH **Background and Technical Foundations** domain.
- □ Explain how traceroute determine routing paths.
- □ Differentiate between a TCP split handshake and TCP three-way handshake.

CEH Topics Breakdown

1. Background
2. Analysis / Assessment
3. Security
4. Tools/ Systems/ Programs
5. Procedures/ Methodology
6. Regulations / Policy
7. Ethics



Activity: Warm-Up Quiz

In this activity, you will work on a quiz that covers topics from each domain that we will cover in today's lesson.

Instructions sent via Slack.

Suggested Time:
10 Minutes

Times Up! Let’s Review.

Warm-Up Quiz

Warm-Up Review

1. What is the program that would monitor every keystroke that the victim enters?

- □ Sniffer
- □ Virus
- □ Keylogger
- □ Smurf

Warm-Up Review

1. What is the program that would monitor every keystroke that the victim enters?

- □ Sniffer
- □ Virus
- □ **Keylogger**
- □ Smurf

Warm-Up Review

2. What is a worm? Choose the most correct definition:

- □ It is a form of eavesdropping between two network devices, involving spoofed packets.
- □ It’s a type of DoS attack used to gain access or shutdown remote servers by overflowing them with random packets.
- □ It’s when malware is file-binded into applications or media files.
- □ It’s a self-replicating form of malware.

Warm-Up Review

2. What is a worm? Choose the most correct definition:

- □ It is a form of eavesdropping between two network devices, involving spoofed packets.
- □ It’s a type of DoS attack used to gain access or shutdown remote servers by overflowing them with random packets.
- □ It’s when malware is file-binded into applications or media files.
- □ **It’s a self-replicating form of malware.**

Warm-Up Review

3. Which of the following is a software that steals and sends people's private info?

- ☐ Ransomware
- ☐ Spyware
- ☐ Worms
- ☐ Zombies

Warm-Up Review

3. Which of the following is a software that steals and sends people’s private info?

- □ Ransomware
- □ **Spyware**
- □ Worms
- □ Zombies

Warm-Up Review

4. True or False: Trojans are so effective is because the hacker is able to change the signature and avoid detection.

Warm-Up Review

4. True or False: Trojans are so effective is because the hacker is able to change the signature and avoid detection.

TRUE

Warm-Up Review

5. Which of the following changes their signatures every time they replicate?

- □ Ransomware
- □ Spyware
- □ Polymorphic Viruses
- □ Zombies

Warm-Up Review

5. Which of the following changes their signatures every time they replicate?

- □ Ransomware
- □ Spyware
- □ **Polymorphic Viruses**
- □ Zombies

Warm-Up Review

6. In order to take control early in the boot process, some viruses reside in the:

- □ Memory
- □ Boot sector
- □ Flash drive
- □ Hard drive

Warm-Up Review

6. In order to take control early in the boot process, some viruses reside in the:

- □ Memory
- □ **Boot sector**
- □ Flash drive
- □ Hard drive

Warm-Up Review

7. Which of the following is not a type of malware?

□ Worms

□ Spyware

□ Ransomware

□ Bugs

Warm-Up Review

7. Which of the following is not a type of malware?

- □ Worms
- □ Spyware
- □ Ransomware
- □ **Bugs**

Warm-Up Review

8. Between viruses and worms, which are capable of spreading on their own, without the user having to interact with it?

Warm-Up Review

8. Between viruses and worms, which are capable of spreading on their own, without the user having to interact with it?

Worms

Warm-Up Review

9. Which of the following best describes a rootkit?

- ☐ It’s malware that uses social engineering techniques.
- ☐ It’s malware that intercepts packets in transit without being stored onto a target machine.
- ☐ It’s malware that propagates without a specific target.
- ☐ It’s a type of malware that is used to backdoor a target machine while attempting to remain hidden.

Warm-Up Review

9. Which of the following best describes a rootkit?

- □ It’s malware that uses social engineering techniques.
- □ It’s malware that intercepts packets in transit without being stored onto a target machine.
- □ It’s malware that propagates without a specific target.
- □ **It’s a type of malware that is used to backdoor a target machine while attempting to remain hidden.**

Warm-Up Review

10. Which of the following used to list all of the shared resources on a remote host?

- □ Netstat
- □ Net view
- □ Network
- □ Netcat

Warm-Up Review

10. Which of the following used to list all of the shared resources on a remote host?

- □ Netstat
- □ **Net view**
- □ Network
- □ Netcat

Warm-Up Review

11. What does SNMP stand for?

☐ Sender Null Modulation Protocol

☐ Service Net Modulation Protocol

☐ Simple Network Management Protocol

☐ Simplified Node Management Protocol

Warm-Up Review

11. What does SNMP stand for?

- □ Sender Null Modulation Protocol
- □ Service Net Modulation Protocol
- □ **Simple Network Management Protocol**
- □ Simplified Node Management Protocol

Warm-Up Review

12. Which argument will be used for OS detection in Nmap?

- □ -G
- □ -L
- □ -S
- □ -O

Warm-Up Review

12. Which argument will be used for OS detection in Nmap?

- □ -G
- □ -L
- □ -S
- □ **-O**

Warm-Up Review

13. A Null session is when someone connects with:

☐ Username: admin, password:blank

☐ Username: root, password: root

☐ No username or password

☐ Username: random , password: blank

Warm-Up Review

13. A Null session is when someone connects with:

□ Username: admin, password:blank

□ Username: root, password: root

□ **No username or password**

□ Username: random , password: blank

Warm-Up Review

14. What will the following nmap command accomplish?

NMAP -sS -O -p 123,153 192.168.100.4

- □ A stealth scan, opening port 123 and 153
- □ A stealth scan, determine the operating system and scanning of ports 123 and 153
- □ A stealth scan checking all open ports excluding ports 123 and 153

Warm-Up Review

14. What will the following nmap command accomplish?

NMAP -sS -O -p 123,153 192.168.100.4

- □ A stealth scan, opening port 123 and 153
- □ **A stealth scan, determine the operating system and scanning of ports 123 and 153**
- □ A stealth scan checking all open ports excluding ports 123 and 153

Warm-Up Review

15. What will the following nmap command accomplish?

NMAP -sS -O -p 123-153 192.168.100.4

- □ A stealth scan, determine the operating system and scanning of ports 123 through 153
- □ A TCP-connect scan, determine the operating system and scanning of ports 123 and 153
- □ A stealth scan checking all open ports excluding ports 123 and 153
- □ A SYN scan, opening ports 123 and 153

Warm-Up Review

15. What will the following nmap command accomplish?

NMAP -sS -O -p 123-153 192.168.100.4

- □ **A stealth scan, determine the operating system and scanning of ports 123 through 153**
- □ A TCP-connect scan, determine the operating system and scanning of ports 123 and 153
- □ A stealth scan checking all open ports excluding ports 123 and 153
- □ A SYN scan, opening ports 123 and 153

Warm-Up Review

16. What best describes banner grabbing?

☐ It is used to map a web server.

☐ It is used to remove banner ads from web pages.

☐ It is used to acquire embedded scripting from web pages.

☐ It is used to acquire HTML source code.

Warm-Up Review

16. What best describes banner grabbing?

- □ **It is used to map a web server.**
- □ It is used to remove banner ads from web pages.
- □ It is used to acquire embedded scripting from web pages.
- □ It is used to acquire HTML source code.

Warm-Up Review

17. An Nmap scan of a server shows port 25 is open. Which of the following describes the risk of leaving that port open?

- □ Web portal data leak
- □ Clear text authentication
- □ Open printer sharing
- □ Active mail relay

Warm-Up Review

17. An Nmap scan of a server shows port 25 is open. Which of the following describes the risk of leaving that port open?

- □ Web portal data leak
- □ Clear text authentication
- □ Open printer sharing
- □ **Active mail relay**

Warm-Up Review

18. Regarding port enumeration, which port does DNS zone transfer use?

- □ UDP port 161
- □ TCP / UDP port 389
- □ TCP port 137
- □ TCP port 53

Warm-Up Review

18. Regarding port enumeration, which port does DNS zone transfer use?

□ UDP port 161

□ TCP / UDP port 389

□ TCP port 137

□ **TCP port 53**

Warm-Up Review

19. Which of the following refers to “reverse-engineering” rules that are implemented on a firewall, based on the results of port scans?

