ICSI MODULE 1:

Network Basics

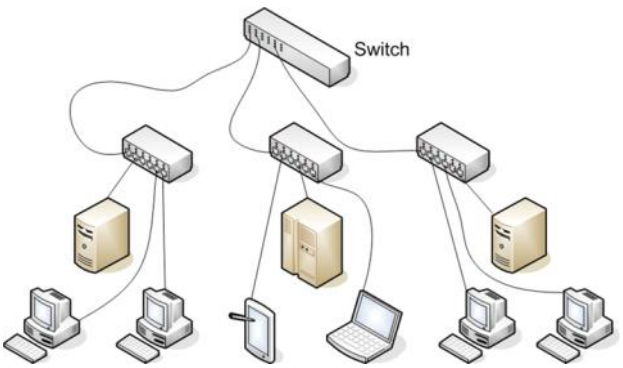
1.1 Network Basics

Before diving into how to protect a network, exploring what networks are, would probably be a good idea.

For many readers this section will be a review, but for some it might be new material. Whether this is a review for you, or new information, having a thorough understanding of basic networking before attempting to study network security is critical. Also, be aware this is just a brief introduction of basic network concepts.

A network is simply a way for machines / computers to communicate.

At the physical level, it consists of all the machines you want to connect and the devices you use to connect them. Individual machines are connected either with a physical connection (a category 5 cable going into a network interface card, or NIC) or wirelessly. To connect multiple machines together, each machine must connect to a hub or switch, and then those hubs / switches must connect together. In larger networks, each subnetwork is connected to the others by a router.

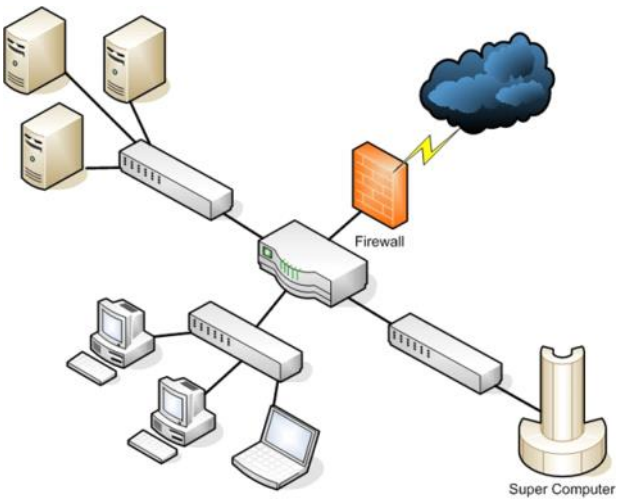


1.1.1 Basic Network Structure

Some connection point(s) must exist between your network and the outside world. A barrier is set up between that network and the Internet, usually in the form of a firewall. The real essence of networks is communication allowing one machine to communicate with another.

However, every path of communication is also a possibility for an attack.

The first step in understanding how to defend a network, is having a detailed understanding of how computers communicate over a network. Network interface cards, switches, routers, hubs, and firewalls are the fundamental physical pieces of a network. The way they are connected and the format they use for communication is the network architecture.



1.1.2 Data Packets

After you have established a connection with the network (whether it is physical or wireless), you need to send data. The first part is to identify where you want to send it. All computers (as well as routers and switches), have an IP address that is a series of four numbers between 0 and 255 and is separated by periods, such as 192.168.0.1.

The second part is to format the data for transmission. All data is in binary form (1s and 0s). This binary data is put into packets, all less than about 65,000 bytes. The first few bytes are the header. That header tells where the packet is going, where it came from, and how many more packets are coming as part of this transmission. There is actually more than one header, but for now, we will just discuss the header as a single entity. Some attacks (IP spoofing, for example) try to change the header of packets in order to give false information. Other methods of attacks simply try to intercept packets and read the content (thus compromising the data).

A packet can have multiple headers. In fact, most packets will have at least three headers. The IP header has information such as IP addresses for the source and destination, as well as what protocol the packet is. The TCP header has information such as port number. The Ethernet header has information such as the MAC address for the source and destination. If a packet is encrypted with Transport Layer Security (TLS), it will also have a TLS header.

1.1.3 IP Addresses

The first major issue to understand is how to get packets to their proper destination. Even small networks have many computers that could potentially be the final destination of any packet sent. The Internet has millions of computers spread out across the globe. How do you ensure that a packet gets to its proper destination? The problem is not unlike addressing a letter and ensuring it gets to the correct destination. Let's begin by looking at IP version 4 addressing because it is the most common in use today. This section also briefly discusses IP version 6.

An IP version 4 address is a series of four three-digit numbers separated by periods (An example is 192.168.1.1.) Each of the three-digit numbers must be between 0 and 255. An address of 192.168.0.257 would not be a valid one. The reason for this rule is that these addresses are actually four binary numbers: The computer simply displays them to you in decimal format.

Table 1-1 IP version 4 Address

Type of Address	First Octet	Second Octet	Third Octet	Fourth Octet
IP address	192	168	1	1
Subnet mask	255	255	255	0

Recall that 1 byte is 8 bits (1s and 0s), and an 8-bit binary number converted to decimal format will be between 0 and 255. The total of 32 bits means that approximately 4.2 billion possible IP version 4 addresses exist.

Table 1-2 Decimal-to-Binary Conversion Example

128	64	32	16	8	4	2	1	Decimal Equivalent
1	1	1	0	0	0	0	0	224
1	0	1	0	1	0	1	0	170
0	1	0	1	0	1	0	1	85

The IP address of a computer tells you a lot about that computer. The first byte (or the first decimal number) in an address reveals what network class that machine belongs to. Table 1-3 summarizes the five network classes.

Table 1-3 Five Network Classes

Class	IP Range	Use
A	0-126	Used for large networks. All of them have been used
B	128-191	Large corporate and government networks. All of them have been used
C	192-223	Most common group of IP addresses.
D	224-247	Reserved for multicasting
E	248-255	Reserved for experimental use.

The IP range of 127 is not listed in the above table. The IP address 127.0.0.1 designates the machine you are on, regardless the IP address assigned to your machine. This address is referred as the loopback address. That address is used in testing the machine and the NIC card.

These particular classes are important as they tell you what part of the address represents the network and what part represents the node. For example, in a Class A address, the first octet represents the network, and the remaining three represent the node. In a Class B address, the first two octets represent the network, and the second two represent the node. And finally, in a Class C address, the first three octets represent the network, and the last represents the node. There are also some very specific IP addresses and IP address ranges you should be aware of.

The first, as previously mentioned, is 127.0.0.1, or the loopback address. It is another way of referring to the network interface card of the machine you are on. Private IP addresses are another issue to be aware of. Certain ranges of IP addresses have been designated for use within networks.

These cannot be used as public IP addresses but can be used for internal

Workstations and servers. Those IP addresses are:

- **10.0.0.10 to 10.255.255.255**
- **172.16.0.0 to 172.31.255.255**
- **192.168.0.0 to 192.168.255.255**

Sometimes people who are new to networking, have some trouble understanding public and private IP addresses. A good example is an office building. Within a single office building, each office number must be unique. You can only have one 101. And within that building, if you refer office 101 it is immediately clear what you are talking about.

But there are other office buildings, many of which have their own office 101. You can think of private IP addresses as office numbers. They must be unique within their network, but there may be other networks with the same private IP. Public IP addresses are more like traditional mailing addresses. Those must be unique worldwide.

