Assignment module 6: Network Security, Maintenance, and Troubleshooting Procedures

Section 1: Multiple Choice

1. What is the primary purpose of a firewall in a network security infrastructure?

b) Filtering and controlling network traffic.

Ans: A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules, it accepts, rejects, or drops that specific traffic. It acts like a security guard that helps keep your digital world safe from unwanted visitors and potential threats.

Accept: allow the traffic

Reject: block the traffic but reply with an “unreachable error”

Drop: block the traffic with no reply

Need For Firewall

A firewall is essential because networks are constantly exposed to both safe and harmful traffic from the internet or other networks. Without a firewall, your systems would have no protection against unwanted access, malicious activity, or accidental data leaks.

1. Preventing Unauthorized Access

Imagine your house door is always open. Anyone passing by could walk in and take your things.

A firewall is like a locked door with a guard, letting only trusted people in and keeping strangers out.

2. Blocking Malicious Traffic

Think of your email inbox. Without a spam filter, you’d get flooded with scam and spam messages. A firewall works like that spam filter it blocks harmful data before it reaches you.

3. Protecting Sensitive Information

It’s like keeping your bank PIN in a safe instead of leaving it on the table where anyone can see it. A firewall ensures your personal and business data stays hidden from cybercriminals.

4. Preventing Cyber Attacks

If you leave your car unlocked in a parking lot, thieves can steal it. A firewall locks your network so attackers can’t hijack it.

5. Controlling Network Usage

Just like parents set parental controls so kids can’t visit unsafe websites, Firewalls control where your computers are allowed to connect.

Working of Firewall

A firewall works like a security guard for your network, standing between your internal systems such as computers, servers, and devices and the outside world, like the internet or other networks. It carefully inspects all data entering or leaving to ensure only safe traffic is allowed through.

When data tries to enter or leave your network, it passes through the firewall first.

The firewall examines the data packets (small chunks of information) using predefined rules.

Rules can be defined on the firewall based on the necessity and security policies of the organization.

FIrewall allows decision making like Allow → If the packet matches safe rules. or Block → If the packet is suspicious, from a blacklisted source, or contains malicious code.

Default policy:

It is very difficult to explicitly cover every possible rule on the firewall. For this reason, the firewall must always have a default policy. Default policy only consists of action (accept, reject or drop). Suppose no rule is defined about SSH connection to the server on the firewall. So, it will follow the default policy. If default policy on the firewall is set to accept, then any computer outside of your office can establish an SSH connection to the server. Therefore, setting default policy as drop (or reject) is always a good practice.

Types of Firewall

1) Network Placement

Packet Filtering Firewall

Stateful Inspection Firewall

Proxy Firewall (Application Level)

Circuit-Level Gateway

Web Application Firewall (WAF)

Next-Generation Firewall (NGFW)

2) Systems Protected

Network Firewall

Host-Based Firewall

3) Data Filtering Method

Perimeter Firewall

Internal Firewall

Distributed Firewall

4) Form Factors

Hardware Firewall

Software Firewall

2. What type of attack involves flooding a network with excessive traffic to disruptnormal operation?

a) Denial of Service (DoS)

The answer is indeed a) Denial of Service (DoS). A DoS attack is a type of cyberattack that involves overwhelming a network or server with a flood of excessive, often irrelevant, traffic from a single source to disrupt its normal operations and make it unavailable to legitimate users.

DoS Attacks Work?

DoS attacks typically exploit vulnerabilities in a target's network or computer systems. Attackers can use a variety of methods to generate overwhelming traffic or requests, including:

Flooding the target with a massive amount of data

Sending repeated requests to a specific part of the system

Exploiting software vulnerabilities to crash the system

Prevention Given that Denial of Service (DoS) attacks are becoming more frequent, it is a good time to review the basics and how we can fight back.

Cloud Mitigation Provider - Cloud mitigation providers are experts at providing DDoS mitigation from the cloud. This means they have built out massive amounts of network bandwidth and DDoS mitigation capacity at multiple sites around the Internet that can take in any type of network traffic, whether you use multiple ISP's, your own data center, or any number of cloud providers. They can scrub the traffic for you and only send "clean" traffic to your data center.

