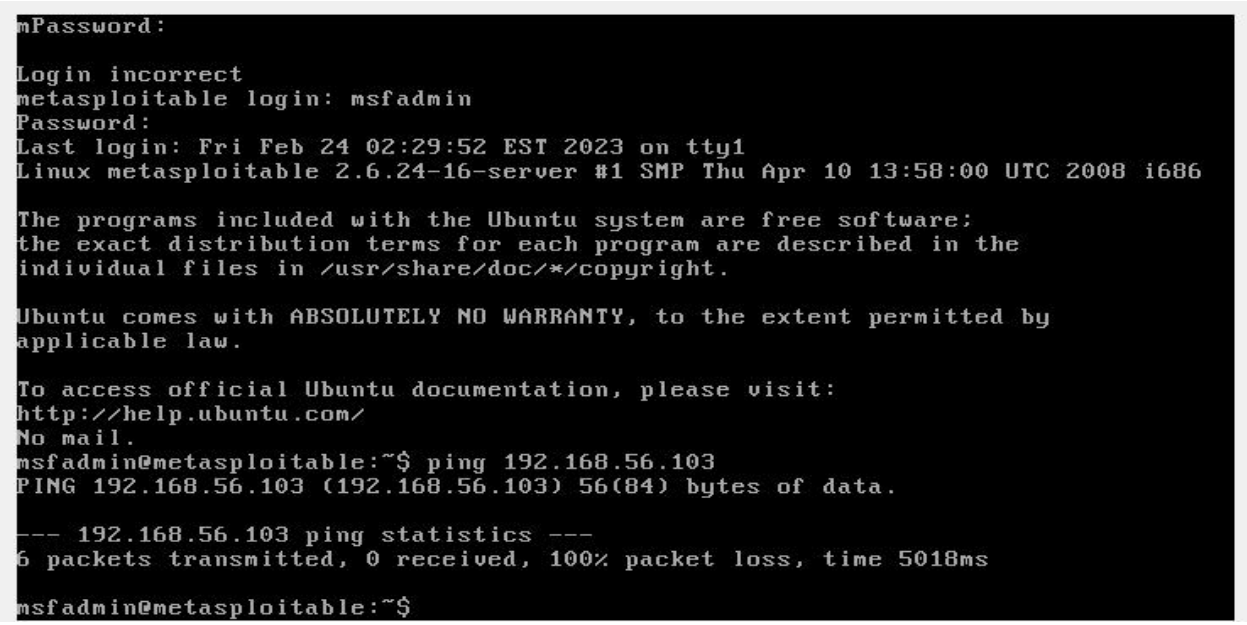
SNIFFING USING ETTERCAP IN KALI LINUX

Ettercap is an open-source tool that can be used to support man-in-the-middle attacks on networks. Ettercap can capture packets and then write them back onto the network. Ettercap enables the diversion and alteration of data virtually in real-time. Ettercap can also be used for the protocol analysis necessary to analyze network traffic.

Man-in-the-middle attacks place a threat actor in the middle of secure communications traffic. The primary purpose of a man-in-the-middle attack is to steal data. If authentication data, then the man-in-the-middle can access resources used by the target. Many times there is little to no interaction other than for the interception of data.

