This is a discussion of different network attacks. A network attack is defined as an intrusion that will analyze the network and gain information to exploit weaknesses that can cause the network to crash or to become corrupted from a denial of service or another attack on a network infrastructure. There are at least seven types of network attacks: **Spoofing**, **Sniffing**, **Mapping**, **Hijacking**, **Trojans**, **DoS and DDoS**, **Social engineering**.[[1]](#footnote-1)

**Spoofing**. Identity spoofing or IP spoofing is if an attacker obtains control over the software running on a network device; the device's protocols can be modified to place an arbitrary IP address into the data packet's source address field. This makes any payload appear to come from any source. To counter spoofing, routers perform ‘ingress filtering,’ which checks the IP address of incoming datagrams and determine whether the source address is in the valid range; if not then such packets are discarded.

**Sniffing**. Data packets traverse a network and a sniffer program works at the Ethernet layer in combination with network interface cards (NIC) to capture all traffic. Further, if a NIC is in promiscuous mode, the sniffer program will pick up all communication packets near the internet host site. A sniffer placed on a backbone device, inter-network link or network aggregation point will be able to passively monitor a whole lot of traffic. There are dozens of freely available packet sniffer programs on the internet. The more sophisticated ones allow more active intrusion. Sniffing can be detected two ways:

1. ***Host-based:*** NICs are configured at the factory to not run in promiscuous mode. Software commands exist to tell if the NIC is running in promiscuous mode.
2. ***Network-based:*** Solutions tend to check for the presence of running processes and log files, which sniffer programs consume a lot of. However, sophisticated intruders almost always hide their tracks by disguising the process and cleaning up the log files.

The best countermeasure against sniffing is end-to-end or user-to-user encryption.

**Mapping (Eavesdropping)**. Attackers gather information about a network so their attack can be more focused and are less likely to cause alarm. They want to know the IP address of machines on the network, the operating systems they use, and the services that they offer. The process of gathering this information is known as mapping. When an attacker is eavesdropping on network communications, it is referred to as *sniffing* or *snooping* the data paths in the network to "listen in" to the traffic. The messages are transmitted unsecured or "clear text" format, which allows an attacker to intercept them and gain access to the data. This is generally the biggest security problem that administrators face in an enterprise. Strong encryption services are the best measures to counter this threat.

**Hijacking (man-in-the-middle attack)**. Hijacking occurs when someone is listening between two computers that are communicating. The man-in-the-middle is actively monitoring, capturing, and controlling your communication transparently, to the point of the attacker re-routing a data exchange. Man-in-middle attacks are like someone assuming your identity in order to read your message. The other person on the other end might believe it is you, because the attacker might be actively replying as you, to keep the exchange going and gain more information. This technique takes advantage of a weakness in the TCP/IP protocol stack and the way to construct the headers. Computers communicate at low levels of the network layer and might not determine with whom they are exchanging data.

**Trojans**. People trust software that they are accustomed to using but a Trojan program may not be discernable from the original. It is a program that looks ordinary but actually performs malicious unintended actions behind the scenes when launched. The Trojan files will look, operate, and appear to be the same size as the compromised system files. Most remote control spyware programs are Trojans. The only protection against a Trojan attack is to verify the source of downloaded software and check files before installing software with the use of a *cryptographic checksum* or *binary digital signature* procedure.

**Denial-of-Service attack (DoS)** and Distributed-Denial-of-Service (DDoS). A denial of service (DoS) attack is an Internet attack aimed at large websites. It is designed to bring the network to its knees by flooding the network with useless traffic and overwhelming the server with service request. Web services can be denied to hosts computers when a system, such as a Web server, has been flooded with illegitimate requests, thus making it impossible to respond to real requests. Yahoo! and e-bay were both victims of such attacks in February 2000. A Dos attack can be perpetrated in a number of ways. There are three basic types of attack.

* Consumption of computational resources, such as band width, disk space or CPU time.
* Disruption of configuration information, such as routing information.
* Disruption of physical network components.

The consequences of a DoS attack are the following:

* Inability to access any web site.
* Unavailability of a particular web site.
* Unusually slow network performance.
* Dramatic increase in the amount of spam you receive in your account.
* A distributed denial of service attack (DDoS) occurs when multiple compromised systems or multiple attackers flood the network with useless traffic, which consumes band width or resources of a targeted system. These systems are compromised by attackers using a variety of methods.
* In DDoS attacks, the attacker first gains access to user accounts on numerous hosts across the Internet. The attacker then installs and runs a slave program at each compromised site that quietly waits for commands from a master program. The master program then contacts the slave programs, instructing each of them to launch a denial-of-service attack directed at the same target host. The resulting coordinated attack is particularly devastating, since it comes from so many attacking hosts at the same time.
* Here also ingress filtering only can control DoS attack and that too to a small extent.

**Common forms of denial of service attacks:**

a) Buffer Overflow Attacks. This is the most common kind of DoS attack. An excess of traffic is received at a network address and is more than the programmer's expectation on the size of the buffers. Internal to the messages, portions are redirected to virus code, hidden in the message. A few of the better known attacks based on the buffer characteristics of a program or system include:

* Sending e-mail messages that have attachments with 256 character file names to Netscape and Microsoft mail programs.
* Sending over sized Internet Control Message Protocol (ICMP) packets.
* Ending to a user of an e-mail program a message with a "From" address longer than 256 characters.

b) Smurf Attack. The attacker sends an IP ping request to a receiving site. The MAC address has been altered to make it appear that the ping packet was sent from another host on the network, which is the target site that is to receive the denial of service attack. The result will be lots of ping replies flooding back to the innocent, spoofed host. If the flood is great enough, the spoofed host will no longer be able to receive or distinguish real traffic.

c) SYN Floods. When a computer wants to make a TCP/IP connection to a server, an exchange of TCP/SYN and TCP/ACK packets of information occur. The user's computer request the connection, sends a TCP/SYN packet which asks the server if it can connect. If the server is ready, it sends a TCP/SYN-ACK packet back to the client to say "Yes, you may connect" and reserves a space for the connection, waiting for the client to respond with a TCP/ACK packet. In a SYN flood, the address of the client is often forged so that when the server sends a TCP/SYN-ACK packet back to the client, the message is never received acknowledged by the client because, either the client doesn't exist or wasn't expecting the packet and subsequently ignores it. This leaves the server with a dead connection, reserved for a client that will never respond. Usually this is done to one server many times in order to reserve all the connections for unresolved clients, which keeps legitimate clients from making connections.

**Social engineering**. The attacker might try to obtain unauthorized access to network devices. Unmonitored network devices are the main source of information leakage in organizations which can include email messages, web page requests, user logons, and transmitted files, handled by a network device. Network attacks cut across all categories of software and platform type.

Social engineering is the use of persuasion or deception to victims to gain access to information systems. The medium is usually a telephone or e-mail message. The attacker usually pretends to be a person of a high position and attempts to deceive a subordinate worker to gain their help to access sensitive data. They have a story that they need some important data left on their network drive but has a reason that they cannot access it themselves. They pressure the help desk to give them the toll-free number of the RAS server to dial and sometimes get their password reset. The main purpose behind social engineering is to place the human element in the network-breaching loop and use it as a weapon. The human element has been referred to as the weakest link in network security.

**Examples of social engineering.**

1. ***Faked Email:*** The attack agent sends a message to users in a domain "as the system administrator and their password must be reset to user 123 " for a temporary period of time. The hacker then continuously monitors for the change and then exploits the whole system.
2. ***Fake Competition:*** The social engineer manipulates a group of users to participate in some fake competition for a jackpot prize, with the ultimate purpose of eventually extracting confidential information about network and password security.
3. ***The Helpful Help Desk:*** The help desk gets a call from the social engineer impersonating a user reporting a forgotten password. In many cases the help desk will change the user's password over the phone. The hacker now has a legitimate user name and password to work with. To avoid problems from the original user, the social engineer will then call the user who was impersonated and say something like "This is Pinocchio from the MIS department. We had some problems with security today, so we have changed your password. Your new password is angel123."

**Injection (SQL or LDAP)**.[[2]](#footnote-2) An attacker can craft an LDAP query to be inserted as user input and be processed by an LDAP server. The purpose is to undermine the security of the target and input can inject additional commands into an LDAP query that could disclose sensitive information. For example, entering a \* in the aforementioned query might return information about all users on the system. This attack is very similar to an SQL injection attack in that it manipulates a query to gather additional information or coerce a particular return value.[[3]](#footnote-3)  
Some good guidelines for implementing authentication is the ‘Authentication Cheat Sheet,’ posted among other security cheat sheets, by the Open Web Application Security Project (OWASP)[[4]](#footnote-4)

1. Different Types of Network Attacks And Security Threats and Counter Measures, By Reeshil N, downloaded from <http://ayurveda.hubpages.com/hub/Types-of-Network-Attacks> [↑](#footnote-ref-1)
2. CAPEC - CAPEC-136: LDAP Injection (Version 2.6) ﻿downloaded from <http://capec.mitre.org/data/definitions/136.html> [↑](#footnote-ref-2)
3. CWE - CWE-90: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') (2.8) downloaded from <http://cwe.mitre.org/data/definitions/90.html> [↑](#footnote-ref-3)
4. ‘Authentication Cheat Sheet’ is posted by the *Open Web Application Security Project* *(OWASP)* listed on this page: <https://www.owasp.org/index.php/Cheat_Sheets> [↑](#footnote-ref-4)