Firewall - This is the simplest and least effective method. Python scripts are often written to filter out malicious traffic, or existing firewalls can be utilized by enterprises to block such traffic.

Internet Service Provider (ISP) - Some enterprises use their ISP to provide DDoS mitigation. These ISPs have more bandwidth than an enterprise would, which can help with large volumetric attacks.

Features to help mitigate these attacks:

Network Segmentation: Segmenting the network can help prevent a DoS attack from spreading throughout the entire network. This limits the impact of an attack and helps to isolate the affected systems.

Implement Firewalls: Firewalls can help prevent DoS attacks by blocking traffic from known malicious IP addresses or by limiting the amount of traffic allowed from a single source.

Use Intrusion Detection and Prevention Systems: Intrusion Detection and Prevention Systems (IDS/IPS) can help to detect and block DoS attacks by analyzing network traffic and blocking malicious traffic.

Limit Bandwidth: Implementing bandwidth limitations on incoming traffic can help prevent a DoS attack from overwhelming the network or server.

Implement Content Delivery Network (CDN): A CDN can help to distribute traffic and reduce the impact of a DoS attack by distributing the load across multiple servers.

Use Anti-Malware Software: Anti-malware software can help to detect and prevent malware from being used in a DoS attack, such as botnets.

Perform Regular Network Scans: Regular network scans can help identify vulnerabilities and misconfigurations that can be exploited in a DoS attack. Patching these vulnerabilities can prevent a DoS attack from being successful.

Develop a Response Plan: Having a DoS response plan in place can help minimize the impact of an attack. This plan should include steps for identifying the attack, isolating affected systems, and restoring normal operations.

3. Which encryption protocol is commonly used to secure wireless network communications?

b) WPA (Wi-Fi Protected Access)

The two security protocols and security certification programs are Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2). These are developed by the Wi-Fi Alliance to secure wireless computer networks. The Alliance defined these protocols because of the serious weaknesses the researchers found in the previous system, Wired Equivalent Privacy (WEP). In this article, we will learn about the wep, wpa, versions of wpa, working with wpa, and how to identify the security type.

What is WEP?

Wired Equivalent Privacy (WEP) is an early security protocol for wireless networks. Introduced in 1997, WEP was designed to provide a level of security comparable to wired networks by encrypting data sent over Wi-Fi. It uses a static key to encrypt data, which is shared between devices and the wireless router. However, WEP has significant weaknesses, such as vulnerabilities to various hacking methods, making it easy for attackers to break the encryption and access the network. Because of these issues, WEP has been largely replaced by more secure protocols like WPA and WPA2.

What is Wifi Protected Access (WPA)?

WPA also referred to as the draft IEEE 802.11i standard became available in 2003. The Wi-Fi Alliance made it an intermediate measure in anticipation of the availability of the more secure and complex WPA2, which became available in 2004 and is a common short for the full IEEE 802.11i standard. In 2003, WPA also known as the TKIP standard became accessible. It was meant to be a stopgap measure by the Wi-Fi Alliance before the more complicated and secure WPA2 became available in 2004. WPA2 is a common acronym for the entire IEEE 802.11i (or IEEE 802.11i-2004) standard.

In January 2018, with several security improvements over WPA2 Wi-Fi Alliance announced the release of WPA3.

Versions of WPA

There are some different versions of WPA which include WPA, WPA2, and WPA3. Different versions have different features, Below mentioned are versions of WiFi Protected Access:

1. WPA

The WPA is an intermediate measure to take the place of WEP. WPA could be implemented through firmware upgrades on wireless network interface cards that were designed for WEP in 1999. However, since more changes were required in the wireless access points (APs) than those needed on the network cards, most pre-2003 APs could not be upgraded to support WPA.

The WPA protocol implements almost all of the IEEE 802.11i standard. WEP used a 64-bit or 128-bit encryption key that must be manually entered on wireless access points and devices which once entered can never be changed. TKIP employs a per-packet key, which means that it dynamically

generates a new 128-bit key for each packet and thus prevents the types of attacks that compromise WEP.

