



CompTIA

Exam Questions PT0-002

CompTIA PenTest+ Certification Exam

NEW QUESTION 1

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

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

Answer: C

NEW QUESTION 2

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

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

Answer: A

Explanation:

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

NEW QUESTION 3

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

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

Answer: D

Explanation:

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

NEW QUESTION 4

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

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

Answer: B

Explanation:

The most important information to have on a penetration testing report that is written for the developers is remediation. Remediation is the process of fixing or mitigating the vulnerabilities or issues that were discovered during the penetration testing. Remediation should include specific recommendations, best practices, and resources to help the developers improve the security of their applications⁴.

NEW QUESTION 5

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

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

Answer: B

Explanation:

Deauth will make the client connect again

NEW QUESTION 6

A penetration tester has gained access to a network device that has a previously unknown IP range on an interface. Further research determines this is an always-on VPN tunnel to a third-party supplier.

Which of the following is the BEST action for the penetration tester to take?

- A. Utilize the tunnel as a means of pivoting to other internal devices.
- B. Disregard the IP range, as it is out of scope.
- C. Stop the assessment and inform the emergency contact.
- D. Scan the IP range for additional systems to exploit.

Answer: D

NEW QUESTION 7

A penetration tester who is working remotely is conducting a penetration test using a wireless connection. Which of the following is the BEST way to provide confidentiality for the client while using this connection?

- A. Configure wireless access to use a AAA server.
- B. Use random MAC addresses on the penetration testing distribution.
- C. Install a host-based firewall on the penetration testing distribution.
- D. Connect to the penetration testing company's VPS using a VPN.

Answer: D

Explanation:

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

NEW QUESTION 8

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 9

Which of the following tools would be best suited to perform a cloud security assessment?

- A. OpenVAS
- B. Scout Suite
- C. Nmap
- D. ZAP
- E. Nessus

Answer: B

Explanation:

The tool that would be best suited to perform a cloud security assessment is Scout Suite, which is an open-source multi-cloud security auditing tool that can evaluate the security posture of cloud environments, such as AWS, Azure, GCP, or Alibaba Cloud. Scout Suite can collect configuration data from cloud providers using APIs and assess them against security best practices or benchmarks, such as CIS Foundations. Scout Suite can generate reports that highlight security issues, risks, or gaps in the cloud environment, and provide recommendations for remediation or improvement. The other options are not tools that are specifically designed for cloud security assessment. OpenVAS is an open-source vulnerability scanner that can scan hosts and networks for vulnerabilities and generate reports with findings and recommendations. Nmap is an open-source network scanner and enumerator that can scan hosts and networks for ports, services, versions, OS, or other information¹. ZAP is an open-source web application scanner and proxy that can scan web applications for vulnerabilities and perform attacks such as SQL injection or XSS. Nessus is a commercial vulnerability scanner that can scan hosts and networks for vulnerabilities and generate reports with findings and recommendations.

NEW QUESTION 10

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

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

Answer:

B

Explanation:

Sinkholing is a technique used by security teams to redirect malicious or unwanted network traffic to a controlled destination, such as a black hole or a honeypot. This can help prevent or mitigate attacks, analyze malware behavior, or isolate infected hosts. If the SOC used sinkholing on the penetration tester's IP address, it means that they detected the tester's activity and blocked it from reaching the client's network. This indicates that the planning process failed to ensure all teams were notified about the penetration testing engagement, which could have avoided this situation.

NEW QUESTION 10

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 11

A penetration tester is able to use a command injection vulnerability in a web application to get a reverse shell on a system. After running a few commands, the tester runs the following:

```
python -c 'import pty; pty.spawn("/bin/bash")'
```

Which of the following actions is the penetration tester performing?

