DNS SPOOFING

DNS spoofing is a malicious technique used by attackers to manipulate the Domain Name System (DNS) to redirect users to fraudulent websites or other destinations without their knowledge. The DNS acts as the internet's directory, translating human-readable domain names (like "example.com") into IP addresses (such as "192.0.2.1") that computers use to communicate with each other. By spoofing DNS responses, attackers can deceive users into unknowingly visiting malicious websites or providing sensitive information.

Here's how DNS spoofing typically works:

1. **Mapping Domain Names to IP Addresses:** When a user enters a domain name into their web browser, the DNS resolver on their computer or network queries a DNS server to obtain the corresponding IP address. This process involves multiple steps of querying authoritative DNS servers to find the correct mapping.
2. **Interception of DNS Requests:** An attacker intercepts DNS requests sent by the victim's computer or network. This interception can occur through various means, such as compromising a DNS server, compromising the victim's router, or conducting a Man-in-the-Middle (MitM) attack.
3. **Falsifying DNS Responses:** Once the attacker intercepts the DNS request, they send a falsified DNS response to the victim's computer or network. This response contains a forged IP address, typically pointing to a server controlled by the attacker rather than the legitimate destination.
4. **Redirecting Traffic:** The victim's computer or network, unaware of the deception, directs its traffic to the IP address provided in the falsified DNS response. As a result, the user may end up on a fake website that resembles the legitimate one or may unknowingly submit sensitive information to the attacker.

DNS spoofing can be used for various malicious purposes, including:

- **Phishing:** Attackers can create fake websites that mimic legitimate ones, tricking users into entering their login credentials, personal information, or financial details.
- **Malware Distribution:** Attackers can redirect users to websites hosting malware, leading to the inadvertent download and installation of malicious software on their devices.
- **Data Interception:** By intercepting DNS requests, attackers can redirect traffic to servers under their control to intercept sensitive data, such as usernames, passwords, or credit card information.

To mitigate the risk of DNS spoofing, organizations and users can implement various security measures, including:

- DNSSEC (Domain Name System Security Extensions): DNSSEC adds cryptographic signatures to DNS responses, allowing clients to verify the authenticity of DNS data and detect DNS spoofing attempts.

- Use of Trusted DNS Servers: Ensure that DNS requests are sent to reputable and secure DNS servers that are less likely to be compromised.
- Implementing DNS Monitoring: Regularly monitor DNS traffic for any signs of unusual activity, such as unexpected changes in DNS records or repeated DNS queries for the same domain.
- Network Segmentation and Access Control: Segmenting networks and implementing access controls can limit the impact of DNS spoofing attacks by containing their effects within isolated network segments.

By understanding how DNS spoofing works and implementing appropriate security measures, organizations and users can reduce the risk of falling victim to this type of cyberattack.

Tools for performing DNS spoofing attacks or detecting and mitigating

- **Ettercap:** Ettercap is a comprehensive suite for Man-in-the-Middle attacks on LAN. It supports various protocols and has features for sniffing live connections, content filtering on the fly, and many other interesting tricks.
- **Cain & Abel:** Cain & Abel is a popular password recovery tool for Microsoft operating systems. However, it also includes features for ARP poisoning, DNS spoofing, and network analysis.
- **Bettercap:** Bettercap is a powerful, flexible, and portable tool for network attacks and monitoring. It supports various MITM attacks, including DNS spoofing, ARP spoofing, and SSL stripping.
- **Wireshark:** Wireshark is a widely-used network protocol analyzer. While not specifically a tool for DNS spoofing, it can be used to detect suspicious DNS traffic and anomalies in network communications, helping to identify potential DNS spoofing attacks.
- **DNSChef:** DNSChef is a highly configurable DNS proxy that can be used for DNS spoofing and redirection. It allows you to create custom DNS responses to redirect DNS queries to a specified IP address.
- **DNSleaktest.com:** While not a tool for performing DNS spoofing attacks, DNSleaktest.com is a useful online tool for detecting DNS leaks. It helps users determine if their DNS queries are being sent outside of their intended network, which could indicate DNS spoofing or other security issues.

