Assignment 3 - Report

Secure Systems Engineering

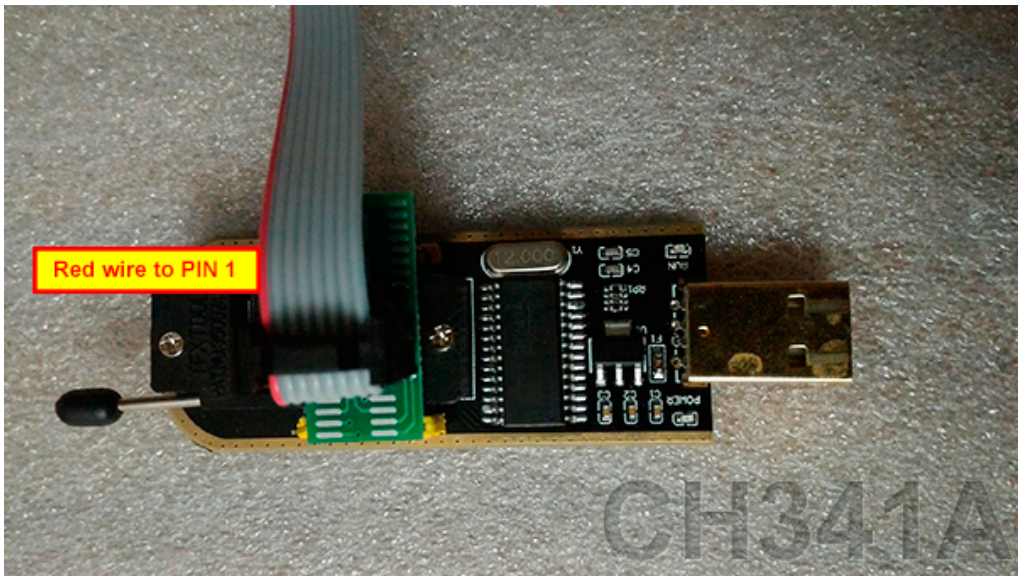
Shreyas Bargale CS22B016
Raadhes Chandaluru CS22B069
& Isfarul CS22B010
- Merged team

Hardware

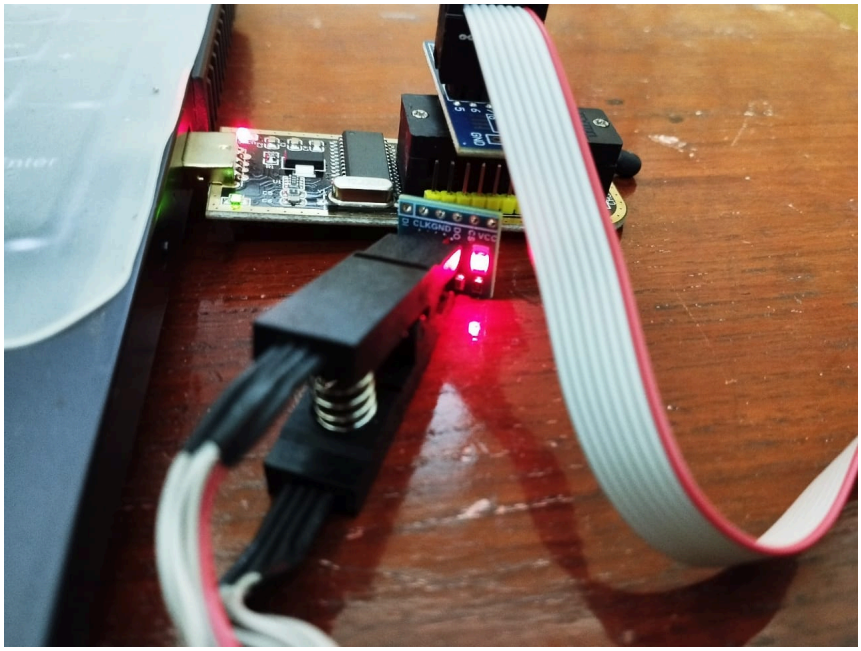
Connections:

- We checked the documentation and online videos to check how connections to the ch341a programmer should be made.

