CHAPTER 9

Understanding Networks and Network Security

Introduction

Before we discuss network vulnerabilities and threats, we should understand why such threats exist. In order to understand this, we need to know the basics of computer communication and networking. In this chapter, we will be discussing the basics of computer networking, Open System Interconnection (OSI), and Transmission Control Protocol/Internet Protocol (TCP/IP) models, and types of networking vulnerabilities that exist and then explore the relevant vulnerabilities and threats.

Networking Fundamentals

A network connects two or more computers to communicate with each other or for the exchange of information among the systems. Networking is sharing of the resources within a network.

In basic communication, there are three components involved: the sender, the receiver, and the media. In the case of two people communicating with each other face to face, within a short distance, the media could be just air. As shown in Figure 9-1, communication is completed only when the sender and receiver understand each other and are able to comprehend the information. In order to comprehend the information that is being exchanged between the sender and the receiver, the communication "protocol" could be common "language." **Protocol** is a set of rules defined by the communication channel in order to comprehend the information that is being exchanged and in normal human communication, it is a common language understood by both the parties.

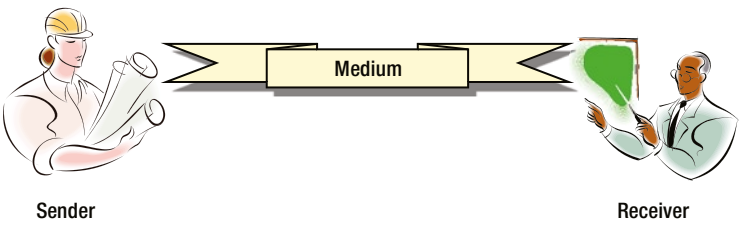

Figure 9-1. *Basic communication*

Let's say that the sender understands a different language and the receiver understands a different language. For discussion's sake, let's say the sender understands French and the receiver understands German. Assume that both have to exchange information, the media is Facsimile (FAX) in France and Telegraph in Germany. This communication has increased the complexity as both sender and receiver do not have a common language and there is no common media. The communication needs translators who understand both the languages or two translators – one who understands the sender's language (e.g., French) and another common language (e.g., English), another who understands a common language (e.g., English) and the receiver's language (e.g., German). These translators translate to the senders and receivers. A media translator transfers facsimile information on to the telegraphic information and vice versa.

As shown in the Figure 9-2, this type of communication is called layered communication. Through the different layer, communication is achieved, each layer has a specific task, and tasks are broken down into simple and specific tasks. Though both sender and receiver do not have a common language, they are still able to interoperate with the help of layered communication.

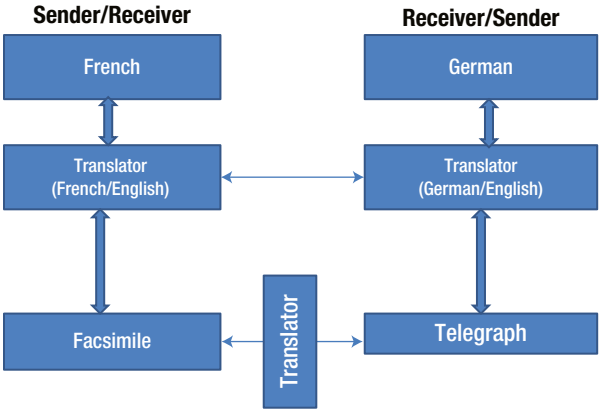

Figure 9-2. *Layered Communication*

Computer Communication

In the case of data communication, computer devices are connected logically to each other and data is transmitted from one computer system to another or from one device to another device as shown in Figure 9-3. A **network** connects two or more computers to communicate with each other or for the exchange of information among the systems. **Networking** is sharing of resources within the network. Data communication and computer networking go hand in hand. Data communication is the exchange of information across a medium and networking is connecting two devices to facilitate the exchange of information from one system to another in a connected network. When computer devices are connected in a network for communication, it consists of the following components: Message, Host, Receiver, Medium, and Protocol. When these network components (the host, receiver, medium, protocol, and other devices) are connected with each other, physically or logically, the primary consideration is whether the systems are able to communicate effectively with each other. Use of appropriate systems or network components with deployment of appropriate protocols ensures effective communication among the systems.

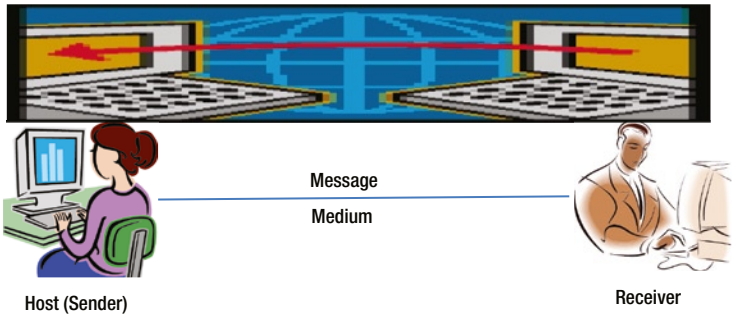

Figure 9-3. *Computer communication*

The network components are:

- **Message** is the information one computer system is sending to another.
- **Host** is the sender of message.
- **Receiver** is one who is receiving the information.
- **Medium** is the channel of communication. It can be copper wire, optical fiber, or wireless.
- **Protocol** is the set of rules in order for two systems to communicate.

Network and its Components

Network "topology" refers to the layout of the network. Topology defines the method of placing different nodes in a network and how the data is getting transferred between these nodes. It can be physical topology or logical topology. In physical topology, there is emphasis on the physical layout of the network whereas logical topology focuses on the transfer of data among the devices.

The common physical topologies that are used are:

- **Bus Topology:** In BUS topology, devices are connected in a series as shown in Figure 9-4. In this topology, all the devices are connected sequentially to the same line (as shown in the figure). This is a simple and low-cost solution but the failure of any single device or damage to the medium can bring down the entire network.

