Vendor: GIAC

Exam Code: GCFW

Exam Name: GIAC Certified Firewall Analyst

Version: Demo

QUESTION NO: 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
Explanation:

QUESTION NO: 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
Explanation:

QUESTION NO: 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
Explanation:

QUESTION NO: 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
Explanation:

QUESTION NO: 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
Explanation:

QUESTION NO: 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
Explanation:

QUESTION NO: 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
Explanation:

QUESTION NO: 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
Explanation:

QUESTION NO: 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
Explanation:

QUESTION NO: 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
Explanation:

QUESTION NO: 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
Explanation:

QUESTION NO: 12

Which of the following is the default port for *POP3*?

A. 25
B. 21
C. 80
D. 110

Answer: B
Explanation:

QUESTION NO: 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
Explanation:

QUESTION NO: 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

Explanation:

QUESTION NO: 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

Explanation:

QUESTION NO: 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

Explanation:

QUESTION NO: 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
Explanation:

QUESTION NO: 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
Explanation:

QUESTION NO: 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

Explanation:

QUESTION NO: 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

Explanation:

QUESTION NO: 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

Explanation:

QUESTION NO: 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
Explanation:

QUESTION NO: 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
Explanation:

QUESTION NO: 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
Explanation:

QUESTION NO: 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
Explanation:

QUESTION NO: 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
Explanation:

QUESTION NO: 27

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

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
Explanation:

QUESTION NO: 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
Explanation:

QUESTION NO: 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
Explanation:

QUESTION NO: 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
Explanation:

QUESTION NO: 31

Adam has installed and configured his wireless network. He has enabled numerous security features such as changing the default SSID, enabling WPA encryption, and enabling MAC filtering on his wireless router. Adam notices that when he uses his wireless connection, the speed is sometimes 16 Mbps and sometimes it is only 8 Mbps or less. Adam connects to the management utility wireless router and finds out that a machine with an unfamiliar name is connected through his wireless connection. Paul checks the router's logs and notices that the unfamiliar machine has

the same MAC address as his laptop.

Which of the following attacks has been occurred on the wireless network of Adam?

A. DNS cache poisoning
B. ARP spoofing
C. MAC spoofing
D. NAT spoofing

Answer: C
Explanation:

QUESTION NO: 32

Which of the following attacks sends false ICMP packets in an attempt to cripple a system using random fake Internet source addresses?

A. Land attack
B. SYN attack
C. Replay attack
D. Twinge attack

Answer: D
Explanation:

QUESTION NO: 33

This is a Windows-based tool that is used for the detection of wireless LANs using the IEEE 802.11a, 802.11b, and 802.11g standards. The main features of these tools are as follows:

l It displays the signal strength of a wireless network, MAC address, SSID, channel details, etc.

l It is commonly used for the following purposes:

a. War driving

b. Detecting unauthorized access points

c. Detecting causes of interference on a WLAN

d. WEP ICV error tracking

e. Making Graphs and Alarms on 802.11 Data, including Signal Strength

This tool is known as _____.

A. NetStumbler
B. Kismet
C. THC-Scan
D. Absinthe

Answer: A
Explanation:

QUESTION NO: 34

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. Install a DMZ firewall
B. Enable verbose logging on the firewall
C. Install a host-based IDS
D. Install a network-based IDS

Answer: D
Explanation:

QUESTION NO: 35

You are implementing passive OS fingerprinting in a network. Which of the following aspects are required to be configured there?

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

A. Edit signature vulnerable OS lists.
B. Limit the attack relevance rating calculation to a specific IP address range.
C. Define event action rules filters using the OS relevancy value of the target.
D. Enable passive analysis.
E. Define and import OS mappings.

Answer: A,B,C,E
Explanation:

QUESTION NO: 36

You work as a Network Administrator for NetTech Inc. You want to prevent your network from Ping flood attacks. Which of the following protocols will you block to accomplish this task?

A. IP
B. PPP
C. ICMP
D. FTP

Answer: C
Explanation:

QUESTION NO: 37

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
Explanation:

QUESTION NO: 38

Which of the following firewall types operates at the Network layer of the OSI model and can filter data by port, interface address, source address, and destination address?

A. Proxy server
B. Application gateway
C. Packet Filtering
D. Circuit-level gateway

Answer: C
Explanation:

QUESTION NO: 39

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 IP actions
C. IDP appliance deployment mode
D. IDP rule notifications

Answer: B,D

Explanation:

QUESTION NO: 40

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

Explanation:

QUESTION NO: 41

When client data is encapsulated into an LWAPP header, the wireless LAN controller improves the coverage areas. Which information does the wireless LAN controller check?

Each correct answer represents a part of the solution. Choose two.

A. CCA
B. SNR
C. WCS
D. RSSI

Answer: B,D

Explanation:

QUESTION NO: 42

Which of the following IPv4 fields become obsolete while removing the hop-by-hop segmentation (fragmentation) procedure from the IP header?

Each correct answer represents a part of the solution. Choose three.

A. Fragment Offset field
B. Datagram Length field
C. Flags field
D. Datagram Identification Number field

Answer: A,C,D
Explanation:

QUESTION NO: 43

Distributed Checksum Clearinghouse (DCC) is a hash sharing method of spam email detection.

Which of the following protocols does the DCC use?

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

Answer: B
Explanation:

QUESTION NO: 44

You are the Network Administrator for a college. Wireless access is widely used at the college. You want the most secure wireless connections you can have. Which of the following would you use?

A. WEP2
B. WPA
C. WPA2
D. WEP

Answer: C
Explanation:

QUESTION NO: 45

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

Explanation:

QUESTION NO: 46 CORRECT TEXT

Fill in the blank with appropriate address translation type.

A_____performs translation of one IP address to a different one automatically. It requires manually defining two sets of addresses on the address translation device (probably a router). One set defines which inside addresses are allowed to be translated, and the other defines what these addresses are to be translated to.

Answer: Dynamic NAT

QUESTION NO: 47

Which of the following tools is described below?

It is a set of tools that are used for sniffing passwords, e-mail, and HTTP traffic. Some of its tools include arpredirect, macof, tcpkill, tcpnice, filesnarf, and mailsnarf. It is highly effective for sniffing both switched and shared networks. It uses the arpredirect and macof tools for switching across switched networks. It can also be used to capture authentication information for FTP, telnet, SMTP, HTTP, POP, NNTP, IMAP, etc.