- A. Privilege escalation
- B. Upgrading the shell
- C. Writing a script for persistence
- D. Building a bind shell

Answer: B

Explanation:

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

NEW QUESTION 14

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 17

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

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

Answer: B

NEW QUESTION 21

Penetration tester who was exclusively authorized to conduct a physical assessment noticed there were no cameras pointed at the dumpster for company. The penetration tester returned at night and collected garbage that contained receipts for recently purchased networking :. The models of equipment purchased are vulnerable to attack. Which of the following is the most likely next step for the penetration?

- A. Alert the target company of the discovered information.
- B. Verify the discovered information is correct with the manufacturer.
- C. Scan the equipment and verify the findings.
- D. Return to the dumpster for more information.

Answer: C

Explanation:

The most likely next step for the penetration tester is to scan the equipment and verify the findings, which is a process of using tools or techniques to probe or test

the target equipment for vulnerabilities or weaknesses that can be exploited. Scanning and verifying the findings can help the penetration tester confirm that the models of equipment purchased are vulnerable to attack, and identify the specific vulnerabilities or exploits that affect them. Scanning and verifying the findings can also help the penetration tester prepare for the next steps of the assessment, such as exploiting or reporting the vulnerabilities. Scanning and verifying the findings can be done by using tools such as Nmap, which can scan hosts and networks for ports, services, versions, OS, or other information¹, or Metasploit, which can exploit hosts and networks using various payloads or modules². The other options are not likely next steps for the penetration tester. Alerting the target company of the discovered information is not a next step, but rather a final step, that involves reporting the findings and recommendations to the client after completing the assessment. Verifying the discovered information with the manufacturer is not a next step, as it may not provide accurate or reliable information about the vulnerabilities or exploits that affect the equipment, and it may also alert the manufacturer or the client of the assessment. Returning to the dumpster for more information is not a next step, as it may not yield any more useful or relevant information than what was already collected from the receipts.

NEW QUESTION 26

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

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

Answer: A

Explanation:

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

NEW QUESTION 27

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 29

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

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

Answer: A

Explanation:

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

Enforcing mandatory employee vacations is the best recommendation to prevent this type of activity in the future, as it will make it harder for an employee to conceal fraudulent transactions or unauthorized changes to a payment system. Mandatory employee vacations are a form of internal control that requires employees to take time off from work periodically and have their duties performed by someone else. This can help detect errors, irregularities, or frauds committed by employees who might otherwise have exclusive access or control over certain processes or systems.

NEW QUESTION 31

A penetration tester gains access to a system and establishes persistence, and then runs the following commands:

```
cat /dev/null > temp
```

```
touch -r .bash_history temp mv temp .bash_history
```

Which of the following actions is the tester MOST likely performing?

- A. Redirecting Bash history to /dev/null

- B. Making a copy of the user's Bash history for further enumeration
- C. Covering tracks by clearing the Bash history
- D. Making decoy files on the system to confuse incident responders

Answer: C

Explanation:

The commands are used to clear the Bash history file of the current user, which records the commands entered in the terminal. The first command redirects /dev/null (a special file that discards any data written to it) to temp, which creates an empty file named temp. The second command changes the timestamp of temp to match that of .bash_history (the hidden file that stores the Bash history). The third command renames temp to .bash_history, which overwrites the original file with an empty one. This effectively erases any trace of the commands executed by the user.

NEW QUESTION 34

During a web application test, a penetration tester was able to navigate to <https://company.com> and view all links on the web page. After manually reviewing the pages, the tester used a web scanner to automate the search for vulnerabilities. When returning to the web application, the following message appeared in the browser: unauthorized to view this page. Which of the following BEST explains what occurred?

- A. The SSL certificates were invalid.
- B. The tester IP was blocked.
- C. The scanner crashed the system.
- D. The web page was not found.

Answer: B

Explanation:

The most likely explanation for what occurred is that the tester IP was blocked by the web server. The web server may have detected the web scanner as a malicious or suspicious activity and blocked the tester's IP address from accessing the web application. This could result in an unauthorized to view this page message in the browser.

NEW QUESTION 39

Which of the following is the MOST common vulnerability associated with IoT devices that are directly connected to the Internet?

