**EXPERIMENT -04**

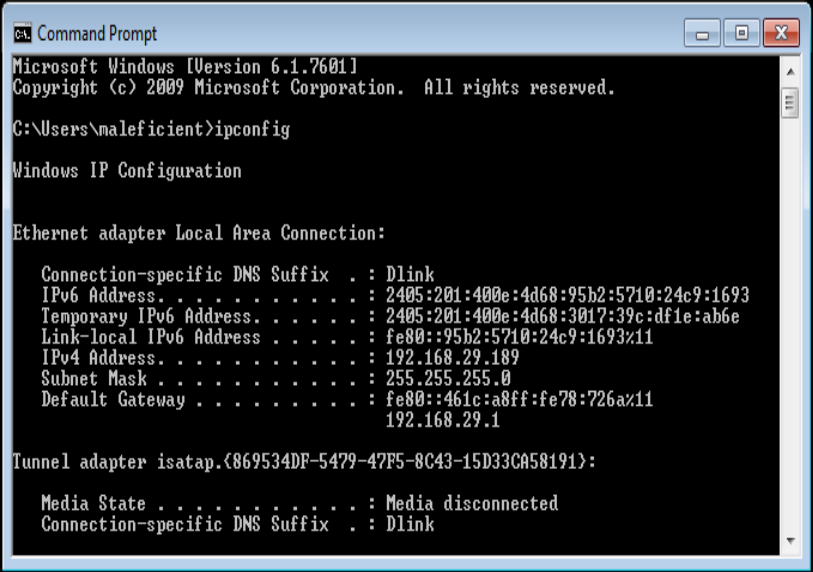
**Aim: DNS (Domain name System) poisioning attack using Bettercap Tool**

**Theory:** DNS Spoofing is the result of alterations to a DNS server’s records resulting in the malicious redirection of traffic. DNS spoofing can be performed by a direct attack on the DNS server (what we will be talking about here) or through any form of a Man-in-the-Middle attack specifically targeting DNS traffic.

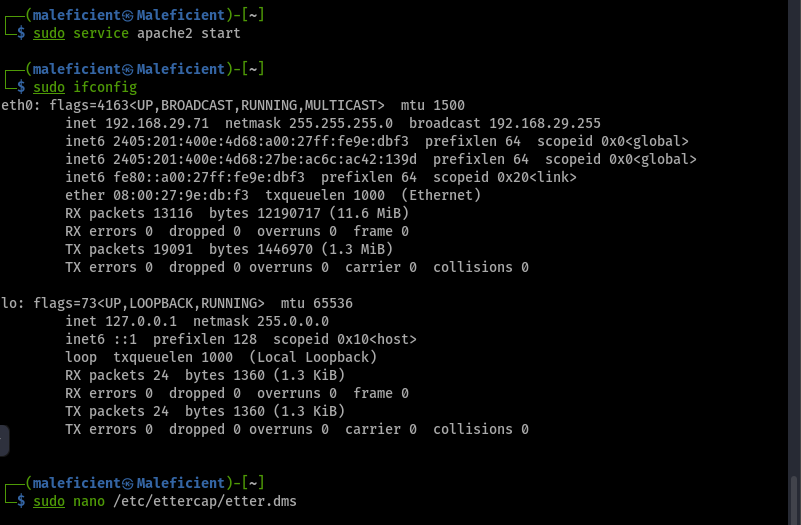
DNS Cache spoofing works explicitly in a way that exploits the way in which DNS communication is structure. When a DNS server attempts to perform a lookup on a domain, it will forward the request along to the root authoritative DNS and iteratively proceed down the chain of DNS servers until it reaches the DNS server authoritative over the domain. Since the local DNS server does not know which server is in charge of which domain, and does not know the full route to each authoritative server, it accepts replies to its queries from anywhere so long as the reply matches the query and is formatted correctly. The attacker can exploit this design by beating the actual Authoritative DNS server in replying to the local DNS server, and if it does so, the local DNS server will use the attacker’s DNS record instead of the actual Authoritative answer. Due to the nature of DNS, the local DNS server has no way of determining which reply is real and which is fake.

