**0**

**DoS (Denial of Service) Attack :-**

**-------------- How hackers crash internet using ARP Spoofing ---------------**

**--- Bhavesh M. Dhake**

**Index**

**Aim………………………………………………………………………………………………1**

**Objective……………………………………………………………………………………..2**

**Concepts ……………………………………………………………………………………..3**

DoS…………………………………………………………………………………………..3.1

ARP…………………………………………………………………………………………..3.2

ARP Spoofing…………………………………………………………………………….3.3

IPv4…………………………………………………………………………………………..3.4

MAC …………………………………………………………………………………………3.5

Subnet………………………………………………………………………………………3.6

Interface……………………………………………………………………………………3.7

**Precautions…………………………………………………………………………………..4**

Anonymity…………………………………………………………………………………4.1

MAC…………………………………………………………………………………………..4.2

IP………………………………………………………………………………………………..4.3

**Procedure……………………………………………………………………………………..5**

Lab Setup ………………………………………………………………………………….5.1

Radar…………………………………………………………………………………………5.2

Gateway…………………………………………………………………………………….5.3

One-Way……………………………………………………………………………………5.4

Attack………………………………………………………………………………………..5.5

**1**

**Aim :** To perform a Denial of Service (DoS) attack to crash the network of our target’s device using the technique ARP Spoofing in a controlled environment.

**2**

**Objective :** To demonstrate and understand the process of conducting a Denial of Service attack using ARP spoofing to crash network of victim device in a controlled and authorized environment .

1. Simulate network disruption : To disrupt the communication between target device and network by poisoning the arp cache of target ang wlan interface’s gateway .

2. Technical Workflow :

* Scanning for all reachable devices on network
* Getting ip and mac addresses of reachable devices
* Changing ip address to maintain anonymity
* Changing mac address to maintain anonymity
* Disabling ip forwarding to block network connection
* Spoofing arp for target of gateway with attacker’s ip

3. Impact of attack : Target device is isolated from the local wifi/Ethernet interface’s subnet , preventing it from accessing domains .

**3**

**Concepts :-**

**3.1**

**Denial of Service(DoS) Attack :** A Denial of Service (DoS) attack is a malicious attempt to disrupt the normal functioning of a network , service or device making it inaccessible to users . Most common methods consist of overwhelming the target with excessive traffic ( sending excessive amount of data packets over specific protocol and ports) or to exploit vulnerabilities to exhaust system resources such as bandwidth , memory or processing power . However , here we have chosen a different approach which is ARP Spoofing , as

best part of being a hacker is to think out of the box strategies to secure/exploit the system .

**3.2**

**ARP(Address Resolution Protocol) :** Is a fundamental communication protocol used in computer networking . It operates at the Data Link Layer (Layer 2) of the OSI model . It’s function is to map the IP(Internet Protocol) address of a device to its MAC(Media Access Control) address . It is vital for communication between devices in a Local Area Network(LAN) .

Working :

1. When a device 1 needs to communicate with another device 2 on the same local wifi/Ethernet network , it first checks the ARP tables if it has the MAC address for the IP address of other device 2 .
2. If the MAC address is not found , it send an ARP request on the broadcast IP ( last IP of the subnet used to send data packet to all devices on network) asking who has the IP address of the other device 2 .
3. The other device 2 with same IP responds with it’s MAC address and device 1 stores it in it’s ARP table where it associated it with device 2’s IP .

**3.3**

**ARP Poisoning** : Also known as ARP Spoofing is a network attack technique In which an attacker sends malicious ARP messages on a network . Purpose is to associate the MAC address of attacker’s device with IP address of another device (here router) for the target device which allows attacker to intercept , modify and block communication between devices on same network .

ARP lacks authentication mechanisms and accepts ARP requests without verifying sender’s origin which enables hacker to inject malicious ARP packets .

Working :

1. The attacker scans network to discover active devices , their IP and MAC addresses .
2. The attacker sends fake ARP packets to target device and/or router gateway , claiming that their MAC address is associated with IP address of another active device ( here router) .
3. The target updates it’s ARP tables by matching attacker’s MAC address with router’s (another device’s) IP address .
4. In our case , now the target device believes , attacker’s device is the router and therefore the network requests from target device’s browser are sent to attacker’s device instead of router .
5. The target will be able to surf the internet and access domain server only if attacker forwards the network requests from target’s device to router and therby blocking IP forwarding we can simply crash the network of target .

