DUMPSARENA

CompTIA PenTest+

CompTIA PT1-002

Version Demo

Total Demo Questions: 10

Total Premium Questions: 110

Buy Premium PDF

https://dumpsarena.com

sales@dumpsarena.com

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 wants to identify CVEs that can be leveraged to gain execution on a Linux server that has an SSHD running. Which of the following would BEST support this task?

A. Run nmap with the –o, -p22, and –sC options set against the target

B. Run nmap with the –sV and –p22 options set against the target

C. Run nmap with the --script vulners option set against the target

D. Run nmap with the –sA option set against the target

ANSWER: D

QUESTION NO: 3

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: 4

Penetration-testing activities have concluded, and the initial findings have been reviewed with the client. Which of the following best describes the NEXT step in the engagement?

A. Acceptance by the client and sign-off on the final report

B. Scheduling of follow-up actions and retesting

C. Attestation of findings and delivery of the report

D. Review of the lessons learned during the engagement

ANSWER: A

QUESTION NO: 5

The results of an Nmap scan are as follows:

Starting Nmap 7.80 (https://nmap.org) at 2021-01-24 01:10 EST Nmap scan report for (10.2.1.22)

Host is up (0.0102s latency).

Not shown: 998 filtered ports

Port State Service

80/tcp open http

|_http-title: 80F 22% RH 1009.1MB (text/html)

|_http-slowloris-check:

| VULNERABLE:

| Slowloris DoS Attack

| <..>

Device type: bridge|general purpose

Running (JUST GUESSING) : QEMU (95%)

OS CPE: cpe:/a:qemu:qemu

No exact OS matches found for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/. Nmap done: 1 IP address (1 host up) scanned in 107.45 seconds

Which of the following device types will MOST likely have a similar response? (Choose two.)

A. Network device

B. Public-facing web server

C. Active Directory domain controller

D. IoT/embedded device

E. Exposed RDP

F. Print queue

ANSWER: A B

QUESTION NO: 6

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: 7

A penetration tester wants to perform reconnaissance without being detected. Which of the following activities have a MINIMAL chance of detection? (Choose two.)

A. Open-source research

B. A ping sweep

C. Traffic sniffing

D. Port knocking

E. A vulnerability scan

F. An Nmap scan

ANSWER: E F

Explanation:

Reference: https://www.sciencedirect.com/topics/computer-science/passive-reconnaissance

QUESTION NO: 8

A penetration tester performs the following command:

curl –I –http2 https://www.comptia.org

Which of the following snippets of output will the tester MOST likely receive?

○ A.
```
HTTP/2 200
...
x-frame-options: SAMEORIGIN
x-xss-protection: 1; mode=block
x-content-type-options: nosniff
referrer-policy: strict-origin
strict-transport-security: max-age=31536000; includeSubdomains; preload
...
```

○ B.
```
<!DOCTYPE html>
<html lang="en">
<head>
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
...
</head>
...
<body lang="en">
</body>
</html>
```

○ C.
```
  %   Total%  Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 1698k  100 1698k    0     0  1566k      0  0:00:01  0:00:01 --:--:-- 1565k
```

○ D.
```
[############################################################] 100%
```

A. Option A

B. Option B

C. Option C

D. Option D

ANSWER: A

Explanation:

Reference: https://research.securitum.com/http-2-protocol-it-is-faster-but-is-it-also-safer/

QUESTION NO: 9

Which of the following are the MOST important items to include in the final report for a penetration test? (Choose two.)

A. The CVSS score of the finding

B. The network location of the vulnerable device

C. The vulnerability identifier

D. The client acceptance form

E. The name of the person who found the flaw

F. The tool used to find the issue

ANSWER: C F

QUESTION NO: 10

A penetration tester who is doing a security assessment discovers that a critical vulnerability is being actively exploited by cybercriminals. Which of the following should the tester do NEXT?

A. Reach out to the primary point of contact

B. Try to take down the attackers

C. Call law enforcement officials immediately

D. Collect the proper evidence and add to the final report

ANSWER: A