GIAC

Exam GCFW

GIAC Certified Firewall Analyst

Version: 6.1

[Total Questions: 391]

Topic break down

Topic	No. of Questions
Topic 1: Volume A	144
Topic 2: Volume B	247

Topic 1, Volume A

Question No : 1 - (Topic 1)

The simplest form of a firewall is a packet filtering firewall. Typically a router works as a packet-filtering firewall and has the capability to filter on some of the contents of packets. On which of the following layers of the OSI reference model do these routers filter information?

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

A. Data Link layer
B. Transport layer
C. Network layer
D. Physical layer

Answer: B,C

Question No : 2 - (Topic 1)

Which of the following can be applied as countermeasures against DDoS attacks?

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

A. Using the network-ingress filtering
B. Limiting the amount of network bandwidth
C. Blocking IP address
D. Using Intrusion detection systems
E. Using LM hashes for passwords

Answer: A,B,C,D

Question No : 3 - (Topic 1)

You want to create a binary log file using tcpdump. Which of the following commands will you use?

A. tcpdump -B
B. tcpdump -w

C. tcpdump -dd
D. tcpdump -d

Answer: B

Question No : 4 - (Topic 1)

Which of the following statements are true about the Network Honeypot rulebase?

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

A. Its operation setting toggles between the network honeypot on and off.
B. It does not support any IP action.
C. It is used to detect reconnoitering activities.
D. Its rules are triggered when a source IP address sends a connection request to the destination IP address and service specified in the rule.

Answer: A,C,D

Question No : 5 - (Topic 1)

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 has limited logging capabilities.
B. It has to open up a large range of ports to allow communication.
C. It is complex to configure.
D. It contains additional overhead of maintaining a state table.

Answer: C,D

Question No : 6 - (Topic 1)

You are implementing a host based intrusion detection system on your web server. You feel that the best way to monitor the web server is to find your baseline of activity (connections, traffic, etc.) and to monitor for conditions above that baseline. This type of IDS is called _____.

A. Reactive IDS
B. Signature Based
C. Passive IDS
D. Anomaly Based

Answer: D

Question No : 7 - (Topic 1)

You work as a Network Administrator for BlueTech Inc. You want to configure Snort as an IDS for your company's wireless network, but you are concerned that Snort does not support all types of traffic. What traffic does Snort support?

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

A. UDP
B. TCP
C. IP
D. ICMP

Answer: A,B,C,D

Question No : 8 - (Topic 1)

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

Question No : 9 - (Topic 1)

A remote-access VPN offers secured and encrypted connections between mobile or remote users and their corporate network across public networks. Which of the following does the remote-access VPN use for offering these types of connections?

Each correct answer represents a complete solution. Choose two.

A. SSL
B. IPsec
C. TLS
D. SSH

Answer: A,B

Question No : 10 - (Topic 1)

Which of the following *ports* cannot be used to access the router from a computer?

A. Aux port
B. Console port
C. Serial port
D. Vty

Answer: C

Question No : 11 - (Topic 1)

Which of the following *Wireless LAN* standard devices is least affected by interference from domestic appliances such as microwave ovens?

A. 802.11b
B. 802.11
C. 802.11a
D. 802.11g

Answer: C

Question No : 12 - (Topic 1)

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 : 13 - (Topic 1)

Which of the following are open-source vulnerability scanners?

A. NetRecon
B. Hackbot
C. Nessus
D. Nikto

Answer: B,C,D

Question No : 14 - (Topic 1)

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He has successfully completed the following steps of the preattack phase:

l Information gathering

l Determining network range

l Identifying active machines

l Finding open ports and applications

l OS fingerprinting

l Fingerprinting services

Now John wants to perform network mapping of the We-are-secure network. Which of the following tools can he use to accomplish his task?

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

A. Ettercap
B. Traceroute
C. NeoTrace
D. Cheops

Answer: B,C,D

Question No : 15 - (Topic 1)

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 : 16 - (Topic 1)

Which of the following terms is used to represent *IPv6* addresses?

A. Colon-dot
B. Hexadecimal-dot notation
C. Colon-hexadecimal
D. Dot notation

Answer: C

Question No : 17 - (Topic 1)

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 : 18 - (Topic 1)

Which of the following Intrusion Detection Systems (IDS) is used to monitor rogue access points and the use of wireless attack tools?

A. LogIDS 1.0
B. WIDS
C. Snort 2.1.0
D. NFR security

Answer: B

Question No : 19 - (Topic 1)

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

Question No : 20 - (Topic 1)

In which of the following IDS evasion techniques does an attacker deliver data in multiple small sized packets, which makes it very difficult for an IDS to detect the attack signatures of such attacks?

A. Fragmentation overwrite
B. Fragmentation overlap
C. Insertion
D. Session splicing

Answer: D

Question No : 21 - (Topic 1)

You work as a Network Administrator for Tech Perfect Inc. The company has a TCP/IP-based network.

A firewall has been configured on the network. You configure a filter on the router. You verify that *SMTP* operations have stopped after the recent configuration. Which of the following ports will you have to open on the router to resolve the issue?

A. 25
B. 80
C. 20
D. 21

Answer: A

Question No : 22 - (Topic 1)

John works as the Security Manager for PassGuide Inc. He wants to create the Profiler database that stores information about the network activity at Layer 3, Layer 4, and Layer 7. Which of the following will he use to accomplish the task?

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

A. Ignore connection
B. Session creation
C. Protocol contexts

D. Session teardown

Answer: B,C,D

Question No : 23 - (Topic 1)

Which of the following types of IP actions are supported by an IDP rulebase?

A. Initiate rules of the rulebase
B. Drop/block session
C. Close connection
D. Notify

Answer: B,C,D

Question No : 24 - (Topic 1)

An organization has more than a couple of external business, and exchanges dynamic routing information with the external business partners. The organization wants to terminate all routing from a partner at an edge router, preferably receiving only summary routes from the partner. Which of the following will be used to change all partner addresses on traffic into a range of locally assigned addresses?

A. ACL
B. IPsec
C. Firewall
D. NAT

Answer: D

Question No : 25 - (Topic 1)

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

Question No : 26 - (Topic 1)

You have to ensure that your Cisco Router is only accessible via telnet and ssh from the following hosts and subnets:

10.10.2.103

10.10.0.0/24

Which of the following sets of commands will you use to accomplish the task?

A. access-list 10 permit host 10.10.2.103
access-list 10 permit 10.10.0.0 0.0.0.255
access-list 10 deny any
line vty 0 4
access-class 10 in
B. access-list 10 permit 10.10.2.103
access-list 10 permit 10.10.0.0 0.0.0.255
access-list 10 deny any
line vty 0 4
access-group 10 in
C. access-list 10 permit host 10.10.2.103
access-list 10 permit 10.10.0.0 0.0.0.255
access-list 10 deny any
line vty 0 4
access-class 10 out
D. access-list 10 permit host 10.10.2.103
access-list 11 permit host 10.10.0.0 255.255.255.0
access-list 12 deny any
line vty 0 4
access-group 10, 11, 12 in

Answer: A

Question No : 27 - (Topic 1)

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

Question No : 28 - (Topic 1)

Jacob is worried about sniffing attacks and wants to protect his SMTP transmissions from this attack. What can he do to accomplish this?

A. Use an SSL certificate.
B. Use a proxy server.
C. Use a firewall.
D. Use EFS.

Answer: A

Question No : 29 - (Topic 1)

Which of the following tools is an open source network intrusion prevention and detection system that operates as a network sniffer and logs activities of the network that is matched with the predefined signatures?

A. KisMAC
B. Dsniff
C. Snort
D. Kismet

Answer: C,D

Question No : 30 - (Topic 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

Question No : 31 - (Topic 1)

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

Question No : 32 - (Topic 1)

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

Question No : 33 - (Topic 1)

You work as a Network Troubleshooter for PassGuide Inc. You want to tunnel the IPv6 traffic across an IPv4 supporting portion of the company's network. You are using the interface configuration mode for the tunnel. Which of the following IP addresses will you enter after the tunnel source command?

A. The IPv4 address assigned to the local interface on which the tunnel is built
B. The IPv4 address assigned to the remote interface on which the tunnel is built
C. The IPv6 address assigned to the local tunnel interface
D. The IPv6 address assigned to the remote tunnel interface

Answer: A

Question No : 34 - (Topic 1)

Which of the following attacking methods allows the bypassing of access control lists on servers or routers, either hiding a computer on a network or allowing it to impersonate another computer by changing the Media Access Control address?

A. IP address spoofing
B. ARP spoofing