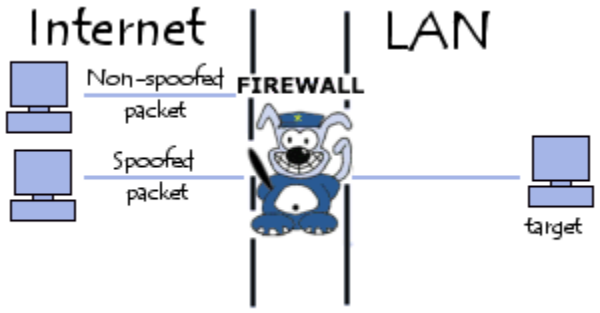
IP address spoofing

IP address spoofing

"**IP address spoofing**" is a technique that involves replacing the IP address of an IP packet's sender with another machine's IP address.
This technique lets a pirate send packets anonymously. It is not a question of changing the IP address, but rather of *impersonating* the IP address when packets are sent.
Some people tend to assimilate the use of a proxy (which makes it possible to hide the IP address) with IP spoofing. Yet proxies merely transfer packets. As such, even if the address appears to be hidden, a pirate can easily be found thanks to the proxy's log file.

Spoofing attack

The IP address spoofing technique can enable a pirate to send packets on a network without having them be intercepted by the packet filtering system (firewall).
Firewall systems are usually based on filtering rules indicating the IP addresses that are authorized to communicate with the network's internal machines.



A packet spoofed with an internal machine's IP address will appear to come from the internal network and will be transferred to the target machine, whereas a packet containing an external IP address will be automatically rejected by the firewall.

However, the TCP protocol (protocol primarily guaranteeing the reliable transfer of data over the Internet) is based on authentication and trust relationships between a network's machines, which means that to accept the packet, the recipient must acknowledge receipt from the sender, and the sender has to acknowledge receipt of the acknowledgement.

TCP header modification

On the internet, information circulates thanks to the IP protocol, which ensures data encapsulation in structures called packets (or more precisely *IP datagrams*). Here is the structure of a datagram:

Version	Header length	Type of service	Total length	
Identification			Flag	Fragment offset
Time to live		Protocol	Header checksum	
Source IP address				
Destination IP address				
Data				

Spoofing an IP address comes down to modifying the *source* field to simulate a datagram coming from another IP address. Yet on the internet, packets are generally sent via the TCP protocol, which guarantees so-called "reliable" transmission.
Before accepting a packet, a machine must first acknowledge receipt of the packet from the sending machine, and wait for the latter to confirm receipt of the acknowledgement.

Trust relationships

The TCP protocol is one of the main protocols of the TCP/IP model's transport layer. It makes it possible, at the application level, to manage data coming from (or going to) the lower layer of the model (that is, the IP protocol).
The TCP protocol makes it possible to reliably transfer data, although it uses the IP protocol (which does not check datagram delivery) thanks to an acknowledgement (ACK) system enabling both the client and the server to make sure data have been received on both sides.

IP datagrams encapsulate TCP packets (called *segments*), which are structured as follows:
<td
URG <td
ACK <td
PSH <td
RST <td
SYN <td
FIN</td
</td

</td
</td
</td
</td

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Source port																Destination port															
Sequence number																															
Acknowledgement number																															
Data offset				reserved						Window																					
Checksum																Urgent pointer															
Options																						Padding									
Data																															

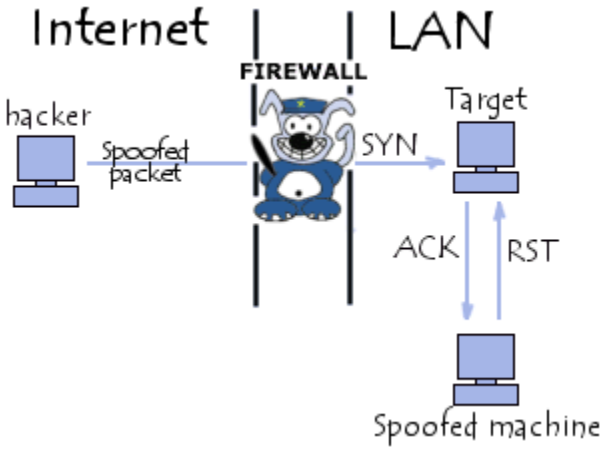
When sending a segment, a sequence number is associated with it, and an exchange of segments containing special fields (called *flags*) makes it possible to synchronize the client and the server.
This dialogue (called a *three-way handshake*) makes it possible to initiate the communication; is it broken down into three phases, as its name suggests:

- Firstly, the sending machine (the client) sends a segment whose SYN flag is at 1 (to show it is a synchronization segment), with a sequence number N, which is called the client's initial sequence number.
- Secondly, the receiving machine (server) receives the client's initial segment, then sends it an acknowledgement, that is, a segment whose ACK flag is non null (acknowledgment) and whose SYN is at 1 (since it is still a synchronization). This segment contains a sequence number that is equal to the client's initial sequence number. The most important field in this segment is the acknowledgement field (ACK), which contains the client's initial sequence number, incremented by 1.
- Then the client sends the server an acknowledgement, that is, a segment whose ACK flag is non null and whose SYN flag is at zero (it is no longer a synchronization segment). Its sequence number is incremented and the acknowledgement number represents the server's initial sequence number incremented by 1.

. The spoofed machine will respond with a TCP packet whose RST (*reset*) flag is non null, which will end the connection.

Destroying the spoofed machine

When carrying out an IP address spoofing attack, the attacker has no information in return since the target machine's responses go to another network machine (this is called a *blind attack*).

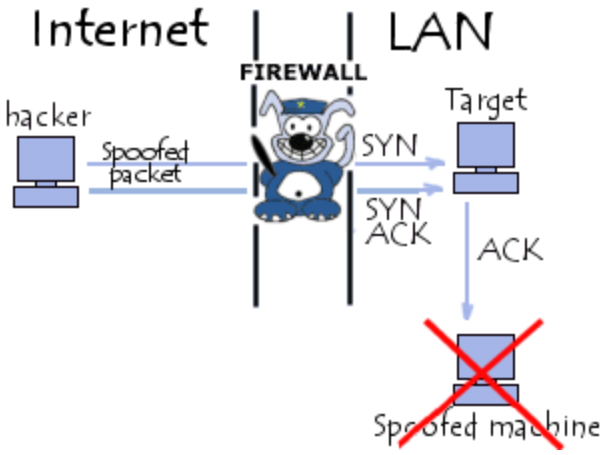


In addition, the "spoofed" machine deprives the hacker of any connection attempt, since it systematically sends an RST flag to the target machine. The pirate's work therefore involves invalidating the spoofed machine by making it unreachable throughout the duration of the attack.

Predicting sequence numbers

When the spoofed machine has been invalidated, the target machine waits for a packet containing the acknowledgment and the right sequence number. The pirate's work involves "guessing" the sequence number to send back to the server to establish the trusting relationship.

To do so, pirates generally use *source routing*, that is, they use the *option* field in the IP header to indicate a specific return route for the packet. As such, thanks to sniffing, the pirate will be capable of reading the content of the return packets...



By knowing the last sequence number sent, the pirate draws up statistics concerning its incrementation and sends acknowledgements until he obtains the right sequence number.

Source: http://en.kioskea.net/contents/41-ip-address-spoofing