CISSP Exam Questions

Exam Guide

Real Exam Questions

1500+ CISSP practice questions and solutions to help you pass the exam on your first try with minimum effort.

Pass First Time

Eddie Vi VCP, VCI

CISSP Exam Secrets

By
Eddie Vi

SMASHWORDS EDITION

PUBLISHED BY:
E Vii on Smashwords

Contents

Introduction

The book is designed to help you pass your CISSP exam on your first attempt with over 1500 multiple choice questions.

We focus on the objectives you need to know, so you will know what to expect on the actual exam.

The exam questions closely mimic those on the actual exam, so there won't be any surprises when you get to the testing centre. You will be able to chart your progress with multiple, full-length exams that simulate exam required to attain you qualification.

CISSP is a security certification carried out by (ISC)², which is a globally recognized, vendor neutral organization for certifying information security professionals. To pass the CISSP exam you'll have to be competent in 10 Domains of the Common Body of Knowledge (CBK):

- Access Control
- Application Security
- Business Continuity and Disaster Recovery Planning
- Cryptography
- Information Security and Risk Management
- Legal, Regulations, Compliance and Investigations
- Operations Security
- Physical (Environmental) Security

- Security Architecture and Design
- Telecommunications and Network Security

To qualify to sit for the exams you need to:

Subscribe to the (ISC)² Code of Ethics.

Have a minimum of four years of direct full-time security professional work experience in one or more of the ten domains of the (ISC)² CISSP® CBK® or three years of direct full-time security professional work experience in one or more of the ten domains of the CISSP® CBK® with a college degree. Additionally, a Master's Degree in Information Security from a National Center of Excellence can substitute for one year toward the four-year requirement.

The exam itself is 6 hours long, with 250 questions based on the 10 domains. 25 out of 250 questions are for research, but you'll have to answer all of them, and there's no way of knowing which one is which. So, 225 questions will be scored, and you'll have to get 700 out of a possible 1000 points on the grading scale to pass. Different questions carry different weight (marks) and there's no way to know which question carries how much marks. As of writing this, the exam costs US$ 499 if you register 16 days ahead of exam date or US$ 599 if you register later.

A - Telecommunications and Network Security (272) / 1569

Question 1

Which of the following is not one of the stages of the DHCP lease process? i. Discover ii. Offer iii. Request iv. Acknowledgment

A. All of them
B. None of them
C. i
D. ii

Answer: B

Summary

The four-step DHCP lease process is:
- DHCPDISCOVER message: This message is used to request an IP address lease from a DHCP server.
- DHCPOFFER message: This message is a response to a DHCPDISCOVER message, and is sent by one or numerous DHCP servers.
- DHCPREQUEST message: The client sends the initial DHCP server which responded to its request a DHCP Request message.

- DHCPACK message: The DHCP Acknowledge message is sent by the DHCP server to the DHCP client and is the process whereby which the DHCP server assigns the IP address lease to the DHCP client.

Question 2

The World Wide Web is a _______ network that is an overlay on top of the Internet.

A. Virtual
B. Private
C. Trusted
D. Analog

Answer: A

Summary

The World Wide Web and the Internet are two terms commonly interchanged as the same thing by the average computer user. They are not the same thing, however. The Web exists on top of the Internet and is a series of pages connected to one another by hyperlinks.

Question 3

Switches marry the technologies of _____ and ______.

A. Hubs and bridges
B. Bridges and routers
C. Network adapters and hubs
D. Bridges and network adapters

Answer: A

Summary

Switches combine the technologies of hubs and bridges. They act as hubs by enhancing performance and act as bridges by distributing traffic to different networks.

Question 4

A switch is a multi-functional networking device that can operate within several OSI layers. Which layer can a switch not function in?

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

Answer: A

Summary

Switches do not operate in the Physical layer, OSI Layer 1. They make packet forwarding decisions (Layer 2), and specific switches exist that make decisions based upon Layer 3 and Layer 4 data information.

Question 5

Which of the following media types is the most easily tapped?

A. Twisted pair
B. Baseband coaxial
C. Broadband coaxial
D. Fiber

Answer: A

Summary

Twisted-pair cabling is very common and inexpensive but can be easily tapped. It is commonly used in small office buildings due to its distance limitations.

Question 6

Which of the following is most resistant to the environment?

A. Infrared
B. Free space optics
C. Satellite
D. Fiber optics

Answer: D

Summary

Fiber optics would be most protected from environmental threats. Infrared signals can be impacted by heavy rain, free space optics can be affected by fog, and satellite transmissions are affected by weather disruptions, such as cloud cover, rain, and snow.

Question 7

Dispersion is a condition that affects which cabling type?

A. Twisted pair
B. Broadband coaxial
C. Directional antennae
D. Fiber optics

Answer: D

Summary

Dispersion is the spreading out of light pulses, which overlap the preceding or upcoming pulses. This is most prevalent in fiber optic cabling.

Question 8

Electromagnetic interference (EMI) would have no impact on which of the following?

A. Fiber optics
B. Category 5 twisted pair
C. Broadband
D. Category 3 twisted pair

Answer: A

Summary

Fiber optics have a sturdy glass or plastic casing that makes them immune to EMI. EMI can result in transmission faults, especially if the cabling is under heavy loads. Although the other choices all have different degrees of EMI vulnerability, fiber optics would be the most resistant to this type of threat.

Question 9

A circuit-switched connection is a physical, _______ connection.

A. Permanent
B. Virtual
C. Temporary
D. Shared

Answer: A

Summary

Circuit switching establishes physical, permanent connections from the time a call begins to the time it ends. The connection is not shared; it is a private end-to-end connection that is built when a call goes up and torn down when the call ends.

Question 10

What type of media access method do Ethernet LANs use?

A. Polling
B. Token passing

C. Token sharing
D. CSMA-CD

Answer: D

Summary

Ethernet LANs use Carrier Sense Multiple Access with Collision Detection (CSMA-CD). In this methodology, each device signals its intent to transmit so that other devices will not block the transmission accidentally.

Question 11

The wireless standard 802.11 has matured over the past few years, but only two provisions have been widely adopted. Which two are commonly accepted?

A. b, g
B. a, b
C. a, g
D. c, d

Answer: A

Summary

802.11b enforces a 11 Mbps data rate, 2.4 GHz frequency bands, and Direct Sequence Spread Spectrum (DSSS). 802.11g was ratified in 2003 to offer backward compatibility with 802.11b in the same network. It enforces 54 Mbps data rate, 2.4 GHz frequency band, and OFDM.

Question 12

X.25 works at the ________ and ________ layers.

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

Answer: B

Summary

X.25 is a packet-switching technology that is used by telecommunications services for data-only traffic. It is a subscriber-based service that operates within the Network and Data Link layers.

Question 13

Frame relay is a simplified version of __________.

A. DSL
B. X.25
C. ISDN
D. SDLC

Answer: B

Summary

Frame relay is very similar to X.25, but it has removed the error checking that was done on the network. Frame relay handles this task at the end node, which helps to improve speed dramatically.

Question 14

Isochronous processes rely on ________.

A. Time constraints
B. Content variables
C. Error checking
D. Malformed packets

Answer: A

Summary

Isochronous processes must deliver data within set time constraints. Applications are typically video related where audio and video must match perfectly. VoIP is another example.

Question 15

Which of the following tunneling protocols is not well suited for dial-up?

A. IPSec
B. PPTP
C. PPP
D. L2TP

Answer: A

Summary

IPSec is a tunneling protocol used in LAN-to-LAN VPN solutions where it can handle multiple connections at the same time. PPTP, PPP, and L2TP are popular protocols used primarily in dial-up environments.

Question 16

A virtual private network is a tunnelling protocol plus __________.

A. Encryption
B. Digital signature
C. DSL connection
D. Bus topology

Answer: A

Summary

A tunnelling protocol alone does not make a VPN. This is a common misunderstanding. A VPN must include both a tunnelling protocol and encryption.

Question 17

Which of the following security association techniques uses multiple layers of protocols through IP tunnelling?

A. Iterated
B. Transport adjacency
C. Encapsulation
D. Replay

Answer: A

Summary

In an iterated association each tunnel can originate or terminate at a different IPSec site along the way. This method supports multiple layers of nesting.

Question 18

An effective method to shield networks from unauthenticated DHCP clients is through the use of ________________ on network switches.

A. DHCP snooping
B. ARP protection
C. DHCP shielding
D. ARP caching

Answer: A

Summary

DHCP snooping ensures that DHCP servers can assign IP addresses to only selected systems, identified by their MAC addresses. Also, advance network switches now have capability to direct clients toward legitimate DHCP servers to get IP addresses and restrict rouge systems from becoming DHCP servers on the network.

Question 19

MPLS offers the following benefits, except:

A. Performance characteristics can be set.
B. VPNs can be created in combination with end user applications.
C. Layer 2 services can be overlaid.
D. Multiple layers can be eliminated.

Answer: B

Summary

Multiprotocol label switching (MPLS) gives service providers the ability to create VPNs without the need of end user applications.

Question 20

IPSec uses ______ for key management.

A. IKE
B. MPLS
C. PPP
D. NAT

Answer: A

Summary

Internet key exchange (IKE) is used within IPSec to negotiate and authenticate keys.

Question 21

IP version ___ includes 128-bit addressing and includes quality of service capabilities.

A. 4
B. 5
C. 6
D. 3

Answer: C

Summary

IP version 6 is only in limited use currently but is expected to be the next big thing. It improves addressing size, quality of service, address authentication, and message confidentiality and integrity.

Question 22

An attack that sends out an overload of UDP packets from a spoofed source so that an overload of ICMP unreachable replies flood the victim is called a ______.

A. Fraggle
B. Worm
C. Logic bomb
D. Remedy

Answer: A

Summary

A fraggle attack is similar to a smurf attack. The attacker broadcasts UDP packets that are spoofed with the victim's address as the source. The victim is then unpleasantly surprised to receive a flood of ICMP "unreachable" responses.

Question 23

Which attack inserts an irrational value into an oversized packet making it difficult for the destination router to re-assemble it?

A. Remedy
B. Ping of Death
C. Garble
D. Teardrop

Answer: D

Summary

Oversized packets must be disassembled by a router and then re-assembled at their destination. Teardrop attacks insert a confusing value in the packet that makes it virtually impossible for the final routing device to re-assemble it.

Question 24

ICMP is a low-level Internet operation message protocol that is used between gateways and hosts. It uses several message codes. What would a code 3 mean?

A. Communication administratively prohibited
B. IP header was bad
C. TTL expired
D. Host unknown, network unreachable

Answer: D

Summary

A listing of ICMP messages includes: 0 Echo reply (ping reply) 3 Delivery failure (host unknown, network unreachable) 4 Source quench 8 Echo request (ping request) 11 Time to live (TTL) expired (used by traceroute) 12 IP header was bad 13 Communication administratively prohibited

Question 25

IGMP is based upon the _________ model in how it shares information with multicast routers.

A. Publish and subscribe
B. Unicast only
C. Send and receive
D. Bell-La Padula

Answer: A

Summary

Internet Group Management Protocol (IGMP) is a method of allowing multicast transmissions to take place in LAN environments. It is a combination of one-to-many and many-to-many delivery methods. IGMP takes on the characteristics of the "publish and subscribe" model only in terms of how it handles IP subscriptions with multicast routers.

Question 26

Name servers and resolvers are the two primary components of ______.

A. DNS
B. ICMP
C. IGMP
D. PGP

Answer: A

Summary

Domain Name Server (DNS) is a global network of name servers that translate hostnames into numerical IP addresses. The two main components of DNS are the name server and the resolver. The name server holds data and responds to users with requested information. The resolver will initiate requests with other name servers when the original cannot provide the answer.

Question 27

Which of the following is the most common attack on DNS servers?

A. Poisoning
B. Flood
C. Ping
D. Masquerading

Answer: A

Summary

When an attacker corrupts a DNS server by changing the host-to-IP relationship information, the table is said to be poisoned. It is a common attack on DNS.

Question 28

ARP tables are built ___________.

A. Manually
B. Dynamically
C. Dynamically or manually
D. Unconventionally

Answer: C

Summary

Address Resolution Protocol (ARP) tables are built either dynamically or manually. Keep in mind that static ARP entries can be built, however, this can be difficult to manage. With dynamic entries, if an address is not found, the node will automatically broadcast a message to all nodes asking for the correct address. This dynamic process keeps ARP tables updated and accurate.

Question 29

Which is not true of hierarchical routing?

A. The region of a node that shares characteristics and behaviours is called an AS.
B. Each AS uses IGP to perform routing functionality.
C. EGP is used in the areas "between" each AS.
D. CAs are specific nodes that are responsible for routing to nodes outside of their region.

Answer: D

Summary

Gateways are designated nodes that are responsible for routing to nodes outside of their region. Autonomous systems (AS) are regions of nodes that share common attributes. Interior Gateway Protocol (IGP) handles routing tasks within each AS, while Exterior Gateway Protocol (EGP) functions "between" each AS.

Question 30

Which protocol was built to scale well in large networks, support hierarchies, and support the simultaneous use of multiple paths?

A. RIP v1
B. OSPF
C. RIP v2
D. EGP

Answer: B

Summary

Because RIP could not scale well in large networks, Open Shortest Path First Protocol (OSPF) was created. It supports hierarchies and the simultaneous use of multiple paths.

Question 31

Remote access represents the best opportunity for a hacker to steal confidential information. Of the following vulnerabilities, which is not inherent with remote access?

A. Software on laptops can be easily exploited.
B. Internet connections are not secure.
C. Sessions are not authenticated.
D. Diagnostic ports on networking devices can be targeted.

Answer: A

Summary

Laptop software is not a specific target of remote access attacks. Software on laptops may or may not contain vulnerabilities, but the real open doors for hackers depend upon the network used to connect and the devices set up to allow remote access.

Question 32

Instant messaging technology is extremely popular in the corporate world, but it brings with it a host of security problems. What is not true of IM?

A. Integrated directories are target lists.
B. Attackers use scripts against IM.

C. Most IM have encryption functionality but few users enable it.
D. Firewalls can be easily bypassed.

Answer: C

Summary

Instant messaging applications rarely have encryption capabilities built in. Scripts can be used against the program. Most can be easily provisioned to bypass firewall controls. Buddy lists serve as instant target lists for attackers.

Question 33

Jake is an IT administrator who is concerned about the vulnerabilities that exist with instant messaging around his office. He knows that it is very popular throughout the company, especially with upper management, so he must tread lightly when tightening security. Which of the following actions should Jake avoid?

A. Install firewalls on desktops
B. Verify central firewall is blocking unapproved messaging
C. Propose a IM security policy
D. Restrict all confidential data from being sent over IM

Answer: D

Summary

Although restricting confidential data from being sent over IM is a good idea from a security standpoint, it might not be the best decision from a career standpoint. Because upper management utilizes IM and it is likely that they deal with confidential information regularly, this action might be too aggressive.

Question 34

Which of the following is not a denial-of-service attack?

A. Teardrop
B. Dictionary
C. Smurf
D. TCP Syn

Answer: B

Summary

Dictionary attacks are password-related attacks that can be categorized as brute-force attacks as well. The other types are all geared to bring down a service or attack a network's availability.

Question 35

Central authenticating systems should perform three primary services. Which service is not one of them?

A. Accountability
B. Authentication
C. Authorization
D. Confidentiality

Answer: D

Summary

The basic services performed by a central authenticating system are: authentication (who the user is), authorization (what the user can do), and accountability (what the user has done).

Question 36

Which of the following is an industry standard for providing repositories for security-related data, such as cryptographic keys, passwords, or user IDs?

A. LDAP
B. CHAP
C. PKI
D. SNMP

Answer: A

Summary

Lightweight Directory Access Protocol (LDAP) is an industry standard for securing and storing directory information. It is compatible with virtually any platform/vendor and is perfect for storing security-related items.

Question 37

All of the following are true of NIS+ except:

A. Does not support MD5 password encryption
B. Uses SecureRPC
C. Hierarchical in nature
D. Supports object access restrictions

Answer: A

Summary

Network Information Systems (NIS) is a distributed database system that lets computers share sets of files. NIS+ offers additional functionality expanding upon regular NIS. It does support MD5 password encryption.

Question 38

____________ is a directory service designed to eliminate the need for duplication across many computers of configuration data such as user accounts, host names and addresses, printer information and NFS disk mounts on individual systems, instead using a central repository on a master server, simplifying system administration.

A. NIS
B. NIS+
C. Yellow Pages
D. DNS

Answer: B

Summary

NIS+ is a directory service developed by Sun Microsystems to replace its older NIS (Network Information Service). It is designed to eliminate the need for duplication across many computers of configuration data such as user accounts, host names and addresses, printer information and NFS disk mounts on individual systems, instead using a central repository on a master server, simplifying system administration. NIS+ client software has been ported to other Unix and Unix-like platforms, notably Linux.

Question 39

DCE is an authentication system that mirrors Kerberos in many ways. Who developed it?

A. Open Group
B. Ron Rivest
C. NSA
D. Microsoft

Answer: A

Summary

Open Group developed the distributed computing environment (DCE) standard that is very similar to Kerberos. It is a framework that never caught on in the industry even though it specified its own authorization techniques, which were lacking in Kerberos.

Question 40

The network perimeter concept restricts access from segment to segment via ________.

A. Choke points
B. Encryption
C. Vendor segregation
D. Trust models

Answer: A

Summary

The network perimeter concept recognizes the need to separate sensitive networks from non-sensitive networks and accomplishes this by using choke points to block segment-to-segment access.

Question 41

Which is untrue of a packet filtering firewall?

A. High security
B. Application independence
C. Performance strength
D. Excellent scalability

Answer: A

Summary

Packet filtering firewalls offer low levels of security, one reason is their inability to screen by protocol. However, they are application-independent, highly scalable, and perform at a high level.

Question 42

Which is not a primary goal of QoS?

A. Content-based filtering is achieved.
B. Jitter and latency are managed.
C. Dedicated bandwidth is maintained.
D. Different traffic types can co-exist (voice, video, data).

Answer: A

Summary

Quality of service is a business commitment to customers to provide and guarantee levels of service by utilizing existing technologies. The main goals of

QoS are maintaining dedicated bandwidth, controlling jitter and latency, and making sure different traffic types can co-exist.

Question 43

Which OSI layer handles flow control?

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

Answer: A

Summary

Flow control is the process of managing data transmission between devices so that the receiving device does not get overwhelmed with traffic. The Transport layer handles this process.

Question 44

Many applications are able to transmit over one physical medium at the same time by the use of ________.

A. Multiplexing
B. Routing
C. Forwarding
D. Asynchronous protocols

Answer: A

Summary

Multiplexing technologies allow many transmissions to fit on a single medium. A multiplexer is the device that enables this type of activity.

Question 45

A node that sends and receives at the same time can perform what type of transmission?

A. Full-duplex
B. Half-duplex
C. Unicast
D. Multi-duplex

Answer: A

Summary

Full-duplex transmissions allow end users to send and receive data at the same time without interruptions or collisions.

Question 46

In TCP, what does a sequence number do?

A. Guarantees message delivery
B. Disassembles and re-assembles packets
C. Functions as a fault code indicator
D. Is used in multiplexing

Answer: A

Summary

Sequence numbers are populated within packets as a way of ensuring that the message is delivered to the appropriate destination and is from the appropriate sender.

Question 47

An ARP cache would provide what type of information?

A. IP and MAC addressing
B. User activity data
C. Firewall specs
D. IT administrator disclaimers

Answer: A

Summary

An ARP cache will show the mapping information of an IP address to a MAC address.

Question 48

Session Initiation Protocol consists of two major components: the _____________ and __________________.

A. User Agent Client, User Agent Server
B. User Agent Client, User Agent Service
C. User Client, User Service
D. User Urgent Client, User Urgent Server

Answer: A

Summary

SIP consists of two major components: the User Agent Client (UAC) and User Agent Server (UAS). The UAC is the application that creates the SIP requests for initiating a communication session. UACs are generally messaging tools and soft-phone applications that are used to place VoIP calls. The UAS is the SIP server, which is responsible for handling all routing and signalling involved in VoIP calls.

Question 49

An autonomous network is controlled by how many entities?

A. One
B. Two
C. Three
D. More than 10

Answer: A

Summary

Autonomous networks are built hierarchically where one governing entity manages traffic flow.

Question 50

The ______________ is an IETF-defined signalling protocol, widely used for controlling multimedia communication sessions such as voice and video calls over Internet Protocol (IP).

A. Session Initiation Protocol
B. Real-time Transport Protocol
C. SS7
D. VoIP

Answer: A

Summary

The Session Initiation Protocol (SIP) is an IETF-defined signalling protocol, widely used for controlling multimedia communication sessions such as voice and video calls over Internet Protocol (IP). The protocol can be used for creating, modifying and terminating two-party (unicast) or multiparty (multicast) sessions consisting of one or several media streams.

Question 51

Which of the following is not considered a passive attack?

A. Spoofing
B. Network sniffing
C. Wiretapping
D. Traffic analysis

Answer: A

Summary

A passive attack means that an attacker is not actually doing something, but is monitoring a connection. Passive attacks can be carried out through sniffing, traffic analysis, or wiretapping. An active attack means the attacker is carrying out some type of activity. Active attacks can be DoS, brute force, or dictionary attacks.

Question 52

What does the term "phreaking" pertain to?

A. Spamming mail servers in the hopes of bringing them down
B. Foot printing and port scanning networks
C. Fraudulent use of telephone services
D. Compromising tunnelling protocols

Answer: C

Summary

A phreaker is a type of hacker that specializes in telephone fraud. This can be carried out by reconfiguring a telecommunication device, social engineering, or attacking a company?s PBX system.

Question 53

What does a packet sniffer do?

A. It performs port scans and footprinting.
B. It identifies cabling faults.
C. It detects hanging modems not protected by the firewall.
D. It captures traffic for data analysis.

Answer: D

Summary

A sniffer is a tool that captures frames from a network for viewing purposes. Most sniffers put the system?s NIC into promiscuous mode so that all traffic can be monitored.

Question 54

What can be used to compromise and defeat callback security?

A. Passive wiretapping
B. Call forwarding
C. Packet spoofing
D. Brute force attack

Answer: B

Summary

A remote access server can be configured to drop a remote user?s connection and call him back at a predefined number. If call forwarding is enabled, this security measure can be compromised.

Question 55

Which is not considered a firewall architecture used to protect networks?

A. Screened host
B. Screened subnet
C. NAT gateway
D. Dual-homed host

Answer: C

Summary

The other answers describe basic firewall architectures, meaning where they can be placed within an environment. Network address translation (NAT) maps public to private addresses and does not provide traffic monitoring capabilities. Some firewalls provide NAT services, but the goals of the services are different.

Question 56

Packet-switching infrastructures are safer environments because ___________.

A. It is harder to sniff traffic since the computers have virtual private connections.
B. They are just as unsafe as non-switched environments.
C. The data link encryption does not permit wiretapping.
D. Switches are more intelligent than bridges and implement security mechanisms.

Answer: A

Summary

Switched environments use switches to allow different network segments and/or systems to communicate. When this communication takes place, a virtual connection is set up between the communicating devices. Since it is a dedicated connection, broadcast and collision data are not available to other systems, as in an environment that uses only bridges and routers.

Question 57

What functionality hangs up on a remote caller and looks at a table of predefined phone numbers?

A. Caller ID
B. RAS
C. Callback
D. NOS

Answer: C

Summary

The goal of a callback system is to provide another layer of authentication. For an attacker to successfully compromise this setup and obtain unauthorized access she would need to be at the predefined phone number or reconfigure the telephone company?s equipment to forward the call on to her.

Question 58

Which of the following protocols is considered connection oriented?

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

Answer: D

Summary

TCP is the only connection-oriented protocol listed. A connection-oriented protocol provides reliable connectivity and data transmission, while connectionless provides unreliable connections and does not promise or ensure data transmission.

Question 59

Which of the following best describes Ethernet transmissions over a LAN?

A. Traffic is sent to a gateway that sends it to the destination system.
B. Traffic is bursty in nature and broadcasts data to all hosts on the subnet.

C. Traffic streams and does not broadcast data.
D. Traffic is contained within collision domains but not broadcast domains.

Answer: B

Summary

Ethernet is a very chatty protocol because it allows all systems to hear each other?s broadcasts. The technology has many collisions because all systems have to share the same medium.

Question 60

Which of the following proxies cannot make access decisions on protocol commands?

A. Application
B. Packet filtering
C. Circuit
D. Stateful

Answer: C

Summary

Application and circuit are the only type of proxy-based firewall solutions listed here; the others do not use proxies. Circuit-level proxy firewalls make decisions based on header information and not the protocol?s command structure. Application-level proxies are the only ones that understand this level of granularity about the individual protocols.

Question 61

A security concern that is prevalent in distributed environments and systems is __________.

A. Knowing the proper proxy and default gateway
B. Knowing whom to trust
C. Knowing what authentication method is most appropriate
D. Knowing how to resolve hostnames

Answer: B

Summary

Distributed environments bring about a lot more complexity and drastically increase the difficulty of access control. Since you now have many different applications, devices, services, and users it is much more difficult to know which entities to trust and to what degree.

Question 62

Which protocol is commonly used to authenticate users on dial-up connections?

A. PPTP
B. IPSec
C. CHAP
D. L2F

Answer: C

Summary

The other protocols listed are used for tunnelling and/or VPN connectivity, not user authentication. CHAP uses the challenge-response method of authenticating a user.

Question 63

Which of the following shows the sequence of layers as Layers 2, 5, 7, 4, and 3?

A. Data Link, Session, Application, Transport, and Network
B. Data Link, Transport, Application, Session, and Network
C. Network, Session, Application, Network, and Transport
D. Network, Transport, Application, Session, and Presentation

Answer: A

Summary

The OSI model is made up of seven layers. Application (Layer 7), Presentation (Layer 6), Session (Layer 5), Transport (Layer 4), Network (Layer 3), Data Link (Layer 2), and Physical (Layer 1).

Question 64

What is another name for a VPN?

A. Transport session
B. Tunnel
C. End-to-end connection
D. Bandwidth

Answer: B

Summary

A VPN sets up a private and secure tunnel by encapsulating and encrypting data. This allows data to be safely transmitted over untrusted networks.

Question 65

When security is a high priority, why is fiber cabling used?

A. It has high data transfer rates and is less vulnerable to EMI.
B. It multiplexes data, which can confuse attackers.
C. It has a high degree of data detection and correction.
D. Data interception is next to impossible.

Answer: D

Summary

It is very difficult to tap into a fiber line, and fiber does not radiate signals as the other cable types do.

Question 66

Why are mainframes considered more secure than LAN environments?

A. They have fewer entry points.
B. They have stronger authentication mechanisms.
C. They have more auditing and encryption implemented.
D. They are actually weaker than LANs.

Answer: A

Summary

This is a relative and general statement. Mainframes are more closed systems and work in more closed environments when compared to the distributed environments we work in today. Mainframes usually have a smaller number of entry points, which are generally very controlled.

Question 67

What does it mean when computers communicate logically and physically with each other?

A. They speak physically through headers and trailers and logically through virtual connections.
B. They speak physically through PVCs and logically through SVCs.
C. They speak physically when connected to a backbone network and logically when they speak to each other within the same LAN.
D. They speak physically through electrons and network cables and logically through layers in the OSI model.

Answer: D

Summary

Systems, of course, communicate physically using network cables or airwaves. But they also communicate logically. An FTP protocol on one system speaks to the FTP protocol on another system and is not aware that many other protocols, devices, and cables are involved. Protocols, services, and applications communicate logically, and this communication is transmitted over physical means.

Question 68

How does data encapsulation work with the protocol stack?

A. Each layer in the OSI model multiplexes other packets to the data as it is passed down the protocol stack.
B. Each layer in the OSI model adds its own information to the data as it is passed down the protocol stack.
C. The packet is encapsulated and grows as it hops from router to router.
D. The packet is encapsulated and grows when it is passed up the protocol stack.

Answer: B

Summary

Data encapsulation means that a piece of data is put inside another type of data. This usually means that individual protocols apply their own instruction set in the form of headers and trailers. As a data package goes down the OSI, or protocol stack, of a system, each protocol that is involved adds its own instructions. This process is reversed at the destination.

Question 69

Systems that are built on the OSI framework are considered open systems. What does this mean?

A. They do not have authentication mechanisms configured by default.
B. They have interoperability issues.
C. They are built with international protocols and standards so they can easily communicate with other systems.
D. They are built with international protocols and standards so they can choose what types of systems they will communicate with.

Answer: C

Summary

An open system is a system that has been developed based on standardized protocols and interfaces. Following these standards allows the systems to interoperate more effectively with other systems that follow the same standards.

Question 70

VoIP's integration with the TCP/IP protocol suite has brought about immense security challenges because it allows malicious users to bring their TCP/IP experience into this relatively new platform, where they can probe for flaws in both the architecture and the VoIP systems. Which of the following is one of the most serious concerns when implementing VoIP?

A. Lack of authentication
B. Lack of authorization
C. Lack of identification
D. H.235 compromise

Answer: A

Summary

SIP-based signaling suffers from the lack of encrypted call channels and authentication of control signals. Attackers can tap into the SIP server and client communication to sniff out login IDs, passwords/PINs, and phone numbers.

Question 71

Which of the following protocols works in the following layers: Application, Data Link, Network, and Transport?

A. FTP, ARP, TCP, and UDP
B. FTP, ICMP, IP, and UDP
C. TFTP, ARP, IP, and UDP
D. TFTP, RARP, IP, and ICMP

Answer: C

Summary

Different protocols have different functionalities. The OSI model is an attempt to conceptually describe where these different functionalities take place in a networking stack. The model is basically trying to draw boxes around reality for people to better understand the stack. Each layer has specific functionality and several different protocols that can live at that layer and carry out that specific functionality.

Question 72

What is the purpose of the Presentation layer?

A. Addressing and routing
B. Data syntax and formatting

C. End-to-end connection
D. Framing

Answer: B

Summary

The Presentation layer does not have any protocols that work there, but has services that carry out data formatting, compression/decompression, and encryption/decryption processes. Putting data into a standardized format allows for a large subset of applications to be able to understand and interpret it.

Question 73

What is the purpose of the Data Link layer?

A. End-to-end connection
B. Dialog control
C. Framing
D. Data syntax

Answer: C

Summary

The Data Link layer, in most cases, is the only layer that understands the environment that the system is working it, whether it be Ethernet, Token Ring, wireless, or connecting to a WAN link. This layer adds the necessary headers and trailers to the data, which frames it. Other systems on the same network using the same technology only understand the specific header and trailer format used in its technology.

Question 74

What takes place at the Session layer?

A. Dialog control
B. Routing
C. Packet sequencing
D. Addressing

Answer: A

Summary

The Session layer is responsible for controlling how applications communicate, not how computers communicate. Not all applications use protocols that work at the Session layer, so this layer is not always used in networking functions. A Session layer protocol will set up the connection to the other application logically and control the dialog going back and forth. Session layer protocols allow applications to keep state of the dialog.

Question 75

What layer does a bridge work at?

A. Session
B. Network
C. Transport
D. Data Link

Answer: D

Summary

A bridge will only read header information in the Data Link layer and no higher because it makes forwarding and filtering decisions based on what is held within this header, which is the MAC address.

Question 76

Which best describes the IP protocol?

A. Connectionless protocol that deals with dialog establishment, maintenance, and destruction
B. Connectionless protocol that deals with addressing and routing of packets
C. Connection-oriented protocol that deals with addressing and routing of packets
D. Connection-oriented protocol that deals with sequencing, error detection, and flow control

Answer: B

Summary

The IP protocol is connectionless and works at the Network layer. It adds source and destination addresses to a packet as it goes through its data encapsulation process. IP can also make routing decisions based on the destination address.

Question 77

Which protocol is described as a "best effort" protocol?

A. TCP
B. SPX
C. UDP
D. ARP

Answer: C

Summary

UDP is commonly referred to as a "best effort" protocol, but this label describes any connectionless protocol, not just UDP.

Question 78

Which of the following best describes TCP versus UDP protocols?

A. TCP provides more services and is more reliable, but UDP provides more security services.
B. TCP provides a best-effort delivery, and UDP sets up a virtual connection with the destination.
C. TCP is reliable, and UDP deals with flow control and ACKs.
D. TCP provides more services and is more reliable in data transmission, whereas UDP takes less resources and overhead to transmit data.

Answer: D

Summary

TCP is a connection-oriented protocol, meaning it provides a more reliable connection, controls data flow, performs error detection and correction, and sets up a virtual connection. UDP (or any connectionless protocol) does not provide any of these services.

Question 79

Which of the following firewall types keeps track of each ongoing dialog between internal and external systems?

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

Answer: C

Summary

Stateful firewalls use state tables to keep track of each step of communication between systems. This provides a higher level of protection than packet filtering, because it makes access decisions based on the steps that have already been completed in the dialog.

Question 80

ThinNet is another name for what type of Ethernet implementation?

A. 10BaseT
B. Gigabyte Ethernet
C. Fiber
D. 10Base2

Answer: D

Summary

10Base2 is called ThinNet because it uses thin, flexible coaxial cable that is easy to work with. Its network segment length is 185 meters and can provide up to 10 Mbps bandwidth.

Question 81

Which of the following tunnelling protocols would be used if tunneled communication needed to take place over IPX, ATM, or frame relay?

A. PPTP
B. L2TP
C. IPSec
D. PPP

Answer: B

Summary

L2TP can tunnel through networks that incorporate many types of protocols, such as X.25, ATM, and frame relay. PPTP and IPSec can only work over IP-based networks. L2TP does not provide any encryption and must be combined with IPSec if this type of protection is needed. L2TP was developed by combining the best of the L2F and PPTP protocols.

Question 82

The network topology in which all computers are connected together in a non-uniform formation is called what?

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

Answer: A

Summary

A mesh topology is one that does not provide the network structure of the other three mentioned topologies (bus, star, ring). In a partial mesh topology all computers are connected in some way (the Internet is a good example). In a full mesh, each computer is connected to each and every other computer. A full mesh topology provides full redundancy, but requires a lot of cabling.

Question 83

If an external router filters traffic before it enters the network and another screening device monitors traffic before it enters the internal network, what type of architecture is this?

A. Screened host
B. Screened subnet
C. Dual-homed firewall
D. Dual subnets

Answer: B

Summary

A screened subnet filters external traffic and passes it on to the firewall (the second screening device) and then on to the internal network. A screened subnet creates a DMZ by using two routers or firewalls. A screened host is a screening router that is in front of a firewall, but does not create a DMZ.

Question 84

Which of the following is not true of application-level proxy firewalls?

A. Provide a higher level of protection than circuit-level firewalls
B. Hide network information from external entities
C. One proxy per service is needed
D. Improve network performance

Answer: D

Summary

Because application-level proxy firewalls work at such an intricate level, they typically reduce the overall network performance. Application-level proxy firewalls look at the data payload to make access decisions and can detect malicious code and commands, while the other firewall types cannot.

Question 85

A network segment located between the protected and unprotected network is called a __________?

A. Honeypot
B. Safe zone
C. DMZ
D. VPN

Answer: C

Summary

Demilitarized zones (DMZ) provide a buffer and help protect the internal network from the untrusted, external network. A DMZ can be created by setting up two routers or firewalls. Only the necessary systems should be placed in the DMZ, since they will be the first ones accessed by people from the Internet or untrusted network.

Question 86

In which of the following areas does application-level proxy firewalls have an advantage over packet filtering firewalls?

A. Application independence
B. Scalability
C. Security
D. Performance

Answer: C

Summary

Proxy firewalls provide better security as they act as middlemen separating the trusted and untrusted networks. They actually break the connection and do not allow external users to have direct access to internal resources.

Question 87

Which of the following protocols replaced SLIP?

A. IPSec
B. L2TP
C. L2F
D. PPP

Answer: D

Summary

Point-to-Point Protocol (PPP) replaced SLIP because it offers more capabilities such as error correction, better support of authentication, encapsulation of protocols other than IP, and compression of header information. Both protocols are encapsulation protocols used to carry data over serial lines.

Question 88

Packets that contain routing information within their headers are referred to as what?

A. Broadcasting
B. Source routing
C. Forwarding
D. Poisoning

Answer: B

Summary

Source routing uses the packet header information to determine destinations. If a packet has this routing information within its header it can override the routes that routers are configured with. Routers should be configured to identify source routing packets and drop them instead of allowing them passage.

Question 89

What device works at the Physical layer to amplify electrical signals between network segments?

A. Switch
B. Router
C. Repeater
D. Gateway

Answer: C

Summary

Repeaters are simple devices that help extend the network by amplifying a signal so it can pass on to the next segment. Otherwise the signal weakens (attenuation) and may not be decipherable by the receiving system.

Question 90

Which of the following VoIP commands correspond to their potentially devastating effects?

A. The bye command causes VoIP devices to close down while in a conversation.
B. The checksync command can be used to reboot VoIP terminals.
C. The reset command causes the server to reset and reestablish the connection.

D. The establish command causes an unauthenticated client to associate to a server.

Answer: D

Summary

Attackers can impersonate a server and issue commands such as bye, checksync, and reset to VoIP clients. The bye command causes VoIP devices to close down while in a conversation, the checksync command can be used to reboot VoIP terminals, and the reset command causes the server to reset and reestablish the connection, which takes considerable time. The establish command causes an unauthenticated client to associate to a server.

Question 91

In which of the following topologies are all computers connected to a central device?

A. Star
B. Bus
C. Mesh
D. Tree

Answer: A

Summary

Star topologies use a centralized device to connect all devices; the centralized device is a single point of failure.

Question 92

ARP broadcasts messages on the network to find what?

A. IP address
B. MAC address
C. Router
D. Hostname

Answer: B

Summary

The Address Resolution Protocol (ARP) knows the IP address of a device and broadcasts messages in order to find the matching MAC address. ARP stores the IP and MAC mappings in an ARP table.

Question 93

Which of the following technologies uses fiber optic rings to connect different networks and is a MAN technology?

A. ATM
B. Token Ring
C. FDDI
D. Frame relay

Answer: C

Summary

Fiber Distributed Data Interface (FDDI) is a high-speed token-passing technology that offers transmission speeds of 100 Mbps. It is used as a metropolitan area network (MAN) technology, meaning it connects different networks together. (FDDI can be used as a LAN technology, but the CISSP exam refers to it mainly as a MAN technology.)

Question 94

What is the central hub called in a Token Ring network?

A. Star
B. MAU
C. PBX
D. MUA

Answer: B

Summary

Each computer in a Token Ring network is connected to a Multistation Access Unit (MAU), which acts as a central hub. The token will go around to each computer connected to this centralized device in a collapsed ring. The topology, in this example, is a physical star while the technology works in a logical ring.

Question 95

What is the maximum cable length of 10Base2?

A. 500 meters
B. 185 meters
C. 85 meters
D. 100 meters

Answer: B

Summary

10Base2, or ThinNet, should only have a network segment length of 185 meters. After that the signal can degrade.

Question 96

Ethernet uses what type of access method?

A. CSMD
B. Polling
C. CSMA
D. Token passing

Answer: C

Summary

Ethernet uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD), which monitors transmission activity on the wire. A computer that wants to transmit data will listen to see if the line is clear before putting data onto the wire. This is done to help avoid collisions.

Question 97

Which of the following is not true of a circuit-switched network?

A. Acts as a dedicate virtual connection
B. Is connection-oriented
C. Usually carries voice traffic
D. Has variable delays

Answer: D

Summary

Because connections must be established and terminated with each session, there are predictable and fixed delays with circuit-switched networks. Packet-switching connections will have variable delays because the packets can take different paths and be queued at different intermediate devices.

Question 98

In which technology do different users share the same network medium?

A. DSL
B. Cable modem
C. Dial-up
D. ISDN

Answer: B

Summary

A major security concern of cable modems is the fact that neighbors use the same coaxial network and can monitor each other?s traffic.

Question 99

How many bearer channels does a BRI ISDN service have?

A. 23
B. 24
C. 2
D. 1

Answer: C

Summary

Basic rate interfaces (BRI) ISDN service provides two bearer, or B channels, and one D or control channel. Data is transferred over B channels and the call setup, maintenance, and teardown take place over the D channel. PRI ISDN service provides 23 B channels and one D channel.

Question 100

A WAN technology that uses 53-byte cells and has low delay levels is called:

A. ATM
B. Frame relay
C. X.25
D. SMDS

Answer: A

Summary

Asynchronous Transfer Mode (ATM) is a cell-switching technology that provides extremely fast and efficient connection paths. It uses fixed length cells rather than packets.

Question 101

The loss of signal strength as it travels is called:

A. Crosstalk
B. Attenuation
C. Noise
D. Preamble

Answer: B

Summary

Attenuation occurs when electrical signals lose strength as they travel across wires. This is because the electrons encounter resistance as they travel.

Question 102

In twisted-pair cabling, the tighter the wire is twisted, the more resistant the cable is to:

A. Attenuation and breaking
B. Causing fire hazards
C. Interference and attenuation
D. Corrosion

Answer: C

Summary

Tightly twisted cabling ensures strong signal strengths and fewer noise interferences. The different categories of UTP have a direct correlation on the amount of twists implemented for the wiring.

Question 103

A new variant to traditional e-mail spam has emerged on VoIP networks, commonly known as ______________________.

A. Zeus messages
B. Session migration messages
C. SPIT
D. Tunneling spam

Answer: C

Summary

SPIT (Spam over Internet Telephony) causes serious loss of VoIP bandwidth and is a time-wasting nuisance for the people on the attacked network. Because SPIT cannot be deleted like spam on first sight, the victim has to go through the entire message. SPIT is also a major cause of overloaded voicemail servers.

Question 104

A telephone switch located on a company's property with a direct connection to the phone company's central office is called a:

A. Hub
B. PBX

C. Router
D. BPX

Answer: B

Summary

A private branch exchange (PBX) is a device used within companies to provide multiple services to users throughout a building or facility. There are several security concerns pertaining to PBX; default configurations and passwords should be changed, maintenance modems should only be enabled when used, phone bills should be continually reviewed, and unused codes should be disabled.

Question 105

A one-to-many transmission is called:

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

Answer: A

Summary

A multicast goes from one source to several destinations. The destinations that receive the data have chosen to participate and accept data from this source. A unicast is a one-to-one transmission, and a broadcast is a one-to-all transmission.

Question 106

Which OSI layer do routers work at?

A. Data Link
B. Session
C. Transport
D. Network

Answer: D

Summary

A router is a Layer 3 device that looks at data held within the network header to make decisions on how to get the packet to its destination. Bridges work at the Data Link layer and repeaters work at the Physical layer. Software gateways work at the Application layer.

Question 107

Backbones that connect businesses to WANs, the Internet, and other businesses, usually via SONET networks, are called:

A. MANs
B. WANs
C. VPNs
D. VLANs

Answer: A

Summary

Metropolitan area networks (MAN) typically use SONET or FDDI rings to connect businesses to the wide area network (WAN), other MANs, the Internet, and the telecommunication networks. They are referred to as backbones because of the high speed at which data can travel over them compared to LAN type transmissions.

Question 108

Which of the following devices typically works at the Application layer and acts as a protocol translator for different environments?

A. Switch
B. Gateway
C. Bridge
D. Hub

Answer: B

Summary

Software gateways are more complex devices than the other mentioned devices because they look within the frame to gain more than just address and routing information. Translation may need to be performed when entities on two unlike environments need to communicate, as in a Novell and Microsoft network using proprietary protocols. (Although gateways can work at different OSI layers, the CISSP exam usually puts them at the Application layer.)

Question 109

Which is a Physical layer standard for transmitting data over fiber optics lines?

A. SDD
B. SONET

C. Frame relay
D. X.25

Answer: B

Summary

Synchronous Optical Network (SONET) is a standard for fiber optic cabling and uses self-healing network rings. SONET describes the interfaces that can be used over fiber lines and the signaling that must be employed. SONET works at the Physical layer of the OSI model.

Question 110

Which of the following can provide up to 45 Mbps of bandwidth?

A. BRI
B. T3
C. T1
D. PRI

Answer: B

Summary

A T3 can provide 45 Mbps of bandwidth and is the same as 28 T1 lines. T1 lines provide up to 1.544 Mbps, and a fractional T1 is a fraction of that bandwidth. BRI is an ISDN service that provides up to 144 Kbps.

Question 111

A high-speed technology that is always on and can provide data rates up to 52 Mbps is called:

A. DSL
B. ISDN
C. Dial-up
D. CHAP

Answer: A

Summary

Digital subscriber line (DSL) uses copper wires from the central office to the end user and is always connected, meaning the user does not need to re-establish a connection. This is true of the technology, but the service provider providing this service might only allow a connection for a certain time period. Always-on technologies are targeted by attackers because the system is always connected and available.

Question 112

Which is not true of dedicated lines?

A. More secure than using public networks
B. Connect two locations
C. Inflexible and expensive
D. Use packet-switching technology

Answer: D

Summary

One of the biggest advantages of dedicated lines is that the connection is private, meaning that it is not a shared medium. This characteristic provides more security. Dedicated lines are usually much more expensive than public-switched technologies as in frame relay, X.25, and SMDS.

Question 113

Paying for a guaranteed amount of frame relay bandwidth is called:

A. CIR
B. SVC
C. QoS
D. LIN

Answer: A

Summary

Committed information rate (CIR) is a premium service offered by service providers in frame relay networks that guarantees a company a specified amount of bandwidth. Frame relay is bursty in nature, meaning that a company may have access to a larger amount of bandwidth until the network gets busy. If a company needs to ensure it will have a certain amount of bandwidth always available, it will have to pay this extra rate.

Question 114

Which of the following is a real threat in wireless communication?

A. Encryption is not available in wireless technologies.
B. Users cannot be authenticated as they move from one AP to another.
C. No data integrity can be performed as users move from one AP to another.
D. Eavesdropping can uncover traffic analysis and AP and station location can be uncovered.

Answer: D

Summary

Wireless traffic can be easily eavesdropped upon. Traffic analysis is watching the behavior of traffic in the hope of uncovering information not intended for the eavesdropper. Access point (AP) and station location can be uncovered by sniffing traffic. Integrity and authentication should not be affected if a user moves from one AP to another and encryption is available in wireless technologies, referred to as Wired Equivalent Privacy (WEP).

Question 115

What cannot be accomplished by a man-in-the-middle attack?

A. Digital signature
B. Masquerading
C. Session hijacking
D. Spoofing

Answer: A

Summary

A man-in-the-middle attack is when an attacker inserts herself into an ongoing communication between two systems. The user spoofs her identity to fool the other entities, which is an example of masquerading. The attacker can then hijack the session, meaning take over the session. This can be done by kicking one of the users off by performing a denial of service. Digital signatures can prevent man-in-the-middle attacks because authentication takes place.

Question 116

How does PPTP provide protection?

A. Through encryption
B. Through encapsulation
C. Through encryption and encapsulation
D. Through CHAP and AEP

Answer: C

Summary

Point-to-Point Tunneling Protocol (PPTP) is a Microsoft virtual private network (VPN) protocol. It provides encapsulation, which means it re-packages the original frame and encrypts it. This allows for secure communication to take place via an untrusted network, such as the Internet. L2TP is a protocol that provides just encapsulation, not encapsulation and encryption.

Question 117

How does a SOCKS-based firewall provide protection?

A. By providing one proxy per protocol
B. By acting as a proxy
C. By denying any access attempts from internal entities
D. By inspecting protocol commands

Answer: B

Summary

Products that are based on the SOCKS firewall technology are circuit-level firewalls. This means that they only look at packet header information (address, port numbers) to make access decisions. They do not look into the packet's payload to review protocol commands or provide a proxy per service. Those are characteristics of an application-level proxy product.

Question 118

Which of the following is the best definition of a socket?

A. A Session layer link
B. A MAC address and a port number
C. An IP address and a port number
D. An IP address and a MAC address

Answer: C

Summary

A socket is the combination of a node address and a port number. When a connection is made between two systems, the packets need to contain the address and port address of the sending and receiving system. This is so that the packet can be properly routed to the receiving system and the receiving system knows who to reply to.

Question 119

Which firewall makes access decisions based only on addresses and port numbers?

A. Circuit-based proxy
B. Application-based proxy
C. Stateful
D. Dual-homed

Answer: A

Summary

A circuit-level proxy firewall looks at header information to make decisions on whether a packet is deemed acceptable for access. This is a different approach than application-level firewalls, which look at the information within the payload of the packet. A stateful firewall maintains a state table to keep track of each communication dialog taking place between systems and makes access decisions based on the information within this table.

Question 120

Which of the following is required for LAN and WAN centralized access control technologies?

A. Single point of failure
B. RADIUS and TACAS+
C. System with database of authentication information
D. Connection to ISP

Answer: C

Summary

A centralized access technology must have a database of user information and authentication information so when users request access their credentials can be properly checked. RADIUS and TACACS+ are example of centralized access control technologies.

Question 121

Which of the following is a reason companies implement routers and packet filters?

A. To provide content filtering
B. To provide protection that is transparent to users
C. To provide circuit-level proxy protection
D. To provide application-level proxy protection

Answer: B

Summary

Routers can provide packet filtering through the use of access control lists (ACLs). These ACLs are compared to incoming and outgoing traffic and only the packets that are outlined as acceptable are allowed through. Packet filters cannot provide content filtering because they do not look that deep into the packet, and they do not provide application or circuit-level proxy protection.

They are transparent to users because when users request to access a resource on the other side of the router, they do not have to log into that device or do anything special. The protection takes place without them knowing about it.

Question 122

Which of the following best describes an ARP attack?

A. Proper IP to MAC address translation is not allowed, which causes masquerading.
B. Two IP address and two MAC addresses are used.
C. A RARP service is poisoned via DNS resource records.
D. An ARP table is completely deleted.

Answer: A

Summary

ARP (Address Resolution Protocol) finds MAC (Media Access Control) addresses for IP addresses. It broadcasts a request and only the system with the IP address within the broadcast domain responds. ARP takes the MAC address from this response and places it in its ARP table. An attacker can manipulate this ARP table so that traffic with the correct IP address goes to an incorrect MAC address. The traffic goes to the attacker's MAC address instead of the intended receiver.

Question 123

The use of secure cryptographic protocols such as ________________ ensures that all SIP packets are conveyed within an encrypted and secure tunnel.

A. Real-time Transport Protocol
B. Session Initiation Protocol
C. Transport Layer Security
D. PPTP

Answer: C

Summary

The use of secure cryptographic protocols such as Transport Layer Security (TLS) ensures that all SIP packets are conveyed within an encrypted and secure tunnel. The use of TLS can provide a secure channel for VoIP client/server communication and prevents the possibility of eavesdropping and packet manipulation.

Question 124

Why are network sniffers dangerous to an environment?

A. They can be used to launch active attacks.
B. Their presence can cause many false positives.
C. Their presence and activities are not auditable.
D. They can access sensitive data within applications.

Answer: C

Summary

Network sniffers are tools that read network traffic as it passes over a network interface card (NIC). When attackers use these it is considered a passive attack because the attacker is not actually doing anything or modifying packets. Sniffers are not detectable or auditable, thus an administrator would not necessarily know that one is installed and working within her network.

Question 125

What is the electronic phenomenon that allows data to escape in a bundle of network cables?

A. TEMPEST
B. Crosstalk
C. Attenuation
D. Cover channels

Answer: B

Summary

When wires are twisted around each other or are in close proximity, crosstalk can occur. Crosstalk means that signals from one wire spill over and disrupt signals on another wire. UTP has different categories and ratings. Many of the ratings pertain to how tightly the wires are twisted around each other. The tighter the twisting, the less vulnerable the wires are to crosstalk.

Question 126

Which layer of the OSI reference model deals with providing reliable and transparent data transfer between end points of a session?

A. Network
B. Data Link
C. Transport
D. Session

Answer: C

Summary

Protocols operating at the Transport layer are responsible for reliability. Session layer protocols are responsible for the session establishment, maintenance and breakdown, but are not responsible for data transfer itself.

Question 127

Routers work at which of the following layers?

A. Network
B. Transport
C. Session
D. Data Link

Answer: A

Summary

Transport layer protocol information does not address information that is valuable to the function of routing. Routers mainly work at Layer 3 (the Network layer), but Layers 1 and 2 are stripped away in the process.

Question 128

Which of the following is a good definition of asynchronous communication?

A. Low data transfer rate using only one channel for transmission
B. High data transfer using many channels
C. High-speed transmission controlled by electronic timing signals
D. Sequential data transfer, using bits framed with start and stop bits

Answer: D

Summary

Asynchronous communication devices, like modems, must first agree upon a communication rate. The communication is not synchronized in that the devices involved can send data at will, sending a sequence of bits framed with start and stop bits that are reassembled into data at the receiving end. Synchronous communication devices, on the other hand, determine a synchronization scheme and communicate data in a stream.

Question 129

Which of the following protocols is considered to be connectionless?

A. ICMP
B. TCP

C. SSL
D. VPN

Answer: A

Summary

ICMP is a protocol within the TCP/IP protocol suite that provides IP node information at the Network layer. While its job, particularly in the case of its role in the PING utility, is often to determine a device?s connection state, it is considered a "connectionless" protocol in that it deals only with messaging and status checking.

Question 130

Which of the following protocols does not map to the Transport layer of the OSI reference model?

A. Transmission Control Protocol
B. Sequenced Packet Exchange
C. User Datagram Protocol
D. Internet Packet Exchange

Answer: D

Summary

Internet Packet Exchange (IPX) is a protocol that exists at the Network layer in the OSI reference model. A good way to remember this is to mentally associate IPX with IP; IPX/SPX is the suite of protocols used originally in Novell Netware networks.

Question 131

Which of the following is a LAN transmission technology that is susceptible to collisions, and provides a mechanism for retransmission?

A. Ethernet
B. Token Ring
C. ATM
D. AppleTalk

Answer: A

Summary

Ethernet transmissions use CSMA/CD (Carrier Sensing, Multiple Access, Collision Detection) and retransmit data after a collision using a random process to avoid further collisions.

Question 132

Which of the following could be considered an advantage of token passing over Carrier Sensing Multiple Access (CSMA) media access technologies?

A. Inexpensive to implement
B. Collision detection
C. Collision avoidance
D. Collision supported by the protocol

Answer: C

Summary

In a token-passing network collisions on the network media are mainly nonexistent, as only the station that has the token is allowed to transmit information.

Question 133

What is the recommended cable that will allow for a 100 Mbps data rate?

A. 10Base2
B. 100Base2
C. Category 3
D. Category 5

Answer: D

Summary

Coaxial 10Base2 allows for 10 Mbps only, 100Base2 exists but is more expensive to install that Category 5, and Category 3 UTP only allows for 10 Mbps data rate. 100 Mbps data rates can be achieved over Category 5 UTP by implementing a Fast Ethernet network.

Question 134

Which of the following does not cause signal attenuation?

A. Asynchronous signals
B. Cable malfunctions
C. Cable breaks
D. Length of the cable

Answer: A

Summary

Cable malfunctions, cable breaks, and the length of the cable have direct correlation on the possibility of weakening a signal, which is attenuation.

Question 135

Which of the following use baseband transmission?

A. CATV
B. Ethernet
C. Cable modem
D. ADSL

Answer: B

Summary

Ethernet is a baseband transmission method that requires a direct current be applied to the wire, high voltages representing a 1 bit and low voltage loads representing a 0 bit. This differs from broadband, the method that the other possible choices use. Broadband method allows multiple channels on the same medium, which in turn allows for multiple simultaneous data

Question 136

Which transmission type sends a packet to multiple specific computers?

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

Answer: A

Summary

Multicast allows for multiple users to receive a packet, while broadcast means that all users on a given network will receive a packet. Unicast is used if only one computer is the intended recipient, and simulcast refers to simultaneously broadcasting a program on TV and on radio.

Question 137

What is the purpose of the ARP protocol in the TCP/IP protocol suite?

A. Resolves names to IP addresses
B. Resolves IP addresses to names
C. Resolves MAC addresses to names
D. Resolves IP addresses to MAC addresses

Answer: D

Summary

ARP makes the connection between the addressing protocol (IP) and the physical address of the IP node, called the MAC address. ARP includes components for resolving, caching, and announcing the MAC address of a given IP node.

Question 138

Which of the following devices does not pass broadcast information?

A. Repeater
B. Router
C. Switch
D. Bridge

Answer: B

Summary

Routers are devices with a bridging function, and thus will pass broadcast information from non-routable protocols. Routers can block all broadcast traffic from passing.

Question 139

On a firewall, what is a function of a state table?

A. To provide virus detection
B. To filter viruses
C. To track packets
D. To detect spyware

Answer: C

Summary

A state table is used in stateful packet filtering to track packets.

Question 140

Which one of the following is not a primary component or aspect of firewall systems?

A. Protocol filtering
B. Packet switching
C. Rule enforcement engine
D. Extended logging capability

Answer: B

Summary

Packet switching is a component of a routing device. All of the other choices represent standard firewall features.

Question 141

Which of the following is not true about an application proxy firewall?

A. Better performance than non-proxy firewalls
B. Works on all seven layers
C. Inspects data within the packet
D. Exists only for a limited set of protocols

Answer: A

Summary

Firewalls that act in a proxy fashion must pass the packet up to the proxy software on the firewall, thus degrading performance. This ability to work on all layers of the packet, and even to be able to filter based on the data within a packet is a key advantage of application proxy firewall.

Question 142

Which of the following is not true about ISDN?

A. Requires both B and D channels
B. Supports voice, video, and data transmission
C. Sends control information over the B channel
D. Uses the same wires as analog media

Answer: C

Summary

The B channels are for sending data, and the D channel is used to send control information.

Question 143

Which of the following provides a framework to enable many types of authentication techniques to be used during PPP connections?

A. CHAP
B. PAP
C. EAP
D. S-EAP

Answer: C

Summary

Extensible Authentication Protocol (EAP) is not a specific authentication mechanism as are PAP and CHAP. Instead, it provides a framework to enable many types of authentication techniques to be used during PPP connections. It extends the authentication possibilities from the norm (PAP and CHAP) to other methods such as one-time passwords, token cards, biometrics, Kerberos, and future mechanisms.

Question 144

Which of the following is a disadvantage of PPTP?

A. Only works over IP
B. Comes bundled with the operating system
C. Easy to configure a new link
D. It is free

Answer: A

Summary

This might be a negligible disadvantage in today, but it should be recognized that the more recently developed tunneling protocol, L2TP, allows for tunneling over IPX and SNA as well as TCP/IP.

Question 145

The application layer in the TCP/IP model equates to what layer in the OSI model?

A. Application
B. Session, Transport, Application
C. Application, Session, Presentation
D. Application, Session, Transport

Answer: C

Summary

The application layer in the TCP/IP architecture model would be equivalent to a combination of the Application, Presentation, and Session layers in the OSI model.

Question 146

Not every data transmission incorporates the Session layer. Which of the following best describes the functionality of the Session layer?

A. End-to-end data transmission
B. Application client/server communication mechanism in a distributed environment
C. Application to computer physical communication
D. Provides application with the proper syntax for transmission

Answer: B

Summary

The communication between two pieces of the same software product that reside on different computers need to be controlled, which is why Session layer protocols even exist. Session layer protocols take on the functionality of middleware, which allow software on two different computers to communicate.

Question 147

In the TCP/IP model, where does the SPX protocol reside?

A. Host-to-host
B. Internet
C. Network access
D. Application

Answer: A

Summary

The host-to-host transport layer in the TCP/IP architecture model would be equivalent to the Transport layer in the OSI model. This is where the SPX protocol resides.

Question 148

In the TCP/IP model, where does the BGP protocol reside?

A. Host-to-host
B. Internet
C. Network access
D. Application

Answer: B

Summary

The Internet layer in the TCP/IP architecture model would be equivalent to the Network layer in the OSI model, which is where all routing protocols work.

Question 149

The OSI Data Link layer is broken down into two sub-layers. Which of the following is the correct IEEE standards for these sub-layers?

A. 802.1 and 802.2
B. 802.3 and 802.4
C. 802.3 and 802.5
D. 802.2 and 802.3

Answer: D

Summary

The Data Link layer is divided into two functional sublayers, Logical Link Control (LLC) and Media Access Control (MAC). LLC, defined in the IEEE 802.2 specification, will communicate with the protocol immediately above it, the Network layer, in either connection or connectionless mode. The MAC will have the appropriately loaded protocols to interface with the protocol requirements of the Physical layer. The IEEE MAC specification for Ethernet is 802.3, Token Ring is 802.5, wireless is 802.11, etc. So when you see IEEE standards as in 802.11, 802.16, 802.3, and so on, this is referring to the protocol what is working at the MAC sub-layer of the Data Link layer of a protocol stack.

Question 150

In the TCP/IP model, where does the PPP protocol reside?

A. Host-to-host
B. Internet
C. Network access
D. Application

Answer: C

Summary

The Network Access layer in the TCP/IP architecture model would be equivalent to a combination of the Data Link and the Physical layers in the OSI model, which is where PPP works.

Question 151

What is the purpose of the Logical Link Control layer in the OSI model?

A. Provides a standard interface for the Network layer protocol
B. Provides the framing functionality of the Data Link layer
C. Provides addressing of the packet during encapsulation
D. Provides the functionality of converting bits into electrical signals

Answer: A

Summary

The Data Link layer has two sublayers, the Logical Link Control (LLC) and Media Access Control (MAC) layers. The LLC provides a standard interface for what ever network protocol is being used. This provides an abstraction layer so that the network protocol does not need to be programmed to communicate with all of the possible MAC level protocols (Ethernet, Token Ring, WLAN, FDDI, and so on.)

Question 152

What is the port range for well-known ports?

A. 0-1024
B. 1-65,565
C. 1-1023
D. 0-1023

Answer: D

Summary

Port numbers up to 1023 (0-1023) are called well-known ports, and almost every computer in the world has the exact same protocol mapped to the exact same port number. That is why they are called well-known?everyone follows this same standardized approach.

Question 153

What is the proper range for a Class D IP network?

A. 0.0.0.0 to 127.255.255.255
B. 128.0.0.0 to 191.255.255.255
C. 192.0.0.0 to 223.255.255.255
D. 224.0.0.0 to 239.255.255.255

Answer: D

Summary

Class A: 0.0.0.0 to 127.255.255.255 Class B: 128.0.0.0 to 191.255.255.255 Class C: 192.0.0.0 to 223.255.255.255 Class D: 224.0.0.0 to 239.255.255.255 Class E: 240.0.0.0 to 255.255.255.255

Question 154

What is the purpose of Classless Inter-Domain Routing (CIDR)?

A. To allow for the traditional classes to be used more efficiently
B. To extend the IP address space to 128 bits in size
C. To provide more security for network traffic
D. To allow for more efficient routing

Answer: A

Summary

Classless Inter-Domain Routing (CIDR) was created because it was clear that available IP addresses were running out as more individuals and corporations participated on the Internet. A class B address range is usually too large for most companies, and a class C address range is too small. So CIDR provides the flexibility to increase or decrease the class sizes as necessary.

Question 155

What is the purpose of a packet time-to-live?

A. Protect against source routing
B. Ensure that a packet does not continue to be routed forever
C. Ensure that a packet contains the correct transport header information
D. Protect against Loki attacks

Answer: B

Summary

To ensure that packets do not continually transverse a network forever, IP provides a time-to-live (TTL) value that is decremented every time the packet passes through a router.

Question 156

Which of the following is not a characteristic of Lightweight Extensible Authentication Protocol?

A. Proprietary wireless LAN authentication method developed by Cisco Systems
B. Provides dynamic keys and mutual authentication
C. Allows for clients to re-authenticate frequently
D. Replaces WEP

Answer: D

Summary

The Lightweight Extensible Authentication Protocol (LEAP) is a proprietary wireless LAN authentication method developed by Cisco Systems. Important features of LEAP are the use of dynamic WEP keys and mutual authentication (between a wireless client and a RADIUS server). LEAP allows for clients to reauthenticate frequently; upon each successful authentication, the clients acquire a new WEP key. LEAP may be configured to use TKIP instead of dynamic WEP.

Question 157

Which of the following is not true of IPng?

A. Uses a 128-bit addressing space
B. IPSec is incorporated into the protocol.
C. Requires NAT
D. Contains autoconfiguration functionality

Answer: C

Summary

IP version 6, also called IP Next Generation (IPng), has an address space of 128 bits, has autoconfiguration (which makes administration easier), has IPSec integrated, but does not require NAT. NAT was developed since IPv4 addresses were running out. The IP address size could make NAT obsolete for the purpose of saving public addresses.

Question 158

Why is it easier for a repeater to "clean up" a digital signal than an analog signal?

A. An analog signal can have an infinite number of states.
B. An analog signal discretely represents binary values.
C. The encoding process is legacy.
D. Digital signals are more fragile than analog signals.

Answer: A

Summary

It is more difficult to extract analog signals from background noise because the amplitudes and frequency waves slowly lose form. This is because an analog signal could have an infinite number of values or states, where a digital signal exists in discrete states. A digital signal is a square wave, which does not have all of the possible values of the different amplitudes and frequencies of an analog signal.

Question 159

What is a beaconing functionality in a token-passing technology?

A. Ensures that a fault domain never occurs
B. Ensures that only one frame is on the network at a time
C. Allows the computers to communicate with each other through the token
D. Excludes a misbehaving computer from the ring

Answer: D

Summary

If a computer detects a problem with the network, it sends a beacon frame. This frame generates a failure domain, which is between the computer that issued the beacon and its neighbor downstream. The computers and devices within this failure domain will attempt to reconfigure certain settings to try and work around the detected fault.

Question 160

How are FDDI and FDDI-2 different?

A. FDDI-2 provides higher bandwidth.
B. FDDI-2 allows for fixed bandwidth to be assigned.
C. FDDI-2 works over fiber.
D. FDDI-2 is an actual standard, where FDDI is a de facto standard.

Answer: B

Summary

FDDI-2 provides fixed bandwidth that can be allocated for specific applications. This makes it work more like a broadband connection, which allows for voice, video, and data to travel over the same lines.

Question 161

What is the importance of using plenum-rated cabling in buildings?

A. They are noncombustible
B. They help ensure human safety
C. They increase speed and bandwidth
D. They are made out of polyvinyl chloride

Answer: B

Summary

Network cabling that is placed in these types of areas, called plenum space, must meet a specific fire rating to ensure that it will not produce and release harmful chemicals in case of a fire. A building?s ventilation usually takes place through this plenum space and if toxic chemicals were to get into that area, they could be easily spread throughout the building in minutes. Nonplenum cables usually have a polyvinyl chloride (PVC) jacket covering, whereas plenum-rated cables have jacket covers made of fluoropolymers.

Question 162

Claude has been told that he needs to integrate IGMP into the corporation routers. What type of functionality is the company wanting to allow?

A. Exterior routing
B. Interior routing
C. Instant messaging
D. Multicasting

Answer: D

Summary

Internet Group Management Protocol (IGMP) is a protocol that is used to report multicast group memberships to routers. When a user chooses to accept multicast traffic, this means that she becomes a member of a particular multicast group. IGMP is the mechanism that allows her computer to inform the local routers that she is part of this group and to send traffic with a specific multicast address to her system.

Question 163

Which of the following is a characteristic of a token-passing technology?

A. Chatty
B. Deterministic
C. Collision-oriented
D. Bursty

Answer: B

Summary

Some applications and network protocol algorithms work better if they can communicate at determined intervals, instead of whenever the data arrives. In token-passing technologies, traffic arrives in this type of deterministic nature because not all systems can communicate at one time, but only when a system has control of the token. Chatty, collision-oriented and bursty all describe Ethernet environments.

Question 164

Kevin has seen an increase in ICMP traffic going toward the company?s Web server. It has not been a lot of ICMP traffic, so he is not sure if he should be concerned or not. What kind of attack that could be going on?

A. Fraggle
B. DoS
C. Birthday
D. Loki

Answer: D

Summary

Loki is actually a client/server program that is used by hackers to set up back doors on systems. A computer is attacked and the server portion of the Loki software is installed. This server portion "listens" on a port, which is the back door that an attacker can use to access the system. To gain access and open a remote shell to this computer, an attacker sends commands inside ICMP packets. This is usually successful because most routers are configured to allow ICMP traffic to come and go out of the network. This is because ICMP has been seen as a basically benign protocol, since it was developed to not hold any data or a payload. The other attacks do not use the ICMP protocol.

Question 165

Which of the following is not a characteristic of a multilayered switch?

A. QoS
B. High speed routing
C. Can use MPLS
D. Works only at the Data Link layer

Answer: D

Summary

Today's Layer 3, Layer 4, and other layer switches have more enhanced functionality than Layer 2 switches. These higher level switches offer routing functionality, packet inspection, traffic prioritization, and quality of service (QoS) functionality. These switches are referred to as multilayered switches because they combine Data Link layer, Network layer, and other layer functionalities.

Question 166

What is the purpose of a tag information base pertaining to switching?

A. SNMP agents keep device status information in this database.
B. MPLS-enabled devices use it to keep track of the different networks.
C. This is necessary for VLAN configuration to take place.
D. It allows switches to build network topologies to protect against DoS attacks.

Answer: B

Summary

When a packet reaches the switch, the switch will compare the destination address with its tag information base, which is a list of all of the subnets and their corresponding tag numbers. The switch appends the tag to the packet and sends it to the next switch. All of the switches in between this first switch and the destination host will just review this tag information to indicate which route it needs to take instead of analyzing the full header.

Question 167

Sam has decided to move from a static routing protocol to a dynamic routing protocol within his LAN. Which of the following is the main advantage of using a dynamic protocol?

A. Route tables can now be built manually so that Sam can have more control over where traffic is routed throughout his network.
B. Route tables will not be modified just because a route goes down or is congested.
C. Route tables will be dynamically built and modified.
D. Routes will now be encrypted without the need of manual configuration by Sam.

Answer: C

Summary

A dynamic routing protocol means that it can discover routes and build a routing table. Routers use these tables to make decisions on the best route for the packets they receive. A dynamic protocol can change the entries in the route table based on changes that take place to the different routes.

Question 168

John was explaining to Dusty that there has been extensive route flapping, which has caused extreme delay in their WAN and LAN connections. What is John referring to?

A. Availability of routes has continually changed
B. Routers were under attack from hackers sending UDP packets with incorrect route table updates
C. Wormhole attacks were being carried out
D. Several routers were going off-line for an unknown reason

Answer: A

Summary

Route flapping is a term that refers to the constant changes in the availability of routes. If a router does not receive an update that a link has gone down, the router will continue to forward packets to that route, which referred to as a black hole.

Question 169

Which of the following best describes the difference between a link-state and a distance-vector routing protocol?

A. A link-state protocol uses more metrics than a distance-vector protocol when making a route decision.
B. A link-state protocol makes routing decisions based on the number of hops between the source and destination and a distance-vector protocol makes the decision based on distance.
C. A distance-vector protocol looks at the congestion of a link and a link-state protocol does not.
D. A distance-vector protocol builds a more accurate routing table than a link-state protocol

Answer: A

Summary

Distance-vector routing protocols make their routing decisions on the distance (or number of hops) and a vector (a direction). The protocol takes these variables and uses them with an algorithm to determine the best route for a packet. Link-state routing protocols build a more accurate routing table because they build a topology database of the network. These protocols look at more variables than just number of hops between two destinations. They use packet size, link speed, delay, loading, and reliability as the variables in their algorithms to determine the best routes for packets to take.

Question 170

Which of the following has a proper mapping between the protocol and the description?

A. OSPF is a distance-vector protocol.
B. RIP is a link-state protocol.
C. IGRP is an exterior routing protocol.
D. BGP is an exterior routing protocol.

Answer: D

Summary

The Border Gateway Protocol (BGP) enables routers on different ASs to share routing information to ensure effective and efficient routing between the different networks. It is commonly used by Internet service providers to route data from one location to the next on the Internet.

Question 171

Which of the following best describes how BGP is considered to be a combination of link-state and distancevector routing protocols?

A. It builds a network topology like a distance-vector protocol and updates periodically as a link-state protocol.
B. It sends updates like a link-state protocol and builds a static table like a distance-vector protocol.
C. It builds a network topology like a link-state protocol and updates periodically like a distance-vector protocol.
D. It makes route decisions based on hops like a link-state protocol and updates periodically like a distancevector protocol.

Answer: C

Summary

BGP uses a combination of link-state and distance-vector routing algorithms. It creates a network topology by using its link-state functionality and transmits updates on a periodic basis instead of continuously, which is how distance-vector protocols work.

Question 172

What is a routing policy and what is it used for?

A. It states the type of traffic that is allowed access to network resources.
B. Administrators can apply filters and assign weights to route metrics.
C. It is derived from the organizational policy and states who can maintain routing devices.
D. It stipulates the type of controls that must be put into place to protect different types of traffic.

Answer: B

Summary

Network administrators can apply filters and weights to the different variables that are used by link-state routing protocols when determining the best routes. These configurations are collectively called the routing policy.

Question 173

Which of the following controls would stop attacks that are carried out by manipulating router route tables?

A. Authentication
B. ACLs
C. Filters
D. MICs

Answer: A

Summary

Hackers send ICMP messages to routers that contain status information. This status information may indicate that a route is down or congested. Routers accept these messages without requiring the sender to authenticate. If the router required authentication, these types of attacks would not be successful.

Question 174

Paul is a network administrator of the ACME wired and wireless LANs. One of his engineers says that they have experienced wormhole attacks over the last month. What does this mean?

A. Attackers are sending ICMP packets to modify their routers.
B. Two attackers have been working together at different places of the network.
C. Someone has been sending unsolicited messages to Bluetooth-enabled devices.
D. Instant messaging has been used to allow the wormhole worm into the environment.

Answer: B

Summary

An attacker can capture a packet at one location and tunnel it to another location on the network. In this type of attack, there are two attackers at each end of this tunnel (which is referred to as a wormhole). Attacker A could capture an authentication token that is being sent to an authorized user, and then send this token to the other attacker, who then uses it to gain unauthorized access to a resource.

Question 175

What is the countermeasure for wormhole attacks?

A. Authentication
B. Longer initialization vectors
C. TKIP
D. Leashes

Answer: D

Summary

The countermeasure for this type of attack requires the use of leashes, which are just data that is put into a header of the individual packets. The leash restricts the packet?s maximum allowed transmission distance. The leash can be geographical, which ensures that a packet stays within a certain distance of the sender, or temporal, which limits the lifetime of the packet.

Question 176

Extensible Authentication Protocol Transport Layer Security (EAP-TLS) uses a __________________________ to enable authentication with an authentication server. EAP-TLS establishes a TLS encrypted tunnel to facilitate ____________________ authentication.

A. One-time passwords, two factor
B. Kerberos, ticket
C. Public Key Infrastructure, certificate-based
D. SESAME, tokens

Answer: C

Summary

Extensible Authentication Protocol Transport Layer Security (EAP-TLS) uses a Public Key Infrastructure (PKI) to enable authentication with an authentication server. EAP-TLS establishes a TLS encrypted tunnel to facilitate certificate-based authentication.

Question 177

Toby has been asked by his boss to set up a three-tiered configuration within the company?s network. Which of the following best describes this type of architecture?

A. Screened host
B. Screened subnet
C. Two screened subnets
D. Multi-homed architecture

Answer: C

Summary

Sometimes a screened-host architecture is referred to as a single-tiered configuration. A screened subnet is referred to as a two-tiered configuration. If there are three firewalls that create two separate DMZs, this can be called a three-tiered configuration.

Question 178

Sam and a forensics team investigated and caught a hacker that had been attacking systems within their network. Sam uncovered a complete topology of their network, along with IP addresses, services running, and accounts for each and every device on the network. What did the hacker most likely carry out to obtain this information?

A. Zone transfer
B. Port scans
C. Loki attacks
D. Smurf attacks

Answer: A

Summary

The primary and secondary DNS servers synchronize their information through a zone transfer. Changes take place to the primary DNS and then those changes need to be replicated to the secondary DNS server. It is important to configure the DNS server to only allow zone transfers to take place between the specific servers. For years now attackers have been carrying out zone transfers to gather very useful network information from victims? DNS servers. Unauthorized zone transfers can take place if the DNS server are not properly configured to restrict this type of activity.

Question 179

Julie has been told that her company has been the victim of a DNS poisoning attack. What were the symptoms that were mostly identified to indicate this type of attack?

A. Routers were misrouting packets.
B. Traffic was bypassing firewalls.
C. Users were able to bypass the company?s proxy server.
D. Web redirection was occurring.

Answer: D

Summary

A DNS poisoning attack means that an attacker provides a DNS server with an incorrect hostname to IP mapping information. This attack is usually carried out to point users to an incorrect Web site.

Question 180

The countermeasure to DNS poisoning is DNSSec. How does it work?

A. All DNS servers encrypt the data sent back and forth between them.
B. All DNS servers digitally sign messages between them.
C. All DNS servers authenticate to the requesting clients.
D. All clients and DNS servers carry out mutual authentication.

Answer: B

Summary

If DNSSEC (DNS security, which is part of the DNS Bind software) was enabled, then when a DNS server received a response from another DNS server, it would validate the digital signature on the message before accepting the information to make sure that the response was from an authorized DNS server.

Question 181

Kathy works in an all-Windows environment and has been told that a Unix network needs to also be set up to support some new applications that cannot run on Windows systems. She has read that she needs to set up an NIS server. Why would she need to set this up?

A. To allow Windows and Unix clients to share files through a virtual file system
B. Security purposes
C. To include a type of firewall that works in Unix environments
D. Central administration

Answer: D

Summary

In a Unix environment, systems use certain system configuration files, and in a network it is usually easier if all of the systems contain identical configuration files. Instead of maintaining these files individually for each computer, NIS is a way to have all of these configuration files stored and maintained locally. This allows for central administration. NIS has no real security components.

Question 182

How does NIS provide functionality like a DNS server?

A. It has a central host table.
B. It forwards hostname to IP mapping requests.
C. It carries out zone transfers.
D. It contains configuration files.

Answer: A

Summary

A host table is a file that contains hostname-to-IP mappings. It is used in the same way that DNS is, but it is a file that computers can use to map a hostname to a specific IP address instead of a technology or a product. This is why NIS is sometimes compared to DNS, because they both provide the necessary mechanisms for computers to be able to uncover the IP address of a system.

Question 183

Two months after Kathy set up her NIS+ server she found out that password file had been captured and brute forced. What most likely took place to allow this to happen?

A. Kathy accidentally chose security level 3 when she was configuring the server.
B. The NIS+ server was configured to be backwards compatible with NIS.
C. Unauthorized zone transfers took place.
D. Kathy did not encrypt the password file on the server.

Answer: B

Summary

NIS+ is backward compatible with NIS, which opens up a hole for hackers to exploit. If a hacker?s system has NIS client software, and the NIS+ server is configured to be backward compatible, the NIS+ server can access files without first having to be authenticated and authorized. So the hacker can get the password file and start cracking away.

Question 184

Which of the following best describes the Lightweight Directory Access Protocol?

A. A protocol designed to access directories that follow the X.500 standard
B. A protocol designed to access directories that follow the X.400 standard
C. A protocol designed to access directories that follow the X.509 standard
D. A protocol designed to access directories that follow the X.300 standard

Answer: A

Summary

Lightweight Directory Access Protocol (LDAP) is a client/server protocol used to access network directories, as in Microsoft?s Active Directory or Novell?s Directory Services (NDS). These directories follow the X.500 standard.

Question 185

Which of the following is not an attribute of LDAP directories?

A. Uses distinguished names
B. Uses attributes
C. Uses values
D. Uses tuples

Answer: D

Summary

The LDAP specification works with directories that organize their database in a hierarchical tree structure. The tree has leaves (entries) with unique distinguished names. These names are hierarchical and describe the object?s place within the tree. The entries can define network resources, computers, people, wireless devices, and more. Each entry has an attribute and a value. A tuple is used in a relational database, not a hierarchical database.

Question 186

What is the purpose of an EDI and how does it relate to a value-added network (VAN)?

A. Standardized electronic communication. A VAN provides the necessary level of security through VLANs.
B. Standardized electronic communication. A VAN is a service bureau that provides this type of service.
C. Technology that connects supplies and their customers. A VAN provides the authentication piece for the transactions.
D. Technology that connects supplies and their customers. A VAN provides the payment gateway for the transactions.

Answer: B

Summary

Instead of using paper purchase orders, receipts, and forms, EDI is the technology to provide all of this digitally. A value-added network (VAN) is when a company pays another company (service bureau) to develop and maintain this EDI infrastructure for them.

Question 187

Companies can use private IP addresses for free, instead of paying for public addresses. Which of the following is an incorrect private IP range?

A. 10.0.0.0 to 10.255.255.255
B. 172.16.0.0 to 172.31.255.255
C. 172.16.0.0 to 172.32.255.255
D. 192.168.0.0 to 192.168.255.255

Answer: C

Summary

The following lists current private IP address ranges: The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private internets: 10.0.0.0 to 10.255.255.255 (10/8 prefix) 172.16.0.0 to 172.31.255.255 (172.16/12 prefix) 192.168.0.0 to 192.168.255.255 (192.168/16 prefix)

Question 188

Monica has a choice of setting up static, dynamic, or port network address translation (NAT). Which of the following is a correct mapping between the type of NAT and its functionality?

A. Static uses a "first come first served" functionality for the one IP address it shares between all systems.
B. In dynamic NAT, each private address has a public address mapped to it at all times.
C. Port NAT uses one private address for all systems on the network.
D. Static NAT uses more public addresses than the other types.

Answer: D

Summary

Static NAT means that one public address is always mapped to the same private address. Dynamic NAT works under the "first come first served" method. Port NAT provides one public IP for all systems. Static NAT uses the most IP addresses.

Question 189

Why would a hacker be disappointed once she figured out that the network she is wanting to attack is using NAT?

A. Internal addresses are hidden.
B. Internal computers have another layer of firewall protection.
C. There is only one entry to the network.
D. NAT is harder to compromise than most firewalls.

Answer: A

Summary

NAT is not a firewall technology. And just because NAT is being used does not mean that there is only one entry point to a network. NAT maps private address to public addresses. All packets leaving the network will have the address of the NAT device, so a hacker cannot see the internal addresses.

Question 190

Which of the following is true when comparing LAN and WAN protocols?

A. WAN environments can introduce more errors in transmission, so these protocols are usually connectionoriented.
B. LAN environments can introduce more errors in transmission, so these protocols are usually connectionoriented.
C. WAN protocols are usually connectionless because they have to transverse so many different network types.
D. LAN protocols are usually connection-oriented because of the amount of collisions that can take place on the network.

Answer: A

Summary

Communication error rates are lower in LAN when compared to WAN environments, which makes sense when you compare the complexity of each environment. WAN traffic may have to travel hundreds or thousands of miles and pass through several different types of devices, cables, and protocols. Because of this difference, most LAN media access control protocols are connectionless and most WAN communication protocols are connection-oriented. Connection-oriented protocols provide reliable transmission, because they have the capability of error detection and correction.

Question 191

In packet-switched environments, routers and switches will make decisions on the best route for a packet to take. This is why different packets of a message can arrive out of order, as they did not necessarily all follow the same path. What technology do these types of protocols use to make the path decisions?

A. Time Division Multiplexing
B. Carrier Sensing Multiple Access
C. Statistical Time Division Multiplexing
D. Frequency Division Multiplexing

Answer: C

Summary

Packet switching is based on Statistical Time Division Multiplexing (STDM), which analyzes statistics on the various possible routes to make the decision on the best route for a packet.

Question 192

Tom is told that his network needs to be isochronous to meet the demands of the new application that the company purchased. What does this mean?

A. It needs to provide quality of service.
B. It needs to provide authentication between the client and server portions of the new software.
C. It needs to integrate EAP and Kerberos to support the application.
D. It needs PVCs set up through the WAN connection.

Answer: A

Summary

Applications that are time sensitive, such as voice and video signals, need to work over an isochronous network. This means that all of the components in the network that are responsible for providing the necessary uniform timing work with a common clock and are properly synchronized.

Question 193

Shane?s company lost their WAN link due to severe weather conditions. The company experienced a loss of $240,000 over the four hours their Web servers were unable to accept customer purchases. Shane has been told to implement a backup option, so that company will not go through this again. Which of the following would Shane implement?

A. MPLS
B. Dial-on demand routing
C. IGMP
D. Link-state redundant point-to-point connection

Answer: B

Summary

Dial-on Demand Routing (DDR) allows a company to send WAN data over their existing telephone lines and use the public circuit-switched network as a temporary type of WAN link. This technology is also implemented as a backup in case the primary WAN link goes down. It provides redundancy and ensures that a company will still be able to communicate if something happens to the primary WAN communication channel.

Question 194

Which of the following is not a characteristic of IDSL?

A. Provides up to 128 Kbps in bandwidth
B. Solution for individuals who cannot get SDSL or ADSL
C. Reaches up to 36,000 feet from a provider?s central office
D. Provides up to 384 Kbps in bandwidth

Answer: D

Summary

IDSL provides DSL for customers who cannot get SDSL or ADSL because of their distance from the central office. It is capable of reaching customers who are up to 36,000 feet from the provider?s central office. IDSL operates at a symmetrical speed of 128 Kbps.

Question 195

Which of the following technologies provides the bandwidth that is equivalent to a T-1 line?

A. ADSL
B. HDSL
C. IDSL
D. DSL

Answer: B

Summary

HDSL (High bit rate Digital Subscriber Line) provides T-1 (1.544 Mbps) speeds over regular copper phone wire without the use of repeaters. Requires two twisted pairs of wires, which many voice grade UTP lines do not have.

Question 196

For two different locations to communicate via satellite links, they must be within the satellite's line of sight and ______________________.

A. Area
B. Distance
C. Coverage
D. Footprint

Answer: D

Summary

Today, satellites are used to provide wireless connectivity between different locations. For two different locations to communicate via satellite links, they must be within the satellite's line of sight and footprint (area covered by the satellite). The sender of information (ground station) modulates the data onto a radio signal that is transmitted to the satellite. A transponder on the satellite receives this signal, amplifies it, and relays it to the receiver.

Question 197

Technologies that do not require a user to go through a dial-up procedure to connect to a service provider?s central office are referred to as always-on technologies. Attackers like these systems because they are always available to be attacked and to be used to attack others. Which of the following is not considered an always-on technology?

A. ADSL
B. Cable modem
C. ISDN
D. SDSL

Answer: C

Summary

ISDN emulates a dial-up connection and requires the user to go through a dial-up procedure.

Question 198

Jan has been told by the network administrator that the VPN he set up needs provide transport adjacency. Which of the following best describes what this means?

A. More than one security protocol is configured for the VPN traffic.
B. PPTP needs to be configured to be used with L2TP.
C. A PPTP tunnel needs to be configured to go through an IPSec tunnel.
D. An ESP IPSec VPN needs to be set up.

Answer: A

Summary

IPSec can be configured to provide transport adjacency, which just means that more than one security protocol (ESP and AH) is applied to a packet.

Question 199

Sean has configured different VPNs for different routes data will take. This is because data that is traveling within the local network is considered to be at a lower risk of being compromised when compared to when the data travels outside of the local network. What is the term that describes what Sean has set up?

A. Transport adjacency
B. Iterated tunneling
C. Multiple tunneling architecture
D. Multiple adjacency

Answer: B

Summary

IPSec can also be configured to provide iterated tunneling, which is tunneling an IPSec tunnel through another IPSec tunnel. Iterated tunneling would be used if the traffic needed different levels of protection at different junctions of its path. For example, if the IPSec tunnel started from an internal host to an internal border router, this may not require encryption, so only the AH protocol is used. But when that data travels from that border router throughout the Internet to another network, then the data requires more protection. So the first packets travel through a semi-secure tunnel until they get ready to hit the Internet and then go through a very secure second tunnel.

Question 200

Spread spectrum works at which of the following OSI layers?

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

Answer: D

Summary

There are different types of spread spectrum technologies. They differ in their approaches, but they are all technologies that modulate data onto frequencies. They are specifications that dictate how signaling will take place in WLAN environments.

Question 201

Which of the following best describes how frequency hopping spread spectrum (FHSS) differs from direct sequence spread spectrum (DSSS)?

A. FHSS uses a chipping sequence.
B. DSSS provides a higher bandwidth.
C. FHSS is used in the 802.11a standard.
D. DSSS is used in the 802.11a standard.

Answer: B

Summary

DSSS uses a chipping sequence, provides higher bandwidth than FHSS, and is used in the 802.11b standard.

Question 202

What is the chipping code in DSSS used for?

A. It is made up of sub-bits that are combined with the original bits before transmission and provide parity protection.

B. It is made up of sub-bits that are combined with the original bits before transmission and provide encryption protection.
C. It is made up of new frequencies that are combined with the original bits before transmission and provide parity protection.
D. It is made up of new frequencies that are combined with the original bits before transmission and provide encryption protection.

Answer: A

Summary

DSSS takes a different approach by applying sub-bits to a message. The sub-bits are used by the sending system to generate a different format of the data before it is transmitted. The receiving end uses these bits to reassemble the signal into the original data format. The sub-bits are collectively called a chip, and the sequence of how the sub-bits are applied is referred to as the chipping code. They work as parity. If a bit is corrupted during transmission, the receiving system uses the sub-bit to rebuild the original bit.

Question 203

Why does DSSS provide more bandwidth when compared to FHSS?

A. A higher number frequencies is used.
B. Data travels in parallel.
C. The algorithm increase the hopping speeds.
D. Data is compressed before being modulated on the radio wave.

Answer: A

Summary

FHSS puts data on different frequencies. It does not use the whole spectrum at one time, as DSSS does. DSSS sends data down all available frequencies at one time, instead of having the data hop from one frequency to the next.

Question 204

Which of the following is the proper mapping?

A. 802.11 uses FHSS.
B. 802.11a uses DSSS.
C. 802.11b provides up to 1 to 2 Mbps.
D. 802.11b provides up to 52 Mbps.

Answer: A

Summary

Since DSSS sends data across all frequencies at once, it has a higher data throughput than FHSS. The first WAN standard, 802.11, used FHSS, but as bandwidth requirements increased DSSS was implemented. By using FHSS, the 802.11 standard can only provide a throughput of 1 to 2 Mbps. By using DSSS instead, 802.11b provides a data throughput of up to 11 Mbps.

Question 205

What is the relationship between a basic service set (BSS) and SSID?

A. A group of wireless devices are segmented into a BSS and assigned an SSID value.
B. A group of wireless devices are segmented into an SSID and assigned a BSS value.
C. The BSS delineates the access point and wireless devices, and the SSID delineates the wireless and wired devices.
D. The SSID delineates the access point and wireless devices, and the BSS delineates the wireless and wired devices.

Answer: A

Summary

When wireless devices work in infrastructure mode, the AP and wireless clients form a group referred to as a basic service set (BSS). This group is assigned a name, which is the SSID value.

Question 206

Some wireless environments authenticate wireless devices before they are allowed access to the wired environment, via SSID and/or MAC values. Which of the following best describes the downfall of these approaches?

A. Both are easily captured through brute force attacks.
B. The SSID is broadcasted by the wireless device and the MAC address is broadcasted by the access point.
C. The MAC is not broadcasted by the wireless device and the SSID address is broadcasted by the access point.
D. Both are sent in cleartext.

Answer: D

Summary

The SSID is usually required when a wireless devices wants to authenticate to an AP. For the device to prove that it should be allowed to communicate with the wired network, it must first provide a valid SSID value. The SSID should not be seen as a reliable security mechanism because many APs broadcast their SSIDs, which can be easily sniffed and used by attackers. If the AP is configured to require a MAC value for authentication, this data is also sent in cleartext from the wireless device.

Question 207

What spread spectrum is used in the 802.11a standard?

A. FHSS
B. DSSS
C. OFDM
D. SSID

Answer: C

Summary

This standard uses a different method of modulating data onto the necessary radio carrier signals. Where 802.11b uses DSSS, 802.11a uses OFDM and works in the 5 GHz frequency band.

Question 208

The 802.11a standard provides a higher bandwidth than 802.11 and 802.11b. Which of the following is a characteristic of 802.11a that is not shared by 802.11 and 802.11b?

A. Maximum distance that the wireless device should be from the access point is 25 feet.
B. It uses TKIP instead of WEB.
C. It uses the AES algorithm instead of the RC4 algorithm.
D. It increases the keying material for encryption.

Answer: C

Summary

802.1x provides port authentication, which means that all traffic is restricted until the user is properly authenticated. 802.1x does not have anything to do with encryption. Extensible Access Protocol (EAP) extends the types of authentication types.

Question 209

Which of the following is not a characteristic of Protected Extensible Authentication Protocol?

A. Authentication protocol used in wireless networks and Point-to-Point connections
B. Designed to provide more secure authentication for 802.11 WLANs
C. Designed to support 802.1X port access control and Transport Layer Security
D. Designed to support password protected connections

Answer: D

Summary

PEAP (Protected Extensible Authentication Protocol) is a version of EAP and is the authentication protocol used in wireless networks and Point-to-Point connections. PEAP is designed to provide more secure authentication for 802.11 WLANs (wireless local area networks) that support 802.1X port access control and Transport Layer Security. It is a protocol that encapsulates EAP within a potentially encrypted and authenticated Transport Layer Security (TLS) tunnel.

Question 210

Julie has learned the 802.11i standard includes 802.1x. Which of the following best describes the 802.1x technology?

A. It extends the types of authentication that can take place.
B. It allows a user to authenticate using Kerberos, smart cards, or one-time passwords.
C. It offers port authentication.
D. It incorporates a stronger encryption algorithm.

Answer: C

Summary

The 802.1x standard offers port-based network access control.

Question 211

Which of the following is not an identified flaw in the Wired Equivalent Privacy (WEP) protocol?

A. Initialization vector was too long.
B. The wrong encryption algorithm was chosen.
C. There is no mutual authentication requirement.
D. Initialization vectors are reused.

Answer: A

Summary

The deficiencies within the original 802.11 standard include no user authentication, no mutual authentication between the wireless device and access point, and a flawed encryption protocol. The initialization vector was too small and not different for each packet that is to be encrypted.

Question 212

Which of the following best describes the Temporal Key Integrity Protocol?s (TKIP) role in the 802.11i standard?

A. It provides 802.1x and EAP to increase the authentication strength.
B. It requires the access point and the wireless device to authenticate to each other.
C. It sends the SSID and MAC value in ciphertext.
D. It adds more keying material for the RC4 algorithm.

Answer: D

Summary

TKIP adds more keying material to be used by the RC4 algorithm during the encryption and decryption process. This adds more randomness to the process so that the encryption cannot be easily broken.

Question 213

The 802.11i standard has two main components to it. Which of the following best describes these two components?

A. One component uses AES to allow for backward compatibility. The other component uses the TKIP algorithm in counter mode and CBC-MAC.
B. One component uses 802.1x to allow for backward compatibility. The other component uses the 3DES algorithm in counter mode and CBC-MAC.
C. One component uses TKIP to allow for backward compatibility. The other component uses the AES algorithm in counter mode and CBC-MAC.
D. One component uses CCMP to allow for backward compatibility. The other component uses the AES algorithm in counter mode and CBC-MAC.

Answer: C

Summary

Companies and individuals that already have a WLAN setup, can apply 802.11i, which uses TKIP. TKIP provides more keying material for the RC4 algorithm that is used within WEP. Companies that have not yet deployed a WLAN, can use the portion of the standard that uses the AES algorithm in counter mode and uses CBC-MAC.

Question 214

WEP has a long list of security vulnerabilities. Which of the following describes why the algorithm that was chosen by the WEP working group was not the best choice?

A. It?s a stream cipher, which has an inherent deficiency in integrity.
B. It?s a stream cipher, which has an inherent deficiency in key size.
C. It?s a stream cipher, which has an inherent deficiency in being vulnerable to man-in-the-middle attacks.
D. It?s a stream cipher, which has an inherent deficiency in being vulnerable to spoofing attacks.

Answer: A

Summary

Stream ciphers, by default, have a deficiency in that someone can capture a message and modify the bits without the receiver being able to identify it. This is because the message will decrypt properly.

Question 215

When a technology that is compliant to the 802.1x standard is implemented, what are the three main components that are involved?

A. Access point, authenticator, authentication server
B. Supplicant, authenticator, RADIUS server
C. Supplicant, RADIUS server, authentication server
D. Supplicant, authenticator, authentication server

Answer: D

Summary

The 802.1X technology actually provides an authentication framework and a method of dynamically distributing encryption keys. The three main entities in this framework are the supplicant (wireless device), the authenticator (access point), and the authentication server (usually a RADIUS server).

Question 216

Peter has set up a wireless LAN that is compliant with the 802.11i standard. This implementation uses the AES algorithm. Before a user of a wireless device is authenticated, what type of traffic is allowed to go from the user to the authentication server?

A. DHCP, SMTP
B. DHCP, POP, FTP
C. Authentication traffic
D. Encrypted traffic

Answer: C

Summary

If this WLAN is using the AES algorithm, that means 802.1x is also being used, which is port authentication. No traffic other than authentication data is available to the user and his wireless device until proper authentication has taken place. After this happens, the user?s wireless device can receive SMTP, DHCP, and all other types of traffic.

Question 217

Different vendors have implemented various solutions to overcome the vulnerabilities of WEP. Which of the following provides an incorrect mapping between these solutions and their characteristics?

A. LEAP requires a PKI.
B. PEAP only requires the server to authenticate using a digital certificate.
C. EAP-TLS requires both the wireless device and server to authenticate using digital certificates.
D. PEAP requires the user to provide a password.

Answer: A

Summary

Cisco uses a purely password-based authentication framework called Lightweight Extensible Authentication Protocol (LEAP). Other vendors, including Microsoft, use EAP and Transport Layer Security (EAP-TLS), which carries out authentication through digital certificates. And yet another choice is Protective EAP (PEAP), where only the server uses a digital certificate.

Question 218

What are the values that are used by TKIP in the encryption and decryption process?

A. SSID, WEP key, IV
B. IV, MAC, WEP key

C. WEP key, BSS, SSID
D. SSID, MAC, IV

Answer: B

Summary

The protocol increases the length of the IV value and ensures that each and every frame has a different IV value. This IV value is combined with the transmitter's MAC address and the original WEP key, so that even if the WEP key is static the resulting encryption key will be different for each and every frame. (WEP key + IV value + MAC address = new encryption key.)

Question 219

Denise found out that she has been a victim of a Bluejacking. What does this mean?

A. Someone sent an unsolicited message through her PDA.
B. Someone captured her ciphertext data.
C. Someone spoofed a message, which caused a DoS.
D. Someone social engineered her.

Answer: A

Summary

Bluejacking is when someone sends an unsolicited message to a device that is Bluetooth enabled. Bluejackers look for a receiving device (phone, PDA, laptop) and then send a message to it. Many times someone is trying to send someone else their business card, which will be added to the victim?s contact list in their address book.

Question 220

Which of the following does not describe a difference between WAP and i-mode?

A. WAP uses a markup language based on XML.
B. i-mode is popular mainly in Asia.
C. i-mode uses a markup language based on XML.
D. WAP is popular mainly in North America.

Answer: C

Summary

i-mode uses a markup language based on HTML (compact HTML) and is popular mainly in Japan. WAP uses a markup language based on XML and is popular mainly in the U.S.

Question 221

Why are packet filter firewalls not always a competent countermeasure against instant messaging (IM) attacks?

A. They are the best type of countermeasure for this type of threat.
B. They cause an internal denial of service when dealing with IM traffic.
C. They can detect worms that are being transmitted through this traffic type.
D. IM clients can reconfigure themselves to work on a port that is open on the firewall.

Answer: A

Summary

Many firewalls do not have the capability to scan for this type of traffic to uncover suspicious activity. Blocking specific ports on the firewalls is not usually effective because IM traffic can use common ports that need to be open (HTTP port 80 and FTP port 21). Many IM clients will auto-configure themselves to work on another port if their default port is unavailable and blocked by the firewall.

Question 222

If a company wants to allow their internal employees to use instant messaging among themselves, which of the following should be implemented?

A. Corporate IM server
B. IPSec and NAT
C. L2TP and PPTP
D. IGMP

Answer: A

Summary

Companies can implement corporate IM servers so that internal employees communicate within the organization?s network only.

Question 223

How does the Domain Name Service match Internet uniform resource locator (URL) requests?

A. With the actual address or location of the client providing that URL
B. With the actual address or location of the server providing that URL

C. With the virtual address or location of the client providing that URL
D. With the virtual address or location of the server providing that URL

Answer: B

Summary

The Domain Name Service matches Internet uniform resource locator (URL) requests with the actual address or location of the server that is providing that URL.

Question 224

Which protocols are used for securing VPN connections?

A. S/MIME and SSH
B. TLS and SSL
C. IPSec and L2TP
D. PKCS#10 and X.509

Answer: C

Summary

VPN connections are secured using IPSec and L2TP.

Question 225

Which of these common backup methods is the fastest when used on a daily basis?

A. Full backup
B. Incremental backup
C. Fast backup
D. Differential backup

Answer: B

Summary

The incremental backup method only copies files that have been recently changed or added. Only files with their archive bit set are backed up. Although this method is fast and uses less tape space, it has some vulnerabilities, such as the fact that all incremental backups need to be available and restored from the date of the last full backup to the desired date if a restore is required.

Question 226

Mirroring is another name for which RAID implementation?

A. RAID level 2
B. RAID level 3
C. RAID level 5
D. RAID level 1

Answer: D

Summary

RAID level 1 mirrors data from one or more disks to another disk or set of disks. Each drive is normally mirrored to an equal drive that is updated at the same time, thus allowing for recovery from the other drive if one drive should fail.

Question 227

Which of the following is not a common firewall function?

A. Logging Internet activity
B. Enforcing an organization?s security policy
C. Protecting against viruses
D. Limiting security exposures

Answer: C

Summary

Firewalls help to enforce a company?s security policy and limit security exposures by filtering traffic passing to and from the Internet and the corporate network. A firewall does log Internet activity but does not typically protect against viruses.

Question 228

A particular disk drive system has 39 disks: 32 disks of user storage and 7 disks of error recovery coding. What type of system is this?

A. RAID level 2
B. RAID level 0
C. RAID level 1
D. RAID level 5

Answer: A

Summary

This type of drive is RAID level 2.

Question 229

Which of the following best describes a SYN flood?

A. Many new TCP connections in a short period of tim
B. Exceeding the limit of TCP connections on a system
C. Denial of service attack that sends a stream of ACK packets
D. Denial of service attack that sends a stream of SYN/ACK packets

Answer: B

Summary

A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system.

Question 230

LAN devices that typically examine the entire packet are called:

A. Routers
B. Brouters
C. Switches
D. Gateways

Answer: D

Summary

Gateways are primarily software products that can be run on computers or other network devices. They can link different protocols and examine the entire packet.

Question 231

To obtain an IP address from a MAC address, what mechanism is used?

A. Reverse Address Resolution Protocol (RARP)
B. Address Resolution Protocol (ARP)
C. Data Link layer
D. Network Address Translation (NAT)

Answer: A

Summary

The Reverse Address Resolution Protocol (RARP) sends out a packet that includes a MAC address and a request to be informed of the IP address that should be assigned to that MAC. Diskless workstations that need to obtain their IP address from the network may use this process.

Question 232

Which of the following layers deals with Media Access Control (MAC) addresses?

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

Answer: A

Summary

The Data Link layer (Layer 2) transfers information to the other end of the Physical link. It handles physical addressing, network topology, error notification, delivery of frames, and flow control.

Question 233

What kind of attacks are the lower layers (Physical, Link, Network, Transport) unable to protect against?

A. Piggyback
B. Brute force
C. Denial of service
D. Content-based

Answer: D

Summary

Lower layer protocols do not interact with data contained in the payload.

Question 234

Of the following authentication mechanisms, which creates a problem for mobile users?

A. Address-based mechanism
B. Reusable password mechanism
C. One-time password mechanism
D. Challenge-response mechanism

Answer: A

Summary

The address-based mechanism is used for establishing connections, not authentication. This leaves mobile users open to vulnerabilities.

Question 235

An IP spoofing attack can be best classified as a:

A. Session hijacking attack
B. Passive attack
C. Fragmentation attack
D. Sniffing attack

Answer: A

Summary

IP spoofing attempts to convince a system that it is communicating with a known entity, thus giving an intruder access. This is a type of session hijacking attack.

Question 236

Before CIDR (Classless Internet Domain Routing) became common, networks were organized in terms of classes. Which would have been true of a Class C network?

A. The first bit of the IP address would be set to 0.
B. The first bit of the IP address would be set to 1 and the second bit set to 0.
C. The first two bits of the IP address would be set to 1 and the third bit set to 0.
D. The first three bits of the IP address would be set to 1.

Answer: C

Summary

Each class contains a block of addresses that are reserved for private networks and are not routable across the public Internet. For Class C, the reserved addresses are 192.168.0.0 to 192.168.255.255.

Question 237

Where is a DMZ located?

A. Behind the first Internet firewall
B. In front of the first Internet firewall
C. Behind the first network active firewall
D. Behind the first network passive Internet HTTP firewall

Answer: A

Summary

RFC 2647 defines a DMZ as a network segment or segments located between protected and unprotected networks. A DMZ is located directly behind the first Internet firewall.

Question 238

Which of the following describes the management of remote computing technology?

A. Remote Access Security Management (RASM)
B. Remote Behavior Security Management (RBSM)
C. Remote Confidentiality Security Management (RCSM)
D. Remote Integrity Security Management (RISM)

Answer: A

Summary

Remote Access Security Management (RASM) is defined as the management of the elements of the technology of remote computing.

Question 239

Which of the following statements is false?

A. Link encryption encrypts all the data along a specific communication path.
B. Link encryption provides protection against packet sniffers and eavesdroppers.
C. With link encryption, information stays encrypted from one end of its journey to the other.
D. With link encryption, user information, header, trailers, addresses, and routing data that are part of the packets are encrypted.

Answer: C

Summary

In link encryption, packets are decrypted at each hop and encrypted again. Information staying encrypted from one end of its journey to the other is a characteristic of end-to-end encryption, not link encryption.

Question 240

TACACS+ has several advantages over TACACS. These do not include:

A. Event logging
B. Two-factor password authentication
C. The capability for a user to change his password
D. The capability for security tokens to be resynchronized

Answer: A

Summary

Although TACACS+ provides better audit trails, event logging is a service that is only provided with TACACS.

Question 241

Of the following choices, which are not remote user management issues?

A. Validation of the use of remote computing systems
B. Hardware and software distribution
C. User support and remote assistance
D. Access badges

Answer: D

Summary

Access badges are not a concern of remote user management.

Question 242

When providing telecommunications continuity, which of the following methods involves the use of alternative media?

A. Alternative routing
B. Diverse routing
C. Long haul network diversity
D. Last mile circuit protection

Answer: A

Summary

Alternative routing is a method of routing information via an alternate medium such as copper cable or fiber optics.

Question 243

Secure Shell (SSH-2) is a strong method to use when:

A. Performing client authentication
B. Performing server authentication
C. Performing host authentication
D. Performing guest authentication

Answer: A

Summary

SSH is a strong method of performing client authentication.

Question 244

A failure-resistant disk system:

A. Enables continuous monitoring of system parts and alerting of their failure
B. Enables continuous monitoring of system parts and auditing of their failure
C. Enables continuous monitoring of system parts and chaining of their failure
D. Enables continuous monitoring of system parts and clearing of their failure

Answer: A

Summary

One feature of a failure-resistant disk system (FRDS) is that it enables the continuous monitoring of system parts and alerting in case of their failure.

Question 245

What?s the difference between a bridge and a router?

A. A bridge connects multiple networks; a router examines packets to determine which network to forward them to.
B. Bridge and router are synonyms for equipment used to join two networks.
C. A bridge is a specific type of router used to connect a LAN to the global Internet.
D. A bridge works at the Link layer; a router works at the Network layer.

Answer: D

Summary

A bridge connects two networks at the Link layer; a router connects two networks at the Network layer.
