Name: Kishan Barvaliya

Batch:Networking (Abdul Hamid Sir) 9:30am to 10:30am

Assignment

Modul: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: Data Encryption

Section 2: True or False

5)True or False: Patch management is the process of regularly updating software and firmware to address security vulnerabilities and improve system performance.

Ans: True

6) True or False: 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

7) True or False: 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 steps involved in conducting a network vulnerability Assignment.

Ans: Define Scope: Identify the network, systems, and devices to be assessed.

Gather Information: Collect details about network architecture, IPs, and operating systems.

Scan for Vulnerabilities: Use tools (e.g., Nessus, OpenVAS) to detect weaknesses.

Analyze Results: Review scan data to identify critical and exploitable vulnerabilities.

Prioritize Risks: Rank vulnerabilities based on severity and impact.

Report Findings: Document vulnerabilities, risk levels, and suggested remediation.

Remediate Issues: Apply patches, update configurations, and fix weaknesses.

Re-test: Verify that vulnerabilities have been resolved.

Section 4: Practical Application

9) Demonstrate how to troubleshoot network connectivity issues using the

ping command.

Ans: Done

Section 5: Eassy

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

Ans: In this digital era, the network serves as the lifeline for communication, data sharing and day to day operational functions of any institution. As with any critical infrastructure, computer networks need to be maintained in order to achieve maximum performance and to be free from security and reliability issues. Maintaining a network isn't a one-time job; it's an ongoing commitment that protects your network against failures, security breaches, and downtime that can cause loss of data as well as loss of money.

Significance of Periodic Network Maintenance

Guarantee for Network Up-time and Performance

Frequent servicing can identify and correct problems that could impede or disrupt the network. This can involve hardware diagnostic, software configuration updates, and bandwidth management. A healthy network means that employees and systems remain in touch with little or no downtime.

Enhances Security

The cyber threat environment is rapidly changing. Document Your Maintenance Routine Regular network maintenance will keep your firewalls, antivirus software, and other forms of protection current. This minimizes the potential attack surface and ensures secure data is not compromised.

Prevents Costly Downtime

Anytime your network is down, it can bring your business to a standstill resulting in lost productivity and resulting loss of income. Preventative maintenance enables the identification and correction of potential issues prior to any issue arising, minimizing the risk of failure without warning.

Supports Business Continuity

Keeping a trusted and safe network up and running is imperative for the company's continuity. It guarantees that services stay available even through updates or downtimes, and that backups are in place to recover things rapidly if they do go wrong.

Improves Resource Management

Monitoring and continuous audit, allow for the efficient handling of resources. It helps to pick up on unused equipment or jam-packed servers and distribute the network load.

Critical Activities for Network Maintenance

Checking Your Network's Performance

Real-time monitoring helps you identify suspicious traffic, pinch points, or hardware faults. Real-time information from tools like network analyzers or monitoring software allows you to respond rapidly.

Updating the Firmware and Software If you want to keep your system up to date with the latest firmware and software updates, you have two options: 1.

Keeping routers, switches, firewalls and other devices up-to-date will keep security holes away and optimize device performance. This spans both system updating and patching.

Testing of Data Backup and Recovery

Frequent backup for important data and regular testing of recovery process reduces chance of losing data due to failures, cyber attack, or natural disaster.

Inspection and Replacement of Hardware

You can avoid mechanical failure and extend the life of your equipment by performing physical inspections on cables, ports, and hardware.

Audit of Security and Configuration Control

When you comb through firewall rules, access permissions and security policies, it makes sure that only people entitled to use it have access to it and that it is within the security policies.

Documentation and Reporting

Network Activity, Change and Maintenance Schedules – keeping records of network activity and all notable changes will enable you to follow up on issues and support future deployments, upgrades etc.

Conclusion

Routine upkeep of a network is critical for the performance of any organization's IT services. It reduces off-time, improves security, and keeps the network meeting business objectives. Companies that focus on the maintenance of networks, are more resistant to emerging challenges, they are easier adapt to new technologies and remain competitive.