

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:

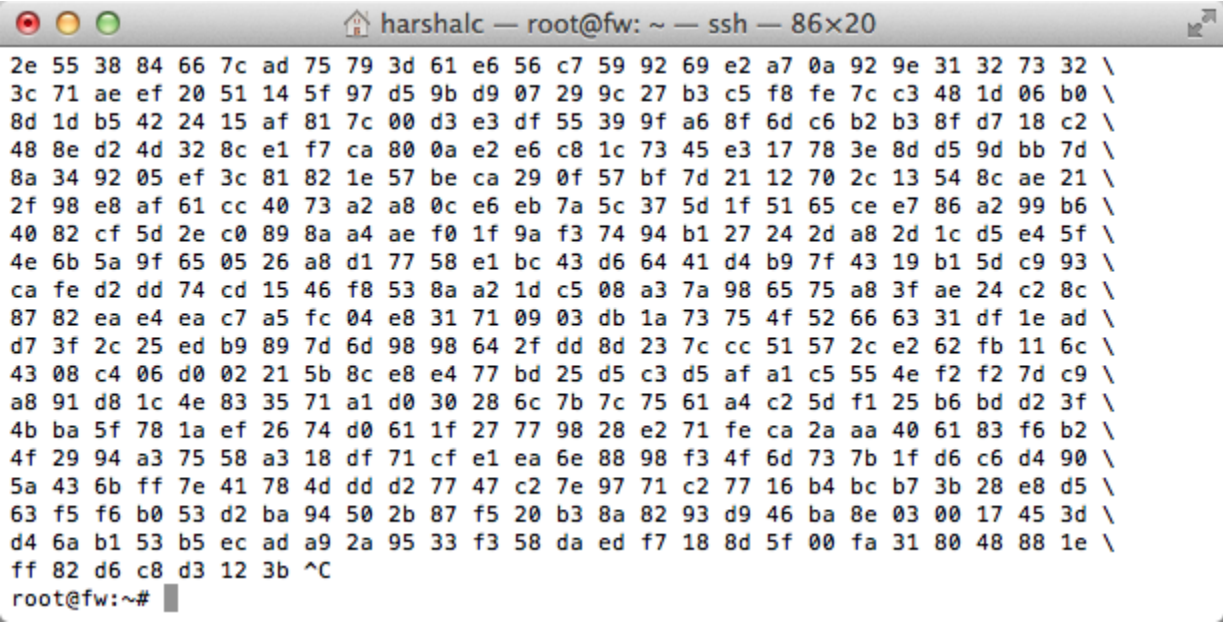
- 1. A VM running Kali Machine [IP 10.0.1.199]
- 2. Ubuntu box working as a gateway (this is required as we need to sniff traffic, this can be achieved in various ways however i did it this way. [10.0.1.2])

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

```
harshalc — root@kali: ~ — ssh — 80x24
69 c8 d4 76 a2 90 39 61 f8 c9 be c2 db 3d 69 78 f2 9f 29 b1 4c e8 80 f8 71 87 \
d5 2f 3a 68 92 6c da 82 4b bf 71 f1 99 1d 79 d2 3a cf d2 66 31 5d ed af 11 93 \
4f 61 a7 a1 26 1c 93 90 1b de cb 4d cf 4c 97 59 f4 3b b0 8d d4 d8 d2 f7 40 48 \
08 5c 72 3b 9b 37 0e 28 c2 ce 60 31 1e 91 12 a7 8f 63 8a d0 c1 fc e2 84 be 13 \
9b 3f 4f d2 e5 6b bd 25 d3 de be 5f 11 c2 9f 60 e1 32 b2 eb 3a 79 2f ad 2f 65 \
f2 8b 1c 94 57 f2 3b 55 c4 44 8a 58 fe 2e e5 e1 3f 50 a4 69 d0 35 33 04 0a b2 \
6c ab 14 ad 3a 5a ed d2 18 03 d6 52 a5 e0 f1 86 87 a0 ab 9e c1 fc 87 8f a4 3c \
1c 78 fb 3f 50 7a f7 0a 6f 0e 72 9b 27 79 f5 87 3c 14 cd a3 48 1d 7f 61 6a f8 \
fa 1c 67 d5 d5 f8 79 2d 2e 85 e5 de ad f6 e3 75 70 7c aa 29 31 4b e5 f9 ca 1c \
3c 50 84 75 41 ac fc 7a 55 28 a1 04 0d 92 3b f1 08 70 71 d5 84 90 75 2b e0 4d \
49 71 14 ef c5 11 4f 5c 53 f3 e8 93 67 8a 51 56 a3 63 f9 b1 ec 68 fe 26 c6 f8 \
dc 9c d2 14 e8 ee 35 6b 54 6d eb ed fa 88 e0 7a d0 3b d2 21 a5 f7 96 d9 75 74 \
45 52 c5 62 30 22 84 e2 c8 eb f3 26 69 ed 80 0c a0 ad e2 7c e3 b7 5c ac 1a 0c \
08 d6 f7 5c eb 0f 60 8b 7c e6 4e 99 6c 00 0d f6 91 8d 7c 41 6a 41 d8 af ed f2 \
cd 55 ab 28 66 f1 64 fa 5b 64 fd 49 6c 96 4a b5 67 46 ba 60 7b 4b 08 c3 96 23 \
39 69 ce b6 ba 81 cc f8 b7 e7 1d 17 48 25 b3 9f 95 df 8d f7 74 68 4e 0e fe 22 \
e6 a9 90 79 1e d9 29 90 db 5f 99 3f 81 dc 04 90 37 b8 90 ec be 17 ce 7b 72 26 \
c0 35 24 a2 66 3c 0e 9e 0c 0c f6 09 40 81 8a 98 11 32 bf 01 ae d2 b6 12 e3 e6 \
99 b7 de 66 5e 03 ca 26 e0 51 ac d9 52 67 b2 26 8d 8d fd ce 82 0c ca f3 32 8f \
61 41
00 05 00 e1 df b9 c4 6e 1f 03 6b 63 08 00 45 00 00 34 ac 17 40 00 3f 06 d2 6b \
ae 71 c3 ec 4a 7d 00 66 df cb 01 bb 81 cc a6 54 0d c5 7d 6b 80 10 00 00 d0 1d \
00 00 01 01 08 0a 0b 92 54 3b 03 df f0 d9
```

Above shows set up is working.

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

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ifconfig dummy0
dummy0      Link encap:Ethernet  HWaddr 9a:1d:7e:e1:8e:b5
            BROADCAST NOARP  MTU:1500  Metric:1

root@kali:~#
```

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

```
Applications Places >_ Wed Apr 8, 6:14 PM
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ifconfig -a
dummy0  Link encap:Ethernet  HWaddr 9a:1d:7e:e1:8e:b5
        BROADCAST NOARP  MTU:1500  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

eth0    Link encap:Ethernet  HWaddr 00:0c:29:c2:c0:01
        inet addr:10.0.1.199  Bcast:10.0.1.255  Mask:255.255.255.0
        inet6 addr: fe80::20c:29ff:fec2:c001/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:28778 errors:0 dropped:0 overruns:0 frame:0
        TX packets:31135 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:5884980 (5.6 MiB)  TX bytes:8836089 (8.4 MiB)

lo      Link encap:Local Loopback
```

Step 5: Assign an ip address to the interface:

```
root@kali:~# ifconfig dummy0 inet 11.12.13.14 netmask 255.255.255.254
```

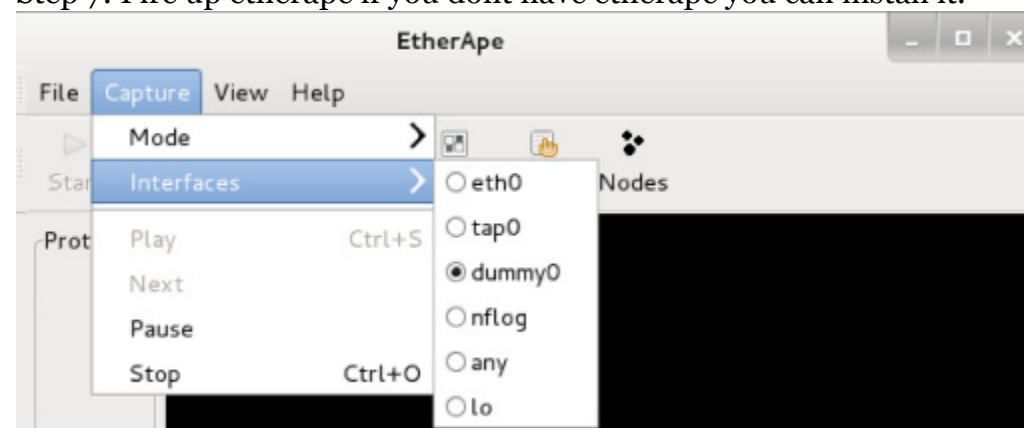
```
root@kali:~# ifconfig -a
```

```
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)
```

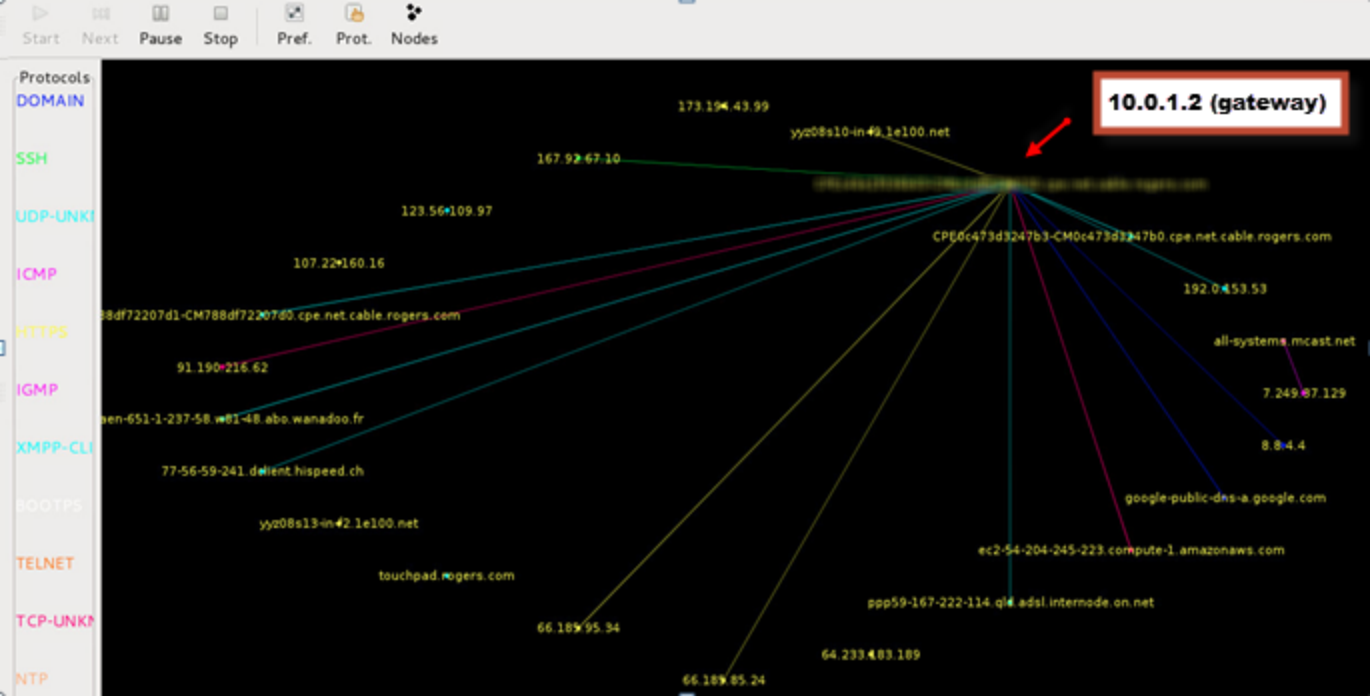
Step 6: Pipe the netcat output to the dummy interface on Kali box

```
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.