When communicating from office to office you can use the office number, but to get a letter to another building you have to use the complete mailing address. It is much the same with networking. You can communicate within your network using private IP addresses, but to communicate with any computer outside your network, you have to use public IP addresses.

One of the roles of a gateway router is to perform what is called network address translation (NAT). Using NAT, a router takes the private IP address on outgoing packets and replaces it with the public IP address of the gateway router so that the packet can be routed through the Internet.

We have already discussed IP version 4 network addresses. Now let's turn our attention to subnetting. Subnetting is simply splitting 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 subnetworks? 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, 224, or 128. Your computer will take your network IP address and the subnet mask and use a binary AND operation to combine them.

It may surprise you to know that you already have a subnet mask even if you have not used subnetting. If you have a Class C IP address, then your network subnet mask is 255.255.255.0. If you have a Class B IP address, then your subnet mask is 255.255.0.0. And finally, if it is Class A, your subnet mask is 255.0.0.0.

Now think about these numbers in relationship to binary numbers. The decimal value 255 converts to 11111111 in binary. So you are literally "masking" the portion of the network address that is used to define the network, and the remaining portion is used to define individual nodes. Now if you want fewer than 255 nodes in your subnet, then you need something like 255.255.255.240 for your subnet. If you convert 240 to binary, it is 11110000. That means the first three octets and the first 4 bits of the last octet define the network. The last 4 bits of the last octet define the node. That means you could have as many as 1111 (in binary) or 15 (in decimal) nodes on this subnetwork. This is the basic essence of subnetting.

Subnetting only allows you to use certain, limited subnets. Another approach is CIDR, or classless interdomain routing. Rather to 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 addresses. This is the most common way to define network IP addresses today.

You should not be concerned that new IP addresses are likely to run out soon. The IP version 6 standard is already available and methods are in place already to extend the use of IPv4 addresses. The IP addresses come in two groups: public and private.

The public IP addresses are for computers connected to the Internet. No two public IP addresses can be the same. However, a private IP address, such as one on a private company network, has to be unique only in that network. It does not matter if other computers in the world have the same IP address, because this computer is never connected to those other worldwide computers.

Network administrators often use private IP addresses that begin with a 10, such as 10.102.230.17. The other private IP addresses are 172.16.0.0–172.31.255.255 and 192.168.0.0–192.168.255.255.

Also, note that an ISP often will buy a pool of public IP addresses and assign them to you when you log on. Therefore, an ISP might own 1,000 public IP addresses and have 10,000 customers. Because all 10,000 customers will not be online at the same time, the ISP simply assigns an IP address to a customer when he or she logs on, and the ISP un-assigns the IP address when the customer logs off.

IPv6 utilizes a 128-bit address (instead of 32) and utilizes a hex numbering method in order to avoid long addresses such as 132.64.34.26.64.156.143.57.1.3.7.44.122.111.201.5.

The hex address format appears in the form of 3FFE:B00:800:2::C, for example. This gives you 2128 possible addresses (many trillions of addresses), so no chance exists of running out of IP addresses in the near future.

There is no subnetting in IPv6. Instead, it only uses CIDR. The network portion is indicated by a slash followed by the number of bits in the address that are assigned to the network portion, such as

- /48
- /64

There is a loopback address for IPv6, and it can be written as ::/128.

Other differences between IPv4 and IPv6 are described here:

- Link/machine-local.
- IPv6 version of IPv4's APIPA or Automatic Private IP Addressing. So if the machine is configured for dynamically assigned addresses and cannot communicate with a DHCP server, it assigns itself a generic IP address. DHCP, or Dynamic Host Configuration Protocol, is used to dynamically assign IP addresses within a network.
- IPv6 link/machine-local IP addresses all start with fe80::. So if your computer has this address, that means it could not get to a DHCP server and therefore made up its own generic IP address.
- Site/network-local.
- IPv6 version of IPv4 private address. In other words, these are real IP addresses, but they only work on this local network. They are not routable on the Internet.
- All site/network-local IP addresses begin with FE and have C to F for the third hexadecimal digit: FEC, FED, FEE, or FEF.
- DHCPv6 uses the Managed Address Configuration Flag (M flag).
- When set to 1, the device should use DHCPv6 to obtain a stateful IPv6 address.
- Other stateful configuration flag (O flag).
- When set to 1, the device should use DHCPv6 to obtain other TCP/IP configuration settings. In other words, it should use the DHCP server to set things like the IP address of the gateway and DNS servers.

1.1.4 Uniform Resource Locator (URL)

For most people, the main purpose for getting on the Internet is web pages (but there are other things such as e-mail and file downloading). If you had to remember IP addresses and type those in, then surfing the Net would be difficult. Fortunately, you do not have to. You type in domain names that make sense to humans and those are translated into IP addresses. For example, you might type in www.microsoft.com to go to Microsoft's website.

Your computer, or your ISP, must translate the name you typed in (called a Uniform Resource Locator, or URL) into an IP address. The DNS (Domain Name Service) protocol, which is introduced along with other protocols a bit later, handles this translation process. Therefore, you are typing in a name that makes sense to humans, but your computer is using a corresponding IP address to connect. If that address is found, your browser sends a packet (using the HTTP protocol) to TCP port 80. If that target computer has software that listens and responds to such requests (like web-server software such as Apache or Microsoft Internet Information Services), then the target computer will respond to your browser's request and communication will be established.

This method is how web pages are viewed. If you have ever received an Error 404: File Not Found, what you're seeing is that your browser received back a packet (from the web server) with error code 404, designating that the web page you requested could not be found. The web server can send back a series of error messages to your web browser, indicating different situations.

E-mail works the same way as visiting websites. Your e-mail client will seek out the address of your e-mail server. Then your e-mail client will use either POP3 to retrieve your incoming e-mail, or SMTP to send your outgoing e-mail. Your e-mail server (probably at your ISP or your company) will then try to resolve the address you are sending to. If you send something to johndoe@gmail.com, your e-mail server will translate that e-mail address into an IP address for the e-mail server at gmail.com, and then your server will send your e-mail there. Note that newer e-mail protocols are out there; however, POP3 is still the most commonly used.

IMAP is now widely used as well. Internet Message Access Protocol operates on port 143. The main advantage of IMAP over POP3 is it allows the client to download only the email headers, and then the user can choose which messages to fully download. This is particularly useful for smart phones.

1.1.5 MAC Addresses

MAC addresses are an interesting topic. A MAC address is a unique address for a network interface card (NIC). Every NIC in the world has a unique address that is represented by a six-byte hexadecimal number. The Address Resolution Protocol (ARP) is used to convert IP addresses to MAC addresses. So, when you type in a web address, the DNS protocol is used to translate that into an IP address. The ARP protocol then translates that IP address into a specific MAC address of an individual NIC.

IEEE assigns the first three bytes (24 bits) of the MAC address to a vendor. This part of the address is known as Organizationally Unique Identifier (OUI). The OUI helps professionals to determine the MAC address manufacturer. The remaining three bytes (24 bits) are assigned by the vendor. The MAC address is equal to 48 bits.

1.1.6 Protocols

Different types of communications exist for different purposes. The different types of network communications are called protocols. A protocol is, essentially, an agreed method of communication. In fact, this definition is exactly how the word protocol is used in standard, non-computer usage. Each protocol has a specific purpose and normally operates on a certain port. The table below lists some of the most important protocols.