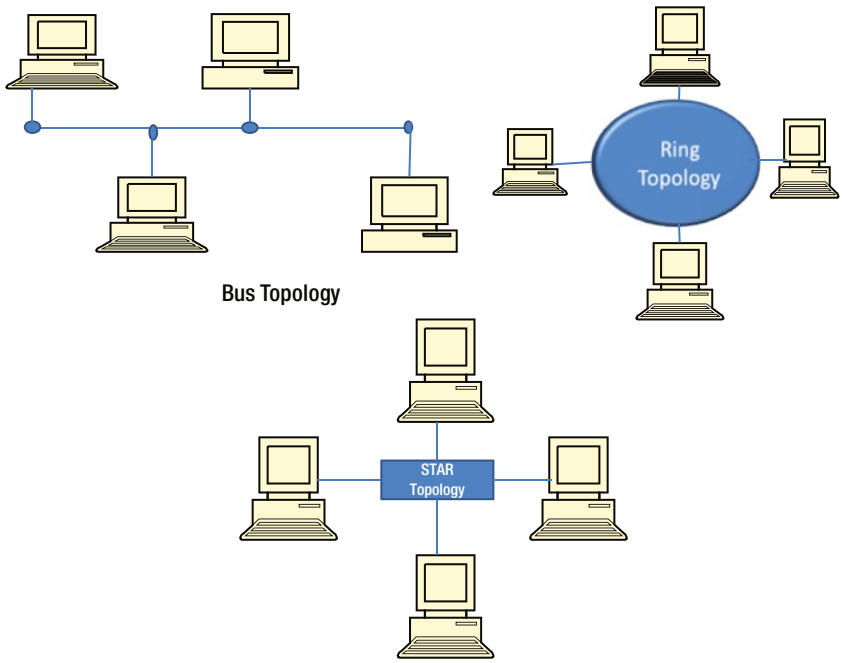

Figure 9-4. *Network Topologies*

- **Ring Topology:** All the devices are connected sequentially in the form of a ring (as shown in Figure 9-4). This topology is similar to the linear bus except that the ring ends at the start of the node. The disadvantage of the ring topology is, if any one of the devices breaks, the entire ring breaks.
- **Star or Y Topology:** All the devices are connected through a central hub (as shown in Figure 9-4). Unlike in the previous topologies, failure of a single device does not necessarily bring down the entire network unless the central hub device is down. This is the most popular topology currently deployed by many organizations because it is simple to build, connect, and it is simple to add and remove devices to/from the network.

Networks can be broadly categorized into:

- **Local Area Network (LAN):** A Local Area Network is a network that is confined to a relatively small geographical area such as a school or an office building and occasionally a group of nearby buildings. LAN connects a relatively small number of systems within the same organization. The most common LAN protocol is Ethernet.
- **Wide Area Network (WAN):** Wide Area Network (WAN) connects two or more LANs which are geographically apart. For example, an organization may have two different offices in two different places or countries and they are connected together to form a WAN. WAN connections comprises of several devices including multiplexers, bridges, and routers. WAN link can be a private dedicated link or a public link.
- **Metropolitan Area Network (MAN):** Metropolitan Area Networks (MAN) is a network of connected systems within the same metropolitan city. A MAN is larger than a LAN but smaller than a WAN. For practical reasons, a MAN is optimized for a large geographical area, and can connect two types of networks – LAN and WAN.

- **Internetworking:** As your organization grows, the networking requirement also changes. What started as one network (LAN) can connect to multiple LANs which are spread across the same geographical area or across different geographical areas. This is called as an internetwork – collection of individual networks. **Internetworking** refers to the connecting of networks of different protocols and procedures, and devices (as shown in Figure 9-5) so that they still can share information.

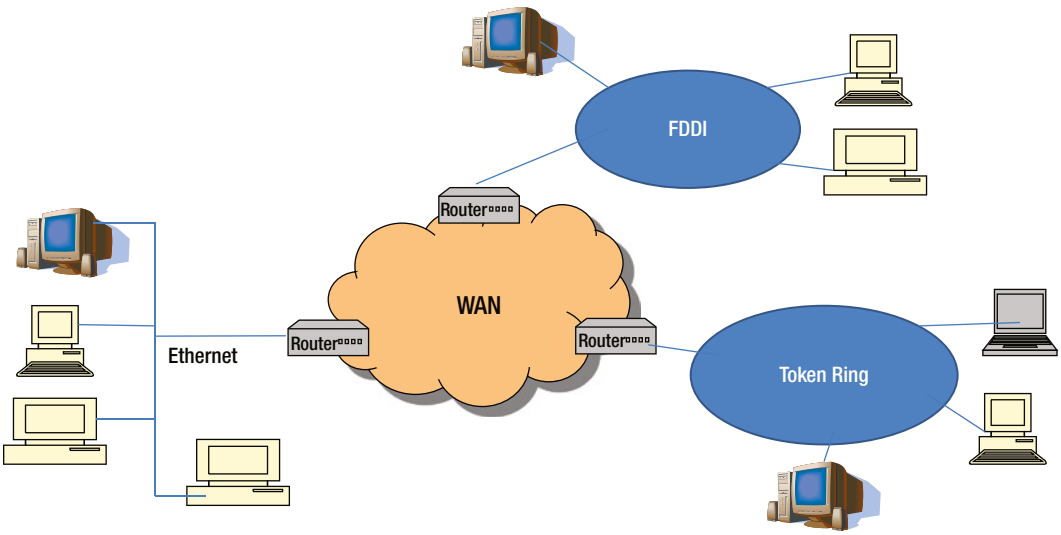

Figure 9-5. *Internetworking*

Network Protocols

A protocol, in computer communications terms, is a set of rules that governs the communication between two or more computers connected on a network. It is a common language for different vendor devices to talk to each other on a network.

