GPPA.VCEplus.premium.exam.285q

Number: GPPA
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

GPPA

GIAC Certified Perimeter Protection Analyst

Version 1.0

Exam A

QUESTION 1
Which of the following tools is an open source protocol analyzer that can capture traffic in real time?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
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. Signature Based
B. Reactive IDS
C. Anomaly Based
D. Passive IDS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3 Which of the following are open-source vulnerability scanners?
(Choose three.)

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

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4 Suppose you are working as a Security Administrator at ABC 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 Switched Port Analyzer (SPAN) port.
B. Connect the sniffer device to a Remote Switched Port Analyzer (RSPAN) port.

C. Configure Network Access Control (NAC).
D. Configure VLAN Access Control List (VACL).

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5 Which of the following techniques is used to identify attacks originating from a botnet?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
John works as a professional Ethical Hacker. He is assigned a project to test the security of www.abc.com. You have searched all open ports of the ABC 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. P0f
B. Superscan
C. Nmap
D. NBTscan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7 Which of the following protocols is used by TFTP as a file transfer protocol?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Which of the following steps are generally followed in computer forensic examinations?
Each correct answer represents a complete solution. (Choose three.)

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

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9 Which of the following monitors program activities and modifies malicious activities on a system?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10 Which of the following wireless security features provides the best wireless security mechanism?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
David works as the Security Manager for ABC 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. SYN Protector rulebase
B. Exempt rulebase
C. Traffic Anomalies rulebase
D. Network Honeyport rulebase

Correct Answer: C

Section: (none)
Explanation
Explanation/Reference:

QUESTION 12 Which of the following terms is used to represent IPv6 addresses?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
You work as a Security Administrator for ABC 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. Denials of service against the TCP/IP stack
C. Server configuration mistakes/errors/version
D. Specific application problems

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
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. Offset field
B. MF flag
C. Length of the data
D. IP identification number
E. IP address
F. MAC address

Correct Answer: ABCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Which of the following types of IP actions are supported by an IDP rulebase? (Choose three.)

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

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16 You work as a Network Administrator for ABC 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. ICMP
B. UDP
C. TCP
D. IP

Correct Answer: ABCD
Section: (none)
Explanation

Explanation/Reference:

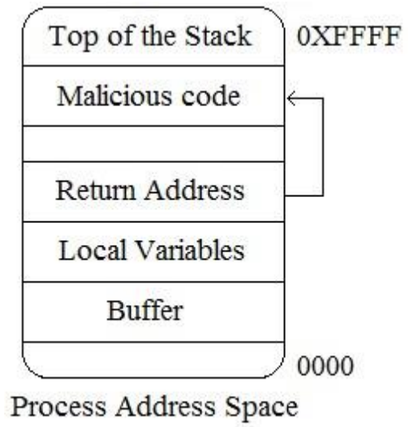
QUESTION 17
Which of the following parts of IP header is used to specify the correct place of the fragment in the original un-fragmented datagram?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
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. SmashGuard
B. Obiwan
C. Kismet
D. Absinthe

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19 Which of the following forms on NAT maps multiple unregistered IP addresses to a single registered IP address by using different ports?

A. Overclocking
B. Dynamic NAT
C. Overloading
D. Static NAT

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20 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. NetStumbler
C. AiroPeek
D. Cain

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21 Which of the following applications cannot proactively detect anomalies related to a computer?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
You work as a Network Administrator for ABC 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. Read the source IP address.
B. Add the path covered by the packet to the routing table.
C. Use the routing table to determine the best path to the destination network address.
D. Read the destination IP address.
E. Use the routing table to determine the best path to the source network address.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
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. Production honeypot

C. Research honeypot
D. Honeyfarm

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
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 Open System Interconnection (OSI) reference model do these routers filter information?

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

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
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. Apache
B. Snort
C. SSH
D. SUDO

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27 Which of the following firewalls operates at three layers - Layer3, Layer4, and Layer5?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28 Which of the following hexadecimal values in the boot field in the configuration register loads the first IOS file found in Flash memory?

A. 2
B. 0
C. 1
D. F

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29 Jain works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.abc.com.

He has successfully completed the following steps of the preattack phase:

>> Information gathering
>> Determining network range
>> Identifying active machines
>> Finding open ports and applications
>> OS fingerprinting
>> Fingerprinting services

Now Jain wants to perform network mapping of the ABC 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. Traceroute
B. Cheops
C. NeoTrace
D. Ettercap

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30 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. Tcpdump
B. Ettercap
C. Fragroute
D. Mendax

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31 Which of the following is a version of netcat with integrated transport encryption capabilities?

A. Encat
B. Nikto
C. Socat
D. Cryptcat

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32 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. IPTables
B. IPFilter
C. Zone Alarm
D. BlackICE

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
You work as a Network Administrator for ABC 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 UDP protocol through ACL.
B. Block the IPv6 protocol through ACL.
C. Block the TCP protocol through ACL.
D. Block the ICMP protocol through ACL.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
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. Packet sniffer

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
You work as a Network Administrator for ABC 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. Broadcast
B. Multicast
C. Anycast
D. Unicast

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36 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. Netfilter
B. iptables
C. WinPcap
D. tcpdump

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
You work as a Network Administrator for ABC 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 WIPS.
B. Implement a dynamic NAT.
C. Implement a firewall.
D. Implement an ACL.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
You work as a Network Administrator for ABC Inc. The company has a TCP/IP network. You have been assigned a task to configure a stateful packet filtering firewall to secure the network of the company. You are encountering some problems while configuring the stateful packet filtering firewall.

Which of the following can be the reasons for your problems?

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

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
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. Traffic Anomalies rulebase
B. SYN Protector rulebase
C. Backdoor rulebase
D. Exempt rulebase

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
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. VLAN hoping
B. ARP spoofing
C. IP address spoofing
D. MAC spoofing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 41 What are the advantages of stateless autoconfiguration in IPv6? Each correct answer represents a part of the solution. (Choose three.)

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

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42 Jain works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.abc.com. In order to do so, he performs the following steps of the preattack phase successfully:

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

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
You work as a technician for ABC 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 32byte ones.

Which of the following commands will you use?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 44
Sam works as a Security Manager for ABC Inc. He has been assigned a project to detect reconnoitering activities. For this purpose, he has deployed a system in the network that attracts the attention of an attacker.

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

A. Backdoor rulebase
B. Network Honeypot rulebase
C. Exempt rulebase

D. SYN Protector rulebase

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45 Which of the following is a valid IPv6 address?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46 Which of the following well-known ports is used by BOOTP?

