



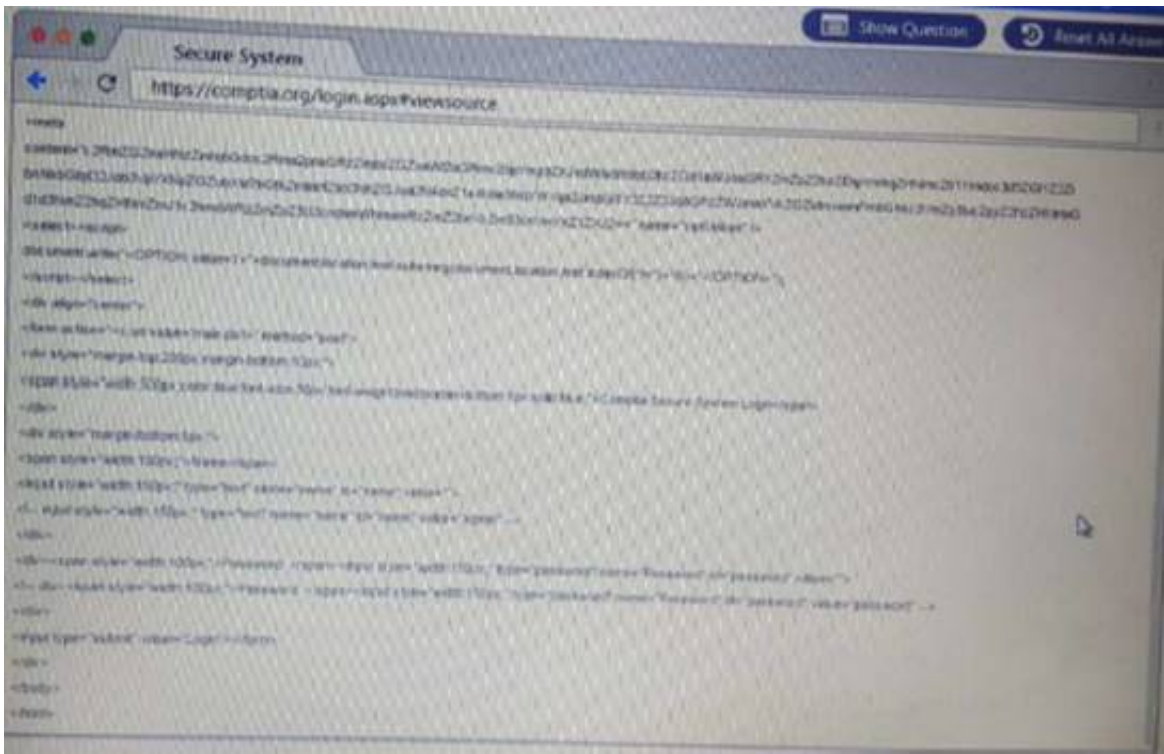
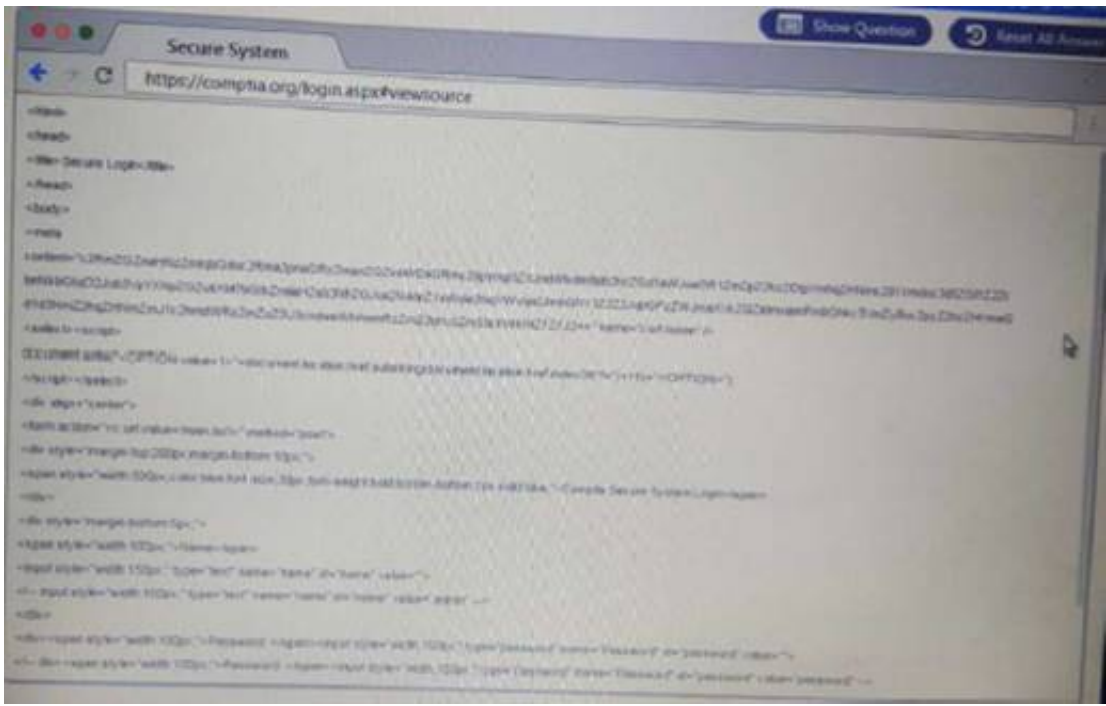
