Computer Security Fundamentals 5th edition William Chuck Easttom Solutions Manual

SKU: 9780137984954-SOLUTIONS

Instructor's Manual Materials to Accompany
COMPUTER SECURITY FUNDAMENTALS, 5E

CHAPTER 2
NETWORKS AND THE INTERNET

CHAPTER 2 OBJECTIVES

When students finish reading this chapter, they will be able to:

- Identify each of the major protocols used in network communication (for example, FTP and Telnet) and what use you can make of each of them
- Understand the various connection methods and speeds used on networks
- Compare and contrast various network devices
- Identify and explain various network protocols
- Understand how data is transmitted over a network
- Explain how the Internet works and the use of IP addresses and URLs
- Recount a brief history of the Internet
- Use network utilities such as ping, IPConfig, and tracert
- Describe the OSI model of network communication and the use of MAC addresses

CHAPTER OVERVIEW

This chapter is a high-level summary on networking. It describes the protocols and devices using the OSI model layers. Students should also understand IP addressing and the Internet as a network. This material will be critical in later chapters.

The major sections in this chapter are:

1. **Network Basics.** Examines the basic technologies, protocols, methods, and devices used for networks and the Internet to communicate.
2. **How the Internet Works.** Covers IP addresses, URLs, network packets, and basic communications.
3. **History of the Internet.** Presents the origins of the Internet and further developments that led to its growth.

4. **Basic Network Utilities.** Presents the basic command-line networking utilities: IPConfig, ping, tracert, netstat, nslookup, arp, route, and pathping.

5. **Other Network Devices.** Reviews firewalls and proxy servers in more detail.

6. **Advanced Network Communications Topics.** Covers some extra information that can provide a broader understanding of networking, including the OSI model, the TCP/IP model, and MAC addresses.

7. **Cloud Computing.** Defines cloud computing and covers the primary cloud classifications, common purposes, and security standards.

CHAPTER OUTLINE

I. Network Basics

- The Physical Connection: Local Networks
- Faster Connection Speeds
- Wireless
- Bluetooth
- Other Wireless Protocols
- Data Transmission

II. How the Internet Works

- IP Addresses
- Uniform Resource Locators
- What Is a Packet?
- Basic Communications

III. History of the Internet

IV. Basic Network Utilities

- IPConfig
- Ping
- Tracert
- Netstat

NSLookup

ARP

Route

PathPing

V. Other Network Devices

VI. Advanced Network Communications Topics

The OSI Model

The TCP/IP Model

Media Access Control (MAC) Addresses

VII. Cloud Computing

KEY TERMS

802.11 The IEEE standard that governs wireless Ethernet, or Wi-Fi.

ARP Address Resolution Protocol, used to map IP addresses to MAC addresses.

Backbones The central Internet connections to which Internet Service Providers must ultimately connect.

Bluetooth A short-range wireless communication standard used primarily to connect wireless peripherals to computing devices using the 2.4GHz to 2.485GHz frequency.

Client errors Errors that occur on the client side rather than the server side.

Cloud computing A computing model that enables convenient, on-demand network access to a shared pool of computing resources.

Domain Name System (DNS) A protocol that translates names, such as www.pearson.com, into an IP address.

Firewall A device or software that provides a barrier between your machine or network and the rest of the world.

Hub A device for connecting computers.

IEEE Institute of Electrical and Electronics Engineers, an organization that publishes standards for technology.

Internet Protocol Security (IPSec) A protocol critical for securing virtual private networks.

Internet Service Provider (ISP) A company that provides Internet access for clients.

IPv4 address A numerical designation for a computer consisting of four 1-byte binary numbers.

IPConfig A utility that provides extensive information about a computer's network connection.

MAC address The physical address of a network card. It is a 6-byte hexadecimal number. The first 3 bytes define the vendor.

netstat A command that tells what connections a computer currently has.

Network Access Points (NAP) Places where you can connect to a network. This often refers to wireless network connectivity points.

Network interface card (NIC) A device that provides connectivity to a network.

nslookup A command that is used to connect with a network's DNS server or verify that it is running.

OSI model A seven-layer model describing network connectivity, devices, and protocols.

Packet A binary piece of data prepared for transmission over a network.

pathping A command that provides detailed information regarding latency at hops between source and destination.

ping To send a single ICMP packet to a destination, usually to confirm that the destination can be reached.

Port A numerical designation for a connection point on a computer. There are well-defined ports for specific protocols, such as FTP port 21, HTTP port 80, and so on.

Protocol An agreed-upon method of communication in networking.

Proxy server A device that hides internal IP addresses and presents a single IP address to the outside world.

Repeater A device used to boost signal.

route A command used to view the IP routing table.