In order to meet the challenges of multi-vendor devices on a network and to break the complexity of computer communications, there are two types of networking models that are developed based on the layered protocol approach. These models are the OSI and the TCP/IP. OSI is a seven-layer model whereas TCP/IP is a four-layer model which overlaps several layers of OSI functionality.

OSI (Open Systems Interconnection) Reference Model

ISO, the International Organization for Standardization,[1] is a global body of representatives from over 150 countries. The ISO is a nongovernmental organization that bridges the gap between the government, public, and private organizations. In 1982, the ISO and the International Telecommunication Union Standardization Sector (ITU-T)[2] developed a vendor-neutral, Open Systems Interconnection (OSI) protocol for devices communicating in a multi-vendor network environment. The OSI reference model divides the complex computer communication into seven distinct layers, with each layer having its own specific functions and protocols.

You may be wondering why the acronyms and name are not matching. Here is the explanation as described by ISO – "Because 'International Organization for Standardization' would have different acronyms in different languages (IOS in English, OIN in French for *Organisation internationale de normalisation*), our founders decided to give it the

short form ISO. ISO is derived from the Greek isos, meaning equal. Whatever the country, whatever the language, the short form of our name is always ISO."[4]

Each of the seven layers is responsible for a particular function of data communication. For example, one layer may be responsible for routing the data between devices, while another layer may be responsible for establishing connection between the devices. The upper layers focus on presenting information to the user at the application level whereas the lower layers focus on transporting the information across the network without any data loss. Each layer is functionally independent of the other layers. In the OSI reference model, each of the layers extends services to the layer directly above it and is given services from the layer directly below it. Hence all the seven layers together bring about the communication between the devices in a network. Figure 9-6 describes the seven layers, and the functions that are performed by each layer.

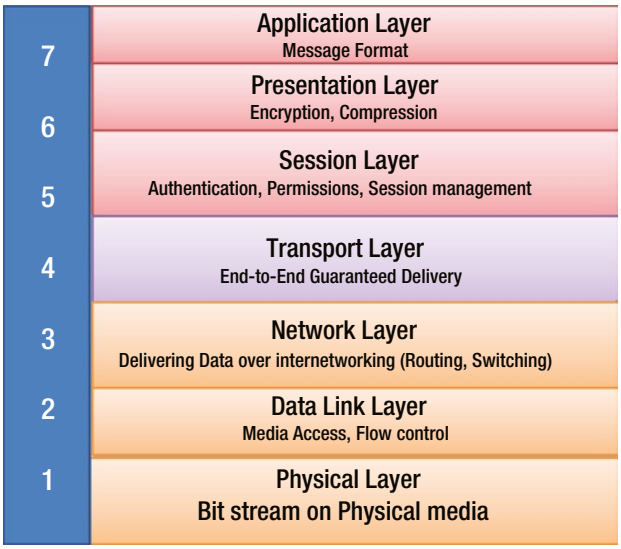

Figure 9-6. *OSI Seven Layer Reference Model*

The layers are described in the following section[2]:

- **Layer 7: Application Layer:** The Application layer has the responsibility of providing application services to the network applications such as e-mail, web, remote connection, file transfers, and database access. Some of the other functions that are performed at this layer include user authentication and data encryption. Application examples include *WWW browsers, Hypertext Transfer Protocol (HTTP), Simple Network Management Protocol (SNMP), Telnet, File Transfer Protocol (FTP), Domain Name System (DNS), Internet Message Access Control (ICMP),* and *Dynamic Host Configuration Protocol (DHCP).*
- **Layer 6: Presentation Layer:** This layer is responsible for presenting the data to the upper layers. This layer transforms the data into a required format that can be accepted by the applications in the application layer. For example, some Web browsers accept jpeg, some accept gif, some accept ASCII, and so on. This layer also manages techniques such as data compression and data encryption. Examples include *ASCII, EBCDIC, TIFF, GIF, PICT, JPEG, MPEG,* and *MIDI.*

- **Layer 5: Session Layer:** This layer manages the establishment, the usage, and the ending of the connections/sessions between the devices. This layer performs the function of establishing sessions between the devices, how long the sessions should be, which side will transmit, when to transmit and how long to transmit. Examples include RPC, SQL, and NetBios.
- **Layer 4: Transport Layer:** This layer's responsibility is to ensure that the delivery of data from one end point to another indeed gets completed without any errors. This layer implements error checking, recovery of lost packets to ensure the completeness of data transfer and flow control. Some examples include Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Sequenced Packet Exchange (SPX).
- **Layer 3: Network Layer:** This layer is responsible for routing of the data within the network. It is responsible for finding the shortest path from source to destination and route the packet through the intermediate devices such as router(s) or switch(es). Examples include Internet Protocol (IP), Internetwork Packet Exchange (IPX), and AppleTalk.
- **Layer 2: Data Link Layer:** This layer consists of two layers: Media Access Control (MAC) and Logical Link Layer (LLC). The Media Access Control Layer is responsible for taking the packets from the above layers and putting them onto the media in the form of bits. The media can be copper (wired), optical fiber, or wireless. LLC connects to the upper network layer. The function of the LLC layer is to control the frame synchronization, flow control of data, and error checking of the frames (Cyclic Redundancy Check). Examples include *IEEE 802.5/ 802.2, IEEE 802.3/802.2, Frame Relay, Asynchronous Transfer Mode (ATM),* and *Integrated Services Digital Network (ISDN).*
- **Layer 1: Physical Layer:** This layer is responsible for transmitting bits (0s and 1s) from one device to another device over a physical media. The media could be wire, wireless, or optical fiber. Both the Data Link layer and the Physical Layer functions are implemented at the hardware level attached to the computer as a peripheral device known as the Network Interface Card (NIC).