- □ Firewalking
- □ Firewalling
- □ Firechalking
- □ Firescaling

Warm-Up Review

19. Which of the following refers to “reverse-engineering” rules that are implemented on a firewall, based on the results of port scans?

□ **Firewalking**

□ Firewalling

□ Firechalking

□ Firescaling

Warm-Up Review

20. You are sent to scan a remote host using nmap. Which of the following scan types is the best choice to gather the most information while minimizing the chance of detection?

- □ TCP connect scan (-sT)
- □ Xmas scan (-sX)
- □ UDP scan (-sU)
- □ SYN scan (-sS)

Warm-Up Review

20. You are sent to scan a remote host using nmap. Which of the following scan types is the best choice to gather the most information while minimizing the chance of detection?

- □ TCP connect scan (-sT)
- □ Xmas scan (-sX)
- □ UDP scan (-sU)
- □ **SYN scan (-sS)**

Warm-Up Review

21. You are asked to access a server at a particular IP address. The server does not respond to ping requests, what could be the reason? (Select all that apply)

- □ The host is down.
- □ Server configured not to respond to ping.
- □ Firewall blocks TCP.
- □ Firewall blocks ICMP.

Warm-Up Review

21. You are asked to access a server at a particular IP address. The server does not respond to ping requests, what could be the reason? (Select all that apply)

- □ **The host is down.**
- □ **Server configured not to respond to ping.**
- □ Firewall blocks TCP.
- □ **Firewall blocks ICMP.**

Warm-Up Review

22. Which command would you issue to scan all TCP ports on 192.168.1.1?

- □ nmap -p 0, 65535 192.168.1.1
- □ nmap -p 1,65536 192.168.1.1
- □ nmap -p 192.168.1.1
- □ nmap -p 0-65535 192.168.1.1

Warm-Up Review

22. Which command would you issue to scan all TCP ports on 192.168.1.1?

- □ nmap -p 0, 65535 192.168.1.1
- □ nmap -p 1,65536 192.168.1.1
- □ nmap -p 192.168.1.1
- □ **nmap -p 0-65535 192.168.1.1**

Warm-Up Review

23. Which of the following nmap arguments are used to perform a Null scan:

- □ -sS
- □ -sP
- □ -sN
- □ -sF

Warm-Up Review

23. Which of the following nmap arguments are used to perform a Null scan:

- □ -sS
- □ -sP
- □ **-sN**
- □ -sF

Warm-Up Review

24. Which argument would you use to perform a Fin Scan in nmap?

- □ -SF
- □ -fs
- □ -sF
- □ -FIN

Warm-Up Review

24. Which argument would you use to perform a Fin Scan in nmap?

- □ -SF
- □ -fs
- □ **-sF**
- □ -FIN

Warm-Up Review

25. Most scan attempts can be detected and flagged by:

- □ Proxy
- □ IDS
- □ Router
- □ Switch

Warm-Up Review

25. Most scan attempts can be detected and flagged by:

□ Proxy

□ **IDS**

□ Router

□ Switch

Warm-Up Review

26. Which of these scan types in nmap would make a full TCP connection to the target system?

- □ XMAS scan
- □ TCP connect scan
- □ All of these
- □ SYN stealth scan

Warm-Up Review

26. Which of these scan types in nmap would make a full TCP connection to the target system?

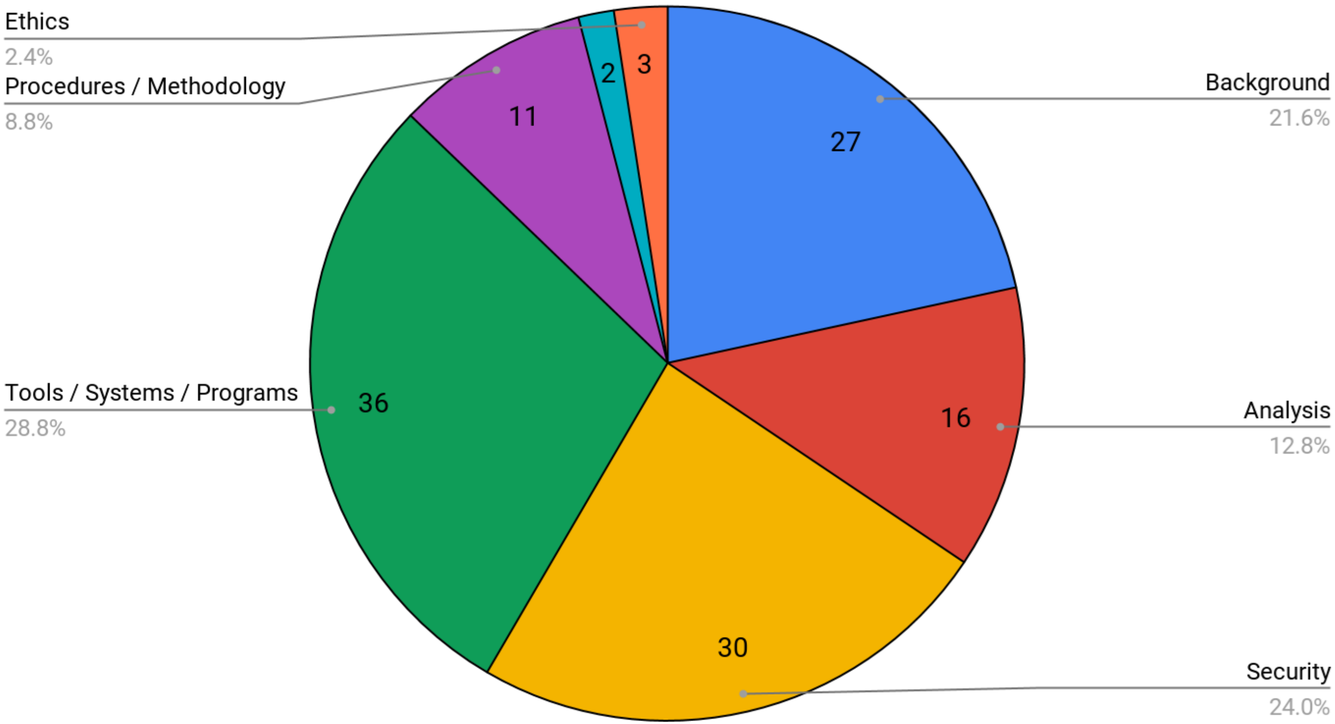
- □ XMAS scan
- □ **TCP connect scan**
- □ All of these
- □ SYN stealth scan

Footprinting, Scanning, and Enumeration

CEH Topics Breakdown

1. Background
2. Analysis / Assessment
3. **Security**
4. **Tools/ Systems/ Programs**
5. Procedures/ Methodology
6. Regulations / Policy
7. Ethics

Breakdown of Domains Covered on CEH



Security and Tools/Systems/Programs Domain

Scanning and Enumeration topics are covered in the Security and Tools Systems Programs domains of the CEH exam.

- Security domain accounts for **24%** of the exam.
- Tools/Systems/Programs makes up **28.8%** of the exam.

In our review of these domains, we will cover the following:

- The Hacking Process / Attack Cycle
- Network Protocols
- Common Types of Scanning and Enumeration

The Hacking Cycle: Information Gathering

During the Information Gathering phase, pentesters begin researching their targets.

What type of information do pentesters collect?

The Hacking Cycle: Information Gathering

During the Information Gathering phase, pentesters begin researching their targets.

What type of information do pentesters collect?