A. UDP 67
B. TCP 21
C. UDP 69
D. TCP 161

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
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 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
B. 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
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 in
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
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. Sniffer
B. tcptraceroute
C. Fpipe
D. tcptrace

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49 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 routes
B. Using Private VLANs
C. Using 8 digit passwords for authentication
D. Looking for large amount of ARP traffic on local subnets

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
You work as a Network Troubleshooter for ABC 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 remote interface on which the tunnel is built.
B. The IPv6 address assigned to the remote tunnel interface.
C. The IPv6 address assigned to the local tunnel interface.
D. The IPv4 address assigned to the local interface on which the tunnel is built.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 51
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. IPsec
B. NAT
C. ACL

D. Firewall

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.abc.com. He is using a tool to crack the wireless encryption keys. The description of the tool is as follows:

It is a Unix-based WLAN WEP cracking tool that recovers encryption keys. It operates by passively monitoring transmissions. It uses Chipertext Only Attack and captures approximately 5 to 10 million packets to decrypt the WEP keys.

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53 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. SysPCap
B. libpcap
C. WinPCap
D. PCAP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
Jain works as a contract Ethical Hacker. He has recently got a project to do security checking for www.abc.com. He wants to find out the operating system of the ABC 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 www.abc.com
C. nmap -v -O 208.100.2.25
D. nc 208.100.2.25 23

Correct Answer: BC

Section: (none)
Explanation

Explanation/Reference:

QUESTION 55 Which of the following protocols is used by voice over IP (VoIP) applications?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
You work as a Network Administrator for ABC 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 running-config file got corrupted.
B. The changes were saved in running-config file.
C. The startup-config file got corrupted.
D. Host name cannot be changed permanently once switch is configured.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57 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 Data-Link layer
B. The Physical layer
C. The Network layer
D. The Presentation layer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
Which of the following vulnerability scanners is used to test Web servers for dangerous files/CGIs, outdated server software, and other problems?

A. Hackbot

B. Nikto
C. Nessus
D. Nmap

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
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. Statistical analysis of abnormal traffic patterns.
B. Monitoring and analysis of user and system activity.
C. Network traffic analysis.
D. Event log analysis.

Correct Answer: ABCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
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. Corrective controls
B. Audit trail
C. Detective controls
D. Security audit

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
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. Elsave
C. Cheops
D. Fport

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62 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? (Choose two.)

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

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
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. Data availabilityC. Authentication
D. Non-repudiation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
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 /I
C. CHKDSK /V /X
D. CHKDSK /C /L

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:

QUESTION 65 Which of the following proxy servers is also referred to as transparent proxies or forced proxies?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
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 -sS
C. nmap -sU -p
D. nmap -sT

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
Which of the following types of firewall functions at the Session layer of Open System Interconnection (OSI) model?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
You work as a Network Administrator for ABC 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 Detection Systems
B. Anti-x
C. Intrusion Prevention Systems
D. Firewall

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
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. TLS
B. SSL
C. SSH
D. IPsec

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
Rick works as the Security Manager for ABC 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. Backdoor rulebase
B. Nonterminal rulebase
C. Terminal rulebase
D. IDP rulebase

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71 Which of the following tools can be used for OS fingerprinting?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72 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 cannot detect events scattered over the network.

B. It can handle encrypted and unencrypted traffic equally.
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.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
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. Replay attack
B. ARP spoofing
C. DoS attack
D. Rainbow attack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
Poplu 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. Poplu 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. Date and time of incident
B. Names of the victims
C. Nature of harassment
D. Location of each incident

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:
QUESTION 75 You work as a Network Administrator for ABC 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. Site-local
C. Global unicast
D. Loopback

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
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. Source and destination Layer 3 address
B. Actual data in the packet
C. Layer 4 protocol information
D. Interface of sent or received traffic

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77 Which of the following IPv6 address types is a single address that can be assigned to multiple interfaces?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
Which of the following is used to provide hook handling facility within the Linux kernel in order to capture and manipulate network packets?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
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. Protocol

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80 Which of the following is the function of the editcap utility of Wireshark?

A. To analyze data packets.
B. To remove duplicate packets.
C. To transfer data packets.
D. To check data packets.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
Which of the following attacks allows an attacker to sniff data frames on a local area network (LAN) or stop the traffic altogether?

A. Port scanning
B. ARP spoofing
C. Session hijacking
D. Man-in-the-middle

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
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. service password-encryption
C. enable password-encryption
D. no enable password-encryption

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83

Mark has been assigned a project to configure a wireless network for a company. The network should contain a Windows 2003 server and 30 Windows XP client computers. Mark has a single dedicated Internet connection that has to be shared among all the client computers and the server. The configuration needs to be done in a manner that the server should act as a proxy server for the client computers.

Which of the following programs can Mark use to fulfill this requirement?

A. Wingate
B. Microsoft Internet Security & Acceleration Server (ISA)
C. Sniffer
D. SOCKS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
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. Network security device
B. Source of the OS identification
C. Victim OS
D. Relevancy to the victim in the alert

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
Paul works as a Technical Representative in a CSIRT for ABC 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. Paul 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, internet traces.
C. Volatile data, file slack, file system, registry, memory dumps, system state backup, internet traces. D. Volatile data, file slack, registry, system state backup, internet traces, file system, memory dumps.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
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. APIDS
B. PIDS

C. NIDS
D. HIDS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87 Which of the following statements about an IDP rule base notification are true?

A. When an action is performed, a notification defines how to log information.
B. It is used to specify the type of network traffic that has to be monitored for attacks.
C. It can be defined as reusable logical entities that the user can apply to the rules.
D. It directs an IDP to drop or close the connection.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
Which of the following libraries does TShark use to capture traffic from the first available network interface?

A. bcap
B. dcap
C. scap
D. pcap

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
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. Ping of death attack
B. SYN Flood attack
C. Fraggle attack
D. Land attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90 Which of the following is the module of OpenSER?

A. TShark
B. Sipsak
C. WireShark
D. SipTrace

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
You are a professional Computer Hacking forensic investigator. You have been called to collect the evidences of Buffer Overflows or Cookie snooping attack.

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

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

A. Event logs
B. System logs
C. Web server logs
D. Program logs

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92 Which of the following is like a malicious cache poisoning where fake data is placed in the cache of the name servers?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 93 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:

• Limit events that occur from security threats such as viruses, worms, and spyware.
• 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. Protocol-Independent Multicast
B. Firewall Service Module
C. Network Admission Control

D. NetFlow

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94 Which of the following tools detects certain types of packet filters and NAT setups?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95 Which of the following features does the Nmap utility have?

