

DUMPS ARENA

Certified Ethical Hacker Exam (CEH v11)

ECCouncil 312-50v11

Version Demo

Total Demo Questions: 15

Total Premium Questions: 400

Buy Premium PDF

<https://dumpsarena.co>

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

On performing a risk assessment, you need to determine the potential impacts when some of the critical business processes of the company interrupt its service.

What is the name of the process by which you can determine those critical businesses?

- A. Emergency Plan Response (EPR)
- B. Business Impact Analysis (BIA)
- C. Risk Mitigation
- D. Disaster Recovery Planning (DRP)

ANSWER: B**QUESTION NO: 2**

You have compromised a server and successfully gained a root access. You want to pivot and pass traffic undetected over the network and evade any possible Intrusion Detection System. What is the best approach?

- A. Use Alternate Data Streams to hide the outgoing packets from this server.
- B. Use HTTP so that all traffic can be routed via a browser, thus evading the internal Intrusion Detection Systems.
- C. Install Cryptcat and encrypt outgoing packets from this server.
- D. Install and use Telnet to encrypt all outgoing traffic from this server.

ANSWER: C**QUESTION NO: 3**

Kevin, an encryption specialist, implemented a technique that enhances the security of keys used for encryption and authentication. Using this technique, Kevin input an initial key to an algorithm that generated an enhanced key that is resistant to brute-force attacks.

What is the technique employed by Kevin to improve the security of encryption keys?

- A. Key stretching
- B. Public key infrastructure
- C. Key derivation function

D. Key reinstallation

ANSWER: A

QUESTION NO: 4

During the enumeration phase, Lawrence performs banner grabbing to obtain information such as OS details and versions of services running. The service that he enumerated runs directly on TCP port 445.

Which of the following services is enumerated by Lawrence in this scenario?

- A. Remote procedure call (RPC)
- B. Telnet
- C. Server Message Block (SMB)
- D. Network File System (NFS)

ANSWER: C

QUESTION NO: 5

Based on the below log, which of the following sentences are true?

Mar 1, 2016, 7:33:28 AM 10.240.250.23 - 54373 10.249.253.15 - 22 tcp_ip

- A. Application is FTP and 10.240.250.23 is the client and 10.249.253.15 is the server.
- B. Application is SSH and 10.240.250.23 is the server and 10.249.253.15 is the client.
- C. SSH communications are encrypted; it's impossible to know who is the client or the server.
- D. Application is SSH and 10.240.250.23 is the client and 10.249.253.15 is the server.

ANSWER: D

QUESTION NO: 6

What is the minimum number of network connections in a multihomed firewall?

- A. 3
- B. 5
- C. 4

D. 2

ANSWER: A**QUESTION NO: 7**

When you are testing a web application, it is very useful to employ a proxy tool to save every request and response. You can manually test every request and analyze the response to find vulnerabilities. You can test parameter and headers manually to get more precise results than if using web vulnerability scanners.

What proxy tool will help you find web vulnerabilities?

- A. Maskgen
- B. Dimitry
- C. Burpsuite
- D. Proxychains

ANSWER: C**QUESTION NO: 8**

Sophia is a shopping enthusiast who spends significant time searching for trendy outfits online. Clark, an attacker, noticed her activities several times and sent a fake email containing a deceptive page link to her social media page displaying all-new and trendy outfits. In excitement, Sophia clicked on the malicious link and logged in to that page using her valid credentials.

Which of the following tools is employed by Clark to create the spoofed email?

- A. Evilginx
- B. Slowloris
- C. PLCinject
- D. PyLoris

ANSWER: A**QUESTION NO: 9**

What piece of hardware on a computer's motherboard generates encryption keys and only releases a part of the key so that decrypting a disk on a new piece of hardware is not possible?

- A. CPU
- B. UEFI
- C. GPU
- D. TPM

ANSWER: D

QUESTION NO: 10

A hacker has successfully infected an internet-facing server which he will then use to send junk mail, take part in coordinated attacks, or host junk email content. Which sort of trojan infects this server?

- A. Botnet Trojan
- B. Banking Trojans
- C. Turtle Trojans
- D. Ransomware Trojans

ANSWER: A

QUESTION NO: 11

As a Certified Ethical Hacker, you were contracted by a private firm to conduct an external security assessment through penetration testing.

What document describes the specifics of the testing, the associated violations, and essentially protects both the organization's interest and your liabilities as a tester?

- A. Service Level Agreement
- B. Project Scope
- C. Rules of Engagement
- D. Non-Disclosure Agreement

ANSWER: C

QUESTION NO: 12

The security team of Debry Inc. decided to upgrade Wi-Fi security to thwart attacks such as dictionary attacks and key recovery attacks. For this purpose, the security team started implementing cuttingedge technology that uses a modern key

establishment protocol called the simultaneous authentication of equals (SAE), also known as dragonfly key exchange, which replaces the PSK concept.

What is the Wi-Fi encryption technology implemented by Debry Inc.?

- A. WPA
- B. WEP
- C. WPA3
- D. WPA2

ANSWER: C

QUESTION NO: 13

A security analyst uses Zenmap to perform an ICMP timestamp ping scan to acquire information related to the current time from the target host machine.

Which of the following Zenmap options must the analyst use to perform the ICMP timestamp ping scan?

- A. -Pn
- B. -PU
- C. -PP
- D. -PY

ANSWER: C

QUESTION NO: 14

Stella, a professional hacker, performs an attack on web services by exploiting a vulnerability that provides additional routing information in the SOAP header to support asynchronous communication. This further allows the transmission of web-service requests and response messages using different TCP connections.

Which of the following attack techniques is used by Stella to compromise the web services?

- A. Web services parsing attacks
- B. WS-Address spoofing
- C. SOAPAction spoofing
- D. XML injection

ANSWER: C

QUESTION NO: 15

David is a security professional working in an organization, and he is implementing a vulnerability management program in the organization to evaluate and control the risks and vulnerabilities in its IT infrastructure. He is currently executing the process of applying fixes on vulnerable systems to reduce the impact and severity of vulnerabilities.

Which phase of the vulnerability-management life cycle is David currently in?

- A. Remediation
- B. Verification
- C. Risk assessment
- D. Vulnerability scan

ANSWER: A