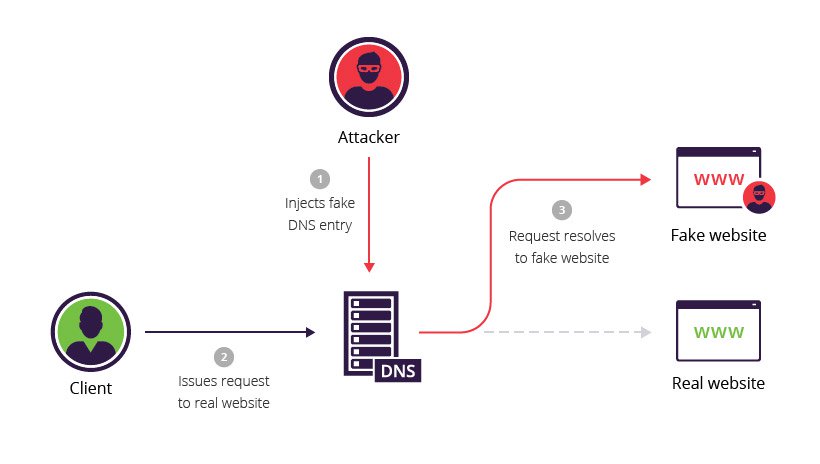
**DNS Spoofing**

DNS Spoofing Attack is a type of cyber-attack in which an attacker corrupts the DNS cache of a user's computer or a DNS server, diverting traffic to a malicious website or server. DNS Spoofing Attack is also known as DNS Cache Poisoning, DNS Spoof Attack, or DNS Cache Spoofing (Zheng, Lin, & Huang, 2019). DNS is an essential component of the internet's infrastructure, and DNS Spoofing Attack can cause significant damage to network traffic, as well as compromise users' data and online privacy.

DNS Spoofing Attack works by exploiting vulnerabilities in the Domain Name System (DNS), which translates domain names into IP addresses. When a user types a URL into their web browser, the DNS server is queried to find the IP address of the requested website. In a DNS Spoofing Attack, an attacker sends a false DNS response to the user's computer or DNS server, with a spoofed IP address, making it believe that the malicious website's IP address is the legitimate one. This can redirect the user to the attacker's website or a website controlled by them, leading to phishing attacks or data theft. DNS Spoofing Attack is a prevalent type of cyber-attack that can cause significant damage to network traffic and users' online privacy. In this attack, an attacker attempts to intercept the DNS lookup request from the user's computer. The attacker will then replace the legitimate IP address of the website with the IP address of the attacker's malicious or fake website. This is done by tricking the DNS server into believing that the malicious IP address is correct by using a forged DNS response packet. The user then interacts with the copycat site unknowingly by sharing passwords their passwords and credentials.



DNS Spoofing Attack is a dominant sort of cyber-attack, and it can be carried out in several ways, such as:

**Cache Poisoning Attack**: In this type of attack, an attacker sends a forged DNS response to the DNS cache, replacing the legitimate IP address with the attacker's IP address.

**Man-in-the-Middle Attack:** In this type of attack, an attacker intercepts the DNS request and sends a forged response to the user's computer or DNS server, directing the user to a malicious website.

**DNS Server Spoofing Attack:** In this type of attack, an attacker spoofs a DNS server and sends a forged DNS response to the user's computer or DNS server.

**Implementation of DNS Spoofing Attack**

The general steps involved in a DNS Spoofing Attack are:

Performing the DNS cache poisoning attack required two machines one will be kali Linux and the other will be the target machine on which a DNS spoofing attack will happen. In the first step edit the Ettercap configuration file by using the command sudo nano /etc/Ettercap/Ettercap.config and it will open the configuration file of Ettercap. In the configuration file replace the ec\_uid and e\_gid to “0”. After that move below and under the Linux removed the # from two lines and save the file. After that edit, the second file sudo nano /etc/Ettercap/Ettercap.dns in this dns file add this line www.facebook.com A 10.20.30.130 so whenever the user try to browse the facebook.com it will come to a spoofed hosted site. In Kali Linux under the folder /var/www/html create a new file named it index.html and add the html code or make a landing page, then restart the apache server to affect the new configuration.

After that launch the Ettercap and click on the tick sign to start it. Once Ettercap has been opened then from the menu select the option scan hosts and it will scan and show you the available host on the network. Open the host list and select the target machine IP address and add it to target1. After setting up a target in “ettercap” then open Plugins -> Manage the Plugins -> double click DNS Spoof plugin. From the menu click on the ARP poisoning it will show the MTM Attack: ARP Poisoning popup tick mark on the option sniff remote connections and click ok, the attack will be initialized. Then go to the target machine and access the website [www.facebook.com](http://www.facebook.com) and it will show the spoofed website.

**Prevention of DNS spoofing attacks**

* Implementing DNS spoofing Detection measures: The DNSSEC provides an authentication mechanism for data from the DNS server. It helps the confidentiality of data and works to ensure that the data records have not been tampered with. Use of VPN: A VPN creates an encrypted tunnel between the computer and the websites by encrypting the traffic flow.
* Incorporation of Firewalls: This will help to block incoming connections that have not been allowed
* Keeping the software and security systems up-to-date: Apply security updates to operating systems, applications, and databases on a regular basis to ensure that any security vulnerabilities are patched promptly.