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

A. It uses operating system fingerprinting technology to identify the operating system running on a target system.
B. It identifies services running on systems in a specified range of IP addresses using scanning and sweeping feature.
C. It has a stealth approach to scanning and sweeping.
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.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96 Which of the following is the default port for POP3?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
Secure Shell (SSH) is a network protocol that allows data to be exchanged using a secure channel between two networked devices.

Which of the following features are supported by Secure Shell?

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

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

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
Which of the following wireless security policies helps to prevent the wireless enabled laptops from peer-to-peer attacks when the laptops are used in public access network? (Choose two.)

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

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
Which of the following types of firewalls increases the security of data packets by remembering the state of connection at the network and the session layers as they pass through the filter?

A. Stateless packet filter firewall
B. Virtual firewall
C. PIX firewall
D. Stateful packet filter firewall

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 100
Which of the following commands is recommended by Cisco for latest switches and routers to erase the contents of NVRAM?

A. reload
B. erase startup-config
C. erase nvram:
D. write erase

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
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 autoconfiguration
C. Stateful configuration
D. Stateless autoconfiguration

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
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 is easy to install packet filtering firewalls in comparison to the other network security solutions.
B. It makes security transparent to end-users which provide easy use of the client applications.
C. It prevents application-layer attacks.
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.

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103 You work as a Network Administrator for ABC 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 Remote Desktop Protocol (RDP).
C. Use the HFNETCHK utility.
D. Use the URL Scan tool.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
Jain works as a professional Ethical Hacker. He has been assigned a project for testing the security of www.abc.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 ABC 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. Evasion attack
B. Polymorphic shell code attack
C. Insertion attack
D. Session splicing attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
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. Blowfish
C. RC4
D. IDEA

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106
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. Private Address Translation
C. Per-user Address Translation
D. Pool Address Translation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
An attacker makes an attempt against a Web server. The result is that the attack takes the form of URLs. These URLs search for a certain string that identifies an attack against the Web server.

Which IDS/IPS detection method do the URLs use to detect and prevent an attack?

A. Policy-based detection

B. Honey pot detection
C. Anomaly-based detection
D. Signature-based detection

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
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. Core Networking Firewall rules do not allow IPv4 or IPv6.
B. Windows Firewall blocks the command line tools.
C. Windows Firewall rules do not allow Core Networking Tools.
D. Core Networking Firewall rules do not allow ICMPv4 or ICMPv6 Echo Requests.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
You work as a Firewall Analyst in the ABC 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 provides network address and port address translations with both IPv4 and IPv6 addressing schemes.
B. It offers stateless and stateful packet filtering with both IPv4 and IPv6 addressing schemes.
C. It includes a number of layers of API's for third party extensions.
D. It includes many plug-ins or modules in 'patch-o-matic' repository.

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
Jain works as a professional Ethical Hacker. He has been assigned the project of testing the security of testing the security of www.abc.com. Jain notices that the ABC network is vulnerable to a man-in-the-middle attack since the key exchange process of the cryptographic algorithm it is using does not authenticate participants.

Which of the following cryptographic algorithms is being used by the ABC server?

A. RSA
B. Blowfish
C. Diffie-Hellman

D. Twofish

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111 Jain works as a Security Manager for ABC Inc. The company has a Windows-based network.

Jain has been assigned a project to detect the services used by an attack to access the network. For this purpose, he is required to use the predefined service objects of the rulebase. This predefined service object defines the services used in the attack to access the network.

Which of the following objects will he create when he finds that the attack is not defined in the predefined service objects?

A. Custom service objects
B. Compound attack objects
C. Signature attack objects
D. Protocol anomaly attack objects

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
You work as a Network Architect for ABC Inc. The company has a TCP/IP based network. You have established a remote-access VPN network between mobile users and the company's network. You want to implement the following features in the remote-access VPN network:

>> Provide security for the web traffic.
>> Browser clients can support the VPN connection to a host.

Which of the following will you configure to implement the given features in the network?

A. DACL
B. SSL
C. SSH
D. IPsec
Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113
Sam works as a Security Manager for ABC Inc. The company has a Windows-based network. Sam wants to prevent specific traffic from IDP processing in order to reduce false positives.

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114 Fill in the blank with the appropriate tool name.

_____ is a network protocol analyzer tool that is used to capture packet data from an existing network or examine packet data from a pre-saved file.

A. Compound attack objects
B. TShark
C. BlowfishD. Wingate

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116
Which of the following IDs is used to reassemble the fragments of a datagram at the destination point?
A. MAK ID
B. IP address
C. IP identification number
D. SSID

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 117
You work as a Network Administrator at ABC Inc. You want to implement a solution that will automatically disallow connections if an attack is suspected.

Which of the following technologies will you choose to accomplish the task?

A. ACL

B. SRTP
C. IPS
D. IIS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118 Which of the following attacks generates falsified information within an IP header?

A. Web spoofing attack B.
DNS spoofing attack
C. IP spoofing attack
D. ARP spoofing attack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 119 Which of the following statements about Access control list (ACL) are true?

Each correct answer represents a complete solution. (Choose three.)

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

Correct Answer: ABC
Section: (none)
Explanation
Explanation/Reference:

QUESTION 120 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. Internet Key Exchange
B. Authentication Header
C. Encapsulating Security Payload
D. Skinny Client Control Protocol

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 121 Fill in the blank with the appropriate tool name.

_____ consists of flexible system architecture that provides a proper way for conducting industrial audits when it is required to identify unique positions of items.

A. Network-based IDS
B. Baseline audit
C. Active IDS
D. Honey pot detection

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122 You are the Administrator for a corporate network. You are concerned about denial of service attacks.

Which of the following would be most helpful against Denial of Service (DOS) attacks?

A. Honey pot
B. Network surveys
C. Stateful Packet Inspection (SPI) firewall
D. Packet filtering firewall

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 123 Which of the following modules registers DNAT-based and SNAT-based transformations?

A. iptable_raw
B. iptable_nat
C. iptable_mangle
D. iptable_filter

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 124 Which of the following TShark options is used to set capture buffer size in MB?

A. -F
B. -B
C. -G
D. -C

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 125 In which of the following ways can you use the snort tool?