Sniffing with Ettercap:

1. Turn on Meta, Windows 7 and kali-Linux.Login to windows and metasploitable, Transfer packets from metasploitable machine to windows 7[command: ping windowsIP]



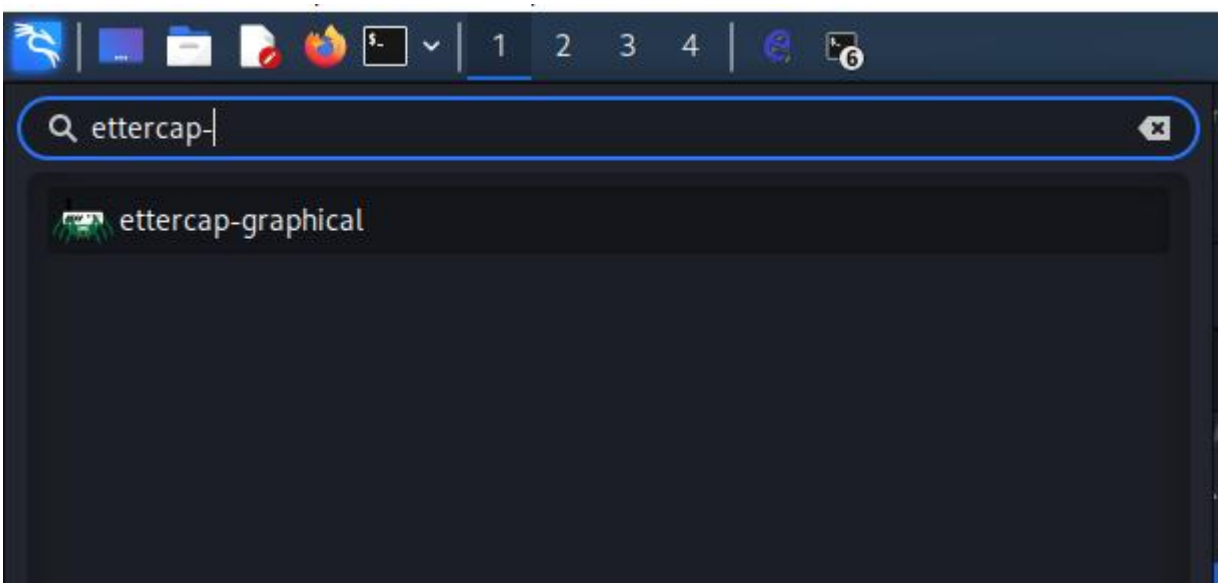
2. Access using root user [command: sudo su]

Scan the IP network for NetBIOS name information.

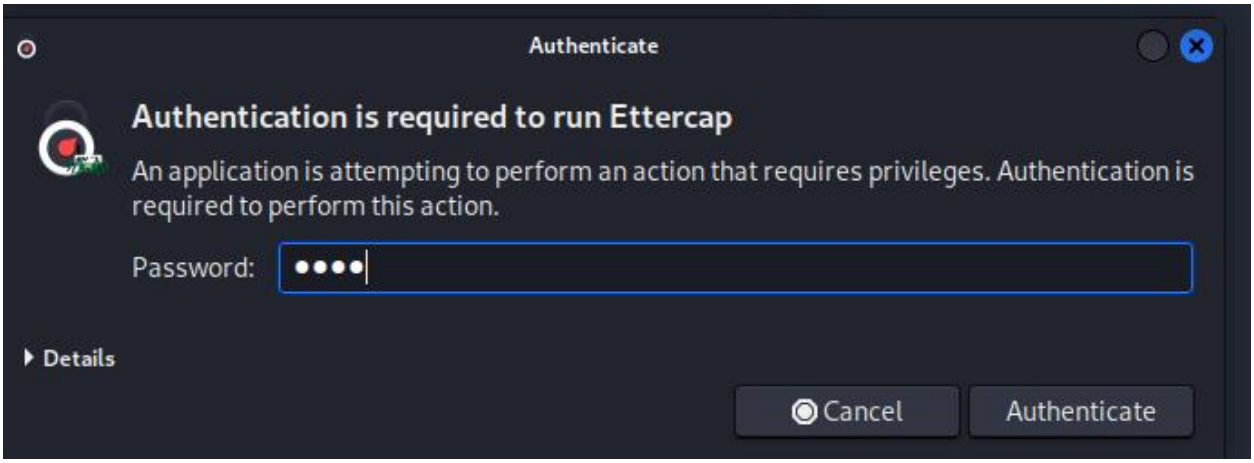
[nbtscan 192.168.56.102/24]

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nbtscan 192.168.56.101/24
Doing NBT name scan for addresses from 192.168.56.101/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
192.168.56.1     DESKTOP-SLE8M3J  <server>  <unknown>        0a:00:27:00:00:0
f
192.168.56.102   METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:0
0
192.168.56.255   Sendto failed: Permission denied

┌──(root㉿kali)-[/home/kali]
└─#
```

