Report exploit telnet su Metasploitable2

Introduzione

In questo esercizio, ho utilizzato il framework Metasploit per sfruttare la vulnerabilità del servizio telnet sulla macchina metasploitable2 per conoscere l'username e la password.

1. Ho avviato Metasploit ed ho usato l'exploit: **auxiliary/scanner/telnet/telnet_version**
2. Ho visualizzato le opzioni disponibili per configurare l'exploit con il comando: **show options.**
3. Ho impostato l'host di destinazione **(RHOSTS) su 192.168.1.40** e lasciato gli altri parametri di default.

```
msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   RHOSTS                     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/
                                        basics/using-metasploit.html
   RPORT     23               yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one per host)
   TIMEOUT   30               yes       Timeout for the Telnet probe
   USERNAME                   no        The username to authenticate as


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.40
rhosts ⇒ 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   RHOSTS    192.168.1.40     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/
                                        basics/using-metasploit.html
   RPORT     23               yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one per host)
   TIMEOUT   30               yes       Timeout for the Telnet probe
   USERNAME                   no        The username to authenticate as
```

Telenet è un protocollo di rete utilizzato per accedere a un computer remoto attraverso una rete, come Internet. Permette agli utenti di aprire una sessione di terminale su un dispositivo remoto e di controllarlo come se fossero fisicamente presenti.
Telenet trasmette i dati, comprese le credenziali di accesso, in testo semplice (non criptato). Questo significa che un attaccante può intercettare queste informazioni.

Esecuzione dell’exploit

- Ho eseguito l'exploit con il comando **run** o **exploit.**

Dopo che l’exploit è andato a buon fine sono riuscito a visualizzare l’username e la password della macchina metasploitable.