Certified Ethical Hacker (CEH)

1. What is the essential difference between an ‘Ethical Hacker’ and a ‘Cracker’?

A. The ethical hacker does not use the same techniques or skills as a cracker.

B. The ethical hacker does it strictly for financial motives unlike a cracker.

C. The ethical hacker has authorization from the owner of the target.

D. The ethical hacker is just a cracker who is getting paid.

Answer(s): C

---

2. What does the term “Ethical Hacking” mean?

A. Someone who is hacking for ethical reasons.

B. Someone who is using his/her skills for ethical reasons.

C. Someone who is using his/her skills for defensive purposes.

D. Someone who is using his/her skills for offensive purposes.

Answer(s): C

---

3. Who is an Ethical Hacker?

A. A person who hacks for ethical reasons

B. A person who hacks for an ethical cause

C. A person who hacks for defensive purposes

D. A person who hacks for offensive purposes

Answer(s): C

---

4. What is "Hacktivism"?

A. Hacking for a cause

B. Hacking ruthlessly

C. An association which groups activists

D. None of the above

Answer(s): A

---

5. Where should a security tester be looking for information that could be used by an attacker against an organization? (Select all that apply)

- [ ] A. CHAT rooms
- [ ] B. WHOIS database
- [ ] C. News groups
- [ ] D. Web sites
- [ ] E. Search engines
- [ ] F. Organization’s own web site

Answer(s): A B C D E F

---

6. What are the two basic types of attacks?(Choose two.

- [ ] A. DoS
- [ ] B. Passive
- [ ] C. Sniffing
- [ ] D. Active
- [ ] E. Cracking

Answer(s): B D

---

7. The United Kingdom (UK) he passed a law that makes hacking into an unauthorized network a felony.
The law states:
Section1 of the Act refers to unauthorized access to computer material. This states that a person commits an offence if he causes a computer to perform any function with intent to secure unauthorized access to any program or data held in any computer. For a successful conviction under this part of the Act, the prosecution must prove that the access secured is unauthorized and that the suspect knew that this was the case. This section is designed to deal with common-or-graden hacking.
Section 2 of the deals with unauthorized access with intent to commit or facilitate the commission of further offences. An offence is committed under Section 2 if a Section 1 offence has been committed and there is the intention of committing or facilitating a further offense (any offence which attacks a custodial sentence of more than five years, not necessarily one covered but the Act). Even if it is not possible to prove the intent to commit the further offence, the Section 1 offence is still committed.
Section 3 Offences cover unauthorized modification of computer material, which generally means the creation and distribution of viruses. For conviction to succeed there must have been the intent to cause the modifications and knowledge that the modification had not been authorized.
What is the law called?

A. Computer Misuse Act 1990

B. Computer incident Act 2000

C. Cyber Crime Law Act 2003

D. Cyber Space Crime Act 1995

Answer(s): A

---

8. Which of the following best describes Vulnerability?

A. The loss potential of a threat

B. An action or event that might prejudice security

C. An agent that could take advantage of a weakness

D. A weakness or error that can lead to compromise

Answer(s): D

---

9. Steven works as a security consultant and frequently performs penetration tests for Fortune 500 companies. Steven runs external and internal tests and then creates reports to show the companies where their weak areas are. Steven always signs a non-disclosure agreement before performing his tests. What would Steven be considered?

A. Whitehat Hacker

B. BlackHat Hacker

C. Grayhat Hacker

D. Bluehat Hacker

Answer(s): A

---

10. Which of the following act in the united states specifically criminalizes the transmission of unsolicited commercial e-mail(SPAM) without an existing business relationship.

A. 2004 CANSPAM Act

B. 2003 SPAM Preventing Act

C. 2005 US-SPAM 1030 Act

D. 1990 Computer Misuse Act

Answer(s): A

---

11. ABC.com is legally liable for the content of email that is sent from its systems, regardless of whether the message was sent for private or business-related purpose. This could lead to prosecution for the sender and for the company's directors if, for example, outgoing email was found to contain material that was pornographic, racist or likely to incite someone to commit an act of terrorism.
You can always defend yourself by "ignorance of the law" clause.

