

Exam Questions PT0-001

CompTIA PenTest+ Certification Exam

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



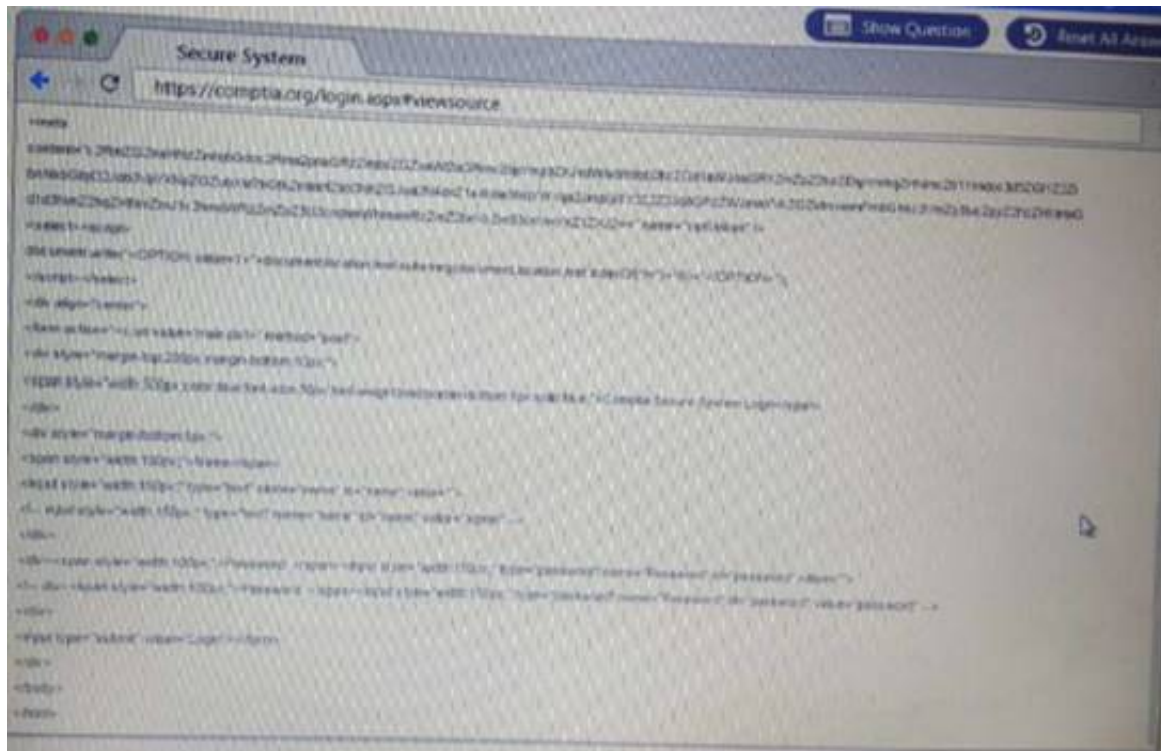
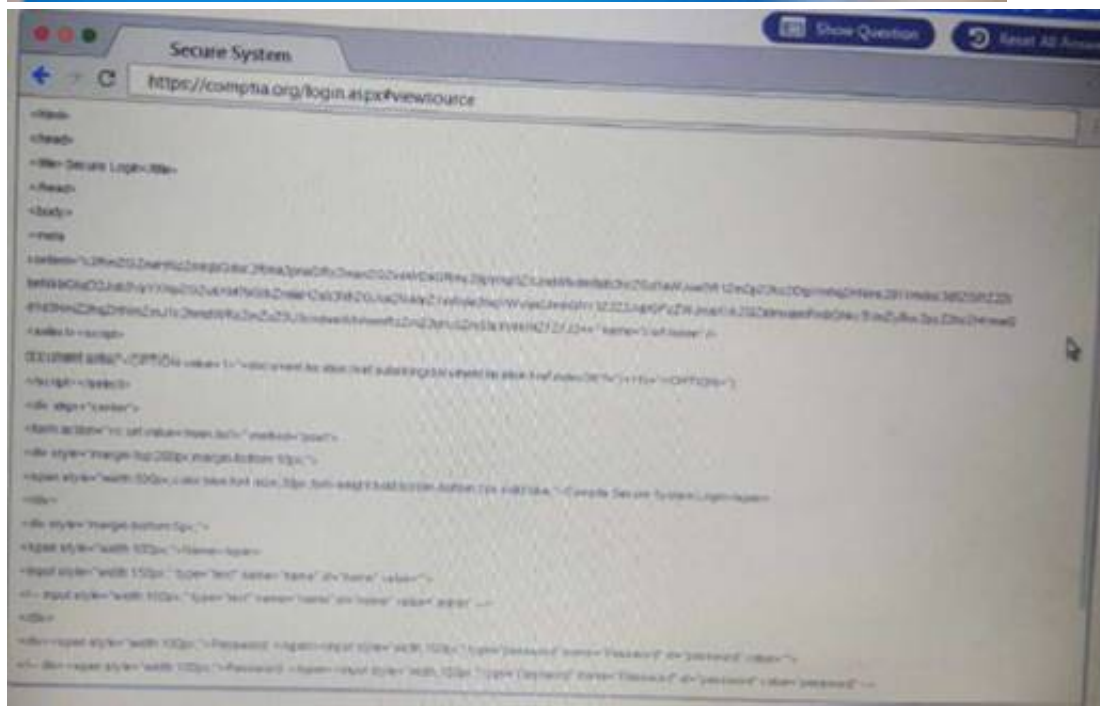
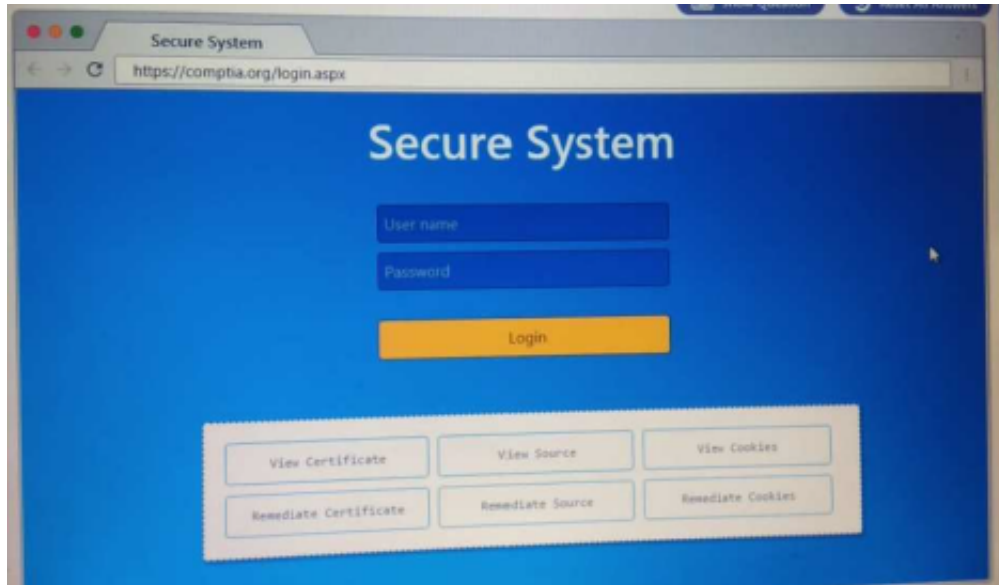
NEW QUESTION 1

