**LIST OF ABBREVIATION**

|  |  |
| --- | --- |
| IP | Internet protocol |
| Tcp | Transmission control protocol |
| Sat | Satellite |
| Nat | network address translation |
| Udp | User defined protocol |
| Acl | Acess control list |
| DoS | Denial of services |

**Abstract**

IP spoofing is a method of attacking a network in order to gain unauthorized access. The attack is based on the fact that Internet communication between distant computers is routinely handled by routers which find the best route by examining the destination address, but generally ignore the origination address. The origination address is only used by the destination machine when it responds back to the source.

In a spoofing attack, the intruder sends messages to a computer indicating that the message has come from a trusted system. To be successful, the intruder must first determine the IP address of a trusted system, and then modify the packet headers to that it appears that the packets are coming from the trusted system.

In essence, the attacker is fooling (spoofing) the distant computer into believing that they are a legitimate member of the network. The goal of the attack is to establish a connection that will allow the attacker to gain root access to the host, allowing the creation of a backdoor entry path into the target system.