

Ho creato la cartella condivisa configurando il supporto per le "cartelle condivise" tra la macchina virtuale (Kali Linux) e l'host tramite le opzioni di VirtualBox o VMware. Questo permette di accedere alla directory condivisa da Kali, copiare i file sulla tua directory Desktop e modificare i permessi per l'analisi successiva.

```
File Actions Edit View Help
└─(root㉿kali)-[~] kali:
└─# cd /media/packages.microsoft.com/repos/code_stable_InRelease [3,590 B]
Get:3 https://packages.microsoft.com/repos/code_stable/main amd64 Packages
└─(root㉿kali)-[/media] microsoft.com/repos/code_stable/main armhf Packages
└─# ls https://packages.microsoft.com/repos/code_stable/main arm64 Packages
sf_Cartella_condivisa download/kali kali-rolling InRelease [41.5 kB]
Get:6 http://kali.download/kali kali-rolling/main amd64 Packages [20.2 MB]
└─(root㉿kali)-[/media] ad/kali kali-rolling/main amd64 Contents (deb) [48
└─# cd sf_Cartella_condivisa kali kali-rolling/contrib amd64 Packages [111 kB]
Get:9 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [1
└─(root㉿kali)-[/media/sf_Cartella_condivisa] non-free amd64 Packages [194
└─# ls -la http://kali.download/kali kali-rolling/non-free amd64 Contents (deb)
total 216 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packa
drwxrwx— 1 root vboxsf 4096 Oct 11 11:52 .
drwxr-xr-x 3 root root 3,44096 Oct 11 11:54 ..
-rw-rw-r— 1 root vboxsf 209024 Oct 11 11:49 Cattura_U3_W1_L3.pcapng.

└─(root㉿kali)-[/media/sf_Cartella_condivisa]
└─# mv Cattura_U3_W1_L3.pcapng /home/kali/Desktop
The following packages were automatically installed and are no longer required:
└─(root㉿kali)-[/media/sf_Cartella_condivisa] libgfapi0 libglusterfs0 lib
└─# cd /home/kali/Desktop libdaxctl libgfprc0 libibverbs1 lib
 libboost-thread1.83.0 libgeos3.12.1t64 libgwdxdr0 libjxl0.7 lib
└─(root㉿kali)-[/home/kali/Desktop] them.
└─# chmod ugo+rw Cattura_U3_W1_L3.pcapng
Summary:
└─(root㉿kali)-[/home/kali/Desktop] ing: 0, Not Upgrading: 978
└─# chwon kali Cattura_U3_W1_L3.pcapng
Command 'chwon' not found, did you mean:
 command 'chown' from deb coreutils
 command 'chcon' from deb coreutils media
Try: apt install <deb name>
└─(kali㉿kali)-[~]
└─(root㉿kali)-[/home/kali/Desktop]
└─# █
└─(kali㉿kali)-[/media]
└─$ ls
sf_Cartella_condivisa
```

Identificazione degli IoC (Indicatori di Compromissione)

