Module 2 Assessment (Basic Networking 3rd)

Due Oct 1 at 11:59pm **Points** 20 **Questions** 18
Available Sep 18 at 12am - Oct 2 at 11:59pm **Time Limit** 45 Minutes
Allowed Attempts 2

Instructions

You have two attempts to take this assessment with the highest score being retained. The assessment has a time limit of 45 minutes.

Suggestion: take the assessment in the beginning of the module and then after the reading and assignments are done. You can then use the results of both to gauge your learning and retention.

Take the Quiz Again

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	37 minutes	12 out of 20 *

* Some questions not yet graded

Answers will be shown after your last attempt

Score for this attempt: **12** out of 20 *
Submitted Sep 28 at 10:20pm
This attempt took 37 minutes.

Question 1

1 / 1 pts

An organization wants to provide protection against sniffing attacks. Of the following choices, what is the easiest traffic to intercept with a sniffer?

○ Coaxial cable

○ Twisted pair cable

○ Fiber-optic cable

● Wireless

PTS: 1

RATIONALE: D is correct. Wireless transmissions are the easiest to intercept because they are transmitted over the air. A, B, and C are incorrect. The other methods require the attacker to have physical access to the network and splice into a cable. Fiber-optic cable is the most difficult to splice.

Incorrect

Question 2

0 / 1 pts

Public IP addresses are used on the Internet and private IP address should be used within an internal network. Which of the following is a private IP address.

○ 11.1.80.4

○ 175.16.5.2

○ 192.168.3.7

● 192.168.7.5

PTS: 1
RATIONALE: c is correct. Addresses starting with 193 are public IP addresses used on the Internet. A, B, and C are incorrect. Private IP addresses are designated in RFC 1918 and in the following ranges: 10.0.0.0 through 10.255.255.255, 172.16.0.0 through 172.31.255.255, and 192.168.0.0 through 192.168.255.255.

Incorrect

Question 3

0 / 1 pts

An organization wants to host a web server that will be available to uses in a partner company, but not to any Internet users. Where should this server be located?

● A DMZ

○ An intranet

○ The Internet

○ An extranet

PTS: 1
RATIONALE: D is correct. An extranet is a network used to host resources via the Internet but only to trusted entities. B, C, and D are incorrect. If placed directly on the Internet or in a demilitarized zone (DMZ), the server will be available to all users via the Internet. If placed on the intranet, it won’t be accessible to any users outside the organization.

Incorrect

Question 4

0 / 1 pts

An organization is configuring a wireless network. The organization wants to configure wireless security using WPA2 Enterprise mode. What is required to support this choice?

● Preshared keys

○ An 802.1X authentication server

○ AES support

○ TKIP support

PTS: 1
RATIONALE: B is correct. Wi-Fi Protected Access 2 (WPA2) Enterprise mode requires an 802.1X authentication server. A, C, and D are incorrect. WPA2 Personal mode uses preshared keys. Advanced Encryption Standard (AES) and Temporal Key Integrity Protocol (TKIP) provide encryption, but both WPA2 Personal and WPA2 Enterprise modes can use AES and TKIP.

Question 5

1 / 1 pts

An organization wants to host a web server that will be available to any users via the Internet but also want to provide that server with some level of security. Where should this server be located?

● A DMZ

○ An intranet

○ The Internet

○ An extranet

PTS: 1
RATIONALE: A is correct. Internet facing servers such as a web server should be placed in a perimeter network, or demilitarized zone (DMZ). B, C, and D are incorrect. If placed on the intranet, the server won’t be accessible via the Internet. If placed directly on the Internet, it won’t have any security protection. An extranet hosts resources via the Internet, but only to trusted entities.

Question 6

1 / 1 pts

Wireless security can be increased by adding authentication. Which of the following choices provides strong wireless security with authentication?

○ WEP Personal

○ WEP Enterprise

○ WPA2 Personal

● WPA2 Enterprise

PTS: 1
RATIONALE: D is correct. Wi-Fi Protected Access 2 (WPA2) Enterprise uses an 802.1X authentication server to increase wireless security. A, B, and C are incorrect. Wired Equivalent Privacy (WEP) shold not be used because it has been cracked. WPA2 Personal uses a preshared key (PSK) and does not provide authentication.

Question 7

1 / 1 pts

Which one of the following protocols translates private IP addresses to public IP addresses?

○ DNS

● NAT

○ ARP

○ HTTP

PTS: 1
RATIONALE: B is correct. Network Address Translation (NAT) translates private IP addresses to public IP addresses, and public addresses back to private addresses. A, C, and D are incorrect. Domain Name System (DNS) resolves host name to IP addresses. The Address Resolution Protocol (ARP) resolves IP addresses to mead access control (MAC) addresses. HyperText Transfer Protocol (HTTP) is used to send files over the Internet.

Question 8

1 / 1 pts

Which of the following protocols uses a three-way handshake to establish a session?

○ UDP

● TCP

○ TFTP

○ ARP

PTS: 1
RATIONALE: B is correct. Transmission Control Protocol (TCP) uses a three-way handshake to establish a session. A, C, and D are in correct. User Datagram Protocol (UDP) is a connectionless protocol and gives a best-effort attempt to send data. Trivial File Transfer Protocol (TFTP) and Address Resolution Protocol (ARP) both use UDP.

Question 9

1 / 1 pts

An administrator wants to allow SSH traffic through a firewall. What port should be opened?

○ Port 20

○ Port 21

● Port 22

○ Port 23

PTS: 1
RATIONALE: C is correct. Secure Shell (SSH) uses Transmission Control Protocol (TCP) port 22, so by opening port 22 in the firewall, the firewall will allow SSH traffic. A, B, and D are incorrect. File Transfer Protocol (FTP) users TCP port 20 and 21 and Telnet uses TCP port 23.

Question 10

1 / 1 pts

Several protocols are available for wireless security. Of the following, what provides the strongest protection?

○ WEP

○ WPA

● WPA2

○ MAC filtering

PTS: 1
RATIONALE: C is correct. Wi-Fi Protected Access 2 (WPA2) is the strongest of the protocols listed. A, B, and D are incorrect. Wired Equivalent Privacy (WEP) has been deprecated and should not be used. WPA was created as a temporary replacement, and WPA2 is a permanent replacement. Media access control (MAC) filtering can be used, but it is easily broken.

Question 11

1 / 1 pts

Which of the following protocols translate IP address to MAC addresses for delivery on a subnet?

○ DNS

○ NAT

● ARP

○ HTTP

PTS: 1
RATIONALE: C is correct. The Address Resolution Protocol (ARP) resolves IP addresses to media access control (MAC) addresses. The ARP command-line tool can be used to show which addresses have been recently resolved. A, B, and D are incorrect. Domain Name System (DNS) resolves host names to IP addresses. Network Address Translation (NAT) translates private IP addresses to public address, and public back to private. HyperText Transfer Protocol (HTTP) is used to send files over the Internet.

Question 12

1 / 1 pts

Registered Ports are numbered from __________ to __________.

☑ 1,024

□ 0

□ 49,152

□ 65,535

☑ 49,151

☐ 1,023

☐ 1,025

☐ 65,536

Question 13

1 / 1 pts

UDP is a connection oriented protocol that provides guaranteed, reliable communication for devices on a network.

○ True

● False

Incorrect

Question 14

0 / 1 pts

Network topography concepts may include bus, star, token ring, or a combination of each.

○ True

● False

Question 15

1 / 1 pts

Address Resolution Protocol (ARP) resolves IP addresses to Media Access Control (MAC) addresses.

● True

○ False

Question 16

1 / 1 pts

The __________ is the public network accessible around the world.

internet

Question 17

Not yet graded / 2 pts

Identify and describe the purposes of the layers of the OSI model.

Your Answer:

Physical Layer: responsible for the actual physical connection between devices.

Data Link Layer: responsible for creating a reliable link between to connecting nodes in a network.

Network Layer: responsible for routing the data packets to their destinations by determining the best path to take across multiple interconnected networks.

Transport Layer: responsible for the end to end data flow by providing error correction and reassembly of the data for reliable data transmission.

Session Layer: responsible for managing the communication between two devices by establishing and terminating that communication at the proper times.

Presentation Layer: responsible for ensuring that the data sent is in a format that the device receiving it on the other end can understand.

Application Layer: responsible for providing the services that the applications and programs that the user interacts with need in order to function properly.

Question 18

Not yet graded / 2 pts

If you had the funds, what type of network would you build in your home and why?

Your Answer:

I would build a fiberoptic star network. Mostly I would build it for the speed at which the fiberoptic cables could push the data within my home. the only bottleneck would really be when my data left and came into my home network because of having to drop from fiber speeds to standard coaxial cable speeds.

Quiz Score: **12** out of 20