**3.4**

**IPv4 : IP(Internet Protocol) address :** An IPv4 address or IP address is a unique identifier given to a device by it’s Internet Service Provider (ISP) using which it is able to communicate with other devices and access public domains such as Google.com , it is of format “xxx.xxx.xxx.xxx”.

Demonstration : When connected to a Wi-Fi network provided by an Internet Service Provider (ISP), your device uses a private IP address to interact with devices within the same local network but uses a public ip address to connect to global domains like Google.com .  
  
 1. IP Address and Subnetting: Suppose ur device's private IP is 192.168.4.34

and ur network is represented by 192.168.4.0/24 . The /24 represent subnet mask of 255.255.255.0 , allowing for up to 256 IP addresses within the local network from 192.168.4.1 to 192.168.4.255 where the first and

last are reserved by ISP .  
  
2. Network and Device Addresses:  
  
A) Local network : 192.168.4.0/24 represents the entire local network.  
  
B) Private ip : 192.168.4.34 is your device’s unique identifier.  
  
C) Range for Devices: IP addresses from 192.168.4.1 to 192.168.4.254 are allocated to devices.  
  
D) Broadcast Address: 192.168.4.255 is used to broadcast data to all devices in the network.  
  
E) Default Gateway: Typically, 192.168.4.1 serves as the gateway to other networks.  
  
3. Communication within the Network:  
  
Suppose there's another device in ur home LAN network with ip address : 192.168.4.45 .  
  
A. To send data to that other device , source ip will be 192.168.4.34 and destination ip will be 192.168.4.45 .  
  
B. To send data to all the reachable devices on the local network , the source ip will be 192.168.4.34 and the destination ip will be 192.168.4.255  
  
C. Although the wifi network will have the same 192.168.4.0/24 ip even in other LAN network's for example in ur neighbourhood ,   
u won't be able to connect to device of another LAN having same network ip , because here we apply the concept of subnet (sub network) where large networks are divided into smaller sub networks which helps in efficient use of ip addresses , improves network management and enhances security , and all subnets are isolated and invisible to each other   
  
4. Connecting to Global Domains:  
  
To access websites like www.example.com, your device sends a request to the default gateway : 192.168.4.1 . The gateway replaces the private IP address (192.168.4.34) with a public IP address (e.g., 203.0.113.4) for routing over the internet.

**3.5**

**MAC(Media Access Control) address :** In order for a system to be able to access internet it should consist of Network Interface Card(NIC) . Each NIC has a unique MAC address embedded into it during manufacturing . MAC address is the unique identifier that a device has assigned by NIC and is used for communication between devices on same local network . Format : xx:xx:xx:xx:xx:xx

**3.6**

**Subnet :** Short for subnetwork – subnet is basically a division of local network into different isolated sub networks on the basis of IP addresses . It forms smaller and more manageable sections of network which helps in improved network performance and all sub networks are isolated from each other .

Example : consider network 192.168.0.0/24

|  |  |  |  |
| --- | --- | --- | --- |
| Subnet | Range | Usable IP’s | Broadcast |
| Subnet 1 | 192.168.0.0 –  192.168.0.63 | 192.168.0.1 –  192.168.0.62 | 192.168.0.63 |
| Subnet 2 | 192.168.0.64-  192.168.0.127 | 192.168.0.65-  192.168.0.126 | 192.168.0.127 |
| Subnet 3 | 192.168.0.128-  192.168.0.191 | 192.168.0.129-  192.168.0.190 | 192.168.0.191 |
| Subnet 4 | 192.168.0.192-  192.168.0.255 | 192.168.0.193-  192.168.0.254 | 192.168.0.254 |

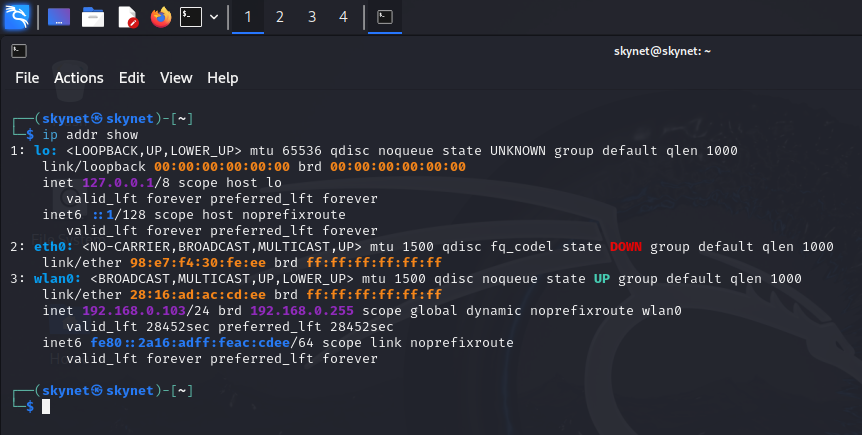
**3.7**

**Interface :** A Network Interface is a platform or medium through which a system or device is connected to a network .

There are 3 types of Interface :

