






Certified Ethical Hacker

Cybersecurity
Certification Prep Day 2



Class Objectives

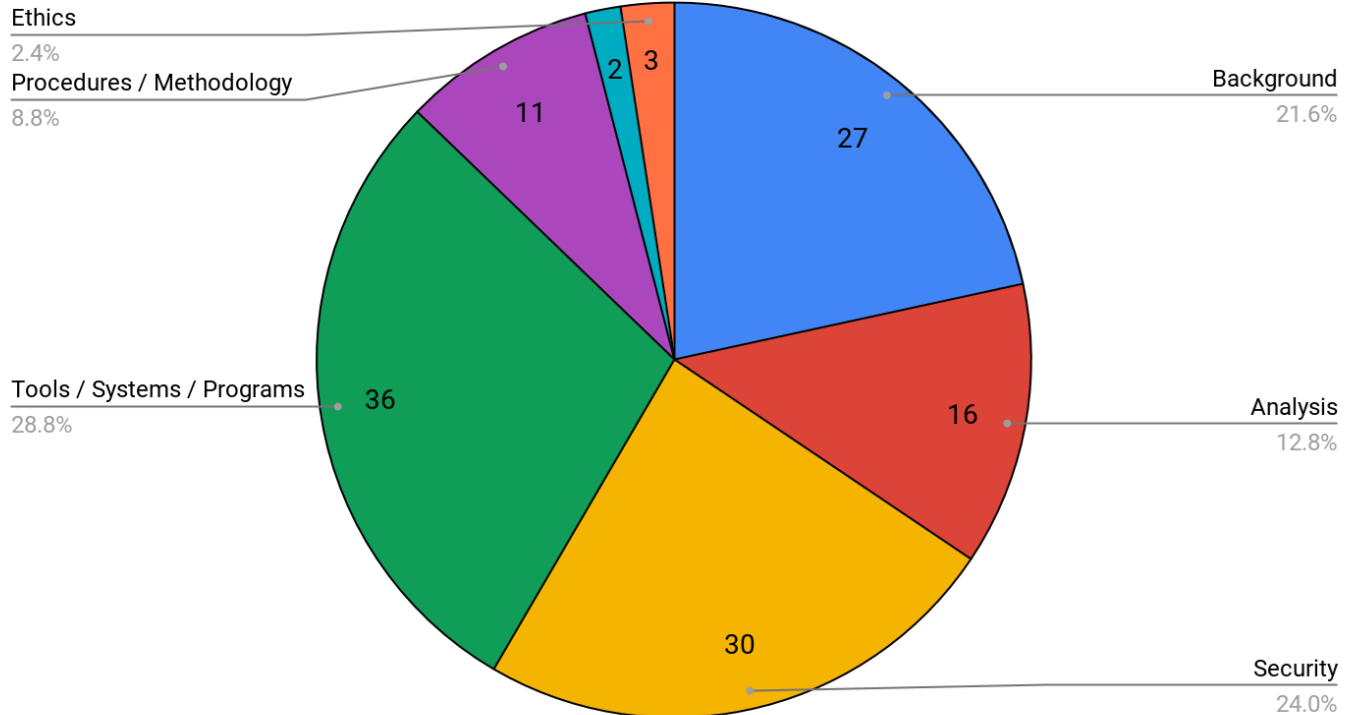
By the end of class today, students will be able to:

-  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

Breakdown of Domains Covered on CEH





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

Which type of hacker is considered unethical?

- ☐ White Hat
- ☐ Grey Hat
- ☐ Black Hat
- ☐ Blue Hat

Warm-Up Review

Which type of hacker is considered unethical?

- ☐ White Hat
- ☐ Grey Hat
- ☐ **Black Hat**
- ☐ Blue Hat

- **Black Hats are unethical, with explicitly malicious intent.**
- White Hats are synonymous with ethical hackers.
- Grey Hats do not care if they act ethically or unethically.

Warm-Up Review

What is the main difference between ethical and malicious hackers?

- ☐ Ethical hackers have written permission.
- ☐ Ethical hackers have verbal permission.
- ☐ Ethical hackers don't use real exploits.
- ☐ Malicious hackers always perform information gathering.

Warm-Up Review

What is the main difference between ethical and malicious hackers?

- ☐ **Ethical hackers have written permission.**
 - ☐ Ethical hackers have verbal permission.
 - ☐ Ethical hackers don't use real exploits.
 - ☐ Malicious hackers never always perform information gathering.
-
- **Ethical hackers must have express, *written* permission from their clients to attack and assess their system. Written permission acts as a *contract*.**
 - Verbal permission isn't sufficient. It doesn't provide non-repudiation!
 - Ethical hackers will use real exploits to assess their clients system.
 - Malicious hackers always perform information gathering.

Warm-Up Review

Which type of testing takes place when pentesters have no knowledge of the target network?

- ☐ Grey Box
- ☐ Black Box
- ☐ White Box
- ☐ Blind Test

Warm-Up Review

Which type of testing takes place when pentesters have no knowledge of the target network?

- ☐ Grey Box
- ☐ **Black Box**
- ☐ White Box
- ☐ Blind Test

- Grey box testers has limited knowledge about an application, such as documents, but not the code.
- **Black box testers have no information about the target application/ network.**
- White box testers know all the details of the target application / network.
- Blind Testing is a made-up term.

Warm-Up Review

You performed a full backup on Monday and an incremental backup on Tuesday. If there is an outage on Wednesday, what do you need to restore operations?

- ☐ Only the full backup from Monday
- ☐ The full backup from Monday and the incremental backup from Tuesday
- ☐ Only the incremental backup from Tuesday

Warm-Up Review

You performed a full backup on Monday and an incremental backup on Tuesday. If there is an outage on Wednesday, what do you need to restore operations?

- ☐ Only the full backup from Monday
 - ☐ **The full backup from Monday and the incremental backup from Tuesday**
 - ☐ Only the incremental backup from Tuesday
-
- Using the full backup without the incremental backup won't restore the machine to the state it was in on Tuesday.
 - You can't restore from just an incremental backup.

Warm-Up Review

Suppose an attacker alters the contents of two files on the server. Which of the following is compromised?

- ☐ Authentication
- ☐ Confidentiality
- ☐ Integrity
- ☐ Availability

Warm-Up Review

Suppose an attacker alters the contents of two files on the server. Which of the following is compromised?

- ☐ Authentication
- ☐ Confidentiality
- ☐ **Integrity**
- ☐ Availability

Warm-Up Review

A SYN Scan is used in which kind of reconnaissance?

- ☐ Active Reconnaissance
- ☐ Passive Reconnaissance
- ☐ Open Source Information Gathering
- ☐ Internal Reconnaissance

Warm-Up Review

A SYN Scan is used in which kind of reconnaissance?

- ☐ **Active Reconnaissance**
 - ☐ Passive Reconnaissance
 - ☐ Open Source Information Gathering
 - ☐ Internal Reconnaissance
-
- **It is active recon because the attacker must directly interact with the target machine. Therefore, it is inherently *not* passive recon.**
 - Open Source Information Gathering uses publicly available databases, not port-scanning tools.
 - Internal Recon is a made-up term.

