For More Questions ***Click Here***

1. Why would a hacker use a proxy server?

A. To create a stronger connection with the target.
B. To create a ghost server on the network.
C. To obtain a remote access connection.
D. To hide malicious activity on the network.

Correct Answer – D
Explanation – Proxy servers exist to act as an intermediary between the hacker and the target and servces to keep the hacker anonymous tot he network.

2. What type of symmetric key algorithm using a streaming cipher to encrypt information?

A. RC4
B. Blowfish
C. SHA
D. MD5

Correct Answer – A
Explanation – RC$ uses streaming ciphers.

3. Which of the following is not a factor in securing the environment against an attack on security?

A. The education of the attacker
B. The system configuration
C. The network architecture
D. The business strategy of the company
E. The level of access provided to employees

Correct Answer – D
Explanation – All of the answers are factors supporting the exploitation or prevention of an attack. The business strategy may provide the motivation for a potential attack, but by itself will not influence the outcome.

4. What type of attack uses a fraudulent server with a relay address?

A. NTLM
B. MITM
C. NetBIOS
D. SMB

Correct Answer – B
Explanation – MITM (Man in the Middle) attacks create a server with a relay address. It is used in SMB relay attacks.

5. What port is used to connect to the Active Directory in Windows 2000?

A. 80
B. 445
C. 139
D. 389

Correct Answer – D
Explanation – The Active Directory Administration Tool used for a Windows 2000 LDAP client uses port 389 to connect to the Active Directory service.

6. To hide information inside a picture, what technology is used?

A. Rootkits
B. Bitmapping
C. Steganography
D. Image Rendering

Correct Answer – C
Explanation – Steganography is the right answer and can be used to hide information in pictures, music, or videos.

7. Which phase of hacking performs actual attack on a network or system?

A. Reconnaissance
B. Maintaining Access
C. Scanning
D. Gaining Access

Correct Answer – D
Explanation – In the process of hacking, actual attacks are performed when gaining access, or ownership, of the network or system. Reconnaissance and Scanning are information gathering steps to identify the best possible action for staging the attack. Maintaining access attempts to prolong the attack.

8. Attempting to gain access to a network using an employee's credentials is called the _____ mode of ethical hacking.

A. Local networking
B. Social engineering
C. Physical entry
D. Remote networking

Correct Answer – A
Explanation – Local networking uses an employee's credentials, or access rights, to gain access to the network. Physical entry uses credentials to gain access to the physical IT infrastructure.

9. Which Federal Code applies the consequences of hacking activities that disrupt subway transit systems?

A. Electronic Communications Interception of Oral Communications
B. 18 U.S.C. § 1029
C. Cyber Security Enhancement Act 2002
D. 18 U.S.C. § 1030

Correct Answer – C
Explanation – The Cyber Security Enhancement Act 2002 deals with life sentences for hackers who recklessly endanger the lives of others, specifically transportation systems.

10. Which of the following is not a typical characteristic of an ethical hacker?

A. Excellent knowledge of Windows.
B. Understands the process of exploiting network vulnerabilities.
C. Patience, persistence and perseverance.
D. Has the highest level of security for the organization.

Correct Answer – D
Explanation – Each answer has validity as a characteristic of an ethical hacker. Though having the highest security clearance is ideal, it is not always the case in an organization.