A. Cain
B. Libnids
C. Dsniff
D. LIDS

Answer: C

Explanation:

QUESTION NO: 48

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
Explanation:

QUESTION NO: 49

In which of the following conditions is the SYN Protector rule base activated in passive mode?

A. When the number of SYN packets per second is equal to 13,425 (default)
B. Only when the number of SYN packets per second is equal to the sum of the lower SYNs-persecond threshold and the upper SYNs-per-second threshold
C. When the number of SYN packets per second is smaller than the sum of the lower SYNs-persecond threshold and the upper SYNs-per-second threshold
D. When the number of SYN packets per second is greater than the sum of the lower SYNs-persecond threshold and the upper SYNs-per-second threshold

Answer: D
Explanation:

QUESTION NO: 50

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

Explanation:

QUESTION NO: 51

Which of the following is a maintenance protocol that permits routers and host computers to swap basic control information when data is sent from one computer to another?

A. ICMP
B. SNMP
C. IGMP
D. BGP

Answer: A
Explanation:

QUESTION NO: 52

Which of the following Denial-of-Service (DoS) attacks employ IP fragmentation mechanism?

Each correct answer represents a complete solution. Choose two.

A. Ping of Death attack
B. SYN flood attack
C. Teardrop attack
D. Land attack

Answer: A,C
Explanation:

QUESTION NO: 53

Adam works as a professional Computer Hacking Forensic Investigator, a project has been assigned to him to investigate and examine files present on suspect's computer. Adam uses a tool with the help of which he can examine recovered deleted files, fragmented files, and other corrupted data. He can also examine the data, which was captured from the network, and access the physical RAM, and any processes running in virtual memory with the help of this tool. Which of the following tools is Adam using?

A. Evidor
B. WinHex
C. Vedit
D. HxD

Answer: B

Explanation:

QUESTION NO: 54

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. Victim OS
C. Network security device
D. Relevancy to the victim in the alert

Answer: A,B,D

Explanation:

QUESTION NO: 55

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. Linux
C. Windows XP
D. MINIX 3

Answer: A

Explanation:

QUESTION NO: 56

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
Explanation:

QUESTION NO: 57

Which of the following types of firewall ensures that the packets are part of the established session?

A. Application-level firewall
B. Switch-level firewall
C. Stateful inspection firewall
D. Circuit-level firewall

Answer: C
Explanation:

QUESTION NO: 58

Which of the following types of audit constructs a risk profile for existing and new projects?

A. Innovative comparison audit
B. Client/Server, Telecommunications, Intranets, and Extranets audits
C. Technological position audit
D. Technological innovation process audit

Answer: D
Explanation:

QUESTION NO: 59

Which of the following IPv4 to IPv6 transition methods uses encapsulation of IPv6 packets to traverse IPv4 networks?

A. Stack
B. Translation

C. Tunneling
D. Dual-stack

Answer: C
Explanation:

QUESTION NO: 60

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
Explanation:

QUESTION NO: 61

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He wants to send malicious data packets in such a manner that one packet fragment overlaps data from a previous fragment so that he can perform IDS evasion on the We-are-secure server and execute malicious data. Which of the following tools can he use to accomplish the task?

A. Hunt
B. Ettercap
C. Alchemy Remote Executor
D. Mendax

Answer: D
Explanation:

QUESTION NO: 62

Which of the following tools performs comprehensive tests against web servers for multiple items, including over 6100 potentially dangerous files/CGIs?

A. Nikto
B. Sniffer

C. Snort
D. Dsniff

Answer: A
Explanation:

QUESTION NO: 63

Which of the following intrusion detection systems (IDS) produces the false alarm because of the abnormal behavior of users and network?

A. Application protocol-based intrusion detection system (APIDS)
B. Network intrusion detection system (NIDS)
C. Protocol-based intrusion detection system (PIDS)
D. Host-based intrusion detection system (HIDS)

Answer: D
Explanation:

QUESTION NO: 64

On which of the following interfaces of the router is the *clock rate* command used?

A. DCE
B. ETHERNET
C. VIRTUAL LINE VTY
D. DTE

Answer: A
Explanation:

QUESTION NO: 65

A company named Tech Perfect Inc. has a TCP/IP based network. An IPS sensor is deployed in the network and configured to operate in promiscuous mode. IP blocking functionality works there in order to stop traffic from an attacking host and it helps in analyzing what happens in the network.

The management wants to initiate a persistent connection with the managed devices until the block is removed. Which of the following will you configure in the network to accomplish the task?

A. Access Control List

B. Firewall
C. Network Admission Control
D. Virtual LAN

Answer: C
Explanation:

QUESTION NO: 66

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
Explanation:

QUESTION NO: 67

In which of the following situations does legal and authorized traffic cause an intrusion detection system (IDS) to generate an alert and slow down performance?

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

A. False alert
B. False illusion
C. False generation
D. False positives

Answer: A,D
Explanation:

QUESTION NO: 68

Mark works as a Network Security Administrator for BlueWells Inc. The company has a Windowsbased network. Mark is giving a presentation on Network security threats to the newly recruited employees of the company. His presentation is about the External threats that the company recently faced in the past. Which of the following statements are true about external threats?

Each correct answer represents a complete solution. Choose three.

A. These are the threats that originate from within the organization.
B. These are the threats that originate from outside an organization in which the attacker attempts to gain unauthorized access.
C. These threats can be countered by implementing security controls on the perimeters of the network, such as firewalls, which limit user access to the Internet.
D. These are the threats intended to flood a network with large volumes of access requests.

Answer: B,C,D
Explanation:

QUESTION NO: 69

Which of the following protocols is used with a tunneling protocol to provide security?

A. EAP
B. FTP
C. IPX/SPX
D. IPSec

Answer: D
Explanation:

QUESTION NO: 70

You work as a Network Administrator for Tech Perfect Inc. You are required to verify security policies configured in the company's networks. Which of the following applications will you use to accomplish the task?

A. Network enumerator
B. Web application security scanner
C. Computer worm
D. Port scanner

Answer: D
Explanation:

QUESTION NO: 71

You are configuring a public access wireless connection. Which of the following is the best way to

secure this connection?

