


EC - Council

Certified Ethical Hacker

312-50 312-50 312-50 312-50 312-50 312-50 312-50 312-50

PRINTABLES

PRINTABLE PRACTICE QUESTIONS
QUESTIONS, ANSWERS, AND
DETAILED EXPLANATIONS IN AN
EASY-TO-USE PRINTABLE FORMAT

 **LearnSmart™**

Chapter 1

Introduction to Ethical Hacking

1. What is a "cracker?" Select the best answer.
- A. A cracker is someone who pushes a computer or network to its limits, and enjoys learning the intricate details of those systems.
 - B. A cracker is someone who performs illegal acts using a computer. Usually, this entails performing network scanning, performing dictionary attacks, and attempting to get unauthorized access to someone else's system.
 - C. A cracker is someone who rapidly develops new programs, or reverse-engineers existing programs, to make software better.
 - D. A cracker is a security professional who uses their skills to test a network for vulnerabilities. This is done for ethical reasons to ensure the network is secure.

[Find the Answer](#) p. 131

2. Choose a physical vulnerability and an administrative vulnerability. Select the best answers.
- A. A software flaw in a program that, if you have administrative privileges, you are granted full access to the data.
 - B. A software flaw in a program that, if you have regular user privileges, you are granted full access to the data.
 - C. The intention of a hostile cracker to exploit a system by circumventing a software security feature.
 - D. A weakness in a server application that allows a user to crash the application.
 - E. Your system administrator leaves the door to the server room propped open all night.
 - F. You, as administrator, misconfigure a share and leave the default of everyone allowed to access it.

[Find the Answer](#) p. 131



3. In the following example, which of these is the "exploit"? Today, Microsoft Corporation released a security notice. It detailed how a person could bring down the Windows 2000 Server operating system by sending malformed packets to it. They detailed how this malicious process has been automated using basic scripting. Even worse, the new automated method for bringing down the server has already been used to perform denial of service attacks on many large commercial websites. Select the best answer.
- A. Windows 2000 Server is the exploit.
 - B. The documented method of how to use the vulnerability to gain unprivileged access is the exploit.
 - C. The security "hole" in the product is the exploit.
 - D. Microsoft Corporation is the exploit.
 - E. The exploit is the hacker that would use this vulnerability.

[Find the Answer](#) p. 131

4. Which of these defines the recommended skill profile of an ethical hacker? Select the best answers.
- A. Advanced knowledge of Windows
 - B. Expert networking knowledge
 - C. A Linux expert
 - D. Educated on what a malicious attacker would do
 - E. Has committed malicious attacks in the past
 - F. An expert programmer

[Find the Answer](#) p. 131



5. Which of the following are true about the Computer Fraud and Abuse Act of 1986? Select the best answers.
- A. It is located at Title 18 of the United States Code in Section 1030.
 - B. It is located at Title 18 of the United States Code in Section 1362.
 - C. It covers Wire and Electronic Communications Interceptions and Interception of Oral Communications.
 - D. Section 1030 and 1029 are the primary US statues that address malicious hacking.
 - E. Cloned cell phones and red boxes fall under this act.
 - F. Doing a ping flood on a .mil site falls under this act.

[Find the Answer](#) p. 131

6. Which of these would probably be the deliverables after an ethical hacker has spent time on your network? Select the best answers.
- A. Documented report
 - B. Vulnerabilities found and countermeasures recommended
 - C. Results of a social engineering test
 - D. Possible security concerns, such as easy methods to get large amounts of proprietary company data out of the organization
 - E. Documenting how to crack the CEO's password
 - F. Firewall upgrade software

