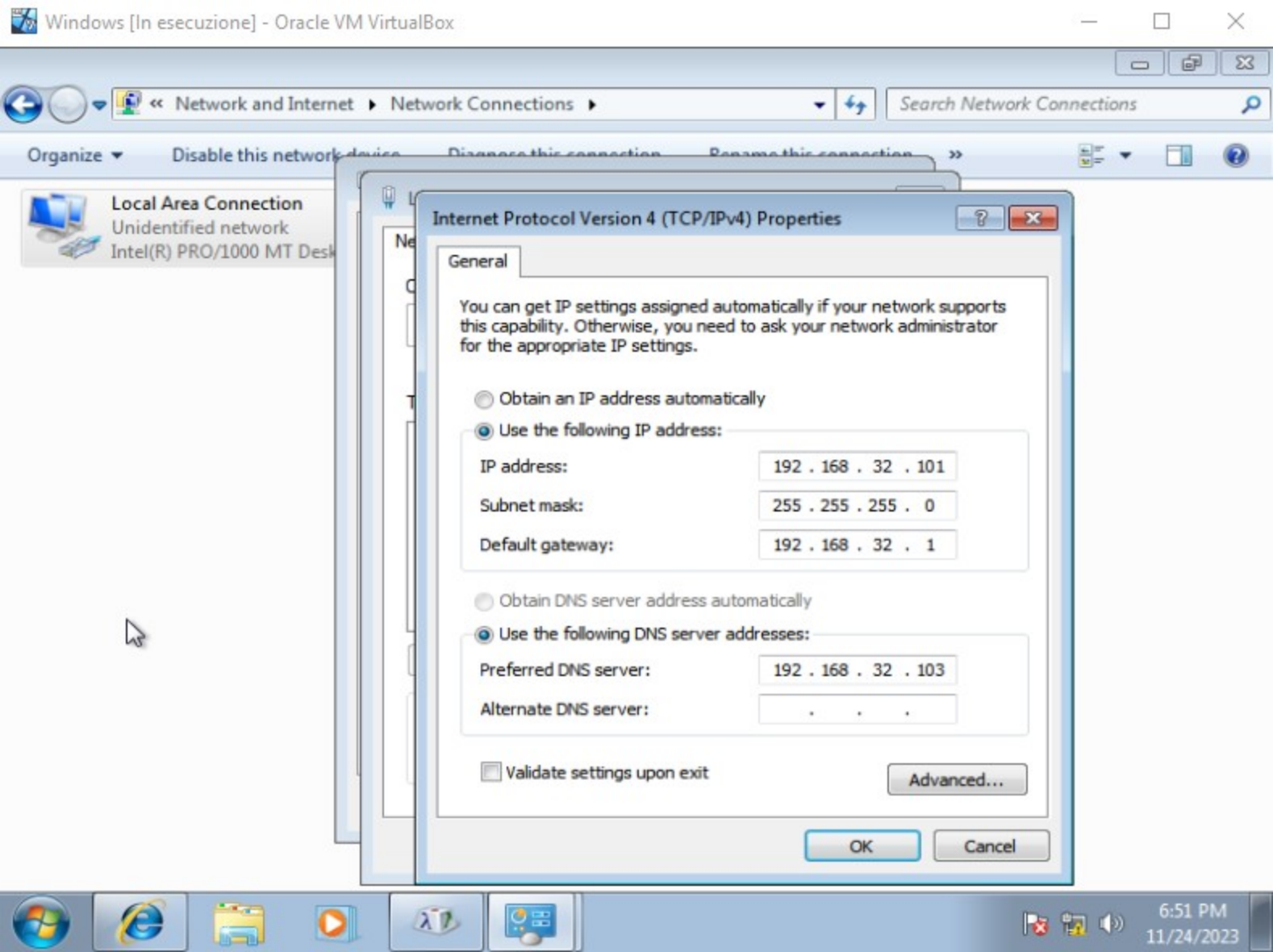
