

Experiment-5

AIM: Emulation an IOT firmware using the Firmware emulator.

Step 1: First, we have to download the firmware name for that we have to visit the Netgear website.

Step 2: To download WNAP320-Firmware follow the below link.

- http://wwwdownloads.netgear.com/files/GDC/WNAP320/WNAP320_V3.7.11.4.zip

Step 3: In firmware WNAP320 we have to use the WNAP320-Firmware-Version-3-7-11-4 version.

The screenshot shows a web browser window with the URL <https://kb.netgear.com/000060419/WNAP320-Firmware-Version-3-7-11-4>. The page content includes:

- Enable/Disable Business central (Cloud Enabled) option resets the AP to factory default but retains IP, DNS and management VLAN settings
- In the following scenarios AP is expected to reboot automatically for the configuration to take effect:
 1. Country/Region change
 2. Firmware upgrade
 3. Restore Configuration
 4. Reset factory defaults
 5. Business central enable/disable

In all the other conditions AP is not supposed to reboot automatically.

To Install

1. Download the new software and save it to a convenient folder location.
Download link : http://wwwdownloads.netgear.com/files/GDC/WNAP320/WNAP320_V3.7.11.4.zip
2. Login to the access point web management GUI.
3. Take back-up of the current configuration and save it at a secure place.
4. Select **Maintenance > Upgrade > Firmware Upgrade**.
5. Click Browse and browse to the location of the software upgrade file that you just downloaded and click APPLY button.
Warning: When uploading software, it is important not to interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, the upload might fail, corrupt the software, and render this AP completely inoperable.

Step 4: Open terminal & write ls/ cd tools/ ls firmware – analysis-toolkit Enter into cd tools for use of firmware analysis toolkit.

```

root@attifyos:/home/iot# ls
Arduino    Downloads  ghidra_scripts  package.json      sketchbook
bin        esp        go             package-lock.json Templates
Desktop   esp32     Music          Pictures         tools
Documents ex.txt    node_modules   Public          Videos
root@attifyos:/home/iot# cd tools/
root@attifyos:/home/iot/tools# ls
arduino              gr-gsm           ook-decoder
baudrate            gr-paint          openocd
bdaddr               hackrf            qiling
bettercap            inspectrum        radare2
buildroot-2019.02.9 jadx              rfcat_150225
burpsuite.jar       kalibrate-rtl    routersploit
create_ap           killerbee        rtl_433
Cutter              libbtbb-2018-12-R1 rtl-sdr
drivers              libmpsse          scapy
dspectrumgui        liquid-dsp        spectrum_painter
dump1090             LTE-Cell-Scanner ubertooh-2018-12-R1
firmware-analysis-toolkit nmap             urh
ghidra_9.1.2_PUBLIC node_modules
root@attifyos:/home/iot/tools# cd firmware-analysis-toolkit/
root@attifyos:/home/iot/tools/firmware-analysis-toolkit# ls
binwalk      firmadyne    README.md  'WNAP320 Firmware Version 2.0.3.zip'
fat.config   LICENSE      reset.py

```

Step 5: Enter into the firmware analysis toolkit we can show a list of directories in the firmware analysis toolkit. After that enters into fat.config file with the help of the cat command. After that,we can see sudo_password in fat.config

cat fat. Config

```

root@attifyos:/home/iot/tools# cd firmware-analysis-toolkit/
root@attifyos:/home/iot/tools/firmware-analysis-toolkit# ls
binwalk      firmadyne    README.md  'WNAP320 Firmware Version 2.0.3.zip'
fat.config   LICENSE      reset.py
fat.py       qemu-builds  setup.sh
root@attifyos:/home/iot/tools/firmware-analysis-toolkit# cat fat.config
[DEFAULT]
sudo_password=attify
firmadyne_path=/home/iot/tools/firmware-analysis-toolkit/firmadyne
root@attifyos:/home/iot/tools/firmware-analysis-toolkit# ls
binwalk      firmadyne    README.md  'WNAP320 Firmware Version 2.0.3.zip'
fat.config   LICENSE      reset.py
fat.py       qemu-builds  setup.sh

