What does tcpdump do? Select all that apply. **1 / 1 point**

- [ ] Generates packets
- [x] Captures packets

Correct
Correct! Tcpdump is a popular, lightweight command line tool for capturing packets and analyzing network traffic.

- [x] Analyzes packets and provides a textual analysis

Correct
Correct! Tcpdump is a popular, lightweight command line tool for capturing packets and analyzing network traffic.

- [ ] Encrypts your packets

2. What does wireshark do differently from tcpdump? Check all that apply. **1 / 1 point**

- [x] It understands more application-level protocols.

Correct
Awesome job! tcpdump is a command line utility, while wireshark has a powerful graphical interface. While tcpdump understands some application-layer protocols, wireshark expands on this with a much larger complement of protocols understood.

- [ ] It can capture packets and analyze them.
- [ ] It can write packet captures to a file.
- [x] It has a graphical interface.

Correct
Awesome job! tcpdump is a command line utility, while wireshark has a powerful graphical interface. While tcpdump understands some application-layer protocols, wireshark expands on this with a much larger complement of protocols understood.

3. What factors should you consider when designing an IDS installation? Check all that apply. **1 / 1 point**

- [x] Storage capacity

Correct
Wohoo! It's important to understand the amount of traffic the IDS would be analyzing. This ensures that the IDS system is capable of keeping up with the volume of traffic. Storage capacity is important to consider for logs and packet capture retention reasons.

- [ ] Internet connection speed
- [ ] OS types in use
- [x] Traffic bandwidth

Correct
Wohoo! It's important to understand the amount of traffic the IDS would be analyzing. This ensures that the IDS system is capable of keeping up with the volume of traffic. Storage capacity is important to consider for logs and packet capture retention reasons.

4. What is the difference between an Intrusion Detection System and an Intrusion Prevention System? **1 / 1 point**

- (•) An IDS can alert on detected attack traffic, but an IPS can actively block attack traffic.
- ( ) An IDS can actively block attack traffic, while an IPS can only alert on detected attack traffic.
- ( ) An IDS can detect malware activity on a network, but an IPS can't
- ( ) They are the same thing.

Correct

That's exactly right! An IDS only detects intrusions or attacks, while an IPS can make changes to firewall rules to actively drop or block detected attack traffic.

5. What factors would limit your ability to capture packets? Check all that apply. **1 / 1 point**

- [x] Network interface not being in promiscuous or monitor mode

Correct
You got it! If your NIC isn't in monitor or promiscuous mode, it'll only capture packets sent by and sent to your host. In order to capture traffic, you need to be able to access the packets. So, being connected to a switch wouldn't allow you to capture other clients' traffic.

- [ ] Anti-malware software
- [ ] Encryption
- [x] Access to the traffic in question

Correct
You got it! If your NIC isn't in monitor or promiscuous mode, it'll only capture packets sent by and sent to your host. In order to capture traffic, you need to be able to access the packets. So, being connected to a switch wouldn't allow you to capture other clients' traffic.