TOPS Tech Assignment-5

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

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)

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)

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

Ans.

- The purpose of a VPN is to create a secure, encrypted connection over an untrusted network (like the internet) to protect data privacy, ensure confidentiality, and allow safe remote access to a private network.

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

TOPS Tech Assignment-5

Section 3: Short Answer:-

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

Ans: Steps to do a Network Vulnerability Assignment:

1. Set the Scope
   - Decide which parts of the network you will check, like computers, servers, or apps. This keeps the work focused and avoids wasting time.
2. Collect Information
   - Note down details such as IP addresses, systems in use, open connections, and how the network is built. This helps you understand the setup.
3. Scan for Weaknesses
   - Use simple tools to look for problems like old software, open connections, or weak settings.
4. Check and Study the Weaknesses
   - Go through the scan results, confirm which problems are real, and think about how they could harm the network.
5. Rank the Problems
   - Put the issues into groups like high, medium, or low risk. This way, the most dangerous ones can be fixed first.
6. Write a Report
   - Make a clear report that shows what problems were found, which systems are at risk, and what actions should be taken.
7. Fix the Problems
   - Update software, close unused connections, and correct weak settings to make the network safer.
8. Check Again
   - After fixing, scan the network one more time to be sure the problems are solved.

Section 4: Practical Application:-

9. Demonstrate how to troubleshoot network connectivity issues on a Windows computer using the ipconfig command.

Ans. Troubleshooting Network Issues with ipconfig:

1. Open Command Prompt
   - Click on the Start button.
   - Type cmd and press Enter.
2. Check Your Computer's Network Details
   - Type ipconfig and press Enter.
   - You will see information about your computer's internet connection.
3. Look for the IP Address
   - Find the section that says IPv4 Address.
   - If you see numbers like 192.168.x.x, your computer has an address.
   - If it says 0.0.0.0 or nothing, your computer is not connected properly.
4. Fix Connection Problems
   - Type ipconfig /release and press Enter.
     (This clears the old connection.)
   - Then type ipconfig /renew and press Enter.
     (This asks for a new connection.)
5. Test the Internet
   - Open your browser and try to visit a website.
   - If it works, the problem is solved.
   - If not, you may need to restart your router or check cables.

TOPS Tech Assignment-5

Section 5: Essay :-

10. Discuss the importance of effective communication skills in a helpdesk or technical support role.

Ans.

Importance of Good Communication Skills in a Helpdesk or Support Role:

- ➢ Good communication skills are very important for people working in helpdesk or support jobs. These roles are not only about fixing problems but also about helping people feel understood and supported. Clear and kind communication makes the whole process easier for both the helper and the user.

1. **Explaining Clearly:**
   - Many people who ask for help may not know much about computers or systems.
   - The helper needs to explain solutions in simple, everyday language so the person can follow along.

2. **Listening Carefully**
   - By listening closely, the helper can understand the real problem instead of guessing.
   - This saves time and makes the person feel respected.

3. **Showing Patience and Kindness**
   - People often feel stressed when things don't work.
   - A calm and patient attitude helps reduce frustration and builds trust.

4. **Being Polite and Professional**
   - Using a respectful tone shows care and creates a positive image of the support team.
   - It also makes the person more comfortable asking for help again in the future.
5. **Solving Problems Faster**
   - When communication is clear, problems are fixed more quickly.
   - It also helps when the issue needs to be passed on to another team.

Conclusion

In helpdesk or support work, good communication is just as important as knowing how to fix problems. It helps people feel valued, makes solutions easier to understand, and improves the overall experience. A helper who communicates well not only solves issues but also leaves a lasting positive impression.