Hands-On Ethical Hacking and Network Defense, 3rd Edition

Chapter 2

TCP/IP Concepts Review

Objectives

After completing this chapter, 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

Overview of TCP/IP

- Protocol
  - Language used by computers to communicate
  - Transmission Control Protocol/Internet Protocol (TCP/IP)
    - Most widely used
- TCP/IP stack
  - Four distinct layers
    - Network
    - Internet
    - Transport
    - Application

Overview of TCP/IP

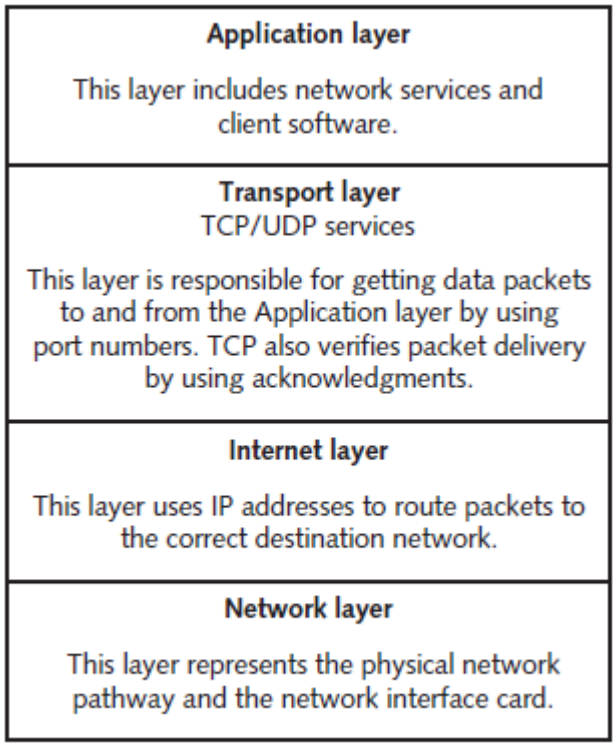


Figure 2-1 The TCP/IP protocol stack

The Application Layer

- Front end to the lower-layer protocols
  - This layer is what you can see and touch

Application	Description
Hypertext Transfer Protocol (HTTP)	The primary protocol used to communicate over the Web (see RFC 2616 at *www.ietf.org* for details)
File Transfer Protocol (FTP)	Allows different OSs to transfer files between one another
Simple Mail Transfer Protocol (SMTP)	The main protocol for transmitting e-mail messages across the Internet
Simple Network Management Protocol (SNMP)	Primarily used to monitor devices on a network, such as monitoring a router's state remotely
Secure Shell (SSH)	Enables users to securely log on to a remote server and issue commands interactively
Internet Relay Chat (IRC)	Enables multiple users to communicate over the Internet in discussion forums
Telnet	Enables users to insecurely log on to a remote server and issue commands interactively

