Network security is essential in today's world. Nowadays, a computer system is useless unless it is networked together with other systems. Networks are used to get information from point A to point B. That's what the world is all about—sending and receiving information. With the explosion of Internet, it's now easier and more convenient than ever. But along with the ease and convenience comes risk. It's almost riskier than ever to send information. The more methods that are developed to share information, the more exploits are developed.

General Network Concepts and Vulnerabilities

There are general network concepts that must be understood in order to get a better understanding of some of the more advanced concepts. The different network features and functions can take a variety of forms and can be implemented in a variety of ways. You have to understand these concepts and what they mean before you can understand the devices that implement them.

OSI Model

The OSI model is the Open Systems Interconnection model. It was developed by the International Standards Organization (ISO). The OSI model approaches network communication using
a layered approach. Each layer consists of different protocols and functions. The OSI model has seven layers: physical, data link, network, transport, session, presentation, and application.

**Physical Layer**
The physical layer (Layer 1) is the lowest layer of the OSI model. The physical layer deals with device interaction with the physical medium. The physical layer references the bits and electric signals that travel through the network medium. Some examples of devices that exist at the physical layer are hubs, repeaters, and network adapters.

**Data Link Layer**
The data link layer (Layer 2) of the OSI model actually consists of two sublayers: the Media Access Control (MAC) sublayer and the Logical Link Control (LLC) sublayer. The MAC sublayer controls device interaction. The LLC sublayer deals with addressing and multiplexing. Physical addressing for network connections exists at the data link layer. The data link layer combines data bits into entities called frames. Network topologies like Ethernet exist at the data link layer. Network switches are the most common network devices that exist at the data link layer.

**Network Layer**
The network layer (Layer 3) of the OSI model controls logical addressing of network systems and devices. These logical addresses are used when one system wants to talk to another system. Network layer addresses are used not only to identify the system but also to determine what network the system resides on. The network layer combines multiple frames into units called packets. Routers are the most common devices that operate at the network layer. Some common protocols that exist at the network layer are Internet Protocol (IP), Internet Protocol Security (IPSec), and Internet Control Message Protocol (ICMP).

**Transport Layer**
The transport layer (Layer 4) of the OSI model controls link reliability. The transport layer is responsible for flow control and error control. The transport layer combines network packets into units called segments. The Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) exist at the transport layer.
Session Layer
The session layer (Layer 5) of the OSI model controls connections between computers. These connections are called sessions. The session layer establishes, maintains, and terminates sessions between computers. The Network File System (NFS) and Server Message Block (SMB) protocols exist at the session layer.

Presentation Layer
The presentation layer (Layer 6) of the OSI model allows for interaction between different application layer implementations. The presentation layer provides somewhat of a translation between two different types of applications. Application layer implementations can use different formats and speak different “languages,” as long as the presentation layer translates the data for them.

Application Layer
The application layer (Layer 7) is the highest layer of the OSI model. It’s the layer that is closest to the end user. The application layer of the OSI model interacts directly with system applications. Some examples of application layer protocols include Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP).

Network Components
A network is divided into a variety of components. These components range from parts of a single computer to part of the network itself. Each of these components plays a different role in helping a network to function and pass information.

MAC Address
Every network device has a physical address called a MAC address associated with it. This MAC address is used to identify the device on the network. MAC addresses exist at the data link layer of the OSI model. MAC addresses consist of two parts. The first part identifies the manufacturer of the device. Each manufacturer has a different address assigned to it. The second part is assigned to the device by the manufacturer. MAC addresses are burned into the device by the manufacturer. In most cases, this address cannot be changed. Some devices, like network cards, however, have the capability to specify a new MAC address via software configuration. This new address is often called a Locally Administered Address (LAA). But even if you use an LAA, the
original MAC is still present, so the configuration can be reverted at any time.

**IP Address**

An IP address is a logical address assigned to a network system. IP addresses exist at the network layer of the OSI model. IP addresses are defined by the IP in the TCP/IP suite. An IP is divided into two components: the network address and the host address. The network address represents the location of a group of computers. The host address represents the location of a single computer within a network. You can think of the network address as a street name and the host address as the house number. When you are looking at an IP address, the subnet mask is used to determine which portion of the address is the network address and which portion is the host address.

Originally, IP addresses consisted of only 32 bits. They were separated into four octets. But as the Internet grew, we began to run out these addresses. So a new version of IP addressing was developed. It is called IPv6. The original version then began to be termed as IPv4. IPv6 addresses contain 128 bits. This offers a greatly increased number of addresses. IPv6 addressing still has not taken off throughout the Internet. But usage is growing. IPv4 addresses still remain by far the most widely used type of IP on the Internet and inside companies.

There are five classes of IPv4 addresses: Class A, B, C, D, and E. The different classes are characterized by the number of networks available and the number of hosts available on each network. IP address class can be identified by their first octet. Table 3.1 outlines the characteristics of each class.

There are public IP addresses and private IP addresses. Public IP addresses can traverse the Internet. Private IP addresses cannot. Buying enough public IP addresses for everyone in your

<table>
<thead>
<tr>
<th>Class</th>
<th>First Octet Range</th>
<th>Number of Networks</th>
<th>Number of Hosts on Each Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>0 to 127</td>
<td>126 (0 and 127 are reserved)</td>
<td>16,777,214</td>
</tr>
<tr>
<td>B</td>
<td>128 to 191</td>
<td>16,384</td>
<td>65,532</td>
</tr>
<tr>
<td>C</td>
<td>192 to 223</td>
<td>2,097,152</td>
<td>254</td>
</tr>
<tr>
<td>D</td>
<td>224 to 247</td>
<td>Reserved for Multicast Addresses</td>
<td>Reserved for Multicast Addresses</td>
</tr>
<tr>
<td>E</td>
<td>248 to 255</td>
<td>Reserved for Experimental Use</td>
<td>Reserved for Experimental Use</td>
</tr>
</tbody>
</table>
organization can be a difficult task, not only because of the cost but also because of the limited availability of IPv4 addresses. What most organizations do is purchase a few public IP addresses for public-facing entities like external routers. They use private IP addresses for internal devices. Then, the company’s router or firewall will do some sort of translation between the public and private IP addresses. There are certain ranges of IP addresses that have been designated as private by the Internet Assigned Numbers Authority (IANA). They are as follows:

- **Class A**: 10.X.X.X
- **Class B**: 172.16.X.X through 172.31.X.X
- **Class C**: 192.168.X.X

**Collision Domain**

A collision domain is a network segment where network packets can potentially “collide.” A network collision is when two systems attempt to send packets on the same physical segment at the same time. Both of the packets will be discarded. Both systems will then wait for a random wait period before resending their packets. Collisions happen only in networks where two different packets can be on the network at the same time. These are multiaccess network topologies like Ethernet.

