



CompTIA

Exam Questions PT0-003

CompTIA PenTest+ Exam

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

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

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

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

NEW QUESTION 1

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

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

Answer: A

Explanation:

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

? Understanding Smishing:

? Why Smishing is Effective:

? Alternative Attack Techniques:

=====

NEW QUESTION 2

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.

Your Partner of IT Exam

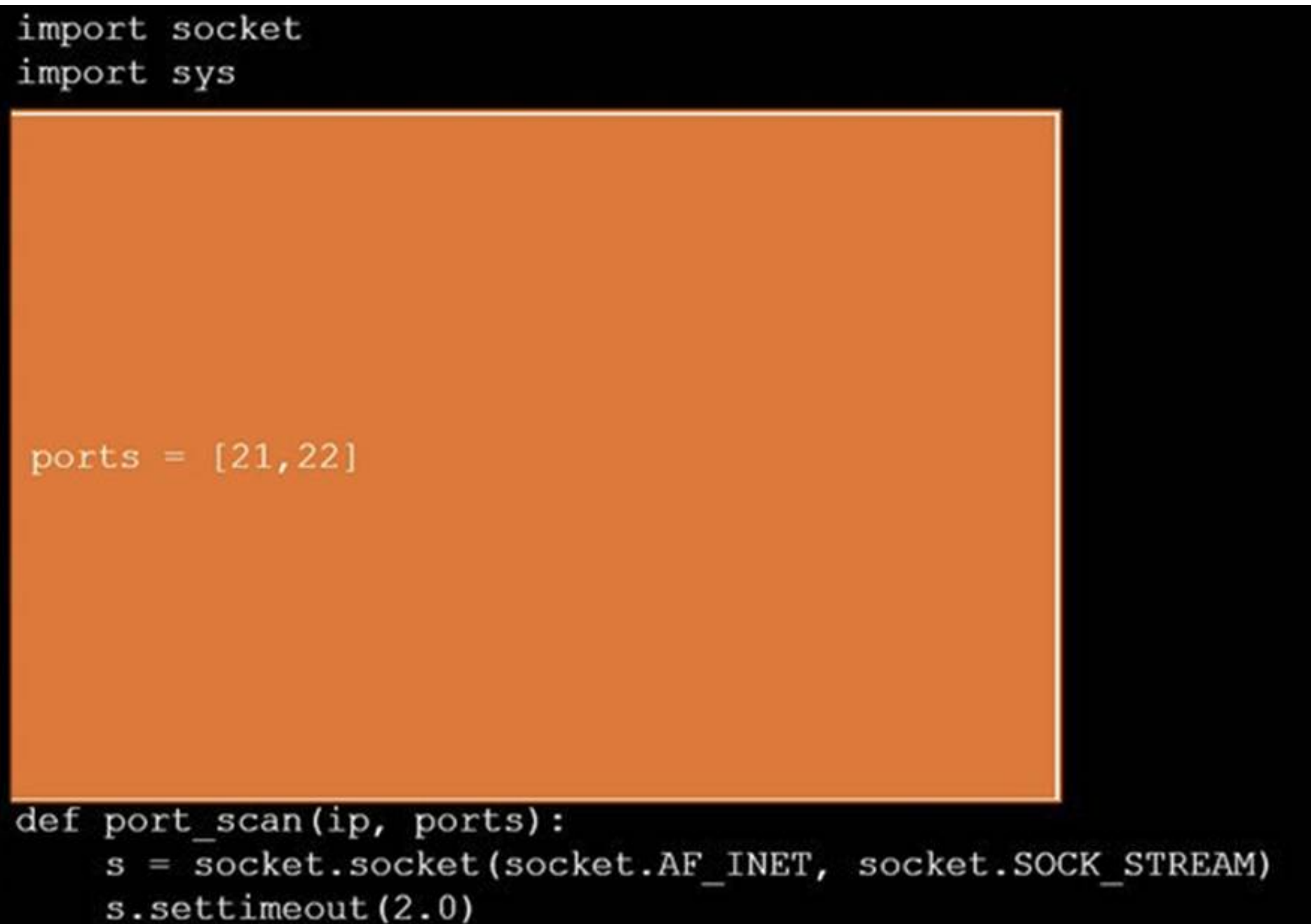
- A. Mastered
- B. Not Mastered

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

A penetration tester would like to leverage a CSRF vulnerability to gather sensitive details from an application's end users. Which of the following tools should the tester use for this task?

- A. Browser Exploitation Framework
- B. Maltego
- C. Metasploit
- D. theHarvester

Answer: A

Explanation:

Cross-Site Request Forgery (CSRF) vulnerabilities can be leveraged to trick authenticated users into performing unwanted actions on a web application. The right tool for this task would help in exploiting web-based vulnerabilities, particularly those related to web browsers and interactions.

