



# GIAC

## GCIA Exam

### GIAC Certified Intrusion Analyst

Thank you for Downloading GCIA exam PDF Demo

You can Buy Latest GCIA Full Version Download

<https://www.certkillers.net/Exam/GCIA>

<https://www.certkillers.net>

---

**Question: 1**

---

Andrew works as a System Administrator for NetPerfect Inc. All client computers on the network run on Mac OS X. The Sales Manager of the company complains that his MacBook is not able to boot. Andrew wants to check the booting process. He suspects that an error persists in the bootloader of Mac OS X. Which of the following is the default bootloader on Mac OS X that he should use to resolve the issue?

- A. LILO
- B. BootX
- C. NT Loader
- D. GRUB

---

**Answer: B**

---

---

**Question: 2**

---

Sasha wants to add an entry to your DNS database for your mail server. Which of the following types of resource records will she use to accomplish this?

- A. ANAME
- B. SOA
- C. MX
- D. CNAME

---

**Answer: C**

---

---

**Question: 3**

---

John, a novice web user, makes a new E-mail account and keeps his password as "apple", his favorite fruit. John's password is vulnerable to which of the following password cracking attacks? Each correct answer represents a complete solution. Choose all that apply.

- A. Dictionary attack
- B. Hybrid attack
- C. Brute Force attack
- D. Rule based attack

---

**Answer: A, B, C**

---

---

**Question: 4**

---

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

- A. Tunneling proxy server

- B. Reverse proxy server
- C. Anonymous proxy server
- D. Intercepting proxy server

---

**Answer: D**

---

---

**Question: 5**

---

Which of the following statements about a host-based intrusion prevention system (HIPS) are true? Each correct answer represents a complete solution. Choose two.

- A. It can detect events scattered over the network.
- B. It can handle encrypted and unencrypted traffic equally.
- C. It cannot detect events scattered over the network.
- D. It is a technique that allows multiple computers to share one or more IP addresses.

---

**Answer: B, C**

---

---

**Question: 6**

---

Victor works as a network administrator for DataSecu Inc. He uses a dual firewall Demilitarized Zone (DMZ) to insulate the rest of the network from the portions that is available to the Internet. Which of the following security threats may occur if DMZ protocol attacks are performed? Each correct answer represents a complete solution. Choose all that apply.

- A. Attacker can perform Zero Day attack by delivering a malicious payload that is not a part of the intrusion detection/prevention systems guarding the network.
- B. Attacker can gain access to the Web server in a DMZ and exploit the database.
- C. Attacker managing to break the first firewall defense can access the internal network without breaking the second firewall if it is different.
- D. Attacker can exploit any protocol used to go into the internal network or intranet of the company

---

**Answer: A, B, D**

---

---

**Question: 7**

---

Which of the following is known as a message digest?

- A. Hash function
- B. Hashing algorithm
- C. Spider
- D. Message authentication code

---

**Answer: A**

---

---

**Question: 8**

---

Ryan, a malicious hacker submits Cross-Site Scripting (XSS) exploit code to the Website of Internet forum for online discussion. When a user visits the infected Web page, code gets automatically executed and Ryan can easily perform acts like account hijacking, history theft etc. Which of the following types of Cross-Site Scripting attack Ryan intends to do?

- A. Document Object Model (DOM)
- B. Non persistent
- C. SAX
- D. Persistent

---

**Answer: D**

---

---

### Question: 9

---

Peter works as a Technical Representative in a CSIRT for SecureEnet Inc. His team is called to investigate the computer of an employee, who is suspected for classified data theft. Suspect's computer runs on Windows operating system. Peter wants to collect data and evidences for further analysis. He knows that in Windows operating system, the data is searched in pre-defined steps for proper and efficient analysis. Which of the following is the correct order for searching data on a Windows based system?

- A. Volatile data, file slack, registry, memory dumps, file system, system state backup, internet traces
- B. Volatile data, file slack, file system, registry, memory dumps, system state backup, internet traces
- C. Volatile data, file slack, internet traces, registry, memory dumps, system state backup, file system
- D. Volatile data, file slack, registry, system state backup, internet traces, file system, memory dumps

---

**Answer: B**

---

---

### Question: 10

---

You are the Network Administrator for a large corporate network. You want to monitor all network traffic on your local network for suspicious activities and receive a notification when a possible attack is in process. Which of the following actions will you take for this?

- A. Enable verbose logging on the firewall
- B. Install a network-based IDS
- C. Install a DMZ firewall
- D. Install a host-based IDS

---

**Answer: B**

---

---

### Question: 11

---

Adam works as a professional Computer Hacking Forensic Investigator. He wants to investigate a suspicious email that is sent using a Microsoft Exchange server. Which of the following files will he review to accomplish the task?

