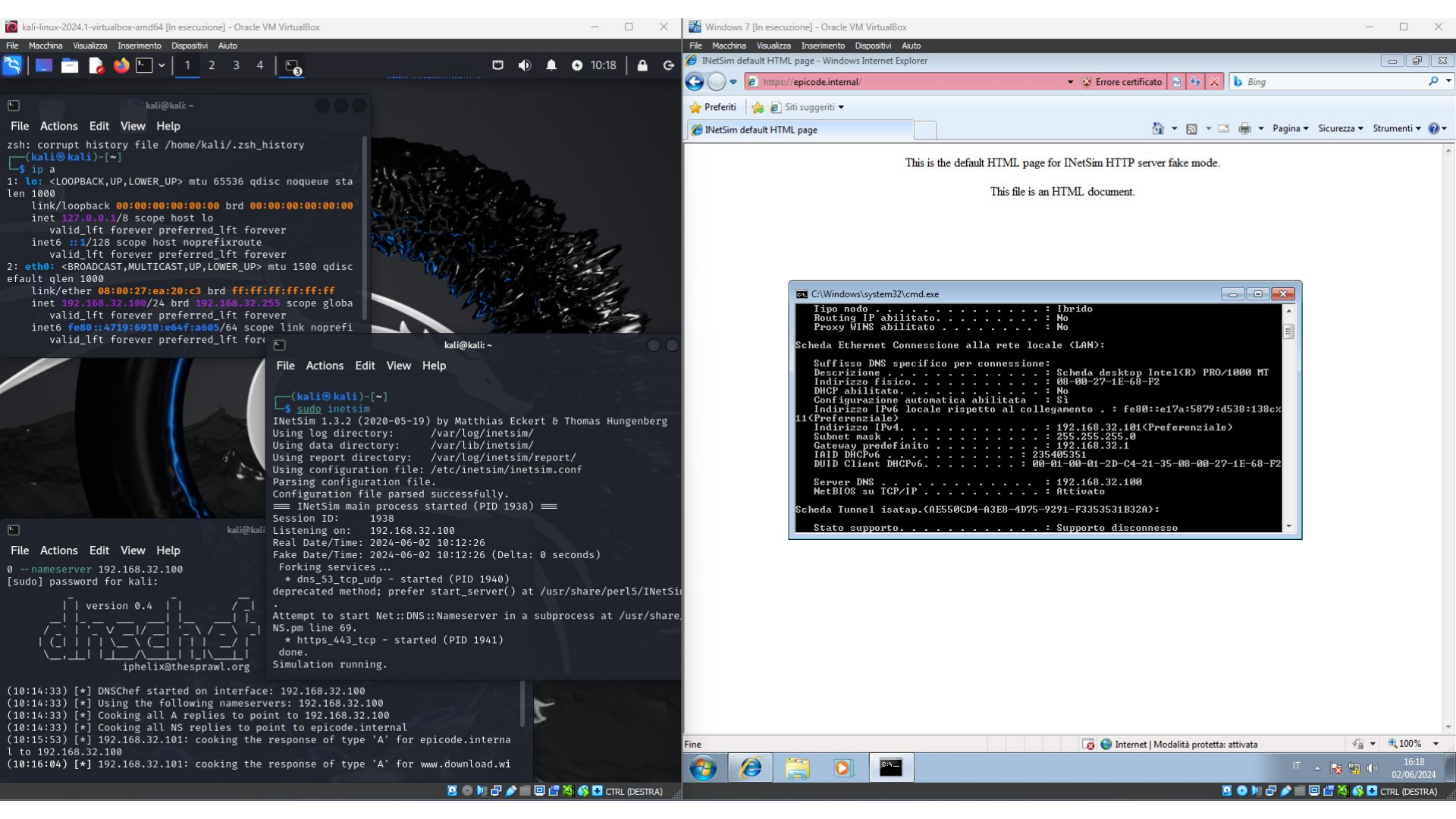

kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
kali@kali: ~
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue sta
len 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
efault qlen 1000
link/ether 08:00:27:ea:20:c3 brd ff:ff:ff:ff:ff:ff
inet 192.168.32.100/24 brd 192.168.32.255 scope globa
valid_lft forever preferred_lft forever
inet6 fe80::4719:6910:e64f:a605/64 scope link noprefi
valid_lft forever preferred_lft fore
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo inetsim
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory: /var/log/inetsim/
Using data directory: /var/lib/inetsim/
Using report directory: /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
=== INetSim main process started (PID 1938) ===
Session ID: 1938
Listening on: 192.168.32.100
Real Date/Time: 2024-06-02 10:12:26
Fake Date/Time: 2024-06-02 10:12:26 (Delta: 0 seconds)
Forking services ...
* dns_53_tcp_udp - started (PID 1940)
deprecated method; prefer start_server() at /usr/share/perl5/INetSi
.
Attempt to start Net::DNS::Nameserver in a subprocess at /usr/share
NS.pm line 69.
* https_443_tcp - started (PID 1941)
done.
Simulation running.
kali@kali
File Actions Edit View Help
0 --nameserver 192.168.32.100
[sudo] password for kali:
version 0.4
iphelix@thesprawl.org
(10:14:33) [*] DNSChef started on interface: 192.168.32.100
(10:14:33) [*] Using the following nameservers: 192.168.32.100
(10:14:33) [*] Cooking all A replies to point to 192.168.32.100
(10:14:33) [*] Cooking all NS replies to point to epicode.internal
(10:15:53) [*] 192.168.32.101: cooking the response of type 'A' for epicode.interna
l to 192.168.32.100
(10:16:04) [*] 192.168.32.101: cooking the response of type 'A' for www.download.wi
CTRL (DESTRA)
Windows 7 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
INetSim default HTML page - Windows Internet Explorer
https://epicode.internal/
Errore certificato
Bing
Preferiti
Siti suggeriti
INetSim default HTML page
Pagina Sicurezza Strumenti
This is the default HTML page for INetSim HTTP server fake mode.
This file is an HTML document.