[Find the Answer](#) p. 131



Answers: Chapter 1

1. B	Review Question p. 2	Detailed Explanation p. 155
2. E, F	Review Question p. 2	Detailed Explanation p. 155
3. B	Review Question p. 3	Detailed Explanation p. 156
4. A, B, C, D	Review Question p. 3	Detailed Explanation p. 157
5. A, D, F	Review Question p. 4	Detailed Explanation p. 157
6. A, B, C, D	Review Question p. 4	Detailed Explanation p. 158
7. A	Review Question p. 5	Detailed Explanation p. 159
8. B, D	Review Question p. 5	Detailed Explanation p. 160
9. A	Review Question p. 6	Detailed Explanation p. 160
10. A, B, C, D	Review Question p. 6	Detailed Explanation p. 161
11. See Explanation	Review Question p. 7	Detailed Explanation p. 162
12. See Explanation	Review Question p. 8	Detailed Explanation p. 163
13. See Explanation	Review Question p. 9	Detailed Explanation p. 164
14. See Explanation	Review Question p. 10	Detailed Explanation p. 166
15. See Explanation	Review Question p. 11	Detailed Explanation p. 167
16. See Explanation	Review Question p. 12	Detailed Explanation p. 168



Explanations: Chapter 1

1. [Review Question](#) p. 2

Answers: B

Explanation A. This is not the correct answer. The definition given is that of a hacker, not a cracker. A hacker is someone who pushes a computer or network to its limits, and enjoys learning the intricate details of those systems. Due to its misuse, the word hacker has gotten a negative connotation in recent news. However, the proper definition of a hacker is someone who is an enthusiast about computers and networks.

Explanation B. This is the correct answer. The definition given was that of a cracker. A cracker is someone who performs malicious or illegal acts using a computer. Usually, this entails performing network scanning, performing dictionary attacks, and attempting to get unauthorized access to someone else's system.

Explanation C. This is not the correct answer. The definition given was that of hacking, not a cracker. Hacking is the rapid development of new programs, or the reverse-engineering of existing programs, to make software better.

Explanation D. This is not the correct answer. The definition given was that of an ethical hacker, not a cracker. An ethical hacker is a security professional who uses their knowledge to test security.

More Information:

 [Webopedia - Definition of a Crack and Cracker](#)

PrepLogic Question: [1015-100](#)

2. [Review Question](#) p. 2

Answers: E, F

Explanation A. This is not a correct answer. This is neither a physical nor administrative vulnerability. The answer states that you had administrative privileges prior to gaining full access to the data, which would be a normal expectation.

Explanation B. This is not a correct answer. This is a vulnerability because it stated that you had regular user privileges, however, it is not a physical or administrative vulnerability.

Explanation C. This is not a correct answer. This is not an example of any type of vulnerability. This definition resembles that of a threat; whereas a vulnerability is a weakness.



Explanation D. This is not a correct answer. This is an example of a vulnerability, but not an administrative or physical vulnerability. A weakness (software flaw) in the server application allows it to be brought down, thereby allowing a cracker to control that application's availability.

Explanation E. This is one of the correct answers. This is an example of a physical vulnerability. By leaving the door open, there is a physical hole allowing anyone access into the server room.

Explanation F. This is one of the correct answers. This is an example of an administrative share because it was an administrator, with full control, who created a vulnerability by leaving the default of everyone on a shared folder.

More Information:

 [Microsoft Security Glossary](#)

PrepLogic Question: [1015-101](#)

3. [Review Question](#) p. 3

Answers: B

Explanation A. This is not the correct answer. In the example given, Windows 2000 Server is the TOE (Target of Evaluation). A TOE is an IT System, product, or component that is being identified or that requires security evaluation.

Explanation B. This is the correct answer. The documented method of how to use the vulnerability to gain unprivileged access is the exploit.

Explanation C. This is not the correct answer. The security "hole" in the product is called the "vulnerability". It is documented in a way that shows how to use the vulnerability to gain unprivileged access, and it then becomes an exploit.

Explanation D. This is not the correct answer. Microsoft is not the exploit, but if Microsoft documents how the vulnerability can be used to gain unprivileged access, then they are creating the exploit. If they just say that there is a hole in the product, then it is only a vulnerability.

Explanation E. This is not the correct answer. The hacker that would use this vulnerability is exploiting it, but the hacker is not the exploit.

