Vendor:GIAC

Exam Code:GCFA

Exam Name:GIAC Certified Forensics Analyst

Version: Demo

QUESTION 1

Brutus is a password cracking tool that can be used to crack the following authentications:

HTTP (Basic Authentication)

HTTP (HTML Form/CGI)

POP3 (Post Office Protocol v3)

FTP (File Transfer Protocol)

SMB (Server Message Block)

Telnet

Which of the following attacks can be performed by Brutus for password cracking?

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

A. Replay attack

B. Dictionary attack

C. Man-in-the-middle attack

D. Hybrid attack

E. Brute force attack

Correct Answer: BDE

QUESTION 2

Which of the following is the process of comparing cryptographic hash functions of system executables and configuration files?

A. Spoofing

B. File integrity auditing

C. Reconnaissance

D. Shoulder surfing

Correct Answer: B

QUESTION 3

In which of the following access control models can a user not grant permissions to other users to see a copy of an object marked as secret that he has received, unless they have the appropriate permissions?

A. Discretionary Access Control (DAC)

B. Access Control List (ACL)

C. Mandatory Access Control (MAC)

D. Role Based Access Control (RBAC)

Correct Answer: C

QUESTION 4

You work as a Network Administrator for Net Perfect Inc. The company has a Windows Server 2008 network environment. The network is configured as a Windows Active Directory-based single forest single domain network. The network is configured on IP version 6 protocol. All the computers on the network are connected to a switch device. One day, users complain that they are unable to connect to a file server. You try to ping the client computers from the server, but the pinging fails. You try to ping the server\\'s own loopback address, but it fails to ping. You restart the server, but the problem persists.

What is the most likely cause?

A. The cable that connects the server to the switch is broken.

B. Automatic IP addressing is not working.

C. The switch device is not working.

D. The server is configured with unspecified IP address.

E. The server\\'s NIC is not working.

Correct Answer: E

QUESTION 5

Which of the following steps are generally followed in computer forensic examinations?

Each correct answer represents a complete solution. Choose three.

A. Encrypt

B. Acquire

C. Authenticate

D. Analyze

Correct Answer: BCD

QUESTION 6

Adam works as a Computer Hacking Forensic Investigator for a garment company in the United States. A project has been assigned to him to investigate a case of a disloyal employee who is suspected of stealing design of the garments, which belongs to the company and selling those garments of the same design under different brand name. Adam investigated that the company does not have any policy related to the copy of design of the garments. He also investigated that the trademark under which the employee is selling the garments is almost identical to the original trademark of the company. On the grounds of which of the following laws can the employee be prosecuted?

A. Trademark law

B. Cyber law

C. Copyright law

D. Espionage law

Correct Answer: A

QUESTION 7

Which of the following Acts enacted in United States amends Civil Rights Act of 1964, providing technical changes affecting the length of time allowed to challenge unlawful seniority provisions, to sue the federal government for discrimination and to bring age discrimination claims?

A. Sexual Predators Act

B. Civil Rights Act of 1991

C. PROTECT Act

D. The USA Patriot Act of 2001

Correct Answer: B

QUESTION 8

Which of the following file attributes are not available on a FAT32 partition?

Each correct answer represents a complete solution. Choose two.

A. Compression

B. Encryption

C. Read Only

D. Hidden

E. Archive

Correct Answer: AB

QUESTION 9

Which of the following Acts enacted in United States allows the FBI to issue National Security Letters (NSLs) to Internet service providers (ISPs) ordering them to disclose records about their customers?

A. Wiretap Act

B. Computer Fraud and Abuse Act

C. Economic Espionage Act of 1996

D. Electronic Communications Privacy Act of 1986

Correct Answer: D

QUESTION 10

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. Melissa

B. Tequila

C. Brain

D. I love you

Correct Answer: C

QUESTION 11

Which of the following command line tools are available in Helix Live acquisition tool on Windows? Each correct answer represents a complete solution. Choose all that apply.

A. .cab extractors

B. ipconfig

C. netstat

D. whois

Correct Answer: ABC

QUESTION 12

Which of the following tools are used to determine the hop counts of an IP packet? Each correct answer represents a complete solution. Choose two.

A. Netstat

B. TRACERT

C. IPCONFIG

D. Ping

Correct Answer: BD