DUMPS ARENA

GIAC Certified Perimeter Protection Analyst

GIAC GPPA

Version Demo

Total Demo Questions: 15

Total Premium Questions: 285

QUESTION NO: 1

Session splicing is an IDS evasion technique in which an attacker delivers data in multiple smallsized packets to the target computer. Hence, it becomes very difficult for an IDS to detect the attack signatures of such attacks.

Which of the following tools can be used to perform session splicing attacks?

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

A. Y.A.T.

B. Fragroute

C. Whisker

D. Nessus

ANSWER: C D

QUESTION NO: 2

Sam works as a Network Administrator for Gentech Inc. He has been assigned a project to develop the rules that define the IDP policy in the rulebase.

Which of the following will he define as the components of the IDP policy rule?

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

A. IDP Profiler

B. IDP rule notifications

C. IDP rule IP actions

D. IDP appliance deployment mode

ANSWER: B C

QUESTION NO: 3

Adam works as a professional Computer Hacking Forensic Investigator. He works with the local police. A project has been assigned to him to investigate an iPod, which was seized from a student of the high school. It is suspected that the explicit child pornography contents are stored in the iPod. Adam wants to investigate the iPod extensively.

Which of the following operating systems will Adam use to carry out his investigations in more extensive and elaborate manner?

A. Mac OS

B. Windows XP

C. MINIX 3

D. Linux

ANSWER: A

QUESTION NO: 4

Which of the following types of IP actions are supported by an IDP rulebase? (Choose three.)

A. Initiate rules of the rulebase

B. Notify

C. Drop/block session

D. Close connection

ANSWER: B C D

QUESTION NO: 5

Jain works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.abc.com. In order to do so, he performs the following steps of the preattack phase successfully:

- Information gathering
- Determination of network range
- Identification of active systems
- Location of open ports and applications

Now, which of the following tasks should he perform next?

A. Install a backdoor to log in remotely on the We-are-secure server.

B. Map the network of We-are-secure Inc.

C. Fingerprint the services running on the we-are-secure network.

D. Perform OS fingerprinting on the We-are-secure network.

ANSWER: D

QUESTION NO: 6

You want to create a binary log file using tcpdump.

Which of the following commands will you use?

A. tcpdump -d

B. tcpdump -B

C. tcpdump -dd

D. tcpdump -w

ANSWER: D

QUESTION NO: 7

Which of the following techniques correlates information found on multiple hard drives?

A. Live analysis

B. Gap analysis

C. Data analysis

D. Cross-drive analysis

ANSWER: D

QUESTION NO: 8

In which of the following CAATs (Computer Assisted Auditing Techniques) does an auditor perform tests on computer files and databases?

A. Parallel Simulation

B. Custom Audit Software (CAS)

C. Generalized Audit Software (GAS)

D. Test Data

ANSWER: C

QUESTION NO: 9

You work as a professional Computer Hacking Forensic Investigator for DataEnet Inc. You want to investigate e-mail information of an employee of the company. The suspected employee is using an online e-mail system such as Hotmail or Yahoo.

Which of the following folders on the local computer will you review to accomplish the task?

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

A. Temporary Internet Folder

B. History folder

C. Download folder

D. Cookies folder

ANSWER: A B D

QUESTION NO: 10

Which of the following devices is used to identify out-of-date software versions, applicable patches, system upgrades, etc?

A. Retinal scanner

B. Vulnerability scanner

C. Fingerprint reader

D. Smart card reader

ANSWER: B

QUESTION NO: 11

Which of the following are the types of intrusion detection systems?

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

A. Network intrusion detection system (NIDS)

B. Client-based intrusion detection system (CIDS)

C. Host-based intrusion detection system (HIDS)

D. Server-based intrusion detection system (SIDS)

ANSWER: A C

QUESTION NO: 12

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. John wants to redirect all TCP port 80 traffic to UDP port 40, so that he can bypass the firewall of the We-are-secure server.

Which of the following tools will John use to accomplish his task?

A. PsList

B. Fpipe

C. Cain

D. PsExec

ANSWER: B

QUESTION NO: 13

Secure Shell (SSH) is a network protocol that allows data to be exchanged using a secure channel between two networked devices.

Which of the following features are supported by Secure Shell?

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

A. SSH uses the client-server model.

B. SSH can transfer files using the associated HTTP or FTP protocols.

C. SSH is typically used to log into a remote machine and execute commands, but it also supports tunneling, forwarding TCP ports and X11 connections.

D. SSH uses public-key cryptography to authenticate the remote computer and allow the remote computer to authenticate the user, if necessary.

ANSWER: A C D

QUESTION NO: 14

You are a professional Computer Hacking forensic investigator. You have been called to collect the evidences of Buffer Overflows or Cookie snooping attack.

Which of the following logs will you review to accomplish the task?

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

A. Event logs

B. System logs

C. Web server logs

D. Program logs

ANSWER: A B D

QUESTION NO: 15

Which of the following is the default port for POP3?

A. 80

B. 25

C. 21

D. 110

ANSWER: D