C:\Windows\system32\cmd.exe
Tipo nodo . . . . . : Ibrido
Routing IP abilitato. . . . . : No
Proxy WINS abilitato . . . . . : No
Scheda Ethernet Connessione alla rete locale (LAN):
Suffisso DNS specifico per connessione:
Descrizione . . . . . : Scheda desktop Intel(R) PRO/1000 MT
Indirizzo fisico. . . . . : 08-00-27-1E-68-F2
DHCP abilitato. . . . . : No
Configurazione automatica abilitata : Sì
Indirizzo IPv6 locale rispetto al collegamento . : fe80::e17a:5879:d538:138c%
11(Preferenziale)
Indirizzo IPv4. . . . . : 192.168.32.101(Preferenziale)
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : 192.168.32.1
IAID DHCPv6 . . . . . : 235405351
DUID Client DHCPv6. . . . . : 00-01-00-01-2D-C4-21-35-08-00-27-1E-68-F2
Server DNS . . . . . : 192.168.32.100
NetBIOS su TCP/IP . . . . . : Attivato
Scheda Tunnel isatap.{AE550CD4-A3E8-4D75-9291-F3353531B32A}:
Stato supporto. . . . . : Supporto disconnesso
Fine
Internet | Modalità protetta: attivata
100%
IT
16:18
02/06/2024
CTRL (DESTRA)

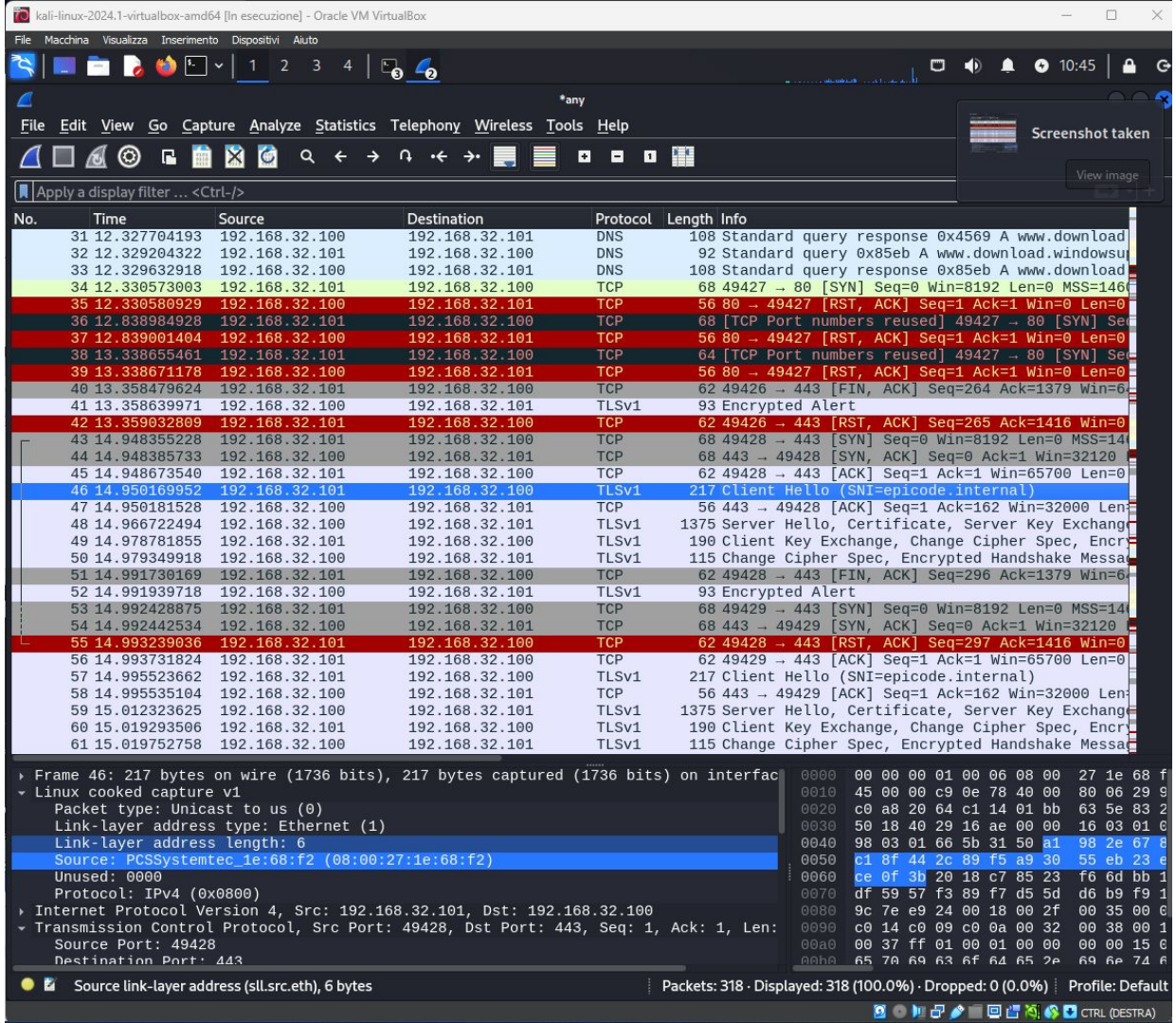
Nella prima slide si nota:

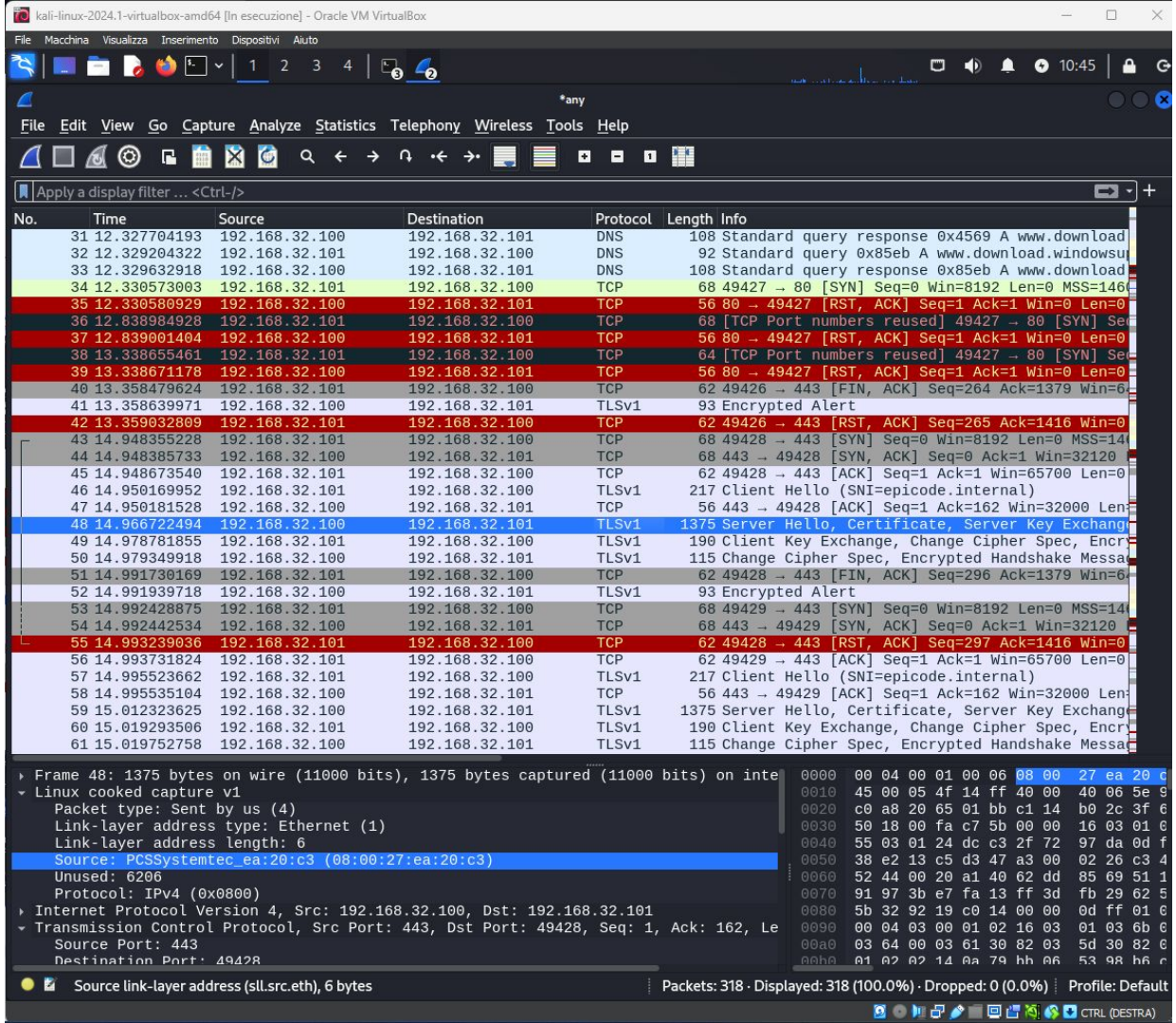
Inetsim

DNSCHEF

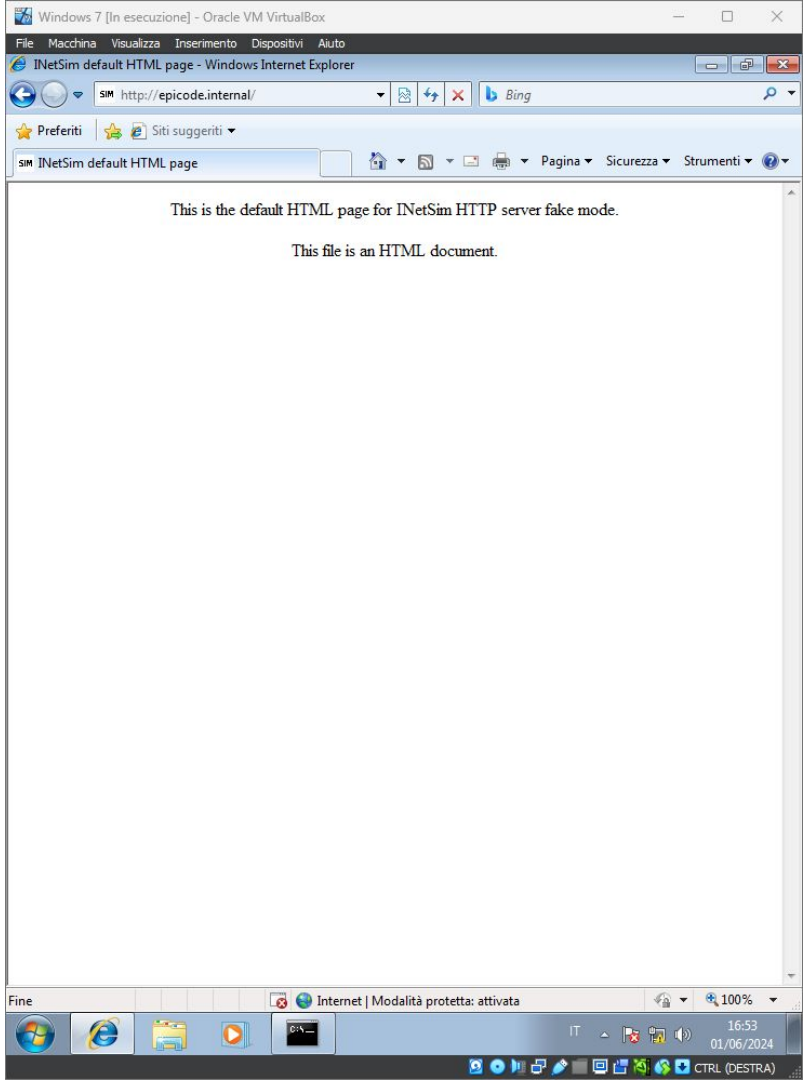
MAC e IP delle macchine

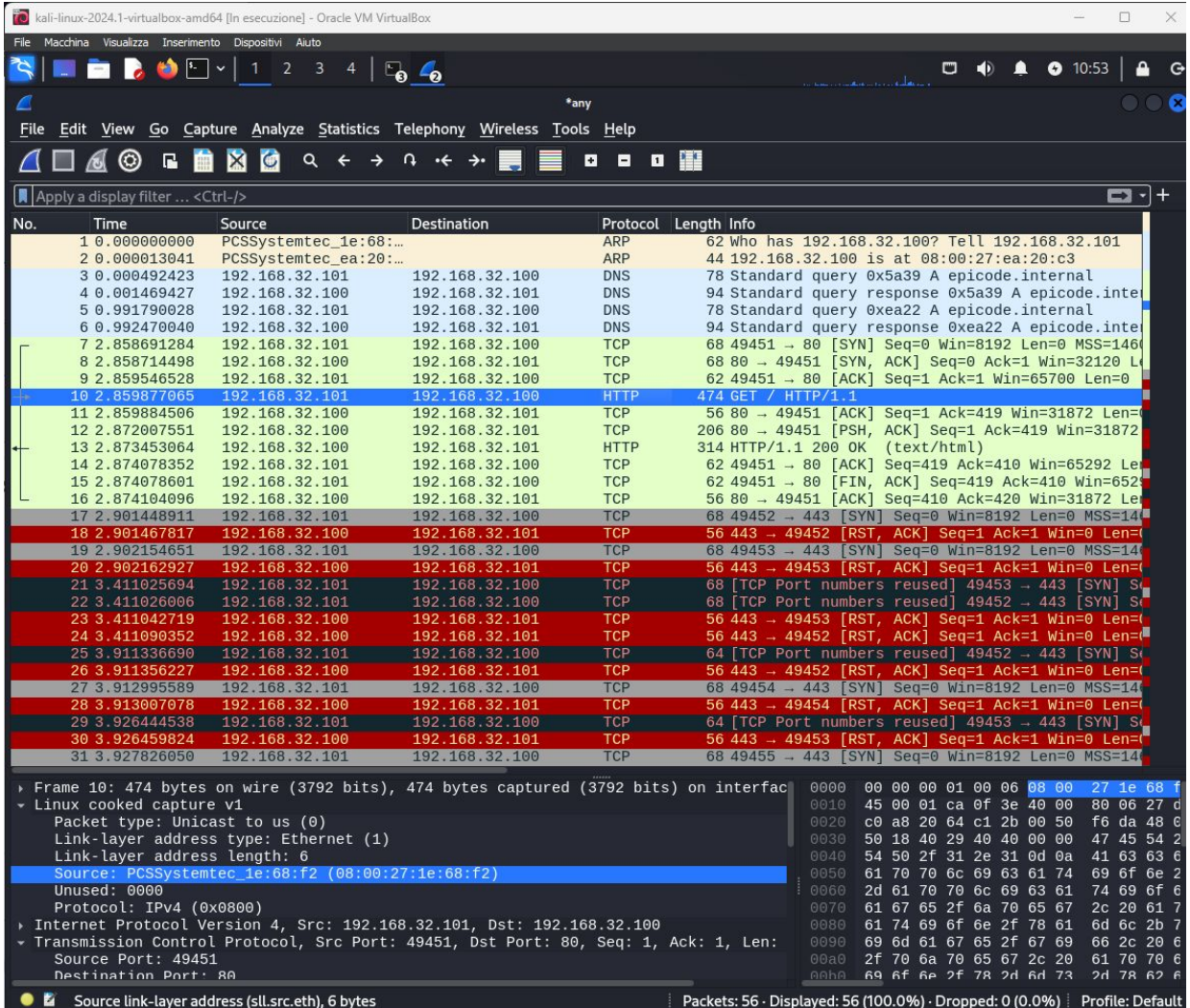
https://epicode.internal

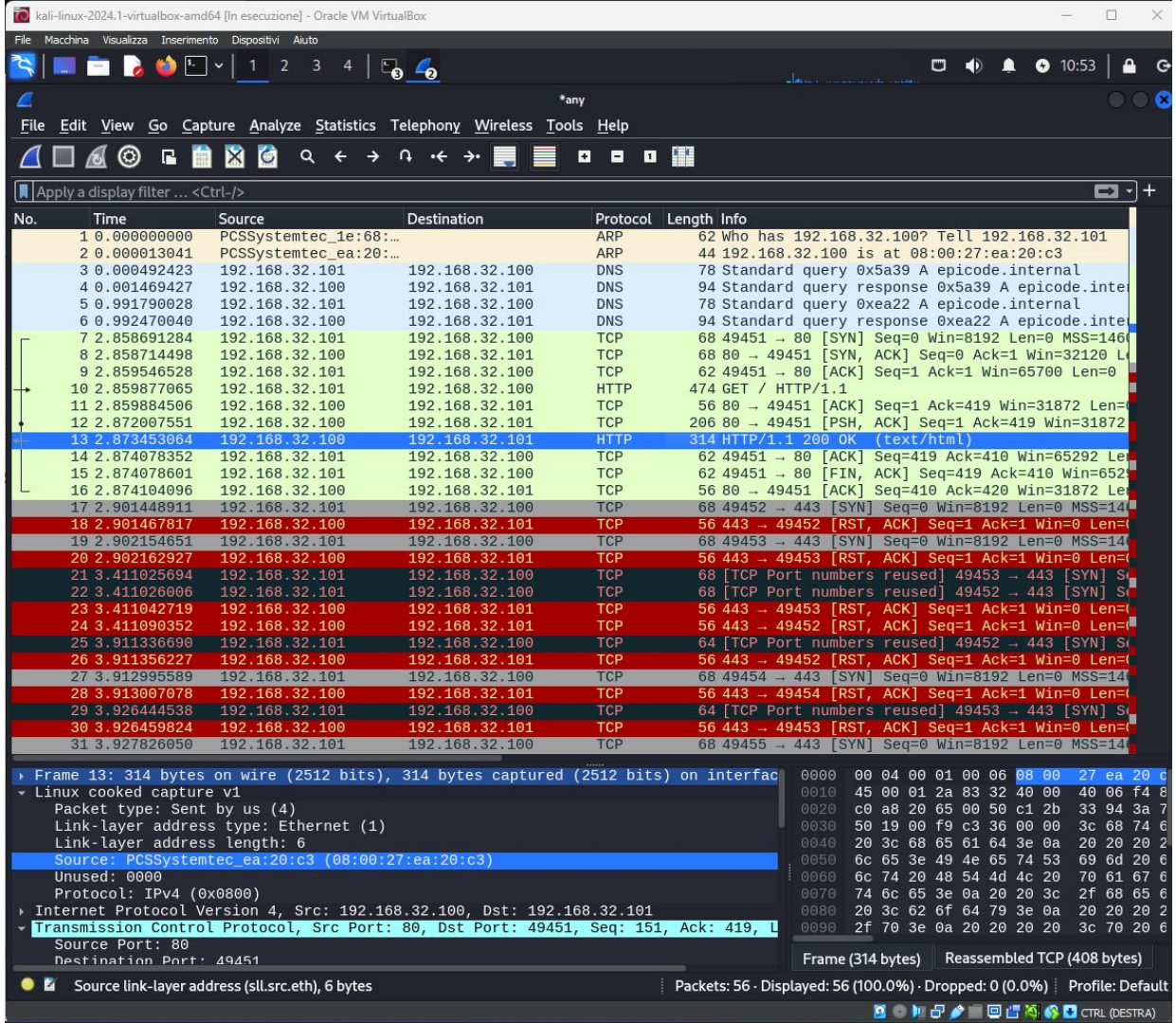

kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
10:45
*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Screenshot taken
View image
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
31 12.327704193 192.168.32.100 192.168.32.101 DNS 108 Standard query response 0x4569 A www.download
32 12.329204322 192.168.32.101 192.168.32.100 DNS 92 Standard query 0x85eb A www.download.windowsu
33 12.329632918 192.168.32.100 192.168.32.101 DNS 108 Standard query response 0x85eb A www.download
34 12.330573003 192.168.32.101 192.168.32.100 TCP 68 49427 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=146
35 12.330580929 192.168.32.100 192.168.32.101 TCP 56 80 → 49427 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
36 12.838984928 192.168.32.101 192.168.32.100 TCP 68 [TCP Port numbers reused] 49427 → 80 [SYN] Se