Router A device that connects two networks.

Server errors Errors that occur on the server side rather than the client side.

Subnetting Chopping up a network into smaller portions.

Switch An intelligent hub that can determine where a packet is being sent.

tracert A command that traces the path of a network packet from source to destination.

Transmission Control Protocol/Internet Protocol (TCP/IP) A suite of protocols used for various types of Internet and networking communication.

Uniform Resource Locator (URL) An Internet address, such as www.pearson.com.

WEP Wired Equivalent Privacy, an older, less-secure form of wireless encryption.

WPA Wi-Fi Protected Access, a form of wireless encryption that improves upon WEP and uses Temporal Key Integrity Protocol (TKIP) as a per-packet key.

WPA2: A form of wireless encryption that improves upon WPA and uses Advanced Encryption Standard (AES) as a per-packet key.

TEACHING NOTES

I. Network Basics

Teaching Tip: Bring in a cable, hub, switch, or router. Show students how easy it is to hook up PCs to these devices. Demonstrate the difficulty to tell the difference between the three devices on the outside. Explain that a hub broadcasts all the network traffic to all ports.

Teaching Tip: Explain that TCP and IP are only two layers of the OSI model. However, TCP/IP is a collection of protocols, two of which are TCP and IP. IP is the network layer, responsible for IP addresses and moving the packet to the correct computer. TCP can guarantee delivery at the cost of overhead. ICMP is the "traffic cop", ensuring the data flow is OK.

II. How the Internet Works

Teaching Tip: Discuss IP addresses and review the differences between IP version 4 (IPv4) and IP version 6 (IPv6). Have students manually convert numbers between binary and decimal, and then for comparison, use the calculator app in Windows.

III. History of the Internet

Teaching Tip: Explain the origins of the Internet and how its roots can be traced to the Cold War. Discuss the major developments that further advanced the Internet and the organizations that were involved. Review the beginnings of HTTP, HTML, and the World Wide Web.

IV. Basic Network Utilities

Teaching Tip: Demonstrate these utilities in class. IPConfig tells you whether your computer is configured correctly. Ping is a great way to tell whether you are actually connected to a computer. Tracert helps to track where there may be a bottleneck or breakdown in the network. Beware that tracert and ping traffic may be blocked at corporate firewalls. Also review the netstat, nslookup, ARP, route, and pathping utilities. Discuss when you would use each of the utilities.

Teaching Tip: Demonstrate ping of 127.0.0.1 as a way to test whether TCP/IP is running on your local computer.

V. Other Network Devices

Teaching Tip: Emphasize to students that firewalls can be complex devices. Some can filter only by protocol, IP addresses, and port numbers. Others can detect potential attacks at the application level and block them. Proxy servers not only show one face (one IP address) to the Internet for protection of LAN IP addresses, but they also buffer web page information, cutting down on Internet traffic.

VI. Advanced Network Communications Topics

Teaching Tip: Explain that the data link, network, and application layers of the OSI model have different addressing (MAC, IP, and URL). As the computer goes through the layers, the URL becomes an IP address, which needs to end up with a MAC address using DNS and ARP.

Teaching Tip: Ask what would happen if two houses had the same street address. How do you avoid having two NICs with identical MAC addresses? Each vendor has a code that is the first part of a MAC address, with the second part being like a serial number. In that way, no two NICs have the same address.

VII. Cloud Computing

Teaching Tip: Discuss common uses for cloud computing and review the three primary classifications of clouds—public, private, and community. Also, discuss a few of the common purposes of cloud computing, such as software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS), and provide specific examples of each.

DISCUSSION QUESTIONS AND WEB PROJECTS

I. **Discussion Questions**

A. Discussion Question 1

Should all hubs be replaced with switches?

Answer: Students' answers may vary. There should be a discussion of cost versus security; a hub is inexpensive but broadcasts all network traffic to all ports.

B. Discussion Question 2

If you were building your home, what cables would you install?

Answer: Students' answers may vary. The issues are cost, transmission speed, and security. See whether any students come up with "wireless" for an answer.

II. **Web Projects**

A. Web Project 1

Search online for your state's building code to find out which type of Cat cable is to be used in new residential and commercial installations.

Answer: This project will further students' understanding of cable types. A discussion of the answers they find should include possible reasons for the state's decision and whether students agree with the state building code.

B. Web Project 2

Go to http://www.faqs.org/docs/linux_network/x-087-2-iface.ifconfig.html to find out what the "if" in "ifconfig" stands for. How is it different from ipconfig? Where is it used?

Answer: This project furthers students' understanding of this network utility. Students should find answers to the questions asked; the discussion could include Linux in general.

