Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 4/19/2022 7:42:44 pm • Time spent: 05:12

Score: 70% Passing Score: 80%

Question 1: ✔ Correct

You need to find the text string New Haven in 100 documents in a folder structure on a Linux server. Which command would you use?

- **chmod**
- **tail**
- **grep**
- **head**

EXPLANATION

You would choose the **grep** command. This command searches through files for a specified character string. By default, **grep** is context-sensitive and displays the string in the context of the line containing the string.

The **chmod** command assigns or removes permissions to users, groups, or others.

The **head** command shows the first few lines of a file.

The **tail** command shows the last few lines of a file.

REFERENCES

12.6.2 Manipulating Files Facts

q_file_manipulate_grep_secp7.question.fex

Question 2: ✔ Correct

You would like to add some entries into the system log file. Which command would you use?

- **logger**
- **cat**
- **grep**
- **chmod**

EXPLANATION

You would choose the **logger** command. This command lets you add entries in the system log file.

The **grep** command searches a file for a specified character string.

The **chmod** command changes permissions for a file.

The **cat** command lists the contents of a file.

REFERENCES

12.6.2 Manipulating Files Facts

q_file_manipulate_logger_secp7.question.fex

Question 3: ✔ Correct

You would like to see only the last 15 lines of /home/user/logfile on your Linux machine. Which command line interface (CLI) command would you use?

- **head -n 15 /home/user/logfile**
- **tail -n 15 /home/user/logfile**
- **tail -f /home/user/logfile**
- **cat -n 15 /home/user/logfile**

EXPLANATION

You would choose the **tail -n 15 /home/user/logfile** command.

The **cat** command displays the entire file.

The **head** command only shows the first requested lines of a file.

The **tail -f** command dynamically monitors the file by showing the last 10 lines of a file and new lines as they are added.

REFERENCES

12.6.2 Manipulating Files Facts

q_file_manipulate_tail_secp7.question.fex

Question 4: ✕ Incorrect

A conditional statement that selects the statements to run depending on whether an expression is true or false is known as which of the following?

- If else statement
- Else statement
- Else if statement
- ~~If statement~~

EXPLANATION

An *if else* statement is a conditional statement that selects the statements to run depending on whether an expression is true or false.

An *if* statement is a conditional statement that, if proven true, performs a function or displays information.

Else is a conditional statement that, if previous conditions are not true, displays alternate information or performs alternate commands.

Else if is a conditional statement performed after an if statement that, if true, performs a function.

REFERENCES

12.6.4 Shells and Scripting Facts

q_shells_ifelse_constant_secp7.question.fex

Question 5: ✔ Correct

Which of the following BEST describes a constant?

- A named unit of data that is assigned a value.
- A sequence of characters.
- A group of related data values or elements.
- Data or a value that does not change.

EXPLANATION

A constant is data or a value that does not change (unlike a variable).

A variable is a named unit of data that is assigned a value.

An array is a group of related data values or elements that are grouped together.

A string is a sequence of characters. Strings exist as either a literal constant or as some kind of variable.

REFERENCES

12.6.4 Shells and Scripting Facts

q_shells_scripting_constant_secp7.question.fex

Question 6: ✕ Incorrect

!= or <> refers to Not Equal in which scripting language?

- Bash
- ~~PowerShell~~
- PuTTY
- Python

EXPLANATION

!= or <> refers to Not Equal in the Python scripting language.

-ne refers to Not Equal in the Bash scripting language.

ne refers to Not Equal in the PowerShell scripting language.

PuTTY is an SSH and Telnet client that was originally developed for the Windows platform.

REFERENCES

12.6.4 Shells and Scripting Facts

q_shells_scripting_python_secp7.question.fex

Question 7: ✔ Correct

Which of the following BEST describes PuTTy?

- A mechanism that allows you to interact with the operating system directly.
- ➡ Open-source software that is developed and supported by a group of volunteers.
- A method that provides an encryption standard that's widely used by internet websites.
- A programming language for a special runtime environment that automates the execution of tasks.

EXPLANATION

PuTTY is open-source software that is developed and supported by a group of volunteers.

Secure Sockets Layer (SSL) is a method that provides an encryption standard that's widely used by internet websites.

A scripting language is a programming language made for a special runtime environment that automates the execution of tasks.

A shell refers to the mechanism that allows you to interact with the operating system directly.

REFERENCES

12.6.4 Shells and Scripting Facts

q_shells_scripting_ssh_secp7.question.fex

Question 8: ✕ Incorrect

Match each network sniffing method with the correct definition.

MAC spoofing

~~The MAC address of the attacker can be associated with the IP address of another host.~~

Allows an attacker's computer to connect to a switch using an authorized MAC address.

MAC flooding

✓ The process of intentionally overwhelming the CAM table with Ethernet frames, each originating from a different MAC address.

ARP poisoning

~~Allows an attacker's computer to connect to a switch using an authorized MAC address.~~

The MAC address of the attacker can be associated with the IP address of another host.

Port mirroring

✓ Creates a duplicate of all network traffic on a port and sends it to another device.

EXPLANATION

MAC spoofing allows an attacker's computer to connect to a switch using an authorized MAC address.
MAC flooding is the process of intentionally overwhelming the CAM table with Ethernet frames, each originating from a different MAC address.
With ARP poisoning, the MAC address of the attacker can be associated with the IP address of another host.
Port mirroring creates a duplicate of all network traffic on a port and sends it to another device.

REFERENCES

12.6.7 Packet Capture Facts

q_capturepkt_layer2_secp7.question.fex

Question 9: ✔ Correct

For some reason, when you capture packets as part of your monitoring, you aren't seeing much traffic. What could be the reason?

- ➡ You forgot to turn on promiscuous mode for the network interface.
- Your machine is set to only capture HTTP packets.
- Your NIC is set to broadcasting instead of receiving.
- You have multiple MAC addresses associated with one NIC.

EXPLANATION

The most likely reason is that you forgot to turn on promiscuous mode for your network interface. Turning on promiscuous mode gives the interface permission to grab every frame that comes its way, even if the frame is addressed to someone else.

REFERENCES

12.6.7 Packet Capture Facts

q_capturepkt_promis_secp7.question.fex

Question 10: ✔ Correct

You would like to simulate an attack on your network so you can test defense equipment and discover vulnerabilities in order to mitigate risk. Which tool would you use to simulate all the packets of an attack?

- TCPDump
- ➡ TCPReplay
- Etherflood
- Wireshark

EXPLANATION

You would use TCPReplay. You could use TCPDump or Wireshark to capture the packets, but you would use TCPReplay to actually replay and simulate the attack.

Etherflood is a tool that can flood a switched network with random MAC addresses.

REFERENCES

12.6.7 Packet Capture Facts

q_capturepkt_tcprelay_secp7.question.fex