Name :- Dave Ujjawal

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?

A) Encrypting Network Traffic
B) Filtering And Controlling Network Traffic
C) Assigning Ip Addresses To Devices
D) Authenticating Users For Network Access

Ans:- B) Filtering And Controlling Network Traffic

Reason: A Firewall Acts Like a Security Guard. It Checks Data Going In And Out Of The Network And Blocks Harmful Or Unwanted Traffic. It Does Not Assign Ips Or Encrypt Data — Its Main Job Is To Filter.

2).. What Type Of Attack Involves Flooding a Network With Excessive Traffic To Disrupt
Normal Operation?

A) Denial Of Service (Dos)
B) Phishing
C) Spoofing
D) Man-In-The-Middle (Mitm)

Ans:- A) Denial Of Service (Dos)

Reason: In a Dos Attack, Hackers Send Too Much Traffic To a Server Or Network So It Becomes Overloaded And Stops Working Properly. The Goal Is To Make The Service Unavailable.

3). Which Encryption Protocol Is Commonly Used To Secure Wireless Network
Communications?

A) Wep (Wired Equivalent Privacy)
B) Wpa (Wi-Fi Protected Access)
C) Ssl/Tls (Secure Sockets Layer/Transport Layer Security)
D) Aes (Advanced Encryption Standard)

Ans:-B) Wpa (Wi-Fi Protected Access)

Reason:- Wpa Is The Standard Security Method For Wi-Fi. Wep Is Old And Weak, Ssl/Tls Is Used For Websites, And Aes Is An Algorithm (Used Inside Wpa2/Wpa3). So Wpa Is The Correct Protocol For Wi-Fi Security.

4. What Is The Purpose Of a Vpn (Virtual Private Network) In a Network Security Context?

Answer: To Create a Secure, Private Connection Over The Internet

Reason:- A Vpn Hides Your Real Ip Address And Encrypts Your Internet Traffic. It's Like Creating a Private Tunnel So No One (Like Hackers Or Even Your Isp) Can See What You Are Doing Online.

Section 2- True Or False

5.) Patch Management Is The Process Of Regularly Updating Software
And Firmware To Address Security Vulnerabilities And Improve System Performance.

Ans:- True

Reason :- Patch Management Means Keeping Software And Device Firmware Up To Date. Updates (Called Patches) Fix Security Holes, Remove Bugs, And Improve Performance. If Patches Are Not Applied, Hackers Can Use Old Weaknesses To Attack The System.

6.) 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

Reason:- Regular Backups Keep a Safe Copy Of Important Data. If The Main System Crashes, Gets Hacked, Or Is Damaged By Disasters, The Backup Can Restore The Lost Data And Prevent Permanent Loss.

7.) 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

Reason:- Traceroute Shows The Path That Data Takes From Your Computer To Another Device On The Network. It Also Measures The Time (Latency) Each Step Takes, Helping To Find Slow Or Failing Network Points.

Section 3: Short Answer

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

Ans:- 1.) Plan And Set Scope – Decide Which Systems, Servers, Or Devices You Want To Check.

2.)Get Permission – Always Take Approval Before Testing.

3.)Collect Information – Find Details About Devices, Ip Addresses, And Services Running.

4.)Scan The Network – Use Tools (Like Nmap, Nessus, Openvas) To Find Open Ports And Weak Points.

5.)Find Vulnerabilities – Check For Missing Updates, Weak Passwords, Or Misconfigurations.

6.)Confirm Issues – Verify Which Problems Are Real (Remove False Alarms).

7.)Prioritize Risks – Mark Them As High, Medium, Or Low Based On Impact.

8.)Suggest Fixes – Give Solutions Like Patching Software, Closing Ports, Or Changing Settings.

9.)Make a Report – Write Results In Simple Form For Management And Technical Team.

10.)Re-Test After Fixes – Scan Again To Confirm Problems Are Solved.

Section 4: Practical Application

9. Demonstrate How To Tro Ubleshoot Network Connectivity Issues Using The Ping Command.

Ans:-

Check Your Own Computer

1. **Command:** `Ping 127.0.0.1`
2. **If Reply Comes → Your Computer's Network Card Is Working.**

Check Connection To Router

1. **Command:** `Ping 192.168.1.1` **(Router Ip)**
2. **If Reply Comes → Your Computer Is Connected To The Router.**

Check Internet Connection

1. **Command:** `Ping 8.8.8.8`
2. **If Reply Comes → Your Internet Is Working.**

Check Website Name

1. **Command:** `Ping Google.Com`

2. **If Reply Comes → Dns (Converts Website Names To Ip) Is Working.**

Conclusion:

- **If Step 1 Fails → Problem In Your Computer.**
- **If Step 2 Fails → Problem In Local Network Or Router.**
- **If Step 3 Fails → Problem With Internet Service.**
- **If Step 4 Fails → Problem With Dns.**

Ping Checks Network Connection Between Your Computer And Another Device Or Website.

Sends Packets And Waits For Replies To See If The Target Is Reachable.

Helps Identify Problems In The Computer, Local Network, Or Internet.

Shows Response Time (Latency) And Packet Loss, Indicating Network Speed And Stability.

Simple And Safe Tool Available On Most Operating Systems For Basic Network Troubleshooting.

Section :- 5

10. Discuss The Importance Of Network Documentation In The Context Of Building And Managing Networks.

Ans:- Network Documentation Is a Detailed Record Of All Parts Of a Network, Like Routers, Switches, Servers, Firewalls, Their Settings, Ip Addresses, Passwords, And How They Are Connected. It Is Very Important When Building And Managing a Network. While Setting Up a Network, Documentation Helps Plan The Layout Properly So Devices Are Connected Correctly. During Network Management, It Makes Troubleshooting Faster Because Administrators Can Check The Records Instead Of Inspecting Every Device. Documentation Also Helps When Upgrading The Network Or Adding New Devices Without Causing Problems Or Downtime. It Is Important For Security Too, As It Shows Which Devices Have Access And Where Risks Might Exist. In Organizations With Many Administrators, Documentation Keeps Everyone Informed About The Network Structure. Overall, Network Documentation Saves Time, Reduces Mistakes, Improves Security, And

Makes Managing And Growing The Network Much Easier.