Chp 4 NS

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 2/16/2022 10:04:13 pm • Time spent: 06:50

Score: 93% Passing Score: 80%

Question 1: ✔ Correct

Which of the following is the strongest form of multi-factor authentication?

- Two passwords
- Two-factor authentication
- A password and a biometric scan
- ➡ A password, a biometric scan, and a token device

EXPLANATION

A password, a biometric scan, and a token device together are the strongest form of multi-factor authentication listed here. Multi-factor authentication is any combination of two or more of the same or different authentication factors. The three common authentication factor types are something you know (such as a password), something you have (such as a smart card or a token device), and something you are (such as a biometric quality, like a fingerprint).

The other three options are all weaker forms of multi-factor authentication. A password and a biometric scan is a multi-factor authentication system, but this is also an example of two-factor authentication. Two-factor authentication is any combination of two or more different authentication factors. Two passwords is an example of multi-factor authentication, but since it uses two of the same type of factors, it is not a true two-factor authentication method.

Question 2: ✔ Correct

You want to give all managers the ability to view and edit a certain file. To do so, you need to edit the discretionary access control list (DACL) associated with the file. You want to be able to easily add and remove managers as their job positions change.

What is the BEST way to accomplish this?

- Create a distribution group for the managers. Add all users as members of the group. Add the group to the file's DACL.
- Add one manager to the DACL that grants all permissions. Have this user add other managers as required.
- ➡ Create a security group for the managers. Add all users as members of the group. Add the group to the file's DACL.
- Add each user account to the file's DACL.

EXPLANATION

Create a security group for the users and add the users to the DACL. A group is an object that identifies a set of users with similar access needs. Microsoft systems have two kinds of groups, which are distribution groups and security groups. Only security groups can be used for controlling access to objects. As manager roles change, add or remove user accounts from the group. Assigning permissions to a group grants those same permissions to all members of the group.

Adding individual user accounts instead of groups to the ACL would require more work as you add or remove managers.

Question 3: ✔ Correct

You have a file server named Srv3 that holds files used by the development department. You want to allow users to access the files over the network and control access to files accessed through the network or through a local logon.

Which solution should you implement?

- ➡ ◉ NTFS and share permissions
- ○ Share permissions and file screens
- ○ NTFS permissions and file screens
- ○ Share permissions and quotas

EXPLANATION

Use New Technology File System (NTFS) and share permissions to control access to files. Share permissions apply when files are accessed through the network, and NTFS permissions apply to both network and local access.

Use file screens to restrict the types of files that can be saved within a folder.

Question 4: ✔ Correct

Which of the following do security templates allow you to do? (Select two.)

- ☐ Apply new software patches
- ☐ Fix a specific software problem
- ☐ Block malicious websites
- ➡ ☑ Configure consistent security settings between devices
- ➡ ☑ Quickly apply settings to multiple computers

EXPLANATION

Security templates allow you to quickly and consistently apply settings to multiple computers in order to bring them into compliance with a security baseline.

Security templates are not used to apply new patches, block malicious websites, or fix specific software problems.

Question 5: ✔ Correct

In which milestone should you use a network scanner and then confirm the scan manually with a room-by-room walkthrough?

- ➡ (●) Map Your Network
- ( ) Reach Your Network
- ( ) Protect Your Network
- ( ) Prepare to Document

EXPLANATION

The Map Your Network milestone ensures that you are aware of all the components of the network and that you know where the physical devices are. The steps are:

- Create a map of the network topology.
- Create a list of all devices.
  - Don't forget to include wireless devices.
  - Use a network scanner and then confirm the scan manually with a room-by-room walkthrough.
  - Identify who is responsible for each device and detail other information, such as IP address, service tag, and physical location.
  - Consider using a database file to store the information.
- Create a list of all protocols being used on the network by using a network analyzer. Consider removing unauthorized devices and protocols from your network.

The Prepare to Document milestone means establishing the process you will use to document your network.

The Protect Your Network (network architecture) milestone identifies the necessary steps to protect your network.

The Reach Your Network (device accessibility) milestone helps to ensure that all of the devices on your network can be easily accessed while still maintaining each device's security. Accessibility includes physical access as well as remote access.

Question 6: ✔ Correct

You have hired 10 new temporary workers who will be with the company for three months. You want to make sure that the user accounts cannot be used for login after that time period. What should you do?

- ➡ Configure account expiration in the user accounts.
- Configure account policies in Group Policy.
- Configure day/time restrictions in the user accounts.
- Configure account lockout in Group Policy.

