# Ourexam

**Higher Quality Better Service!**

We offer free update service for one year

Http://www.ourexam.com

**Exam** : **GCFW**

**Title** : GIAC Certified Firewall Analyst

**Version** : Demo

1.Which of the following can be monitored by using the host intrusion detection system (HIDS)?
Each correct answer represents a complete solution. Choose two.
A. Computer performance
B. File system integrity
C. Storage space on computers
D. System files
**Answer:** B,D

2.Which of the following components are usually found in an Intrusion detection system (IDS).?
Each correct answer represents a complete solution. Choose two.
A. Firewall
B. Console
C. Gateway
D. Modem
E. Sensor
**Answer:** B,E

3.Which of the following are the countermeasures against a man-in-the-middle attack?
Each correct answer represents a complete solution. Choose all that apply.
A. Using Secret keys for authentication.
B. Using public key infrastructure authentication.
C. Using Off-channel verification.
D. Using basic authentication.
**Answer:** A,B,C

4.Which of the following ICMPv6 neighbor discovery messages is sent by hosts to request an immediate router advertisement, instead of waiting for the next scheduled advertisement?
A. Router Advertisement
B. Neighbor Advertisement
C. Router Solicitation
D. Neighbor Solicitation
**Answer:** C

5.Which of the following statements about the traceroute utility are true?
Each correct answer represents a complete solution. Choose all that apply.
A. It generates a buffer overflow exploit by transforming an attack shell code so that the new attack shell code cannot be recognized by any Intrusion Detection Systems.
B. It uses ICMP echo packets to display the Fully Qualified Domain Name (FQDN) and the IP address of each gateway along the route to the remote host.
C. It records the time taken for a round trip for each packet at each router.
D. It is an online tool that performs polymorphic shell code attacks.
**Answer:** B,C

6.Which of the following intrusion detection systems (IDS) monitors network traffic and compares it

against an established baseline?
A. Network-based
B. File-based
C. Signature-based
D. Anomaly-based
**Answer:** D

7.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 security mechanisms for the network of the company. You have decided to configure a packet filtering firewall. Which of the following may be the reasons that made you choose a packet filtering firewall as a security mechanism?
Each correct answer represents a complete solution. Choose all that apply.
A. It makes security transparent to end-users which provide easy use of the client application s.
B. It prevents application-layer attacks.
C. It is easy to install packet filtering firewalls in comparison to the other network security sol utions.
D. It easily matches most of the fields in Layer 3 packets and Layer 4 segment headers, and thus, provides a lot of flexibility in implementing security policies.
**Answer:** A,C,D

8.Which of the following types of Intrusion Detection Systems consists of an agent on a host that identifies intrusions by analyzing system calls, application logs, file-system modifications (binaries, password files, capability/acl databases) and other host activities and state?
A. HIDS
B. NIDS
C. APIDS
D. PIDS
**Answer:** A

9.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

10.Adam works as a Security Administrator for Umbrella Inc. A project has been assigned to him to secure access to the network of the company from all possible entry points. He segmented the network into several subnets and installed firewalls all over the network. He has placed very stringent rules on all the firewalls, blocking everything in and out except the ports that must be used. He does need to have port 80 open since his company hosts a website that must be accessed from the Internet. Adam is still worried about the programs like Hping2 that can get into a network through covert channels.

Which of the following is the most effective way to protect the network of the company from an attacker using Hping2 to scan his internal network?
A. Block ICMP type 13 messages
B. Block ICMP type 3 messages
C. Block all outgoing traffic on port 21
D. Block all outgoing traffic on port 53
**Answer:** A

11.You work as a Security Manger for Tech Perfect Inc. The company has a Windows-based network. You want to scroll real-time network traffic to a command console in a readable format. Which of the following command line utilities will you use to accomplish the task?
A. WinPcap
B. WinDump
C. iptables
D. libpcap
**Answer:** B

12.Which of the following is the default port for POP3?
A. 25
B. 21
C. 80
D. 110
**Answer:** B

13.A scenario involves a pool of users with private IP addresses who need to access the Internet; however, the company has a limited number of IP addresses and needs to ensure users occupy only one public IP address.
Which technology is used to allow a pool of users to share one global IP address for Internet access?
A. Port Address Translation
B. Per-user Address Translation
C. Pool Address Translation
D. Private Address Translation
**Answer:** A

14.Which of the following protocols does IPsec use to perform various security functions in the network? Each correct answer represents a complete solution. Choose all that apply.
A. Skinny Client Control Protocol
B. Authentication Header
C. Encapsulating Security Payload
D. Internet Key Exchange
**Answer:** B,C,D