- A. Unsupported operating systems
- B. Susceptibility to DDoS attacks
- C. Inability to network
- D. The existence of default passwords

Answer: A

NEW QUESTION 42

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 44

A software company has hired a penetration tester to perform a penetration test on a database server. The tester has been given a variety of tools used by the company's privacy policy. Which of the following would be the BEST to use to find vulnerabilities on this server?

- A. OpenVAS
- B. Nikto
- C. SQLmap
- D. Nessus

Answer: C

NEW QUESTION 47

A penetration tester conducted an assessment on a web server. The logs from this session show the following:

`http://www.thecompanydomain.com/servicestatus.php?serviceID=892&serviceID=892 ' ; DROP TABLE SERVICES; -`

Which of the following attacks is being attempted?

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

Answer: C

NEW QUESTION 49

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 50

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 52

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 56

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 59

A company that requires minimal disruption to its daily activities needs a penetration tester to perform information gathering around the company's web presence. Which of the following would the tester find MOST helpful in the initial information-gathering steps? (Choose two.)

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

Answer: AD

Explanation:

* A. IP addresses and subdomains. This is correct. IP addresses and subdomains are useful information for a penetration tester to identify the scope and range of the company's web presence. IP addresses can reveal the location, network, and service provider of the company's web servers, while subdomains can indicate the different functions and features of the company's website. A penetration tester can use tools like whois, Netcraft, or DNS lookups to find IP addresses and subdomains associated with the company's domain name.

* D. Internet search engines. This is correct. Internet search engines are powerful tools for a penetration tester to perform passive information gathering around the company's web presence. Search engines can provide a wealth of information, such as the company's profile, history, news, social media accounts, reviews, products, services, customers, partners, competitors, and more. A penetration tester can use advanced search operators and keywords to narrow down the results and find relevant information. For example, using the site: operator can limit the results to a specific domain or subdomain, while using the intitle: operator can filter the results the title of the web pages.

NEW QUESTION 60

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

```
3af068faa81326ffe6ca48e2ab36a779
48ec2f4f526303a9ded67938e6ce11c6
9493bf035c534197d9810a5e65a10632
C847b4a2e76ec1f9cbbbe30d2046d5e8
ed225542767a810e6fcee6f640164b140
cfbe1fdd6e6b0c5c9abd8c947f272ef4
c05cbc5a69bcc91f56a7e0a6c391ad79
9ee3564cbf15421ebabc43dcb67949ad
5a2ad0bcb902e20c4efcf057b01050be
4865a2ed25ed18515b7e97beb2b40346
b0236938a6518fc65b72159687e3a27b
9c96354712595ef2ff96675496d3a464
a5ab3f6c6159b85209ea0c186531a49f
9b38816e791f1400245f4c629a503bc8
d12e624a20d54fd3b34b89ee7169df17
```

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

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

Answer: B

NEW QUESTION 65

A penetration tester needs to access a building that is guarded by locked gates, a security team, and cameras. Which of the following is a technique the tester can use to gain access to the IT framework without being detected?

- A. Pick a lock.
- B. Disable the cameras remotely.
- C. Impersonate a package delivery worker.
- D. Send a phishing email.

Answer: C

NEW QUESTION 68

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 73

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="c2RmZGZnaHhZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JobGFzZwJmaXVkaZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2=="name="csrf-token"/>
<script>
document.write("<OPTION value=1>" + document.location.href.substring(document.location.href.indexOf("=")+16) + "</OPTION>");
</script></script>
<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	h1bcdctse2ewvqwf4bdcb3v	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	36104370.12=Account%20Type=Not%20Defined=1	.comptia.o...	/	2019-10-1...	48			
__utmz	36104370.1508266963.1.1.utmcsr=google[utmccn=(organic)]utmC...	.comptia.o...	/	2018-04-1...	99			
_sp_id.0767	4a84866c6ffff51c.1508266964.1508258019.1508266964.81ff34f7...	.comptia.o...	/	2019-10-1...	99			
_sp_ses.0767	*	.comptia.o...	/	2017-10-1...	13			