EXPLANATION

You should configure account expiration to disable an account after a specific date.

Use day/time restrictions to limit the days and hours when users can log on. Use account policies in Group Policy to configure requirements for passwords. Use account lockout settings in Group Policy to automatically lock accounts when a specific number of incorrect passwords are entered.

Question 7: ✔ Correct

FTPS uses which mechanism to provide security for authentication and data transfer?

- Token devices
- IPsec
- Multi-factor authentication
- ➡ SSL

EXPLANATION

File Transfer Protocol Secure (FTPS) uses Secure Sockets Layer (SSL) to provide security for authentication and data transfer. FTPS is an FTP replacement that brings reasonable security to an otherwise unsecure file-transfer mechanism. FTP by itself is unsecure because FTP transmits logon credentials in cleartext and does not encrypt transmitted files.

Question 8: ✔ Correct

You have recently experienced a security incident with one of your servers. After some research, you determine that a new hotfix has recently been released, which would have protected the server.

Which of the following recommendations should you follow when applying the hotfix?

- Apply the hotfix immediately to all servers.
- Apply the hotfix immediately to the server. Apply the hotfix to other devices only as the security threat manifests itself.
- Test the hotfix and then apply it to the server that had the problem.
- ➡ Test the hotfix and then apply it to all servers.

EXPLANATION

In this scenario, you should test the hotfix and only apply it to all other servers if the test is successful. Applying it only to the server that was compromised does not protect other servers with the same vulnerability. A common testing strategy is to:

1. Apply and test patches in a lab environment
2. Deploy patches to a set of systems, such as a single department
3. Deploy patches system-wide

Question 9: ✔ Correct

Which type of packet would the sender receive if they sent a connection request to TCP port 25 on a server with the following command applied?

sudo iptables -A OUTPUT -p tcp --dport 25 -j REJECT

- ICMP Unreachable Port
- ➡ RST
- ACK
- SYN

EXPLANATION

Because the packet is TCP and is blocked by the Reject action, the server would send a TCP RST packet back to the sender.

ICMP Unreachable Port is sent by iptables if a UDP packet is blocked by the Reject action.

A SYN packet would indicate that the server is proceeding with the connection, which would not happen with the Reject action. If it were allowed, the ACK would generally be sent with the SYN to acknowledge the initial connection while the SYN starts the next part of the TCP three-way handshake.

Question 10: ✔ Correct

You have configured the following rules. What is the effect?

sudo iptables -A INPUT -p tcp --dport 25 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
sudo iptables -A OUTPUT -p tcp --sport 25 -m conntrack --ctstate ESTABLISHED -j ACCEPT

- Block SSH traffic
- ➡ Allow SMTP traffic
- Block SMTP traffic
- Allow SSH traffic

EXPLANATION

These rules would allow inbound and outbound Simple Mail Transfer Protocol (SMTP) connections on TCP port 25, which is the default port for SMTP.

These rules use the Accept action, so they would not block SMTP or Secure Shell (SSH).

SSH is on TCP port 22, so these rules would not affect SSH.

Question 11: ✔ Correct

Prepare to Document means establishing the process you will use to document your network.

Which of the following makes this documentation more useful?

- ➡ ◉ Have a printed hard copy kept in a secure location.
- ○ Identify the choke points on the network.
- ○ Automate administration as much as possible.
- ○ Identify who is responsible for each device.

EXPLANATION

Prepare to Document means establishing the process you will use to document your network. A useful document:

- Is easy to use
- Includes enough detail
- Documents the important things
- Uses timestamps
- Is protected with restricted access and possibly encryption
- Has a printed hard copy kept in a secure location

Identifying who is responsible for each device is included in the Map Your Network milestone.

Identifying the choke points on the network is included in the Protect Your Network milestone.

Automating administration as much as possible is included in the Reach Your Network milestone.

Question 12: ✔ Correct

You want to make sure no unneeded software packages are running on your Linux server.

Select the command from the drop-down list that you can use to see all installed RPM packages.

yum list installed ✔

EXPLANATION

Unneeded software takes disk space and could introduce security flaws. To see all the RPM packages installed on your Linux server, run the following command:

yum list installed

After running this command, complete the following:

- Research the function of any unrecognized RPM package to determine whether it is necessary.
- Use **yum** or **rpm** to uninstall unneeded packages.

Question 13: ✔ Correct

What does the **netstat -a** command show?