A. Not broadcasting SSID
B. Using WPA encryption
C. Implementing anti virus
D. Using MAC filtering

Answer: B
Explanation:

QUESTION NO: 72

Which of the following security protocols uses a single, manually configured, static key for data encryption that is shared by the client and the WAP?

A. WEP
B. WPA
C. L2TP
D. IPSec

Answer: A
Explanation:

QUESTION NO: 73

Which of the following firewalls filters the traffic based on the header of the datagram?

A. Application-level firewall
B. Packet filtering firewall
C. Circuit-level firewall
D. Stateful inspection firewall

Answer: B
Explanation:

QUESTION NO: 74

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 performed the following steps of the pre-attack phase to check the security of the We-are-secure network:

l Gathering information

l Determining the network range

l Identifying active systems

Now, he wants to find the open ports and applications running on the network. Which of the following tools will he use to accomplish his task?

A. APNIC
B. ARIN
C. SuperScan
D. RIPE

Answer: C
Explanation:

QUESTION NO: 75

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
Explanation:

QUESTION NO: 76

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
Explanation:

QUESTION NO: 77

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
Explanation:

QUESTION NO: 78

What is the easiest way to verify that name resolution is functioning properly on a *TCP/IP* network?

A. Use the TRACERT command with the /pingname parameter.
B. Ping the source host with its computer name.
C. Ping the source host with its IP address.
D. Check the IP statistics on the file server.

Answer: B
Explanation:

QUESTION NO: 79

Which of the following is a Cisco *IOS* management term described in the statement below?

"It is the fourth digit in the configuration register and contains a hexadecimal value. The bootstrap program uses its value to choose which operating system to load into RAM."

A. Boot check
B. Boot field

C. Boot value
D. Boot

Answer: B
Explanation:

QUESTION NO: 80

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
Explanation:

QUESTION NO: 81

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
Explanation:

QUESTION NO: 82

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
Explanation:

QUESTION NO: 83

Which of the following protocols is used by voice over IP (*VoIP*) applications?

A. ICMP
B. IPv6
C. UDP
D. TCP

Answer: C
Explanation:

QUESTION NO: 84

Which of the following tools allows an attacker to intentionally craft the packets to gain unauthorized access?

Each correct answer represents a complete solution. Choose two.

A. Mendax **B.**
Fragroute **C.**
Tcpdump **D.**
Ettercap

Answer: A,B
Explanation:

QUESTION NO: 85

Which of the following tools is used to detect wireless LANs using the 802.11b, 802.11a, and 802.11g WLAN standards on the Windows platform?

A. Snort
B. Cain

C. NetStumbler
D. AiroPeek

Answer: C
Explanation:

QUESTION NO: 86

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
Explanation:

QUESTION NO: 87

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
Explanation:

QUESTION NO: 88

At which of the following layers of the Open System Interconnection (OSI) model the Internet Control Message Protocol (ICMP) and the Internet Group Management Protocol (IGMP) work?

A. The Physical layer
B. The Presentation layer
C. The Network layer
D. The Data-Link layer

Answer: C
Explanation:

QUESTION NO: 89

Which of the following tools can be used as a Linux vulnerability scanner that is capable of identifying operating systems and network services?

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

A. Cheops-ng
B. Fport
C. Cheops
D. Elsave

Answer: A,C
Explanation:

QUESTION NO: 90

John works as a professional Ethical Hacker. He is assigned a project to test the security of www.we-are-secure.com. You have searched all open ports of the we-are-secure server. Now, you want to perform the next information-gathering step, i.e., passive OS fingerprinting. Which of the following tools can you use to accomplish the task?

A. Nmap
B. NBTscan
C. P0f
D. Superscan

Answer: C
Explanation:

QUESTION NO: 91
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 handle encrypted and unencrypted traffic equally.
B. It cannot detect events scattered over the network.
C. It can detect events scattered over the network.
D. It is a technique that allows multiple computers to share one or more IP addresses.

Answer: A,B
Explanation:

QUESTION NO: 92

You have just taken over as the Network Administrator for a medium sized company. You want to check to see what services are exposed to the outside world. What tool would you use to accomplish this?

A. Protocol analyzer
B. Network mapper
C. Packet sniffer
D. A port scanner

Answer: D
Explanation:

QUESTION NO: 93

You work as a Network Administrator for Tech Perfect Inc. The office network is configured as an *IPv6* network. You have to configure a computer with the IPv6 address, which is equivalent to an IPv4 publicly routable address. Which of the following types of addresses will you choose?

A. Local-link
B. Global unicast
C. Site-local
D. Loopback

Answer: B
Explanation:

QUESTION NO: 94

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
Explanation:

QUESTION NO: 95

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
Explanation:

QUESTION NO: 96

Which of the following firewalls operates at three layers- Layer3, Layer4, and Layer5?

A. Application layer firewall
B. Proxy firewall
C. Dynamic packet-filtering firewall
D. Circuit-level firewall

Answer: C
Explanation:

QUESTION NO: 97

Which of the following protocols is used by *TFTP* as a file transfer protocol?

A. TCP
B. SNMP
C. UDP **D.**
SMTP

Answer: C
Explanation:

QUESTION NO: 98

Which of the following techniques is used to identify attacks originating from a botnet?

A. BPF-based filter
B. Recipient filtering
C. IFilter
D. Passive OS fingerprinting

Answer: D
Explanation:

QUESTION NO: 99

You work as a Network Administrator for Net Perfect Inc. The company has a Windows Server 2008- based network. You have created a test domain for testing *IPv6* addressing. Which of the following types of addresses are supported by IPv6?

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

A. Multicast
B. Anycast
C. Broadcast
D. Unicast

Answer: A,B,D
Explanation:

QUESTION NO: 100

You work as a Security Administrator for Tech Perfect Inc. You have implemented and configured a web application security scanner in the company's network. It helps in the automated review of

the web applications with the defined purpose of discovering security vulnerabilities. In order to perform this task, the web application security scanner examines a number of vulnerabilities. What are these vulnerabilities?

Each correct answer represents a complete solution. Choose three.