C. Web Project 3

There is talk of the ability of IPv6 saving the Internet from the shortcomings of IPv4. Search online for "IPv5." What happened to this version of IP?

Answer: This project provides more in-depth research into Internet protocols. Students should find the answer to the question asked. They might compare and contrast the different IP versions and find out the reasons for revising IP.

WEB RESOURCES

- http://www.freesoft.org/CIE/Topics/75.htm Freesoft.org, an Internet Encyclopedia; *Domain Name Service DNS* topic

- http://www.faqs.org/docs/linux_network/x-087-2-iface.html Linux Network Administrator's Guide; Chapter 5: Configuring TCP/IP Networking

CHAPTER REVIEW/ANSWERS TO TEST YOUR SKILLS

Multiple Choice

1. Malek is purchasing cable to use in setting up small office networks. He wants to stock up on commonly used cable. What type of cable do most networks use?

   D

2. You are assigned to attach connectors to segments of cable. What type of connector is used with network cables?

   D

3. What type of cable is used in most networks?

   A

4. John is trying to simply connect three computers in a small network. He does not need any sort of routing capability and is not concerned about network traffic. What is the simplest device for connecting computers?

   C

5. Sharice is trying to teach a new technician basic networking terms. What should she tell this new technician NIC stands for?

A

6. Which of the following is a device used to connect two or more networks?

B

7. Juan has just installed a new T1 line into a doctor's office. The doctor's front desk receptionist has asked what speed they can expect. A T1 line sends data at what speed?

B

8. Which of the following best describes polycloud?

D

9. What protocol translates web addresses into IP addresses?

A

10. What protocol is used to send email, and on what port does it work?

C

11. Gunther is setting up encrypted remote communications so that the server administrators can remotely access servers. What protocol is used for remotely logging on to a computer in a secure manner?

A

12. Mohammed needs to open a firewall port so that web traffic can be passed through the firewall. What protocol is used for web pages, and on which port does it work?

B

13. What is the name for the point where the backbones of the Internet connect?

C

14. You are examining a list of IP addresses. Some are internal, some are external, and some are not valid. Which of the following is not a valid IP address?

B

15. What class of address is the IP address 193.44.34.12?

C

16. The IP address 127.0.0.1 always refers to your what?

C

17. Internet addresses of the form www.chuckeasttom.com are called what?

B

18. Which U.S. government agency created the distributed network that formed the basis for the Internet?

A

19. Which of the following was one of the three universities involved in the original distributed network set up by a government agency?

A

20. You are explaining the history of networking to a group of first-year students. What did Vint Cerf invent?

C

21. You are explaining the history of networking to a group of first-year students. What did Tim Berners-Lee invent?

A

22. John is working with command-line utilities to gather diagnostic information about a computer that cannot connect to the network. Which utility provides information about a machine's network configuration?

B

23. Sheryl is explaining the OSI model to new technicians at her company. She is trying to explain what protocols operate at the various layers of the OSI model. At what layer of the OSI model does TCP operate?

A

24. Which layer of the OSI model is divided into two sublayers?

A

25. Which of the following is a unique hexadecimal number that identifies your network card?

B

Exercises

EXERCISE 2.1: USING IPCONFIG

Note if the students effectively use the utility; if so, then they have successfully grasped the concept. In this exercise, students should list their computer's IP address, default gateway, and subnet mask.

EXERCISE 2.2: USING TRACERT

As in the previous exercise, note if the students effectively use the utility. In this exercise, students should discuss what hops were taken, what hops are the same, and why some steps were the same for different destinations.

EXERCISE 2.3: NSLOOKUP

The key to this exercise about nslookup is that the student is going beyond merely a cursory description of what the protocol does. See if the student discusses its history, application, or technical nuances.

EXERCISE 2.4: MORE ABOUT IPCONFIG AND EXERCISE 2.5: MORE ABOUT PING

Exercises 2.4 and 2.5 are both procedural. If the students are able to use the utilities and the options described with success, they have also successfully completed the exercises.

Projects

PROJECT 2.1: LEARNING ABOUT DNS

The key to this project is to go beyond student's knowledge of basic DNS functionality. The goal for each student is to be able to describe how and why this protocol was developed, who devised it, and when it was invented. Furthermore, the student should be able to explain which problem it was designed to solve.

PROJECT 2.2: LEARNING ABOUT YOUR SYSTEM

This exercise is about the student's ability to make good equipment choices. In almost all cases, a switch is preferred to a hub.

PROJECT 2.3: LEARNING ABOUT NETSTAT

This project asks the students to interpret the information they get from netstat. Students should go beyond simply reporting on what the utility displays. This project is successfully completed when students make accurate assumptions about the network based on the information they get from this utility.