Table 2-1 Application-layer programs

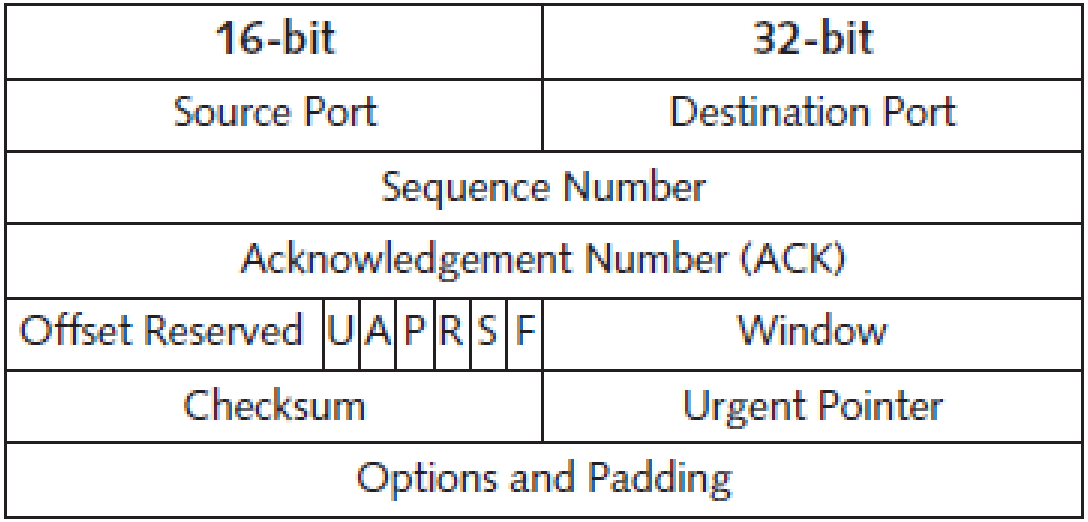
The Transport Layer

- Encapsulates data into segments
  - Use TCP or UDP to reach a destination host
    - TCP is a connection-oriented protocol, which means the sender doesn't send any data to the destination node until the destination acknowledges that it's listening to the sender
- TCP three-way handshake
  - Computer A sends computer B a SYN packet
  - Computer B replies with a SYN-ACK packet
  - Computer A replies with an ACK packet

TCP Segment Headers

- Critical components of a TCP header:
  - TCP flags
  - Initial sequence number (ISN)
  - Source and destination port numbers
- Abused by hackers
  - You need to know hacking basics to protect a network

TCP Segment Headers



16-bit							32-bit
Source Port							Destination Port
Sequence Number							
Acknowledgement Number (ACK)							
Offset Reserved	U	A	P	R	S	F	Window
Checksum							Urgent Pointer
Options and Padding							

Figure 2-2 TCP header diagram

TCP Flags

- Each flag occupies one bit of the TCP segment
  - Can be set to 0 (off) or 1 (on)
- Six TCP segment flags
  - *SYN flag*: synch flag
  - *ACK flag*: acknowledgment flag
  - *PSH flag*: push flag
  - *URG flag*: urgent flag
  - *RST flag*: reset flag
  - *FIN flag*: finish flag

Initial Sequence Number

- ISN is a 32-bit number
  - Tracks packets received by a node
  - Allows reassembly of large packets that have been broken up into smaller packets
  - Sent on steps one and two of TCP three-way handshake
    - Sending node ISN is sent with SYN packet
    - Receiving node ISN is sent back to sending node with SYN-ACK packet

TCP Ports

- TCP packet
  - Two 16-bit fields
    - Contains source and destination port numbers
- Port
  - Logical, not physical, TCP connection component
  - Identifies running service
    - Example: HTTP uses port 80
- Helps you stop or disable unneeded services
  - More running services, more ports open for attack

TCP Ports

- Only the first 1023 ports are considered well-known
  - List of well-known ports
    - Internet Assigned Numbers Authority: *www.iana.org*
- Ports 20 and 21
  - File Transfer Protocol (FTP)
  - Was the standard for moving or copying large files
    - Used today to a lesser extent due to popularity of HTTP
  - Requires a logon name and password
  - More secure than Trivial File Transfer Protocol (TFTP)