- **Open Source Intelligence**
  - Publicly available information about the target that is obtains via social media, websites, freely available public records, etc.
- **DNS Enumeration**
  - Given a target domain, https://vulnerable.com, attackers will often try to enumeration subdomains such as https://admin.vulnerable.com, https://api.vulnerable.com,
- **Network Reconnaissance:**
  - Tasks include Host Discovery, port scanning and service fingerprinting.

Information Gathering: Network Reconnaissance

Network Reconnaissance consists of:

- Identifying live hosts on a network,
- Scanning them for open ports;
- Determining which service each machine exposes;
- Generating a map / profile of the target.

The CEH exam includes many questions about recon tools **whois**, **nslookup** and **Nmap**.

The exam also focuses on these steps of the reconnaissance process:

- Determining Network Ranges
- Host Discovery
- Port Scanning (Finding Open Ports)
- Service Fingerprinting
- Network Mapping

DNS Enumeration

DNS is the protocol that translates domain names into IP addresses

A domain can have subdomains:

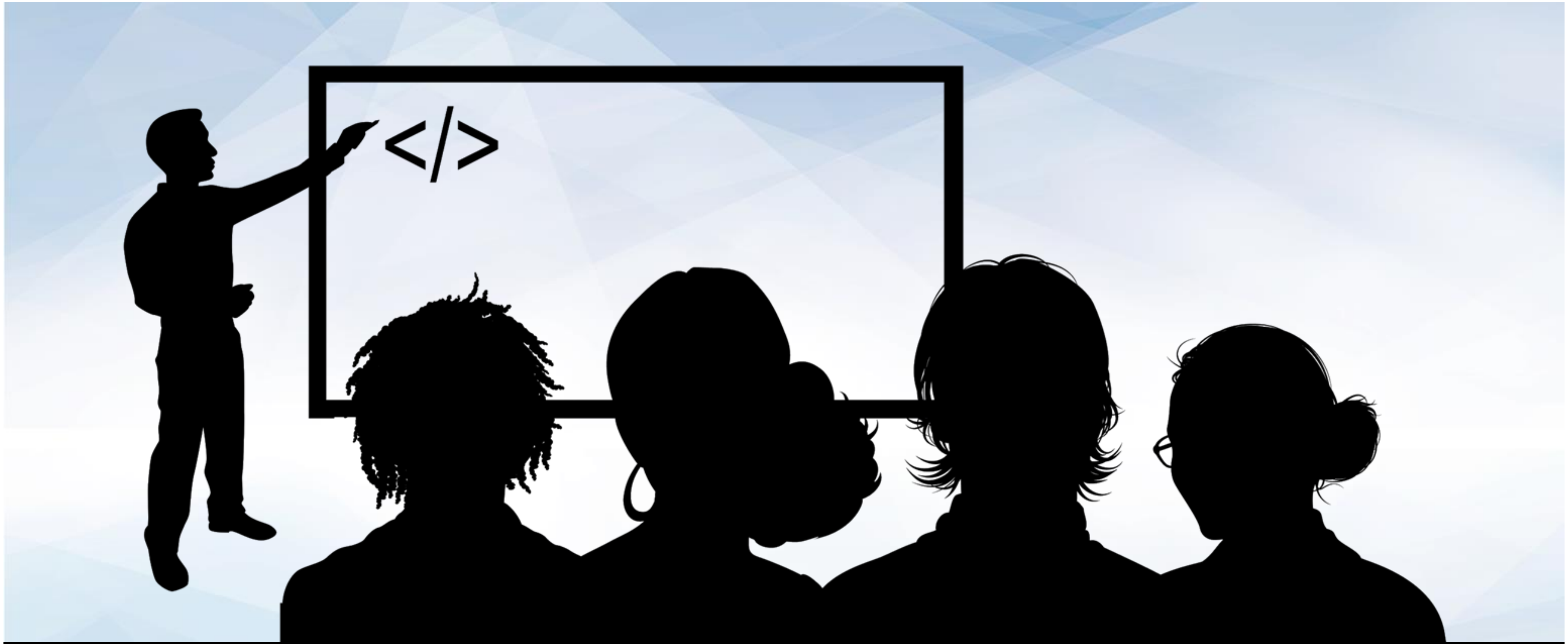
- Domain: https://vulnerable.com
- Sub domains: https://**admin.**vulnerable.com , https://**api.**vulnerable.com

Each subdomain provides a specific service and is typically associated with different machines.

Domains and subdomains typically have different IP addresses, but will belong to the same **range** of addresses.

A **name server** is responsible for remembering which IP address is associated with each domain name.

- Name servers usually named as https://**ns1**.vulnerable.com, https://**ns2**.vulnerable.com.



Instructor Demonstration

DNS Lookup Demo

DNS Lookup Demo

nslookup google.com

```
$ nslookup google.com
Server:                 192.168.1.1
Address:192.168.1.1#53

Non-authoritative answer:
Name:    google.com
  Address: 172.217.10.110
```

- nslookup sends a DNS request to the local network's default gateway (192.168.1.1)
- The gateway forwards the DNS request to Google's nameservers.
- Google's nameserver responds with the IP address of google.com
- 172.217.10.110 is the IP address for google.com.

DNS Lookup Demo

nslookup fake.google.com

```
$ nslookup fake.google.com
  Server:             192.168.1.1
  Address:            192.168.1.1#53


  ** server can't find fake.google.com: NXDOMAIN
```

This reveals fake.google.com is not in use.

Netblocks and ARIN

Public IP addresses such as 172.217.10.110 (google.com) belong to ranges of IP addresses.

- Both of the previously demoed Google subdomains belong to the range 172.217.10.0-255

Thes IP ranges are sometimes called **netblocks**.

Info on which netblocks belong to which domain names is managed by a group called **American Registry for Internet Numbers** (ARIN) and stored in detailed databases.

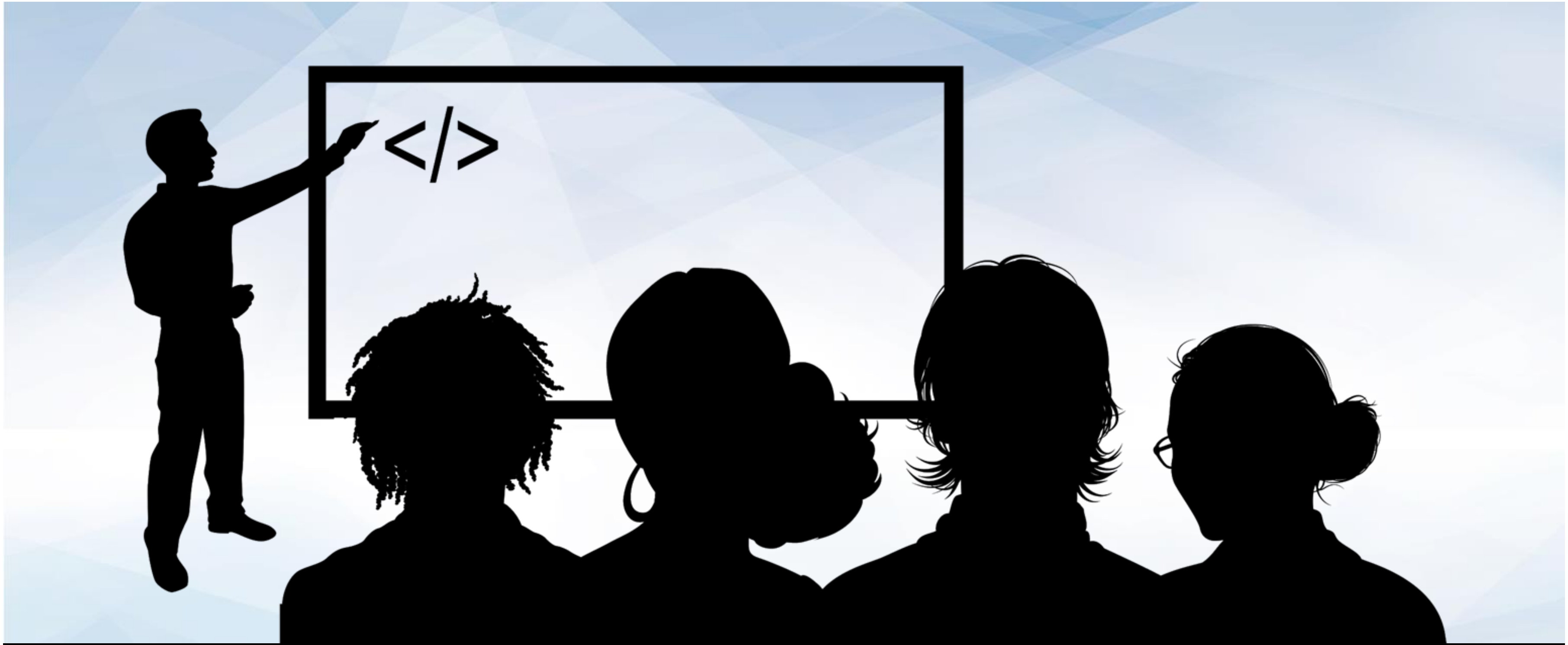
- Information from ARIN can be very useful for attackers who are entering engagements without much information about their targets.