Each correct answer represents a part of the solution. Choose all that apply.

- A. Checkpoint files

- B. EDB and STM database files
- C. Temporary files
- D. cookie files

---

**Answer: A, B, C**

---

---

### Question: 12

---

This is a Windows-based tool that is used for the detection of wireless LANs using the IEEE 802.11a, 802.11b, and 802.11g standards. The main features of these tools are as follows:

It displays the signal strength of a wireless network, MAC address, SSID, channel details, etc.

It is commonly used for the following purposes:

- a. War driving
- b. Detecting unauthorized access points
- c. Detecting causes of interference on a WLAN
- d. WEP ICV error tracking
- e. Making Graphs and Alarms on 802.11 Data, including Signal Strength

This tool is known as \_\_\_\_\_.

- A. Kismet
- B. Absinthe
- C. NetStumbler
- D. THC-Scan

---

**Answer: C**

---

---

### Question: 13

---

John, a novice web user, makes a new E-mail account and keeps his password as "apple", his favorite fruit. John's password is vulnerable to which of the following password cracking attacks?

Each correct answer represents a complete solution. Choose all that apply.

- A. Brute Force attack
- B. Dictionary attack
- C. Rule based attack
- D. Hybrid attack

---

**Answer: A,B,D**

---

---

### Question: 14

---

Mark works as a Network Security Administrator for BlueWells Inc. The company has a Windowsbased network. Mark is giving a presentation on Network security threats to the newly recruited employees of the company. His presentation is about the External threats that the company recently faced in the past. Which of the following statements are true about external threats?

Each correct answer represents a complete solution. Choose three.

- A. These threats can be countered by implementing security controls on the perimeters of the

network, such as firewalls, which limit user access to the Internet.

B. These are the threats intended to flood a network with large volumes of access requests.

C. These are the threats that originate from outside an organization in which the attacker attempts to gain unauthorized access.

D. These are the threats that originate from within the organization.

---

**Answer: A,B,C**

---

---

### Question: 15

---

SSH is a network protocol that allows data to be exchanged between two networks using a secure channel. Which of the following encryption algorithms can be used by the SSH protocol?

Each correct answer represents a complete solution. Choose all that apply.

A. Blowfish

B. IDEA

C. DES

D. RC4

---

**Answer: A, B, C**

---

---

### Question: 16

---

Adam works as a Security Analyst for Umbrella Inc. He is performing real-time traffic analysis on IP networks using Snort. Adam is facing problems in analyzing intrusion data. Which of the following software combined with Snort can Adam use to get a visual representation of intrusion data?

Each correct answer represents a complete solution. Choose all that apply.

A. Basic Analysis and Security Engine (BASE)

B. sguil

C. KFSensor

D. OSSIM

---

**Answer: A, B, D**

---

---

### Question: 17

---

Mark works as a Network Security Administrator for BlueWells Inc. The company has a Windowsbased network. Mark is giving a presentation on Network security threats to the newly recruited employees of the company. His presentation is about the External threats that the company recently faced in the past. Which of the following statements are true about external threats?

Each correct answer represents a complete solution. Choose three.

A. These are the threats that originate from outside an organization in which the attacker attempts to gain unauthorized access.

B. These are the threats that originate from within the organization.

C. These are the threats intended to flood a network with large volumes of access requests.

D. These threats can be countered by implementing security controls on the perimeters of the network, such as firewalls, which limit user access to the Internet.

---

**Answer: A, C, D**

---

---

**Question: 18**

---

Which of the following file systems is designed by Sun Microsystems?

- A. NTFS
- B. CIFS
- C. ZFS
- D. ext2

---

**Answer: C**

---

---

**Question: 19**

---

You work as a Network Administrator for Tech Perfect Inc. The office network is configured as an IPv6 network. You have to configure a computer with the IPv6 address, which is equivalent to an IPv4 publicly routable address. Which of the following types of addresses will you choose?

- A. Site-local
- B. Global unicast
- C. Local-link
- D. Loopback

---

**Answer: B**

---

---

**Question: 20**

---

Which of the following is the default port for Simple Network Management Protocol (SNMP)?

- A. TCP port 110
- B. TCP port 25
- C. TCP port 80
- D. UDP port 161

---

**Answer: D**

---

## Thank You for trying GCIA PDF Demo

To Buy Latest GCIA Full Version Download visit link below

<https://www.certkillers.net/Exam/GCIA>

## Start Your GCIA Preparation

**[Limited Time Offer]** Use Coupon “CKNET” for Further discount on your purchase. Test your GCIA preparation with actual exam questions.

<https://www.certkillers.net>