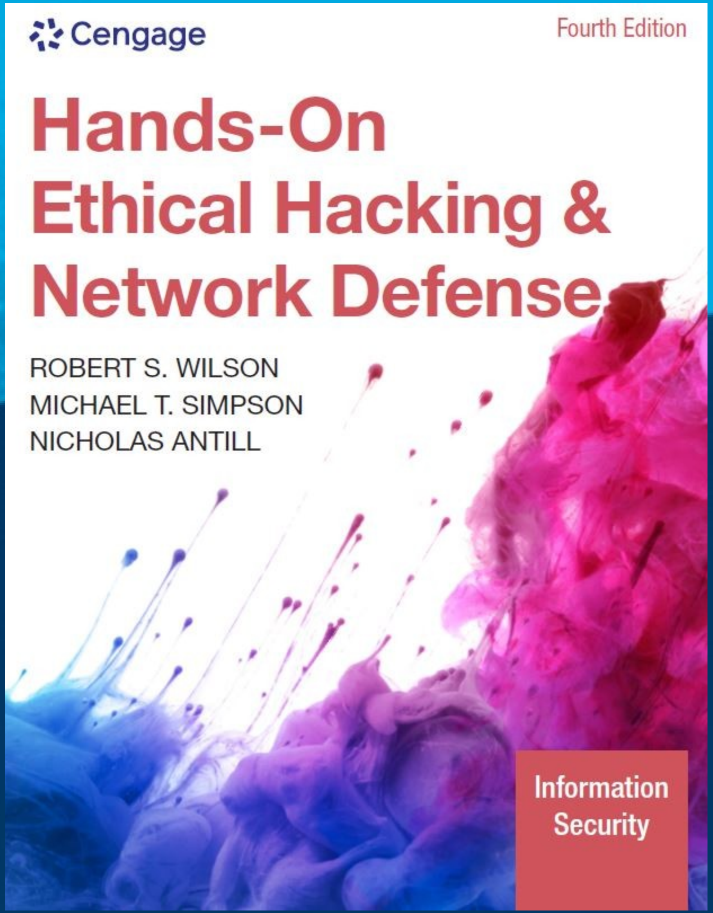


Cengage

Fourth Edition

Hands-On Ethical Hacking & Network Defense

ROBERT S. WILSON
MICHAEL T. SIMPSON
NICHOLAS ANTILL

Information Security

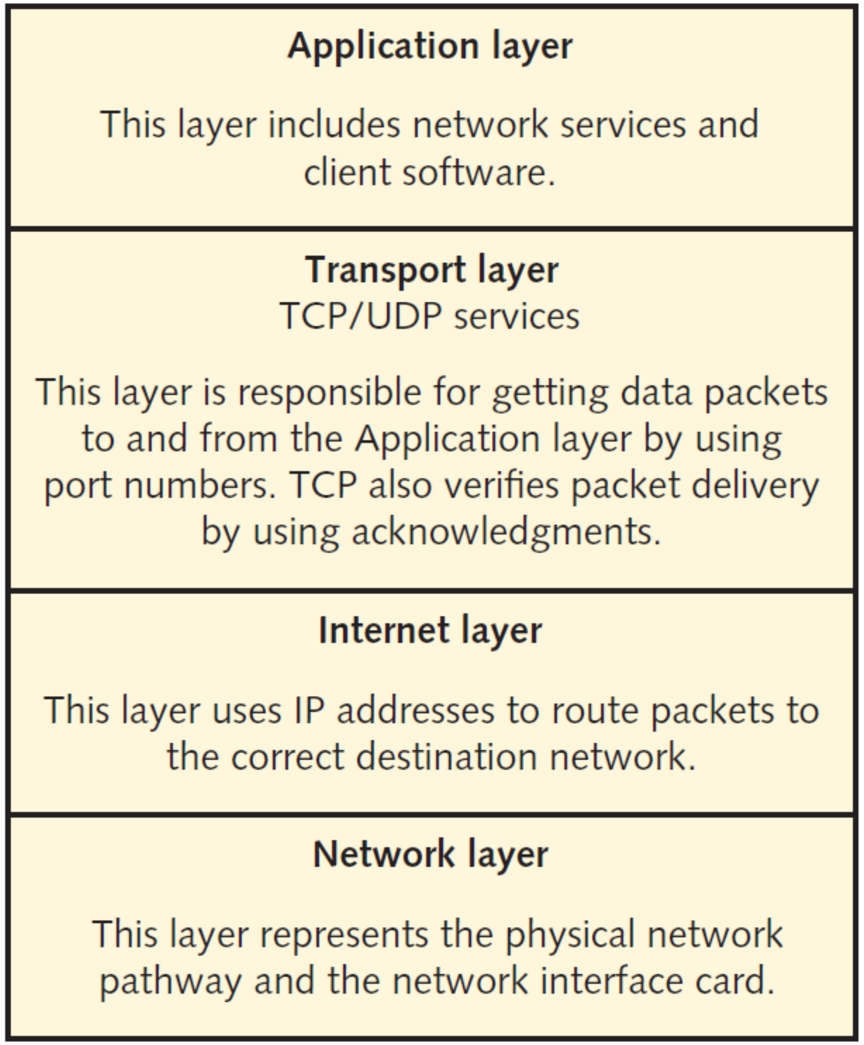
# Hands-On Ethical Hacking and Network Defense, Edition 4