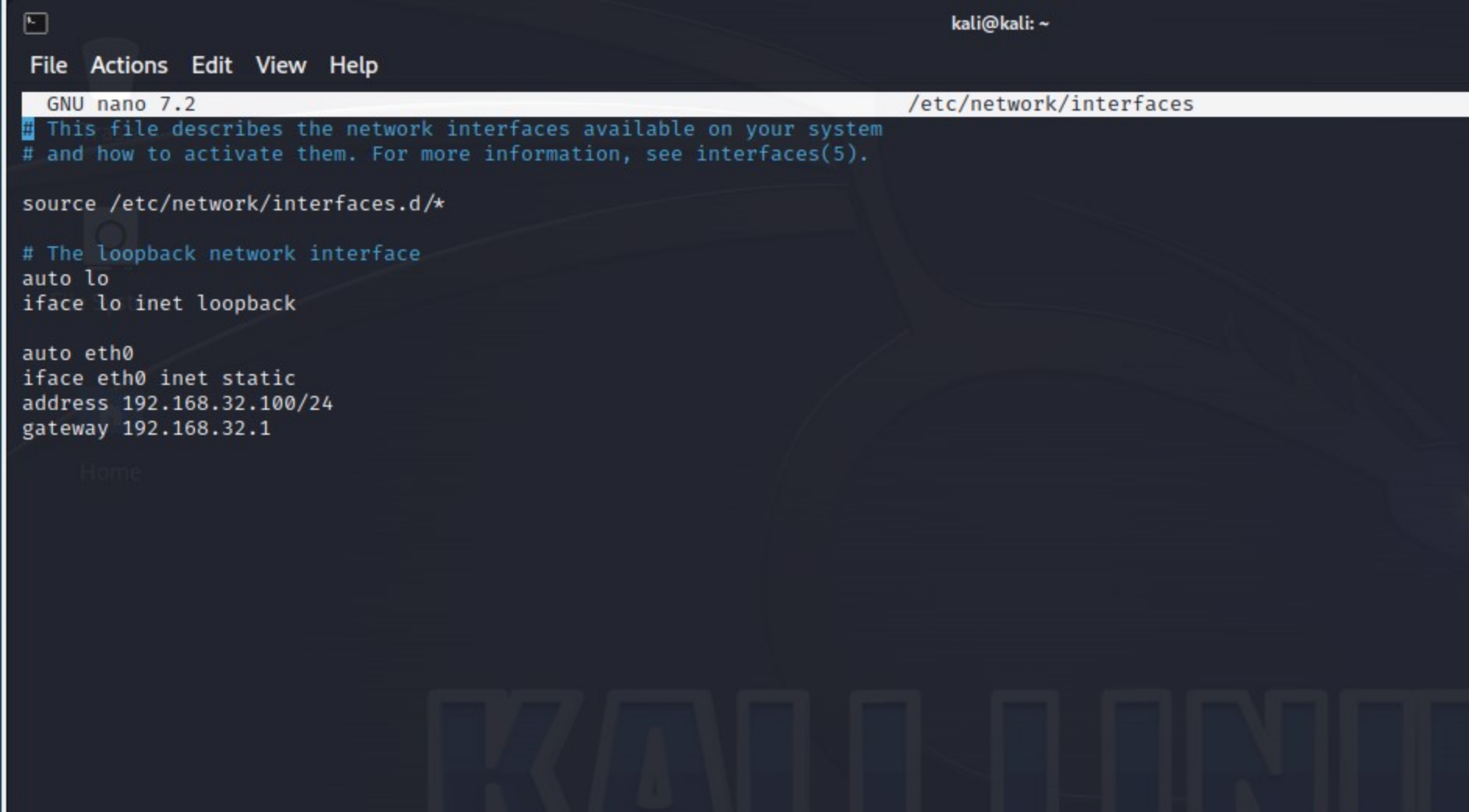