Secure System

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

```
1 <html>
2 <head>
3 <title>Secure Login </title>
4 </head>
5 <body>
6 <meta
7 content="c2RmZGZnaHhZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
8 bnNkbGtqO2Job3VpYXNpZGZubXM7bGtZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JobGFzZwJmaXVkaZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
9 d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2=="name="csrf-token"/>
10 <script>
11 document.write("<OPTION value=1>" + document.location.href.substring(document.location.href.indexOf("=")+16) + "</OPTION>");
12 </script></script>
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	h1bcdctse2ewwqw4bdcbv3v	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 76

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 80

A penetration tester is looking for vulnerabilities within a company's web application that are in scope. The penetration tester discovers a login page and enters the following string in a field:

1;SELECT Username, Password FROM Users;

Which of the following injection attacks is the penetration tester using?

- A. Blind SQL
- B. Boolean SQL
- C. Stacked queries
- D. Error-based

Answer: C

Explanation:

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

NEW QUESTION 84

A penetration tester downloaded the following Perl script that can be used to identify vulnerabilities in network switches. However, the script is not working properly.

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

- A. Change line 2 to \$ip= €10.192.168.254€;
- B. Remove lines 3, 5, and 6.
- C. Remove line 6.
- D. Move all the lines below line 7 to the top of the script.

Answer: B

Explanation:

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

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

NEW QUESTION 89

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 94

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 95

A penetration tester is scanning a corporate lab network for potentially vulnerable services. Which of the following Nmap commands will return vulnerable ports that might be interesting to a potential attacker?

- A. nmap192.168.1.1-5-PU22-25,80
- B. nmap192.168.1.1-5-PA22-25,80

- C. nmap192.168.1.1-5-PS22-25,80
- D. nmap192.168.1.1-5-Ss22-25,80

Answer: C

Explanation:

PS/PA/PU/PY are host discovery flags which use TCP SYN/ACK, UDP or SCTP discovery respectively. And since the ports in the options are mostly used by TCP protocols, then it's either the PS or PA flag. But since we need to know if the ports are live, sending SYN packet is a better alternative. Hence, I choose PS in this case.

The nmap -PS22-25,80 192.168.1.1-5 command will return vulnerable ports that might be interesting to a potential attacker, as it will perform a TCP SYN scan on ports 22, 23, 24, 25, and 80 of the target hosts. A TCP SYN scan is a stealthy technique that sends a SYN packet to each port and waits for a response. If the response is a SYN/ACK packet, it means the port is open and listening for connections. If the response is a RST packet, it means the port is closed and not accepting connections. If there is no response, it means the port is filtered by a firewall or IDS.

NEW QUESTION 100

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 102

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 103

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 106

A penetration tester has established an on-path position between a target host and local network services but has not been able to establish an on-path position between the target host and the Internet. Regardless, the tester would like to subtly redirect HTTP connections to a spoofed server IP. Which of the following methods would BEST support the objective?

- A. Gain access to the target host and implant malware specially crafted for this purpose.
- B. Exploit the local DNS server and add/update the zone records with a spoofed A record.
- C. Use the Scapy utility to overwrite name resolution fields in the DNS query response.
- D. Proxy HTTP connections from the target host to that of the spoofed host.

Answer: D

NEW QUESTION 109

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

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

Answer: C

Explanation:

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

NEW QUESTION 110

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

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

Answer: B

Explanation:

A hypervisor is a type of virtualization software that allows multiple virtual machines (VMs) to run on a single physical host machine. If the hypervisor is compromised, an attacker could potentially gain access to all of the VMs running on that host, which could lead to a significant data breach or other security issues.

One common type of attack against hypervisors is known as a VM escape attack. In this type of attack, an attacker exploits a vulnerability in the hypervisor to break out of the VM and gain access to the host machine. From there, the attacker can potentially gain access to other VMs running on the same host.

By ensuring that all hypervisors have the latest available patches installed, the company can reduce the likelihood that a VM escape attack will be successful. Patches often include security updates and vulnerability fixes that address known issues and can help prevent attacks.

NEW QUESTION 112

A company provided the following network scope for a penetration test:

- * 169.137.1.0/24
- * 221.10.1.0/24
- * 149.14.1.0/24

A penetration tester discovered a remote command injection on IP address 149.14.1.24 and exploited the system. Later, the tester learned that this particular IP address belongs to a third party. Which of the following stakeholders is responsible for this mistake?

- A. The company that requested the penetration test
- B. The penetration testing company
- C. The target host's owner
- D. The penetration tester
- E. The subcontractor supporting the test

Answer: A

Explanation:

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

NEW QUESTION 114

The following PowerShell snippet was extracted from a log of an attacker machine:

```
1.$net="192.168.1."
2.$setipaddress ="192.168.2."
3.function Test-Password {
4.if (args[0] -eq 'Dummy12345') {
5. return 1
6. }
7.else {
8.$cat = 22, 25, 80, 443
9. return 0
10. }
11. }
12.$cracked = 0
13.crackedpd = [ 192, 168, 1, 2]
14.$i =0
15.Do {
16. $test = 'Dummy' + $i
17. $cracked = Test - Password Test
18.$i++
19.$crackedp = ( 192, 168, 1, 1) + $cat
20. }
21.While($cracked -eq 0)
22.Write-Host " Password found : " $test
23.$setipaddress = [ 192, 168, 1, 4]
```

A penetration tester would like to identify the presence of an array. Which of the following line numbers would define the array?

- A. Line 8
- B. Line 13
- C. Line 19
- D. Line 20

Answer: A

Explanation:

\$X=2,4,6,8,9,20,5

\$y=[System.Collections.ArrayList]\$X

\$y.RemoveRange(1,2) As you can see the array has no brackets and no periods. IT HAS SEMICOLLONS TO SEPERATE THE LISTED ITEMS OR VALUES.

NEW QUESTION 117

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 118

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 120

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

- A. dig company.com MX
- B. whois company.com
- C. curl www.company.com
- D. dig company.com A

Answer: A

Explanation:

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

NEW QUESTION 122

In Python socket programming, SOCK_DGRAM type is:

- A. reliable.
- B. matrixed.
- C. connectionless.
- D. slower.

Answer: C

Explanation:

In Python socket programming, SOCK_DGRAM type is connectionless. This means that the socket does not establish a reliable connection between the sender and the receiver, and does not guarantee that the packets will arrive in order or without errors. SOCK_DGRAM type is used for UDP (User Datagram Protocol) sockets, which are faster and simpler than TCP (Transmission Control Protocol) sockets.

NEW QUESTION 127

A penetration tester conducts an Nmap scan against a target and receives the following results:

Port	State	Service
1080/tcp	open	socks

Which of the following should the tester use to redirect the scanning tools using TCP port 1080 on the target?

- A. Nessus
- B. ProxyChains
- C. OWASPZAP
- D. Empire

Answer: B

NEW QUESTION 129

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 133

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 135

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 136

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

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

Answer: C

NEW QUESTION 138

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

- A. Determine if visas are required.
- B. Ensure all testers can access all sites.
- C. Verify the tools being used are legal for use at all sites.

D. Establish the time of the day when a test can occur.

Answer: D

Explanation:

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

NEW QUESTION 141

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 146

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 147

A compliance-based penetration test is primarily concerned with:

- A. obtaining PII from the protected network.
- B. bypassing protection on edge devices.
- C. determining the efficacy of a specific set of security standards.
- D. obtaining specific information from the protected network.

Answer: C

NEW QUESTION 151

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

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

Answer: AD

Explanation:

➤ A. The libraries may be vulnerable to security bugs or exploits that can compromise the application or the data. According to the web search results, open-source libraries often have vulnerabilities that can be exploited by attackers, such as Heartbleed, Shellshock, DROWN, or npm left-pad1234. These vulnerabilities can allow attackers to extract sensitive data, execute arbitrary commands, decrypt encrypted traffic, or break the functionality of the application. Therefore, using third-party open-source libraries in application code poses a significant security risk.

➤ D. The provenance of code is unknown, meaning that the origin and history of the code are not verified or documented. According to the web search results, open-source libraries and client projects are developed and continuously evolving in an asynchronous way, which makes it difficult to track the changes and updates of the code2. Moreover, open-source libraries may have dependencies on other libraries, which can introduce additional risks or vulnerabilities1. Therefore, using third-party open-source libraries in application code poses a significant quality risk.

NEW QUESTION 155

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