**Broadcast Domain**

A broadcast domain is a network segment where network systems can reach one another through a message sent to the network’s broadcast address. Devices on the same network subnet or VLAN are generally in the same broadcast domain.

**NAT**

NAT is Network Address Translation. NAT works at Layer 3 of the OSI model. NAT is used to hide the IP address of internal computers. NAT can be done for security purposes or for scalability purposes. You may not have enough public IP addresses available for all the systems on your network. As an example of how NAT works let’s say Riley wants to connect to a Web server on the Internet. NAT would work as follows:

1. Riley’s computer sends a request to the NAT routing using a private IP address.
2. The NAT router will map Riley’s computer IP address to an outgoing network port. This mapping is stored in its mapping table.
3. The router will then contact the Internet Web server with a connection originating from the previously mapped network port and the router’s externally facing public IP address.
4. The Internet Web server will then respond to the router’s externally facing public IP address on the same port.
5. The router will then look that port up in its mapping table.
6. The router will then send the response back to Riley’s computer.

**PAT**

PAT is Port Address Translation. It is very similar to NAT. Some people consider PAT a subset of NAT. PAT works at Layer 3 and Layer 4 of the OSI model. Not only does PAT hide the source IP address, it also hides the source port. This adds an additional layer of obfuscation.

**DMZ**

A DMZ is a network Demilitarized Zone. A DMZ is a network segment set aside to allow untrusted connections to a company’s network resources. A DMZ usually sits between a company’s internal network and the Internet. A company will put its externally facing Web servers in the DMZ, so if these servers are compromised, the company’s internal network is still safe.

**Network Services and Network Devices**

Network communication consists of different services and devices. Each of these services and devices provides a different function. They also have their own vulnerabilities and exploits associated with them. You need to know what these vulnerabilities and exploits are in order to properly protect your organization.

**DHCP**

DHCP is the Dynamic Host Configuration Protocol. It is used to automatically provide IP addressing information to clients. A DHCP server can assign IP addresses, subnet masks, a DNS server address, and much more. This frees you from having to manually enter this information on all your client systems.

The problem with the DHCP process is that it uses broadcast messages. Clients do not know what DHCP server they should be contacting. They just accept information from the first one that responds. This can be trouble because someone could install a rogue DHCP server on the network. This could be done for malicious reasons or accidentally. Either way, it disrupts your network’s operation. To combat rogue DHCP servers, Microsoft developed the concept of DHCP server activation. Unless a DHCP server is activated, it cannot service DHCP requests in your organization.
DNS

DNS is the Domain Name System. DNS is used to translate computer domain names to IP addresses. Computers are assigned domain names because domain names are easier to remember than IP addresses. In order for one system to talk to another system, they need to know each other’s IP address. A DNS server is used to supply the systems with the IP addresses.

DNS servers contain special types of records. Here are a few:

- **Address (A):** It is used to map host names to IPv4 addresses.
- **Address (AAAA):** It is used to map host names to IPv6 addresses.
- **Canonical Name (CNAME):** It is used as an alias for another name.
- **Name Server (NS):** It is used to denote a DNS server.
- **Mail Exchanger (MX):** It is used to denote a mail server.
- **Domain Name Pointer (PTR):** It is used to point a domain name to an IP address.
- **Start of Authority (SOA):** It is used to denote the Start of Authority for a domain.
- **Sender Policy Framework (SPF):** It is used to validate e-mail sources. They help prevent e-mail spamming.
- **Server selection or Service Location (SRV):** It is used to denote a service residing on a server. Active Directory makes extensive use of SRV records to reference services.

DNS servers are often the victims of attempted denial-of-service attacks. The idea is that if someone can effectively deny access to a DNS server, then the clients who depend on this DNS server will not be able to get to any other servers or network services. You can protect against this through the use of a redundant DNS setup. You can use redundant hardware or set up secondary DNS servers.

**Network Switches**

In general, switches work at the data link layer (Layer 2) of the OSI model. Devices connected via a switch are on separate collision domain. Devices connected via a switch are in the same broadcast domain. Switches do filtering and forwarding based on MAC addresses. Switches keep a MAC table that lists all the devices that it has access to. When someone attempts to connect to a device, the switch knows which port to forward the request out on. If the switch does not know, then an ARP request will be sent. Based on who replies to the broadcast, the switch knows where to forward the traffic.
Routers
Routers work at the network layer (Layer 3) of the OSI model. Routers are used to connect two separate networks, often called subnets. These networks will be in separate broadcast domains. Routers use routing tables to keep track of routes between different networks. Sometimes, there are multiple paths to a given network. Routers will use routing metrics to determine the best, most efficient route to a destination.

Wireless Security and Vulnerabilities
Wireless networks offer a great degree of flexibility. Computers are no longer tied to a desk. They are free to move about your organization. Along with this flexibility, comes an increased administrative burden. The administrator must ensure that these wireless networks run efficiently and securely.

802.11 Standards
Most wireless networks adhere to one of the 802.11 technology standards. These standards define the equipment used to implement the network and the functionality supported. Each standard has different signal ranges, maximum bandwidths, and frequency ranges.

802.11a
802.11a networks operate at a frequency of 5 GHz. They support a maximum data rate of 54 Mbps. Because 802.11a networks use the less crowded 5GHz range, they do not really suffer much from interference. 802.11a networks do have a problem with range. 802.11a signals have a problem going through walls and other objects. This limited the standard’s overall effectiveness and therefore hindered its widespread usage.