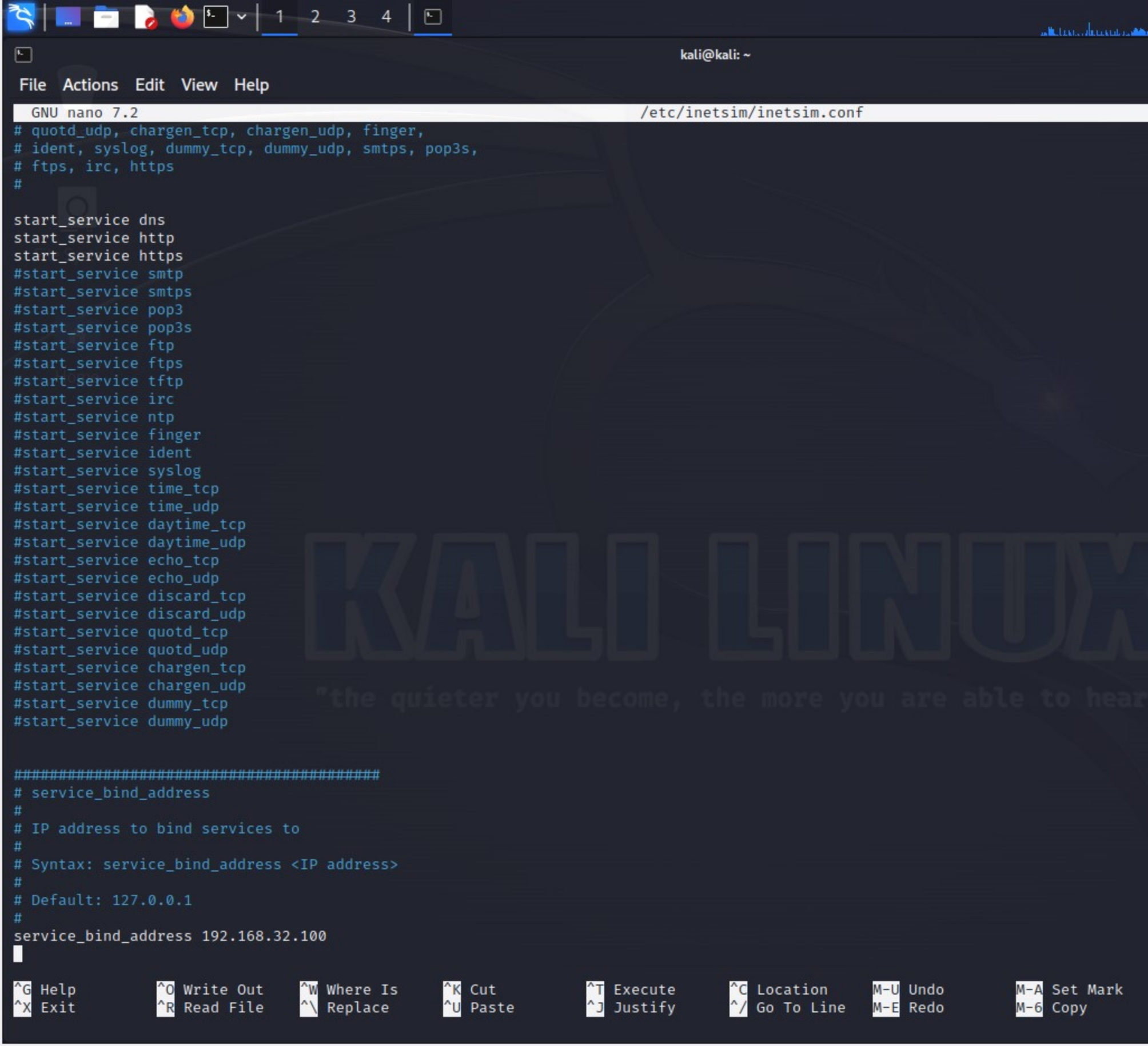

