EC-Council Security Specialist

1. Firewalking is a technique that can be used to gather information about a remote network protected by a firewall. This technique can be used effectively to perform information gathering attacks. In this technique, an attacker sends a crafted packet with a TTL value that is set to expire one hop past the firewall. Which of the following are pre-requisites for an attacker to conduct firewalking?
Each correct answer represents a complete solution. Choose all that apply.

- [ ] A. ICMP packets leaving the network should be allowed.
- [ ] B. An attacker should know the IP address of the last known gateway before the firewall.
- [ ] C. There should be a backdoor installed on the network.
- [ ] D. An attacker should know the IP address of a host located behind the firewall.

Answer(s): A B D

---

2. Which of the following security protocols are based on the 802.11i standard?
Each correct answer represents a complete solution. Choose all that apply.

- [ ] A. WEP
- [ ] B. WPA2
- [ ] C. WPA
- [ ] D. WEP2

Answer(s): B C

---

3. Which of the following OSI layers is responsible for protocol conversion, data encryption/decryption, and data compression?

- A. Transport layer
- B. Presentation layer
- C. Data-link layer
- D. Network layer

Answer(s): B

---

4. You are responsible for security at a company that uses a lot of Web applications. You are most concerned about flaws in those applications allowing some attacker to get into your network. What method would be best for finding such flaws?

A. Vulnerability scanning

B. Manual penetration testing

C. Automated penetration testing

D. Code review

Answer(s): A

---

5. Which of the following representatives of incident response team takes forensic backups of the systems that are the focus of the incident?

A. Lead investigator

B. Information security representative

C. Technical representative

D. Legal representative

Answer(s): C

---

6. Which of the following statements are true about routers?
Each correct answer represents a complete solution. Choose all that apply.

- [ ] A. Routers are responsible for making decisions about which of several paths network (or Internet) traffic will follow.
- [ ] B. Routers do not limit physical broadcast traffic.
- [ ] C. Routers organize addresses into classes, which are used to determine how to move packets from one network to another.
- [ ] D. Routers act as protocol translators and bind dissimilar networks.

Answer(s): A C D

---

7. Which of the following types of attacks cannot be prevented by technical measures only?

A. Brute force

B. Ping flood attack

C. Smurf DoS

D. Social engineering

Answer(s): D

---

8. You work as a Network Administrator for Tech Perfect Inc. The company requires a secure wireless network. To provide security, you are configuring ISA Server 2006 as a firewall. While configuring ISA Server 2006, which of the following is NOT necessary?

A. Defining how ISA Server would cache Web contents

B. Defining ISA Server network configuration

C. Setting up of monitoring on ISA Server

D. Configuration of VPN access

Answer(s): D

---

9. Which of the following attacks CANNOT be detected by an Intrusion Detection System (IDS)? Each correct answer represents a complete solution. Choose all that apply.

- [ ] A. Denial-of-Service (DoS) attack
- [ ] B. E-mail spoofing
- [ ] C. Port scan attack
- [ ] D. Shoulder surfing

Answer(s): B D

---

10. Which of the following statements best describes a certification authority?

A. A certification authority is a type of encryption that uses a public key and a private key pair for data encryption.

B. A certification authority is an entity that issues digital certificates for use by other parties.

C. A certification authority is a technique to authenticate digital documents by using computer cryptography.

D. A certification authority is a type of encryption that uses a single key to encrypt and decryp t data.

Answer(s): B

---

11. You have just set up a wireless network for customers at a coffee shop. Which of the following are good security measures to implement?
Each correct answer represents a complete solution. Choose two.

- [ ] A. Using WEP encryption
- [ ] B. Using WPA encryption
- [ ] C. Not broadcasting SSID
- [ ] D. MAC filtering the router

Answer(s): A B

---

12. Linux traffic monitoring tools are used to monitor and quickly detect faults in the network or a system. Which of the following tools are used to monitor traffic of the Linux operating system?
Each correct answer represents a complete solution. Choose all that apply.

- [ ] A. PsExec
- [ ] B. IPTraf
- [ ] C. MRTG
- [ ] D. PsLogList
- [ ] E. Ntop

Answer(s): B C E

---

13. John works as an Office Assistant in DataSoft Inc. He has received an e-mail from duesoft_lotterygroup@us.com with the following message:
The DueSoft Lottery Incorporation
This is to inform you that you have just won a prize of $7,500.00 for this year's Annual Lottery promotion, which was organized by Msn/Yahoo Lottery in conjunction with DueSoft. We collect active online e-mails and select five people every year as our winners through an electronic balloting machine. Please reply within three days of receiving this e-mail with your full details like Name, Address, Sex, Occupation, Age, State, Telephone number, and Country to claim your prize.
If John replies to this e-mail, which of the following attacks may he become vulnerable to?

- A. Salami attack
- B. Man-in-the-Middle attack
- C. Phishing attack
- D. DoS attack

Answer(s): C

---

14. Fill in the blank with the appropriate word ___is software that is a subcategory of malware and refers to unwanted software that performs malicious actions on a user's computer. Some its examples are Trojan, adware, and spyware.

A. Crimeware

Answer(s): A

---

15. John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He is using a tool to crack the wireless encryption keys. The description of the tool is as follows:

It is a Linux-based WLAN WEP cracking tool that recovers encryption keys. It operates by passively monitoring transmissions. It uses Ciphertext Only Attack and captures approximately 5 to 10 million packets to decrypt the WEP keys.

Which of the following tools is John using to crack the wireless encryption keys?

A. AirSnort

B. Kismet

C. PsPasswd

D. Cain

Answer(s): A

---

16. Which of the following proxy servers is also referred to as transparent proxies or forced proxies?

A. Intercepting proxy server

B. Anonymous proxy server

C. Reverse proxy server

D. Tunneling proxy server

Answer(s): A

---

17. Which of the following security policies will you implement to keep safe your data when you connect your Laptop to the office network over IEEE 802.11 WLANs?
Each correct answer represents a complete solution. Choose two.

- [ ] A. Using a protocol analyzer on your Laptop to monitor for risks.
- [ ] B. Using an IPSec enabled VPN for remote connectivity.

- [ ] C. Using portscanner like nmap in your network.
- [ ] D. Using personal firewall software on your Laptop.

Answer(s): B D

---

18. Which of the following is the first computer virus that was used to infect the boot sector of storage media formatted with the DOS File Allocation Table (FAT) file system?

A. I love you

B. Melissa

C. Tequila

D. Brain

Answer(s): D

---

19. Which of the following needs to be documented to preserve evidences for presentation in court?

A. Incident response policy

B. Account lockout policy

C. Separation of duties

D. Chain of custody

Answer(s): D

---

20. Kerberos is a computer network authentication protocol that allows individuals communicating over a non-secure network to prove their identity to one another in a secure manner. Which of the following statements are true about the Kerberos authentication scheme?
Each correct answer represents a complete solution. Choose all that apply.

- [ ] A. Kerberos requires continuous availability of a central server.
- [ ] B. Kerberos builds on Asymmetric key cryptography and requires a trusted third party.
- [ ] C. Dictionary and brute force attacks on the initial TGS response to a client may reveal the subject's passwords.
- [ ] D. Kerberos requires the clocks of the involved hosts to be synchronized.

Answer(s): A C D