# Types of Attacks

- We can categorize the types of network-based attacks at a high-level as **Active** and **Passive** attacks.

## Active Attacks

- Denial of Service
- Compromising a Site:
    - Intelligence gathering
    - Resource usage
    - Deception

## Passive attacks

- Sniffing
    - Passwords
    - Network traffic
    - Sensitive information
- Information gathering

- An **active attack** involves a deliberate action on the part of the attacker to **gain access** to the information she is after.
- An example is trying to telnet to port 25 on a given machine to find out information about the mail server that a company is running.
- As an analogy, this is the equivalent of a burglar trying to pick the lock on your front door or throw a brick through a window to gain access.
- The attacker is actively doing something against you or your company. Because of this, these attacks are fairly easy to detect, if you are looking for them.
- However, most active attacks often go undetected because companies do not know what to look for or are looking at the wrong thing.
- **Passive attacks**, on the other hand, are geared toward **gathering information** as opposed to gaining access. These attempts to learn more about a system do not affect a system's resources (RFC 2828).
- This is not to say that active attacks cannot gather information or that passive attacks cannot be used to gain access-in most cases, the two types are used together to compromise a site.
- Unfortunately, most passive attacks do not necessarily involve traceable activity and therefore are much harder to detect. For example an attacker will make normal connections to services such as web services, mail server and DNS to learn the version of software in place.

## Categories of Exploits

- An attacker will use several different types of attacks and will always look for the easiest way into a machine or network.
- In some cases, systems are so open that an attacker can just launch one type of attack and be successful in compromising the system.
- In other cases, he will have to launch several different attacks to succeed. Some of the more popular attacks are described next.

## Internet Attacks

- This category of attack is what most people think of when they hear of hackers breaking into machines.
- This is also what our knowledgeable media tends to emphasize in terms of dangers posed to your system by hackers: teenagers in t-shirts, working in dark rooms at 2:00 a.m., high on pop and doughnuts, compromising systems via their dial-up connection.
- This is an ideal way to compromise a machine because most companies have connectivity to the Internet.
- Attacks over the Internet involve compromising a machine by using the Internet as the path into a remote host.
- Some of the more common over the Internet attacks are the following:
    - Coordinated attacks
    - Session hijacking
    - Spoofing
    - Relaying
    - Trojan horses or viruses

### Coordinated Attacks

- Since the Internet allows for worldwide connectivity, it makes it very easy for people from all over the world to collaborate or participate in an attack.
- In order for some exploits to be successful, hackers have to coordinate with other users and machines on a network.
- Note that the beauty of this attack is that other people do not even need to know that they are helping the attacker.
- After compromising machines on several large networks, an attacker could then use those machines to coordinate attacks against other networks.
- Programs such as Tribal Flood Network 2000 (TFN2K) are very powerful programs that are easy to use for these types of attacks.

## Session Hijacking

- In some instances, it is easier to sneak in as a legitimate user, rather than break into a system directly.
- This technique is called **session hijacking** and it works by finding all established session and then taking over that session after a legitimate user has gained access and authentication.
- Once a user is logged on, an attacker can take over the session and stay connected for several hours-plenty of time to gain additional access or plant backdoors.
- Session hijacking looks fairly simple on paper but is complicated to implement for several reasons.
- One of the main reasons is that since an attacker is taking over an existing session they must impersonate the legitimate user.
- This means getting all the traffic that is routed to their IP address to come to the hacker's system.

## Spoofing

- Spoofing is a term that describes the act of impersonating or assuming an identity that is not one's own.
- In the case of Internet attacks, this identity can be an email address, user ID, IP address, and so on.
- This becomes important when an attacker is exploiting trust relationships. On many systems, multiple hosts are usually setup with trust relationships.
- IP address spoofing helps attackers undermine various applications, particularly those that rely only on IP addresses for authentication or filtering.
- Spoofing can be considered as more of a passive attack than session hijacking. With session hijacking, an attacker takes over an existing session and actively takes a user offline.
- With spoofing, an attacker takes advantage of an implied trust relationship between people and/or machines and fools them into trusting him.

