Chapter 02 – TCP/IP Concepts Review

Notes

Overview

This chapter describes major concepts and aspects of the TCP/IP protocol, including each of the four layers of the protocol stack: Application, Transport, Internet, and Network. You will also review the IP addressing schemes and how they relate to TCP/IP protocol and security. Finally, the chapter ends with a discussion of three numbering systems commonly used with TCP/IP: binary, octal, and hexadecimal. You will learn how to convert from one system to other.

Chapter Objectives

After reading this chapter and completing the exercises, you will be able to:

- Explain the TCP/IP protocol stack
- Explain the basic concepts of IP addressing
- Explain the binary, octal, and hexadecimal numbering systems

Tips

Overview of TCP/IP

1. The role of a protocol when two or more computers attempt to communicate with each other.

2. The Transmission Control Protocol/Internet Protocol (TCP/IP) is the most widely used computer communication protocol.

3. See Figure 2-1 for the TCP/IP stack and its four layers. We will explain each layer (except the Network layer) later:
    a. Application
    b. Transport
    c. Internet
    d. Network

Tip	Consider the TCP/IP stack with the OSI Model stack, which is composed of seven layers: Physical, Data Link, Network, Session, Transport, Presentation, and Application. For more information about the OSI Model, check out http://www.webopedia.com/quick_ref/OSI_Layers.asp.

The Application Layer

1. The Application-layer protocols is the front end to the lower-layer protocols of the TCP/IP stack.

2. See Table 2-1 for the different programs that run at the Application layer.

The Transport Layer

1. The Transport layer is where data is encapsulated into segments. These segments are then sent using either TCP or UDP protocols.

2. TCP is a connection-oriented protocol, which means the sender does not send any data to the destination node until the destination node acknowledges that it is listening to the sender.

3. The TCP three-way handshake process:
    a. Host A sends a TCP packet with the SYN flag set (that is, a SYN packet) to Host B.
    b. After receiving the packet, Host B sends Host A its own SYN packet with an ACK flag (a SYN-ACK packet) set.
    c. In response to the SYN-ACK packet from Host B, Host A sends Host B a TCP packet with the ACK flag set (an ACK packet).

TCP Segment Headers

1. As a security professional, it is important to clearly understand the critical components of a TCP header. Hackers usually try to exploit these components to discover vulnerabilities and perform attacks. Critical components include:
    a. TCP flags
    b. Initial sequence number (ISN)
    c. Source and destination port numbers

TCP Flags

1. Flags occupy one bit of the segment and can be set to either 0 (off) or 1 (on).

2. Understand the six flags used by the TCP segment header:
    a. *SYN*: synch flag
    b. *ACK*: acknowledgment flag
    c. *PSH*: push flag
    d. *URG*: urgent flag
    e. *RST*: reset flag
    f. *FIN*: finish flag

Initial Sequence Number (ISN)

1. ISN is a 32-bit number that tracks packets received by the node and allows reassembling of large packets that have been broken up into smaller packets.

2. Understand how two hosts exchange their ISNs during Steps one and two of the TCP three-way handshake.

Tip	Kevin Mitnick, the well-known hacker, is now a security consultant to corporations worldwide and a cofounder of Defensive Thinking. Find out more about him at https://www.mitnicksecurity.com/.

TCP Ports

1. A TCP packet has two 16-bit fields containing the source and destination port numbers.

2. A port is the logical, not physical component, of a TCP connection. The port identifies the service that is running.

3. Ports also help network administrators to stop or disable services that are not needed. As a network administrator or security professional, you should be familiar with ports and control their use. Open ports are invitations for potential attacks.

4. Port numbers can go up to 65,535 but only the first 1023 ports are considered well-known. Check *www.iana.org* for a list of well-known ports.

5. Some of the most important or frequently used ports and the services they represent include
    a. Ports 20 and 21 for FTP
    b. Port 25 for SMTP
    c. Port 53 for DNS
    d. Port 69 for TFTP
    e. Port 80 for HTTP
    f. Port 443 for HTTPS
    g. Port 110 for POP3
    h. Port 119 for NNTP
    i. Port 135 for RPC
    j. Port 139 for NetBIOS
    k. Port 143 for IMAP4

Tip	Read about these services and play around with them. Although this is not a network course, it is important for you to become familiar with all these ports.

User Datagram Protocol (UDP)

1. UDP is a fast but unreliable protocol that also operates on the Transport layer of the TCP/IP stack. UDP is unreliable because it does not verify whether the receiver is listening or ready to receive. This is the reason why UDP is also known as a connectionless protocol.

2. Although unreliable, UDP is widely used on the Internet because of its speed. Higher layers of the TCP/IP stack are responsible for providing reliability.

The Internet Layer

1. The Internet layer is responsible for routing packets to their destination using a logical addressing scheme, called IP addressing. Like UDP, IP addressing packet delivery is connectionless.

2. Understand the Internet Control Message Protocol (ICMP) and the major commands that help network administrators troubleshoot network connectivity problems, including:
    a. Ping
    b. Traceroute

3. See Table 2-2 for the ICMP type codes that can be used by network administrators and security professionals to block ICMP packets from entering or leaving the network. Several attacks can be avoided by blocking ICMP traffic.

Tip	Read about the Ping of Death attack at: http://www.webopedia.com/TERM/P/ping_of_death.html.

IP Addressing

1. Addressing uses IP addresses. IP addresses are divided into two components: the network address and the host address. Depending on how many bytes are used for each component, IP addresses can be divided into classes:
   a. Class A
   b. Class B
   c. Class C

2. See Table 2-3 for the differences between these three classes.

3. The main characteristics of a Class A address:
   a. First byte is reserved for the network address.
   b. Last three bytes are for the host computers.
   c. Supports more than 16 million hosts.
   d. Limited number of Class A addresses.
   e. Reserved for large corporations and governments.
   f. Format: *network.node.node.node*

4. The main characteristics of a Class B address:
   a. Addresses are divided evenly between a two-octet network address and a two-octet host address.
   b. Supports more than 65,000 host computers.
   c. Assigned to large corporations and Internet Service Providers (ISPs).
   d. Format: *network.network.node.node*

5. The main characteristics of a Class C address:
   a. Addresses have a three-octet network address and a one-octet host address.
   b. More than two million Class C addresses.
   c. Each address supports up to 254 host computers.
   d. Usually available for small business and home networks.
   e. Format: *network.network.network.node*

Tip	There are also Class D and E IP addresses. Read more about their characteristics at http://computer.howstuffworks.com/question549.htm.

6. The concept of subnetting, where a network administrator can divide a larger network into smaller network segments.

7. Understand the process of using a subnet mask to determine the network address portion and the host address portion of an IP address.

CIDR Notation

1. Classless Inter-Domain Routing (CIDR) was developed in 1993 and helped prolong the life of IPv4 by allowing for more efficient IP-assignment space.
2. See Table 2-4 for the list of important CIDR prefixes.

Planning IP Address Assignments

1. Understand the process of assigning a network address to each network segment. You must be familiar with this process in order to understand how packets reach destination networks.

2. The process of sending a packet to a different network using a gateway. When a packet is sent by a computer, TCP/IP uses the sender's subnet mask to determine the destination computer's network address. If the destination network address is different, the sending computer sends the packet to the address specified by the gateway. Next, the gateway forwards this packet to its next destination. This process goes on until the packet reaches its destination network.