- All listening sockets
- All network users
- All connected hosts
- ➡ All listening and non-listening sockets

EXPLANATION

The **netstat -a** command shows the status of all listening and non-listening sockets.

Question 14: ✔ Correct

In which of the iptables default chains would you configure a rule to allow an external device to access the HTTPS port on the Linux server?

- Forward
- ➡ Input
- Output
- Accept

EXPLANATION

The Input chain would be where you would place the rule as it is used for inbound connections.

The Output chain is for outbound connections.

The Forward chain is for sending connections through the Linux server to another device.

The Accept action can be used in a rule to allow a connection. However, it is not a chain.

Question 15: ✔ Correct

To increase security on your company's internal network, the administrator has disabled as many ports as possible. However, now you can browse the internet, but you are unable to perform secure credit card transactions.

Which port needs to be enabled to allow secure transactions?

- 69
- ➡ 443
- 21
- 23
- 80

EXPLANATION

To perform secure transactions, SSL on port 443 needs to be enabled. HTTPS uses port 443 by default.

Question 16: ✔ Correct

Which type of update should be prioritized even outside of a normal patching window?

- ➡ Critical updates
- Monthly updates
- Microsoft updates
- Security updates

EXPLANATION

The correct answer is critical updates. These updates are often marked critical because of the severity of the exploit or how widespread it is.

Microsoft, monthly, and security updates do not necessarily demand to be installed outside of a normal patching window.

Question 17: ✔ Correct

Which of the following is defined as an operating system that comes hardened and validated to a specific security level as defined in the Common Criteria for Information Technology Security Evaluation (CC)?

- UNIX
- Windows
- OS X
- ➡ TOS

EXPLANATION

A trusted operating system (TOS) is one that has been hardened and validated to a specific level as defined by the Common Criteria.

Windows, UNIX, and OS X are not TOSs by default.

Question 18: ✔ Correct

As you go through the process of making your network more manageable, you discover that employees in the sales department are on the same network segment as the human resources department.

Which of the following steps can be used to isolate these departments?

- ➡ Create a separate VLAN for each department.
- Identify the choke points on your network.
- Move the sales department into the DMZ.
- Implement the principle of least privilege for the human resources department.

EXPLANATION

VLANs can be used to isolate these departments.

The sales department is not a lower-trust part of the network, so they do not belong in the DMZ.

You would identify choke points as part of the process of limiting the number of internet access points on your network in order to decrease the attack surface.

The principle of least privilege is used to control user access to network resources. However, this principle does not segregate and isolate network segments from each other.

Question 19: ✔ Correct

For Milestone 4 (Reach Your Network), which of the following would be considered a secure protocol to use to reach your network?

- Telnet
- ➡ SSH
- HTTP
- FTP

EXPLANATION

Of the protocols listed, only Secure Shell (SSH) is encrypted. The other protocols would expose data to being easily intercepted.

Question 20: ✕ Incorrect

You have recently been hired as the new network administrator for a startup company. The company's network was implemented prior to your arrival. One of the first tasks you need to complete in your new position is to develop a manageable network plan for the network.

You have already completed the first and second milestones, in which documentation procedures were identified and the network was mapped. You are now working on the third milestone, which is identifying ways to protect the network.

Which tasks should you complete as a part of this milestone? (Select two.)

- [ ] Apply critical patches whenever they are released.
- [x] ~~Set account expiration dates.~~
- [ ] Identify and document each user on the network.
- [x] Physically secure high-value systems.
- [ ] Create an approved application list for each network device.

EXPLANATION

In the third milestone (Protect Your Network), you should take the following steps:

- Identify and document each user on the network and the information he or she has access to.
- Identify high-value network assets.
- Document the trust boundaries.
- Identify the choke points on the network.
- Segregate and isolate networks.
- Isolate server functions.
- Physically secure high-value systems.

Setting account expiration dates is part of the fifth milestone (Control Your Network).

Applying critical patches and creating an approved application list are both tasks associated with the sixth milestone (Manage Your Network).

Question 21: ✔ Correct

You want to close all ports associated with NetBIOS on your network's firewalls to prevent attacks directed against NetBIOS. Which ports should you close?

- 67, 68
- 135, 137-139
- 161, 162
- 389, 636

EXPLANATION

NetBIOS uses the following ports:

- TCP 135
- TCP and UDP 137
- TCP and UDP 138
- TCP 139

Dynamic Host Configuration Protocol (DHCP) uses ports 67 and 68. Simple Network Management Protocol (SNMP) uses ports 161 and 162. Lightweight Directory Access Protocol (LDAP) uses ports 389 and 636.