? Browser Exploitation Framework (BeEF) (Answer: A):

? Maltego (Option B):

? Metasploit (Option C):

? theHarvester (Option D):

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

NEW QUESTION 4

A penetration tester is working on an engagement in which a main objective is to collect confidential information that could be used to exfiltrate data and perform a ransomware attack. During the engagement, the tester is able to obtain an internal foothold on the target network. Which of the following is the next task the tester should complete to accomplish the objective?

- A. Initiate a social engineering campaign.
- B. Perform credential dumping.
- C. Compromise an endpoint.
- D. Share enumeration.

Answer: D

Explanation:

Given that the penetration tester has already obtained an internal foothold on the target network, the next logical step to achieve the objective of collecting confidential information and potentially exfiltrating data or performing a ransomware attack is to perform credential dumping. Here's why:

? Credential Dumping:

? Comparison with Other Options:

Performing credential dumping is the most effective next step to escalate privileges and access sensitive data, making it the best choice.

=====

NEW QUESTION 5

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

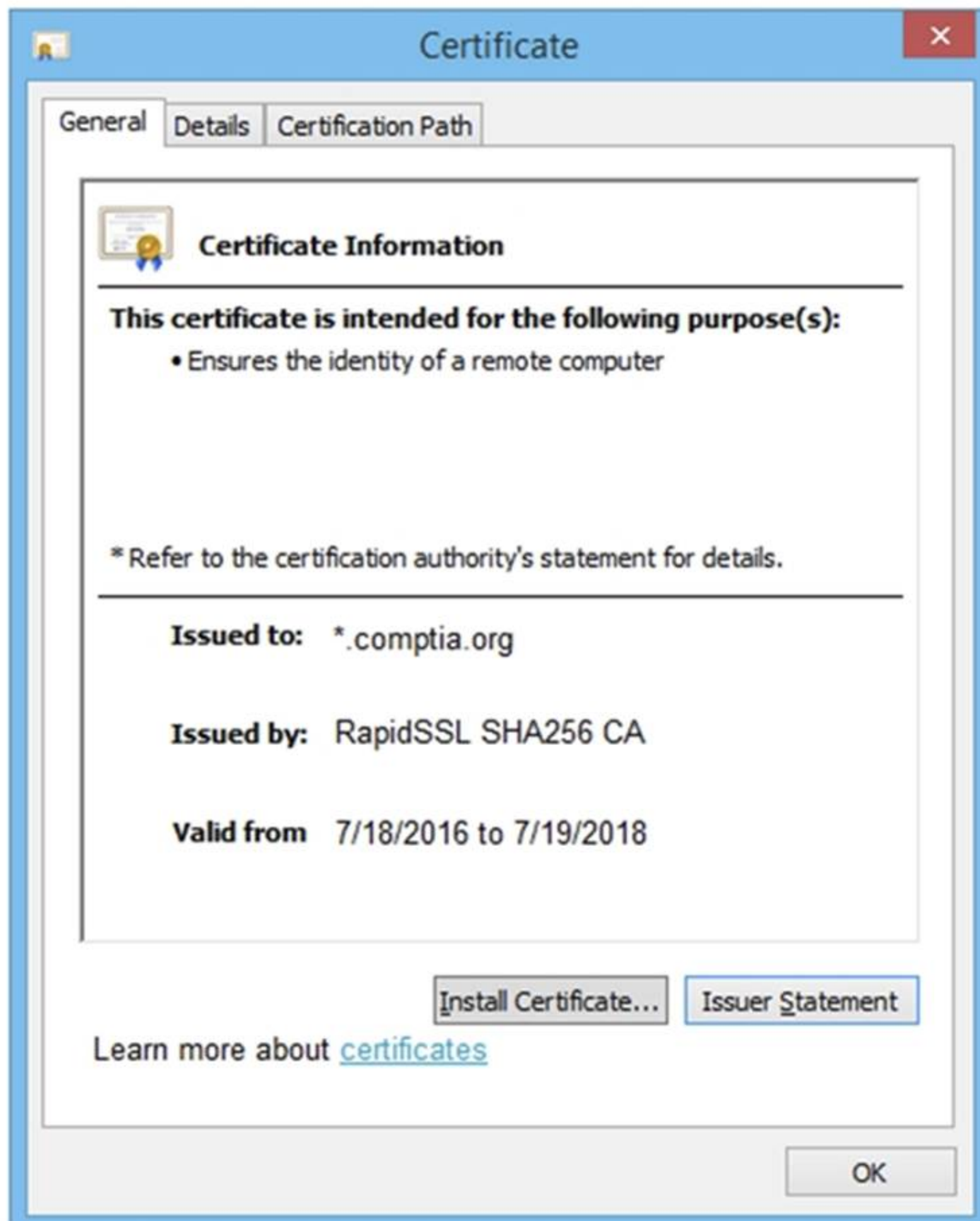
Remediate Certificate

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

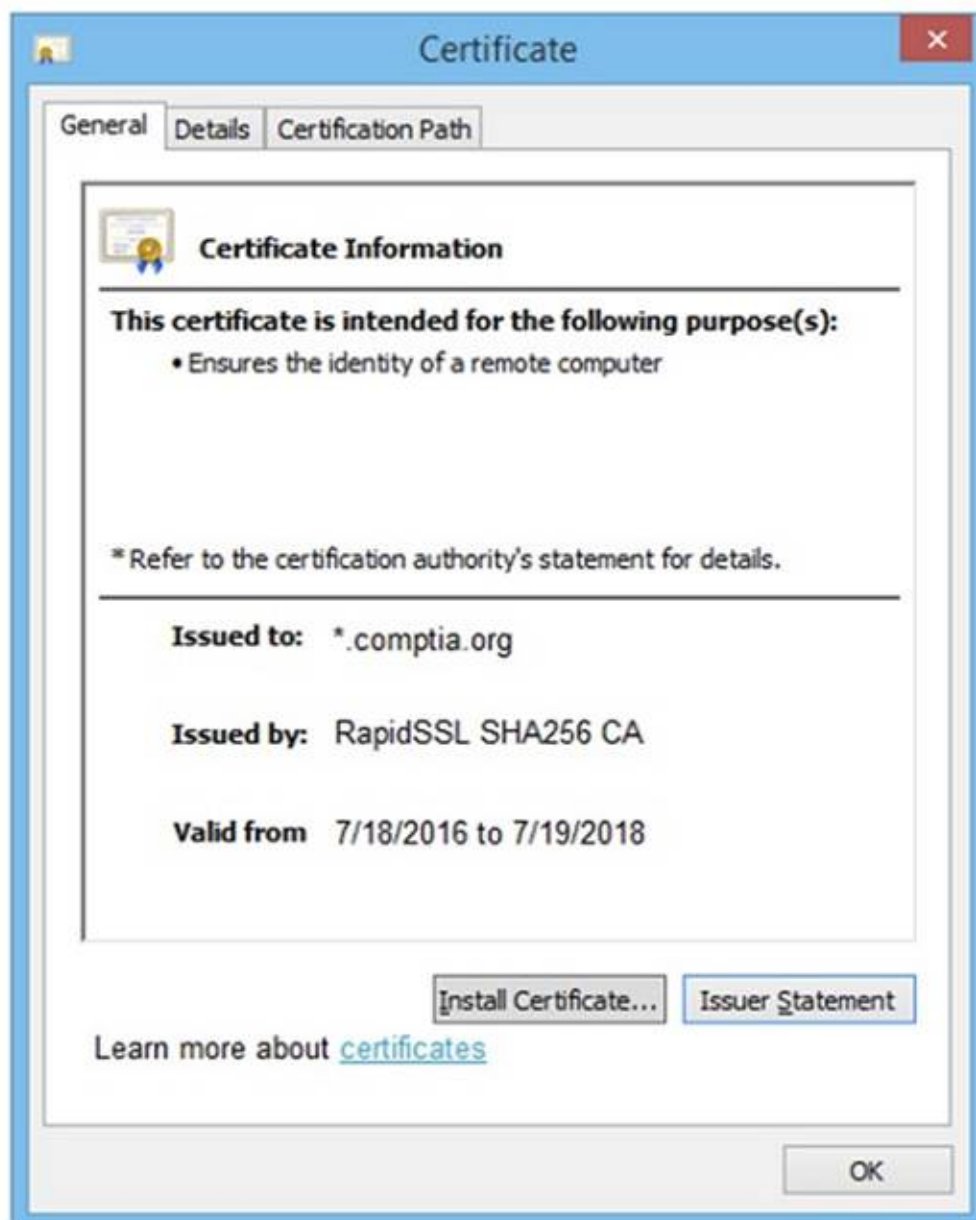
← → ↻ <https://comptia.org/login.aspx#remediatesource>

```
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	h1bcdtse2ewvqwf4bdcby3v	www.com...	/	Session	41	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utmb	361044370.7.9.1508267988443	.comptia.o...	/	2017-10-1...	32	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utmc	36104370	.comptia.o...	/	Session	14	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utmt	1	.comptia.o...	/	2017-10-1...	7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utmv	36104370.[2=Account%20Type=Not%20Defined=1	.comptia.o...	/	2019-10-1...	48	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utmz	36104370.1508266963.1.1.utmcsr=google[utmccn=(organic)]utm...	.comptia.o...	/	2018-04-1...	99	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
_sp_id.0767	4a84866c6ffff51c.1508266964.1.1508258019.1508266964.81ff34f7...	.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

?

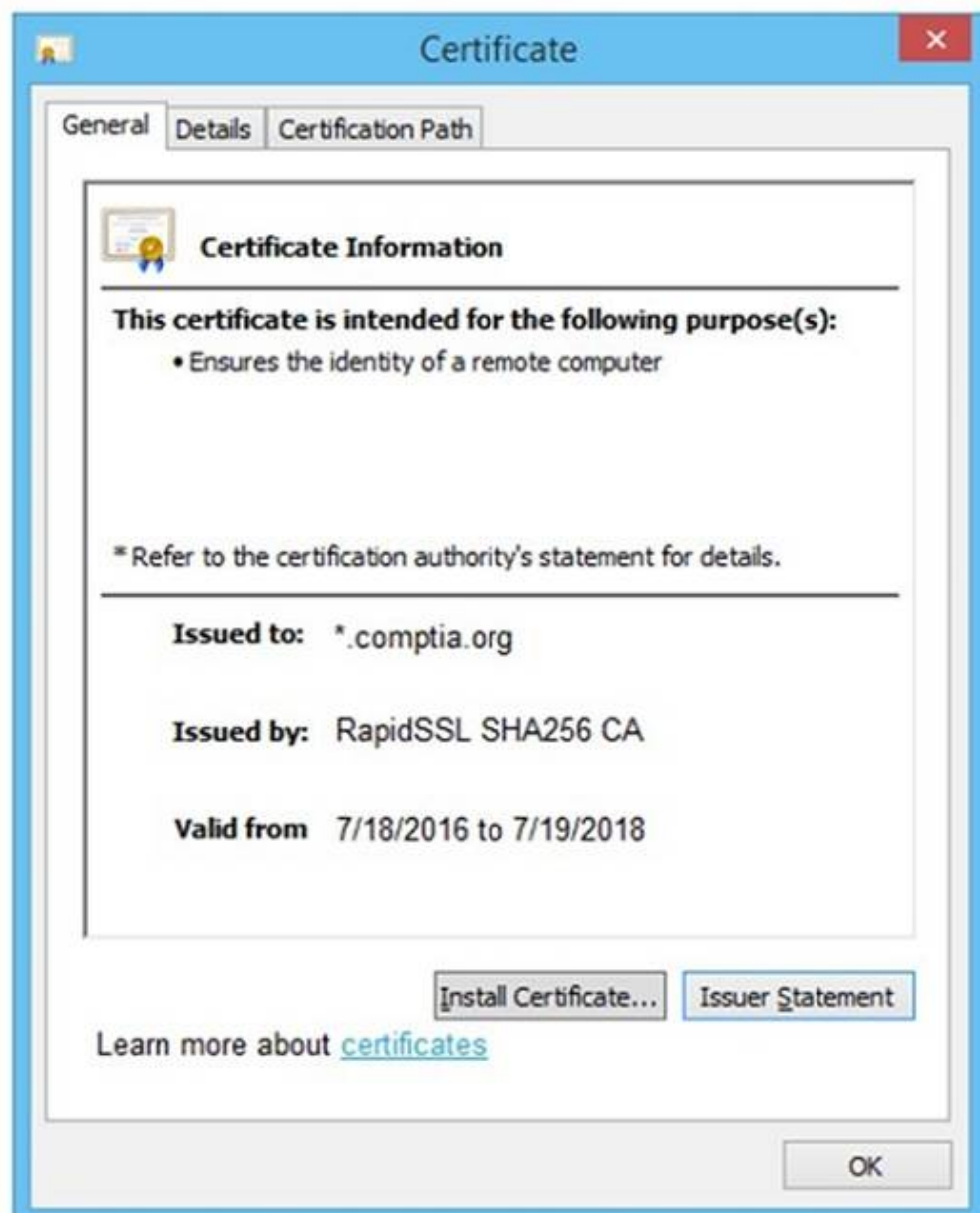
Step 4

?

- 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 6

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 7

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 8

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 9

A penetration tester writes the following script to enumerate a 1724 network:

```
1 #!/bin/bash
```

```
2 for i in {1..254}; do
```

```
3 ping -c1 192.168.1.$i 4 done
```

The tester executes the script, but it fails with the following error:

```
-bash: syntax error near unexpected token `ping'
```

Which of the following should the tester do to fix the error?

- A. Add do after line 2.
- B. Replace {1..254} with \$(seq 1 254).
- C. Replace bash with tsh.
- D. Replace \$i with \${i}.

Answer: A

Explanation:

The error in the script is due to a missing do keyword in the for loop. Here's the corrected script and

? Original Script:

```
1 #!/bin/bash
```

```
2 for i in {1..254}; do
```

```
3 ping -c1 192.168.1.$i 4 done
```

? Error

Explanation

? Corrected Script: 1 #!/bin/bash

```
2 for i in {1..254}; do
```

```
3 ping -c1 192.168.1.$i 4 done
```

Adding do after line 2 corrects the syntax error and allows the script to execute properly.

=====

NEW QUESTION 10

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

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

Answer: C

Explanation:

? Installation: sudo apt-get install nmap

? Basic Network Scanning: nmap -sP 192.168.1.0/24
? Service and Version Detection: nmap -sV 192.168.1.10
? Enumerating Domain Systems:
nmap -p 445 --script=smb-enum-domains 192.168.1.10
? Advanced Scanning Options: nmap -sS 192.168.1.10
? uk.co.certification.simulator.questionpool.PList@623a95bc nmap -A 192.168.1.10
? Real-World Example:
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
=====

NEW QUESTION 10

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 15

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 19

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 20

During an engagement, a penetration tester wants to enumerate users from Linux systems by using finger and rwho commands. However, the tester realizes these commands alone will not achieve the desired result. Which of the following is the best tool to use for this task?

- A. Nikto
- B. Burp Suite
- C. smbclient
- D. theHarvester

Answer: C

Explanation:

The smbclient tool is used to access SMB/CIFS resources on a network. It allows penetration testers to connect to shared resources and enumerate users on a network, particularly in Windows environments. While finger and rwho are more common on Unix/Linux systems, smbclient provides better functionality for enumerating users across a network.

? Understanding smbclient:

? User Enumeration:

Step-by-Step Explanationsmbclient -L //target_ip -U username

? uk.co.certification.simulator.questionpool.PList@10ddf175 smbclient -L //192.168.50.2 -U anonymous

? Advantages:

? References from Pentesting Literature: References:

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups
=====

NEW QUESTION 22

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 25

During a penetration test, a junior tester uses Hunter.io for an assessment and plans to review the information that will be collected. Which of the following describes the information the junior tester will receive from the Hunter.io tool?

- A. A collection of email addresses for the target domain that is available on multiple sources on the internet
- B. DNS records for the target domain and subdomains that could be used to increase the external attack surface
- C. Data breach information about the organization that could be used for additional enumeration
- D. Information from the target's main web page that collects usernames, metadata, and possible data exposures

Answer: A

Explanation:

Hunter.io is a tool used for finding professional email addresses associated with a domain. Here??s what it provides:

? Functionality of Hunter.io:

? Comparison with Other Options:

Hunter.io is specifically designed to collect and validate email addresses for a given domain, making it the correct answer.

=====

NEW QUESTION 29

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

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

Answer: A

Explanation:

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

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

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

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

References from Pentest:

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

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

=====

NEW QUESTION 30

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 35

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 36

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

- A. Cryptographic flaws
- B. Protocol scanning
- C. Cached pages

D. Job boards

Answer: D

Explanation:

? Reconnaissance:

? Job Boards:

? Examples of Job Boards:

Pentest References:

? OSINT (Open Source Intelligence): Using publicly available sources to gather information about a target.

? Job boards are a key source of OSINT, providing indirect access to the internal technologies of a company.

? This information can be used to tailor subsequent phases of the penetration test, such as vulnerability scanning and exploitation, to the specific technologies identified.

By examining job boards, a penetration tester can gain insights into the hardware and software environments of the target, making this a valuable reconnaissance tool.

=====

NEW QUESTION 38

A penetration tester is performing an authorized physical assessment. During the test, the tester observes an access control vestibule and on-site security guards near the entry door in the lobby. Which of the following is the best attack plan for the tester to use in order to gain access to the facility?

A. Clone badge information in public areas of the facility to gain access to restricted areas.

B. Tailgate into the facility during a very busy time to gain initial access.

C. Pick the lock on the rear entrance to gain access to the facility and try to gain access.

D. Drop USB devices with malware outside of the facility in order to gain access to internal machines.

Answer: B

Explanation:

In an authorized physical assessment, the goal is to test physical security controls. Tailgating is a common and effective technique in such scenarios. Here??s why option B is correct:

? Tailgating: This involves following an authorized person into a secure area without

proper credentials. During busy times, it??s easier to blend in and gain access without being noticed. It tests the effectiveness of physical access controls and security personnel.

? Cloning Badge Information: This can be effective but requires proximity to

employees and specialized equipment, making it more complex and time- consuming.

? Picking Locks: This is a more invasive technique that carries higher risk and is less stealthy compared to tailgating.

? Dropping USB Devices: This tests employee awareness and response to malicious devices but does not directly test physical access controls.

References from Pentest:

? Writeup HTB: Demonstrates the effectiveness of social engineering and tailgating techniques in bypassing physical security measures.

? Forge HTB: Highlights the use of non-invasive methods like tailgating to test physical security without causing damage or raising alarms.

Conclusion:

Option B, tailgating into the facility during a busy time, is the best attack plan to gain access to the facility in an authorized physical assessment.

=====

NEW QUESTION 42

A penetration tester is testing a power plant's network and needs to avoid disruption to the grid. Which of the following methods is most appropriate to identify vulnerabilities in the network?

A. Configure a network scanner engine and execute the scan.

B. Execute a testing framework to validate vulnerabilities on the devices.

C. Configure a port mirror and review the network traffic.

D. Run a network mapper tool to get an understanding of the devices.

Answer: C

Explanation:

When testing a power plant's network and needing to avoid disruption to the grid, configuring a port mirror and reviewing the network traffic is the most appropriate method to identify vulnerabilities without causing disruptions.

? Port Mirroring:

? Avoiding Disruption:

? Other Options:

Pentest References:

? Passive Monitoring: Passive techniques such as port mirroring are essential in environments where maintaining operational integrity is critical.

? Critical Infrastructure Security: Understanding the need for non-disruptive methods in critical infrastructure penetration testing to ensure continuous operations.

By configuring a port mirror and reviewing network traffic, the penetration tester can identify vulnerabilities in the power plant's network without risking disruption to the grid.

=====

NEW QUESTION 45

During an engagement, a penetration tester needs to break the key for the Wi-Fi network that uses WPA2 encryption. Which of the following attacks would accomplish this objective?

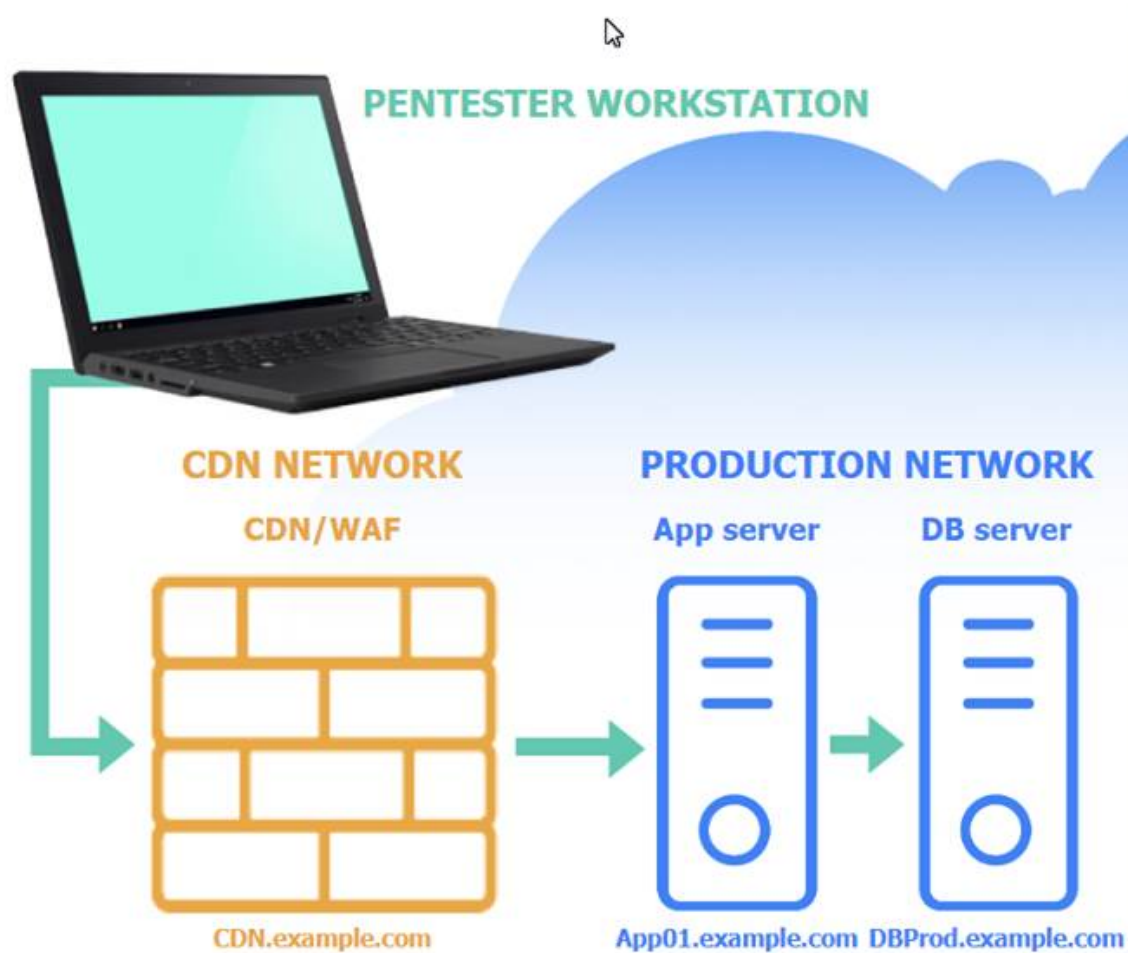
A. ChopChop

B. Replay

C. Initialization vector

D. KRACK

Answer: D



Vulnerability

Remediation

Select the two **best** remediation options:

- ☐ Restrict direct communications to App01.example.com to only approved components.
- ☐ Require an additional authentication header value between CDN.example.com and App01.example.com.
- ☐ Throttle the number of concurrent connections to CDN.example.com.
- ☐ Change the default port used for the MySQL Database Connection to DBProd.example.com.
- ☐ Change the default ports used for the web server on App01.example.com.
- ☐ Configure a host-based intrusion detection system on App01.example.com.

CDN/WAF



```
Nmap scan report for 205.3.45.68
Host is up (0.016s latency).
PORT      STATE      SERVICE      VERSION
80/tcp    open      http         nginx
443/tcp    open      ssl/https    nginx
3306/tcp   filtered   mysql
```


App server



Nmap scan report for 103.2.45.51

Host is up (0.341s latency).

PORT	STATE	SERVICE	VERSION
80/tcp	open	http	nginx 1.18.0
443/tcp	open	ssl/http	nginx 1.18.0
3306/tcp	filtered	mysql	

DB server



Nmap scan report for 103.1.45.50

Host is up (0.046s latency).

PORT	STATE	SERVICE	VERSION
80/tcp	filtered	http	
443/tcp	filtered	ssl/http	
3306/tcp	filtered	mysql	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Vulnerability

Remediation

Based on the output text, select the most likely vulnerability:

- ☐ Bypass the WAF to communicate directly with App01.example.com.
- ☐ Execute a SQL injection attack against DBProd.example.com.
- ☒ Perform a SSRF attack against App01.example.com from CDN.example.com.
- ☐ Exploit a privilege escalation attack on App01.example.com.

Vulnerability

Remediation

Select the two best remediation options:

- ☒ Restrict direct communications to App01.example.com to only approved components.
- ☒ Require an additional authentication header value between CDN.example.com and App01.example.com.
- ☐ Throttle the number of concurrent connections to CDN.example.com.
- ☐ Change the default port used for the MySQL Database Connection to DBProd.example.com.
- ☐ Change the default ports used for the web server on App01.example.com.
- ☐ Configure a host-based intrusion detection system on App01.example.com.

Most likely vulnerability: Perform a SSRF attack against App01.example.com from CDN.example.com.

The scenario suggests that the CDN network (with a WAF) can be used to perform a Server-Side Request Forgery (SSRF) attack. Since the penetration tester has the pentester workstation interacting through the CDN/WAF and the production network is behind it, the most plausible attack vector is to exploit SSRF to interact with the internal services like App01.example.com.

Two best remediation options:

? Restrict direct communications to App01.example.com to only approved components.

? Require an additional authentication header value between CDN.example.com and App01.example.com.

? Restrict direct communications to App01.example.com to only approved components: This limits the exposure of the application server by ensuring that only specified, trusted entities can communicate with it.

? Require an additional authentication header value between CDN.example.com

and App01.example.com: Adding an authentication layer between the CDN and the app server helps ensure that requests are legitimate and originate from trusted sources, mitigating SSRF and other indirect attack vectors.

Nmap Scan Observations:

? CDN/WAF shows open ports for HTTP and HTTPS but filtered for MySQL, indicating it acts as a filtering layer.

? App Server has open ports for HTTP, HTTPS, and filtered for MySQL.

? DB Server has all ports filtered, typical for a database server that should not be directly accessible.

These findings align with the SSRF vulnerability and the appropriate remediation steps to enhance the security of internal communications.

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 56

Which of the following elements in a lock should be aligned to a specific level to allow the key cylinder to turn?

- A. Latches
- B. Pins
- C. Shackle
- D. Plug

Answer: B

Explanation:

In a pin tumbler lock, the key interacts with a series of pins within the lock cylinder. Here??s a detailed breakdown:

? Components of a Pin Tumbler Lock:

? Operation:

? Why Pins Are the Correct Answer:

? Illustration in Lock Picking:

=====

NEW QUESTION 57

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 58

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 61

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 63

A penetration tester is attempting to discover vulnerabilities in a company's web application. Which of the following tools would most likely assist with testing the security of the web application?

- A. OpenVAS
- B. Nessus
- C. sqlmap
- D. Nikto

Answer: D

Explanation:

When testing the security of a web application, specific tools are designed to uncover vulnerabilities and issues. Here??s an overview of the tools mentioned and why Nikto is the most suitable for this task:

? Nikto:

? Comparison with Other Tools:

=====

NEW QUESTION 65

Which of the following OT protocols sends information in cleartext?

- A. TTEthernet
- B. DNP3
- C. Modbus
- D. PROFINET

Answer: C

Explanation:

Operational Technology (OT) protocols are used in industrial control systems (ICS) to manage and automate physical processes. Here??s an analysis of each protocol regarding whether it sends information in cleartext:

? TTEthernet (Option A):

? DNP3 (Option B):

? Modbus (Answer: C):

? PROFINET (Option D):

Conclusion: Modbus is the protocol that most commonly sends information in cleartext, making it vulnerable to eavesdropping and interception.

NEW QUESTION 69

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

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

Answer: A

Explanation:

? Debugging Mode:

? Common Causes:

? Best Practices:

? References from Pentesting Literature: References:

? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
=====

NEW QUESTION 70

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 73

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 76

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 78

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

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

Answer: D

Explanation:

Evaluating a container orchestration cluster, such as Kubernetes, requires specialized tools designed to assess the security and configuration of container environments. Here's an analysis of each tool and why Kube-hunter is the best choice:

? Trivy (Option A):

? Nessus (Option B):

? Gripe (Option C):

? Kube-hunter (Answer: D):

Conclusion: Kube-hunter is the most appropriate tool for evaluating a container orchestration cluster, such as Kubernetes, due to its specialized focus on identifying security vulnerabilities and misconfigurations specific to such environments.

NEW QUESTION 83

A penetration tester is conducting reconnaissance for an upcoming assessment of a large corporate client. The client authorized spear phishing in the rules of engagement. Which of the following should the tester do first when developing the phishing campaign?

- A. Shoulder surfing
- B. Recon-ng
- C. Social media
- D. Password dumps

Answer: C

Explanation:

When developing a phishing campaign, the tester should first use social media to gather information about the targets.

? Social Media:

? Process:

? Other Options:

Pentest References:

? Spear Phishing: A targeted phishing attack aimed at specific individuals, using personal information to increase the credibility of the email.

? OSINT (Open Source Intelligence): Leveraging publicly available information to gather intelligence on targets, including through social media.

By starting with social media, the penetration tester can collect detailed and personalized information about the targets, which is essential for creating an effective spear phishing campaign.

=====

NEW QUESTION 84

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 87

A tester completed a report for a new client. Prior to sharing the report with the client, which of the following should the tester request to complete a review?

- A. A generative AI assistant
- B. The customer's designated contact
- C. A cybersecurity industry peer
- D. A team member

Answer: B

Explanation:

Before sharing a report with a client, it is crucial to have it reviewed to ensure accuracy, clarity, and completeness. The best choice for this review is a team member. Here's why:

? Internal Peer Review:

? Alternative Review Options:

In summary, an internal team member is the most suitable choice for a thorough and contextually accurate review before sharing the report with the client.

=====

NEW QUESTION 90

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:

? Understanding Tailgating:
? Methods to Prevent Tailgating:
? Examples in Penetration Testing:
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups

=====

NEW QUESTION 91

A penetration tester is authorized to perform a DoS attack against a host on a network. Given the following input:

```
ip = IP("192.168.50.2")
tcp = TCP(sport=RandShort(), dport=80, flags="S") raw = RAW(b"X"*1024)
p = ip/tcp/raw
send(p, loop=1, verbose=0)
```

Which of the following attack types is most likely being used in the test?

- A. MDK4
- B. Smurf attack
- C. FragAttack
- D. SYN flood

Answer: D

Explanation:

A SYN flood attack exploits the TCP handshake by sending a succession of SYN requests to a target's system. Each request initializes a connection that the target system must acknowledge, thus consuming resources.

? Understanding the Script:
? Purpose of SYN Flood:
? Detection and Mitigation:
? References from Pentesting Literature: Step-by-Step ExplanationReferences:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups

NEW QUESTION 96

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 101

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 106

.....

Relate Links

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

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

Contact us

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

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