ssh -M -S /tmp/t1 root@10.50.24.200

**Using socket (doesn’t create additional logs)**

ssh -o “ControlPath=/tmp/t1” a@1

watch w

vim /etc/passwd

**Win**

net user

tasklist /v

**Lin**

cat /etc/passwd

**Privilege escalation**

sudo -l (what can i run?)

sudo su

whoami

id (groups)

cd (home directory)

ls -a

cat /etc/passwd

w

who

ps -elf

ps -elf | grep log

find . -type f -iname \*Keel\* 2>/dev/null

-name (case sensitive)

-iname (case doesn’t matter)

cd /etc

ls -la | grep syslog

less rsyslog.conf

less rsyslog.d/

**Services**

systemctl list-units --type service

cat /etc/crontab (cron service)

service --status-all

systemctl list-units --type=service \| grep running

ls /var/spool/cron/crontabs/

sudo !!

ip addr

cat /etc/hosts

sudo vim /etc/hosts

ssh root@jmp

netstat -natpu

ss -an4 (active connections)

tcpdump (connection to/from a box)

**Windows**

wmic process get name

**Registry**

regedit

HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

systeminfo

cat /proc/cpuinfo

**Data Exfiltration**

Obfuscation

**ROT1**

cat /etc/passwd | tr 'a-zA-Z0-9' 'b-zA-Z0-9a' > shifted.txt

ssh root@jmp | tee aitee919

cat /etc/passwd

cat /etc/shadow (passwords in this file)

cat aitee919

10.50.24.161:8000

**Exploit PE’s**

**T1**

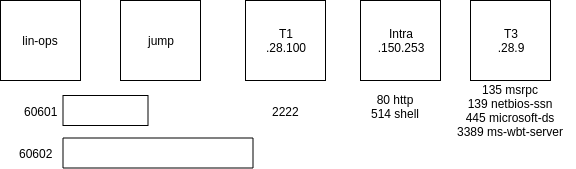
ssh student@10.50.35.200 -L 60601:localhost:22

ssh student@localhost -p 60601 -L 60602:192.168.28.100:2222 -NT

ssh comrade@localhost -p 60602 -D 9050 -NT

Intranet

proxychains comrade@192.168.150.253 -p 3201



ss -anp

cat /etc/shadow

cat /etc/hosts

cd /etc/rsyslog.d

**cd /etc**

ls -la

cat rkhunter.conf

**T3**

#lin-ops

ssh -J student@10.50.35.200 comrade@192.168.28.100 -p 2222 -D 9050 -L 60610:192.168.28.9:3389

#lin-ops

xfreerdp /v:localhost:60610 /u:comrade /p:StudentMidwayPassword /size:1920x1000 +clipboard