## **Module 2:** TCP/IP Concepts Review

# Overview of TCP/IP (1 of 2)

- **Protocol**
  - Language used by computers to communicate with one another over the Internet or across an office
  - **Transmission Control Protocol/Internet Protocol (TCP/IP)**
    - Most widely used
- TCP/IP stack: Combination of two protocols (TCP and IP)
  - Four distinct layers
    - Network
    - Internet
    - Transport
    - Application

# Overview of TCP/IP (2 of 2)



**Application layer**

This layer includes network services and client software.

**Transport layer**

TCP/UDP services

This layer is responsible for getting data packets to and from the Application layer by using port numbers. TCP also verifies packet delivery by using acknowledgments.

**Internet layer**

This layer uses IP addresses to route packets to the correct destination network.

**Network layer**

This layer represents the physical network pathway and the network interface card.

**Figure 2-1** The TCP/IP protocol stack

# The Application Layer

- Protocols are the front end to the lower-layer protocols in the TCP/IP stack
  - This layer is what you can see and touch

# Application-Layer Programs

| Application | Description |
|---|---|
| Hypertext Transfer Protocol Secure (HTTPS) | The primary protocol used to communicate over the web (see RFC 2818 at www.ietf.org for details) |
| File Transfer Protocol (FTP) | Allows different operating systems (OSs) to transfer files between one another |
| Simple Mail Transfer Protocol (SMTP) | The main protocol for transmitting email 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 |