**Steps:**

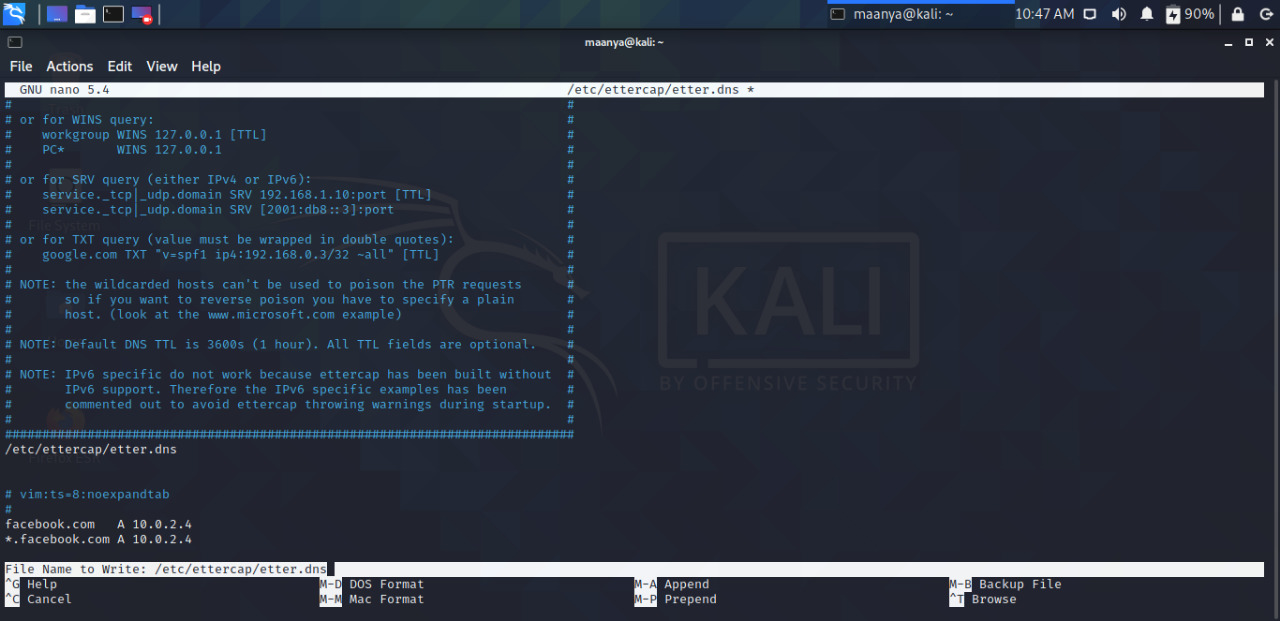
1. Start the windows device and note its IP Address and Subnet Mask using ‘ipconfig command’.

****

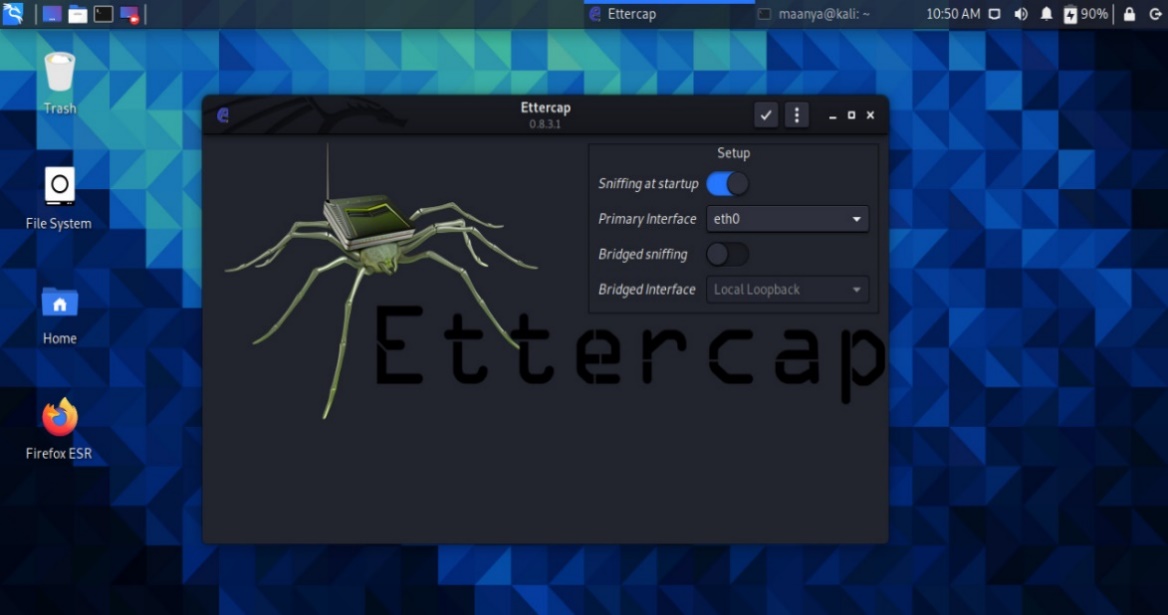
1. Enable Apache Service and open ‘etter.dns’ file using the command, sudo nano /etc/ettercap/etter.dns.