Warm-Up Review

How long is an IPv6 address?

- ☐ 64 bits
- ☐ 128 bits
- ☐ 256 bits
- ☐ 32 bits

Warm-Up Review

How long is an IPv6 address?

- ☐ 64 bits
- ☐ **128 bits**
- ☐ 256 bits
- ☐ 32 bits

Warm-Up Review

How long is an IPv4 address?

- ☐ 64 bits
- ☐ 128 bits
- ☐ 256 bits
- ☐ 32 bits

Warm-Up Review

How long is an IPv4 address?

- ☐ 64 bits
- ☐ 128 bits
- ☐ 256 bits
- ☐ **32 bits**

Warm-Up Review

An ICMP Type 8 message indicates which of the following?

- ☐ Ping Request
- ☐ Router Advertisement
- ☐ Host Unreachable Message
- ☐ TTL Failure

Warm-Up Review

An ICMP Type 8 message indicates which of the following?

- ☐ **Ping Request**
- ☐ Router Advertisement
- ☐ Host Unreachable Message
- ☐ TTL Failure

An ICMP Type 8 message is an “Echo Request”, generated by a ping command.

Warm-Up Review

Which of the following ports is an attacker most likely to scan when attacking a Windows machine?

- ☐ 445/tcp
- ☐ 53/udp
- ☐ 80/tcp
- ☐ 443/tcp

Warm-Up Review

Which of the following ports is an attacker most likely to scan when attacking a Windows machine?

- ☐ **445/tcp**
- ☐ 53/udp
- ☐ 80/tcp
- ☐ 443/tcp

Windows machines often run SMB on 445/tcp.

Warm-Up Review

Suppose you run a SYN scan against a target host. Which of the following best described the state of connections to the target machine after the scan?

- ☐ Half Open
- ☐ Fully Open
- ☐ Full Duplex
- ☐ Half Duplex

Warm-Up Review

Suppose you run a SYN scan against a target host. Which of the following best described the state of connections to the target machine after the scan?

- ☐ **Half Open**
- ☐ Fully Open
- ☐ Full Duplex
- ☐ Half Duplex

- In a Syn scan, the attacker sends a SYN packet; receives a SYN/ACK packet; and then *stops communication*. The target is left waiting for the attacker to complete the connection. Since the attacker's ports are closed and the victim's are open, the connection is *half-open*.

Warm-Up Review

Which of the following is a Layer 2 attack?

- ☐ ARP Spoofing
- ☐ SQL Injection
- ☐ BGP Hijacking
- ☐ Ping Sweep

Warm-Up Review

Which of the following is a Layer 2 attack?

- ☐ **ARP Spoofing**
- ☐ SQL Injection
- ☐ BGP Hijacking
- ☐ Ping Sweep

Layer 2 is the Data Link Layer.

ARP is the only protocol in the list that runs on Layer 2.

Warm-Up Review

Which of the following would an attacker use to retrieve all DNS records from a nameserver

- ☐ Zone Transfer
- ☐ AAAA Request
- ☐ CNAME Attack
- ☐ DHCP Exhaustion

Warm-Up Review

Which of the following would an attacker use to retrieve all DNS records from a nameserver

- ☐ **Zone Transfer**
- ☐ AAAA Request
- ☐ CNAME Attack
- ☐ DHCP Exhaustion

A Zone Transfer request asks a nameserver for all of its DNS records.

Warm-Up Review

You determined that ports 80 and 443 on a target machine are open. What is the next step?

- ☐ Banner-Grab and Service-Scan Ports 80 and 443
- ☐ Brute-Force Ports 80 and 443
- ☐ Attempts to Exploit Ports 80 and 443
- ☐ Scan for Additional Open Ports

Warm-Up Review

You determined that ports 80 and 443 on a target machine are open. What is the next step?

- ☐ **Banner-Grab and Service-Scan Ports 80 and 443**
 - ☐ Brute-Force Ports 80 and 443
 - ☐ Attempts to Exploit Ports 80 and 443
 - ☐ Scan for Additional Open Ports
-
- The next step is to determine which services are running on ports 80 and 443 before mounting an attack.

Warm-Up Review

Which of the following Nmap flags is used for OS fingerprinting?

- ☐ -A
- ☐ -oN
- ☐ -sS
- ☐ -sU

Warm-Up Review

Which of the following Nmap flags is used for OS fingerprinting?

- ☐ **-A**
- ☐ -oN
- ☐ -sS
- ☐ -sU

- -A is used for active OS fingerprinting.
- -oN is used to save Nmap's output into a file.
- -sS is used to launch a SYN scan.
- -sU is used to launch a UDP scan.

Warm-Up Review

Identify what the following Nmap command does: `nmap -sn 192.168.12.0/24`

- ☐ Port-Scan all devices in 192.168.12.0/24
- ☐ Perform a UDP scan on 192.168.12.0/24
- ☐ Service-Scan 192.168.12.0/24
- ☐ Perform a Ping Sweep on 192.168.12.0/24

Warm-Up Review

Identify what the following Nmap command does: `nmap -sn 192.168.12.0/24`

- ☐ Port-Scan all devices in 192.168.12.0/24
 - ☐ Perform a UDP scan on 192.168.12.0/24
 - ☐ Service-Scan 192.168.12.0/24
 - ☐ **Perform a Ping Sweep on 192.168.12.0/24**
-
- -sn flag tells Nmap to skip port scans and only ping.

Warm-Up Review

Suppose you capture a packet from a system you're investigating. Its IP header is 20 bytes long and it has a datagram of 84 bytes. Which OS is most likely to have sent this packet?

- ☐ Windows XP
- ☐ Windows 10
- ☐ Linux
- ☐ Solaris

Warm-Up Review

Suppose you capture a packet from a system you're investigating. Its IP header is 20 bytes long and it has a datagram of 84 bytes. Which OS is most likely to have sent this packet?

- ☐ Windows XP
- ☐ Windows 10
- ☐ **Linux**
- ☐ Solaris

- Linux computers typically sends packets with these characteristics.

Warm-Up Review

Suppose you run the following command. If the port 22 is open, which TCP flag is set on the response? `$ nmap -sS -p 22 192.168.12.7`

- ☐ ACK
- ☐ SYN/ACK
- ☐ RST
- ☐ URG

Warm-Up Review

Suppose you run the following command. If the port 22 is open, which TCP flag is set on the response? `$ nmap -sS -p 22 192.168.12.7`

- ☐ ACK
- ☐ **SYN/ACK**
- ☐ RST
- ☐ URG

The target machine will send an SYN/ACK packet in response to a SYN packet.

Warm-Up Review

Which of the following netcat commands banner-grabs the HTTP server of a target machine?

- ☐ `ncat -lvp 2222`
- ☐ `ncat -v 192.168.12.8 80`
- ☐ `ncat -v192.168.12.8 8080 < cat /etc/shadow`
- ☐ `ncat 192.168.12.8 443`

Warm-Up Review

Which of the following netcat commands banner-grabs the HTTP server of a target machine?

- ☐ `ncat -lvp 2222`
- ☐ **`ncat -v 192.168.12.8 80`**
- ☐ `ncat -v192.168.12.8 8080 < cat /etc/shadow`
- ☐ `ncat 192.168.12.8 443`

Only the second command connects to port 80 on the target machine.