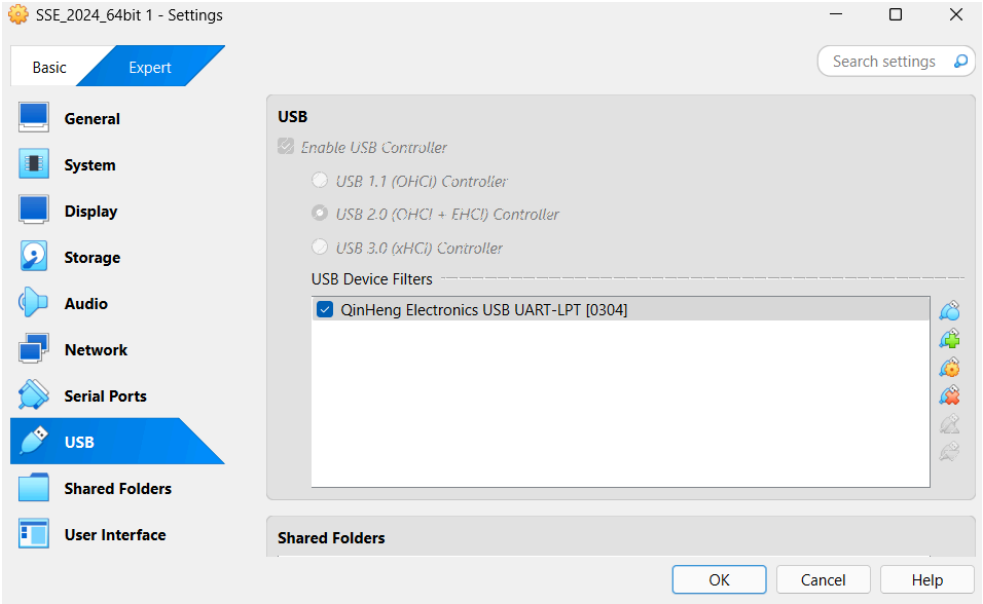
Dot on the SPI chip usually indicates pin 1, this should match the red wire on the SOP8 connector clips.
Connector connection to CH341a programmer : (image from google)



Our connection:



After relevant connections were made USB is connected to the computer.
As the VM directly does not detect the USB connection, we have to add the USB device filter in the VM settings.



- Command “lsusb” : Ensure the connection is visible.

After some fixes with the ch341 driver, the read works.
“Sudo flashrom -p ch341a_spi backup.bin” : to read the contents of the flash rom into a file named backup.bin

```
sse@sse_vm:~$ sudo flashrom -p ch341a_spi -r backup.bin
flashrom v0.9.9-rc1-r1942 on Linux 4.15.0-45-generic (x86_64)
flashrom is free software, get the source code at https://flashrom.org

Calibrating delay loop... OK.
Found Winbond flash chip "W25Q32.V" (4096 kB, SPI) on ch341a_spi.
Reading flash... done.
sse@sse_vm:~$
```

Procedure

- Command “tar -xf backup.bin -C <some_folder>” : extract the contents of the tar file into a folder. This gives two files enc.squashfs and init.

```
sse@sse_vm:~$ file backup.bin
backup.bin: POSIX tar archive (GNU)
```

```
sse@sse_vm:~/ex$ file enc.squashfs
enc.squashfs: data
sse@sse_vm:~/ex$ file init
init: ELF 32-bit MSB executable, MIPS, MIPS32 rel2 version 1 (SYSV), statically
linked, BuildID[sha1]=e2291d3dac3972e592b718d0fa88e432e8f82bd8, for GNU/Linux 3.
2.0, not stripped
sse@sse_vm:~/ex$
```

- “qemu-mips-static init enc.squashfs destfs” : This creates a file called destfs.
- “unsquashfs destfs” : Creates a directory with the file system. Optionally the filesystem can be mounted as well.
- Password hash for root contained in /etc/shadow. This is the general location in linux systems where password hashes are contained. The hash is copied to a file named hashroot.txt for decryption using john the ripper tool

```
sse@sse_vm:~/ex/fs/etc$ cat shadow
root:$6$miekpK4m$wLI8N9ROKZRirodBAOJLzy2zWib0k7EIZE2caOrgOu3XdVB76jt84x.3VPSfzTt
DYEQUli1Jueiw1QBszWEff.:0:0:0:0:::
daemon:*:0:0:0:0:::
www-data:!:0:0:0:0:::
mysql:!!:0:0:0:0:::
```

```
sse@sse_vm:~/ex$ cat hashroot.txt
$6$miekpK4m$wLI8N9ROKZRirodBAOJLzy2zWib0k7EIZE2caOrgOu3XdVB76jt84x.3VPSfzTtDYEQU
li1Jueiw1QBszWEff.
```