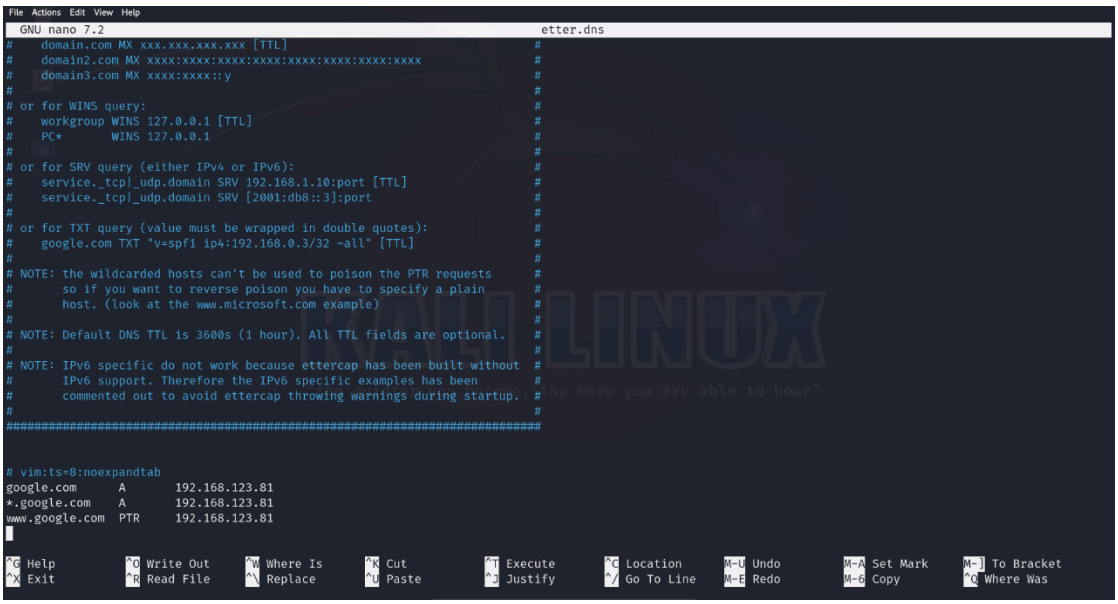
These tools have legitimate uses for network analysis, security testing, and troubleshooting, but they can also be abused for malicious purposes. It's important to use them responsibly and ethically, within the boundaries of applicable laws and regulations. Additionally, network administrators and security professionals should be familiar with these tools to better understand and mitigate the risks associated with DNS spoofing attacks.

Now let’s carry out example of DNS poisoning with ETTERCAP

1st setup the index or fake sample page index.html

Now edit the etter.dns file in the /etc/ettercap directory. This file contains all entries for DNS address which are used by Ettercap to resolve URL addresses.

> sudo nano etter.dns



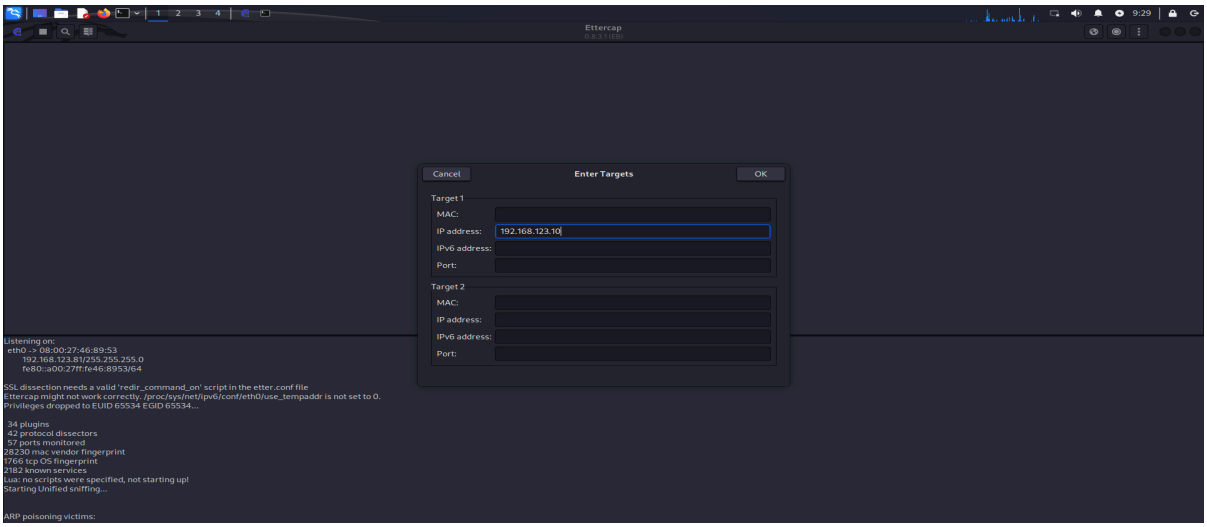
In this file we created our own DNS entry redirecting google.com to 192.168.123.81. Save and exit.