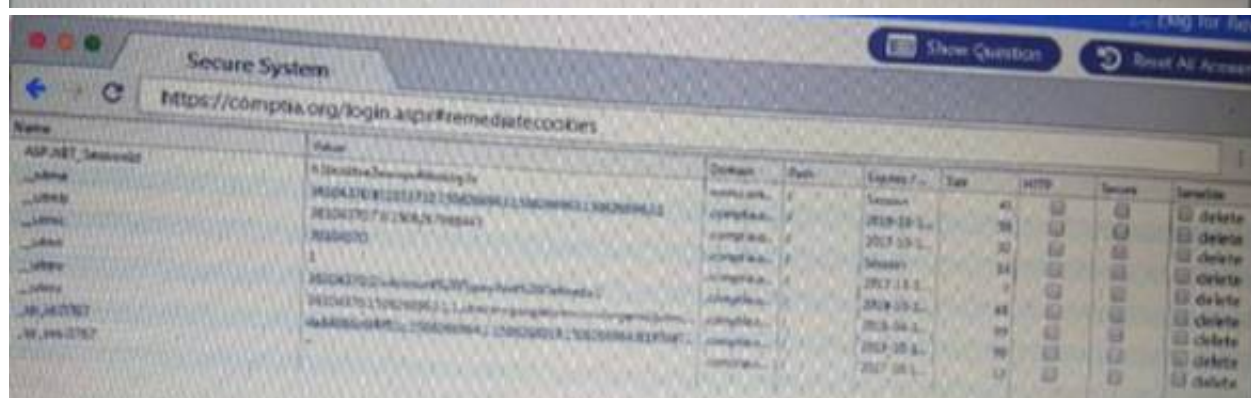
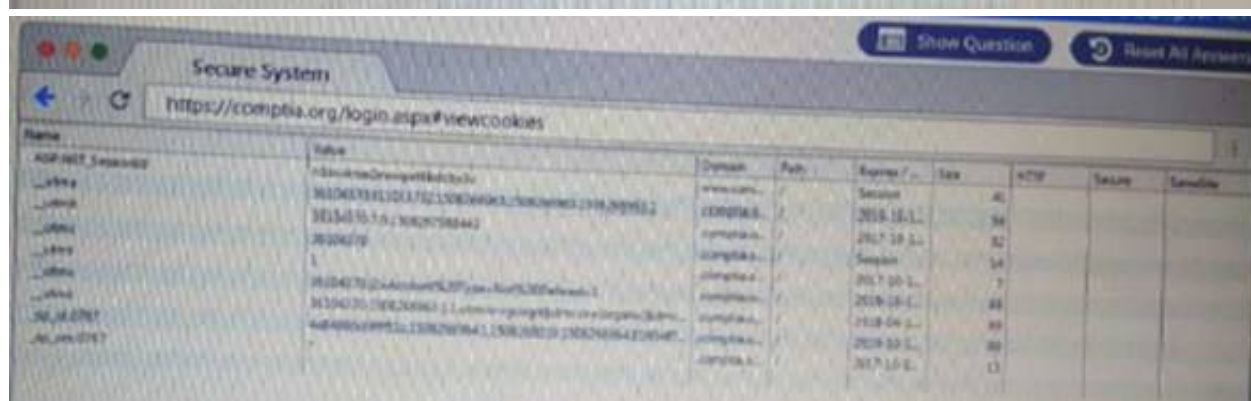
