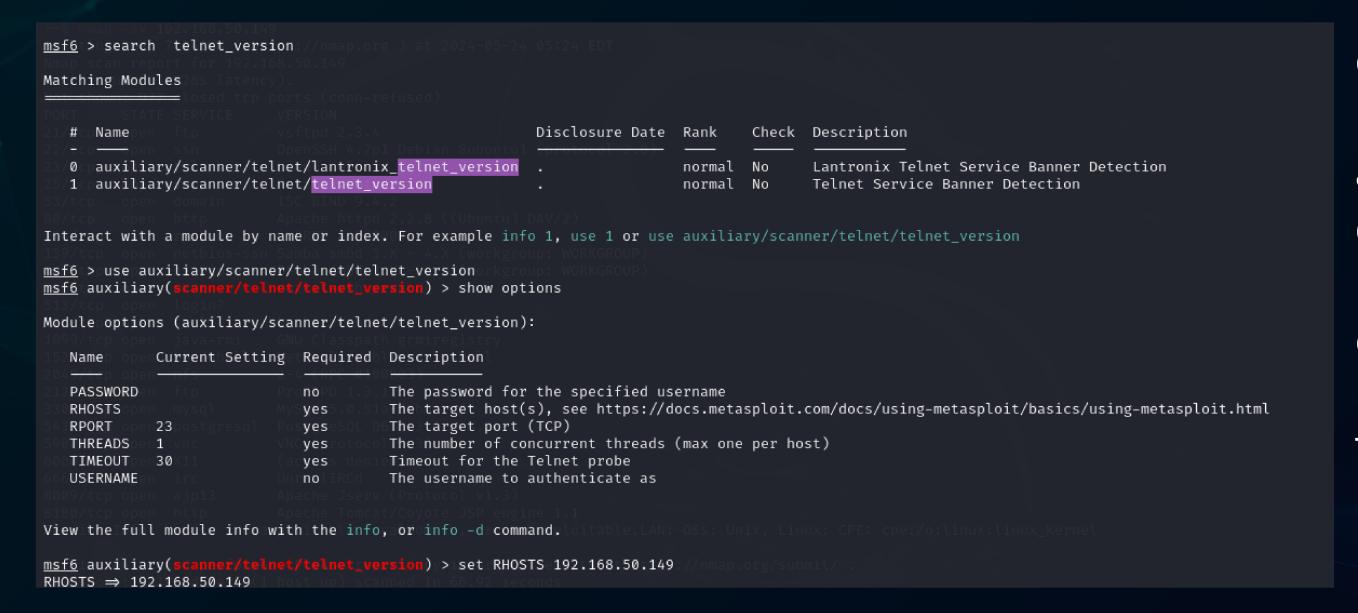


Home Video About Us Contact





Telnet è un protocollo di rete che consente l'accesso remoto a dispositivi attraverso una connessione di rete non crittografata. L'obiettivo di questa sessione è stato esplorare e sfruttare una vulnerabilità nel servizio Telnet per ottenere l'accesso non autorizzato alla macchina target.

Telnet è noto per essere vulnerabile a molte forme di attacchi, inclusi i Brute Force per le password deboli.

Ho selezionato auxiliary/scanner/telnet/telnet_version come modulo di exploit. Poi ho impostato l'indirizzo IP del bersaglio mentre gli altri parametri erano già impostati di default. Infine ho eseguito l'exploit per sfruttare la vulnerabilità e ottenere l'accesso non autorizzato alla macchina target.



L'exploit è stato eseguito per sfruttare la vulnerabilità e ottenere l'accesso non autorizzato alla macchina target.

Una volta finito viene visualizzato l'username e la password del per poter entrare nel servizio, così ho provato ad accedere inserendo telnet <ip_target> e dopo l'username e la password trovate, riuscendo così ad entrare nella macchina.

Per confermare la riuscita dell'exploit ho eseguito il comando ifconfig per verificare se l'ip fosse quello coretto.

–(kali⊕kali)-[~] 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: Fri May 24 05:24:26 EDT 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:~\$ ifconfig

Link encap:Ethernet HWaddr 08:00:27:2d:a6:3b

Base address:0×d020 Memory:f0200000-f0220000

collisions:0 txqueuelen:1000

inet6 addr: fe80::a00:27ff:fe2d:a63b/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:1567 errors:0 dropped:0 overruns:0 frame:0
TX packets:1568 errors:0 dropped:0 overruns:0 carrier:0

RX bytes:125298 (122.3 KB) TX bytes:129020 (125.9 KB)

03