Google IT Support Certificate: Course 5: IT Security - Defense Against the Digital Dark Arts

Week 4: Securing Your Networks

Quiz: Securing Your Networks

Question 1:

What does tcpdump do?

Performs packet capture and analysis

Brute forces password databases

Generates DDoS attack traffic

Handles packet injection

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

Question 2:

What can protect your network from DoS attacks?

IP Source Guard

Dynamic ARP Inspection

DHCP Snooping

Flood Guard

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

Question 3:

What occurs after a Network Intrusion Detection System (NIDS) first detects an attack?

Disables network access

Triggers alerts

Shuts down

Blocks traffic

A NIDS only alerts when it detects a potential attack.

Question 4:

What does a Network Intrusion Prevention System (NIPS) do when it detects an attack?

It triggers an alert.

It blocks the traffic.

It attacks back.

It does nothing.

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

Question 5:

How do you protect against rogue DHCP server attacks?

Flood Guard

IP Source Guard

DHCP Snooping

Dynamic ARP Inspection

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.

Question 6:

What underlying symmetric encryption cipher does WEP use?

RSA

RC4

DES

AES

WEP uses the RC4 stream cipher.

Question 7:

What traffic would an implicit deny firewall rule block?

Outbound traffic only

Inbound traffic only

Everything that is not explicitly permitted or allowed

Nothing unless blocked

Implicit deny means that everything is blocked, unless it's explicitly allowed.

Question 8:

What allows you to take all packets from a specified port, port range, or an entire VLAN and mirror the packets to a specified switch port?

Network hub

DHCP Snooping

Port Mirroring

Promiscuous Mode

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.

Question 9:

What kind of attack does IP Source Guard (IPSG) protect against?

Rogue DHCP Server attacks

DoS attacks

IP Spoofing attacks

ARP Man-in-the-middle attacks

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.

Question 10:

What can be configured to allow secure remote connections to web applications without requiring a VPN?

Web browser

RC4

Reverse proxy

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