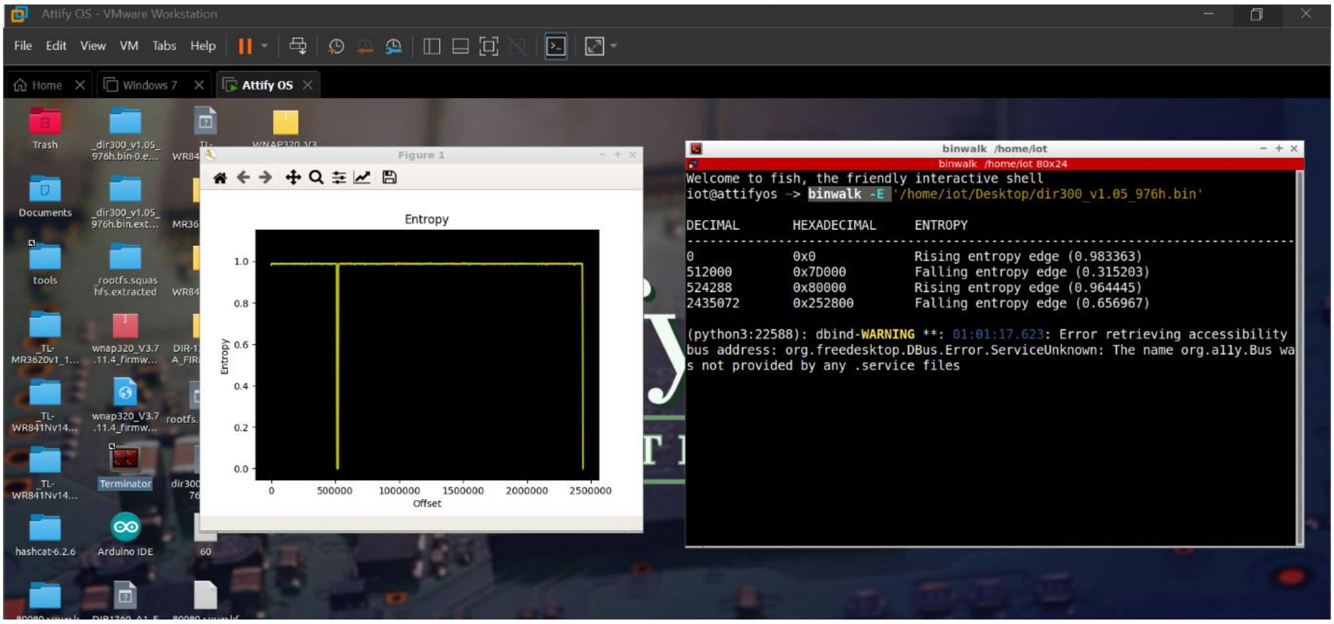
Practical-4

AIM: Finding Vulnerabilities in IoT system.

Step 1: First we have download the firmware name **DIR300**

Step 2: then we will check this firmware is encrypted or not . for this we will use

- Binwalk -E ‘file path’
- After check we will know thatthis firmware is not encrypted .



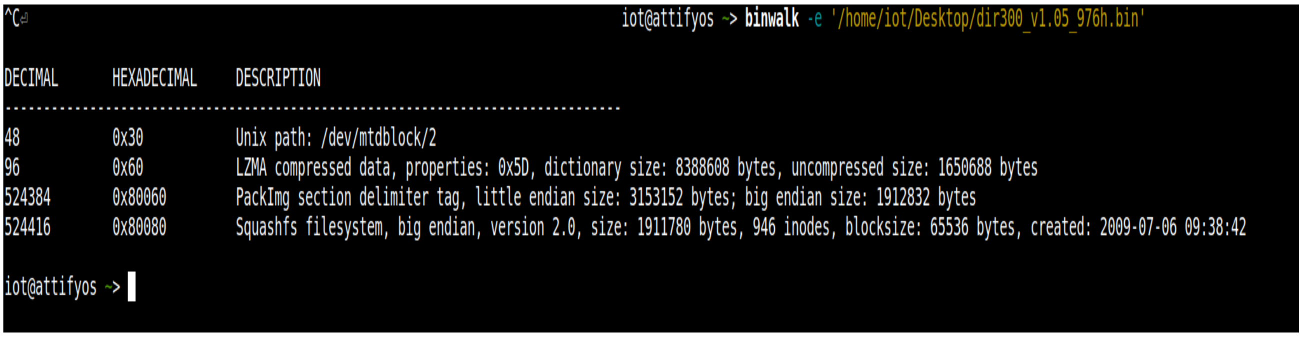
```
Welcome to fish, the friendly interactive shell
iot@attifyos -> binwalk -E '/home/iot/Desktop/dir300_v1.05_976h.bin'

DECIMAL       HEXADECIMAL     ENTROPY
--------------------------------------------------------------------------------
0             0x0             Rising entropy edge (0.983363)
512000        0x7D000         Falling entropy edge (0.315203)
524288        0x80000         Rising entropy edge (0.964445)
2435072       0x252800        Falling entropy edge (0.656967)

(python3:22588): dbind-WARNING **: 01:01:17.623: Error retrieving accessibility
bus address: org.freedesktop.DBus.Error.ServiceUnknown: The name org.ally.Bus wa
s not provided by any .service files
```

