

ARP cache poisoning - ARP spoofing

Pentru aceasta temă am ales să implementez atacul ARP poisoning: un atac greu detectabil și ușor de folosit în rețelele actuale, totodată.

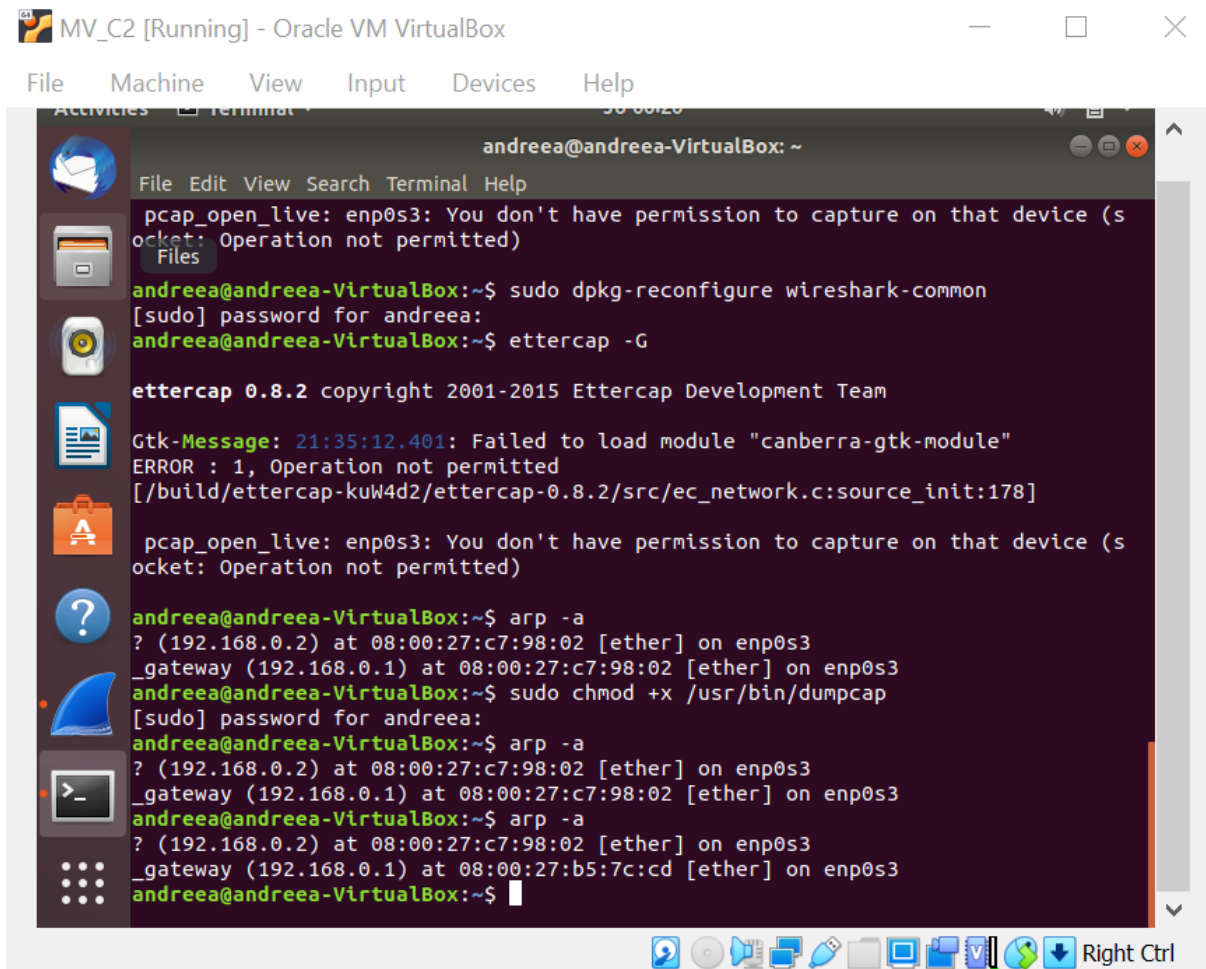
Pe scurt, în cadrul atacului ARP poisoning, traficul dintre o rețea locală și router este redirecționat spre atacator; acest lucru este posibil deoarece atacatorul trimite spre rețea și spre router două pachete false, conținând propria lui adresă MAC, astfel încât, când cei doi vor începe comunicarea și vor crede că fac schimb de mesaje, acestea vor ajunge la atacator.

În cazul nostru, cele trei părți implicate sunt: routerul, C1 și C2.

Comunicarea se desfășoară între C2 și router, iar C1 este atacatorul.

