EC1-349$^{Q\&As}$

Computer Hacking Forensic Investigator Exam

Pass EC-COUNCIL EC1-349 Exam with 100% Guarantee

QUESTION 1

What will the following command produce on a website login page?

SELECT email, passwd, login_id, full_name FROM members

WHERE email = \\'someone@somehwere.com\\';

DROP TABLE members; --\\'

A. Retrieves the password for the first user in the members table

B. This command will not produce anything since the syntax is incorrect

C. Deletes the entire members table

D. Inserts the Error! Reference source not found. email address into the members table

Correct Answer: C

QUESTION 2

If you see the files Zer0.tar.gz and copy.tar.gz on a Linux system while doing an investigation, what can you conclude?

A. The system files have been copied by a remote attacker

B. The system administrator has created an incremental backup

C. The system has been compromised using a t0rn rootkit

D. Nothing in particular as these can be operational files

Correct Answer: C

QUESTION 3

You are working as a computer forensics investigator for a corporation on a computer abuse case. You discover evidence that shows the subject of your investigation is also embezzling money from the company. The company CEO and the corporate legal counsel advise you to contact local law enforcement and provide them with the evidence that you have found. The law enforcement officer that responds requests that you put a network sniffer on your network and monitor all traffic to the subject computer. You inform the officer that you will not be able to comply with thatnetwork sniffer on your network and monitor all traffic to the subject? computer. You inform the officer that you will not be able to comply with that request because doing so would:

A. Violate your contract

B. Cause network congestion

C. Make you an agent of law enforcement

D. Write information to the subject hard driveWrite information to the subject? hard drive

Correct Answer: C

QUESTION 4

What is a good security method to prevent unauthorized users from "tailgating"?

A. Pick-resistant locks

B. Electronic key systems

C. Man trap

D. Electronic combination locks

Correct Answer: C

QUESTION 5

Michael works for Kimball Construction Company as senior security analyst. As part of yearly security audit, Michael scans his network for vulnerabilities. Using Nmap, Michael conducts XMAS scan and most of the ports scanned do not give a response. In what state are these ports?

A. Filtered

B. Closed

C. Open

D. Stealth

Correct Answer: C

QUESTION 6

Harold is a web designer who has completed a website for ghttech.net. As part of the maintenance agreement he signed with the client, Harold is performing research online and seeing how much exposure the site has received so far. Harold navigates to google.com and types in the following search. link:www.ghttech.net What will this search produce?

A. All search engines that link to .net domains

B. All sites that link to ghttech.net

C. Sites that contain the code: link:www.ghttech.net

D. All sites that ghttech.net links to

Correct Answer: B

QUESTION 7

Which of the following network attacks refers to sending huge volumes of email to an address in an attempt to overflow the mailbox, or overwhelm the server where the email address is hosted, to cause a denial-of-service attack?

A. Email spamming

B. Mail bombing

C. Phishing

D. Email spoofing

Correct Answer: B

QUESTION 8

A picture file is recovered from a computer under investigation. During the investigation process, the file is enlarged 500% to get a better view of its contents. The picture quality is not degraded at all from this process. What kind of picture is this file?its contents. The picture? quality is not degraded at all from this process. What kind of picture is this file?

A. Raster image

B. Vector image

C. Metafile image

D. Catalog image

Correct Answer: B

QUESTION 9

What binary coding is used most often for e-mail purposes?

A. SMTP

B. Uuencode

C. IMAP

D. MIME

Correct Answer: D

QUESTION 10

Paul\\'s company is in the process of undergoing a complete security audit including logical and physical security testing. After all logical tests were performed; it is now time for the physical round to begin. None of the employees are made aware of this round of testing. The security-auditing firm sends in a technician dressed as an electrician. He waits outside in the lobby for some employees to get to work and follows behind them when they access the restricted areas. After entering the main office, he is able to get into the server room telling the IT manager that there is a problem with the outlets in that room. What type of attack has the technician performed?

A. Fuzzing

B. Tailgating

C. Backtrapping

D. Man trap attack

Correct Answer: B

QUESTION 11

Under which Federal Statutes does FBI investigate for computer crimes involving e- mail scams and mail fraud?

A. 18 U.S.C. 1029 Possession of Access Devices

B. 18 U.S.C. 1030 Fraud and related activity in connection with computers

C. 18 U.S.C. 1343 Fraud by wire, radio or television

D. 18 U.S.C. 1361 Injury to Government Property

E. 18 U.S.C. 1362 Government communication systems

F. 18 U.S.C. 1831 Economic Espionage Act

G. 18 U.S.C. 1832 Trade Secrets Act

Correct Answer: B

QUESTION 12

What is the first step that needs to be carried out to investigate wireless attacks?

A. Obtain a search warrant

B. Identify wireless devices at crime scene

C. Document the scene and maintain a chain of custody

D. Detect the wireless connections

Correct Answer: A

QUESTION 13

Email archiving is a systematic approach to save and protect the data contained in emails so that it can tie easily accessed at a later date.

A. True

B. False

Correct Answer: A

QUESTION 14

Windows Security Event Log contains records of login/logout activity or other security-related events specified by the system\\'s audit policy. What does event ID 531 in Windows Security Event Log indicates?

A. A user successfully logged on to a computer

B. The logon attempt was made with an unknown user name or a known user name with a bad password

C. An attempt was made to log on with the user account outside of the allowed time

D. A logon attempt was made using a disabled account

Correct Answer: D

QUESTION 15

When a file or folder is deleted, the complete path, including the original file name, is stored in a special hidden file called "INF02" in the Recycled folder. If the INF02 file is deleted, it is re-created when you___________.

A. Restart Windows

B. Kill the running processes in Windows task manager

C. Run the antivirus tool on the system

D. Run the anti-spyware tool on the system

Correct Answer: A

Latest EC1-349 Dumps EC1-349 Exam Questions EC1-349 Braindumps