3. From Kali tools search for ettercap-graphical.



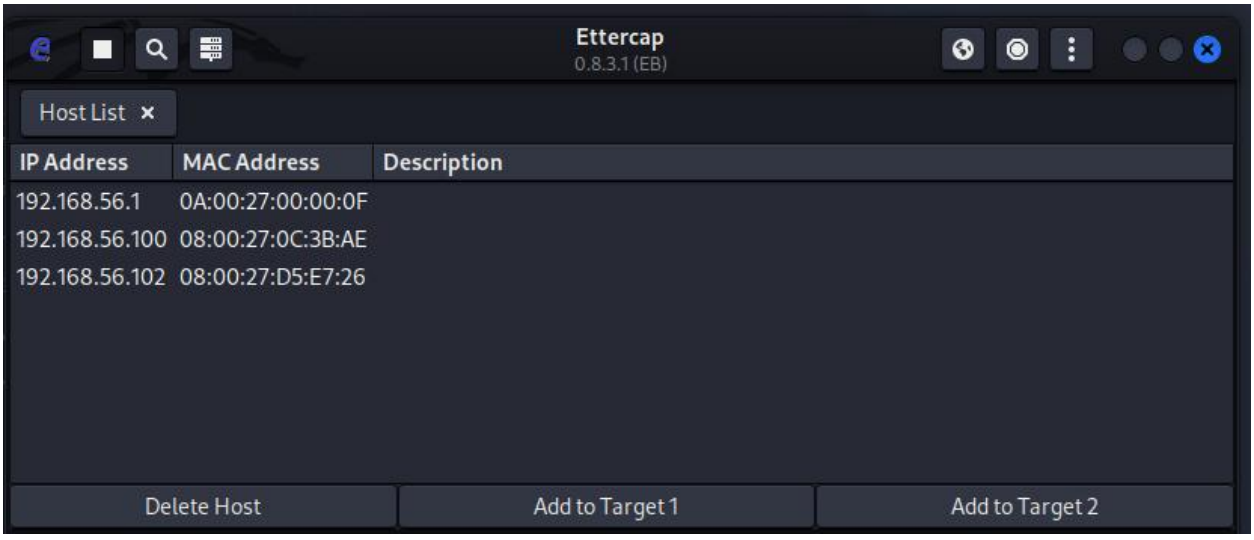
4. Enter the password as kali



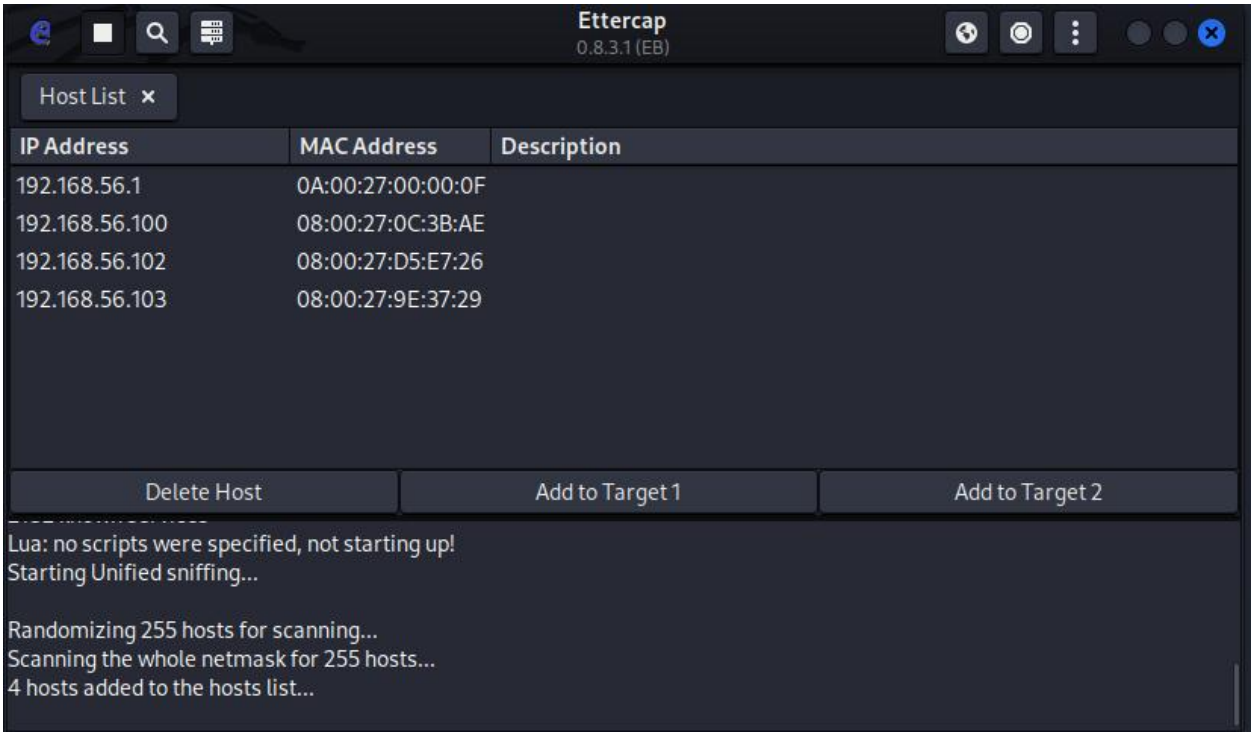
5. Select the checkbox in the below page.