IPv6 Addressing

1. IPv4 wasn't designed with security in mind, and many current network vulnerabilities are caused by this oversight.

2. IPv6 was developed to increase the IP address space and provide additional security.

3. IPv6 uses 16 bytes, or a 128-bit address, so 2^{128} addresses are available.

Overview of Numbering Systems

1. A review of the binary, octal, and hexadecimal numbering systems.

Reviewing the Binary Numbering System

1. The decimal numbering system uses 10 as its base. Each number can be represented as the sum of each digit multiplied by a power of 10. So, 3742 represents three thousand seven hundred forty-two and can be computed as follows:
   2 x 1 + 4 x 10 + 7 x 100 + 3 x 1000 = 3742

2. The binary numbering system uses the number 2 as its base. The only numbers supported by this system are 0 and 1. These values are called bits (binary digits). A byte is a group of 8 bits.

4. Review some examples on how to convert binary numbers to decimal numbers.

5. A nibble is a half-byte or a group of four bits. Nibbles help with reading byte values. Any nibble has two components: the low-order nibble and the high-order nibble.

6. The process for converting nibbles to decimal values can be summarized as follows:
   a. Convert the low-order nibble to its decimal representation.
   b. Convert the high-order nibble to its decimal representation and multiply this value by 16.
   c. Add both decimal representations to obtain the final decimal value.

Reviewing the Octal Numbering System

1. The octal numbering system uses the number 8 as its base, so the only digits accepted are 0, 1, 2, 3, 4, 5, 6, and 7. Any octal digit can be represented with three bits.

2. Using the UNIX permission scheme, we can illustrate the use of the octal numbering system. In UNIX, we can specify three sets of permissions over a file or directory: Owner, Group, and Other. Start by assigning permissions for each set using three bits per set. Next, convert each set's permissions into an octal number. For example 111 (base 2) is equivalent to 7 (base 8).

Reviewing the Hexadecimal Numbering System

1. The hexadecimal numbering system uses the number 16 as its base, so the only digits accepted are from 0 to 15. Hexadecimal values consist of two characters. Each character represents a nibble. Observe that letters are used when writing a hexadecimal value. A represents 10, B stands for 11, C is 12, D is 13, E is 14, and F is 15.

2. Understand how to convert hexadecimal values to binary and decimal representations. First, convert each nibble to its binary representation. Then, convert both nibbles to its decimal equivalent.

Reviewing the Base-64 Numbering System

1. A common use for base-64 is for the encoding and transportation of binary files sent through e-mail.

2. See Table 2-5 for how the base-64 numbering system is represented. Review the examples on how to convert a base-64 string into its decimal equivalent.

Additional Resources

1. IP addressing links: http://www.webopedia.com/TERM/I/IP_address.html
2. IP addressing and subnetting for new users: http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a00800a67f5.shtml
3. SMTP links: http://www.webopedia.com/TERM/S/SMTP.html
4. DNS stuff: http://www.dnsstuff.com
5. DNS links: http://www.webopedia.com/TERM/D/DNS.html
6. How Domain Name Servers Work: http://computer.howstuffworks.com/dns.htm
7. SNMP links: http://www.webopedia.com/TERM/S/SNMP.html
8. HTTP links: http://www.webopedia.com/TERM/H/HTTP.html

Key Terms

- **ACK**
- **connection-oriented protocol**
- **connectionless**
- **initial sequence number (ISN)**
- **Internet Assigned Numbers Authority (IANA)**
- **Internet Control Message Protocol (ICMP)**
- **network session hijacking**

- **port**
- **protocol**
- **SYN**
- **SYN-ACK**
- **TCP flag**
- **three-way handshake**
- **Transmission Control Protocol/Internet Protocol (TCP/IP)**
- **User Datagram Protocol (UDP)**
- **ACK**
- **connection-oriented protocol**
- **connectionless**
- **initial sequence number (ISN)**
- **Internet Assigned Numbers Authority (IANA)**
- **Internet Control Message Protocol (ICMP)**
- **network session hijacking**
- **port**
- **protocol**
- **SYN**
- **SYN-ACK**
- **TCP flag**
- **three-way handshake**
- **Transmission Control Protocol/Internet Protocol (TCP/IP)**
- **User Datagram Protocol (UDP)**