Protocol	Purpose	Port
FTP (File Transfer Protocol)	For transferring files between computers	20,21
SSH (Secure Shell)	A secure way to transfer files and remotely login to a system	22
Telnet	Remotely login to a system	23
SMTP (Simple Mail Transfer Protocol)	For sending emails	25
WhoIS	A command to query a target for information	43
DNS (Domain Name Service)	For translating URLs to IP addresses	53
TFTP (Trivial File Transfer Protocol)	Quick but less reliable FTP server	69
HTTP (Hypertext Transfer Protocol)	For displaying web pages	80
POP3 (Post Office Protocol v3)	Retrieves email	110
NNTP (Network News Transfer Protocol)	Used for network news group	119
NetBIOS	An old Microsoft protocol for naming systems on a local network	137,138,139
IRC (Internet Relay Chat)	Chat Room	194
HTTPS (Secure Hypertext Transfer Protocol)	Encrypted HTTP (SSL/TLS)	443
SMB (Server message Block)	Used by Microsoft Active Directory	445
ICMP (Internet Control Message Protocol)	Simple packets containing error messages, informational and control messages	No specific port

You should note that this list is not complete and hundreds of other protocols exist. All these protocols are part of a suite of protocols referred to as TCP/IP (Transmission Control Protocol/Internet Protocol).

The most important thing for you to realize is that the communication on networks takes place via packets, and those packets are transmitted according to certain protocols, depending on the type of communication that is occurring.

You might be wondering what a port is. Don't confuse this type of port with the connections on the back of your computer, such as a serial port or parallel port. A port in networking terms is a handle, a connection point. It is a numeric designation for a particular pathway of communications.

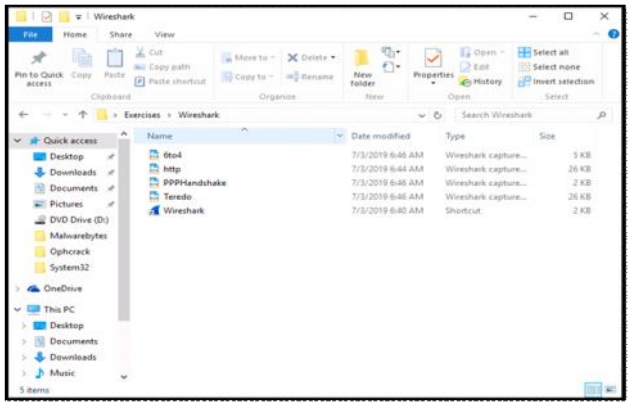
All network communication, regardless of the port used, comes into your computer through the connection on your NIC. You might think of a port as a channel on your TV. You probably have one cable coming into your TV but you can view many channels. You have one cable coming into your computer, but you can communicate on many different ports.

Guided Exercise: Analysing Network Traffic

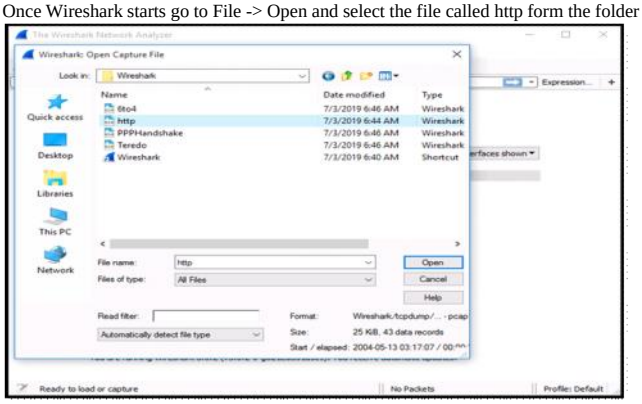
1.2 Guided Exercise: Analysing Network Traffic

Resources	
Files	http.pcap
Machines	Windows 10

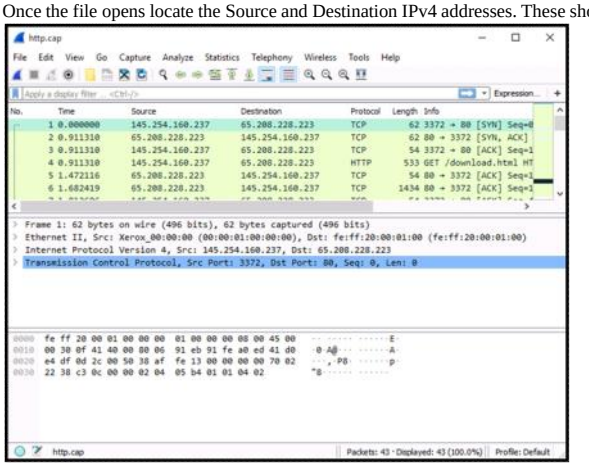
In this exercise you will use Wireshark to analyse network traffic.
Wireshark is already installed and you may start it by openening the Desktop folder called Exercises and then Wireshark. Double click Wireshark to open it.



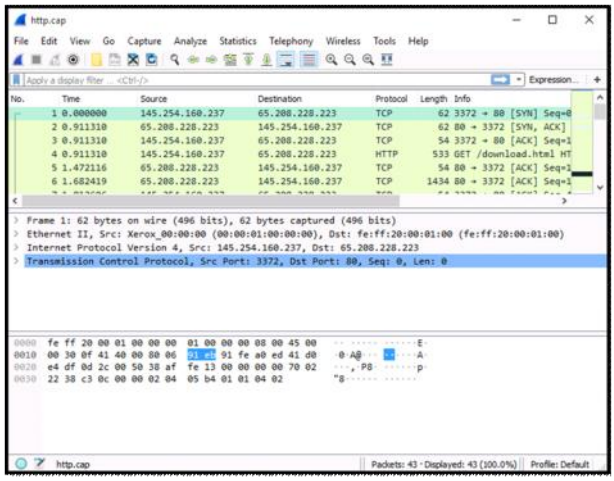
Once Wireshark starts go to File -> Open and select the file called http form the folder Exercises -> Wireshark.



Once the file opens locate the Source and Destination IPv4 addresses. These should be 145.254.160.237 and 65.208.228.223 respectively.



Determine the Source Port and the Destination Port. These should be 3372 and 80 respectively.

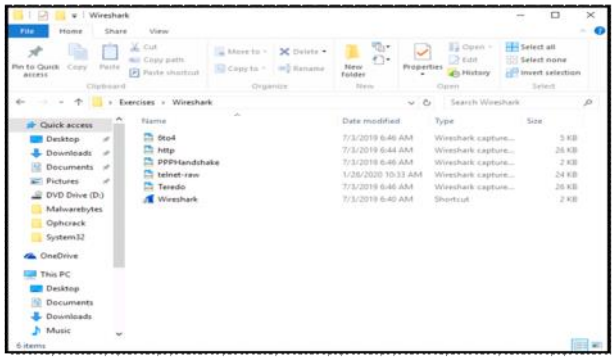


Guided Exercise: Analysing Telnet Network Traffic

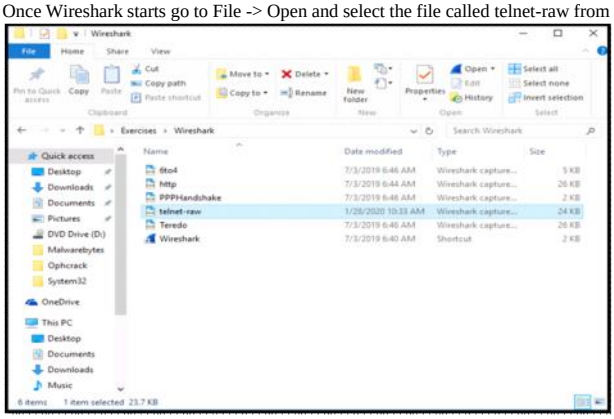
1.3 Guided Exercise: Analysing Telnet Network Traffic