A. Server configuration mistakes/errors/version
B. Specific application problems
C. Input/Output validation
D. Denials of service against the TCP/IP stack

Answer: A,B,C
Explanation:

QUESTION NO: 101

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
Explanation:

QUESTION NO: 102

Which of the following are open-source vulnerability scanners?

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

Answer: B,C,D
Explanation:

QUESTION NO: 103

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
Explanation:

QUESTION NO: 104

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
Explanation:

QUESTION NO: 105

Which of the following is a valid *IPv6* address?

A. 45CF. 6D53: 12CD. AFC7: E654: BB32: 54AT: FACE
B. 45CF. 6D53: 12KP: AFC7: E654: BB32: 543C. FACE
C. 123.111.243.123
D. 45CF. 6D53: 12CD. AFC7: E654: BB32: 543C. FACE

Answer: D
Explanation:

QUESTION NO: 106

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
Explanation:

QUESTION NO: 107

Which of the following wireless security features provides the best wireless security mechanism?

A. WPA with 802.1X authentication
B. WPA with Pre Shared Key
C. WEP
D. WPA

Answer: A
Explanation:

QUESTION NO: 108

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He is using a tool to crack the wireless encryption keys. The description of the tool is as follows:

Which of the following tools is John using to crack the wireless encryption keys?

A. Kismet
B. PsPasswd
C. AirSnort
D. Cain

Answer: C
Explanation:

QUESTION NO: 109

Peter works as a Computer Hacking Forensic Investigator. He has been called by an organization to conduct a seminar to give necessary information related to sexual harassment within the work place. Peter started with the definition and types of sexual harassment. He then wants to convey that it is important that records of the sexual harassment incidents should be maintained, which helps in further legal prosecution. Which of the following data should be recorded in this documentation?

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

A. Names of the victims

B. Location of each incident
C. Date and time of incident
D. Nature of harassment

Answer: A,B,C
Explanation:

QUESTION NO: 110

Which of the following parts of IP header is used to specify the correct place of the fragment in the original un-fragmented datagram?

A. Fragment offset
B. Source address
C. TTL
D. Fragment ID

Answer: A
Explanation:

QUESTION NO: 111

John, a malicious hacker, forces a router to stop forwarding packets by flooding it with many open connections simultaneously so that all hosts behind it are effectively disabled. Which of the following attacks is John performing?

A. ARP spoofing
B. Replay attack **C.** Rainbow attack **D.** DoS attack

Answer: D
Explanation:

QUESTION NO: 112

You send and receive messages on Internet. A man-in-the-middle attack can be performed to capture and read your message. Which of the following *Information assurance* pillars ensures the security of your message or data against this type of attack?

A. Confidentiality

B. Non-repudiation
C. Data availability
D. Authentication

Answer: C
Explanation:

QUESTION NO: 113

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
Explanation:

QUESTION NO: 114

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
Explanation:

QUESTION NO: 115

Which of the following is a chronological record of system activities to enable the reconstruction and examination of the sequence of events and/or changes in an event?

A. Security audit
B. Corrective controls
C. Audit trail
D. Detective controls

Answer: C
Explanation:

QUESTION NO: 116

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
Explanation:

QUESTION NO: 117

Which of the following techniques allows probing firewall rule-sets and finding entry points into the targeted system or network?

A. Packet collision
B. Network enumerating
C. Packet crafting
D. Distributed Checksum Clearinghouse

Answer: C
Explanation:

QUESTION NO: 118

What are the advantages of stateless autoconfigration in IPv6?

Each correct answer represents a part of the solution. Choose three.

A. No server is needed for stateless autoconfiguration.
B. No host configuration is necessary.
C. It provides basic authentication to determine which systems can receive configuration data

D. Ease of use.

Answer: A,B,D

Explanation:

QUESTION NO: 119

John works as a contract Ethical Hacker. He has recently got a project to do security checking for www.we-are-secure.com. He wants to find out the operating system of the we-are-secure server in the information gathering step. Which of the following commands will he use to accomplish the task?

Each correct answer represents a complete solution. Choose two.

A. nc -v -n 208.100.2.25 80
B. nmap -v -O 208.100.2.25
C. nmap -v -O www.we-are-secure.com
D. nc 208.100.2.25 23

Answer: B,C

Explanation:

QUESTION NO: 120

Adam works as a Security administrator for Umbrella Inc. He runs the following traceroute and notices that hops 19 and 20 both show the same IP address.

1 172.16.1.254 (172.16.1.254) 0.724 ms 3.285 ms 0.613 ms 2 ip68-98-176-

1.nv.nv.cox.net (68.98.176.1) 12.169 ms 14.958 ms 13.416 ms 3 ip68-98-176-

1.nv.nv.cox.net (68.98.176.1) 13.948 ms ip68-100-0-1.nv.nv. cox.net (68.100.0.1)

16.743 ms 16.207 ms 4 ip68-100-0-137.nv.nv.cox.net (68.100.0.137) 17.324 ms 13.933

ms 20.938 ms 5 68.1.1.4 (68.1.1.4) 12.439 ms 220.166 ms 204.170 ms

6 so-6-0-0.gar2.wdc1.Level3.net (67.29.170.1) 16.177 ms 25.943 ms 14.104 ms 7

unknown.Level3.net (209.247.9.173) 14.227 ms 17.553 ms 15.415 ms "PassGuide" -

8 so-0-1-0.bbr1.NewYork1.level3.net (64.159.1.41) 17.063 ms 20.960 ms 19.512 ms 9

so-7-0-0.gar1. NewYork1.Level3.net (64.159.1.182) 20.334 ms 19.440 ms 17.938 ms

10 so-4-0-0.edge1.NewYork1.Level3.

net (209.244.17.74) 27.526 ms 18.317 ms 21.202 ms 11 uunet-level3-

oc48.NewYork1.Level3.net

(209.244.160.12) 21.411 ms 19.133 ms 18.830 ms 12 0.so-6-0-0.XL1.NYC4.ALTER.NET

(152.63.21.78)

21.203 ms 22.670 ms 20.111 ms 13 0.so-2-0-0.TL1.NYC8.ALTER.NET (152.63.0.153)

30.929 ms 24.858 ms

23.108 ms 14 0.so-4-1-0.TL1.ATL5.ALTER.NET (152.63.10.129) 37.894 ms 33.244 ms

33.910 ms 15 0.so-7-0-0.XL1.MIA4.ALTER.NET (152.63.86.189) 51.165 ms 49.935 ms

49.466 ms 16 0.so-3-0-0.XR1.MIA4.ALTER.