DNS Process

DNS enumeration is typically performed via either **brute force** or **zone transfer**.

DNS enumeration workflow:

1. Determine the target netrange and name server addresses.
2. Query the nameserver for list of all subdomains (**zone transfer).**
3. If the zone transfer fails, request the IP addresses of subdomains, such as ftp.google.com, and keep track of which subdomains exist. (**brute-force**)
4. If the brute-force doesn't yield useful results, attempt to scan the entire net range with Nmap.



Instructor Demonstration

ARIN whois and Zone Transfer

ARIN whois and Zone Transfers

We can query the ARIN database from the command line with a whois-a

```
$ nslookup google.com
Server:                         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
Name:           google.com
Address: 172.217.12.174

$ whois -a 172.217.12.174
...

NetRange:       172.217.0.0 - 172.217.255.255
CIDR:           172.217.0.0/16
NetName:        GOOGLE
...
Name Server: NS1.GOOGLE.COM
Name Server: NS2.GOOGLE.COM
Name Server: NS3.GOOGLE.COM
Name Server: NS4.GOOGLE.COM
. . .
```

`nslookup google.com` retrieves the IP address of google.com, which is `172.217.12.174`.

`whois -a 172.217.12.174` retrieves a wealth of information about `google.com`.

- NetRange, CIDR, and the name server entries.

The Name Server fields list the domain names for Google's DNS servers.

- These are the servers your machine sends DNS requests to.
- There are multiple nameservers so DNS will work even if one or even two of the name servers go down.

ARIN whois and Zone Transfers

Next, we’ll determine which IP address in that range are up and running. These IP addresses correspond to potential targets for the attacker.

- A **zone transfers** is a special type of DNS request that causes a target nameserver to send back a full list of all the subdomains and IP addresses it knows.

- Most nameservers are configured to not allow zone transfers, but some administrators forget. So, it's always worth trying a zone transfer before relying on brute-force.

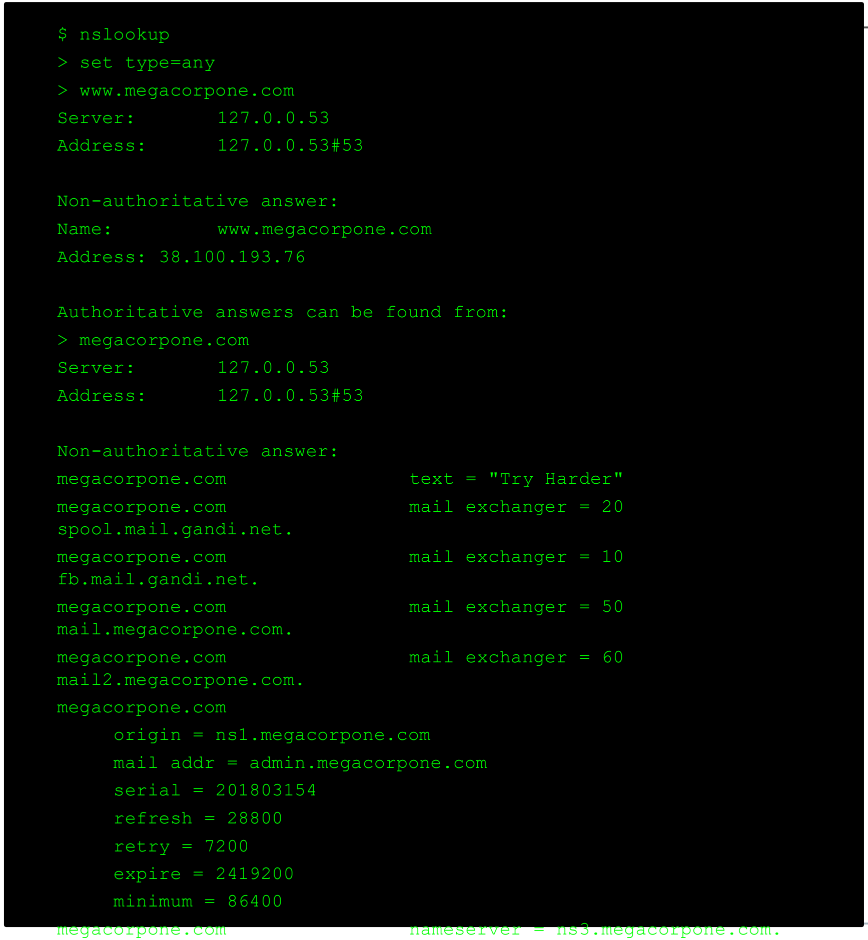
ARIN whois and Zone Transfers

We can query the ARIN database from the command line with a whois-a

```
$ nslookup

> server ns1.google.com

Default server: ns1.google.com

Address: 216.239.32.10#53

> set type=any

> www.google.com

Server:                              ns1.google.com

Address:        216.239.32.10#53


*** Can\'t find www.google.com: No answer

 Transfer failed.
```

- nslookup starts nslookup in "interactive mode".
- server ns1.google.com tells nslookup to use ns1.google.com to perform DNS queries
- set type=any tells nslookup to perform a zone transfer. any is the name for DNS zone-transfer requests.
- www.google.com tells nslookup to use ns1.google.com to attempt a zone transfer for www.google.com.
- This request fails because Google is a secure site.

ARIN whois and Zone Transfers



```
$ nslookup
> set type=any
> www.megacorpone.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:           www.megacorpone.com
Address: 38.100.193.76

Authoritative answers can be found from:
> megacorpone.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
megacorpone.com                 text = "Try Harder"
megacorpone.com                 mail exchanger = 20
spool.mail.gandi.net.
megacorpone.com                 mail exchanger = 10
fb.mail.gandi.net.
megacorpone.com                 mail exchanger = 50
mail.megacorpone.com.
megacorpone.com                 mail exchanger = 60
mail2.megacorpone.com.
megacorpone.com
     origin = ns1.megacorpone.com
     mail addr = admin.megacorpone.com
     serial = 201803154
     refresh = 28800
     retry = 7200
     expire = 2419200
     minimum = 86400
megacorpone.com                 nameserver = ns3.megacorpone.com.
megacorpone.com                 nameserver = ns1.megacorpone.com.
```

The following depicts a successful Zone transfer against the fictional MegaCorp One website.

- When successful, attackers can use these subdomains to begin attacking additional targets.

- When zone-transfer does not work, attackers use brute force to figure out which subdomains are available.

DNS Enumeration Tool

Manual DNS enumeration is tedious and time consuming, but there are many tools to help expedite the process:

- **fierce**: A command-line tool for DNS enumeration, available by default on Kali Linux.
- **dnsrecon**: Also a command-line tool for DNS enumeration, available by default on Kali Linux.
- Netcraft Search Engine: A website that automatically lists known subdomains associated with a given domain.
- Netcraft has the following advantages over command-line tools:
  - **Stealth**: Using Netcraft allows you to enumerate subdomains without putting traffic onto the network yourself.
  - **Information Density**: Netcraft collects information from a wide variety of sources.

