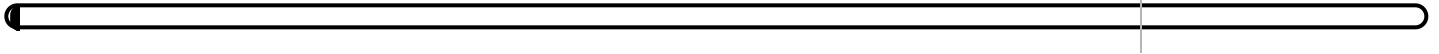


Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 2/24/2022 8:06:00 pm • Time spent: 00:11

Score: 0%

Passing Score: 80%



▼ Question 1: ✕ Incorrect

Which of the following should be configured on the router to filter traffic at the router level?

- ☐ Telnet
- ☐ Anti-spoofing rules
- ☒ Access control list
- ☐ SSH

EXPLANATION





Router access control lists (ACLs) can be configured to increase security and limit traffic, much like a firewall but on the router level. ACLs filter the traffic and determine if the data should be blocked or forwarded.

Anti-spoofing rules counter spoofing attacks where IP packets have a source address that does not belong to the sender.

Secure Shell (SSH) is a secure protocol that can be used to connect to the router.

Telnet is an older protocol used to connect to remote devices. It should not be used any longer.

REFERENCES

-  4.3.3 File Permission Facts
-  5.3.2 Firewall Facts
-  5.13.3 Router Security Facts
-  6.3.3 Authorization Facts


q_router_sec_acl_secp7.question.fex

▼ 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 username 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?

- ☐ Change the default administrative username and password.
- ☐ Use encrypted Type 7 passwords.
- ☐ Use a Telnet client to access the router configuration.
- ☒  Move the router to a secure server room.

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 into 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 username 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.


REFERENCES

 5.13.3 Router Security Facts

q_router_sec_area_secp7.question.fex

▼ Question 3: **✕ Incorrect**

Which of the following happens by default when you create and apply a new ACL on a router?

- ☐ All traffic is permitted.
-  ☒ All traffic is blocked.
- ☐ ACLs are not created on a router.
- ☐ The ACL is ignored until applied.

EXPLANATION

When first created and applied on a router, an ACL almost always includes a hidden Deny Any statement at the end of the list. This means all traffic is automatically blocked.


All traffic is not permitted by default with a new ACL.

The ACL is immediately applied and blocks all traffic until configured.

ACLs are created on the router itself.

REFERENCES


 4.4.5 Configure iptables Facts

 5.13.3 Router Security Facts

q_router_sec_blocked_secp7.question.fex

▼ Question 4:  Incorrect

Which type of ACL should be placed as close to the source as possible?

-  ☒ Extended
- ☐ Standard
- ☐ Advanced
- ☐ Basic



EXPLANATION

Extended ACLs are used to filter traffic based on a lot more parameters than standard ACLs. In addition to filtering based on source host name or host IP address, an extended ACL can filter based on source IP protocol, source or destination socket number, and destination host name or host IP address. Extended ACLs should be placed as close to the source as possible.

A standard ACL is only able to filter traffic based on the source host name or host IP address. Standard ACLs should be placed as close to the destination as possible.

Basic and advanced are not types of ACLs.

REFERENCES

-  4.4.5 Configure iptables Facts
-  5.13.3 Router Security Facts

q_router_sec_extended_secp7.question.fex

▼ Question 5: **✕** Incorrect

You are deploying a brand new router. After you change the factory default settings, what should you do next?

- ➡ ☒ **Update the firmware.**
- ☐ Configure anti-spoofing rules.
- ☐ Configure SSH to access the router configuration.
- ☐ Secure the configuration file.

EXPLANATION









After changing the default settings on the router, you should update the firmware. Updates to the firmware fix any vulnerabilities that have been resolved by the manufacturer in the past.

After updating the firmware, you should configure the protocol used to connect to the router.

The configuration file stores all the configuration settings for the router, including open ports, usernames, firewall settings, and more. If possible, store the router configuration file in an encrypted form and back up the file to a secure location.

Anti-spoofing rules counter spoofing attacks where IP packets have a source address that does not belong to the sender. This is configured after the router is set up.


REFERENCES

-  2.4.1 Vulnerability Concerns
-  2.4.2 Vulnerability Concerns Facts
-  2.4.3 Impact of Vulnerabilities
-  2.4.4 Impact of Vulnerabilities Facts
-  4.1.1 Manageable Network Plan
-  4.1.2 Manageable Network Plan 2
-  4.1.3 Manageable Network Plan Facts
-  5.13.3 Router Security Facts

q_router_sec_firmware_secp7.question.fex

▼ Question 6:  Incorrect

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

- ☐ Using SSH to remotely connect to a router
- ☐ Using the MD5 hashing algorithm to encrypt the password
-  ☒ **Not controlling physical access to the router**
- ☐ Storing the router configuration file in a secure location

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:

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

REFERENCES

5.13.3 Router Security Facts



q_router_sec_locks_secp7.question.fex

▼ Question 7:  Incorrect

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 username of admin and a password of P@ssW0rd. You have used the MD5 hashing algorithm to protect the password.

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

-  ☒ Change the default administrative username and password.
- ☐ Use a web browser to access the router configuration using an HTTP connection.
-  ☒ Use an SSH client to access the router configuration.
- ☐ Use encrypted Type 7 passwords.
- ☐ Use TFTP to back up the router configuration to a remote location.

EXPLANATION

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

- 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 username and password. Default usernames and passwords are readily available from websites 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 these protocols transmit data in cleartext.

REFERENCES

-  5.13.3 Router Security Facts

q_router_sec_ssh_01_secp7.question.fex

▼ Question 8: **✕ 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 username 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?

- ☐ 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.**
- ☐ Use an SSH client to access the router configuration.

EXPLANATION

In this scenario, the router configuration is being copied to a remote location using an unsecure protocol (File Transfer Protocol) 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 is also 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

 5.13.3 Router Security Facts

q_router_sec_ssh_02_secp7.question.fex

▼ Question 9:  Incorrect

You have configured your ACL to block outgoing traffic from a device with the IP address 192.168.1.52. Which type of ACL have you configured?

-  ☒ Standard
- ☐ Basic
- ☐ Advanced
- ☐ Extended



EXPLANATION

A standard ACL is only able to filter traffic based on the source host name or host IP address.

Extended ACLs are used to filter traffic based on many more parameters than standard ACLs. In addition to filtering based on source host name or host IP address, an extended ACL can filter based on source IP protocol, source or destination socket number, and destination host name or host IP address.

Basic and advanced are not types of ACLs.

REFERENCES

-  4.4.5 Configure iptables Facts
-  5.13.3 Router Security Facts

q_router_sec_standard_secp7.question.fex

▼ Question 10: **✕ Incorrect**

Which of the following does a router use to determine where packets are forwarded to?

- ➡ ☒ Routing table
- ☐ Access control list
- ☐ Anti-spoofing rules
- ☐ Firewall

EXPLANATION



Routers use a routing table to determine where network packets are forwarded to.

Router access control lists (ACLs) can be configured to increase security and limit traffic, much like a firewall but on the router level. ACLs filter the traffic and determine if the data should be blocked or forwarded.

Anti-spoofing rules counter spoofing attacks where IP packets have a source address that does not belong to the sender.

Firewalls are used on a network or host level to filter packets.

REFERENCES

-  4.4.5 Configure iptables Facts
-  5.13.3 Router Security Facts

q_router_sec_table_secp7.question.fex