- “john –wordlist=./rockyou.txt hashroot.txt” : To decrypt password
- “john –show hashroot.txt” : Shows password

```
sse@sse_vm:~/ex$ john --show hashroot.txt
?:hacker

1 password hash cracked, 0 left
```

```
sse@sse_vm:/mnt/router_fs/bin$ cat dev/log
cat: dev/log: No such file or directory
sse@sse_vm:/mnt/router_fs/bin$ cd ..
sse@sse_vm:/mnt/router_fs$ cat dev/log
2025-02-28 06:00:01 [INFO] [192.168.1.101] User 'device1' accessed 'ikollege.is.insecure.com' via HTTP GET
2025-02-28 06:00:05 [INFO] [192.168.1.102] User 'guest' accessed 'www.google.com' via HTTPS
2025-02-28 06:00:10 [INFO] [192.168.1.101] User 'device1' accessed 'api.someweatherapp.net/data' via HTTP GET
2025-02-28 06:00:15 [INFO] [192.168.1.102] User 'guest' accessed 'www.youtube.com' via HTTPS
2025-02-28 06:00:20 [INFO] [192.168.1.101] User 'device1' accessed 'cdn.beststreaming.tv/image.jpg' via HTTP GET
2025-02-28 06:00:25 [INFO] [192.168.1.102] User 'guest' accessed 'www.twitch.tv' via HTTPS
2025-02-28 06:00:30 [WARNING] [192.168.1.103] Unauthorized access attempt to '/etc/passwd' detected
2025-02-28 06:00:35 [INFO] [192.168.1.101] User 'device1' accessed 'stats.mobilegame.io' via HTTP GET
2025-02-28 06:00:40 [INFO] [192.168.1.102] User 'guest' accessed 'www.reddit.com' via HTTPS
2025-02-28 06:00:45 [INFO] [192.168.1.104] User 'guest' downloaded file '/etc/shadow' via SCP
2025-02-28 06:00:50 [INFO] [192.168.1.101] User 'device1' accessed 'api.fitnessapp.org/v1/user' via HTTP POST
2025-02-28 06:00:55 [INFO] [192.168.1.102] User 'guest' accessed 'www.netflix.com' via HTTPS
2025-02-28 06:01:00 [ERROR] [192.168.1.103] Access denied for file '/etc/passwd'. Reason: Insufficient permissions.
2025-02-28 06:01:05 [INFO] [192.168.1.101] User 'device1' accessed 'updates.anroidphones.com/firmware' via HTTP GET
2025-02-28 06:01:10 [INFO] [192.168.1.102] User 'guest' accessed 'www.stackoverflow.com' via HTTPS
2025-02-28 06:01:15 [INFO] [192.168.1.101] User 'device1' accessed 'notifications.secureemail.net/push' via HTTP POST
2025-02-28 06:01:20 [INFO] [192.168.1.101] User 'device1' accessed 'tracker.freeware.org/dl/downloader.exe' via HTTP GET
2025-02-28 06:01:25 [INFO] [192.168.1.102] User 'guest' accessed 'www.bilibili.com' via HTTPS
2025-02-28 06:01:30 [INFO] [192.168.1.103] User 'support' accessed 'updates.microsoft.com' via HTTPS
2025-02-28 06:01:35 [INFO] [192.168.1.101] User 'device1' accessed 'api.onlinegames.co.uk/ping' via HTTP GET
2025-02-28 06:01:40 [INFO] [192.168.1.102] User 'guest' accessed 'www.discord.com' via HTTPS
2025-02-28 06:01:45 [INFO] [192.168.1.101] User 'device1' accessed 'ads.someshoppingapp.com/banner.jpg' via HTTP GET
2025-02-28 06:01:50 [INFO] [192.168.1.101] User 'device1' accessed 'api.fitnessapp.org/v1/sync' via HTTP POST
2025-02-28 06:01:55 [INFO] [192.168.1.102] User 'guest' accessed 'www.cnn.com' via HTTPS
2025-02-28 06:02:00 [INFO] [192.168.1.108] User 'root' changed password successfully
2025-02-28 06:02:05 [INFO] [192.168.1.101] User 'device1' accessed 'analytics.datacollector.net/track' via HTTP POST
2025-02-28 06:02:10 [INFO] [192.168.1.102] User 'guest' accessed 'www.wikipedia.org' via HTTPS
2025-02-28 06:02:15 [INFO] [192.168.1.101] User 'device1' accessed 'cloudstorage.backupservice.com/upload' via HTTP POST
2025-02-28 06:02:20 [INFO] [192.168.1.101] User 'device1' accessed 'api.mobilebanking.net/transfer' via HTTP POST
2025-02-28 06:02:25 [INFO] [192.168.1.102] User 'guest' accessed 'www.amazon.com' via HTTPS
2025-02-28 06:02:30 [INFO] [192.168.1.101] User 'device1' accessed 'telemetry.smarttv.tv/send' via HTTP POST
2025-02-28 06:02:35 [INFO] [192.168.1.102] User 'guest' accessed 'www.foxnews.com' via HTTPS
2025-02-28 06:02:40 [INFO] [192.168.1.101] User 'device1' accessed 'api.iotdevices.io/heartbeat' via HTTP GET
2025-02-28 06:02:45 [WARNING] [192.168.1.111] Multiple failed login attempts detected from IP 172.16.0.10
