**Module 8**

**Sniffing and Network Hacking**

Packet sniffing is process of capturing the data , passing through the client and server.

First Understand How to see all network device around us

Command for it:- netdiscover

**MAC Flooding** :- Mac flooding is the process through which we make the CAM address full . So that switch will behave like a hub.

In simple word we can say that if the CAM table which known as Content Address Mamory become full , than switch start broadcast the network.

How CAM table work ?



Everything will be clear after seeing above pic .

After that all packet are visible to every network device.

So attackers can sniff the data.



Command :- macof -i [interface] -d [target IP] -n [no for times]

-n is optional want to use or not

We can analyze it with wireshark how packets are sent.

**ARP (Adress Resolution Protocol)**

**What is ARP ?**

It is simple protocol used to link MAC address to IP address.

But lets understand how arp packet is sent , arp also is a layer of internet or we can say osi or tcp layer.



|  |  |  |  |
| --- | --- | --- | --- |
| ip of  sender | Mac of sender | Ip of reciver | Mac of receiver in the form of 12f:- ff:ff:ff:ff:ff:ff |

Here we can see that attacker broadcast the IP to the network in the form of ip|mac|ip|mac|

This is the form of broadcast , mac is 48 bit encrypted data.

But response will be a unicast ,because only one device that is victim will respond .



All Ip will ignore this broadcast except the one who has same IP , in the term of response we can see that machine reveals its MAC address.

Know lets see our IP gateway

Command :- arp -a

**What is Arp Poisoning ?**

ARP poisoning is the process of intercepting the data from the victim by becoming man in the middle .

Basically an attacker send two ARP request , one to the gateway and another to the victim. He send request to gateway that he is a victim and similarly he send request to the victim that he is a gateway . By the process of this Acces point update his table .

**Why ARP spoofing is possible ?**

ARP spoofing is possible because –

* Client accept request even if they don’t send a request.
* Client trust response without any verifiction.

Lets do ARP spoof with arpspoof tool,

Before doing this lets run arp command our target system

Command:- arp -a

Know lets do arpspoof

Command :-arpspoof -i [interface] -t [client IP] [gateway]

arpspoof -i [interface] -t [gateway] [client IP]

One time he will fooled the victim and another time he will fooled the gateway(accespoiinta).

After running the arpspoof command. Go the our Target system and run arp command

We can see here that our router(gateway) mac address changed , set same as kali have mac address.

But here also we have one problem , target machine is not able to use internet because kali machine is not behaving like a router.

Whenever kali get request it stop them here , it is security feature of kali linux . We can fix it by port forwarding .

Command :- echo 1 > /proc/sys/net/ipv4/ip\_forward

We can analyze all packet from wireshark tool

Know we will do arp spoofing with tool called Ettercap which is previously known as Bettercap

Command:- bettercap -iface eth0

Type help after open bettercap , we will get all modules.

If we want to know about any module just type help & module name

Command :- help [module name ]

For on any module name and just type on like,

Command :- [module name] on

Know we will do ARP spoof with bettercap

Lets see help of arp.spoof

We can see all parameter of the arp.spoof



Arp.spoof.fullduplex parameter is usefull parameter , we need to set it

Command :- set arp.spoof.fullduplex true

This command spoof both side router and victim , If we put it false it only spoof victim or target

Another command is also need to set

Command :- set arp.spoof.targets [target IP]

Know switch on the arp.spoof

Command :- arp.spoof on

If we do arp -a in target system we can see that mac address of router is same as kali have.

I become man in the middle , know I need to analyze the data we can do this by wireshark but in bettercap have a nice module net.sniff, turn it on .

Command :- net.sniff on

Know every http request of victim are will go through our computer screen.

Only HTTP request

For sniffing the HTTPS data we need to set some parameter of net.sniff before turning it on

Command :- set net.sniff.local true

Know turn on the net.sniff

**MITIGATION**

For prevention always take a good look of mac address of gateway that should not be dublicate,

Always use https instead of http .

**Ettercap**

Command:- Ettercap -T -S -i (interface) -M arp:remote /gateway-ip// /target-ip//