TCP/IP Model

The Department of Defense (DOD), as a part of research project, developed the ARPAnet protocol to connect devices in a network of networks (the "Internet"). Modification of this protocol for the public is what we know today as TCP/IP – Transmission Control Protocol (TCP) and Internet Protocol (IP). TCP/IP is made up of the following four layers:

- **Application Layer:** This layer combines the Application, Presentation, and Session layer functionalities of the OSI reference model. The function of this layer is to hand over the data received from the bottom layer to the application and to make sure the application is able to interpret the data that it has received from the other network device.
- **Transmission Control Protocol (TCP) Layer:** The function of this layer is to deliver data from the client to the server without errors or loss. Data can be lost during the transmission but TCP ensures that the data is not lost and triggers retransmission process until the data is correctly and completely received by the destination device. This layer overlaps the functionality of Transport Layer of OSI reference model. In this layer, the data received from the application is broken down into smaller "chunks" called segments.
- **Internet Protocol (IP) Layer:** This layer is responsible for moving the data from one node to another node. IP forwards the segments received from the TCP, referred to as packets, to the destination based on the IP address. This layer's function is very similar to the Network Layer function of the OSI reference model and implements various routing protocols such as Remote Imaging Protocol (RIP), Open Shortest Path First (OSPF), and Border Gateway Protocol (BGP).

- **Network Access Layer:** It combines the functions of the Data Link and the Physical Layers of the OSI reference model. The Network Access layer is responsible for creating data 'frames' for transmitting and receiving data from the physical layer. This function is implemented by a hardware and software Network Interface Card (NIC), an adapter connected to the computer through physical wires or optical fiber cables. There are several protocols implemented in this layer: Ethernet, Gigabit Ethernet, ATM, ISDN, and frame relay. It can support copper or optical interface.

Figure 9-7 illustrates the relationship between the OSI seven layers and TCP/IP.

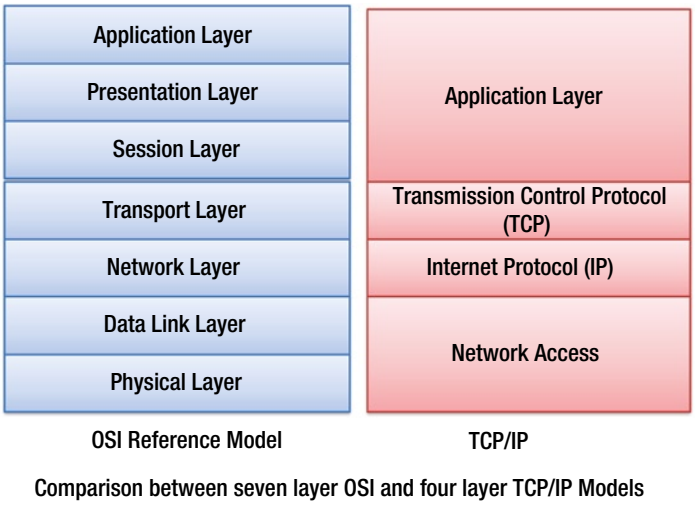

Figure 9-7. *OSI and TCP/IP models compared*

Each layer provides a distinct function and works with its upper layer and lower layer. Each layer "encapsulates" its function and passes on to the next layer while transmitting the data. When the data is received from lower layers, each layer peels off its encapsulation to perform its function. For the complete data transfer, functions of all the layers are equally important and all the layers have to work together. Layered architecture breaks the network communication into simpler components thus aiding easy design, development, and troubleshooting. With the layered architecture, each layer's functions can be developed by a different vendor who needs to adhere to the standards specified by the OSI reference model. The OSI model ensures different types of network devices built by different manufacturers such as routers, switches, hubs, and adapters, are able to interoperate within the network.

The (Internet Engineering Task Force) IETF is an international community consisting of network designers, equipment manufacturers, internet operators, and researchers who maintain the Internet protocol and the smooth operation of the Internet. *RFC 1122*[3] explains the details of host-to-host communication. *RFC 791*[4] describes IP and *RFC 793*[5] describes TCP architecture.

Figure 9-8 shows the TCP/IP protocol architecture and shows the major applications in each layer. This is by no means an exhaustive or a complete list.

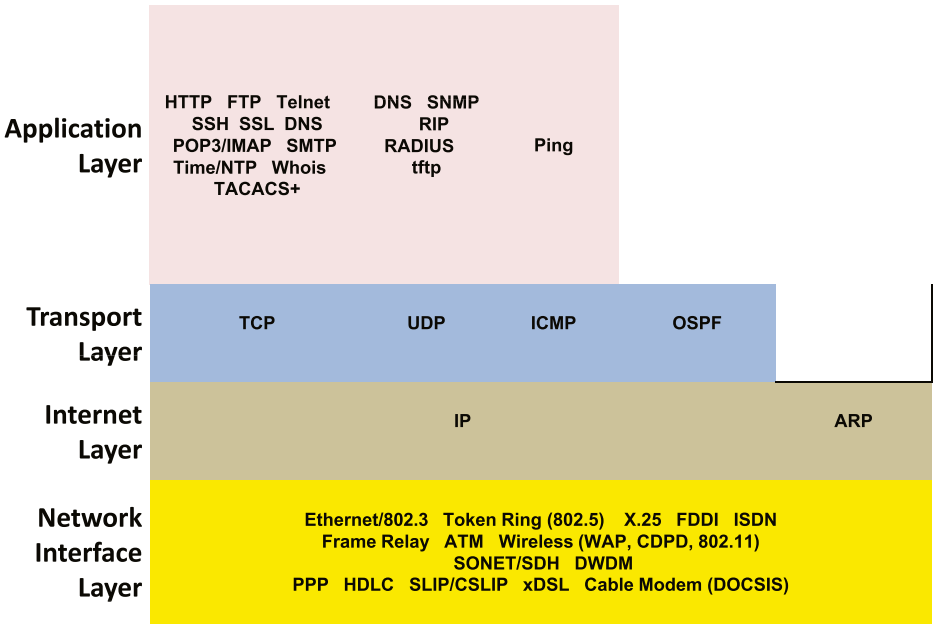

Figure 9-8. *TCP/IP and its functions*[6]