Resources	
Files	None
Machines	Windows 10

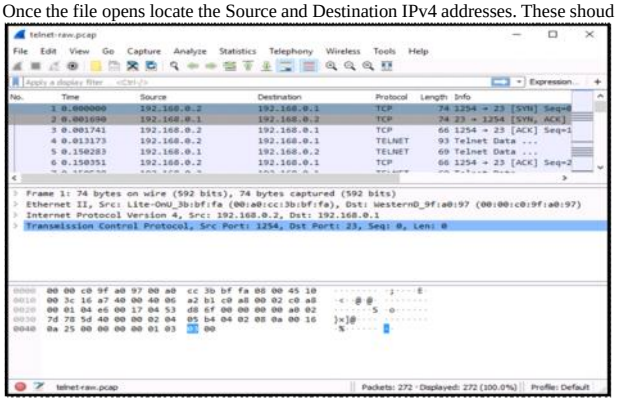
In this exercise you will use Wireshark to analyse network traffic.
Wireshark is already installed and you may start it by opening the Desktop folder called Exercises and then Wireshark. Double click Wireshark to open it.



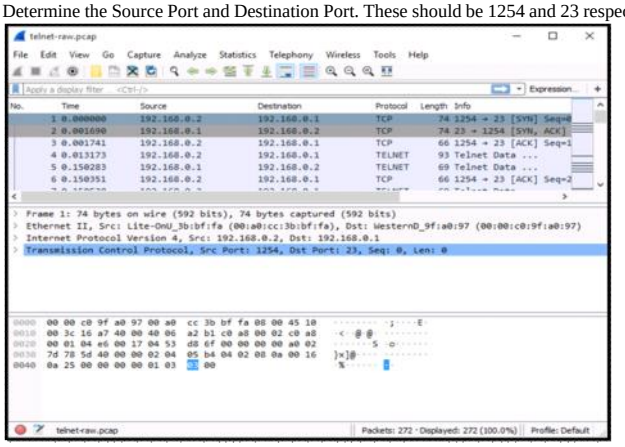
Once Wireshark starts go to File -> Open and select the file called telnet-raw from the folder Exercises -> Wireshark.



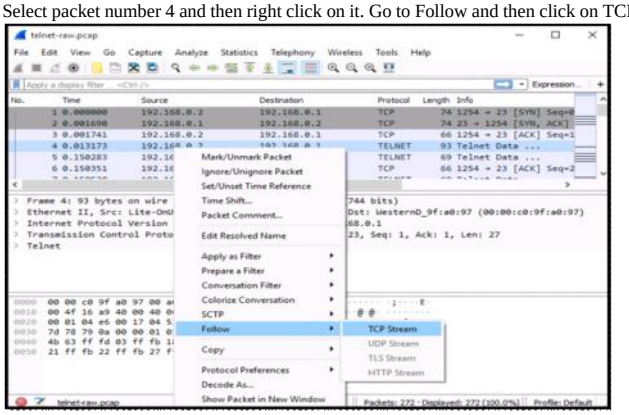
Once the file opens locate the Source and Destination IPv4 addresses. These shoud be 192.168.0.2 and 192.168.0.1 respectively.



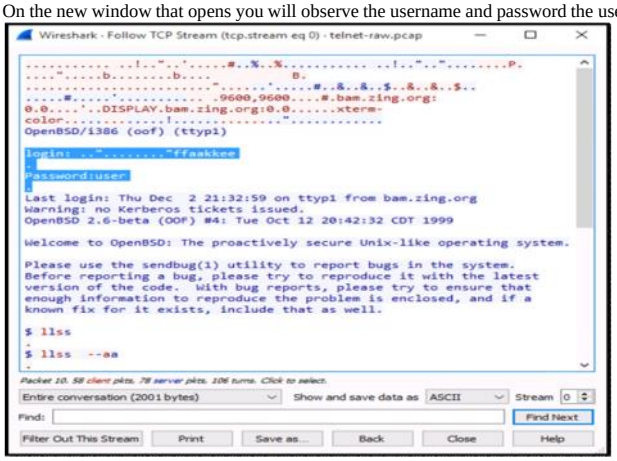
Determine the Source Port and Destination Port. These should be 1254 and 23 respectively.



Select packet number 4 and then right click on it. Go to Follow and then click on TCP Stream.



On the new window that opens you will observe the username and password the user used to login to the telnet server. This username is “fake” and the password is “user”.



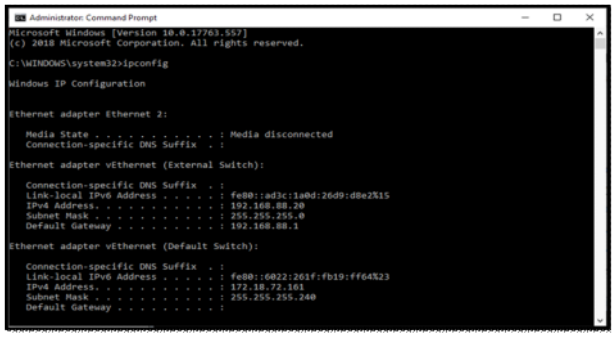
Basic Network Utilities

1.4 Basic Network Utilities

Now that you know what IP addresses and URLs are, you need to be familiar with some basic network utilities. You can execute some network utilities from a command prompt (Windows) or from a shell (Unix/Linux). Many people are already familiar with Windows, so we will focus on how to execute the commands from the Windows command-prompt perspective. However, these utilities are available in all operating systems.

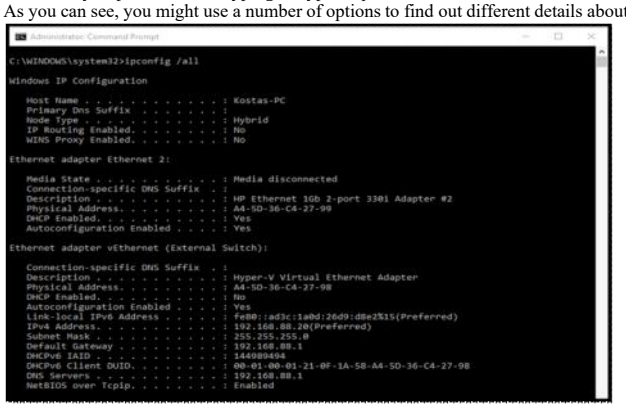
1.4.1 Ipconfig

The first thing you want to do is get information about your own system. To accomplish this, you must get a command prompt. In Windows, you do this by going to the Start menu, selecting All Programs, and then choosing Accessories. You can also go to Start, Run, and type cmd to get a command prompt. In Windows 10 you go to Search and type cmd. Now you can type in ipconfig. (You could input the same command in UNIX or Linux by typing in ifconfig from the shell.) After typing in ipconfig (ifconfig or ip addr in Linux), you should see something much like the below screenshot.



