An attack can be considered a spoofing attack anytime an attacker injects traffic that appears to be sourced from a system other than the attacker's system itself. Spoofing is not specifically an attack, but spoofing can be incorporated into various types of attacks.

The figure below illustrates IP address spoofing. Attacker 172.25.9.7 sends a packet to server 10.1.2.3 but specifies 192.168.6.4 as the source address of the packet. Server 10.1.2.3 sends its response packet to what it believes to be the originating system, host 192.168.6.4.

A computer screen with a computer and a graph

Description automatically generated with medium confidence

There are several types of spoofing, including the following:

* **IP address spoofing:** IP address spoofing is the most common type of spoofing. To perform IP address spoofing, attackers use source IP addresses that are different than their real IP addresses.
* **MAC address spoofing:** To perform MAC address spoofing, attackers use MAC addresses that are not their own. MAC address spoofing is generally used to exploit weakness at Layer 2 of the network.
* **Application or service spoofing:** One example is DHCP spoofing, which can be done with either the DHCP server or the DHCP client. To perform DHCP server spoofing, the attacker enables a rogue DHCP server on a network. When a victim host requests a DHCP configuration, the rogue DHCP server responds before the authentic DHCP server. The victim is assigned an attacker-defined IP configuration. From the client side, an attacker can spoof many DHCP client requests, specifying a unique MAC address per request. The DHCP server's IP address pool may become exhausted, leading to a DoS against valid DHCP client requests. Another simple example of spoofing at the application layer is an email from an attacker which appears to have been sourced from a trusted email account.

Another example of spoofing is a land attack. The attack is named for the name of the file, land.c, used for the original source code that is compiled into an attack tool. In a land attack, the attacker sends a TCP SYN request using the same IP address and port as both the source and destination IP address and port. The IP address and port combination that is used is that of the target system. The target system replies to itself and, if the system is vulnerable, the response leads to a system crash.