

ECCouncil.312-38.vJun-2024.by.Lien.195q

Number: 312-38
Passing Score: 800
Time Limit: 120
File Version: 21.0

Exam Code: 312-38

Exam Name: Certified Network Defender



Exam A

QUESTION 1

Which of the following layers of the OSI model provides physical addressing?

- A. Application layer
- B. Network layer
- C. Physical layer
- D. Data link layer

Correct Answer: D

Section:

QUESTION 2

Which of the following protocols is described as a connection-oriented and reliable delivery transport layer protocol?

- A. UDP
- B. IP
- C. SSL
- D. TCP

Correct Answer: D

Section:

QUESTION 3

Which of the following protocols is used for inter-domain multicast routing?

- A. BGP
- B. RPC
- C. VoIP
- D. RADIUS

Correct Answer: A

Section:

QUESTION 4

How many layers are present in the OSI layer model?

- A. 5
- B. 4
- C. 7
- D. 9

Correct Answer: C



Section:

QUESTION 5

Which of the following is an electronic device that helps in forwarding data packets along networks?

- A. Router
- B. Hub
- C. Repeater
- D. Gateway

Correct Answer: A

Section:

QUESTION 6

Which of the following protocols sends a jam signal when a collision is detected?

- A. ALOHA
- B. CSMA/CA
- C. CSMA/CD
- D. CSMA

Correct Answer: C

Section:

QUESTION 7

Which of the following key features limits the rate a sender transfers data to guarantee reliable delivery?

- A. Ordered data transfer
- B. Error-free data transfer
- C. Flow control
- D. Congestion control

Correct Answer: C

Section:

QUESTION 8

Blake is working on the company's updated disaster and business continuity plan. The last section of the plan covers computer and data incidence response. Blake is outlining the level of severity for each type of incident in the plan. Unsuccessful scans and probes are at what severity level?

- A. Extreme severity level
- B. Low severity level
- C. High severity level
- D. Mid severity level

Correct Answer: B

Section:



QUESTION 9

An IDS or IDPS can be deployed in two modes. Which deployment mode allows the IDS to both detect and stop malicious traffic?

- A. passive mode
- B. inline mode
- C. promiscuous mode
- D. firewall mode

Correct Answer: B

Section:

QUESTION 10

Which protocol could choose the network administrator for the wireless network design, if he need to satisfied the minimum requirement of 2.4 GHz, 22 MHz of bandwidth, 2 Mbits/s stream for data rate and use DSSS for modulation.

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

Correct Answer: C

Section:

QUESTION 11

Which of the following is designed to detect unwanted changes by observing the flame of the environment associated with combustion?

- A. Fire extinguishing system
- B. None
- C. Gaseous fire-extinguishing systems
- D. sprinkler
- E. Smoke alarm system

Correct Answer: E

Section:

QUESTION 12

Which of the following features is used to generate spam on the Internet by spammers and worms?

- A. AutoComplete
- B. SMTP relay
- C. Server Message Block (SMB) signing
- D. AutoFill

Correct Answer: B

Section:

Explanation:

SMTP relay feature of e-mail servers allows them to forward e-mail to other e-mail servers. Unfortunately, this feature is exploited by spammers and worms to generate spam on the Internet.

QUESTION 13

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:

Explanation:

Dsniff is a set of tools that are used for sniffing passwords, e-mail, and HTTP traffic. Some of the tools of Dsniff include dsniiff, arpredirect, macof, tcpkill, tcpnice, filesnarf, and mailsnarf. Dsniff 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.

Answer option B is incorrect. Cain is a multipurpose tool that can be used to perform many tasks such as Windows password cracking, Windows enumeration, and VoIP session sniffing. This password cracking program can perform the following types of password cracking attacks:

Dictionary attack

Brute force attack

Rainbow attack Hybrid attack

Answer options D and C are incorrect. These tools are port scan detection tools that are used in the Linux operating system.

QUESTION 14

Which of the following IP class addresses are not allotted to hosts? Each correct answer represents a complete solution. Choose all that apply.

- A. Class C
- B. Class D
- C. Class A
- D. Class B
- E. Class E

Correct Answer: B, E

Section:

Explanation:

Class addresses D and E are not allotted to hosts. Class D addresses are reserved for multicasting, and their address range can extend from 224 to 239. Class E addresses are reserved for experimental purposes. Their addresses range from 240 to 254.

Answer option C is incorrect. Class A addresses are specified for large networks. It consists of up to 16,777,214 client devices (hosts), and their address range can extend from 1 to 126.

Answer option D is incorrect. Class B addresses are specified for medium size networks. It consists of up to 65,534 client devices, and their address range can extend from 128 to 191.

Answer option A is incorrect. Class C addresses are specified for small local area networks (LANs). It consists of up to 245 client devices, and their address range can extend from 192 to 223.

QUESTION 15

A war dialer is a tool that is used to scan thousands of telephone numbers to detect vulnerable modems. It provides an attacker unauthorized access to a computer. Which of the following tools can an attacker use to perform war dialing? Each correct answer represents a complete solution. Choose all that apply.

- A. ToneLoc
- B. Wingate
- C. THC-Scan
- D. NetStumbler

Correct Answer: A, C

Section:

Explanation:

THC-Scan and ToneLoc are tools used for war dialing. A war dialer is a tool that is used to scan thousands of telephone numbers to detect vulnerable modems. It provides the attacker unauthorized access to a computer.

Answer option D is incorrect. NetStumbler 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. It detects wireless networks and marks their relative position with a GPS. It uses an 802.11 Probe Request that has been sent to the broadcast destination address. Answer option B is incorrect. Wingate is a proxy server.

QUESTION 16

Which of the following protocols is used to share information between routers to transport IP Multicast packets among networks?

- A. RSVP
- B. DVMRP
- C. RPC
- D. LWAPP

Correct Answer: B

Section:

Explanation:

The Distance Vector Multicast Routing Protocol (DVMRP) is used to share information between routers to transport IP Multicast packets among networks. It uses a reverse path-flooding technique and is used as the basis for the Internet's multicast backbone (MBONE). In particular, DVMRP is notorious for poor network scaling, resulting from reflooding, particularly with versions that do not implement pruning. DVMRP's flat unicast routing mechanism also affects its capability to scale.

Answer option A is incorrect. The Resource Reservation Protocol (RSVP) is a Transport layer protocol designed to reserve resources across a network for an integrated services Internet. RSVP does not transport application data but is rather an Internet control protocol, like ICMP, IGMP, or routing protocols. RSVP provides receiver-initiated setup of resource reservations for multicast or unicast data flows with scaling and robustness. RSVP can be used by either hosts or routers to request or deliver specific levels of quality of service (QoS) for application data streams. RSVP defines how applications place reservations and how they can leave the reserved resources once the need for them has ended. RSVP operation will generally result in resources being reserved in each node along a path.

Answer option C is incorrect. A remote procedure call (RPC) hides the details of the network by using the common procedure call mechanism familiar to every programmer. Like any ordinary procedure, RPC is also synchronous and parameters are passed to it. A process of the client calls a function on a remote server and remains suspended until it gets back the results.

Answer option D is incorrect. LWAPP (Lightweight Access Point Protocol) is a protocol used to control multiple Wi-Fi wireless access points at once. This can reduce the amount of time spent on configuring, monitoring, or troubleshooting a large network. This also allows network administrators to closely analyze the network.

QUESTION 17

Which of the following is a technique for gathering information about a remote network protected by a firewall?

- A. Firewalking
- B. Warchalking
- C. Wardriving
- D. Wardialing

Correct Answer: A

Section:

Explanation:

Fire walking is a technique for gathering information about a remote network protected by a firewall. This technique can be used effectively to perform information gathering attacks. In this technique, an attacker sends a crafted packet with a TTL value that is set to expire one hop past the firewall. If the firewall allows this crafted packet through, it forwards the packet to the next hop. On the next hop, the packet expires and elicits an ICMP "TTL expired in transit" message to the attacker. If the firewall does not allow the traffic, there should be no response, or an ICMP "administratively prohibited" message should be returned to the attacker. A malicious attacker can use firewalking to determine the types of ports/ protocols that can bypass the firewall. To use firewalking, the attacker needs the IP address of the last known gateway before the firewall and the IP address of a host located behind the firewall. The main drawback of this technique is that if an administrator blocks ICMP packets from leaving the network, it is ineffective.

Answer option B is incorrect. Warchalking is the drawing of symbols in public places to advertise an open Wi-Fi wireless network. Having found a Wi-Fi node, the warchalker draws a special symbol on a nearby object, such as a wall, the pavement, or a lamp post. The name warchalking is derived from the cracker terms war dialing and war driving.

Answer option C is incorrect. War driving, also called access point mapping, is the act of locating and possibly exploiting connections to wireless local area networks while driving around a city or elsewhere. To do war driving, one needs a vehicle, a computer (which can be a laptop), a wireless Ethernet card set to work in promiscuous mode, and some kind of an antenna which can be mounted on top of or positioned inside the car. Because a wireless LAN may have a range that extends beyond an office building, an outside user may be able to intrude into the network, obtain a free Internet connection, and possibly gain access to company records and other resources.

Answer option D is incorrect. War dialing or wardialing is a technique of using a modem to automatically scan a list of telephone numbers, usually dialing every number in a local area code to search for computers, Bulletin board systems, and fax machines. Hackers use the resulting lists for various purposes, hobbyists for exploration, and crackers - hackers that specialize in computer security - for password guessing.

QUESTION 18

Which of the following is an Internet application protocol used for transporting Usenet news articles between news servers and for reading and posting articles by end-user client applications?

- A. NNTP
- B. BOOTP
- C. DCAP
- D. NTP

Correct Answer: A

Section:

Explanation:

The Network News Transfer Protocol (NNTP) is an Internet application protocol used for transporting Usenet news articles (netnews) between news servers and for reading and posting articles by end user client applications. NNTP is designed so that news articles are stored in a central database, allowing the subscriber to select only those items that he wants to read.

Answer option D is incorrect. Network Time Protocol (NTP) is used to synchronize the timekeeping among the number of distributed time servers and clients. It is used for the time management in a large and diverse network that contains many interfaces. In this protocol, servers define the time, and clients have to be synchronized with the defined time. These clients can choose the most reliable source of time defined from the several NTP servers for their information transmission. Answer option C is incorrect. The Data Link Switching Client Access Protocol (DCAP) is an application layer protocol that is used between workstations and routers for transporting SNA/NetBIOS traffic over TCP sessions. It was introduced in order to address a few deficiencies by the Data Link Switching Protocol (DLSw). The DLSw raises the important issues of scalability and efficiency, and since DLSw is a switch-to-switch protocol, it is not efficient when implemented on workstations. DCAP was introduced in order to address these issues.

Answer option B is incorrect. The BOOTP protocol is used by diskless workstations to collect configuration information from a network server. It is also used to acquire a boot image from the server.

QUESTION 19

Which of the following attacks is a class of brute force attacks that depends on the higher likelihood of collisions found between random attack attempts and a fixed degree of permutations?

- A. Phishing attack
- B. Replay attack
- C. Birthday attack
- D. Dictionary attack

Correct Answer: C

Section:

Explanation:

A birthday attack is a class of brute force attacks that exploits the mathematics behind the birthday problem in probability theory. It is a type of cryptography attack. The birthday attack depends on the higher likelihood of collisions found between random attack attempts and a fixed degree of permutations.

Answer option D is incorrect. A dictionary attack is a technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or passphrase by searching likely possibilities. A dictionary attack uses a brute-force technique of successively trying all the words in an exhaustive list (from a prearranged list of values). In contrast with a normal brute force attack, where a large proportion key space is searched systematically, a dictionary attack tries only those possibilities which are most likely to succeed, typically derived from a list of words in a dictionary. Generally, dictionary attacks succeed because many people have a tendency to choose passwords which are short (7 characters or fewer), single words found in dictionaries, or simple, easily-predicted variations on words, such as appending a digit.

Answer option A is incorrect. Phishing is a type of internet fraud attempted by hackers. Hackers try to log into system by masquerading as a trustworthy entity and acquire sensitive information, such as, username, password, bank account details, credit card details, etc. After collecting this information, hackers try to use this information for their gain.

Answer option B is incorrect. A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack by IP packet substitution.

QUESTION 20

Which of the following is a digital telephone/telecommunication network that carries voice, data, and video over an existing telephone network infrastructure?

- A. PPP
- B. Frame relay
- C. ISDN
- D. X.25

Correct Answer: C

Section:

Explanation:

Integrated Services Digital Network (ISDN) is a digital telephone/telecommunication network that carries voice, data, and video over an existing telephone network infrastructure. It requires an ISDN modem at both the ends of a transmission. ISDN is designed to provide a single interface for hooking up a telephone, fax machine, computer, etc.

ISDN has two levels of service, i.e., Basic Rate Interface (BRI) and Primary Rate Interface (PRI).

Answer option A is incorrect. The Point-to-Point Protocol, or PPP, is a data link protocol commonly used to establish a direct connection between two networking nodes. It can provide connection authentication, transmission encryption privacy, and compression. PPP is commonly used as a data link layer protocol for connection over synchronous and asynchronous circuits, where it has largely superseded the older, non-standard Serial Line Internet Protocol (SLIP) and telephone company mandated standards (such as Link Access Protocol, Balanced (LAPB) in the X.25 protocol suite). PPP was designed to work with numerous network layer protocols, including Internet Protocol (IP), Novell's Internetwork Packet Exchange (IPX), NBF, and AppleTalk.

Answer option D is incorrect. The X.25 protocol, adopted as a standard by the Consultative Committee for International Telegraph and Telephone (CCITT), is a commonly-used network protocol. The X.25 protocol allows computers on different public networks (such as CompuServe, Tymnet, or a TCP/IP network) to communicate through an intermediary computer at the network layer level. X.25's protocols correspond closely to the data-link and physical-layer protocols defined in the Open Systems Interconnection (OSI) communication model.

Answer option B is incorrect. Frame relay is a telecommunication service designed for cost-efficient data transmission for intermittent traffic between local area networks (LANs) and between end-points in a wide area network (WAN). Frame relay puts data in a variable-size unit called a frame. It checks for lesser errors as compared to other traditional forms of packet switching and hence speeds up data transmission. When an error is detected in a frame, it is simply dropped.

The end points are responsible for detecting and retransmitting dropped frames.

**QUESTION 21**

FILL BLANK

Fill in the blank with the appropriate term.

_____ is a prime example of a high-interaction honeypot.

- A. Honeynet

Correct Answer: A

Section:

Explanation:

Honeynet is a prime example of a high-interaction honeypot. Two or more honeypots on a network form a honeynet. Typically, a honeynet is used for monitoring a larger and/or more diverse network in which one honeypot may not be sufficient. Honeynets and honeypots are usually implemented as parts of larger network intrusion-detection systems. A honeyfarm is a centralized collection of honeypots and analysis tools.

QUESTION 22

FILL BLANK

Fill in the blank with the appropriate term.

_____ is an enumeration technique used to glean information about computer systems on a network and the services running its open ports.

- A. Banner grabbing

Correct Answer: A

Section:

Explanation:

Banner grabbing is an enumeration technique used to glean information about computer systems on a network and the services running its open ports.

Administrators can use this to take inventory of the systems and services on their network. An intruder however can use banner grabbing in order to find network hosts that are running versions of applications and operating systems with known exploits.

Some examples of service ports used for banner grabbing are those used by Hyper Text Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP); ports 80, 21, and 25 respectively. Tools commonly used to perform banner grabbing are Telnet, which is included with most operating systems, and Netcat.

For example, one could establish a connection to a target host running a Web service with netcat, then send a bad html request in order to get information about the service on the host: [root@prober] nc

```
www.targethost.com 80
```

```
HEAD / HTTP/1.1
```

```
HTTP/1.1 200 OK
```

```
Date: Mon, 11 May 2009 22:10:40 EST
```

```
Server: Apache/2.0.46 (Unix) (Red Hat/Linux)
```

```
Last-Modified: Thu, 16 Apr 2009 11:20:14 PST
```

```
ETag: "1986-69b-123a4bc6"
```

```
Accept-Ranges: bytes
```

```
Content-Length: 1110
```

```
Connection: close
```

```
Content-Type: text/html
```

The administrator can now catalog this system or an intruder now knows what version of Apache to look for exploits.

QUESTION 23

John works as a C programmer. He develops the following C program:

```
#include <stdlib.h>
#include <stdio.h>
#include <string.h>
int buffer(char *str) {
    char buffer1[10];
    strcpy(buffer1, str);
    return 1;
}
int main(int argc, char *argv[]) {
    buffer (argv[1]);
    printf("Executed\n");
    return 1;
}
```

His program is vulnerable to a _____ attack.

- A. SQL injection
- B. Denial-of-Service
- C. Buffer overflow
- D. Cross site scripting

Correct Answer: C

Section:

Explanation:

This program takes a user-supplied string and copies it into 'buffer1', which can hold up to 10 bytes of data. If a user sends more than 10 bytes, it would result in a buffer overflow.

QUESTION 24

FILL BLANK



Fill in the blank with the appropriate term. _____ is the complete network configuration and information toolkit that uses multi-threaded and multi-connection technologies in order to be very fast and efficient.

A. NetRanger

Correct Answer: A

Section:

Explanation:

NetRanger is the complete network configuration and information toolkit that includes the following tools: a Ping tool, Trace Route tool, Host Lookup tool, Internet time synchronizer, Whois tool, Finger Unix hosts tool, Host and port scanning tool, check multiple POP3 mail accounts tool, manage dialup connections tool, Quote of the day tool, and monitor Network Settings tool. These tools are integrated in order to use an application interface with full online help. NetRanger is designed for both new and experienced users. This tool is used to help diagnose network problems and to get information about users, hosts, and networks on the Internet or on a user computer network. NetRanger uses multi-threaded and multi-connection technologies in order to be very fast and efficient.

QUESTION 25

FILL BLANK

Fill in the blank with the appropriate term. A _____ device is used for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits.

A. biometric

Correct Answer: A

Section:

Explanation:

A biometric device is used for uniquely recognizing humans based upon one or more intrinsic, physical, or behavioral traits.

Biometrics is used as a form of identity access management and access control. It is also used to identify individuals in groups that are under surveillance.

Biometric characteristics can be divided into two main classes:

1. Physiological: These devices are related to the shape of the body. These are not limited to the fingerprint, face recognition, DNA, hand and palm geometry, and iris recognition, which has largely replaced the retina and odor/scent.
2. Behavioral: These are related to the behavior of a person. They are not limited to the typing rhythm, gait, and voice.

QUESTION 26

Which of the following analyzes network traffic to trace specific transactions and can intercept and log traffic passing over a digital network? Each correct answer represents a complete solution. Choose all that apply.

- A. Wireless sniffer
- B. Spectrum analyzer
- C. Protocol analyzer
- D. Performance Monitor

Correct Answer: A, C

Section:

Explanation:

Protocol analyzer (also known as a network analyzer, packet analyzer or sniffer, or for particular types of networks, an Ethernet sniffer or wireless sniffer) is computer software or computer hardware that can intercept and log traffic passing over a digital network. As data streams flow across the network, the sniffer captures each packet and, if needed, decodes and analyzes its content according to the appropriate RFC or other specifications.

Answer option D is incorrect. Performance Monitor is used to get statistical information about the hardware and software components of a server.

Answer option B is incorrect. A spectrum analyzer, or spectral analyzer, is a device that is used to examine the spectral composition of an electrical, acoustic, or optical waveform. It may also measure the power spectrum.

QUESTION 27

In which of the following conditions does the system enter ROM monitor mode? Each correct answer represents a complete solution. Choose all that apply.

- A. The router does not have a configuration file.

- B. There is a need to set operating parameters.
- C. The user interrupts the boot sequence.
- D. The router does not find a valid operating system image.

Correct Answer: C, D

Section:

Explanation:

The system enters ROM monitor mode if the router does not find a valid operating system image, or if a user interrupts the boot sequence. From ROM monitor mode, a user can boot the device or perform diagnostic tests. Answer option A is incorrect. If the router does not have a configuration file, it will automatically enter Setup mode when the user switches it on. Setup mode creates an initial configuration. Answer option B is incorrect. Privileged EXEC is used for setting operating parameters.

QUESTION 28

Which of the following protocols is used for exchanging routing information between two gateways in a network of autonomous systems?