37 12.839001404 192.168.32.100 192.168.32.101 TCP 56 80 → 49427 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
38 13.338655461 192.168.32.101 192.168.32.100 TCP 64 [TCP Port numbers reused] 49427 → 80 [SYN] Se
39 13.338671178 192.168.32.100 192.168.32.101 TCP 56 80 → 49427 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
40 13.358479624 192.168.32.101 192.168.32.100 TCP 62 49426 → 443 [FIN, ACK] Seq=264 Ack=1379 Win=6
41 13.358639971 192.168.32.100 192.168.32.101 TLSv1 93 Encrypted Alert
42 13.359032809 192.168.32.101 192.168.32.100 TCP 62 49426 → 443 [RST, ACK] Seq=265 Ack=1416 Win=0
43 14.948355228 192.168.32.101 192.168.32.100 TCP 68 49428 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=14
44 14.948385733 192.168.32.100 192.168.32.101 TCP 68 443 → 49428 [SYN, ACK] Seq=0 Ack=1 Win=32120
45 14.948673540 192.168.32.101 192.168.32.100 TCP 62 49428 → 443 [ACK] Seq=1 Ack=1 Win=65700 Len=0
46 14.950169952 192.168.32.101 192.168.32.100 TLSv1 217 Client Hello (SNI=epicode.internal)
47 14.950181528 192.168.32.100 192.168.32.101 TCP 56 443 → 49428 [ACK] Seq=1 Ack=162 Win=32000 Len
48 14.966722494 192.168.32.100 192.168.32.101 TLSv1 1375 Server Hello, Certificate, Server Key Exchang
49 14.978781855 192.168.32.101 192.168.32.100 TLSv1 190 Client Key Exchange, Change Cipher Spec, Encr
50 14.979349918 192.168.32.100 192.168.32.101 TLSv1 115 Change Cipher Spec, Encrypted Handshake Messa
51 14.991730169 192.168.32.101 192.168.32.100 TCP 62 49428 → 443 [FIN, ACK] Seq=296 Ack=1379 Win=6
52 14.991939718 192.168.32.100 192.168.32.101 TLSv1 93 Encrypted Alert
53 14.992428875 192.168.32.101 192.168.32.100 TCP 68 49429 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=14
54 14.992442534 192.168.32.100 192.168.32.101 TCP 68 443 → 49429 [SYN, ACK] Seq=0 Ack=1 Win=32120
55 14.993239036 192.168.32.101 192.168.32.100 TCP 62 49428 → 443 [RST, ACK] Seq=297 Ack=1416 Win=0
56 14.993731824 192.168.32.101 192.168.32.100 TCP 62 49429 → 443 [ACK] Seq=1 Ack=1 Win=65700 Len=0
57 14.995523662 192.168.32.101 192.168.32.100 TLSv1 217 Client Hello (SNI=epicode.internal)