- A. S/MIME

- B. FTPS
- C. DNSSEC
- D. AS2

Answer: A

Explanation:

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

NEW QUESTION 159

During the scoping phase of an assessment, a client requested that any remote code exploits discovered during testing would be reported immediately so the vulnerability could be fixed as soon as possible. The penetration tester did not agree with this request, and after testing began, the tester discovered a vulnerability and gained internal access to the system. Additionally, this scenario led to a loss of confidential credit card data and a hole in the system. At the end of the test, the penetration tester willfully failed to report this information and left the vulnerability in place. A few months later, the client was breached and credit card data was stolen. After being notified about the breach, which of the following steps should the company take NEXT?

- A. Deny that the vulnerability existed
- B. Investigate the penetration tester.
- C. Accept that the client was right.
- D. Fire the penetration tester.

Answer: B

Explanation:

The penetration tester violated the client's request and the code of ethics by not reporting the vulnerability immediately and leaving it in place. This could have contributed to the breach and the data loss. The company should investigate the penetration tester's actions and motives, and hold them accountable for any negligence or malpractice.

NEW QUESTION 164

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

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

Answer: B

Explanation:

A clickjacking vulnerability allows an attacker to trick a user into clicking on a hidden element on a web page, such as a login button or a link. A watering-hole attack is a technique where the attacker compromises a website that is frequently visited by the target users, and injects malicious code or content into the website. The attacker can then use the clickjacking vulnerability to redirect the users to a malicious website or perform unauthorized actions on their behalf.

* A. Perform XSS. This is incorrect. XSS (cross-site scripting) is a vulnerability where an attacker injects malicious scripts into a web page that are executed by the browser of the victim. XSS can be used to steal cookies, session tokens, or other sensitive information, but it is not directly related to clickjacking.

* C. Use BeEF. This is incorrect. BeEF (Browser Exploitation Framework) is a tool that allows an attacker to exploit various browser vulnerabilities and take control of the browser of the victim. BeEF can be used to launch clickjacking attacks, but it is not the only way to do so.

* D. Use browser autopwn. This is incorrect. Browser autopwn is a feature of Metasploit that automatically exploits browser vulnerabilities and delivers a payload to the victim's system. Browser autopwn can be used to compromise the browser of the victim, but it is not directly related to clickjacking.

References:

> 1: OWASP Foundation, "Clickjacking", <https://owasp.org/www-community/attacks/Clickjacking>

> 2: PortSwigger, "What is clickjacking? Tutorial & Examples",
<https://portswigger.net/web-security/clickjacking>

> 4: Akto, "Clickjacking: Understanding vulnerability, attacks and prevention", <https://www.akto.io/blog/clickjacking-understanding-vulnerability-attacks-and-prevention>

NEW QUESTION 166

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

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

Answer: B

Explanation:

<https://hackertarget.com/nikto-website-scanner/>

NEW QUESTION 168

A red team completed an engagement and provided the following example in the report to describe how the team gained access to a web server:

x' OR role LIKE '%admin%

Which of the following should be recommended to remediate this vulnerability?

- A. Multifactor authentication

- B. Encrypted communications
- C. Secure software development life cycle
- D. Parameterized queries

Answer: D

Explanation:

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

NEW QUESTION 172

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

- A. Cost of the assessment
- B. Report distribution
- C. Testing restrictions
- D. Liability

Answer: B

NEW QUESTION 175

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

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

Answer: D

Explanation:

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

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

NEW QUESTION 177