WPA includes a Message Integrity Check, which is designed to prevent an attacker from altering or resending data packets. This replaced the cyclic redundancy check (CRC) that was used by the WEP standard. CRC's had a main flaw in that it did not provide a sufficiently strong data integrity guarantee for the packets it handled. Well-tested message authentication codes existed to solve these problems, but they required too much computation to be used on old network cards. WPA uses a message integrity check algorithm called TKIP to verify the integrity of the packets. TKIP is much stronger than a CRC, but the algorithm used in WPA2 is stronger. Researchers discovered a flaw in WPA similar to older weaknesses in WEP and the limitations of the message integrity code hash function, named Michael, that is used to retrieve the keystream from short packets to use for re-injection and spoofing.

2. WPA2

WPA2 replaced WPA. WPA2, which requires testing and certification by the Wi-Fi Alliance, implemented the mandatory elements of IEEE 802.11i. Particularly, it included mandatory support for CCMP(Counter Mode CBC-MAC Protocol), an AES(Advanced Encryption Standard) based encryption mode. Certification began in September 2004. WPA2 certification is mandatory for all new devices to bear the Wi-Fi trademark from March 13, 2006.

What are the New Features Does the WPA2 Protocol Offer?

WPA was replaced in 2004 with WPA2. WPA2 employs the Block Chaining Message Authentication Code Protocol (CCMP), a Counter Mode Cypher. The Advanced Encryption Standard (AES) algorithm, which verifies the authenticity and integrity of messages, forms the foundation of the CCMP protocol. Compared to the original Temporal Key Integrity Protocol (TKIP) used by WPA, CCMP is more robust and dependable.

However, WPA2 still has security flaws. The risk of unwanted access to the company wireless network is the main one among those weaknesses. This occurs when an attack vector on specific Wi-Fi Protected Setup (WPS) access points is compromised. To deter such threats, it is advised that WPS be turned off for every WPA2 attack vector access point. Threat actors can use downgrade attacks to target more vulnerabilities in WPA2.

3. WPA3

In 2018, Wi-Fi Protected Access 3, or WPA3, replaced WPA2. The most recent and improved version of WPA is WPA3. In 2018, the Wi-Fi Alliance started certifying goods that had been WPA3-approved. Not all devices immediately incorporate WPA3 capability. Users must either purchase brand-new routers that support WPA3 or have the equipment upgraded by the manufacturer in order to use WPA3-approved devices, such as wireless routers.

What are the New Features Does the WPA3 Protocol Offer?

In 2018, Wi-Fi Protected Access 3, or WPA3, replaced WPA2. WPA3 is the most recent version of the WPA protocol. In 2018, the Wi-Fi Alliance started to certify products that met WPA3 standards. Not every device has WPA3 support added to it automatically. If users want to use wireless routers or other WPA3-approved devices, they have two options: either purchase new routers that enable WPA3 or have the manufacturer update the device. A comparable 192-bit cryptographic strength (in WPA3-EAP enterprise mode), 384-bit Hashed Message Authentication Mode (HMAC), 256-bit Broadcast/Multicast Integrity Protocol (BIP-GMAC-256), 256-bit Galois/Counter Mode Protocol encryption (GCMP-256), SAE exchange, and WiFi Device Provisioning Protocol (DPP).

Working with WPA

When establishing a network for others to connect to and when connecting to a wireless network, you'll see options for employing WPA. Although it was intended to enable pre-WPA devices like those that use WEP, some only function with WPA after a firmware update. Some things are just not compatible.

Despite the protocol being more secure than WEP, attacks can still be made against WPA pre-shared keys. Your best line of defence is a passphrase that can withstand brute-force attacks.

Security Issues with WPA

Key shared ahead of time If users rely on a weak password or passphrase, WPA and WPA2 are still susceptible to password cracking attempts.

Insufficient upfront secrecy

Due to the lack of forward secrecy offered by WPA and WPA2, an adversary may be able to passively and covertly gather all packets encrypted with that PSK transmitted in the past and even in the future once they ascertain the pre-shared key.

Tactics known as denial of service, in which an attacker overloads the network with messages, impairing the availability of network resources

Eavesdropping is the practice of unauthorised third parties intercepting data being transferred across secure networks. Spoofing and session hijacking are methods by which an attacker obtains access to network resources and data by impersonating a legitimate user.

How to Identify Your Wi-Fi Security Type?