58 14.995535104 192.168.32.100 192.168.32.101 TCP 56 443 → 49429 [ACK] Seq=1 Ack=162 Win=32000 Len
59 15.012323625 192.168.32.100 192.168.32.101 TLSv1 1375 Server Hello, Certificate, Server Key Exchang
60 15.019293506 192.168.32.101 192.168.32.100 TLSv1 190 Client Key Exchange, Change Cipher Spec, Encr
61 15.019752758 192.168.32.100 192.168.32.101 TLSv1 115 Change Cipher Spec, Encrypted Handshake Messa
Frame 46: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interfac
Linux cooked capture v1
Packet type: Unicast to us (0)
Link-layer address type: Ethernet (1)
Link-layer address length: 6
Source: PCSSystemtec_1e:68:f2 (08:00:27:1e:68:f2)
Unused: 0000
Protocol: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100
Transmission Control Protocol, Src Port: 49428, Dst Port: 443, Seq: 1, Ack: 1, Len:
Source Port: 49428
Destination Port: 443
0000 00 00 00 01 00 06 08 00 27 1e 68 f
0010 45 00 00 c9 0e 78 40 00 80 06 29 9
0020 c0 a8 20 64 c1 14 01 bb 63 5e 83 2
0030 50 18 40 29 16 ae 00 00 16 03 01 0
0040 98 03 01 66 5b 31 50 a1 98 2e 67 8
0050 c1 8f 44 2c 89 f5 a9 30 55 eb 23 e
0060 ce 0f 3b 20 18 c7 85 23 f6 6d bb 1
0070 df 59 57 f3 89 f7 d5 5d d6 b9 f9 1
0080 9c 7e e9 24 00 18 00 2f 00 35 00 0
0090 c0 14 c0 09 c0 0a 00 32 00 38 00 1
00a0 00 37 ff 01 00 01 00 00 00 00 15 0
00b0 65 70 69 63 6f 64 65 2e 69 6e 74 6
Source link-layer address (sll.src.eth), 6 bytes
Packets: 318 · Displayed: 318 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
CTRL (DESTRA)


kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
10:45
*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
31 12.327704193 192.168.32.100 192.168.32.101 DNS 108 Standard query response 0x4569 A www.download
32 12.329204322 192.168.32.101 192.168.32.100 DNS 92 Standard query 0x85eb A www.download.windowsu
33 12.329632918 192.168.32.100 192.168.32.101 DNS 108 Standard query response 0x85eb A www.download
34 12.330573003 192.168.32.101 192.168.32.100 TCP 68 49427 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=146
35 12.330580929 192.168.32.100 192.168.32.101 TCP 56 80 → 49427 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