- A. IGMP
- B. ICMP
- C. EGP
- D. OSPF

Correct Answer: C

Section:

Explanation:

EGP stands for Exterior Gateway Protocol. It is used for exchanging routing information between two gateways in a network of autonomous systems. This protocol depends upon periodic polling with proper acknowledgements to confirm that network connections are up and running, and to request for routing updates. Each router requests its neighbor at an interval of 120 to 480 seconds, for sending the routing table updates. The neighbor host then responds by sending its routing table. EGP-2 is the latest version of EGP.

Answer option B is incorrect. Internet Control Message Protocol (ICMP) is a maintenance protocol that allows routers and host computers to swap basic control information when data is sent from one computer to another. It is generally considered a part of the IP layer. It allows the computers on a network to share error and status information. An ICMP message, which is encapsulated within an IP datagram, is very useful to troubleshoot the network connectivity and can be routed throughout the Internet.

Answer option A is incorrect. Internet Group Management Protocol (IGMP) is a communication protocol that multicasts messages and information among all member devices in an IP multicast group. However, multicast traffic is sent to a single MAC address but is processed by multiple hosts. It can be effectively used for gaming and showing online videos. IGMP is vulnerable to network attacks.

Answer option D is incorrect. Open Shortest Path First (OSPF) is a routing protocol that is used in large networks. Internet Engineering Task Force (IETF) designates OSPF as one of the Interior Gateway Protocols. A host uses OSPF to obtain a change in the routing table and to immediately multicast updated information to all the other hosts in the network.

QUESTION 29

Which of the following is a 16-bit field that identifies the source port number of the application program in the host that is sending the segment?

- A. Sequence Number
- B. Header Length
- C. Acknowledgment Number
- D. Source Port Address

Correct Answer: D

Section:

Explanation:

Source Port Address is a 16-bit field that identifies the source port number of the application program in the host that is sending the segment.

Answer option C is incorrect. This is a 32-bit field that identifies the byte number that the sender of the segment is expecting to receive from the receiver.

Answer option B is incorrect. This is a 4-bit field that defines the 4-byte words in the TCP header. The header length can be between 20 and 60 bytes. Therefore, the value of this field can be between 5 and 15. Answer option A is incorrect. This is a 32-bit field that identifies the number assigned to the first byte of data contained in the segment.

QUESTION 30

Which of the following OSI layers establishes, manages, and terminates the connections between the local and remote applications?

- A. Data Link layer
- B. Network layer
- C. Application layer
- D. Session layer

Correct Answer: D

Section:

Explanation:

The session layer of the OSI/RM controls the dialogues (connections) between computers. It establishes, manages and terminates the connections between the local and remote application. It provides for full-duplex, half-duplex, or simplex operation, and establishes checkpointing, adjournment, termination, and restart procedures. The OSI model made this layer responsible for graceful close of sessions, which is a property of the Transmission Control Protocol, and also for session checkpointing and recovery, which is not usually used in the Internet Protocol Suite. The Session Layer is commonly implemented explicitly in application environments that use remote procedure calls.

Answer option C is incorrect. The Application Layer of TCP/IP model refers to the higher-level protocols used by most applications for network communication.

Examples of application layer protocols include the File Transfer Protocol (FTP) and the Simple Mail Transfer Protocol (SMTP). Data coded according to application layer protocols are then encapsulated into one or more transport layer protocols, which in turn use lower layer protocols to affect actual data transfer.

Answer option A is incorrect. The Data Link Layer is Layer 2 of the seven-layer OSI model of computer networking. It corresponds to or is part of the link layer of the TCP/IP reference model. The Data Link Layer is the protocol layer which transfers data between adjacent network nodes in a wide area network or between nodes on the same local area network segment. The Data Link Layer provides the functional and procedural means to transfer data between network entities and might provide the means to detect and possibly correct errors that may occur in the Physical Layer. Examples of data link protocols are Ethernet for local area networks (multi-node), the Point-to-Point Protocol (PPP), HDLC, and ADCCP for point-to-point (dual-node) connections.

Answer option B is incorrect. The network layer controls the operation of subnet, deciding which physical path the data should take, based on network conditions, priority of service, and other factors. Routers work on the Network layer of the OSI stack.

QUESTION 31

Adam, a malicious hacker, is sniffing an unprotected Wi-Fi network located in a local store with Wireshark to capture hotmail e-mail traffic. He knows that lots of people are using their laptops for browsing the Web in the store. Adam wants to sniff their e-mail messages traversing the unprotected Wi-Fi network. Which of the following Wireshark filters will Adam configure to display only the packets with hotmail email messages?

- A. (http = "login.pass.com") && (http contains "SMTP")
- B. (http contains "email") && (http contains "hotmail")
- C. (http contains "hotmail") && (http contains "Reply-To")
- D. (http = "login.passport.com") && (http contains "POP3")

Correct Answer: C

Section:

Explanation:

Adam will use (http contains "hotmail") && (http contains "Reply-To") filter to display only the packets with hotmail email messages. Each Hotmail message contains the tag Reply-To: and "xxx-xxx- xxx.xxx.hotmail.com" in the received tag. Wireshark is a free packet sniffer computer application. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Wireshark is very similar to tcpdump, but it has a graphical front-end, and many more information sorting and filtering options. It allows the user to see all traffic being passed over the network (usually an Ethernet network but support is being added for others) by putting the network interface into promiscuous mode. Wireshark uses pcap to capture packets, so it can only capture the packets on the networks supported by pcap. It has the following features: Data can be captured "from the wire" from a live network connection or read from a file that records the already-captured packets. Live data can be read from a number of types of network, including Ethernet, IEEE 802.11, PPP, and loopback. Captured network data can be browsed via a GUI, or via the terminal (command line) version of the utility, tshark. Captured files can be programmatically edited or converted via command-line switches to the "editcap" program. Data display can be refined using a display filter. Plugins can be created for dissecting new protocols.

Answer options B, A, and D are incorrect. These are invalid tags.

QUESTION 32

Which of the following are the distance-vector routing protocols? Each correct answer represents a complete solution. Choose all that apply.

- A. IS-IS
- B. OSPF
- C. IGRP
- D. RIP

Correct Answer: C, D

Section:

Explanation:

Following are the two distance-vector routing protocols:

RIP: RIP is a dynamic routing protocol used in local and wide area networks. As such, it is classified as an interior gateway protocol (IGP). It uses the distancevector routing algorithm. It employs the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination. It implements the split horizon, route poisoning, and hold-down mechanisms to prevent incorrect routing information from being propagated.

IGRP: Interior Gateway Routing Protocol (IGRP) is a Cisco proprietary distance vector Interior Gateway Protocol (IGP). It is used by Cisco routers to exchange routing data within an autonomous system (AS). This is a classful routing protocol and does not support variable length subnet masks (VLSM). IGRP supports multiple metrics for each route, including bandwidth, delay, load, MTU, and reliability. Answer options B and A are incorrect. OSPF and IS-IS are link state routing protocols.

QUESTION 33

With which of the following forms of acknowledgment can the sender be informed by the data receiver about all segments that have arrived successfully?

- A. Block Acknowledgment
- B. Negative Acknowledgment
- C. Cumulative Acknowledgment
- D. Selective Acknowledgment

Correct Answer: D

Section:

Explanation:

Selective Acknowledgment (SACK) is one of the forms of acknowledgment. With selective acknowledgments, the sender can be informed by a data receiver about all segments that have arrived successfully, so the sender retransmits only those segments that have actually been lost. The selective acknowledgment extension uses two TCP options: The first is an enabling option, "SACK-permitted", which may be sent in a SYN segment to indicate that the SACK option can be used once the connection is established. The other is the SACK option itself, which can be sent over an established connection once permission has been given by "SACK-permitted".

Answer option A is incorrect. Block Acknowledgment (BA) was initially defined in IEEE 802.11e as an optional scheme to improve the MAC efficiency. IEEE 802.11n capable devices are also referred to as High Throughput (HT) devices.

Instead of transmitting an individual ACK for every MPDU, multiple MPDUs can be acknowledged together using a single BA frame. Block Ack (BA) contains bitmap size of 64*16 bits. Each bit of this bitmap represents the status (success/ failure) of an MPDU.

Answer option B is incorrect. With Negative Acknowledgment, the receiver explicitly notifies the sender which packets, messages, or segments were received incorrectly that may need to be retransmitted.

Answer option C is incorrect. With Cumulative Acknowledgment, the receiver acknowledges that it has correctly received a packet, message, or segment in a stream which implicitly informs the sender that the previous packets were received correctly. TCP uses cumulative acknowledgment with its TCP sliding window.

QUESTION 34

FILL BLANK

Fill in the blank with the appropriate term. _____ is a method for monitoring the e-mail delivery to the intended recipient.

- A. Email tracking

Correct Answer: A

Section:

Explanation:

Email tracking is a method for monitoring the e-mail delivery to the intended recipient. Most tracking technologies utilize some form of digitally time-stamped record to reveal the exact time and date at which e-mail was received or opened, as well the IP address of the recipient. When a user uses such tools to send an e-mail, forward an e-mail, reply to an e-mail, or modify an e-mail, the resulting actions and tracks of the original e-mail are



logged. The sender is notified of all actions performed on the tracked e-mail by an automatically generated e-mail. eMailTracker Pro and MailTracking.com are the tools that can be used to perform email tracking.

QUESTION 35

You work as the network administrator for uCertify Inc. The company has planned to add the support for IPv6 addressing. The initial phase deployment of IPv6 requires support from some IPv6-only devices. These devices need to access servers that support only IPv4. Which of the following tools would be suitable to use?

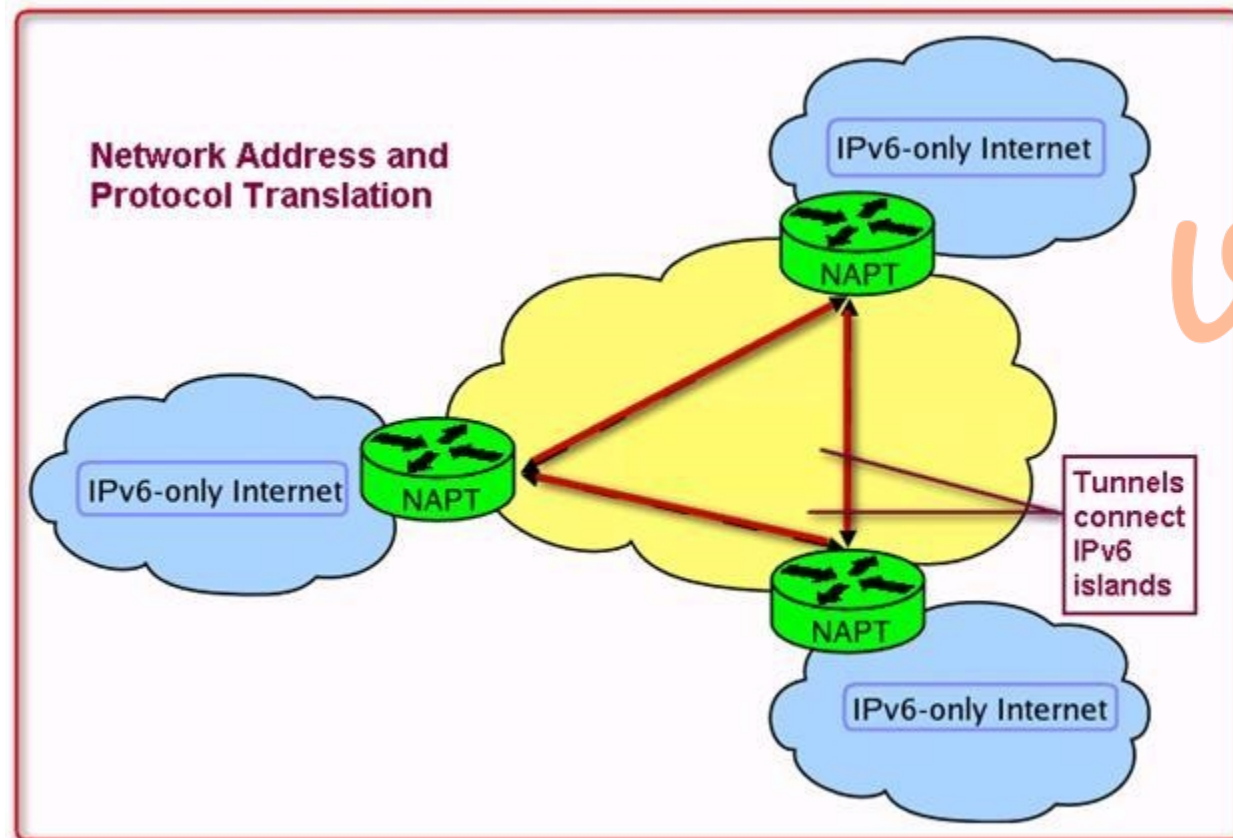
- A. Multipoint tunnels
- B. NAT-PT
- C. Point-to-point tunnels
- D. Native IPv6

Correct Answer: B

Section:

Explanation:

NAT-PT (Network address translation-Protocol Translation) is useful when an IPv4-only host needs to communicate with an IPv4-only host. NAT-PT (Network Address Translation-Protocol Translation) is an implementation of RFC 2766 as specified by the IETF. NAT-PT was designed so that it can be run on low-end, commodity hardware. NAT-PT runs in user space, capturing and translating packets between the IPv6 and IPv4 networks (and vice-versa). NAT-PT uses the Address Resolution Protocol (ARP) and Neighbor Discovery (ND) on the IPv4 and IPv6 network systems, respectively.



NAT-Protocol Translation can be used to translate both the source and destination IP addresses.

Answer option D is incorrect. Native IPv6 is of use when the IPv6 deployment is pervasive, with heavy traffic loads.

Answer option C is incorrect. Point-to-point tunnels work well when IPv6 is needed only in a subset of sites. These point-to-point tunnels act as virtual point-to-point serial link. These are useful when the traffic is of very high volume.

Answer option A is incorrect. The multipoint tunnels are used for IPv6 deployment even when IPv6 is needed in a subset of sites and is suitable when the traffic is infrequent and of less predictable volume.

QUESTION 36

Which of the following types of cyberstalking damages the reputation of their victim and turns other people against them by setting up their own Websites, blogs, or user pages for this purpose?

- A. False accusation
- B. Attempts to gather information about the victim

- C. Encouraging others to harass the victim
- D. False victimization

Correct Answer: A

Section:

Explanation:

In false accusations, many cyberstalkers try to damage the reputation of their victim and turn other people against them. They post false information about them on Websites. They may set up their own Websites, blogs, or user pages for this purpose. They post allegations about the victim to newsgroups, chat rooms, or other sites that allow public contributions.

Answer option D is incorrect. In false victimization, the cyberstalker claims that the victim is harassing him/her.

Answer option C is incorrect. In this type of cyberstalking, many cyberstalkers try to involve third parties in the harassment. They claim that the victim has harmed the stalker in some way, or may post the victim's name and telephone number in order to encourage others to join the pursuit.

Answer option B is incorrect. In an attempt to gather information, cyberstalkers may approach their victim's friends, family, and work colleagues to obtain personal information. They may advertise for information on the Internet. They often will monitor the victim's online activities and attempt to trace their IP address in an effort to gather more information about their victims.

QUESTION 37

Which of the following IP class addresses are not allotted to hosts? Each correct answer represents a complete solution. Choose all that apply.

- A. Class A
- B. Class B
- C. Class D
- D. Class E
- E. Class C

Correct Answer: C, D

Section:

Explanation:

Class addresses D and E are not allotted to hosts. Class D addresses are reserved for multicasting, and their address range can extend from 224 to 239. Class E addresses are reserved for experimental purposes. Their addresses range from 240 to 254.

Answer option A is incorrect. Class A addresses are specified for large networks. It consists of up to 16,777,214 client devices (hosts), and their address range can extend from 1 to 126.

Answer option B is incorrect. Class B addresses are specified for medium size networks. It consists of up to 65,534 client devices, and their address range can extend from 128 to 191.

Answer option E is incorrect. Class C addresses are specified for small local area networks (LANs). It consists of up to 245 client devices, and their address range can extend from 192 to 223.

QUESTION 38

Which of the following is a management process that provides a framework for promoting quick recovery and the capability for an effective response to protect the interests of its brand, reputation, and stakeholders?

- A. Log analysis
- B. Incident handling
- C. Business Continuity Management
- D. Patch management

Correct Answer: C

Section:

Explanation:

Business Continuity Management is a management process that determines potential impacts that are likely to threaten an organization. It provides a framework for promoting quick recovery and the capability for an effective response to protect the interests of its brand, reputation, and stakeholders. Business continuity management includes disaster recovery, business recovery, crisis management, incident management, emergency management, product recall, contingency planning, etc.

Answer option D is incorrect. Patch management is an area of systems management that involves acquiring, testing, and installing multiple patches (code changes) to an administered computer system. Patch management includes the following tasks:

Maintaining current knowledge of available patches Deciding what patches are appropriate for particular systems Ensuring that patches are installed properly Testing systems after installation, and documenting all associated procedures, such as specific configurations required A number of products are available to automate patch management tasks, including RingMaster's Automated Patch Management, PatchLink Update, and Gibraltar's Everguard.

Answer option A is incorrect. This option is invalid.

Answer option B is incorrect. Incident handling is the process of managing incidents in an Enterprise, Business, or an Organization. It involves the thinking of the prospective suitable to the enterprise and then the implementation of the prospective in a clean and manageable manner. It involves completing the incident report and presenting the conclusion to the management and providing ways to improve the process both from a technical and administrative aspect. Incident handling ensures that the overall process of an enterprise runs in an uninterrupted continuity.

QUESTION 39

FILL BLANK

Fill in the blank with the appropriate term. In the _____ method, a device or computer that transmits data needs to first listen to the channel for an amount of time to check for any activity on the channel.

A. CSMA/CA

Correct Answer: A

Section:

Explanation:

Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) is an access method used by wireless networks (IEEE 802.11). In this method, a device or computer that transmits data needs to first listen to the channel for an amount of time to check for any activity on the channel. If the channel is sensed as idle, the device is allowed to transmit data. If the channel is busy, the device postpones its transmission. Once the channel is clear, the device sends a signal telling all other devices not to transmit data, and then sends its packets. In Ethernet (IEEE 802.3) networks that use CSMA/CD, the device or computer continues to wait for a time and checks if the channel is still free. If the channel is free, the device transmits packets and waits for an acknowledgment signal indicating that the packets were received.

QUESTION 40

Which of the following organizations is responsible for managing the assignment of domain names and IP addresses?

A. ISO

B. ICANN

C. W3C

D. ANSI

Correct Answer: B

Section:

Explanation:

ICANN stands for Internet Corporation for Assigned Names and Numbers. ICANN is responsible for managing the assignment of domain names and IP addresses. ICANN's tasks include responsibility for IP address space allocation, protocol identifier assignment, top-level domain name system management, and root server system management functions.

Answer option A is incorrect. The International Organization for Standardization, widely known as ISO, is an international-standard-setting body composed of representatives from various national standards organizations. Founded on 23 February 1947, the organization promulgates worldwide proprietary industrial and commercial standards. It has its headquarters in Geneva, Switzerland. While ISO defines itself as a non-governmental organization, its ability to set standards that often become law, either through treaties or national standards, makes it more powerful than most non-governmental organizations. In practice, ISO acts as a consortium with strong links to governments.

Answer option C is incorrect. The World Wide Web Consortium (W3C) is an international industry consortium that develops common standards for the World Wide Web to promote its evolution and interoperability. It was founded in October 1994 by Tim Berners-Lee, the inventor of the Web, at the Massachusetts Institute of Technology, Laboratory for Computer Science [MIT/LCS] in collaboration with CERN, where the Web had originated, with support from DARPA and the European Commission.

Answer option D is incorrect. ANSI (American National Standards Institute) is the primary organization for fostering the development of technology standards in the United States. ANSI works with industry groups and is the U.S. member of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Long-established computer standards from ANSI include the American Standard Code for Information Interchange (ASCII) and the Small Computer System Interface (SCSI).

QUESTION 41

Which of the following recovery plans includes specific strategies and actions to deal with specific variances to assumptions resulting in a particular security problem, emergency, or state of affairs?

- A. Contingency plan
- B. Disaster recovery plan
- C. Business continuity plan
- D. Continuity of Operations Plan

Correct Answer: A

Section:

Explanation:

A contingency plan is a plan devised for a specific situation when things could go wrong. Contingency plans are often devised by governments or businesses who want to be prepared for anything that could happen. Contingency plans include specific strategies and actions to deal with specific variances to assumptions resulting in a particular problem, emergency, or state of affairs. They also include a monitoring process and "triggers" for initiating planned actions. They are required to help governments, businesses, or individuals to recover from serious incidents in the minimum time with minimum cost and disruption.