NET (152.63.101.41) 50.937 ms 49.005 ms 51.055 ms 17 117.ATM6-

0.GW5.MIA1.ALTER.NET (152.63.82.73) 51.897 ms 50.280 ms 53.647 ms 18 PassGuidegw1.

customer.alter.net (65.195.239.14) 51.921 ms 51.571 ms 56.855 ms 19

www.PassGuide.com (65.195.239.22) 52.191 ms 52.571 ms 56.855 ms 20

www.PassGuide.com (65.195.239.22) 53.561 ms 54.121 ms 58.333 ms

Which of the following is the most like cause of this issue?

A. A stateful inspection firewall
B. An application firewall
C. Network Intrusion system
D. Intrusion Detection System

Answer: A
Explanation:

QUESTION NO: 121

You work as a Network Administrator for Tech Perfect Inc. The company has a TCP/IP-based routed network. Two *routers* have been configured on the network. A router receives a packet. Which of the following actions will the router take to route the incoming packet?

Each correct answer represents a part of the solution. Choose two.

A. Use the routing table to determine the best path to the destination network address.
B. Read the destination IP address.

C. Add the path covered by the packet to the routing table.
D. Read the source IP address.
E. Use the routing table to determine the best path to the source network address.

Answer: A,B
Explanation:

QUESTION NO: 122

Which of the following types of firewall functions at the Session layer of OSI model?

A. Switch-level firewall
B. Circuit-level firewall
C. Packet filtering firewall
D. Application-level firewall

Answer: B
Explanation:

QUESTION NO: 123

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
C. MAC spoofing
D. VLAN hoping

Answer: C
Explanation:

QUESTION NO: 124

Which of the following forms on NAT maps multiple unregistered IP addresses to a single registered IP address by using different ports?

A. Overloading **B.**
Dynamic NAT **C.**
Overclocking

D. Static NAT

Answer: A
Explanation:

QUESTION NO: 125

You work as a Network Administrator for Tech Perfect Inc. The company has a TCP/IP-based network. A Cisco switch is configured on the network. You change the original host name of the switch through the hostname command. The prompt displays the changed host name. After some time, power of the switch went off due to some reason. When power restored, you find that the prompt is displaying the old host name. What is the most likely cause?

A. The changes were saved in running-config file.
B. The startup-config file got corrupted.
C. The running-config file got corrupted.
D. Host name cannot be changed permanently once switch is configured.

Answer: A
Explanation:

QUESTION NO: 126

Sandra, a novice computer user, works on Windows environment. She experiences some problem regarding bad sectors formed in a hard disk of her computer. She wants to run CHKDSK command to check the hard disk for bad sectors and to fix the errors, if any, occurred. Which of the following switches will she use with CHKDSK command to accomplish the task?

A. CHKDSK /R /F
B. CHKDSK /C /L
C. CHKDSK /V /X
D. CHKDSK /I

Answer: A
Explanation:

QUESTION NO: 127

Which of the following proxy servers is also referred to as transparent proxies or forced proxies?

A. Reverse proxy server

B. Intercepting proxy server
C. Anonymous proxy server
D. Tunneling proxy server

Answer: B
Explanation:

QUESTION NO: 128

Which of the following steps are generally followed in computer forensic examinations?

Each correct answer represents a complete solution. Choose three.

A. Encrypt
B. Analyze
C. Acquire
D. Authenticate

Answer: B,C,D
Explanation:

QUESTION NO: 129

Which of the following actions can be taken as the countermeasures against the ARP spoofing attack?

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

A. Using Private VLANs
B. Looking for large amount of ARP traffic on local subnets
C. Placing static ARP entries on servers and routers
D. Using 8 digit passwords for authentication

Answer: A,B,C
Explanation:

QUESTION NO: 130

Which of the following well-known ports is used by *BOOTP*?

A. UDP 69
B. TCP 161

C. TCP 21
D. UDP 67

Answer: D
Explanation:

QUESTION NO: 131

Which of the following vulnerability scanners is used to test Web servers for dangerous files/CGIs, outdated server software, and other problems?

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

Answer: A
Explanation:

QUESTION NO: 132

You work as a technician for Net Perfect Inc. You are troubleshooting a connectivity issue on a network. You are using the *ping* command to verify the connectivity between two hosts. You want ping to send larger sized packets than the usual 32-byte ones. Which of the following commands will you use?

A. ping -l
B. ping -t
C. ping -a
D. ping -4

Answer: A
Explanation:

QUESTION NO: 133

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

l Information gathering

l Determination of network range

l Identification of active systems

l Location of open ports and applications

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

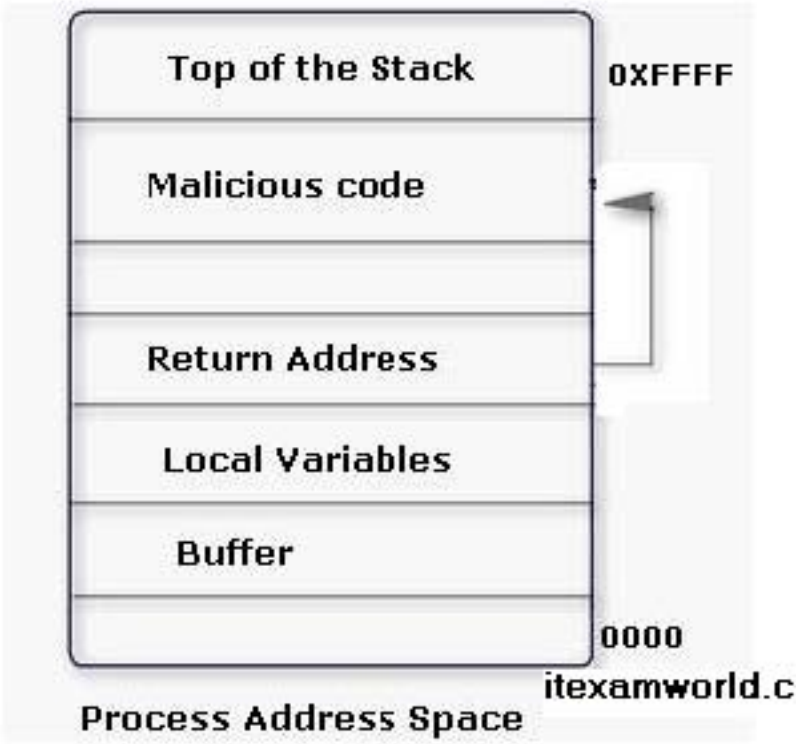
A. Install a backdoor to log in remotely on the We-are-secure server.
B. Map the network of We-are-secure Inc.
C. Perform OS fingerprinting on the We-are-secure network.
D. Fingerprint the services running on the we-are-secure network.