Warm-Up Review

Which of the following tools would an attacker use to poison a target's ARP cache?

- ☐ Nmap
- ☐ Kismet
- ☐ Cain & Abel
- ☐ enum4linux

Warm-Up Review

Which of the following tools would an attacker use to poison a target's ARP cache?

- ☐ Nmap
- ☐ Kismet
- ☐ **Cain & Abel**
- ☐ enum4linux

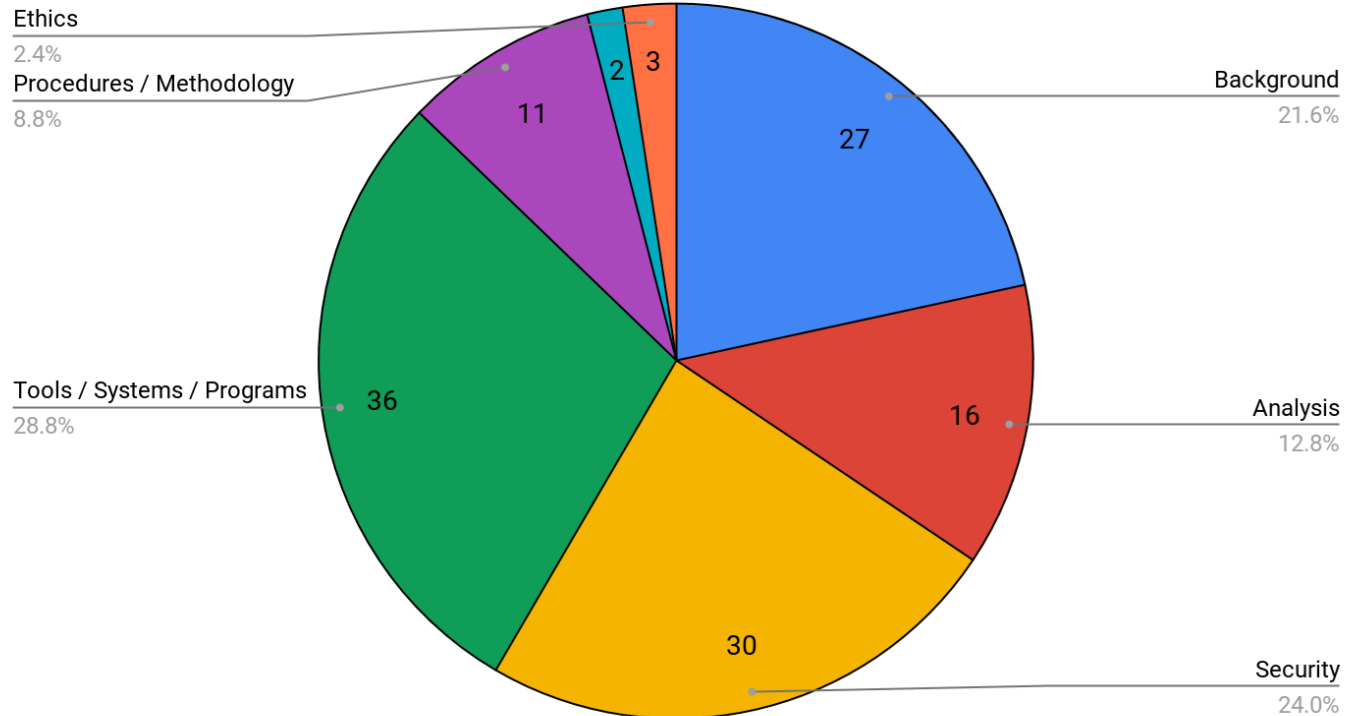
Cain & Abel is the only tool on the list that can be used for ARP poisoning.

“Background” Sub-Topic

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



Domain 1: Background

Subtopics Included:

-  Networking technologies
-  Web technologies
-  System technologies
-  Communication Protocols
-  Malware Operations
-  Mobile technologies
-  Telecommunications Technologies
-  Backups and archiving



Domain 1: Background

Subtopics Covered In-Class:

-  Networking technologies - **Networking 101, Networking Security**
-  Web technologies - **Cyber 101, Web Development**
-  System technologies - **Cyber 101, Networking 101, Operating Systems**
-  Communication Protocols- **Networking 101, Networking Security**
-  Malware Operations- **Penetration Testing, Web Vulnerabilities**
-  Mobile technologies- **Not Covered**
-  Telecommunications Technologies- **Not Covered**
-  Backups and archiving- **Linux System Administration**



OCTAVE & OSSTMM

CEH covers the processes and methodologies of professional hackers, such as:

- OCTAVE
- OSSTMM
- NIST SP 800-15 (Security Assessment Stages)
- Pentesting Execution Standard

The CEH exam does not require comprehensive knowledge of these methods, but you may be expected to enumerate their steps and identify what they're used for.

OCTAVE

Operationally Critical Threat, Asset, and Vulnerability Evaluation

- OCTAVE is a *high-live* risk assessment framework.
- It is designed for usage by small, cross-departmental teams consisting of IT, Security and Business representatives.
- Encourages teams to think of their organization in terms of **views**, where each view consists of threats, vulnerabilities, current practices etc. that could potential damage an business.
 - **OCTAVE** differentiates between Organizational views and Technological views.

OCTAVE

Operationally Critical Threat, Asset, and Vulnerability Evaluation

Phase 1: Build Asset-Based Threat Profiles (An Organizational View)

Identifying, classifying, and prioritizing organizational assets, such as confidential records, intellectual property, etc.

Phase 2: Identify Infrastructure Vulnerabilities (A Technological View)

Identifying, classifying, and prioritizing technical assets, such as file servers.

Phase 3: Strategy and Plan Development

Determining the most relevant threats to the organization, based on their respective views.

Open Source Security Testing Methodology Manual

- A framework for how to conduct a security assessment.
- Consists of six steps / levels that organizations commonly invest in protecting and auditing:
 - Defining the Test
 - Data Network Security Testing
 - Human Security Testing
 - Physical Security Testing
 - Telecommunications Security Testing
 - Wireless Security Testing

The Hacking Process

Many CEH holders work on pentesting teams.

Therefore, it is very useful to be familiar with the **Pentesting Execution Standard**

1. Pre-Engagement Interactions
2. Intelligence Gathering
3. Threat Modeling
4. Vulnerability Analysis
5. Exploitation
6. Post-Exploitation
7. Reporting

The CEH exam tests candidates knowledge on which tasks correspond to which phases.

- For example: Port Scanning

Matching Tasks to Phases

Many of the Background / Technical Foundations questions evaluate your knowledge of which tasks are performed during which PTES phases of an engagement.

- For example: you'll be expected to know that host discovery is performed as part of intelligence gathering, not exploitation.
- You may be asked if DNS Reconnaissance is performed during the Exploitation. (*It typically is not.*)

In the next exercise, you will determine at what point in an engagement recently discovered attackers are in the attack cycle.

On the job, Blue Teams commonly use this information to identify which hackers are closest to exploitation and post-exploitation.



Activity: Matching Tasks to Phases

In this activity, you will determine at what point in an engagement recently discovered attackers are in the attack cycle.

