ESERCIZIO 2 SETTIMANA 7

Inizio subito con nmap per fare una scansione e veder qiali sono le porte e i servizi attivi. Nell'esercizio di oggi mi conventrerò sul servizio telnet.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV 192.168.178.125
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-23 03:31 EST
Nmap scan report for 192.168.178.125
Host is up (0.0037s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec?
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Lin
ux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/sub
mit/ .
Nmap done: 1 IP address (1 host up) scanned in 63.83 seconds
```

Individuato il servizio. Dopo essermi connesso alla msfconsole cerco gli ausiliari per quella vulnerabilità.

```
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
```

Con set rhostsn imposto l’IP della vittima e verifico sia stato settato correttamente con show options.

```
msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.178.125
rhosts ⇒ 192.168.178.125
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    192.168.178.125  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
```

Infine esegue l’exploit.

```
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[+] 192.168.178.125:23    - 192.168.178.125:23 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
:
[*] 192.168.178.125:23    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Come test per verificare che tutto abbia funzionato utilizzo ifconfig; se tutto ha funzionato vedrò l’IP della vittima.

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:f2:31:c7
          inet addr:192.168.178.125  Bcast:192.168.178.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fef2:31c7/64 Scope:Link
```