A. Virus, Keylogger, and Packet logger
B. Worm, Sniffer, and Password cracker
C. Firewall, Sniffer, and Keylogger
D. IDS, Packet logger, and Sniffer

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 126 Which of the following would allow you to automatically close connections or restart a server or service when a DoS attack is detected?

A. Signature-based IDS
B. Passive IDS
C. Network-based IDS
D. Active IDS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 127
Which of the following attacks can be mitigated by providing proper training to the employees in an organization?
A. Smurf
B. Social engineering
C. Denial-of-Service
D. Man-in-the-middle

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 128 Which of the following modes is also referred to as client mode?

A. Ad-hoc mode
B. Manage mode
C. Monitor mode
D. Master mode

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 129 Which of the following command-line utilities is used to show the state of current TCP/IP connections?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 130 When no anomaly is present in an Intrusion Detection, but an alarm is generated, the response is known as _____.

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
QUESTION 131
You are the Network Administrator and your company has recently implemented encryption for all emails. You want to check to make sure that the email packages are being encrypted.

What tool would you use to accomplish this?

A. Password cracker
B. Performance Monitor
C. Packet sniffer
D. Vulnerability analyzer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 132 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. Dsniff
B. Kismet
C. KisMAC
D. Snort

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 133
Adam works on a Linux system. He is using Sendmail as the primary application to transmit emails. 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/mailog
B. /log/var/logd
C. /var/log/logmail
D. /var/log/mailog

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 134
You work as a Security Manager 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. WinDump
B. libpcap
C. WinPcap
D. iptables

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 135
Adam works as a Network Administrator for ABC Inc. He wants to prevent the network from DOS attacks.

Which of the following is most useful against DOS attacks?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 136

You work as a System Administrator for ABC Inc. The company has a Linux-based network. You are a root user on the Red Hat operating system. Your network is configured for IPv6 IP addressing.

Which of the following commands will you use to test TCP/IP connectivity?

A. ping
B. ping6
C. traceroute
D. ifconfig

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 137
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 smash guard utility.
B. Using ARP 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.

Correct Answer: BCDE
Section: (none)
Explanation
Explanation/Reference:

QUESTION 138 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. Prepare a chain of custody and handle the evidence carefully.
C. Never exceed the knowledge base of the forensic investigation.
D. Examine original evidence and never rely on the duplicate evidence.

Correct Answer: ABCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 139 Which of the following steps is involved in the network planning process?

A. Documentation and analysis of results
B. Data acquisition
C. Analysis/Forecasting
D. Network-synthesis

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 140 Choose the best explanation for the resulting error when entering the command below.

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 141
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

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 142 Which of the following is a Windows-based tool used for packet analysis?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 143 You work as a Network Administrator for NetTech Inc. Your manager needs to access a particular server on the network from outside the company network. You have a registered IP address assigned to a router on the company network.

Which of the following will be useful for accessing the server from outside the network?

A. Overloading
B. Switch
C. Static NAT
D. Dynamic VLAN

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 144 Which of the following tools is used to detect spam email without checking the content?

A. DCC
B. Sniffer
C. EtherApe
D. Kismet

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:

QUESTION 145
You work as a Network Administrator for a bank. For securing the bank's network, you configure a firewall and an IDS. In spite of these security measures, intruders are able to attack the network. After a close investigation, you find that your IDS is not configured properly and hence is unable to generate alarms when needed.

What type of response is the IDS giving?

A. False Negative
B. False Positive
C. True Positive
D. True Negative

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 146
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. FTP
C. PPP
D. ICMP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 147
You work as a Network Administrator for Net World Inc. You have configured a few routers on the company's network. You are required to accomplish the following goals:

• Encrypt all service passwords immediately.
• Ensure that encryption is also applied on the passwords changed in the future.

You run the following command service password-encryption.

Which of the goals will this action accomplish?

A. The action will accomplish neither of the goals.
B. The action will encrypt all passwords immediately.
C. The action will accomplish both the goals.
D. The action will ensure that encryption is also applied on the passwords changed in the future.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
QUESTION 148 Which of the following commands can change the IOS to be loaded in a router?

A. reload system
B. reboot system
C. boot system
D. load system

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 149 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. RSSI
B. SNR
C. WCS
D. CCA

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 150
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:

• It displays the signal strength of a wireless network, MAC address, SSID, channel details, etc.
• 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. THC-Scan
B. Kismet
C. Absinthe
D. NetStumbler

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 151 Which of the following is known as DNS spoofing?

A. Malicious cache poisoning
B. Trojan horse
C. Smurf attack
D. Social engineering

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 152
Which of the following is a console-based 802.11 layer2 wireless network detector, sniffer, and intrusion detection system?

A. Kismet
B. Hping2
C. Nemesis
D. Scapy

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 153 What is the function of baseline audit?

A. Packet filtering
B. Packet sniffing
C. ARP spoofing
D. Data capturing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 154
Andrew works as a Forensic Investigator for PassGuide Inc. The company has a Windows-based environment. The company's employees use Microsoft Outlook Express as their e-mail client program. E-mails of some employees have been deleted due to a virus attack on the network. Andrew is therefore assigned the task to recover the deleted mails.

Which of the following tools can Andrew use to accomplish the task?

Each correct answer represents a complete solution. (Choose two.)

A. FINALeMAIL
B. EventCombMT
C. R-mail
D. eMailTrackerPro

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 155 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. Forced proxy server
C. Open proxy server
D. Caching proxy server

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 156 Which of the following limits the number of packets seen by tcpdump?

A. IFilters
B. Sender filtering

C. Recipient filtering
D. BPF-based filter

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 157 Which of the following programs can be used to detect stealth port scans performed by a malicious hacker?

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

A. nmap
B. portsentry
C. libnids
D. scanlogd

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 158
Which of the following program loads IOS image into RAM?
A. POST
B. NVRAM
C. Bootstrap
D. TFTP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 159
John works as a Network Administrator for Web Perfect Inc. The company has a wireless LAN network. John has configured shared key authentication on a client. The client and the AP start exchanging the frames to enable authentication.

Which of the following vulnerabilities may occur while the client and the AP exchange the challenge text over the wireless link?

A. Land attack
B. DoS attack
C. Vulnerability attack
D. Man-in-the-middle attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 160
Which of the following attacks sends false ICMP packets in an attempt to cripple a system using random fake Internet source addresses?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 161
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. ARP spoofing
B. NAT spoofing
C. MAC spoofing
D. DNS cache poisoning

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 162 Which of the following types of vulnerability scanners performs a black-box test?

A. Port scanner
B. Web application security scanner
C. CGI scanner
D. Network scanner

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 163 Which of the following devices works as a transparent bridge between the wireless clients and the wired network?