1 0.000000000	192.168.200.150	192.168.200.255	BROWSER	286 Host Announcement METASPLIOTABLE_ Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Potential
2 23.764214900	192.168.200.100	192.168.200.150	TCP	74 53600 - > [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810522427 Tsecr=0 WS=128
3 23.764214900	192.168.200.100	192.168.200.150	TCP	74 53600 - > [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810522427 Tsecr=0 WS=128
4 23.7642177323	192.168.200.150	192.168.200.150	TCP	74 88 - 53069 [SYN, ACK] Seq=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 Tsvl=4294951165 Tsecr=0 WS=64
5 23.764777427	192.168.200.150	192.168.200.150	TCP	68 443 - 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6 23.764815289	192.168.200.100	192.168.200.150	TCP	66 53066 - 88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810522428 Tsecr=0 WS=128
7 23.764899691	192.168.200.100	192.168.200.150	TCP	66 53066 - 88 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810522428 Tsecr=0 WS=128
8 28.774499146	192.168.200.150	PcsCompu_39:7d:fe	ARP	69 103 - 103 [ARP] Seq=0 Win=100 Len=64 Tsvl=810535438 Tsecr=0 WS=128
9 28.7745164619	PcsCompu_39:7d:fe	192.168.200.150	ARP	42 192 - 168.200.100.15 18 08:00:27:39:7d:fe
10 28.774852257	PcsCompu_39:7d:fe	192.168.200.150	ARP	42 who has 192.168.200.150 Tell 192.168.200.100
11 28.775230909	PcsCompu_39:7d:fe	192.168.200.150	ARP	42 192 - 168.200.100.15 18 08:00:27:fd:87:1e
12 36.774414345	192.168.200.150	192.168.200.150	TCP	74 41384 - 23 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535437 Tsecr=0 WS=128
13 36.774414345	192.168.200.150	192.168.200.150	TCP	74 41384 - 111 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535437 Tsecr=0 WS=128
14 36.7744237641	192.168.200.150	192.168.200.150	TCP	74 41384 - 103 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535437 Tsecr=0 WS=128
15 36.774436305	192.168.200.150	192.168.200.150	TCP	74 58636 - 543 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535438 Tsecr=0 WS=128
16 36.774436305	192.168.200.150	192.168.200.150	TCP	74 52358 - 543 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535438 Tsecr=0 WS=128
17 36.774435534	192.168.200.150	192.168.200.150	TCP	74 40138 - 99 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535438 Tsecr=0 WS=128
18 36.774614776	192.168.200.150	192.168.200.150	TCP	74 41382 - 21 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535438 Tsecr=0 WS=128
19 36.774614776	192.168.200.150	192.168.200.150	TCP	74 41384 - 46138 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535438 Tsecr=0 WS=128
20 36.774614776	192.168.200.150	192.168.200.150	TCP	74 41384 - 46138 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535438 Tsecr=0 WS=128