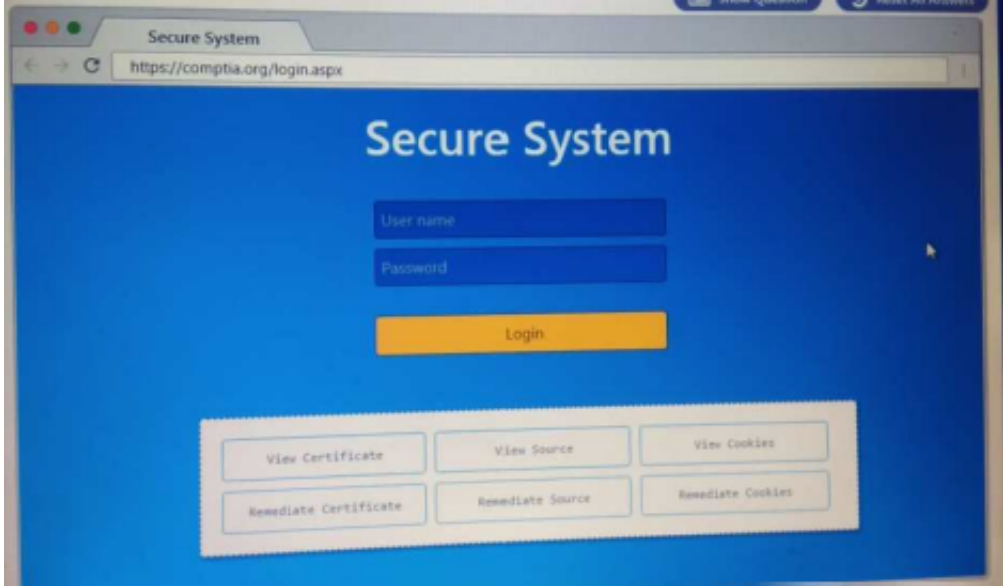
CompTIA

