DUMPSQUEEN

Certified Ethical Hacker Exam (CEH v11)

ECCouncil 312-50v11

Version Demo

Total Demo Questions: 15

Total Premium Questions: 400

Buy Premium PDF

https://dumpsqueen.com

support@dumpsqueen.com

QUESTION NO: 1

Louis, a professional hacker, had used specialized tools or search engines to encrypt all his browsing activity and navigate anonymously to obtain sensitive/hidden information about official government or federal databases. After gathering the information, he successfully performed an attack on the target government organization without being traced.

Which of the following techniques is described in the above scenario?

A. Website footprinting

B. Dark web footprinting

C. VPN footprinting

D. VoIP footprinting

ANSWER: C

QUESTION NO: 2

In an internal security audit, the white hat hacker gains control over a user account and attempts to acquire access to another account's confidential files and information. How can he achieve this?

A. Privilege Escalation

B. Shoulder-Surfing

C. Hacking Active Directory

D. Port Scanning

ANSWER: A

QUESTION NO: 3

```
env x='(){ :;};echo exploit' bash -c 'cat/etc/passwd'
```

What is the Shellshock bash vulnerability attempting to do on a vulnerable Linux host?

A. Removes the passwd file

B. Changes all passwords in passwd

C. Add new user to the passwd file

D. Display passwd content to prompt

ANSWER: D

QUESTION NO: 4

Jack, a disgruntled ex-employee of Incalsol Ltd., decided to inject fileless malware into Incalsol's systems. To deliver the malware, he used the current employees' email IDs to send fraudulent emails embedded with malicious links that seem to be legitimate. When a victim employee clicks on the link, they are directed to a fraudulent website that automatically loads Flash and triggers the exploit.

What is the technique used by Jack to launch the fileless malware on the target systems?

A. In-memory exploits

B. Legitimate applications

C. Script-based injection

D. Phishing

ANSWER: A

QUESTION NO: 5

This wireless security protocol allows 192-bit minimum-strength security protocols and cryptographic tools to protect sensitive data, such as GCMP-256, HMAC-SHA384, and ECDSA using a 384-bit elliptic curve.

Which is this wireless security protocol?

A. WPA3-Personal

B. WPA3-Enterprise

C. WPA2-Enterprise

D. WPA2-Personal

ANSWER: B

QUESTION NO: 6

Which of the following is a low-tech way of gaining unauthorized access to systems?

A. Social Engineering

B. Eavesdropping

C. Scanning

D. Sniffing

ANSWER: A

QUESTION NO: 7

Which of the following commands checks for valid users on an SMTP server?

A. RCPT

B. CHK

C. VRFY

D. EXPN

ANSWER: C

QUESTION NO: 8

Which of the following is a passive wireless packet analyzer that works on Linux-based systems?

A. Burp Suite

B. OpenVAS

C. tshark

D. Kismet

ANSWER: C

QUESTION NO: 9

Clark, a professional hacker, was hired by an organization to gather sensitive information about its competitors surreptitiously. Clark gathers the server IP address of the target organization using Whois footprinting. Further, he entered the server IP address as an input to an online tool to retrieve information such as the network range of the target organization and to identify the network topology and operating system used in the network.

What is the online tool employed by Clark in the above scenario?

A. DuckDuckGo

B. AOL

C. ARIN

D. Baidu

ANSWER: C

QUESTION NO: 10

You have successfully comprised a server having an IP address of 10.10.0.5. You would like to enumerate all machines in the same network quickly.

What is the best Nmap command you will use?

A. nmap -T4 -q 10.10.0.0/24

B. nmap -T4 -F 10.10.0.0/24

C. nmap -T4 -r 10.10.1.0/24

D. nmap -T4 -O 10.10.0.0/24

ANSWER: B

QUESTION NO: 11

Websites and web portals that provide web services commonly use the Simple Object Access Protocol (SOAP).

Which of the following is an incorrect definition or characteristics of the protocol?

A. Exchanges data between web services

B. Only compatible with the application protocol HTTP

C. Provides a structured model for messaging

D. Based on XML

ANSWER: B

QUESTION NO: 12

You are tasked to configure the DHCP server to lease the last 100 usable IP addresses in subnet 10.1.4.0/23.

Which of the following IP addresses could be leased as a result of the new configuration?

A. 10.1.255.200

B. 10.1.4.156

C. 10.1.4.254

D. 10.1.5.200

ANSWER: D

QUESTION NO: 13

Dorian is sending a digitally signed email to Poly. With which key is Dorian signing this message and how is Poly validating it?

A. Dorian is signing the message with his public key, and Poly will verify that the message came from Dorian by using Dorian's private key.

B. Dorian is signing the message with Poly's private key, and Poly will verify that the message came from Dorian by using Dorian's public key.

C. Dorian is signing the message with his private key, and Poly will verify that the message came from Dorian by using Dorian's public key.

D. Dorian is signing the message with Poly's public key, and Poly will verify that the message came from Dorian by using Dorian's public key.

ANSWER: C

QUESTION NO: 14

Which of the following antennas is commonly used in communications for a frequency band of 10 MHz to VHF and UHF?

A. Yagi antenna

B. Dipole antenna

C. Parabolic grid antenna

D. Omnidirectional antenna

ANSWER: A

QUESTION NO: 15

In this form of encryption algorithm, every individual block contains 64-bit data, and three keys are used, where each key consists of 56 bits. Which is this encryption algorithm?

A. IDEA

B. Triple Data Encryption Standard

C. AES

D. MD5 encryption algorithm

ANSWER: B