Step 3: after checking that firmware is not encrypted . we can extract the firmware so that we can use

- ***‘binwalk -e filepath’***



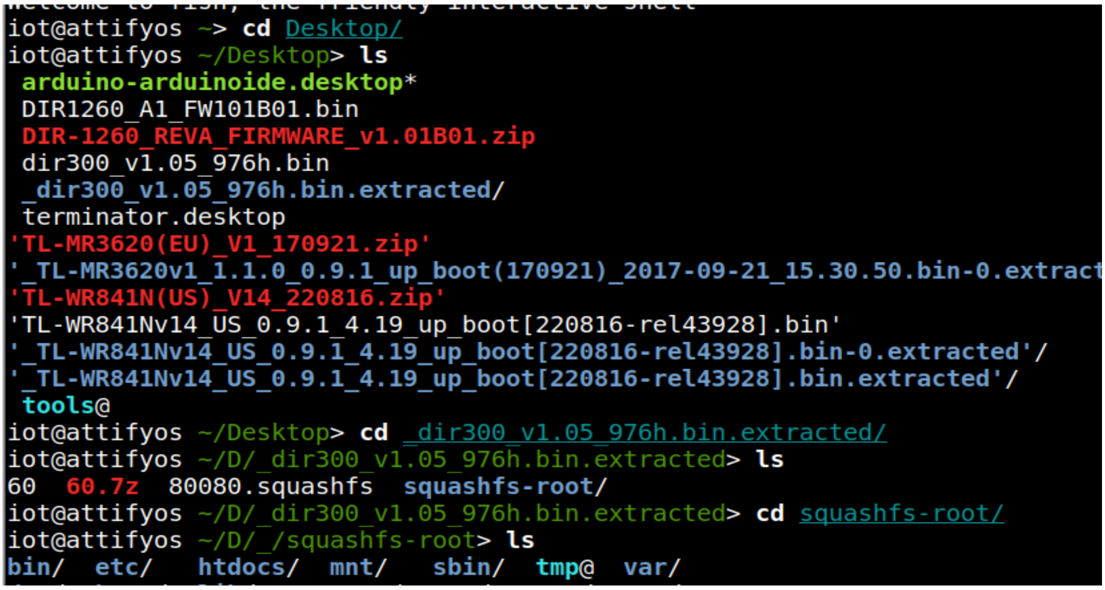
```
^C⏎                                                       iot@attifyos -> binwalk -e '/home/iot/Desktop/dir300_v1.05_976h.bin'

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
48            0x30            Unix path: /dev/mtdblock/2
96            0x60            LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, uncompressed size: 1650688 bytes
524384        0x80060         PackImg section delimiter tag, little endian size: 3153152 bytes; big endian size: 1912832 bytes
524416        0x80080         Squashfs filesystem, big endian, version 2.0, size: 1911780 bytes, 946 inodes, blocksize: 65536 bytes, created: 2009-07-06 09:38:42

iot@attifyos -> ▌
```