21 36.774656596	192.168.200.150	192.168.200.150	TCP	68 443 - 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22 36.774656597	192.168.200.150	192.168.200.150	TCP	68 554 - 58633 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23 36.774656597	192.168.200.150	192.168.200.150	TCP	68 139 - 52356 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24 36.774709464	192.168.200.100	192.168.200.150	TCP	66 41384 - 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535438 Tsecr=0 WS=128
25 36.774732121	192.168.200.100	192.168.200.150	TCP	66 565128 - 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535438 Tsecr=0 WS=128
26 36.774732121	192.168.200.100	192.168.200.150	TCP	67 41384 - 110 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535438 Tsecr=0 WS=128
27 36.77511104	192.168.200.150	192.168.200.150	TCP	74 21 - 41102 [SYN, ACK] Seq=1 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 Tsvl=4294952466 Tsecr=0 WS=64
28 36.77511104	192.168.200.150	192.168.200.150	TCP	74 41182 - 21 [ACK] Seq=1 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535438 Tsecr=0 WS=128
29 36.775337890	192.168.200.100	192.168.200.150	TCP	74 59174 - 111 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535438 Tsecr=0 WS=128
30 36.775337890	192.168.200.100	192.168.200.150	TCP	74 59174 - 111 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535438 Tsecr=0 WS=128
31 36.775342504	192.168.200.100	192.168.200.150	TCP	74 55682 - 80 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535438 Tsecr=0 WS=128
32 36.775342504	192.168.200.100	192.168.200.150	TCP	74 55682 - 80 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535438 Tsecr=0 WS=128
33 36.775619454	192.168.200.100	192.168.200.150	TCP	66 41384 - 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535439 Tsecr=0 WS=128
34 36.775652497	192.168.200.100	192.168.200.150	TCP	66 565128 - 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535439 Tsecr=0 WS=128
35 36.775652497	192.168.200.100	192.168.200.150	TCP	67 41384 - 110 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535439 Tsecr=0 WS=128
36 36.775652497	192.168.200.100	192.168.200.150	TCP	74 22 - 55565 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 Tsvl=4294952466 Tsecr=0 WS=128
37 36.775808180	192.168.200.100	192.168.200.150	TCP	74 40980 - 53062 [SYN, ACK] Seq=0 Ack=1 Win=64256 Len=0 MSS=1460 SACK_PERM=1 Tsvl=4294952466 Tsecr=0 WS=128
38 36.775808180	192.168.200.100	192.168.200.150	TCP	74 55682 - 80 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535439 Tsecr=0 WS=128
39 36.775861964	192.168.200.100	192.168.200.150	TCP	66 41182 - 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535439 Tsecr=0 WS=128
40 36.775975876	192.168.200.100	192.168.200.150	TCP	66 55656 - 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535439 Tsecr=0 WS=128

- Questo screenshot mostra pacchetti SYN e RST, che sono tipici di una scansione SYN da Nmap. Può essere utilizzato per spiegare come questi pacchetti indicano un tentativo di scoperta di porte aperte (IoC).

Analisi del traffico sospetto

48 36.775975876	192.168.200.100	192.168.200.150	TCP	66 55056 - 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535439 Tsecr=0 WS=128
49 36.775975876	192.168.200.100	192.168.200.150	TCP	66 55092 - 103 [SYN, ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535439 Tsecr=0 WS=128
50 36.775975876	192.168.200.100	192.168.200.150	TCP	74 40980 - 130 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535439 Tsecr=0 WS=128
51 36.775975876	192.168.200.100	192.168.200.150	TCP	74 52358 - 985 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535439 Tsecr=0 WS=128
52 36.776338618	192.168.200.100	192.168.200.150	TCP	74 34648 - 587 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tsecr=0 WS=128
53 36.776338618	192.168.200.100	192.168.200.150	TCP	74 33842 - 445 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tsecr=0 WS=128
54 36.776385694	192.168.200.100	192.168.200.150	TCP	74 49814 - 256 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tsecr=0 WS=128
55 36.776425098	192.168.200.100	192.168.200.150	TCP	74 49814 - 50868 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535439 Tsecr=0 WS=128
56 36.776425098	192.168.200.100	192.168.200.150	TCP	66 993 - 50868 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535439 Tsecr=0 WS=128
57 36.776425098	192.168.200.100	192.168.200.150	TCP	74 40980 - 139 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tsecr=0 WS=128
58 36.776425098	192.168.200.100	192.168.200.150	TCP	74 33266 - 143 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tsecr=0 WS=128
59 36.776512221	192.168.200.100	192.168.200.150	TCP	74 68632 - 25 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tsecr=0 WS=128
60 36.776512221	192.168.200.100	192.168.200.150	TCP	74 68632 - 110 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tsecr=0 WS=128
61 36.776512221	192.168.200.100	192.168.200.150	TCP	74 68632 - 110 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tsecr=0 WS=128
62 36.776512221	192.168.200.100	192.168.200.150	TCP	74 73780 - 99 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tsecr=0 WS=128
63 36.776512221	192.168.200.100	192.168.200.150	TCP	74 54598 - 599 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tsecr=0 WS=128
64 36.776729715	192.168.200.100	192.168.200.150	TCP	68 587 - 33468 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
65 36.776843223	192.168.200.100	192.168.200.150	TCP	74 51534 - 487 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tsecr=0 WS=128
66 36.776843223	192.168.200.100	192.168.200.150	TCP	74 445 - 33642 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tsecr=0 WS=128
67 36.776948422	192.168.200.100	192.168.200.150	TCP	66 250 - 49814 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
68 36.776948422	192.168.200.100	192.168.200.150	TCP	68 143 - 32366 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
69 36.776958004	192.168.200.100	192.168.200.150	TCP	74 25 - 68632 - 139 [SYN] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 Tsvl=4294952466 Tsecr=0 WS=64
70 36.776958004	192.168.200.100	192.168.200.150	TCP	68 143 - 54981 [SYN] Seq=0 Ack=1 Win=64256 Len=0 MSS=1460 SACK_PERM=1 Tsvl=4294952466 Tsecr=0 WS=64
71 36.776958004	192.168.200.100	192.168.200.150	TCP	68 143 - 54982 [SYN] Seq=0 Ack=1 Win=64256 Len=0 MSS=1460 SACK_PERM=1 Tsvl=4294952466 Tsecr=0 WS=64
72 36.776958004	192.168.200.100	192.168.200.150	TCP	74 34126 - 98 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tsecr=0 WS=128
73 36.777337394	192.168.200.100	192.168.200.150	TCP	74 47980 - 78 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535441 Tsecr=0 WS=128
74 36.777118481	192.168.200.100	192.168.200.150	TCP	68 687 - 56999 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
75 36.777438741	192.168.200.100	192.168.200.150	TCP	66 436 - 35638 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
76 36.777438741	192.168.200.100	192.168.200.150	TCP	66 436 - 35639 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
77 36.777522914	192.168.200.100	192.168.200.150	TCP	74 52428 - 982 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535441 Tsecr=0 WS=128
78 36.777623882	192.168.200.100	192.168.200.150	TCP	68 98 - 34128 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
79 36.777623882	192.168.200.100	192.168.200.150	TCP	68 78 - 49780 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