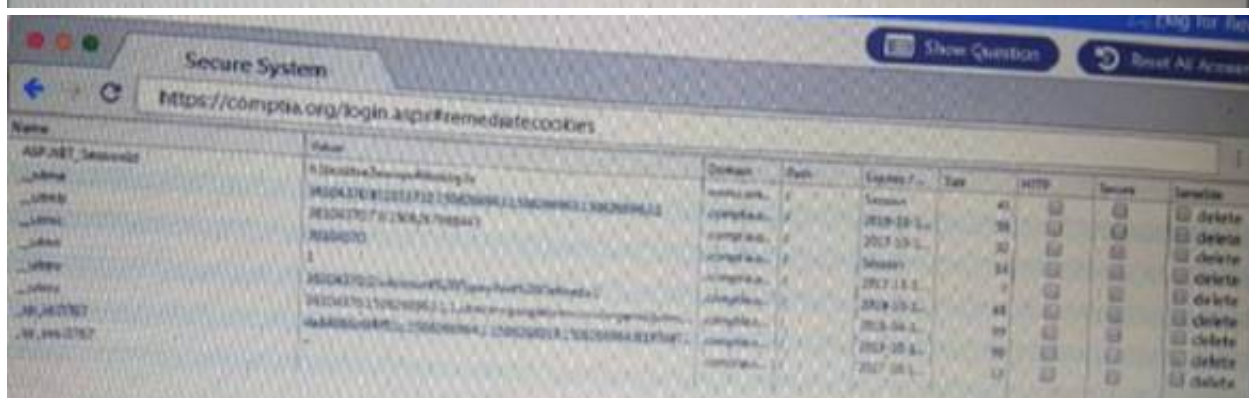
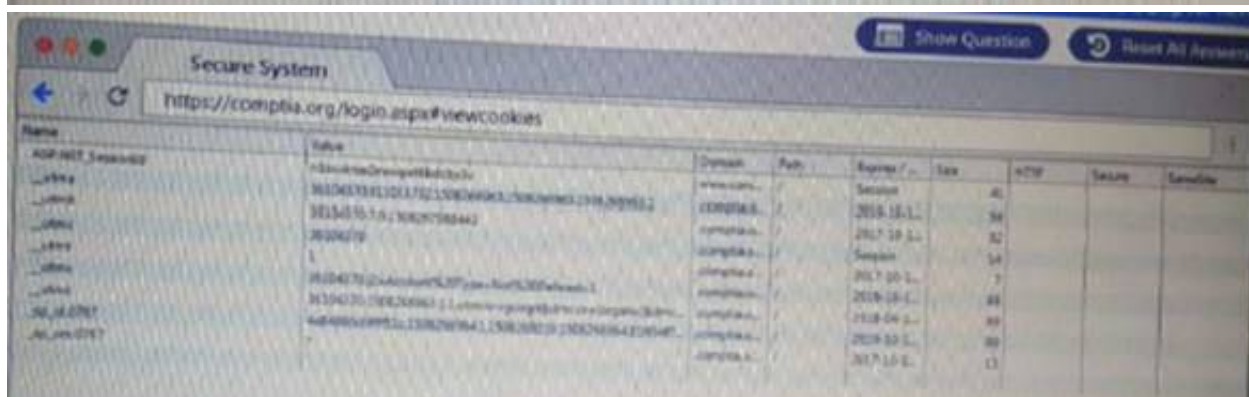