Answer option D is incorrect. It includes the plans and procedures documented that ensure the continuity of critical operations during any period where normal operations are impossible.

Answer option B is incorrect. Disaster recovery planning is a subset of a larger process known as business continuity planning and should include planning for resumption of applications, data, hardware, communications (such as networking), and other IT infrastructure. A business continuity plan (BCP) includes planning for non-IT related aspects such as key personnel, facilities, crisis communication, and reputation protection, and should refer to the disaster recovery plan (DRP) for IT-related infrastructure recovery/continuity.

Answer option C is incorrect. Business continuity planning (BCP) is the creation and validation of a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a business continuity plan. The BCP lifecycle is as follows:



QUESTION 42

Which of the following examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware, and policy violations?

- A. Network Behavior Analysis
- B. Network-based Intrusion Prevention
- C. Wireless Intrusion Prevention System
- D. Host-based Intrusion Prevention

Correct Answer: A

Section:

Explanation:

Network Behavior Analysis examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware, and policy violations.

Answer option B is incorrect. Network-based Intrusion Prevention (NIPS) monitors the entire network for suspicious traffic by analyzing protocol activity.

Answer option C is incorrect. Wireless Intrusion Prevention System (WIPS) monitors a wireless network for suspicious traffic by analyzing wireless networking protocols.

Answer option D is incorrect. Host-based Intrusion Prevention (HIPS) is an installed software package that monitors a single host for suspicious activity by analyzing events occurring within that host.

QUESTION 43

Which of the following routing metrics refers to the length of time that is required to move a packet from source to destination through the internetwork?

- A. Routing delay
- B. Bandwidth
- C. Load
- D. Path length

Correct Answer: A

Section:

Explanation:

Routing delay refers to the length of time that is required to move a packet from source to destination through the internetwork. Delay depends on many factors, including the following: Bandwidth of intermediate network links Port queues at each router along the way Network congestion on all intermediate network links Physical distance to be traveled Since delay is a conglomeration of several important variables, it is a common and useful metric.

Answer option D is incorrect. Path length is defined as the sum of the costs associated with each link traversed.

Answer option B is incorrect. Bandwidth refers to the available traffic capacity of a link.

Answer option C is incorrect. Load refers to the degree to which a network resource, such as a router, is busy.

QUESTION 44

FILL BLANK

Fill in the blank with the appropriate term. The _____ model is a description framework for computer network protocols and is sometimes called the Internet Model or the DoD Model.

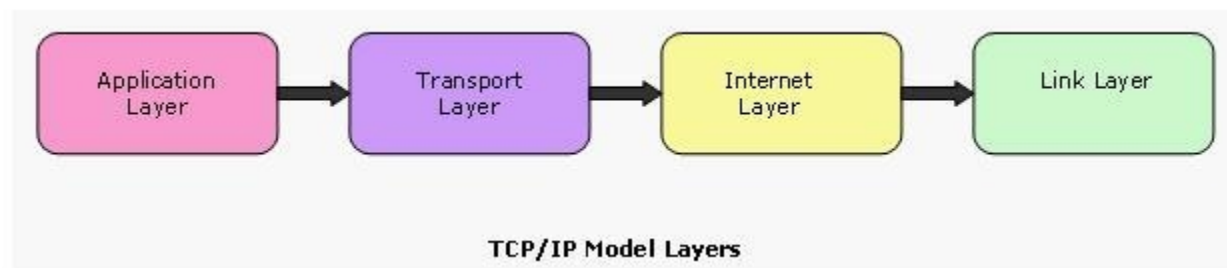
- A. TCP/IP

Correct Answer: A

Section:

Explanation:

The TCP/IP model is a description framework for computer network protocols. It describes a set of general design guidelines and implementations of specific networking protocols to enable computers to communicate over a network. TCP/IP provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination. Protocols exist for a variety of different types of communication services between computers. The TCP/IP Model is sometimes called the Internet Model or the DoD Model. The TCP/IP model has four unique layers as shown in the image. This layer architecture is often compared with the seven-layer OSI Reference Model. The TCP/IP model and related protocols are maintained by the Internet Engineering Task Force (IETF).



QUESTION 45

Which of the following topologies is a type of physical network design where each computer in the network is connected to a central device through an unshielded twisted-pair (UTP) wire?

- A. Mesh topology
- B. Star topology
- C. Ring topology
- D. Bus topology

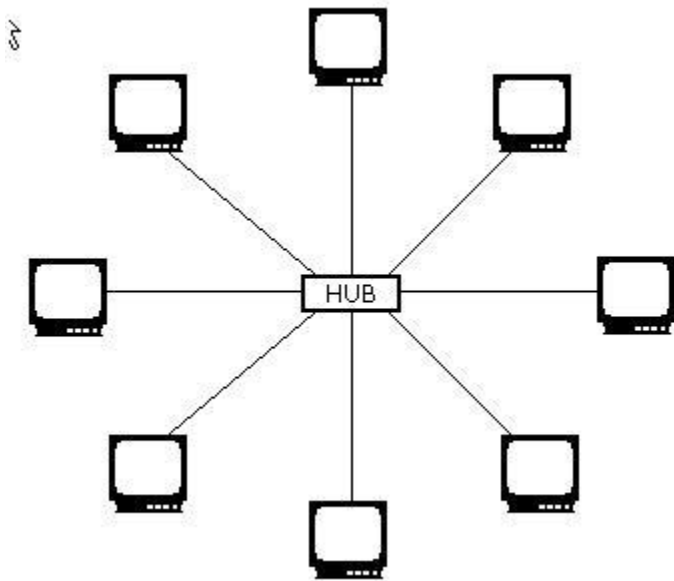
Correct Answer: B

Section:

Explanation:

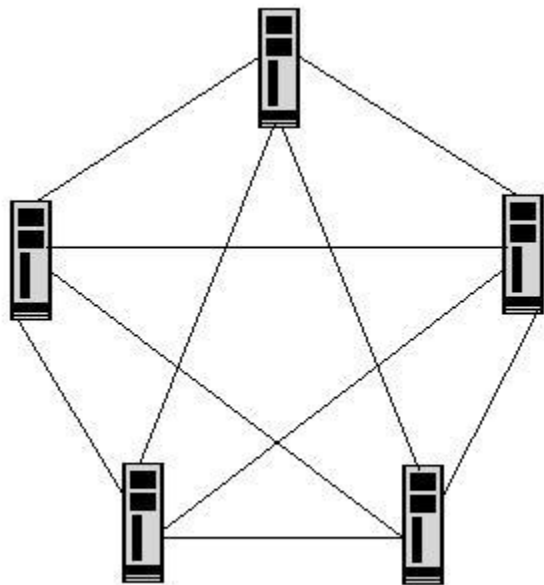
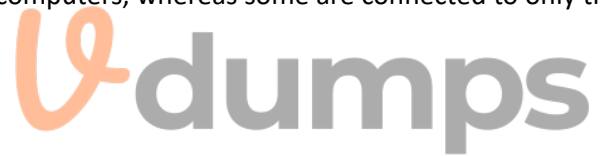
Star topology is a type of physical network design where each computer in the network is connected to a central device, called hub, through an unshielded twisted-pair (UTP) wire. Signals from the sending computer go to the hub and are then transmitted to all the computers in the network. Since each workstation has a separate connection to the hub, it is easy to troubleshoot. Currently, it is the most popular topology used for networks.

Star Topology:



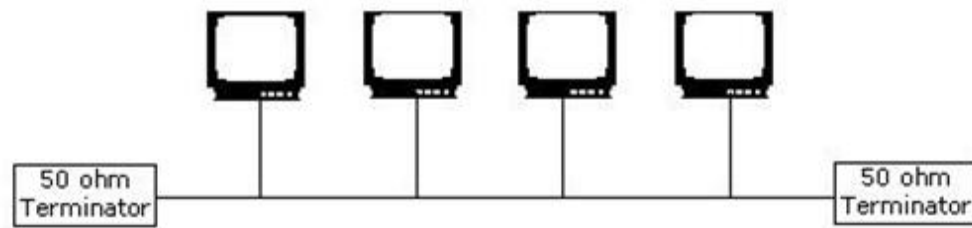
Answer option A is incorrect. Mesh network topology is a type of physical network design where all devices in a network are connected to each other with many redundant connections. It provides multiple paths for the data traveling on the network to reach its destination. Mesh topology also provides redundancy in the network. It employs the full mesh and partial mesh methods to connect devices. In a full mesh topology network, each computer is connected to all the other computers. In a partial mesh topology network, some of the computers are connected to all the computers, whereas some are connected to only those computers with which they frequently exchange data.

Mesh Topology:



Answer option D is incorrect. Bus topology is a type of physical network design where all computers in the network are connected through a single coaxial cable known as bus. This topology uses minimum cabling and is therefore, the simplest and least expensive topology for small networks. In this topology, 50 ohm terminators terminate both ends of the network. A Bus topology network is difficult to troubleshoot, as a break or problem at any point along the cable can cause the entire network to go down.

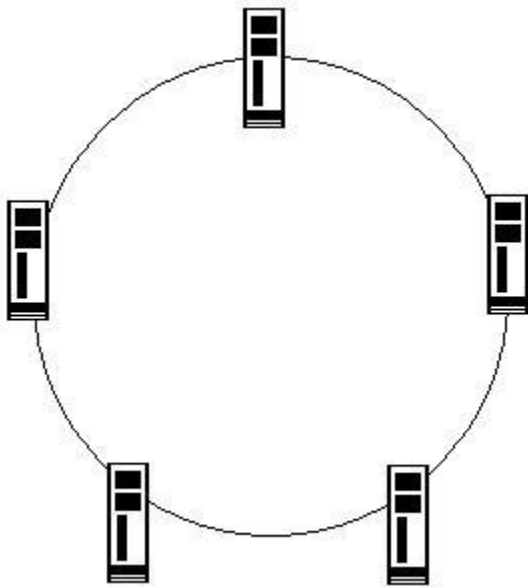
Bus Topology:



Answer option C is incorrect. Ring topology is a type of physical network design where all computers in the network are connected in a closed loop. Each computer or device in a Ring topology network acts as a repeater. It transmits data by passing a token around the network in order to prevent the collision of data between two computers that want to send messages at the same time. If a token is free, the computer waiting to send data takes it, attaches the data and destination address to the token, and sends it. When the token reaches its destination computer, the data is copied. Then, the token gets back to the originator.

The originator finds that the message has been copied and received and removes the message from the token. Now, the token is free and can be used by the other computers in the network to send data. In this topology, if one computer fails, the entire network goes down.

Ring Topology:



 The logo for Vdumps, featuring a stylized orange 'V' followed by the word 'dumps' in a grey sans-serif font.

QUESTION 46

FILL BLANK

Fill in the blank with the appropriate term. A _____ is a technique to authenticate digital documents by using computer cryptography.

A. signature

Correct Answer: A

Section:

Explanation:

A digital signature is a technique to authenticate digital documents by using computer cryptography. A digital signature not only validates the sender's identity, but also ensures that the document's contents have not been altered. It verifies that the source and integrity of the document is not compromised since the document is signed. A digital signature provides the following assurances: Authenticity, Integrity, and Non-repudiation. Microsoft Office 2007 Excel and Word provide a feature known as Signature line to insert a user's digital signature on a document.

QUESTION 47

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

Correct Answer: D

Section:

Explanation:

A network intrusion detection system (NIDS) is an intrusion detection system that tries to detect malicious activity such as denial of service attacks, port scans or even attempts to crack into computers by monitoring network traffic. A NIDS reads all the incoming packets and tries to find suspicious patterns known as signatures or rules. It also tries to detect incoming shell codes in the same manner that an ordinary intrusion detection system does.

Answer option A is incorrect. A host-based intrusion detection system (HIDS) produces a false alarm because of the abnormal behavior of users and the network.

A host-based intrusion detection system (HIDS) is an intrusion detection system that monitors and analyses the internals of a computing system rather than the network packets on its external interfaces. A host-based Intrusion Detection System (HIDS) monitors all or parts of the dynamic behavior and the state of a computer system. HIDS looks at the state of a system, its stored information, whether in RAM, in the file system, log files or elsewhere; and checks that the contents of these appear as expected. Answer option B is incorrect. An intrusion prevention system (IPS) is a network security device that monitors network and/ or system activities for malicious or unwanted behavior and can react, in real-time, to block or prevent those activities. When an attack is detected, it can drop the offending packets while still allowing all other traffic to pass.

Answer option C is incorrect. A demilitarized zone (DMZ) is a physical or logical subnetwork that contains and exposes external services of an organization to a larger network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's Local Area Network (LAN); an external attacker only has access to equipment in the DMZ, rather than the whole of the network. Hosts in the DMZ have limited connectivity to specific hosts in the internal network, though communication with other hosts in the DMZ and to the external network is allowed. This allows hosts in the DMZ to provide services to both the internal and external networks, while an intervening firewall controls the traffic between the DMZ servers and the internal network clients. In a DMZ configuration, most computers on the LAN run behind a firewall connected to a public network such as the Internet.

QUESTION 48

Fill in the blank with the appropriate term. The _____ is typically considered as the top InfoSec officer in the organization and helps in maintaining current and appropriate body of knowledge required to perform InfoSec management functions.

A. CISO

Correct Answer: A

Section:

Explanation:

The Chief InfoSec Officer (CISO) is typically considered as the top InfoSec officer in the organization, though the CISO is usually not an executive-level position and commonly reports to the CIO. Following are the job competencies for the Chief InfoSec Officer (CISO):

Maintaining current & appropriate body of knowledge required to perform InfoSec management functions
Effectively applying InfoSec management knowledge for improving security of open network and associated systems and services
Maintaining working knowledge of external legislative & regulatory initiatives
Interpreting and translating requirements for implementation
Developing appropriate InfoSec policies, standards, guidelines, and procedures
Providing meaningful input, preparing effective presentations, and communicating InfoSec objectives
Participating in short and long term planning

QUESTION 49

In which of the following types of port scans does the scanner attempt to connect to all 65535 ports?

A. UDP

B. Strobe

C. FTP bounce

D. Vanilla

Correct Answer: D

Section:

Explanation:

In a vanilla port scan, the scanner attempts to connect to all 65,535 ports.

Answer option B is incorrect. The scanner attempts to connect to only selected ports.

Answer option A is incorrect. The scanner scans for open User Datagram Protocol ports.

Answer option C is incorrect. The scanner goes through a File Transfer Protocol server to disguise the cracker's location.

QUESTION 50

Which of the following is a firewall that keeps track of the state of network connections traveling across it?

- A. Stateful firewall
- B. Stateless packet filter firewall
- C. Circuit-level proxy firewall
- D. Application gateway firewall

Correct Answer: A

Section:

Explanation:

A stateful firewall is a firewall that keeps track of the state of network connections (such as TCP streams, UDP communication) traveling across it. The firewall is programmed to distinguish legitimate packets for different types of connections. Only packets matching a known connection state will be allowed by the firewall; others will be rejected. Answer option B is incorrect. A stateless packet filter firewall allows direct connections from the external network to hosts on the internal network and is included with router configuration software or with Open Source operating systems.

Answer option C is incorrect. It applies security mechanisms when a TCP or UDP connection is established.

Answer option D is incorrect. An application gateway firewall applies security mechanisms to specific applications, such as FTP and Telnet servers.

QUESTION 51

FILL BLANK

Fill in the blank with the appropriate term. _____ encryption is a type of encryption that uses two keys, i.e., a public key and a private key pair for data encryption. It is also known as public key encryption.

- A. Asymmetric

Correct Answer: A

Section:

Explanation:

Asymmetric encryption is a type of encryption that uses two keys, i.e., a public key and a private key pair for data encryption. The public key is available to everyone, while the private or secret key is available only to the recipient of the message. For example, when a user sends a message or data to another user, the sender uses the public key to encrypt the data. The receiver uses his private key to decrypt the data.

QUESTION 52

FILL BLANK

Fill in the blank with the appropriate term. _____ is a protocol used to synchronize the timekeeping among the number of distributed time servers and clients.

- A. NTP

Correct Answer: A

Section:

Explanation:

Network Time Protocol (NTP) is used to synchronize the timekeeping among the number of distributed time servers and clients. It is used for the time management in a large and diverse network that contains many interfaces. In this protocol, servers define the time, and clients have to be synchronized with the defined time. These clients can choose the most reliable source of time defined from the several NTP servers for their information transmission.

QUESTION 53

FILL BLANK

Fill in the blank with the appropriate term. The _____ is a communication protocol that communicates information between the network routers and the multicast end stations.

- A. IGMP

Correct Answer: A

Section:

Explanation:

The Internet Group Management Protocol (IGMP) is a communication protocol that communicates information between the network routers and the multicast end stations. It allows the receivers to request a multicast data stream from a specific group address. However, multicast traffic is sent to a single MAC address but is processed by multiple hosts. The IGMP allows an end station to connect to a multicast group and leave it, while being connected to the group address. It can be effectively used for gaming and showing online videos. Although it does not actually act as a transport protocol, it operates above the network layer. It is analogous to ICMP for unicast connections. It is susceptible to some attacks, so firewalls commonly allow the user to disable it if not needed.

QUESTION 54

Which of the following can be performed with software or hardware devices in order to record everything a person types using his or her keyboard?

- A. Warchalking
- B. Keystroke logging
- C. War dialing
- D. IRC bot

Correct Answer: B

Section:

Explanation:

Keystroke logging is a method of logging and recording user keystrokes. It can be performed with software or hardware devices. Keystroke logging devices can record everything a person types using his or her keyboard, such as to measure employee's productivity on certain clerical tasks. These types of devices can also be used to get usernames, passwords, etc.

Answer option C is incorrect. War dialing is a technique of using a modem to automatically scan a list of telephone numbers, usually dialing every number in a local area code to search for computers, BBS systems, and fax machines.

Hackers use the resulting lists for various purposes, hobbyists for exploration, and crackers (hackers that specialize in computer security) for password guessing.

Answer option A is incorrect. Warchalking is the drawing of symbols in public places to advertise an open Wi-Fi wireless network. Having found a Wi-Fi node, the warchalker draws a special symbol on a nearby object, such as a wall, the pavement, or a lamp post. The name warchalking is derived from the cracker terms war dialing and war driving.

Answer option D is incorrect. An Internet Relay Chat (IRC) bot is a set of scripts or an independent program that connects to Internet Relay Chat as a client, and so appears to other IRC users as another user. An IRC bot differs from a regular client in that instead of providing interactive access to IRC for a human user, it performs automated functions.

QUESTION 55

FILL BLANK

Fill in the blank with the appropriate term.

A _____ is a translation device or service that is often controlled by a separate Media Gateway Controller, which provides the call control and signaling functionality.

- A. Media gateway

Correct Answer: A

Section:

Explanation:

A Media gateway is a translation device or service that converts digital media streams between disparate telecommunications networks such as PSTN, SS7,

Next Generation Networks (2G, 2.5G and 3G radio access networks) or PBX. Media gateways enable multimedia communications across Next Generation

Networks over multiple transport protocols such as Asynchronous Transfer Mode (ATM) and Internet Protocol (IP). Because the media gateway connects different types of networks, one of its main functions is to convert between different transmission and coding techniques. Media streaming functions such as echo cancellation, DTMF, and tone sender are also located in the media gateway. Media gateways are often controlled by a separate Media Gateway Controller, which provides the call control and signaling functionality.

QUESTION 56

Which of the following is a mechanism that helps in ensuring that only the intended and authorized recipients are able to read data?

- A. Integrity
- B. Data availability
- C. Confidentiality

D. Authentication

Correct Answer: C

Section:

Explanation:

Confidentiality is a mechanism that ensures that only the intended and authorized recipients are able to read data. The data is so encrypted that even if an unauthorized user gets access to it, he will not get any meaning out of it.

Answer option A is incorrect. In information security, integrity means that data cannot be modified without authorization. This is not the same thing as referential integrity in databases. Integrity is violated when an employee accidentally or with malicious intent deletes important data files, when a computer virus infects a computer, when an employee is able to modify his own salary in a payroll database, when an unauthorized user vandalizes a web site, when someone is able to cast a very large number of votes in an online poll, and so on. There are many ways in which integrity could be violated without malicious intent. In the simplest case, a user on a system could mistype someone's address. On a larger scale, if an automated process is not written and tested correctly, bulk updates to a database could alter data in an incorrect way, leaving the integrity of the data compromised. Information security professionals are tasked with finding ways to implement controls that prevent errors of integrity.