802.11b
802.11b networks operate at a frequency of 2.4 GHz. They support a maximum data rate of 11 Mbps. Because of the use of the 2.4GHz frequency range, 802.11b networks can suffer from interference. There are many devices like microwaves and cordless phones that also operate within this range. When the 802.11b networking standard was developed, the equipment used for the networks cost significantly less than 802.11a equipment. This lower cost helped increase uptake and acceptance of the standard. It was the first standard to gain widespread acceptance.
802.11g
802.11g networks operate at a frequency of 2.4 GHz. They have a maximum transfer rate of 54 Mbps. 802.11g equipment is compatible with 802.11b network equipment. This has aided in its uptake. 802.11g is currently the most rapidly growing standard for wireless connections, especially in home networks.

802.11n
802.11n is a relatively new wireless networking standard. 802.11n networks can operate at 2.4 or 5 GHz. 802.11n networks support throughputs from 54 Mbps up to 600 Mbps. 802.11n networks also offer compatibility with previous standards.

Wireless Encryption Protocols
Traditional networks use some sort of physical transmission media. You cannot gain access to these networks unless you can gain physical access to the transmission media. This makes it at least a little difficult to tap into these networks. Wireless networks do not have this limitation. Wireless transmissions travel through the air and can be accessed by anyone. This makes encryption increasingly important. There are currently two widely used standards for wireless encryption. They are WEP and WPA.

WEP Encryption
WEP is the Wired Equivalent Privacy protocol. Most wireless access points support the WEP standard. WEP is probably the most widely used wireless encryption standard. WEP, however, has known security vulnerabilities. There have been known cracks of WEP encryption. Because of these vulnerabilities, WEP is slowly being phased out in corporate networks.

WPA Encryption
WPA is the Wi-Fi Protected Access protocol. WPA was developed by the Wi-Fi alliance to be a secure wireless encryption protocol to replace WEP. WPA usage is growing in popularity. Originally, WPA only used a preshared key to establish encryption. But the standard has been expanded to include Extensible Authentication Protocol (EAP) extensions. WPA2 has begun replacing the original WPA standard. WPA2 increases security and adds more features from the new 802.11i network standard.

Wireless Vulnerabilities
Although wireless networks share some of the same vulnerabilities as wired networks, wireless networking does have a set of vulnerabilities that are specific to only that technology. A lot of
them revolve around the widespread availability of wireless network access points. The easier something is to access, the harder it is to protect.

Lack of Authentication and Encryption
One of the most common vulnerabilities seen in wireless networks is the lack of authentication and/or encryption. It's possible that administrators may forget to enable authentication or encryption when they set up their wireless networks. Without encryption, anyone may connect to your wireless network. Without encryption, all your network traffic will flow in clear text. This makes it vulnerable to network sniffing. This can be avoided by ensuring that authentication and encryption are added to wireless networks.

Using Defaults
Using the default wireless network settings in your access point can introduce vulnerabilities into your network. If you use default settings, attackers don't have to try very hard to figure out how your wireless network is configured. One glaring mistake is the use of the default Service Set Identifier (SSID). Many vendors have a default SSID that is used in all their access points. Attackers may scan the airwaves using the default SSIDs from various vendors in an attempt to connect to an insecure network. So, even if you don't broadcast your SSID, using the default SSID puts you at risk because it is very easy for an attacker to guess what it is.

Eavesdropping
Wireless networks are very susceptible to eavesdropping. As long as someone is in a relatively close vicinity of the radio signals, they can pick up your wireless network. They don't have to be in the building. They could be in the parking lot. To protect against eavesdropping, you should secure your wireless network using authentication and encryption.

Rogue Access Points
In an attempt to access systems on your network, someone may set up a rogue access point. This is an unauthorized access point set up in your company's vicinity. Users in your company may then connect to this access point believing it to be an authorized one. The most effective way to combat this is through user education. Users should be educated as to which access points are safe to connect to. You can also periodically scan to see which access points show up within the vicinity of your company.
War Driving
War Driving is when attackers drive from location to location looking for a wireless network they can access. In general, they look for ones with no authentication. Once they find a network they can access, they attempt to sniff networks or try to connect to other systems on the network. There are two main ways to combat war driving. First, you can make sure your network is properly protected using authentication and encryption. Second, you can train your security staff to look for suspicious activity around the building and in the parking lot.

SSID Broadcasting
SSID broadcasting itself is not a vulnerability. But it does make it a little easier for an attacker to try to connect to your wireless network. In order for someone to connect to a wireless network, they need to know the network’s SSID. If you are broadcasting your SSID, you have already given an attacker one piece of information he or she needs in order to hack into your network. So as a security precaution, you should disable broadcasting of your network’s SSID, if possible. The problem is that if you are not broadcasting the SSID, anyone who wants to connect to the network will have to know it, in order to connect. In some instances, this may not be feasible.

Weak Encryption
Because wireless networks are more easily accessible by attackers, you need to ensure that you are using secure levels of encryption. Even though WEP is probably the most popular encryption method used in wireless networks, it’s not the most secure. If possible, WEP encryption should be replaced with some form of WPA2 encryption.

Remote Access Technologies and Vulnerabilities
Remote access can mean a few different things. First, remote access to systems can simply be any access that doesn’t occur from the system console. You could be on the corporate network, just not physical at the system console. Second, remote access could allow employees to access your corporate systems from noncorporate locations. Nowadays, the idea of a “mobile office” is putting more emphasis on the ability to provide this type of remote access. With remote access, it can be very difficult to determine who is actually accessing a system, especially when you start discussing access from remote locations. It’s very important that appropriate consideration is taken when planning remote access to your systems.
Client Access VPNs (Virtual Private Network)

A virtual private network (VPN) establishes a private network connection through a public network, like the Internet. Some consider it a form of tunnelling. There are many types of VPNs. VPNs are often used to join two networks together. But what we want to look at are client access VPNs. Client access VPNs are an extremely popular tool for providing external users access to a corporate network. The two most used technologies for this are IPSec VPNs and SSL VPNs.

IPSec VPNs use the IPSec protocol to create the VPN tunnel. IPSec VPNs operate at the network layer of the OSI model. When a client connects through an IPSec VPN, he or she has virtually full access to the network. Clients appear as just another node on the network. IPSec VPNs have been around for a long time. For years, IPSec VPNs were the standard for client access VPNs.