Instructions sent via Slack.

Suggested Time:
10 Minutes





Times Up! Let's Review.

Matching Tasks to Phases

Matching Tasks to Phases Review

Based on the descriptions of suspicious activity, identify which phase each attacker is in.

1. An unidentified machine on the corporate intranet has been sending requests for lists of usernames to all administrative servers on the network.

Matching Tasks to Phases Review

Based on the descriptions of suspicious activity, identify which phase each attacker is in.

1. An unidentified machine on the corporate intranet has been sending requests for lists of usernames to all administrative servers on the network.

This occurs during the Information Gathering.

However, if the attacker is performing reconnaissance on an *internal* network, they've already managed to exploit at least one machine.

This means they are already in the organization and should be promptly containing.

Matching Tasks to Phases Review

Based on the descriptions of suspicious activity, identify which phase each attacker is in.

2. The SOC team noticed that an administrative server on the private network has been sending HTTP traffic from port 8080, but IT says they only run HTTP on port 80.

Matching Tasks to Phases Review

Based on the descriptions of suspicious activity, identify which phase each attacker is in.

2. The SOC team noticed that an administrative server on the private network has been sending HTTP traffic from port 8080, but IT says they only run HTTP on port 80.

This most likely indicates that the attacker has infiltrated the network, started their own HTTP in the admin machine and began exfiltrating data.

This occurs in the **Post-Exploitation phase.**

Matching Tasks to Phases Review

Based on the descriptions of suspicious activity, identify which phase each attacker is in.

3. *X Corp* tunnels all traffic to and from the corporate intranet through a VPN server. This VPN server has been hit with numerous Nmap scans from the same IP this week.

Matching Tasks to Phases Review

Based on the descriptions of suspicious activity, identify which phase each attacker is in.

3. *X Corp* tunnels all traffic to and from the corporate intranet through a VPN server. This VPN server has been hit with numerous Nmap scans from the same IP this week.

These actions occur during the **Intelligence Gathering** phase.

Matching Tasks to Phases Review

Based on the descriptions of suspicious activity, identify which phase each attacker is in.

4. The VPN server has SSH enabled. The logs indicate someone has attempted to brute-force the SSH server recently, but has not yet managed to break in.

Matching Tasks to Phases Review

Based on the descriptions of suspicious activity, identify which phase each attacker is in.

4. The VPN server has SSH enabled. The logs indicate someone has attempted to brute-force the SSH server recently, but has not yet managed to break in.

This occurs during the **Exploitation** phase of an attack.

Matching Tasks to Phases Review

Based on the descriptions of suspicious activity, identify which phase each attacker is in.

5. A user of *X Corp's* public website recently reported that someone had hacked into their account and changed their profile information, including their password.

Matching Tasks to Phases Review

Based on the descriptions of suspicious activity, identify which phase each attacker is in.

5. A user of *X Corp's* public website recently reported that someone had hacked into their account and changed their profile information, including their password.

This occurs during the **Exploitation** and **Post-Exploitation** phases of an attack.

Network Protocols

Network Protocols

Fundamental networking knowledge accounts for the bulk of the remaining Background domain.

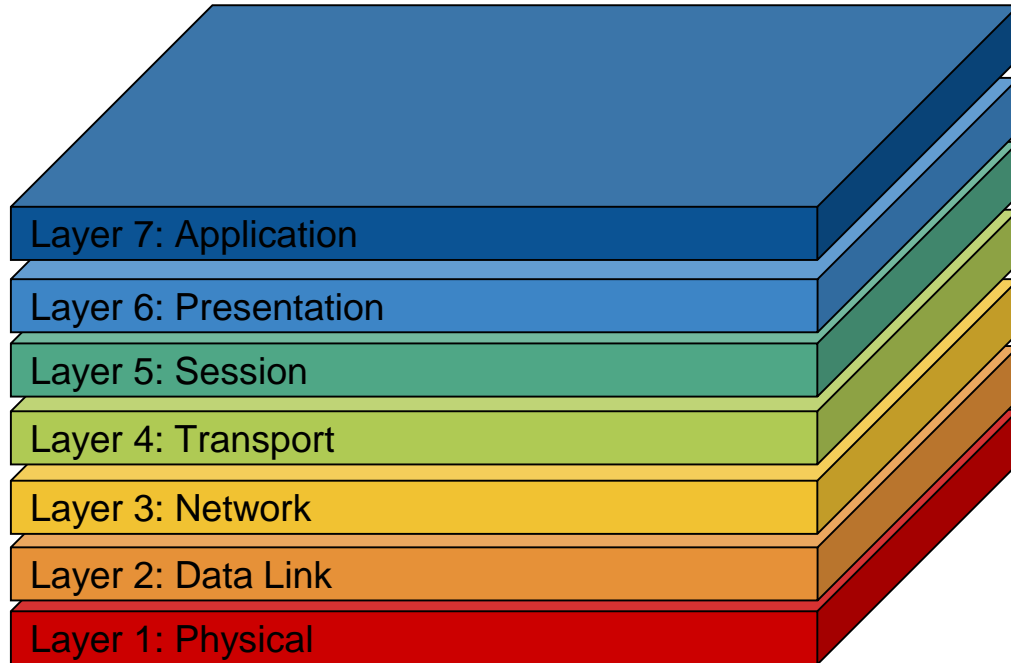
We've covered this content in Networks 101, Web and Web Vulnerabilities and Pentesting.

We'll continue with a review of:

- Layers of the OSI Model
- Common Protocols and their Use Cases

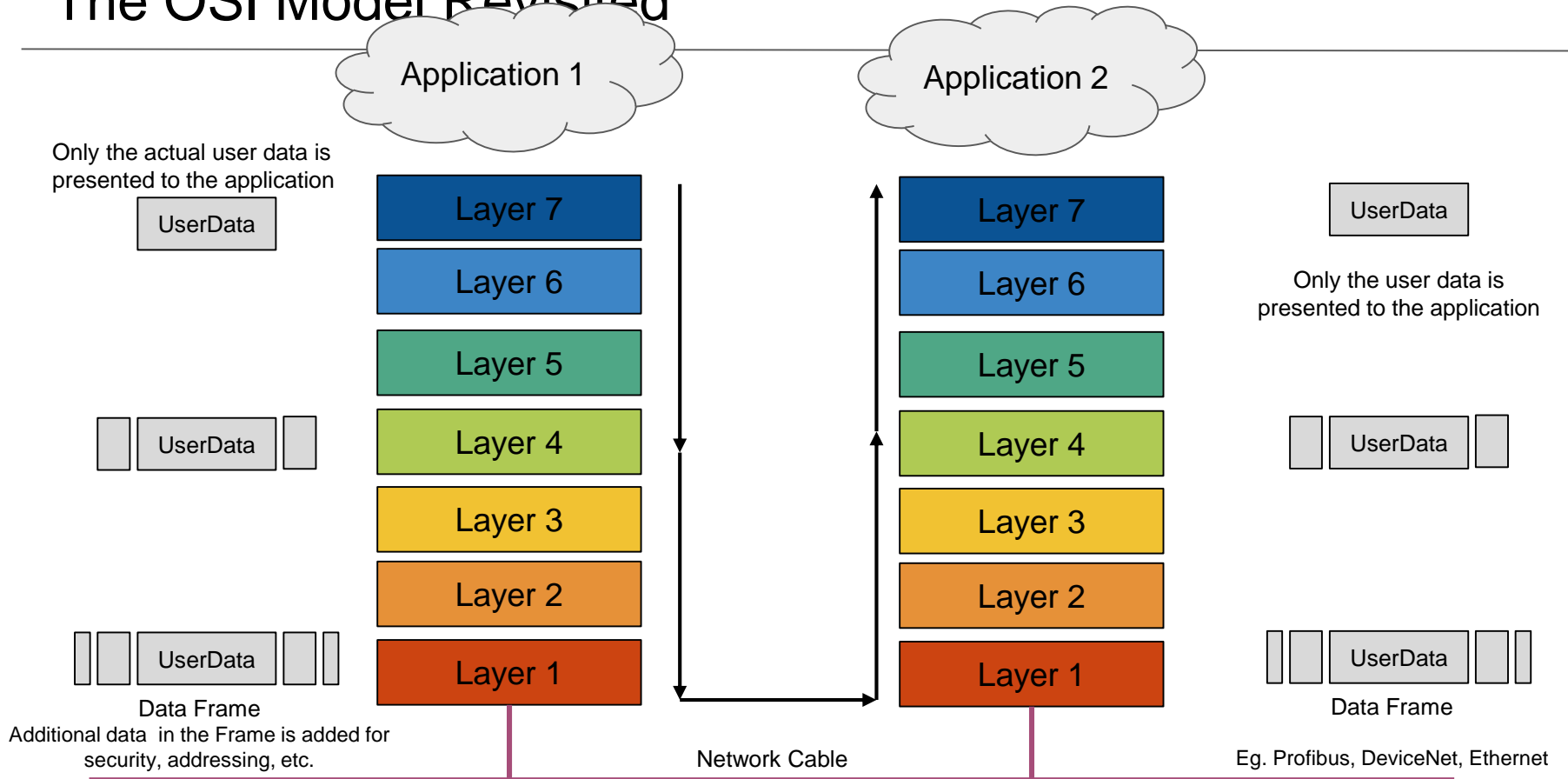
The OSI Model Revisited

The OSI Model provides a framework to categorize and conceptualize the overwhelming volume of ports and protocols.

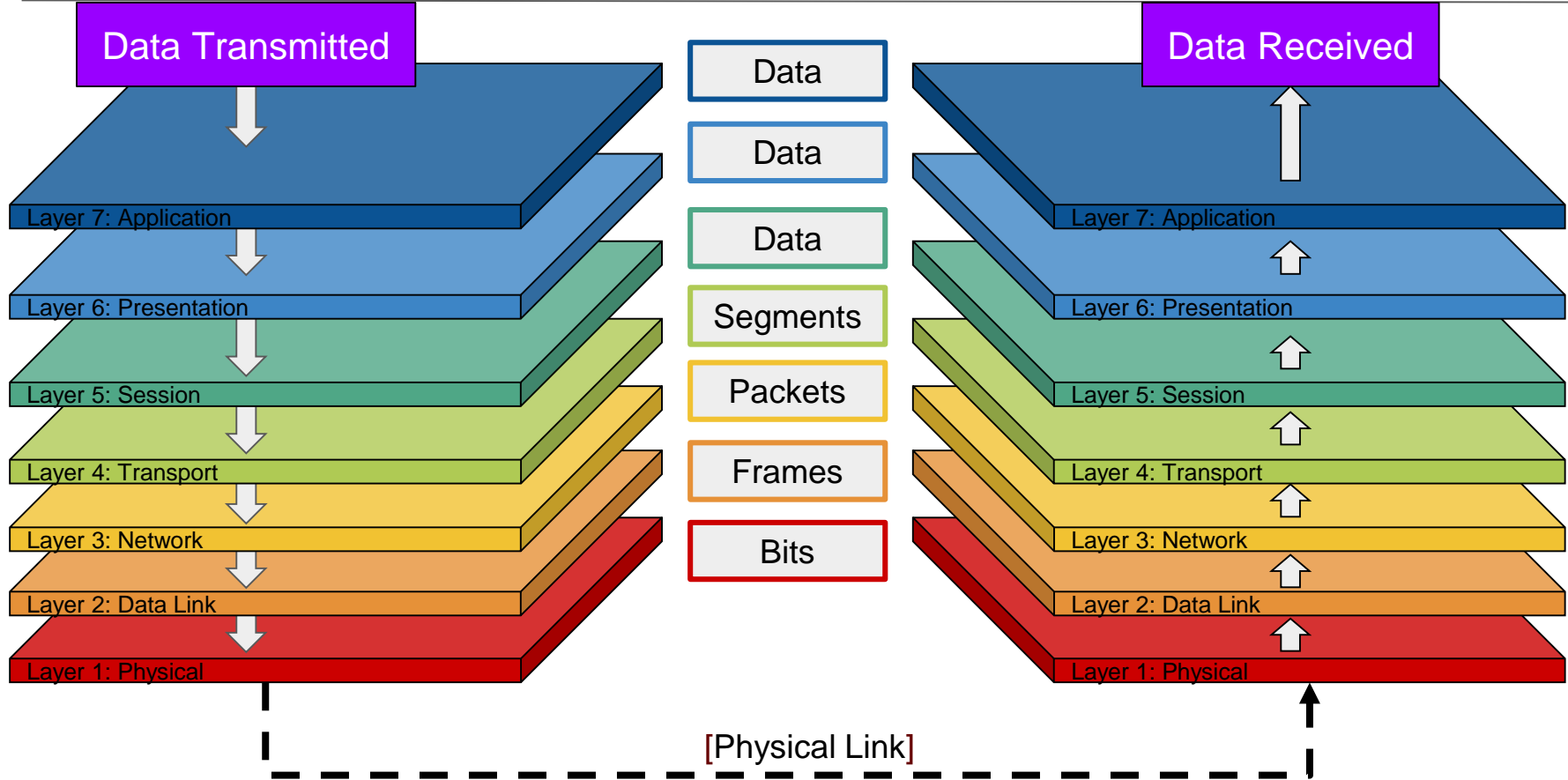


The OSI Model depicts the travel of communication through 7 layers, slowly growing the data frame to incorporate aspects like protocol information, security measures, and other pertinent information.

The OSI Model Revisited



The OSI Model Revisited



OSI Layer 1: Physical Layer

What occurs on the Physical Layer?

Examples of devices and protocols?

OSI Layer 1: Physical Layer

What occurs on the Physical Layer?

The Physical Layer is responsible for transforming voltages from a battery or wall socket into a sequence of 1s and 0s that a computer can interpret.

Examples of devices and protocols?

OSI Layer 1: Physical Layer

What occurs on the Physical Layer?

The Physical Layer is responsible for transforming voltages from a battery or wall socket into a sequence of 1s and 0s that a computer can interpret.

Examples of devices and protocols?

- WiFi adapters and Ethernet cables are examples of Layer 1 devices.
- Ethernet and wlan 802.11a/n are examples of physical protocols.

OSI Layer 2: Data Link Layer

What occurs on the Data Link Layer?

Examples of devices and protocols?

OSI Layer 2: Data Link Layer

What occurs on the Data Link Layer?

The Data Link Layer protocols enables machines to find each other on **local** network.

Examples of devices and protocols?

OSI Layer 2: Data Link Layer

What occurs on the Data Link Layer?

The Data Link Layer protocols enables machines to find each other on **local** network.

Examples of devices and protocols?

- Layer 2 protocols rely on **MAC Address**, a **48-bit** hexadecimal string that uniquely identifies a device.
- Devices send messages on a LAN by sending data to the MAC Address of their recipient.
- **Address Resolution Protocol (ARP)** enables computers on a LAN to learn the MAC addresses of other devices on the same network.

OSI Layer 2: Data Link Layer

How does the Address Resolution Protocol work?

Address Resolution Protocol (ARP) enables computers on a LAN to learn the MAC addresses of other devices on the same network.

1.

2.

3.

OSI Layer 2: Data Link Layer

How does the Address Resolution Protocol work?

Address Resolution Protocol (ARP) enables computers on a LAN to learn the MAC addresses of other devices on the same network.

1. First, the client sends an **ARP Request** to every machine on the LAN.
 - This request contains the IP Address of the desired recipient.
- 2.
- 3.

OSI Layer 2: Data Link Layer

How does the Address Resolution Protocol work?

Address Resolution Protocol (ARP) enables computers on a LAN to learn the MAC addresses of other devices on the same network.

1. First, the client sends an **ARP Request** to every machine on the LAN.
 - This request contains the IP Address of the desired recipient.
2. If a machine has the IP Address that is contained in the request, it sends an **ARP Reply**.
 - This reply contains both the recipient's IP Address and its MAC Address.
- 3.

OSI Layer 2: Data Link Layer

How does the Address Resolution Protocol work?

Address Resolution Protocol (ARP) enables computers on a LAN to learn the MAC addresses of other devices on the same network.

1. First, the client sends an **ARP Request** to every machine on the LAN.
 - This request contains the IP Address of the desired recipient.
2. If a machine has the IP Address that is contained in the request, it sends an **ARP Reply**.
 - This reply contains both the recipient's IP Address and its MAC Address.
3. When the client receives this reply, the network's **switch** adds the IP Address / MAC Address combination to its internal **CAM Table**.
 - It will look up the IP Address in the CAM instead of sending an ARP Request in the future.

OSI Layer 3: Network Layer

What occurs on the Network Layer?

Examples of devices and protocols?

OSI Layer 3: Network Layer

What occurs on the Network Layer?

Protocols on the Network Layer enable devices and locate each other on the Internet.

Examples of devices and protocols?

- Routers are the most important Layer 3 devices.
- The Internet Protocol (IP) is the most important Network protocol.
- Other important routing protocols include: **OSPF**, **RIPv2** and **BGP**.
- Network protocols use IP Addresses to determine the fastest and most reliable path between two machines.

OSI Layer 3: Network Layer

IP Addresses Recap:

Public IP Addresses are assigned to servers and **routers** on the Internet.

Private IP Addresses are *never* assigned to machines on the public Internet. They are only assigned to machines on a LAN.

Routers have at least **two network interfaces**.

- One has a private IP address, used to communicate with machines on LAN.
- The other has a public IP address, used to communicate with machines on public Internet. (This is why routers are often called **gateways**).

OSI Layer 3: Network Layer

IP Addresses Recap Cont'd.

How do clients on LAN communicate with the Internet?

OSI Layer 3: Network Layer

IP Addresses Recap Cont'd.

How do clients on LAN communicate with the Internet?

- Clients on the LAN send HTTP requests to the router.
- These requests contain the clients' *private* IP address as their source and their recipient server's *public* IP address as their destination.
- When the router receives this request, it replaces the private IP address with its own public IP address.
- Then, it forwards the request to the original destination, causing the server to send its response to the *router*.
- When the router receives the request, it replaces its own IP address with the original clients address, then forwards the response to the device that initially requested it.

This process of replacing IP addresses is called **Network Address Translation (NAT)**.

OSI Layer 4: Transport Layer

What occurs on the Transport Layer?

Examples of protocols?

OSI Layer 4: Transport Layer

What occurs on the Transport Layer?

Transport Layer protocols are responsible for transferring the data between machines that have found each other's MAC and IP addresses.

Examples of protocols?

Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)

OSI Layer 4: Transport Layer

What occurs on the Transport Layer?

Transport Layer protocols are responsible for transferring the data between machines that have found each other's MAC and IP addresses.

What is TCP? UDP?

OSI Layer 4: Transport Layer

What occurs on the Transport Layer?

Transport Layer protocols are responsible for transferring the data between machines that have found each other's MAC and IP addresses.

What is TCP? UDP?

TCP is a **connection-oriented** protocol.

- It can detect and handle errors in data transmissions
- Used for familiar protocols such as HTTP and FTP.

UDP is a **connectionless** protocol.

- It sends data to the target, but cannot confirm if the target received it.
- UDP is useful for video and audio streaming.

OSI Layer 5: Session Layer

What occurs on the Session Layer?

Examples of devices and protocols?

OSI Layer 5: Session Layer

What occurs on the Session Layer?

Session Layer protocols establish dedicated “channels” / connections for applications to send requests and responses through.

Examples of devices and protocols?

- Layer 5 protocols use TCP or UDP to transfer data “under the hood”.
- Layer 5 is not covered very much on the CEH exam.

OSI Layer 6: Presentation Layer

What occurs on the Presentation Layer?

OSI Layer 6: Presentation Layer

What occurs on the Presentation Layer?

Presentation layer protocols turn raw data from the network into strings, which computers and applications can easily understand.

- Layer 6 is not covered very much on the CEH exam.

OSI Layer 7: Application Layer

What occurs on the Presentation Layer?

OSI Layer 7: Application Layer

What occurs on the Presentation Layer?

Layer 7 protocols support applications used by users, such as Google Chrome or FileZilla FTP Server.

- The Application layer contains familiar protocols, such as HTTP, FTP, and DNS.

traceroute, Revisited

traceroute, revisited

traceroute is used to determine how many routers are between you and a given server.

- Each transfer from one packet to the next packet is called a **hop**.
- Packets can only “survive” a certain number of hops, known as their **time to live (TTL)**.
 - TTL is also known as hop limit
 - TTL ranges from 1 to 225.

