2.3 IP Spoofing

IP spoofing is essentially a technique used by hackers to gain unauthorised access to computers. Although this is the most common reason for IP spoofing, it is occasionally done simply to mask the origins of a DoS attack. In fact DoS attacks often mask the actual IP address from where the attack has originated from.

With IP spoofing, the intruder sends messages to a computer system with an IP address indicating that the message is coming from a different IP address than it is actually coming from. If the intent is to gain unauthorised access, then the spoofed IP address will be that of a system the target considers a trusted host.

To successfully perpetrate an IP spoofing attack, the hacker must first find the IP address of a machine that the target system considers a trusted source. Hackers might employ a variety of techniques to find an IP address of a trusted host. After they have obtained the trusted IP address, they can then modify the packet headers of their transmissions so it appears that the packets are coming from that host.

IP spoofing, unlike many other types of attacks, had been known to security experts on a theoretical level before it was ever used in a real attack. The concept of IP spoofing was initially discussed in academic circles as early as the 1980s. Although the concept behind this technique was known for some time, it was primarily theoretical until Robert Morris discovered a security weakness in the TCP protocol known as sequence prediction.

IP spoofing attacks are becoming less frequent, primarily because the venues they use have become more secure, and in some cases, simply no longer used. However, spoofing can still be used and all security administrators should address it.

A couple of different ways to address IP spoofing include:

- Do not reveal any information regarding your internal IP addresses. This helps prevent those addresses from being “spoofed.”
- Monitor incoming IP packets for signs of IP spoofing using network monitoring software. One popular product is Netlog. Netlog, alongside other similar products, seeks incoming packets to the external interface that have both the source and destination IP addresses in your local domain. This essentially means an incoming packet that claims to be from inside the network is actually coming from outside your network. Finding one means that an attack is underway.

The danger that IP spoofing contains is that some firewalls do not examine packets that appear to come from an internal IP address. Routing packets through filtering routers is possible, if they are not configured to filter incoming packets, whose source address is in the local domain.

Examples of router configurations that are potentially vulnerable include:

- Routers to external networks that support multiple internal interfaces
- Proxy firewalls where the proxy applications use the source IP address for authentication
- Routers with two interfaces that support subnetting on the internal network
- Routers that do not filter packets whose source address is in the local domain