Step 4: after extracting the firmware use

- ***cd desktop/ cd file path/ cd squashfs-root***

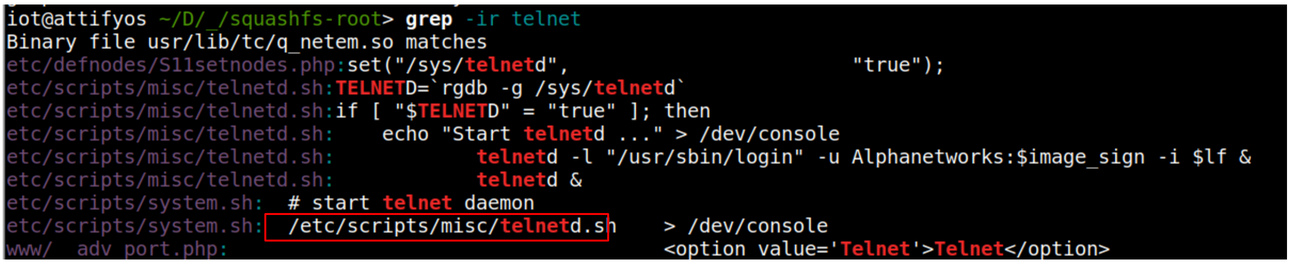


```
iot@attifyos ~> cd Desktop/
iot@attifyos ~/Desktop> ls
 arduino-arduinoide.desktop*
 DIR1260_A1_FW101B01.bin
 DIR-1260_REVA_FIRMWARE_v1.01B01.zip
 dir300_v1.05_976h.bin
 _dir300_v1.05_976h.bin.extracted/
 terminator.desktop
'TL-MR3620(EU)_V1_170921.zip'
'_TL-MR3620v1_1.1.0_0.9.1_up_boot(170921)_2017-09-21_15.30.50.bin-0.extract
'TL-WR841N(US)_V14_220816.zip'
'TL-WR841Nv14_US_0.9.1_4.19_up_boot[220816-rel43928].bin'
'_TL-WR841Nv14_US_0.9.1_4.19_up_boot[220816-rel43928].bin-0.extracted'/
'_TL-WR841Nv14_US_0.9.1_4.19_up_boot[220816-rel43928].bin.extracted'/
 tools@
iot@attifyos ~/Desktop> cd _dir300_v1.05_976h.bin.extracted/
iot@attifyos ~/D/_dir300_v1.05_976h.bin.extracted> ls
60  60.7z  80080.squashfs  squashfs-root/
iot@attifyos ~/D/_dir300_v1.05_976h.bin.extracted> cd squashfs-root/
iot@attifyos ~/D/_/squashfs-root> ls
bin/  etc/   htdocs/  mnt/   sbin/  tmp@  var/
```

Step 5: after entering in to squashfs -root folder . we can use grep -ir telnet to know location of password .

grep -ir telnet

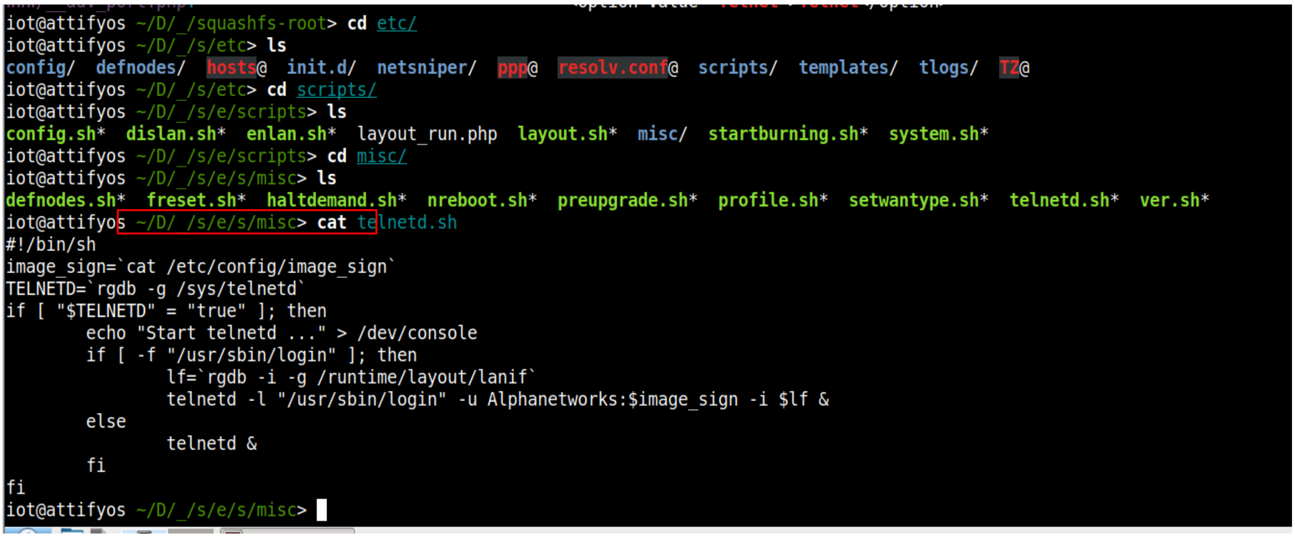
*location : **/etc/scripts /misc/telnetd.sh***



```
iot@attifyos ~/D/_/squashfs-root> grep -ir telnet
Binary file usr/lib/tc/q_netem.so matches
etc/defnodes/S11setnodes.php:set("/sys/telnetd",                        "true");
etc/scripts/misc/telnetd.sh:TELNETD=`rgdb -g /sys/telnetd`
etc/scripts/misc/telnetd.sh:if [ "$TELNETD" = "true" ]; then
etc/scripts/misc/telnetd.sh:    echo "Start telnetd ..." > /dev/console
etc/scripts/misc/telnetd.sh:            telnetd -l "/usr/sbin/login" -u Alphanetworks:$image_sign -i $lf &
etc/scripts/misc/telnetd.sh:            telnetd &
etc/scripts/system.sh:  # start telnet daemon
etc/scripts/system.sh:  /etc/scripts/misc/telnetd.sh    > /dev/console
www/  adv port.php:                                     <option value='Telnet'>Telnet</option>
```

Step 6: after the getting the path of password. We can follow this path for find a password.

