ISLEVER

312-50

ECCouncil Certified Ethical Hacker

DEMO

Topic 1, Introduction to Ethical Hacking

QUESTION NO: 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: C
Explanation: The ethical hacker uses the same techniques and skills as a cracker and the motive is to find the security breaches before a cracker does. There is nothing that says that a cracker does not get paid for the work he does, a ethical hacker has the owners authorization and will get paid even if he does not succeed to penetrate the target.

QUESTION NO: 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: C
Explanation: Ethical hacking is only about defending your self or your employer against malicious persons by using the same techniques and skills.

QUESTION NO: 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: C

Explanation: The Ethical hacker is a security professional who applies his hacking skills for defensive purposes.

QUESTION NO: 4

What is "Hacktivism"?

A. Hacking for a cause
B. Hacking ruthlessly
C. An association which groups activists
D. None of the above

Answer: A

Explanation: The term was coined by author/critic Jason Logan King Sack in an article about media artist Shu Lea Cheang. Acts of hacktivism are carried out in the belief that proper use of code will have leveraged effects similar to regular activism or civil disobedience.

QUESTION NO: 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: A,B,C,D,E,F

Explanation: A Security tester should search for information everywhere that he/she can access. You never know where you find that small piece of information that could penetrate a strong defense.

QUESTION NO: 6

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

A. DoS
B. Passive
C. Sniffing
D. Active
E. Cracking

Answer: B,D

Explanation: Passive and active attacks are the two basic types of attacks.

QUESTION NO: 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