```

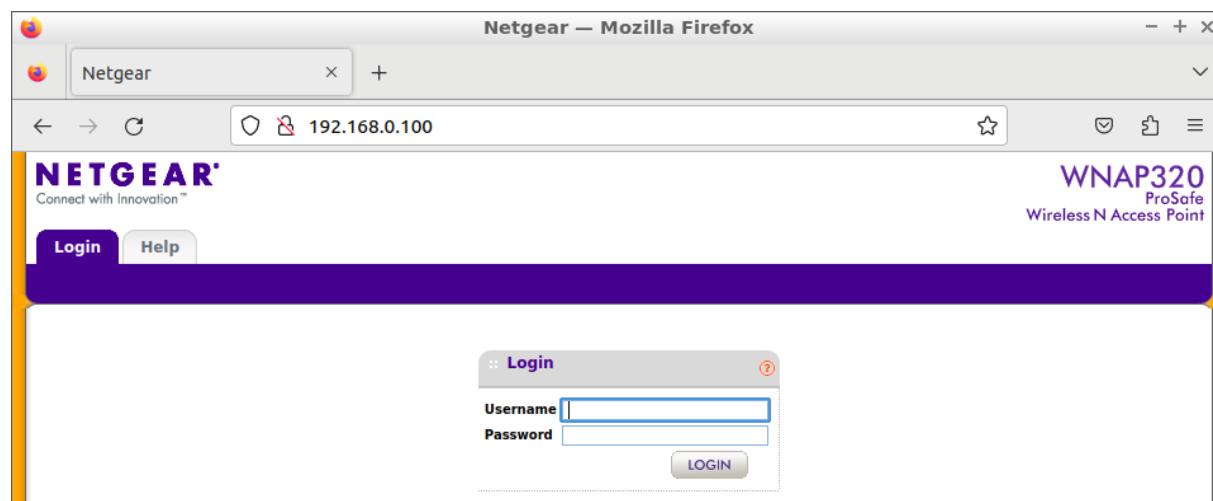
Step 6: Then enter into the ./fat.py file to see so many files are in the ./fat.py file. this file is used to gain the device to be accessible for all files & perform activities in the device.This fat creates an IP address to emulate the device.

./fat.py ‘file path’

Step 7: After performing fat create that is create an IP address to emulate IoT devices.

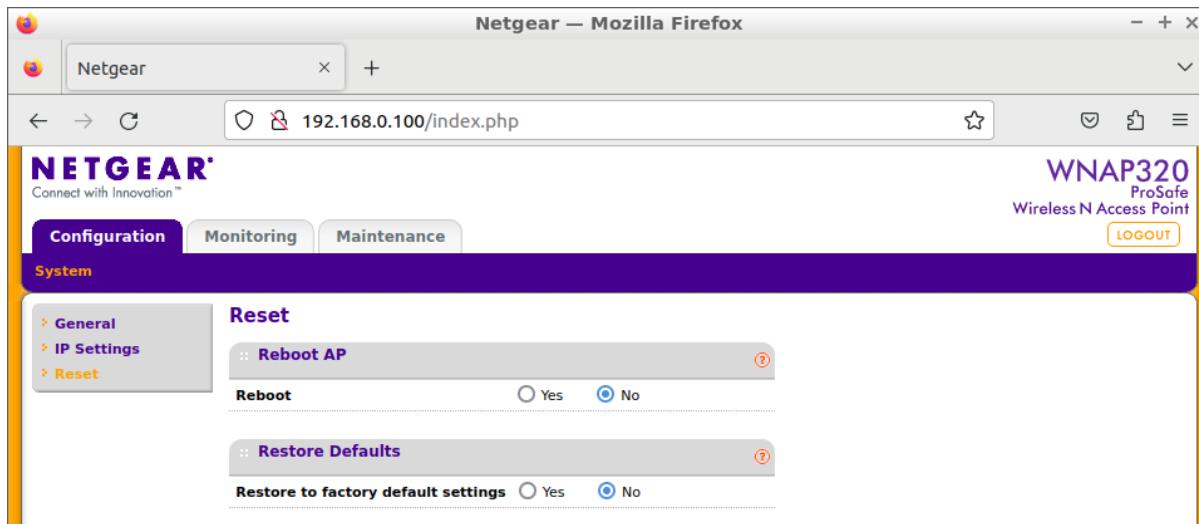
This IP address runs into a browser that can show a login page of the DIR-300 device.

After entering login credentials like Username & password. Username & password shows in emulating process use of FAT.



Step 8: After entering the Username & password we can redirect to the page of this device for emulating that's IoT device. we can access files & perform any activity on this device.

We can change or modify the data of this device.



- We can show the configuration, maintenance & monitoring section on this page. we can perform any activity, change, or modify a file in this section.

Conclusion: To perform emulation for an IOT device we can create a page of DIR 300 firmware with the use of a firmware analysis toolkit. This tool kit creates an IP address for DIR300. we can run this IP address on the browser. We can show the page of DIR 300 then enter Username & password which can show in the fat emulation process. Then perform any activity, change, or modify file in the IoT device. In this way, we can perform emulation of IoT device.