1. Ethernet (eth(X)) : It represents a wired connection to the network . X is variable which varied according to number of Ethernet ports system has . An Ethernet cable is used .
2. Wireless Fidelity (Wi-Fi)(wlan(X)) : It represents the wireless network connection . A wireless adapter/router is used.
3. Loopback (lo) : It is a virtual interface for internal network communication within the device . It always uses the specific IP address : 127.0.0.1 and called local host. It is used to check functionality of service software running on device by reverting it back to device .

To check enter command “ip addr show “ in kali linux terminal :-



**4**

**Precautions :**

**4.1**

**Anonymity :** First step of performing a hacking attack is to ensure self anonymity to protect ourselves from being detected and facing legal consequences . Ensuring total anonymity is a vast concept but for this particular attack we need to stay anonymous over 2 parameters : IP and MAC address.

**4.2**

**MAC :** MAC address is unique identity of our device and can be used to identify and track our device on netwok .

Procedure to change MAC address temporarily :

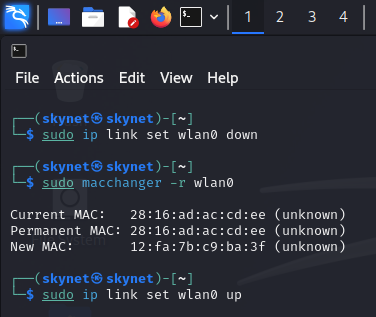
Step 1 : Open kali linux terminal

Step 2 : Enter command : “sudo ip link set wlan0 down” which will turn off our wifi service so that we can perform changed safely .

Step 3 : Enter command : “sudo macchanger –r wlan0” which will use tool named macchanger to allocate a random fake MAC address to our device .

Step 4 : Enter command : “sudo ip link set wlan0 up” which will switch on the wifi service again .

Step 5 : u can use command “ ip addr show “ to check if MAC address has been changed .



**4.3**

**IP :** After changing MAC address we can move forward to change our IP address for sake of same which is to maintain anonymity on network and prevent our system from being detected with original properties .

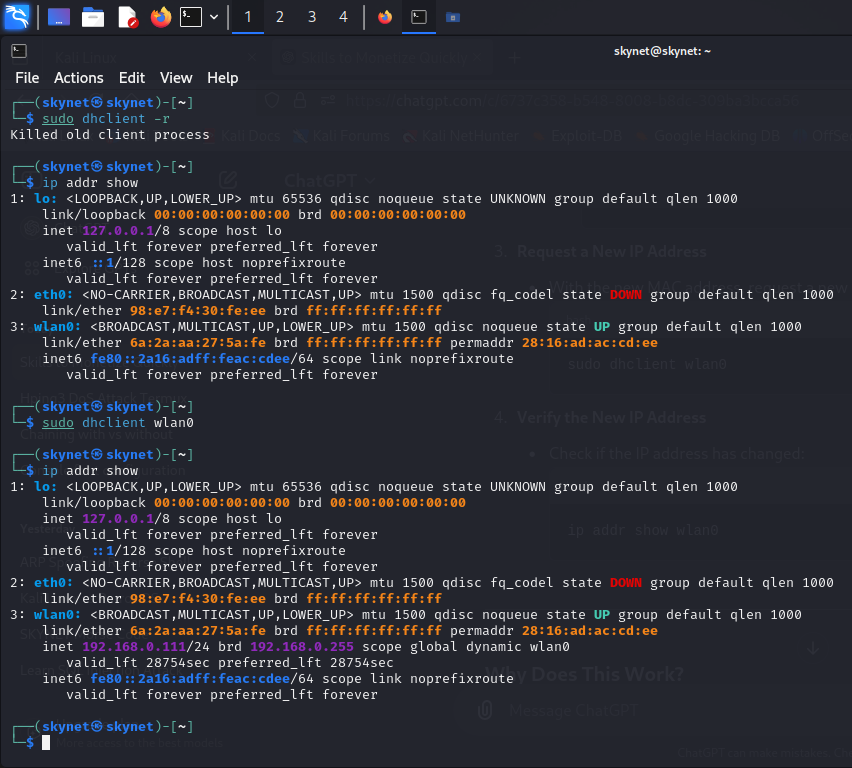
Procedure to change IP address :

Step 1 : Enter command “sudo dhclient –r” which will using dhclient tool erase/delete/release our current IP address of device

Step 2 : Enter commad “ip addr show” and it should not show any ip address under current interface .

