**CCNA Assignment**

**By**

**Himanshu Kalambe**

**Guided by**

**Rohit Sir**

**Module 4**

Q-1 List of IP services Types and Example of HSRP?

**DNS (Domain Name System)**

Resolves domain names to IP addresses.

Example: When you type www.google.com, DNS converts it to Google's IP address.

**DHCP (Dynamic Host Configuration Protocol)**

Automatically assigns IP addresses to devices on a network.

Example: When you connect to Wi-Fi, DHCP assigns an IP address to your device.

**HTTP/HTTPS (Hypertext Transfer Protocol / Secure)**

Used for accessing and transferring web pages on the internet.

Example: Accessing https://www.example.com in your browser.

**FTP (File Transfer Protocol)**

Transfers files between computers over a network.

Example: Uploading files to a web server.

**SMTP (Simple Mail Transfer Protocol)**

Used for sending emails.

Example: Sending an email from yourname@example.com.

**NTP (Network Time Protocol)**

Synchronizes clocks of computer systems over packet-switched, variable-latency data networks.

Example: Ensuring all computers in a company have the same time.

**HSRP (Hot Standby Router Protocol)**

HSRP is a Cisco proprietary redundancy protocol for establishing a fault-tolerant default gateway.

Example:

Primary Router: Active router managing traffic.

Secondary Router: Standby router that takes over if the primary router fails

Q2 Example of Backup and restore Router managing IOS?

Ans **Backup Process:**

Connect to the router and enter privileged mode.

Use the copy running-config tftp command to save the current configuration to a TFTP server.

Verify the backup file on the TFTP server.

**Restore Process:**

Connect to the router and enter privileged mode.

Use the copy tftp running-config command to load the backup configuration from the TFTP server to the router's running configuration.

Save the running configuration to the startup configuration to ensure it is retained after a reboot.

Verify the restored configuration to ensure everything is as expected.

Q3 Explain Security Threat.

Ans:

Malware

Description: Malicious software designed to harm, exploit, or otherwise compromise the security of a computer system.

Examples:

Viruses: Programs that attach themselves to legitimate software and spread.

Worms: Self-replicating malware that spreads across networks.

Trojan Horses: Malware disguised as legitimate software.

Ransomware: Encrypts data and demands ransom for decryption keys.

Spyware: Collects user information without consent.

2. Phishing

Description: A technique used to trick individuals into providing sensitive information by masquerading as a trustworthy entity.

Examples:

Email Phishing: Fraudulent emails that appear to be from reputable sources asking for personal information.

Spear Phishing: Targeted phishing attacks aimed at specific individuals or organizations.

Smishing: Phishing via SMS messages.

3. Denial of Service (DoS) / Distributed Denial of Service (DDoS)

Description: Attacks designed to overwhelm a system, network, or website, rendering it unavailable to users.

Examples:

DoS Attack: Single source flooding a target with traffic.

DDoS Attack: Multiple compromised systems (botnet) flooding a target.

4. Man-in-the-Middle (MitM) Attack

Description: An attacker intercepts and possibly alters the communication between two parties without their knowledge.

Examples:

Eavesdropping: Intercepting and monitoring data traffic.

Session Hijacking: Taking over a user session to gain unauthorized access.

5. Insider Threats

Description: Threats posed by individuals within the organization who have authorized access to systems and data.

Examples:

Disgruntled Employees: Employees who misuse their access to harm the organization.

Negligent Employees: Employees who accidentally cause security breaches.

6. Social Engineering

Description: Manipulating individuals into divulging confidential information or performing actions that compromise security.

Examples:

Pretexting: Creating a fabricated scenario to steal personal information.

Baiting: Offering something enticing to lure victims into a trap.

7. SQL Injection

Description: An attack that involves inserting malicious SQL code into a query to manipulate the database.

Examples:

Unauthorized Access: Retrieving, altering, or deleting database data.

Data Breach: Exposing sensitive information stored in databases.

8. Zero-Day Exploit

Description: An attack that takes advantage of a previously unknown vulnerability in software or hardware before the vendor can issue a fix.

Examples:

Exploiting a New Vulnerability: Attacks that occur on the same day a vulnerability is discovered and before it is patched.

9. Advanced Persistent Threats (APTs)

Description: Prolonged and targeted cyberattacks in which an intruder gains access to a network and remains undetected for an extended period.

Examples:

State-Sponsored Attacks: Attacks carried out by nation-states.

Corporate Espionage: Long-term infiltration for stealing sensitive data.

Q4 List of Basic security of Password – Example with apply password in Router ?

Ans:

· Use Strong Passwords:

· Combine uppercase letters, lowercase letters, numbers, and special characters.

Example: S3cur3P@ssw0rd!

· Avoid Common Words:

· Do not use easily guessable passwords like "password," "123456," or "admin."

Example: Avoid password123.

· Use Unique Passwords:

· Do not reuse passwords across multiple accounts.

Example: Different password for email and bank accounts.

· Enable Multi-Factor Authentication (MFA):

· Add an extra layer of security by requiring a second form of verification.

Example: Password + SMS code.

Access the Router:

· Connect via console cable, SSH, or Telnet.

Enter Global Configuration Mode:

Router> enableRouter# configure terminal

Set Console Password:

· This password is required to access the router via console.

Router(config)# line console 0Router(config-line)# password yourStrongPasswordRouter(config-line)# loginRouter(config-line)# exit

· Set VTY (Virtual Teletype) Password:

· This password is required to access the router via Telnet or SSH.

Router(config)# line vty 0 4Router(config-line)# password yourStrongPasswordRouter(config-line)# loginRouter(config-line)# exit

· Set Enable Password:

· This password is required to enter privileged EXEC mode.

Router(config)# enable password yourStrongPassword

· Set Enable Secret (More Secure):

· This password is encrypted and preferred over the enable password.

Router(config)# enable secret yourStrongSecretPassword

· Encrypt All Plain Text Passwords:

· Ensures all passwords are encrypted in the configuration file.

Router(config)# service password-encryption

· Save Configuration:

· Save the changes to the startup configuration to ensure they persist after a reboot.

Router(config)# exitRouter# write memory

Q5 Describe threat defense technologies.

Ans:

**Firewalls:**

Function: Act as a barrier between your internal network and external networks (e.g., the internet).

Purpose: Block unauthorized access while allowing legitimate communication.

Example: Your home router's firewall prevents outside hackers from accessing your home network.

**Antivirus Software:**

Function: Detects, quarantines, and removes malware from your computer.

Purpose: Protects against viruses, worms, Trojans, and other malicious software.

Example: Software like Norton or McAfee scans your computer for harmful programs and removes them.

**Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS):**

Function: Monitors network traffic for suspicious activity (IDS) and can block it (IPS).

Purpose: Detects and prevents cyberattacks in real time.

Example: An IDS might alert you to a potential hack attempt, while an IPS can automatically block the attack.

**Encryption:**

Function: Converts data into a coded format that can only be read by someone with the correct decryption key.

Purpose: Protects sensitive information from being accessed by unauthorized parties.

Example: Encrypted emails ensure that only the intended recipient can read the message.

**Virtual Private Network (VPN):**

· Function: Creates a secure, encrypted connection over a less secure network, such as the internet.

Purpose: Protects your data and privacy when accessing the internet.

Example: Using a VPN on public Wi-Fi to keep your online activities private.