PT0-002 Q&As

CompTIA PenTest+ Certification Exam

QUESTION 1

A company hired a penetration-testing team to review the cyber-physical systems in a manufacturing plant. The team immediately discovered the supervisory systems and PLCs are both connected to the company intranet. Which of the following assumptions, if made by the penetration-testing team, is MOST likely to be valid?

A. PLCs will not act upon commands injected over the network.

B. Supervisors and controllers are on a separate virtual network by default.

C. Controllers will not validate the origin of commands.

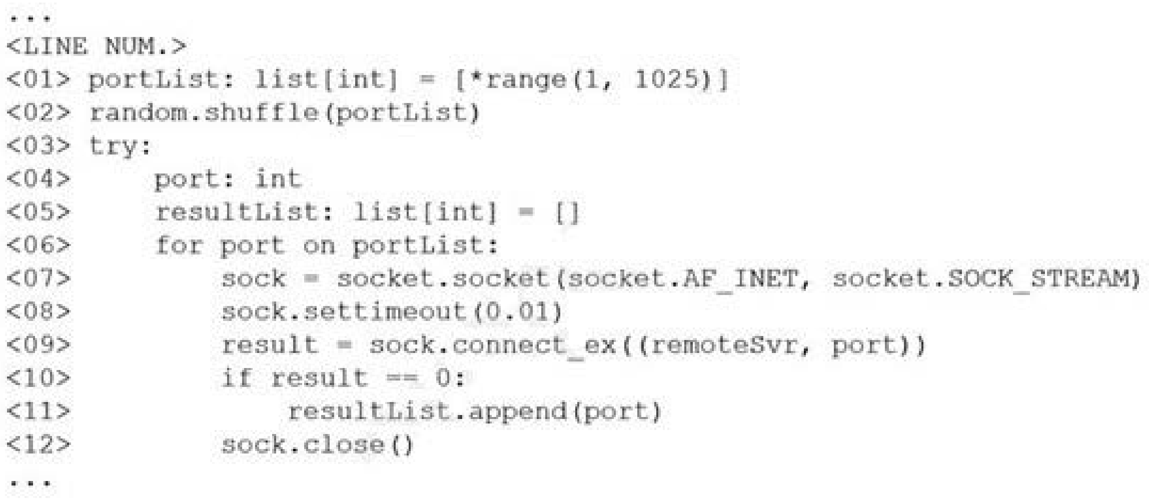
D. Supervisory systems will detect a malicious injection of code/commands.

Correct Answer: C

PLCs are programmable logic controllers that execute logic operations on input signals from sensors and output signals to actuators. They are often connected to supervisory systems that provide human-machine interfaces and data acquisition functions. If both systems are connected to the company intranet, they are exposed to potential attacks from internal or external adversaries. A valid assumption is that controllers will not validate the origin of commands, meaning that an attacker can send malicious commands to manipulate or sabotage the industrial process. The other assumptions are not valid because they contradict the facts or common practices.

QUESTION 2

The following line-numbered Python code snippet is being used in reconnaissance:



```
...
<LINE NUM.>
<01> portList: list[int] = [*range(1, 1025)]
<02> random.shuffle(portList)
<03> try:
<04>     port: int
<05>     resultList: list[int] = []
<06>     for port on portList:
<07>         sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
<08>         sock.settimeout(0.01)
<09>         result = sock.connect_ex((remoteSvr, port))
<10>         if result == 0:
<11>             resultList.append(port)
<12>         sock.close()
...
```

Which of the following line numbers from the script MOST likely contributed to the script triggering a "probable port scan" alert in the organization\\'s IDS?

A. Line 01

B. Line 02

C. Line 07

D. Line 08

Correct Answer: D

QUESTION 3

A penetration tester is conducting an on-path link layer attack in order to take control of a key fob that controls an electric vehicle. Which of the following wireless attacks would allow a penetration tester to achieve a successful attack?

A. Bluejacking

B. Bluesnarfing

C. BLE attack

D. WPS PIN attack

Correct Answer: C

A BLE (Bluetooth Low Energy) attack is specifically designed to exploit vulnerabilities in the Bluetooth Low Energy protocol, which is commonly used in modern wireless devices, including key fobs for electric vehicles. This type of attack can allow a penetration tester to intercept, manipulate, or take control of the communication between the key fob and the vehicle. Bluejacking and Bluesnarfing are older Bluetooth attacks that are less effective against modern BLE implementations. WPS PIN attacks target Wi- Fi Protected Setup, which is unrelated to key fobs and electric vehicles.

QUESTION 4

A consultant is reviewing the following output after reports of intermittent connectivity issues:

```
(192.168.1.1) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet]

(192.168.1.12) at 34:a4:be:09:44:f4 on en0 ifscope [ethernet]

(192.168.1.17) at 92:60:29:12:ac:d2 on en0 ifscope [ethernet]

(192.168.1.34) at 88:de:a9:12:ce:fb on en0 ifscope [ethernet]

(192.168.1.136) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet]

(192.168.1.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]

(224.0.0.251) at 01:02:5e:7f:ff:fa on en0 ifscope permanent [ethernet]

(239.255.255.250) at ff:ff:ff:ff:ff:ff on en0 ifscope permanent [ethernet]
```

Which of the following is MOST likely to be reported by the consultant?

A. A device on the network has an IP address in the wrong subnet.

B. A multicast session was initiated using the wrong multicast group.

C. An ARP flooding attack is using the broadcast address to perform DDoS.

D. A device on the network has poisoned the ARP cache.

Correct Answer: D

The gateway for the network (192.168.1.1) is at 0a:d1:fa:b1:01:67, and then, another machine (192.168.1.136) also claims to be on the same MAC address. With this on the same network, intermittent connectivity will be inevitable as along as

the gateway remains unreachable on the IP known by the others machines on the network, and given that the new machine claiming to be the gateway has not been configured to route traffic. The output shows an ARP table that contains

entries for IP addresses and their corresponding MAC addresses on a local network interface (en0). ARP stands for Address Resolution Protocol and is used to map IP addresses to MAC addresses on a network.

However, one entry in the table is suspicious:

? (192.168.1.136) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet] This entry has the same MAC address as another entry:

? (192.168.1.1) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet] This indicates that a device on the network has poisoned the ARP cache by sending false ARP replies that associate its MAC address with multiple IP addresses, including

192.168.1.136 and 192.168.1.1 (which is likely the gateway address). This allows the device to intercept or redirect traffic intended for those IP addresses.

QUESTION 5

A penetration tester is trying to bypass an active response tool that blocks IP addresses that have more than 100 connections per minute. Which of the following commands would allow the tester to finish the test without being blocked?

A. nmap -sU -p 1-1024 10.0.0.15

B. nmap -p 22,25, 80, 3389 -T2 10.0.0.15 -Pn

C. nmap -T5 -p 1-65535 -A 10.0.0.15

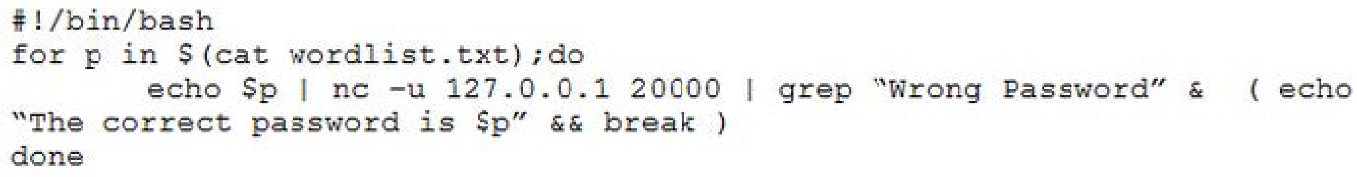
D. nmap -T3 -F 10.0.0.15

Correct Answer: B

The -T2 flag in Nmap sets the timing template to "polite", which means that Nmap will limit the number of parallel probes to 10 and the scan delay to 0.4 seconds. This will reduce the number of connections per minute and avoid triggering the active response tool. The -Pn flag tells Nmap to skip the host discovery phase and scan the target regardless of its ping response. The other options are not suitable for bypassing the active response tool, as they either scan too many ports (sU, -T5, -F) or use a faster timing template (-T5, -T3) that will generate more connections per minute. References: map Cheat Sheet 2024: All the Commands and Flags - StationX map Commands - 17 Basic Commands for Linux Network - phoenixNAP MAP Flag Guide: What They Are, When to Use Them - CBT Nuggets

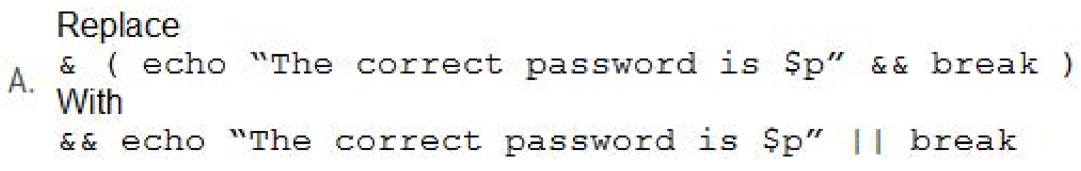
QUESTION 6

A penetration tester wrote the following Bash script to brute force a local service password:

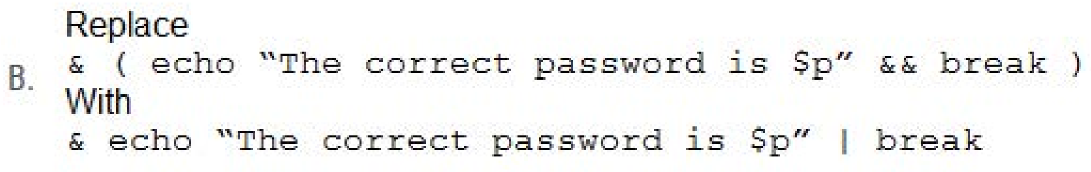


```
#!/bin/bash
for p in $(cat wordlist.txt);do
        echo $p | nc -u 127.0.0.1 20000 | grep “Wrong Password” &  ( echo
“The correct password is $p” && break )
done
```

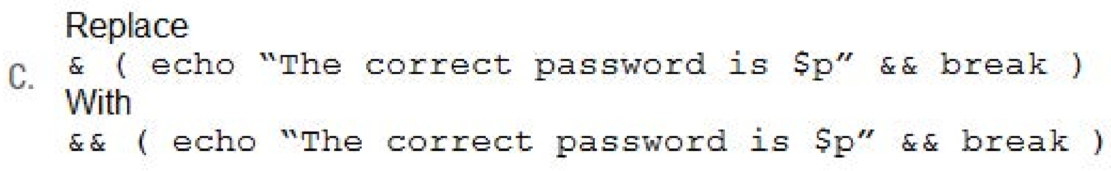
The script is not working as expected. Which of the following changes should the penetration tester make to get the script to work?



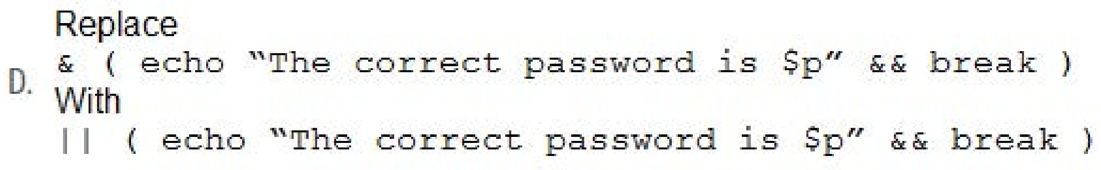
A.
Replace
```
& ( echo “The correct password is $p” && break )
```
With
```
&& echo “The correct password is $p” || break
```



B.
Replace
```
& ( echo “The correct password is $p” && break )
```
With
```
& echo “The correct password is $p” | break
```



C.
Replace
```
& ( echo “The correct password is $p” && break )
```
With
```
&& ( echo “The correct password is $p” && break )
```



D.
Replace
```
& ( echo “The correct password is $p” && break )
```
With
```
|| ( echo “The correct password is $p” && break )
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: A

QUESTION 7

A penetration tester managed to exploit a vulnerability using the following payload:

IF (1=1) WAIT FOR DELAY \\'0:0:15\\'

Which of the following actions would best mitigate this type ol attack?

A. Encrypting passwords

B. Parameterizing queries

C. Encoding output

D. Sanitizing HTML

Correct Answer: B

The payload used by the penetration tester is a type of blind SQL injection attack that delays the response of the database by 15 seconds if the condition is true. This can be used to extract information from the database by asking a series of true or false questions. To prevent this type of attack, the best practice is to use parameterized queries, which separate the user input from the SQL statement and prevent the injection of malicious code. Encrypting passwords, encoding output, and sanitizing HTML are also good security measures, but they do not directly address the SQL injection vulnerability. References: The Official CompTIA PenTest+ Study Guide (Exam PT0-002), Chapter 5: Attacks and Exploits, Section 5.2: Perform Network Attacks, Subsection: SQL Injection, p. 235-237 Blind SQL Injection | OWASP Foundation, Description and Examples sections Time-Based Blind SQL Injection Attacks, Introduction and Microsoft SQL Server sections

QUESTION 8

Which of the following assessment methods is MOST likely to cause harm to an ICS environment?

A. Active scanning

B. Ping sweep

C. Protocol reversing

D. Packet analysis

Correct Answer: A

QUESTION 9

During enumeration, a red team discovered that an external web server was frequented by employees. After compromising the server, which of the following attacks would best support ------------company systems?

A. Aside-channel attack

B. A command injection attack

C. A watering-hole attack

D. A cross-site scripting attack

Correct Answer: C

The best attack that would support compromising company systems after compromising an external web server frequented by employees is a watering-hole attack, which is an attack that involves compromising a website that is visited by a specific group of users, such as employees of a target company, and injecting malicious code or content into the website that can infect or exploit the users\\' devices when they visit the website. A watering-hole attack can allow an attacker to compromise company systems by targeting their employees who frequent the external web server, and taking advantage of their trust or habit of visiting the website. A watering-hole attack can be performed by using tools such as BeEF, which is a tool that can hook web browsers and execute commands on them2. The other options are not likely attacks that would support compromising company systems after compromising an external web server frequented by employees. A side- channel attack is an attack that involves exploiting physical characteristics or implementation flaws of a system or device, such as power consumption, electromagnetic radiation, timing, or sound, to extract sensitive information or bypass security mechanisms. A command injection attack is an attack that exploits a vulnerability in a system or application that allows an attacker to execute arbitrary commands on the underlying OS or shell. A cross-site scripting attack is an attack that exploits a vulnerability in a web application that allows an attacker to inject malicious scripts into web pages that are viewed by other users.

QUESTION 10

An assessor wants to run an Nmap scan as quietly as possible. Which of the following commands will give the LEAST chance of detection?

A. nmap -"T3 192.168.0.1

B. nmap - "P0 192.168.0.1

C. nmap - T0 192.168.0.1

D. nmap - A 192.168.0.1

Correct Answer: C

QUESTION 11

During a test of a custom-built web application, a penetration tester identifies several vulnerabilities. Which of the following would be the most interested in the steps to reproduce these vulnerabilities?

A. Operations staff

B. Developers

C. Third-party stakeholders

D. C-suite executives

Correct Answer: B

The developers would be the most interested in the steps to reproduce the web application vulnerabilities, because they are responsible for fixing the code and implementing security best practices. The steps to reproduce the vulnerabilities would help them understand the root cause of the problem, test the patches, and prevent similar issues in the future. The other options are less interested in the technical details of the vulnerabilities, as they have different roles and responsibilities. The operations staff are more concerned with the availability and performance of the web application, the third-party stakeholders are more interested in the business impact and risk assessment of the vulnerabilities, and the C-suite executives are more focused on the strategic and financial implications of the vulnerabilities123.

QUESTION 12

A red team gained access to the internal network of a client during an engagement and used the Responder tool to capture important data. Which of the following was captured by the testing team?

A. Multiple handshakes

B. IP addresses

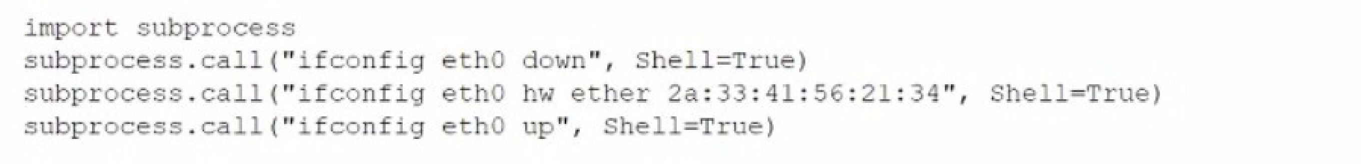
C. Encrypted file transfers

D. User hashes sent over SMB

Correct Answer: B

QUESTION 13

During an assessment, a penetration tester found a suspicious script that could indicate a prior compromise. While reading the script, the penetration tester noticed the following lines of code:



```
import subprocess
subprocess.call("ifconfig eth0 down", Shell=True)
subprocess.call("ifconfig eth0 hw ether 2a:33:41:56:21:34", Shell=True)
subprocess.call("ifconfig eth0 up", Shell=True)
```

Which of the following was the script author trying to do?

A. Spawn a local shell.

B. Disable NIC.

C. List processes.

D. Change the MAC address

Correct Answer: D

This Python script uses the subprocess.call function to execute shell commands that first bring down the network interface eth0 (though it seems there\\'s a typo with "etho0"), change its MAC address to "2a:33:41:56:21:34", and then bring the interface back up. The purpose of these actions is to change the MAC address of the network interface card (NIC) associated with eth0. Changing a MAC address can be used for various reasons, including bypassing MAC address filters or anonymizing the device on the network.

QUESTION 14

When accessing the URL http://192.168.0-1/validate/user.php, a penetration tester obtained the following output:

..d index: eid in /apache/www/validate/user.php line 12

..d index: uid in /apache/www/validate/user.php line 13

..d index: pw in /apache/www/validate/user.php line 14

..d index: acl in /apache/www/validate/user.php line 15

A. Lack of code signing

B. Incorrect command syntax

C. Insufficient error handling

D. Insecure data transmission

Correct Answer: C

The most probable cause for this output is insufficient error handling, which is a coding flaw that occurs when a program does not handle errors or exceptions properly or gracefully. Insufficient error handling can result in unwanted or unexpected behavior, such as crashes, hangs, or leaks. In this case, the output shows that the program is displaying warning messages that indicate undefined indexes in the user.php file. These messages reveal the names of the variables and the file path that are used by the program, which can expose sensitive information or clues to an attacker. The program should have implemented error handling mechanisms, such as try-catch blocks, error logging, or sanitizing output, to prevent these messages from being displayed or to handle them appropriately. The other options are not plausible causes for this output. Lack of code signing is a security flaw that occurs when a program does not have a digital signature that verifies its authenticity and integrity. Incorrect command syntax is a user error that occurs when a command is entered with wrong or missing parameters or options. Insecure data transmission is a security flaw that occurs when data is sent over a network without encryption or protection.

QUESTION 15

A penetration tester who is conducting a web-application test discovers a clickjacking vulnerability associated with a login page to financial data. Which of the following should the tester do with this information to make this a successful exploit?

A. Perform XSS.

B. Conduct a watering-hole attack.

C. Use BeEF.

D. Use browser autopwn.

Correct Answer: B

A clickjacking vulnerability allows an attacker to trick a user into clicking on a hidden element on a web page, such as a login button or a link. A watering-hole attack is a technique where the attacker compromises a website that is frequently visited by the target users, and injects malicious code or content into the website. The attacker can then use the clickjacking vulnerability to redirect the users to a malicious website or perform unauthorized actions on their behalf.

A. Perform XSS. This is incorrect. XSS (cross-site scripting) is a vulnerability where an attacker injects malicious scripts into a web page that are executed by the browser of the victim. XSS can be used to steal cookies, session tokens, or

other sensitive information, but it is not directly related to clickjacking.

C. Use BeEF. This is incorrect. BeEF (Browser Exploitation Framework) is a tool that allows an attacker to exploit various browser vulnerabilities and take control of the browser of the victim. BeEF can be used to launch clickjacking attacks,

but it is not the only way to do so.

D. Use browser autopwn. This is incorrect. Browser autopwn is a feature of Metasploit that automatically exploits browser vulnerabilities and delivers a payload to the victim\\'s system. Browser autopwn can be used to compromise the browser

of the victim, but it is not directly related to clickjacking.

References:

1: OWASP Foundation, "Clickjacking", https://owasp.org/www- community/attacks/Clickjacking

2: PortSwigger, "What is clickjacking? Tutorial and Examples", https://portswigger.net/web-security/clickjacking

4: Akto, "Clickjacking: Understanding vulnerability, attacks and prevention", https://www.akto.io/blog/clickjacking-understanding-vulnerability-attacks-and- prevention