Router technical audit checklist

Password Encryption

1. Do passwords appear in encrypted form when viewed at the configuration file?

Passwords should appear encrypted when viewed through the configuration file.

The following command is used to implement the same.

```
Router(config)#service password-encryption
```

Authentication Settings

1. Is enable secret used for the router enable mode?

The enable secret command should be enabled to implement MD5 hashed password on enable mode.

```
Router(config)#enable secret password
```

2. Does the enable secret password match any other username password; enable password, or the enable secret password of another router in the network?

The enable secret password should be unique across each router. If the routers are too many, instead of keeping a single enable secret password for all, the password could be different for routers in different zones.

Authentication Settings

3. Is a Message of the Day (MOTD) banner defined?

Login banners should be used as a preventive measure against unauthorized access to the routers.
Use the following command to enable a MOTD banner:

```
Router# config t
Router(config)# banner motd ^
```

4. Is the following defined on the console port: Exec-timeout, Password

These parameters should be defined on the console port to reduce the chance of an unauthorized access on the console port.

The following commands can be used to implement the same:

```
Cisco(config)#line con 0
Cisco(config-line)#exec-timeout 5 0
Cisco(config-line)#password password
Cisco(config-line)#login
```

Authentication Settings

5. Is a Message of the Day (MOTD) banner defined?

Login banners should be used as a preventive measure against unauthorized access to the routers.

Use the following command to enable a MOTD banner:

```
Router# config t
Router(config)# banner motd ^
```

6. Is the aux port disabled?

The aux port should be disabled if there is no business need for the same.

Use the following command to disable the aux port:

```
Router(config)#line aux 0
Router(config-line)#no exec
```

Authentication Settings

7. Is the vty lines restricted to certain IP Addresses only?

If the vty lines use telnet as the transport protocol, it is advisable to restrict access to certain IP Addresses only since telnet transmits data in clear text.
Use the following command to restrict vty access to certain ip addresses:
Router(config)#access-list 50 permit 192.168.1.x (x represents the IP address of the administrator’s machine)
Router(config)#access-list 50 deny any log
Router(config)#line vty 0 4
Router(config-line)#access-class 50 in

8. Is SSH used for the vty lines?

SSH is a preferred protocol over Telnet for vty access since it encrypts the data while in transit on the network.

Authentication Settings

9. Do any applications use telnet to perform management activities such as backing up configuration?

The Telnet protocol transfers data in clear text thereby allowing an intruder to sniff valuable data such as passwords.
As a remedy the following can be done:

- Using secure protocols such as SSH wherever possible
- Restricting access from certain workstations only
- Maintaining strong passwords

10. Do the router passwords meet with the required complexity as defined by the policy?

All password defined on the router should meet the following criteria:

- Minimum 8 characters in length
- Should be alphanumeric along with special characters (@#$%)
- Should not include organization’s name in it

Disable Unneeded Services

1. Are unused interfaces disabled?

Unused interfaces on the router should be disabled.

```
Router(config-if)# shutdown
```

2. Is DNS lookups for the router turned off?

This client service is enabled by default and is not required on most routers.

The following command is used to turn DNS lookup off.

```
Router(config)#no ip domain-lookup
```

3. Is Cisco Discovery Protocol disabled on the router?

CDP which is used to obtain information such as the ip address, platform type of the neighboring Cisco devices should be disabled on the router if not used by any application.

```
Router(config)# no cdp run OR
Router(config-if)# no cdp enable
```

Disable Unneeded Services

4. Is Bootp server disabled on the routers?

The Bootp server service which is enabled by default allows other routers to boot from this router.
This feature should be disabled on the router as it is rarely used on today's networks.

The following command is used to disable the service.
Router(config)#no ip bootp server

5. Is directed broadcast disabled on all interfaces?

Directed broadcasts permit a host on one LAN segment to initiate a physical broadcast on a different LAN segment. This feature should be disabled on the router as it could be used in denial-of-service attacks.
The following command is used to disable the service.
Router(config-if)#no ip directed-broadcast

Disable Unneeded Services

6. Is Proxy ARP disabled on the router?

Proxy ARP helps in extending a LAN at layer 2 across multiple segments thereby breaking the LAN security perimeter.
This feature should be disabled on the router.
The following command is used to disable the service on individual interfaces.

```
Router(config-if)#no ip proxy-arp
```

7. Is ICMP redirects disabled on the router?

The three ICMP messages that are commonly used by attackers for network mapping and diagnosis are: Host unreachable, ‘Redirect’ and ‘Mask Reply’. Automatic generation of these messages should be disabled on all interfaces, especially those connected to untrusted networks.
The following command is used to disable the service.

```
Router(config-if)#no ip redirects
Router(config-if)#no ip unreachables
Router(config-if)#no ip-mask reply
```

Administrator Authentication

1. Does each router administrator have a unique account for himself/herself?

Each router administrator should have a unique account for him/her to maintain accountability.
The following commands can be executed to create unique local usernames on the router:

```
Router(config)#username username password password
Router(config)#line vty 0 4
```

2. Are all user accounts assigned the lowest privilege level that allows them to perform their duties?

All user accounts should be assigned the lowest privilege level that allows them to perform their duties.

If multiple administrators exist on the router, each administrator should be given an individual username and password and assigned the lowest privilege levels.

Management Access

1. Which version of SNMP is used to manage the router?

Ideally SNMP version 3 should be used on the router since it introduces authentication in the form of a username and password and offers encryption as well.
Since the SNMP process is enabled by default, it should be disabled if not used.
Router(config)# no snmp-server

2. Is the NTP server service used to synchronize the clocks of all the routers?

The NTP service which is disabled by default helps to synchronize clocks between networking devices thereby maintaining a consistent time which is essential for diagnostic and security alerts and log data. However if configured insecurely, it could used to corrupt the time clock of the network devices. To prevent this, restrict which devices have access to NTP.
The service should also be disabled if not used.

novateca

Configuration Maintenance

1. How often is the router configurations backed up?

Router configurations should be backed up periodically depending on importance and frequency of changes made to the configuration.

2. Is the backup moved to an off-site/DR site?

Backup copies should be maintained off-site for quick recovery during a disaster.

3. Is the TFTP protocol used to transfer configuration or image files to and from the router?

The TFTP protocol which is disabled by default transfers files in clear text and hence is unsafe to use.
The TFTP process should be restricted to certain addresses only (management workstations) to reduce the risk. The service should also be disabled when not in use because it allows access to certain files in the router flash.

Security Updates

1. Is the network engineer aware of the latest vulnerabilities that could affect the router?

   The network engineer should receive periodic updates on the vulnerabilities and patches affecting the router.

THE END
Thank you for listening!