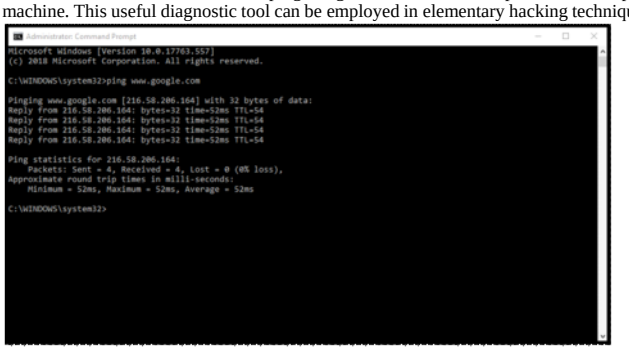
This command gives you information about your connection to a network (or to the Internet). Most importantly, you find out your own IP address. The command also has the IP address for your default gateway, which is your connection to the outside world. Running the ipconfig command is a first step in determining your system’s network configuration. Most commands including ipconfig have a number of parameters, or flags, which can be passed to the commands to make the computer behave in a certain way. You can find out what these commands are by typing in the command, followed by a space, and then typing in hyphen question mark: -?.

As you can see, you might use a number of options to find out different details about your computer’s configuration. The most commonly used method would probably be ipconfig/all.



1.4.2 Ping

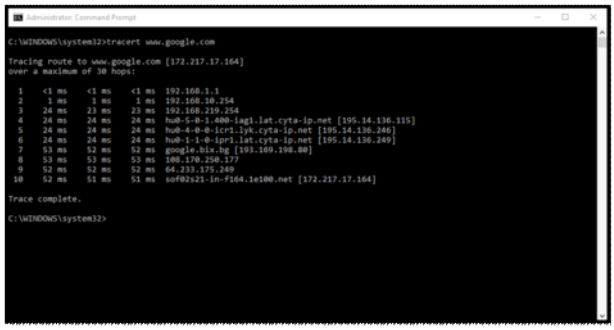
Another common used command is ping. Ping is used to send a test packet, or echo packet, to a machine to find out whether the machine is reachable and how long the packet takes to reach the machine. This useful diagnostic tool can be employed in elementary hacking techniques. Figure 1-3 shows the command.



The above command shows that a 32-byte echo packet was sent to the destination and returned. The TTL means “time to live.” That time unit is how many intermediary steps, or hops, the packet should take to the destination before giving up. Remember that the Internet is a vast conglomerate of interconnected networks. Your packet probably won’t go straight to its destination. It will have to take several hops to get there. As with ipconfig, you can type in ping -? to find out various ways you can refine your ping.

1.4.3 Tracert

The next command is tracert. This command is a sort of “ping deluxe.” Tracert not only tells you whether the packet got there and how long it took, but it also tells you all the intermediate hops it took to get there. (This same command can be executed in Linux or UNIX, but it is called traceroute rather than tracert.) You can see this utility in Figure 1-4.



With tracert, you can see (in milliseconds) the time 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.

1.4.4 Netstat

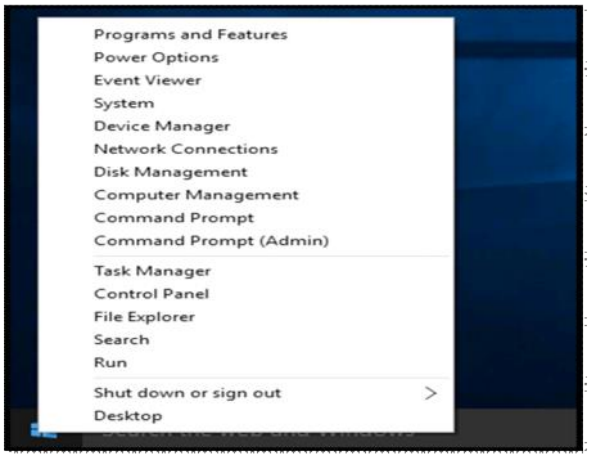
Netstat is another interesting command. It is an abbreviation for Network Status. Essentially, this command tells you what connections your computer currently has. Don't panic if you see several connections; that does not mean a hacker is in your computer. You will see many private IP addresses. This means your network has internal communication going on. You can see this in Figure 1-5. Certainly, other utilities can be used when working with network communications. However, the four we just examined are the core utilities. These four (ipconfig, ping, tracert, and netstat) are absolutely essential to any network administrator.

Guided Exercise: Using Basic Network Utilities

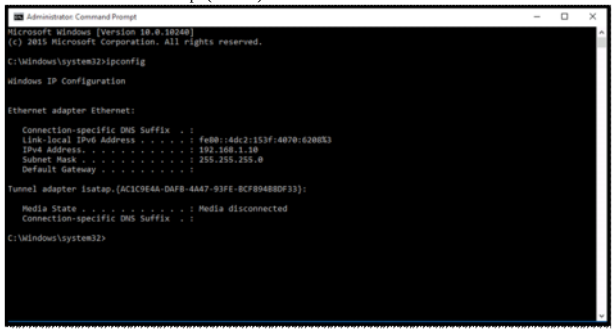
1.5 Guided Exercise: Using Basic Network Utilities

Resources	
Files	None
Machines	Windows 10, Windows Server 2012, Ubuntu Server

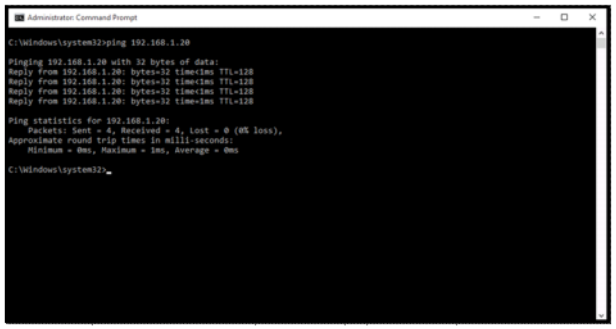
In this exercise, you will use basic network utilities.
Use the ipconfig command on Windows 10 to identify the IP address.
Login to Windows 10 using the following credentials:
Username: Admin
Password: Pa$$w0rd
Once logged in right click on Start button.



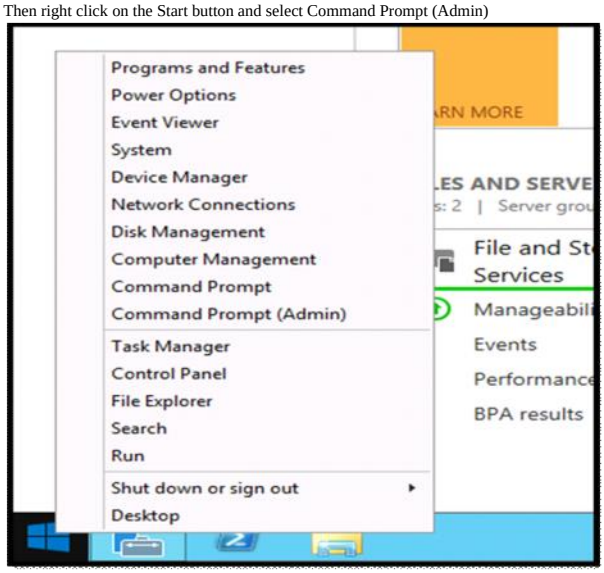
Then select Command Prompt (Admin) and click Yes on the User Account Control window. On the command prompt window write the command ipconfig and then press the enter button.