Windows [In esecuzione] - Oracle VM VirtualBox
Network and Internet ▸ Network Connections ▸
Search Network Connections
Organize
Disable this network device
Diagnose this connection
Rename this connection
Local Area Connection
Unidentified network
Intel(R) PRO/1000 MT Desk
Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 32 . 101
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 32 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 32 . 103
Alternate DNS server: . . .
Validate settings upon exit
Advanced...
OK
Cancel
6:51 PM
11/24/2023


kali@kali: ~
File Actions Edit View Help
GNU nano 7.2 /etc/network/interfaces
This file describes the network interfaces available on your system
and how to activate them. For more information, see interfaces(5).
source /etc/network/interfaces.d/*
The loopback network interface
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet static
address 192.168.32.100/24
gateway 192.168.32.1


kali@kali: ~
File Actions Edit View Help
GNU nano 7.2 /etc/inetsim/inetsim.conf
quotd_udp, chargen_tcp, chargen_udp, finger,
ident, syslog, dummy_tcp, dummy_udp, smtps, pop3s,
ftps, irc, https
#
start_service dns
start_service http
start_service https
#start_service smtp
#start_service smtps
#start_service pop3
#start_service pop3s
#start_service ftp
#start_service ftps
#start_service tftp
#start_service irc
#start_service ntp
#start_service finger
#start_service ident
#start_service syslog
#start_service time_tcp
#start_service time_udp
#start_service daytime_tcp
#start_service daytime_udp
#start_service echo_tcp
#start_service echo_udp
#start_service discard_tcp
#start_service discard_udp
#start_service quotd_tcp
#start_service quotd_udp
#start_service chargen_tcp
#start_service chargen_udp
#start_service dummy_tcp
#start_service dummy_udp
##
service_bind_address
#
IP address to bind services to
#
Syntax: service_bind_address <IP address>
#
Default: 127.0.0.1
#
service_bind_address 192.168.32.100
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy

```
##############################################################
# dns_static
#
# Static mappings for DNS
#
# Syntax: dns_static <fqdn hostname> <IP address>
#
# Default: none
#
dns_static epicode.internal 192.168.32.100
#dns_static ns1.foo.com 10.70.50.30
#dns_static ftp.bar.net 10.10.20.30
```

