What is a Spoofing Attack?

A spoofing attack is when an attacker or malicious program successfully acts on another person’s (or program’s) behalf by impersonating data.

takes place when the attacker pretends to be someone else (or another computer, device, etc.) on a network in order to trick other computers, devices or people into performing legitimate actions or giving up sensitive data. Some common types of spoofing attacks include ARP spoofing, DNS spoofing and IP address spoofing. These types of spoofing attacks are typically used to attack networks, spread malware and to access confidential information and data.

**Types of Spoofing Attacks**

* 1. ARP Spoofing Attack

The Address Resolution Protocol (ARP) is a protocol used to translate IP addresses into Media Access Control (MAC) addresses in order to be properly transmitted. In short, the protocol maps an IP address to a physical machine address.

This type of spoofing attack occurs when a malicious attacker links the hacker’s MAC address with the IP address of a company’s network. This allows the attacker to intercept data intended for the company computer. ARP spoofing attacks can lead to data theft and deletion, compromised accounts and other malicious consequences. ARP can also be used for DoS, hijacking and other types of attacks.

* 1. DNS Spoofing Attack

The Domain Name System (DNS) is responsible for associating domain names to the correct IP addresses. When a user types in a domain name, the DNS system corresponds that name to an IP address, allowing the visitor to connect to the correct server. For a DNS spoofing attack to be successful, a malicious attacker reroutes the DNS translation so that it points to a different server which is typically infected with malware and can be used to help spread viruses and worms. The DNS server spoofing attack is also sometimes referred to as DNS cache poisoning, due to the lasting effect when a server caches the malicious DNS responses and serving them up each time the same request is sent to that server.

* 1. IP Spoofing Attack

The most commonly-used spoofing attack is the IP spoofing attack. This type of spoofing attack is successful when a malicious attacker copies a legitimate IP address in order to send out IP packets using a trusted IP address. Replicating the IP address forces systems to believe the source is trustworthy, opening any victims up to different types of attacks using the ‘trusted’ IP packets.

The most popular type of IP spoofing attack is a Denial of Service attack, or DoS, which overwhelm and shut down the targeted servers. One outcome attackers can achieve using IP spoofing attacks is the ability to perform DoS attacks, using multiple compromised computers to send out spoofed IP packets of data to a specific server. If too many data packets reach the server, the server will be unable to handle all of the requests, causing the server to overload. If trust relationships are being used on a server, IP spoofing can be used to bypass authentication methods that depend on IP address verification.