Congratulations! You passed!
TO PASS 80% or higher

Keep Learning

GRADE
100%

Week Four Practice Quiz

TOTAL POINTS 17

1. What traffic would an implicit deny firewall rule block? **1 / 1 point**

- ○ Inbound traffic
- ○ Outbound traffic
- ○ Nothing unless blocked
- ◉ Everything not allowed

Correct
You got it! Implicit deny means that everything is blocked, unless it's explicitly allowed.

2. The process of converting log entry fields into a standard format is called _____. **1 / 1 point**

- ○ Log encryption
- ○ Log analysis
- ○ Log auditing
- ◉ Log normalization

Correct
That's correct! Normalizing logs is the process of ensuring that all log fields are in a standardized format for analysis and search purposes.

3. A _____ can protect your network from DoS attacks. **1 / 1 point**

- ○ IP Source Guard
- ○ DHCP Snooping
- ◉ Flood Guard
- ○ Dynamic ARP Inspection

Correct
Yep! Flood guards provide protection from DoS attacks by blocking common flood attack traffic when it's detected.

4. Using different VLANs for different network devices is an example of _____. **1 / 1 point**

- ◉ Network Separation
- ○ Implicit Denial
- ○ Remote Access
- ○ Network Encryption

Correct
Exactly! Using VLANs to keep different types of devices on different networks is an example of network separation.

5. How do you protect against rogue DHCP server attacks? **1 / 1 point**

- ◉ DHCP Snooping
- ○ Dynamic ARP Inspection
- ○ Flood Guard
- ○ IP Source Guard

Correct
Nice job! DHCP snooping prevents rogue DHCP server attacks. It does this by creating a mapping of IP addresses to switch ports and keeping track of authoritative DHCP servers.

6. What does Dynamic ARP Inspection protect against? **1 / 1 point**

- ○ DoS attacks
- ◉ ARP Man-in-the-middle attacks
- ○ IP Spoofing attacks
- ○ Rogue DHCP Server attacks

Correct
Great work! Dynamic ARP inspection will watch for forged gratuitous ARP packets that don't correspond to the known mappings of IP addresses and MAC address, and drop the fake packets.

7. What kind of attack does IP Source Guard protect against? **1 / 1 point**

- ○ DoS attacks
- ○ Rogue DHCP Server attacks
- ○ ARP Man-in-the-middle attacks
- ◉ IP Spoofing attacks

Correct
You nailed it! IP Source Guard protects against IP spoofing. It does this by dynamically generating ACLs for each switch port, only permitting traffic for the mapped IP address for that port.

8. A reverse proxy is different from a proxy because a reverse proxy provides _____. **1 / 1 point**

- ◉ Remote Access
- ○ DoS protection
- ○ Authentication
- ○ Privacy

Correct
Correct! A reverse proxy can be used to allow remote access into a network.

9. What underlying symmetric encryption cipher does WEP use? **1 / 1 point**

- ○ DES
- ○ AES
- ◉ RC4
- ○ RSA

Correct
Awesome! WEP uses the RC4 stream cipher.

10. What key lengths does WEP encryption support? Check all that apply. **1 / 1 point**

- ☐ 40-bit
- ☑ 64-bit

Correct
Nice! WEP supports 64-bit and 128-bit encryption keys.

- ☑ 128-bit

Correct
Nice! WEP supports 64-bit and 128-bit encryption keys.

- ☐ 256-bit

11. What's the recommended way to protect a WPA2 network? Check all that apply. **1 / 1 point**

- ☐ Hide the SSID
- ☑ Use a unique SSID

Correct
That's exactly right! Because the SSID is used as a salt, it should be something unique to protect against rainbow table attacks. A long, complex password will protect against brute-force attacks.

- ☑ Use a long, complex passphrase

Correct
That's exactly right! Because the SSID is used as a salt, it should be something unique to protect against rainbow table attacks. A long, complex password will protect against brute-force attacks.

- ☐ Use WEP64

12. If you're connected to a switch and your NIC is in promiscuous mode, what traffic would you be able to capture? Check all that apply. **1 / 1 point**

- ☐ No traffic
- ☑ Traffic to and from your machine

Correct
Great job! Since you're connected to a switch, you'd only see packets that are sent to your switch port, meaning traffic to or from your machine or broadcast packets.

- ☐ All traffic on the switch
- ☑ Broadcast traffic

Correct
Great job! Since you're connected to a switch, you'd only see packets that are sent to your switch port, meaning traffic to or from your machine or broadcast packets.

13. What could you use to sniff traffic on a switch? **1 / 1 point**

- ○ Promiscuous Mode
- ○ Network hub
- ◉ Port Mirroring
- ○ DHCP Snooping

Correct
Yep! Port mirroring allows you to capture traffic on a switch port transparently, by sending a copy of traffic on the port to another port of your choosing.

14. What does tcpdump do? **1 / 1 point**

- ○ Brute forces password databases
- ◉ Performs packet capture and analysis
- ○ Generates DDoS attack traffic
- ○ Handles packet injection

Correct
Right on! tcpdump captures and analyzes packets for you, interpreting the binary information contained in the packets and converting it into a human-readable format.

15. Compared to tcpdump, wireshark has a much wider range of supported _____. **1 / 1 point**

- ○ Packet sizes
- ◉ Protocols
- ○ Packet types
- ○ Languages

Correct
Yep! Wireshark supports a very wide range of various networking protocols.

16. A Network Intrusion Detection System watches for potentially malicious traffic and _____ when it detects an attack. **1 / 1 point**

- ◉ Triggers alerts
- ○ Blocks traffic
- ○ Shuts down
- ○ Disables network access

Correct
Correct! A NIDS only alerts when it detects a potential attack.

17. What does a Network Intrusion Prevention System do when it detects an attack? **1 / 1 point**

- ○ It does nothing.
- ○ It attacks back.
- ◉ It blocks the traffic.
- ○ It triggers an alert.

Correct
Exactly! An NIPS would make adjustments to firewall rules on the fly, and drop any malicious traffic detected.