kali-linux-2023.3-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

1 2 3 4 12:44

*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

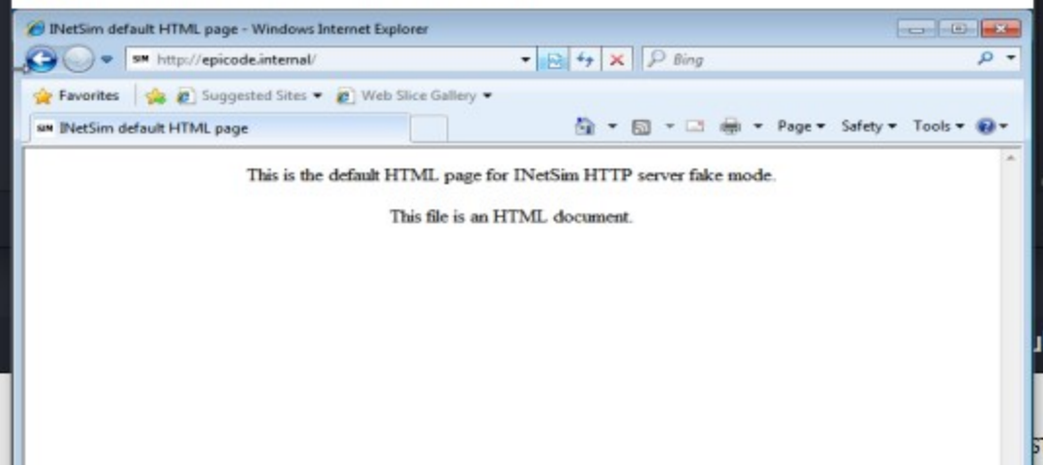
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PcsCompu_67:4b:8b	Broadcast	ARP	60	Who has 192.168.32.100? Tell 192.168.32.101
2	0.000063489	PcsCompu_cb:7e:f5	PcsCompu_67:4b:8b	ARP	42	192.168.32.100 is at 08:00:27:cb:7e:f5
3	0.000579557	192.168.32.101	192.168.32.100	TCP	66	49160 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
4	0.000641205	192.168.32.100	192.168.32.101	TCP	66	80 → 49160 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_…
5	0.001015778	192.168.32.101	192.168.32.100	TCP	60	49160 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
6	0.001286685	192.168.32.101	192.168.32.100	HTTP	340	GET / HTTP/1.1
7	0.001305408	192.168.32.100	192.168.32.101	TCP	54	80 → 49160 [ACK] Seq=1 Ack=287 Win=64128 Len=0
8	0.070399678	192.168.32.100	192.168.32.101	TCP	204	80 → 49160 [PSH, ACK] Seq=1 Ack=287 Win=64128 Len=150 [TCP segme…
9	0.075698054	192.168.32.100	192.168.32.101	HTTP	312	HTTP/1.1 200 OK (text/html)
10	0.076223412	192.168.32.101	192.168.32.100	TCP	60	49160 → 80 [ACK] Seq=287 Ack=410 Win=65292 Len=0
11	0.076486031	192.168.32.101	192.168.32.100	TCP	60	49160 → 80 [FIN, ACK] Seq=287 Ack=410 Win=65292 Len=0
12	0.076514407	192.168.32.100	192.168.32.101	TCP	54	80 → 49160 [ACK] Seq=410 Ack=288 Win=64128 Len=0

```
Frame 6: 340 bytes on wire (2720 bits), 340 bytes captured (2720 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_67:4b:8b (08:00:27:67:4b:8b), Dst: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5)
  Destination: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5)
  Source: PcsCompu_67:4b:8b (08:00:27:67:4b:8b)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100
Transmission Control Protocol, Src Port: 49160, Dst Port: 80, Seq: 1, Ack: 1, Len: 286
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
  Accept: */*\r\n
  Accept-Language: en-US\r\n
  User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET C…
  Accept-Encoding: gzip, deflate\r\n
  Host: epicode.internal\r\n
  Connection: Keep-Alive\r\n
  \r\n
  [Full request URI: http://epicode.internal/]
  [HTTP request 1/1]
  [Response in frame: 9]
```

