# Cyber Security Project Report

## Clash of Teams 101 – Breach & Defend Simulation

**Submitted By:** Aniket Pandurang Pawar
SOC Analyst Aspirant | Cyber Security
LinkedIn: https://www.linkedin.com/in/aniket-pawar-109a312ba

**Project Type:** Red Team & Blue Team Simulation

## 1. Executive Summary

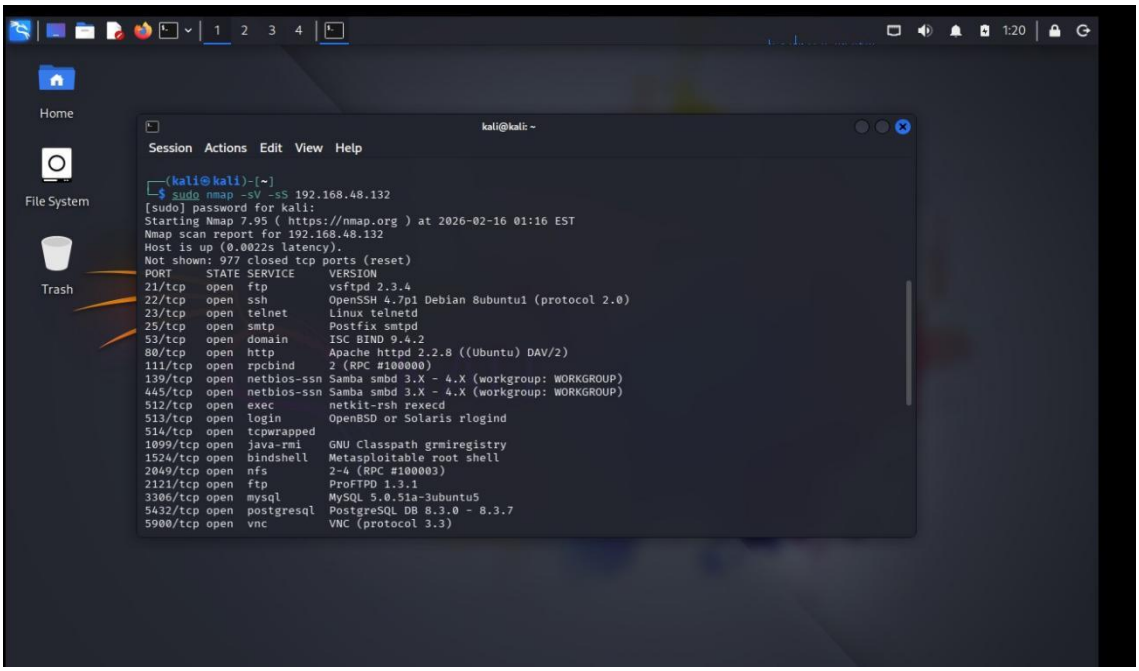
This project demonstrates a complete Red Team and Blue Team adversarial simulation using a vulnerable vsftpd 2.3.4 service hosted on a Metasploitable virtual machine. The Red Team performed reconnaissance, identified an exposed FTP service, and exploited a known backdoor vulnerability to gain unauthorized root access. The Blue Team analyzed system logs, detected suspicious activity, identified the attacker IP address, and implemented firewall rules to contain the threat.

## 2. Lab Environment Setup

Attacker Machine: Kali Linux (192.168.48.143)
Target Machine: Metasploitable 2 (192.168.48.102) Network Mode: Host-Only Adapter

