DUMPSARENA

CompTIA PenTest+

CompTIA PT1-002

Version Demo

Total Demo Questions: 10

Total Premium Questions: 110

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

During a penetration-testing engagement, a consultant performs reconnaissance of a client to identify potential targets for a phishing campaign. Which of the following would allow the consultant to retrieve email addresses for technical and billing contacts quickly, without triggering any of the client's cybersecurity tools? (Choose two.)

A. Scraping social media sites

B. Using the WHOIS lookup tool

C. Crawling the client's website

D. Phishing company employees

E. Utilizing DNS lookup tools

F. Conducting wardriving near the client facility

ANSWER: B C

QUESTION NO: 2

A penetration tester runs a scan against a server and obtains the following output:

21/tcp open ftp Microsoft ftpd

| ftp-anon: Anonymous FTP login allowed (FTP code 230) | 03-12-20 09:23AM 331 index.aspx

| ftp-syst:

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds Microsoft Windows Server 2012 Std 3389/tcp open ssl/ms-wbt-server

| rdp-ntlm-info:

| Target Name: WEB3

| NetBIOS_Computer_Name: WEB3

| Product_Version: 6.3.9600

|_ System_Time: 2021-01-15T11:32:06+00:00

8443/tcp open http Microsoft IIS httpd 8.5

| http-methods:

|_ Potentially risky methods: TRACE

|_http-server-header: Microsoft-IIS/8.5 |_http-title: IIS Windows Server

Which of the following command sequences should the penetration tester try NEXT?

A. ftp 192.168.53.23

B. smbclient \\\\WEB3\\IPC$ -I 192.168.53.23 –U guest

C. ncrack –u Administrator –P 15worst_passwords.txt –p rdp 192.168.53.23

D. curl –X TRACE https://192.168.53.23:8443/index.aspx

E. nmap –-script vuln –sV 192.168.53.23

ANSWER: A

QUESTION NO: 3

A penetration tester who is doing a company-requested assessment would like to send traffic to another system using double tagging. Which of the following techniques would BEST accomplish this goal?

A. RFID cloning

B. RFID tagging

C. Meta tagging

D. Tag nesting

ANSWER: C

QUESTION NO: 4

Which of the following BEST describe the OWASP Top 10? (Choose two.)

A. The most critical risks of web applications

B. A list of all the risks of web applications

C. The risks defined in order of importance

D. A web-application security standard

E. A risk-governance and compliance framework

F. A checklist of Apache vulnerabilities

ANSWER: A C

Explanation:

Reference: https://www.synopsys.com/glossary/what-is-owasp-top-10.html

QUESTION NO: 5

A penetration tester would like to obtain FTP credentials by deploying a workstation as an on-path attack between the target and the server that has the FTP protocol. Which of the following methods would be the BEST to accomplish this objective?

A. Wait for the next login and perform a downgrade attack on the server.

B. Capture traffic using Wireshark.

C. Perform a brute-force attack over the server.

D. Use an FTP exploit against the server.

ANSWER: B

Explanation:

Reference: https://shahmeeramir.com/penetration-testing-of-an-ftp-server-19afe538be4b

QUESTION NO: 6

A penetration tester is preparing to perform activities for a client that requires minimal disruption to company operations. Which of the following are considered passive reconnaissance tools? (Choose two.)

A. Wireshark

B. Nessus

C. Retina

D. Burp Suite

E. Shodan

F. Nikto

ANSWER: A E

Explanation:

Reference: https://resources.infosecinstitute.com/topic/top-10-network-recon-tools/

QUESTION NO: 7

A company conducted a simulated phishing attack by sending its employees emails that included a link to a site that mimicked the corporate SSO portal. Eighty percent of the employees who received the email clicked the link and provided their corporate credentials on the fake site. Which of the following recommendations would BEST address this situation?

A. Implement a recurring cybersecurity awareness education program for all users.

B. Implement multifactor authentication on all corporate applications.

C. Restrict employees from web navigation by defining a list of unapproved sites in the corporate proxy.

D. Implement an email security gateway to block spam and malware from email communications.

ANSWER: A

Explanation:

Reference: https://resources.infosecinstitute.com/topic/top-9-free-phishing-simulators/

QUESTION NO: 8

A penetration tester has been hired to configure and conduct authenticated scans of all the servers on a software company's network. Which of the following accounts should the tester use to return the MOST results?

A. Root user

B. Local administrator

C. Service

D. Network administrator

ANSWER: C

QUESTION NO: 9

Which of the following expressions in Python increase a variable val by one (Choose two.)

A. val++

B. +val

C. val=(val+1)

D. ++val

E. val=val++

F. val+=1

ANSWER: D F

Explanation:

Reference: https://stackoverflow.com/questions/1485841/behaviour-of-increment-and-decrement-operators-in-python

QUESTION NO: 10

A penetration tester is reviewing the following SOW prior to engaging with a client:

“Network diagrams, logical and physical asset inventory, and employees’ names are to be treated as client confidential. Upon completion of the engagement, the penetration tester will submit findings to the client’s Chief Information Security Officer (CISO) via encrypted protocols and subsequently dispose of all findings by erasing them in a secure manner.”

Based on the information in the SOW, which of the following behaviors would be considered unethical? (Choose two.)

A. Utilizing proprietary penetration-testing tools that are not available to the public or to the client for auditing and inspection

B. Utilizing public-key cryptography to ensure findings are delivered to the CISO upon completion of the engagement

C. Failing to share with the client critical vulnerabilities that exist within the client architecture to appease the client’s senior leadership team

D. Seeking help with the engagement in underground hacker forums by sharing the client’s public IP address

E. Using a software-based erase tool to wipe the client’s findings from the penetration tester’s laptop

F. Retaining the SOW within the penetration tester’s company for future use so the sales team can plan future engagements

ANSWER: C E