DNS Spoofing by GOVERDHAN

Let fire up Ettercap in graphical mode

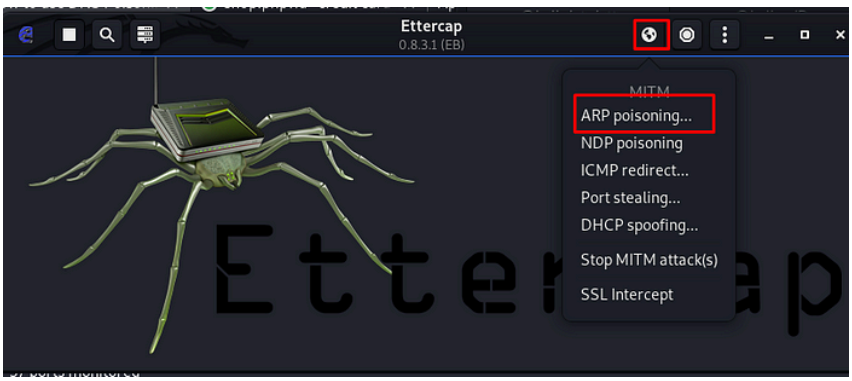
We are going to use Ettercap to carry out this attack.

First let’s add target

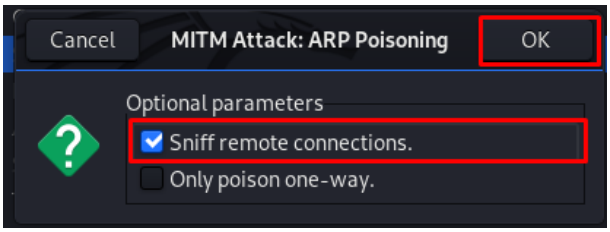


Now Start sniffing the network

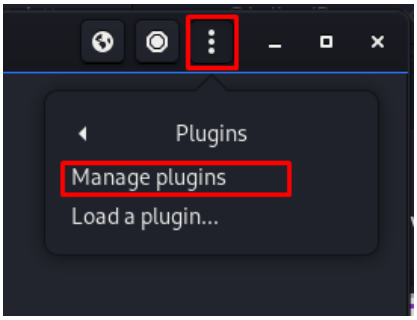
Now click the MITM menu and select ARP poisoning to start the ARP poisoning attack

