

S9L3,

BENVENUTI LUIGI

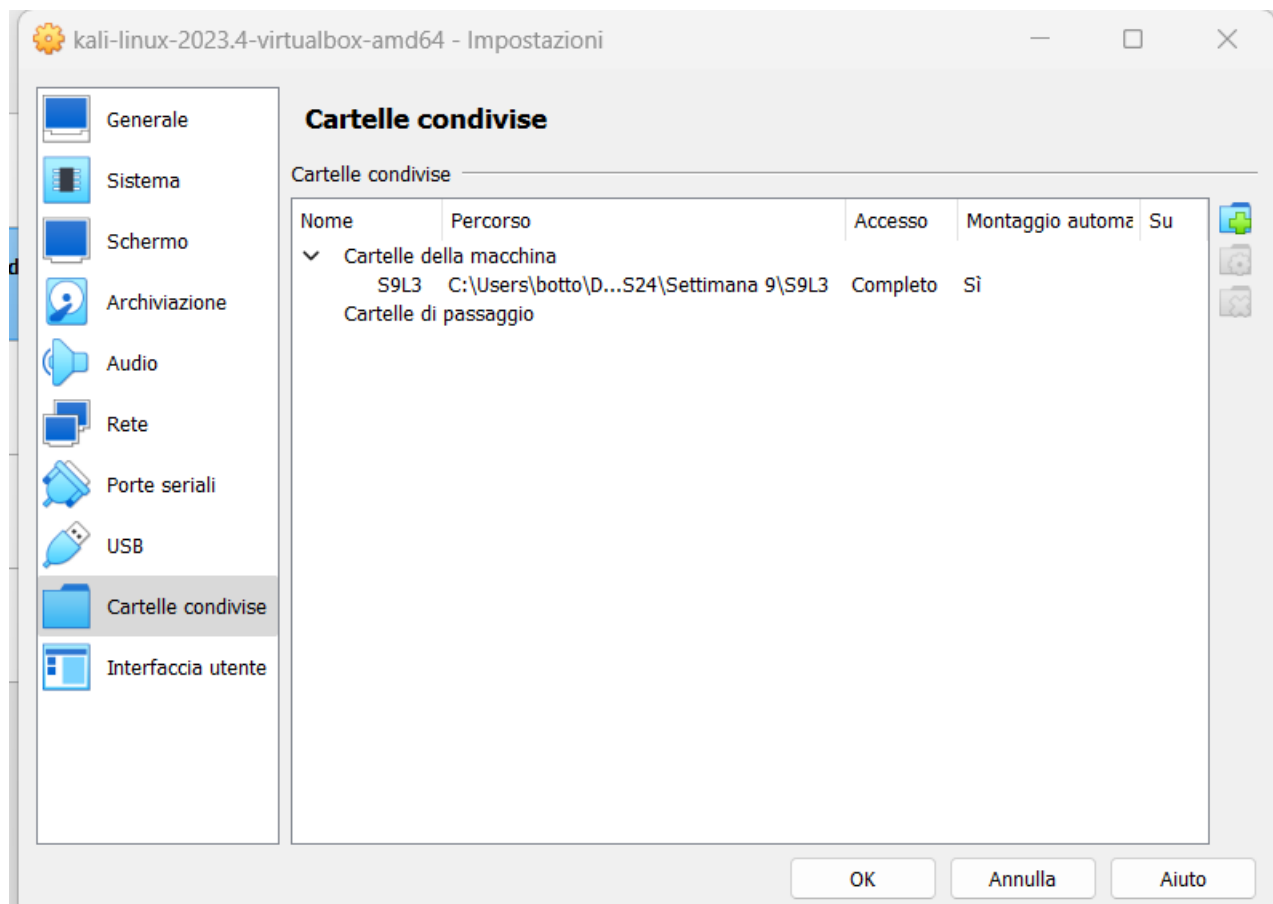
### **Traccia:**

Durante la lezione teorica, abbiamo visto la Threat Intelligence e gli indicatori di compromissione. Abbiamo visto che gli IOC sono evidenze o eventi di un attacco in corso, oppure già avvenuto.

Per l'esercizio pratico di oggi, trovate in allegato una cattura di rete effettuata con Wireshark. Analizzate la cattura attentamente e rispondere ai seguenti quesiti: Identificare eventuali IOC, ovvero evidenze di attacchi in corso in base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati.

Consigliate un'azione per ridurre gli impatti dell'attacco.

Condividiamo il file scaricato in una cartella condivisa con la macchina virtuale Kali Linux in Virtual Box.