- Questo screenshot evidenzia la ripetizione di pacchetti SYN e RST, il che può indicare una scansione di rete Nmap. Qui si può approfondire come questo tipo di traffico sia indicativo di un'attività sospetta.

Ipotesi sui vettori di attacco

79 36_777623149	192.168.200.150	192.168.200.100	TCP	69 78 - 49780	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
80 36_777645627	192.168.200.100	192.168.200.150	TCP	74 48974 - 764	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535441 Tsecr=0 WS=128
81 36_777645627	192.168.200.150	192.168.200.100	TCP	74 49000 - 764	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535441 Tsecr=0 WS=128
82 36_777758636	192.168.200.150	192.168.200.100	TCP	69 580 - 36138	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
83 36_777758696	192.168.200.150	192.168.200.100	TCP	69 962 - 52428	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
84 36_777871245	192.168.200.150	192.168.200.100	TCP	69 764 - 41874	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
85 36_777871293	192.168.200.150	192.168.200.100	TCP	69 435 - 51508	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
86 36_777893298	192.168.200.100	192.168.200.150	TCP	69 33042 - 441	[RST, ACK]	Seq=1 Ack=1 Win=64256 Len=0 Tsvval=810535441 Tsecr=4294952466
87 36_777912717	192.168.200.100	192.168.200.150	TCP	69 46990 - 131	[RST, ACK]	Seq=1 Ack=1 Win=64256 Len=0 Tsvval=810535441 Tsecr=4294952466
88 36_777967597	192.168.200.100	192.168.200.150	TCP	69 60632 - 25	[RST, ACK]	Seq=1 Ack=1 Win=64256 Len=0 Tsvval=810535441 Tsecr=4294952466
89 36_778031265	192.168.200.100	192.168.200.150	TCP	69 37282 - 53	[RST, ACK]	Seq=1 Ack=1 Win=64256 Len=0 Tsvval=810535441 Tsecr=4294952466
90 36_778031265	192.168.200.150	192.168.200.100	TCP	74 48974 - 36138	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535441 Tsecr=0 WS=128
91 36_778209161	192.168.200.100	192.168.200.150	TCP	74 48448 - 896	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535441 Tsecr=0 WS=128
92 36_778207838	192.168.200.100	192.168.200.150	TCP	74 54566 - 221	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535442 Tsecr=0 WS=128
93 36_778385846	192.168.200.150	192.168.200.100	TCP	69 148 - 51459	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
94 36_778385948	192.168.200.150	192.168.200.100	TCP	69 886 - 48444	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
95 36_778449494	192.168.200.150	192.168.200.100	TCP	69 221 - 54561	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
96 36_778427791	192.168.200.100	192.168.200.150	TCP	74 42428 - 1667	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535442 Tsecr=0 WS=128
97 36_778591226	192.168.200.100	192.168.200.150	TCP	74 34646 - 268	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535442 Tsecr=0 WS=128
98 36_778614095	192.168.200.100	192.168.200.150	TCP	74 34646 - 268	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535442 Tsecr=0 WS=128
99 36_778614095	192.168.200.150	192.168.200.100	TCP	69 131 - 54262	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
100 36_778614095	192.168.200.150	192.168.200.100	TCP	69 392 - 46316	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
101 36_778614095	192.168.200.150	192.168.200.100	TCP	69 677 - 51276	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
102 36_778614095	192.168.200.150	192.168.200.100	TCP	74 47238 - 84	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535442 Tsecr=0 WS=128
103 36_778614095	192.168.200.150	192.168.200.100	TCP	69 266 - 34646	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
104 36_778614095	192.168.200.150	192.168.200.100	TCP	74 48318 - 392	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535442 Tsecr=0 WS=128
105 36_778614095	192.168.200.150	192.168.200.100	TCP	74 51276 - 677	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535442 Tsecr=0 WS=128
106 36_778826794	192.168.200.150	192.168.200.100	TCP	69 131 - 54262	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
107 36_778844933	192.168.200.150	192.168.200.100	TCP	69 39566 - 856	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535442 Tsecr=0 WS=128
108 36_778844933	192.168.200.150	192.168.200.100	TCP	74 47238 - 84	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535442 Tsecr=0 WS=128
109 36_778844933	192.168.200.150	192.168.200.100	TCP	69 266 - 34646	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
110 36_779122799	192.168.200.150	192.168.200.100	TCP	69 84 - 47238	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
111 36_779145094	192.168.200.150	192.168.200.100	TCP	74 49138 - 948	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535442 Tsecr=0 WS=128
112 36_779252884	192.168.200.150	192.168.200.100	TCP	69 887 - 56542	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
113 36_779273781	192.168.200.150	192.168.200.100	TCP	74 43140 - 214	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535443 Tsecr=0 WS=128
114 36_779389462	192.168.200.150	192.168.200.100	TCP	74 46886 - 106	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535443 Tsecr=0 WS=128
115 36_779354564	192.168.200.150	192.168.200.100	TCP	69 948 - 46138	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
116 36_779378638	192.168.200.150	192.168.200.100	TCP	74 50284 - 138	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535443 Tsecr=0 WS=128
117 36_779397023	192.168.200.150	192.168.200.100	TCP	74 51262 - 266	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535443 Tsecr=0 WS=128
118 36_779605648	192.168.200.150	192.168.200.100	TCP	69 214 - 43140	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0

