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?**

Ans : *B) Filtering and controlling network traffic*

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

Ans : *A) Denial of Service (DoS)*

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

Ans: *B) WPA (WI-FI Protected Access)*

4. **What is the purpose of a VPN (Virtual private network) in a network security context ?**

Ans : *A) Encrypting network traffic to prevent eavesdropping*

Section 2: True or false

1. **Patch management is the process of regularly updating software and firmware to address security vulnerabilities and improve system performance.**

Ans : *True*

2. **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*

3. **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 answer

8. **Describe the involved in conducting a network vulnerability assignment.**

Ans : it is identifying all devices on a network, analysing their configurations and software for known vulnerabilities, scanning for open ports and services, testing for weak passwords, and ultimately prioritising and addressing any discovered weaknesses to mitigate potential security risks.

Key steps in conducting a network vulnerability assessment:

1.**Planning and Scoping**

- ➔ We need to Define the scope of the assessment, including which systems and networks will be evaluated
- ➔ We need to Establish a methodology and identify critical assets.
- ➔ We Obtain necessary permissions and stakeholder buy-i.

2. **Asset Discover :**
   - ➔ Firstly we identify all devices connected to the network, including servers, routers, workstations, and network appliances.

3**.Configuration Analysis**
   - ➔ We need to Review system configurations on identified devices for potential vulnerabilities like weak passwords, outdated software, or insecure protocols.
   - ➔ We need to Check firewall rules and access controls.

4. **Vulnerability Scanning**
   - ➔ We need to Run automated scanning tools to detect known vulnerabilities in operating systems, applications, and services on the network.
   - ➔ We Scan for open ports and services that could be exploited.

5.**Result Analysis:**
   - ➔ We need to Evaluate the scan results to identify the severity and potential impact of each vulnerability.
   - ➔ We Categorise vulnerabilities based on criticality and exploitability.

6. **Risk Assessment:**
   - ➔ We need to Assess the likelihood of a vulnerability being exploited and the potential consequences.
   - ➔ We Prioritise vulnerabilities based on risk level.

<u>Section 4: Practical Application</u>

9. **Demonstrate how to troubleshoot network connectivity issues using the ping command.**

- ➢ Troubleshooting network connectivity issues using the `ping` command is a simple process.
- ➢ Now we see here’s how to do it step by step:

Step 1: **firstly we Open Command Prompt**
- ➔ Windows: We Press `Windows + R` or we type `cmd`, and press Enter

Step 2: **Now we can do Ping a Local Address**
- ➔ For example : ping 127.0.0.1
- ➔ This tests the loopback interface. If we receive replies, our network stack is functioning correctly.

Step 3: **We need to do Ping the Default Gateway**

- ➔ For example : ping <our_default_gateway>
- ➔ Replace `<our_default_gateway>` with the actual IP address. If we get replies, our device can communicate with the router.

Step 4: **We need to do Ping an External Address**

- ➔ Here we do Ping a Public IP Address
- ➔ For example : ping 8.8.8.8
- ➔ This tests our connection to an external server (Google's DNS). Successful replies indicate that the device has internet connectivity.

Step 5: **We need to do Ping a Domain Name**

- ➔ For example : ping www.tops.com
- ➔ If this works but the previous step did not, there may be a DNS issue.

Step 6: **we need to Analyse the Results**

- ➔ Here we got Successful Replies: Indicates connectivity is generally good.
- ➔ Here we got Request Timed Out: Indicates that packets are not being sent/received. Possible issues include.
- ★ Network configuration problems
- ★ Firewall settings blocking pings
- ★ Connectivity issues with the target device

- ➔ Destination Unreachable: Indicates the target host is not reachable.

Step 7**:Here we see Additional Troubleshooting**

- ➔ Here we need to do Check Firewall Settings: Ensure that ICMP packets (used by ping) are not being blocked.
- ➔ Here we do Use Traceroute: If ping fails, try `tracert <address>` (Windows) to see the path our packets take and identify where the failure occurs.
- ➔ Here we Check Network Cables/Wi-Fi: Ensure physical connections are secure, and Wi-Fi is enabled.

Conclusion

- ➔ By using the `ping` command, we can quickly diagnose network connectivity issues and gather information about our network's status. If problems persist, further investigation into hardware, configurations, or service provider issues may be necessary.

<u>Section 5</u>

10. **Discuss the importance of regular network maintenance and the key tasks involved in maintaining network infrastructure**

- ➔ Firstly, We see Importance of Regular Network Maintenance

- ➢ 1. Keeps the Network Running Smoothly: everydays maintenance helps find and fix problems before they cause major disruptions.
- ➢ 2. Improves Performance: By monitoring the network, we can spot issues that slow things down. This helps ensure everything runs fast and efficiently.
- ➢ 3. Enhanced Security: We need to do everydays updates and checks to help protect the network from hackers and viruses. This helps keep sensitive information safe.
- ➢ 4.Save Money: We need to fix problems early to prevent costly repairs later. It also reduces downtime, which means the business keeps running without interruptions.
- ❖ Key Tasks in Maintaining Network Infrastructure
- ➔ 1.Regular Update Software and Hardware: we need to update operating systems and firmware everyday to protect against vulnerabilities.
- ➔ 2.Regularly Monitor Network Performance: we need to use tools to check how well the network is running. Look for slowdowns or issues that need attention.
- ➔ 3.Backup Data: everydays we need to back up important data so it can be restored if something goes wrong.
- ➔ 4.Document Configurations: We need to keep detailed records of how the network is set up. This makes it easier to troubleshoot problems and make changes.
- ➔ 5.Inspect Hardware: we need to Physically check devices like routers and switches. Clean them and replace any that are not working.
- ➔ 6.Run Security Checks: We need to do everydays tests on the network for security weaknesses and fix any vulnerabilities we find.
- ➔ 7.Manage User Access: We need to Review who has access to the network to make sure only authorised users can enter sensitive areas.

Conclusion

- ➢ We need to do everydays network maintenance which is essential for keeping everything running good and securely. By doing these key tasks, businesses can avoid problems, improve performance, and ensure their network can grow and adapt as needed.