Activity: DNS Enumeration

In this activity, you will perform DNS enumeration against Mega Corp One using whois, nslookup and Netcraft.

Instructions sent via Slack.

Suggested Time:
20 Minutes

Times Up! Let’s Review.

DNS Enumeration

DNs Enumeration Review

Determine the net range and name server addresses of megacorpone.com

DNs Enumeration Review

Determine the net range and name server addresses of megacorpone.com

Run whois megacorpone.com to retrieve the following information:

- Name Server: NS1.MEGACORPONE.COM
- Name Server: NS2.MEGACORPONE.COM
- Name Server: NS3.MEGACORPONE.COM

DNs Enumeration Review

Attempt a zone transfer against each name server you discover:

DNs Enumeration Review

Attempt a zone transfer against each name server you discover:

Run the following code:

```
bash
$ nslookip
> server=ns2.megacorpone.com
> set type=axfr
> www.megacorpone.com
...
```

Only ns2.megacorpone.com allows zone transfers.

DNs Enumeration Review

Use Netcraft to enumerate subdomains of megacorpone.com

DNs Enumeration Review

Use Netcraft to enumerate subdomains of megacorpone.com

Netcraft reveals the five domains below.

- www.megacorpone.com
- intranet.megacorpone.com
- admin.megacorpone.com
- support.megacorpone.com
- vpn.megacorpone.com

Scanning with Nmap

Take a Break!

Host Discovery

After identifying the network range that their target belongs to, attackers typically scan it for other live hosts.

For the CEH exam, you should be familiar with the following methods of host discovery:

- **ARP Discovery:** Sends ARP requests out for every IP address in the target range. Only live hosts will respond.

- **Ping Sweep**: Sends a ping request to every IP address in the target range. Only live hosts will respond.

What process comes after host discovery?

Port Scanning

Port scanning is the process of attempting to connect every port on a target machine and keeping track of which connection attempts are successful.

What tool do we use for port scanning?

Port Scanning

Port scanning is the process of attempting to connect every port on a target machine and keeping track of which connection attempts are successful.

What tool do we use for port scanning?

Nmap is the most important tool for scanning ports.

- SYN Scan is the default scan type.
    - Nmap sends TCP flags to a target port with the SYN flag set.
    - If the target is open, it responds with a packet using the SYN/ACK flag set.
    - Then, nmap does not respond, leaving the target port in a **half-open** state.

Port Scanning

What do the following commands do?

- nmap -sS -p 445 192.168.12.50:

- nmap -sT -p 445 192.168.12.50:

- nmap -sU -p 53 192.168.12.50:

- nmap -sS -p U:53,T:53 192.168.12.50:

Port Scanning

What do the following commands do?

- nmap -sS -p 445 192.168.12.50:
    - Performs a SYN scan against port 445 on 192.169.12.50.
- nmap -sT -p 445 192.168.12.50:
- nmap -sU -p 53 192.168.12.50:
- nmap -sS -p U:53,T:53 192.168.12.50:

Port Scanning

What do the following commands do?

- nmap -sS -p 445 192.168.12.50:
  - Performs a SYN scan against port 445 on 192.169.12.50.
- nmap -sT -p 445 192.168.12.50:
  - Performs a TCP Connect scan against port 445 on 192.169.12.50.
- nmap -sU -p 53 192.168.12.50:
- nmap -sS -p U:53,T:53 192.168.12.50:

Port Scanning

What do the following commands do?

- nmap -sS -p 445 192.168.12.50:
  - Performs a SYN scan against port 445 on 192.169.12.50.
- nmap -sT -p 445 192.168.12.50:
  - Performs a TCP Connect scan against port 445 on 192.169.12.50.
- nmap -sU -p 53 192.168.12.50:
  - Performs a UDP scan of port 53 on 192.168.12.50.
- nmap -sS -p U:53,T:53 192.168.12.50:

Port Scanning

What do the following commands do?

- nmap -sS -p 445 192.168.12.50:
  - Performs a SYN scan against port 445 on 192.169.12.50.
- nmap -sT -p 445 192.168.12.50:
  - Performs a TCP Connect scan against port 445 on 192.169.12.50.
- nmap -sU -p 53 192.168.12.50:
  - Performs a UDP scan of port 53 on 192.168.12.50.
- nmap -sS -p U:53,T:53 192.168.12.50:
  - Scans UDP port 53 and TCP port 53. Use a SYN scan on the TCP port.

What process comes after port scanning?

OS and Service Fingerprinting

After identifying open ports on a target machine, the next step is to determine which operating system is running on each target and which services are running on each open port.

The following Nmap flags allow you to profile both operating systems and services.

- -sV flag enables **service version detection.**
  - Nmap not only determines if a target port is open, but also determines which services are running on that port.

- -O enables **passive OS detection.**
  - Determines the target machine’s operating system based only on the data it collects during a normal port scan.

- -A flag enables **active OS detection**.
  - Sends additional packets meant specifically to elicit responses revealing the target’s OS.

OS and Service Fingerprinting

What do the following commands do?

- nmap -sV -p 80, 443 192.168.12.50

- nmap -0 -sV -p 80, 443 192.168.12.50

- nmap -A -sV -p 80, 443 192.168.12.50

OS and Service Fingerprinting

What do the following commands do?

- nmap -sV -p 80, 443 192.168.12.50
    - Performs a service scan of ports 80 and 443 on 192.168.12.50. Does not determine the OS.
- nmap -0 -sV -p 80, 443 192.168.12.50
- nmap -A -sV -p 80, 443 192.168.12.50

OS and Service Fingerprinting

What do the following commands do?

- nmap -sV -p 80, 443 192.168.12.50
  - Performs a service scan of ports 80 and 443 on 192.168.12.50. Does not determine the OS.
- nmap -0 -sV -p 80, 443 192.168.12.50
  - Performs a service scan of ports 80 and 443 on 192.168.12.50 and determines the OS through passive methods.
- nmap -A -sV -p 80, 443 192.168.12.50

OS and Service Fingerprinting

What do the following commands do?

- nmap -sV -p 80, 443 192.168.12.50
  - Performs a service scan of ports 80 and 443 on 192.168.12.50. Does not determine the OS.
- nmap -0 -sV -p 80, 443 192.168.12.50
  - Performs a service scan of ports 80 and 443 on 192.168.12.50 and determines the OS through passive methods.
- nmap -A -sV -p 80, 443 192.168.12.50
  - Performs a service scan of ports 80 and 443 on 192.168.12.50 and determines the OS through active methods.

What’s next after OS and Service Fingerprinting?

Networking Mapping

Networking mapping is the process of collecting all the information gathering into a single document (a network map).

- There are tools for generating graphical network maps, such as **Maltego**.

- Hand-drawn maps should work just as well.

Creating maps helps clarify attack tactics and provides a good opportunity to synthesize all the information collected during the intelligence gathering phase.

Your Turn: Footprinting, Scanning and Enumeration Problem Set

In this activity, you will answer questions on the Scanning and Enumeration sections of the CEH exam.

Instructions sent via Slack.

Suggested Time:

20 Minutes

Times Up! Let’s Review.