A. True

B. False

Answer(s): B

---

12. You are footprinting Acme.com to gather competitive intelligence. You visit the acme.com websire for contact information and telephone number numbers but do not find it listed there. You know that they had the entire staff directory listed on their website 12 months ago but now it is not there. How would it be possible for you to retrieve information from the website that is outdated?

A. Visit google search engine and view the cached copy.

B. Visit Archive.org site to retrieve the Internet archive of the acme website

C. Crawl the entire website and store them into your computer.

D. Visit the company’s partners and customers website for this information.

Answer(s): B

---

13. User 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

Answer(s): B

---

14. Which of the following activities will NOT be considered as passive footprinting?

A. Go through the rubbish to find out any information that might have been discarded.

B. Search on financial site such as Yahoo Financial to identify assets.

C. Scan the range of IP address found in the target DNS database.

D. Perform multiples queries using a search engine.

Answer(s): C

---

15. Which one of the following is defined as the process of distributing incorrect Internet Protocol (IP) addresses/names with the intent of diverting traffic?

A. Network aliasing

B. Domain Name Server (DNS) poisoning

C. Reverse Address Resolution Protocol (ARP)

D. Port scanning

Answer(s): B

---

16. You are footprinting an organization to gather competitive intelligence. You visit the company's website for contact information and telephone numbers but do not find it listed there. You know that they had the entire staff directory listed on their website 12 months ago but not it is not there. How would it be possible for you to retrieve information from the website that is outdated?

A. Visit google's search engine and view the cached copy.

B. Visit Archive.org web site to retrieve the Internet archive of the company's website

C. Crawl the entire website and store them into your computer.

D. Visit the company's partners and customers website for this information.

Answer(s): B

---

17. A Company security System Administrator is reviewing the network system log files. He notes the following:
Network log files are at 5 MB at 12:00 noon. At 14:00 hours, the log files at 3 MB.
What should he assume has happened and what should he do about the situation?

A. He should contact the attacker’s ISP as soon as possible and have the connection disconnected.

B. He should log the event as suspicious activity, continue to investigate, and take further steps according to site security policy.

C. He should log the file size, and archive the information, because the router crashed.

D. He should run a file system check, because the Syslog server has a self correcting file system problem.

E. He should disconnect from the Internet discontinue any further unauthorized use, because an attack has taken place.

Answer(s): B

---

18. To what does “message repudiation” refer to what concept in the realm of email security?

A. Message repudiation means a user can validate which mail server or servers a message was passed through.

B. Message repudiation means a user can claim damages for a mail message that damaged their reputation.

C. Message repudiation means a recipient can be sure that a message was sent from a particular person.

D. Message repudiation means a recipient can be sure that a message was sent from a certain host.

E. Message repudiation means a sender can claim they did not actually send a particular message.

Answer(s): E

---

19. How does Traceroute map the route that a packet travels from point A to point B?

A. It uses a TCP Timestamp packet that will elicit a time exceed in transit message.

B. It uses a protocol that will be rejected at the gateways on its way to its destination.

C. It manipulates the value of time to live (TTL) parameter packet to elicit a time exceeded in transit message.

D. It manipulated flags within packets to force gateways into generating error messages.

Answer(s): C

---

20. Snort has been used to capture packets on the network. On studying the packets, the penetration tester finds it to be abnormal. If you were the penetration tester, why would you find this abnormal?
(Note: The student is being tested on concept learnt during passive OS fingerprinting, basic TCP/IP connection concepts and the ability to read packet signatures from a sniff dumo.)
05/20-17:06:45.061034 192.160.13.4:31337 -> 172.16.1.101:1
TCP TTL:44 TOS:0x10 ID:242
***FRP** Seq: 0XA1D95 Ack: 0x53 Win: 0x400
.
.
.
05/20-17:06:58.685879 192.160.13.4:31337 -> 172.16.1.101:1024
TCP TTL:44 TOS:0x10 ID:242

***FRP** Seg: 0XA1D95 Ack: 0x53 Win: 0x400
What is odd about this attack? (Choose the most appropriate statement)

A. This is not a spoofed packet as the IP stack has increasing numbers for the three flags.

B. This is back orifice activity as the scan comes from port 31337.

C. The attacker wants to avoid creating a sub-carrier connection that is not normally valid.

D. There packets were created by a tool; they were not created by a standard IP stack.

Answer(s): B