TCP Ports

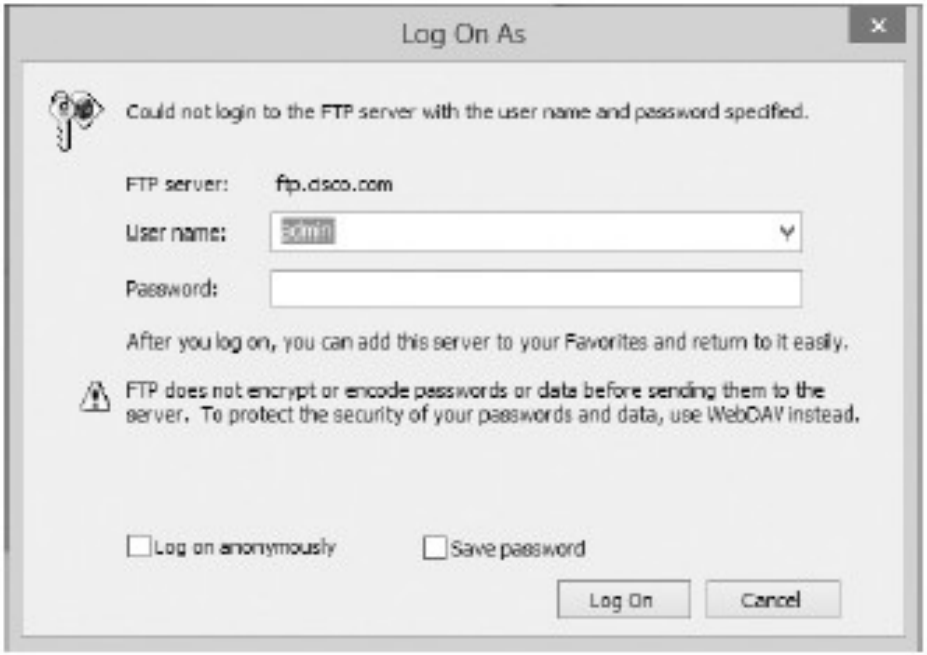


Figure 2-3 Connecting to an FTP site

Source: Microsoft

TCP Ports

- Port 25
  - Simple Mail Transfer Protocol (SMTP)
    - E-mail servers listen on this port
- Port 53
  - Domain Name Service (DNS)
    - Used to connect users to Web sites using URLs instead of IP addresses
- Port 69
  - Trivial File Transfer Protocol
    - Used for transferring router configurations

TCP Ports

- Port 80
  - Hypertext Transfer Protocol (HTTP)
    - Used when connecting to a Web server
- Port 443
  - Secure Hypertext Transfer Protocol
    - Reserved for secure connections to a Web server
- Port 110
  - Post Office Protocol 3 (POP3)
    - Used for retrieving e-mail

TCP Ports

- Port 119
  - Network News Transfer Protocol
    - Used to connect to a news server for use with newsgroups
- Port 135
  - Remote Procedure Call (RPC)
    - Critical for operation of Microsoft Exchange Server and Active Directory
- Port 139
  - NetBIOS
    - Used by Microsoft's NetBIOS Session Service

TCP Ports

- Port 143
  - Internet Message Access Protocol 4 (IMAP4)
    - Used for retrieving e-mail

User Datagram Protocol (UDP)

- Fast but unreliable delivery protocol
  - Operates on Transport layer
  - Used for speed
    - Does not need to verify receiver is listening or ready
    - Depends on higher layers of TCP/IP stack to handle problems
  - Referred to as a connectionless protocol

The Internet Layer

- Routes packets to destination address
  - Uses a logical address (i.e., IP address)
  - IP addressing packet delivery is connectionless
- Internet Control Message Protocol (ICMP)
  - Sends messages related to network operations
  - Helps troubleshoot network connectivity problems
    - `ping` command
  - Tracks the route a packet traverses
    - `traceroute` command

The Internet Layer

ICMP type code	Description
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect
6	Alternate Host Address
8	Echo
9	Router Advertisement
10	Router Solicitation
11	Time Exceeded
12	Parameter Problem
13	Timestamp
14	Timestamp Reply
15	Information Request
16	Information Reply

Table 2-2 ICMP type codes (*continues*)

The Internet Layer

ICMP type code	Description
17	Address Mask Request
18	Address Mask Reply
19	Reserved (for Security)
20–29	Reserved (for Robustness Experiment)
30	Traceroute
31	Datagram Conversion Error
32	Mobile Host Redirect
33	IPv6 Where-Are-You
34	IPv6 I-Am-Here
35	Mobile Registration Request
36	Mobile Registration Reply
37	Domain Name Request
38	Domain Name Reply
39	Skip
40	Photuris
41–255	Reserved