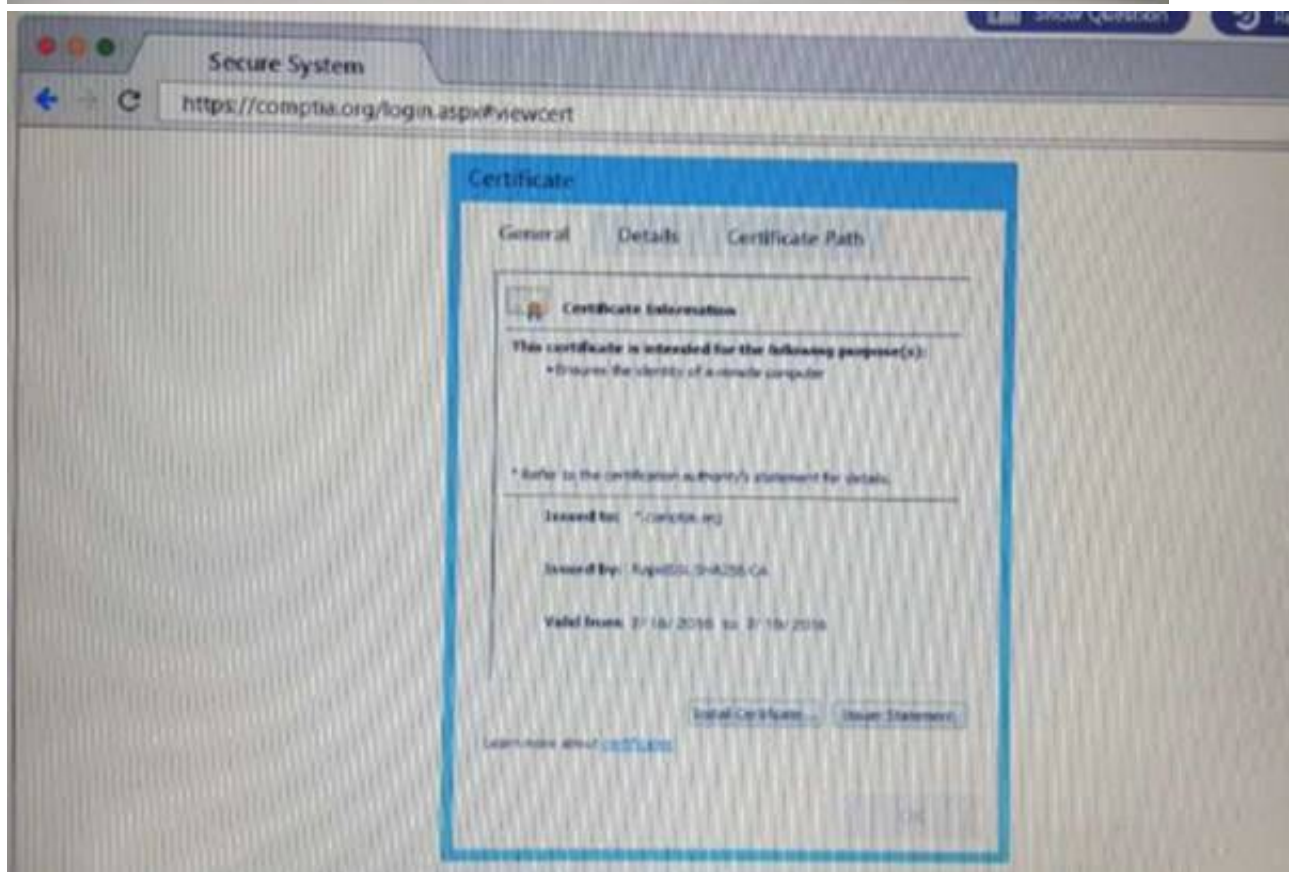
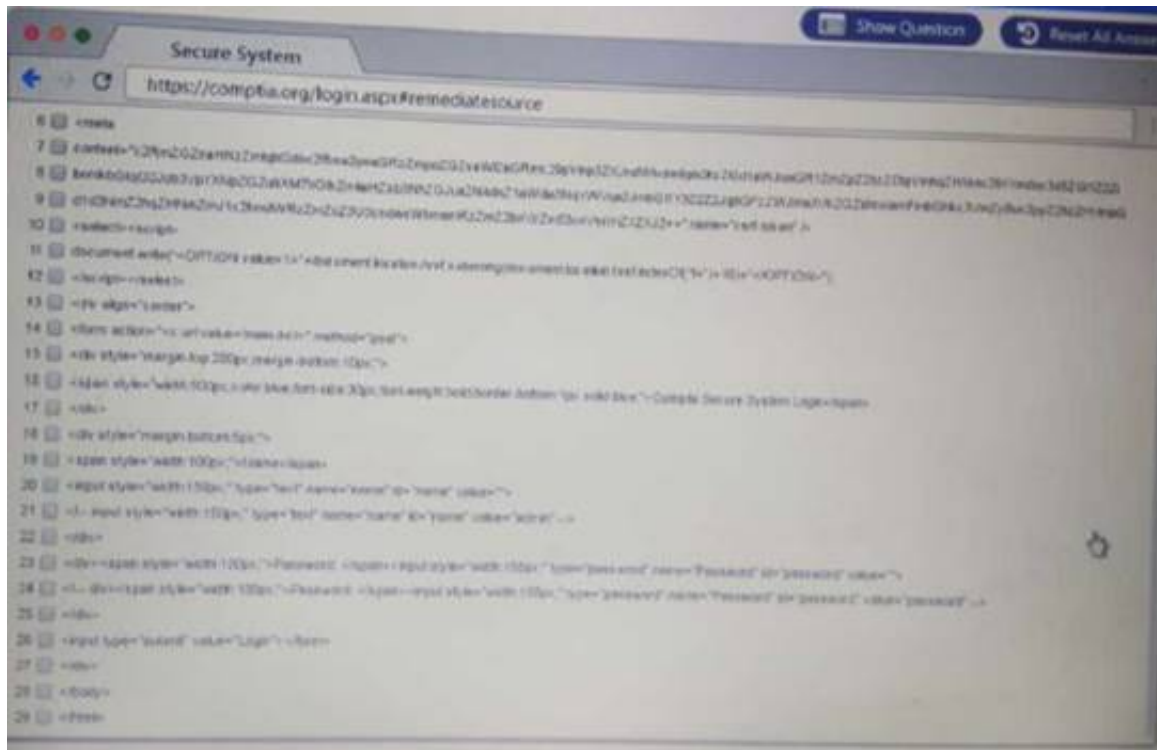
Exam Questions PT0-001

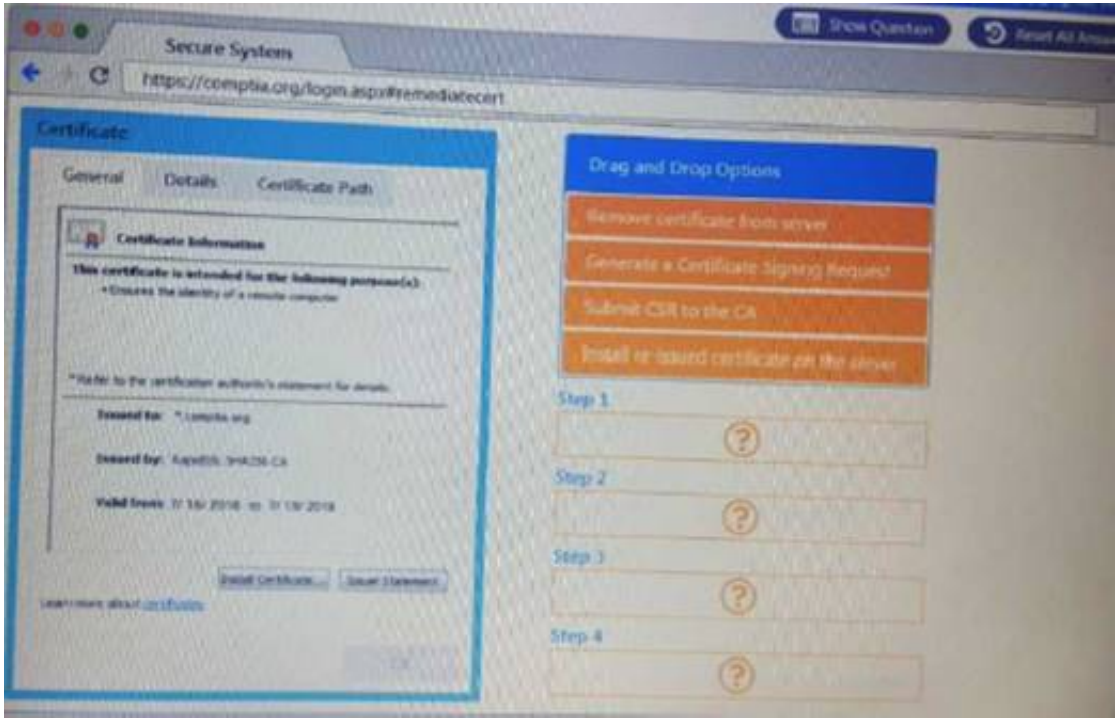
CompTIA PenTest+ Certification Exam

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.







- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



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]	<div></div> <div>iita</div> <div>imdA</div>
s[4:12:2]	<div></div> <div>inis</div> <div>nist</div>
s[3::-1]	<div></div> <div>nsrt</div> <div>rota</div>
s[-7:-2]	<div></div> <div>snmA</div> <div>trat</div>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Nsrt
Snma
Trat
Imda