6. Select three dots in the top right corner then select hosts-> scan for the hosts from the page displayed below.

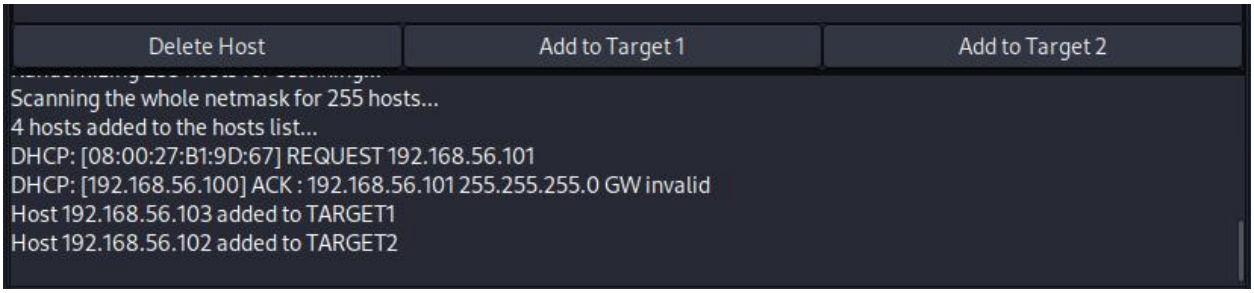
7.And then again select 3 dots ->hosts->hostlists and the below window is displayed.