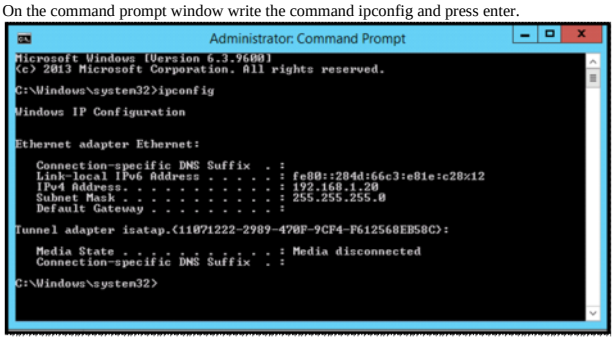
Use the ping command on Windows 10 to ping the host 192.168.1.20



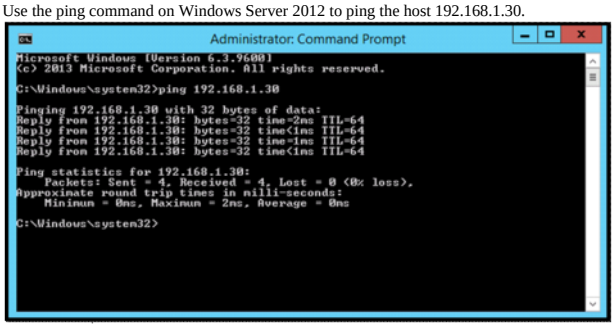
Use the ipconfig command on Windows Server 2012 to identify the IP address.
Login to Windows Server 2012 using the following credentials:
Username: Administrator
Password: Pa$$w0rd
Then right click on the Start button and select Command Prompt (Admin)



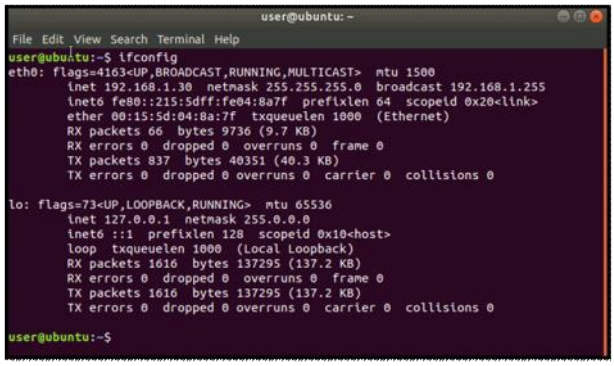
On the command prompt window write the command ipconfig and press enter.



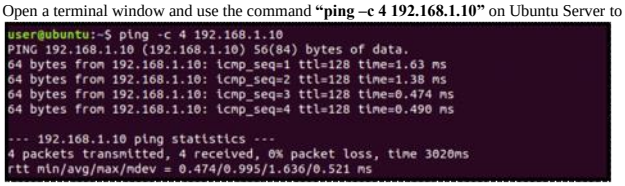
Use the ping command on Windows Server 2012 to ping the host 192.168.1.30.



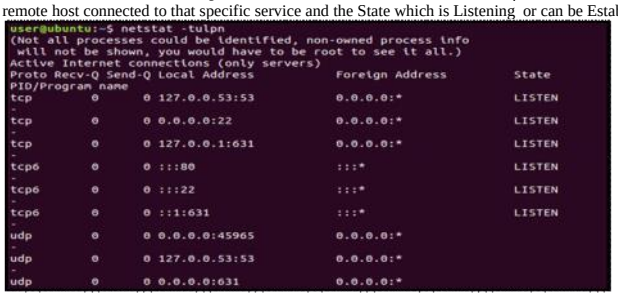
Use the ifconfig command on Ubuntu Server to identify the IP address. Login with the following credentials:
Username: user
Password: Pa$$w0rd
Once logged in click on the terminal icon (last icon) the left side menu.
On the terminal window write the command ifconfig and press enter.



Open a terminal window and use the command **"ping –c 4 192.168.1.10"** on Ubuntu Server to ping the host 192.168.1.10.



Use the command **"netstat -tulpn"** on the Ubuntu Server and observe the output. You will notice the Local Address bound with a port which is a specific service listening on that port and the Foreign Address which is a remote host connected to that specific service and the State which is Listening or can be Established in the case of a remote host connection.

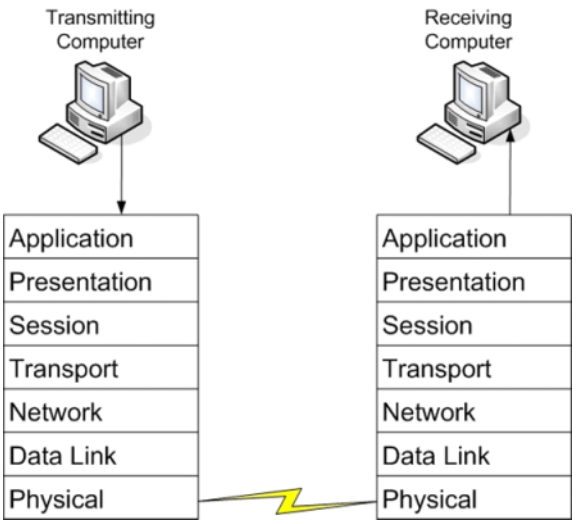


Use the command **"netstat –a"** on the Windows Server 2012 and observe the output. You will notice the Local Address bound with a port which is a specific service listening on that port and the Foreign Address which is a remote host connected to that specific service and the State which is Listening or can be Established in the case of a remote host connection.

The OSI Model

1.6 The OSI Model

The Open Systems Interconnect (OSI) model describes how networks communicate (see Table 1-3). It describes the various protocols and activities and states how the protocols and activities relate to each other. This model is divided into seven layers. It was originally developed by the International Organisation for Standardization (ISO) in the 1980s.



Layer	Description	Protocols
Application (7)	This layer interfaces directly to applications and performs common application services for the application processes	POP, SMTP, DNS, FTP, Telnet, HTTP
Presentation (6)	Relieves the application layer of concern regarding syntactical differences in data representation within the end-user systems.	Network Data Representation (NDR), Lightweight Presentation Protocol (LPP)
Session (5)	Provides the mechanism for managing the dialogue between end-user application processes	NetBIOS
Transport	Provides end-to-end communication control	TCP,UDP

(4)		
Network (3)	Routes information in the network	IP,ARP,ICMP
Data Link (2)	Describes the logical organisation of data bits transmitted on a particular medium. The data link layer is divided in two sublayers: the Media Access Control Layer (MAC) and the Logical Link Control Layer (LLC)	SLIP, PPP
Physical (1)	Describes the physical properties of various communication media as well as the electrical properties and interpretation of the exchanged signals. The physical layer is the actual NIC and the Ethernet cable.	IEEE 1394, DSL, ISDN

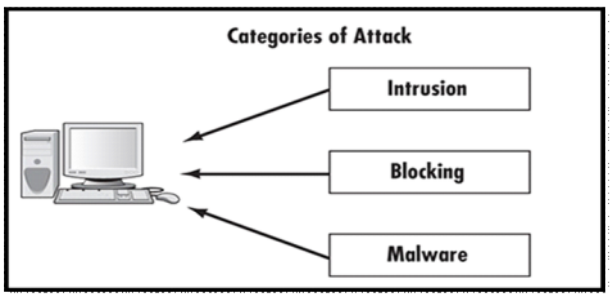
Threat Classification

1.7 Threat Classification

Your network certainly faces real security threats, and these threats can manifest themselves in a variety forms. There are different ways one might choose to classify the various threats to your system. You could choose to classify them by the damage caused, the level of skill required to execute the attack, or perhaps even by the motivation behind the attack. For our purposes we categorize attacks by what they actually do. Based on that philosophy most attacks can be categorized as one of three broad classes:

- Intrusion
- Blocking
- Malware

Figure 1-6 shows the three categories. The intrusion category includes attacks meant to breach security and gain unauthorised access to a system. This group of attacks includes any attempt to gain unauthorised access to a system. This is generally, what hackers do. The second category of attack, blocking, includes attacks designed to prevent legitimate access to a system. Blocking attacks are often called denial of service attacks (or simply DoS). In these types of attacks, the purpose is not to actually get into your system but simply to block legitimate users from gaining access. The third category of threats is the installation of malware on a system. Malware is a generic term for software that has a malicious purpose. It includes virus attacks, Trojan horses, and spyware.



1.7.1 Malware

Malware is probably the most common threat to any system, including home users' systems, small networks, and large enterprise wide-area networks. One reason is that malware is designed to spread on its own, without the creator of the malware having to be directly involved. This makes the malware attack much easier to spread across the Internet, and hence more widespread.

The most obvious example of malware is the computer virus. You probably have a general idea of what a virus is. If you consult different textbooks you will probably see the definition of a virus worded slightly differently. One definition for a virus is "a program that can 'infect' other programs by modifying them to include a possibly evolved copy of itself." A computer virus is analogous to a biological virus in that both replicate and spread. The most common method for spreading a virus is using the victim's e-mail account to spread the virus to everyone in his address book. Some viruses do not actually harm the system itself, but all of them cause network slowdowns or shutdowns due to the heavy network traffic caused by the virus replication.

Another type of malware, often closely related to the virus, is the Trojan horse. The term is borrowed from the ancient tale. In this tale, the city of Troy was besieged for a long period of time, but the attackers could not gain entrance. They constructed a huge wooden horse and left it one night in front of the gates to Troy. The next morning, the residents of Troy saw the horse and assumed it a gift, consequently rolling the wooden horse into the city. Unbeknownst to them, several soldiers were hidden inside the horse. That evening, the soldiers left the horse, opened the city gates, and let their fellow attackers into the city.

An electronic Trojan horse works in the same manner, appearing to be benign software but secretly downloading a virus or some other type of malware onto your computer. In short, you have an enticing gift that you install on your computer, and later find out it has unleashed something quite different from what you expected. It is a fact that Trojan horses are more likely to be found in illegitimate software. There are many places on the Internet to get pirated copies of commercial software. Finding that such software is actually part of a Trojan horse is not at all uncommon.

Trojan horses and viruses are the two most widely encountered forms of malware. A third category of malware is spyware, which is increasing in a dramatic pace. Spyware is software that literally spies on what you do on your computer. This can be as simple as a cookie, a text file that your browser creates and stores on your hard drive.

Cookies are downloaded onto your machine by websites you visit. This text file is then used to recognise you when you return to the same site. That file can enable you to access pages more quickly and save you from having to enter your information multiple times on pages you visit frequently. However, in order to do this, that file must be read by the website; this means it can also be read by other websites. Any data that the file saves can be retrieved by any website, so your entire Internet browsing history can be tracked.

Another form of spyware, called a key logger, records all of your keystrokes. Some also take periodic screen shots of your computer. Data is then either stored for retrieval later by the party who installed the key logger or is sent immediately back via e-mail. In either case, everything you do on your computer is recorded for the interested party.

1.7.2 Intrusions

Intrusions are those attacks that are actually trying to intrude into the system. They are different from attacks that simply deny users access to the system (blocking), or attacks that are not focused on a particular target such as viruses and worms (malware). Intrusion attacks are designed to gain access to a specific targeted system and are commonly referred to as hacking, although that is not the term hackers use. Hackers call this type of attack cracking, which means intruding onto a system without permission, usually with malicious intent. Any attack designed to breach security, either via some operating system flaw or any other means, can be classified as cracking.

Using security flaws is not the only method for intruding into a system. In fact, some methods can be technologically much easier to execute. For example, one completely not technologically based method for breaching a system's security is called social engineering, which, as the name implies, relies more on human nature than technology. This was the type of attack that the famous hacker Kevin Mitnick most often used. Social engineering uses techniques to get users to offer up the information needed to gain access to a target system. The way this method works is rather simple.

The perpetrator obtains preliminary information about a target organisation, such as the name of its system administrator, and leverages it to gain additional information from the system's users. For example, he might call someone in accounting and claim to be one of the company's technical support personnel. The intruder could use the system administrator's name to validate that claim. He could then ask various questions to learn additional details about the system's specifications. A well-informed intruder might even get a person to provide a username and password. As you can see, this method is based on how well the intruder can manipulate people and actually has little to do with computer skills.

Social engineering and exploiting software flaws are not the only means of executing an intrusion attack. The growing popularity of wireless networks gives rise to new kinds of attacks. The most obvious and dangerous activity is war driving. This type of attack is an offshoot of war-dialing. With war-dialing, a hacker sets up a computer to call phone numbers in sequence until another computer answers to try and gain entry to its system. War driving, using much the same concept, is applied to locating vulnerable wireless networks. In this scenario, a hacker simply drives around trying to locate wireless networks. Many people forget that their wireless network signal often extends as much as 100 feet (thus, past walls). At DEFCON 2003, the annual hackers' convention, contestants participated in a war-driving contest in which they drove around the city trying to locate as many vulnerable wireless networks as they could.

1.7.3 Denial of Service

The third category of attacks is blocking attacks, an example of which is the denial of service attack (DoS). In this attack, the attacker does not actually access the system, but rather simply blocks access to the system from legitimate users. In the words of the CERT (Computer Emergency Response Team) Coordination Centre (the first computer security incident response team), "A 'denial-of-service' attack is characterised by an explicit attempt by attackers to prevent legitimate users of a service from using that service." One often-used blocking method is flooding the targeted system with so many false connection requests that it cannot respond to legitimate requests. DoS is an extremely common attack method.

Security Terminology

1.8 Security Terminology

Security professionals have specific terminology. Individuals or system administrators having experience in network administration are probably already familiar with most of these terms. Although most hacking terminology describes the activity or the person performing it (phreaking, sneaker, etc.).

The first and most basic security device is the firewall. A firewall is a barrier between a network and the outside world. Sometimes a firewall is a stand-alone server, sometimes a router, and sometimes software running on a machine. Whatever it's physical form, the purpose is the same: to filter traffic entering and exiting a network. Firewalls are related to, and often used in conjunction with, a proxy server. A proxy server hides your internal network IP addresses and presents a single IP address (its own) to the outside world.

Firewalls and proxy servers are added to networks to provide basic perimeter security. They filter incoming and outgoing network traffic but do not affect traffic on the network. Sometimes these devices are augmented by an intrusion-detection system (IDS). An IDS monitor's traffic looking for suspicious activity that might indicate an attempted intrusion.

Access control is another important computer security term. Access control is the aggregate of all measures taken to limit access to resources. This includes logon procedures, encryption, and any method that is designed to prevent unauthorised personnel from accessing a resource. Authentication is clearly a subset of access control, perhaps the most basic security activity.

