## **---------------------------------------------------------------------------------Sniffing----------------------------------------------------------------------------**

## 

## **# Basic**

## **With sniffing, you can monitor all sorts of traffic either protected or unprotected with connected network.**

## **The attacker can reveal information from it such as usernames and passwords.**

## **Anyone within the same LAN can sniff the packets.**

## 

## **# Working of Sniffers**

## **In the process of sniffing, the attacker gets connected to the target network to start sniffing.**

## **Capture the packet in network**

## **The attacker decrypt the packets to extract information.**

## 

## **# Switch vs Hub**

## **- \*\*Switch\*\* switch is a intelligent device beacause it is use mac and ip in packet destination.(send data packet with specific ip )**

## **- \*\*Hub\*\* transmits all packets to all ports.(send data packet with any ip in network)**

## 

## **--------------------------------------------------------------------------------------------------------------**

## **# Spoofing Attacks**

## 

## **# MAC Attacks**

## **\*\*Media Access Control\*\* (MAC) is the physical address of a device. MAC address is a 48-bit unique identification number that is assigned**

## **to a network device for communication at data-link layer (layer 2).**

## 

## **# MAC Flooding**

## **Tool - \*\*macof\*\***

## **python3 macof.py -i <network interface > -s <src ip> -d <dst ip>**

## **python3 macof.py -i eth0 -s 192.168.0.111 -d 192.168.174.130**

## 

## 

## **#Linux#**

## **MAC Changer \*\*\*github link = https://github.com/sbdchd/macchanger\*\*\* :-**

## 

## **\*Automatic Method\***

## **- ifconfig and check your mac address**

## **- random mac = macchanger -r <interface>**

## **macchanger -r eth0**

## 

## **\*Manual Method\***

## **- ifconfig and check your mac address**

## **- command to change mac adress = macchanger -m <mac address> <interface>**

## **macchanger -m 00-11-22-33-44-55 eth0**

## 

## **\*Other\***

## 

## **-ifconfig (check mac)**

## **-ifconfig eth0 down**

## **-ifconfig eth0 hw ether <mac >**

## **-ifconfig eth0 up**

## **-now check your mac it is changed**

## 

## **#Windows#**

## 

## **Technitium MAC address Changer (Windows) :-**

## 

## **\*Automatic Mac\***

## 

## **- Start Application**

## **- click yes when ask for .tpf (only first time)**

## **- click on "Random MAC Address"**

## **- Now you can see mac is changed**

## 

## **\*Manual Method\***

## 

## **- Start Application**

## **- Select Presets**

## **- Then click New**

## **- Then give Preset Name**

## **- Then click on MAC Address and Go to Use Custom**

## **- And then type Your Target Mac Address**

## **- Then Save**

## **- Then click your Presets Name which you give**

## **- Then click on Apply**

## **- Now your can see Mac is Changed**

## 

## 

## **--------------------------------------------------------------------------------------------------------------**

## **# DHCP Attacks**

## **# Dynamic Host Configuration Protocol (DHCP) - DHCP is the process of allocating the IP address dynamically so these addresses are assigned**

## **automatically to connected device**

## 

## 

## **- \*\*IPv4 Ports\*\*:**

## **- UDP port 67 for Server**

## **- UDP port 68 for Client**

## **-----------------------------------------------**

## **- \*\*IPv6 Ports\*\*:**

## **- UDP port 546 for Client**

## **- UDP port 547 for Server**

## 

## **--------------------------------------------------------------------------------------------------------------**

## **# ARP Poisoning**

## **# Address Resolution Protocol (ARP)**

## **The Address Resolution Protocol (ARP) is a communication protocol**

## **# ARP Spoofing Attack**

## **Attacker send forged(fake) ARP packets over Local Area Network (LAN). In this case, switch will update the attacker's MAC address with the IP address**

## **of a legitimate user or server, then start forwarding the packets to the attacker. Attacker can steal information by extracting it from packets.(legitimate**

## **user ki ip ke sath apni(attacker) mac address ko connect ke lena taki wo packet hamer pass aae )**

## 

## **ARP Poisoning used for:**

## **- Session hijacking**

## **- Denial-of-Service attacks**

## **- Man-in-the-Middle attacks**

## **- Packet sniffing**

## **- Data interceptions**

## **- Stealing passwords**

## **--------------------------------------------------------**

## **# Spoofing Attacks**

## **# MAC Spoofing/Duplicating**

## **Manipulating the MAC address to impersonate the legitimate user or launch attack such as DoS.**

## **Attacker sniffs the MAC address of users which are active on switch ports and duplicate the MAC address.**

## **This can intercept the traffic and traffic destined to the legitimate user may direct to the attacker.**

## 

## 

## **------------------------------------------------------------------------------------------------------------**

## **# Wireshark**

## **Filters in Wireshark:**

## **- `==` Equal**

## **- `eq` Equal**

## **- `!=` Not equal**

## **- `ne` Not equal**

## **- ip.src source addresses (Filter ip )**

## **- ip.dst destin addresses**

## **- ip.addr Match at both the places (source and destin)**

## **--------------------------------------------------------------------------------------------------------------**

## **# Sniffing Countermeasures**

## **- Use Secure Protocol instead of base Protocols (HTTPS over HTTP, SFTP over FTP, etc)**

## **- Switch instead of Hub (Hub broadcast packet by default, but Switch does not)**

## **- Strong encryption protocol (Strong Encrypted data is secure to transmit over any type of network)**