Se poate observa în poza de mai jos că adresele MAC (atât cea a routerului, cât și cea a rețelei) sunt diferite.

Pentru afișarea cache-ului ARP am folosit comanda `arp -a`.

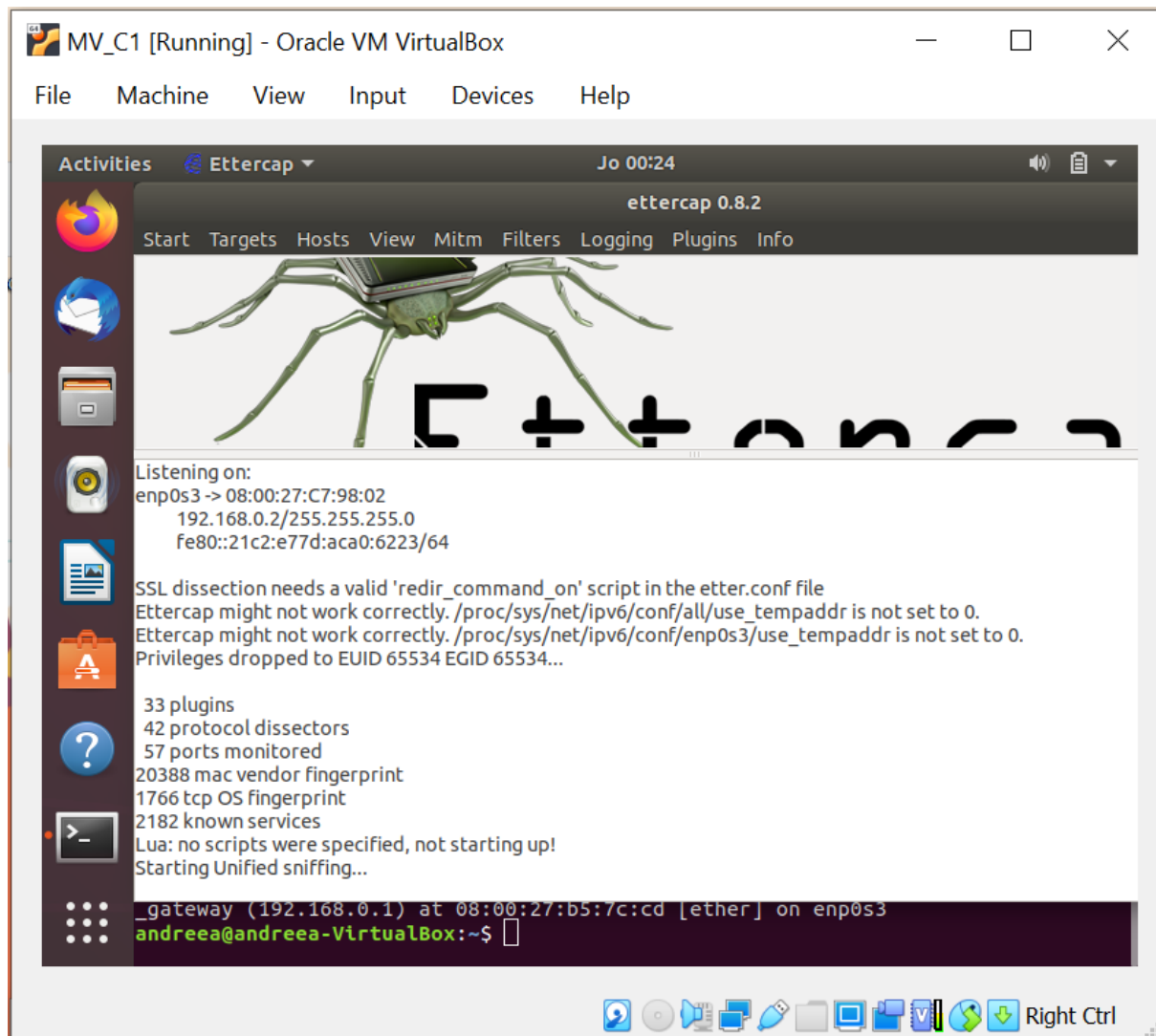


The screenshot shows a terminal window titled "MV_C2 [Running] - Oracle VM VirtualBox" with a menu bar (File, Machine, View, Input, Devices, Help). The terminal output is as follows:

```
andreea@andreea-VirtualBox: ~  
File Edit View Search Terminal Help  
pcap_open_live: enp0s3: You don't have permission to capture on that device (socket: Operation not permitted)  
andreea@andreea-VirtualBox:~$ sudo dpkg-reconfigure wireshark-common  
[sudo] password for andreea:  
andreea@andreea-VirtualBox:~$ ettercap -G  
ettercap 0.8.2 copyright 2001-2015 Ettercap Development Team  
Gtk-Message: 21:35:12.401: Failed to load module "canberra-gtk-module"  
ERROR : 1, Operation not permitted  
[/build/ettercap-kuW4d2/ettercap-0.8.2/src/ec_network.c:source_init:178]  
pcap_open_live: enp0s3: You don't have permission to capture on that device (socket: Operation not permitted)  
andreea@andreea-VirtualBox:~$ arp -a  
? (192.168.0.2) at 08:00:27:c7:98:02 [ether] on enp0s3  
_gateway (192.168.0.1) at 08:00:27:c7:98:02 [ether] on enp0s3  
andreea@andreea-VirtualBox:~$ sudo chmod +x /usr/bin/dumpcap  
[sudo] password for andreea:  
andreea@andreea-VirtualBox:~$ arp -a  
? (192.168.0.2) at 08:00:27:c7:98:02 [ether] on enp0s3  
_gateway (192.168.0.1) at 08:00:27:c7:98:02 [ether] on enp0s3  
andreea@andreea-VirtualBox:~$ arp -a  
? (192.168.0.2) at 08:00:27:c7:98:02 [ether] on enp0s3  
_gateway (192.168.0.1) at 08:00:27:b5:7c:cd [ether] on enp0s3  
andreea@andreea-VirtualBox:~$
```

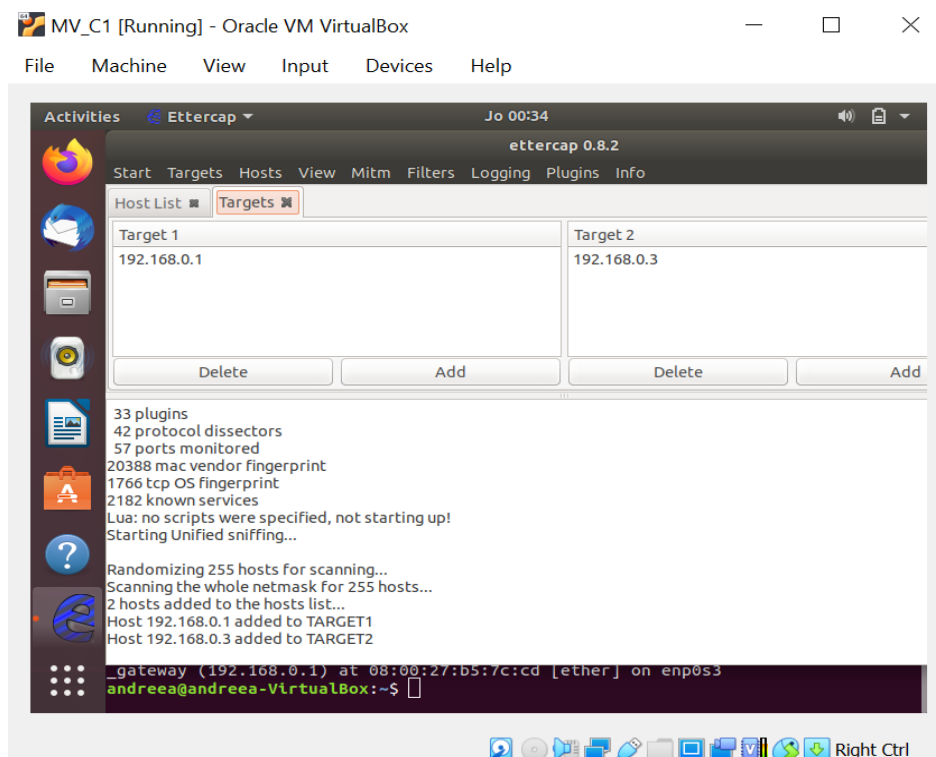
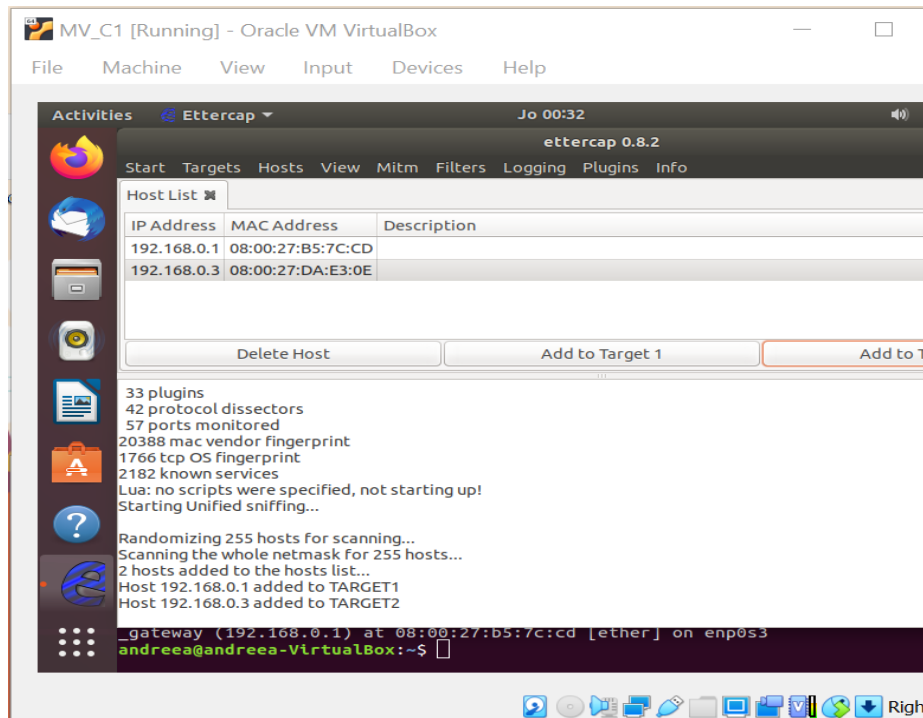
The terminal window has a sidebar with icons for Files, Home, Recent, and a search icon. The bottom status bar shows system icons and the text "Right Ctrl".

Am pornit Ettercap.

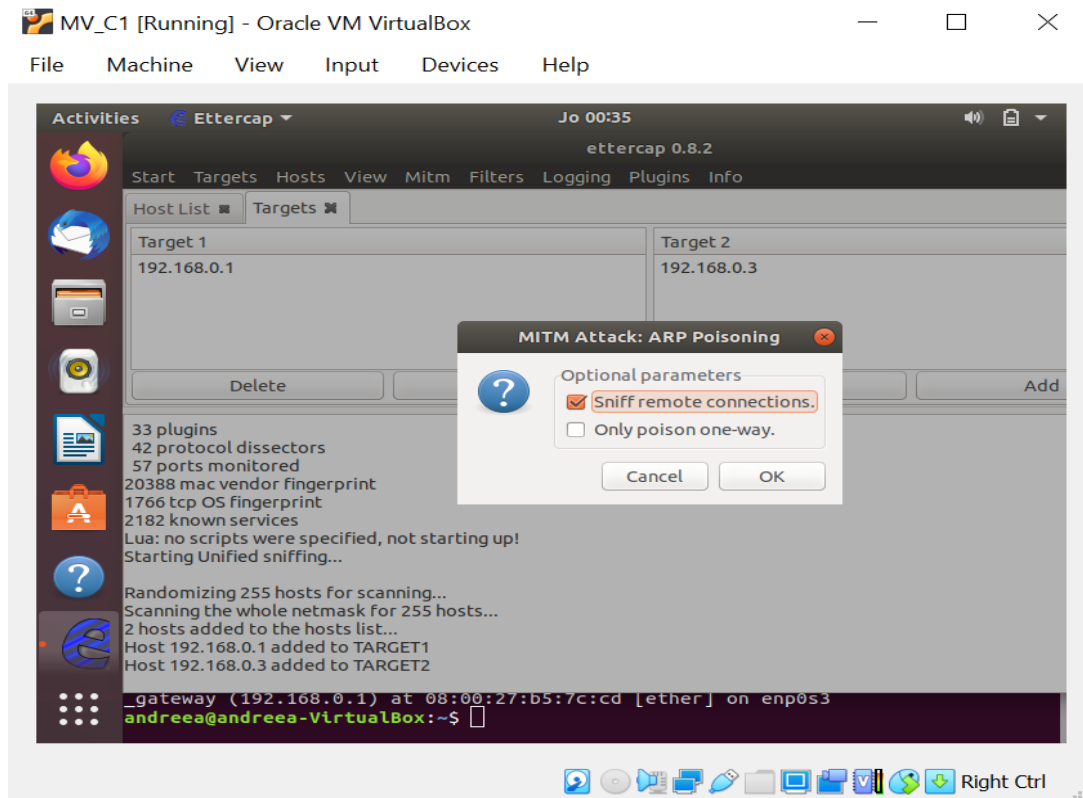


"Otravim" routerul și C2.

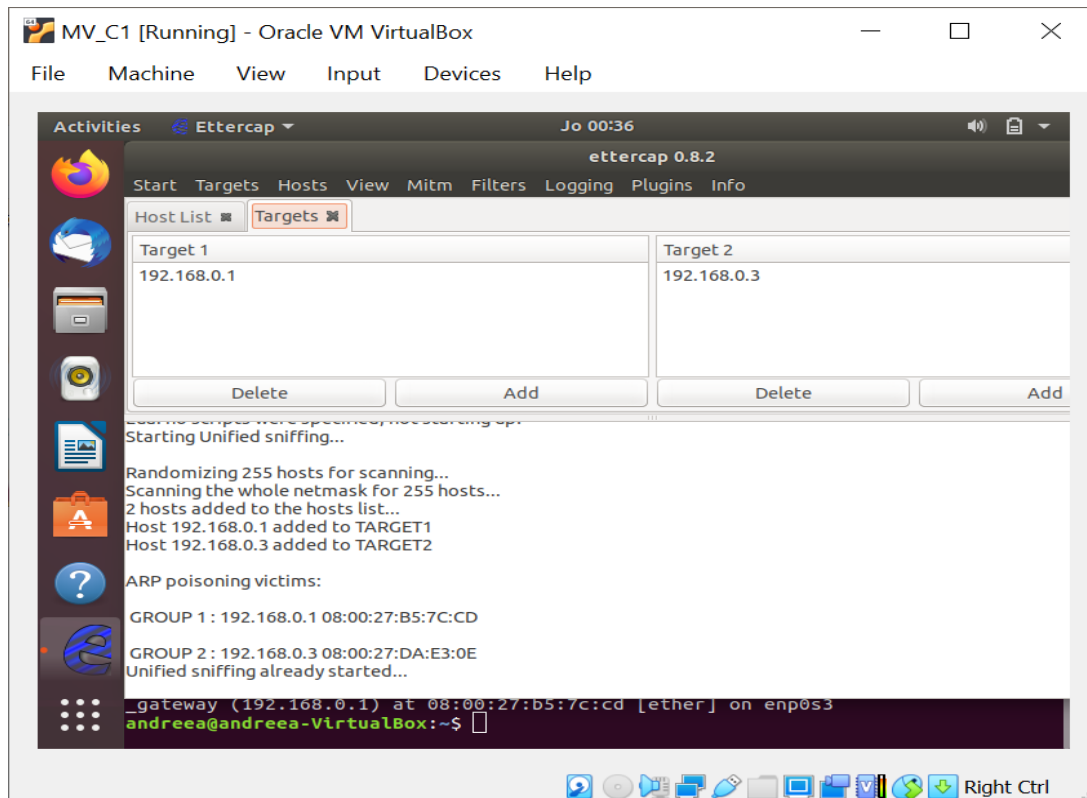
Din lista de hosts, am adăugat routerul(192.168.0.1) ca target 1 și pe C2(192.168.0.3) ca target 2.



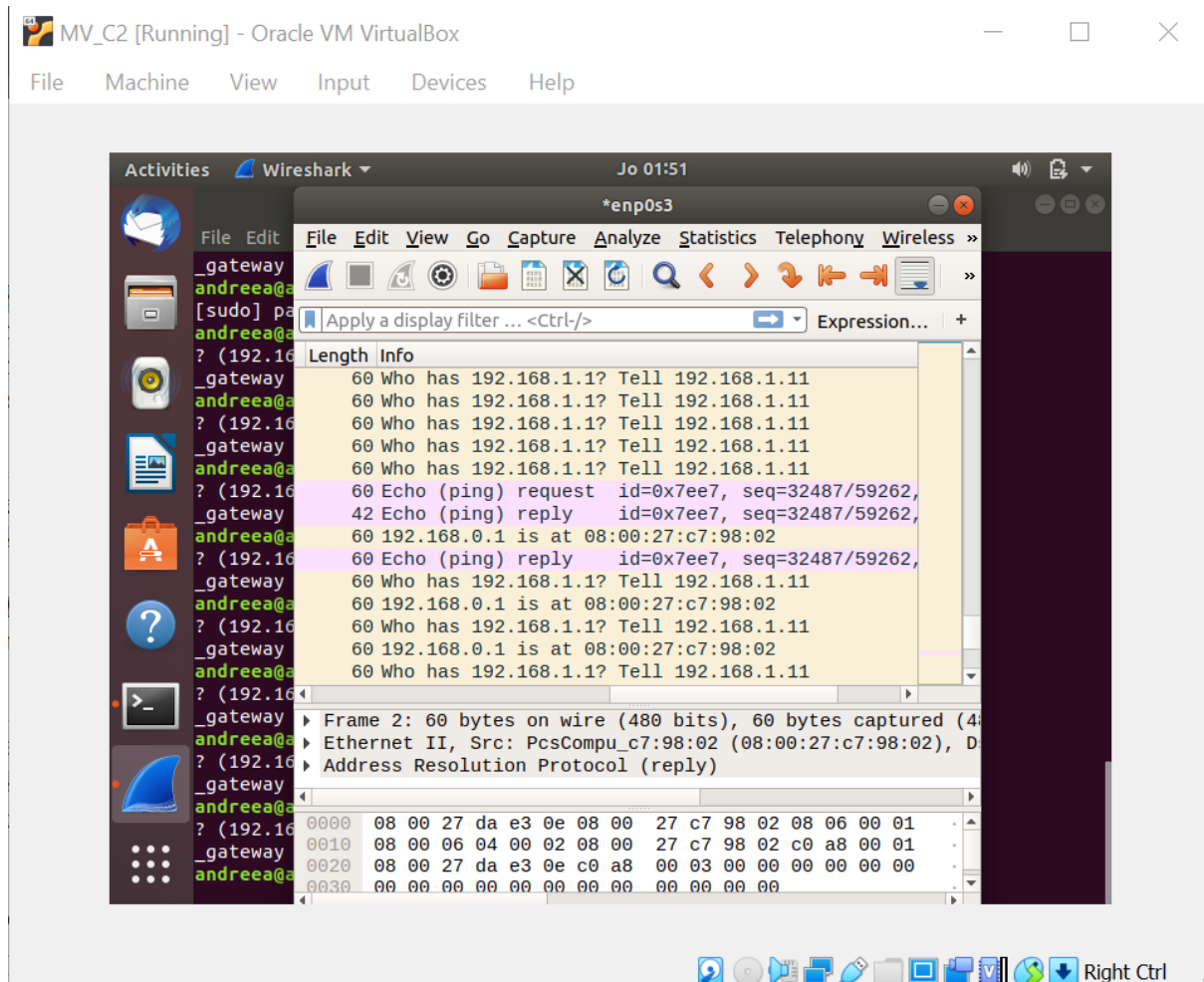
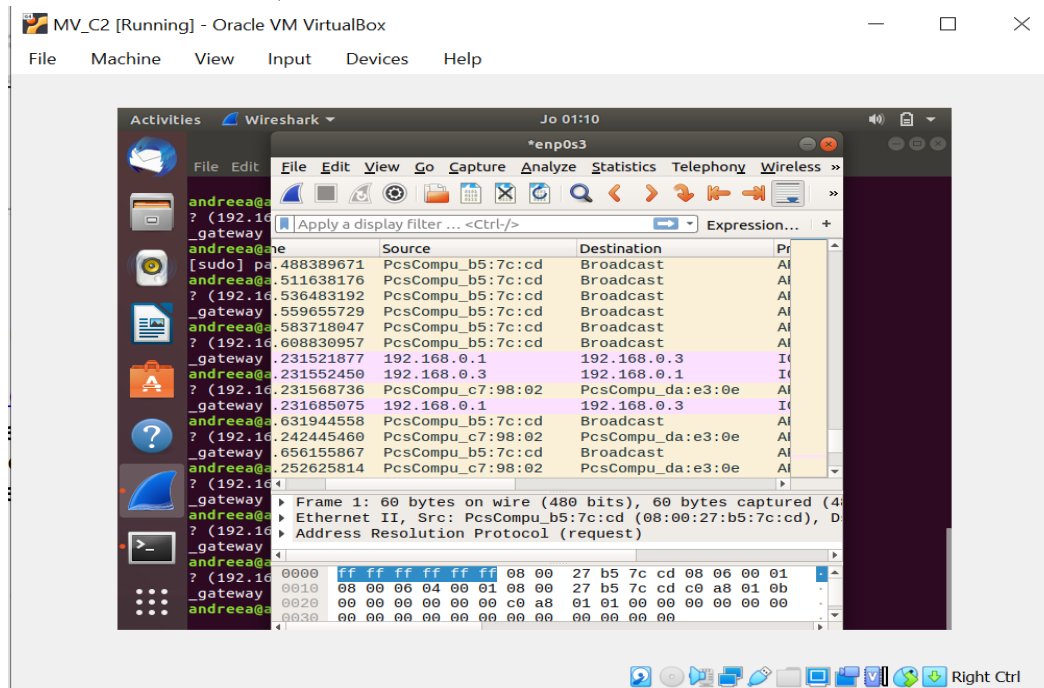
E momentul în care se pornește "otrăvirea" (ARP poisoning).



Și start sniffing.

