Module Practice and Quiz

3.11.1

Packet Tracer - Network Security Exploration

In this Packet Tracer Physical Mode (PTPM) activity, you will explore and implement several security procedures in different locations within the city of Greenville, North Carolina. Included are networks in a Data Center, an ISP, a Coffee Shop, and a Home.

The Data Center is provisioned for environmental and physical security. There is also software included to maintain access control. You will install an Internet of Things (IoT) smoke detector.

The Coffee Shop offers free wireless access to their patrons. You will implement a VPN to secure traffic.

The Home includes an office, a student's bedroom, and a living room. You will configure two home wireless LANs (WLANs) to require authentication for two different user types: family members and guests. These networks will also be configured with MAC address filtering to restrict access.

Network Security Exploration - Physical Mode

Network Security Exploration - Physical Mode

3.11.2

What did I learn in this module?

Network security breaches can disrupt e-commerce, cause the loss of business data, threaten people's privacy, and compromise the integrity of information. Assets must be identified and protected. Vulnerabilities must be addressed before they become a threat and are exploited. Mitigation techniques are required before, during, and after an attack. An attack vector is a path by which a threat actor can gain access to a server, host, or network. Attack vectors originate from inside or outside the corporate network.

The term 'threat actor' includes hackers and any device, person, group, or nation state that is, intentionally or unintentionally, the source of an attack. There are "White Hat", "Gray Hat", and "Black Hat" hackers. Cyber criminals operate in an underground economy where they buy, sell, and trade attack toolkits, zero day exploit code, botnet services, banking Trojans, keyloggers, and more. Hacktivists tend to rely on fairly basic, freely available tools. State-sponsored hackers create advanced, customized attack code, often using previously undiscovered software vulnerabilities called zero-day vulnerabilities.

Attack tools have become more sophisticated and highly automated. These new tools require less technical knowledge to implement. Ethical hacking involves many different types of tools used to test the network and keep its data secure. To validate the security of a network and its systems, many network penetration testing tools have been developed. Common types of attacks are: eavesdropping, data modification, IP address spoofing, password-based, denial-of-service, man-in-the-middle, compromised-key, and sniffer.

The three most common types of malware are worms, viruses, and Trojan horses. A worm executes arbitrary code and installs copies of itself in the memory of the infected computer. A virus executes a specific unwanted, and often harmful, function on a computer. A Trojan horse is non-self-replicating. When an infected application or file is downloaded and opened, the Trojan horse can attack the end device from within. Other types of malware are: adware, ransomware, rootkit, and spyware.

Networks are susceptible to the following types of attacks: reconnaissance, access, and DoS. Threat actors use reconnaissance (or recon) attacks to do unauthorized discovery and mapping of systems, services, or vulnerabilities. Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services. Types of access attacks are: password, spoofing, trust exploitations, port redirections, man-in-the-middle, and buffer overflow. Social engineering is an access attack that attempts to manipulate individuals into performing actions or divulging confidential information. DoS and DDoS are attacks that create some sort of interruption of network services to users, devices, or applications.

Threat actors can send packets using a spoofed source IP address. Threat actors can also tamper with the other fields in the IP header to carry out their attacks. IP attack techniques include: ICMP, amplification and reflection, address spoofing, MITM, and session hijacking. Threat actors use ICMP for reconnaissance and scanning attacks. They launch information-gathering attacks to map out a network topology, discover which hosts are active (reachable), identify the host operating system (OS fingerprinting), and determine the state of a firewall. Threat actors often use amplification and reflection techniques to create DoS attacks.

TCP segment information appears immediately after the IP header. TCP provides reliable delivery, flow control, and stateful communication. TCP attacks include: TCPSYN Flood attack, TCP reset attack, and TCP Session hijacking. UDP is commonly used by DNS, TFTP, NFS, and SNMP. It is also used with real-time applications such as media streaming or VoIP. UDP is not protected by encryption. UDP Flood attacks send a flood of UDP packets, often from a spoofed host, to a server on the subnet. The result is very similar to a DoS attack.

Any client can send an unsolicited ARP Reply called a "gratuitous ARP." This mean that any host can claim to be the owner of any IP or MAC. A threat actor can poison the ARP cache of devices on the local network, creating an MITM attack to redirect traffic. ARP cache poisoning can be used to launch various man-in-the-middle attacks. DNS attacks include: open resolver attacks, stealth attacks, domain shadowing attacks, and tunneling attacks. To stop DNS tunneling, the network administrator must use a filter that inspects DNS traffic. A DHCP spoofing attack occurs when a rogue DHCP server is connected to the network and provides false IP configuration parameters to legitimate clients.