SSL VPNs have just begun to grow in popularity fairly recently. SSL VPNs use general SSL traffic over port 443 to establish the VPN connection. This is very useful when a user must initiate a connection from within a protected network. Many networks, especially corporate networks, filter what traffic is allowed to leave out through the firewall. In most cases, however, SSL over port 443 is allowed. SSL VPNs are considered most secure than IPSec VPNs because you have more control over what users can access. Another advantage SSL VPNs have over IPSec VPNs is the fact that most SSL VPNs can provide clientless access. Most IPSec VPNs require that some sort of VPN client software be installed on client systems in order for them to access the VPN.

Telnet

The Terminal Network or Telnet protocol is used to make virtual terminal connections to network devices. These devices could be computer systems or network equipment. Telnet can be used for remote shell connections or application connections. Telnet uses TCP port 23 for communications. By default, Telnet does not use authentication or secure connections. Although Telnet is still widely used, its lack of security has caused it to be replaced by Secure Shell (SSH).

Secure Shell (SSH)

SSH is being used as a secure replacement for Telnet. It uses public-key cryptography to verify the identity of the remote computer. SSH also provides for key re-exchange during the session. This helps to ensure continued security. SSH also supports secure tunnelling and X.11 connections. So not only authentication but also the sessions themselves can be secured. SSH uses TCP port 22 for making connections, although this port can be changed.
RDP

RDP is the Remote Desktop Protocol. RDP was developed by Microsoft as a protocol to be used for connecting to Windows desktops and servers running Remote Desktop Services (originally Terminal Services). RDP uses port 3389 by default. In order to make a connection, the client must be running a Remote Desktop Client. There are Remote Desktop Clients installed on all newer Microsoft operating systems.

Before you can use the Remote Desktop Client to access Windows 7 or Windows Server 2008 R2 systems, you must first enable Remote Desktop Services on the system.

Enabling Remote Desktop Services on Windows 7

1. From the Start menu, right-click Computer and select Properties. Or from the Control Panel, open the System applet.
2. In the left pane, select Remote Settings. This brings up the Remote tab of the System Properties window, as seen in Figure 3.1.

![Figure 3.1 System Properties window – Remote tab.](image-url)
3. In the Remote Desktop section, choose the option for Allow connection only from computers running Remote Desktop with Network Level Authentication. Note: Users who are not running at least Windows 7 will not be able to make Remote Desktop connections to the system.

4. Click the button Select Users. This brings up the Remote Desktop Users window, as seen in Figure 3.2. Here, you can choose who will be able to access the system via Remote Desktop.

![Remote Desktop Users window](image)

**Tools & Traps**

**Remote Desktop Connection**

The Remote Desktop Connection application is used to make connections to Remote Desktop Services. This application can be accessed from Start menu | Programs | Accessories. When you make a connection using this application, you are connected to a regular Remote Desktop session. The Remote Desktop Connection application also allows you to connect remotely to the console session of the server. In some cases, there may be actions you cannot perform in a regular Remote Desktop, and you will need to connect to the console session. Also, there is only a limited number of Remote Desktop connections allowed to a system. If this limit has been reached, you will not be allowed to make a new one until one of the others has been disconnected or unless you connect to the console session. To connect to a console session, run the command mstsc /admin. This will start the Remote Desktop Connection in console connection mode.
Note: There is a built-in group called Remote Desktop Users. The easiest way to give users Remote Desktop access to a system is to add them to this built-in group.

**ICA**

ICA is the Independent Computing Architecture protocol. It’s a protocol developed by Citrix Systems used for remote connections to desktops and applications. ICA generally makes connections on TCP port 1494. But ICA can also be tunneled inside the Common Gateway Protocol (CGP), also developed by Citrix, on port 2598. ICA has built-in compression that makes it highly useful over lower bandwidth connections.

**IPSec**

IPSec is Internet Protocol Security. IPSec operates at Layer 3 of the OSI model. It is used for securing communications between systems. IPSec authenticates and encrypts all the packets in a data stream.

IPSec starts by using an Internet Key Exchange (IKE) to negotiate which protocols and algorithms will be used in the communication. During the IKE, the keys that will be used for encryption are also exchanged between the two systems. The Authentication Header (AH) is used to authenticate and verify the packets that are being exchanged. Encapsulating Security Payload (ESP) is used to protect the data itself. ESP provides the encryption that is used to secure the data inside the packet.

**Internet Security and Vulnerabilities**

The Internet is an extremely useful tool. It puts an unlimited amount of information right at your fingertips and connects you to sources of information that you would never have been able to access just a few years back. The Internet and usage of the Internet are growing exponentially. But, unfortunately, so is the number of people trying to take advantage of others on the Internet. It’s important that everyone understands not only the capabilities but also the dangers and how they can protect themselves.

**General Internet Concepts and Vulnerabilities**

The Internet is made up of a number of different components. It’s a huge collection of different technologies that come together. Each of these components and technologies has its own role and function.
SSL and TLS
Secure Sockets Layer (SSL) is used to provide secure network communications. There were three versions of SSL. The fourth version was renamed to Transport Security (TLS). Although most people still refer to SSL usage, in many cases, what is actually being used is TLS. SSL and TLS work at the transport layer of the OSI model. They generally use a public-key algorithm for establishing encryption. SSL and TLS use x.509 certificates for handling key information.

HTTP and HTTPS
HTTP is the Hypertext Transfer Protocol. HTTP works at Layer 7 of the OSI model. HTTP generally uses port 80 for network communications. It is the main protocol used when accessing content over the Internet.

HTTP is based on a request-and-response system. For example, a user makes an HTTP request to a Web server. Then, the Web server sends back an HTTP response. HTTP uses a standard set of request types called verbs. When securing a Web server, it's important that you understand which verbs are required for your site. Some verbs are less secure than others. You want to make sure that you have disabled verbs that are not necessary for your site to function. Some of the most common verbs used are GET, POST, and PUT.
- GET: An HTTP GET is used for retrieving information from a Web server.
- POST: An HTTP POST is used to send information to a Web server, like when you fill in a form.
- PUT: An HTTP PUT is used to upload something to a Web server.

By default, information sent using HTTP is sent in clear text. This can present a problem when sending sensitive data or passwords. This is where HTTPS comes in. HTTPS is HTTP over SSL. With HTTPS, SSL or TLS is used to encrypt information sent using the HTTP. By default, HTTPS uses port 443 to send information.

