//PAM

$ nano /etc/pam.conf

$ ls -l /etc/pam.d/

$ nano *

// pam_permit.so

//shell configs

$ ls -lA

$ nono .profile OR .bashrc

$ nano /etc/bash.bashrc => there was a line which made the password - password1 after you change and log back in

// file permissions

$find / -type f -executable -perm -4000

// usr/bin/fish, cat

//su and mount has to have user id

//world writable

$ ls -ld /dev/shm

$find / -xdev -perm -o+w /(-type f -or -type d \)

$ls -l /etc/shadow = should be owned by root, root shadow

$ chmod 660 /etc/shadow

//network

$ifconfig

$ip -c a

$lsb

$lsb_release -a

$ nano /etc/passwd //

// look at the users which has the id 0

// when checking the file, all the users we should normally have has to have bin/bash in their address

//if there is a user who does have

connect to machines: ssh root@10.20.165.10

(shadow password)

external: 10.20.165.10, 10.20.165.11

Internal: 192.168.1.X

$ sudo openvpn --config redteam.ovpn

= network address gives us a hint

Users/groups

users of the machine: $ w //if you see multiple roots that's not good

// what you can do is to kick some of the users

// can double check what the scoring engine's IP

$ host scoring.defsec.club //167.172.15.1

// we can check their user id

$ ps auxf | grep bash //find their process id, 139999

$ kill -9 139999 OR $ pkill -9 -t pts/1

stuff to check: $ nano .bashrc //config of the shell

// if there is a nc (netcat) it is a backdoor

// just comment them out, like "alias" would set the cmds to different commands

$ lsattr /etc/passwd //check attributes of.. to see the permissions

//if it is ---i---e-- //i means noone is allowed to change this file

// $ chattr -i /etc/passwd to able to edit and change

$ cat /etc/passwd | grep bash //if someting stands out use

// $ chsh -s /usr/sbin/nologin <username> or /bin/false

// $ userdel -rf <username>

//lock out accounts $usermod -L <sus-username>

$ nano /etc/shadow //look at the shadow filem shows passwords

// you can see if the account is locked up or not by looking at their infront of the passwords !

$ nano /etc/group //sketchy ones are in the sudo, backup, operator, kvm, netdev groups

//back up file is $nano /etc/group-

$ ls -l /etc/sudoers.d/ //could see files like space and double space

$ nano /etc/sudoers //maybe comment admin group could gain root privs

//or group sudo to execute any command

// $ chattr -i *

$ rm -rf ' ' & rm -rf ' ' //check readme also and remove it accordingly