W9D1 – Nicholas Di Angelo -

Premesso che il modus operandi del prot. TCP per stabilire una comunicazione è composta da tre step SYN – SYN/ACK – ACK il 3 way hanshake viene sfruttato per capire lo stato della porta aperta o chiusa così da creare un eventuale canale di comunicazione

In questo esercizio abbiamo effettuato tre tipologie di scansioni, usando un tool scan (nmap) ,raccolto nonchè analizzato i dati intercettati da wireshark.

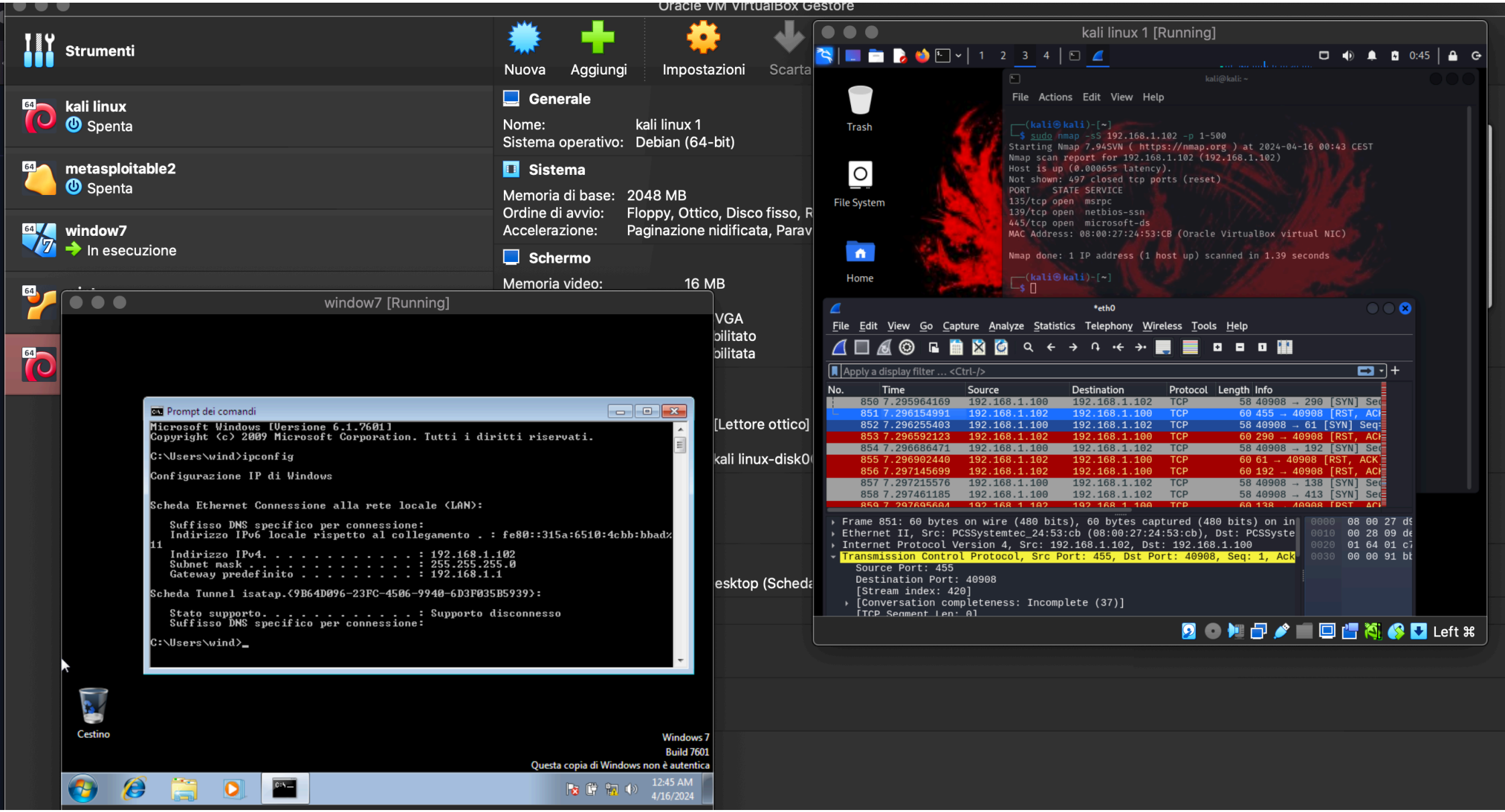
Abbiamo effettuato tre diverse scansioni :

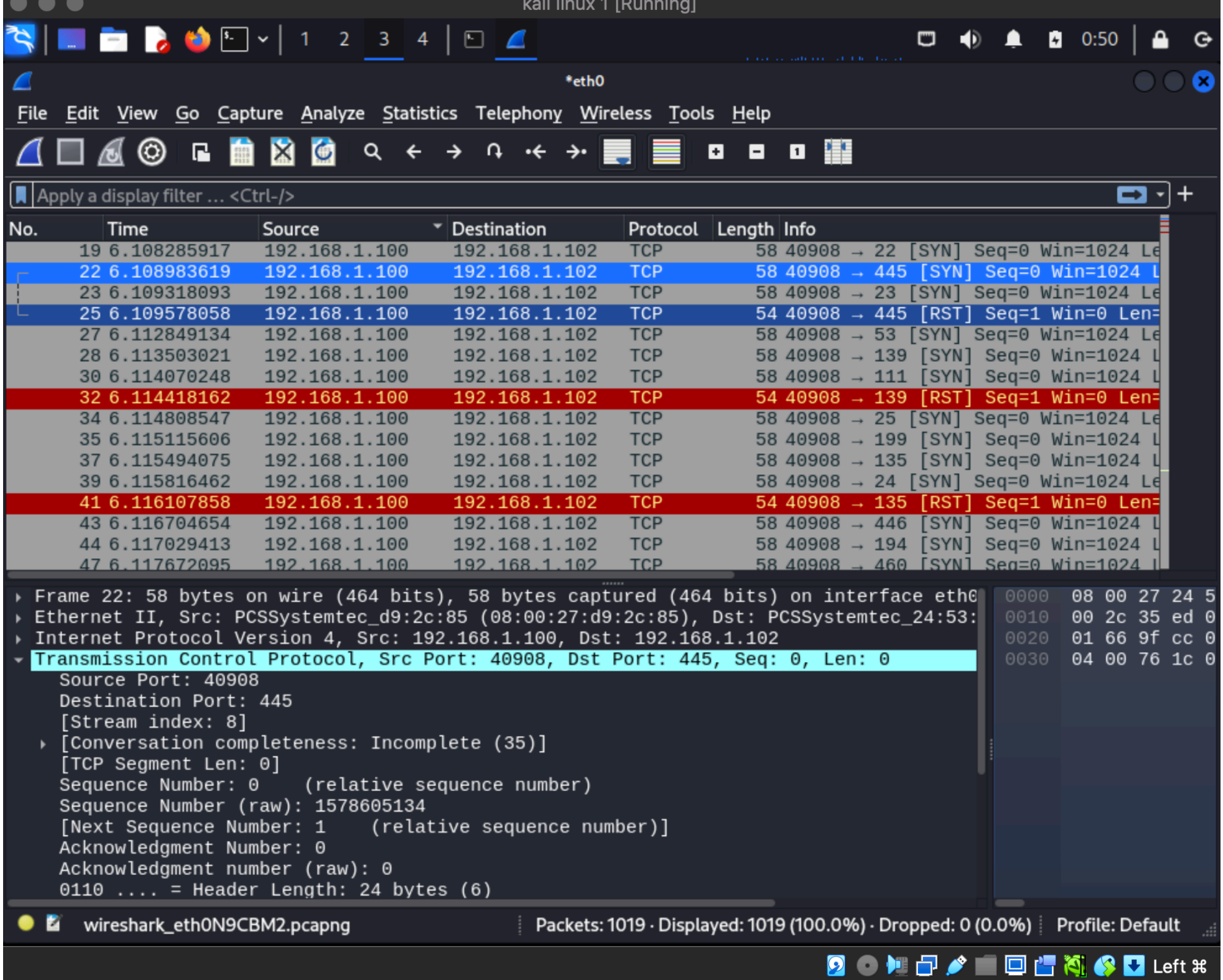
- **Sudo nmap -sS ip -p port range** abbiamo detto al tool di effettuare una scansione non invasiva (SYN , SYN-ACK)prendendo comunque dati utili . Tanto è vero che dall'estrapolazione dei dati dal tool wireshark si evince sulla porta 445 il SYN , SYN/ACK ma non l'Acknowledge finale per la conversazione rimmarrà incopleta per non destare sospetto .

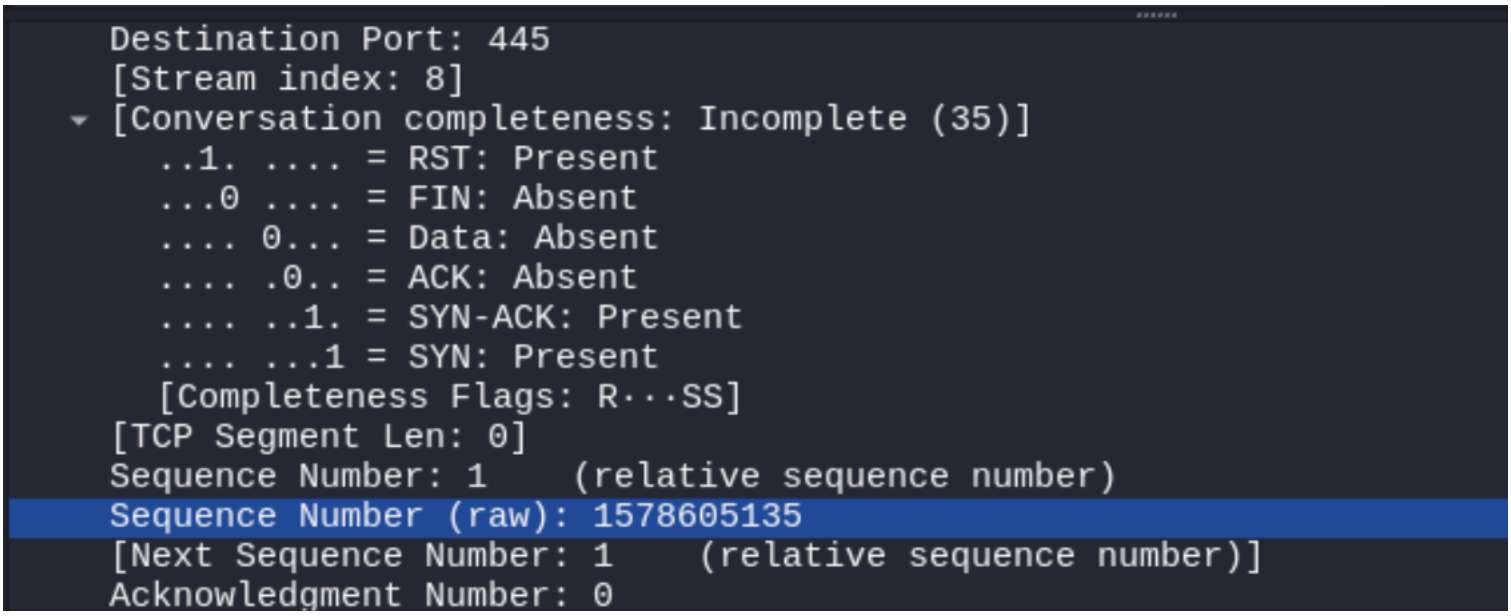
- **Sudo nmap -sT ip -p port range** abbiamo effettuato una scansione invasiva poiché contrariamente a quella sopra abbiamo richiesto alla macchina una comunicazione completa del 3 way hanshake (SYN , SYN/HACK , HACK) stabilendo così un canale di comunicazione . Tanto è vero che con wairshark abbiamo intercettato gli acknowaledge finali e stabilito definitivamente la connessione .

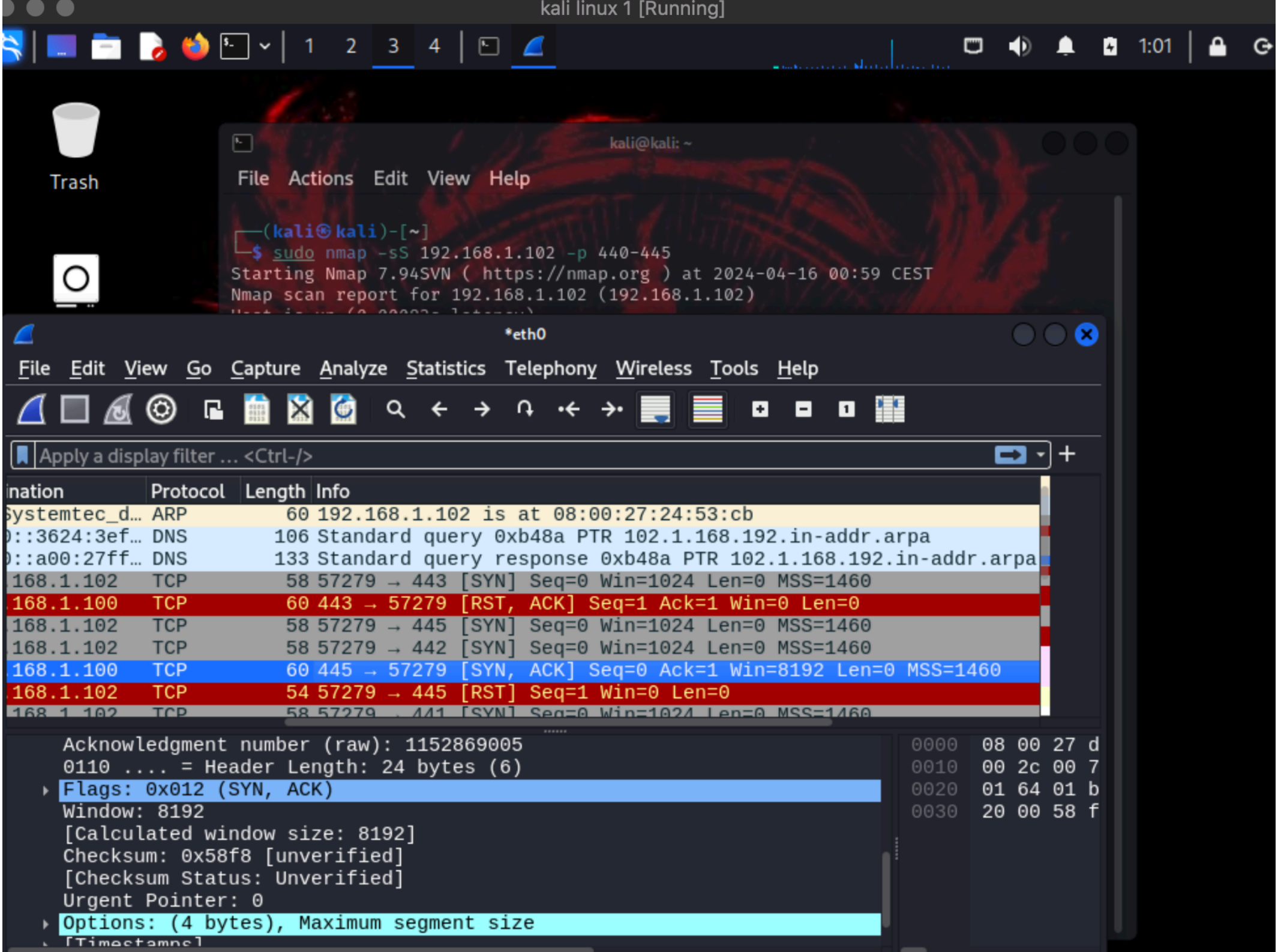
- **Sudo nmap -A ip -p range port** abbiamo raccolto tutti i dati del sistema operativo utilizzato il mac address e ulteriori dati generali utili .

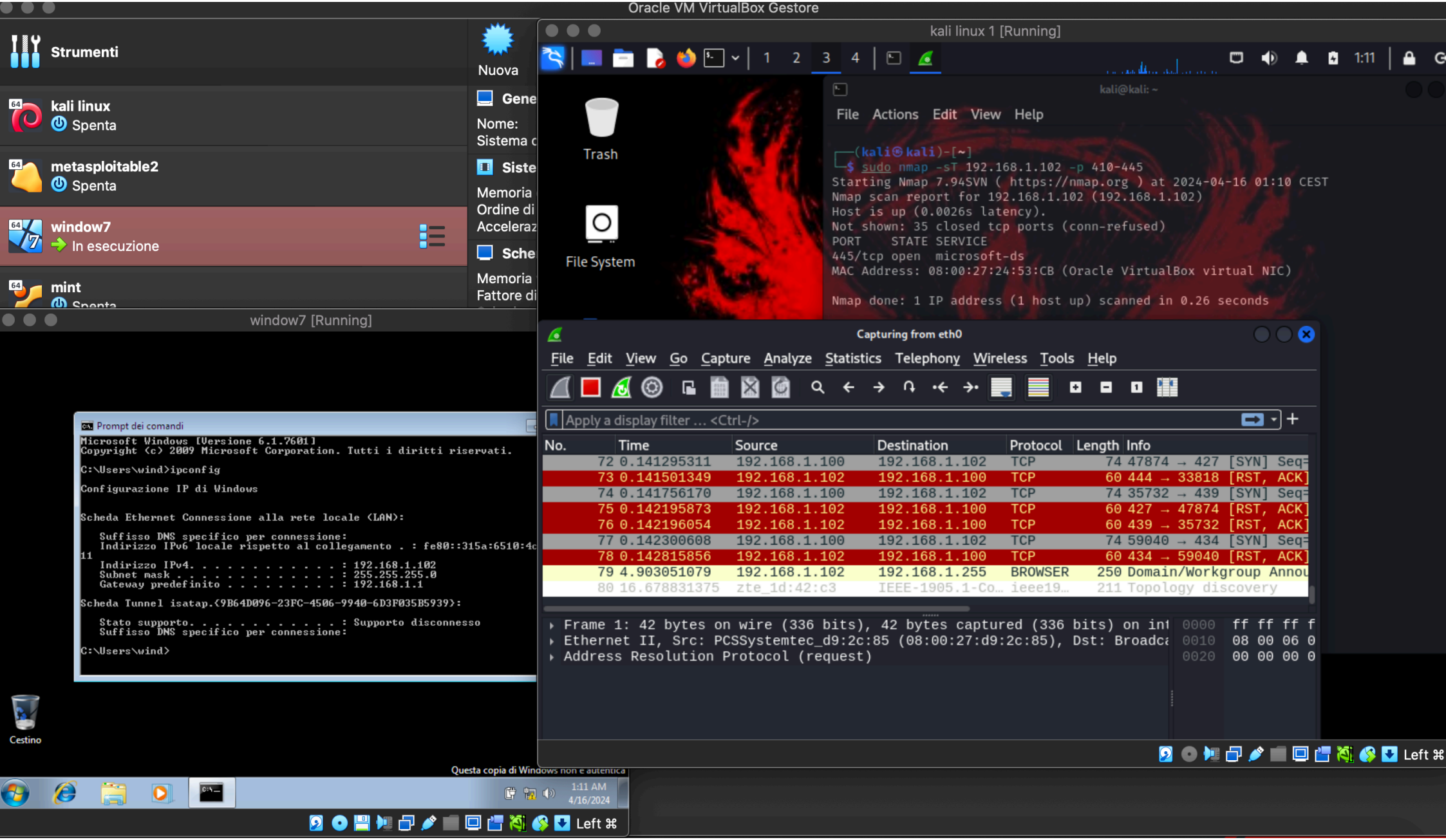
Note finali ho effettuato scan map con range port variabili da 1 a 500 , le porte scannerizzate sono sia porte aperte che chiuse nel mio caso ho preso in considerazione la porta 445 TCP Microsoft.ds pronta per un bel payload .

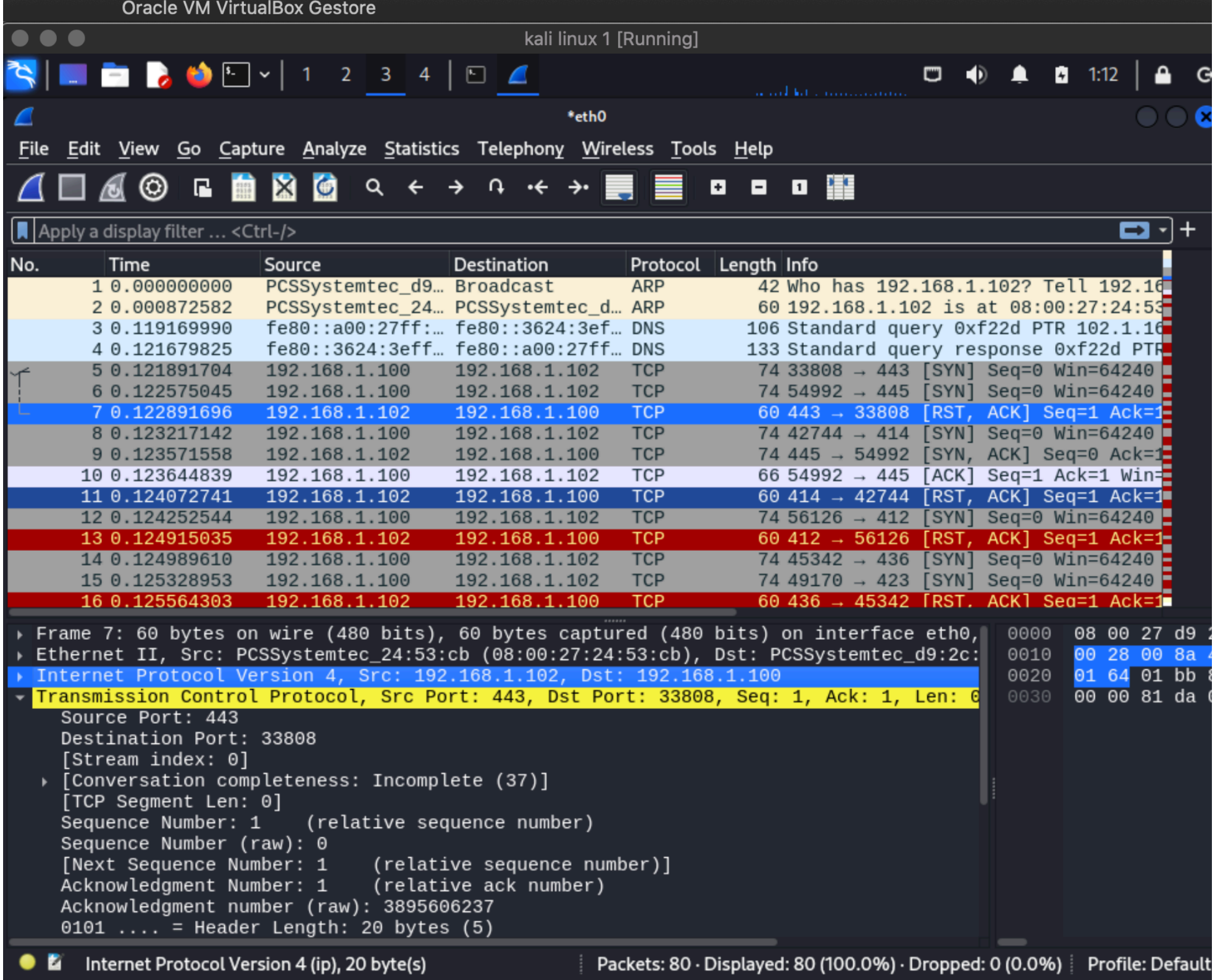

Oracle VM VirtualBox Gestore
Strumenti
kali linux
Spenta
metasploitable2
Spenta
window7
In esecuzione
Nuova
Aggiungi
Impostazioni
Scarta
Generale
Nome: kali linux 1
Sistema operativo: Debian (64-bit)
Sistema
Memoria di base: 2048 MB
Ordine di avvio: Floppy, Ottico, Disco fisso, R
Accelerazione: Paginazione nidificata, Parav
Schermo
Memoria video: 16 MB
VGA
bilitato
bilitata
[Lettore ottico]
kali linux-disk0
esktop (Scheda
window7 [Running]
Prompt dei comandi
Microsoft Windows [Versione 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tutti i diritti riservati.
C:\Users\wind>ipconfig
Configurazione IP di Windows
Scheda Ethernet Connessione alla rete locale (LAN):
Suffisso DNS specifico per connessione:
Indirizzo IPv6 locale rispetto al collegamento . : fe80::315a:6510:4cbb:bbad%
11
Indirizzo IPv4. . . . . : 192.168.1.102
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : 192.168.1.1
Scheda Tunnel isatap.{9B64D096-23FC-4506-9940-6D3F035B5939}:
Stato supporto. . . . . : Supporto disconnesso
Suffisso DNS specifico per connessione:
C:\Users\wind>
Cestino
Windows 7
Build 7601
Questa copia di Windows non è autentica
12:45 AM
4/16/2024
kali linux 1 [Running]
Trash
File System
Home
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo nmap -sS 192.168.1.102 -p 1-500
Starting Nmap 7.94SVN (https://nmap.org) at 2024-04-16 00:43 CEST
Nmap scan report for 192.168.1.102 (192.168.1.102)
Host is up (0.00065s latency).
Not shown: 497 closed tcp ports (reset)
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
MAC Address: 08:00:27:24:53:CB (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 1.39 seconds
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
850 7.295964169 192.168.1.100 192.168.1.102 TCP 58 40908 → 290 [SYN] Seq
851 7.296154991 192.168.1.102 192.168.1.100 TCP 60 455 → 40908 [RST, ACK
852 7.296255403 192.168.1.100 192.168.1.102 TCP 58 40908 → 61 [SYN] Seq
853 7.296592123 192.168.1.102 192.168.1.100 TCP 60 290 → 40908 [RST, ACK
854 7.296686471 192.168.1.100 192.168.1.102 TCP 58 40908 → 192 [SYN] Seq
855 7.296902440 192.168.1.102 192.168.1.100 TCP 60 61 → 40908 [RST, ACK
856 7.297145699 192.168.1.102 192.168.1.100 TCP 60 192 → 40908 [RST, ACK
857 7.297215576 192.168.1.100 192.168.1.102 TCP 58 40908 → 138 [SYN] Seq
858 7.297461185 192.168.1.100 192.168.1.102 TCP 58 40908 → 413 [SYN] Seq
Frame 851: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on in
Ethernet II, Src: PCSSystemtec_24:53:cb (08:00:27:24:53:cb), Dst: PCSSyste
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 192.168.1.100
Transmission Control Protocol, Src Port: 455, Dst Port: 40908, Seq: 1, Ack
Source Port: 455
Destination Port: 40908
[Stream index: 420]
[Conversation completeness: Incomplete (37)]
0000 08 00 27 d
0010 00 28 09 de
0020 01 64 01 c7
0030 00 00 91 b
Left ⌘

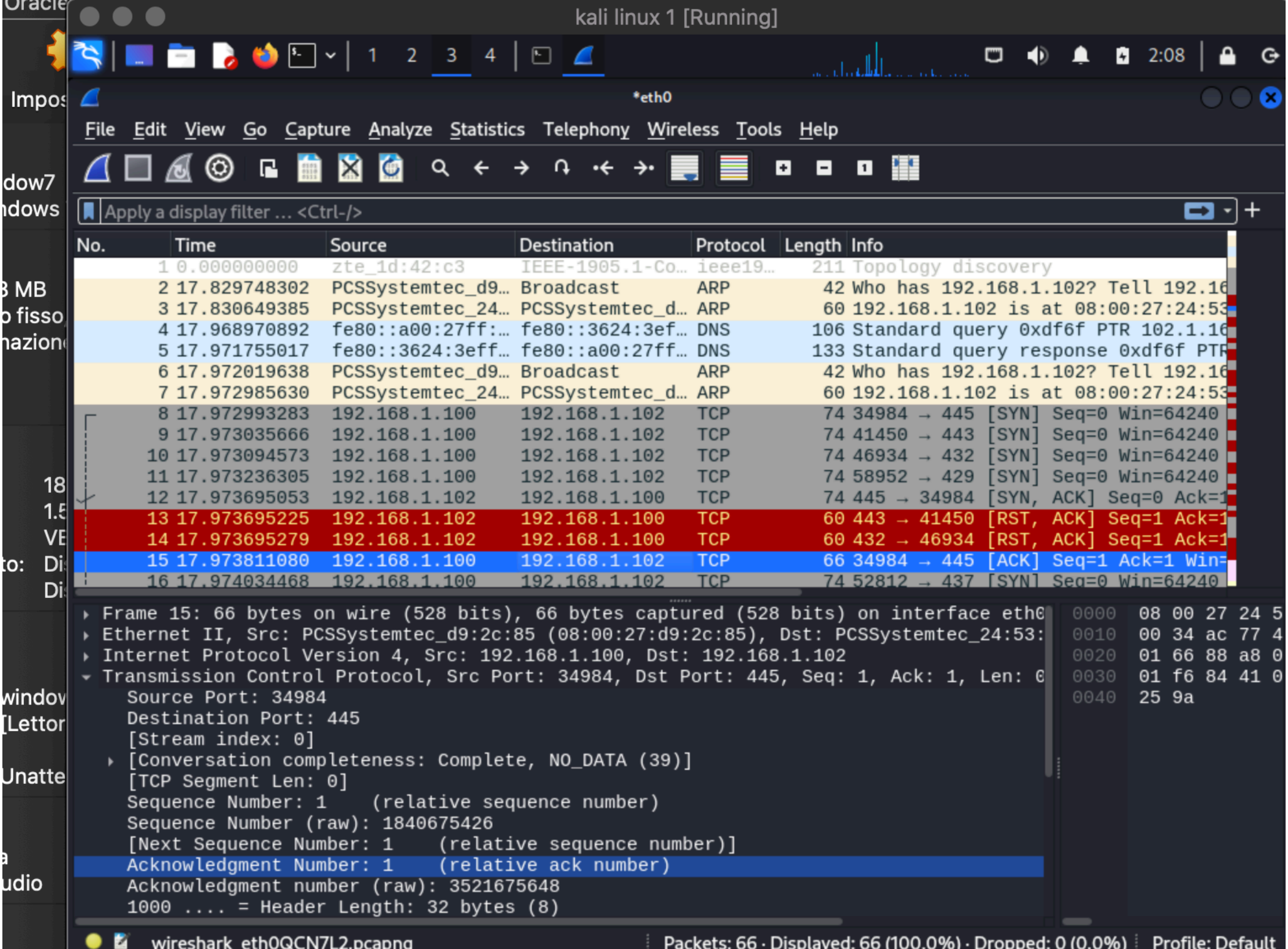

kali linux 1 [Running]
1 2 3 4
0:50
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
19 6.108285917 192.168.1.100 192.168.1.102 TCP 58 40908 → 22 [SYN] Seq=0 Win=1024 Le
22 6.108983619 192.168.1.100 192.168.1.102 TCP 58 40908 → 445 [SYN] Seq=0 Win=1024 L
23 6.109318093 192.168.1.100 192.168.1.102 TCP 58 40908 → 23 [SYN] Seq=0 Win=1024 Le
25 6.109578058 192.168.1.100 192.168.1.102 TCP 54 40908 → 445 [RST] Seq=1 Win=0 Len=
27 6.112849134 192.168.1.100 192.168.1.102 TCP 58 40908 → 53 [SYN] Seq=0 Win=1024 Le
28 6.113503021 192.168.1.100 192.168.1.102 TCP 58 40908 → 139 [SYN] Seq=0 Win=1024 L
30 6.114070248 192.168.1.100 192.168.1.102 TCP 58 40908 → 111 [SYN] Seq=0 Win=1024 L
32 6.114418162 192.168.1.100 192.168.1.102 TCP 54 40908 → 139 [RST] Seq=1 Win=0 Len=
34 6.114808547 192.168.1.100 192.168.1.102 TCP 58 40908 → 25 [SYN] Seq=0 Win=1024 Le
35 6.115115606 192.168.1.100 192.168.1.102 TCP 58 40908 → 199 [SYN] Seq=0 Win=1024 L
37 6.115494075 192.168.1.100 192.168.1.102 TCP 58 40908 → 135 [SYN] Seq=0 Win=1024 L
39 6.115816462 192.168.1.100 192.168.1.102 TCP 58 40908 → 24 [SYN] Seq=0 Win=1024 Le
41 6.116107858 192.168.1.100 192.168.1.102 TCP 54 40908 → 135 [RST] Seq=1 Win=0 Len=
43 6.116704654 192.168.1.100 192.168.1.102 TCP 58 40908 → 446 [SYN] Seq=0 Win=1024 L
44 6.117029413 192.168.1.100 192.168.1.102 TCP 58 40908 → 194 [SYN] Seq=0 Win=1024 L
47 6.117672095 192.168.1.100 192.168.1.102 TCP 58 40908 → 460 [SYN] Seq=0 Win=1024 L
Frame 22: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface eth0
Ethernet II, Src: PCSSystemtec_d9:2c:85 (08:00:27:d9:2c:85), Dst: PCSSystemtec_24:53:
Internet Protocol Version 4, Src: 192.168.1.100, Dst: 192.168.1.102
Transmission Control Protocol, Src Port: 40908, Dst Port: 445, Seq: 0, Len: 0
Source Port: 40908
Destination Port: 445
[Stream index: 8]
[Conversation completeness: Incomplete (35)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 1578605134
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
0110 .... = Header Length: 24 bytes (6)
0000 08 00 27 24 5
0010 00 2c 35 ed 0
0020 01 66 9f cc 0
0030 04 00 76 1c 0
wireshark_eth0N9CBM2.pcapng
Packets: 1019 · Displayed: 1019 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
Left ⌘

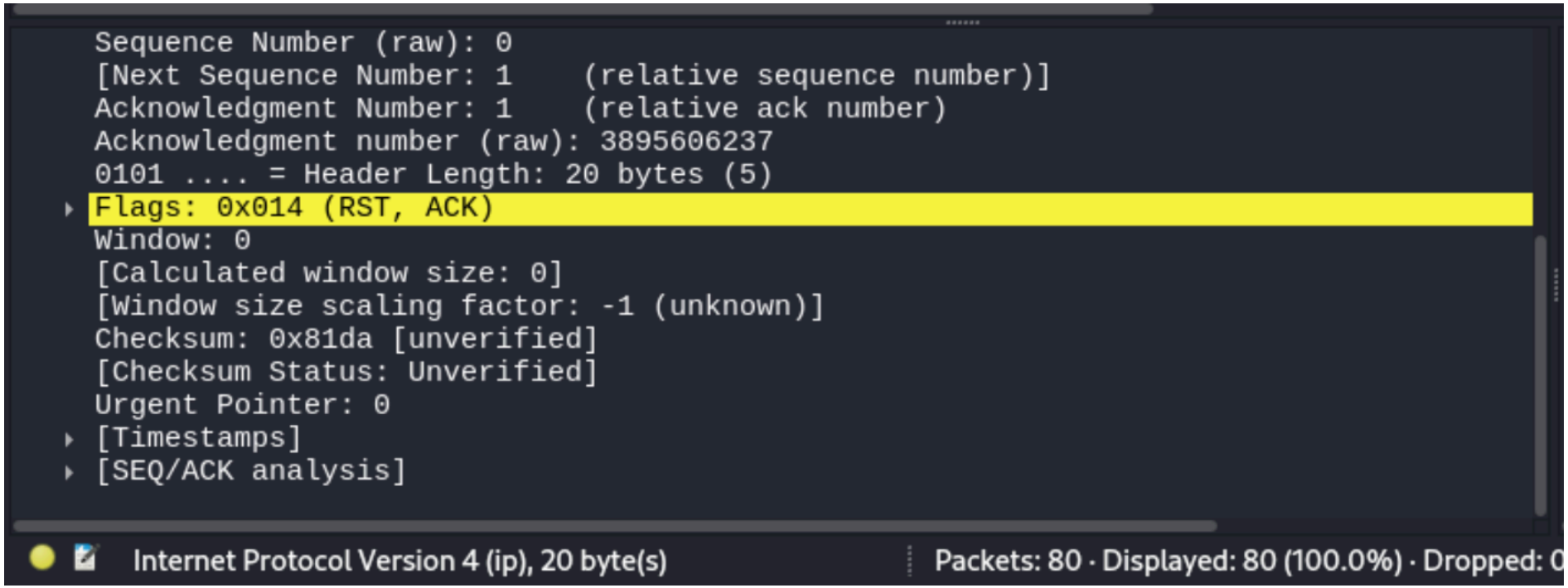

Destination Port: 445
[Stream index: 8]
[Conversation completeness: Incomplete (35)]
..1. .... = RST: Present
...0 .... = FIN: Absent
.... 0... = Data: Absent
.... .0.. = ACK: Absent
.... ..1. = SYN-ACK: Present
....1 = SYN: Present
[Completeness Flags: R···SS]
[TCP Segment Len: 0]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 1578605135
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0

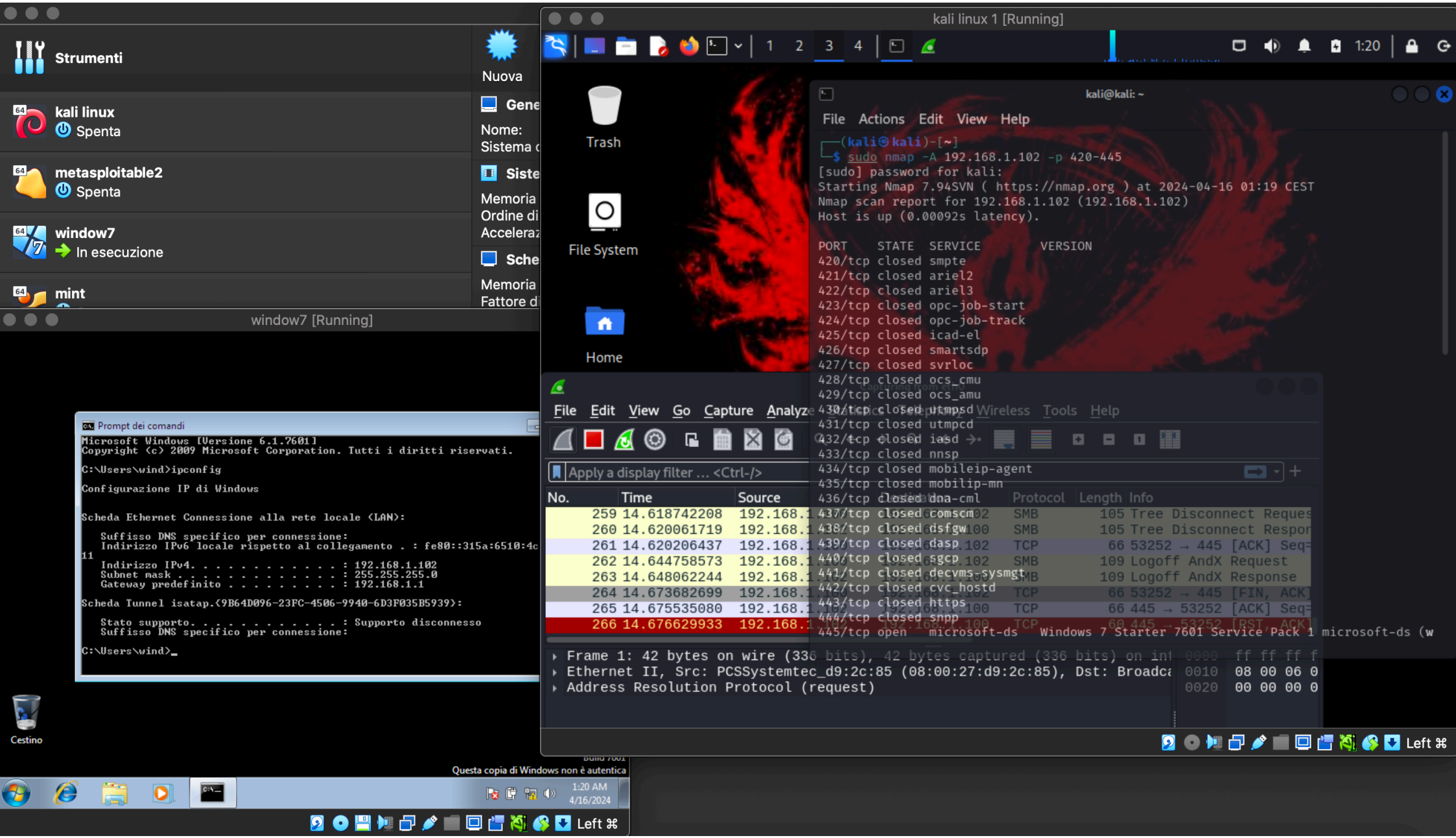

kali linux 1 [Running]
1 2 3 4
1:01
Trash
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo nmap -sS 192.168.1.102 -p 440-445
Starting Nmap 7.94SVN (https://nmap.org) at 2024-04-16 00:59 CEST
Nmap scan report for 192.168.1.102 (192.168.1.102)
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
ination Protocol Length Info
Systemtec_d… ARP 60 192.168.1.102 is at 08:00:27:24:53:cb
0::3624:3ef… DNS 106 Standard query 0xb48a PTR 102.1.168.192.in-addr.arpa
0::a00:27ff… DNS 133 Standard query response 0xb48a PTR 102.1.168.192.in-addr.arpa
168.1.102 TCP 58 57279 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
168.1.100 TCP 60 443 → 57279 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
168.1.102 TCP 58 57279 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
168.1.102 TCP 58 57279 → 442 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
168.1.100 TCP 60 445 → 57279 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
168.1.102 TCP 54 57279 → 445 [RST] Seq=1 Win=0 Len=0
Acknowledgment number (raw): 1152869005
0110 .... = Header Length: 24 bytes (6)
Flags: 0x012 (SYN, ACK)
Window: 8192
[Calculated window size: 8192]
Checksum: 0x58f8 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (4 bytes), Maximum segment size
0000 08 00 27 d
0010 00 2c 00 7
0020 01 64 01 b
0030 20 00 58 f

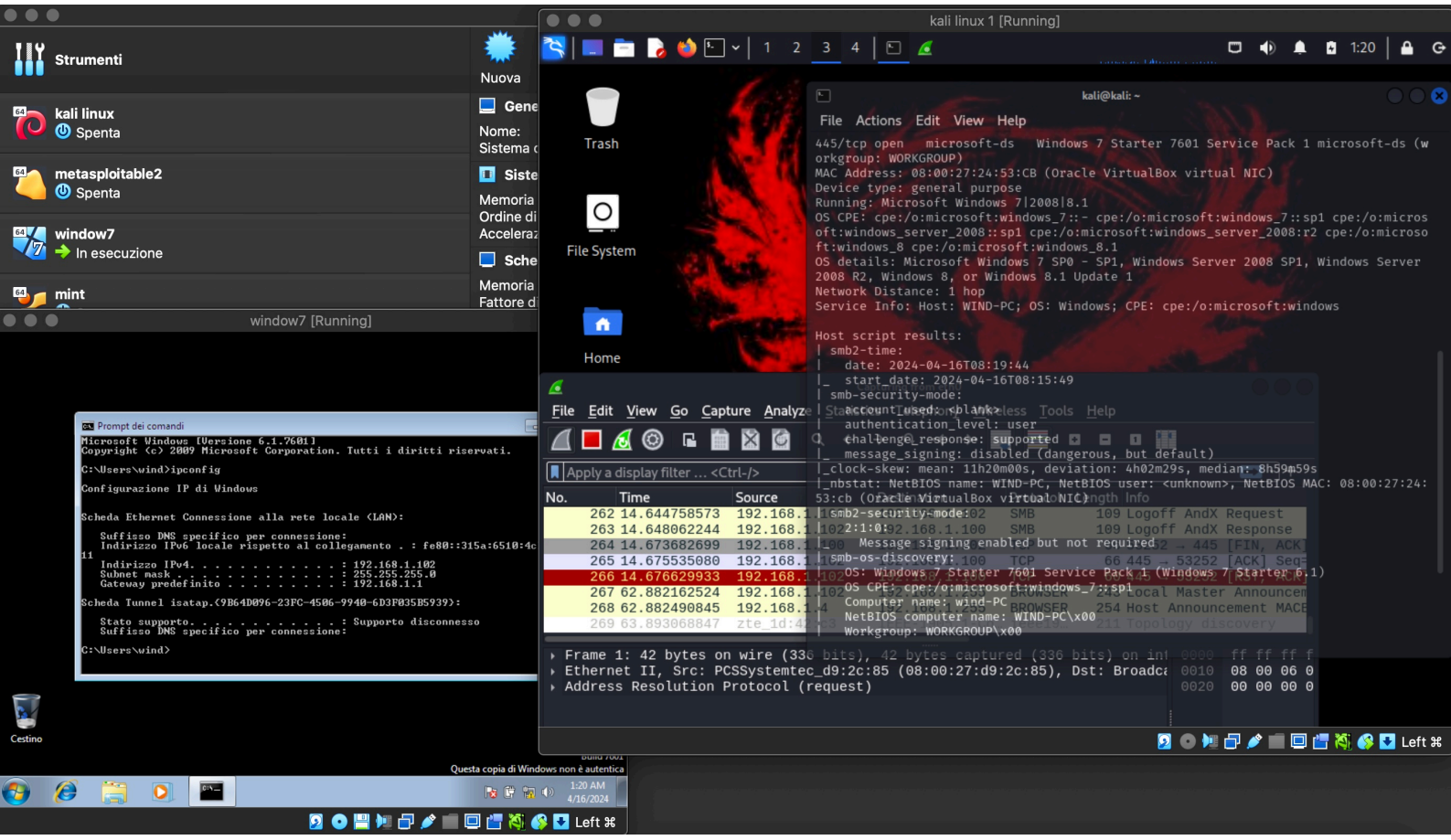

Oracle VM VirtualBox Gestore
Strumenti
kali linux
Spenta
metasploitable2
Spenta
window7
In esecuzione
mint
Nuova
Gene
Nome:
Sistema
Siste
Memoria
Ordine di
Acceleraz
Sche
Memoria
Fattore di
kali linux 1 [Running]
1 2 3 4
1:11
Trash
File System
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo nmap -sT 192.168.1.102 -p 410-445
Starting Nmap 7.94SVN (https://nmap.org) at 2024-04-16 01:10 CEST
Nmap scan report for 192.168.1.102 (192.168.1.102)
Host is up (0.0026s latency).
Not shown: 35 closed tcp ports (conn-refused)
PORT STATE SERVICE
445/tcp open microsoft-ds
MAC Address: 08:00:27:24:53:CB (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
window7 [Running]
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
72 0.141295311 192.168.1.100 192.168.1.102 TCP 74 47874 → 427 [SYN] Seq=
73 0.141501349 192.168.1.102 192.168.1.100 TCP 60 444 → 33818 [RST, ACK]
74 0.141756170 192.168.1.100 192.168.1.102 TCP 74 35732 → 439 [SYN] Seq=
75 0.142195873 192.168.1.102 192.168.1.100 TCP 60 427 → 47874 [RST, ACK]
76 0.142196054 192.168.1.102 192.168.1.100 TCP 60 439 → 35732 [RST, ACK]
77 0.142300608 192.168.1.100 192.168.1.102 TCP 74 59040 → 434 [SYN] Seq=
78 0.142815856 192.168.1.102 192.168.1.100 TCP 60 434 → 59040 [RST, ACK]
79 4.903051079 192.168.1.102 192.168.1.255 BROWSER 250 Domain/Workgroup Annou
80 16.678831375 zte_1d:42:c3 IEEE-1905.1-Co… ieee19… 211 Topology discovery
Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on int
Ethernet II, Src: PCSSystemtec_d9:2c:85 (08:00:27:d9:2c:85), Dst: Broadca
Address Resolution Protocol (request)
0000 ff ff ff f
0010 08 00 06 0
0020 00 00 00 0
Prompt dei comandi
Microsoft Windows [Versione 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tutti i diritti riservati.
C:\Users\wind>ipconfig
Configurazione IP di Windows
Scheda Ethernet Connessione alla rete locale (LAN):
Suffisso DNS specifico per connessione:
Indirizzo IPv6 locale rispetto al collegamento . : fe80::315a:6510:4c
11
Indirizzo IPv4. . . . . : 192.168.1.102
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : 192.168.1.1
Scheda Tunnel isatap.{9B64D096-23FC-4506-9940-6D3F035B5939}:
Stato supporto. . . . . : Supporto disconnesso
Suffisso DNS specifico per connessione:
C:\Users\wind>
Cestino
Questa copia di Windows non è autentica
1:11 AM
4/16/2024
Left ⌘
Left ⌘

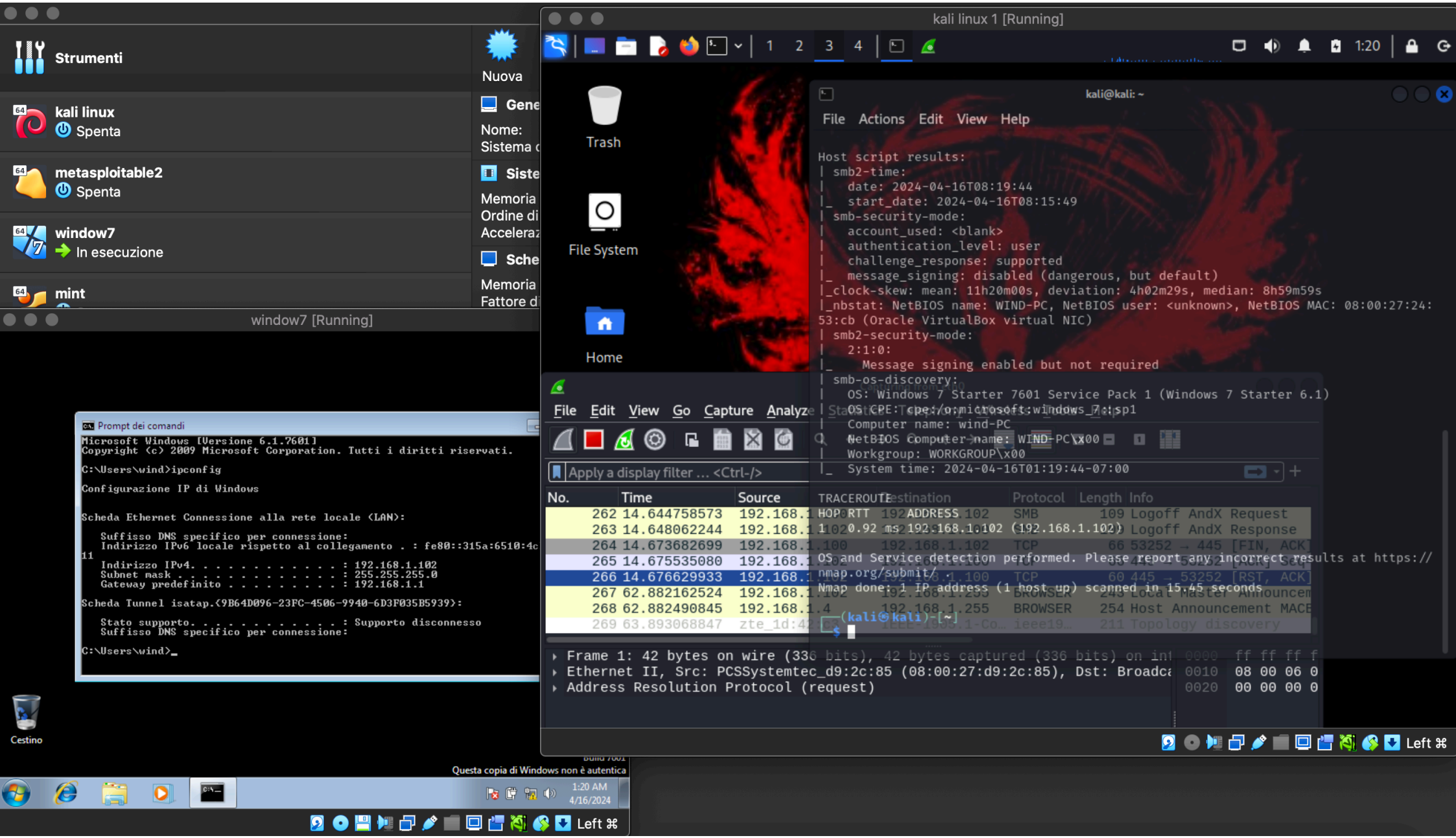

Oracle VM VirtualBox Gestore
kali linux 1 [Running]
1 2 3 4
1:12
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000000 PCSSystemtec_d9... Broadcast ARP 42 Who has 192.168.1.102? Tell 192.16
2 0.000872582 PCSSystemtec_24... PCSSystemtec_d... ARP 60 192.168.1.102 is at 08:00:27:24:53
3 0.119169990 fe80::a00:27ff:... fe80::3624:3ef... DNS 106 Standard query 0xf22d PTR 102.1.16
4 0.121679825 fe80::3624:3eff... fe80::a00:27ff... DNS 133 Standard query response 0xf22d PTR
5 0.121891704 192.168.1.100 192.168.1.102 TCP 74 33808 → 443 [SYN] Seq=0 Win=64240
6 0.122575045 192.168.1.100 192.168.1.102 TCP 74 54992 → 445 [SYN] Seq=0 Win=64240
7 0.122891696 192.168.1.102 192.168.1.100 TCP 60 443 → 33808 [RST, ACK] Seq=1 Ack=1
8 0.123217142 192.168.1.100 192.168.1.102 TCP 74 42744 → 414 [SYN] Seq=0 Win=64240
9 0.123571558 192.168.1.102 192.168.1.100 TCP 74 445 → 54992 [SYN, ACK] Seq=0 Ack=1
10 0.123644839 192.168.1.100 192.168.1.102 TCP 66 54992 → 445 [ACK] Seq=1 Ack=1 Win=
11 0.124072741 192.168.1.102 192.168.1.100 TCP 60 414 → 42744 [RST, ACK] Seq=1 Ack=1
12 0.124252544 192.168.1.100 192.168.1.102 TCP 74 56126 → 412 [SYN] Seq=0 Win=64240
13 0.124915035 192.168.1.102 192.168.1.100 TCP 60 412 → 56126 [RST, ACK] Seq=1 Ack=1
14 0.124989610 192.168.1.100 192.168.1.102 TCP 74 45342 → 436 [SYN] Seq=0 Win=64240
15 0.125328953 192.168.1.100 192.168.1.102 TCP 74 49170 → 423 [SYN] Seq=0 Win=64240
16 0.125564303 192.168.1.102 192.168.1.100 TCP 60 436 → 45342 [RST, ACK] Seq=1 Ack=1
Frame 7: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0,
Ethernet II, Src: PCSSystemtec_24:53:cb (08:00:27:24:53:cb), Dst: PCSSystemtec_d9:2c:
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 192.168.1.100
Transmission Control Protocol, Src Port: 443, Dst Port: 33808, Seq: 1, Ack: 1, Len: 0
Source Port: 443
Destination Port: 33808
[Stream index: 0]
[Conversation completeness: Incomplete (37)]
[TCP Segment Len: 0]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 0
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 3895606237
0101 .... = Header Length: 20 bytes (5)
0000 08 00 27 d9
0010 00 28 00 8a
0020 01 64 01 bb
0030 00 00 81 da
Internet Protocol Version 4 (ip), 20 byte(s)
Packets: 80 · Displayed: 80 (100.0%) · Dropped: 0 (0.0%)
Profile: Default


kali linux 1 [Running]
1 2 3 4
2:08
*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 zte_1d:42:c3 IEEE-1905.1-Co... ieee19... 211 Topology discovery
2 17.829748302 PCSSystemtec_d9... Broadcast ARP 42 Who has 192.168.1.102? Tell 192.16
3 17.830649385 PCSSystemtec_24... PCSSystemtec_d... ARP 60 192.168.1.102 is at 08:00:27:24:53
4 17.968970892 fe80::a00:27ff:... fe80::3624:3ef... DNS 106 Standard query 0xdf6f PTR 102.1.16
5 17.971755017 fe80::3624:3eff... fe80::a00:27ff... DNS 133 Standard query response 0xdf6f PTR
6 17.972019638 PCSSystemtec_d9... Broadcast ARP 42 Who has 192.168.1.102? Tell 192.16
7 17.972985630 PCSSystemtec_24... PCSSystemtec_d... ARP 60 192.168.1.102 is at 08:00:27:24:53
8 17.972993283 192.168.1.100 192.168.1.102 TCP 74 34984 → 445 [SYN] Seq=0 Win=64240
9 17.973035666 192.168.1.100 192.168.1.102 TCP 74 41450 → 443 [SYN] Seq=0 Win=64240
10 17.973094573 192.168.1.100 192.168.1.102 TCP 74 46934 → 432 [SYN] Seq=0 Win=64240
11 17.973236305 192.168.1.100 192.168.1.102 TCP 74 58952 → 429 [SYN] Seq=0 Win=64240
12 17.973695053 192.168.1.102 192.168.1.100 TCP 74 445 → 34984 [SYN, ACK] Seq=0 Ack=1
13 17.973695225 192.168.1.102 192.168.1.100 TCP 60 443 → 41450 [RST, ACK] Seq=1 Ack=1
14 17.973695279 192.168.1.102 192.168.1.100 TCP 60 432 → 46934 [RST, ACK] Seq=1 Ack=1
15 17.973811080 192.168.1.100 192.168.1.102 TCP 66 34984 → 445 [ACK] Seq=1 Ack=1 Win=
16 17.974034468 192.168.1.100 192.168.1.102 TCP 74 52812 → 437 [SYN] Seq=0 Win=64240
Frame 15: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0
Ethernet II, Src: PCSSystemtec_d9:2c:85 (08:00:27:d9:2c:85), Dst: PCSSystemtec_24:53:
Internet Protocol Version 4, Src: 192.168.1.100, Dst: 192.168.1.102
Transmission Control Protocol, Src Port: 34984, Dst Port: 445, Seq: 1, Ack: 1, Len: 0
Source Port: 34984
Destination Port: 445
[Stream index: 0]
[Conversation completeness: Complete, NO_DATA (39)]
[TCP Segment Len: 0]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 1840675426
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 3521675648
1000 .... = Header Length: 32 bytes (8)
0000 08 00 27 24 5
0010 00 34 ac 77 4
0020 01 66 88 a8 0
0030 01 f6 84 41 0
0040 25 9a
wireshark_eth0QCN7L2.pcapng
Packets: 66 · Displayed: 66 (100.0%) · Dropped: 0 (0.0%)
Profile: Default


Sequence Number (raw): 0
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 3895606237
0101 .... = Header Length: 20 bytes (5)
Flags: 0x014 (RST, ACK)
Window: 0
[Calculated window size: 0]
[Window size scaling factor: -1 (unknown)]
Checksum: 0x81da [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[SEQ/ACK analysis]
Internet Protocol Version 4 (ip), 20 byte(s)
Packets: 80 · Displayed: 80 (100.0%) · Dropped: 0


Strumenti
kali linux
Spenta
metasploitable2
Spenta
window7
In esecuzione
mint
Nuova
Nome:
Memoria
Ordine di
Memoria
Fattore d
window7 [Running]
kali linux 1 [Running]
1 2 3 4
1:20
Trash
File System
Home
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo nmap -A 192.168.1.102 -p 420-445
[sudo] password for kali:
Starting Nmap 7.94SVN (https://nmap.org) at 2024-04-16 01:19 CEST
Nmap scan report for 192.168.1.102 (192.168.1.102)
Host is up (0.00092s latency).
PORT STATE SERVICE VERSION
420/tcp closed smpte
421/tcp closed ariel2
422/tcp closed ariel3
423/tcp closed opc-job-start
424/tcp closed opc-job-track
425/tcp closed icad-el
426/tcp closed smartsdp
427/tcp closed svrloc
428/tcp closed ocs_cmu
429/tcp closed ocs_amu
430/tcp closed utmpsd
431/tcp closed utmpcd
432/tcp closed iasd
433/tcp closed nnsp
434/tcp closed mobileip-agent
435/tcp closed mobilip-mn
436/tcp closed dna-cml
437/tcp closed comscm
438/tcp closed dsfgw
439/tcp closed dasp
440/tcp closed sgcp
441/tcp closed decvms-sysmgt
442/tcp closed cvc_hostd
443/tcp closed https
444/tcp closed snpp
445/tcp open microsoft-ds Windows 7 Starter 7601 Service Pack 1 microsoft-ds (w
Prompt dei comandi
Microsoft Windows [Versione 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tutti i diritti riservati.
C:\Users\wind>ipconfig
Configurazione IP di Windows
Scheda Ethernet Connessione alla rete locale (LAN):
Suffisso DNS specifico per connessione:
Indirizzo IPv6 locale rispetto al collegamento . : fe80::315a:6510:4c11
Indirizzo IPv4. . . . . : 192.168.1.102
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : 192.168.1.1
Scheda Tunnel isatap.{9B64D096-23FC-4506-9940-6D3F035B5939}:
Stato supporto. . . . . : Supporto disconnesso
Suffisso DNS specifico per connessione:
C:\Users\wind>
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Protocol Length Info
259 14.618742208 192.168.1 SMB 105 Tree Disconnect Reques
260 14.620061719 192.168.1 SMB 105 Tree Disconnect Respon
261 14.620206437 192.168.1 TCP 66 53252 → 445 [ACK] Seq=
262 14.644758573 192.168.1 SMB 109 Logoff AndX Request
263 14.648062244 192.168.1 SMB 109 Logoff AndX Response
264 14.673682699 192.168.1 TCP 66 53252 → 445 [FIN, ACK]
265 14.675535080 192.168.1 TCP 66 445 → 53252 [ACK] Seq=
266 14.676629933 192.168.1 TCP 60 445 → 53252 [RST, ACK]
Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on int
Ethernet II, Src: PCSSystemtec_d9:2c:85 (08:00:27:d9:2c:85), Dst: Broadca
Address Resolution Protocol (request)
0000 ff ff ff f
0010 08 00 06 0
0020 00 00 00 0
Cestino
Questa copia di Windows non è autentica
1:20 AM
4/16/2024
Left ⌘
Left ⌘


Strumenti
kali linux
Spenta
metasploitable2
Spenta
window7
In esecuzione
mint
Nuova
Gene
Nome:
Sistema
Siste
Memoria
Ordine di
Accelera
Sche
Memoria
Fattore d
window7 [Running]
Prompt dei comandi
Microsoft Windows [Versione 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tutti i diritti riservati.
C:\Users\wind>ipconfig
Configurazione IP di Windows
Scheda Ethernet Connessione alla rete locale (LAN):
Suffisso DNS specifico per connessione:
Indirizzo IPv6 locale rispetto al collegamento . : fe80::315a:6510:4c
11
Indirizzo IPv4. . . . . : 192.168.1.102
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : 192.168.1.1
Scheda Tunnel isatap.{9B64D096-23FC-4506-9940-6D3F035B5939}:
Stato supporto. . . . . : Supporto disconnesso
Suffisso DNS specifico per connessione:
C:\Users\wind>
Cestino
Questa copia di Windows non è autentica
1:20 AM
4/16/2024
Left ⌘
kali linux 1 [Running]
Trash
File System
Home
kali@kali: ~
File Actions Edit View Help
445/tcp open microsoft-ds Windows 7 Starter 7601 Service Pack 1 microsoft-ds (w
orkgroup: WORKGROUP)
MAC Address: 08:00:27:24:53:CB (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::~ cpe:/o:microsoft:windows_7::sp1 cpe:/o:micros
oft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microso
ft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server
2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: WIND-PC; OS: Windows; CPE: cpe:/o:microsoft:windows
Host script results:
| smb2-time:
| date: 2024-04-16T08:19:44
|_ start_date: 2024-04-16T08:15:49
| smb-security-mode:
| account_used: <blank>
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 11h20m00s, deviation: 4h02m29s, median: 8h59m59s
|_nbstat: NetBIOS name: WIND-PC, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:24:
53:cb (Oracle VirtualBox virtual NIC)
| smb2-security-mode:
| 2:1:0:
| Message signing enabled but not required
| smb-os-discovery:
| OS: Windows 7 Starter 7601 Service Pack 1 (Windows 7 Starter 6.1)
| OS CPE: cpe:/o:microsoft:windows_7::spi
| Computer name: wind-PC
| NetBIOS computer name: WIND-PC\x00
|_ Workgroup: WORKGROUP\x00
File Edit View Go Capture Analyze
Apply a display filter ... <Ctrl-/>
No. Time Source
262 14.644758573 192.168.1.
263 14.648062244 192.168.1.
264 14.673682699 192.168.1.
265 14.675535080 192.168.1.
266 14.676629933 192.168.1.
267 62.882162524 192.168.1.
268 62.882490845 192.168.1.
269 63.893068847 zte_1d:47
SMB 109 Logoff AndX Request
SMB 109 Logoff AndX Response
TCP 66 445 → 53252 [ACK] Seq=
Protocol Master Announcem
254 Host Announcement MACE
211 Topology discovery
Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on int
Ethernet II, Src: PCSSystemtec_d9:2c:85 (08:00:27:d9:2c:85), Dst: Broadca
Address Resolution Protocol (request)
0000 ff ff ff f
0010 08 00 06 0
0020 00 00 00 0
Left ⌘


Strumenti
kali linux
Spenta
metasploitable2
Spenta
window7
In esecuzione
mint
Nuova
Gene
Nome:
Sistema
Siste
Memoria
Ordine di
Acceleraz
Sche
Memoria
Fattore d
window7 [Running]
kali linux 1 [Running]
1 2 3 4
1:20
Trash
File System
Home
kali@kali: ~
File Actions Edit View Help
Host script results:
| smb2-time:
| date: 2024-04-16T08:19:44
|_ start_date: 2024-04-16T08:15:49
| smb-security-mode:
| account_used: <blank>
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 11h20m00s, deviation: 4h02m29s, median: 8h59m59s
|_nbstat: NetBIOS name: WIND-PC, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:24:53:cb (Oracle VirtualBox virtual NIC)
| smb2-security-mode:
| 2:1:0:
|_ Message signing enabled but not required
| smb-os-discovery:
| OS: Windows 7 Starter 7601 Service Pack 1 (Windows 7 Starter 6.1)
| OS CPE: cpe:/o:microsoft:windows_7::sp1
| Computer name: wind-PC
| NetBIOS Computer name: WIND-PC\x00
| Workgroup: WORKGROUP\x00
|_ System time: 2024-04-16T01:19:44-07:00
TRACEROUTE
HOP RTT ADDRESS
1 0.92 ms 192.168.1.102 (192.168.1.102)
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.45 seconds
(kali㉿kali)-[~]
$
Prompt dei comandi
Microsoft Windows [Versione 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tutti i diritti riservati.
C:\Users\wind>ipconfig
Configurazione IP di Windows
Scheda Ethernet Connessione alla rete locale (LAN):
Suffisso DNS specifico per connessione:
Indirizzo IPv6 locale rispetto al collegamento . : fe80::315a:6510:4c11
Indirizzo IPv4. . . . . : 192.168.1.102
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : 192.168.1.1
Scheda Tunnel isatap.{9B64D096-23FC-4506-9940-6D3F035B5939}:
Stato supporto. . . . . : Supporto disconnesso
Suffisso DNS specifico per connessione:
C:\Users\wind>
File Edit View Go Capture Analyze
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
262 14.644758573 192.168.1.102 SMB 109 Logoff AndX Request
263 14.648062244 192.168.1.102 SMB 109 Logoff AndX Response
264 14.673682699 192.168.1.100 192.168.1.102 TCP 66 53252 → 445 [FIN, ACK]
265 14.675535080 192.168.1.102 192.168.1.100 TCP 60 445 → 53252 [ACK]
266 14.676629933 192.168.1.100 192.168.1.102 TCP 60 445 → 53252 [RST, ACK]
267 62.882162524 192.168.1.102 192.168.1.255 BROWSER 243 Local Master Announcem
268 62.882490845 192.168.1.4 192.168.1.255 BROWSER 254 Host Announcement MACE
269 63.893068847 zte_1d:42 IEEE-1905.1-Co… ieee19… 211 Topology discovery
Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on int
Ethernet II, Src: PCSSystemtec_d9:2c:85 (08:00:27:d9:2c:85), Dst: Broadca
Address Resolution Protocol (request)
0000 ff ff ff f
0010 08 00 06 0
0020 00 00 00 0
Cestino
Questa copia di Windows non è autentica
1:20 AM
4/16/2024
Left ⌘
Left ⌘