Answer option B is incorrect. Data availability is one of the security principles that ensures that the data and communication services will be available for use when needed (expected). It is a method of describing products and services availability by which it is ensured that data continues to be available at a required level of performance in situations ranging from normal to disastrous. Data availability is achieved through redundancy, which depends upon where the data is stored and how it can be reached.

Answer option D is incorrect. Authentication is the act of establishing or confirming something (or someone) as authentic, i.e., the claims made by or about the subject are true ("authentication" is a variant of this word).

QUESTION 57

Which of the following help in estimating and totaling up the equivalent money value of the benefits and costs to the community of projects for establishing whether they are worthwhile? Each correct answer represents a complete solution. Choose all that apply.

- A. Business Continuity Planning
- B. Benefit-Cost Analysis
- C. Disaster recovery
- D. Cost-benefit analysis



Correct Answer: B, D

Section:

Explanation:

Cost-benefit analysis is a process by which business decisions are analyzed. It is used to estimate and total up the equivalent money value of the benefits and costs to the community of projects for establishing whether they are worthwhile. It is a term that refers both to:

helping to appraise, or assess, the case for a project, program, or policy proposal; an approach to making economic decisions of any kind. Under both definitions, the process involves, whether explicitly or implicitly, weighing the total expected costs against the total expected benefits of one or more actions in order to choose the best or most profitable option. The formal process is often referred to as either CBA (Cost-Benefit Analysis) or BCA (Benefit-Cost Analysis).

Answer option A is incorrect. Business Continuity Planning (BCP) is the creation and validation of a practiced logistical plan that defines how an organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a Business Continuity Plan.

Answer option C is incorrect. Disaster recovery is the process, policies, and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster.

Disaster recovery planning is a subset of a larger process known as business continuity planning and should include planning for resumption of applications, data, hardware, communications (such as networking) and other IT infrastructure. A business continuity plan (BCP) includes planning for non-IT related aspects such as key personnel, facilities, crisis communication and reputation protection, and should refer to the disaster recovery plan (DRP) for IT related infrastructure recovery / continuity.

QUESTION 58

Which of the following steps will NOT make a server fault tolerant? Each correct answer represents a complete solution. (Choose two.)

- A. Adding a second power supply unit
- B. Performing regular backup of the server
- C. Adding one more same sized disk as mirror on the server

- D. Implementing cluster servers' facility
- E. Encrypting confidential data stored on the server

Correct Answer: B, E

Section:

Explanation:

Encrypting confidential data stored on the server and performing regular backup will not make the server fault tolerant.

Fault tolerance is the ability to continue work when a hardware failure occurs on a system. A fault-tolerant system is designed from the ground up for reliability by building multiples of all critical components, such as CPUs, memories, disks and power supplies into the same computer. In the event one component fails, another takes over without skipping a beat. Answer options A, C, and D are incorrect. The following steps will make the server fault tolerant:

Adding a second power supply unit Adding one more same sized disk as a mirror on the server implementing cluster servers facility

QUESTION 59

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 _____.
- F. Kismet
- G. Absinthe
- H. THC-Scan
- I. NetStumbler



Correct Answer: D

Section:

Explanation:

NetStumbler 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 NetStumbler 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

Answer option A is incorrect. Kismet is an IEEE 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. Answer option C is incorrect.

THC-Scan is a war-dialing tool.

Answer option B is incorrect. Absinthe is an automated SQL injection tool.

QUESTION 60

Which of the following are the common security problems involved in communications and email? Each correct answer represents a complete solution. Choose all that apply.

- A. False message
- B. Message digest
- C. Message replay
- D. Message repudiation
- E. Message modification

- F. Eavesdropping
- G. Identity theft

Correct Answer: A, C, D, E, F, G

Section:

Explanation:

Following are the common security problems involved in communications and email:

Eavesdropping: It is the act of secretly listening to private information through telephone lines, e-mail, instant messaging, and any other method of communication considered private.

Identity theft: It is the act of obtaining someone's username and password to access his/her email servers for reading email and sending false email messages.

These credentials can be obtained by eavesdropping on SMTP, POP, IMAP, or Webmail connections.

Message modification: The person who has system administrator permission on any of the SMTP servers can visit anyone's message and can delete or change the message before it continues on to its destination. The recipient has no way of telling that the email message has been altered.

False message: It the act of constructing messages that appear to be sent by someone else.

Message replay: In a message replay, messages are modified, saved, and re-sent later.

Message repudiation: In message repudiation, normal email messages can be forged. There is no way for the receiver to prove that someone had sent him/her a particular message. This means that even if someone has sent a message, he/she can successfully deny it.

Answer option B is incorrect. A message digest is a number that is created algorithmically from a file and represents that file uniquely.

QUESTION 61

Which of the following are the six different phases of the Incident handling process? Each correct answer represents a complete solution. Choose all that apply.

- A. Containment
- B. Identification
- C. Post mortem review
- D. Preparation
- E. Lessons learned
- F. Recovery
- G. Eradication

Correct Answer: A, B, D, E, F, G

Section:

Explanation:

Following are the six different phases of the Incident handling process:

1.Preparation: Preparation is the first step in the incident handling process. It includes processes like backing up copies of all key data on a regular basis, monitoring and updating software on a regular basis, and creating and implementing a documented security policy. To apply this step a documented security policy is formulated that outlines the responses to various incidents, as a reliable set of instructions during the time of an incident. The following list contains items that the incident handler should maintain in the preparation phase i.e. before an incident occurs:

Establish applicable policies

Build relationships with key players

Build response kit

Create incident checklists

Establish communication plan

Perform threat modeling

Build an incident response team

Practice the demo incidents

2.Identification: The Identification phase of the Incident handling process is the stage at which the Incident handler evaluates the critical level of an incident for an enterprise or system. It is an important stage where the distinction between an event and an incident is determined, measured and tested.

3.Containment: The Containment phase of the Incident handling process supports and builds up the incident combating process. It helps in ensuring the stability of the system and also confirms that the incident does not get any worse.



4.Eradication: The Eradication phase of the Incident handling process involves the cleaning-up of the identified harmful incidents from the system. It includes the analyzing of the information that has been gathered for determining how the attack was committed. To prevent the incident from happening again, it is vital to recognize how it was conceded out so that a prevention technique is applied.

5.Recovery: Recovery is the fifth step of the incident handling process. In this phase, the Incident Handler places the system back into the working environment.

In the recovery phase the Incident Handler also works with the questions to validate that the system recovery is successful. This involves testing the system to make sure that all the processes and functions are working normal. The Incident Handler also monitors the system to make sure that the systems are not compromised again. It looks for additional signs of attack.

6.Lessons learned: Lessons learned is the sixth and the final step of incident handling process. The Incident Handler utilizes the knowledge and experience he learned during the handling of the incident to enhance and improve the incidenthandling process. This is the most ignorant step of all incident handling processes. Many times the Incident Handlers are relieved to have systems back to normal and get busy trying to catch up other unfinished work. The Incident Handler should make documents related to the incident or look for ways to improve the process.

Answer option C is incorrect. The post mortem review is one of the phases of the Incident response process.

QUESTION 62

Which of the following steps of the OPSEC process examines each aspect of the planned operation to identify OPSEC indicators that could reveal critical information and then compare those indicators with the adversary's intelligence collection capabilities identified in the previous action?

- A. Analysis of Threats
- B. Application of Appropriate OPSEC Measures
- C. Identification of Critical Information
- D. Analysis of Vulnerabilities
- E. Assessment of Risk

Correct Answer: D

Section:

Explanation:

OPSEC is a 5-step process that helps in developing protection mechanisms in order to safeguard sensitive information and preserve essential secrecy. The OPSEC process has five steps, which are as follows:

1.Identification of Critical Information: This step includes identifying information vitally needed by an adversary, which focuses the remainder of the OPSEC process on protecting vital information, rather than attempting to protect all classified or sensitive unclassified information.

2.Analysis of Threats: This step includes the research and analysis of intelligence, counter-intelligence, and open source information to identify likely adversaries to a planned operation.

3.Analysis of Vulnerabilities: It includes examining each aspect of the planned operation to identify OPSEC indicators that could reveal critical information and then comparing those indicators with the adversary's intelligence collection capabilities identified in the previous action.

4.Assessment of Risk: Firstly, planners analyze the vulnerabilities identified in the previous action and identify possible OPSEC measures for each vulnerability.

Secondly, specific OPSEC measures are selected for execution based upon a risk assessment done by the commander and staff.

5.Application of Appropriate OPSEC Measures: The command implements the OPSEC measures selected in the assessment of risk action or, in the case of planned future operations and activities, includes the measures in specific OPSEC plans.

QUESTION 63

Which of the following is a network interconnectivity device that translates different communication protocols and is used to connect dissimilar network technologies?

- A. Gateway
- B. Router
- C. Bridge
- D. Switch

Correct Answer: A

Section:

Explanation:

A gateway is a network interconnectivity device that translates different communication protocols and is used to connect dissimilar network technologies. It provides greater functionality than a router or bridge because a gateway functions both as a translator and a router. Gateways are slower than bridges and routers. A gateway is an application layer device.

Answer option B is incorrect. A router is an electronic device that interconnects two or more computer networks. It selectively interchanges packets of data between them. It is a networking device whose software and

hardware are customized to the tasks of routing and forwarding information. It helps in forwarding data packets between networks.

Answer option C is incorrect. A bridge is an interconnectivity device that connects two local area networks (LANs) or two segments of the same LAN using the same communication protocols, and provides address filtering between them.

Users can use this device to divide busy networks into segments and reduce network traffic. A bridge broadcasts data packets to all the possible destinations within a specific segment. Bridges operate at the data-link layer of the OSI model. Answer option D is incorrect. A switch is a network device that selects a path or circuit for sending a data unit to its next destination. It is not required in smaller networks, but is required in large inter-networks, where there can be many possible ways of transmitting a message from a sender to destination. The function of switch is to select the best possible path.

On an Ethernet local area network (LAN), a switch determines from the physical device (Media Access Control or MAC) address in each incoming message frame which output port to forward it to and out of. In a wide area packet-switched network, such as the Internet, a switch determines from the IP address in each packet which output port to use for the next part of its trip to the intended destination.

QUESTION 64

Which of the following is a tool that runs on the Windows OS and analyzes iptables log messages to detect port scans and other suspicious traffic?

- A. PSAD
- B. Hping
- C. NetRanger
- D. Nmap

Correct Answer: A

Section:

Explanation:

PSAD is a tool that runs on the Windows OS and analyzes iptables log messages to detect port scans and other suspicious traffic. It includes many signatures from the IDS to detect probes for various backdoor programs such as EvilFTP, GirlFriend, SubSeven, DDoS tools (mstream, shaft), and advanced port scans (FIN, NULL, XMAS). If it is combined with fwsnort and the Netfilter string match extension, it detects most of the attacks described in the Snort rule set that involve application layer data.

Answer option C is incorrect. NetRanger is the complete network configuration and information toolkit that includes the following tools: Ping tool, Trace Route tool, Host Lookup tool, Internet time synchronizer, Whois tool, Finger Unix hosts tool, Host and port scanning tool, check multiple POP3 mail accounts tool, manage dialup connections tool, Quote of the day tool, and monitor Network Settings tool. These tools are integrated in order to use an application interface with full online help. NetRanger is designed for both new and experienced users. This tool is used to help diagnose network problems and to get information about users, hosts, and networks on the Internet or on a user computer network. NetRanger uses multi-threaded and multi-connection technologies in order to be very fast and efficient.

Answer option D is incorrect. Nmap is a free open-source utility for network exploration and security auditing. It is used to discover computers and services on a computer network, thus creating a "map" of the network. Just like many simple port scanners, Nmap is capable of discovering passive services. In addition, Nmap may be able to determine various details about the remote computers. These include operating system, device type, uptime, software product used to run a service, exact version number of that product, presence of some firewall techniques and, on a local area network, even vendor of the remote network card.

Nmap runs on Linux, Microsoft Windows, etc.

QUESTION 65

FILL BLANK

Fill in the blank with the appropriate term.

A _____ is a physical or logical subnetwork that contains and exposes external services of an organization to a larger network.

- A. demilitarized zone

Correct Answer: A

Section:

Explanation:

A demilitarized zone (DMZ) is a physical or logical subnetwork that contains and exposes external services of an organization to a larger network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's Local Area Network (LAN); an external attacker only has access to equipment in the DMZ, rather than the whole of the network. Hosts in the DMZ have limited connectivity to specific hosts in the internal network, though communication with other hosts in the DMZ and to the external network is allowed. This allows hosts in the DMZ to provide services to both the internal and external networks, while an intervening firewall controls the traffic between the DMZ servers and the internal network clients. In a DMZ configuration, most computers on the LAN run behind a firewall connected to a public network such as the Internet.

QUESTION 66

Which of the following tools is a free laptop tracker that helps in tracking a user's laptop in case it gets stolen?

- A. SAINT
- B. Adeona
- C. Snort
- D. Nessus

Correct Answer: B

Section:

Explanation:

Adeona is a free laptop tracker that helps in tracking a user's laptop in case it gets stolen. All it takes is to install the Adeona software client on the user's laptop, pick a password, and make it run in the background. If at one point, the user's laptop gets stolen and is connected to the Internet, the Adeona software sends the criminal's IP address. Using the Adeona Recovery, the IP address can then be retrieved. Knowing the IP address helps in tracking the geographical location of the stolen device.

Answer option D is incorrect. Nessus is proprietary comprehensive vulnerability scanning software. It is free of charge for personal use in a non-enterprise environment. Its goal is to detect potential vulnerabilities on tested systems. It is capable of checking various types of vulnerabilities, some of which are as follows: Vulnerabilities that allow a remote cracker to control or access sensitive data on a system Misconfiguration (e.g. open mail relay, missing patches, etc), Default passwords, a few common passwords, and blank/absent passwords on some system accounts. Nessus can also call Hydra (an external tool) to launch a dictionary attack. Denials of service against the TCP/IP stack by using mangled packets Answer option A is incorrect. SAINT stands for System Administrator's Integrated Network Tool. It is computer software used for scanning computer networks for security vulnerabilities, and exploiting found vulnerabilities. The SAINT scanner screens every live system on a network for TCP and UDP services. For each service it finds running, it launches a set of probes designed to detect anything that could allow an attacker to gain unauthorized access, create a denialofwww. service, or gain sensitive information about the network.

Answer option C is incorrect. Snort is an open source network intrusion detection system. The Snort application analyzes network traffic in realtime mode. It performs packet sniffing, packet logging, protocol analysis, and a content search to detect a variety of potential attacks.

QUESTION 67

FILL BLANK

Fill in the blank with the appropriate term. _____ is a free open-source utility for network exploration and security auditing that is used to discover computers and services on a computer network, thus creating a "map" of the network.

- A. Nmap

Correct Answer: A

Section:

Explanation:

Nmap is a free open-source utility for network exploration and security auditing. It is used to discover computers and services on a computer network, thus creating a "map" of the network. Just like many simple port scanners, Nmap is capable of discovering passive services. In addition, Nmap may be able to determine various details about the remote computers. These include operating system, device type, uptime, software product used to run a service, exact version number of that product, presence of some firewall techniques and, on a local area network, even vendor of the remote network card. Nmap runs on Linux, Microsoft Windows, etc.

QUESTION 68

FILL BLANK

Fill in the blank with the appropriate term. _____ is a powerful and low-interaction open source honeypot.

- A. Honeyd

Correct Answer: A

Section:

Explanation:

Honeyd is a powerful and low-interaction open source honeypot. It was released by Niels Provos in 2002. It was written in C and designed for Unix platforms. It introduced a variety of new concepts, including the ability to monitor millions of unused IPs, IP stack spoofing, etc. It can also simulate hundreds of operating systems and monitor all UDP and TCP-based ports.

QUESTION 69

Which of the following statements are true about volatile memory? Each correct answer represents a complete solution. Choose all that apply.

- A. Read-Only Memory (ROM) is an example of volatile memory.
- B. The content is stored permanently, and even the power supply is switched off.
- C. The volatile storage device is faster in reading and writing data.
- D. It is computer memory that requires power to maintain the stored information.

Correct Answer: C, D

Section:

Explanation:

Volatile memory, also known as volatile storage, is computer memory that requires power to maintain the stored information, unlike non-volatile memory which does not require a maintained power supply. It has been less popularly known as temporary memory. Most forms of modern random access memory (RAM) are volatile storage, including dynamic random access memory (DRAM) and static random access memory (SRAM). A volatile storage device is faster in reading and writing data. Answer options B and A are incorrect. Non-volatile memory, nonvolatile memory, NVM, or non-volatile storage, in the most basic sense, is computer memory that can retain the stored information even when not powered. Examples of non-volatile memory include read-only memory, flash memory, most types of magnetic computer storage devices (e.g. hard disks, floppy disks, and magnetic tape), optical discs, and early computer storage methods such as paper tape and punched cards.

QUESTION 70

Which of the following firewalls are used to track the state of active connections and determine the network packets allowed to enter through the firewall? Each correct answer represents a complete solution. Choose all that apply.

- A. Circuit-level gateway
- B. Stateful
- C. Proxy server
- D. Dynamic packet-filtering

Correct Answer: B, D

Section:

Explanation:

A dynamic packet-filtering firewall is a fourth generation firewall technology. It is also known as a stateful firewall. It tracks the state of active connections and determines which network packets are allowed to enter through the firewall. It records session information, such as IP addresses and port numbers to implement a more secure network. The dynamic packet-filtering firewall operates at Layer3, Layer4, and Layer5.

Answer option A is incorrect. A circuit-level gateway is a type of firewall that works at the session layer of the OSI model between the application layer and the transport layer of the TCP/IP stack. They monitor TCP handshaking between packets to determine whether a requested session is legitimate. Information passed to a remote computer through a circuit level gateway appears to have originated from the gateway. This is useful for hiding information about protected networks.

Circuit-level gateways are relatively inexpensive and have the advantage of hiding information about the private network they protect.

Answer option C is incorrect. A proxy server firewall intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

QUESTION 71

Which of the following statements are NOT true about the FAT16 file system? Each correct answer represents a complete solution. Choose all that apply.

- A. It does not support file-level security.
- B. It works well with large disks because the cluster size increases as the disk partition size increases.
- C. It supports the Linux operating system.
- D. It supports file-level compression.

Correct Answer: B, D

Section:

Explanation:

The FAT16 file system was developed for disks larger than 16MB. It uses 16-bit allocation table entries. The FAT16 file system supports all Microsoft operating systems. It also supports OS/2 and Linux. Answer options C and A



are incorrect. All these statements are true about the FAT16 file system.

QUESTION 72

FILL BLANK

Fill in the blank with the appropriate term. The _____ is used for routing voice conversations over the Internet. It is also known by other names such as IP Telephony, Broadband Telephony, etc.

A. VoIP

Correct Answer: A

Section:

Explanation:

The Voice over Internet Protocol (VoIP) is used for routing of voice conversation over the Internet. The VoIP is also known by other names such as IP Telephony, Broadband Telephony, etc. Analog signals are used in telephones in which the sound is received as electrical pulsation, which is amplified and then carried to a small loudspeaker attached to the other phone, and the call receiver can hear the sound. In VoIP, analog signals are changed into digital signals, which are transmitted on the Internet. VoIP is used to make free phone calls using an Internet connection, and this can be done by using any VoIP software available in the market. There are various modes for making phone calls through the Internet. Some of the important modes are as follows:

Through Analog Telephone Adapter (ATA) In this mode, the traditional phone is attached to the computer through AT

A. ATA receives analog signals from the phone and then converts these signals to digital signals. The digital signals are then received by the Internet Service Providers (ISP), and the system is ready to make calls over VoIP.

Through IP Phone IP Phones look exactly like the traditional phones, but they differ in that they have RJ-45 Ethernet connectors, instead of RJ-11 phone connectors, for connecting to the computers.

Computer To Computer This is the easiest way to use VoIP. For this, we need software, microphone, speakers, sound card and an Internet connection through a cable or a DSL modem.

Soft Phones

Soft phone is a software application that can be loaded onto a computer and used anywhere in the broadband connectivity area.

QUESTION 73

FILL BLANK

Fill in the blank with the appropriate term. The _____ protocol is a feature of packet-based data transmission protocols. It is used to keep a record of the frame sequences sent and their respective acknowledgements received by both the users.

A. Sliding Window

Correct Answer: A

Section:

Explanation:

The Sliding Window protocol is a feature of packet-based data transmission protocols. It is used in the data link layer (OSI model) as well as in TCP (transport layer of the OSI model). It is used to keep a record of the frame sequences sent, and their respective acknowledgements received, by both the users. Its additional feature over a simpler protocol is that can allow multiple packets to be "in transmission" simultaneously, rather than waiting for each packet to be acknowledged before sending the next. In transmit flow control, sliding window is a variable-duration window that allows a sender to transmit a specified number of data units before an acknowledgment is received or before a specified event occurs. An example of a sliding window is one in which, after the sender fails to receive an acknowledgment for the first transmitted frame, the sender "slides" the window, i.e., resets the window, and sends a second frame. This process is repeated for the specified number of times before the sender interrupts transmission. Sliding window is sometimes called acknowledgment delay period.

QUESTION 74

FILL BLANK

Fill in the blank with the appropriate term. A _____ is a set of tools that take Administrative control of a computer system without authorization by the computer owners and/or legitimate managers.

A. rootkit

Correct Answer: A

Section:

Explanation:

A rootkit is a set of tools that take Administrative control of a computer system without authorization by the computer owners and/or legitimate managers. A rootkit requires root access to be installed in the Linux operating system, but once installed, the attacker can get root access at any time. Rootkits have the following features:

They allow an attacker to run packet sniffers secretly to capture passwords.

They allow an attacker to set a Trojan into the operating system and thus open a backdoor for anytime access.

They allow an attacker to replace utility programs that can be used to detect the attacker's activity. They provide utilities for installing Trojans with the same attributes as legitimate programs.

QUESTION 75

Which of the following standards is an amendment to the original IEEE 802.11 and specifies security mechanisms for wireless networks?

- A. 802.11b
- B. 802.11e
- C. 802.11i
- D. 802.11a

Correct Answer: C

Section:

Explanation:

802.11i is an amendment to the original IEEE 802.11. This standard specifies security mechanisms for wireless networks. It replaced the short Authentication and privacy clause of the original standard with a detailed Security clause. In the process, it deprecated the broken WEP. 802.11i supersedes the previous security specification, Wired Equivalent Privacy (WEP), which was shown to have severe security weaknesses. Wi-Fi Protected Access (WPA) had previously been introduced by the Wi-Fi Alliance as an intermediate solution to WEP insecurities. The Wi-Fi Alliance refers to their approved, interoperable implementation of the full 802.11i as WPA2, also called RSN (Robust Security Network). 802.11i makes use of the Advanced Encryption Standard (AES) block cipher, whereas WEP and WPA use the RC4 stream cipher.

Answer option D is incorrect. 802.11a is an amendment to the IEEE 802.11 specification that added a higher data rate of up to 54 Mbit/s using the 5 GHz band. It has seen widespread worldwide implementation, particularly within the corporate workspace. Using the 5 GHz band gives 802.11a a significant advantage, since the 2.4 GHz band is heavily used to the point of being crowded. Degradation caused by such conflicts can cause frequent dropped connections and degradation of service.

Answer option A is incorrect. 802.11b is an amendment to the IEEE 802.11 specification that extended throughput up to 11 Mbit/s using the same 2.4 GHz band.

This specification under the marketing name of Wi-Fi has been implemented all over the world. 802.11b is used in a point-to-multipoint configuration, wherein an access point communicates via an omni-directional antenna with one or more nomadic or mobile clients that are located in a coverage area around the access point.

Answer option B is incorrect. The 802.11e standard is a proposed enhancement to the 802.11a and 802.11b wireless LAN (WLAN) specifications. It offers quality of service (QoS) features, including the prioritization of data, voice, and video transmissions. 802.11e enhances the 802.11 Media Access Control layer (MAC layer) with a coordinated time division multiple access (TDMA) construct, and adds error-correcting mechanisms for delay-sensitive applications such as voice and video.

QUESTION 76

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. KisMAC
- C. Snort
- D. Kismet

Correct Answer: C

Section:

Explanation:

Snort is an open source network intrusion prevention and detection system that operates as a network sniffer. It logs activities of the network that is matched with the predefined signatures. Signatures can be designed for a wide range of traffic, including Internet Protocol (IP), Transmission Control Protocol (TCP), User

Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP). The three main modes in which Snort can be configured are as follows:

Sniffer mode: It reads the packets of the network and displays them in a continuous stream on the console. Packet logger mode: It logs the packets to the disk.

Network intrusion detection mode: It is the most complex and configurable configuration, allowing Snort to analyze network traffic for matches against a userdefined rule set.

Answer option A is incorrect. Dsniff is a set of tools that are used for sniffing passwords, e-mail, and HTTP traffic. Some of the tools of Dsniff include dsniff, arpredirect, macof, tcpkill, tcpnice, filesnarf, and mailsnarf. Dsniff 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.

Answer option D is incorrect. Kismet is a Linux-based 802.11 wireless network sniffer and intrusion detection system. It can work with any wireless card that supports raw monitoring (rfmon) mode. Kismet can sniff 802.11b, 802.11a, 802.11g, and 802.11n traffic. Kismet can be used for the following tasks:

To identify networks by passively collecting packets To detect standard named networks To detect masked networks To collect the presence of non-beaconing networks via data traffic Answer option B is incorrect. KisMAC is a wireless network discovery tool for Mac OS X. It has a wide range of features, similar to those of Kismet, its Linux/BSD namesake and far exceeding those of NetStumbler, its closest equivalent on Windows. The program is geared towards the network security professionals, and is not as novice-friendly as the similar applications. KisMAC will scan for networks passively on supported cards, including Apple's AirPort, AirPort Extreme, and many third-party cards. It will scan for networks actively on any card supported by Mac OS X itself.

Cracking of WEP and WPA keys, both by brute force, and exploiting flaws, such as weak scheduling and badly generated keys is supported when a card capable of monitor mode is used, and when packet reinsertion can be done with a supported card. The GPS mapping can be performed when an NMEA compatible GPS receiver is attached. Data can also be saved in pcap format and loaded into programs, such as Wireshark.

QUESTION 77

Which of the following is a non-profit organization that oversees the allocation of IP addresses, management of the DNS infrastructure, protocol parameter assignment, and root server system management?

- A. ANSI
- B. IEEE
- C. ITU
- D. ICANN

Correct Answer: D

Section:

Explanation:

ICANN stands for Internet Corporation for Assigned Names and Numbers. ICANN is responsible for managing the assignment of domain names and IP addresses. ICANN's tasks include responsibility for IP address space allocation, protocol identifier assignment, top-level domain name system management, and root server system management functions. Internet Corporation for Assigned Names and Numbers (ICANN) is a non-profit organization that oversees the allocation of IP addresses, management of the DNS infrastructure, protocol parameter assignment, and root server system management.

Answer option B is incorrect. Institute of Electrical and Electronics Engineers (IEEE) is an organization of engineers and electronics professionals who develop standards for hardware and software.

Answer option C is incorrect. The International Telecommunication Union is an agency of the United Nations which regulates information and communication technology issues. ITU coordinates the shared global use of the radio spectrum, promotes international cooperation in assigning satellite orbits, works to improve telecommunication infrastructure in the developing world and establishes worldwide standards. ITU is active in areas including broadband Internet, latest-generation wireless technologies, aeronautical and maritime navigation, radio astronomy, satellite-based meteorology, convergence in fixed-mobile phone, Internet access, data, voice, TV broadcasting, and next-generation networks. Answer option A is incorrect. ANSI (American National Standards Institute) is the primary organization for fostering the development of technology standards in the United States. ANSI works with industry groups and is the U.S. member of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Long-established computer standards from ANSI include the American Standard Code for Information Interchange (ASCII) and the Small Computer System Interface (SCSI).

QUESTION 78

With which of the following flag sets does the Xmas tree scan send a TCP frame to a remote device? Each correct answer represents a part of the solution.

Choose all that apply.

- A. PUSH
- B. RST
- C. FIN
- D. URG

Correct Answer: A, C, D

Section:

Explanation:

With the URG, PUSH, and FIN flag sets, the Xmas tree scan sends a TCP frame to a remote device. The Xmas tree scan is called an Xmas tree scan because the alternating bits are turned on and off in the flags byte (00101001), much like the lights of a Christmas tree. Answer option B is incorrect. The RST flag is not set when the Xmas tree scan sends a TCP frame to a remote device.

QUESTION 79

Network security is the specialist area, which consists of the provisions and policies adopted by the Network Administrator to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and network-accessible resources. For which of the following reasons is network security needed? Each correct answer represents a complete solution. Choose all that apply.

- A. To protect information from loss and deliver it to its destination properly
- B. To protect information from unwanted editing, accidentally or intentionally by unauthorized users
- C. To protect private information on the Internet
- D. To prevent a user from sending a message to another user with the name of a third person

Correct Answer: A, B, C, D

Section:

Explanation:

Network security is needed for the following reasons:

To protect private information on the Internet To protect information from unwanted editing, accidentally or intentionally by unauthorized users To protect information from loss and deliver it to its destination properly To prevent a user from sending a message to another user with the name of a third person

QUESTION 80

Which of the following policies helps in defining what users can and should do to use network and organization's computer equipment?

- A. General policy
- B. Remote access policy
- C. IT policy
- D. User policy

Correct Answer: D

Section:

Explanation:

A user policy helps in defining what users can and should do to use network and organization's computer equipment. It also defines what limitations are put on users for maintaining the network secure such as whether users can install programs on their workstations, types of programs users are using, and how users can access data.

Answer option C is incorrect. IT policy includes general policies for the IT department. These policies are intended to keep the network secure and stable. It includes the following: Virus incident and security incident Backup policy Client update policies Server configuration, patch update, and modification policies (security) Firewall policies Dmz policy, email retention, and auto forwarded email policy

Answer option A is incorrect. It defines the high level program policy and business continuity plan.

Answer option B is incorrect. Remote access policy is a document that outlines and defines acceptable methods of remotely connecting to the internal network.

QUESTION 81

FILL BLANK

Fill in the blank with the appropriate term. In computing, _____ is a class of data storage devices that read their data in sequence.

- A. SAM

Correct Answer: A

Section:

Explanation:

In computing, sequential access memory (SAM) is a class of data storage devices that read their data in sequence. This is in contrast to random access memory (RAM) where data can be accessed in any order. Sequential access devices are usually a form of magnetic memory. While sequential access memory is read in sequence, access can still be made to arbitrary locations by "seeking" to the requested location. Magnetic sequential access memory is typically used for secondary storage in general-purpose computers due to their higher density at lower cost compared to RAM, as well as resistance to wear and non-volatility.

Examples of SAM devices include hard disks, CD-ROMs, and magnetic tapes.

QUESTION 82

Which of the following are the responsibilities of the disaster recovery team? Each correct answer represents a complete solution. Choose all that apply.

- A. To monitor the execution of the disaster recovery plan and assess the results

- B. To modify and update the disaster recovery plan according to the lessons learned from previous disaster recovery efforts
- C. To notify management, affected personnel, and third parties about the disaster
- D. To initiate the execution of the disaster recovery procedures

Correct Answer: A, B, C, D

Section:

Explanation:

The responsibilities of the disaster recovery team are as follows: To develop, deploy, and monitor the implementation of appropriate disaster recovery plans after analysis of business objectives and threats to organizations To notify management, affected personnel, and third parties about the disaster To initiate the execution of the disaster recovery procedures To monitor the execution of the disaster recovery plan and assess the results To return operations to normal conditions

To modify and update the disaster recovery plan according to the lessons learned from previous disaster recovery efforts To increase the level of the organization's disaster recovery preparedness by conducting mock drills, regular DR systems testing, and threat analysis to create awareness among various stakeholders of the organization by conducting training and awareness sessions

QUESTION 83

FILL BLANK

Fill in the blank with the appropriate term. _____ is an open wireless technology standard for exchanging data over short distances from fixed and mobile devices.

- A. Bluetooth

Correct Answer: A

Section:

Explanation:

Bluetooth is an open wireless technology standard for exchanging data over short distances from fixed and mobile devices, creating personal area networks with high levels of security. Created by telecoms vendor Ericsson in 1994, it was originally conceived as a wireless alternative to RS-232 data cables. It can connect several devices, overcoming problems of synchronization. Today Bluetooth is managed by the Bluetooth Special Interest Group.

QUESTION 84

In which of the following attacks does an attacker use software that tries a large number of key combinations in order to get a password?

- A. Buffer overflow
- B. Brute force attack
- C. Zero-day attack
- D. Smurf attack

Correct Answer: B

Section:

Explanation:

In a brute force attack, an attacker uses software that tries a large number of key combinations in order to get a password. To prevent such attacks, users should create passwords that are more difficult to guess, i.e., by using a minimum of six characters, alphanumeric combinations, and lower-upper case combinations.

Answer option D is incorrect. Smurf is an attack that generates significant computer network traffic on a victim network. This is a type of denial-of-service attack that floods a target system via spoofed broadcast ping messages. In such attacks, a perpetrator sends a large amount of ICMP echo request (ping) traffic to IP broadcast addresses, all of which have a spoofed source IP address of the intended victim. If the routing device delivering traffic to those broadcast addresses delivers the IP broadcast to all hosts, most hosts on that IP network will take the ICMP echo request and reply to it with an echo reply, which multiplies the traffic by the number of hosts responding.

Answer option A is incorrect. Buffer overflow is a condition in which an application receives more data than it is configured to accept. It helps an attacker not only to execute a malicious code on the target system but also to install backdoors on the target system for further attacks. All buffer overflow attacks are due to only sloppy programming or poor memory management by the application developers. The main types of buffer overflows are: Stack overflow Format string overflow Heap overflow Integer overflow Answer option C is incorrect. A zero-day attack, also known as zero-hour attack, is a computer threat that tries to exploit computer application vulnerabilities which are unknown to others, undisclosed to the software vendor, or for which no security fix is available. Zero-day exploits (actual code that can use a security hole to carry out an attack) are used or shared by attackers before the software vendor knows about the mvulnerability. User awareness training is the most effective technique to mitigate such attacks.

QUESTION 85

In an Ethernet peer-to-peer network, which of the following cables is used to connect two computers, using RJ-45 connectors and Category-5 UTP cable?

- A. Loopback
- B. Serial
- C. Parallel
- D. Crossover

Correct Answer: D

Section:

Explanation:

In an Ethernet peer-to-peer network, a crossover cable is used to connect two computers, using RJ-45 connectors and Category-5 UTP cable. Answer options C and B are incorrect. Parallel and serial cables do not use RJ-45 connectors and Category-5 UTP cable. Parallel cables are used to connect printers, scanners etc., to computers, whereas serial cables are used to connect modems, digital cameras etc., to computers. Answer option A is incorrect. A loopback cable is used for testing equipments.

QUESTION 86

Which of the following is a credit card-sized device used to securely store personal information and used in conjunction with a PIN number to authenticate users?

- A. Proximity card
- B. Java card
- C. SD card
- D. Smart card

Correct Answer: D

Section:

Explanation:

A smart card is a credit card-sized device used to securely store personal information such as certificates, public and private keys, passwords, etc. It is used in conjunction with a PIN number to authenticate users. In Windows, smart cards are used to enable certificate-based authentication. To use smart cards, Extensible Authentication Protocol (EAP) must be configured in Windows.

Answer option B is incorrect. Java Card is a technology that allows Java-based applications to be run securely on smart cards and small memory footprint devices. Java Card gives a user the ability to program devices and make them application specific. It is widely used in SIM cards and ATM cards. Java Card products are based on the Java Card Platform specifications developed by Sun Microsystems, a subsidiary of Oracle Corporation. Many Java card products also rely on the global platform specifications for the secure management of applications on the card. The main goals of the Java Card technology are portability and security.

Answer option A is incorrect. Proximity card (or Prox Card) is a generic name for contactless integrated circuit devices used for security access or payment systems. It can refer to the older 125 kHz devices or the newer 13.56 MHz contactless RFID cards, most commonly known as contactless smartcards. Modern proximity cards are covered by the ISO/IEC 14443 (Proximity Card) standard. There is also a related ISO/IEC 15693 (Vicinity Card) standard. Proximity cards are powered by resonant energy transfer and have a range of 0-3 inches in most instances. The user will usually be able to leave the card inside a wallet or purse. The price of the cards is also low, usually US\$2-\$5, allowing them to be used in applications such as identification cards, keycards, payment cards and public transit fare cards.

Answer option C is incorrect. Secure Digital (SD) card is a non-volatile memory card format used in portable devices such as mobile phones, digital cameras, and handheld computers. SD cards are based on the older MultiMediaCard (MMC) format, but they are a little thicker than MMC cards. Generally an SD card offers a write-protect switch on its side. SD cards generally measure 32 mm x 24 mm x 2.1 mm, but they can be as thin as 1.4 mm. The devices that have SD card slots can use the thinner MMC cards, but the standard SD cards will not fit into the thinner MMC slots. Some SD cards are also available with a USB connector. SD card readers allow SD cards to be accessed via many connectivity ports such as USB, FireWire, and the common parallel port.

QUESTION 87

Which of the following types of transmission is the process of sending one bit at a time over a single transmission line?

- A. Unicast transmission
- B. Serial data transmission
- C. Multicast transmission
- D. Parallel data transmission

Correct Answer: B

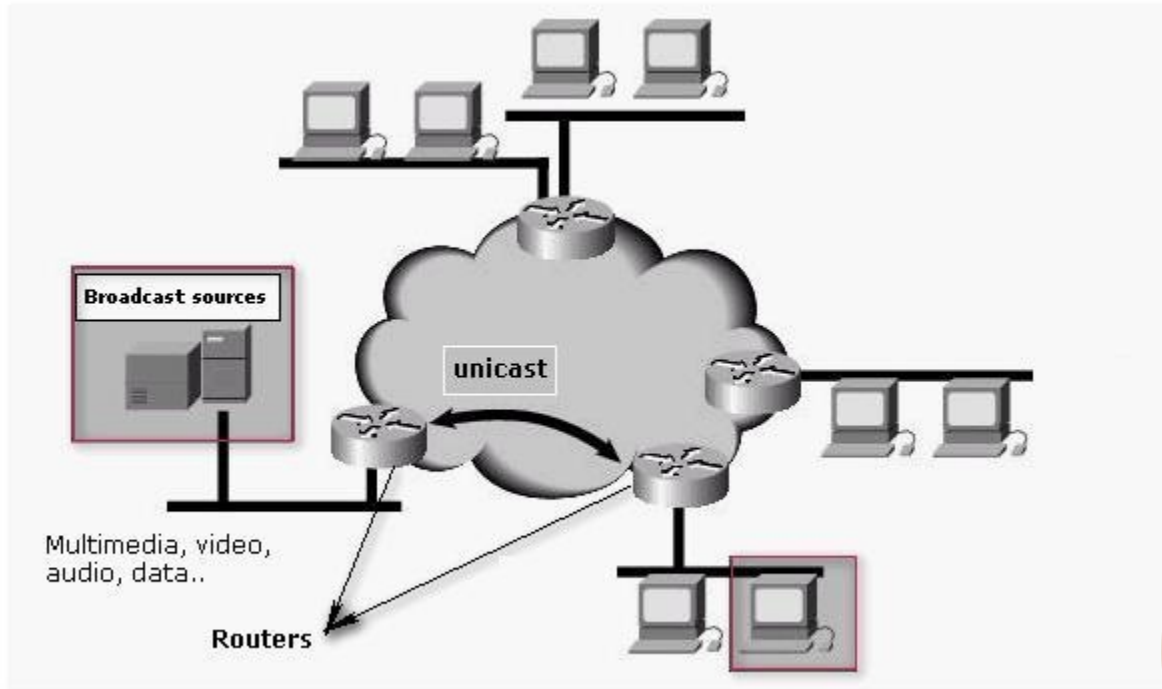


Section:

Explanation:

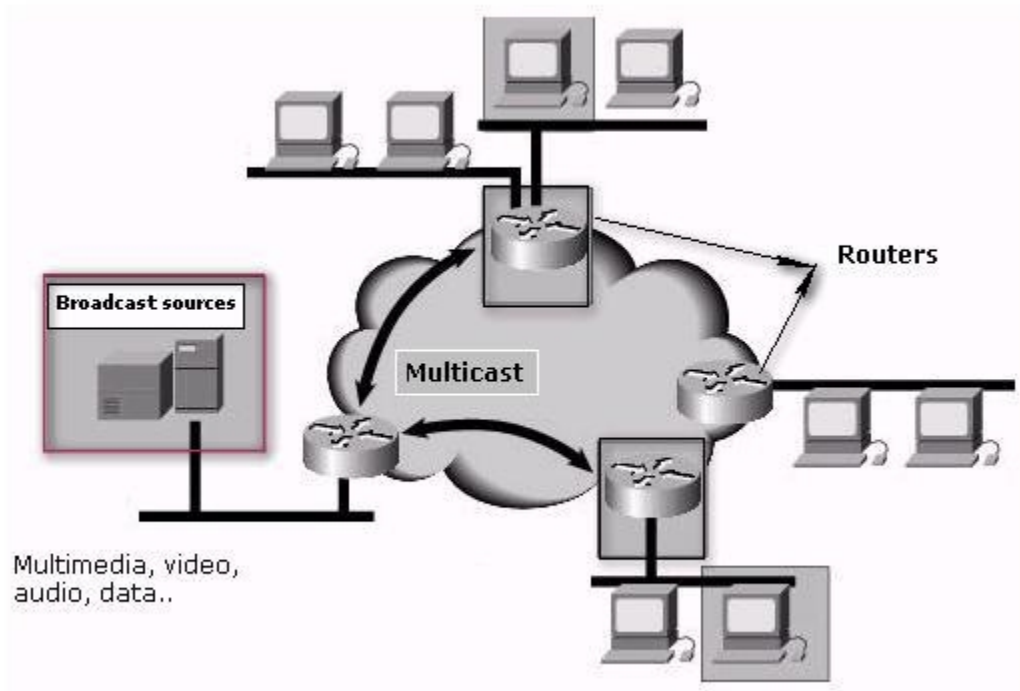
In serial data transmission, one bit is sent after another (bit-serial) on a single transmission line. It is the simplest method of transmitting digital information from one point to another. This transmission is suitable for providing communication between two participants as well as for multiple participants. It is used for all longhaul communication and provides high data rates. It is also inexpensive and beneficial in transferring data over long distances. Answer option D is incorrect. In parallel data transmission, several data signals are sent simultaneously over several parallel channels. Parallel data transmission is faster than serial data transmission. It is used primarily for transferring data between devices at the same site. For instance, communication between a computer and printer is most often parallel, allowing the entire byte to be transferred in one operation.