Authentication is simply the process of determining whether the credentials given by a user or another system, such as a username and password, are authorised to access the network resource in question. When a user logs in with a username and password, the system attempts to authenticate that username and password. If they are authenticated, the user will be granted access.

Non-repudiation is another term you encounter frequently in computer security. It is any technique that is used to ensure that someone performing an action on a computer cannot falsely deny that they performed that action. Non-repudiation provides reliable records of what user took a particular action at a specific time. In short, it is methods to track what actions are taken by what user. Various system logs provide one method for non-repudiation. One of the most important security activities is auditing. Auditing is the process of reviewing logs, records, and procedures to determine whether they meet standards.

Least privilege is a concept you should keep in mind when assigning privileges to any user or device. The concept is that you only assign the minimum privileges required for that person to do his job, no more. Keep this simple but critical concept in mind.

You should also keep in mind the CIA triad, or Confidentiality, Integrity, and Availability. All security measures should affect one or more of these areas. For example, hard drive encryption and good passwords help protect confidentiality. Digital signatures help ensure integrity, and a good backup system, or network server redundancy, can support availability.

1.8.1 Hacking Terminology

Note that hacking terminology is not precise, and that many definitions can be debated. No "official" hacker vocabulary exists. The terms evolve through their use by the hacker community. Clearly, beginning this examination by defining hacker, a term used in movies and news broadcasts, would be sensible.

Most people use it to describe any person who breaks into a computer system. However, security professionals and hackers themselves use this term differently. In the hacking community, a hacker is an expert on a particular system or systems who wants to learn more about the system. Hackers feel that looking at a system's flaws is the best way to learn about it.

For example, someone well versed in the Linux operating system who works to understand that system by learning its weaknesses and flaws would be a hacker. However, this does often means seeing whether a flaw can be exploited to gain access to a system. This "exploiting" part of the process is where hackers differentiate themselves into three groups:

- White hat hackers, upon finding vulnerability in a system, will report the vulnerability to the vendor of that system. For example, if they were to discover some flaw in Red Hat Linux, they would then e-mail the Red Hat company (probably anonymously) and explain what the flaw is and how it was exploited.
- Black hat hackers are the people normally depicted in the media (e.g., movies and news). After they gain access to a system, their goal is to cause some type of harm. They might steal data, erase files, or deface websites. Black hat hackers are sometimes referred to as crackers.
- Grey hat hackers are typically law-abiding citizens, but in some cases will venture into illegal activities. They might do so for a wide variety of reasons. Commonly, grey hat hackers conduct illegal activities for reasons they feel are ethical, such as hacking into a system belonging to a corporation that the hacker feels is engaged in unethical activities.

Approaches of Network Security

1.9 Approaches of Network Security

Organisations can choose from several approaches to network security. A particular approach, or paradigm, will influence all subsequent security decisions and set the tone for the entire organisation's network security infrastructure. Network security paradigms can be classified by either the scope of security measures taken (perimeter, layered) or how proactive the system is.

1.9.1 Perimeter Security Approach

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, and any technology or procedure that makes unauthorised access of the network less likely. Little or no effort is made to secure the systems within the network. In this approach, the perimeter is secured, but the various systems within that perimeter are often vulnerable.

This perimeter approach is clearly flawed. So why do some companies use it? A small organisation might use the perimeter approach if they have budget constraints or inexperienced network administrators. This method might be adequate for small organisations that do not store sensitive data, but it rarely works in a larger corporate setting.

1.9.2 Layered Security Approach

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 that, if perimeter security is compromised, not all internal systems are affected. Layered security is the preferred approach whenever possible.

You should also measure your security approach by how proactive and/or reactive it is. You do this by determining how much of the system's security infrastructure and policies are dedicated to preventive measures as opposed to how much are devoted to simply responding to an attack after it has occurred.

A passive security approach takes few or no steps to prevent an attack. Conversely a dynamic security approach, or proactive defence, is one in which steps are taken to prevent attacks before they occur. One example of a proactive defence is the use of an IDS, which works to detect attempts to circumvent security measures. These systems can tell a system administrator that an attempt to breach security has been made, even if that attempt is not successful. An IDS can also be used to detect various techniques intruders use to assess a target system, thus alerting a network administrator to the potential for an attempted breach before the attempt is even initiated.

1.9.3 Hybrid Security Approach

In the real world, network security is rarely completely in one paradigm or another. Networks generally fall along a continuum with elements of more than one security paradigm. The two categories also combine to form a hybrid approach. One can have a network that is predominantly passive but layered, or one that is primarily perimeter, but proactive. Considering approaches to computer security along a Cartesian coordinate system, with the x axis representing the level of passive-active approaches and the y axis depicting the range from perimeter to layered defence, can be helpful. The most desirable hybrid approach is a layered paradigm that is dynamic.

Law and Network Security

1.10 Law and Network Security

An increasing number of legal issues affect how administrators approach network security. If your organisation is a publicly traded company, a government agency, or does business with either, there may be legal constraints to choose your security approach. Legal constraints include any laws that affect how information is stored or accessed. Even if your network is not legally bound to these security guidelines, reviewing the various laws impacting computer security and perhaps deriving ideas that can apply to your own security standards is useful.

One of the oldest pieces of legislation in the United States affecting computer security is the Computer Security Act of 1987 (100th Congress, 1987). This act requires government agencies to identify sensitive systems, conduct computer security training, and develop computer security plans. This law is a vague mandate ordering federal agencies in the United States to establish security measures without specifying any standards.

This legislation established a legal mandate to enact specific standards, paving the way for future guidelines and regulations. It also helped define certain terms, such as what information is indeed "sensitive," according to the following quote found in the legislation itself:

Sensitive information is any information, the loss, misuse, or unauthorised access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorised under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defence or foreign policy.

Keep this definition in mind, for it is not just Social Security information or medical history that must be secured. When considering what information needs to be secure, simply ask the question: Would the unauthorised access or modification of this information adversely affect my organisation? If the answer is "yes," then you must consider that information "sensitive" and in need of security precautions.

Computer Misuse Act 1990 is the base law for all other computer related laws in the UK. It applies to the whole of UK and is usually the underlying law used to charge a suspect over a computer crime. Crimes like credential stealing, hacking and phishing are considered Section 1 offences, which can lead to 6 months to 2 years in prison. Section 2 crimes are the crimes intended to be performed, after a hacker has penetrated the system, such as using the credentials stolen to access a server, or committing fraud. Guilty with the section 2 act of the computer misuse act can lead to up to 5 years in prison.

Keep in mind that any law that governs privacy (such as the Health Insurance Portability and Accountability Act [HIPAA], for medical records) also has a direct impact on computer security. If a system is compromised and data that is covered under any privacy statute is compromised, you might need to prove that you exercised due diligence to protect that data. A finding that you did not take proper precautions can result in civil liability.

QUIZ:

1. Blocking attacks seek to accomplish what?

2. The most desirable approach to security is one which is:

3. Server Message Block (SMB) protocol runs on which port?

4. What is the acronym of URL.

5. Malware is NOT a common threat for systems.

6. Class A IPs with range 0-126 are reserved for multicasting.

7. Subnetting is used to split a network into smaller portions.

8. Trivial File Transfer Protocol (TFTP) runs on which port?

9. Which of the following is the best definition for non-repudiation?

10. Which of the following is NOT one of the three major classes of threats?