A. Hub
B. Access point
C. Switch
D. Wireless router

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 164 Which of the following group management messages is used by routers to handle the IPv6 multicast routing?

A. OSPF
B. ARP
C. ICMPv6
D. IGMP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 165 Which of the following techniques correlates information found on multiple hard drives?

A. Live analysis B.
Gap analysis
C. Data analysis
D. Cross-drive analysis
Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 166
John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. John wants to redirect all TCP port 80 traffic to UDP port 40, so that he can bypass the firewall of the We-aresecure server.

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

A. PsList
B. Fpipe
C. Cain
D. PsExec

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 167 Which of the following attacks are prevented from a mutual authentication solution?

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

A. Phishing

B. Eavesdropping attack
C. Man-in-the-middle attack
D. Hijacking

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 168 Which of the following are the reasons that network administrators use Access Control Lists?

Each correct answer represents a complete solution. (Choose two.)

A. Removing weak user password
B. Encrypting data to be routed
C. Controlling VTY access into a router
D. Filtering traffic as it passes through a router

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
QUESTION 169 Which of the following tools can be used for passive OS fingerprinting?

A. nmap
B. dig
C. tcpdump
D. ping

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 170 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 host-based IDS
B. Enable verbose logging on the firewall
C. Install a DMZ firewall
D. Install a network-based IDS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 171 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. Enable passive analysis.
C. Define and import OS mappings.
D. Define event action rules filters using the OS relevancy value of the target.
E. Limit the attack relevance rating calculation to a specific IP address range.

Correct Answer: ACDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 172
Adam works as a Senior Programmer for Umbrella Inc. A project has been assigned to him to write a short program to gather user input for a Web application. He wants to keep his program neat and simple. His chooses to use printf(str) where he should have ideally used printf("%s", str).

What attack will his program expose the Web application to?

A. Cross Site Scripting attack
B. Format string attack
C. Sequence++ attack
D. SQL injection attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 173
At which of the following layers of the OSI reference model does a Proxy firewall, also known as Application Gateway Firewall, filter information?

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

A. Transport layer
B. Physical layer
C. Application layer
D. Presentation layer

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 174 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 value
B. Boot field
C. Boot
D. Boot check

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 175 Which of the following is used as a default port by the TELNET utility?

A. 21
B. 80
C. 20
D. 23

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 176 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. Circuit-level gateway
B. Application gateway
C. Proxy server
D. Packet Filtering

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 177 Which of the following is an intrusion detection system that reads all incoming packets and tries to find suspicious patterns known as signatures or rules?

A. IPS
B. NIDS
C. HIDS
D. DMZ

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 178
Which of the following devices is used to identify out-of-date software versions, applicable patches, system upgrades, etc?

A. Retinal scanner
B. Vulnerability scanner
C. Fingerprint reader
D. Smart card reader

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 179
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. Mendax
C. Alchemy Remote Executor
D. Ettercap
Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 180 Which of the following algorithms is used as a default algorithm for ESP extension header in IPv6?

A. Cipher Block Chaining (CBC) Mode
B. Electronic Codebook (ECB) Mode
C. Propagating Cipher Block Chaining (PCBC) Mode
D. Cipher Feedback (CFB) Mode

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 181
Sam works as a Network Administrator for Gentech Inc. He has been assigned a project to develop the rules that define the IDP policy in the rulebase.

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

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

A. IDP Profiler
B. IDP rule notifications
C. IDP rule IP actions
D. IDP appliance deployment mode

Correct Answer: BC

Section: (none)
Explanation

Explanation/Reference:

QUESTION 182 Which of the following files is a Cisco IOS configuration file that resides in RAM?

A. temp-config
B. running-config
C. startup-config
D. ram-config

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 183
Audit trail or audit log is a chronological sequence of audit records, each of which contains evidence directly pertaining to and resulting from the execution of a business process or system function. Under which of the following controls does audit control come?

A. Protective controls
B. Reactive controls
C. Detective controls
D. Preventive controls

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 184 Which of the following fields is NOT included in packet fragmentation?

A. Identification
B. Flag
C. Time to Live
D. Fragment Offset

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 185 Which of the following number ranges is used for the IP Standard ACL?

A. 100-199
B. 1-99
C. 600-699

D. 1000-1099

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 186 Which of the following can be used in an extended access list to filter traffic?

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

A. Source IP address
B. Protocol
C. Destination IP address
D. TCP or UDP port numberE. Destination MAC address

Correct Answer: ABCD
Section: (none)
Explanation
Explanation/Reference:

QUESTION 187 Which of the following responsibilities does not come under the audit process?

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

A. Reviewing the results of the audit procedures.
B. Reporting all facts and circumstances of the irregular and illegal acts.
C. Planning the IT audit engagement based on the assessed level of risk.
D. Applying security policies.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 188 Which of the following firewalls inspects the actual contents of packets?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 189 Which of the following intrusion detection systems (IDS) monitors network traffic and compares it against an established baseline?

A. File-based
B. Network-based
C. Anomaly-based
D. Signature-based

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 190 In which of the following steps of firewall log analysis process is aggregation for nodes defined?

A. Assess available data
B. Visual transformation
C. View transformationD. Process information **Correct Answer:** C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 191 Which of the following has a set of system-independent functions for packet capture and network analysis?

A. WinDump
B. WinPcap
C. libpcap
D. tcpdump

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 192 The general form of the Cisco IOS is a.b.c.de.

Which of the following indicates the major version number of the Cisco IOS?

A. b
B. a
C. e
D. d

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 193 Which of the following protocols is built in the Web server and browser to encrypt data traveling over the Internet?

A. HTTP
B. UDP
C. SSL
D. IPSec

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 194 Which of the following is an attack with IP fragments that cannot be reassembled?

A. Password guessing attack
B. Smurf attack
C. Teardrop attack
D. Dictionary attack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 195
The simplest form of a firewall is a packet filtering firewall. A packet filtering firewall filters packets at the Network layer and Transport layer.

What are the types of information that are filtered at the Network layer of the OSI reference model?

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

A. TCP and UDP port numbers
B. IP addresses
C. TCP/IP protocols
D. TCP control flags

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 196
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. Protocol contexts
B. Ignore connection

C. Session creation
D. Session teardown

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 197 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. FIR filter
B. IM filter
C. Web filter
D. Berkeley Packet Filter

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 198 Which of the following devices are used to implement Network Address Translation (NAT)?

A. Routers and switches
B. Routers and firewalls
C. Firewalls and file servers
D. Switches and firewalls

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 199 Which of the following statements about segmentation of a network using router is true?

Each correct answer represents a complete solution. (Choose three.)

A. Broadcast will not be forwarded to other segment through the router.
B. Number of broadcast domains will be decreased.
C. Filtering can be done based on layer 3 information.
D. Segmenting of a network using router will increase latency.

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 200
Which of the following commands will you use with the tcpdump command to capture the traffic from a filter stored in a file?

A. tcpdump -F file_name
B. tcpdump -D file_name
C. tcpdump -A file_nameD. tcpdump -X file_name

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 201 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. Dsniff
B. Cain
C. Libnids
D. LIDS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 202 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. Implementing anti-virus
C. Using MAC filtering
D. Using WPA encryption

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 203
Which of the following is used to implement a procedure to control inbound and outbound traffic on a network?

A. Sam Spade
B. ACL
C. Cookies
D. NIDS

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 204
You work as a Network Administrator for Net Perfect Inc. The company has a Windows Server 2008 network environment. The network is configured as a Windows Active Directory-based single forest single domain network. The network is configured on IP version 6 protocol. All the computers on the network are connected to a switch device. One day, users complain that they are unable to connect to a file server. You try to ping the client computers from the server, but the pinging fails. You try to ping the server's own loopback address, but it fails to ping. You restart the server, but the problem persists.

What is the most likely cause?

A. The server's NIC is not working.
B. Automatic IP addressing is not working.
C. The server is configured with unspecified IP address.
D. The cable that connects the server to the switch is broken.
E. The switch device is not working.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 205 You are tasked with configuring your routers with a minimum security standard that includes the following:

• A local Username and Password configured on the router
• A strong privilege mode password
• Encryption of user passwords
• Configuring telnet and ssh to authenticate against the router user database

Choose the configuration that meets these requirements best.

A. RouterA(config)#service password-encryption
RouterA(config)#username cisco password PaS$w0Rd
RouterA(config)#enable password n56e&$te
RouterA(config)#line vty 0 4
RouterA(config-line)#login local
B. RouterA(config)#service password-encryption
RouterA(config)#username cisco password PaS$w0Rd
RouterA(config)#enable secret n56e&$te
RouterA(config)#line vty 0 4
RouterA(config-line)#login
C. RouterA(config)#service enable-password-encryption
RouterA(config)#username cisco password PaS$w0Rd
RouterA(config)#enable secret n56e&$te
RouterA(config)#line vty 0 4
RouterA(config-line)#login user
D. RouterA(config)#service password-encryption
RouterA(config)#username cisco password PaS$w0Rd
RouterA(config)#enable secret n56e&$te
RouterA(config)#line vty 0 4
RouterA(config-line)#login local

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 206
Which of the following tools performs comprehensive tests against web servers for multiple items, including over 6100 potentially dangerous files/CGIs?

A. Sniffer
B. Dsniff
C. Snort
D. Nikto

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 207
Which of the following types of firewall ensures that the packets are part of the established session?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 208
Adam works as a professional Computer Hacking Forensic Investigator. A project has been assigned to him to investigate computer of an unfaithful employee of SecureEnet Inc. Suspect's computer runs on Windows operating system.

Which of the following sources will Adam investigate on a Windows host to collect the electronic evidences?

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

A. Slack spaces
B. Swap files
C. Unused and hidden partition
D. Allocated cluster

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 209 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 IP address.

C. Ping the source host with its computer name.
D. Check the IP statistics on the file server.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 210 Distributed Checksum Clearinghouse (DCC) is a hash sharing method of spam email detection.

Which of the following protocols does the DCC use?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 211
Host-based IDS (HIDS) is an Intrusion Detection System that runs on the system to be monitored. HIDS monitors only the data that it is directed to, or originates from the system on which HIDS is installed. Besides monitoring network traffic for detecting attacks, it can also monitor other parameters of the system such as running processes, file system access and integrity, and user logins for identifying malicious activities.

Which of the following tools are examples of HIDS?

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

A. HPing
B. Legion
C. Tripwire
D. BlackIce Defender

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 212
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. Datagram Identification Number field
B. Flags field
C. Fragment Offset field
D. Datagram Length field

Correct Answer: ABC

Section: (none)
Explanation

Explanation/Reference:

QUESTION 213
Which of the following IPv4 to IPv6 transition methods uses encapsulation of IPv6 packets to traverse IPv4 networks?

A. Translation
B. Stack
C. Tunneling
D. Dual-stack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
QUESTION 214
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. 20
B. 21
C. 80
D. 25

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 215
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 EFS.
D. Use a firewall.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 216 Which of the following ports cannot be used to access the router from a computer?

A. Console port

B. Vty
C. Aux port
D. Serial port

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 217
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 218 Which of the following statements are true about the Network Honeypot a 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. Its rules are triggered when a source IP address sends a connection request to the destination IP address and service specified in the rule.
C. It does not support any IP action.
D. It is used to detect reconnoitering activities.

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 219
Which of the following address translation types only translates one (and only one) IP address to another without using ports?

A. Dynamic NAT
B. NAT
C. PAT
D. Static NAT

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 220
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 preattack phase to check the security of the We-aresecure network:

• Gathering information
• Determining the network range
• 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. RIPE
D. SuperScan

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 221 Which of the following methods is used by forensic investigators to acquire an image over the network in a secure manner?

A. DOS boot disk
B. EnCase with a hardware write blocker
C. Linux Live CD
D. Secure Authentication for EnCase (SAFE)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 222 On which of the following interfaces of the router is the clock rate command used?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 223 In which of the following locations can the Cisco IOS file reside?

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

A. NVRAM
B. TFTP server
C. ROM
D. Flash memory

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 224 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

C.

B. WIDS
Snort 2.1.0
D. NFR security

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 225
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. WEP
B. WPA2
C. WPA
D. WEP2

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 226
Which of the following components are used in the implementation of a wireless intrusion prevention system? Each

correct answer represents a part of the solution. (Choose three.)

A. Sensor
B. Console
C. Analyzer
D. Server

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 227 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.

A. None
B. Dynamic NAT
C. Static NAT
D. Both

Correct Answer: B
Section: (none)

Explanation
Explanation/Reference:

QUESTION 228 Which of the following types of audit constructs a risk profile for existing and new projects?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 229
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. Port scanner
C. Web application security scanner
D. Computer worm

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 230
You work as a Network Security Administrator for NetPerfect Inc. The company has a Windowsbased network. You are in charge of the data and network security of the company. While performing a threat log analysis, you observe that one of the database administrators is pilfering confidential data.