wireshark_eth02VXEF2.pcapng

Ready to load or capture

Windows [In esecuzione] - Oracle VM VirtualBox



kali-linux-2023.3-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

1 2 3 4 12:49

*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

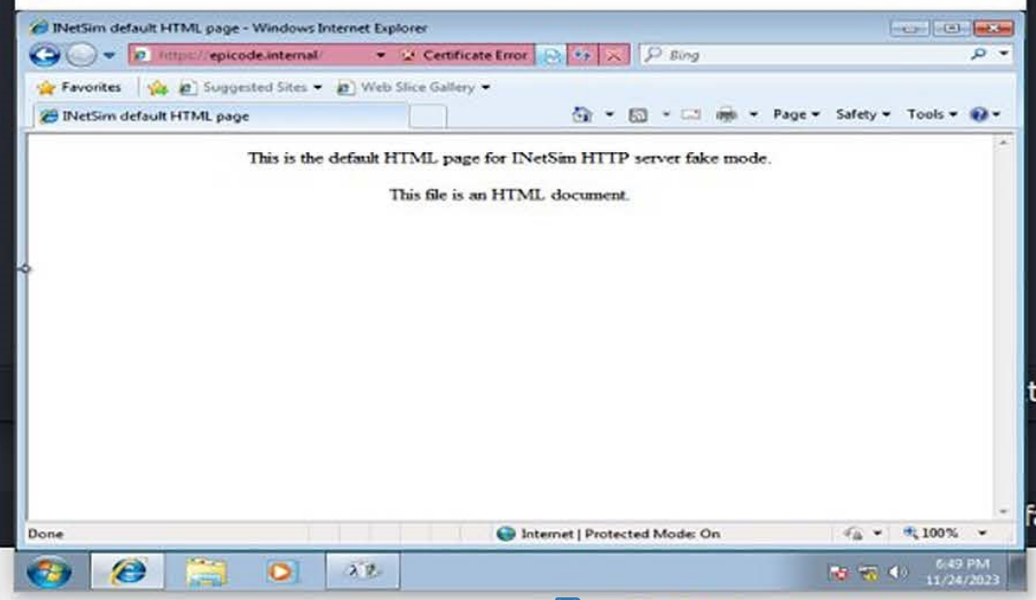
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.32.101	192.168.32.100	TCP	66	49172 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PE
2	0.000113063	192.168.32.100	192.168.32.101	TCP	66	443 → 49172 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
3	0.000622514	192.168.32.101	192.168.32.100	TCP	60	49172 → 443 [ACK] Seq=1 Ack=1 Win=65700 Len=0
4	0.002280813	192.168.32.101	192.168.32.100	TLSv1	215	Client Hello
5	0.002337380	192.168.32.100	192.168.32.101	TCP	54	443 → 49172 [ACK] Seq=1 Ack=162 Win=64128 Len=0
6	0.091240852	192.168.32.100	192.168.32.101	TLSv1	1373	Server Hello, Certificate, Server Key Exchange, Server Hello
7	0.103868547	192.168.32.101	192.168.32.100	TLSv1	188	Client Key Exchange, Change Cipher Spec, Encrypted Handshake
8	0.103944765	192.168.32.100	192.168.32.101	TCP	54	443 → 49172 [ACK] Seq=1320 Ack=296 Win=64128 Len=0
9	0.105410870	192.168.32.100	192.168.32.101	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
10	0.117110089	PcsCompu_67:4b:8b	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.101
11	0.301079236	192.168.32.101	192.168.32.100	TCP	60	49172 → 443 [ACK] Seq=296 Ack=1379 Win=64320 Len=0
12	1.052428389	PcsCompu_67:4b:8b	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.101
13	2.051058522	PcsCompu_67:4b:8b	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.101
14	3.259301772	fe80::5530:d90c:baa…	ff02::1:3	LLMNR	84	Standard query 0xc605 A wpad
15	3.259499225	192.168.32.101	224.0.0.252	LLMNR	64	Standard query 0xc605 A wpad
16	3.364761121	fe80::5530:d90c:baa…	ff02::1:3	LLMNR	84	Standard query 0xc605 A wpad
17	3.364761828	192.168.32.101	224.0.0.252	LLMNR	64	Standard query 0xc605 A wpad

```
▸ Frame 9: 113 bytes on wire (904 bits), 113 bytes captured (904 bits) on interface eth0, id 0
▾ Ethernet II, Src: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5), Dst: PcsCompu_67:4b:8b (08:00:27:67:4b:8b)
  ▸ Destination: PcsCompu_67:4b:8b (08:00:27:67:4b:8b)
  ▸ Source: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5)
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 192.168.32.100, Dst: 192.168.32.101
▸ Transmission Control Protocol, Src Port: 443, Dst Port: 49172, Seq: 1320, Ack: 296, Len: 59
▾ Transport Layer Security
  ▾ TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
      Content Type: Change Cipher Spec (20)
      Version: TLS 1.0 (0x0301)
      Length: 1
      Change Cipher Spec Message
  ▾ TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 48
      Handshake Protocol: Encrypted Handshake Message
```

wireshark_eth05DHIF2.pcapng

Ready to load or capture

Windows [In esecuzione] - Oracle VM VirtualBox



CTRL (DESTRA)

Il protocollo HTTPS integra l'interazione del protocollo HTTP utilizzando i protocolli SSL (Secure Sockets Layer) o TLS (Transport Layer Security) per proteggere il canale di comunicazione.

Nella cattura fatta con Wireshark, questo è subito visibile in quanto, nella richiesta attraverso HTTPS, differentemente rispetto la stessa cattura con HTTP, è presente il protocollo TLS che tenta di criptare il canale di comuicazione.

Il traffico in HTTP viene invece trasmesso in testo semplice. Ciò significa che tutti i dati scambiati tra il client e il server, comprese le informazioni sensibili come credenziali di accesso o dettagli personali, possono essere facilmente intercettati e letti.