NEW QUESTION 3

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



- A. Mastered
- B. Not Mastered

Answer: A

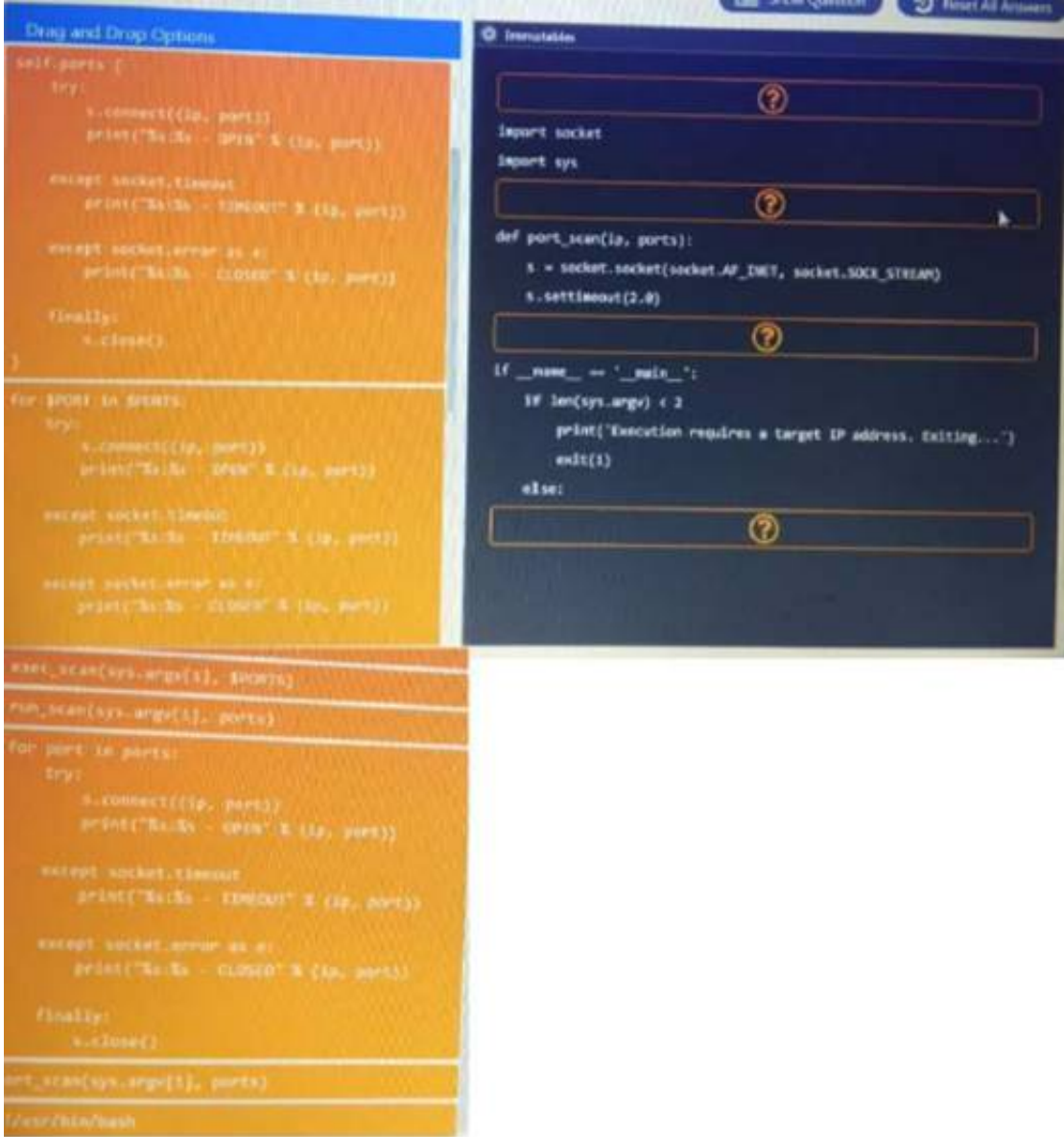
Explanation:

Zverlory
Zverl0ry
zv3rlory
Zv3rl0ry

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.



- A. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 5

A constant wants to scan all the TCP Pots on an identified device. Which of the following Nmap switches will complete this task?

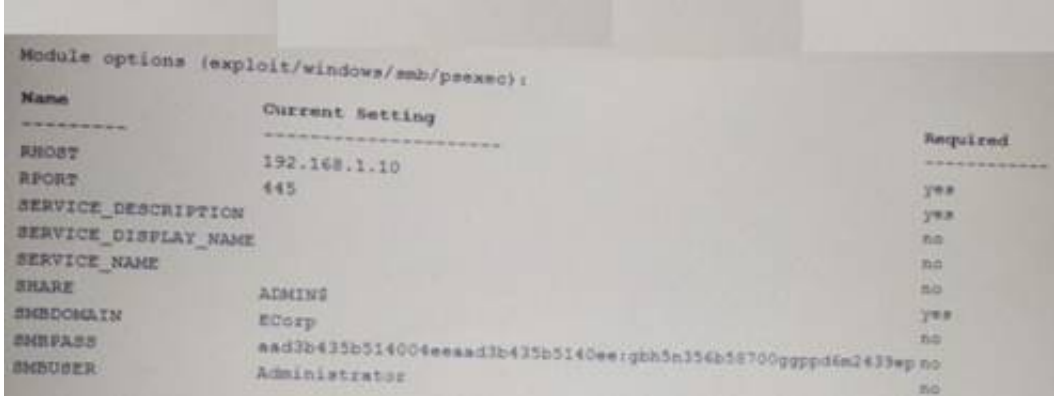
- A. -p-

- B. -p ALX,
- C. -p 1-65534
- D. -port 1-65534

Answer: A

NEW QUESTION 6

A security consultant is trying to attack a device with a previous identified user account.



