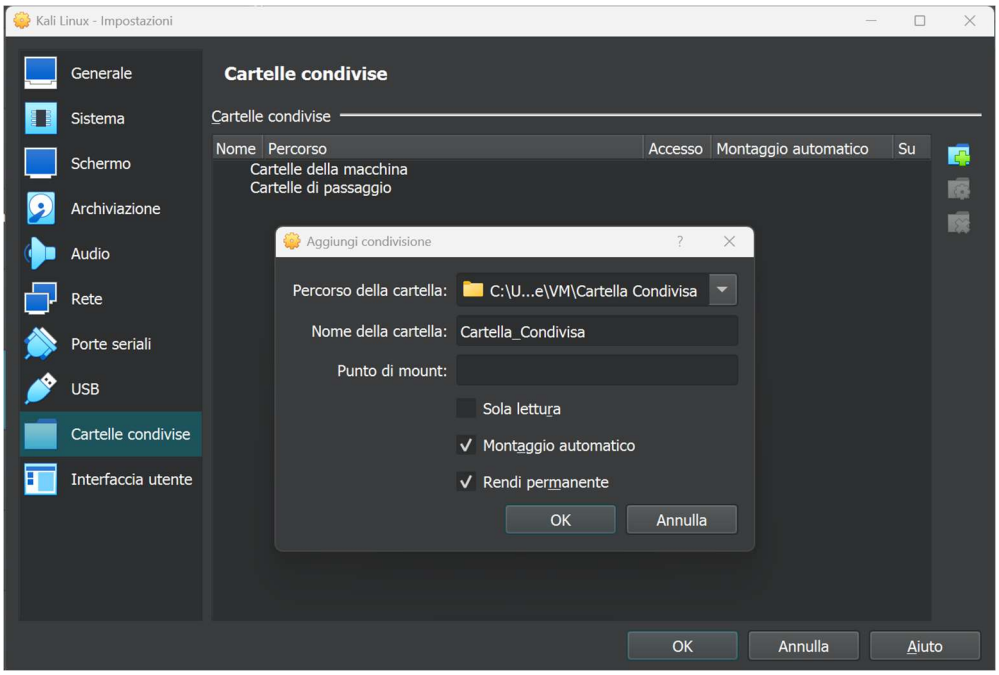
Per prima cosa andiamo a creare la cartella condivisa:



Andiamo poi a trasferire il file e dare i permessi al nostro utente sul file stesso

```
┌──(kali㉿kali)-[~]
└─$ cd /

┌──(kali㉿kali)-[/]
└─$ cd media

┌──(kali㉿kali)-[/media]
└─$ ls
sf_Cartella_Condivisa

┌──(kali㉿kali)-[/media]
└─$ cd sf_Cartella_Condivisa

┌──(kali㉿kali)-[/media/sf_Cartella_Condivisa]
└─$ ls
Cattura_U3_W1_L3.pcapng

┌──(kali㉿kali)-[/media/sf_Cartella_Condivisa]
└─$ mv Cattura_U3_W1_L3.pcapng /home/kali/Desktop

┌──(kali㉿kali)-[/media/sf_Cartella_Condivisa]
└─$ cd /home/kali/Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ chmod ugo+rw Cattura_U3_W1_L3.pcapng

┌──(kali㉿kali)-[~/Desktop]
└─$ chown kali Cattura_U3_W1_L3.pcapng

┌──(kali㉿kali)-[~/Desktop]
└─$ ls -a
.  ..  Cattura_U3_W1_L3.pcapng

┌──(kali㉿kali)-[~/Desktop]
└─$ ls -la
total 216
drwxr-xr-x  2 kali kali     4096 Oct 11 10:29 .
drwx------ 22 kali kali     4096 Oct 11 10:23 ..
-rwxrwxrw-  1 kali vboxsf 209024 Oct 11 10:18 Cattura_U3_W1_L3.pcapng

┌──(kali㉿kali)-[~/Desktop]
└─$
```

Una volta aperto il file, ci accorgiamo di essere davanti a un attacco DOS, in particolare un SYN Flood, una tipologia di attacco dove l'attaccante manda una grande quantità di pacchetti SYN alla vittima, senza mai chiudere l'handshake e andando così a sovraccaricare il destinatario.

Identificare ed analizzare eventuali IOC, ovvero evidenze di attacchi in corso:

Gli indicatori di compromissione presenti a mio avviso sono, una grande quantità di pacchetti SYN che partono dallo stesso host e arrivano allo stesso destinatario, il fatto che l'handshake non venga mai completato e il server rigetti tutte le connessioni (ciò potrebbe accadere sia grazie al firewall ma anche a causa di un sovraccarico delle risorse) e il fatto che tutte queste richieste partano e arrivino dallo stesso host ma a porte differenti, probabilmente come tecnica di evasione dei sistemi di sicurezza.

In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati:

La soluzione più semplice potrebbe essere un software come LOIC , che permette l'invio in grandi quantità di una serie di pacchetti di piccole dimensioni.

Si potrebbe azzardare anche l'ipotesi di un attacco DDoS o di una botnet, dove il traffico prima di essere indirizzato verso il bersaglio viene mascherato o fatto passare per un indirizzo "ponte", in modo da mascherare gli IP iniziali degli attaccanti, ma mi sembra la soluzione meno probabile, perché questo effetto a "collo di bottiglia" faciliterebbe la difesa del nostro server, permettendoci di chiudere una connessione sola per bloccarle tutte.

Consigliate un'azione per ridurre gli impatti dell'attacco attuale ed eventualmente un simile attacco futuro

La prima soluzione che suggerirei è implementare una regola di firewall che va a mettere in blacklist un indirizzo IP sospetto che genera una grande quantità di richieste in pochissimo tempo.

Anche l'introduzione di un IPS potrebbe essere una valida soluzione, in modo che possa mitigare eventuali attacchi.

Infine, una soluzione ottima potrebbe essere affidarsi a un servizio di protezione DDoS come Cloudflare.