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

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

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

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
- ○ Dynamic ARP Inspection
- ◉ Flood Guard

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**

- ( ) IP Source Guard
- ( ) Flood Guard
- ( ) Dynamic ARP Inspection
- (●) DHCP Snooping

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**

- ( ) IP Spoofing attacks
- ( ) DoS attacks

- [x] ARP Man-in-the-middle 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**

- [ ] Rogue DHCP Server attacks
- [ ] ARP Man-in-the-middle attacks
- [x] IP Spoofing attacks
- [ ] DoS 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**

- [ ] Privacy
- [ ] DoS protection
- [ ] Authentication
- [x] Remote Access

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**

- ○ AES
- ○ RSA
- ○ DES
- ◉ RC4

✓ **Correct**
Awesome! WEP uses the RC4 stream cipher.

10. What key lengths does WEP encryption support? Check all that apply. **0 / 1 point**

- ☐ 40-bit
- ☑ 64-bit

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

- ☐ 128-bit
- ☐ 256-bit

You didn’t select all the correct answers

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

- ☑ 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.

- ☐ Hide the SSID
- ☑ 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. **0.75 / 1 point**

- [x] 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
- [ ] No traffic
- [ ] Broadcast traffic

You didn't select all the correct answers

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

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

Correct

Yes! 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**

- (●) Performs packet capture and analysis
- ( ) Brute forces password databases
- ( ) 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 types
- ( ) Packet sizes
- ( ) Languages
- (●) Protocols

✓ **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
- ( ) Disables network access
- ( ) Blocks traffic
- ( ) Shuts down

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

Correct

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