Name	Current Setting	Required
RHOST	192.168.1.10	
RPORT	445	yes
SERVICE_DESCRIPTION		yes
SERVICE_DISPLAY_NAME		no
SERVICE_NAME		no
SHARE	ADMIN\$	no
SMBDOMAIN	ECorp	yes
SMBPASS	aad3b435b51404eeaad3b435b5140e:gbh5n356b56700gpppd6m2433ep	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

Answer: D

NEW QUESTION 7

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 8

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)

- B)

- C)

- D)


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

Answer: D

NEW QUESTION 9

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. NetNTLMv1
- C. NTLM
- D. SHA-1

Answer: C

NEW QUESTION 10

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

Answer: BDG

NEW QUESTION 10

A penetration tester has successfully exploited an application vulnerability and wants to remove the command history from the Linux session. Which of the following will accomplish this successfully?

- A. history --remove
- B. cat history | clear
- C. rm -f ./history
- D. history -c

Answer: D

NEW QUESTION 11

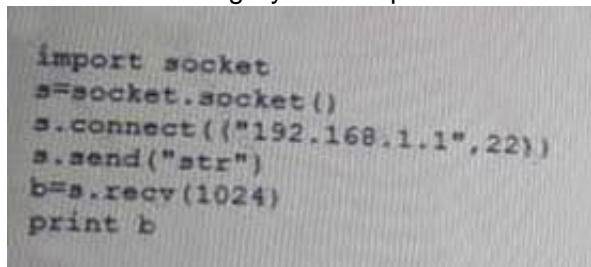
A recently concluded penetration test revealed that a legacy web application is vulnerable to SQL injection Research indicates that completely remediating the vulnerability would require an architectural change, and the stakeholders are not in a position to risk the availability of the application Under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

- A. Identify 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

Answer: DE

NEW QUESTION 15

Given the following Python script:



```
import socket
s=socket.socket()
s.connect(("192.168.1.1",22))
s.send("str")
b=s.recv(1024)
print b
```

Which of the following actions will it perform?

- A. ARP spoofing
- B. Port scanner
- C. Reverse shell
- D. Banner grabbing

Answer: A

NEW QUESTION 17

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

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

Answer: A

NEW QUESTION 19

Given the following script:

```
import pyHook, pythoncom, logging, sys
f="f.txt"
def OnKeyboardEvent(event):
    logging.basicConfig(filename=f, level=logging.DEBUG, format='%(message)s')
    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 20

Which of the following types of physical security attacks does a mantrap mitigate-?

- A. Lock picking
- B. Impersonation
- C. Shoulder surfing
- D. Tailgating

Answer: D

NEW QUESTION 21

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

Answer: A

NEW QUESTION 25

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 employee on-site. Which of the following would be MOST effective in accomplishing this?

- A. Badge cloning
- B. Lock picking
- C. Tailgating
- D. Piggybacking

Answer: A

NEW QUESTION 30

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

Answer: A

NEW QUESTION 35

A company planned for and secured the budget to hire a consultant to perform a web application penetration test. Upon discovered vulnerabilities, the company asked the consultant to perform the following tasks:

- Code review
- Updates to firewall setting

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

Answer: C

NEW QUESTION 38

A penetration tester has been asked to conduct OS fingerprinting 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? (Select TWO).

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

Answer: EF

NEW QUESTION 40

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 wordlist.txt
- B. hashcat -m 5600 hash.txt
- C. hashcat -m 5600 -a 3 hash.txt ?a?a?a?a?a?a
- D. hashcat -m 5600 -o result.txt hash.txt wordlist.txt

Answer: A

NEW QUESTION 41

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 44

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. Master services agreement
- C. Statement of work
- D. End-user license agreement

Answer: D

NEW QUESTION 46

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 ADMIN\$
- C. SERVICES and ADMIN\$
- D. ADMIN\$ and IPCS

Answer: C

NEW QUESTION 48

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 port.

Answer: A

NEW QUESTION 52

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 -D 192.168.1.1,192.168.1.2,192.168.1.3 -sV -o - --max-rate 2 192.168.130`. Which of the following BEST describes why multiple IP addresses are specified?

- A. The network is segmented 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.

Answer: C

NEW QUESTION 53

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 54

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

PT0-001 Practice Exam Features:

- * PT0-001 Questions and Answers Updated Frequently
- * PT0-001 Practice Questions Verified by Expert Senior Certified Staff
- * PT0-001 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * PT0-001 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The PT0-001 Practice Test Here](#)