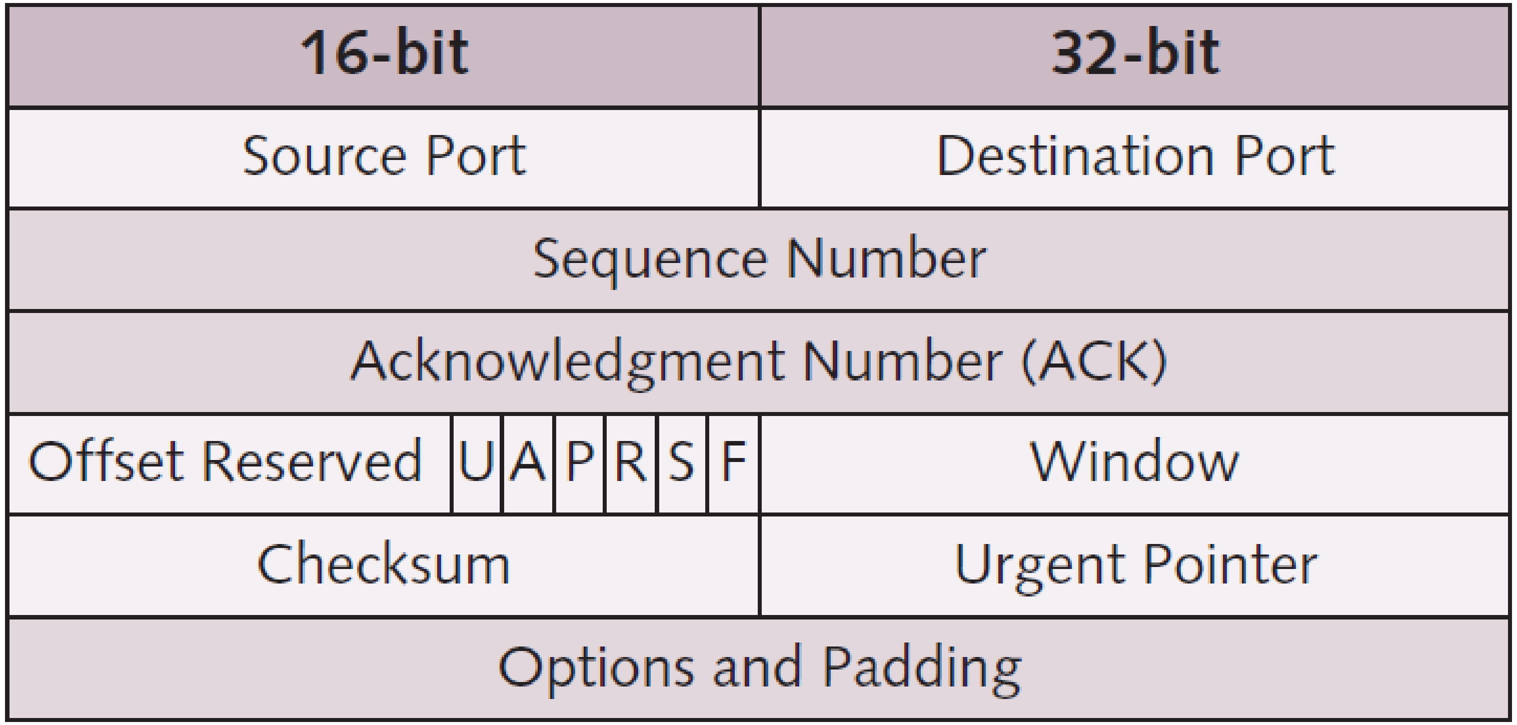
# The Transport Layer

- Encapsulates data into segments
  - Segments can 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 node acknowledges that it’s listening to the sender
- TCP **three-way handshake** example
  - Computer A sends computer B a **SYN** (synchronize) packet
  - Computer B replies with a **SYN-ACK** packet set
  - Computer A replies with an **ACK** (acknowledgement) packet

# TCP Segment Headers (1 of 2)

- Critical components of a TCP header:
  - TCP flags
  - Initial sequence number (ISN)
  - Source and destination port numbers
- Abused by hackers
  - To protect a network, you need to know the basic methods of hacking into networks

# TCP Segment Headers (2 of 2)



| 16-bit | 32-bit |
|---|---|
| Source Port | Destination Port |
| Sequence Number | |
| Acknowledgment 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 flags of a TCP segment
  - *SYN flag*: Synchronize flag signifies the beginning of a session
  - *ACK flag*: Acknowledgment flag acknowledges a connection
  - *PSH flag*: Push flag is used to deliver data directly to an application
  - *URG flag*: Urgent flag signifies urgent data
  - *RST flag*: Reset flag resets or drops a connection
  - *FIN flag*: Finish flag signifies that the connection is finished

# 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
  - ISN is sent through steps one and two of TCP three-way handshake
    - Sending node ISN is sent with SYN packet
    - Receiving node ISN is sent back to the sending node with SYN-ACK packet

# TCP Ports (1 of 8)

- TCP packet
  - Has two 16-bit fields
    - Contains source and destination port numbers
- **Port**
  - Logical, not physical, component of a TCP connection
  - Can be assigned to a process that requires network connectivity
  - Example: The HTTPS service uses port 443 by default
- Helps you stop or disable unnecessary services
  - The more services running on a server, the more ports are open for a potential attack