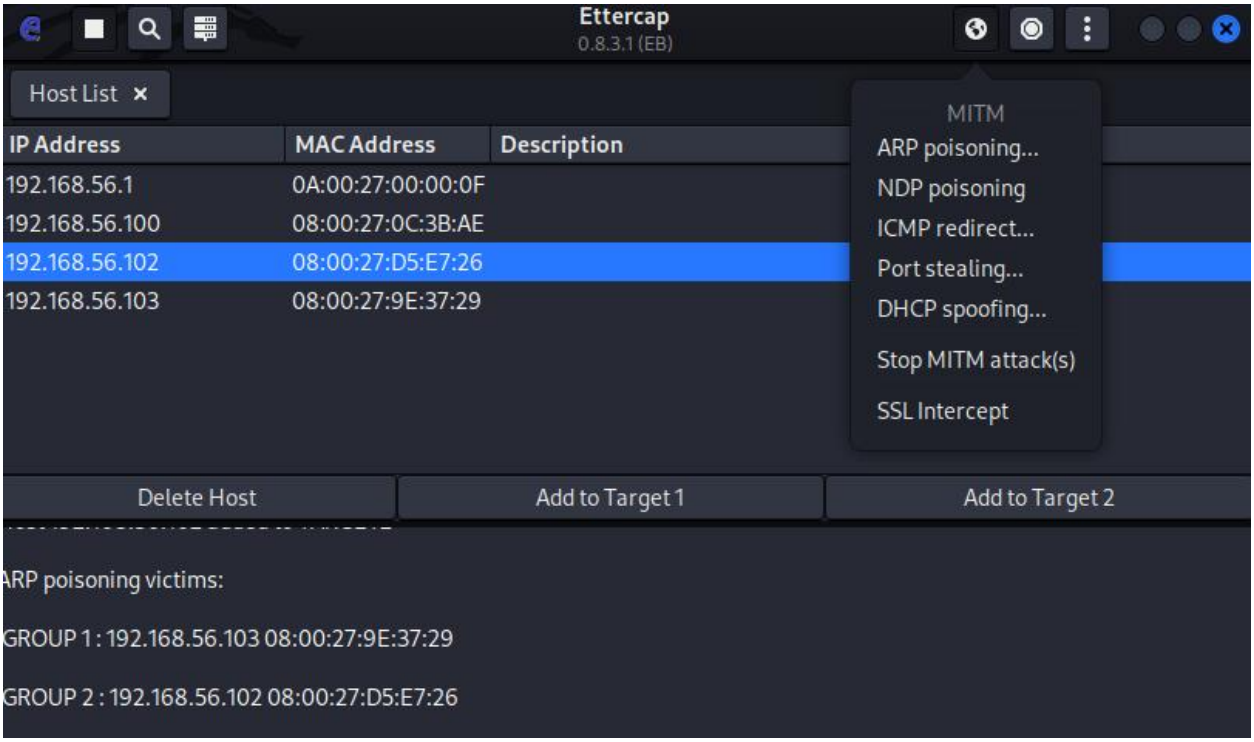
8. Select the IP network of windows7 as Add to target1 and select IP network of Metasploitable machine as Add to target2.



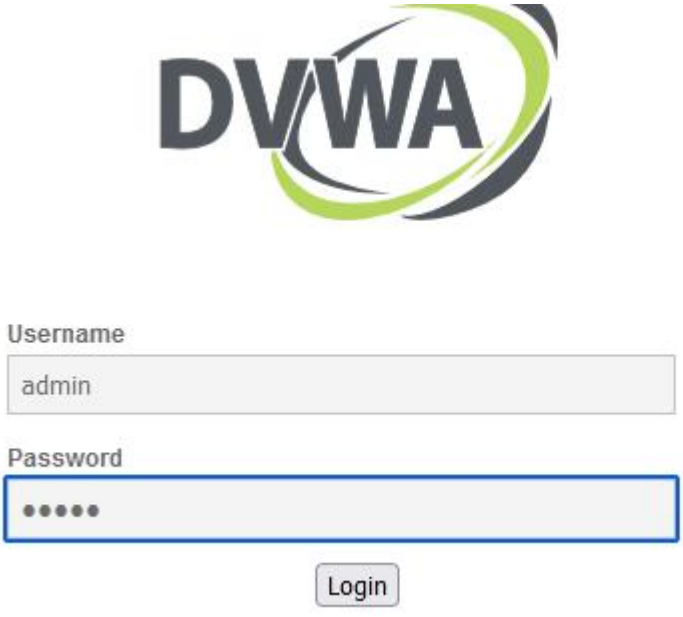
9. Below window displays that target1 and target2 has been set.



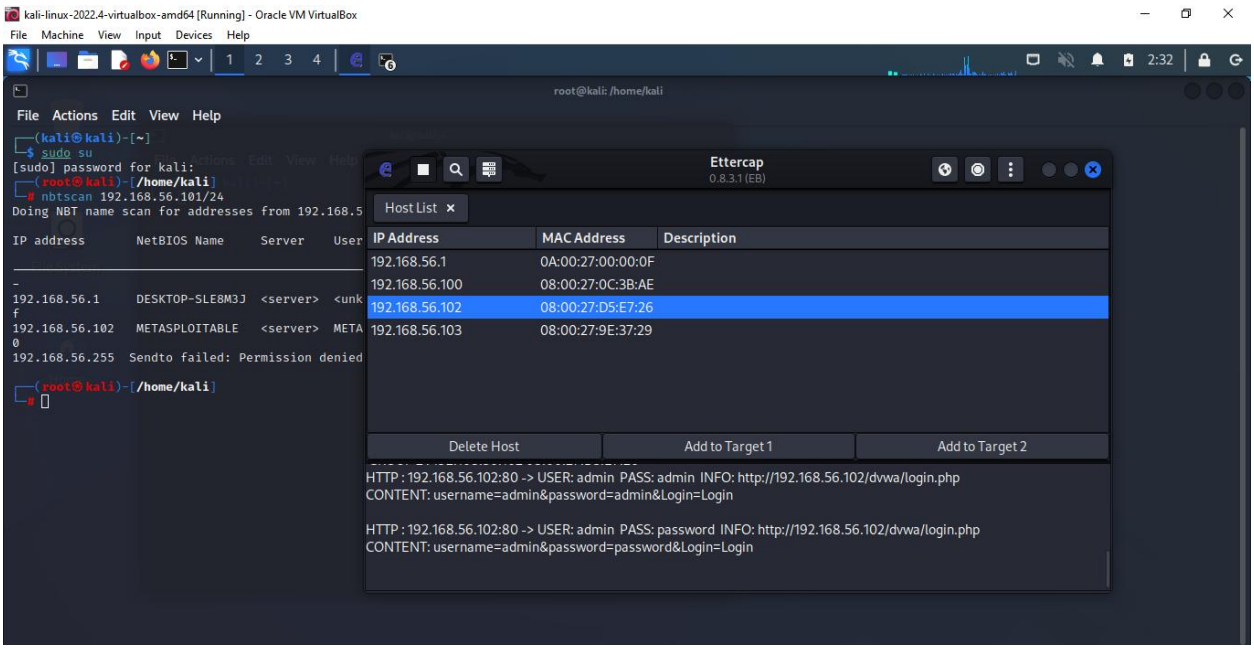
10. Select ARP poisoning from the drop down menu on clicking globe icon. In ARP poisoning attacker sends falsified ARP messages over a LAN to link an attacker's MAC address with the IP address of a legitimate computer or server on the network.



11. Open firefox in the windows 7 and browse the IP address of metasploitable machine and select DVWA option and enter the username and password to login.



12. The entered username and password in Windows 7 will be now visible at Kali linux. By this successful sniffing between win7 and Metasploitable machines done using ettercap tool.


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
(root㉿kali)-[/home/kali]
nbtscan 192.168.56.101/24
Doing NBT name scan for addresses from 192.168.5
IP address NetBIOS Name Server User
192.168.56.1 DESKTOP-SLE8M3J <server> <unk
192.168.56.102 METASPLOITABLE <server> META
192.168.56.255 Sendto failed: Permission denied
(root㉿kali)-[/home/kali]
Ettercap
0.8.3.1 (EB)
Host List
IP Address
MAC Address
Description
192.168.56.1 0A:00:27:00:00:0F
192.168.56.100 08:00:27:0C:3B:AE
192.168.56.102 08:00:27:D5:E7:26
192.168.56.103 08:00:27:9E:37:29
Delete Host
Add to Target 1
Add to Target 2
HTTP : 192.168.56.102:80 -> USER: admin PASS: admin INFO: http://192.168.56.102/dvwa/login.php
CONTENT: username=admin&password=admin&Login=Login
HTTP : 192.168.56.102:80 -> USER: admin PASS: password INFO: http://192.168.56.102/dvwa/login.php
CONTENT: username=admin&password=password&Login=Login