Tipovi napada

izvor

- DoS- Denial of Service
- Trojan Horse - Comes with other software.
- Virus - Reproduces itself by attaching to other executable files.
- Worm - Self-reproducing program. Creates copies of itself. Worms that spread using e-mail address books are often called viruses.
- Logic Bomb - Dormant until an event triggers it (Date, user action, random trigger, etc.).

Hacker Attacks

I use the term “hacker attacks” to indicate hacker attacks that are not automated by programs such as viruses, worms, or trojan horse programs. There are various forms that exploit weakneses in security. Many of these may cause loss of service or system crashes.

- IP spoofing - An attacker may fake their IP address so the receiver thinks it is sent from a location that it is not actually from. There are various forms and results to this attack. The attack may be directed to a specific computer addressed as though it is from that same computer. This may make the computer think that it is talking to itself. This may cause some operating systems such as Windows to crash or lock up.
- Gaining access through source routing. Hackers may be able to break through other friendly but less secure networks and get access to your network using this method.
- Man in the middle attack -
- Session hijacking - An attacker may watch a session open on a network. Once authentication is complete, they may attack the client computer to disable it, and use IP spoofing to claim to be the client who was just authenticated and steal the session. This attack can be prevented if the two legitimate systems share a secret which is checked periodically during the session.
- Server spoofing - A C2MYAZZ utility can be run on Windows 95 stations to request LANMAN (in the clear) authentication from the client. The attacker will run this utility while acting like the server while the user attempts to login. If the client is tricked into sending LANMAN authentication, the attacker can read their username and password from the network packets sent.
- DNS poisoning - This is an attack where DNS information is falsified. This attack can succeed under the right conditions, but may not be real practical as an attack form. The attacker will send incorrect DNS information which can cause traffic to be diverted. The DNS information can be falsified since name servers do not verify the source of a DNS reply. When a DNS request is sent, an attacker can send a false DNS reply with additional bogus information which the requesting DNS server may cache. This attack can be used to divert users from a correct webserver such as a bank and capture information from customers when they attempt to logon.
- Password cracking - Used to get the password of a user or administrator on a network and gain unauthorized access.

Some DoS Attacks

- Ping broadcast - A ping request packet is sent to a broadcast network address where there are many hosts. The source address is shown in the packet to be the IP address of the computer to be attacked. If the router to the network passes the ping broadcast, all computers on the network will respond with a ping reply to the sttacked system. The attacked system will be flooded with ping responses which will cause it to be unable to operate on the network for some time, and may even cause it to lock up. The attacked computer may be on someone else's network. One countermeasure to this attack is to block incoming traffic that is sent to a broadcast address.

- Ping of death - An oversized ICMP datagram can crash IP devices that were made before 1996.
- Smurf - An attack where a ping request is sent to a broadcast network address with the sending address spoofed so many ping replies will come back to the victim and overload the ability of the victim to process the replies.
- Teardrop - a normal packet is sent. A second packet is sent which has a fragmentation offset claiming to be inside the first fragment. This second fragment is too small to even extend outside the first fragment. This may cause an unexpected error condition to occur on the victim host which can cause a buffer overflow and possible system crash on many operating systems.