More Information:

 [ITSecurity.com Dictionary - Exploit](#)

PrepLogic Question: [1015-102](#)



4. [Review Question](#) p. 3**Answers: A, B, C, D**

Explanation A. This is one of the correct answers. An ethical hacker should have advanced knowledge of Windows, Linux, and Networks. Many of the systems scanned, vulnerabilities found, and settings to be performed will be in the area of Microsoft Windows.

Explanation B. This is one of the correct answers. An ethical hacker should have advanced knowledge of Windows, Linux, and Networks. The primary vehicle of attack from a malicious attacker, and the most difficult system to secure, is going to be the network. For this reason, expert networking knowledge is required.

Explanation C. This is one of the correct answers. An ethical hacker should have advanced knowledge of Windows, Linux, and Networks.

Explanation D. This is one of the correct answers. An Ethical hacker must be educated on what a malicious attacker would do. As an ethical hacker, you must "know your enemy".

Explanation E. This is not a correct answer. The question asked what are the recommended skills for an "ethical hacker". It is not recommended that an ethical hacker has committed malicious attacks in the past. Sometimes hackers who were once malicious decide to become ethical, but this is not the norm for an ethical hacker.

Explanation F. This is not a correct answer. While being an expert programmer could be helpful in being an ethical hacker, this is not considered a normal skill for an ethical hacker. An expert programmer may be able to specialize in securing applications, but ethical hackers usually spend most of their time securing the network and systems, not programs.

More Information:

[CEH Official Course Material - Ethical Hacking \(Module 1, page 30-31\)](#)

PrepLogic Question: [1015-103](#)

5. [Review Question](#) p. 4**Answers: A, D, F**

Explanation A. This is one of the correct answers. The Computer Fraud and Abuse Act of 1986 is located at Title 18 of the United States Code in Section 1030. It specifies crimes for 3 felonies and 3 misdemeanors. Many of these crimes have to do with unauthorized access to federal computers. Section 1030 also criminalizes individuals who try to defraud others.



Explanation B. This is not a correct answer. The Computer Fraud and Abuse Act of 1986 is located at Title 18 of the United States Code in Section 1030. Section 1362 covers communication lines, stations, or systems.

Explanation C. This is not a correct answer. Section 1030 does not cover these areas. The area that covers Wire and Electronic Communications Interceptions and Interception of Oral Communications is section 2510.

Explanation D. This is one of the correct answers. Section 1029 and 1030 are the primary US statutes that address cybercrime. Section 1030 is the Computer Fraud and Abuse Act of 1986.

Explanation E. This is not a correct answer. Cloned cell phones and red boxes fall under Section 1029, not Section 1030 (the Computer Fraud and Abuse Act of 1986).

Explanation F. This is one of the correct answers. The Computer Fraud and Abuse Act of 1986 is located at Title 18 of the United States Code in Section 1030. Many of the crimes it defines have to do with unauthorized access to federal computers. Thus, doing a ping flood on a .mil site would fall under this act.

More Information:

 [Windows Security - Computer Crime Law Series](#)

PrepLogic Question: [1015-104](#)

6. [Review Question](#) p. 4

Answers: A, B, C, D

Explanation A. This is one of the correct answers. A certified ethical hacker who was contracted to perform a security evaluation would provide a detailed report of test results, vulnerabilities, and recommendations for countermeasures.

Explanation B. This is one of the correct answers. A certified ethical hacker who was contracted to perform a security evaluation would provide a detailed report of test results, vulnerabilities, and recommendations for countermeasures.

Explanation C. This is one of the correct answers. A certified ethical hacker who was contracted to perform a security evaluation would provide a detailed report of test results, vulnerabilities, and recommendations for countermeasures. This report may contain the results of a social engineering test, if that was part of the scope of the project.

Explanation D. This is one of the correct answers. Part of any security evaluation would be obvious security concerns, such as easy methods to get large amounts of proprietary company data out of the organization.

