

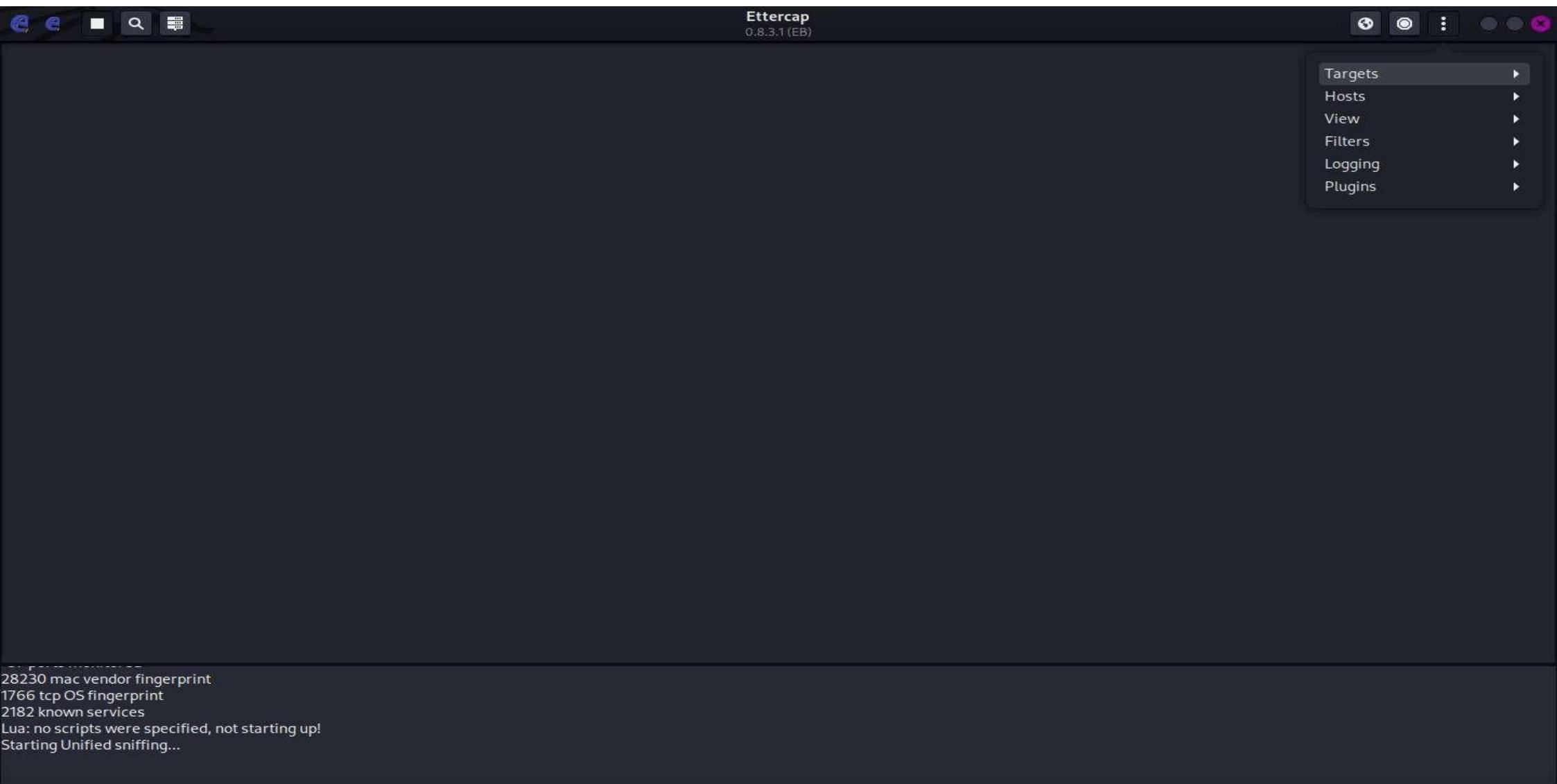
Sniffing using Ettercap

Step 1: Open Ettercap

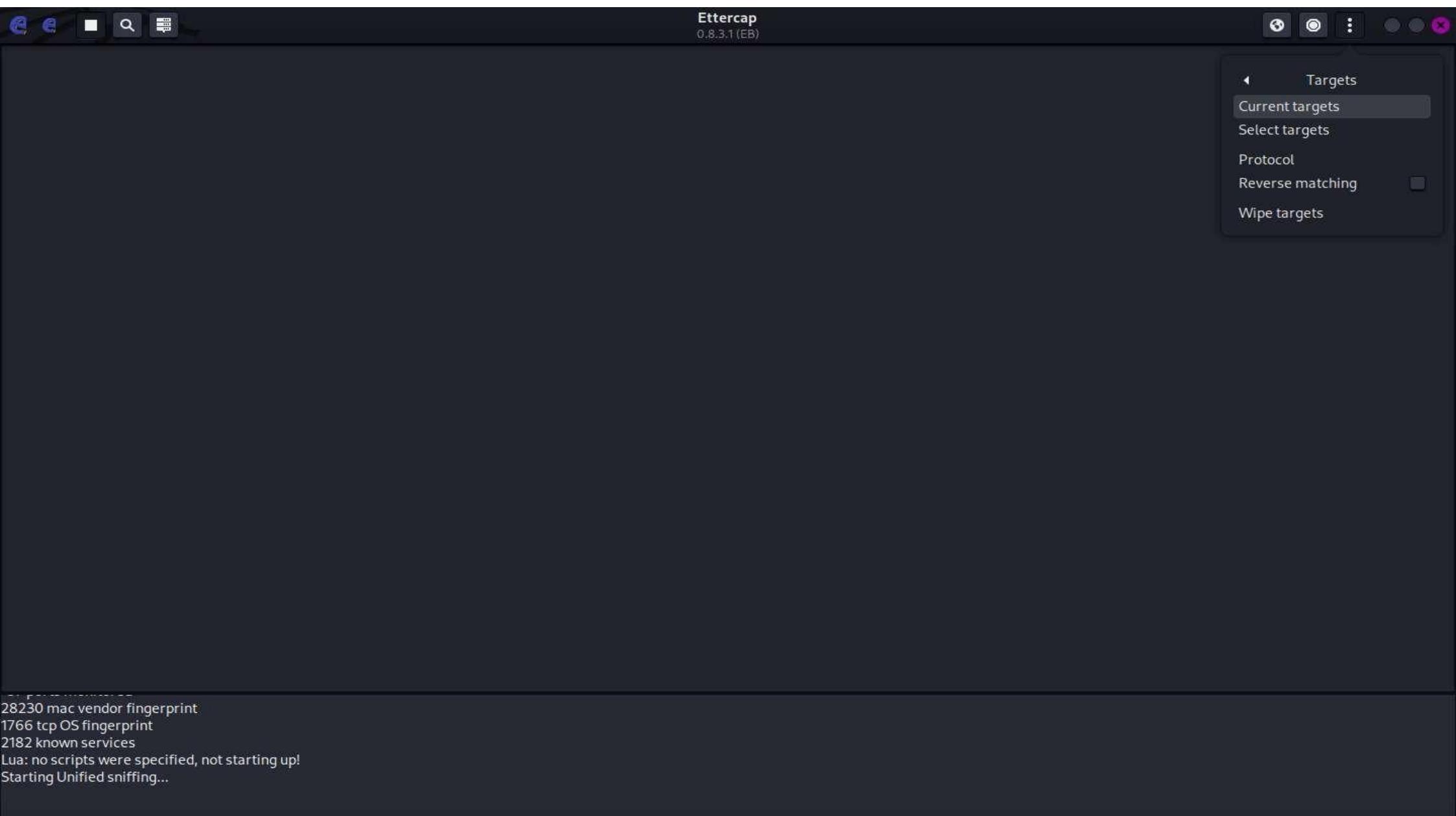
Step 2: Change eth0 to wlan0 and click on check mark



Step 3: Click on three dots → Targets



Step 4: Click on Current targets



Step 5: Click on Scan for host

The screenshot shows the Ettercap 0.8.3.1 interface. At the top, there's a toolbar with icons for file operations like Open, Save, and Print. The title bar reads "Ettercap 0.8.3.1 (EB)". Below the title bar, a menu bar has "Targets" selected, and the sub-menu "Scan for hosts" is highlighted. The main window is divided into two sections: "Target 1" on the left and "Target 2" on the right. Both sections are currently empty. At the bottom of the interface, there are two rows of buttons: "Delete" and "Add" for each target section. A status message at the very bottom of the screen reads:
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

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

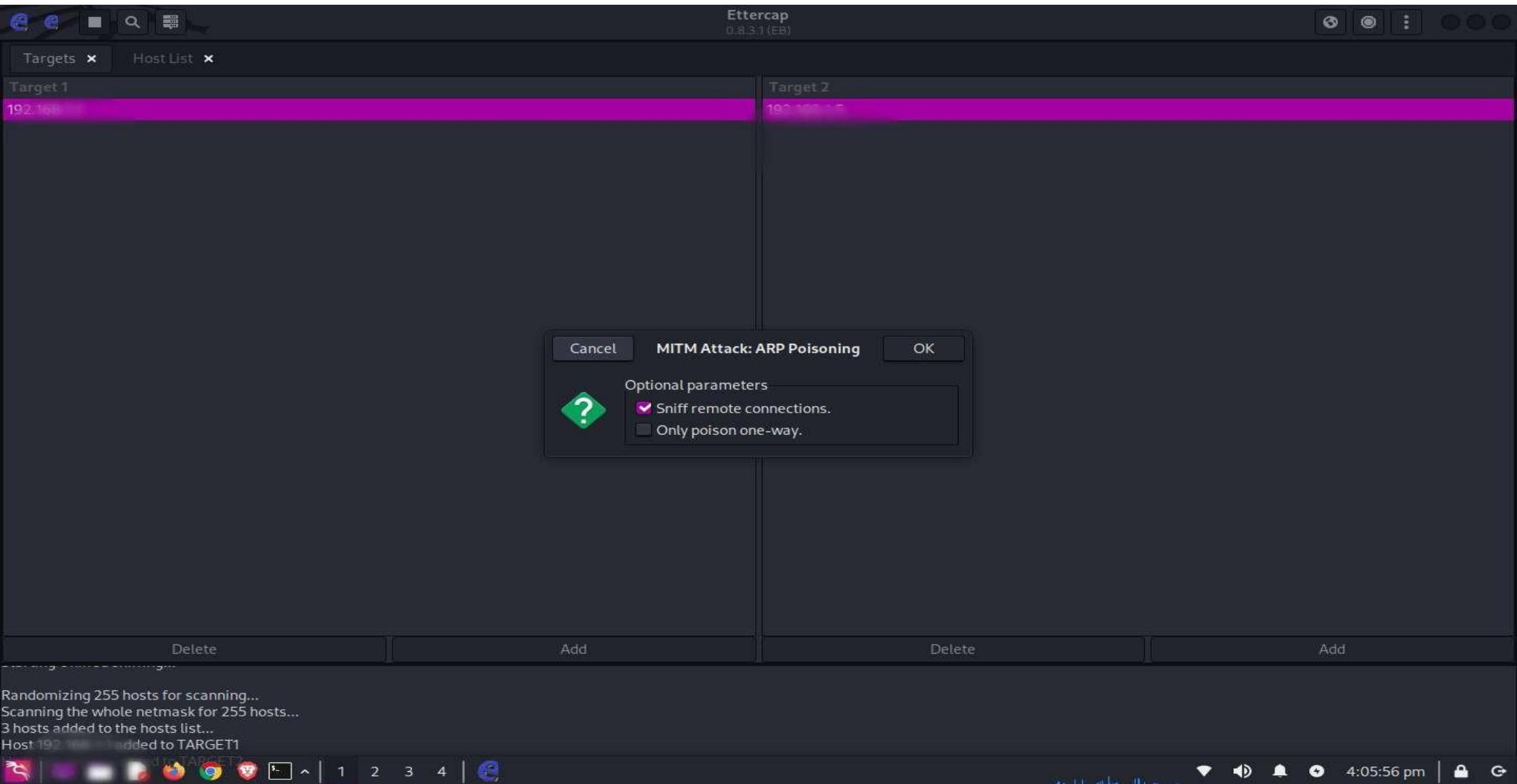
The screenshot shows the Ettercap 0.8.3.1 (EB) interface. At the top, there's a toolbar with various icons. Below it is a menu bar with 'Targets' and 'Host List'. The main window has a title 'Ettercap 0.8.3.1 (EB)' and displays a table with three columns: 'IP Address', 'MAC Address', and 'Description'. The IP addresses listed are blurred for security. At the bottom of the window, there are three buttons: 'Delete Host', 'Add to Target 1', and 'Add to Target 2'. A status message at the bottom left says: 'Lua: no scripts were specified, not starting up! Starting Unified sniffing...'. Another message at the bottom left says: '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 interface version 0.8.3.1 (EB). The window title is "Ettercap". The main area displays two targets: "Target 1" (IP 192.168.1.1) and "Target 2" (IP 192.168.1.5). Below the targets are "Delete" and "Add" buttons. A context menu is open over "Target 2", specifically over its entry in the list. The menu is titled "MITM" and includes the following options: ARP poisoning..., NDP poisoning, ICMP redirect..., Port stealing..., DHCP spoofing..., Stop MITM attack(s), and SSL Intercept. At the bottom of the screen, there is a status message: "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

The screenshot shows the Ettercap 0.8.3.1 interface. At the top, there are tabs for "Targets" and "Host List". Below the tabs, two sections are visible: "Target 1" and "Target 2". The "Target 1" section contains the IP address "192.168.1.5". The "Target 2" section is currently empty. At the bottom of the interface, there are buttons for "Add", "Delete", and another "Add".

GROUP 2 : 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

GROUP 2 : 192.168.1.5
HTTP : 65.61.137.117:80 -> USER: Dfhhdd PASS: INFO: http://testfire.net/login.jsp
CONTENT: uid=Dfhhdd&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