TTL Example:

- If you send a packet with a TTL of 1, it will get to your default gateway, which is *one* hop away.
 - Packets with a TTL of 1 can never leave the LAN
- If a packet has a TTL of 2, the packet would make it to one router on the Internet.
 - Communicating with a VPN server often takes two hops.

traceroute, revisited

How traceroutes use TTL to determine the distance between machines:

- First, traceroute sends *three* pings to the Target IP with a TTL of 1.
- This packet reaches the first-hop router. The router sees the packet's TTL is 1.
 - Because this indicates the packet is expired, the router *rejects* the packet instead of forwarding it to the next hop.
- After rejecting the packet, the first-hop router notifies the client that it has dropped its request.
 - It does this by sending a "special type of ping", called an ICMP — TTL Exceeded message.
- The traceroute machine receives the TTL Time Exceeded message, which contains the IP address of the first-hop router. It logs as the first machine on the path to your target.

traceroute, revisited

How traceroutes use TTL to determine the distance between machines:

- Next, traceroute pings the target IP with a TTL of 2.
 - This time, the traffic gets to the *second* hop router before getting rejected.
 - traceroute then remembers the IP address of this machine, and repeats the whole process, incrementing the TTL by one each time.
- Eventually, traceroute will either receive an ICMP — TTL Exceeded message from the target IP, in which case it's successfully mapped every router between you and the destination.
 - If the target is more than 64 hops away, traceroute will simply give up.

traceroute, revisited

How traceroutes use TTL to determine the distance between machines:

```
$ traceroute 52.45.210.41

. traceroute to 52.45.210.41 (52.45.210.41), 64 hops max, 52 byte packets
. 1  192.168.0.1 (192.168.0.1)  2.633 ms  3.098 ms  1.752 ms
. 2  142.254.213.93 (142.254.213.93)  11.192 ms  13.351 ms  12.281 ms
. 3  agg63.fyvlnyhe02h.northeast.rr.com (24.58.240.221)  28.298 ms  31.329 ms  24.600 ms
...
```

- The first row explains that `traceroute` will send 52 byte packets to 52.45.210.41, and count how many hops they take to get there.
- The second row (starting with `. 1`) identifies the IP Address that is *one* hop away. In this case, the IP address is 192.168.0.1. This is noteworthy because it is a *private* address, so we know this is the IP address of the LAN's default gateway.
- Each number after the IP address is the number of milliseconds it took for each of the three UDP packets to come back. These are called Round-Trip Times, or RTTs.
- The third row contains the IP address and RTTs for the second-hop router; the fourth row contains the IP address and RTTs for the third-hop router; etc.



Activity: Tracing traceroute

In this activity, you will play the role of a network administrator who is responsible for verifying that machines on your network are routing as expected.

Instructions sent via Slack.

Suggested Time:
15 Minutes





Times Up! Let's Review.

Tracing traceroutes

Tracing Traceroute Review

1. Find the first packet sent by your machine and identify the following:

- Your **source IP address**
- The destination IP address
- The packet's TTL value

Tracing Traceroute Review

1. Find the first packet sent by your machine and identify the following:

- Your **source IP address:** 192.168.100.138
- The destination IP address: 4.2.2.1
- The packet's TTL value: 1

Tracing Traceroute Review

2. Find the response to this packet and identify the following:

- The **source IP address**:
- The ICMP message type and code:

Tracing Traceroute Review

2. Find the response to this packet and identify the following:

- The **source IP address:** 192.168.100.1
- The ICMP message type and code: ICMP Time-to-Live Exceeded (Code 11)

Tracing Traceroute Review

3. Repeat the last step for the next four requests sent from your machine and verify the IP addresses of each router along the path.

- Hop 1 IP Address:
- Hop 2 IP Address:
- Hop 3 IP Address:
- Hop 4 IP Address:
- Hop 5 IP Address:

Tracing Traceroute Review

3. Repeat the last step for the next four requests sent from your machine and verify the IP addresses of each router along the path.

- Hop 1 IP Address: 192.168.100.1
- Hop 2 IP Address: 12.180.241.1
- Hop 3 IP Address: 12.153.21.202
- Hop 4 IP Address: 12.86.61.157
- Hop 5 IP Address: 12.122.133.110

Take a Break!



TCP Split Handshake

TCP Handshake

The standard TCP handshake involves three packets:

- The **client** sends a SYN packet to the server.
- The **server** sends a SYN/ACK packet to the client.
- The **client** sends an ACK packet to the server

After the three steps, a **connection** is established between the two machines.

TCP **Split** Handshake

With a TCP Split Handshake, the server sends SYN and ACK packets *separately*:

- The **client** sends a SYN packet to the server.
- The **server** sends *only* ACK packet to the client.
- The **server** sends *only* SYN packet to the client.
- The **client** sends an ACK packet to the server

This small difference has a big impact on a real network:

- Network admins often forget to write the firewall rules to identify split handshakes.
- Split handshakes can allow attackers to bypass firewalls, making it easier for attackers to send malicious payloads to their targets.



Activity: TCP Split Handshake

In this activity, you will use Wireshark to identify the IP address of an attacker and determine ways for the IR team to prevent further incidents.

Instructions sent via Slack.

Suggested Time:
15 Minutes





Times Up! Let's Review.

TCP Split Handshake



Activity: Background Domain Problem Set

In this activity, you will answer and review questions pertaining to the Background topic of the CEH exam.

Instructions sent via Slack.

Suggested Time:
15 Minutes





Times Up! Let's Review.

TCP Split Handshake

Background Domain Review

Which of the following packets came from a private network?

- ☐ 12.27.3.3
- ☐ 172.217.12.174
- ☐ 66.108.36.233
- ☐ 192.168.15.98

Background Domain Review

Which of the following packets came from a private network?

- ☐ 12.27.3.3
- ☐ 172.217.12.174
- ☐ 66.108.36.233
- ☐ **192.168.15.98**

Background Domain Review

Which DNS record contains administrative contact information?

- ☐ A Record
- ☐ AAAA Record
- ☐ SOA
- ☐ CNAME Record

Background Domain Review

Which DNS record contains administrative contact information?

- ☐ A Record
- ☐ AAAA Record
- ☐ **SOA**
- ☐ CNAME Record

Background Domain Review

Suppose an attacker has infiltrated a LAN and wants to redirect traffic from another user's machine to her own. The attacker and her target are on the same local network, which sits behind a NAT-ting router and firewall.

Which of the following techniques is the attacker most likely to use?

- ☐ Kerberos Golden Ticket
- ☐ DNS Spoofing
- ☐ ARP Spoofing
- ☐ Pass the Hash Attack

Background Domain Review

Suppose an attacker has infiltrated a LAN and wants to redirect traffic from another user's machine to her own. The attacker and her target are on the same local network, which sits behind a NAT-ting router and firewall.

Which of the following techniques is the attacker most likely to use?

- ☐ Kerberos Golden Ticket
- ☐ DNS Spoofing
- ☐ **ARP Spoofing**
- ☐ Pass the Hash Attack

Background Domain Review

At which layer of the OSI model does a DNS hijacking attack occur?

- ☐ Layer 4
- ☐ Layer 6
- ☐ Layer 7
- ☐ Layer 2

Background Domain Review

At which layer of the OSI model does a DNS hijacking attack occur?

- ☐ Layer 4
- ☐ Layer 6
- ☐ **Layer 7**
- ☐ Layer 2

Background Domain Review

Which of the following best describes the practice of exposing only the minimum number of ports, services, and applications required?

- ☐ Principle of Least Privilege
- ☐ Access Control List
- ☐ Defense in Depth
- ☐ Deny All By Default

Background Domain Review

Which of the following best describes the practice of exposing only the minimum number of ports, services, and applications required?

- ☐ **Principle of Least Privilege**
- ☐ Access Control List
- ☐ Defense in Depth
- ☐ Deny All By Default

Background Domain Review

Which of the following best describes the practice of exposing only the minimum number of ports, services, and applications required?