Step 3 : Enter command “ sudo dhclient wlan0” which will assign a new IP address to our system .

Step 4 : Enter command “ip addr show” to check if IP address has been changed .



**5**

**Procedure :**

**5.1**

**Lab Setup :** My Lab :

* An hp, i5 processor, 8 GB RAM, 256 GB ROM laptop with Operating system Kali Linux which is the attacker device .
* An hp, i3 processor , 12 GB RAM , 512 GB ROM laptop with Operating system windows 11 which is the target device .
* Both devices are connected to same local private wifi service.

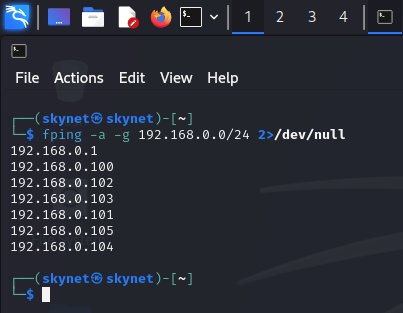
**5.2**

**Radar :** We will scan our wifi network to find the active devices or reachable hosts or potential targets .

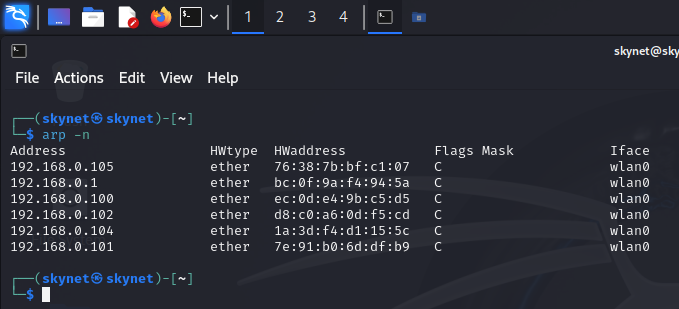
Procedure :

Step 1 : Open terminal

Step 2 : Enter command “fping –a –g 192.168.0.0/24 2>/dev/null” where u should enter ur respective network , this command will use fping tool to ping or send data packets to all IP’s on ur network and on basis of responses from those IP’s ,it will give list of active devices .



Step 3 : Enter command “arp –n” which will use arp to return MAC and IP addresses of active device from arp table .



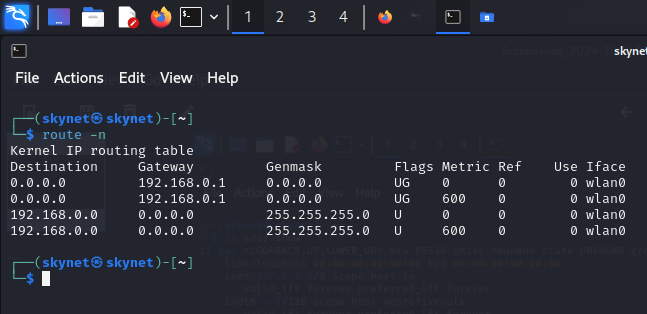
**5.3**

**Gateway :** Here , we will find out the gateway of our wifi network which means the pathway through which each network request from each device goes to before reaching any other device or domain server.

Procedure :

Step 1 : Open terminal

Step 2 : Enter command “route –n”



**5.4**

**One-Way :** As explained earlier the working of ARP Spoofing attack , when we do the ARP Spoofing , means when we tell the target device that the attacker’s device’s MAC is associated with IP of gateway , the network request data packets will first flow towards our target device instead of actual router and if we forward the data packets to the router then the target device will function normally except that we will be able to intercept the http traffic . But in order to crash the network of target device we don’t want to forward the data packets , so we will have to disable it .

Procedure :

Step 1 : Enter command

“echo 0 | sudo tee /proc/sys/net/ipv4/ip\_forward”

**5.5**

**Attack :** Finally now we will execute the ARP spoofing attack that will indirectly cause DoS attack . For this we will use tool arpspoof which take parameters interface of network , ip address of target device and ip address of gateway .

Procedure :

Step 1 : Enter command :

“sudo arpspoof –i wlan0 –t 192.168.0.102 –r 192.168.0.1 ”