Botnets
A botnet is a collection of agents called robots or bots that are used to perform automated tasks, usually malicious tasks. Botnets are used for spamming, distributed denial-of-service attacks, and many other exploits. In many cases, the bots that are performing these tasks are computers that have been compromised. So the owners of these computers may not be aware of what their computer is doing.
Because of their hidden nature, botnets are growing all over the Internet without widespread interference. Botnets can extend to hundreds of thousands, even millions of computers. Bots can be programmed with methods used to infect other computers and create other bots.

The computers in a botnet are controlled by a central server called a command-and-control server. The command-and-control server sends out periodic instructions to the computers in its botnet. In some cases, there can be more than one command-and-control server in a botnet. This makes it even more difficult to stop. You may find and shut down one command-and-control server, but the bots will then just receive instructions from another command-and-control server in the botnet.

Botnets themselves can be hard to detect and take down. But there are a few things you can do to protect your organization. First, make sure antivirus software is installed and up-to-date on all your systems. This will help prevent systems from being infected. You can also purchase heuristic-based intrusion detection systems. These systems can help identify infected systems. Network monitoring can also be used. You should look for excessive network traffic between systems or excessive traffic destined for a single external system.

**Peer-to-Peer File Sharing**

Peer-to-Peer File Sharing systems are no longer just a new fad technology. They have become ingrained in our Internet culture. You have to remember that just because Samantha is hosting a file that she says is a video of the Olympics, that doesn't mean that it really is the Olympics. It could be some sort of Trojan or malware. Nowadays, many botnets are built using Peer-to-Peer File Sharing systems.

Most corporate organizations do not use Peer-to-Peer File Sharing systems for business purposes. So the easiest way to protect against abuse is to take steps to prevent their usage within your organization. You can do this by blocking access to any external servers or services that are used to control the peer-to-peer software. You can also internally block any ports that are used by peer-to-peer systems to talk to each other.

**Denial-of-Service (DOS) Attacks**

Denial-of-service (DOS) attacks attempt to prevent normal usage of a system or service. DOS attacks can take many forms. An attacker may send a malformed or bad request to a system, hoping that request will cause the system to crash. An attack may
also send a flood of valid requests to a system, hoping that the system cannot handle the volume of requests being sent. This volume may either cause the system to crash or just prevent the system from processing valid requests.

Oftentimes, in order to implement a successful denial-of-service attack, you need to have more than one performing the attack. This is especially the case when the attack is attempting to flood the device with requests. This is called a distributed denial-of-service attack (DDOS). The perpetrator of a DOS attack will recruit other systems to help perform the attack. Oftentimes, these other systems will be part of a botnet. The DOS coordinator will install software or agents on the infected system that will cause them to send the desired requests to the system under attack.

**Malware**

Malware is a general name given to software developed for malicious purposes. Most computers that access the Internet have some sort of malware installed on them, usually without the owners' knowledge. The only thing they may notice is that their computer is a little slower or less responsive than before. But they don't know what to attribute it to. Two common types of malware most people encounter are spyware and adware.

**Spyware**

Spyware is a type of malware used to spy on user activity on a computer. Spyware will gather information on users' habits such as browsed Web sites, accessed applications, and downloaded programs. This information is then sent to an attacker, so he or she knows what attacks can be perpetrated on a system. Spyware can have even more direct effects, like stealing of passwords and credit card information. This type of information can lead to direct financial benefits for an attacker. Spyware is generally not self-proliferating. It is not spread from infected system to infected system. Usually, spyware is downloaded from a Web site or server that the user believes contains beneficial software. In fact, many times, spyware will be bundled in a download with some sort of legitimate software.

**Adware**

Adware is a type of malware that is used to display advertisements on infected systems. Adware may display a series of pop-up ads on infected systems in an attempt to direct traffic to those sites. These pop-up ads can be annoying, and the sites that are being advertised can also be malicious. Some adware programs can replace ads that show up on legitimate Web sites. In these cases, the user
would assume that the products and services being advertised are legitimate because they show up on a legitimate site.

**Browser Security**

Most of the content on the Internet is accessed via a Web browser, like Internet Explorer or Firefox. Your Web browser is the main interface between your computer and the Internet. It’s important that you understand what capabilities exist in your browsers. It’s also important that you understand the vulnerabilities introduced in a browser.

**General Browser Security Concepts**

Each Web browser is different and has different features. But there are certain concepts and technologies that are implemented in all browsers. They may be implemented differently in different browsers, but the core functionality is still there.

**JavaScript**

JavaScript is a scripting language understood by most browsers. Many Web sites use JavaScript to perform tasks that cannot be performed with simple HTML code. Scripts written using JavaScript are processed on the client side. This is what causes the potential for damage to be done to a client system. Malicious Web sites can insert JavaScript into their Web pages. These scripts can be used to perform actions on the client system. JavaScript can be used for files access, file upload, cache access, and changing certain system settings. You can use your browser’s security settings to govern how JavaScript will be run on your system.

**Java Applets**

Java is a platform used for creating operating system independent applications. These applications are called Java applets. All you need to have installed on the system is a Java Virtual Machine (JVM). The Java applets will run inside this Java Virtual Machine. Java applets are much more robust than scripts written in JavaScript. Therefore, they can also be much more dangerous. One thing you can do to protect against systems running malicious Java applets is to require your system to run signed only Java applets. A digital signature will help to ensure that the application is created by a known entity that can be tracked.

**ActiveX Controls**

ActiveX is a technology Microsoft developed to allow robust applications to be run inside of a Web browser. The applications written for this technology are called ActiveX controls. ActiveX
controls can be embedded inside the Web browser itself. They can then be activated by various Web sites. ActiveX controls have the capability to perform a lot of system-level functions. Because of this, they can be very dangerous. But you can configure whether or not to allow your system to execute ActiveX controls.

**ActiveX Settings in Microsoft Office:** In addition to being able to use ActiveX controls in Internet Explorer, you can also use ActiveX controls in Microsoft Office documents. Because of this, Microsoft Office allows you to configure when and how ActiveX controls can be used. As seen in Figure 3.3, these settings are configured under Trust Center | ActiveX Settings. You have the following options:

- Disable all controls without notification
- Prompt me before enabling Unsafe for Initialization (UFI) controls with additional restrictions and Safe for Initialization (SFI) controls with minimal restrictions
- Prompt me before enabling all controls with minimal restrictions
- Enable all controls without restrictions and without prompting (not recommended; potentially dangerous controls can run)

You also have the option to enable Safe mode for ActiveX controls. Safe mode will apply a set of predetermined restrictions to limit the access of ActiveX controls.

