



Network Security Laboratory Session 5

LAYER 3 ATTACKS

IP Spoofing

- ▶ Similar to ARP spoofing attack but it relies on the IP address of a victim host
- ▶ There are many different techniques to perform this attack but the most common is to use an ARP poisoner
- ▶ In this case the ARP poisoner will send ARP reply associating its MAC address to the victim IP Address
- ▶ When the router will forward packets the attacker will receive all the data

DNS Spoofing

- ▶ DNS cache poisoning (or DNS Spoofing), is a form of computer security hacking in which corrupt Domain Name System data is introduced into the DNS resolver's cache
- ▶ It causes the name server to return an incorrect result record (for example, an wrong IP address)
- ▶ All the traffic is diverted to the attacker's computer (or to any other computer)

Man In The Middle (MITM)

- ▶ All the attacks we built so far are part of MITM
- ▶ A MITM is a type of attack in which an Host is able to capture, read and forward packets of other hosts
- ▶ We will try to create a full-duplex MITM, based on ARP Spoofing, using ettercap

Ettercap

- ▶ Ettercap is a well-known tool for MITM attacks
- ▶ We will focus on ARP and DNS spoofing attacks
- ▶ Install Ettercap using the following command
 - ▶ `sudo apt install ettercap-text-only`