What type of threat is this?

A. Zombie
B. External threat
C. Malware
D. Internal threat

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 231 Which of the following types of firewall functions by creating two different communications, one between the client and the firewall, and the other between the firewall and the end server?

A. Stateful firewall

C.

B. Proxy-based firewall
Endian firewall
D. Packet filter firewall

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 232 Which of the following number ranges is used for the IPX Standard ACL?

A. 1200-1299
B. 800-899
C. 1000-1099
D. 900-999

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 233 Which of the following Linux file systems is a journaled file system?

A. ext4
B. ext3
C. ext
D. ext2

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 234
You work as a Network Administrator for Rick International. The company has a TCP/IP-based network. A user named Kevin wants to set an SSH terminal at home to connect to the company's network. You have to configure your company's router for it.

By default, which of the following standard ports does the SSH protocol use for connection?

A. 21
B. 443
C. 80
D. 22

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 235
Which of the following Wireless LAN standard devices is least affected by interference from domestic appliances such as microwave ovens?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 236
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 positives
C. False generation
D. False illusion

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 237
Which of the following vulnerability scanners detects vulnerabilities by actually performing attacks?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 238
Adam works as a professional Computer Hacking Forensic Investigator. He works with the local police. A project has been assigned to him to investigate an iPod, which was seized from a student of the high school. It is suspected that the explicit child pornography contents are stored in the iPod. Adam wants to investigate the iPod extensively.

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

A. Mac OS
B. Windows XP
C. MINIX 3
D. Linux

C.

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 239 Which of the following can be used to mitigate the evil twin phishing attack?

A. Obiwan
B. Magic Lantern
C. SARA
D. IPSec VPN

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 240 Which of the following methods will allow data to be sent on the Internet in a secure format?

A. Browsing
B. Virtual Private Networks
C. Serial Line Interface Protocol
D. Point-to-Point Protocol

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 241 Which of the following protocols is used with a tunneling protocol to provide security?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 242 Which of the following firewalls filters the traffic based on the header of the datagram?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 243 Which of the following intrusion detection systems (IDS) produces the false alarm because of the abnormal behavior of users and network?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 244 Fill in the blank with the appropriate utility.

_____ is a table-based system or structure that defines the rulesets needed to transform or filter network packets.

A. Port Address Translation (PAT)
B. Magic Lantern
C. Static NAT
D. iptables

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 245 Which of the following Denial-of-Service (DoS) attacks employ IP fragmentation mechanism?

Each correct answer represents a complete solution. (Choose two.)

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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 246
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. When the number of SYN packets per second is greater than the sum of the lower SYNs-per-second threshold and the upper SYNs-per-second threshold.
C. Only when the number of SYN packets per second is equal to the sum of the lower SYNs-per-second threshold and the upper SYNs-per-second threshold.
D. When the number of SYN packets per second is smaller than the sum of the lower SYNs-per-second threshold and the upper SYNs-per-second threshold.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 247 Which of the following types of Network Address Translation (NAT) uses a pool of public IP addresses?

A. Dynamic NAT
B. Static NAT
C. Cache NAT
D. Port Address Translation (PAT)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 248
Which of the following technologies is used to detect unauthorized attempts to access and manipulate computer systems locally or through the Internet or an intranet?

A. Intrusion detection system (IDS)
B. Firewall
C. Demilitarized zone (DMZ)
D. Packet filtering

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 249
In which of the following IDS evasion attacks does an attacker send a data packet such that IDS accepts the data packet but the host computer rejects it?

A. Fragmentation overwrite attack
B. Fragmentation overlap attack
C. Evasion attack
D. Insertion attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 250

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. HxD
B. Vedit
C. WinHex
D. Evidor

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 251
Which of the following is a hardware/software platform that is designed to analyze, detect and report on security related events.

NIPS is designed to inspect traffic and based on its configuration or security policy, it can drop the malicious traffic?

A. NIDS
B. HIDS
C. HIPS
D. NIPS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 252
In which of the following attacks does an attacker change the MAC address on the sniffer to one that is the same in another system on the local subnet?

A. MAC duplicating
B. IP spoofing
C. ARP spoofing
D. MAC flooding

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 253
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 threats can be countered by implementing security controls on the perimeters of the network, such as firewalls, which limit user access to the Internet.

B. These are the threats that originate from outside an organization in which the attacker attempts to gain unauthorized access.
C. These are the threats that originate from within the organization.
D. These are the threats intended to flood a network with large volumes of access requests.

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 254
Which of the following tools uses PDA and barcode technologies in order to enable effective identification, control, and reporting of items in a site?

A. Biometric device
B. Smart card
C. Baseline audit
D. Vulnerability scanner

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 255 You want to create a binary log file using tcpdump.
Which of the following commands will you use?

A. tcpdump -d
B. tcpdump -B
C. tcpdump -dd
D. tcpdump -w

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 256
You work as a Network Administrator for Blue Bell Inc. The company has a TCP-based network. The company has two offices in different cities. The company wants to connect the two offices by using a public network. You decide to configure a virtual private network (VPN) between the offices.

Which of the following protocols is used by VPN for tunneling?

A. L2TP
B. IPSec
C. HTTPS
D. SSL

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:

QUESTION 257 Which of the following fields are specified when rules are created for the Network Honeypot rulebase?

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

A. A destination/service match condition
B. Detection settings
C. Response options
D. Operation mode

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 258 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. Insertion
B. Fragmentation overlap
C. Fragmentation overwrite
D. Session splicing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 259
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. IGMP
B. BGP
C. SNMP
D. ICMP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 260 Which of the following are the types of intrusion detection systems?

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

A. Network intrusion detection system (NIDS)
B. Client-based intrusion detection system (CIDS)
C. Host-based intrusion detection system (HIDS)
D. Server-based intrusion detection system (SIDS)

Correct Answer: AC

Section: (none)
Explanation

Explanation/Reference:

QUESTION 261 Which of the following statements are true about an IPv6 network?

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

A. For interoperability, IPv4 addresses use the last 32 bits of IPv6 addresses.
B. It provides improved authentication and security.
C. It uses 128-bit addresses.
D. It increases the number of available IP addresses.
E. It uses longer subnet masks than those used in IPv4.

Correct Answer: ABCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 262 Which of the following can be applied as countermeasures against DDoS attacks?