Table 2-2 ICMP type codes (*continued*)

IP Addressing

- Consists of 4 bytes divided into two components
  - Network address
  - Host address
- Classes – based on the starting number of the first byte:
  - Class A
  - Class B
  - Class C

IP Addressing

Address class	Range	Address bytes	Number of networks	Host bytes	Number of hosts
Class A	1–126	1	126	3	16,777,214
Class B	128–191	2	16,128	2	65,534
Class C	192–223	3	2,097,152	1	254

Table 2-3 TCP/IP address classes

IP Addressing

- An IP Address is composed of 4 bytes (an octet)
  - A byte is equal to 8 bits (octet)
  - Sometimes defined as four octets instead of 4 bytes
- Class A
  - First byte is reserved for network address
  - Last three bytes are available for host computers
  - Supports more than 16 million host computers
  - Limited number of Class A networks
    - Reserved for large corporations and governments
  - Format: *network.node.node.node*

IP Addressing

- Class B
  - Divided evenly
    - Two-octet network address
    - Two-octet host address
  - Supports more than 65,000 hosts
    - Assigned to large corporations and Internet Service Providers (ISPs)
  - Format: *network.network.node.node*

IP Addressing

- Class C
  - Three-octet network address and one-octet host address
    - More than two million Class C addresses
  - Supports up to 254 host computers
    - Usually available for small business and home use
  - Format: *network.network.network.node*

IP Addressing

- Subnetting
  - Allows a network administrator to divide large networks into smaller segments (subnets)
  - Subnetting concepts are important
    - For performance and security purposes
- Subnet mask
  - Each network must be assigned a subnet mask
    - Helps distinguish network from host address bits

IP Addressing

- Subnet mask example:
  - The IP address 128.214.018.016 in binary is:
    10000000.11010110.00010010.00010000
  - If the subnet mask is 255.255.255.0, it's expressed in binary as:
    11111111.11111111.11111111.00000000
  - The subnet part of the IP address is:
    10000000.11010110.00010010
  - The host part of the IP address is:
    00010000

CIDR Notation

- Almost all of the world's IPv4 addresses are in use
  - Long-term solution is IPv6 addressing
- Short-term fix was CIDR (Classless Inter-Domain Routing)
  - Allowed more efficient IP-assignment space
- Example:
  - 192.168.1.0/24
  - The number following the "/" is the prefix

CIDR Notation

CIDR prefix	# Class C equivalent	Number of usable hosts
/27	1/8th of a Class C	30 hosts
/26	1/4th of a Class C	62 hosts
/25	1/2 of a Class C	126 hosts
/24	1 Class C	254 hosts
/23	2 Class C	510 hosts
/22	4 Class C	1022 hosts
/21	8 Class C	2046 hosts
/20	16 Class C	4094 hosts
/19	32 Class C	8190 hosts
/18	64 Class C	16,382 hosts
/17	128 Class C	32,766 hosts
/16	1 Class B	65,534 hosts
/15	2 Class B	131,070 hosts

Table 2-4 CIDR addressing

CIDR Notation

CIDR prefix	# Class C equivalent	Number of usable hosts
/14	4 Class B	262,142 hosts
/13	8 Class B	524,286 hosts
/12	16 Class B	1,048,574 hosts
/11	32 Class B	2,097,150 hosts
/10	64 Class B	4,194,302 hosts
/9	128 Class B	8,388,606 hosts
/8	1 Class A	16,777,214 hosts

Table 2-4 CIDR addressing (*continued*)

Planning IP Address Assignments

- Each network segment must have a unique network address
  - Network portion and host portion of an address cannot contain all 0s or all 1s
- Accessing entities and services on other networks
  - Each computer needs IP address of gateway
  - TCP/IP Internet layer uses subnet mask to determine destination computer's network address
    - If addresses are different, relays packet to gateway
    - Gateway forwards packet to its next destination
    - Packet eventually reaches destination