![Figure 3.3 Microsoft Office ActiveX Settings.](image-url)
XSS (Cross-Site Scripting)

Cross-site scripting is when an attacker attempts to use someone else’s Web site to execute his or her code. Different Web sites can have different abilities to execute scripts on your system. There are also Web sites where you would be more apt to allow a script to perform actions on your system. In a cross-site scripting attack, an attacker attempts to fool you and your system into thinking that a trusted site is the one actually executing the script. This is often done by using a specially formed URL sent in an e-mail link.

For example, you may want to go to http://arlenes-trusted-site.com/page.aspx. But instead, you may be sent to http://arlenes-trusted-site.com/page.aspx?http://claudes-site/execute-claudes-script.aspx. In this example, you are going to arlenes-trusted-site, but you are executing a script from claudes-site. The problem is that there is something wrong with the page.aspx file on arlenes-trusted-site that allows you to execute arbitrary code. This vulnerability needs to be fixed on arlenes-trusted-site. In fact, most cross-site scripting vulnerabilities are a result of a flaw on a trusted site.

Cookies

Cookies are small files that are stored on computer systems to store user information. This information could be preferences, site settings, personal information, or browsing habits. In general, the use of cookies is a very effective way of storing information that can be used by Web sites. Without cookies, you might have to reenter personalization information every time you visited a Web site.

Many feel that cookies that store user information are an invasion of privacy. Cookies may contain a lot of personal information. This information could then potentially become available to sites that you did not intend to be able to view this data.

Securing Internet Explorer

Internet Explorer is the Web browser most commonly used on Windows systems. If you are using Internet Explorer, it’s important that you understand some of the security measures in place to protect your system. The most prevalent of which is the configuring of security zones.

Security Zones

In order to help simplify protecting Internet Explorer, Microsoft developed the concept of security zones. Instead of attempting to apply a one-size-fits-all approach to security settings, you
can have different settings for different security zones. A security zone represents the level of trust you have in a Web site. You set specific browser settings for each security zone. Then, depending on which zone a particular Web site falls into, it will have those settings applied. Internet zones are configured on the Security tab of Internet Options. Each zone has default settings that are already configured, but they can be customized to fit your needs. There are four security zones in Internet Explorer: Internet, Local intranet, Trusted sites, and Restricted sites.

**Internet:** Internet sites are basically sites that do not fit into any other zone. Most of the sites you encounter will fall into the Internet zone. By default, Internet zone settings are set to Medium-high, as seen in Figure 3.4.

![Internet Options](image)

**Figure 3.4** Internet Explorer Internet zone.
**Local intranet:** The local intranet zone is intended for sites that exist on your local LAN. The theory here is that you would have a greater level of trust for sites that exist on your local network. By default, the Local intranet zone has settings set to Medium-low, as seen in Figure 3.5.

To determine which sites will be categorized as part of the intranet zone, click the **Sites** button. This brings up the Local intranet window, as seen in Figure 3.6.

If you want, you can have Internet Explorer automatically determine which sites should be a part of the Local intranet zone, based on the requirements you specify. You can also manually specify which sites to add to the Local intranet zone. This is done by clicking the **Advanced** button in the Local intranet window. This brings up the Local intranet Add Sites window, as seen in Figure 3.7.

**Trusted sites:** Trusted sites are sites that you explicitly trust. You know these sites to be safe. Trusted sites have an even more relaxed level of security. Some features and functions require that sites be in the Trusted sites zone in order for them to work properly. By default, the Trusted sites zone has its settings set to Medium, as seen in Figure 3.8.

You can manually specify which sites you want to be added to this zone. You can do this by clicking the **Sites** button. This brings up the Add Trusted Sites window, as seen in Figure 3.9. By default, you can only add HTTPS sites as trusted sites, but this can be changed by unchecking the option for Require server verification (https:) for all sites in this window.
Restricted sites: The Restricted sites zone is for sites known to be potentially harmful to your system. This is the most restrictive security zone available. By default, settings for the Restricted zone are set to High, as seen in Figure 3.10.

You have to manually add sites to the Restricted zone. This is done by clicking the Sites button. This brings up the Add Restricted sites window, as seen in Figure 3.11.

E-mail and Messaging Security

E-mail and messaging systems provide an easy method for users to communicate with one another. E-mail and instant messaging systems provide similar functionality, but they serve different purposes. They are also implemented very differently. These differences mean they have different vulnerabilities and are secured differently.

E-mail Concepts and Vulnerabilities

E-mail is short for electronic mail. E-mail messages are sent from a client to an originating e-mail server, to a destination e-mail server, and to the receiving client. Each of these entities can save a copy of the message. E-mail is used for personal use and business use. This is one difference between e-mail and instant messaging systems. Instant messaging is generally used for personal use.

E-mail Spam

Spam is bulk e-mail sent out to individuals who neither requested nor expected to receive a message. Spamming is usually done for two reasons. First, spam may contain some sort of advertisement. Someone may send out spam in
an attempt to get people to buy something. The second reason is to cause e-mail disruption. The large volume of e-mails being sent out can cause problems for e-mail messages. E-mail systems may be so busy processing spam e-mails that they cannot process legitimate e-mails.

Spam may be sent out to random e-mail addresses or to the e-mail addresses of people who used their e-mail address to sign up for something. Some companies sell valid e-mail addresses to spammers. So you may use your e-mail address to sign up for something you want, but end up getting spam, which you don't want. The privacy policy of a Web site will generally give you an idea of whether they might sell your e-mail address to someone else.

There are a couple of things that can be done to protect against spam. First, you can educate users about where to and where not to enter their addresses. Have them check a Web site's privacy policy before they register their e-mail addresses on the site. You can also install spam filters on your e-mail servers. Spam filters are specific applications designed to detect spam. Spam often has certain keywords in the subject or body of the message. For example, if your company sells paper products and there is an e-mail coming in that offers “Male Enhancement,” it's probably spam, and the spam filter will detect it and prevent it from being delivered.