- Mostra ulteriori dettagli del traffico, con sequenze di pacchetti SYN e RST. Potrebbe essere usato per spiegare l'ipotesi che si tratti di una **SYN scan**, in cui l'attaccante cerca di scoprire quali porte siano aperte.

Azioni correttive per mitigare l'attacco

118 36_779665648	192.168.200.150	192.168.200.100	TCP	69 214 - 43140	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
119 36_779665750	192.168.200.150	192.168.200.100	TCP	69 106 - 46886	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
120 36_779665798	192.168.200.150	192.168.200.100	TCP	69 138 - 58204	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
121 36_779695841	192.168.200.150	192.168.200.100	TCP	69 138 - 51126	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
122 36_779705753	192.168.200.150	192.168.200.100	TCP	74 47238 - 36138	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535442 Tsecr=0 WS=128
123 36_779705753	192.168.200.150	192.168.200.100	TCP	74 47238 - 36138	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535442 Tsecr=0 WS=128
124 36_779705841	192.168.200.150	192.168.200.100	TCP	74 47238 - 36138	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535443 Tsecr=0 WS=128
125 36_779714170	192.168.200.150	192.168.200.100	TCP	74 55137 - 42444	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
126 36_779714170	192.168.200.150	192.168.200.100	TCP	74 55137 - 42444	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535443 Tsecr=0 WS=128
127 36_779835851	192.168.200.150	192.168.200.100	TCP	69 783 - 43630	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
128 36_779842789	192.168.200.150	192.168.200.100	TCP	69 274 - 55136	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
129 36_779844973	192.168.200.150	192.168.200.100	TCP	74 47238 - 36138	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535443 Tsecr=0 WS=128
130 36_779844973	192.168.200.150	192.168.200.100	TCP	74 47238 - 36138	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535443 Tsecr=0 WS=128
131 36_7798215176	192.168.200.150	192.168.200.100	TCP	69 42 - 40522	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
132 36_7798301759	192.168.200.150	192.168.200.100	TCP	69 58 - 57552	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
133 36_7798325837	192.168.200.150	192.168.200.100	TCP	74 37252 - 11	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535444 Tsecr=0 WS=128
134 36_7798346429	192.168.200.150	192.168.200.100	TCP	74 49648 - 235	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535444 Tsecr=0 WS=128
135 36_7798499818	192.168.200.150	192.168.200.100	TCP	74 36548 - 739	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535444 Tsecr=0 WS=128
136 36_779842789	192.168.200.150	192.168.200.100	TCP	74 36548 - 56	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535444 Tsecr=0 WS=128
137 36_7798472839	192.168.200.150	192.168.200.100	TCP	74 52136 - 999	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535444 Tsecr=0 WS=128
138 36_7798498897	192.168.200.150	192.168.200.100	TCP	74 38822 - 317	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535444 Tsecr=0 WS=128
139 36_779857789	192.168.200.150	192.168.200.100	TCP	69 266 - 48822	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
140 36_779857789	192.168.200.150	192.168.200.100	TCP	69 11 - 37252	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
141 36_779857892	192.168.200.150	192.168.200.100	TCP	69 235 - 40648	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
142 36_7798578974	192.168.200.150	192.168.200.100	TCP	69 739 - 36548	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
143 36_7798578119	192.168.200.150	192.168.200.100	TCP	69 55 - 38861	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
144 36_7798578158	192.168.200.150	192.168.200.100	TCP	69 999 - 52136	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
145 36_7798578198	192.168.200.150	192.168.200.100	TCP	69 317 - 38822	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
146 36_780617671	192.168.200.150	192.168.200.100	TCP	74 49446 - 961	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535444 Tsecr=0 WS=128
147 36_780781625	192.168.200.150	192.168.200.100	TCP	74 51192 - 241	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535444 Tsecr=0 WS=128
148 36_780805939	192.168.200.150	192.168.200.100	TCP	69 961 - 49446	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
149 36_7808247418	192.168.200.150	192.168.200.100	TCP	74 42642 - 293	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535444 Tsecr=0 WS=128
150 36_780889399	192.168.200.150	192.168.200.100	TCP	69 24 - 51192	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
151 36_780906549	192.168.200.150	192.168.200.100	TCP	74 41826 - 974	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535444 Tsecr=0 WS=128
152 36_780953937	192.168.200.150	192.168.200.100	TCP	74 49014 - 137	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535444 Tsecr=0 WS=128
153 36_781007599	192.168.200.150	192.168.200.100	TCP	69 29 - 42642	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
154 36_781116689	192.168.200.150	192.168.200.100	TCP	69 974 - 41828	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
155 36_781116971	192.168.200.150	192.168.200.100	TCP	69 137 - 49614	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
156 36_781138769	192.168.200.150	192.168.200.100	TCP	74 45464 - 223	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535444 Tsecr=0 WS=128
157 36_						

