ECCouncil

Exam 312-50

Ethical Hacking and Countermeasures

Version: 7.3

[Total Questions: 765]

Topic break down

Topic	No. of Questions
Topic 1: Introduction to Ethical Hacking	11
Topic 10: Session Hijacking	10
Topic 11: Hacking Web Servers	24
Topic 12: Web Application Vulnerabilities	20
Topic 13: Web Based Password Cracking Techniques	4
Topic 14: SQL Injection	15
Topic 15: Hacking Wireless Networks	28
Topic 16: Virus and Worms	9
Topic 17: Physical Security	5
Topic 18: Linux Hacking	22
Topic 19: Evading IDS, Firewalls and Honeypots	60
Topic 2: Footprinting	23
Topic 20: Buffer Overflows	17
Topic 21: Cryptography	20
Topic 22: Penetration Testing Methodologies	10
Topic 23: Mixed Questions	200
Topic 3: Scanning	94
Topic 4: Enumeration	48
Topic 5: System Hacking	51
Topic 6: Trojans and Backdoors	20
Topic 7: Sniffers	27
Topic 8: Denial of Service	28
Topic 9: Social Engineering	19

Topic 1, Introduction to Ethical Hacking

Question No : 1 - (Topic 1)

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 : 2 - (Topic 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 : 3 - (Topic 1)

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: A

Explanation: A white hat hacker, also rendered as ethical hacker, is, in the realm of information technology, a person who is ethically opposed to the abuse of computer systems. Realization that the Internet now represents human voices from around the world has made the defense of its integrity an important pastime for many. A white hat generally focuses on securing IT systems, whereas a black hat (the opposite) would like to break into them.

Question No : 4 - (Topic 1)

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: D

Explanation: A vulnerability is a flaw or weakness in system security procedures, design or implementation that could be exercised (accidentally triggered or intentionally exploited) and result in a harm to an IT system or activity.

Question No : 5 - (Topic 1)

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 : 6 - (Topic 1)

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 : 7 - (Topic 1)

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: B

Explanation: *Ignorantia juris non excusat* or *Ignorantia legis neminem excusat* (Latin for "ignorance of the law does not excuse" or "ignorance of the law excuses no one") is a public policy holding that a person who is unaware of a law may not escape liability for violating that law merely because he or she was unaware of its content; that is, persons have presumed knowledge of the law. Presumed knowledge of the law is the principle in jurisprudence that one is bound by a law even if one does not know of it. It has also been defined as the "prohibition of ignorance of the law".

Question No : 8 - (Topic 1)

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 : 9 - (Topic 1)

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: A

Explanation: Computer Misuse Act (1990) creates three criminal offences:

- Unauthorised access to computer material
- Unauthorised access to a computer system with intent to commit or facilitate the commission of a further offence
- Unauthorised modification of computer material

Question No : 10 - (Topic 1)

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: A

Explanation: The CAN-SPAM Act of 2003 (Controlling the Assault of Non-Solicited Pornography and Marketing Act) establishes requirements for those who send commercial email, spells out penalties for spammers and companies whose products are advertised in spam if they violate the law, and gives consumers the right to ask emailers to stop spamming them. The law, which became effective January 1, 2004, covers email whose primary purpose is advertising or promoting a commercial product or service, including content on a Web site. A "transactional or relationship message" – email that facilitates an agreed-upon transaction or updates a customer in an existing business relationship – may not contain false or misleading routing information, but otherwise is exempt from most provisions of the CAN-SPAM Act.

Question No : 11 - (Topic 1)

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.

Topic 10, Session Hijacking

Question No : 12 - (Topic 10)

You want to carry out *session hijacking* on a remote server. The server and the client are communicating via TCP after a successful TCP three way handshake. The server has just received packet #120 from the client. The client has a receive window of 200 and the server has a receive window of 250.

Within what range of sequence numbers should a packet, sent by the client fall in order to be accepted by the server?

A. 200-250
B. 121-371
C. 120-321
D. 121-231
E. 120-370

Answer: B

Explanation: Package number 120 have already been received by the server and the window is 250 packets, so any package number from 121 (next in sequence) to 371

(121+250).

Question No : 13 - (Topic 10)

Which of the following attacks takes best advantage of an existing authenticated connection

A. Spoofing
B. Session Hijacking
C. Password Sniffing
D. Password Guessing

Answer: B

Explanation: Session hijacking is the act of taking control of a user session after successfully obtaining or generating an authentication session ID. Session hijacking involves an attacker using captured, brute forced or reverse-engineered session IDs to seize control of a legitimate user's Web application session while that session is still in progress.

Question No : 14 - (Topic 10)

Which is the right sequence of packets sent during the initial TCP three way handshake?

A. FIN, FIN-ACK, ACK
B. SYN, URG, ACK
C. SYN, ACK, SYN-ACK
D. SYN, SYN-ACK, ACK

Answer: D