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

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

Correct Answer: ABDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 263
You work as a Network Administrator for Tech Perfect Inc. The company has a TCP/IP-based network. You have configured an 802.11g Wireless LAN (WLAN) on your network.

Which of the following factors can deteriorate the performance and range of the WLAN?

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

A. Fiberglass partitions
B. Cordless phones
C. Metal ceilings
D. Concrete walls

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 264
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. IPSec
B. WPA
C. WEP
D. L2TP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 265
The promiscuous mode is a configuration of a network card that makes the card pass all traffic it receives to the central processing unit rather than just packets addressed to it.

Which of the following tools works by placing the host system network card into the promiscuous mode?

A. Sniffer
B. THC-Scan
C. NetStumbler
D. Snort

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 266 What netsh command should be run to enable IPv6 routing?

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

A. netsh interface IPv6 show interface
B. netsh interface IPv6 set interface
C. netsh interface IPv6 add address
D. netsh interface IPv6 add routes

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 267 Which of the following commands in MQC tool matches IPv4 and IPv6 packets when IP parameter is missing?

A. Match fr-dlci
B. Match IP precedence
C. Match access-group

D. Match cos

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 268
Which of the following can be configured so that when an alarm is activated, all doors lock and the suspect or intruder is caught between the doors in the dead-space?

A. Host Intrusion Detection System (HIDS)
B. Network Intrusion Detection System (NIDS)
C. Man trap
D. Biometric device

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 269
Your customer is concerned about security. He wants to make certain no one in the outside world can see the IP addresses inside his network.

What feature of a router would accomplish this?

A. Firewall
B. Port forwarding
C. NAT
D. MAC filtering

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 270 The stateful firewalls combine the significant flows into conversations.

Which of the following properties is used to classify a flow?

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

A. Destination port B. Source port
C. Source address
D. Protocol
E. Destination address

Correct Answer: ABCDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 271
In which of the following CAATs (Computer Assisted Auditing Techniques) does an auditor perform tests on computer files and databases?

A. Parallel Simulation
B. Custom Audit Software (CAS)
C. Generalized Audit Software (GAS)
D. Test Data

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 272
You work as a technician for Tech Perfect Inc. You are troubleshooting an Internet name resolution issue. You ping your ISP's DNS server address and find that the server is down. You want to continuously ping the DNS address until you have stopped the command.

Which of the following commands will you use?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 273
You work as a Network Administrator for Infonet Inc. The company has a Windows Server 2008 Active Directory-based single forest multiple domain IPv4 network. All the DNS servers on the network run Windows Server 2008. The users in the network use NetBIOS name to connect network application on the network. You have migrated the network to IPv6-enabled network. Now you want to enable DNS Server to perform lookups in GlobalNames Zone.

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

A. Dnscmd <server name> /config /enableglobalnames 1
B. Dnscmd <server name> /config /globalnamesqueryorder 0
C. Dnscmd <server name> /config /enableglobalnamessupport 1
D. Dnscmd <server name> /config /enableglobalnamessupport 0

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 274
A firewall is a combination of hardware and software, used to provide security to a network. It is used to protect an internal network or intranet against unauthorized access from the Internet or other outside networks. It restricts inbound and outbound access and can analyze all traffic between an internal network and the Internet. Users can configure a firewall to pass or block packets from specific IP addresses and ports.
Which of the following tools works as a firewall for the Linux 2.4 kernel?

A. OpenSSH
B. IPChains
C. Stunnel
D. IPTables

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 275
As a professional hacker, you want to crack the security of secureserver.com. For this, in the information gathering step, you performed scanning with the help of nmap utility to retrieve as many different protocols as possible being used by the secureserver.com so that you could get the accurate knowledge about what services were being used by the secure server.com.

Which of the following nmap switches have you used to accomplish the task?

A. nmap -sS
B. nmap -sT
C. nmap -vO
D. nmap -sO

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 276 You run the tcpdump command line utility and get a report produced by tcpdump.

What information does this report include?

Each correct answer represents a complete solution. (Choose three.)

A. Packets captured
B. Packets dropped by kernel
C. Packets discarded
D. Packets received by filter

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 277 Which of the following methods is a behavior-based IDS detection method?

A. Pattern matching detection
B. Protocol detection
C. Knowledge-based detection
D. Statistical anomaly detection

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 278
Jony works as the Security Manager in ABC Inc. He wants to protect his network from a variant of the Denial-of-Service (DoS) attack. When the rulebase is enabled for protection, the IDP engine checks the traffic that exceeds the traffic thresholds.

Which of the following rulebases is used for this purpose?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 279
An organization has a TCP/IP based network. It uses IPv6 addressing in its network. IPv6 tackles addressing and routing-table problems, and improves the protocol as well.

Which of the following statements is true about IPv6?

A. It implements broadcasting.
B. It eliminates the primary need for Network Address Translation (NAT).
C. It uses symmetric key encryption.
D. Its address is 32 bits in length.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 280 Which of the following IPv6 transition technologies is used by the DirectAccess if a user is in a remote location and a public IPv4 address, instead of public IPv6 address, has been assigned to the computer?

A. 6to4
B. PortProxy
C. Teredo
D. ISATAP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 281 Which of the following describes the term inside global in NAT configuration?

A. It is a local MAC address assigned to a host in a private network.

B. It is the data that comes inside a local network from an external host.
C. It is a local IP address assigned to a host in a private network.
D. It is the registered (public) IP address that represents the inside hosts in private network to the outside network.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 282 Which of the following statements is true about ICMP packets?

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

A. They guarantee the delivery of datagrams.
B. They are used to report errors if a problem in IP processing occurs.
C. The PING utility uses them to verify connectivity between two hosts.
D. They are encapsulated within IP datagrams.
E. They use UDP datagrams.

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 283
You work as the Security Administrator for Prodotxiss Inc. You want to ensure the security of your Wi-Fi enterprise network against the wireless snooping attacks.

Which of the following measures will you take over the site network devices of the network?

A. Disable the SSID broadcast feature of the router.
B. Apply firewalls at appropriate spots.
C. Download and install new firmware patch for the router.
D. Apply a standard ACL on the router.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 284
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. Neighbor Advertisement
B. Neighbor Solicitation
C. Router Solicitation
D. Router Advertisement

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 285 Session splicing is an IDS evasion technique in which an attacker delivers data in multiple small-sized packets to the target computer. Hence, it becomes very difficult for an IDS to detect the attack signatures of such attacks.

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

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

A. Y.A.T.
B. Fragroute
C. Whisker
D. Nessus

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference: