**1.** What does it mean if someone says they were a victim of a Bluejacking attack?

**A.** An unsolicited message was sent.

**B.** A cell phone was cloned.

**C.** An IM channel introduced a worm.

**D.** Traffic was analyzed.

**2.** How does TKIP provide more protection for WLAN environments?

**A.** It uses the AES algorithm.

**B.** It decreases the IV size and uses the AES algorithm.

**C.** It adds more keying material.

**D.** It uses MAC and IP filtering.

**3.** Which of the following is not a characteristic of the IEEE 802.11a standard?

**A.** It works in the 5GHz range.

**B.** It uses the OFMD spread spectrum technology.

**C.** It provides 52 Mbps in bandwidth.

**D.** It covers a smaller distance than 802.11b.

**4.** What can be used to compromise and defeat callback security?

**A.** Passive wiretapping

**B.** Call forwarding

**C.** Packet spoofing

**D.** A brute force attack

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

**A.** A screened host

**B.** A screened subnet

**C.** A NAT gateway

**D.** A two-tiered DMZ

**6.** Why are switched infrastructures safer environments than routed networks?

**A.** It is more difficult to sniff traffic since the computers have virtual private

connections.

**B.** They are just as unsafe as nonswitched environments.

**C.** The data link encryption does not permit wiretapping.

**D.** Switches are more intelligent than bridges and implement security

mechanisms.

**7.** What functionality hangs up on a remote caller and looks at a table of

predefined valid phone numbers?

**A.** Caller ID

**B.** RAS

**C.** Callback

**D.** NOS

**8.** Which of the following protocols is considered connection-oriented?

**A.** IP

**B.** ICMP

**C.** UDP

**D.** TCP

**9.** 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.

**10.** Which of the following proxies cannot make access decisions on protocol

commands?

**A.** Application

**B.** Packet filtering

**C.** Circuit

**D.** Stateful

**11.** 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

**12.** Which protocol is commonly used to authenticate users on dial-up

connections?

**A.** PPTP

**B.** IPSec

**C.** CHAP

**D.** L2F

**13.** Which of the following shows the sequence of layers as layer 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

**14.** What is another name for a VPN?

**A.** Transport session

**B.** Tunnel

**C.** End-to-end connection

**D.** Bandwidth

**15.** 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 very difficult.

**16.** Why are mainframe environments considered more secure than LAN

environments?

**A.** They usually 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.

**17.** What does it mean when computers communicate logically and physically

with each other?

**A.** They speak physically through headers and trailers and logically through

physical 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.

**18.** How does data encapsulation and the protocol stack work?

**A.** Each protocol or service at each layer in the OSI model multiplexes other

packets to the data as they are passed down the protocol stack.

**B.** Each protocol or service at each layer in the OSI model adds its own

information to the data as they are 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.

**19.** 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 internationally accepted 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.

**20.** Which of the following protocols work 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

**21.** What is the purpose of the presentation layer?

**A.** Addressing and routing

**B.** Data syntax and formatting

**C.** End-to-end connection

**D.** Framing

**22.** What is the purpose of the data link layer?

**A.** End-to-end connection

**B.** Dialog control

**C.** Framing

**D.** Data syntax

**23.** What takes place at the session layer?

**A.** Dialog control

**B.** Routing

**C.** Packet sequencing

**D.** Addressing

**24.** At what layer does a bridge work?

**A.** Session

**B.** Network

**C.** Transport

**D.** Data link

**25.** Which best describes the IP protocol?

**A.** A connectionless protocol that deals with dialog establishment,

maintenance, and destruction

**B.** A connectionless protocol that deals with the addressing and routing of

packets

**C.** A connection-oriented protocol that deals with the addressing and routing

of packets

**D.** A connection-oriented protocol that deals with sequencing, error

detection, and flow control

**Answers**

**1. A.** Bluejacking occurs 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. Often, the Bluejacker is trying

to send someone else their business card, which will be added to the victim’s

contact list in their address book.

**2. C.** The TKIP protocol actually works with WEP by feeding it keying material,

which is data to be used for generating random keystreams. TKIP increases

the IV size, ensures it is random for each packet, and adds the sender’s MAC

address to the keying material.

**3. C.** The IEEE standard 802.11a uses the OFDM spread spectrum technology,

works in the 5GHz frequency band, and provides bandwidth of up to 54 Mbps.

**4. B.** 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.

**CISSP All-in-One Exam Guide**

656

**5. C.** The other answers describe basic firewall architectures, meaning where

they can be placed within an environment. Network address translation

(NAT) maps public addresses to private addresses and does not provide traffic

monitoring capabilities. Some firewalls provide NAT services, but the goals of

the services are different.

**6. A.** 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 purely bridges and routers.

**7. C.** The goal of a callback system is to provide another layer of authentication.

For an attacker to compromise this setup successfully and obtain unauthorized

access, she would need to be at the preconfigured phone number or

reconfigure the telephone company’s equipment to forward the call to her.

**8. D.** TCP is the only connection-oriented protocol listed. A connection-oriented

protocol provides reliable connectivity and data transmission, while a

connectionless protocol provides unreliable connections and does not promise

or ensure data transmission.

**9. B.** Ethernet is a very “chatty” protocol because it allows all systems to hear

each other’s broadcasts, and the technology has many collisions because all

systems have to share the same medium.

**10. C.** Application and circuit are the only types of proxy-based firewall solutions

listed here. The others do not use proxies. Circuit-based proxy firewalls

make decisions based on header information, not the protocol’s command

structure. Application-based proxies are the only ones that understand this

level of granularity about the individual protocols.

**11. B.** 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.

**12. C.** The other protocols listed are used for tunneling and/or VPN connectivity,

not user authentication. CHAP uses the challenge-response method of

authenticating a user.

**13. A.** 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).

**14. B.** A VPN sets up a private and secure tunnel by encapsulating and encrypting

data. This allows data to be safely transmitted over untrusted networks.

**15. D.** It is difficult to tap into a fiber line, and fiber does not radiate signals as

other cable types do.

**Chapter 7: Telecommunications and Network Security**

657

**16. A.** This is a relative and general statement. Mainframes are more closed

systems and work in more closed environments compared to the distributed

environments we work in today. Mainframes usually have a smaller number

of entry points, which are generally very controlled.

**17. D.** 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 any

other protocols, devices, and cables are involved. Protocols, services, and

applications communicate logically, and this communication is transmitted

over physical means.

**18. B.** Data encapsulation means 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

layers, or protocol stack, of a system, each protocol involved adds its own

instructions. This process is reversed at the destination.

**19. C.** 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.

**20. C.** Different protocols have different functionalities. The OSI model is an

attempt to describe conceptually where these different functionalities take

place in a networking stack. The model attempts to draw boxes around

reality to help people better understand the stack. Each layer has a specific

functionality and has several different protocols that can live at that layer and

carry out that specific functionality.

**21. B.** No protocols work at the presentation layer, but services that carry out data

formatting, compression/decompression, and encryption/decryption processes

do occur at that layer. Putting data into a standardized format allows for a large

subset of applications to be able to understand and interpret it.

**22. C.** The data link layer, in most cases, is the only layer that understands the

environment in which the system is working, whether it be Ethernet, Token

Ring, wireless, or a connection to a WAN link. This layer adds the necessary

headers and trailers to the frame. Other systems on the same type of network

using the same technology understand only the specific header and trailer

format used in their data link technology.

**23. A.** 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 track of the dialog.

**CISSP All-in-One Exam Guide**

658

**24. D.** A bridge will read header information only 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.

**25. B.** 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.