Path : cd etc/ls/cd scripts/ls/cd misc/ls/cat telnetd.sh

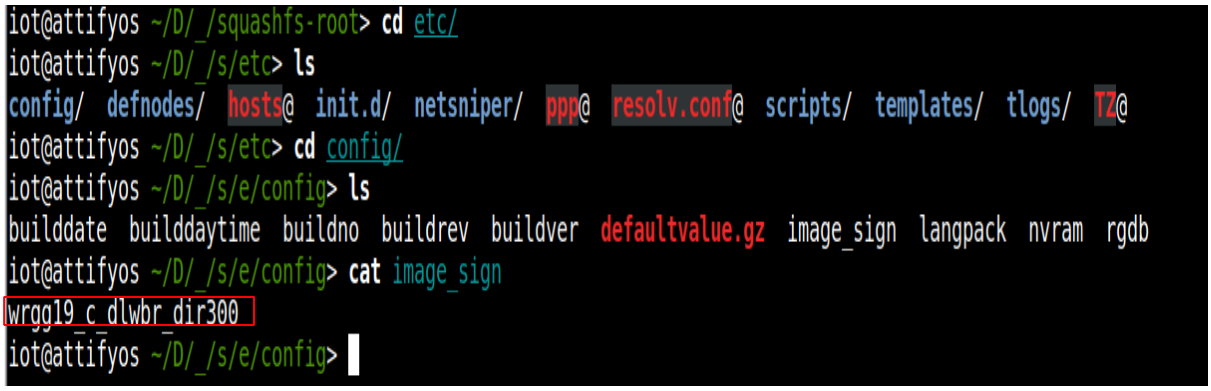


```
iot@attifyos ~/D/_/squashfs-root> cd etc/
iot@attifyos ~/D/_/s/etc> ls
config/  defnodes/  hosts@  init.d/  netsniper/  ppp@  resolv.conf@  scripts/  templates/  tlogs/  TZ@
iot@attifyos ~/D/_/s/etc> cd scripts/
iot@attifyos ~/D/_/s/e/scripts> ls
config.sh*  dislan.sh*  enlan.sh*  layout_run.php  layout.sh*  misc/  startburning.sh*  system.sh*
iot@attifyos ~/D/_/s/e/scripts> cd misc/
iot@attifyos ~/D/_/s/e/s/misc> ls
defnodes.sh*  freset.sh*  haltdemand.sh*  nreboot.sh*  preupgrade.sh*  profile.sh*  setwantype.sh*  telnetd.sh*  ver.sh*
iot@attifyos ~/D/_/s/e/s/misc> cat telnetd.sh
#!/bin/sh
image_sign=`cat /etc/config/image_sign`
TELNETD=`rgdb -g /sys/telnetd`
if [ "$TELNETD" = "true" ]; then
        echo "Start telnetd ..." > /dev/console
        if [ -f "/usr/sbin/login" ]; then
                lf=`rgdb -i -g /runtime/layout/lanif`
                telnetd -l "/usr/sbin/login" -u Alphanetworks:$image_sign -i $lf &
        else
                telnetd &
        fi
fi
iot@attifyos ~/D/_/s/e/s/misc> 
```

Step 7: after follow path we can get image_ sign password file path.

- ***Path : cd etc/ls/cd config/ls/cat image_sign*** .

- after follow cd etc/ls/cd config/ls/cat image_sign this path we get the password



```
iot@attifyos ~/D/_/squashfs-root> cd etc/
iot@attifyos ~/D/_/s/etc> ls
config/  defnodes/  hosts@  init.d/  netsniper/  ppp@  resolv.conf@  scripts/  templates/  tlogs/  TZ@
iot@attifyos ~/D/_/s/etc> cd config/
iot@attifyos ~/D/_/s/e/config> ls
builddate  builddaytime  buildno  buildrev  buildver  defaultvalue.gz  image_sign  langpack  nvram  rgdb
iot@attifyos ~/D/_/s/e/config> cat image_sign
wrgg19_c_dlwbr_dir300
iot@attifyos ~/D/_/s/e/config> 
```

Conclusion: The main disadvantage of this firmware is not encrypted. We can get the password and explore any file of this device.