


Initial Exploitation Report

Executive Summary

This phase involved testing known vulnerabilities discovered during the vulnerability assessment using **Metasploit** and **Hydra**. A successful remote code execution (RCE) was achieved via the vsFTPD 2.3.4 backdoor exploit, confirming system compromise. Additionally, password attack techniques were attempted on the SSH service using a wordlist with Hydra. All actions were executed within a controlled lab environment.

♦ Methodical Exploitation with Metasploit

- **Tool Used:** Metasploit Framework v6.3.54-dev
 - **Target Service:** FTP (`vsftpd 2.3.4`)
 - **Exploit Module Used:** `exploit/unix/ftp/vsftpd_234_backdoor`
 - **Steps Taken:**
 - Launched `msfconsole`
 - Selected the exploit module for vsFTPD backdoor
 - Set `RHOSTS` to the target: `10.138.16.109`
 - Ran the exploit
 - **Result:**
 - Backdoor service was triggered
 - A command shell session was opened as **root** (`UID=0`)
 - Verified file system access using `ls` command
 -  **Exploit Successful**
 - **Proof of Concept:** Root shell obtained (Screenshot provided)
-

Password Attack Attempt with Hydra

- **Tool Used:** Hydra v9.4
- **Target Service:** SSH (`port 22`)

Command Used:

bash

CopyEdit

```
hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://10.138.16.109
```

•

- **Result:**
 - Attempt failed due to missing wordlist file: `rockyou.txt`
 - No brute force performed
- **✗ Attack Unsuccessful (for now)**
 - **Error:** `[ERROR] File for passwords not found: /usr/share/wordlists/rockyou.txt`

Recommendation: Re-download the `rockyou.txt` file using:

bash

CopyEdit

```
sudo gzip -d /usr/share/wordlists/rockyou.txt.gz
```

◦

Summary of Activities

Activity	Tool	Target Service	Result
RCE Exploitation	Metasploit	FTP (vsFTPD)	✓ Successful (shell)
Password Brute Force	Hydra	SSH	✗ Failed (missing wordlist)

Safety and Scope

- All tests were performed within the isolated **Parrot OS – Metasploitable 2** lab setup.
- No tests were conducted outside the defined environment.
- No real-world systems were targeted.