Answer option A is incorrect. The unicast transmission method is used to establish communication between a single host and a single receiver. Packets sent to a unicast address are delivered to the interface recognized by that IP address, as shown in the following figure:



vdumps

Answer option C is incorrect. The multicast transmission method is used to establish communication between a single host and multiple receivers. Packets are sent to all interfaces recognized by that IP address, as shown in the figure below:



QUESTION 88

FILL BLANK

Fill in the blank with the appropriate term. _____ management is an area of systems management that involves acquiring, testing, and installing multiple patches (code changes) to an administered computer

system.

A. Patch

Correct Answer: A

Section:

Explanation:

Patch management is an area of systems management that involves acquiring, testing, and installing multiple patches (code changes) to an administered computer system. Patch management includes the following tasks:

Maintaining current knowledge of available patches

Deciding what patches are appropriate for particular systems

Ensuring that patches are installed properly

Testing systems after installation, and documenting all associated procedures, such as specific configurations required A number of products are available to automate patch management tasks, including RingMaster's Automated Patch Management, PatchLink Update, and Gibraltar's Everguard.

QUESTION 89

Which of the following are used as a cost estimating technique during the project planning stage? Each correct answer represents a complete solution. (Choose three.)

A. Function point analysis

B. Program Evaluation Review Technique (PERT)

C. Expert judgment

D. Delphi technique

Correct Answer: A, C, D

Section:

Explanation:

Delphi technique, expert judgment, and function point analysis are used as a cost estimating technique during the project planning stage. Delphi is a technique to identify potential risk. In this technique, the responses are gathered via a questionnaire from different experts and their inputs are organized according to their contents. The collected responses are sent back to these experts for further input, addition, and comments. The final list of risks in the project is prepared after that. The participants in this technique are anonymous and therefore it helps prevent a person from unduly influencing the others in the group. The Delphi technique helps in reaching the consensus quickly. Expert judgment is a technique based on a set of criteria that has been acquired in a specific knowledge area or product area. It is obtained when the project manager or project team requires specialized knowledge that they do not possess. Expert judgment involves people most familiar with the work of creating estimates. Preferably, the project team member who will be doing the task should complete the estimates. Expert judgment is applied when performing administrative closure activities, and experts should ensure the project or phase closure is performed to the appropriate standards.

A function point is a unit of measurement to express the amount of business functionality an information system provides to a user. Function points are the units of measure used by the IFPUG Functional Size Measurement Method. The IFPUG FSM Method is an ISO recognized software metric to size an information system based on the functionality that is perceived by the user of the information system, independent of the technology used to implement the information system.

Answer option B is incorrect. A PERT chart is a project management tool used to schedule, organize, and coordinate tasks within a project. PERT stands for Program Evaluation Review Technique, a methodology developed by the U.S.

Navy in the 1950s to manage the Polaris submarine missile program. A PERT chart presents a graphic illustration of a project as a network diagram consisting of numbered nodes (either circles or rectangles) representing events, or milestones in the project linked by labeled vectors (directional lines) representing tasks in the project. The direction of the arrows on the lines indicates the sequence of tasks.

QUESTION 90

Which of the following UTP cables uses four pairs of twisted cable and provides transmission speeds of up to 16 Mbps?

A. Category 5e

B. Category 5

C. Category 3

D. Category 6

Correct Answer: C

Section:**Explanation:**

Category 3 type of UTP cable uses four pairs of twisted cable and provides transmission speeds of up to 16 Mbps. They are commonly used in Ethernet networks that operate at the speed of 10 Mbps. A higher speed is also possible by these cables implementing the Fast Ethernet (100Base-T4) specifications. This cable is used mainly for telephone systems.

Answer option B is incorrect. This category of UTP cable is the most commonly used cable in present day networks. It consists of four twisted pairs and is used in those Ethernet networks that run at the speed of 100 Mbps.

Category 5 cable can also provide a higher speed of up to 1000 Mbps.

Answer option A is incorrect. It is also known as Category 5 Enhanced cable. Its specification is the same as category 5, but it has some enhanced features and is used in Ethernets that run at the speed of 1000 Mbps.

Answer option D is incorrect. This category of UTP cable is designed to support high-speed networks that run at the speed of 1000 Mbps. It consists of four pairs of wire and uses all of them for data transmission. Category 6 provides more than twice the speed of Category 5e, but is also more expensive.

QUESTION 91

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

„It is a Linux-based WLAN WEP cracking tool that recovers encryption keys. It operates by passively monitoring transmissions. It uses Ciphertext 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. Cain
- B. PsPasswd
- C. Kismet
- D. AirSnort

Correct Answer: D

Section:**Explanation:**

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

Answer option C is incorrect. Kismet is a Linux-based 802.11 wireless network sniffer and intrusion detection system. It can work with any wireless card that supports raw monitoring (rfmon) mode. Kismet can sniff 802.11b, 802.11a, 802.11g, and 802.11n traffic. Kismet can be used for the following tasks:

To identify networks by passively collecting packets

To detect standard named networks

To detect masked networks

To collect the presence of non-beaconing networks via data traffic Answer option A is incorrect. Cain is a multipurpose tool that can be used to perform many tasks such as Windows password cracking, Windows enumeration, and VoIP session sniffing. This password cracking program can perform the following types of password cracking attacks: Dictionary attack

Brute force attack

Rainbow attack

Hybrid attack

Answer option B is incorrect. PsPasswd is a tool that helps Network Administrators change an account password on the local or remote system. The command syntax of PsPasswd is as follows: pspasswd

```
[\\computer[,computer[,...] | @file [-u user [-p psswd]] Username [NewPassword]
```

QUESTION 92

Which of the following statements are true about volatile memory? Each correct answer represents a complete solution. Choose all that apply.

- A. The content is stored permanently and even the power supply is switched off.
- B. A volatile storage device is faster in reading and writing data.
- C. Read only memory (ROM) is an example of volatile memory.
- D. It is computer memory that requires power to maintain the stored information.

Correct Answer: B, D

Section:**Explanation:**

Volatile memory, also known as volatile storage, is computer memory that requires power to maintain the stored information, unlike non-volatile memory which does not require a maintained power supply. It has been less popularly known as temporary memory. Most forms of modern random access memory (RAM) are volatile storage, including dynamic random access memory (DRAM) and static random access memory (SRAM). A volatile storage device is faster in reading and writing data.

Answer options A and C are incorrect. Non-volatile memory, nonvolatile memory, NVM, or non-volatile storage, in the most basic sense, is computer memory that can retain the stored information even when not powered. Examples of nonvolatile memory include read-only memory, flash memory, most types of magnetic computer storage devices (e.g. hard disks, floppy disks, and magnetic tape), optical discs, and early computer storage methods such as paper tape and punched cards.

QUESTION 93

You are a professional Computer Hacking forensic investigator. You have been called to collect evidences of buffer overflow and cookie snooping attacks. Which of the following logs will you review to accomplish the task? Each correct answer represents a complete solution. Choose all that apply.

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

Correct Answer: A, C, D

Section:

Explanation:

Evidences of buffer overflow and cookie snooping attacks can be traced from system logs, event logs, and program logs, depending on the type of overflow or cookie snooping attack executed and the error recovery method used by the hacker.

Answer option B is incorrect. Web server logs are used to investigate cross-site scripting attacks.

QUESTION 94

John works as an Ethical Hacker for www.company.com Inc. He wants to find out the ports that are open in www.company.com's server using a port scanner. However, he does not want to establish a full TCP connection. Which of the following scanning techniques will he use to accomplish this task?

- A. TCP SYN
- B. Xmas tree
- C. TCP SYN/ACK
- D. TCP FIN

Correct Answer: A

Section:

Explanation:

According to the scenario, John does not want to establish a full TCP connection. Therefore, he will use the TCP SYN scanning technique. TCP SYN scanning is also known as half-open scanning because in this type of scanning, a full TCP connection is never opened. The steps of TCP SYN scanning are as follows:

- 1.The attacker sends a SYN packet to the target port.
- 2.If the port is open, the attacker receives the SYN/ACK message.
- 3.Now the attacker breaks the connection by sending an RST packet.
- 4.If the RST packet is received, it indicates that the port is closed.

This type of scanning is hard to trace because the attacker never establishes a full 3-way handshake connection and most sites do not create a log of incomplete TCP connections.

Answer option C is incorrect. In TCP SYN/ACK scanning, an attacker sends a SYN/ACK packet to the target port. If the port is closed, the victim assumes that this packet was mistakenly sent by the attacker, and sends the RST packet to the attacker. If the port is open, the SYN/ACK packet will be ignored and the port will drop the packet. TCP SYN/ACK scanning is stealth scanning, but some intrusion detection systems can detect TCP SYN/ACK scanning.

Answer option D is incorrect. TCP FIN scanning is a type of stealth scanning through which the attacker sends a FIN packet to the target port.

If the port is closed, the victim assumes that this packet was sent mistakenly by the attacker and sends the RST packet to the attacker. If the port is open, the FIN packet will be ignored and the port will drop that packet. TCP FIN scanning is useful only for identifying ports of non-Windows operating systems because

Windows operating systems send only RST packets irrespective of whether the port is open or closed.

Answer option B is incorrect. Xmas Tree scanning is just the opposite of null scanning. In Xmas Tree scanning, all packets are turned on. If the target port is open, the service running on the target port discards the packets without any reply. According to RFC 793, if the port is closed, the remote system replies with the RST packet. Active monitoring of all incoming packets can help system network administrators detect an Xmas Tree scan.

QUESTION 95

FILL BLANK

Fill in the blank with the appropriate term.

_____ is a prime example of a high-interaction honeypot.

A. Honeynet

Correct Answer: A

Section:

Explanation:

Honeynet is a prime example of a high-interaction honeypot. Two or more honeypots on a network form a honeynet. Typically, a honeynet is used for monitoring a larger and/or more diverse network in which one honeypot may not be sufficient. Honeynets and honeypots are usually implemented as parts of larger network intrusion-detection systems. A honeyfarm is a centralized collection of honeypots and analysis tools.

QUESTION 96

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

A. NetResident

B. Wireshark

C. Bridle

D. NetWitness

E. None

Correct Answer: B

Section:

Explanation:

Wireshark is an open source protocol analyzer that can capture traffic in real time. Wireshark is a free packet sniffer computer application. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Wireshark is very similar to tcpdump, but it has a graphical frontend, and many more information sorting and filtering options. It allows the user to see all traffic being passed over the network (usually an Ethernet network but support is being added for others) by putting the network interface into promiscuous mode.

Wireshark uses pcap to capture packets, so it can only capture the packets on the networks supported by pcap. It has the following features:

Data can be captured "from the wire" from a live network connection or read from a file that records the already-captured packets.

Live data can be read from a number of types of network, including Ethernet, IEEE 802.11, PPP, and loopback.

Captured network data can be browsed via a GUI, or via the terminal (command line) version of the utility, tshark.

Captured files can be programmatically edited or converted via command-line switches to the "editcap" program.

Data display can be refined using a display filter. Plugins can be created for dissecting new protocols.

Answer option C is incorrect. Snort is an open source network intrusion prevention and detection system that operates as a network sniffer. It logs activities of the network that is matched with the predefined signatures.

Signatures can be designed for a wide range of traffic, including Internet Protocol (IP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP). Answer option D is incorrect. NetWitness is used to analyze and monitor the network traffic and activity.

Answer option A is incorrect. Netresident is used to capture, store, analyze, and reconstruct network events and activities.

QUESTION 97

Which of the following tools are NOT used for logging network activities in the Linux operating system? Each correct answer represents a complete solution.

Choose all that apply.

A. PsLoggedOn

B. PsGetSid



- C. Timbersee
- D. Swatch

Correct Answer: A, B

Section:

Explanation:

PsLoggedOn and PsGetSid are not logging tools. They are command-line utilities used in the Windows operating system.

PsLoggedOn is an applet that displays both the local and remote logged on users. If an attacker specifies a user name instead of a computer, PsLoggedOn searches the computers in the network and tells whether the user is currently logged on or not. The command syntax for PsLoggedOn is as follows: psloggedon [-] [-l] [-x] [\\computername | username] PsGetSid is a tool that is used to query SIDs remotely. Using PsGetSid, the attacker can access the SIDs of user accounts and translate an SID into the user name. The command syntax for PsGetSid is as follows: psgetsid [\\computer[,computer[,...]] | @file] [-u username [-p password]] [account|SID]

Answer options C and D are incorrect. Timbersee and Swatch are tools used for logging network activities in the Linux operating system.

QUESTION 98

FILL BLANK

Fill in the blank with the appropriate term.

The _____ model is a description framework for computer network protocols and is sometimes called the Internet Model or the DoD Model.

- A. TCP/IP

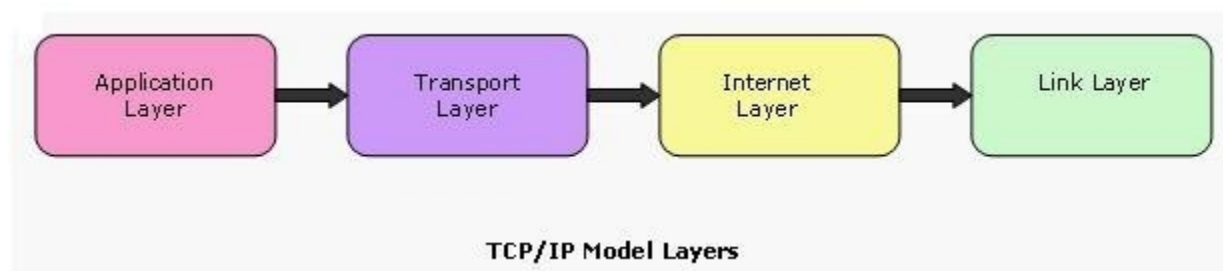
Correct Answer: A

Section:

Explanation:

The TCP/IP model is a description framework for computer network protocols. It describes a set of general design guidelines and implementations of specific networking protocols to enable computers to communicate over a network. TCP/IP provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination. Protocols exist for a variety of different types of communication services between computers. The TCP/IP Model is sometimes called the Internet Model or the DoD Model.

The TCP/IP model has four unique layers as shown in the image. This layer architecture is often compared with the seven-layer OSI Reference Model. The TCP/ IP model and related protocols are maintained by the Internet Engineering Task Force (IETF).



QUESTION 99

Which of the following is a software tool used in passive attacks for capturing network traffic?

- A. Intrusion prevention system
- B. Intrusion detection system
- C. Warchalking
- D. Sniffer

Correct Answer: D

Section:

Explanation:

A sniffer is a software tool that is used to capture any network traffic. Since a sniffer changes the NIC of the LAN card into promiscuous mode, the NIC begins to record incoming and outgoing data traffic across the network. A sniffer attack is a passive attack because the attacker does not directly connect with the target host. This attack is most often used to grab logins and passwords from network traffic. Tools such as Ethereal, Snort, Windump, EtherPeek, Dsniff are some good examples of sniffers. These tools provide many facilities to users such as graphical user interface, traffic statistics graph, multiple sessions tracking, etc.

Answer option A is incorrect. An intrusion prevention system (IPS) is a network security device that monitors network and/or system activities for malicious or unwanted behavior and can react, in real-time, to block or prevent those activities. When an attack is detected, it can drop the offending packets while still allowing all other traffic to pass.

Answer option B is incorrect. An IDS (Intrusion Detection System) is a device or software application that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station. Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators.

Answer option C is incorrect. Warchalking is the drawing of symbols in public places to advertise an open Wi-Fi wireless network. Having found a Wi-Fi node, the warchalker draws a special symbol on a nearby object, such as a wall, the pavement, or a lamp post. The name warchalking is derived from the cracker terms war dialing and war driving.

QUESTION 100

Which of the following types of coaxial cable is used for cable TV and cable modems?

- A. RG-8
- B. RG-62
- C. RG-59
- D. RG-58

Correct Answer: C

Section:

Explanation:

RG-59 type of coaxial cable is used for cable TV and cable modems.

Answer option A is incorrect. RG-8 coaxial cable is primarily used as a backbone in an Ethernet LAN environment and often connects one wiring closet to another. It is also known as 10Base5 or ThickNet.

Answer option B is incorrect. RG-62 coaxial cable is used for ARCNET and automotive radio antennas.

Answer option D is incorrect. RG-58 coaxial cable is used for Ethernet networks. It uses baseband signaling and 50-Ohm terminator. It is also known as 10Base2 or ThinNet.

QUESTION 101

In which of the following transmission modes is communication bi-directional?

- A. Root mode
- B. Simplex mode
- C. Full-duplex mode
- D. Half-duplex mode

Correct Answer: C

Section:

QUESTION 102

Which of the following is a presentation layer protocol?

- A. TCP
- B. RPC
- C. BGP
- D. LWAPP

Correct Answer: D

Section:

QUESTION 103

Which of the following is a session layer protocol?



- A. RPC
- B. SLP
- C. RDP
- D. ICMP

Correct Answer: A

Section:

QUESTION 104

Which of the following IEEE standards is an example of a DQDB access method?

- A. 802.3
- B. 802.5
- C. 802.6
- D. 802.4

Correct Answer: C

Section:

QUESTION 105

Which of the following classes of IP addresses provides a maximum of only 254 host addresses per network ID?

- A. Class D
- B. Class B
- C. Class C
- D. Class A

Correct Answer: C

Section:

QUESTION 106

Which of the following ranges of addresses can be used in the first octet of a Class C network address?

- A. 128-191
- B. 192-223
- C. 0-127
- D. 224-255

Correct Answer: B

Section:

QUESTION 107

Which of the following standards defines Logical Link Control (LLC)?

- A. 802.2
- B. 802.3



- C. 802.5
- D. 802.4

Correct Answer: A

Section:

QUESTION 108

Which of the following layers performs routing of IP datagrams?

- A. Transport layer
- B. Link layer
- C. Application layer
- D. Internet layer

Correct Answer: D

Section:

QUESTION 109

Which of the following IP addresses is the loopback address in IPv6?

- A. 0:0:0:0:0:0:0:1
- B. 0:0:0:1:1:0:0:0
- C. 0:0:0:0:0:0:0:0
- D. 1:0:0:0:0:0:0:0

Correct Answer: A

Section:

QUESTION 110

What is the bit size of the Next Header field in the IPv6 header format?

- A. 2 bits
- B. 4 bits
- C. 8 bits
- D. 20 bits

Correct Answer: C

Section:

QUESTION 111

Which of the following layers of the OSI model provides interhost communication?