Answer: C
Explanation:

QUESTION NO: 134

An attacker changes the address of a sub-routine in such a manner that it begins to point to the address of the malicious code. As a result, when the function has been exited, the application can be forced to shift to the malicious code. The image given below explains this phenomenon:

Which of the following tools can be used as a countermeasure to such an attack?



A. Kismet
B. Absinthe

C. SmashGuard
D. Obiwan

Answer: C
Explanation:

QUESTION NO: 135

An IDS is a group of processes working together in a network. These processes work on different computers and devices across the network. Which of the following processes does an IDS perform?

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

A. Event log analysis
B. Monitoring and analysis of user and system activity
C. Statistical analysis of abnormal traffic patterns
D. Network traffic analysis

Answer: A,B,C,D
Explanation:

QUESTION NO: 136

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
Explanation:

QUESTION NO: 137

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
Explanation:

QUESTION NO: 138

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
Explanation:

QUESTION NO: 139

Windump is a Windows port of the famous TCPDump packet sniffer available on a variety of platforms. In order to use this tool on the Windows platform a user must install a packet capture library.

What is the name of this library?

A. PCAP
B. WinPCap
C. libpcap
D. SysPCap

Answer: B
Explanation:

QUESTION NO: 140

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
Explanation:

QUESTION NO: 141

John works as a Security Manager for Gentech Inc. He uses an IDP engine to detect the type of interactive traffic produced during an attack in which the attacker wants to install the mechanism on a host system that facilitates the unauthorized access and breaks the system confidentiality.

Which of the following rulebases will he use to accomplish the task?

A. Backdoor rulebase
B. Traffic Anomalies rulebase
C. Exempt rulebase
D. SYN Protector rulebase

Answer: A
Explanation:

QUESTION NO: 142

You work as a Network Administrator for Tech Perfect Inc. The company has a TCP/IP-based routed network. You have recently come to know about the Slammer worm, which attacked computers in 2003 and doubled the number of infected hosts every 9 seconds or so. Slammer infected 75000 hosts in the first 10 minutes of the attack. To mitigate such security threats, you want to configure security tools on the network. Which of the following tools will you use?

A. Intrusion Prevention Systems
B. Firewall
C. Anti-x
D. Intrusion Detection Systems

Answer: A

Explanation:

QUESTION NO: 143

Which of the following monitors program activities and modifies malicious activities on a system?

A. Back door
B. NIDS
C. HIDS
D. RADIUS

Answer: C

Explanation:

QUESTION NO: 144

You work as a Network Administrator for TechPerfect Inc. The company has a corporate intranet setup.

A router is configured on your network to connect outside hosts to the internetworking. For security, you want to prevent outside hosts from pinging to the hosts on the internetwork. Which of the following steps will you take to accomplish the task?

A. Block the ICMP protocol through ACL.
B. Block the TCP protocol through ACL.
C. Block the IPv6 protocol through ACL.
D. Block the UDP protocol through ACL.

Answer: A

Explanation:

QUESTION NO: 145

Which of the following are packet filtering tools for the Linux operating system?

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

A. Zone Alarm
B. BlackICE
C. IPFilter
D. IPTables

Answer: C,D

Explanation:

QUESTION NO: 146

Which of the following tools is an open source protocol analyzer that can capture traffic in real time?

A. Netresident
B. Snort
C. Wireshark
D. NetWitness

Answer: C

Explanation:

QUESTION NO: 147

Which of the following tools can be used for OS fingerprinting?

A. netstat
B. nmap
C. DIG
D. whois

Answer: B

Explanation:

QUESTION NO: 148

You work as a Security Administrator for Tech Perfect Inc. The company has a switched network. You have configured tcpdump in the network which can only see traffic addressed to itself and broadcast traffic. What will you do when you are required to see all traffic of the network?

A. Connect the sniffer device to a Remote Switched Port Analyzer (RSPAN) port.
B. Configure VLAN Access Control List (VACL).
C. Configure Network Access Control (NAC).
D. Connect the sniffer device to a Switched Port Analyzer (SPAN) port.

Answer: D

Explanation:

QUESTION NO: 149

Sam works as a Security Manager for GenTech Inc. He has been assigned a project to detect reconnoitering activities. For this purpose, he has deployed a system in the network that attractsthe attention of an attacker. Which of the following rulebases will he use to accomplish the task?

A. Network Honeypot rulebase
B. Exempt rulebase
C. Backdoor rulebase
D. SYN Protector rulebase

Answer: A
Explanation:

QUESTION NO: 150

Which of the following applications cannot proactively detect anomalies related to a computer?

A. NIDS
B. Anti-virus scanner
C. Firewall installed on the computer
D. HIDS

Answer: A
Explanation:

QUESTION NO: 151

Which of the following utilities provides an efficient way to give specific users permission to use specific system commands at the root level of a Linux operating system?

A. Snort **B.**
SUDO **C.**
Apache **D.**
SSH

Answer: B
Explanation:

QUESTION NO: 152

You work as a Network Administrator for Tech Perfect Inc. The company has a wireless LAN infrastructure. The management wants to prevent unauthorized network access to local area networks and other information assets by the wireless devices. What will you do?

A. Implement a dynamic NAT.
B. Implement a firewall.
C. Implement an ACL.
D. Implement a WIPS.

Answer: D
Explanation:

QUESTION NO: 153

Rick works as the Security Manager for TechPerfect Inc. He wants to continue the evaluation of rules according to the ordered list to identify matches even if a match is found. Which of the following rulebases will he use to accomplish the task?

