Quiz Results

Name: Ignas Kamugisha
Attempt: 1st Attempt

Assessment Statistics

- **Score:** 77.5% (7.75 out of 10 points)
- **Time for this attempt:** 5 minutes 55 seconds
- **Attempts Left:** 1 attempt

Attempt History

Attempt	Points	Score	Highest Score Kept?
Attempt 1	7.75 of 10	77.5%	(Highest score)

Your Answers

Question 1 (1/1 point)

Question:
What is the primary difference between a denial of service (DOS) attack and a distributed denial of service (DDOS) attack? Which one is typically more harmful? (choose all that apply)

Your Answer: - A DOS attack is typically more harmful as it is a single target with more resources.

Correct Answers: - A DDOS attack is typically more harmful.
- A distributed denial of service attack involves multiple hosts that willingly or more likely, unwillingly, attack a target.
- A denial of service attack is where a target is attacked with the goal of reducing or eliminating the availability of the service that target provides.
- A denial of service attack can affect a web server where you may not be able to access a web application.

Other Provided Answer (Incorrect): - A distributed denial of service attack involves one host attacking a distributed network.

Question 2 (0/1 point)

Question:
Which of the following best describes how a TCP SYN flood attack works?

Your Answer (Incorrect): - By spoofing the destination port number in the packet, a TCP SYN is generated and sent right back to the sender.

Correct Answer: - By spoofing the source IP address, another hosts sends SYN-ACK packets to a target.

Other Options (Not Selected): - By spoofing the destination IP address, another hosts sends SYN-ACK packets to a target.
- By spoofing the source port number in the packet, a TCP SYN is generated and sent by the host to itself.
- By spoofing the source IP address, another hosts sends SYN-ACK packets to a target.

Question 3 (1/1 point)

Question:
Which of the following commands allow you to start, stop, and manage services on a Linux operating system?

Other Options (Not Selected): - chown
- services.msc
- journalctl

Correct Answer: - systemctl

Question 4 (1/1 point)

Question:
Using the whois service, what is the technical contact phone number for the following domain: CWRU

Other Options (Not Selected): - 216-578-0092
- 216-368-1234
- 216-534-0029

Correct Answer: - 216-368-1253

Question 5 (0.75/1 point)

Question:
If a browser is warning that a site cannot be trusted, what issues could exist with the certificate?

Correct Answers: - The certificate expired
- Your operating system does not trust the issuer of the certificate
- The certificate has been revoked
- The certificate DN does not match the domain name of the website

Incorrect Answer (Selected): - The public key was not verified with the private key that we have for the web server

Question 6 (1/1 point)

Question:
What are the differences between symmetric and asymmetric? (Choose all that apply)

Your Incorrect Answers: - Symmetric encryption uses a private/public key pair where asymmetric uses a single shared key.
- A symmetric key is typically larger than an asymmetric key.
- Symmetric encryption is typically slower than asymmetric.

Correct Answers: - A symmetric key is typically smaller than an asymmetric key.
- Symmetric encryption is typically faster than asymmetric.
- Symmetric encryption uses a single shared key where asymmetric uses a private/public key pair.

Question 7 (1/1 point)

Question:
The CIA triad serves as our compass in the security field. Match each term below to its correct definition:

Term	Definition
Confidentiality	Ensuring only those that should have access to view data can view it.
Availability	Ensuring that systems are available.
Integrity	Ensuring that data was not modified from an unauthorized source.

Question 8 (1/1 point)

Question:
Which of the following flags will help determine the software version of services when scanning a host using nmap?

Other Options (Not Selected): - –version
- –scan-full
- -v

Correct Answer: - -sV

Question 9 (1/1 point)

Question:
Which of the following commands would allow a user to read and execute a file, a group to read the file, and everyone else to have no permissions?

Other Options (Not Selected): - chmod 640 somefile
- chmod 650 somefile
- chmod 620 somefile

Correct Answer: - chmod 540 somefile

Question 10 (0/1 point)

Question:
What best describes the difference between a packet filter and a stateful firewall?

Your Incorrect Answer: - A packet filter firewall will block or allow traffic based on just the source and destination IPs where a stateful firewall detects the current state of the network zone to determine if an intrusion has occurred.

Correct Answer: - A packet filter firewall will block or allow traffic based on the source and destination IPs and ports where a stateful firewall will additionally detect the current state of traffic such as a closed TCP connection and not allow subsequent TCP packets for that connection.

Other Options (Not Selected): - There are no differences between the two types of firewalls.
- A packet filter firewall will block or allow traffic based on the source and destination IPs and ports where a stateful firewall will additionally detect the current state of traffic such as a closed TCP connection and not allow subsequent TCP packets for that connection.
- A packet filter firewall will block or allow traffic based on just the source and destination IPs where a stateful firewall allows you to allow/block traffic using ports.