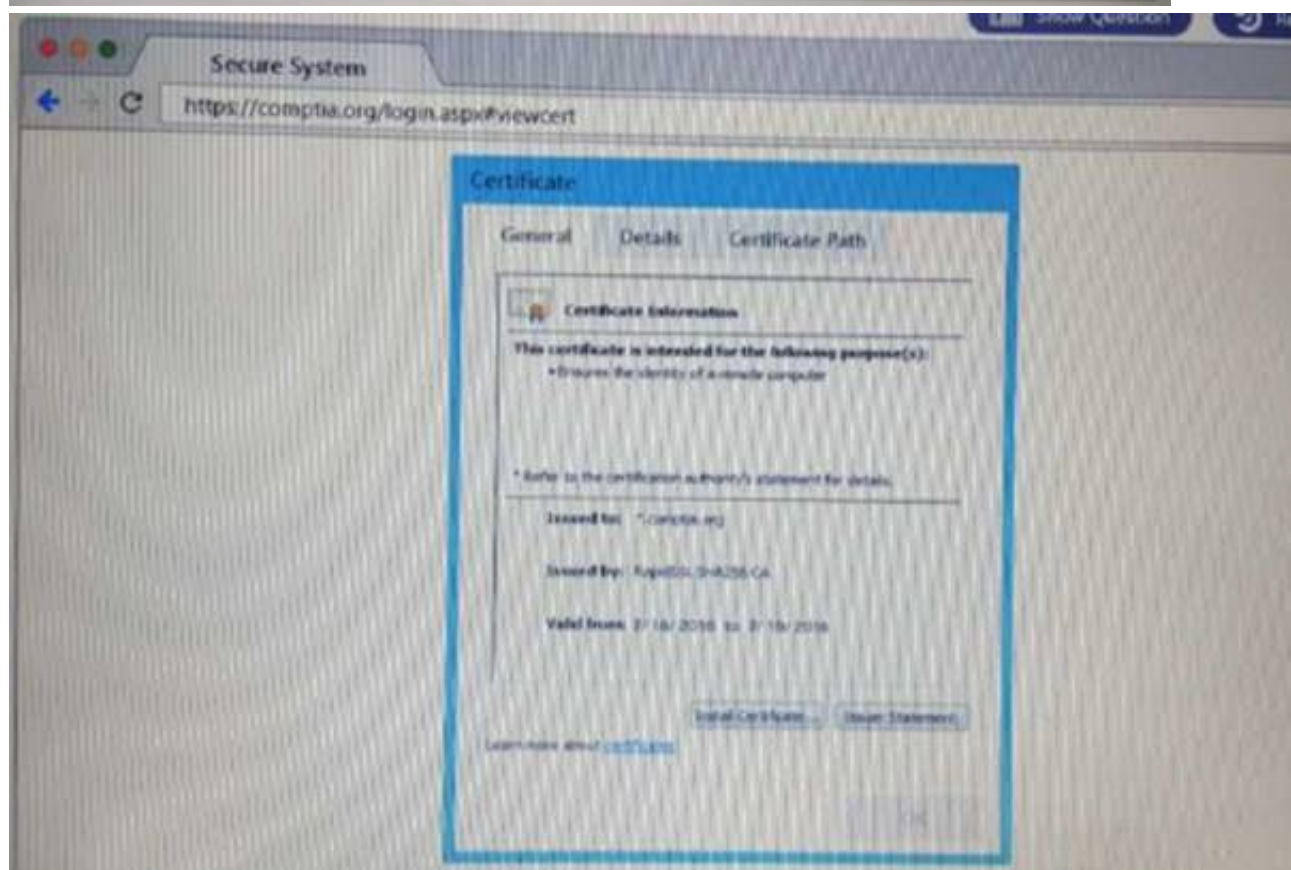
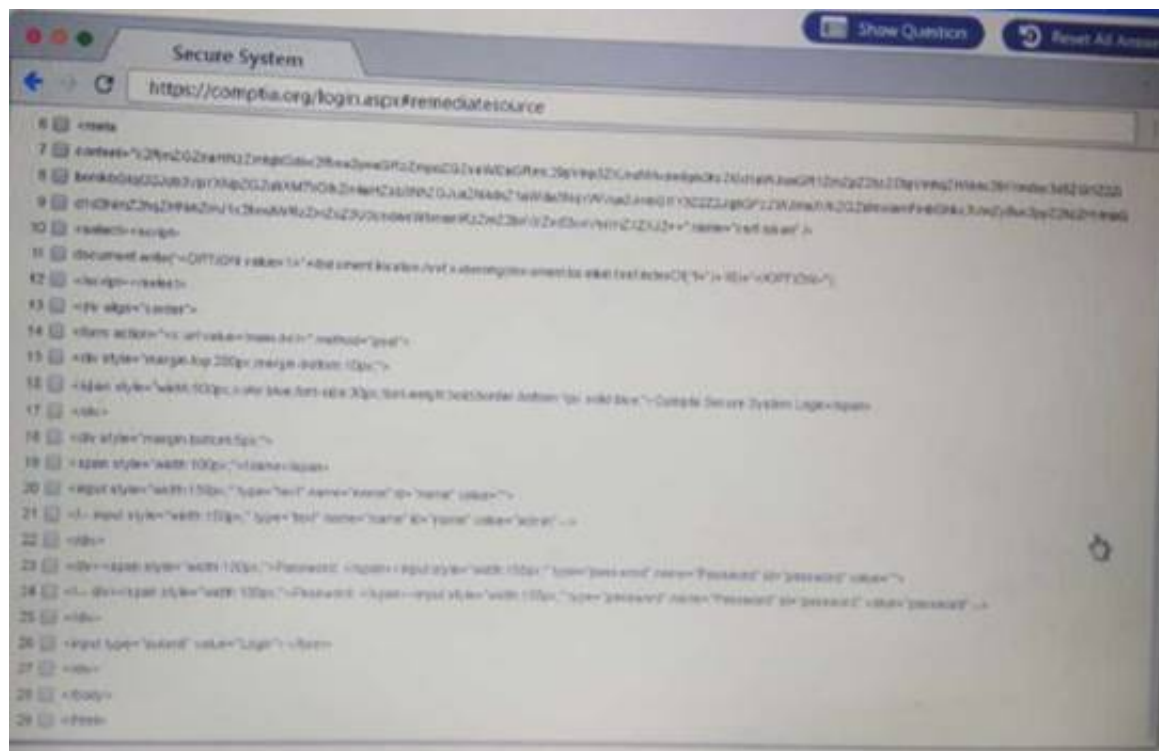
DRAG DROP