15.Address Resolution Protocol (ARP) spoofing, also known as ARP poisoning or ARP Poison Routing (APR), is a technique used to attack an Ethernet wired or wireless network. ARP spoofing may allow an

attacker to sniff data frames on a local area network (LAN), modify the traffic, or stop the traffic altogether. The principle of ARP spoofing is to send fake ARP messages to an Ethernet LAN.
What steps can be used as a countermeasure of ARP spoofing?
Each correct answer represents a complete solution. Choose all that apply.
A. Using ARP Guard utility
B. Using smash guard utility
C. Using static ARP entries on servers, workstation and routers
D. Using ARP watch utility
E. Using IDS Sensors to check continually for large amount of ARP traffic on local subnets
**Answer:** A,C,D,E

16.Which of the following IDs is used to reassemble the fragments of a datagram at the destination point?
A. IP identification number
B. SSID
C. MAK ID
D. IP address
**Answer:** A

17.You work as a Network Architect for Tech Perfect Inc. The company has a corporate LAN network. You will have to perform the following tasks:
l Limit events that occur from security threats such as viruses, worms, and spyware.
l Restrict access to the network based on identity or security posture.
Which of the following services will you deploy in the network to accomplish the tasks?
A. NetFlow
B. Protocol-Independent Multicast
C. Network Admission Control
D. Firewall Service Module
**Answer:** C

18.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, internet traces, registry, memory dumps, system state backup, file system
B. Volatile data, file slack, registry, memory dumps, file system, system state backup, interne t traces
C. Volatile data, file slack, file system, registry, memory dumps, system state backup, interne t traces
D. Volatile data, file slack, registry, system state backup, internet traces, file system, memory dumps
**Answer:** C

19.Which of the following statements are true about an IDP rule base notification?
A. It can be defined as reusable logical entities that the user can apply to the rules.
B. When an action is performed, a notification defines how to log information.

C. It is used to specify the type of network traffic that has to be monitored for attacks.
D. It directs an IDP to drop or close the connection.
**Answer:** B

20.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

21.Which of the following commands configures a router to encrypt all passwords entered after the command has been executed, as well as all passwords already on the running configuration?
A. no service password-encryption
B. enable password-encryption
C. no enable password-encryption
D. service password-encryption
**Answer:** D

22.Which of the following devices is used to identify out-of-date software versions, applicable patches, system upgrades, etc?
A. Retinal scanner
B. Fingerprint reader
C. Smart card reader
D. Vulnerability scanner
**Answer:** D

23.Which of the following proxy servers is placed anonymously between the client and remote server and handles all of the traffic from the client?
A. Web proxy server
B. Open proxy server
C. Forced proxy server
D. Caching proxy server
**Answer:** C

24.Which of the following algorithms is used as a default algorithm for ESP extension header in IPv6?
A. Electronic Codebook (ECB) Mode
B. Cipher Block Chaining (CBC) Mode

C. Propagating Cipher Block Chaining (PCBC) Mode
D. Cipher Feedback (CFB) Mode
**Answer:** B

25.Which of the following limits the number of packets seen by tcpdump?
A. BPF-based filter
B. Recipient filtering
C. Sender filtering
D. IFilters
**Answer:** A

26.Which of the following are the reasons that network administrators use Access Control Lists?
Each correct answer represents a complete solution. Choose two.
A. Encrypting data to be routed
B. Removing weak user password
C. Controlling VTY access into a router
D. Filtering traffic as it passes through a router
**Answer:** C,D

27.Choose the best explanation for the resulting error when entering the command below.

```
RouterA(config)#access-list 10 permit tcp host 192.168.100.100 host 10.10.100.1 eq 23
                                        ^
% Invalid input detected at '^' marker.
```

A. The command is attempting to create a standard access list with extended access list param eters.
B. The ACL commands should be entered from the (config-router) configuration mode.
C. The wildcard mask is not provided for the source and destination addresses.
D. The port number given does not correspond with the proper transport protocol.
**Answer:** A

28.Which of the following is an attack with IP fragments that cannot be reassembled?
A. Dictionary attack
B. Smurf attack
C. Teardrop attack
D. Password guessing attack
**Answer:** C

29.WinDump, tcpdump, and Wireshark specify which fields of information libpcap should record.
Which of the following filters do they use in order to accomplish the task?
A. Berkeley Packet Filter
B. IM filter
C. Web filter
D. FIR filter
**Answer:** A

30.Which of the following number ranges is used for the IP Standard ACL?

A. 100-199

B. 1000-1099

C. 600-699

D. 1-99

**Answer:** D