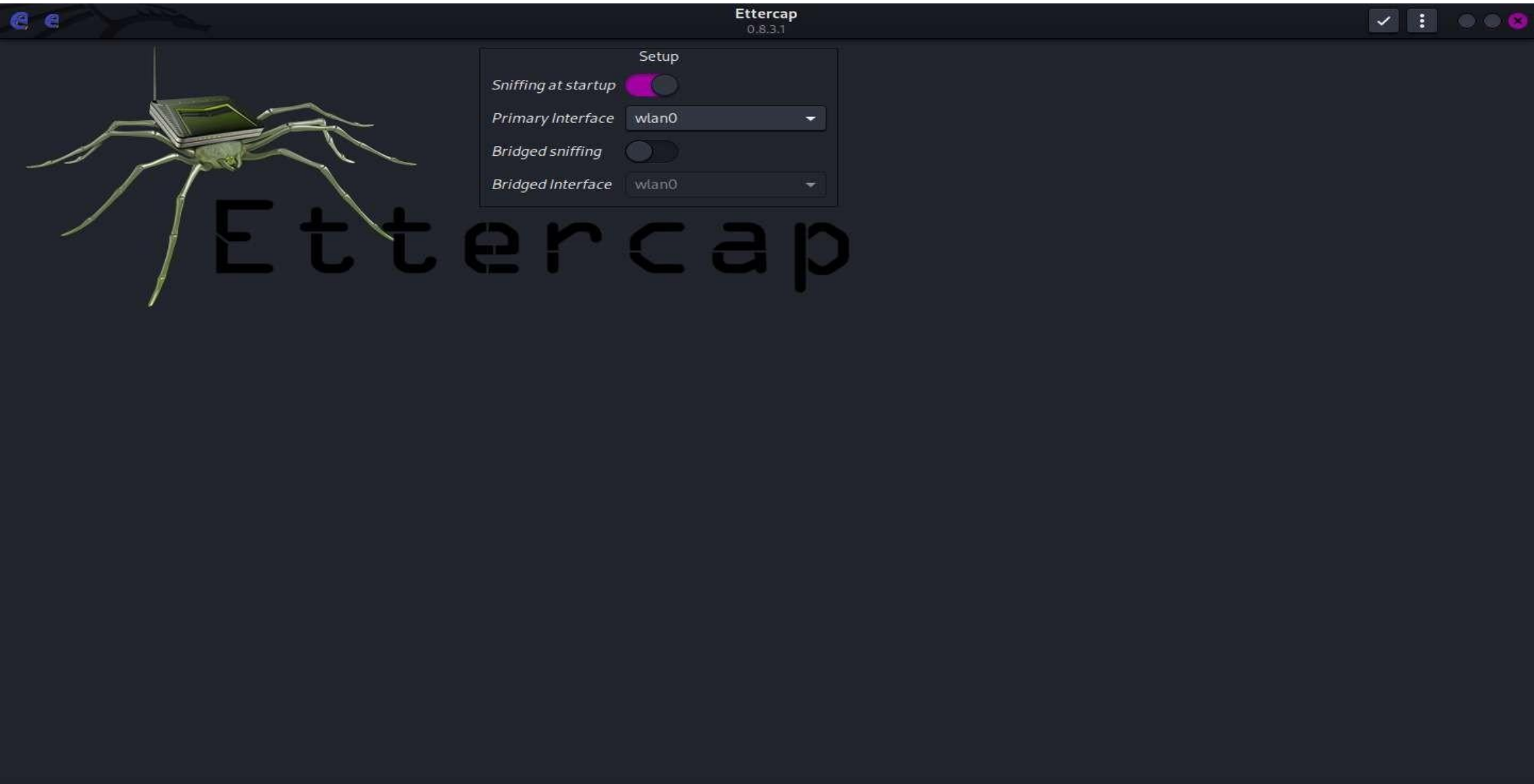


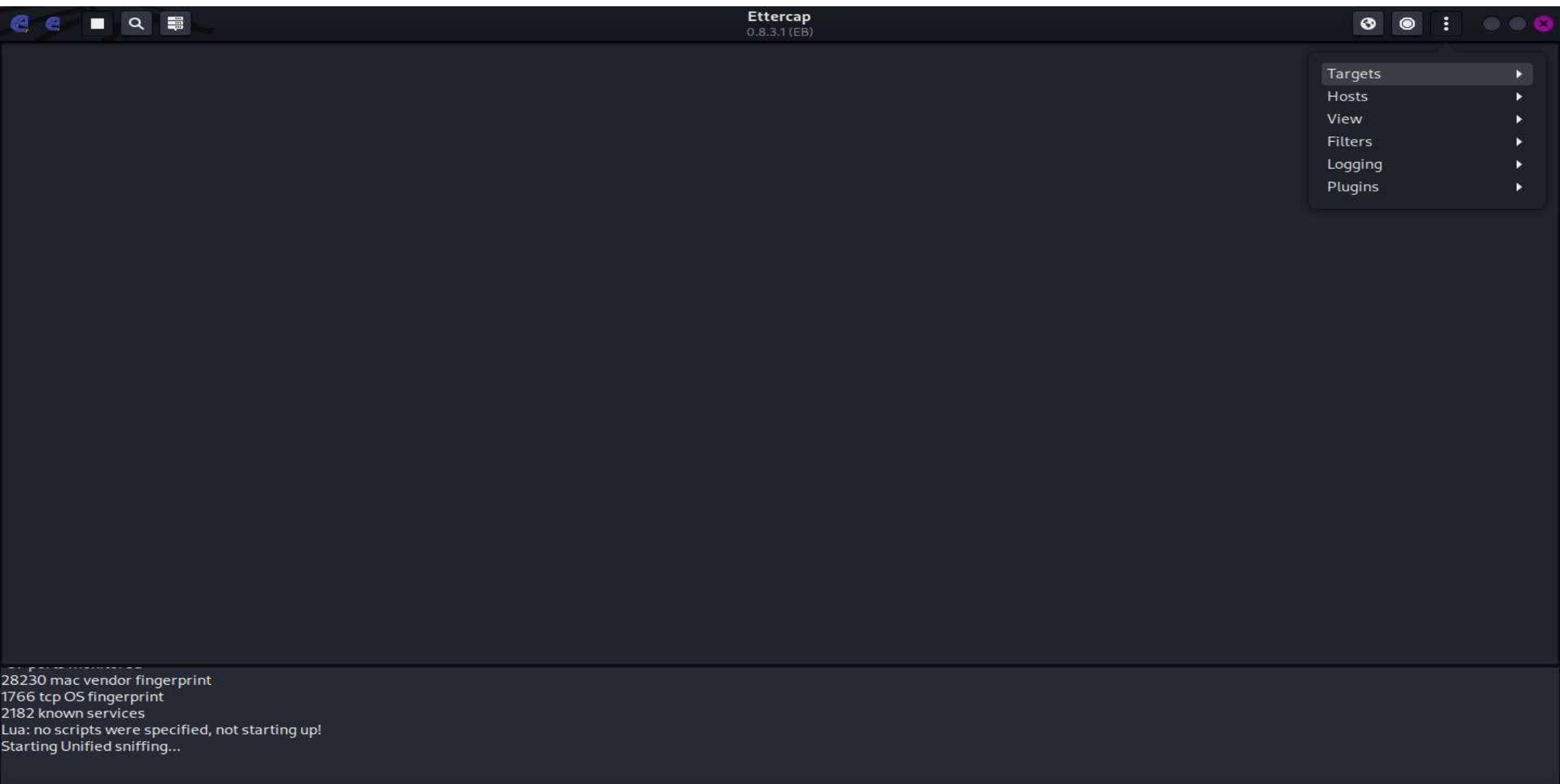