Scanning and Enumeration
Problem Set

Footprinting, Scanning and Enumeration

1. What does the Nmap -sU flag do?

☐ Enables TCP scanning

☐ Enables UDP scanning

☐ Enables Service Scanning

☐ Banner-grabs all ports on the target

Footprinting, Scanning and Enumeration

1. What does the Nmap -sU flag do?

□ Enables TCP scanning

□ **Enables UDP scanning**

□ Enables Service Scanning

□ Banner-grabs all ports on the target

Footprinting, Scanning and Enumeration

2. Which of the following is not part of the information gathering phase?

- □ Host Discovery
- □ Finding Physical Addresses
- □ Spidering the Clients Website
- □ Exploiting a Database Server

Footprinting, Scanning and Enumeration

2. Which of the following is not part of the information gathering phase?

- □ Host Discovery
- □ Finding Physical Addresses
- □ Spidering the Clients Website
- □ **Exploiting a Database Server**

Footprinting, Scanning and Enumeration

3. Which of the following is also known as a Zombie scan?

□ SYN Scan

□ IDLE Scan

□ UDP Scan

□ Full-Connect Scan

Footprinting, Scanning and Enumeration

3. Which of the following is also known as a Zombie scan?

- □ SYN Scan
- □ **IDLE Scan**
- □ UDP Scan
- □ Full-Connect Scan

Footprinting, Scanning and Enumeration

4. Which of the following commands scans both TCP and UDP port 445?

- □ nmap -sT -sU -p 445 192.168.12.75
- □ nmap -p U:445,T:445 192.168.12.75
- □ nmap -sU 445 -pT 192.168.12.75
- □ nmap -sS --all-protocols 192.168.12.75

Footprinting, Scanning and Enumeration

4. Which of the following commands scans both TCP and UDP port 445?

- □ nmap -sT -sU -p 445 192.168.12.75
- □ **nmap -p U:445,T:445 192.168.12.75**
- □ nmap -sU 445 -pT 192.168.12.75
- □ nmap -sS --all-protocols 192.168.12.75

Footprinting, Scanning and Enumeration

5. Suppose you discover the following IP addresses on a target network: 192.168.1.24 and 192.168.1.35. Both machines have a netmask of 255.255.255.0. Which of the following is true?

□ The machines are on the same subnet.

□ The machines are on separate subnets.

□ The machines are unreachable from one another.

□ Neither machine is running Windows.

Footprinting, Scanning and Enumeration

5. Suppose you discover the following IP addresses on a target network: 192.168.1.24 and 192.168.1.35. Both machines have a netmask of 255.255.255.0. Which of the following is true?

- □ **The machines are on the same subnet.**
- □ The machines are on separate subnets.
- □ The machines are unreachable from one another.
- □ Neither machine is running Windows.

Footprinting, Scanning and Enumeration

6. Which of the following scan types is used to infer firewall rules?

- □ Full Connect Scan
- □ ACK Scan
- □ SYN Scan
- □ IDLE Scan

Footprinting, Scanning and Enumeration

6. Which of the following scan types is used to infer firewall rules?

- □ Full Connect Scan
- □ **ACK Scan**
- □ SYN Scan
- □ IDLE Scan

Footprinting, Scanning and Enumeration

7. Suppose you find ports 137, 138, and 139 open on a target machine. Which OS is it probably running?

- □ Kali
- □ Solaris
- □ Ubuntu
- □ Windows

Footprinting, Scanning and Enumeration

7. Suppose you find ports 137, 138, and 139 open on a target machine. Which OS is it probably running?

- □ Kali
- □ Solaris
- □ Ubuntu
- □ **Windows**

Footprinting, Scanning and Enumeration

8. Which of the following is commonly used for enumeration?

□ Hyena

□ John

□ IAM Tool

□ LCP

Footprinting, Scanning and Enumeration

8. Which of the following is commonly used for enumeration?

- □ Hyena
- □ John
- □ **IAM Tool**
- □ LCP

Footprinting, Scanning and Enumeration

9. Which of the following hash types are you most likely to encounter when enumerating password hashes on a Windows machine?

- □ NTLMv2
- □ SHA512-Crypt
- □ BlowFish
- □ ElGamal

Footprinting, Scanning and Enumeration

9. Which of the following hash types are you most likely to encounter when enumerating password hashes on a Windows machine?

- □ **NTLMv2**
- □ SHA512-Crypt
- □ BlowFish
- □ ElGamal

Footprinting, Scanning and Enumeration

10. Which of the following protocols can be used to enumerate usernames? Check all that apply.

□ SMTP

□ SMB

□ DNS

□ IRC

Footprinting, Scanning and Enumeration

10. Which of the following protocols can be used to enumerate usernames? Check all that apply.

- □ **SMTP**
- □ **SMB**
- □ DNS
- □ IRC

Footprinting, Scanning and Enumeration

11. Which of the following is a potential result of user enumeration?
Check all that apply.

- □ Brute-Force Attacks
- □ Pass the Hash
- □ Horizontal Escalation / Lateral Movement
- □ DoS

Footprinting, Scanning and Enumeration

11. Which of the following is a potential result of user enumeration?
Check all that apply.

- □ **Brute-Force Attacks**
- □ Pass the Hash
- □ **Horizontal Escalation / Lateral Movement**
- □ DoS

Footprinting, Scanning and Enumeration

12. Which of the following tools would you use to scan a target for vulnerabilities? Check all that apply.

- ☐ tcpdump
- ☐ Nessus
- ☐ Nmap
- ☐ Metasploit

Footprinting, Scanning and Enumeration

12. Which of the following tools would you use to scan a target for vulnerabilities? Check all that apply.

- □ tcpdump
- □ **Nessus**
- □ **Nmap**
- □ **Metasploit**

Footprinting, Scanning and Enumeration

13. Which tool would you use to enumerate SMB users on a WIndows target from a Kali Linux machine?

- □ net
- □ enum4linux
- □ smbmap
- □ dig

Footprinting, Scanning and Enumeration

13. Which tool would you use to enumerate SMB users on a WIndows target from a Kali Linux machine?

- □ net
- □ **enum4linux**
- □ smbmap
- □ dig

Footprinting, Scanning and Enumeration

14. Suppose you dump a Linux machine’s /etc/passwd file during the information gathering phase. You see the lines /bin/nlogin and /bin/false for many users. What does this mean?

- □ The user doesn’t exist.
- □ These users exist, but aren’t stored in the database.
- □ These users exist, but can’t use an interactive shell.
- □ These users exist, but their accounts have been disabled.

Footprinting, Scanning and Enumeration

14. Suppose you dump a Linux machine’s /etc/passwd file during the information gathering phase. You see the lines /bin/nlogin and /bin/false for many users. What does this mean?

□ The user doesn’t exist.

□ These users exist, but aren’t stored in the database.

□ **These users exist, but can’t use an interactive shell.**

□ These users exist, but their accounts have been disabled.

Footprinting, Scanning and Enumeration

15. Suppose you attempt to enumerate users on the website www.foosports.com. You're able to send 5 requests upon launching the attack, but stop receiving responses after that. What most likely happened?

- ☐ The attack failed because the site doesn't have enough users to enumerate.
- ☐ The target server blocked your IP address.
- ☐ Your scan crashed the target server.
- ☐ Your router no longer recognized the target IP address.

Footprinting, Scanning and Enumeration

15. Suppose you attempt to enumerate users on the website www.foosports.com. You’re able to send 5 requests upon launching the attack, but stop receiving responses after that. What most likely happened?

- □ The attack failed because the site doesn’t have enough users to enumerate.
- □ **The target server blocked your IP address.**
- □ Your scan crashed the target server.
- □ Your router no longer recognized the target IP address.

Footprinting, Scanning and Enumeration

16. Identify one advantage of an IDLE scan.

- □ They allow an attacker to get information about a target’s open ports without actually sending packets.
- □ They allow an attacker to scan a target without revealing their IP address.
- □ They are undetectable.
- □ They can find all open ports on a machine, including those that are filtered by a firewall.

Footprinting, Scanning and Enumeration

16. Identify one advantage of an IDLE scan.

- □ They allow an attacker to get information about a target’s open ports without actually sending packets.
- □ **They allow an attacker to scan a target without revealing their IP address.**
- □ They are undetectable.
- □ They can find all open ports on a machine, including those that are filtered by a firewall.

Footprinting, Scanning and Enumeration

17. Identify two disadvantage of an IDLE scan.

- □ They require more machines than a SYN scan.
- □ They are unreliable.
- □ They rarely work.
- □ They are slow.