Most organizations follow the CIA information security triad: confidentiality, integrity, and availability. To ensure secure communications across both public and private networks, you must secure devices including routers, switches, servers, and hosts. This is known as defense-in-depth. A firewall is a system, or group of systems, that enforces an access control policy between networks. To defend against fast-moving and evolving attacks, you may need an intrusion detection systems (IDS), or the more scalable intrusion prevention systems (IPS).

The four elements of secure communications are data integrity, origin authentication, data confidentiality, and data non-repudiation. Hash functions guarantee that message data has not changed accidentally or intentionally. Three well-known hash functions are MD5 with 128-bit digest, SHA hashing algorithm, and SHA-2. To add authentication to integrity assurance, use a keyed-hash message authentication code (HMAC). HMAC is calculated using any cryptographic algorithm that combines a cryptographic hash function with a secret key. Symmetric encryption algorithms using DES, 3DES, AES, SEAL, and RC are based on the premise that each communicating party knows the pre-shared key. Data confidentiality can also be ensured using asymmetric algorithms, including Rivest, Shamir, and Adleman (RSA) and the public key infrastructure (PKI). Diffie-Hellman (DH) is an asymmetric mathematical algorithm where two computers generate an identical shared secret key without having communicated before.

3.11.3

Module Quiz - Network Security Concepts

1. The IT department is reporting that a company web server is receiving an abnormally high number of web page requests from different locations simultaneously. Which type of security attack is occurring?
   - (•) DDoS
   - ( ) phishing
   - ( ) adware
   - ( ) social engineering
   - ( ) spyware

2. What causes a buffer overflow?
   - (•) attempting to write more data to a memory location than that location can hold
   - ( ) sending too much information to two or more interfaces of the same device, thereby causing dropped packets
   - ( ) sending repeated connections such as Telnet to a particular device, thus denying other data sources
   - ( ) launching a security countermeasure to mitigate a Trojan horse
   - ( ) downloading and installing too many software updates at one time

3. Which objective of secure communications is achieved by encrypting data?
   - (•) confidentiality
   - ( ) availability
   - ( ) integrity
   - ( ) authentication

4. What type of malware has the primary objective of spreading across the network?
   - ( ) Trojan horse
   - (•) worm
   - ( ) botnet
   - ( ) virus

5. What three items are components of the CIA triad? (Choose three.)
   - [ ] access
   - [x] availability
   - [ ] intervention
   - [x] confidentiality
   - [ ] scalability
   - [x] integrity

6. Which cyber attack involves a coordinated attack from a botnet of zombie computers?
   - ( ) MITM
   - (•) DDoS
   - ( ) address spoofing
   - ( ) ICMP redirect

7. What specialized network device is responsible for enforcing access control policies between networks?
   - ( ) switch
   - (•) firewall
   - ( ) bridge
   - ( ) IDS

8. To which category of security attacks does man-in-the-middle belong?
   - (•) access
   - ( ) DoS
   - ( ) social engineering
   - ( ) reconnaissance

9. What is the role of an IPS?
   - ( ) to filter traffic based on defined rules and connection context
   - ( ) to filter traffic based on Layer 7 information
   - (•) to detect patterns of malicious traffic by the use of signature files
   - ( ) to enforce access control policies based on packet content

10. Which type of DNS attack involves the cybercriminal compromising a parent domain and creating multiple subdomains to be used during the attacks?
    - ( ) tunneling
    - (•) shadowing
    - ( ) cache poisoning
    - ( ) amplification and reflection

11. Which two types of hackers are typically classified as grey hat hackers? (Choose two.)
    - [ ] state-sponsored hackers
    - [x] vulnerability brokers
    - [ ] script kiddies
    - [ ] cyber criminals
    - [x] hacktivists

12. What is a significant characteristic of virus malware?
    - ( ) A virus can execute independently of the host system.
    - (•) A virus is triggered by an event on the host system.
    - ( ) Once installed on a host system, a virus will automatically propagate itself to other systems.
    - ( ) Virus malware is only distributed over the Internet.

13. A cleaner attempts to enter a computer lab but is denied entry by the receptionist because there is no scheduled cleaning for that day. What type of attack was just prevented?
    - ( ) phishing
    - ( ) war driving
    - ( ) shoulder surfing
    - (•) social engineering
    - ( ) Trojan

Check

Show Me

Reset