E-mail Hoaxes

E-mail hoaxes are e-mails circulated that spread some sort of false information. But the intent of the e-mail is not to spread misinformation; the intent is to affect the functioning of e-mail
systems. Generally, e-mail hoaxes will include something to the nature of “forward this to everyone you know, so they are aware, too.” So Shawn will forward to Leo and Isaac. Leo will forward to Victor and Pam. Isaac will forward to Jayden, Shyheim, and Denzil, and so on, and so on. Before you know it, everyone in your organization will be forwarding the e-mail around. The volume of hoax e-mails being forwarded may affect your system’s capability to process legitimate e-mails.

To help prevent e-mail hoax problems, you can educate your user population not to forward nonbusiness e-mails. Many times e-mail hoaxes may contain false information about some new computer virus that is going around. Users may think they are doing something good by forwarding these e-mails around. There are Web sites that keep track of legitimate and fake viruses. Users can use one of these sites to verify the information in the e-mail, instead of assuming it to be true.

SMTP Relay

SMTP relays are basically servers that are used to forward SMTP messages. SMTP relays can help you protect your internal e-mail servers. An SMTP relay server can be used to forward messages that are destined for or originating from the Internet. This way your internal e-mail servers are not exposed directly to the Internet. The problem occurs when there are what’s called “open” SMTP relay servers. Open SMTP relay servers are those that are not secure; they allow anyone to send a message through them. Spammers use open SMTP relay servers to forward e-mails through. If your SMTP relay service is open, your system may be spamming without your knowledge. Eventually, your server may end up on an e-mail blacklist. This could greatly hinder your company’s capability to send legitimate e-mails.

If you are not using SMTP relay, you should make sure that your e-mail servers have the service turned off. If you are using the service, you should make sure the service is secure. You should limit who can send e-mails through your SMTP relay server. If your SMTP relay is only for internal forwarding,
you should also limit where your SMTP relay server can send e-mails.

**Instant Messaging**

Instant messaging (IM) systems can be very useful. It allows immediate and convenient communication between two parties. If you use an externally administered system, then you don’t have to worry about managing the infrastructure. But along with the convenience and ease of IM come many potential threats. With IM, you have to worry about information flowing in clear text, Internet links in messages, file transfers, and social engineering.

Information sent via IM is generally sent in clear text. There are programs available that can be used to encrypt IM traffic, but these are usually separate add-ons. If someone is sending sensitive information via IM, that information is vulnerable to network sniffing.

You have to be very careful with IM systems because you never really know who is on the other end. IM systems allow you to post Internet links inside of messages. This can be very dangerous. The links you receive could direct you to malicious sites. Many e-mail systems can scan messages for dangerous links, but IM generally does not do this. IM clients may warn you about clicking links in messages, but they will not block them.

IM clients also allow file transfers. Usually, these are just pictures or something harmless. But that’s not always the case. Sometimes, these files are malicious executables. IM clients do not scan messages to see if these files are malicious or not, by default. It’s up to the users to use their best judgment.

Social engineering attacks are also common with instant messaging systems. Because of their relaxed and informal nature, IM systems often give people a false sense of familiarity and trust. You must still remember that you do not really know who is on the other side of the connection. If you send confidential information through an instant message, you need to be aware that you could be sending it to anyone.

There are several steps that can be taken to secure instant messenger usage. First, you can prevent the usage of external IM clients. Most public e-mail clients require users to log into a central authentication system. You can block users within your network from accessing this central authentication server. If you need IM within your organization, you can set up an internal IM system.

If preventing the use of external IM systems is not feasible, then you should do what you can to protect the users and client
systems. You can use an add-on application to encrypt the content of your IM messages. This will help protect against network sneaking. IM encryption applications generally require the use of a shared key. The key is usually exchanged the first time communication occurs. Second, you should enable the file transfer protection settings in the IM client. Certain antivirus applications also have plug-ins for IM clients. You can use these to scan transferred files for malicious content. Finally, end-user education is essential. You can educate users not to click links in e-mail messages. You can also educate users on the dangers of instant messaging in an attempt to help prevent social engineering attacks.

Network Security Tools and Devices

In addition to general network security devices, there are tools and devices developed specifically for network security. Depending on the organization, these devices may be administered by the company’s security team or by the company’s networking team. It depends on whether you consider network security a subset of networking or a subset of security.

Proxy Servers

A proxy server is an intermediate server that sits between a client and resources the client is trying to access. A proxy server will make requests on behalf of the client. The client never talks directly to the resource. Proxy servers can serve many functions. They mask the IP of the client making the request. Proxy servers can speed up Web page access through the use of caching. Pages can be pulled from the cache on the proxy server instead of downloading the page from the Internet. Proxy servers can also be used to scan and monitor traffic to and from the Internet.

Clients can be configured to use proxy servers in a few different ways. The proxy server can be manually specified. You can have your browser automatically detect the proxy server. Or you can use a proxy configuration file. We’ll walk through configuring a proxy server in Internet Explorer and Firefox.

Configuring a Proxy Server in Internet Explorer

1. Inside Internet Explorer, go to Tools | Internet Options.
2. Go to the Connections tab, as seen in Figure 3.12.
3. In the Local Area Network (LAN) settings, click LAN settings.
4. In the LAN Settings window, as seen in Figure 3.13, you can configure your system’s Proxy Server settings. If you need to
configure a SOCKS Proxy or you want to configure Proxy exceptions, click the **Advanced** button.

5. In the Proxy Settings window, as seen in Figure 3.14, you can configure a SOCKS Proxy, by unchecking the box for Use the same proxy server for all protocols and entering the name of the SOCKS Proxy Server.

**Configuring a Proxy Server in Firefox**

1. Inside Firefox, go to Tools | Options.
2. Under the Advanced menu, as seen in Figure 3.15, go to the Network tab.
3. In the Connections section, click **Settings**.
4. On the Connection Settings window, you can configure your system's proxy settings. Figure 3.16 shows Firefox configured to use a Proxy Server called drproxy01.drdomain.com.