- A. Application layer
- B. Network layer
- C. Transport layer
- D. Session layer



Correct Answer: D

Section:

QUESTION 112

Which of the following IEEE standards provides specifications for wireless ATM systems?

- A. 802.1
- B. 802.5
- C. 802.3
- D. 802.11a

Correct Answer: D

Section:

QUESTION 113

The IP addresses reserved for multicasting belong to which of the following classes?

- A. Class B
- B. Class E
- C. Class C
- D. Class D

Correct Answer: D

Section:

QUESTION 114

Which of the following is a computer network that covers a broad area?

- A. SAN
- B. PAN
- C. CAN
- D. WAN

Correct Answer: D

Section:

QUESTION 115

Which of the following layers of the OSI model provides end-to-end connections and reliability?

- A. Transport layer
- B. Session layer
- C. Network layer
- D. Physical layer

Correct Answer: A

Section:



QUESTION 116

In an Ethernet peer-to-peer network, which of the following cables is used to connect two computers, using RJ-45 connectors and Category-5 UTP cable?

- A. Serial
- B. Loopback
- C. Crossover
- D. Parallel

Correct Answer: C

Section:

Explanation:

In an Ethernet peer-to-peer network, a crossover cable is used to connect two computers, using RJ-45 connectors and Category-5 UTP cable.



Answer options D and A are incorrect. Parallel and serial cables do not use RJ-45 connectors and Category-5 UTP cable. Parallel cables are used to connect printers, scanners etc., to computers, whereas serial cables are used to connect modems, digital cameras etc., to computers.

Answer option B is incorrect. A loopback cable is used for testing equipments.

QUESTION 117

You work as a Network Security Analyzer. You got a suspicious email while working on a forensic project. Now, you want to know the IP address of the sender so that you can analyze various information such as the actual location, domain information, operating system being used, contact information, etc. of the email sender with the help of various tools and resources. You also want to check whether this email is fake or real. You know that analysis of email headers is a good starting point in such cases. The email header of the suspicious email is given below:

```

X-Apparently-To: itzme_adee@yahoo.com via 209.191.91.180; Mon, 10 Aug 2009 07:59:47 -0700
Return-Path: <bounce@vetpaintmail.com>
X-YahooFilteredBulk: 216.168.54.25
X-YMailISG: II0jRIWLDshqPeX9g5WgzYv2NbqcgrXw47uBekfvpP65bE42euHuhU20U9QtaJk9thI3dhriCmF.cmku96g9o8ggD
X-Originating-IP: [216.168.54.25]
Authentication-Results: mta251.mail.re3.yahoo.com from=vetpaintmail.com; domainkeys=pass (ok)
Received: from 216.168.54.25 (EHLO mail.vetpaintmail.com) (216.168.54.25) by mta251.mail.re3.yahoo.com with SM
Received: from vetpaintmail.com ([172.16.10.90]) by mail.vetpaintmail.com (StrongMail Enterprise 4.1.1.1(4.1.1-448:
X-VirtualServer: Digest, mail.vetpaintmail.com, 172.16.10.93
X-VirtualServerGroup: Digest
X-MailingID: 1101167079::64600::1249057716::9100::1133::1133
X-SMHeaderMap: mid="X-MailingID"
X-Mailer: StrongMail Enterprise 4.1.1.1(4.1.1-44827)
X-Destination-ID: itzme_adee@yahoo.com
X-SMFBID: aXR6bWVfYWRIZUB5YWhvby5jb20=
DomainKey-Signature: a=rsa-sha1; c=noofs; s=customer; d=vetpaintmail.com; q=dns; b=Yv6LNRzb+8Jaik8frIKfeO2WPnpkJMzJ1F
Content-Transfer-Encoding: 7bit
Content-Type: multipart/alternative; boundary="-----_NextPart_0F9_1F0B_2109CDA4.577F5A4D"
Reply-To: <no-reply@vetpaintmail.com>
MIME-Version: 1.0
Message-ID: <1101167079.1133@vetpaintmail.com>
Subject: The Ethical Hacking Weekly Digest
Date: Mon, 10 Aug 2009 07:37:02 -0700
To: itzme_adee@yahoo.com
From:  The Ethical Hacking <info@vetpaintmail.com> 
Content-Length: 35382

```

What is the IP address of the sender of this email?

- A. 209.191.91.180

- B. 141.1.1.1
- C. 172.16.10.90
- D. 216.168.54.25

Correct Answer: D

Section:

Explanation:

The IP address of the sender of this email is 216.168.54.25. According to the scenario, you want to know the IP address of the sender so that you can analyze various information such as the actual location, domain information, operating system being used, contact information, etc. of the email sender with the help of various tools and resources. You also want to check whether this email is fake or real. You know that analysis of email headers is a good starting point in such cases. Once you start to analyze the email header, you get an entry entitled as X-Originating-IP. You know that in Yahoo, the X-Originating-IP is the IP address of the email sender and in this case, the required IP address is 216.168.54.25. Answer options A, C, and B are incorrect. All these are the IP addresses of the Yahoo and Wetpaint servers.

QUESTION 118

Which of the following is the practice of sending unwanted e-mail messages, frequently with commercial content, in large quantities to an indiscriminate set of recipients? Each correct answer represents a complete solution. Choose all that apply.

- A. Email spoofing
- B. Junk mail
- C. E-mail spam
- D. Email jamming

Correct Answer: B, C

Section:

Explanation:

E-mail spam, also known as unsolicited bulk email (UBE), junk mail, or unsolicited commercial email (UCE), is the practice of sending unwanted e-mail messages, frequently with commercial content, in large quantities to an indiscriminate set of recipients.

Answer option A is incorrect. Email spoofing is a fraudulent email activity in which the sender address and other parts of the email header are altered to appear as though the email originated from a different source. Email spoofing is a technique commonly used in spam and phishing emails to hide the origin of the email message. By changing certain properties of the email, such as the From, Return-Path and Reply-To fields (which can be found in the message header), illintentioned users can make the email appear to be from someone other than the actual sender. The result is that, although the email appears to come from the address indicated in the From field (found in the email headers), it actually comes from another source.

Answer option D is incorrect. Email jamming is the use of sensitive words in e-mails to jam the authorities that listen in on them by providing a form of a red herring and an intentional annoyance. In this attack, an attacker deliberately includes "sensitive" words and phrases in otherwise innocuous emails to ensure that these are picked up by the monitoring systems. As a result, the senders of these emails will eventually be added to a "harmless" list and their emails will be no longer intercepted, hence it will allow them to regain some privacy.

QUESTION 119

Which of the following is a worldwide organization that aims to establish, refine, and promote Internet security standards?

- A. ANSI
- B. WASC
- C. IEEE
- D. ITU

Correct Answer: B

Section:

Explanation:

Web Application Security Consortium (WASC) is a worldwide organization that aims to establish, refine, and promote Internet security standards. WASC is vendor-neutral, although members may belong to corporations involved in the research, development, design, and distribution of Web security-related products.

Answer option A is incorrect. ANSI (American National Standards Institute) is the primary organization for fostering the development of technology standards in the United States. ANSI works with industry groups and is the

U.S. member of the International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC). Long-established computer standards from ANSI include the American Standard Code for Information Interchange (ASCII) and the Small Computer System Interface (SCSI).

Answer option D is incorrect. The International Telecommunication Union (ITU) is an organization established to standardize and regulate international radio and telecommunications. Its main tasks include standardization, allocation of the radio spectrum, and organizing interconnection arrangements between different countries to allow international phone calls. ITU sets standards for global telecom networks.

The ITU's telecommunications division (ITU-T) produces more than 200 standard recommendations each year in the converging areas of telecommunications, information technology, consumer electronics, broadcasting and multimedia communications. ITU was streamlined into the following three sectors:

ITU-D (Telecommunication Development)

ITU-R (Radio communication)

ITU-T (Telecommunication Standardization)

Answer option C is incorrect. The Institute of Electrical and Electronic Engineers (IEEE) is a society of technical professionals. It promotes the development and application of electro-technology and allied sciences. IEEE develops communications and network standards, among other activities. The organization publishes number of journals, has many local chapters, and societies in specialized areas.

QUESTION 120

Which of the following statements are TRUE about Demilitarized zone (DMZ)? Each correct answer represents a complete solution. Choose all that apply.

- A. In a DMZ configuration, most computers on the LAN run behind a firewall connected to a public network like the Internet.
- B. Demilitarized zone is a physical or logical sub-network that contains and exposes external services of an organization to a larger un-trusted network.
- C. The purpose of a DMZ is to add an additional layer of security to the Local Area Network of an organization.
- D. Hosts in the DMZ have full connectivity to specific hosts in the internal network.

Correct Answer: A, B, C

Section:

Explanation:

A demilitarized zone (DMZ) is a physical or logical subnetwork that contains and exposes external services of an organization to a larger network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's Local Area Network (LAN); an external attacker only has access to equipment in the DMZ, rather than the whole of the network. Hosts in the DMZ have limited connectivity to specific hosts in the internal network, though communication with other hosts in the DMZ and to the external network is allowed. This allows hosts in the DMZ to provide services to both the internal and external networks, while an intervening firewall controls the traffic between the DMZ servers and the internal network clients. In a DMZ configuration, most computers on the LAN run behind a firewall connected to a public network such as the Internet.

QUESTION 121

Which of the following network scanning tools is a TCP/UDP port scanner that works as a ping sweeper and hostname resolver?

- A. Hping
- B. SuperScan
- C. Netstat
- D. Nmap

Correct Answer: B

Section:

Explanation:

SuperScan is a TCP/UDP port scanner. It also works as a ping sweeper and hostname resolver. It can ping a given range of IP addresses and resolve the host name of the remote system. The features of SuperScan are as follows:

It scans any port range from a built-in list or any given range.

It performs ping scans and port scans using any IP range.

It modifies the port list and port descriptions using the built in editor.

It connects to any discovered open port using user-specified "helper" applications. It has the transmission speed control utility.

Answer option D is incorrect. Nmap is a free open-source utility for network exploration and security auditing. It is used to discover computers and services on a computer network, thus creating a "map" of the network. Just like many simple port scanners, Nmap is capable of discovering passive services. In addition, Nmap may be able to determine various details about the remote computers. These include operating system, device type, uptime, software product used to run a service, exact version number of that product, presence of some firewall techniques and, on a local area network, even vendor of the remote network card.

Nmap runs on Linux, Microsoft Windows, etc.

Answer option C is incorrect. Netstat (network statistics) is a command-line tool that displays network connections (both incoming and outgoing), routing tables, and a number of network interface statistics. It is available on Unix, Unix-like, and Windows NT-based operating systems. It is used to find problems on the network and to determine the amount of traffic on the network as a performance measurement.

Answer option A is incorrect. Hping is a free packet generator and analyzer for the TCP/IP protocol. Hping is one of the de facto tools for security auditing and testing of firewalls and networks. The new version of hping, hping3, is scriptable using the Tcl language and implements an engine for string based, human readable description of TCP/IP packets, so that the programmer can write scripts related to low level TCP/IP packet manipulation and analysis in very short time.

Like most tools used in computer security, hping is useful to both system administrators and crackers (or script kiddies).

QUESTION 122

Which of the following is a network layer protocol used to obtain an IP address for a given hardware (MAC) address?

- A. IP
- B. PIM
- C. RARP
- D. ARP

Correct Answer: C

Section:

Explanation:

Reverse Address Resolution Protocol (RARP) is a Network layer protocol used to obtain an IP address for a given hardware (MAC) address. RARP is sort of the reverse of an ARP. Common protocols that use RARP are BOOTP and DHCP. Answer option D is incorrect. Address Resolution Protocol (ARP) is a network maintenance protocol of the TCP/IP protocol suite. It is responsible for the resolution of IP addresses to media access control (MAC) addresses of a network interface card (NIC). The ARP cache is used to maintain a correlation between a MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions. ARP is limited to physical network systems that support broadcast packets.

Answer option B is incorrect. Protocol-Independent Multicast (PIM) is a family of multicast routing protocols for Internet Protocol (IP) networks that provide oneto-many and many-to-many distribution of data over a LAN, WAN, or the Internet. It is termed protocol-independent because PIM does not include its own topology discovery mechanism, but instead uses routing information supplied by other traditional routing protocols, such as Border Gateway Protocol (BGP).

Answer option A is incorrect. The Internet Protocol (IP) is a protocol used for communicating data across a packet-switched inter-network using the Internet Protocol Suite, also referred to as TCP/IP.

IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses. For this purpose, the Internet Protocol defines addressing methods and structures for datagram encapsulation. The first major version of addressing structure, now referred to as Internet Protocol Version 4 (IPv4), is still the dominant protocol of the Internet, although the successor, Internet Protocol Version 6 (IPv6), is being deployed actively worldwide.

QUESTION 123

FILL BLANK

Fill in the blank with the appropriate term.

A _____ is a term in computer terminology used for a trap that is set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems.

- A. honeypot

Correct Answer: A

Section:

Explanation:

A honeypot is a term in computer terminology used for a trap that is set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems. Generally it consists of a computer, data, or a network site that appears to be part of a network, but is actually isolated, and monitored, and which seems to contain information or a resource of value to attackers.

QUESTION 124

James is working as a Network Administrator in a reputed company situated in California. He is monitoring his network traffic with the help of Wireshark. He wants to check and analyze the traffic against a PING sweep attack. Which of the following Wireshark filters will he use?

- A. icmp.type==8 or icmp.type==16
- B. icmp.type==8 or icmp.type==0

- C. icmp.type==8 and icmp.type==0
- D. icmp.type==0 and icmp.type==16

Correct Answer: B

Section:

QUESTION 125

Management wants to bring their organization into compliance with the ISO standard for information security risk management. Which ISO standard will management decide to implement?

- A. ISO/IEC 27005
- B. ISO/IEC 27006
- C. ISO/IEC 27002
- D. ISO/IEC 27004

Correct Answer: A

Section:

QUESTION 126

Which of the following systems includes an independent NAS Head and multiple storage arrays?

- A. FreeNAS
- B. None of these
- C. Gateway NAS System
- D. Integrated NAS System

Correct Answer: C

Section:

QUESTION 127

You are monitoring your network traffic with the Wireshark utility and noticed that your network is experiencing a large amount of traffic from a certain region.

You suspect a DoS incident on the network. What will be your first reaction as a first responder?

- A. Avoid Fear, Uncertainty and Doubt
- B. Communicate the incident
- C. Make an initial assessment
- D. Disable Virus Protection

Correct Answer: A

Section:

QUESTION 128

The security network team is trying to implement a firewall capable of operating only in the session layer, monitoring the TCP inter-packet link protocol to determine when a requested session is legitimate or not. Using this type of firewall, they could be able to intercept the communication, making the external network see that the firewall is the source, and facing the user, who responds from the outside is the firewall itself. They are just limiting a requirements previous listed, because they already have a packet filtering firewall and they must add a cheap solution that meets the objective. What kind of firewall would you recommend?

- A. Packet Filtering with NAT
- B. Circuit Level Gateway



- C. Application Proxies
- D. Application Level Gateways

Correct Answer: B

Section:

QUESTION 129

FILL BLANK

Fill in the blank with the appropriate term.

A _____ gateway is a type of network gateway that provides the added capability to control devices across the Internet.

- A. home automation

Correct Answer: A

Section:

Explanation:

A home automation gateway is a type of network gateway that provides the added capability to control devices across the Internet. Most gateways plug in to the home broadband router (and a wall outlet for power). When connected to a router that has Internet connectivity, the automation gateway helps in enabling computers and Web-enabled phones to remotely access automation devices at home.

QUESTION 130

Which of the following is a network maintenance protocol of the TCP/IP protocol suite that is responsible for the resolution of IP addresses to media access control (MAC) addresses of a network interface card (NIC)?

- A. DHCP
- B. ARP
- C. PIM
- D. RARP



Correct Answer: B

Section:

Explanation:

Address Resolution Protocol (ARP) is a network maintenance protocol of the TCP/IP protocol suite. It is responsible for the resolution of IP addresses to media access control (MAC) addresses of a network interface card (NIC). The ARP cache is used to maintain a correlation between a MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions. ARP is limited to physical network systems that support broadcast packets.

Answer option A is incorrect. The Dynamic Host Configuration Protocol (DHCP) is a computer networking protocol used by hosts (DHCP clients) to retrieve IP address assignments and other configuration information. DHCP uses a clientserver architecture. The client sends a broadcast request for configuration information. The DHCP server receives the request and responds with configuration information from its configuration database. In the absence of DHCP, all hosts on a network must be manually configured individually - a time-consuming and often error-prone undertaking. DHCP is popular with ISP's because it allows a host to obtain a temporary IP address.

Answer option D is incorrect. Reverse Address Resolution Protocol (RARP) is a Network layer protocol used to obtain an IP address for a given hardware (MAC) address. RARP is sort of the reverse of an ARP. Common protocols that use RARP are BOOTP and DHCP.

Answer option C is incorrect. Protocol-Independent Multicast (PIM) is a family of multicast routing protocols for Internet Protocol (IP) networks that provide oneto-many and many-to-many distribution of data over a LAN, WAN, or the Internet. It is termed protocol-independent because PIM does not include its own topology discovery mechanism, but instead uses routing information supplied by other traditional routing protocols, such as Border Gateway Protocol (BGP).

QUESTION 131

What is the range for registered ports?

- A. 1024 through 49151
- B. 0 through 1023
- C. Above 65535

D. 49152 through 65535

Correct Answer: A

Section:

QUESTION 132

How many layers are present in the TCP/IP model?

- A. 10
- B. 5
- C. 4
- D. 7

Correct Answer: B

Section:

QUESTION 133

In which of the following transmission modes is communication uni-directional?

- A. Root mode
- B. Full-duplex mode
- C. Half-duplex mode
- D. Simplex mode

Correct Answer: D

Section:

QUESTION 134

CSMA/CD is specified in which of the following IEEE standards?

- A. 802.3
- B. 802.2
- C. 802.1
- D. 802.15

Correct Answer: A

Section:

QUESTION 135

What is the response of an Xmas scan if a port is either open or filtered?

- A. RST
- B. No response
- C. FIN
- D. PUSH

Correct Answer: B



Section:

QUESTION 136

Which of the following fields in the IPv6 header replaces the TTL field in the IPv4 header?

- A. Next header
- B. Traffic class
- C. Hop limit
- D. Version

Correct Answer: C

Section:

QUESTION 137

Which of the following IEEE standards defines a physical bus topology?

- A. 802.4
- B. 802.5
- C. 802.6
- D. 802.3

Correct Answer: A

Section:

QUESTION 138

Which of the following represents a network that connects two or more LANs in the same geographical area?

- A. PAN
- B. WAN
- C. MAN
- D. SAN

Correct Answer: C

Section:

QUESTION 139

The IP addresses reserved for experimental purposes belong to which of the following classes?

- A. Class E
- B. Class C
- C. Class A
- D. Class D

Correct Answer: A

Section:

QUESTION 140



Which of the following layers is closest to the end user?

- A. Application layer
- B. Physical layer
- C. Session layer
- D. Presentation layer

Correct Answer: A

Section:

QUESTION 141

Which of the following IEEE standards defines the token passing ring topology?

- A. 802.4
- B. 802.5
- C. 802.3
- D. 802.7

Correct Answer: B

Section:

QUESTION 142

Physical access controls help organizations monitor, record, and control access to the information assets and facility. Identify the category of physical security controls which includes security labels and warning signs.

- A. Technical control
- B. Environmental control
- C. Physical control
- D. Administrative control

Correct Answer: D

Section:

QUESTION 143

Which Internet access policy starts with all services blocked and the administrator enables safe and necessary services individually, which provides maximum security and logs everything, such as system and network activities?

- A. Internet access policy
- B. Paranoid policy
- C. Permissive policy
- D. Prudent policy

Correct Answer: D

Section:

QUESTION 144

Daniel who works as a network administrator has just deployed an IDS in his organization's network. He wants to calculate the False Positive rate for his implementation. Which of the following formulas will he use, to calculate the False Positive rate?

- A. False Negative/True Negative+True Positive
- B. False Positive/False Positive+True Negative
- C. True Negative/False Negative+True Positive
- D. False Negative/False Negative+True Positive

Correct Answer: B

Section:

QUESTION 145

The SNMP contains various commands that reduce the burden on the network administrators. Which of the following commands is used by SNMP agents to notify SNMP managers about an event occurring in the network?

