UNIT – I

Introduction to Cyber Security

Cyber Security Introduction - Cyber Security Basics:

Cyber security is the most concerned matter as cyber threats and attacks are overgrowing. Attackers are now using more sophisticated techniques to target the systems. Individuals, small-scale businesses or large organization, are all being impacted. So, all these firms whether IT or non-IT firms have understood the importance of Cyber Security and focusing on adopting all possible measures to deal with cyber threats.

What is cyber security?

"Cyber security is primarily about people, processes, and technologies working together to encompass the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, etc."

Cyber security is the protection of Internet-connected systems, including hardware, software, and data from cyber attacks.

It is made up of two words one is cyber and other is security.

- Cyber is related to the technology which contains systems, network and programs or data.

- Whereas security related to the protection which includes systems security, network security and application and information security.

Why is cyber security important?

Listed below are the reasons why cyber security is so important in what's become a predominant digital world:

- Cyber attacks can be extremely expensive for businesses to endure.
- In addition to financial damage suffered by the business, a data breach can also inflict untold reputational damage.
- Cyber-attacks these days are becoming progressively destructive. Cybercriminals are using more sophisticated ways to initiate cyber attacks.
- Regulations such as GDPR are forcing organizations into taking better care of the personal data they hold.

Identifying Types of Threats

Some threats are common to all networks; others are more likely with specific types of networks. Most attacks can be categorized as one of seven broad classes:

- **Malware:** This is a generic term for software that has a malicious purpose. It includes virus attacks, worms, adware, Trojan horses, and spyware. This is the most prevalent danger to your system.
- **Security breaches:** This group of attacks includes any attempt to gain unauthorized access to your system. This includes cracking passwords, elevating privileges, breaking into a server…all the things you probably associate with the term *hacking*.
- **DoS attacks:** These are designed to prevent legitimate access to your system. And, as you will see in later chapters, this includes distributed denial of service (DDoS).
- **Web attacks:** This is any attack that attempts to breach your website. Two of the most common such attacks are SQL injection and cross-site scripting.
- **Session hijacking:** These attacks are rather advanced and involve an attacker attempting to take over a session.
- **Insider threats:** These are breaches based on someone who has access to your network misusing his access to steal data or compromise security.
- **DNS poisoning:** This type of attack seeks to compromise a DNS server so that users can be redirected to malicious websites, including phishing websites.

There are other attacks, such as social engineering. The forgoing list is just an attempt to provide a broad categorization of attack types. This section offers a broad description of each type of attack. Later chapters go into greater detail with each specific attack, how it is accomplished, and how to avoid it.

Malware

Malware is a generic term for software that has a malicious purpose. This section discusses four types of malware: viruses, Trojan horses, spyware, and logic bombs. Trojan horses and viruses are the most widely encountered. One could also include rootkits, but these usually spread as viruses and are regarded as simply a specific type of virus.

- Software with a malicious purpose
  - Virus

- ❑ Trojan horse
- ❑ Spyware
- ❑ Logic Bomb

Virus: A virus is a program that attempts to damage a computer system and replicate itself to other computer systems.

- Requires a host to replicate and usually attaches itself to a host file or a hard drive sector. • Replicates each time the host is used.
- Often focuses on destruction or corruption of data. •
- Usually attaches to files with execution capabilities such as .doc, .exe, and .bat extensions.
- Often distributes via e-mail. Many viruses can e-mail themselves to everyone in your address book.
- Examples: Stoned, Michelangel

Spyware: Spyware is simply software that literally spies on what you do on your computer. Spyware can be as simple as a cookie—a text file that your browser creates and stores on your hard drive—that a website you have visited downloads to your machine and uses to recognize you when you return to the site.

Another form of spyware, called a key logger, records all of your keystrokes. Some key loggers also take periodic screenshots of your computer. Data is then either stored for later retrieval by the person who installed the key logger or is sent immediately back via email. We will discuss specific types of key loggers later in this book.