**Network Firewalls**

Firewalls are used to separate two networks. Most often they are used to separate an internal corporate network from an external public network. Firewalls can also be used to create a DMZ. Firewalls can also be used to separate internal networks. You may have certain areas of your network that you want to secure the general network traffic. You may want to separate your user network from your infrastructure network or your data network.

Firewalls can be implemented using hardware or software. Many software firewalls come preinstalled on hardware with a hardened OS. There are three general types of firewalls: packet filtering, stateful inspection, and application gateway.

**Packet-Filtering Firewalls**

Packet-filtering firewalls operate at the network layer (Layer 3) of the OSI model. Packet-filtering firewalls make processing decisions based on network addresses, ports, or protocols.

Packet-filtering firewalls are very fast because there is not much logic going behind the decisions they make. They do not do any internal inspection of the traffic. They also do not store
any state information. You have to manually open ports for all traffic that will flow through the firewall.

Packet-filtering firewalls are considered not to be very secure. This is because they will forward any traffic that is flowing on an approved port. So there could be malicious traffic being sent, but as long as it’s on an acceptable port, it will not be blocked.

**Stateful Inspection Firewalls**

Stateful inspection firewalls keep track of connection status. Ports can be dynamically opened and closed if necessary for completing a transaction. For example, when you make a connection to a server using HTTP, the server will initiate a new connection back to your system on a random port. A stateful inspection firewall will automatically open a port for this return connection.

Stateful inspection firewalls are considered more secure than packet filtering firewalls. Stateful inspection firewalls process application layer data. Therefore, they are able to take a deeper look into the transaction to understand what is going on.

**Application Gateway Firewalls**

Application gateway firewalls operate at the application layer (Layer 7) of the OSI model. They filter access based on application definitions. Application definitions can include not only port numbers but also specific application information like acceptable HTTP verbs. Application gateway firewalls are considered to be some of the most secure firewalls available because of their capability to inspect packets and ensure the
packets are conforming to application specifications.

Because of the amount of information being processed, application gateway firewalls can be a little slower than other firewalls. Sometimes, people use application gateway firewalls in conjunction with another firewall. The application gateway firewall will be used only to protect servers. Or the application gateway firewall will sit behind the other firewall. The first firewall will be used as a first-level filter. The application gateway firewall will process only packets that pass through the first firewall.

**Personal Firewalls**

Personal firewalls are system-level firewalls that are used to protect a system from network-based threats. Personal firewalls control what ports your system is allowed to listen on. They also control what processes on your system are allowed to make network connections. Many antivirus vendors include personal firewalls.

**Windows Firewall**

The Windows Firewall is used to protect your Windows system from network-based threats. You can control who has access to your system and what access is granted. The Windows Firewall applet allows you to configure these firewall settings. In the Windows Firewall section of the Control Panel, you have two options: Check firewall status and Allow a program through Windows Firewall.

**Check firewall status:** This option brings up the Windows Firewall window, as seen in Figure 3.17. This
option will allow you to see if Windows Firewall is enabled or disabled on your system. You can also see Windows Firewall settings for incoming connections and notifications.

Allow a program through Windows Firewall: This option brings up the Allowed Programs window, as seen in Figure 3.18. Here, you can see what programs are allowed by Windows Firewall. If you want to change these settings, you must choose the Change settings option. You can now select a program to allow access to and what networks the program is allowed to communicate on. The Details option will show you the path to the executable for the application being allowed. If you want to allow a program not listed, you can choose the Allow another program option. You can then specify the location of another program you want to allow through the firewall.

Honey Pots
Honey pots are systems set up to attract hackers. They are set up in such a way that hackers will have access to them. Monitoring honey pots allows you discover ways in which a hacker may attack your systems. You can use the data discovered to secure your important systems.
Network Tools

`Ipconfig`: The `ipconfig` command is used to manage the IP configuration of your system. You can use it to view IP information on your system, like your IP address, subnet mask, and DNS server. Or you can use it to manage IP configuration information. You can clear your DNS cache or renew your DHCP settings. `Ipconfig` usage is shown in Figure 3.19.

`Ping`: The ping utility is used to test connectivity between two systems. Ping sends Internet Control Message Protocol (ICMP) echo request messages to the target system and waits for an ICMP reply. If a reply is received, then you know there is basic network connectivity between the client system and the target system. Ping usage is shown in Figure 3.20.

`Tracert`: Tracert is the Windows implementation of the traceroute utility. Tracert is used to check connectivity between two systems at a more granular level. Tracert will actually show you the path between two systems. If there is a failure in connectivity, tracert can also help you pinpoint where in the route the failure occurred. Tracert usage is shown in Figure 3.21.

`Nslookup`: Nslookup is used for querying a DNS server. You can use it to test name resolution on your system. Nslookup can tell you
what DNS server your system is using to look up domain names. It can also tell you what the response is. If you are having trouble connecting to a system, it could be because the name is not resolving or resolving to the wrong address. Windows uses SRV records in DNS for pointing clients to services. You can use nslookup to determine what server is assigned to carry out a particular service. Nslookup usage is shown in Figure 3.22.

Netstat: Netstat is used to show network statistics and connections. You can use it to determine what systems a client is connected to and vice versa. You can also use it to determine what ports a system is listening on. This can be very useful if you think a system may be propagating a virus. Or if you think the system may be connected to a botnet. Netstat usage is shown in Figure 3.23.
Chapter 3  NETWORK SECURITY  

Figure 3.21  Tracert usage.

Figure 3.22  Nslookup usage.
A good understanding of networking and networking components will help give you a better understanding of some of the vulnerabilities that affect these components. Considering the fact that nowadays almost all computers are connected to some type of network, it's increasingly important that you understand how to protect against network threats. Most attacks are actually initiated via a network, and most viruses are spread through a network. So in many instances, a good network security plan will help protect against the proliferation of attacks and system compromises.

The Internet, which is actually the largest network in the world, is also the most dangerous. You can have no idea of the true intentions of the people and systems you come across on the Internet. Because of this, you should treat all Internet traffic as hostile. In some cases, it may be unwarranted, but it's better to be safe than sorry. The most common interface to the Internet is
the Web browser. It's key that you understand what mechanisms are in place to secure the Web browsers used on your systems. For your physical networks, firewalls and proxies provide your basic protection. Your firewall is often seen as the fence separating you from the outside world. This fence needs to be secured and consistently monitored.