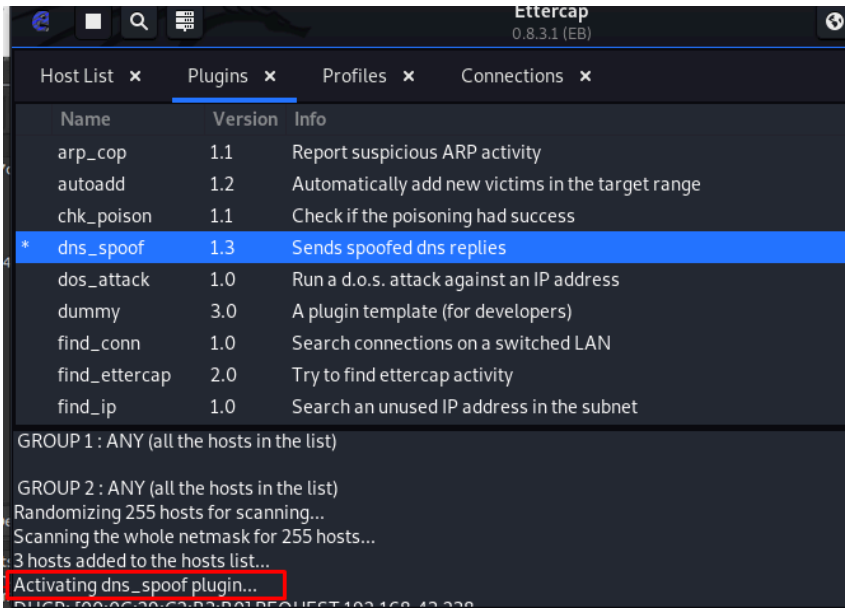


DNS Spoofing by GOVERDHAN



After starting the ARP poisoning select menu -> plugins -> manage plugins and then double click on dns_spoof to start the dns_spoof attack



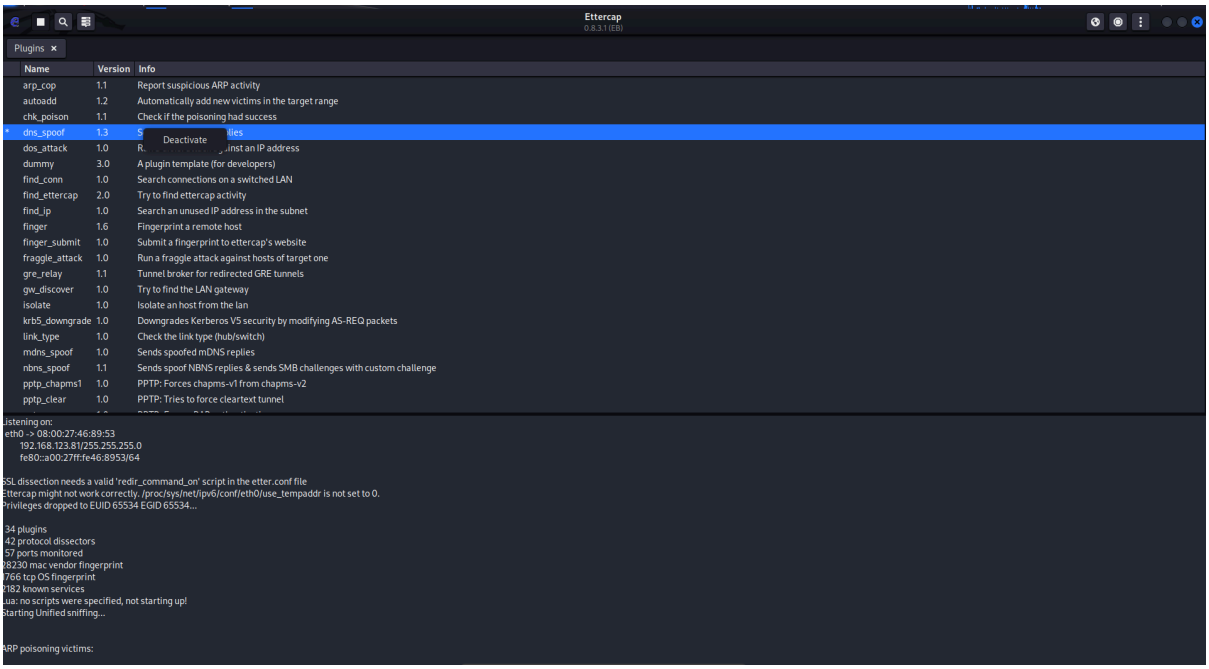


for more follow

linkedin.com/in/goverdhankumar

github.com/wh04m1i

DNS Spoofing by GOVERDHAN



Ok now it says activating dns_spoof plugin. view the connections to see if our attack worked. Below in the screenshot you'll see a user trying to access google.com being redirected to our server 192.168.123.81