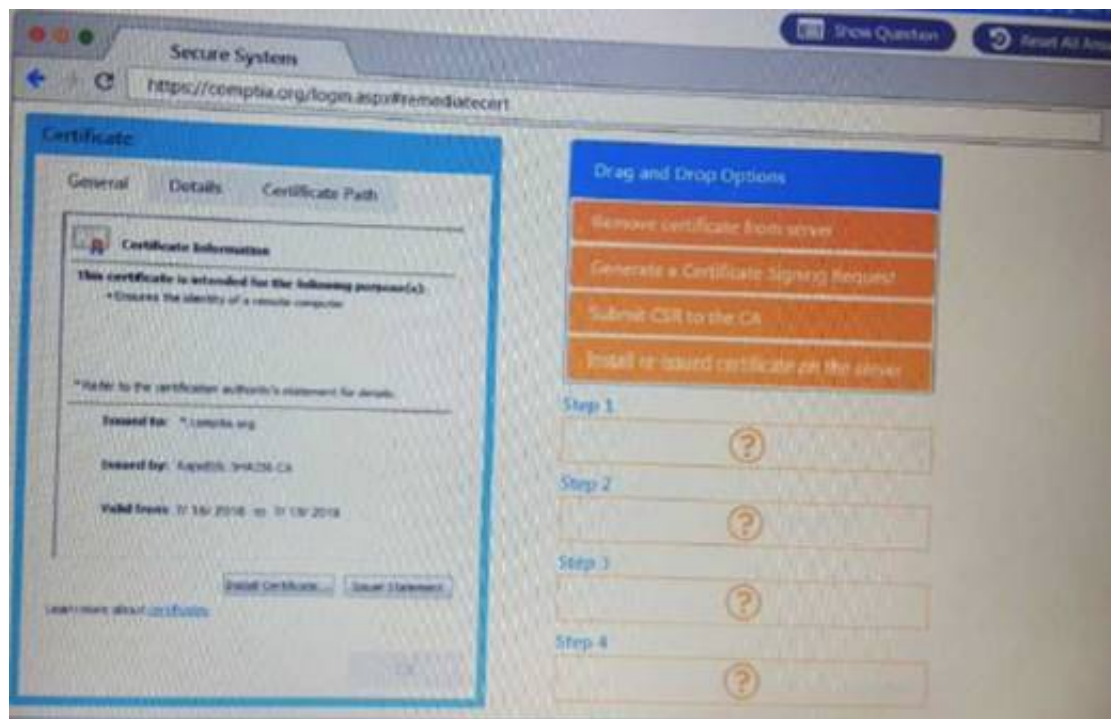
Performance based

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

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 UseLogonCredential /t REG_DWORD /d 0
```
- B)
- ```
reg add HKCU\System\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 1
```
- C)
- ```
reg add HKLM\System\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 1
```
- D)
- ```
reg add HKLM\System\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 1
```

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

Answer: D

NEW QUESTION 3

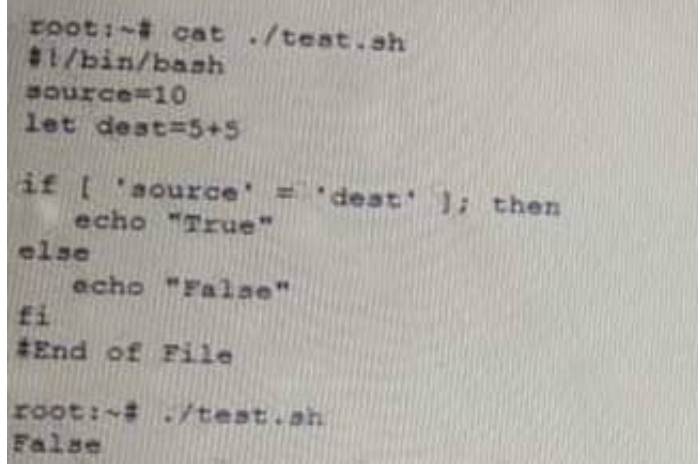
A penetration tester is required to perform OSINT on staff at a target company after completing the infrastructure aspect. Which of the following would be the BEST step for the penetration tester to take?

- 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 4

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 5

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 6

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 7

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 8

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. Hacktrivist groups

Answer: B

NEW QUESTION 9

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 10

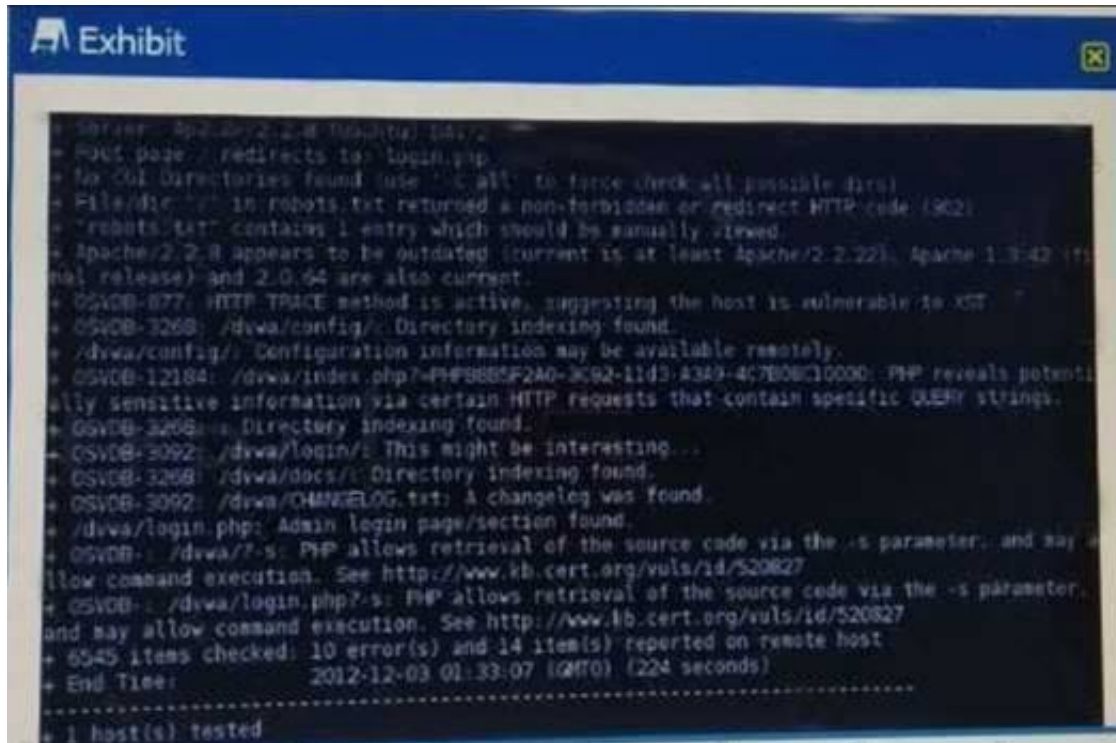
A penetration tester has been asked to conduct OS fingerprinting with Nmap using a company-provided text file that contains a list of IP addresses. Which of the following are needed to conduct this scan? (Select TWO).

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

Answer: EF

NEW QUESTION 10

Click the exhibit button.



Given the Nikto vulnerability scan output shown in the exhibit, which of the following exploitation techniques might be used to exploit 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 14

A penetration tester successfully exploits 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:31d6cfe0d16a6931b73c59d7e0c089c0:dfc312aead123
```

C)

```
Administrator:SNTLM$1122334455667788$B2B2220790F40C88BCFF347C652F67A7C4A70D3BEND70233:::ffff
```

D)

```
Administrator:SNTLMv2$NTLMv2WORKGROUP$1122334455667788$07659A55GD5E9D02996DFD95CE7EC1D5401010000000000006CF6385B74CA01B3610B02D99732CD000000000200120
```

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

Answer: D

NEW QUESTION 15

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 18

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 21

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 25

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 26

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 31

.....

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