## Sniffing using Ettercap

Step 1: Open Ettercap

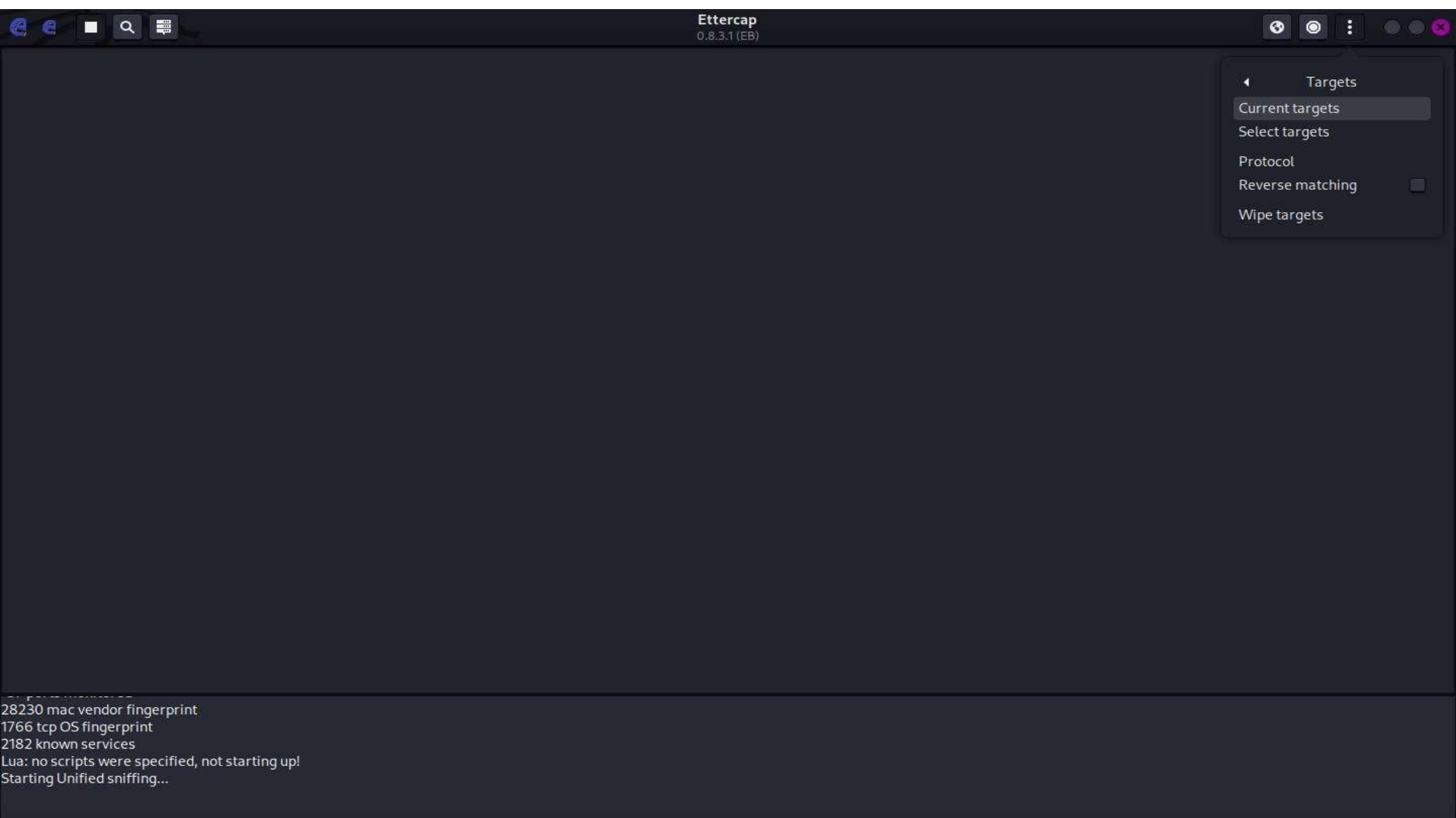
Step 2: Change eth0 to wlan0 and click on check mark



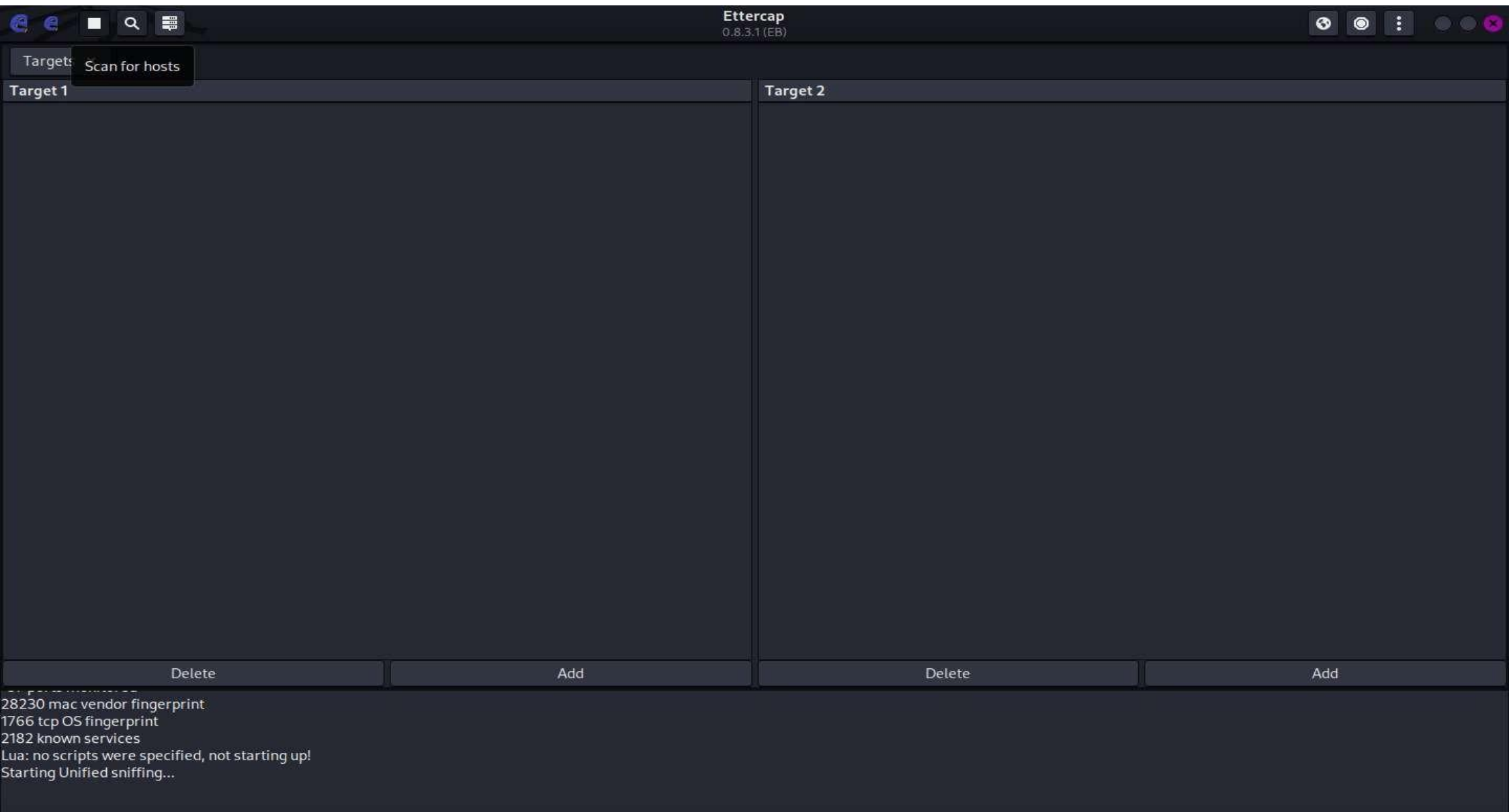
Step 3: Click on three dots → Targets



Step 4: Click on Current targets



Step 5: Click on Scan for host



Step 6: Click on host list

Step 7: Look for your wifi IP address → right click on it and add to target 1

Again look for client Ip address → add to target 2

Ettercap  
0.8.3.1 (EB)

Targets x

Host List x

IP Address	MAC Address	Description
10.0.0.1	08:00:27:00:00:00	
10.0.0.2	08:00:27:00:00:00	
10.0.0.3	08:00:27:00:00:00	
10.0.0.4	08:00:27:00:00:00	

Delete Host

Add to Target 1

Add to Target 2

Lua: no scripts were specified, not starting up!

Starting Unified sniffing...

Randomizing 255 hosts for scanning...

Scanning the whole netmask for 255 hosts...

3 hosts added to the hosts list...

Step 8: Click on Targets and select both IP addresses

Step 9: click on MITM (globe like symbol) → select ARP poisoning

The screenshot shows the Ettercap 0.8.3.1 (EB) application window. The 'Targets' tab is active, displaying two target lists. The first target, 'Target 1', has the IP address '192.168.1.1' selected. The second target, 'Target 2', has the IP address '192.168.1.5' selected. A context menu is open over the selected IP addresses, showing the 'MITM' section with the following options: 'ARP poisoning...', 'NDP poisoning', 'ICMP redirect...', 'Port stealing...', 'DHCP spoofing...', 'Stop MITM attack(s)', and 'SSL Intercept'. The 'ARP poisoning...' option is highlighted. At the bottom of the window, a status bar displays the following text: 'Randomizing 255 hosts for scanning...', 'Scanning the whole netmask for 255 hosts...', '3 hosts added to the hosts list...', 'Host 192.168.1.1 added to TARGET1', and 'Host 192.168.1.5 added to TARGET2'.

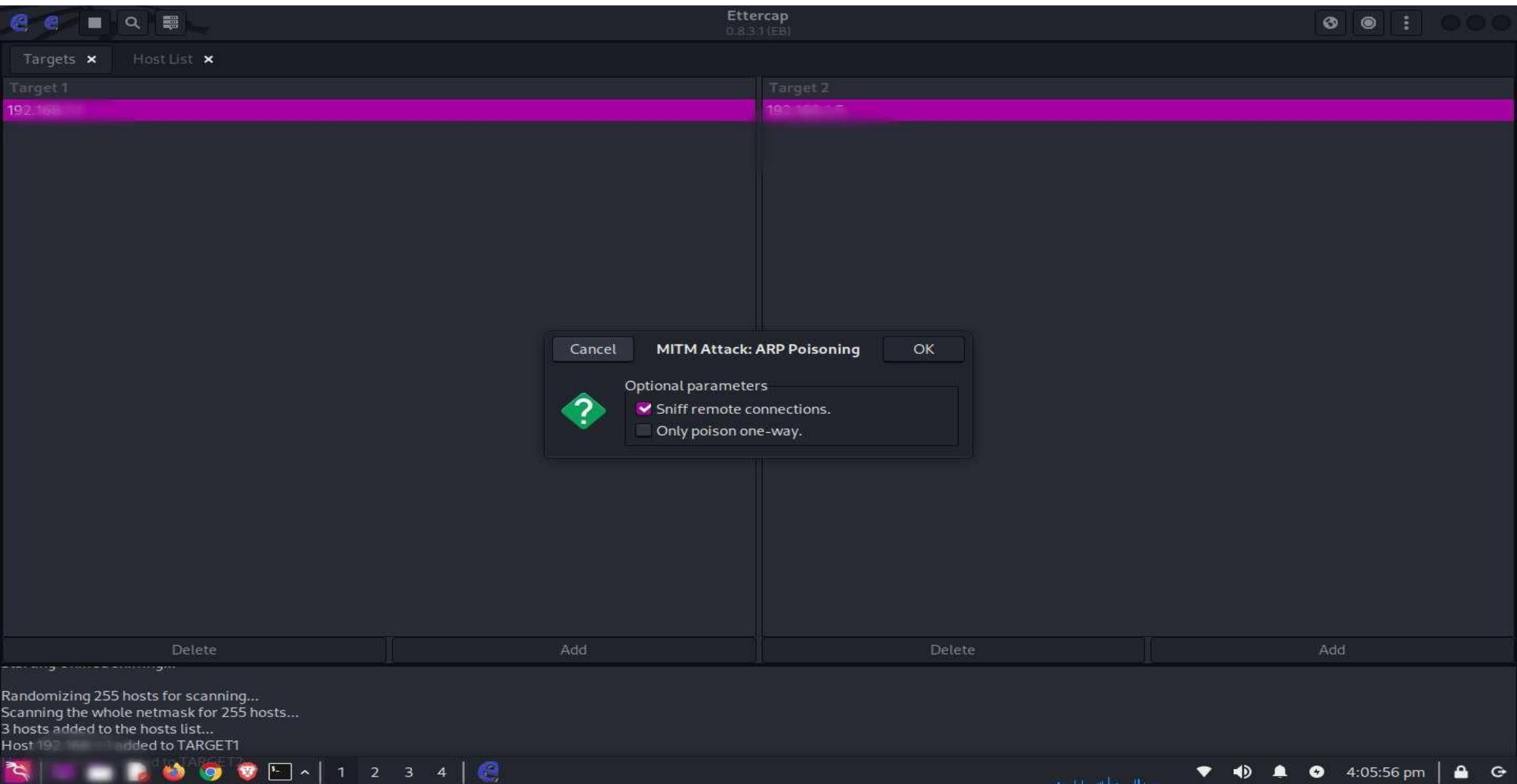
Target 1	Target 2
192.168.1.1	192.168.1.5

MITM

- ARP poisoning...
- NDP poisoning
- ICMP redirect...
- Port stealing...
- DHCP spoofing...
- Stop MITM attack(s)
- SSL Intercept

Randomizing 255 hosts for scanning...  
Scanning the whole netmask for 255 hosts...  
3 hosts added to the hosts list...  
Host 192.168.1.1 added to TARGET1  
Host 192.168.1.5 added to TARGET2

Step 10: In MITM Attack: ARP Poisoning select Sniff remote connections then click OK



Step 11: Let your client login something (like any website: instagram, twitter, etc) in browser

Step 12: Now you will get yours client ID, Password

Ettercap  
0.8.3.1 (EB)

Targets x Host List x

Target 1  
192.168.1.5

Target 2  
192.168.1.5

Add Delete

GROUP 2 : 192.168.1.5 -> 192.168.1.5  
Host 192.168.1.1 added to TARGET 1  
Host 192.168.1.5 added to TARGET 1  
ARP poisoner deactivated.  
RE-ARPing the victims...

ARP poisoning victims:

GROUP 1 : 192.168.1.5 -> 192.168.1.5

GROUP 2 : 192.168.1.5 -> 192.168.1.5

HTTP : 65.61.137.117:80 -> USER: Dfhdd PASS: INFO: http://testfire.net/login.jsp  
CONTENT: uid=Dfhdd&passw=245678g&btnSubmit=Login

HTTP : 65.61.137.117:80 -> USER: Kaushal+ PASS: INFO: http://testfire.net/login.jsp  
CONTENT: uid=Kaushal+&passw=3568gdtu%403577&btnSubmit=Login