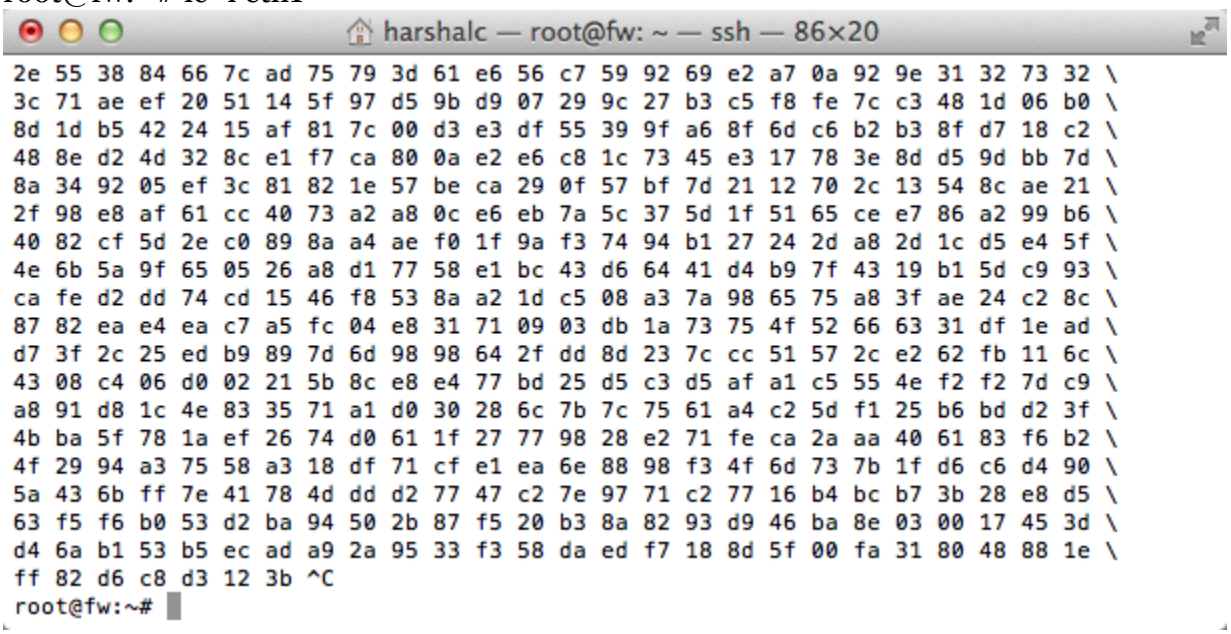
Linkcat - A Brahmastra for security professionals
Author - Harshal Chandorkar

A few days back my mentor asked me to read a book "Stealing the network". When I started, it first appeared as I am in some fantasy world. I was wondering should I take a step further see if everything written there is true? What if every command that is given there actually works as they say. With that excitement I couldn't wait a minute longer, I did a small experiment that was used as a real hack in one of the chapters of the book.

The set-up I have is as under:
1. A VM running Kali Machine [IP 10.0.1.199]
2. Ubuntu box working as a gateway (this is required as we need to sniff traffic, this can be achieved in various ways however i did it this way. [10.0.1.2]

Tools required:
1. linkcat
2. netcat
3. etherape
4. links web browser (for testing purposes only)

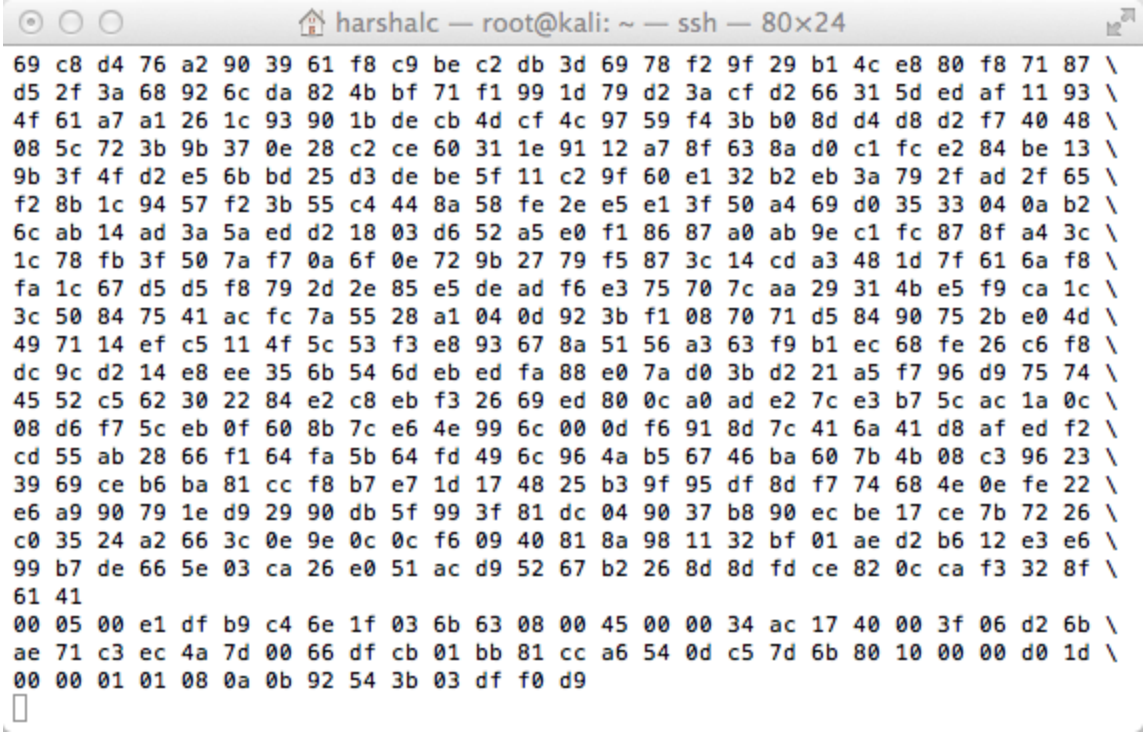
Step 1: On your gateway machine install linkcat tool and then proceed to see if the linkcat is working:
root@fw:~# lc -l eth1



Your output should be something like above.

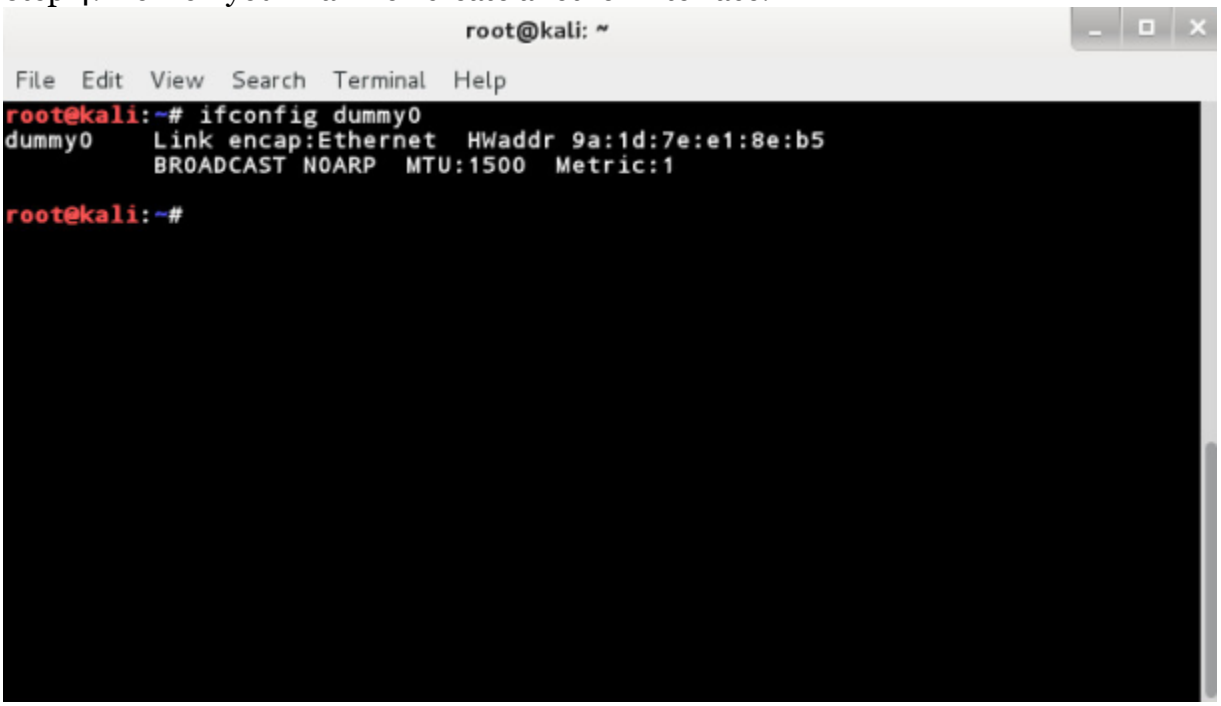
Step 2: Pipe the output of linkcat to netcat: We are doing this because we want to push the traffic from our gateway machine to kali box just so that we can analyze the traffic.
root@fw:~# lc -l eth1 | nc -l 10.0.1.2 2000
The output would look like its stuck. This means basically that the linkcat output is being piped to netcat on port 2000.

Step 3: On your Kali Machine connect to the gateway ip with netcat
root@kali:~# nc 10.0.1.2 2000

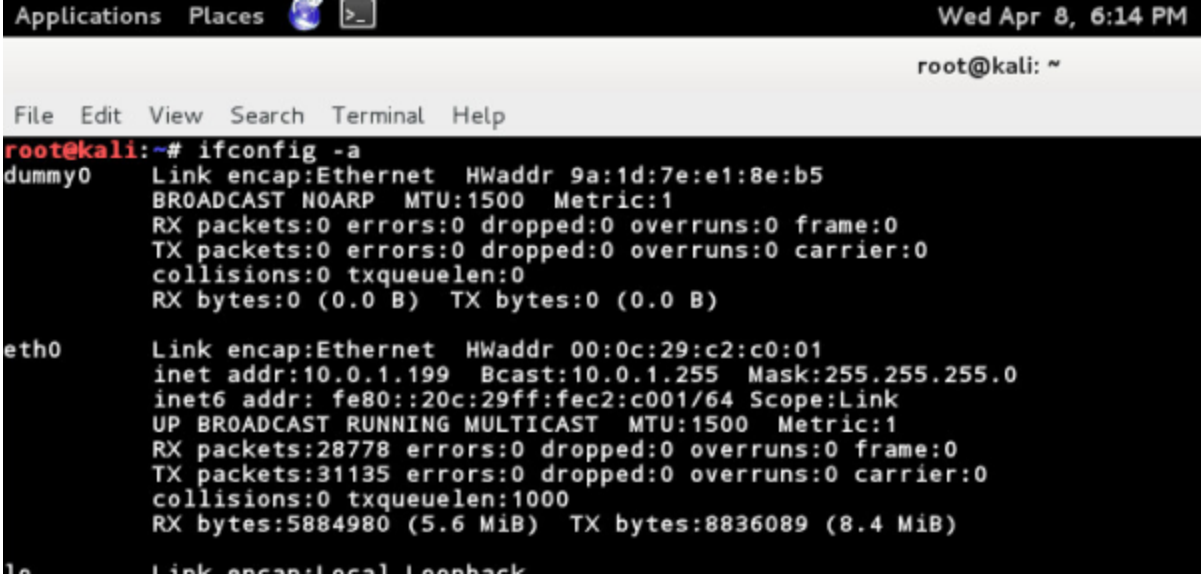


Above shows set up is working.

Step 4: Now on your Kali Box create another interface:



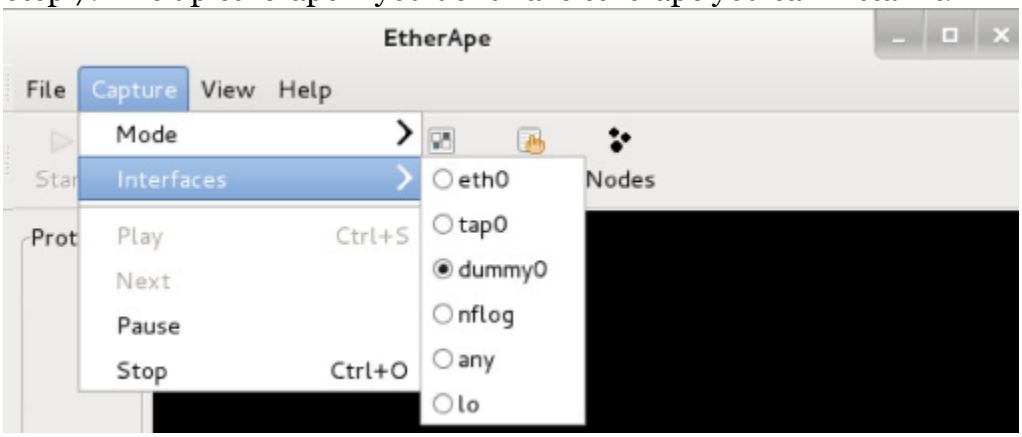
Your *ifconfig -a* should give you following screen:



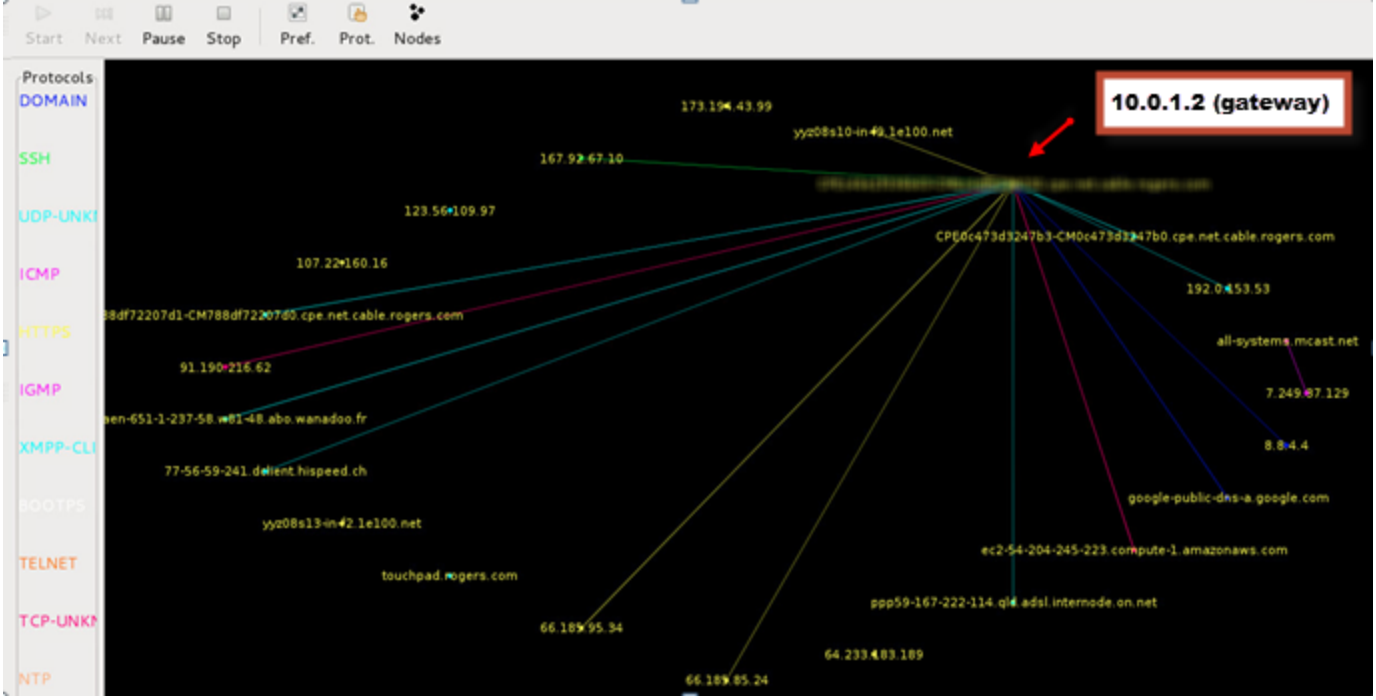
Step 5: Assign an ip address to the interface:
root@kali:~# ifconfig dummy0 inet 11.12.13.14 netmask 255.255.255.254
root@kali:~# ifconfig -a
dummy0 Link encap:Ethernet HWaddr 9a:1d:7e:e1:8e:b5
inet addr:11.12.13.14 Bcast:11.255.255.255 Mask:255.255.255.254
inet6 addr: fe80::981d:7eff:fee1:8eb5/64 Scope:Link
UP BROADCAST RUNNING NOARP MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:2287 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:0 (0.0 B) TX bytes:858822 (838.6 KiB)

Step 6: Pipe the netcat output to the dummy interface on Kali box
root@kali:~# nc 10.0.1.2 2000 | lc -m dummy0

Step 7: Fire up etherape if you dont have etherape you can install it.



You should see something like interstar gallactica



Use more options of etherape to sniff the traffic.

This is all folks, one of the lessons that I learnt. You will see more tutorials on what I learnt using linkcat soon.