## Relaying

- Relaying is where an attacker relays or bounces her traffic through a third party's machine so the attack looks like it came from the third party, not her.

- A popular type of relaying attack is email relaying. This involves is connecting to another individual's email system and using their computer to send email to someone else.

- To test if your system allows relaying, try to connect to your mail server from an outside address and send an email to a foreign email address. If you do not receive the following message, your system allows relaying:

  **Server error: Can't send to The server gives this reason: "550 Relaying is prohibited"**

## Trojan Horses or Viruses

- Trojan horses can cause extensive damage due to the following quality that they possess: they have both an overt and a covert function.

- The overt function can be anything that the target victim would find interesting. A perfect example is seen around the holiday season. People send around the animated images that have things like dancing reindeers and small creatures hurling snowballs.

- Users cannot resist the urge to pass these on and open them on their own machines. This becomes a problem when we bring the covert function into the equation.

- The covert function is launched when the overt function is being executed, so most users do not even know that it is happening.

- They think they are running an entertaining file, and in reality they are infecting their machine and their friends are doing the same.

- A common use of Trojan horses is to install backdoors so that a user can get back into the system at a later time.

- Computer viruses are like human viruses, there goal is to infect as many hosts or computers as possible.

- Once a computer becomes infected, it becomes a carrier to infect other hosts. The impact from viruses can range from annoying to extremely dangerous.

- Some emails will just popup a funny or annoying message. Other viruses will delete entire hard drives and crash systems.

# LAN Attacks

- Attacks that occur over a LAN are usually more detrimental because most company security is set up in a way that it assumes that those with local access to the LAN, such as employees, can be trusted.

- This is dangerous for two reasons. First, a large number of attacks come from trusted insiders.

- Second, attackers can gain access to the LAN by breaking into a legitimate user's account and gain the full access that a normal employee would have.

- The following are some of the more popular types of attacks that can be perpetrated over a LAN:

    - Sniffing traffic
    - Broadcasts
    - File access
    - Remote control
    - Application hijacking

## Sniffing Traffic

- This is a passive attack that involves watching all of the traffic that occurs on a network. Since it is a passive attack, some people overlook it saying that an attacker cannot do any damage to their network.

- This statement is not true in that attackers cannot perform a Denial of Service attack or actively break into a machine, but they can find information that would make it much easier to gain access at a later date.

- Also, from a corporate espionage standpoint, someone can gain access to extremely sensitive files, which a company would have a hard time detecting.

- Since most users do not encrypt traffic and they send sensitive information via the network or especially email, there are large amounts of information an attacker can pull off the network.

- One possible way to use a sniffer is to embed it with a Trojan horse program. The user would open this neat program to play a game and it would install a sniffer on their computer, which would send back all traffic to the attacker.

- Even in a switched environment, users should encrypt any sensitive traffic on their networks. It is just not worth the risk to do otherwise.

- It is important to point out that even if you have a switched environment someone can still sniff the network.

- It is just a little harder since they need physical access to the machines. Most switches have a port that you can plug into which allows the machine to see all traffic. If someone can get access to the switch they can sniff the traffic (yet another reason for physical security).

- In order for a network card to receive all traffic it has to be switched to a different mode, otherwise it drops packets not destined for the machine.

- Promiscuous mode is the mode that will allow the network card to receive all packets that are being sent on the network segment.

**Broadcasts**

- All machines that are connected to the same network segment have to have the same network number.

- Every IP address that is assigned to a machine has a network and a host portion. The network portion must be the same for all machines on the same network and the host portion must be unique for each host.

- Normally, packets are sent to a unique host address, but there are times when packets want to be sent to all of the addresses on the network segment.

- This is accomplished using the broadcast property of TCP/IP, which will send a packet to every machine on the network segment.

