Spoofing attack is unlike sniffing attack, there is a little difference between spoofing and sniffing. Sniffing is an act to capture or view the incoming and outgoing packets from the network while spoofing is an act to forging one's source address. In spoofing attack an attacker make himself a source or desire address. This is basically done by using some tricks.

Spoofing is so general word and it contains attack like DNS spoofing, IP spoofing and others.

**What Is DNS Spoofing?**

DNS spoofing is an attack that can categorize under Man-In-The-Middle-Attack, beside DNS Spoofing MIMA contain:
- ARP poisoning
- Sessions hijacking
- SSL hijacking
- DNS Spoofing

Each attack has its own importance but to be sure it is very difficult to discuss all attacks in single article, I will post some more articles related to MIMA.

DNS spoofing is an attack in which an attacker force victim to enter his credential into a fake website, the term fake does not mean that the website is a phishing page while. To understand DNS spoofing refer to this pictures.

In the normal communication a user send request to the real DNS server while if an attacker spoof the DNS server than this attack is called Man-In-The-Middle-Attack.
Now the question is how to perform DNS spoofing attack, the term spoofing is very similar with sniffing and the sniffing tools can be used to perform spoofing attack. For this article I will use ettercap.

**What Is Ettercap?**

According to the official website, "Ettercap is a suite for man in the middle attacks on LAN. It features sniffing of live connections, content filtering on the fly and many other interesting tricks". It supports cross operating systems like Windows, Linux, BSD, and MAC.

**DNS Spoofing Tutorial With Ettercap-Backtrack5**

If you want to learn more background theory than you can ask questions by using a comment box, now this section will teach you how to perform Spoofing (Man-In-The-Middle-Attack) attack.

**Requirement:**
- An Operating system (Linux, Windows etc)
- Ettercap
- SET

I am using backtrack 5 for this tutorial you can use some other OS, social engineering toolkit is not a necessary part but as discussed before about SET tutorial for hacking windows by using fake IP so you can use Spoof your IP into a website. So this is little advance tutorial.

It is recommended to use DNS spoofing attack with Social engineering toolkit attack to...
make the job done effectively.

Note: If you want to learn more about Linux and Windows based Penetration testing, you might want to subscribe our RSS feed and Email Subscription or become our Facebook fan! You will get all the latest updates at both the places.

Other Readings
- DNS, ISA and 2003 server (edugeek.net)
- MIT researchers craft defense against wireless man-in-middle attacks (infoworld.com)
- Responsibilities of the DNS: "Oh YES you will!", "Oh NO you will not!" (via CommunityDNS Blog) (chrisbuijs.com)

Related post

BackTrack
- Fern wifi Cracker- A Wireless Penetration Testing Tool
- DarkMYSQL- MYSQL Injection Tool Tutorial
- Tabnapping Tutorial– Social Engineering Toolkit Backtrack 5
- Autopwn Metasploit Backtrack 5– Postgresql Solved

Backtrack5
- DarkMYSQL– MYSQL Injection Tool Tutorial
- Tabnapping Tutorial– Social Engineering Toolkit Backtrack 5
- Autopwn Metasploit Backtrack 5– Postgresql Solved
- Complemento Backtrack 5 Toolkit

Like

Add New Comment

Like

Showing 4 comments

nanak12

thanks for the fast reply.. another question please.. is it possible with backtrack5 to create a spyware ( or whatever its called ) in a webpage and when a victim visits it, u own his computer & passwords .. is there a tutorial here for that ?? and what is it called ?? ... thanks very much

1 week ago

Ethical Hacking, Ethical Hacking is a blog where you can learn IT security with tips ...

You can do a lot of things on backtrack but remember backtrack is not only a single player, for webpage if you find any XSS bug on a web page than XSS shell for this purpose. We have not shared any tutorial on it but surely you will get it on Internet.

6 days ago in reply to nanak12

nanak12

i have my friend's IP but he is not on my lan.. can i still hack on his computer with backtrack5 ??

Yes you can hack but it requires some advance knowledge, do not worry we will soon publish a
detail tutorial for Metasploit WAN (remote) hacking.