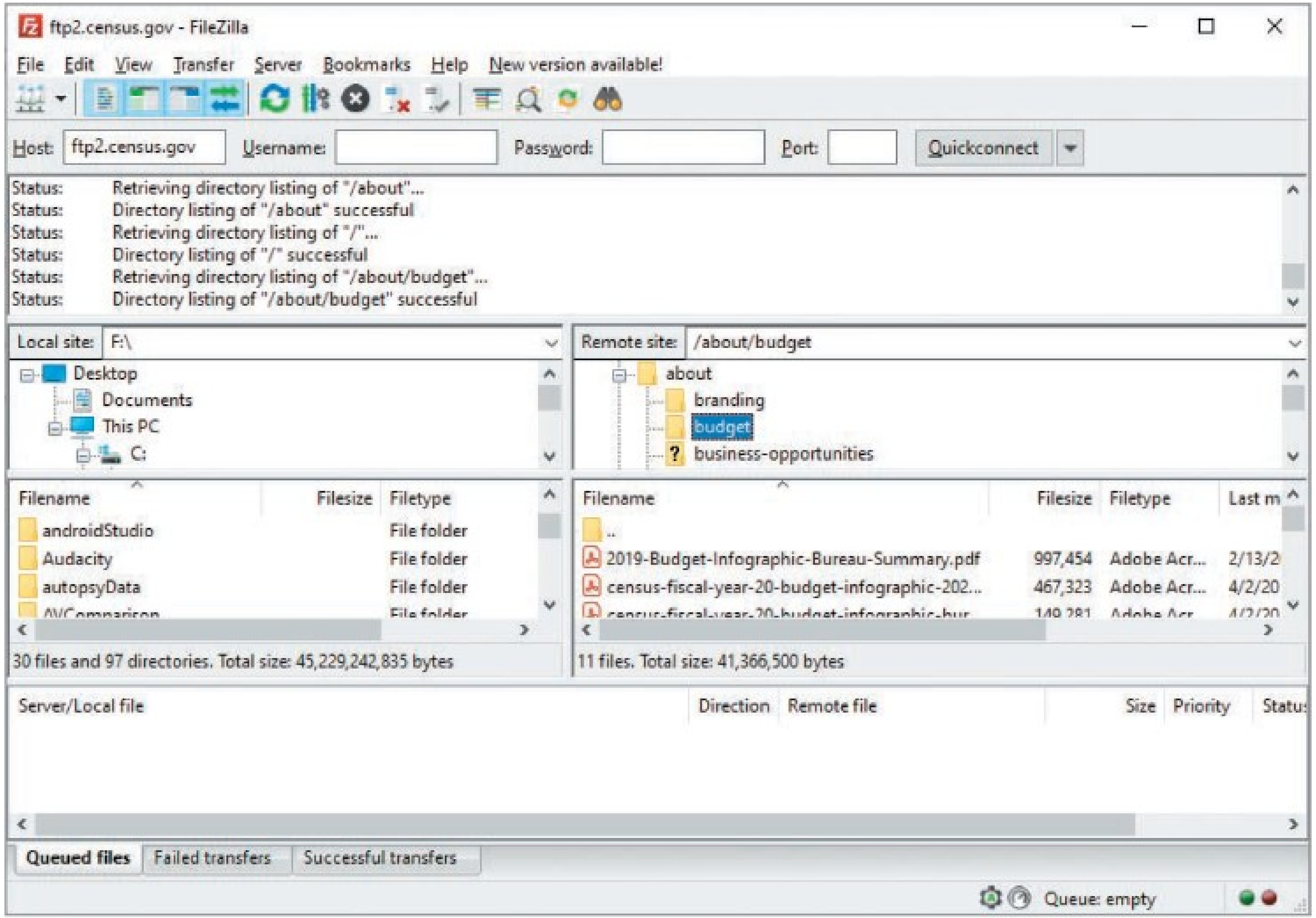
# TCP Ports (2 of 8)

- Only 1023 ports are considered well known
  - List of well-known ports
    - Visit the **Internet Assigned Numbers Authority (IANA)**: 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 because of the popularity of HTTP
  - Requires a logon name and password
  - More secure than Trivial File Transfer Protocol (TFTP)

# TCP Ports (3 of 8)

- Port 22
  - Secure Shell (SSH)
  - Uses encryption and authentication
    - To create a secure channel over an unsecure network
  - Used to secure logons, file transfers, and port forwarding
  - FTP using SSH is known as SFTP
- Port 25
  - Simple Mail Transfer Protocol (SMTP)
    - Email servers listen on this port

# TCP Ports (4 of 8)



Host: ftp2.census.gov Username: Password: Port:

```
Status:     Retrieving directory listing of "/about"...
Status:     Directory listing of "/about" successful
Status:     Retrieving directory listing of "/"...
Status:     Directory listing of "/" successful
Status:     Retrieving directory listing of "/about/budget"...
Status:     Directory listing of "/about/budget" successful
```

Local site: F:\

- Desktop
  - Documents
  - This PC
    - C:

Remote site: /about/budget

- about
  - branding
  - budget
  - business-opportunities

| Filename | Filesize | Filetype |
|---|---|---|
| androidStudio | | File folder |
| Audacity | | File folder |
| autopsyData | | File folder |
| AVComparison | | File folder |

30 files and 97 directories. Total size: 45,229,242,835 bytes

| Filename | Filesize | Filetype | Last m |
|---|---|---|---|
| .. | | | |
| 2019-Budget-Infographic-Bureau-Summary.pdf | 997,454 | Adobe Acr... | 2/13/2 |
| census-fiscal-year-20-budget-infographic-202... | 467,323 | Adobe Acr... | 4/2/20 |
| census-fiscal-year-20-budget-infographic-bur... | 149,281 | Adobe Acr... | 4/2/20 |

11 files. Total size: 41,366,500 bytes

| Server/Local file | Direction | Remote file | Size | Priority | Status |
|---|---|---|---|---|---|

**Figure 2-3** Connecting to an FTP site

# TCP Ports (5 of 8)

- Port 53
  - Domain Name System (DNS)
    - Used to connect users to websites using URLs instead of IP addresses
    - Most networks require a DNS server
- Port 69
  - Trivial File Transfer Protocol
    - Used for transferring router and backup router configurations
- Port 80
  - Hypertext Transfer Protocol (HTTP)
    - Used when connecting to a web server

# TCP Ports (6 of 8)

- Port 143
  - IMAP
  - Used by email clients to retrieve email messages from a mail server over a TCP/IP connection
- Port 443
  - Secure Hypertext Transfer Protocol
    - Used when you connect to a web server
    - Typically, reserved for secure connections
- Port 993
  - IMAP over SSL/TLS uses port 993
  - Preferred over the unsecured version IMAP, which uses port 143

# TCP Ports (7 of 8)

- Port 110
  - Post Office Protocol 3 (POP3)
    - Used for retrieving email messages from a mail server
- Port 119
  - Network News Transfer Protocol
    - Used to connect to a news server for use with newsgroups

# TCP Ports (8 of 8)

- 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 to share resources
- Port 143
  - Internet Message Access Protocol 4
    - IMAP4 uses this port to retrieve email

# User Datagram Protocol (UDP)

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

# The Internet Layer

- Routes packets to a 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 network professionals to troubleshoot network connectivity problems
    - `ping` command
  - Tracks the route a packet traverses from a source IP address to a destination IP address
    - `traceroute` command

# ICMP Type Codes (1 of 3)

| 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 |

# ICMP Type Codes (2 of 3)

| ICMP type code | Description |
|---|---|
| 15 | Information Request |
| 16 | Information Reply |
| 17 | Address Mask Request |
| 18 | Address Mask Reply |
| 19 | Reserved (for Security) |
| 20 to 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 |

# ICMP Type Codes (3 of 3)

| ICMP type code | Description |
|---|---|
| 36 | Mobile Registration Reply |
| 37 | Domain Name Request |
| 38 | Domain Name Reply |
| 39 | Skip |
| 40 | Photuris |
| 41 to 255 | Reserved |

# IP Addressing (1 of 5)

- An IPv4 address consists of 4 bytes divided into two components:
  - Network address
  - Host address
- IP addresses can be classified into three classes based on the starting decimal number of the first byte:
  - Class A
  - Class B
  - Class C

# TCP/IP Address Classes

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

# IP Addressing (2 of 5)

- An IP address is composed of 4 bytes (an octet)
  - A byte is equal to 8 bits (octet)
  - Sometimes, an IP address is defined as four octets instead of 4 bytes
- Class A
  - The first byte of a Class A address is reserved for the network address
    - Makes the last three bytes available to assign to host computers
  - Supports more than 16 million host computers
  - Limited number of Class A addresses
    - Reserved for large corporations and governments
  - Format: *network.node.node.node*

# IP Addressing (3 of 5)

- Class B
  - Divided evenly between a two-octet network address and a 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 (4 of 5)

- Class C
  - Three-octet network address and one-octet host address
    - Resulting in more than two million Class C addresses
  - Each address supports up to 254 host computers
    - Usually available for small businesses and home use
  - Format: *network.network.network.node*
- Subnetting
  - Allows a network administrator to divide large networks into smaller segments (subnets)
  - Subnetting concepts are important
    - For performance and security purposes

# IP Addressing (5 of 5)

- Subnet mask
  - Each network must be assigned a subnet mask
    - Helps distinguish the network address bits from the host address bits
- 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 for more efficient IP-assignment space
- Example:
  - 192.168.1.0/24
  - The number following the “/” is the prefix

# CIDR Addressing (1 of 2)

| 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 |

# CIDR Addressing (2 of 2)

| 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 |

# Planning IP Address Assignments

- Each network segment that's separated by a router must have a unique IP address
  - Network portion and host portion of an IP address cannot contain all 0s or all 1s
- Accessing entities and services on other networks
  - Each computer must have the IP address of its gateway
  - TCP/IP Internet layer uses subnet mask to determine destination computer's network address before sending a packet to another computer
    - If the address is different from the sending computer's network address, the sending computer relays the packet to the IP address specified in the gateway parameter
    - Gateway computer then forwards the packet to its next destination
    - The packet eventually reaches the destination

# IPv6 Addressing

- Internet Protocol version 6 (IPv6)
  - IPv4 wasn’t designed with security in mind
    - Has caused 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
  - Security testers should be aware that all newer OSs are configured to enable IPv6
    - Some router-filtering devices, firewalls, and intrusion detection systems are not
      - ○ Hackers can bypass these 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 (1 of 2)

- Binary numbering system uses 2 as its base
  - Each binary digit (bit) is represented by a 0 or 1
- Byte
  - Contains 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 the file but not write to it

# Reviewing the Binary Numbering System (2 of 2)

- Example of determining binary values:
  - Learn and memorize the columns for binary numbers
    - From right to left, these numbers represent increasing powers of two

|  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|
| 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 (1 of 2)

- Nibble: Half a byte or 4 bits
  - Helps with reading numbers by separating the byte
    - Example: 1111 1010 versus 11111010
- Components
  - High-order nibble: 4 bits on the left
  - Low-order nibble: 4 bits on the right

# Understanding Nibbles (2 of 2)

- 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 (1 of 2)

- Uses 8 as its base
  - Written by using these eight values: 0, 1, 2, 3, 4, 5, 6, and 7
- Octal digits can be represented with only 3 bits
  - The number 7 is written as 00000111
- 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 Octal Numbering System (2 of 2)

- Changing permissions with the `chmod` Command
  - `chmod` command: Allows altering the permissions of files and directories in Unix and Linux systems
  - Used to change permissions in two ways
    - To provide the permissions as an octal number
    - Allows targeting specific permission sets (owner, group, or other) and turning individual read, write, or execute permissions on or off
      - Need to specify who you are setting permissions for, what change are you making (adding or removing the permission), and which permission you are setting

# Reviewing the Hexadecimal Numbering System

- Hexadecimal: A base-16 numbering system
  - Valid numbers range from 0 to 15
- Hex number consists of two characters
  - Each character represents a nibble
  - Value contains alphabetic letters
    - Example: A represents the number 10 and F represents 15
  - Hex numbers are sometimes expressed with “0×” in front of them
    - You multiply the value in each column by the value of the column to determine hex numbers
  - Converting a hex number to binary
    - Write each nibble from left to right

# Reviewing the Base-64 Numbering System

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

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