Vendor: GIAC

Exam Code: GCIA

Exam Name: GIAC Certified Intrusion Analyst

Version: DEMO

QUESTION NO: 1

Andrew works as a System Administrator for ABC 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 NO: 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 NO: 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 NO: 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 NO: 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 NO: 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 com pany

Answer: A,B,D

QUESTION NO: 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 NO: 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 NO: 9

Peter works as a Technical Representative in a *CSIRT* for ABC 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, interne t traces

B. Volatile data, file slack, file system, registry, memory dumps, system state backup, interne t 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 NO: 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