A physical penetration tester needs to get inside an organization's office and collect sensitive information without acting suspiciously or being noticed by the security guards. The tester has observed that the company's ticket gate does not scan the badges, and employees leave their badges on the table while going to the restroom. Which of the following techniques can the tester use to gain physical access to the office? (Choose two.)

- A. Shoulder surfing
- B. Call spoofing
- C. Badge stealing
- D. Tailgating
- E. Dumpster diving
- F. Email phishing

Answer: CD

NEW QUESTION 182

A penetration tester is cleaning up and covering tracks at the conclusion of a penetration test. Which of the following should the tester be sure to remove from the system? (Choose two.)

- A. Spawned shells
- B. Created user accounts
- C. Server logs
- D. Administrator accounts
- E. Reboot system
- F. ARP cache

Answer: AB

Explanation:

Removing shells: Remove any shell programs installed when performing the pentest.

Removing tester-created credentials: Be sure to remove any user accounts created during the pentest. This includes backdoor accounts.

Removing tools: Remove any software tools that were installed on the customer's systems that were used to aid in the exploitation of systems.

NEW QUESTION 185

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 189

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 192

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

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

Answer: A

Explanation:

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

NEW QUESTION 197

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 201

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

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

Answer: C

Explanation:

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

NEW QUESTION 202

A Chief Information Security Officer wants to evaluate the security of the company's e-commerce application. Which of the following tools should a penetration tester use FIRST to obtain relevant information from the application without triggering alarms?

- A. SQLmap
- B. DirBuster
- C. w3af
- D. OWASP ZAP

Answer: C

Explanation:

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

NEW QUESTION 205

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 210

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 214

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

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

Answer: A

Explanation:

<https://steemit.com/informatica/@jordiurbina1/tutorial-hacking-wi-fi-wireless-networks-with-wifislax> The penetration tester should send deauthentication frames to the stations to force them to disconnect from their current access point and reconnect to another one, which may be the malicious AP deployed by the tester. Deauthentication frames are part of the 802.11 protocol and are used to terminate an existing wireless association between a station and an access point. However, they can also be spoofed by an attacker to disrupt or hijack wireless connections. The other options are not effective or relevant for this purpose. Performing jamming on all 2.4GHz and 5GHz channels would interfere with all wireless signals in the area, which may cause unwanted attention or legal issues. Setting the malicious AP to broadcast within dynamic frequency selection channels would not help, as these channels are used to avoid interference with radar systems and are not commonly used by wireless stations or access points. Modifying the malicious AP configuration to not use a pre-shared key would not help, as it would make it less likely for wireless stations to connect to it if they are configured to use encryption.

NEW QUESTION 216

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 220

A client has requested that the penetration test scan include the following UDP services: SNMP, NetBIOS, and DNS. Which of the following Nmap commands will perform the scan?

- A. `nmap -vv sUV -p 53, 123-159 10.10.1.20/24 -oA udpscan`
- B. `nmap -vv sUV -p 53,123,161-162 10.10.1.20/24 -oA udpscan`
- C. `nmap -vv sUV -p 53,137-139,161-162 10.10.1.20/24 -oA udpscan`
- D. `nmap -vv sUV -p 53, 122-123, 160-161 10.10.1.20/24 -oA udpscan`

Answer: C

NEW QUESTION 225

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

PT0-002 Practice Exam Features:

- * PT0-002 Questions and Answers Updated Frequently
- * PT0-002 Practice Questions Verified by Expert Senior Certified Staff
- * PT0-002 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * PT0-002 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The PT0-002 Practice Test Here](#)