To identify your Wi-Fi security type, follow these steps:

1. On Windows:

Click the Wi-Fi icon in the taskbar and select your network.

Right-click on your Wi-Fi network and select Properties.

Look for the Security type under the "Network security settings" section.

2. On macOS:

Click the Wi-Fi icon in the menu bar and select Open Network Preferences.

Click Advanced, then select your network.

Look for the Security field in the details.

3. On Mobile Devices:

iOS: Open Settings > Wi-Fi > Tap on your network (i) > Check the Security field.

Android: Open Settings > Wi-Fi > Tap on your network > Check the Security field.

4. Router Settings:

Log in to your router's admin page (typically by entering the router's IP address in your browser).

Navigate to the Wireless or Security settings section.

Check the Security Mode or Encryption settings to see your Wi-Fi security type.

Common security types include WPA2, WPA3, WEP, and WPA

Difference Between WEP and WPA

A security standard for computers with wireless internet connections is called Wi-Fi Protected Access (WPA). The Wi-Fi Alliance developed it to improve upon the original Wi-Fi security standard, Wired Equivalent Privacy (WEP), in terms of data encryption and user authentication.

Features

WEP

WPA

Encryption

Relies on RC4 encryption set of rules.

Supports TKIP and AES encryption algorithms for more potent protection.

Vulnerabilities

Vulnerable to numerous attacks, including brute-pressure attacks, packet sniffing, and key restoration assaults.

Addresses among the vulnerabilities found in WEP, presenting stronger safety towards attacks.

Key Management

Uses static encryption keys which can be manually configured and infrequently changed.

Supports dynamic key exchange protocols, such as WPA-Personal (the use of Pre-Shared Key) or WPA-Enterprise (using IEEE 802.1X authentication), for advanced key management and protection.

Compatibility

Widely supported by older Wi-Fi devices, however compatibility can be reducing as it's far considered outdated.

Compatible with most present day Wi-Fi devices, although older devices won't aid newer encryption protocols like AES.

Security Protocol

Uses WEP encryption protocol.

Uses more potent encryption protocols inclusive of TKIP (Temporal Key Integrity Protocol) and later AES (Advanced Encryption Standard).

For more, you can refer to Difference Between WEP and WPA.

Conclusion

Wi-Fi Protected Access (WPA) improved the security of wireless networks by fixing the weaknesses in older methods like WEP. It introduced better encryption and key management. While WPA2 and WPA3 are now more commonly used because they are even more secure, WPA was an important step in making Wi-Fi safer. Knowing about WPA helps us understand why it’s important to use up-to-date security for protecting Wi-Fi connections.

Section 2: True or false

Patch management is the process of regularly updating software

and firmware to address security vulnerabilities and improve system

performance.

Ans: True

A network administrator should perform regular backups of

critical data to prevent data loss in the event of hardware failures, disasters, or

security breaches.

Ans: True

Traceroute is a network diagnostic tool used to identify the

route and measure the latency of data packets between a source and

destination device

Ans: True

Section 3: Short

8. Describe the steps involved in conducting a network vulnerability Assignment.

Define Scope and Objectives.

Identify what parts of the network will be assessed (e.g., internal, external, specific servers).

Set goals: compliance, security hardening, risk identification, etc.

Gather Information (Reconnaissance)

Collect data about the network, IP ranges, devices, operating systems, open ports, etc.

Use tools like Nmap for network scanning.

Identify Vulnerabilities

Use vulnerability scanning tools (e.g., Nessus, OpenVAS, Qualys) to detect known weaknesses.

Look for outdated software, misconfigurations, weak passwords, etc.

Analyze and Validate Findings

Review scan results to confirm true vulnerabilities (reduce false positives).

Prioritize vulnerabilities based on severity and risk level (e.g., using CVSS scores).

Report Results

Document findings with descriptions, risk levels, affected systems, and remediation suggestions.

Create both a technical and a management-level report.

Recommend and Implement RemediatiProvide clear recommendations to fix the vulnerabilities (e.g., patching, config changes).

Work with IT/security teams to implement fixes.

Re-test and Continuous Monitoring

Re-scan after fixes to ensure issues are resolved.

Set up regular assessments and monitoring as part of ongoing security practices.