REPORT S7-L2

Per lo svolgimento dell'esercizio ho prima configurato le due macchine per stare sulla stessa rete. Successivamente ho lanciato msfconsole da Kali e cercato il modulo per la vulnerabilità (scanner/telnet/telnet_version). Ho configurato l'RHOST con l'IP della Metasploitable e usato a questo punto il comando run.
Il risultato ci conferisce i parametri del login che poi ho provato per creare una connessione Telnet.


File Actions Edit View Help
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > bg
[-] Unknown command: bg. Run the help command for more details.
msf6 auxiliary(scanner/telnet/telnet_version) > back
msf6 > telnet 192.168.1.40
[*] exec: telnet 192.168.1.40
Trying 192.168.1.40 ...
Connected to 192.168.1.40.
Escape character is '^]'.
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: Tue Dec 17 08:23:57 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.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
::1 ff02::1 ip6-allhosts ip6-localhost
fe00::0 ff02::2 ip6-allnodes ip6-localnet
ff00::0 ff02::3 ip6-allrouters ip6-loopback
msfadmin@metasploitable:~$