Question 22: ✔ Correct

You have placed a File Transfer Protocol (FTP) server in your DMZ behind your firewall. The FTP server is to be used to distribute software updates and demonstration versions of your products. However, users report that they are unable to access the FTP server.

What should you do to enable access?

- Define user accounts for all external visitors.
- Open ports 20 and 21 for inbound and outbound connections.
- Move the FTP outside of the firewall.
- Install a VPN.

EXPLANATION

To allow FTP traffic into your DMZ, you must open the correct ports on the firewall. For FTP, the correct ports are 20 and 21 for outbound connections.

Installing a VPN is not necessary to grant access to external users. Defining user accounts may be required in some situations, but this scenario requires anonymous access. Moving the FTP server outside the firewall is not a secure action.

Question 23: ✕ Incorrect

To answer this question, complete the lab using the information below. **Launch Lab**

You did not attempt the lab.

Question 24: ✔ Correct

Which of the following describes a configuration baseline?

- ➡ ◉ A list of common security settings that a group or all devices share
- ○ A collection of security settings that can be automatically applied to a device
- ○ The minimum services required for a server to function
- ○ A set of performance statistics that identifies normal operating performance

EXPLANATION

A configuration baseline is a set of consistent requirements for a workstation or server. Configuration baselines include a component that ensures that all workstations and servers comply with the security goals of the organization.

A security template is a saved set of configuration values that produce the system configuration as specified in the configuration baseline. When you apply the security template to a system, the settings within the template are applied to the system.

A performance baseline is a set of performance statistics that identify normal operating performance.

Question 25: ✔ Correct

You need to increase the security of your Linux system by finding and closing open ports. Which of the following commands should you use to locate open ports?

- **traceroute**
- **nmap**
- **nslookup**
- **netstat**

EXPLANATION

Use **nmap** to locate open ports. Open ports can provide information about which operating system a computer uses and might provide entry points or information about ways to formulate an attack. Use one of the following commands to scan for open ports:

- **nmap -sT** scans for TCP ports.
- **nmap -sU** scan for UDP ports.

The **netstat** command shows the status of listening and non-listening sockets. A socket is an endpoint of a bidirectional communication flow across a computer network. The **nslookup** command is used for name resolution requests. The **traceroute** command tests and displays connectivity between devices.

Question 26: ✔ Correct

What should you consider security baselines?

- Static
- Unchangeable
- Dynamic
- Suggestion

EXPLANATION

Because most environments are constantly changing, security baselines must also be dynamic and react to the changes.

They are not static or unchangeable due to changes in the environment.

They are not a suggestion. If implemented correctly, they provide the rules for how to configure devices.

Question 27: ✔ Correct

To answer this question, complete the lab using the information below.
You have already answered this question.
You are not allowed to view the lab again.

Launch Lab

You completed the lab correctly.

View Lab Report

Question 28: ✔ Correct

Which action would you use in a rule to disallow a connection silently?

- Forward
- Accept
- ➡ Drop
- Reject

EXPLANATION

The Drop action is used to silently disallow a connection; the sending system receives no notice. The Reject action also disallows a connection but sends a TCP RST packet or an ICMP port unreachable packet back to the system that sent the original packet.

Accept would allow the packet.

Forward is a chain, not an action in iptables.

Question 29: ✔ Correct

Which command would you use to list all of the currently defined iptables rules?

- ➡ **sudo iptables -L**
- **sudo iptables -F**
- **sudo /sbin/iptables-save**
- **sudo iptables -A INPUT -j DROP**

EXPLANATION

sudo iptables -L lists all of the currently defined rules.

sudo iptables -A INPUT -j DROP would drop all incoming traffic.

sudo /sbin/iptables-save saves changes to iptables on Ubuntu.

sudo iptables -F would flush all current rules from iptables.

Question 30: ✔ Correct

To transfer files to your company's internal network from home, you use FTP. The administrator has recently implemented a firewall at the network perimeter and disabled as many ports as possible.

Now, you can no longer make the FTP connection. You suspect the firewall is causing the issue. Which ports need to remain open so you can still transfer the files? (Select two.)

- ☐ 80
- ➡ ☑ 20
- ☐ 443
- ☐ 23
- ➡ ☑ 21

EXPLANATION

FTP uses port 21 for connection requests and port 20 for data transfers. Both ports need to remain open for you to transfer files to your company's internal network from home.

Telnet uses port 23, SSL uses port 443, and HTTP uses port 80.