36 12.838984928 192.168.32.101 192.168.32.100 TCP 68 [TCP Port numbers reused] 49427 → 80 [SYN] Se
37 12.839001404 192.168.32.100 192.168.32.101 TCP 56 80 → 49427 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
38 13.338655461 192.168.32.101 192.168.32.100 TCP 64 [TCP Port numbers reused] 49427 → 80 [SYN] Se
39 13.338671178 192.168.32.100 192.168.32.101 TCP 56 80 → 49427 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
40 13.358479624 192.168.32.101 192.168.32.100 TCP 62 49426 → 443 [FIN, ACK] Seq=264 Ack=1379 Win=6
41 13.358639971 192.168.32.100 192.168.32.101 TLSv1 93 Encrypted Alert
42 13.359032809 192.168.32.101 192.168.32.100 TCP 62 49426 → 443 [RST, ACK] Seq=265 Ack=1416 Win=0
43 14.948355228 192.168.32.101 192.168.32.100 TCP 68 49428 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=14
44 14.948385733 192.168.32.100 192.168.32.101 TCP 68 443 → 49428 [SYN, ACK] Seq=0 Ack=1 Win=32120
45 14.948673540 192.168.32.101 192.168.32.100 TCP 62 49428 → 443 [ACK] Seq=1 Ack=1 Win=65700 Len=0
46 14.950169952 192.168.32.101 192.168.32.100 TLSv1 217 Client Hello (SNI=epicode.internal)
47 14.950181528 192.168.32.100 192.168.32.101 TCP 56 443 → 49428 [ACK] Seq=1 Ack=162 Win=32000 Len
48 14.966722494 192.168.32.100 192.168.32.101 TLSv1 1375 Server Hello, Certificate, Server Key Exchang
49 14.978781855 192.168.32.101 192.168.32.100 TLSv1 190 Client Key Exchange, Change Cipher Spec, Encr
50 14.979349918 192.168.32.100 192.168.32.101 TLSv1 115 Change Cipher Spec, Encrypted Handshake Messa
51 14.991730169 192.168.32.101 192.168.32.100 TCP 62 49428 → 443 [FIN, ACK] Seq=296 Ack=1379 Win=6
52 14.991939718 192.168.32.100 192.168.32.101 TLSv1 93 Encrypted Alert
53 14.992428875 192.168.32.101 192.168.32.100 TCP 68 49429 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=14
54 14.992442534 192.168.32.100 192.168.32.101 TCP 68 443 → 49429 [SYN, ACK] Seq=0 Ack=1 Win=32120
55 14.993239036 192.168.32.100 192.168.32.101 TCP 62 49428 → 443 [RST, ACK] Seq=297 Ack=1416 Win=0
56 14.993731824 192.168.32.101 192.168.32.100 TCP 62 49429 → 443 [ACK] Seq=1 Ack=1 Win=65700 Len=0
57 14.995523662 192.168.32.101 192.168.32.100 TLSv1 217 Client Hello (SNI=epicode.internal)
58 14.995535104 192.168.32.100 192.168.32.101 TCP 56 443 → 49429 [ACK] Seq=1 Ack=162 Win=32000 Len
59 15.012323625 192.168.32.100 192.168.32.101 TLSv1 1375 Server Hello, Certificate, Server Key Exchang
60 15.019293506 192.168.32.101 192.168.32.100 TLSv1 190 Client Key Exchange, Change Cipher Spec, Encr
61 15.019752758 192.168.32.100 192.168.32.101 TLSv1 115 Change Cipher Spec, Encrypted Handshake Messa
Frame 48: 1375 bytes on wire (11000 bits), 1375 bytes captured (11000 bits) on inte
Linux cooked capture v1
Packet type: Sent by us (4)
Link-layer address type: Ethernet (1)
Link-layer address length: 6
Source: PCSSystemtec_ea:20:c3 (08:00:27:ea:20:c3)
Unused: 6206
Protocol: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.32.100, Dst: 192.168.32.101
Transmission Control Protocol, Src Port: 443, Dst Port: 49428, Seq: 1, Ack: 162, Le
Source Port: 443
Destination Port: 49428
0000 00 04 00 01 00 06 08 00 27 ea 20 c
0010 45 00 05 4f 14 ff 40 00 40 06 5e 9
0020 c0 a8 20 65 01 bb c1 14 b0 2c 3f 6
0030 50 18 00 fa c7 5b 00 00 16 03 01 0
0040 55 03 01 24 dc c3 2f 72 97 da 0d f
0050 38 e2 13 c5 d3 47 a3 00 02 26 c3 4
0060 52 44 00 20 a1 40 62 dd 85 69 51 1
0070 91 97 3b e7 fa 13 ff 3d fb 29 62 5
0080 5b 32 92 19 c0 14 00 00 0d ff 01 0
0090 00 04 03 00 01 02 16 03 01 03 6b 0
00a0 03 64 00 03 61 30 82 03 5d 30 82 0
00b0 01 02 02 14 0a 79 bb 06 53 98 b6 c
Source link-layer address (sll.src.eth), 6 bytes
Packets: 318 · Displayed: 318 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
CTRL (DESTRA)

Si nota che è HTTPS in quanto è criptata visto che dopo il three -way-handshake (SYN,SYN-ACK,ACK) vengono scambiati i pacchetti TLSv1(Transport Layer Security) dopo di ciò si scambiano la chiave


Windows 7 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
INetSim default HTML page - Windows Internet Explorer
http://epicode.internal/
Bing
Preferiti
Siti suggeriti
INetSim default HTML page
Pagina Sicurezza Strumenti
This is the default HTML page for INetSim HTTP server fake mode.
This file is an HTML document.
Fine
Internet | Modalità protetta: attivata
100%
IT
16:53
01/06/2024
CTRL (DESTRA)


kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
10:53
*any
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 PCSSystemtec_1e:68:... ARP 62 Who has 192.168.32.100? Tell 192.168.32.101
2 0.000013041 PCSSystemtec_ea:20:... ARP 44 192.168.32.100 is at 08:00:27:ea:20:c3
3 0.000492423 192.168.32.101 192.168.32.100 DNS 78 Standard query 0x5a39 A epicode.internal
4 0.001469427 192.168.32.100 192.168.32.101 DNS 94 Standard query response 0x5a39 A epicode.inte
5 0.991790028 192.168.32.101 192.168.32.100 DNS 78 Standard query 0xea22 A epicode.internal
6 0.992470040 192.168.32.100 192.168.32.101 DNS 94 Standard query response 0xea22 A epicode.inte
7 2.858691284 192.168.32.101 192.168.32.100 TCP 68 49451 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=146
8 2.858714498 192.168.32.100 192.168.32.101 TCP 68 80 → 49451 [SYN, ACK] Seq=0 Ack=1 Win=32120 L
9 2.859546528 192.168.32.101 192.168.32.100 TCP 62 49451 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
10 2.859877065 192.168.32.101 192.168.32.100 HTTP 474 GET / HTTP/1.1
11 2.859884506 192.168.32.100 192.168.32.101 TCP 56 80 → 49451 [ACK] Seq=1 Ack=419 Win=31872 Len=
12 2.872007551 192.168.32.100 192.168.32.101 TCP 206 80 → 49451 [PSH, ACK] Seq=1 Ack=419 Win=31872
13 2.873453064 192.168.32.100 192.168.32.101 HTTP 314 HTTP/1.1 200 OK (text/html)
14 2.874078352 192.168.32.101 192.168.32.100 TCP 62 49451 → 80 [ACK] Seq=419 Ack=410 Win=65292 Le
15 2.874078601 192.168.32.101 192.168.32.100 TCP 62 49451 → 80 [FIN, ACK] Seq=419 Ack=410 Win=652
16 2.874104096 192.168.32.100 192.168.32.101 TCP 56 80 → 49451 [ACK] Seq=410 Ack=420 Win=31872 Le
17 2.901448911 192.168.32.101 192.168.32.100 TCP 68 49452 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=14
18 2.901467817 192.168.32.100 192.168.32.101 TCP 56 443 → 49452 [RST, ACK] Seq=1 Ack=1 Win=0 Len=
19 2.902154651 192.168.32.101 192.168.32.100 TCP 68 49453 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=14
20 2.902162927 192.168.32.100 192.168.32.101 TCP 56 443 → 49453 [RST, ACK] Seq=1 Ack=1 Win=0 Len=
21 3.411025694 192.168.32.101 192.168.32.100 TCP 68 [TCP Port numbers reused] 49453 → 443 [SYN] S
22 3.411026006 192.168.32.101 192.168.32.100 TCP 68 [TCP Port numbers reused] 49452 → 443 [SYN] S
23 3.411042719 192.168.32.100 192.168.32.101 TCP 56 443 → 49453 [RST, ACK] Seq=1 Ack=1 Win=0 Len=
24 3.411090352 192.168.32.100 192.168.32.101 TCP 56 443 → 49452 [RST, ACK] Seq=1 Ack=1 Win=0 Len=
25 3.911336690 192.168.32.101 192.168.32.100 TCP 64 [TCP Port numbers reused] 49452 → 443 [SYN] S
26 3.911356227 192.168.32.100 192.168.32.101 TCP 56 443 → 49452 [RST, ACK] Seq=1 Ack=1 Win=0 Len=
27 3.912995589 192.168.32.101 192.168.32.100 TCP 68 49454 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=14
28 3.913007078 192.168.32.100 192.168.32.101 TCP 56 443 → 49454 [RST, ACK] Seq=1 Ack=1 Win=0 Len=
29 3.926444538 192.168.32.101 192.168.32.100 TCP 64 [TCP Port numbers reused] 49453 → 443 [SYN] S
30 3.926459824 192.168.32.100 192.168.32.101 TCP 56 443 → 49453 [RST, ACK] Seq=1 Ack=1 Win=0 Len=
31 3.927826050 192.168.32.101 192.168.32.100 TCP 68 49455 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=14
Frame 10: 474 bytes on wire (3792 bits), 474 bytes captured (3792 bits) on interfac
Linux cooked capture v1
Packet type: Unicast to us (0)
Link-layer address type: Ethernet (1)
Link-layer address length: 6
Source: PCSSystemtec_1e:68:f2 (08:00:27:1e:68:f2)
Unused: 0000
Protocol: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100
Transmission Control Protocol, Src Port: 49451, Dst Port: 80, Seq: 1, Ack: 1, Len:
Source Port: 49451
Destination Port: 80
0000 00 00 00 01 00 06 08 00 27 1e 68 f
0010 45 00 01 ca 0f 3e 40 00 80 06 27 d
0020 c0 a8 20 64 c1 2b 00 50 f6 da 48 6
0030 50 18 40 29 40 40 00 00 47 45 54 2
0040 54 50 2f 31 2e 31 0d 0a 41 63 63 6
0050 61 70 70 6c 69 63 61 74 69 6f 6e 2
0060 2d 61 70 70 6c 69 63 61 74 69 6f 6
0070 61 67 65 2f 6a 70 65 67 2c 20 61 7
0080 61 74 69 6f 6e 2f 78 61 6d 6c 2b 7
0090 69 6d 61 67 65 2f 67 69 66 2c 20 6
00a0 2f 70 6a 70 65 67 2c 20 61 70 70 6
Source link-layer address (sll.src.eth), 6 bytes
Packets: 56 · Displayed: 56 (100.0%) · Dropped: 0 (0.0%)
Profile: Default


kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
10:53
*any
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 PCSSystemtec_1e:68:... ARP 62 Who has 192.168.32.100? Tell 192.168.32.101
2 0.000013041 PCSSystemtec_ea:20:... ARP 44 192.168.32.100 is at 08:00:27:ea:20:c3
3 0.000492423 192.168.32.101 192.168.32.100 DNS 78 Standard query 0x5a39 A epicode.internal
4 0.001469427 192.168.32.100 192.168.32.101 DNS 94 Standard query response 0x5a39 A epicode.inte
5 0.991790028 192.168.32.101 192.168.32.100 DNS 78 Standard query 0xea22 A epicode.internal
6 0.992470040 192.168.32.100 192.168.32.101 DNS 94 Standard query response 0xea22 A epicode.inte
7 2.858691284 192.168.32.101 192.168.32.100 TCP 68 49451 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=146
8 2.858714498 192.168.32.100 192.168.32.101 TCP 68 80 → 49451 [SYN, ACK] Seq=0 Ack=1 Win=32120 L
9 2.859546528 192.168.32.101 192.168.32.100 TCP 62 49451 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
10 2.859877065 192.168.32.101 192.168.32.100 HTTP 474 GET / HTTP/1.1
11 2.859884506 192.168.32.100 192.168.32.101 TCP 56 80 → 49451 [ACK] Seq=1 Ack=419 Win=31872 Len=
12 2.872007551 192.168.32.100 192.168.32.101 TCP 206 80 → 49451 [PSH, ACK] Seq=1 Ack=419 Win=31872
13 2.873453064 192.168.32.100 192.168.32.101 HTTP 314 HTTP/1.1 200 OK (text/html)
14 2.874078352 192.168.32.101 192.168.32.100 TCP 62 49451 → 80 [ACK] Seq=419 Ack=410 Win=65292 Le
15 2.874078601 192.168.32.101 192.168.32.100 TCP 62 49451 → 80 [FIN, ACK] Seq=419 Ack=410 Win=652
16 2.874104096 192.168.32.100 192.168.32.101 TCP 56 80 → 49451 [ACK] Seq=410 Ack=420 Win=31872 Le
17 2.901448911 192.168.32.101 192.168.32.100 TCP 68 49452 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=14
18 2.901467817 192.168.32.100 192.168.32.101 TCP 56 443 → 49452 [RST, ACK] Seq=1 Ack=1 Win=0 Len=
19 2.902154651 192.168.32.101 192.168.32.100 TCP 68 49453 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=14
20 2.902162927 192.168.32.100 192.168.32.101 TCP 56 443 → 49453 [RST, ACK] Seq=1 Ack=1 Win=0 Len=
21 3.411025694 192.168.32.101 192.168.32.100 TCP 68 [TCP Port numbers reused] 49453 → 443 [SYN] S
22 3.411026006 192.168.32.101 192.168.32.100 TCP 68 [TCP Port numbers reused] 49452 → 443 [SYN] S
23 3.411042719 192.168.32.100 192.168.32.101 TCP 56 443 → 49453 [RST, ACK] Seq=1 Ack=1 Win=0 Len=
24 3.411090352 192.168.32.100 192.168.32.101 TCP 56 443 → 49452 [RST, ACK] Seq=1 Ack=1 Win=0 Len=
25 3.911336690 192.168.32.101 192.168.32.100 TCP 64 [TCP Port numbers reused] 49452 → 443 [SYN] S
26 3.911356227 192.168.32.100 192.168.32.101 TCP 56 443 → 49452 [RST, ACK] Seq=1 Ack=1 Win=0 Len=
27 3.912995589 192.168.32.101 192.168.32.100 TCP 68 49454 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=14
28 3.913007078 192.168.32.100 192.168.32.101 TCP 56 443 → 49454 [RST, ACK] Seq=1 Ack=1 Win=0 Len=
29 3.926444538 192.168.32.101 192.168.32.100 TCP 64 [TCP Port numbers reused] 49453 → 443 [SYN] S
30 3.926459824 192.168.32.100 192.168.32.101 TCP 56 443 → 49453 [RST, ACK] Seq=1 Ack=1 Win=0 Len=
31 3.927826050 192.168.32.101 192.168.32.100 TCP 68 49455 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=14
Frame 13: 314 bytes on wire (2512 bits), 314 bytes captured (2512 bits) on interfac
Linux cooked capture v1
Packet type: Sent by us (4)
Link-layer address type: Ethernet (1)
Link-layer address length: 6
Source: PCSSystemtec_ea:20:c3 (08:00:27:ea:20:c3)
Unused: 0000
Protocol: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.32.100, Dst: 192.168.32.101
Transmission Control Protocol, Src Port: 80, Dst Port: 49451, Seq: 151, Ack: 419, L
Source Port: 80
Destination Port: 49451
0000 00 04 00 01 00 06 08 00 27 ea 20 c
0010 45 00 01 2a 83 32 40 00 40 06 f4 8
0020 c0 a8 20 65 00 50 c1 2b 33 94 3a 7
0030 50 19 00 f9 c3 36 00 00 3c 68 74 6
0040 20 3c 68 65 61 64 3e 0a 20 20 20 2
0050 6c 65 3e 49 4e 65 74 53 69 6d 20 6
0060 6c 74 20 48 54 4d 4c 20 70 61 67 6
0070 74 6c 65 3e 0a 20 20 3c 2f 68 65 6
0080 20 3c 62 6f 64 79 3e 0a 20 20 20 2
0090 2f 70 3e 0a 20 20 20 20 3c 70 20 6
Frame (314 bytes)
Reassembled TCP (408 bytes)
Source link-layer address (sll.src.eth), 6 bytes
Packets: 56 · Displayed: 56 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
CTRL (DESTRA)

Per quanto riguarda http si nota una richiesta GET e successivamente la risposta del server 200OK.
Analizzando la risposta del server si può vedere il contenuto html di conseguenza non è criptato e quindi HTTP non HTTPS.