Individuiamo il path del file dal terminale.

```
root@kali: /media/sf_S9L3
File Actions Edit View Help
(kali@kali)-[~]
$ cd /
(kali@kali)-[/]
$ sudo su
[sudo] password for kali:
(root@kali)-[/]
# ls
bin  dev  home  initrd.img.old  lib32  lost+found  mnt  proc  run  srv  sys  usr  vmlinuz
boot  etc  initrd.img  lib  lib64  media  opt  root  sbin  swapfile  tmp  var  vmlinuz.old
(root@kali)-[/]
# cd /media
(root@kali)-[/media]
# ls
sf_S9L3  sf_Settimana_8
(root@kali)-[/media]
# cd sf_S9L3
(root@kali)-[/media/sf_S9L3]
# ls
Cattura_U3_W1_L3.pcapng  Cattura_U3_W1_L3.zip  condivisa.png
(root@kali)-[/media/sf_S9L3]
#
```

E spostiamo il file sul desktop.

```
(root@kali)-[/media/sf_S9L3]
# mv Cattura_U3_W1_L3.pcapng /home/kali/Desktop
```

E verifichiamo quali permessi abbiamo sul file.

```
(root@kali)-[/home/kali/Desktop]
# ls -la
total 216
drwxr-xr-x  2 kali kali    4096 Mar 20 11:37 .
drwx----- 22 kali kali    4096 Mar 20 11:34 ..
-rwxrwx---  1 root vboxsf 209024 Nov 13 10:00 Cattura_U3_W1_L3.pcapng
```

A questo punto vediamo quali aspetti prendere in considerazione nel monitoraggio:

1. Identificare eventuali IOC, ovvero evidenze di attacchi in corso;
2. In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati;
3. Consigliate un'azione per ridurre gli impatti dell'attacco;
4. Potremmo configurare delle policy firewall per bloccare accesso a tutte le porta da parte di quel determinato attaccante, in modo tale da evitare che informazioni circa porta / servizi in ascolto finiscano nelle mani dell'attaccante.

Dalla cattura notiamo che ci sono un numero elevato di richieste TCP (SYN) su porte sempre diverse in destinazione.

13	36.774218116	192.168.200.100	192.168.200.150	TCP	74 56120 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
14	36.774257841	192.168.200.100	192.168.200.150	TCP	74 33878 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
15	36.774366305	192.168.200.100	192.168.200.150	TCP	74 58636 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
16	36.774485627	192.168.200.100	192.168.200.150	TCP	74 52358 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
17	36.774535534	192.168.200.100	192.168.200.150	TCP	74 46138 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
18	36.774614776	192.168.200.100	192.168.200.150	TCP	74 41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
19	36.774685505	192.168.200.150	192.168.200.100	TCP	74 23 → 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
20	36.774685652	192.168.200.150	192.168.200.100	TCP	74 111 → 56120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
21	36.774685696	192.168.200.150	192.168.200.100	TCP	60 443 → 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	36.774685737	192.168.200.150	192.168.200.100	TCP	60 554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	36.774685776	192.168.200.150	192.168.200.100	TCP	60 135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	36.774709464	192.168.200.100	192.168.200.150	TCP	66 41304 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TS=
25	36.774711072	192.168.200.100	192.168.200.150	TCP	66 56120 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TS=
26	36.775111004	192.168.200.150	192.168.200.100	TCP	60 993 → 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	36.775141273	192.168.200.150	192.168.200.100	TCP	74 21 → 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
28	36.775174948	192.168.200.100	192.168.200.150	TCP	66 41182 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TS=
29	36.775337880	192.168.200.100	192.168.200.150	TCP	74 59174 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
30	36.775386694	192.168.200.100	192.168.200.150	TCP	74 55656 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
31	36.775524204	192.168.200.100	192.168.200.150	TCP	74 53062 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
32	36.775589806	192.168.200.150	192.168.200.100	TCP	60 113 → 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	36.775619454	192.168.200.100	192.168.200.150	TCP	66 41304 → 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0
34	36.775652497	192.168.200.100	192.168.200.150	TCP	66 56120 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0
35	36.775790936	192.168.200.150	192.168.200.100	TCP	74 22 → 55656 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
36	36.775797004	192.168.200.150	192.168.200.100	TCP	74 80 → 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
37	36.775803786	192.168.200.100	192.168.200.150	TCP	66 55656 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TS=

Questo ci fa pensare ad una potenziale scansione in corso da parte dell'host 192.168.200.100 verso l'host target 192.168.200.150.

Questa ipotesi è supportata dal fatto che per alcune righe della cattura vediamo risposte positive del target [SYN+ACK] ad indicare che la porta è aperta; per altre, invece, notiamo la risposta [RST+ACK] ad indicare che la porta è chiusa.

Lato target, si potrebbero configurare delle regole firewall per respingere le richieste in entrata dall'host 192.168.200.100.

```
(kali㉿kali)-[~]  
$ sudo iptables -A INPUT -s 192.168.200.0/24 -j DROP
```

La nuova regola è stata inserita.

```
(kali㉿kali)-[~]  
$ sudo iptables -S  
-P INPUT ACCEPT  
-P FORWARD ACCEPT  
-P OUTPUT ACCEPT  
-A INPUT -s 192.168.200.0/24 -j DROP
```