Exam Report: 6.7.8 Practice Questions

Date: 1/21/2020 8:11:20 pm
Time Spent: 4:30

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 60%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

You've just deployed a new Cisco router that connects several network segments in your organization.

The router is physically located in a server room that requires an ID for access. You've backed up the router configuration to a remote location in an encrypted file. You access the router configuration interface from your notebook computer using a Telnet client with a user name of **admin** and a password of **admin**. You have used the MD5 hashing algorithm to protect the password.

What should you do to increase the security of this device? (Select two.)

- [ ] Use a web browser to access the router configuration using an HTTP connection.
- [x] Use an SSH client to access the router configuration.
- [ ] Use encrypted type 7 passwords.
- [x] Change the default administrative user name and password.
- [ ] Use TFTP to back up the router configuration to a remote location.

Explanation

In this scenario, two key security issues need to be addressed:

- You should use an SSH client to access the router configuration. Telnet transfers data in cleartext over the network connection, exposing sensitive data to sniffing.
- You should change the default administrative user name and password. Default user names and passwords are readily available from web sites on the internet.

Encrypted type 7 passwords on a Cisco device are less secure than those protected with MD5. Using HTTP and TFTP to manage the router configuration could expose sensitive information to sniffers as they transmit data in cleartext.

References

LabSim for Security Pro, Section 6.7.
[All Questions SecPro2017_v6.exm ROUTER_SECURITY_01]

Question 2: Incorrect

You've just deployed a new Cisco router that connects several network segments in your organization.

The router is physically located in a cubicle near your office. You've backed up the router configuration to a remote location in an encrypted file. You access the router configuration interface from your notebook computer using an SSH client with the user name **admin01** and the password **P@ssW0rd**. You have used the MD5 hashing algorithm to protect the password.

What should you do to increase the security of this device?

- ( ) Use encrypted type 7 passwords.

- Use a Telnet client to access the router configuration.
- ~~Change the default administrative user name and password.~~
- Move the router to a secure server room.
- Use TFTP to back up the router configuration to a remote location.

Explanation

In this scenario, the router is not physically secure. Anyone with access to the area could gain access to the router and manipulate its configuration by plugging in to the console port. The device should be moved to a secure location, such as a server room, that requires an ID badge for access.

You should not use a Telnet client to access the router configuration. Telnet transfers data in cleartext over the network connection, exposing sensitive data to sniffing. The user name and password used to access the router configuration are reasonably strong. Encrypted type 7 passwords on a Cisco device are less secure than those protected with MD5. Using TFTP to manage the router configuration could expose sensitive information to sniffers, as TFTP transmits data in cleartext.

References

LabSim for Security Pro, Section 6.7.
[All Questions SecPro2017_v6.exm ROUTER_SECURITY_02]

Question 3: Incorrect

You've just deployed a new Cisco router that connects several network segments in your organization.

The router is physically located in a locked server closet. You use an FTP client to regularly back up the router configuration to a remote server in an encrypted file. You access the router configuration interface from a notebook computer that is connected to the router's console port. You've configured the device with the user name **admin01** and the password **P@ssW0rd**. You have used the MD5 hashing algorithm to protect the password.

What should you do to increase the security of this device?

- ~~Use an SSH client to access the router configuration.~~
- Move the router to a secure data center.
- Use encrypted type 7 passwords.
- Use SCP to back up the router configuration to a remote location.

Explanation

In this scenario, the router configuration is being copied to a remote location using an insecure protocol (FTP) that transfers data in cleartext. You should instead use the secure copy protocol (SCP) to transfer the backup from the router to the remote storage location.

It is not necessary to use an SSH client when using the console port to configure the router. It also is not necessary to move the device to a data center if it is currently located in a locked server closet. Encrypted type 7 passwords on a Cisco device are less secure than those protected with MD5.

References

LabSim for Security Pro, Section 6.7.
[All Questions SecPro2017_v6.exm ROUTER_SECURITY_03]

Question 4: Correct

You can use a variety of methods to manage the configuration of a network router. Match the management option on the right with its corresponding description on the left. (Each option can be used more than once.)

SSL

- ✓ Uses public-key cryptography

HTTP

✔ Transfers data in cleartext

SSH

✔ Uses public-key cryptography

Telnet

✔ Transfers data in cleartext

Console port

✔ Cannot be sniffed

Explanation

The following router management options transfer data in cleartext and should not be used:

- HTTP
- Telnet

The following management options use public-key cryptography to protect data transferred between the router and the management station:

- SSL (used in conjunction with HTTP)
- SSH

The most secure way to manage a router's configuration is to connect the management station to the router's console port. This creates a dedicated transmission path that can't be sniffed by hosts on the network.

References

LabSim for Security Pro, Section 6.7.
[All Questions SecPro2017_v6.exm ROUTER_SECURITY_04]

Question 5: Correct

Which of the following can make passwords useless on a router?

- ○ Using the MD5 hashing algorithm to encrypt the password
- ○ Using SSH to connect to a router remotely
- ○ Storing the router configuration file to a secure location
- ➡ ◉ Not controlling physical access to the router

Explanation

If someone can gain access to the physical device, they can easily bypass any configured passwords. Passwords are useless if physical access is not controlled.

Other security measures you can use include:

- Using the MD5 hashing algorithm to encrypt the password
- Storing the router configuration file in encrypted form to a secure location
- Using SSH when you connect to a router remotely

References

LabSim for Security Pro, Section 6.7.
[All Questions SecPro2017_v6.exm ROUTER_SECURITY_05]