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

A. Terminal rulebase
B. Nonterminal rulebase
C. Backdoor rulebase
D. IDP rulebase

Answer: B,D
Explanation:

QUESTION NO: 154

David works as the Security Manager for PassGuide Inc. He has been assigned a project to detect the attacks over multiple connections and sessions and to count the number of scanned ports in a defined time period. Which of the following rulebases will he use to accomplish the task?

A. Traffic Anomalies rulebase
B. Exempt rulebase
C. SYN Protector rulebase
D. Network Honeypot rulebase

Answer: A
Explanation:

QUESTION NO: 155

Which of the following information must the fragments carry for the destination host to reassemble them back to the original unfragmented state?

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

A. MF flag
B. Length of the data
C. IP address
D. Offset field
E. MAC address
F. IP identification number

Answer: A,B,D,F
Explanation:

QUESTION NO: 156

Which of the following honeypots is a low-interaction honeypot and is used by companies or corporations for capturing limited information about malicious hackers?

A. Honeynet
B. Research honeypot
C. Honeyfarm
D. Production honeypot

Answer: D
Explanation:

QUESTION NO: 157

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. 2
D. F

Answer: B

Explanation:

QUESTION NO: 158

Which of the following is like a malicious cache poisoning where fake data is placed in the cache of the name servers?

A. Smurf attack
B. Host name spoofing
C. DNS spoofing
D. SYN flood attack

Answer: C

Explanation:

QUESTION NO: 159

Which of the following configuration schemes in IPv6 allows a client to automatically configure its own IP address with or without IPv6 routers?

A. Stateless configuration
B. Stateful configuration
C. Stateful autoconfiguration
D. Stateless autoconfiguration

Answer: D

Explanation:

QUESTION NO: 160

Adam works on a Linux system. He is using Sendmail as the primary application to transmit e-mails. Linux uses Syslog to maintain logs of what has occurred on the system. Which of the following log files contains e-mail information such as source and destination IP addresses, date and time stamps etc?

A. /log/var/logd
B. /log/var/mailog
C. /var/log/mailog
D. /var/log/logmail

Answer: C

Explanation:

QUESTION NO: 161

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 can transfer files using the associated HTTP or FTP protocols.
B. SSH is typically used to log into a remote machine and execute commands, but it also supports tunneling, forwarding TCP ports and X11 connections.
C. SSH uses public-key cryptography to authenticate the remote computer and allow the remote computer to authenticate the user, if necessary.
D. SSH uses the client-server model.

Answer: B,C,D

Explanation:

QUESTION NO: 162

When no anomaly is present in an Intrusion Detection, but an alarm is generated, the response is known as _____.

A. False negative
B. False positive
C. True negative
D. True positive

Answer: B

Explanation:

QUESTION NO: 163

Which of the following can provide security against man-in-the-middle attack?

A. Anti-virus programs
B. Strong data encryption during travel
C. Strong authentication method
D. Firewall

Answer: B

Explanation:

QUESTION NO: 164

Which of the following is used to provide hook handling facility within the Linux kernel in order to capture and manipulate network packets?

A. Tcpdump
B. WinDump
C. Netfilter
D. WinPcap

Answer: C
Explanation:

QUESTION NO: 165

Which of the following statements about *Access control list (ACL)* is true?

Each correct answer represents a complete solution. Choose three.

A. Extended IP Access Control List permits or denies packets only from a specific source IP addresses.
B. Standard IP Access Control List permits or denies packets only from specific source IP addr esses.
C. Standard IP Access Control List can be used to permit or deny traffic from a specific source IP addresses or for a specific destination IP address, and port.
D. Extended IP Access Control List permits or denies traffic from a specific source IP addresses or for a specific destination IP address, and port.
E. Access control list filters packets or network traffic by controlling whether routed packets are forwarded or blocked at the router's interfaces.

Answer: B,D,E
Explanation:

QUESTION NO: 166

You work as a Desktop Support Technician for umbrella Inc. The company uses a Windows-based network. An employee from the sales department is facing problem in the IP configuration of the network connection. He called you to resolve the issue. You suspect that the IP configuration is not configured properly. You want to use the ping command to ensure that IPv4 protocol is working on a computer. While running the ping command from the command prompt, you find that

Windows Firewall is blocking the ping command. What is the cause of the issue?

A. Windows Firewall blocks the command line tools.
B. Core Networking Firewall rules do not allow ICMPv4 or ICMPv6 Echo Requests.
C. Core Networking Firewall rules do not allow IPv4 or IPv6.
D. Windows Firewall rules do not allow Core Networking Tools.

Answer: B
Explanation:

QUESTION NO: 167

SSH is a network protocol that allows data to be exchanged between two networks using a secure channel. Which of the following encryption algorithms can be used by the SSH protocol?

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

A. DES
B. IDEA
C. Blowfish
D. RC4

Answer: A,B,C
Explanation:

QUESTION NO: 168

Which of the following features does the Nmap utility have?

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

A. It has a stealth approach to scanning and sweeping.
B. It identifies services running on systems in a specified range of IP addresses using scanning and sweeping feature.
C. It uses operating system fingerprinting technology to identify the operating system running on a target system.
D. It is a location where an organization can easily view the event of a disaster, such as fire, flood, terrorist threat, or other disruptive events.

Answer: A,B,C
Explanation:

QUESTION NO: 169

Which of the following attacks can be mitigated by providing proper training to the employees in an organization?

A. Social engineering
B. Smurf
C. Man-in-the-middle
D. Denial-of-Service

Answer: A

Explanation:

QUESTION NO: 170

You work as a Network Administrator for SmartCert Inc. The company's network contains five Windows 2003 servers and ninety Windows XP Professional client computers. You want to view all the incoming requests to an Internet Information Services (IIS) server and allow only requests that comply with a rule set, created by you, to be processed. You also want to detect the intrusion attempts by recognizing the strange characters in a URL on a Web server. What will you do to accomplish the task?

A. Configure a connection to the SQL database by using the RELOG command-line utility.
B. Use the URLScan tool.
C. Use the Remote Desktop Protocol (RDP).
D. Use the HFNETCHK utility.

Answer: B

Explanation:

QUESTION NO: 171

Adam works as a Network Administrator for PassGuide Inc. He wants to prevent the network from DOS attacks. Which of the following is most useful against DOS attacks?

A. Distributive firewall
B. Honey Pot
C. SPI
D. Internet bot

Answer: C

Explanation:

QUESTION NO: 172

Which of the following IPv6 address types is a single address that can be assigned to multiple interfaces?

A. Loopback
B. Unicast
C. Multicast
D. Anycast

Answer: D

Explanation:

QUESTION NO: 173

Adam, a malicious hacker purposely sends fragmented ICMP packets to a remote target. The total size of this ICMP packet once reconstructed is over 65,536 bytes.

On the basis of above information, which of the following types of attack is Adam attempting to perform?

A. Fraggle attack
B. SYN Flood attack
C. Ping of death attack
D. Land attack

Answer: C

Explanation:

QUESTION NO: 174

Which of the following fields is 13 bits long and specifies the offset of a particular fragment relative to the beginning of the original un-fragmented IP datagram?

A. Time to live
B. Protocol
C. Header checksum
D. Fragment offset

Answer: D

Explanation:

QUESTION NO: 175

Which of the following command-line utilities is used to show the state of current *TCP/IP* connections?

A. PING
B. NSLOOKUP
C. NETSTAT
D. TRACERT

Answer: C
Explanation:

QUESTION NO: 176

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. Kismet
B. Dsniff
C. Snort
D. KisMAC

Answer: C
Explanation:

QUESTION NO: 177

Which of the following wireless security policies helps to prevent the wireless enabled laptops from peer-topeer attacks when the laptops are used in public access network?

A. Use protocol analyzer
B. Use Port Address Translation
C. Use security protocols
D. Use firewall

Answer: C,D
Explanation:

QUESTION NO: 178

Which of the following steps are generally followed in computer forensic examinations?

Each correct answer represents a complete solution. Choose three.

A. Authenticate
B. Acquire
C. Encrypt
D. Analyze

Answer: A,B,D
Explanation:

QUESTION NO: 179

You work as a Network Administrator for Tech Perfect Inc. The company has a wireless LAN infrastructure. The management wants to prevent unauthorized network access to local area networks and other information assets by the wireless devices. What will you do?

A. Implement an ACL.
B. Implement a firewall.
C. Implement a dynamic NAT.
D. Implement a WIPS.

Answer: D
Explanation:

QUESTION NO: 180

Which of the following tools can be used as a Linux vulnerability scanner that is capable of identifying operating systems and network services?

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

A. Cheops-ng
B. Fport **C.**
Elsave **D.**
Cheops

Answer: A,D
Explanation:

QUESTION NO: 181

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. Firewall
C. NAT
D. IPsec

Answer: C
Explanation:

QUESTION NO: 182

SSH is a network protocol that allows data to be exchanged between two networks using a secure channel. Which of the following encryption algorithms can be used by the SSH protocol?

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

A. DES
B. IDEA
C. RC4
D. Blowfish

Answer: A,B,D
Explanation:

QUESTION NO: 183

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. WinPcap
B. Netfilter
C. tcpdump
D. iptables

Answer: C

Explanation:

QUESTION NO: 184

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
Explanation:

QUESTION NO: 185

Which of the following actions can be taken as the countermeasures against the ARP spoofing attack?

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

A. Placing static ARP entries on servers and routers
B. Looking for large amount of ARP traffic on local subnets
C. Using Private VLANs
D. Using 8 digit passwords for authentication

Answer: A,B,C
Explanation:

QUESTION NO: 186

John works as a professional Ethical Hacker. He is assigned a project to test the security of www.we-are-secure.com. You have searched all open ports of the we-are-secure server. Now, you want to perform the next information-gathering step, i.e., passive OS fingerprinting. Which of the following tools can you use to accomplish the task?

A. NBTscan
B. Nmap
C. P0f

D. Superscan

Answer: C
Explanation:

QUESTION NO: 187

You work as a Forensic Investigator. Which of the following rules will you follow while working on a case?

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

A. Follow the rules of evidence and never temper with the evidence.
B. Examine original evidence and never rely on the duplicate evidence.
C. Never exceed the knowledge base of the forensic investigation.
D. Prepare a chain of custody and handle the evidence carefully.

Answer: A,B,C,D
Explanation:

QUESTION NO: 188

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. PIDS
B. APIDS
C. HIDS
D. NIDS

Answer: C
Explanation:

QUESTION NO: 189

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
Explanation:

QUESTION NO: 190

You work as a Security Administrator for Tech Perfect Inc. You have implemented and configured a web application security scanner in the company's network. It helps in the automated review of the web applications with the defined purpose of discovering security vulnerabilities. In order to perform this task, the web application security scanner examines a number of vulnerabilities.

What are these vulnerabilities?

Each correct answer represents a complete solution. Choose three.

A. Input/Output validation
B. Server configuration mistakes/errors/version
C. Specific application problems
D. Denials of service against the TCP/IP stack

Answer: A,B,C
Explanation:

QUESTION NO: 191

Which of the following tools detects certain types of packet filters and NAT setups?

A. TShark
B. Vulnerability scanner
C. Wireshark
D. Passive OS fingerprinting

Answer: D
Explanation:

Trying our product !

★ **100%** Guaranteed Success

★ **100%** Money Back Guarantee

★ **365 Days** Free Update

★ **Instant Download** After Purchase

★ **24x7** Customer Support

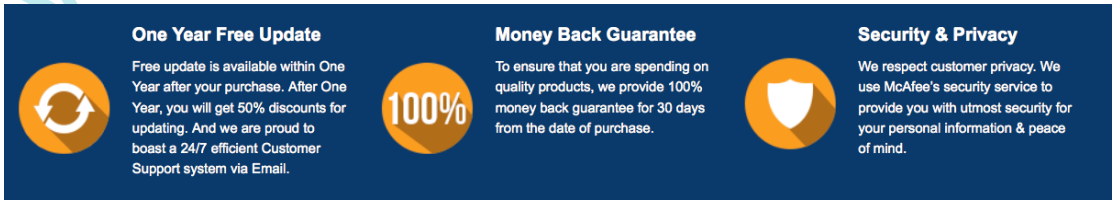
★ Average **99.9%** Success Rate

★ More than **69,000** Satisfied Customers Worldwide

★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



Guarantee & Policy | Privacy & Policy | Terms & Conditions

Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.