- ☐ Principle of Least Privilege
- ☐ Access Control List
- ☐ Defense in Depth
- ☐ Deny All By Default

Background Domain Review

Which of the following best describes the practice of exposing only the minimum number of ports, services, and applications required?

- ☐ **Principle of Least Privilege**
- ☐ Access Control List
- ☐ Defense in Depth
- ☐ Deny All By Default

Background Domain Review

Which of the following tools would you use to look for evidence of suspicious activity in system log files?

- ☐ nc
- ☐ nmap
- ☐ grep
- ☐ kismet

Background Domain Review

Which of the following tools would you use to look for evidence of suspicious activity in system log files?

- ☐ nc
- ☐ nmap
- ☐ **grep**
- ☐ kismet

Background Domain Review

Which of the following protocols can be exploited by manipulating sequence and acknowledgement numbers?

- ☐ ARP
- ☐ TCP
- ☐ UDP
- ☐ IP

Background Domain Review

Which of the following protocols can be exploited by manipulating sequence and acknowledgement numbers?

- ☐ ARP
- ☐ **TCP**
- ☐ UDP
- ☐ IP

Background Domain Review

This protocol allows computers to automatically acquire IP addresses when joining a network:

- ☐ DNS
- ☐ RIPv2
- ☐ DoS
- ☐ DNS

Background Domain Review

This protocol allows computers to automatically acquire IP addresses when joining a network:

- ☐ DNS
- ☐ RIPv2
- ☐ DoS
- ☐ **DNS**

Background Domain Review

Traceroutes use which kind of ICMP packet to determine routing paths?

- ☐ Type 8
- ☐ Type 4
- ☐ Type 3
- ☐ Type 9

Background Domain Review

Traceroutes use which kind of ICMP packet to determine routing paths?

- ☐ Type 8
- ☐ Type 4
- ☐ **Type 3**
- ☐ Type 9

Background Domain Review

Which attack is most similar to ARP Poisoning?

- ☐ DNS Hijacking
- ☐ DHCP Flooding
- ☐ Zone Transfer
- ☐ Eternal Blue

Background Domain Review

Which attack is most similar to ARP Poisoning?

- ☐ **DNS Hijacking**
- ☐ DHCP Flooding
- ☐ Zone Transfer
- ☐ Eternal Blue

Background Domain Review

Which flag is set on a packet returned from a closed port?

- ☐ PSH
- ☐ RST
- ☐ URG
- ☐ SYN

Background Domain Review

Which flag is set on a packet returned from a closed port?

- ☐ PSH
- ☐ **RST**
- ☐ URG
- ☐ SYN

Background Domain Review

Suppose you perform an Nmap scan against a machine behind a firewall that drops all packets to your target. How can Nmap tell that the machine isn't reachable?

- ☐ It looks for RST flags in the response.
- ☐ It waits for a response, but reports that the host is unreachable after a timeout.
- ☐ It attempts to ping other hosts with similar IP addresses.
- ☐ It determines if the routing path to the target machine is broken.

Background Domain Review

Suppose you perform an Nmap scan against a machine behind a firewall that drops all packets to your target. How can Nmap tell that the machine isn't reachable?

- ☐ It looks for RST flags in the response.
- ☐ **It waits for a response, but reports that the host is unreachable after a timeout.**
- ☐ It attempts to ping other hosts with similar IP addresses.
- ☐ It determines if the routing path to the target machine is broken.

Background Domain Review

Check all the tools that you might use to perform DNS enumeration.

- ☐ dnsrecon
- ☐ nslookup
- ☐ aircrack-ng
- ☐ dig

Background Domain Review

Check all the tools that you might use to perform DNS enumeration.

- ☐ **dnsrecon**
- ☐ **nslookup**
- ☐ aircrack-ng
- ☐ **dig**

Background Domain Review

During which stage of a penetration test does an attacker attempt to gain access to a system?

- ☐ Maintaining Access
- ☐ Post-Exploitation
- ☐ Exploitation
- ☐ Reconnaissance

Background Domain Review

During which stage of a penetration test does an attacker attempt to gain access to a system?

- ☐ Maintaining Access
- ☐ Post-Exploitation
- ☐ **Exploitation**
- ☐ Reconnaissance

Background Domain Review

Which framework provides guidelines for security assessments?

- ☐ NIST SP 800-115
- ☐ NIST Open Assessment Guidelines
- ☐ NIST SP 909
- ☐ NIST SP 110

Background Domain Review

Which framework provides guidelines for security assessments?

- ☐ **NIST SP 800-115**
- ☐ NIST Open Assessment Guidelines
- ☐ NIST SP 909
- ☐ NIST SP 110

Background Domain Review

Which of the following is not a section of the OSSTMM?

- ☐ Defining a security test
- ☐ Wireless security testing
- ☐ Engaging Negotiations
- ☐ Human security testing

Background Domain Review

Which of the following is not a section of the OSSTMM?

- ☐ Defining a security test
- ☐ Wireless security testing
- ☐ **Engaging Negotiations**
- ☐ Human security testing

Background Domain Review

Which protocol works at Layer 5 of the OSI Model

- ☐ NetBIOS
- ☐ UDP
- ☐ ARP
- ☐ IP

Background Domain Review

Which protocol works at Layer 5 of the OSI Model

- ☐ **NetBIOS**
- ☐ UDP
- ☐ ARP
- ☐ IP

Background Domain Review

Which protocol works at Layer 3 of the OSI Model

- ☐ DNS
- ☐ IP
- ☐ TCP
- ☐ SNMP

Background Domain Review

Which protocol works at Layer 3 of the OSI Model

- ☐ DNS
- ☐ **IP**
- ☐ TCP
- ☐ SNMP

Background Domain Review

Check all protocols that can be useful for network enumeration.

- ☐ SMB
- ☐ HTTP
- ☐ SMTP
- ☐ SNMP

Background Domain Review

Check all protocols that can be useful for network enumeration.

- ☐ **SMB**
- ☐ HTTP
- ☐ **SMTP**
- ☐ **SNMP**

Background Domain Review

Which two layers of the OSI model are *not* layers of the TCP / IP model?

- ☐ Application
- ☐ Presentation
- ☐ Network
- ☐ Session

Background Domain Review

Which two layers of the OSI model are *not* layers of the TCP / IP model?

- ☐ Application
- ☐ **Presentation**
- ☐ Network
- ☐ **Session**

Background Domain Review

Which of the following is the correct syntax for attempting a Zone Transfer against the domain foosports.com using the name server ns.foosports.com?

- ☐ dig @ns.foosports.com -t axfr
- ☐ dig AXFR foosports.com @ns.foosports.com
- ☐ nslookup foosports.com
- ☐ nslookup @ns.foosports.com -t AZFR foosports.com

Background Domain Review

Which of the following is the correct syntax for attempting a Zone Transfer against the domain foosports.com using the name server ns.foosports.com?

- ☐ dig @ns.foosports.com -t axfr
- ☐ **dig AXFR foosports.com @ns.foosports.com**
- ☐ nslookup foosports.com
- ☐ nslookup @ns.foosports.com -t AZFR foosports.com