Trojan horse: A Trojan horse is a malicious program that is disguised as legitimate software. Discretionary environments are often more vulnerable and susceptible to Trojan horse attacks because security is user focused and user directed. Thus the compromise of a user account could lead to the compromise of the entire environment.

- Cannot replicate itself.
- Often contains spying functions (such as a packet sniffer) or backdoor functions that allow a computer to be remotely controlled from the network. •
- Often is hidden in useful software such as screen savers or games.
- Example: Back Orifice, Net Bus, Whack-a-Mole.

Logic Bomb A Logic Bomb is malware that lies dormant until triggered. A logic bomb is a specific example of an asynchronous attack.

- A trigger activity may be a specific date and time, the launching of a specific program, or the processing of a specific type of activity.
- Logic bombs do not self-replicate.

DoS Attacks

It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It uses the single system and single internet connection to attack a server. It can be classified into the following-

Volume-based attacks- Its goal is to saturate the bandwidth of the attacked site, and is measured in bit per second.
Protocol attacks- It consumes actual server resources, and is measured in a packet.
Application layer attacks- Its goal is to crash the web server and is measured in request per second.

Web Attacks

By their nature, web servers have to allow communications. Oftentimes, websites allow users to interact with the website. Any part of a website that allows for user interaction is also a potential point for attempting a web-based attack. SQL injections involve entering SQL (Structured Query Language) commands into login forms (username and password text fields) in an attempt to trick the server into executing those commands. The most common purpose is to force the server to log the attacker on, even though the attacker does not have a legitimate username and password. While SQL injection is just one type of web attack, it is the most common.

- **SQL Injection**
- **Cross Scripting**

SQL Injection

It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information**.**

SQL is relatively easy to understand; in fact, it looks a lot like English. There are commands like SELECT to get data, INSERT to put data in, and UPDATE to change data. In order to log in to a website, the web page has to query a database table to see if that username and password are correct. The general structure of SQL is like this:

select column1, column2 from tablename

or

The most basic form of SQL injection seeks to subvert this process. The idea is to create a statement that will always be true. For example, instead of putting an actual username and password into the appropriate text fields, the attacker will enter ' or '1' = '1 into the username and password boxes. This will cause the program to create this query:

SELECT * FROM Users WHERE USERNAME = '' or '1' = '1' AND PASSWORD = '' or '1' = '1'.

So you are telling the database and application to return all records where username and password are blank or if 1 = 1. It is highly unlikely that the username and password are blank. But I am certain that 1

=1 always. Any true statement can be substituted. Examples are a = a and bob = bob.

Cross-Site Scripting

This attack is closely related to SQL injection. It involves entering data other than what was intended, and it depends on the web programmer not filtering input. The perpetrator finds some area of a website that allows users to type in text that other users will see and then instead injects client-side script into those fields.

To better understand this process, let's look at a hypothetical scenario. Let's assume that ABC online book sales has a website. In addition to shopping, users can have accounts with credit cards stored, post reviews, and more. The attacker first sets up an alternate web page that looks as close to the real one as possible. Then the attacker goes to the real ABC online book sales website and finds a rather popular book. He goes to the review section, but instead of typing in a review he types in this:

```
<script> window.location = "http://www.fakesite.com"; </script>
```

Now when users go to that book, this script will redirect them to the fake site, which looks a great deal like the real one. The attacker then can have the website tell the user that his session has timed out and to please log in again. That would allow the attacker to gather a lot of accounts and passwords. That is only one scenario, but it illustrates the attack

Session Hijacking

It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.

Insider Threats

Insider threats are a type of security breach. However, they present such a significant issue that we will deal with them separately. An insider threat is simply when someone inside your organization either misuses his access to data or accesses data he is not authorized to access.

Here are a few examples:

- A hospital employee who accesses patient records to use the data to steal a patient's identity, or someone with no access at all who accesses records.
- A salesperson who takes the list of contacts with him before leaving the company.

DNS Poisoning (spoofing)

Domain Name Server (DNS) spoofing (a.k.a. DNS cache poisoning) is an attack in which altered DNS records are used to redirect online traffic to a fraudulent website that resembles its intended destination. Once there, users are prompted to login into (what they believe to be) their account, giving the perpetrator the opportunity to steal their access credentials and other types of sensitive information. Furthermore, the malicious website is often used to install worms or viruses on a user's computer, giving the perpetrator long-term access to it and the data it stores.

Methods for executing a DNS spoofing attack include:

- **Man in the middle (MITM)** – The interception of communications between users and a DNS server in order to route users to a different/malicious IP address.
- **DNS server compromise** – The direct hijacking of a DNS server, which is configured to return a malicious IP address.

Example:

The following example illustrates a DNS cache poisoning attack, in which an attacker (IP 192.168.3.300) intercepts a communication channel between a client (IP 192.168.1.100) and a server computer belonging to the website www.estores.com (IP 192.168.2.200).

In this scenario, a tool (e.g., arpspoof) is used to dupe the client into thinking that the server IP is 192.168.3.300. At the same time, the server is made to think that the client's IP is also 192.168.3.300.

Basic Security Terminology

People:

- **Hackers**
  - **White hats**
  - **Black hats**
  - **Gray hats**
- **Script kiddies**
- **Sneakers**
- **Ethical hackers**

A white hat hacker, upon finding some flaw in a system, will report the flaw to the vendor of that system. For example, if a white hat hacker were to discover some flaw in Red Hat Linux, he would then email the Red Hat company (probably anonymously) and explain exactly what the flaw is and how it was exploited. White hat hackers are often hired specifically by companies to do penetration tests. The EC Council even has a certification test for white hat hackers: the Certified Ethical Hacker test.

A black hat hacker is the person normally depicted in the media. Once she gains access to a system, her goal is to cause some type of harm. She might steal data, erase files, or deface websites. Black hat hackers are sometimes referred to as crackers.

A gray hat hacker is normally a law-abiding citizen, but in some cases will venture into illegal activities.

Script Kiddies

A hacker is an expert in a given system. As with any profession, it includes its share of frauds. So what is the term for someone who calls himself a hacker but lacks the expertise? The most common term for this sort of person is *script kiddy* (Raymond, 1993)

A classic example is the Low Earth Orbit Ion Cannon tool for executing a DoS attack. Someone who downloads such a tool without really understanding the target system is considered a script kiddy.

Ethical Hacking: Penetration Testers

When and why would someone give permission to another party to hack his system? The most common answer is in order to assess system vulnerabilities. This used to be called a *sneaker*, but now the term *penetration tester* is far more widely used.

Anyone hired to assess the vulnerabilities of a system should be both technically proficient and ethical. Run a criminal background check, and avoid those people with problem pasts. There are plenty of legitimate security professionals available who know and understand hacker skills but have never committed security crimes. If you take the argument that hiring convicted hackers means hiring talented people to its logical conclusion, you could surmise that obviously those in question are not as good at hacking as they would like to think because they were caught.

Phreaking

One specialty type of hacking involves breaking into telephone systems. This subspecialty of hacking is referred to as phreaking. The New Hacker's Dictionary actually defines phreaking as "the action of using mischievous and mostly illegal ways in order to not pay for some sort of telecommunications bill, order, transfer, or other service". Phreaking requires a rather significant knowledge of telecommunications, and many phreakers have some professional experience working for a phone company or other telecommunications business.

Professional Terms

Security Devices

- Firewall
  - Filters network traffic
- Proxy server
  - Disguises IP address of internal host
- Intrusion Detection System
  - Monitors traffic, looking for attempted attacks

Security Activities

- Authentication
- Auditing

Security Devices

A firewall is a barrier between a network and the outside world. Sometimes a firewall takes the form of a standalone server, sometimes a router, and some- times software running on a machine. Whatever its physical form, a firewall filters traffic entering and exiting the network.

A *proxy server* is often used with a firewall to hide the internal network's IP address and present a single IP address (its own) to the outside world.

Firewalls and proxy servers guard the perimeter by analyzing traffic (at least inbound and in many cases outbound as well) and blocking traffic that has been disallowed by the administrator.

These two safeguards are often augmented by an ***intrusion detection system*** **(IDS).** An IDS simply monitors traffic, looking for suspicious activity that might indicate an attempted intrusion

Security Activities

Authentication is the most basic security activity. It is merely the process of determining if the credentials given by a user or another system (such as a username and password) are authorized to access the network resource in question. When you log in with your username and password, the system will attempt to authenticate that username and password. If it is authenticated, you will be granted access.

Another crucial safeguard is *auditing*, which is the process of reviewing logs, records, and procedures to determine if these items meet standards. This activity will be mentioned in many places throughout this book and will be a definite focus in a few chapters.

Concepts and approaches

- ❑ CIA Triangle
- ❑ Least Privileges
- ❑ Perimeter security approach
- ❑ Layered security approach
- ❑ Proactive versus reactive
- ❑ Hybrid security method

CIA is a reference to the three pillars of security: confidentiality, integrity, and availability. When you are thinking about security, your thought processes should always be guided by these three principles. First and foremost, are you keeping the data confidential? Does your approach help guarantee the integrity of data? And does your approach still make the data readily available to authorized users?

Least privileges. This means that each user or service running on your network should have the least number of privileges/access required to do her job. No one should be granted access to anything unless it is absolutely required for the job.

.

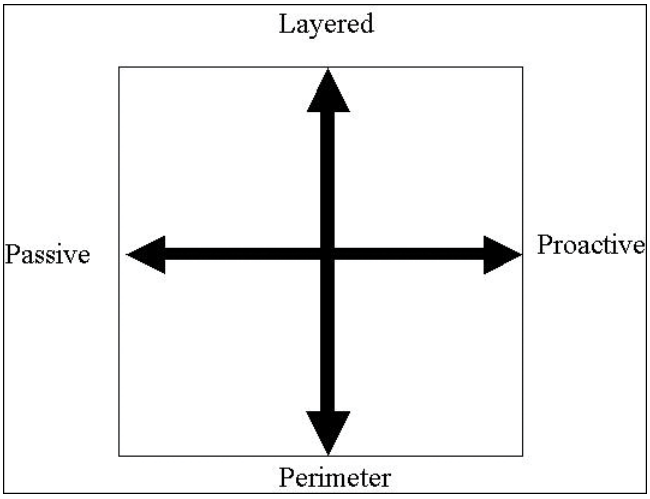
In a **perimeter security approach**, the bulk of security efforts are focused on the perimeter of the network. This focus might include firewalls, proxy servers, password policies, or any technology or procedure to make unauthorized access of the network less likely. Little or no effort is put into securing the systems within the network. In this approach the perimeter is secured, but the various systems within that perimeter are often vulnerable.

There are additional issues regarding perimeter security that include physical security. That can include fences, closed-circuit TV, guards, locks, and so on, depending on the security needs of your organization.

A **layered security approach** is one in which not only is the perimeter secured, but individual systems within the network are also secured. All servers, workstations, routers, and hubs within the network are secure. One way to accomplish this is to divide the network into segments and secure each segment as if it were a separate network, so if the perimeter security is compromised, not all the internal systems are affected. This is the preferred method whenever possible.

You should also measure your security approach by how proactive/reactive it is. This is done by gauging how much of the system's security infrastructure and policies are dedicated to preventive measures and how much of the security system is designed to respond to attack. **A passive security** approach takes few or no steps to prevent an attack. A **dynamic or proactive** defense is one in which steps are taken to prevent attacks before they occur.

In the real world, network security is usually not completely in one paradigm or another; it is usually a **hybrid** approach. Networks generally include elements of both security paradigms. The two categories also combine. One can have a network that is predominantly passive but layered, or one that is primarily perimeter but proactive.



The most desirable hybrid approach is a layered paradigm that is dynamic, which is the upper-right quadrant of the figure.

Online Security Resources

As you read this book, and when you move out into the professional world, you will have frequent need for additional security resources. Appendix B, "Resources," includes a more complete list of resources, but this section highlights a few of the most important ones you may find useful now.

CERT

The *Computer Emergency Response Team* (CERT, www.cert.org) is sponsored by Carnegie-Mellon University. CERT was the first computer incident-response team, and it is still one of the most respected in the industry. Anyone interested in network security should visit the site routinely. On the website you will find a wealth of documentation, including guidelines for security policies, cutting- edge security research, and more.

Microsoft Security Advisor

Because so many computers today run Microsoft operating systems, another good resource is the Microsoft Security Advisor website: https://technet.microsoft.com/en-us/library/security/ dn631936.aspx. This site is a portal to all Microsoft security information, tools, and updates. If you use any Microsoft software, then it is advised that you visit this website regularly.

F-Secure

The F-Secure corporation maintains a website at www.f-secure.com. This site is, among other things, a repository for detailed information on virus outbreaks. Here you will find not only notifications about a particular virus but detailed information about the virus. This information includes how the virus spreads, ways to recognize the virus, and frequently, specific tools for cleaning an infected system of a particular virus.

SANS Institute

The SANS Institute website (www.sans.org) is a vast repository of security-related documentation. On this site you will find detailed documentation on virtually every aspect of computer security you can imagine. The SANS Institute also sponsors a number of security research projects and publishes information about those projects on its website.

Networks and the Internet

Network Basics

Getting two or more computers to communicate and transmit data is a process that is simple in concept but complex in application. Consider all the factors involved. First you will need to physically connect the computers. This connection usually requires either a cable that plugs into your computer or wireless connection. The cable then is plugged either directly to another computer or into a device that will, in turn, connect to several other computers.

Of course, wireless communication is being used with more frequency, and wireless connecting, obvi ously, doesn't require a cable. However, even wireless communication relies on a physical device to transmit the data. There is a card in most modern computers called a *network interface card*, or NIC. If the connection is through a cable, the part of the NIC that is external to the computer has a connection slot that looks like a telephone jack, only slightly bigger. Wireless networks also use a NIC; but rather than having a slot for a cable to connect to, the wireless network simply uses radio signals to transmit to a nearby wireless router or hub. Wireless routers, hubs, and NICs must have an antenna to transmit and receive signals. These devices are connective devices that will be explained in detail later in this chapter.

TABLE 2.1 Cable Types and Uses

Category	Specifications	Uses
1	Low-speed analog (less than 1MHz)	Telephone, doorbell
2	Analog line (less than 10MHz)	Telephone
3	Up to 16MHz or 100Mbps (megabits per second)	Voice transmissions
4	Up to 20MHz/100Mbps	Data lines, Ethernet networks
5	100MHz/100Mbps	Most common a few years ago, still widely used
6	1000Mbps (some get 10Gbps)	Most common type of network cable
6a	10Gbps	High-speed networks
7	10Gbps	Very high-speed networks
8	40Gbps	Not yet commonly found

The Hub

The simplest connection device is the hub. A hub is a small box-shaped electronic device into which you can plug network cables. It will have four or more (commonly up to 24) RJ-45 jacks, each called a port. A hub can connect as many computers as it has ports. (For example, an 8-port hub can connect eight computers.) You can also connect one hub to another; this strategy is referred to as "stacking" hubs. Hubs are quite inexpensive and simple to set up; just plug in the cable. However, hubs have a downside. If you send a packet (a unit of data transmission) from one computer to another, a copy of that packet is actually sent out from every port on the hub.

Repeater

A repeater is a device used to boost signal. Basically if your cable needs to go further than the maximum length (which is 100 meters for UTP), then you need a repeater. There are two types of repeaters: amplifier and signal. Amplifier repeaters simply boost the entire signal they receive, including any noise. Signal repeaters regenerate the signal, and thus don't rebroadcast noise.

The Switch

The next connection device option is the switch. A switch is basically an intelligent hub; it works and looks exactly like a hub, with one significant difference. When a switch receives a packet, it will send that packet only out the port for the computer to which it needs to go. A switch is essentially a hub that is able to determine where a packet is being sent. How this determination is made is explained in the "Data Transmission" section.

The Router

Finally, if you wish to connect two or more networks, you use a router. A router is similar in concept to a hub or switch, as it does relay packets; but it is far more sophisticated. You can program most routers and control how they relay packets. Most routers have interfaces allowing you to configure them. The more robust routers also offer more programming possibilities. The specifics of how you program the router are different from vendor to vendor, and there are entire books written specifically on just programming routers. It is not possible to cover specific router programming techniques in this book; however, you should be aware that most routers are programmable, allowing you to change how they route traffic. Also, unlike using a hub or switch, the two networks connected by a router are still separate networks.

How the Internet Works

Now that you have a basic idea of how computers communicate with each other over a network, it is time to discuss how the Internet works. The Internet is essentially a large number of networks that are connected to each other. Therefore, the Internet works exactly the same way as your local network. It sends the same sort of data packets, using the same protocols. These various networks are simply connected into main transmission lines called backbones. The points where the backbones connect to each other are called network access points (NAPs). When you log on to the Internet, you probably use an Internet service provider (ISP). That ISP has a connection either to the Internet backbone or to yet another provider that has a backbone. So, logging on to the Internet is a process of connecting your computer to your ISP's network, which is, in turn, connected to one of the back- bones on the Internet.

IP Addresses

With tens of thousands of networks and millions of individual computers communicating and sending data, a predictable problem arises. That problem is ensuring that the data packets go to the correct computer. This task is accomplished in much the same way as traditional "snail" letter mail is delivered to the right person: via an address. With network communications, this address is a special one, referred to as an "IP" address. An IP address can be IP version 4 or version 6.

IPv4

An IP address is a series of four values, separated by periods. (An example would be 107.22.98.198.) Each of the three-digit numbers must be between 0 and 255; thus, an address of 107.22.98.466 would not be a valid one. These addresses are actually four binary numbers; you just see them in decimal format. Since each of these numbers is really just a decimal representation of 8 bits, they are often referred to as octets. So there are four octets in an IP v4 address. Recall that a byte is 8 bits (1s and 0s), and an 8-bit binary number converted to decimal format will be between 0 and 255.

TABLE 2.4 Network Classes

Class	IP Range for the First Byte	Use
A	0–126	Extremely large networks. No Class A network IP addresses are left. All have been used.
B	128–191	Large corporate and government networks. All Class B IP addresses have been used.
C	192–223	The most common group of IP addresses. Your ISP probably has a Class C address.
D	224–247	These are reserved for multicasting (transmitting different data on the same channel).
E	248–255	Reserved for experimental use.

Subnetting and CIDR

Subnetting is simply chopping up a network into smaller portions. For example, if you have a network using the IP address 192.168.1.X (x being whatever the address is for the specific computer), then you have allocated 255 possible IP addresses. What if you want to divide that into two separate subnet- works? Subnetting is how you do that.

More technically, the subnet mask is a 32-bit number that is assigned to each host to divide the 32-bit binary IP address into network and node portions. You also cannot just put in any number you want. The first value of a subnet mask must be 255; the remaining three values can be 255, 254, 252, 248, 240, or 224. Your computer will take your network IP address and the subnet

mask and use a binary AND operation to combine them.

CIDR

Subnetting only allows you to use certain, limited subnets. Another approach is CIDR, or classless interdomain routing. Rather than define a subnet mask, you have the IP address followed by a slash and a number. That number can be any number between 0 and 32, which results in IP addresses like these:

192.168.1.10/24 (basically a Class C IP address)

192.168.1.10/31 (much like a Class C IP address with a subnet mask)

When you use this, rather than having classes with subnets, you have variable-length subnet masking (VLSM) that provides classless IP address. This is the most common way to define network IP addresses today.

IPv6

You have probably heard talk of IP version 6, or IPv6, as an extension of IPv4. Essentially, IP version 4 is limited to 4.2 billion IP addresses. Even with the use of private IP addresses, we will run out of available IP addresses. Think of all the computers, printers, routers, servers, smart phones, tablets, and so on connected to the Internet. IP version 6 was designed to alleviate this problem. And if you looked around in the network settings described in the last section, you probably saw the option to enable IPv6. IPv6 utilizes a 128-bit address (instead of 32), so there is no chance of running out of IP addresses in the foreseeable future. IPv6 also utilizes a hex numbering method.

Uniform Resource Locators

A URL (Uniform Resource Locator) is a unique identifier used to locate a resource on the Internet. It is also referred to as a web address. URLs consist of multiple parts -- including a protocol and domain name -- that tell a web browser how and where to retrieve a resource.

End users use URLs by typing them directly into the address bar of a browser or by clicking a hyperlink found on a webpage, bookmark list, in an email or from another application.

Packets

We have mentioned network packets and how they are routed through a network and through the Internet. What we have not discussed is exactly what a packet is. You probably know that network traffic is really a lot of 1s and 0s that are in turn transmitted as voltages (over UTP), light wave (over optic cable), or radio frequencies (over Wi-Fi). The data is divided into small chunks called packets.

Packets are divided into three sections. Those are header (actually there are at least three headers, but we will get to that in just a moment), data, and footer. The header will contain information about how to address the packet, what kind of packet it is, and related data. The data portion is obviously the information you want to send. The footer serves both to show where the packet ends and to provide error detection.

.

Basic Network Utilities

IP Config

Displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. Used without parameters, ipconfig displays Internet Protocol version 4 (IPv4) and IPv6 addresses, subnet mask, and default gateway for all adapters.

>>ipconfig

This command gives you some information about your connection to a network (or to the Internet). Most importantly, you find out your own IP address. The command also has the IP address for your default gateway, which is your connection to the outside world. Running the IPConfig command is a first step in determining your system's network configuration. Most commands that this book will mention, including IPConfig, have a number of parameters, or flags, that can be passed to the commands to make the computer behave in a certain way

Ping

Another commonly used command is ping. ping is used to send a test packet, or echo packet, to a machine to find out if the machine is reachable and how long the packet takes to reach the machine. This useful diagnostic tool can be employed in elementary hacking techniques. Below ping command executed on www.yahoo.com.

>>ping www.yahoo.com

It tells you that a 32-byte echo packet was sent to the destination and returned. The TTL (Time To Live) item shows how many intermediary steps, or hops, the packet should take to the destination before giving up.

Tracert

This command is a more or less “ping deluxe.” tracert not only tells you if the packet got to its destination and how long it took, but also tells you all the intermediate hops it took to get there.

With tracert, you can see (in milliseconds) the IP addresses of each intermediate step listed and how long it took to get to that step. Knowing the steps required to reach a destination can be very important, as you will find later in this book.

Netstat

Netstat is another interesting command. It is an abbreviation for Network Status. Essentially this command tells you what connections your computer currently has. Don’t panic if you see several connections; that does not mean a hacker is in your computer. You will see many private IP addresses. This means your network has internal communication going on.

NSLookup

This command is an abbreviation for Name Server lookup. It is used to connect with your network’s DNS server. Often it can be used just to verify the DNS server is running. It can also be used to execute commands.