157	36.781159927	192.168.200.100	192.168.200.150	TCP	74 427/08 - 1014 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535444 Tsecr=0 WS=128
158	36.781255484	192.168.200.150	192.168.200.100	TCP	60 223 - 45464 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
159	36.78125593	192.168.200.150	192.168.200.100	TCP	60 1014 - 42708 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
160	36.781321950	192.168.200.100	192.168.200.150	TCP	74 55368 - 918 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535445 Tsecr=0 WS=128
161	36.781356928	192.168.200.100	192.168.200.150	TCP	74 45468 - 512 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535445 Tsecr=0 WS=128
162	36.781426319	192.168.200.100	192.168.200.150	TCP	74 45324 - 354 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535445 Tsecr=0 WS=128
163	36.781487105	192.168.200.150	192.168.200.100	TCP	66 918 - 55369 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
164	36.781487210	192.168.200.150	192.168.200.100	TCP	74 512 - 45468 [SYN, ACK] Seq=1 Ack=1 Win=0 Len=0
165	36.781512468	192.168.200.100	192.168.200.150	TCP	66 45648 - 512 [ACK] Seq=1 Ack=1 Win=0 Len=0 Tsvval=810535445 Tsecr=4294952466 WS=64
166	36.781621871	192.168.200.150	192.168.200.100	TCP	66 354 - 53246 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
167	36.781621871	192.168.200.100	192.168.200.150	TCP	74 55368 - 958 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535445 Tsecr=0 WS=128
168	36.781734419	192.168.200.100	192.168.200.150	TCP	74 35898 - 512 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535445 Tsecr=0 WS=128
169	36.781812691	192.168.200.150	192.168.200.100	TCP	66 550 - 55166 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
170	36.782069557	192.168.200.100	192.168.200.150	TCP	66 5540 - 54166 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
171	36.782069592	192.168.200.150	192.168.200.100	TCP	66 683 - 35866 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
172	36.782126749	192.168.200.100	192.168.200.150	TCP	74 38218 - 681 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535445 Tsecr=0 WS=128
173	36.782149866	192.168.200.100	192.168.200.150	TCP	74 47098 - 561 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535445 Tsecr=0 WS=128
174	36.782215891	192.168.200.100	192.168.200.150	TCP	74 32959 - 576 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535445 Tsecr=0 WS=128
175	36.782248180	192.168.200.100	192.168.200.150	TCP	74 38338 - 371 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535445 Tsecr=0 WS=128
176	36.782396789	192.168.200.150	192.168.200.100	TCP	66 681 - 38218 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
177	36.782396884	192.168.200.150	192.168.200.100	TCP	66 561 - 47098 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
178	36.782396930	192.168.200.150	192.168.200.100	TCP	66 570 - 32958 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
179	36.782396978	192.168.200.150	192.168.200.100	TCP	66 371 - 38396 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
180	36.782422713	192.168.200.100	192.168.200.150	TCP	74 43862 - 966 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535446 Tsecr=0 WS=128
181	36.782459407	192.168.200.100	192.168.200.150	TCP	74 42162 - 595 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535446 Tsecr=0 WS=128
182	36.782534412	192.168.200.100	192.168.200.150	TCP	74 55234 - 838 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535446 Tsecr=0 WS=128
183	36.782582077	192.168.200.100	192.168.200.150	TCP	74 3310 - 512 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535446 Tsecr=0 WS=128
184	36.782696538	192.168.200.150	192.168.200.100	TCP	66 966 - 43862 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
185	36.782696651	192.168.200.150	192.168.200.100	TCP	66 595 - 42162 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
186	36.782699713	192.168.200.150	192.168.200.100	TCP	66 838 - 52334 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
187	36.782786553	192.168.200.100	192.168.200.150	TCP	74 53949 - 0 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535446 Tsecr=0 WS=128
188	36.782854473	192.168.200.150	192.168.200.100	TCP	66 51 - 33102 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
189	36.782887993	192.168.200.100	192.168.200.150	TCP	74 44194 - 144 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535446 Tsecr=0 WS=128
190	36.783026182	192.168.200.150	192.168.200.100	TCP	66 55 - 59408 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
191	36.783042408	192.168.200.100	192.168.200.150	TCP	74 42628 - 974 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535446 Tsecr=0 WS=128
192	36.783084243	192.168.200.100	192.168.200.150	TCP	74 58118 - 928 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535446 Tsecr=0 WS=128
193	36.783329650	192.168.200.150	192.168.200.100	TCP	66 144 - 41184 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
194	36.783329795	192.168.200.150	192.168.200.100	TCP	66 874 - 42628 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
195	36.783329836	192.168.200.150	192.168.200.100	TCP	66 926 - 58110 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
196	36.783391839	192.168.200.100	192.168.200.150	TCP	74 42696 - 964 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvval=810535447 Tsecr=0 WS=128

- Un'ultima panoramica del traffico di rete catturato, che mostra ulteriori tentativi di connessione falliti (pacchetti RST). Questa immagine è utile per riassumere l'analisi e collegare il tutto all'uso di Nmap.