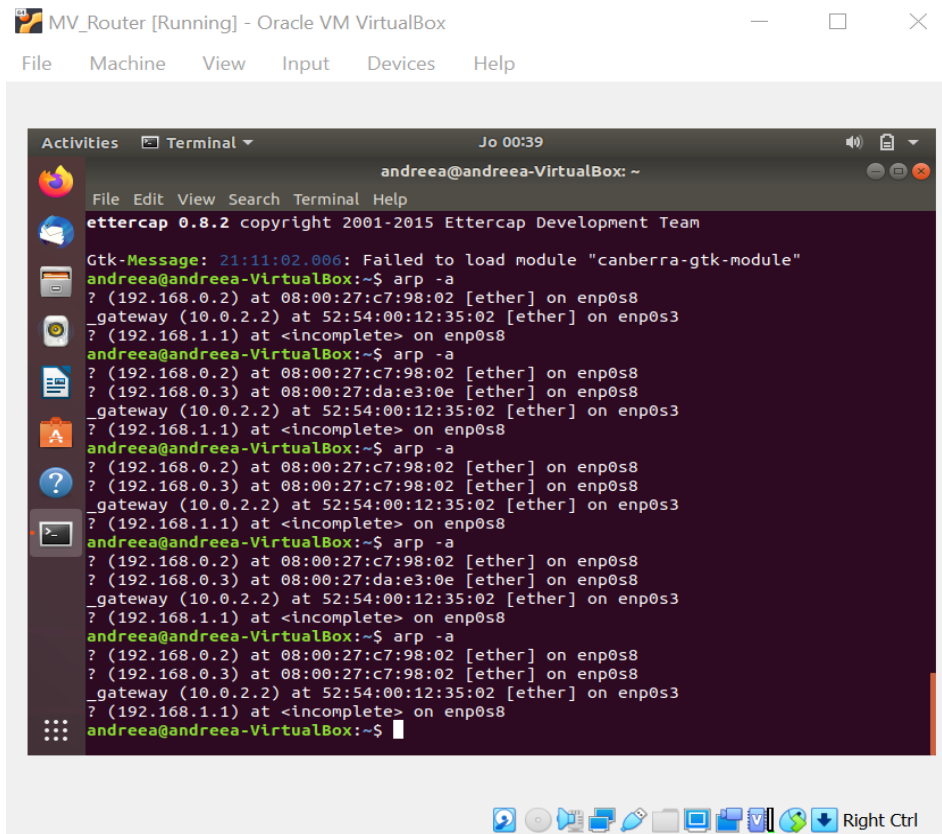


Între timp, am pornit și wireshark pentru a monitoriza traficul de date din rețea.



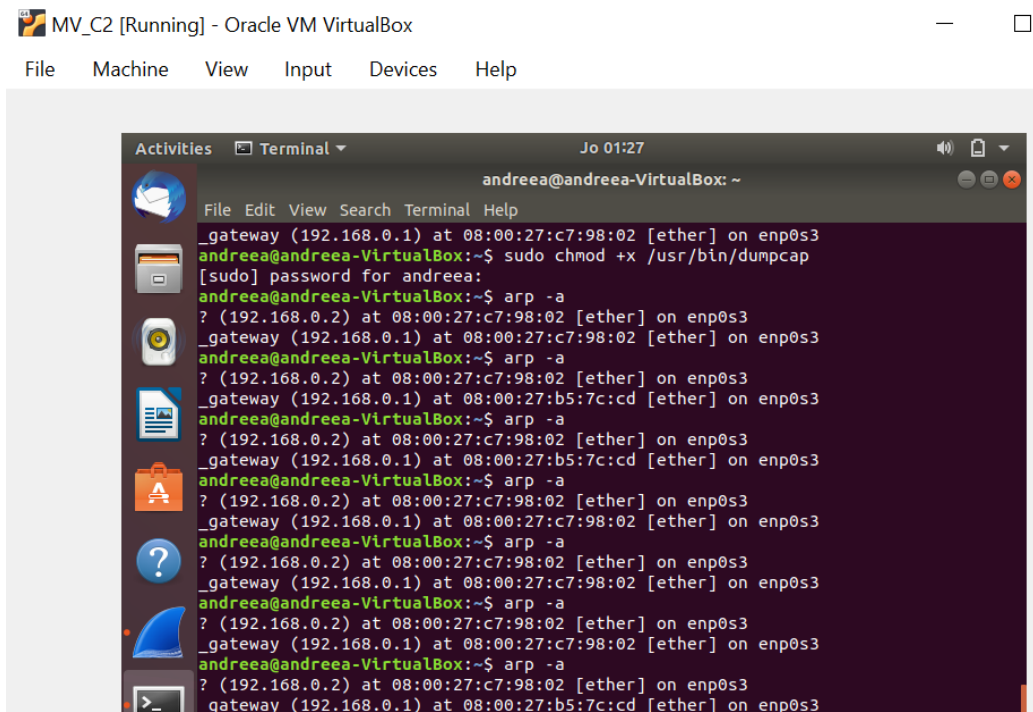
Se poate observa că după otrăvire adresa MAC spre care routerul trimite pachetele s-a schimbat în adresa atacatorului; astfel că, routerul va trimite mesaje spre atacator.

Iar acum, adresa MAC a lui C2 este aceeași cu cea a atacatorului.



```
andreea@andreea-VirtualBox: ~  
File Edit View Search Terminal Help  
ettercap 0.8.2 copyright 2001-2015 Ettercap Development Team  
Gtk-Message: 21:11:02.006: Failed to load module "canberra-gtk-module"  
andreea@andreea-VirtualBox:~$ arp -a  
? (192.168.0.2) at 08:00:27:c7:98:02 [ether] on enp0s8  
_gateway (10.0.2.2) at 52:54:00:12:35:02 [ether] on enp0s3  
? (192.168.1.1) at <incomplete> on enp0s8  
andreea@andreea-VirtualBox:~$ arp -a  
? (192.168.0.2) at 08:00:27:c7:98:02 [ether] on enp0s8  
? (192.168.0.3) at 08:00:27:da:e3:0e [ether] on enp0s8  
_gateway (10.0.2.2) at 52:54:00:12:35:02 [ether] on enp0s3  
? (192.168.1.1) at <incomplete> on enp0s8  
andreea@andreea-VirtualBox:~$ arp -a  
? (192.168.0.2) at 08:00:27:c7:98:02 [ether] on enp0s8  
? (192.168.0.3) at 08:00:27:c7:98:02 [ether] on enp0s8  
_gateway (10.0.2.2) at 52:54:00:12:35:02 [ether] on enp0s3  
? (192.168.1.1) at <incomplete> on enp0s8  
andreea@andreea-VirtualBox:~$ arp -a  
? (192.168.0.2) at 08:00:27:c7:98:02 [ether] on enp0s8  
? (192.168.0.3) at 08:00:27:c7:98:02 [ether] on enp0s8  
_gateway (10.0.2.2) at 52:54:00:12:35:02 [ether] on enp0s3  
? (192.168.1.1) at <incomplete> on enp0s8  
andreea@andreea-VirtualBox:~$ arp -a  
? (192.168.0.2) at 08:00:27:c7:98:02 [ether] on enp0s8  
? (192.168.0.3) at 08:00:27:c7:98:02 [ether] on enp0s8  
_gateway (10.0.2.2) at 52:54:00:12:35:02 [ether] on enp0s3  
? (192.168.1.1) at <incomplete> on enp0s8  
andreea@andreea-VirtualBox:~$
```

Odată oprită otrăvirea, prin rularea comenzii `atr -a` putem observa că adresele MAC ale celor doi participanți la conversație au revenit la forma inițială:



```
andreea@andreea-VirtualBox: ~  
File Edit View Search Terminal Help  
_gateway (192.168.0.1) at 08:00:27:c7:98:02 [ether] on enp0s3  
andreea@andreea-VirtualBox:~$ sudo chmod +x /usr/bin/dumpcap  
[sudo] password for andreea:  
andreea@andreea-VirtualBox:~$ arp -a  
? (192.168.0.2) at 08:00:27:c7:98:02 [ether] on enp0s3  
_gateway (192.168.0.1) at 08:00:27:c7:98:02 [ether] on enp0s3  
andreea@andreea-VirtualBox:~$ arp -a  
? (192.168.0.2) at 08:00:27:c7:98:02 [ether] on enp0s3  
_gateway (192.168.0.1) at 08:00:27:b5:7c:cd [ether] on enp0s3  
andreea@andreea-VirtualBox:~$ arp -a  
? (192.168.0.2) at 08:00:27:c7:98:02 [ether] on enp0s3  
_gateway (192.168.0.1) at 08:00:27:c7:98:02 [ether] on enp0s3  
andreea@andreea-VirtualBox:~$ arp -a  
? (192.168.0.2) at 08:00:27:c7:98:02 [ether] on enp0s3  
_gateway (192.168.0.1) at 08:00:27:c7:98:02 [ether] on enp0s3  
andreea@andreea-VirtualBox:~$ arp -a  
? (192.168.0.2) at 08:00:27:c7:98:02 [ether] on enp0s3  
_gateway (192.168.0.1) at 08:00:27:c7:98:02 [ether] on enp0s3  
andreea@andreea-VirtualBox:~$ arp -a  
? (192.168.0.2) at 08:00:27:c7:98:02 [ether] on enp0s3  
_gateway (192.168.0.1) at 08:00:27:b5:7c:cd [ether] on enp0s3  
andreea@andreea-VirtualBox:~$
```