- Setting the host portion to all 1's or the broadcast address does this, which converted to decimal, would give you 255.255.

- If we combined this with the network portion we would get 25.10.255.255, which represents the broadcast address for that network segment.

- A packet is sent to that address goes to every single machine on that segment. If there are only 10 machines, it is probably not that big of a deal, but what if there are 60,000 machines?

- That could generate a lot of traffic and cause numerous problems. This is actually a common type of attack where an attacker sends a single packet to a broadcast address with the goal of generating so much traffic that it causes a Denial of Service attack against the network.

- If proper filtering is not applied at a company's firewall or routers, this attack could also be performed via the Internet, but this is primarily performed on a LAN.

## File Access

- In most companies, passwords are the first and only line of defense against attacks. However, since most companies do not have proper access control lists, which limit access to specific files, an attacker can usually gain access (using a user ID and password) to all of the files on a network.
- A common remark made is "we do not have any sensitive files and we do not care if anyone gains access to them."
- A simple example is usually enough to change that mindset. Attackers compromised your systems and used them to compromise several systems at a large and important corporation and it was traced back to your company and you were held liable.
- The front page of every major newspaper (not to mention the other media) states that this company was successfully broken into and shows all of the sensitive files that were found.

## Remote Control

- Remote access to a sensitive system can be gained using one of two ways:
    - Physical access to the machine
    - Remotely control it over a network.
- Remotely controlling a machine involves controlling the machine over a network as if you were sitting at the machine.
- One example is Back Orifice, which once it is installed on a machine will let you have fall access to that machine.
- If proper filtering is not performed you can remotely control a machine over the Internet and, due to poor security, this is possible in many companies.

## Application Hijacking

- Application hijacking is similar in concept to session hijacking, which involves taking over an application and gaining unauthorized access.
- In many cases, if you can gain access to an application, you can access all the data that it has access to.
- If an attacker can gain access to a billing system or to HR records, they can acquire a lot of sensitive information about the company.
- This is an area that a lot of companies neglect. They worry about putting in firewalls and they are aware of their network security threats, but they totally ignore their applications.
- From a corporate or business office standpoint, applications provide the gateway into a company's most sensitive data.
- If these are not properly secured, firewalls will do little to protect against such attacks.

## Attack Routes

- In addition to the types of exploits, it is also important that we understand what can be exploited.

- Knowing what can be exploited shows us the weaknesses in our systems and what we need to do to protect against them.

- If you do not fully understand what can be exploited, you might be missing a huge vulnerability that an attacker can use to compromise your system. The main reason networks that have security and houses that have alarms get broken into is because they protect the wrong things or concentrate their efforts in the wrong area-in other words, they do not fully understand all points of exposure.

- A creative attacker will be able to attack almost anything and find ways to compromise a system. The following are some of the common things that can be exploited on a network:

    - Ports
    - Services
    - Third-party software
    - Passwords
    - Trojan horses
    - Inference channels
    - Covert channels

## Ports

- Ports are the entry points (windows and doors) into a computer system. There are literally thousands of different ports that can be open on a system.

- Actually, ports range in value from 1 to 65,535 for TCP and UDP. Because TCP and UDP use different ports, there are more than 100,000 different ports that can be open on a machine.

- The more ports that are open, the more points of vulnerability into a system. For a complete list of all of the ports and the protocols assigned to each, look at RFC1700.

- Some of the more common ones are the following:

  21. FTP (File Transfer Protocol)
  23. Telnet
  25. SMTP (Simple Mail Transfer Protocol)
  53. DNS (Domain Name Server)
  79. Finger
  80. HTTP (Hypertext Transfer Protocol)
  110. POP (Post Office Protocol)
  137-139. NETBIOS

- It is very important to run a port scanner on your own system and determine what ports are open and what the vulnerabilities are.