Network Vulnerabilities and Threats

With the advancement in computing, networking, and technology, the world is becoming more and more connected. Internet connects millions of computers and most of the geographies of this world. The Internet is a network of networks and consists of billions of users across private, public, university, and government networks sharing information across the networks. The Internet uses TCP/IP protocol and the underlying physical media can be wire, optical, or wireless technologies. The Internet serves an extensive range of applications, starting with e-mail, the World Wide Web (www), and social networks. Each application may use one or more protocols. There is a large amount of personal, commercial, business, government, and military information being shared on the Internet. There are billions of users, both good and bad, accessing the Internet. The bad guys, known as hackers and such other persons with malicious intent are a concern.

With so many computers, networking devices, protocols, and applications on the network, it has become a serious threat to information security. Any application, network device, or protocol can be vulnerable. The internet is crawling with people from all over the world who are continuously trying to test the security of various systems and networks. Some are simply testing for fun and others are fuelled by treacherous motives of stealing or revenge. A threat is an event that can occur by taking advantage of any vulnerabilities that exist in the network.

Any discussion on network security will include these three common terms:

- **Vulnerability:** An inherent weakness in the network, and network device. It could be hardware or software or both. Possible vulnerabilities could include routers, switches, servers, and security devices themselves.
- **Threat:** A threat is what can go wrong because of the exploit of the vulnerabilities or attack on the assets, such as data theft or unauthorized modification of the data.
- **Attack:** An attack is an unauthorized action with the intent to cause damage, or hinder or breach security of a network. An attack is launched by intruders to damage the network and network resources such as end-point devices, servers, or desktops which are vulnerable.

Vulnerabilities

One of the following three types of vulnerabilities or weaknesses can exist in the network:

- Security policy weakness
- Technology weakness
- Configuration weakness

Security Policy Weaknesses

Every organization should have security policies defined. However, the network can pose a security threat if the users do not follow the organizational security policy. Table 9-1 summarizes some of the common security policy weaknesses.

Table 9-1. *Common Security Policy Weaknesses*

Weakness	What can go wrong?
No written security policy	No enforcement of security policy across the organization leading to security incidents.
	Because of ignorance, mistakes may happen which can compromise the security.
	Intentional malicious acts also can be disguised as acts of ignorance.
No policy for hardware and software installations or updates	Unauthorized installations leading to theft of information; unauthorized modifications to the information.
	Unapproved modifications leading to unstable, attack prone network; ultimately leading to network crash.
	Unauthorized installations leading to malware infection. Intentional misuse of the network for personal gain.
Lack of Disaster recovery and Business continuity Plans	Confusion during disaster.
	Disasters may not be effectively and efficiently handled leading to reputation loss, business loss, or customer loss.
No Incident Response Team	Not able to handle security incidents / crisis, sometimes further complicating the situation rather than solving the problem.
No policy on usage of official assets	Misuse of official assets. Reputation Loss. Productivity loss. Can lead to malware infection.
No policy on Teleworking or Working from Home	Use of personal machines to connect to the network leading to the theft of data or infection of the office network.

Technology Weaknesses

Protocols are standards created to specify how an application should communicate. All connection oriented protocols have a state. Each state triggers certain events at certain time. Each state can be part of the connection, for example, a server waiting for response from a client or the transition between the close of connections. Specifications are not always complete, they are a good starting point and they could have limitations. Not all the applications are created by taking care of all the points mentioned in the specification. Such weaknesses in the protocol can be exploited.

All data traffic on the network is not malicious. However, traffic is allowed or denied by the security policies defined. By exploiting the weakness of the policy, attackers can bypass the security rules that can lead to policy violations. For example, TCP packets with SYN and RST flags enabled or an IP packet length can exceed the actual length specified in the standards. Although this packet can bypass security rules, if the remote device is not able to handle this erroneous packet, it leads to a possible attack. Table 9-2 summarizes the technology weaknesses that include protocol weaknesses, operating system weaknesses, and network equipment weaknesses.

Table 9-2. *Technology Weaknesses That Affect Networks*

Weakness	Description
TCP/IP Applications and protocols	HTTP, FTP, SNMP, SMTP, TCP, IP, and DNS are implemented as per the standards and specifications which have inherent limitations that can be exploited
Operating system	Microsoft Windows, Apple Macintosh, IBM OS/2, UNIX, and other operating systems have several security issues
Network device	Password weaknesses like default passwords not changed or lack of strong passwords requirement, authentication weaknesses, firewall holes, and user interface weaknesses

Configuration Weaknesses

Network administrators need to have adequate skills to configure networks and network devices to prevent security threats. Table 9-3 describes some of the possible configuration weaknesses.

Table 9-3. *Configuration Weaknesses That Affect Networks*

Weakness	Description
User Accounts	User accounts stored on devices must be secured. Exposing usernames and passwords can be a security threat.
Passwords	Password policy should be enforced at the user level. Passwords of major devices such as servers, routers, databases, should follow password policy set by the IT policy of the organization. Default passwords should not be allowed to be continued. The password secrecy should be preserved. These passwords have to be changed when an administrator leaves the organization. Passwords have to be periodically changed.
Configuration of TCP ports and Internet services	Should have a policy to define what application services should be allowed and for what purposes. A common problem is the lack of clarity in this regard and enabling some of the attack-prone ones like Java Script and VB Script or enabling the remote services or such other services without understanding the risks.
Default settings	If the network administrators do not change the default policy of the devices, it can cause serious security threats, such as default passwords are known to public, default permissions may be continued giving scope for attacks.
Misconfiguration of security and network devices	Misconfiguration of firewall and other network devices can cause serious security problems. For example, misconfiguration of access lists, routing protocol can cause serious security threats.

Threats

Internal threats and external threats are the two primary classes of threats to network security. They are illustrated in Figure 9-9. These threats are caused by attackers.

- **Internal Threats:** Internal threats are threats from someone within the organization, who has proper access to the network and network resources, who understands the network infrastructure well, who understands the security applications and the security loop holes. Someone within the organization can create and send out attacks by hiding his identity as he already knows enough inside information. According to the FBI, 80 percent of the reported security incidents are due to internal access and misuse of information by an insider of the company.
- **External Threats:** External threats are threats from outside the organization. They do not possess authorized access to the network resources. They work by gaining unauthorized access to the network and network resources with the intention of damaging the resources or for profit. These can be structured or unstructured:
  - **Structured:** Structured attacks come from technically competent hackers who belong to a class of highly motivated individuals. They understand vulnerabilities and develop sophisticated tools and techniques to penetrate without anyone knowing. These groups (also called hackers or crackers) may often be found to be involved in major crimes such as credit card theft or identity theft.
  - **Unstructured:** These threats are from inexperienced individuals testing their skills using some of the tools available in the public domain. Sometimes, these can do serious damage to company assets.

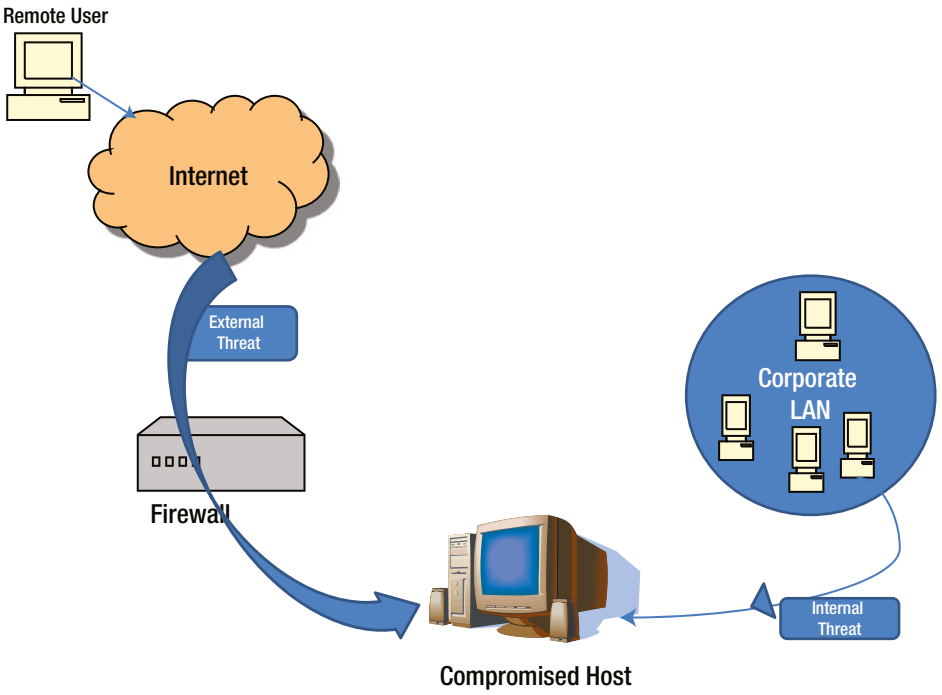

Figure 9-9. *Types of Threats*

Attacks

Attackers generally abuse the network "rules" established by security policies. The rules are broken in such a way that attackers send their traffic that appears to be normal traffic. Attacks can be classified into the following categories:

- Reconnaissance
- Denial of Service (DOS)/Distributed Denial of Service (DDoS)
- Other network attacks

Reconnaissance

To effectively launch an attack, the attacker should have the knowledge of the network, hardware used, software deployed, and its topology. Before an attack is launched, the attacker tries to gain this knowledge by scanning the network, which is called ***reconnaissance***. Reconnaissance is not an attack by itself; however, this could cause a serious security threat by allowing the weaknesses of the network or network resources to be made known to the attacker. This is more an information-gathering mission.

Quite often, reconnaissance is not detected for a considerable amount of time because they have no impact on the network.

Sniffing is one of the important reconnaissance methods used by the attackers to collect the information, such as user IDs and passwords, other information like session id, transactions being carried out, other confidential details, and business discussions carried out. Other popular methods used are pinging, banner grabbing, and port scanning.

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS)

The purpose of the DoS attack, as shown in Figure 9-10, is to make the network resources inaccessible to the user and bring down the network itself by generating a huge amount of network traffic that overwhelms or crashes the server, exceeding the capacity of the routers and switches, overwhelming the CPU and memory utilization. In some cases, DoS attacks can target a specific device and cause the system to hang.

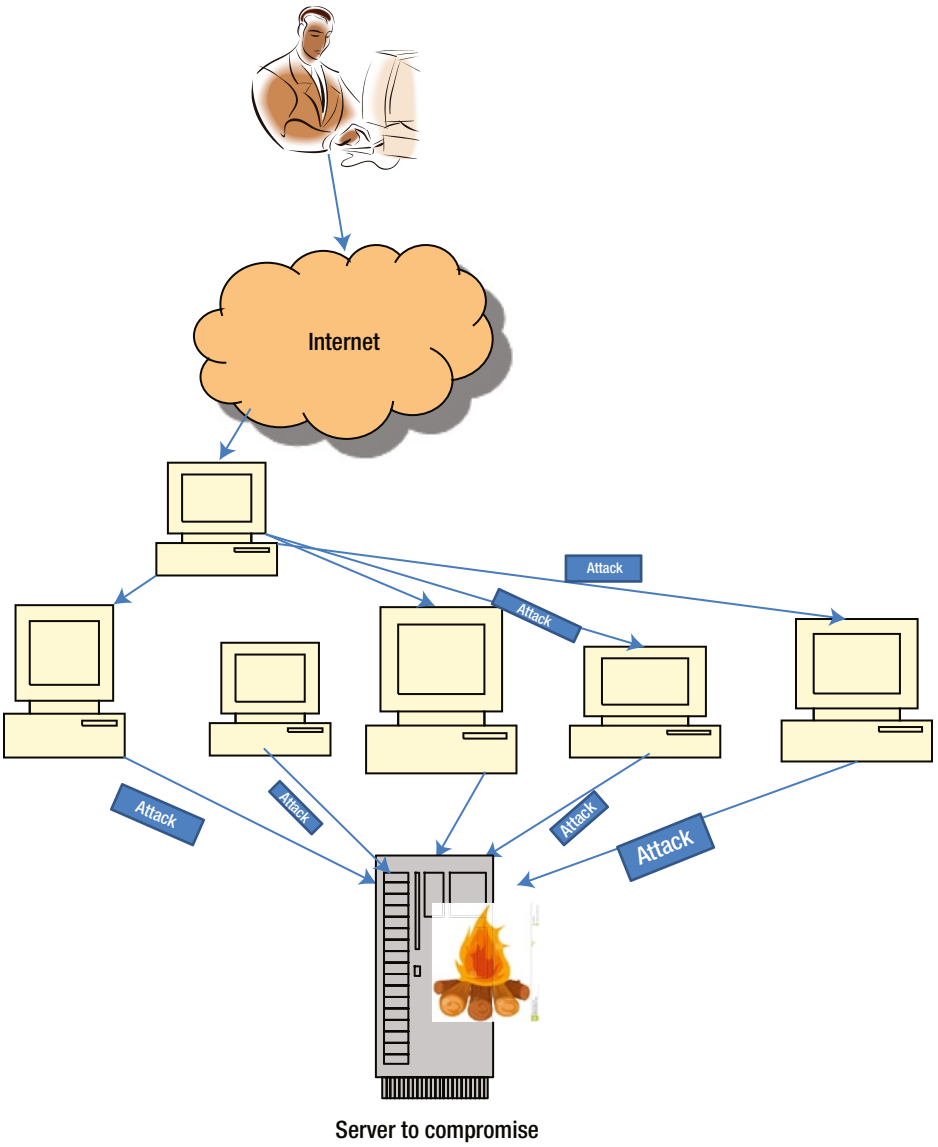

Figure 9-10. *Distributed Denial of Service Attack*

Sometimes, the attacker gets into one device in the network remotely and triggers simultaneous exploitation of systems on the network or uses multiple compromised machines to initiate simultaneous attacks, causing interruptions of network and network resources. The sudden increase in the network traffic can cause the server or router to go down quickly and become inaccessible to the legitimate users. This kind of an attack is called a Distributed Denial-of-Service (DDOS) attack which hides the true origin of the attack.

A DoS (DDoS) attack is an explicit attack to prevent legitimate users from accessing network and network services. Examples include:

- Flood the network, thereby preventing legitimate network traffic
- Target single device with too many requests thus bringing down the device
- Disrupt the connections between two legitimate devices thereby preventing access to a genuine service request
- Destruction or alteration of network configurations
- Consume the network bandwidth

The list of DDoS attack victims includes some major players including Microsoft, Amazon, HSBC, and YAHOO. In November 2011, the international bank HSBC was under an attack which targeted their servers that resulted in numerous customers being unable to withdraw money from the cash machines, as well as affecting its HSBC and First Direct websites.[7]

In 2004, the Microsoft Corp. was assailed by a DDoS attack induced by a Windows-based Mydoom-B worm.[8]

The following are some of the common (D)DoS attacks (by name):

- Ping of Death – This is an exploit of TCP/IP protocol implementation. As per the RFC specification, the maximum size of an IP packet is 65536. The attacker uses the "ping" application to make up an IP packet whose size exceeds the maximum size specified. The remote system may crash or reboot if it does not know how to handle the oversized packets.
- **TCP SYN Flood Attack:** This attack is an exploit of TCP implementation of connection establishment process. TCP connection establishment requires three handshakes, as shown in Figure 9-11, before the actual data starts being transmitted. Each time a client application, such as a web browser, attempts to open a connection with the server, it sends a request (SYN flag), to the server and waits for the acknowledgement from the server. If the server accepts the connection, then it sends back an (SYN-ACK) acknowledgement and waits for the acknowledgement.

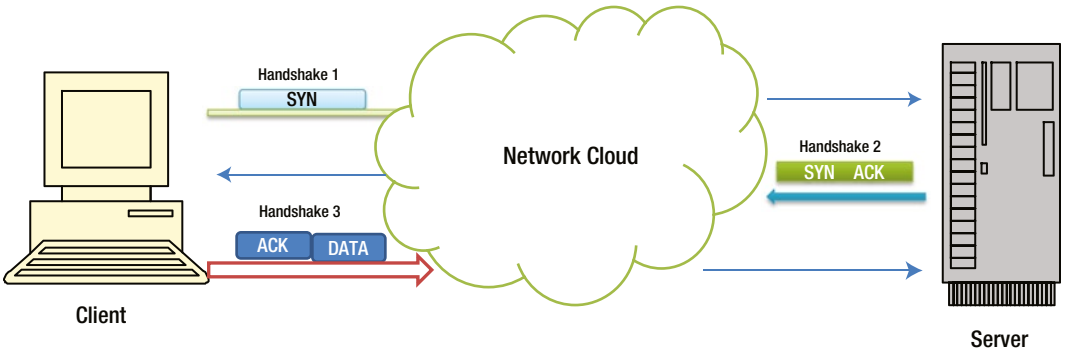

Figure 9-11. *TCP 3 Way Connection Handshake*

Once the client receives the acknowledgement from the server, it sends one more segment (ACK) acknowledging the receipt of the server's information. Once both the server and client handshake completes, the actual data transmission starts. This is sometimes referred to as TCP 3-way handshake. Since each connection information takes up memory and CPU resources, only a limited number of in-progress connections are possible. When the server establishes connection with the client, the server considers the connection as open and frees up the queued resources for accepting new connections. During a SYN flood attack, the server never sends back the ACK packet to the hostile client. Instead, the hostile client application keeps sending repeated SYN requests causing DoS. The attacking application generates spoofed packets that appear to be valid new connections and enter into the queue, but connections are never completed (RFC 4987)[9].

- E-mail bombs – An Application program that can send bulk e-mails to individuals, organizations, lists, or domains to vandalize an e-mail server
- Teardrop – An IP protocol exploit where the IP packet is fragmented in such a way that reassembling the packet can cause the system to crash
- **Smurf Attack:** Internet Control Message Protocol (ICMP) is used to test the availability of a network device by pinging the concerned node to determine its operational status. When the remote host sends a PING, the end device responds by sending a "reply" message. A smurf is a type of DoS attack in which a system is flooded with spoofed ping (ICMP) messages. This creates high network traffic and high consumption of network bandwidth and leads ultimately to the crashing of the remote system.

Other Attacks on Networks

Apart from the attacks that we have described previously, there are other attacks that can cause serious damage to the network security. Some common ones include spoofing attacks, HTTP Tunneling, and session hijacking:

- **Masquerade/Spoofing Attacks:** The network intruder masquerades the TCP/IP packet by an illegal IP address, falsifying the source address. The intruder fools the remote machine by an illegitimate source address but with valid user access privileges. In an IP spoofing attack, a malicious hacker from outside the network hacks into the network pretending to be an insider, a trusted user, of the organization, and spoofs the source address of a legitimate inside user thus gaining access to the network resources. This attack can also cause a broadcast in the network causing high network traffic. If the attacker manages to alter the routing tables, then response from the network resource can go to the spoofed destination address.
- **ARP Spoofing & DNS Spoofing:** The Address Resolution Protocol (ARP) spoofing is used to confuse the system to map incorrect MAC address to a particular IP address in the ARP table. Similarly DNS (Domain Name Service protocol) spoofing is to change the mapping of DNS entries in the DNS cache. Mac Flooding attacks are also similar to this.
- **HTTP Tunneling:** This method may be used by the insiders to overcome the firewall controls and send confidential information to the outside world without anyone inside being aware of the same.
- **SSH Tunneling:** These may be used to directly connect to a network stealthily and initiate attacks. This is an illegitimate use of a legitimate tool.
- **Session Hijacking:** A session between the user and the server can be hijacked by the attacker. Some of the methods used in this regard are session fixing and session prediction. Here, usually a valid session between the user and server is taken over by the attacker.

- **Attacks on Network Equipment including Routers:** The network equipment is traditionally prone to default password vulnerabilities because the network administrators not taking sufficient care in resetting these passwords. The weakness of the network configurations of a router is a new point of vulnerability. In addition to the administrator passwords, some vendors have a so-called "back-door" to their system for debugging purposes and to support the client in case an admin password is forgotten or lost. This back-door could also be exploited, if it is known to the attackers.

How to counter the Network Attacks

The following measures can be taken to counter the network attacks:

- Hardening of all network equipment with appropriate configurations and appropriate patching including firmware updates
- All default passwords to be substituted with strong passwords
- Defense in depth is implemented to avoid attacks like session hijacking
- Use safe session ID handling
- Session time-out to be set as appropriate to the application and its risks
- Set complicated session ID creation logic
- Use encrypted handshakes like SSL with Digital certificate or TLS, techniques like VPN
- Do not store passwords or critical information in the cookies
- Ensure that all the software used including utilities / tools are patched / updated
- Set easy-to-understand and clear security policies
- Create awareness among the employees on what can go wrong and what is expected from them – do's and don'ts
- Do not have the same user name and passwords for all the systems – use different ones
- Logout promptly after the work is over
- Ensure cookies, history, and offline content are removed after sensitive transaction sessions
- Do not click on the links in the suspect e-mails

Chapter Summary

- We looked into basic communication, computer communication, and the parties to and components of the communication. We also looked into the context of computer communication, and defined a network and networking. We equated the language of the oral or written communication to that of the protocol in the networked world.
- We explored the networks in particular and looked in to various network topologies like BUS, Ring, Star, or Y. We also identified the differences and weaknesses of each of these. We also looked into what is meant by LAN, MAN, and WAN and the differences among these.

- We elaborated upon the two models of networking: Open Systems Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP). We looked into how the OSI model divides the entire structure of computer communication into seven layers and how the TCP/IP model divides the entire structure into four corresponding layers. We also looked at the method of communication between various layers like the upper layer being serviced by the lower layer while concurrently servicing its upper layer and that is how the communication happens between various equipment / components of network. We also looked at the details of the functions carried out by various layers and the different protocols used by various layers. We also explored and understood how the layers, protocols, and the specifications help vendors to create the equipment which interoperates with each other.
- We defined vulnerabilities, threats, and attacks to make the further discussions clear to the readers.
- We categorized the weaknesses or vulnerabilities into three groups: security policy implementation related, technology related, and configuration related. We also looked at various examples from each of these categories.
- We differentiated between internal and external threats; and between structured and unstructured threats.
- Then we detailed the issue of "reconnaissance," which is usually carried out by the attackers to gather information and how sniffing is an important part of this activity.
- We explored DoS/DDoS attacks and the various ways in which these attacks can be executed. In this context, we elaborated upon Ping-of-Death, TCP SYN flooding, e-mail bombing, teardrop, and smurf attacks. We also went through some of the real-world DoS/DDoS attacks.
- We explored other network threats like spoofing, session hijacking, HTTP tunneling, SSH Tunneling, and backdoors.
- We looked briefly at the measures we can take individually or at the organization level to counter the network attacks.