- A. INFORM
- B. RESPONSE
- C. TRAPS
- D. SET

Correct Answer: C

Section:

QUESTION 146

As a network administrator, you have implemented WPA2 encryption in your corporate wireless network. The WPA2's _____ integrity check mechanism provides security against a replay attack.

- A. CBC-MAC
- B. CRC-MAC
- C. CBC-32
- D. CRC-32



Correct Answer: A

Section:

QUESTION 147

Paul is a network security technician working on a contract for a laptop manufacturing company in Chicago. He has focused primarily on securing network devices, firewalls, and traffic traversing in and out of the network. He just finished setting up a server a gateway between the internal private network and the outside public network. This server will act as a proxy, limited amount of services, and will filter packets. What is this type of server called?

- A. Session layer firewall.
- B. SOCKS host.
- C. Bastion host.
- D. Edge transport server.

Correct Answer: C

Section:

QUESTION 148

Your company is planning to use an uninterruptible power supply (UPS) to avoid damage from power fluctuations. As a network administrator, you need to suggest an appropriate UPS solution suitable for specific resources or conditions. Match the type of UPS with the use and advantage:

1. Line Interactive	i. Unstable when operating a modern computer power supply load
2. Double Conversion On-Line	ii. Used for server rooms
3. Delta Conversion On-Line	iii. Useful where complete isolation and/or direct connectivity is required
4. Standby-Ferro	iv. Used in environments where electrical isolation is necessary
	v. Used for small business, Web, and departmental servers

- A. 1-i,2-iv,3-ii,4-v
- B. 1-v,2-iii,3-i,4-ii
- C. 1-ii,2-iv,3-iii,4-i
- D. 1-iii,2-iv,3-v,4-iv

Correct Answer: C
Section:

QUESTION 149

John has successfully remediated the vulnerability of an internal application that could have caused a threat to the network. He is scanning the application for the existence of a remediated vulnerability, this process is called a _____ and it has to adhere to the _____.

- A. Mitigation, Security policies
- B. Verification, Security Policies
- C. Vulnerability scanning, Risk Analysis
- D. Risk analysis, Risk matrix

Correct Answer: D
Section:

QUESTION 150

Which filter to locate unusual ICMP request an Analyst can use in order to detect a ICMP probes from the attacker to a target OS looking for the response to perform ICMP based fingerprinting?

- A. (icmp.type==9 && (!(icmp.code==9))
- B. (icmp.type==8 && (!(icmp.code==8))
- C. (icmp.type==12) | | (icmp.type==15| |(icmp.type==17)
- D. (icmp.type==14) | | (icmp.type==15| |(icmp.type==17)

Correct Answer: B
Section:

QUESTION 151

You are using Wireshark to monitor your network traffic and you see a lot of packages with the FIN, PUSH and URG flags activated; what can you infer about this behavior?

- A. The Layer 3 Controls are activated in the Switches
- B. The Spanning Tree Protocol is activated in the Switches
- C. One NIC is broadcasting erroneous traffic
- D. An attacker is running a XMAS scan against the network

Correct Answer: D

Section:

QUESTION 152

The Circuit-level gateway firewall technology functions at which of the following OSI layer?

- A. Transport layer
- B. Data-link layer
- C. Session layer
- D. Network layer

Correct Answer: C

Section:

QUESTION 153

Individuals in the organization using system resources in a way that violates acceptable usage policies indicates which of the following security incident(s):

- A. Unauthorized Access
- B. Improper Usage
- C. Denial-of-Service (DoS)
- D. Malicious Code



Correct Answer: B

Section:

QUESTION 154

The GMT enterprise is working on their internet and web usage policies. GMT would like to control internet bandwidth consumption by employees. Which group of policies would this belong to?

- A. Enterprise Information Security Policy
- B. Network Services Specific Security Policy
- C. Issue Specific Security Policy
- D. System Specific Security Policy

Correct Answer: C

Section:

QUESTION 155

Which of the following intrusion detection techniques observes the network for abnormal usage patterns by determining the performance parameters for regular activities and monitoring for actions beyond the normal parameters?

- A. Statistical anomaly detection

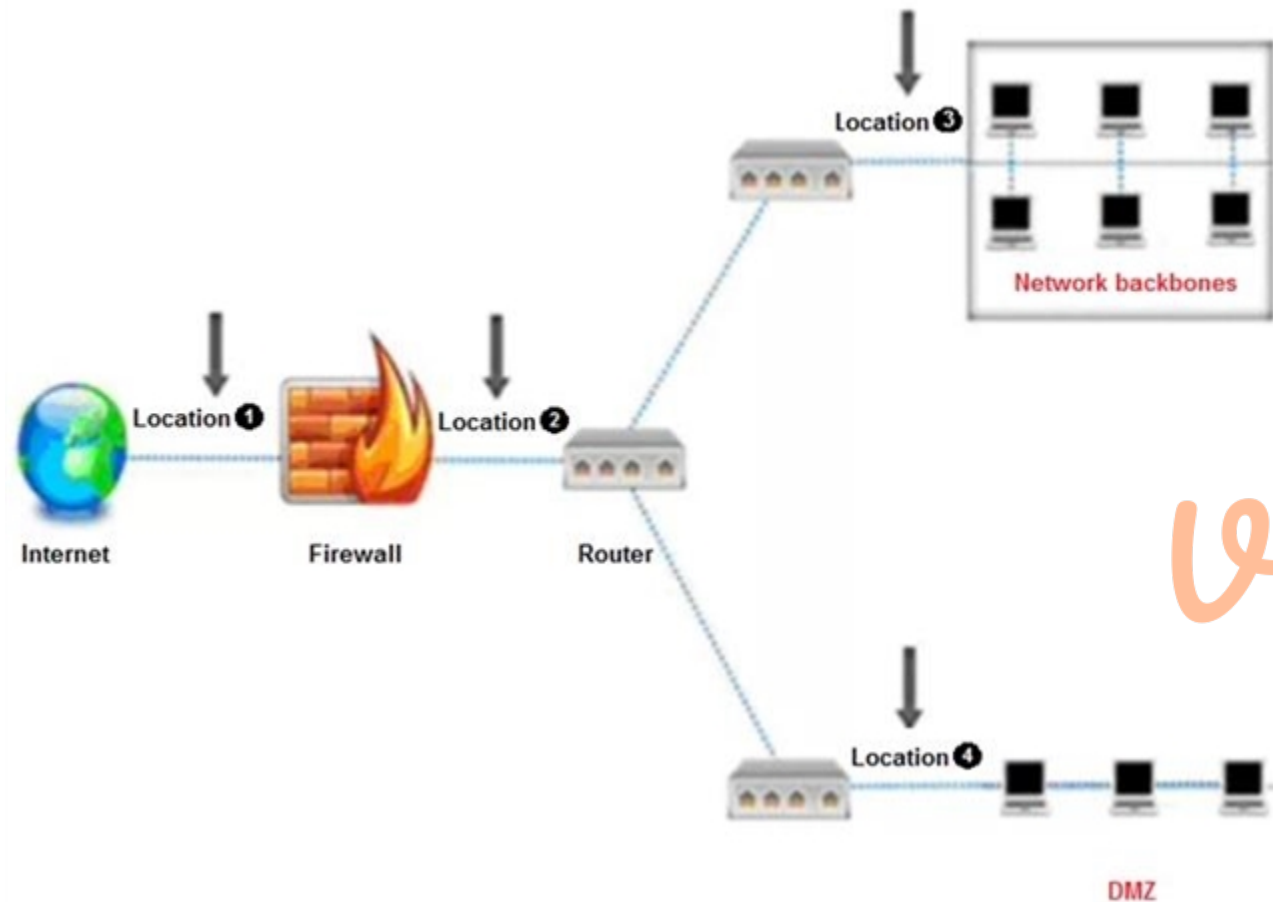
- B. Signature/Pattern matching
- C. None of these
- D. Stateful protocol analysis

Correct Answer: A

Section:

QUESTION 156

An administrator wants to monitor and inspect large amounts of traffic and detect unauthorized attempts from inside the organization, with the help of an IDS. They are not able to recognize the exact location to deploy the IDS sensor. Can you help him spot the location where the IDS sensor should be placed?



- A. Location 1
- B. Location 2
- C. Location 3
- D. Location 4

Correct Answer: A

Section:

QUESTION 157

Steven's company has recently grown from 5 employees to over 50. Every workstation has a public IP address and navigated to the Internet with little to no protection. Steven wants to use a firewall. He also wants IP addresses to be private addresses, to prevent public Internet devices direct access to them. What should Steven implement on the firewall to ensure this happens?

- A. Steven should use Open Shortest Path First (OSPF).
- B. Steven should enable Network Address Translation (NAT).

- C. Steven should use a Demilitarized Zone (DMZ).
- D. Steven should use IPsec.

Correct Answer: C

Section:

QUESTION 158

Assume that you are a network administrator and the company has asked you to draft an Acceptable Use Policy (AUP) for employees. Under which category of an information security policy does AUP fall into?

- A. Incident Response Policy (IRP)
- B. Issue Specific Security Policy (ISSP)
- C. Enterprise Information Security Policy (EISP)
- D. System Specific Security Policy (SSSP)

Correct Answer: D

Section:

QUESTION 159

During the recovery process, RTO and RPO should be the main parameters of your disaster recovery plan. What does RPO refer to?

- A. The encryption feature, acting as add-on security to the data
- B. The hot plugging technique used to replace computer components
- C. The duration required to restore the data
- D. The interval after which the data quality is lost

Correct Answer: C

Section:

QUESTION 160

Ryan works as a network security engineer at an organization the recently suffered an attack. As a countermeasure, Ryan would like to obtain more information about the attacker and chooses to deploy a honeypot into the organizations production environment called Kojoney. Using this honeypot, he would like to emulate the network vulnerability that was attacked previously. Which type of honeypot is he trying to implement?

- A. High interaction honeypots
- B. Research honeypot
- C. Low interaction honeypots
- D. Pure honeypots

Correct Answer: C

Section:

QUESTION 161

Which of the following is an open source implementation of the syslog protocol for Unix?

- A. syslog-os
- B. syslog Unix
- C. syslog-ng
- D. Unix-syslog



Correct Answer: C

Section:

QUESTION 162

Which of the following systems is formed by a group of honeypots?

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

Correct Answer: C

Section:

QUESTION 163

Which of the following protocols is a more secure version of the Point-to-Point Tunneling Protocol (PPTP) and provides tunneling, address assignment, and authentication?

- A. IP
- B. L2TP
- C. PPP
- D. DHCP

Correct Answer: B

Section:

QUESTION 164

Which of the following sets of incident response practices is recommended by the CERT/CC?

- A. Prepare, notify, and follow up
- B. Notify, handle, and follow up
- C. Prepare, handle, and notify
- D. Prepare, handle, and follow up

Correct Answer: D

Section:

QUESTION 165

Which of the following tools scans the network systems for well-known and often exploited vulnerabilities?

- A. Nessus
- B. SAINT
- C. SATAN
- D. HPing

Correct Answer: C

Section:



QUESTION 166

Which of the following tools examines a system for a number of known weaknesses and alerts the administrator?

- A. Nessus
- B. COPS
- C. SATAN
- D. SAINT

Correct Answer: B

Section:

QUESTION 167

Which of the following is the full form of SAINT?

- A. System Automated Integrated Network Tool
- B. Security Admin Integrated Network Tool
- C. System Admin Integrated Network Tool
- D. System Administrators Integrated Network Tool

Correct Answer: D

Section:

QUESTION 168

Which of the following is a type of VPN that involves a single VPN gateway?

- A. Remote-access VPN
- B. Extranet-based VPN
- C. PPTP VPN
- D. Intranet-based VPN

Correct Answer: B

Section:

QUESTION 169

Which of the following is a free security-auditing tool for Linux?

- A. SAINT
- B. SATAN
- C. Nessus
- D. HPing

Correct Answer: C

Section:

QUESTION 170

Which of the following types of RAID is also known as disk striping?



- A. RAID 0
- B. RAID 2
- C. RAID 1
- D. RAID 3

Correct Answer: A

Section:

QUESTION 171

Which of the following is a process of transformation where the old system can no longer be maintained?

- A. Disaster
- B. Risk
- C. Threat
- D. Crisis

Correct Answer: D

Section:

QUESTION 172

Which of the following phases is the first step towards creating a business continuity plan?

- A. Business Impact Assessment
- B. Scope and Plan Initiation
- C. Business Continuity Plan Development
- D. Plan Approval and Implementation

Correct Answer: B

Section:

QUESTION 173

James is a network administrator working at a student loan company in Minnesota. This company processes over 20,000 student loans a year from colleges all over the state. Most communication between the company, schools, and lenders is carried out through emails. Much of the email communication used at his company contains sensitive information such as social security numbers. For this reason, James wants to utilize email encryption. Since a server-based PKI is not an option for him, he is looking for a low/no cost solution to encrypt emails. What should James use?

- A. James should utilize the free OTP software package.
- B. James can enforce mandatory HTTPS in the email clients to encrypt emails.
- C. James could use PGP as a free option for encrypting the company's emails.
- D. James can use MD5 algorithm to encrypt all the emails.

Correct Answer: C

Section:

QUESTION 174

David is working in a mid-sized IT company. Management asks him to suggest a framework that can be used effectively to align the IT goals to the business goals of the company. David suggests the _____ framework, as it provides a set of controls over IT and consolidates them to form a framework.



- A. COBIT
- B. ITIL
- C. ISO 27007
- D. RMIS

Correct Answer: A

Section:

QUESTION 175

Identify the password cracking attempt involving precomputed hash values stored as plaintext and used to crack the password.

- A. Bruteforce
- B. Rainbow table
- C. Hybrid
- D. Dictionary

Correct Answer: B

Section:

QUESTION 176

John, the network administrator and he wants to enable the NetFlow feature in Cisco routers to collect and monitor the IP network traffic passing through the router. Which command will John use to enable NetFlow on an interface?

- A. Router IP route
- B. Router(Config-if) # IP route cache flow
- C. Router# Netmon enable
- D. Router# netflow enable

Correct Answer: B

Section:

QUESTION 177

Which of the following types of information can be obtained through network sniffing? (Choose all that apply.)

- A. DNS traffic
- B. Telnet passwords
- C. Programming errors
- D. Syslog traffic

Correct Answer: A, C, D

Section:

QUESTION 178

The network administrator wants to strengthen physical security in the organization. Specifically, to implement a solution stopping people from entering certain restricted zones without proper credentials. Which of following physical security measures should the administrator use?

- A. Mantrap



- B. Bollards
- C. Video surveillance
- D. Fence

Correct Answer: A

Section:

QUESTION 179

Which of the following incident handling stage removes the root cause of the incident?

- A. Eradication
- B. Recovery
- C. Detection
- D. Containment

Correct Answer: A

Section:

QUESTION 180

Justine has been tasked by her supervisor to ensure that the company's physical security is on the same level as their logical security measures. She installs video cameras at all entrances and exits and installs badge access points for all doors. The last item she wants to install is a method to prevent unauthorized people piggybacking employees. What should she install to prevent piggybacking?

- A. Justine needs to install a biometrics station at each entrance.
- B. She should install a mantrap.
- C. She should install a Thompson Trapdoor.
- D. Justine will need to install a revolving security door.



Correct Answer: B

Section:

QUESTION 181

An attacker has access to password hashes of a windows 7 computer. Which of the following attacks can the attacker use to reveal the passwords?

- A. XSS
- B. Rainbow table
- C. Brute force
- D. Dictionary attacks

Correct Answer: B

Section:

QUESTION 182

Which NIST Incident category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service or any combination for later exploit?

- A. Malicious code
- B. Scans/ Probes/ Attempted Access
- C. Denial-of-Service

D. Improper usage

Correct Answer: B

Section:

QUESTION 183

If a network is at risk resulting from misconfiguration performed by unskilled and/or unqualified individuals, what type of threat is this?

- A. External Threats
- B. Unstructured Threats
- C. Structured Threats
- D. Internal Threats

Correct Answer: B

Section:

QUESTION 184

John is a network administrator and is monitoring his network traffic with the help of Wireshark. He suspects that someone from outside is making a TCP OS fingerprinting attempt on his organization's network. Which of following Wireshark filter(s) will he use to locate the TCP OS fingerprinting attempt? (Choose all that apply.)

- A. tcp.flags=0x00
- B. tcp.options.wscale_val==20
- C. tcp.flags==0x2b
- D. tcp.options.mss_val<1460

Correct Answer: A, C, D

Section:

QUESTION 185

Michael decides to view the _____ to track employee actions on the organization's network.

- A. Firewall policy
- B. Firewall settings
- C. Firewall log
- D. Firewall rule set

Correct Answer: C

Section:

QUESTION 186

Which of the following acts as a verifier for the certificate authority?

- A. Registration authority
- B. Certificate authority
- C. Directory management system
- D. Certificate Management system



Correct Answer: A

Section:

QUESTION 187

What is the best way to describe a mesh network topology?

- A. A network in which every computer in the network has a connection to each and every computer in the network.
- B. A network in which every computer meshes together to form a hybrid between a star and bus topology.
- C. A network in which every computer in the network can communicate with a single central computer.
- D. A network that is extremely cost efficient, offering the best option for allowing computers to communicate amongst each other.

Correct Answer: A

Section:

QUESTION 188

You are tasked to perform black hat vulnerability assessment for a client. You received official written permission to work with: company site, forum, Linux server with LAMP, where this site hosted. Which vulnerability assessment tool should you consider to use?

- A. dnsbrute
- B. hping
- C. OpenVAS
- D. wireshark

Correct Answer: C

Section:

QUESTION 189

Which phase of vulnerability management deals with the actions taken for correcting the discovered vulnerability?

- A. Verification
- B. Mitigation
- C. Remediation
- D. Assessment

Correct Answer: C

Section:

QUESTION 190

Nancy is working as a network administrator for a small company. Management wants to implement a RAID storage for their organization. They want to use the appropriate RAID level for their backup plan that will satisfy the following requirements:

- 1- It has a parity check to store all the information about the data in multiple drives
- 2- Help reconstruct the data during downtime.
- 3- Process the data at a good speed.
- 4- Should not be expensive.

The management team asks Nancy to research and suggest the appropriate RAID level that best suits their requirements. What RAID level will she suggest?

- A. RAID 3.



- B. RAID 1
- C. RAID 0
- D. RAID 10

Correct Answer: A

Section:

QUESTION 191

A network designer needs to submit a proposal for a company, which has just published a web portal for its clients on the internet. Such a server needs to be isolated from the internal network, placing itself in a DMZ. Faced with this need, the designer will present a proposal for a firewall with three interfaces, one for the internet network, another for the DMZ server farm and another for the internal network. What kind of topology will the designer propose?

- A. Screened subnet
- B. Multi-homed firewall
- C. Bastion host
- D. DMZ, External-Internal firewall

Correct Answer: B

Section:

QUESTION 192

The bank where you work has 600 windows computers and 400 Red Hat computers which primarily serve as bank teller consoles. You have created a plan and deployed all the patches to the Windows computers and you are now working on updating the Red Hat computers. What command should you run on the network to update the Red Hat computers, download the security package, force the package installation, and update all currently installed packages?

- A. You should run the up2data -u command.
- B. You should run the up2date --d -f -u command.
- C. You should run the WSUS --d -f -u command.
- D. You should type the sysupdate --d command.

Correct Answer: B

Section:

QUESTION 193

Dan and Alex are business partners working together. Their Business-Partner Policy states that they should encrypt their emails before sending to each other. How will they ensure the authenticity of their emails?

- A. Dan will use his digital signature to sign his mails while Alex will use Dan's public key to verify the authenticity of the mails.
- B. Dan will use his digital signature to sign his mails while Alex will use his private key to verify the authenticity of the mails.
- C. Dan will use his private key to encrypt his mails while Alex will use his digital signature to verify the authenticity of the mails.
- D. Dan will use his public key to encrypt his mails while Alex will use Dan's digital signature to verify the authenticity of the mails.

Correct Answer: A

Section:

QUESTION 194

A VPN Concentrator acts as a bidirectional tunnel endpoint among host machines. What are the other function(s) of the device? (Choose all that apply.)

- A. Enables input/output (I/O) operations
- B. Provides access memory, achieving high efficiency
- C. Manages security keys
- D. Assigns user addresses

Correct Answer: C, D

Section:

QUESTION 195

Which characteristic of an antenna refers to how directional an antennas radiation pattern is?

- A. Radiation pattern
- B. Polarization
- C. Directivity
- D. Typical gain

Correct Answer: A

Section:

