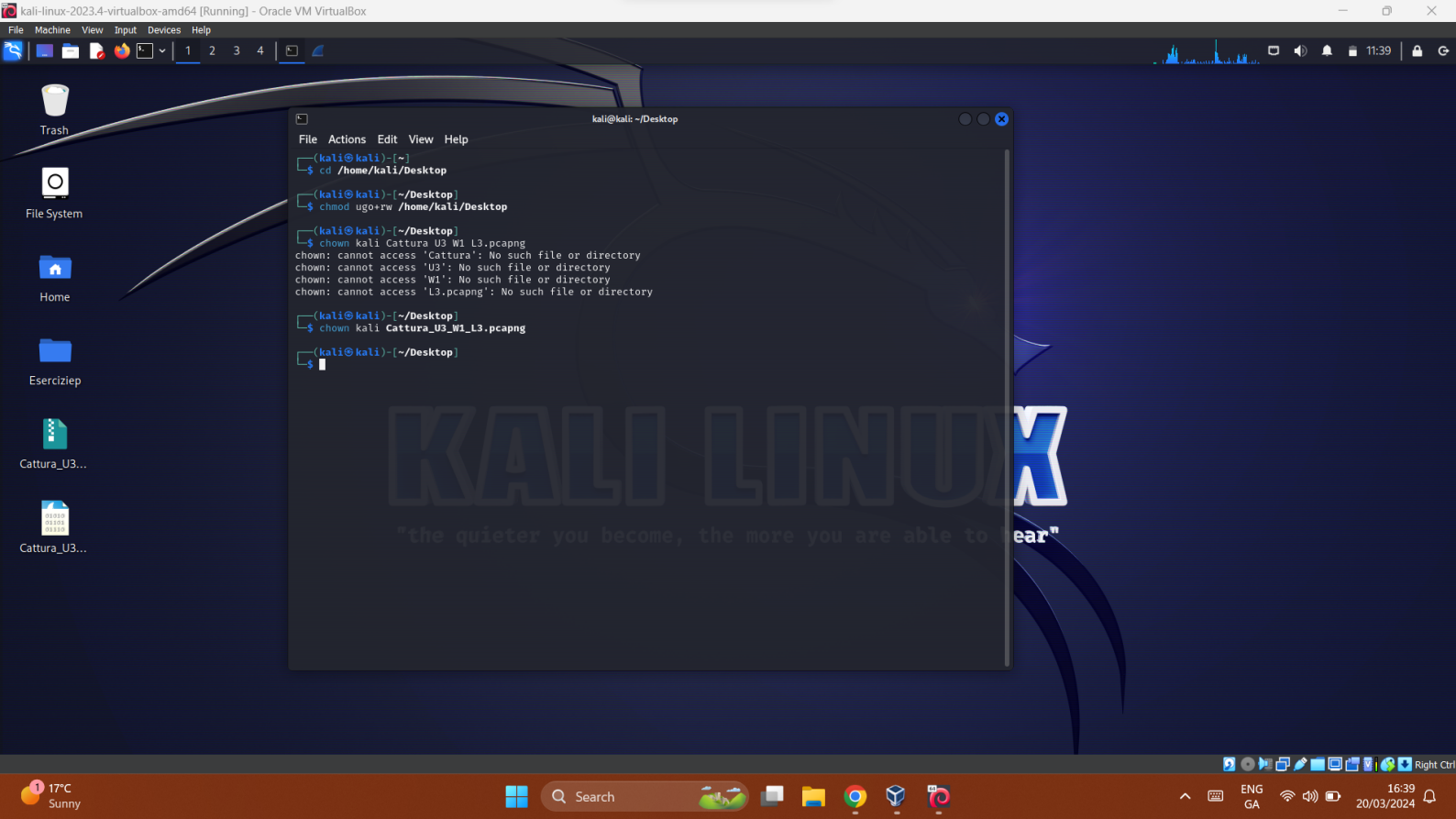
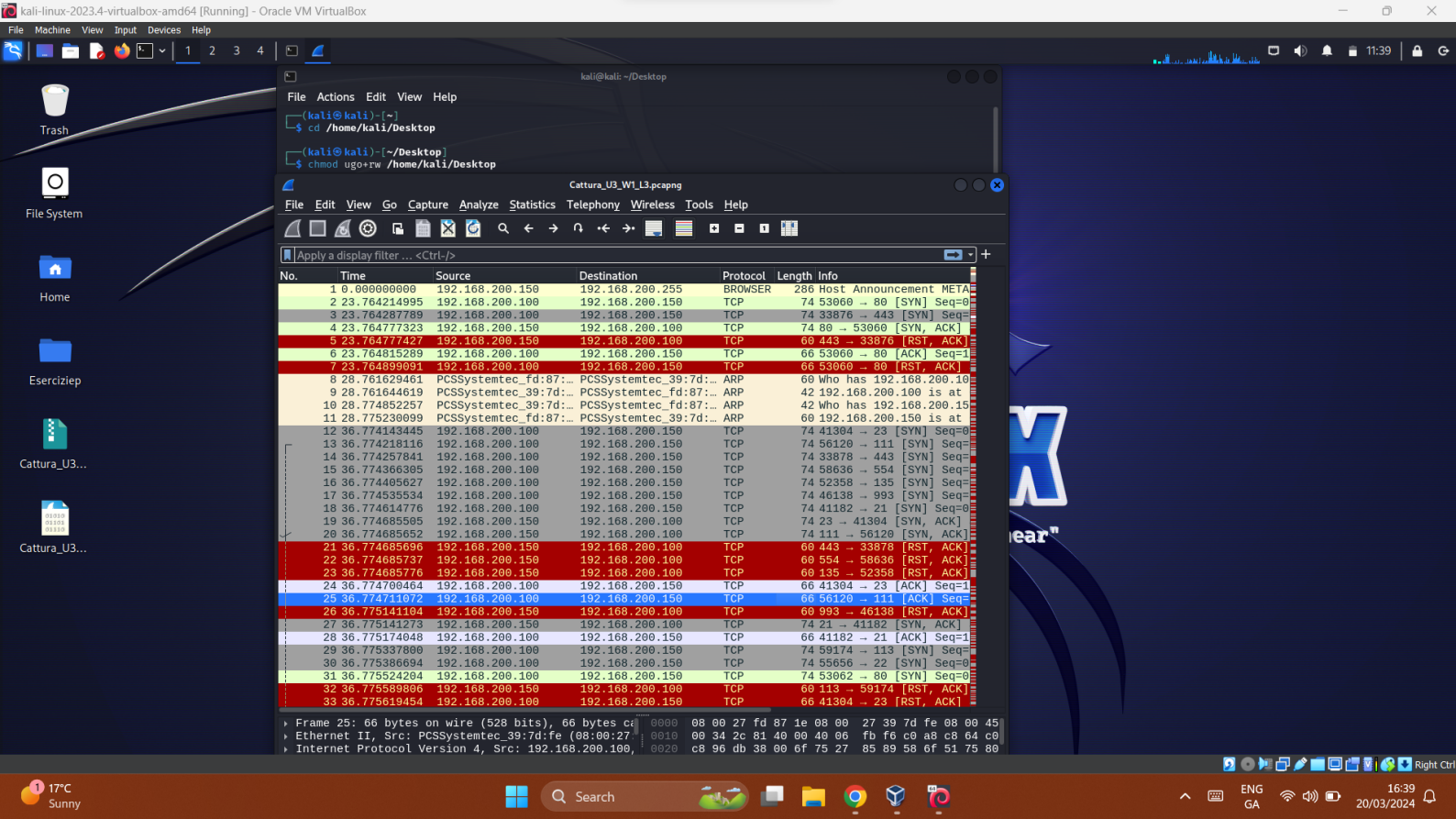
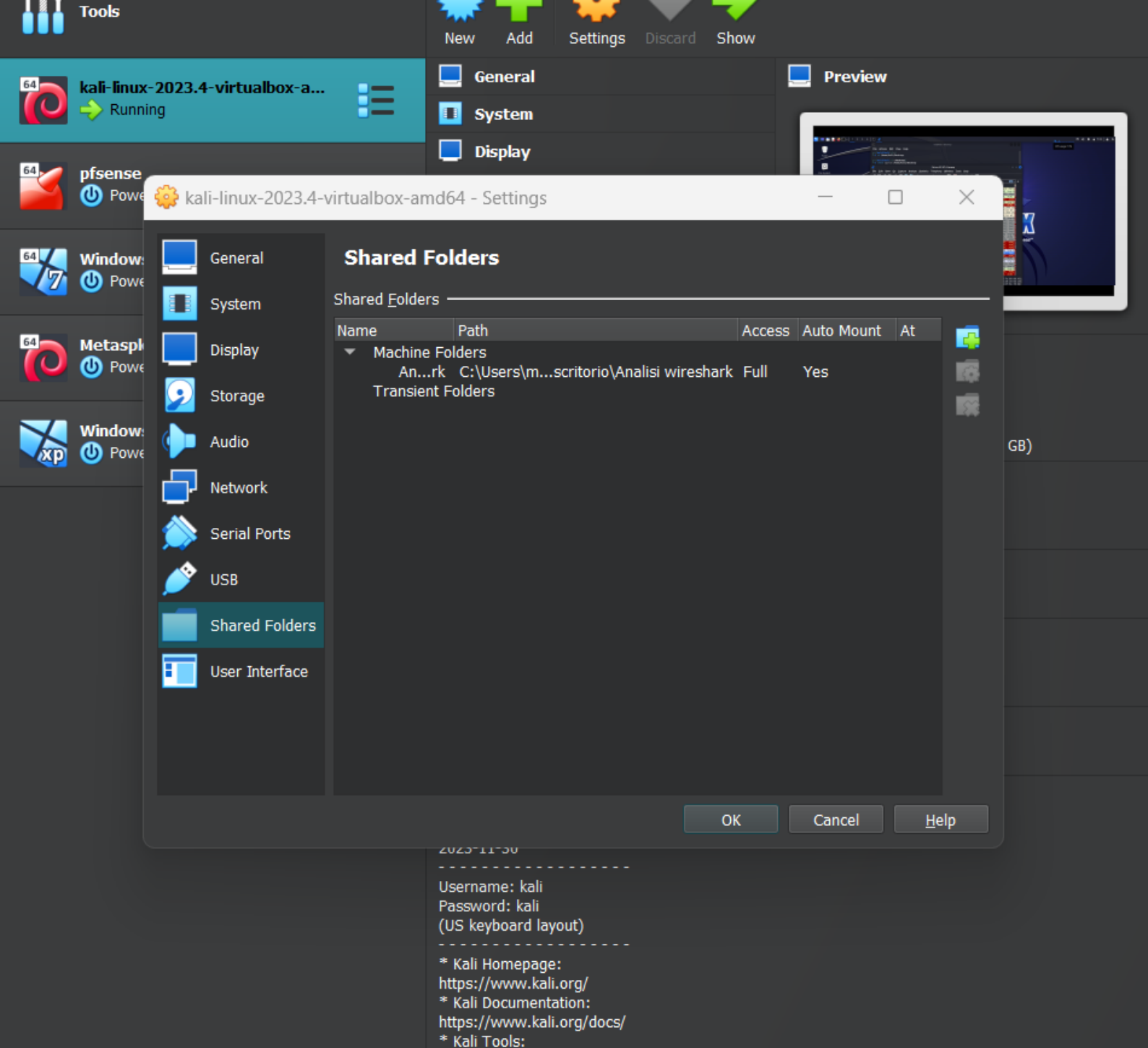
Analizzando le tabelle del traffico salvate da Wireshark si puo' dedurre che la scansione e' stata effettuata dall'attaccante con l'IP 192.168.200.100 e che le macchine comunicano nella stessa rete interna tramite un dispositivo router/switch di cui conosciamo quindi l'indirizzo di broadcast 192.168.200.255,osserviamo di fatto i protocolli TCP ed ARP sostenuti.
Osserviamo dati ottenuti come SACK_PERM tra le prime richieste riconducibile ad un three handshake(SYN,SYN,ACK),la connessione ACK fallisce...
Le prime porte prese di mira sono 80,443,mentre l'attaccante comunica dalle porte 5360,33876.
Il dato "who has 192.168.200.100? tell 192.168.200.150" ci suggerisce invece che l'attaccante sta cercando di fare il ping tra le macchine tramite una richiesta ARP cosi da rincodurre indirizzo IP ad MAC.
Nonostante i primi tentavi falliti successivamente l'attaccante riuscira' ad mettersi in ascolto sulle porte.


kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
11:39
Trash
File System
Home
Eserciziep
Cattura_U3...
Cattura_U3...
kali@kali: ~/Desktop
File Actions Edit View Help
(kali㉿kali)-[~]
$ cd /home/kali/Desktop
(kali㉿kali)-[~/Desktop]
$ chmod ugo+rw /home/kali/Desktop
(kali㉿kali)-[~/Desktop]
$ chown kali Cattura U3 W1 L3.pcapng
chown: cannot access 'Cattura': No such file or directory
chown: cannot access 'U3': No such file or directory
chown: cannot access 'W1': No such file or directory
chown: cannot access 'L3.pcapng': No such file or directory
(kali㉿kali)-[~/Desktop]
$ chown kali Cattura_U3_W1_L3.pcapng
(kali㉿kali)-[~/Desktop]
$
KALI LINUX
"the quieter you become, the more you are able to hear"
Right Ctrl
17°C
Sunny
Search
ENG
GA
16:39
20/03/2024


kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
Eserciziep
Cattura_U3...
Cattura_U3...
kali@kali: ~/Desktop
File Actions Edit View Help
(kali㉿kali)-[~]
$ cd /home/kali/Desktop
(kali㉿kali)-[~/Desktop]
$ chmod ugo+rw /home/kali/Desktop
Cattura_U3_W1_L3.pcapng
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 192.168.200.150 192.168.200.255 BROWSER 286 Host Announcement META
2 23.764214995 192.168.200.100 192.168.200.150 TCP 74 53060 → 80 [SYN] Seq=0
3 23.764287789 192.168.200.100 192.168.200.150 TCP 74 33876 → 443 [SYN] Seq=
4 23.764777323 192.168.200.150 192.168.200.100 TCP 74 80 → 53060 [SYN, ACK]
5 23.764777427 192.168.200.100 192.168.200.150 TCP 60 443 → 33876 [RST, ACK]
6 23.764815289 192.168.200.100 192.168.200.150 TCP 66 53060 → 80 [ACK] Seq=1
7 23.764899091 192.168.200.100 192.168.200.150 TCP 66 53060 → 80 [RST, ACK]
8 28.761629461 PCSSystemtec_fd:87:... PCSSystemtec_39:7d:... ARP 60 Who has 192.168.200.10
9 28.761644619 PCSSystemtec_39:7d:... PCSSystemtec_fd:87:... ARP 42 192.168.200.100 is at
10 28.774852257 PCSSystemtec_39:7d:... PCSSystemtec_fd:87:... ARP 42 Who has 192.168.200.15
11 28.775230099 PCSSystemtec_fd:87:... PCSSystemtec_39:7d:... ARP 60 192.168.200.150 is at
12 36.774143445 192.168.200.100 192.168.200.150 TCP 74 41304 → 23 [SYN] Seq=0
13 36.774218116 192.168.200.100 192.168.200.150 TCP 74 56120 → 111 [SYN] Seq=
14 36.774257841 192.168.200.100 192.168.200.150 TCP 74 33878 → 443 [SYN] Seq=
15 36.774366305 192.168.200.100 192.168.200.150 TCP 74 58636 → 554 [SYN] Seq=
16 36.774405627 192.168.200.100 192.168.200.150 TCP 74 52358 → 135 [SYN] Seq=
17 36.774535534 192.168.200.100 192.168.200.150 TCP 74 46138 → 993 [SYN] Seq=
18 36.774614776 192.168.200.100 192.168.200.150 TCP 74 41182 → 21 [SYN] Seq=0
19 36.774685505 192.168.200.150 192.168.200.100 TCP 74 23 → 41304 [SYN, ACK]
20 36.774685652 192.168.200.150 192.168.200.100 TCP 74 111 → 56120 [SYN, ACK]
21 36.774685696 192.168.200.150 192.168.200.100 TCP 60 443 → 33878 [RST, ACK]
22 36.774685737 192.168.200.150 192.168.200.100 TCP 60 554 → 58636 [RST, ACK]
23 36.774685776 192.168.200.150 192.168.200.100 TCP 60 135 → 52358 [RST, ACK]
24 36.774700464 192.168.200.100 192.168.200.150 TCP 66 41304 → 23 [ACK] Seq=1
25 36.774711072 192.168.200.100 192.168.200.150 TCP 66 56120 → 111 [ACK] Seq=
26 36.775141104 192.168.200.150 192.168.200.100 TCP 60 993 → 46138 [RST, ACK]
27 36.775141273 192.168.200.150 192.168.200.100 TCP 74 21 → 41182 [SYN, ACK]
28 36.775174048 192.168.200.100 192.168.200.150 TCP 66 41182 → 21 [ACK] Seq=1
29 36.775337800 192.168.200.100 192.168.200.150 TCP 74 59174 → 113 [SYN] Seq=
30 36.775386694 192.168.200.100 192.168.200.150 TCP 74 55656 → 22 [SYN] Seq=0
31 36.775524204 192.168.200.100 192.168.200.150 TCP 74 53062 → 80 [SYN] Seq=0
32 36.775589806 192.168.200.150 192.168.200.100 TCP 60 113 → 59174 [RST, ACK]
33 36.775619454 192.168.200.100 192.168.200.150 TCP 66 41304 → 23 [RST, ACK]
Frame 25: 66 bytes on wire (528 bits), 66 bytes ca
Ethernet II, Src: PCSSystemtec_39:7d:fe (08:00:27
Internet Protocol Version 4, Src: 192.168.200.100,
0000 08 00 27 fd 87 1e 08 00 27 39 7d fe 08 00 45
0010 00 34 2c 81 40 00 40 06 fb f6 c0 a8 c8 64 c0
0020 c8 96 db 38 00 6f 75 27 85 89 58 6f 51 75 80
Right Ctrl
17°C Sunny
Search
ENG GA
16:39 20/03/2024


Tools
New
Add
Settings
Discard
Show
kali-linux-2023.4-virtualbox-a...
Running
pfsense
Windows
Metasploit
Windows
General
System
Display
Preview
kali-linux-2023.4-virtualbox-amd64 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Shared Folders
Shared Folders
Name
Path
Access
Auto Mount
At
Machine Folders
An...rk
C:\Users\m...scritorio\Analisi wireshark
Full
Yes
Transient Folders
OK
Cancel
Help
GB)
Username: kali
Password: kali
(US keyboard layout)
* Kali Homepage:
https://www.kali.org/
* Kali Documentation:
https://www.kali.org/docs/
* Kali Tools: