Networking Guided Notes

Lesson 4.2.1 - Technology-Based Attacks

Use the following passage to answer questions 1-3.

David, a software engineer, became disgruntled with his employer and decided to shutdown the company website using computers he previously infected. The computers were used to deliver an attack against the website that shut the site down for 24 hours.

1. What kind of network attack was this?

DDos

2. What are the infected computers known as?

A Bonet

3. What is David known as?

Botmaster

4. Match the following network attack types with their proper description.

A. Adversary-in-the-middle attack	____	Server impersonates a legitimate server, offering IP addresses and other network information
B. DNS poisoning	____	Malicious actor accessing ports that a typical system does not have access to
C. VLAN hopping	____	Attacker positions themselves in between a user and their intended destination
D. ARP spoofing	____	Network device has been installed on a secure network without proper authorization
E. Rogue DHCP	____	Device on a network lies about their MAC address
F. Rogue AP	____	Server has been altered and does not translate the proper IP address to a domain name

5. Minion Healthcare has experienced a network attack that has encrypted all their patient's medical files. They just recently received a notification demanding $10 million for the encryption key. What kind of attack has Minion Healthcare witnessed?

Ransomware

6. Name four types of Malware

Ransomware, spyware, keyloggers, RATs, rootKits, trojans, virus, worm, Adware

7. What is the difference between a brute force attack and a dictionary attack?

Brute force attack uses all possible combinations of valid letters, numbers, and symbols. However, a dictionary attack uses commonly used passwords and commonly used words in passwords in order to try and crack the password faster.

8. What is a deauthentication attack?

A deauthentication attack is an attack that sends a deauthentication frame to a wireless network point in order to disconnect a device from the network.