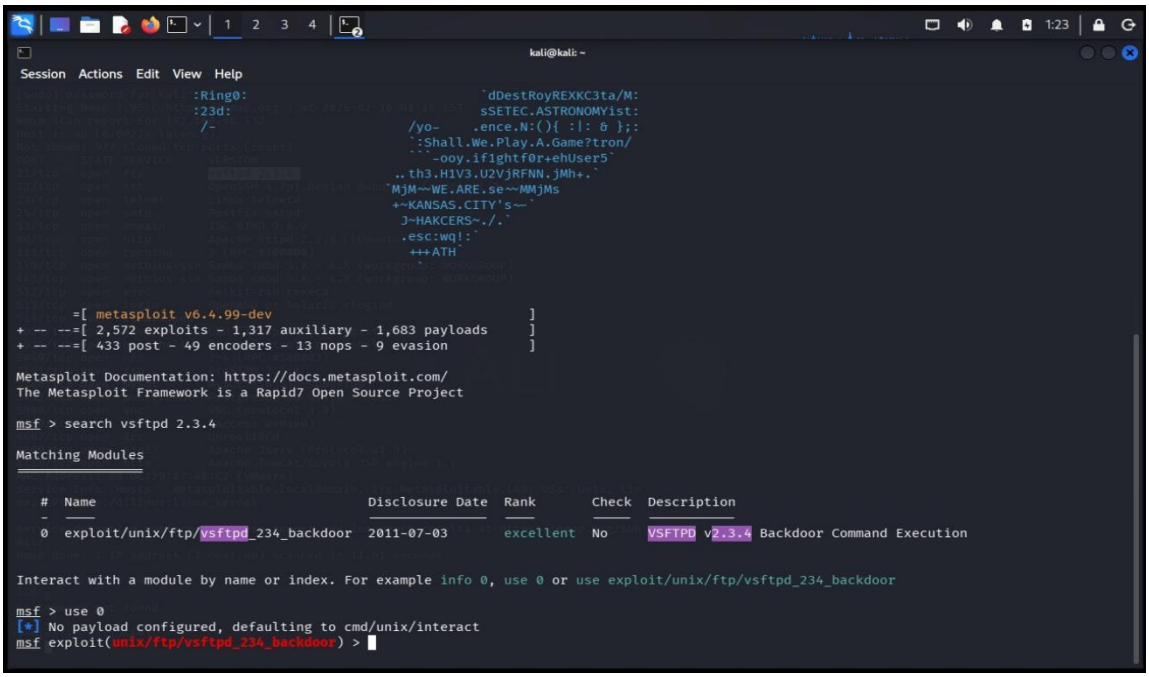
## 1. Reconnaissance – Nmap Scan

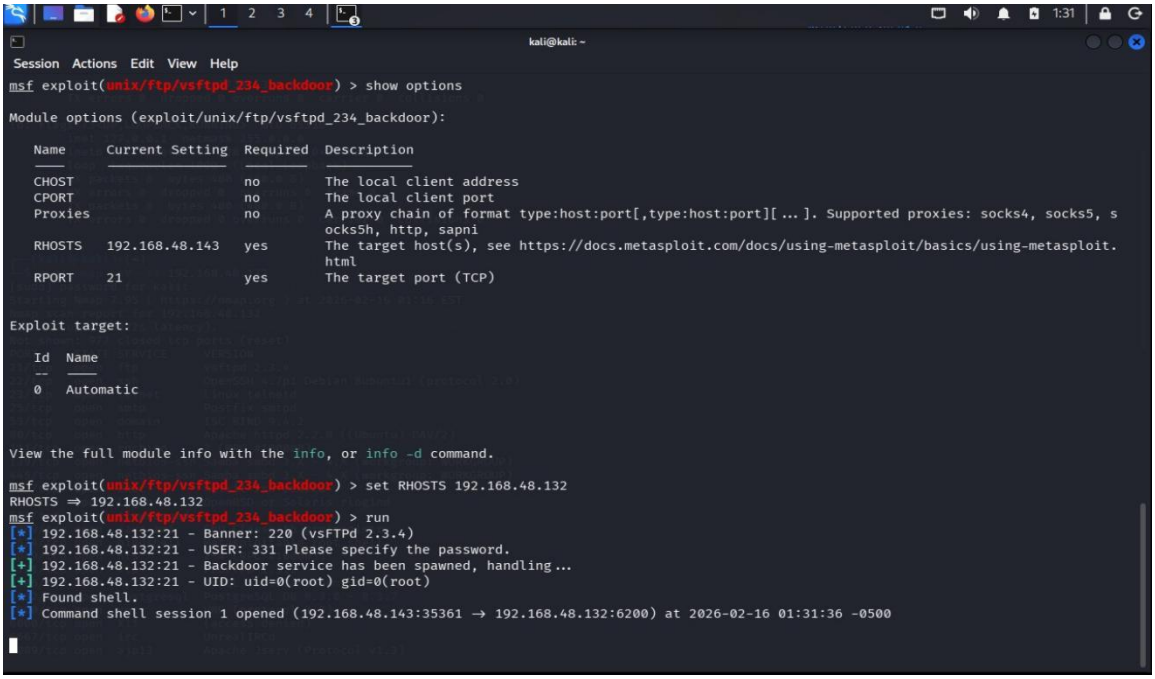
Initial scan identified vsftpd 2.3.4 running on port 21.