Footprinting, Scanning and Enumeration

17. Identify two disadvantage of an IDLE scan.

□ **They require more machines than a SYN scan.**

□ They are unreliable.

□ They rarely work.

□ **They are slow.**

Footprinting, Scanning and Enumeration

18. Which of the following tools allows you to enumerate URLs? Check all that apply.

- □ Burp Suite
- □ dirb
- □ wfuzz
- □ kismet

Footprinting, Scanning and Enumeration

18. Which of the following tools allows you to enumerate URLs? Check all that apply.

- □ **Burp Suite**
- □ **dirb**
- □ **wfuzz**
- □ kismet

Footprinting, Scanning and Enumeration

19. Which of the following tools is used for wireless attacks and enumeration?

- □ kismet
- □ PowerShell
- □ zsh
- □ ZAP Proxy

Footprinting, Scanning and Enumeration

19. Which of the following tools is used for wireless attacks and enumeration?

- □ **kismet**
- □ PowerShell
- □ zsh
- □ ZAP Proxy

Footprinting, Scanning and Enumeration

20. Which of the following commands runs all of Nmap’s SMB scripts against a target?

- ☐ nmap --smb-all -sV -p 445 192.168.12.17
- ☐ nmap --script --smb-scripts 192.168.12.17
- ☐ nmap --script smb-enum-* -sV -p 445 192.168.12.17
- ☐ nmap --script smb-enum-* 192.168.12.17

Footprinting, Scanning and Enumeration

20. Which of the following commands runs all of Nmap’s SMB scripts against a target?

- □ nmap --smb-all -sV -p 445 192.168.12.17
- □ nmap --script --smb-scripts 192.168.12.17
- □ **nmap --script smb-enum-* -sV -p 445 192.168.12.17**
- □ nmap --script smb-enum-* 192.168.12.17

Malware & Passwords

Malware & Passwords

Many of the vulnerabilities discovered by Nmap can be exploited with malware.

One of the most common tasks that malware performs is **finding and dumping passwords** from a target machine.

CEH tests on the basic understanding of malware and password attacks, such as:

- Types of Malware and Infection Methods
- Windows Password Hash Format
- Linux Password Hash Formats

Malware Types

The most important types of malware:

- **Virus**: Malware that requires human interaction to run and spread. Hackers often spread viruses by tricking users into downloading and executing them, as in phishing attacks.

- **Trojan**: Malware that "poses" as legitimate software. For example, a hacker might send a phishing email with an attachment called WindowsUpdate.exe, which actually contains malware.

- **Worm**: Malware that can spread without human interaction, making them especially dangerous.

Malware Types

Viruses, trojans and worms can infect the following parts of a computer:

- **Boot Record**: Viruses that infect the code that computers use to boot up. These are extremely dangerous viruses, as they are difficulty to detect.
- **File Infection**: Infect normal files, such as PNG images.
- **Macro Infection**: Viruses embedded in Word or Excel macros. This is commonly used to spread malware through phishing attacks.
- **Polymorphic**: Changes its code every time it infects a new computer. This makes them very hard to detect.
- **Multipart**: A multipart virus is one that can infect multiple parts of a computer, such as both the boot records and the file system.

Malware Phases

Regardless of type or result, all malware spreads through five phases:

- **Search Routine**: The virus is downloaded onto the target and begins looking for a place to infect.
- **Infection Routine**: The virus actually infects its target. The virus payload does not necessarily run. It just embeds itself into the target and lies dormant until it receives a command to run.
- **Trigger Routine**: The virus executes and actually delivers its payload.
- **Anti-Detection Routine**: Some sophisticated viruses can hide themselves from anti-virus software. Those that do are said to have an "anti-detection routine".

Honeypots

A machine tailor-made for catching real malware is called a **honey pot**.

- Researchers often study malware by "tricking" attackers into hacking "dummy" machines that they control, collecting the malware the attacker plants on the device, and studying its actions and effects.

- All secure networks should have at least one honeypot, so administrators and security analysts can keep track of which kinds of malicious software is entering their network.

Windows Passwords Hash Types

Remember: Operating systems store passwords in hashes, so if hackers can’t retrieve the cleartext passwords if they dump the hashes.

Window Password Hash Types include:

- LM
- NTHash
- NTLM

Windows Passwords Hash Types

LM

- LM is a weak hash type used before Windows Vista/Windows Server 2008.
- LM hashes are rarely used today, but sometimes appear in legacy networks.
- LM hashes look like: 299BD128C1101FD6
- Cracking an LM hash with john looks like: john --format=lm hash.txt
- Note: the important part of this command is --format=lm.

Windows Passwords Hash Types

NTHash

- The NTHash is stronger than LM and is used in modern Windows systems.
- NT hashes look like: B4B9B02E6F09A9BD760F388B67351E2B
- Cracking an NTHash looks like: john --format=nt hash.txt.

Windows Passwords Hash Types

NTHash

- NTLM uses an NTHash in combination with other information to authenticate users.
- NTLM has two versions: NTLMv1 and NTLMv2. Both are commonly found on the network.
- NTLMv1 and NTLMv2 hashes look similar. See below for an example.
- To crack an NTLMv1 hash: john --format=netntlm hash.txt
- To crack an NTLMv2 hash: john --format=netntlmv2 hash.txt

Linux Passwords Hash Types

The CEH exam also requires familiarity with Linux hash types.

- Linux password hashes are stored in /etc/shadow as the second field in rach row
    - root:$6$Ke02nYgo.9v0SF4p$hjztYvo/M4buqO4oBX8KZTftjCn6fE4cV5oI95QPekeQpITwFTRbDUBYBLIUx2mhorQoj9bLN8v.w6btE9xy1:16431:0:99999:7:::
- Linux uses the following hash formats:
    - `$1$` MD5
    - `$2$` Blowfish
    - `$2a$` eksBlowfish
    - `$5$` SHA-256 Crypt
    - `$6$` SHA-512 Crypt (This is the strongest and most common format currently used.)

Activity: Malware & Passwords Problem Set

In this activity, you will work on a Malware and Passwords CEH problem set.

Instructions sent via Slack.

Suggested Time:
20 Minutes

Times Up! Let’s Review.

Passwords & Malware Problem Set

Malware and Passwords Review

1. Which of the following is the weakest?

- □ NTLMv1
- □ Kerberos
- □ NTLMv2
- □ LM

Malware and Passwords Review

1. Which of the following is the weakest?

□ NTLMv1

□ Kerberos

□ NTLMv2

□ **LM**

Malware and Passwords Review

2. Which format is used to hash passwords on modern Windows machines?

- □ DES
- □ RC4
- □ NTLM
- □ SHA512

Malware and Passwords Review

2. Which format is used to hash passwords on modern Windows machines?

- □ DES
- □ RC4
- □ **NTLM**
- □ SHA512

Malware and Passwords Review

3. Which hash format was used to generate the credentials below:

admin::N46iSNekpT:08ca45b7d7ea58ee:88dcbe4446168966a153a0064958dac6:5c7830315c783031
0000000000000b45c67103d07d7b95acd12ffa11230e0000000052920b85f78d013c31cdb3b92f5d765c
783030

- □ DES
- □ RC4
- □ NTLM
- □ SHA512

Malware and Passwords Review

3. Which hash format was used to generate the credentials below:

admin::N46iSNekpT:08ca45b7d7ea58ee:88dcbe4446168966a153a0064958dac6:5c7830315c7830310000000000000b45c67103d07d7b95acd12ffa11230e0000000052920b85f78d013c31cdb3b92f5d765c783030

- □ DES
- □ RC4
- □ **NTLM**
- □ SHA512

Malware and Passwords Review

4. Which command would you use to crack the password hash below:

```
299BD128C1101FD6
```

□ john --format=nt hash.txt

□ john --format=lm hash.txt

□ john --format=netntlm hash.txt

□ john --format=raw-md5 hash.txt

Malware and Passwords Review

4. Which command would you use to crack the password hash below:

299BD128C1101FD6

- □ john --format=nt hash.txt
- □ **john --format=lm hash.txt**
- □ john --format=netntlm hash.txt
- □ john --format=raw-md5 hash.txt

Malware and Passwords Review

5. Suppose you dump the following passwords from /etc/shadow. Which algorithm was used to generate them?

```
$6$0LNgXS95nJv2B6hm$BRNf00hyT5xGNRnsLSSn3xDPXIs6l34g2kpex4mh0w/fvGz4MYs02qWjV
U5NrbVktoNVNRsHU6MUTUua4J5nO0
```

- □ MD5
- □ Blowfish
- □ SHA512-Crypt
- □ SHA256-Crypt

Malware and Passwords Review

5. Suppose you dump the following passwords from /etc/shadow. Which algorithm was used to generate them?

```
$6$0LNgXS95nJv2B6hm$BRNf00hyT5xGNRnsLSSn3xDPXIs6l34g2kpex4mh0w/fvGz4MYs02qWjVU5NrbVktoNVNRsHU6MUTUua4J5nO0
```

□ MD5

□ Blowfish

□ **SHA512-Crypt**

□ SHA256-Crypt

Malware and Passwords Review

6. Suppose you dump the following passwords from /etc/shadow. Which algorithm was used to generate them?

```
$1$3JUKmV3R$vZVeb51f1t6QZUecwuRHX0
```

- □ SHA512-Crypt
- □ Blowfish
- □ MD5
- □ SHA256-Crypt

Malware and Passwords Review

6. Suppose you dump the following passwords from /etc/shadow. Which algorithm was used to generate them?

```
$1$3JUKmV3R$vZVeb51f1t6QZUecwuRHX0
```

□ SHA512-Crypt

□ Blowfish

□ **MD5**

□ SHA256-Crypt

Malware and Passwords Review

7. Which of the following exploits leverages a buffer overflow vulnerability?

- □ Heartbleed
- □ Shellshock
- □ BEAST
- □ UAC Bypass

Malware and Passwords Review

7. Which of the following exploits leverages a buffer overflow vulnerability?

- □ **Heartbleed**
- □ Shellshock
- □ BEAST
- □ UAC Bypass

Malware and Passwords Review

8. Which of the following is commonly achieved with a buffer overflow exploit? Check all that apply.

- ☐ Escalating privileges to root
- ☐ Shellcode Injection
- ☐ Reading Protected Memory
- ☐ Dumping Remote Database

Malware and Passwords Review

8. Which of the following is commonly achieved with a buffer overflow exploit? Check all that apply.

- □ **Escalating privileges to root**
- □ **Shellcode Injection**
- □ **Reading Protected Memory**
- □ Dumping Remote Database

Malware and Passwords Review

9. What is the difference between a virus and a worm?

□ A worm can spread without human interaction, whereas a virus must be downloaded or executed by a user.

□ A virus can infect multiple computers, but a worm can only infect one at a time.

□ A virus can copy itself perfectly, but worms change every time the copy themselves.

□ Worms are used for DoS, while viruses can be used for many things.

Malware and Passwords Review

9. What is the difference between a virus and a worm?

- □ **A worm can spread without human interaction, whereas a virus must be downloaded or executed by a user.**
- □ A virus can infect multiple computers, but a worm can only infect one at a time.
- □ A virus can copy itself perfectly, but worms change every time the copy themselves.
- □ Worms are used for DoS, while viruses can be used for many things.

Malware and Passwords Review

10. Which type of malware is most associated with spearphishing?

- □ Worm
- □ Virus
- □ Trojan
- □ Ransomware

Malware and Passwords Review

10. Which type of malware is most associated with spearphishing?

- □ Worm
- □ Virus
- □ **Trojan**
- □ Ransomware

Malware and Passwords Review

11. Which part of a computer does bootkit infect?

- □ NIC
- □ Master Boot Record
- □ BIOS
- □ Files

Malware and Passwords Review

11. Which part of a computer does bootkit infect?

- □ NIC
- □ **Master Boot Record**
- □ BIOS
- □ Files

Malware and Passwords Review

12. Which part of a computer does rootkit infect?

- □ NIC
- □ Master Boot Record
- □ BIOS
- □ Files

Malware and Passwords Review

12. Which part of a computer does rootkit infect?

- □ NIC
- □ Master Boot Record
- □ **BIOS**
- □ Files

Malware and Passwords Review

13. Which ring does a kernel rootkit run in?

- □ Ring 0
- □ Ring 1
- □ Ring 2
- □ Ring 7

Malware and Passwords Review

13. Which ring does a kernel rootkit run in?

- □ **Ring 0**
- □ Ring 1
- □ Ring 2
- □ Ring 7

Malware and Passwords Review

14. Why are rootkits difficult to detect?

- ☐ They are usually very small and hard to find.
- ☐ Anti-Virus can’t find them because they only execute in RAM.
- ☐ Their code is obfuscated and hard to identify as malicious.
- ☐ They can bypass nearly all security controls because they run with full root privileges.

Malware and Passwords Review

14. Why are rootkits difficult to detect?

- □ They are usually very small and hard to find.
- □ Anti-Virus can’t find them because they only execute in RAM.
- □ Their code is obfuscated and hard to identify as malicious.
- □ **They can bypass nearly all security controls because they run with full root privileges.**

Malware and Passwords Review

15. Which technique do viruses to spread through Microsoft Word and Excel documents.

□ Cluster Infection

□ Multipartite Infection

□ Macro Infection

□ Fast Infection

Malware and Passwords Review

15. Which technique do viruses to spread through Microsoft Word and Excel documents.

- □ Cluster Infection
- □ Multipartite Infection
- □ **Macro Infection**
- □ Fast Infection

Malware and Passwords Review

16. What infection method is used by viruses that spread as fake PNG files?

□ File Infection

□ Latent Infection

□ Cluster Infection

□ Hoax Infection

Malware and Passwords Review

16. What infection method is used by viruses that spread as fake PNG files?

- □ **File Infection**
- □ Latent Infection
- □ Cluster Infection
- □ Hoax Infection

Malware and Passwords Review

17. During which phase of infection does a virus identify places to infect?

□ Infection Routine

□ Search Routine

□ Payload Delivery

□ Anti-Detection Routine

Malware and Passwords Review

17. During which phase of infection does a virus identify places to infect?

- □ Infection Routine
- □ **Search Routine**
- □ Payload Delivery
- □ Anti-Detection Routine

Malware and Passwords Review

18. Which if the following might happen when a virus runs it Trigger Routine? Check all that apply.

- ☐ Uninstall itself.
- ☐ Communicate with a CC server.
- ☐ Trigger the Anti-Virus scanner to see if it will be detected.
- ☐ Encrypt the disk so users can’t access their data.

Malware and Passwords Review

18. Which if the following might happen when a virus runs it Trigger Routine? Check all that apply.

- □ Uninstall itself.
- □ **Communicate with a CC server.**
- □ Trigger the Anti-Virus scanner to see if it will be detected.
- □ **Encrypt the disk so users can’t access their data.**

Malware and Passwords Review

19. Which of the following can be used to generate Trojans? Check all that apply.

- □ msfvenom
- □ PowerView.ps1
- □ PowerUp.ps1
- □ Veil Framework

Malware and Passwords Review

19. Which of the following can be used to generate Trojans? Check all that apply.

- □ **msfvenom**
- □ PowerView.ps1
- □ PowerUp.ps1
- □ **Veil Framework**

Malware and Passwords Review

20. Which of the following can be used to read encrypted passwords from RAM?

- □ Empire
- □ Mimikatz
- □ Metasploit
- □ hashcat

Malware and Passwords Review

20. Which of the following can be used to read encrypted passwords from RAM?

- □ Empire
- □ **Mimikatz**
- □ Metasploit
- □ hashcat