GIAC Certified Firewall Analyst

GIAC GCFW

Version Demo

Total Demo Questions: 15

Total Premium Questions: 391

Topic Break Down

Topic	No. of Questions
Topic 1, Volume A	143
Topic 2, Volume B	248
Total	391

QUESTION NO: 1

Host-based IDS (HIDS) is an Intrusion Detection System that runs on the system to be monitored.

HIDS monitors only the data that it is directed to, or originates from the system on which HIDS is installed. Besides monitoring network traffic for detecting attacks, it can also monitor other parameters of the system such as running processes, file system access and integrity, and user logins for identifying malicious activities. Which of the following tools are examples of HIDS?

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

A. Legion

B. BlackIce Defender

C. Tripwire

D. HPing

ANSWER: B C

QUESTION NO: 2

Which of the following hexadecimal values in the boot field in the configuration register loads the first IOS file found in Flash memory?

A. 0

B. 1

C. F

D. 2

ANSWER: B

QUESTION NO: 3

Passive OS fingerprinting (POSFP) is configured in an organization's network in order to improve the alert output by reporting some information. Which of the following information does it include?

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

A. Source of the OS identification

B. Relevancy to the victim in the alert

C. Network security device

D. Victim OS

ANSWER: A B D

QUESTION NO: 4

You work as the Security Administrator for Prodotxiss Inc. You want to ensure the security of your Wi- Fi enterprise network against the wireless snooping attacks. Which of the following measures will you take over the site network devices of the network?

A. Download and install new firmware patch for the router.

B. Apply firewalls at appropriate spots.

C. Apply a standard ACL on the router.

D. Disable the SSID broadcast feature of the router.

ANSWER: D

QUESTION NO: 5

You work as a Network Administrator for Net Perfect Inc. The company has a TCP/IP network. You have been assigned a task to configure a stateful packet filtering firewall to secure the network of the company. You are encountering some problems while configuring the stateful packet filtering firewall. Which of the following can be the reasons for your problems?

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

A. It contains additional overhead of maintaining a state table.

B. It has to open up a large range of ports to allow communication.

C. It is complex to configure.

D. It has limited logging capabilities.

ANSWER: A C

QUESTION NO: 6

A firewall is a combination of hardware and software, used to provide security to a network.

It is used to protect an internal network or intranet against unauthorized access from the Internet or other outside networks. It restricts inbound and outbound access and can analyze all traffic between an internal network and the Internet. Users can configure a firewall to pass or block packets from specific IP addresses and ports. Which of the following tools works as a firewall for the Linux 2.4 kernel?

A. IPChains

B. OpenSSH

C. Stunnel

D. IPTables

ANSWER: D

QUESTION NO: 7

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

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

A. Client-based intrusion detection system (CIDS)

B. Network intrusion detection system (NIDS)

C. Server-based intrusion detection system (SIDS)

D. Host-based intrusion detection system (HIDS)

ANSWER: B D

QUESTION NO: 8

You work as a Firewall Analyst in the Tech Perfect Inc. The company has a Linux-based environment. You have installed and configured netfilter/iptables on all computer systems.

What are the main features of netfilter/iptables?

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

A. It includes many plug-ins or modules in 'patch-o-matic' repository

B. It includes a number of layers of API's for third party extensions

C. It offers stateless and stateful packet filtering with both IPv4 and IPv6 addressing schemes

D. It provides network address and port address translations with both IPv4 and IPv6 addressing schemes

ANSWER: A B C

QUESTION NO: 9

Which of the following vulnerability scanners detects vulnerabilities by actually performing attacks?

A. Network enumerator

B. Computer worm

C. Port scanner

D. Web application security scanner

ANSWER: D

QUESTION NO: 10

TCP/IP stack fingerprinting is the passive collection of configuration attributes from a remote device during standard layer 4 network communications. The combination of parameters may then be used to infer the remote operating system (OS fingerprinting), or incorporated into a device fingerprint. Which of the following Nmap switches can be used to perform TCP/IP stack fingerprinting?

A. nmap -O -p

B. nmap -sT

C. nmap -sU -p

D. nmap -sS

ANSWER: A

QUESTION NO: 11

A packet filtering firewall inspects each packet passing through the network and accepts or rejects it based on user-defined rules. Based on which of the following information are these rules set to filter the packets?

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

A. Layer 4 protocol information

B. Actual data in the packet

C. Interface of sent or received traffic

D. Source and destination Layer 3 address

ANSWER: A C D

QUESTION NO: 12

Which of the following tools is used to analyze the files produced by several popular packetcapture programs such as tcpdump, WinDump, Wireshark, and EtherPeek?

A. Fpipe

B. tcptrace

C. tcptraceroute

D. Sniffer

ANSWER: B

QUESTION NO: 13

John works as a professional Ethical Hacker. He has been assigned a project for testing the security of www.we-are-secure.com. He wants to corrupt an IDS signature database so that performing attacks on the server is made easy and he can observe the flaws in the We-are-secure server. To perform his task, he first of all sends a virus that continuously changes its signature to avoid detection from IDS. Since the new signature of the virus does not match the old signature, which is entered in the IDS signature database, IDS becomes unable to point out the malicious virus. Which of the following IDS evasion attacks is John performing?

A. Session splicing attack

B. Evasion attack

C. Polymorphic shell code attack

D. Insertion attack

ANSWER: C

QUESTION NO: 14

Which of the following statements are true about an IPv6 network?

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

A. It uses longer subnet masks than those used in IPv4.

B. It increases the number of available IP addresses.

C. For interoperability, IPv4 addresses use the last 32 bits of IPv6 addresses.

D. It provides improved authentication and security.

E. It uses 128-bit addresses.

ANSWER: B C D E

QUESTION NO: 15

Which of the following is used for debugging the network setup itself by determining whether all necessary routing is occurring properly, allowing the user to further isolate the source of a problem?

A. iptables

B. WinPcap

C. Netfilter

D. tcpdump

ANSWER: D