## 2. Exploitation – Metasploit Execution

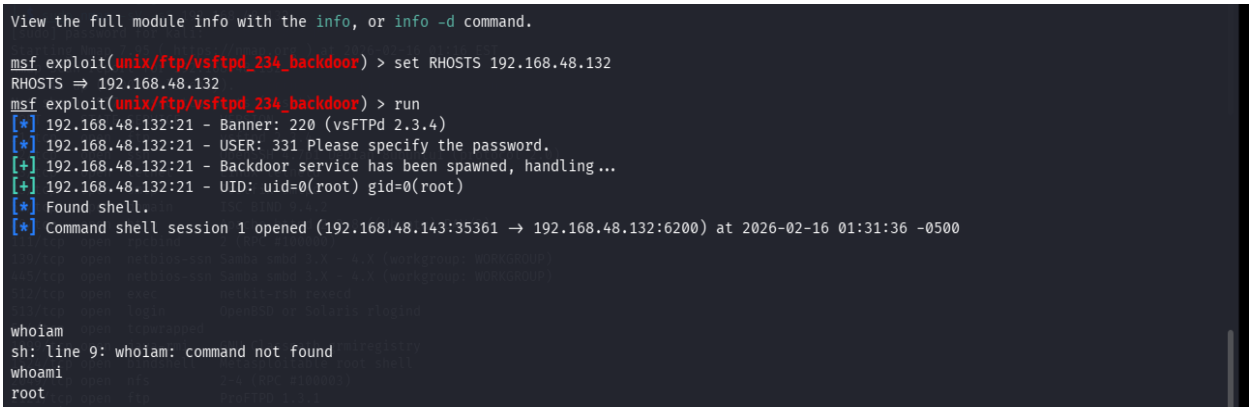
The exploit/unix/ftp/vsftpd_234_backdoor module was used to gain root shell access.



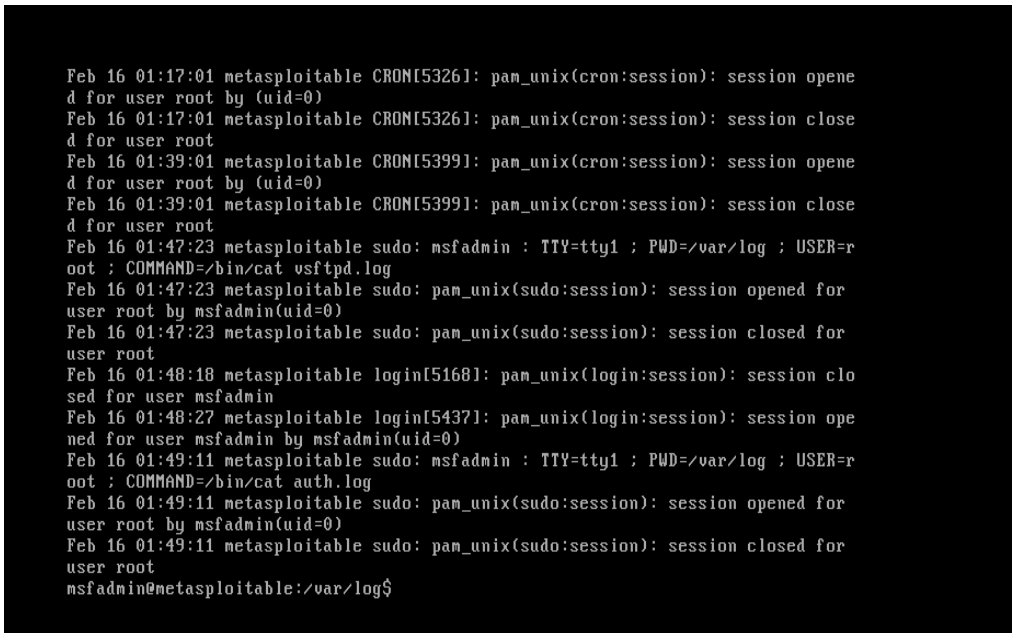
## 3. Root Access Confirmation

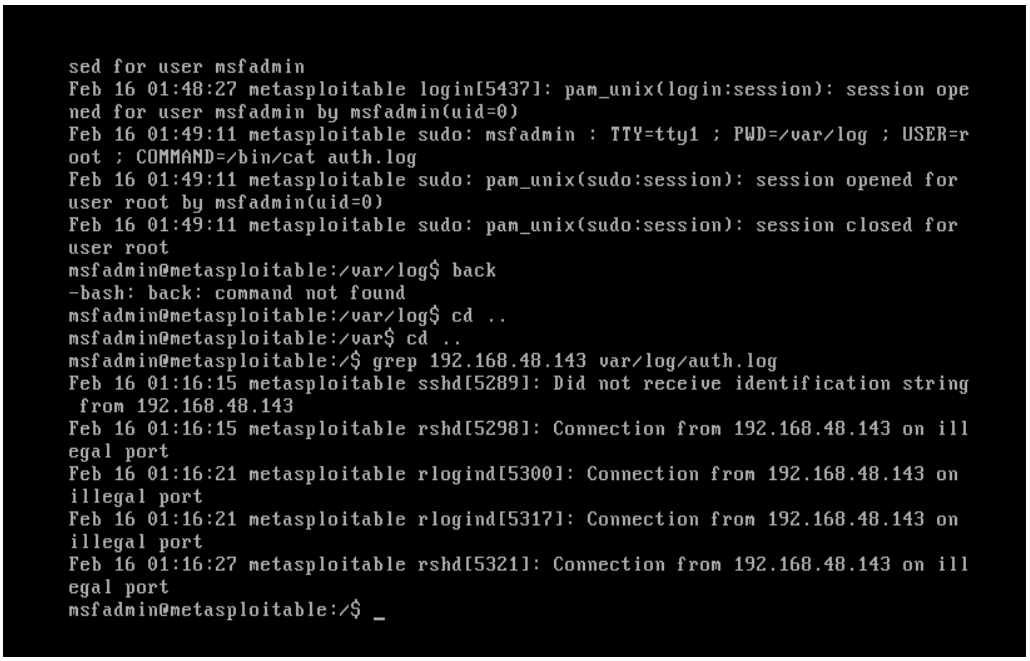
Successful privilege escalation confirmed root-level access.



## 4. Blue Team Detection – Log Evidence

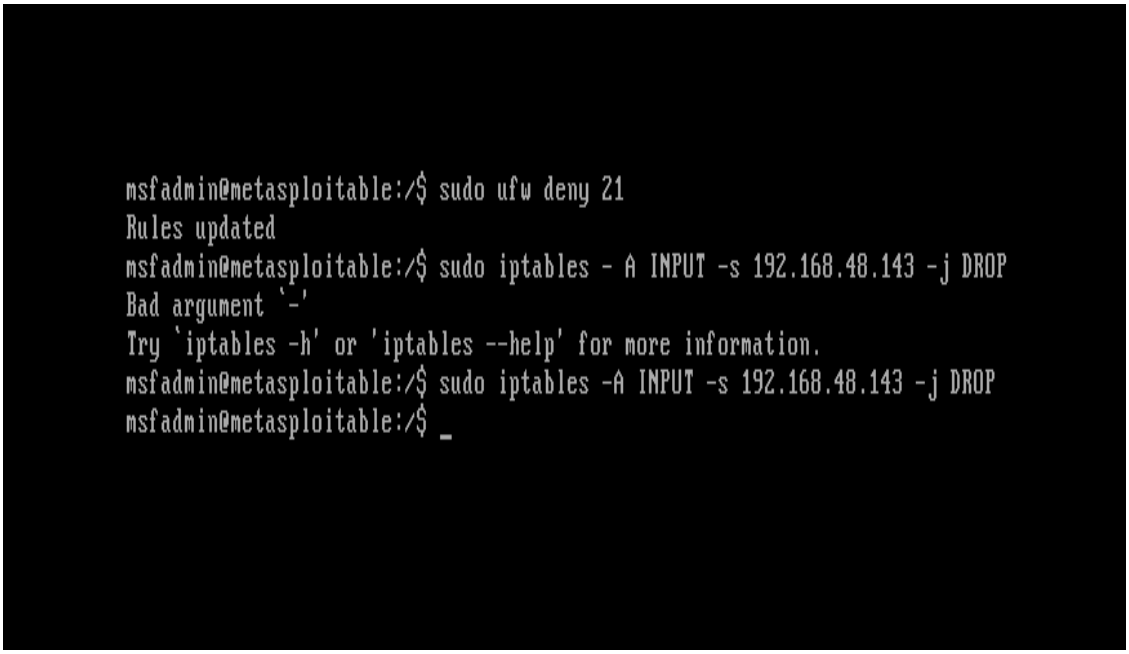
System logs detected suspicious connection attempts from attacker IP 192.168.48.143.



## 5. Firewall Remediation

Firewall rule implemented to block attacker IP using ip tables.



## 6. Validation – Nmap After Blocking

Post-remediation scan shows all ports filtered, confirming successful containment.

## 7.MITRE ATT&CK; Mapping

T1046 - Network Service Scanning
T1190 - Exploit Public-Facing Application
T1059 - Command Shell
T1068 - Privilege Escalation
T1571 - Non-Standard Port Usage

## 8. Lessons Learned

• Regular patching is critical.
• Monitor logs continuously.
• Restrict unnecessary services.
• Implement firewall protections.
• Use SIEM for automated detection.

## 9. Conclusion

The simulation successfully demonstrated reconnaissance, exploitation, detection, containment, and validation in a real-world SOC workflow scenario.