****

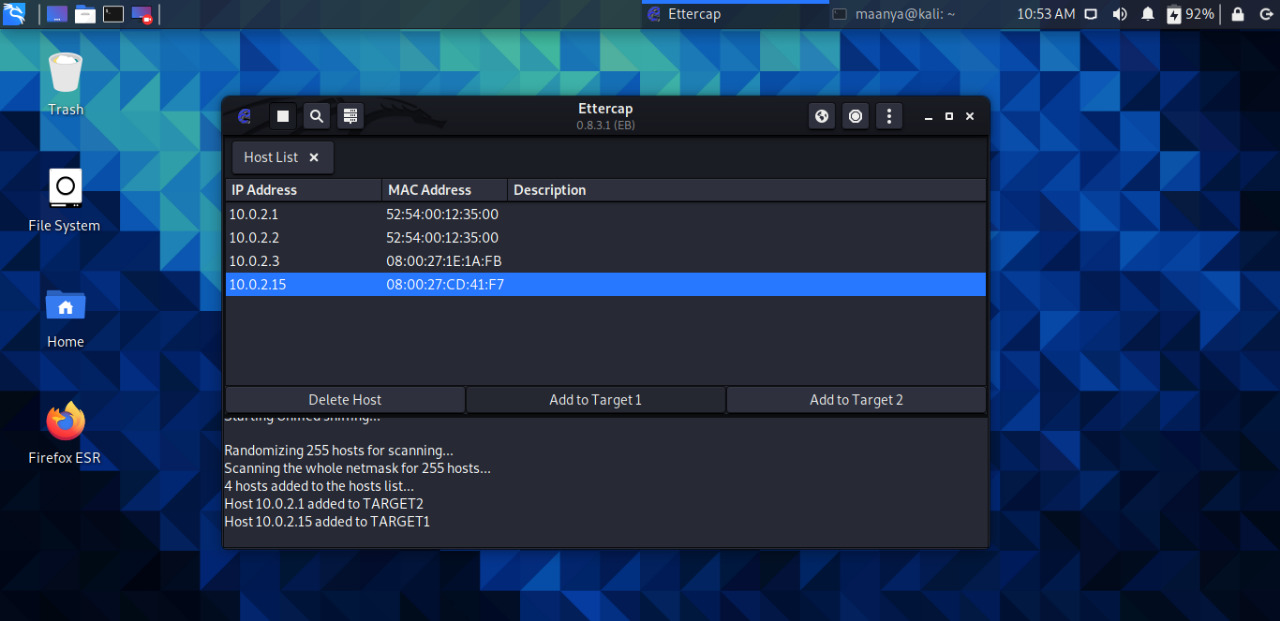
1. Make the changes in dns file.



1. Open Ettercap tool and select the target hosts from the scanned hosts list.



1. Open Plugins and activate the dns spoof plugin by double clicking it.



1. Now in the windows machine open the target website, here Facebook.com.

