**CCNA - Security Fundamentals**

**Module-4**

**• List of IP services Types and Example of HSRP?**

**Ans.** IP services types include DHCP, DNS, NAT, VPN, dynamic routing protocol, HSRP, QoS, SNMP, IPsec, and BGP.

HSRP (Hot Standby Router Protocol) is a redundancy protocol used in cisco networks to provide high availability by allowing two or more routers to work together, presenting a single virtual router IP address to the LAN.

For EX. The virtual IP address is 192.168.1.254 and the virtual MAC is 0000.0c07.AC0A

**• Example of Backup and restore Router managing IOS?**

**Ans.**

1. **Backup Configuration:**

* Access the router's command-line interface (CLI) via SSH, Telnet, or console cable.
* Enter privileged EXEC mode by typing enable and providing the appropriate password.
* Use the show running-config command to display the current configuration.
* Copy the configuration to a TFTP server using the copy running-config tftp command, specifying the IP address of the TFTP server and the desired filename.

**For Ex.**

Router# copy running-config tftp

Address or name of remote host []? 192.168.1.100

Destination filename [router-config]? backup-router-config

1. **Restore Configuration:**

* Access the router's CLI.
* Enter privileged EXEC mode.
* Use the copy tftp running-config command to retrieve the configuration from the TFTP server and replace the current running configuration.

**For ex.**

Router# copy tftp running-config

Address or name of remote host []? 192.168.1.100

Source filename []? backup-router-config

Destination filename [running-config]?

**• Explain Security Threat.**

**Ans.** A security threat is a burglar traying to break into your home. In the digital world, it’s like someone trying to sneak into your computer system or network to steal information, disrupt services, or cause damage. Just as you would take measures to protect your home from intruders, organization implement security measures to safeguard their digital assets from threats like hackers, malware, and other malicious activities.

OR

* Security Threats are any type of malicious activity or attack that could potentially cause harm or damage to an organization, its data or its personnel. Security threats, such as theft or vandalism, as well as digital threats, such as malware or ransomware.

**• List of Basic security of Password – Example with apply password in Router.**

**Ans.**

1. **Use Complex Passwords**: Create passwords that are at least 8 characters long and include a mix of uppercase and lowercase letters, numbers, and special characters.
2. **Avoid Common Words or Patterns:** Don't use easily guessable passwords like "password" or sequential patterns like "123456."
3. **Change Passwords Regularly:** Update passwords periodically to reduce the risk of them being compromised.
4. **Unique Passwords:** Use different passwords for different accounts and systems to prevent a single breach from compromising multiple accounts.
5. **Enable Password Encryption:** Ensure that passwords are stored in an encrypted format to protect them from being easily accessed if the system is compromised.
6. **Two-Factor Authentication (2FA):** Implement 2FA where possible to add an extra layer of security beyond just passwords.

Example of Applying a Password in a Router (Cisco IOS):

1. Access the router's command-line interface (CLI) via SSH, Telnet, or console cable.

2. Enter privileged EXEC mode by typing enable and providing the appropriate password.

3. Enter global configuration mode by typing configure terminal.

4. Set the enable password using the enable password <password> command.Example:

Router(config)# enable password mysecurepassword

5. Optionally, set an enable secret password for additional security using the enable secret <password> command.Example:

Router(config)# enable secret mystrongerpassword

6. Exit configuration mode by typing exit.

7. Save the configuration changes using the copy running-config startup-config command to ensure they are retained after a reboot.Example:

Router# copy running-config startup-config

**• Describe threat defence technologies.**

**Ans.** Threat defence technologies in refer to tools and techniques used to protect computer networks from cyber threats. These include firewalls, intrusion detection system (IDS), Intrusion prevention systems (IPS), antivirus software, virtual private network (VPNs), and encryption. These technologies help detect, prevent, and mitigate security breaches and unauthorized access, ensuring the integrity and confidentiality of network data.

1. **Firewalls**: Think of firewalls as digital bouncers. They monitor and control incoming and outgoing traffic based on predetermined security rules, deciding what gets in and what stays out of your network.
2. **Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS):** These are like digital watchdogs. IDS monitors network traffic for suspicious activity, while IPS not only detects but also takes action to block or prevent potential threats.
3. **Antivirus Software:** This is your digital immune system. It scans your devices and networks for viruses, malware, and other malicious software, then removes or quarantines them to keep your systems healthy.
4. **Encryption:** Encryption is like sending messages in secret code. It scrambles your data into an unreadable format, making it indecipherable to anyone without the key, thus protecting sensitive information from prying eyes.
5. **Virtual Private Networks (VPNs):** VPNs are like digital tunnels. They create a secure, encrypted connection between your device and a remote server, ensuring your online activities are private and protected from eavesdropping.
6. **Endpoint Security:** This is like putting locks on all your doors and windows. Endpoint security solutions protect individual devices (endpoints) from cyber threats, ensuring that each device is fortified against attacks.
7. **Behavioral Analytics:** Think of behavioral analytics as digital detectives. They analyse patterns of behaviour on your network or device to identify anomalies that could indicate potential threats, allowing you to take action before any harm is done.