IPv6 Addressing

- Internet Protocol version 6 (IPv6)
  - IPv4 wasn't designed with security in mind
    - Many current network vulnerabilities
  - Developed to increase IP address space and provide additional security
    - Uses 16 bytes, or a 128-bit address
    - 2^{128} available addresses
  - All newer OSs are configured to enable IPv6
    - Many router filtering devices, firewalls, and intrusion detection systems are not
      - Hackers bypass security systems

Overview of Numbering Systems

- As a security professional, knowledge of numbering systems will come into play
  - Binary
  - Octal
  - Hexadecimal

Reviewing the Binary Numbering System

- Uses number 2 as its base
  - Binary digits (bits) represented by 0 or 1
- Byte
  - Group of 8 bits
    - Can represent 2^8 (256) different numbers
- File permissions are represented with bits
  - 1 represents having permission
    - 111 (rwx): all permissions apply
  - 0 removes permission
    - 101 (r-x): user can read and execute but not write

Reviewing the Binary Numbering System

- Example of binary:
  - Learn and memorize the columns for binary

128 64 32 16 8 4 2 1

2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0

  - To determine the value of binary number 01000001

128 64 32 16 8 4 2 1

2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0

0 1 0 0 0 0 0 1

Add the columns containing 1s to convert to a decimal number

64 + 1 = **65**

Understanding Nibbles

- Half a byte or four bits
  - Helps with reading numbers by separating the byte
    - Example: 1111 1010 versus 11111010
- Components
  - High-order nibble: left side
  - Low-order nibble: right side

Understanding Nibbles

- Converting 1010 1010 to decimal
  - Low-order nibble
    - 1010 = 10 (base 10)
  - Multiply high-order nibble by 16
    - 1010 = 10 x 16 = 160 (base 10)
    - 128 + 32 = 160

Reviewing the Octal Numbering System

- Uses 8 as its base
  - Supports values from 0 to 7
- Octal digits can be represented with only three bits
- UNIX permissions
  - Owner permissions (rwx)
  - Group permissions (rwx)
  - Other permissions (rwx)
    - Setting permission (rwxrwxrwx) means they all have read, write, and execute permissions

Reviewing the Hexadecimal Numbering System

- Uses 16 as its base
  - Supports numbers from 0 to 15
- Hex number consists of two characters
  - Each character represents a nibble
  - Value contains alphabetic letters
    - A representing 10 and F representing 15
  - Sometimes expressed with “0x” in front
- Hex number in binary or decimal
  - Convert each nibble to binary
  - Convert binary value to decimal

Reviewing the Base-64 Numbering System

- A common use for base-64
  - The encoding and transportation of binary files sent through e-mail
- All you need to know now:
  - There are a number of ways in which attackers can use base-64 to obfuscate their actions

Reviewing the Base-64 Numbering System

Character or symbol	Representation in base-64
Uppercase A to Z	0–25
Lowercase a to z	26–51
Numerals 0 to 9	52–61
+ and / symbols	62, 63

Table 2-5 Base-64 character mappings

Summary

- TCP/IP
  - Most widely used Internet communication protocol
  - TCP/IP stack consists of four layers
    - Network, Internet, Transport, and Application
- Application layer
  - Front end
- Transport layer
  - Encapsulation
  - Uses UDP or TCP headers
    - TCP is a connection-oriented protocol

Summary

- Critical components of TCP segment headers
  - TCP flags
  - Initial sequence number (ISN)
  - Source and destination ports
- TCP ports
  - Identify running services
- Internet layer
  - Packet routing
- IP addressing
  - Four bytes and three classes (A, B, and C)

Summary

- IPv6 addresses
  - 16 bytes
  - Written in hexadecimal notation
- Binary numbering system
  - Uses 2 as its base
- Octal numbering system
  - Uses 8 as its base
- Hexadecimal numbering system
  - Uses 16 as its base