- To conduct a scan, an attacker has a wide variety of tools to choose from:
    - Nmap, by Fyodor ( www.insecure.org/nmap)
    - Strobe, by Julian Assange (packetstorm.securify.com)
    - Ultrascan, a Windows port scanner (packetstorm.securify.com)

- These will identify all the open ports on a system. From a security perspective it is very important to know which ports are open on your machine and close any that are not needed.

**Services**

- Services are programs that are running on a machine to perform a specific function. For example, a Windows server runs the server service to allow it to process requests, and a DNS server runs a service that handles the requests.

- Services become dangerous when they are running with root privileges. If a service is running as root, any command that it executes will also inherit the root privileges and run as root.

- This means that if the attacker is a normal user and wants to execute a process as root, all she has to do is exploit a service that is running as root and acquires root access to the system.

- Just as with ports, the more services that are running, the more points of vulnerability are available to an attacker.

- Therefore not only should the number of services be limited, but also the priority at which they are running.

## Third-Party Software

- Most of us place blind trust in the software vendors that their software works as advertised. History has shown that this is a very dangerous assumption to make, but we have no choice.
- There have been cases where viruses were embedded within shrink-wrapped software or software had back doors that were put in by the vendor.
- Think of the many hidden features there are in various operating systems. These are called easter eggs, and there are a large number of them available on the Web (www.eeggs.com).
- Check out the Solitaire egg for Windows XP.
- If an operating system can get shipped with these hidden features embedded within the code that no one knew about (including testing and quality control), one can only imagine what other back doors exist.
- People now publicize easter eggs because they are fun, but if a developer put a back door in an operating system so he could get back in whenever he wanted, he would not publicize it.

## Passwords

- Passwords cannot be the only line of defense in an organization. Even if there is a strong passwords policy in place, you must have access controls to limit who can access what, and logging to see if an attacker is trying to violate the policy.
- Passwords are also a common way to get into a system because employees generally have very weak passwords.
- To make the problem worse, the passwords never have to be changed, old accounts are not removed from the system, and backdoor accounts are created for easy access.
- All of these issues lead to the fact that passwords are a very easy way for an attacker to breach a company.
- Interestingly, passwords are one of the easiest things to secure because all of the tools you need are built into the operating system.
- That, combined with some user awareness sessions, and we can switch passwords from being the weakest link to being the strongest link.

## Trojan Horses

- A common way that an attacker gains access to a machine on a remote network is through the use of a Trojan horse program.
- A Trojan horse is a program that has two features: an overt (or open) feature and a covert (or hidden) feature.
- A Trojan horse works by running a hidden feature in the background while the open feature is running.
- For example, if an attacker wants to gain access to your system, she could send you an email attachment that does something cool; but in the background, it is creating a way for the attacker to get back into your system whenever she wants.

## Inference Channels

- An inference channel gathers information from open sources and surrounding events to collect sensitive information.
- In this case, indirect information can be just as valuable as direct information. For example, let's say the government is awarding a contract for a very sensitive project and it does not want to reveal who won the contract, but an attacker knows the five finalists.
- In the following weeks, he can sit outside the headquarters of the five companies and read the newspaper. If he notices one company receiving a large number of shipments and it is also advertising in the paper for several new positions, the attacker can infer who won the contract.
- Or in another example, if an attacker sits outside an office building and notices that a company receives several boxes from Microsoft three weeks after the release of Windows XP, he can make a pretty good guess that this company is upgrading its systems.
- With inference channels, there is no breach in security because the attacker is using open, available information to gather data about a company.

## Covert Channels

- A covert channel has a security breach because it involves a trusted insider who is sending information to an unauthorized outsider in a covert fashion.
- For example, an employee wants to let an outsider know if his company won a big contract and start investing in company stock before this information becomes public.
- The two could come up with a scheme to communicate this information secretly say using email.
- The employee could send an embedded document in a photograph say taken during her vacation to the outsider as soon as she finds out that the bid she worked on has been awarded the contract.
- Covert channels can also be used to send out company secrets and proprietary documents to outside agents.