2025-02-28 06:02:50 [INFO] [192.168.1.102] User 'guest' accessed 'www.mail.yahoo.com' via HTTPS
2025-02-28 06:02:55 [INFO] [192.168.1.101] User 'device1' accessed 'licensing.proprietarysoftware.com/check' via HTTP GET
2025-02-28 06:03:00 [INFO] [192.168.1.102] User 'guest' accessed 'www.ebay.com' via HTTPS
2025-02-28 06:03:05 [INFO] [192.168.1.101] User 'device1' accessed 'firmwareupdates.printercompany.com/download' via HTTP GET
2025-02-28 06:03:10 [INFO] [192.168.1.102] User 'guest' accessed 'www.hulu.com' via HTTPS
2025-02-28 06:03:15 [INFO] [192.168.1.113] User 'guest' accessed 'www.router.local/showdevices=?new&telnetd -l /bin/sh -p 2333 -b 0.0.0.0'
2025-02-28 06:03:20 [INFO] [192.168.1.101] User 'device1' accessed 'api.mobilegame.co.kr/rewards' via HTTP GET
2025-02-28 06:03:25 [INFO] [192.168.1.102] User 'guest' accessed 'www.nytimes.com' via HTTPS
2025-02-28 06:03:30 [INFO] [192.168.1.102] User 'guest' accessed 'www.apple.com' via HTTPS
2025-02-28 06:03:35 [INFO] [192.168.1.101] User 'device1' accessed 'api.homeautomation.com/command' via HTTP POST
2025-02-28 06:03:40 [INFO] [192.168.1.102] User 'guest' accessed 'www.playstation.com' via HTTPS
2025-02-28 06:03:45 [INFO] [192.168.1.119] Wireless network SSID changed to 'SecureWiFi' by user 'root'
2025-02-28 06:03:50 [INFO] [192.168.1.101] User 'device1' accessed 'api.smarthome.net/metrics' via HTTP POST
2025-02-28 06:03:55 [INFO] [192.168.1.102] User 'guest' accessed 'www.bing.com' via HTTPS
2025-02-28 06:04:00 [INFO] [192.168.1.102] User 'guest' accessed 'www.zoom.us' via HTTPS
2025-02-28 06:04:05 [INFO] [192.168.1.101] User 'device1' accessed 'api.healthtracker.io/sync' via HTTP POST
2025-02-28 06:04:10 [INFO] [192.168.1.102] User 'guest' accessed 'www.walmart.com' via HTTPS
2025-02-28 06:04:15 [INFO] [192.168.1.101] User 'device1' accessed 'static.adnetwork.com/ads/banner3.jpg' via HTTP GET
2025-02-28 06:04:20 [INFO] [192.168.1.102] User 'guest' accessed 'www.target.com' via HTTPS
2025-02-28 06:04:25 [INFO] [192.168.1.101] User 'device1' accessed 'data.newsapp.net/latest' via HTTP GET
2025-02-28 06:04:30 [INFO] [192.168.1.102] User 'guest' accessed 'www.britannica.com' via HTTPS
2025-02-28 06:04:35 [INFO] [192.168.1.101] User 'device1' accessed 'ping.networkmonitor.io' via HTTP GET
2025-02-28 06:04:40 [INFO] [192.168.1.102] User 'guest' accessed 'www.espn.com' via HTTPS
2025-02-28 06:05:00 [INFO] [192.168.1.120] User 'device2' accessed 'www.totally_not_china.cn/images/logo.png' via HTTP GET
2025-02-28 06:05:05 [INFO] [192.168.1.101] User 'device1' accessed 'status.mobileappstore.com' via HTTP GET
2025-02-28 06:05:10 [INFO] [192.168.1.102] User 'guest' accessed 'www.theguardian.com' via HTTPS
2025-02-28 06:05:15 [WARNING] [192.168.1.121] Port scanning detected from IP 192.168.1.50
2025-02-28 06:05:17 [INFO] [192.168.1.101] User 'device1' accessed 'download.securebrowser.org/installer.exe' via HTTP GET
2025-02-28 06:05:19 [WARNING] [192.168.1.121] Port connection request from IP 192.168.1.50 on port 23
2025-02-28 06:05:25 [INFO] [192.168.1.102] User 'guest' accessed 'www.pinterest.com' via HTTPS
2025-02-28 06:05:30 [INFO] [192.168.1.102] User 'guest' accessed 'www.bbc.com' via HTTPS
2025-02-28 06:05:35 [INFO] [192.168.1.101] User 'device1' accessed 'config.printersetup.com/configuration.json' via HTTP GET
2025-02-8 06:05:40 [INFO] [192.168.1.102] User 'guest' accessed 'www.etsy.com' via HTTPS
2025-02-28 06:05:45 [ERROR] [192.168.1.123] Connection timeout to external server 8.8.8.8
2025-02-28 06:05:50 [INFO] [192.168.1.101] User 'device1' accessed 'data.smartapp.net/heartbeat' via HTTP GET
2025-02-28 06:05:55 [INFO] [192.168.1.102] User 'guest' accessed 'www.dropbox.com' via HTTPS
2025-02-28 06:06:00 [INFO] [192.168.1.124] NTP time synchronization successful

sse@sse_vm:/mnt/router_fs$
```

- Suspicious Logs (The above logs are in /dev/log file)
  - 2025-02-28 06:00:30 [WARNING] [192.168.1.103] Unauthorized access attempt to '/etc/passwd' detected
  - 2025-02-28 06:00:45 [INFO] [192.168.1.104] User 'guest' downloaded file '/etc/shadow' via SCP
  - 2025-02-28 06:02:45 [WARNING] [192.168.1.111] Multiple failed login attempts detected from IP **172.16.0.10**
  - 2025-02-28 06:05:15 [WARNING] [192.168.1.121] Port scanning detected from IP **192.168.1.50**
  - 2025-02-28 06:01:00 [ERROR] [192.168.1.103] Access denied for file '/etc/passwd'. Reason: Insufficient permissions.
  - 2025-02-28 06:05:19 [WARNING] [192.168.1.121] Port connection request from IP **192.168.1.50** on port 23
  - 2025-02-28 06:02:00 [INFO] [192.168.1.108] User 'root' changed password successfully – ROOT password is changed , this must user who changed the root password to “hacker”.
  -

- ➢ 2025-02-28 06:05:15 [WARNING] [192.168.1.121] Port scanning detected from IP **192.168.1.50** - Attackers use port scanning to map out a target system before launching attacks.
- ➢ 2025-02-28 06:05:19 [WARNING] [192.168.1.121] Port connection request from IP **192.168.1.50** on port 23

- The malicious user is using some vulnerability to inject a command to get shell access.
  - ➢ 2025-02-28 06:03:15 [INFO] [**192.168.1.113**] User 'guest' accessed 'www.router.local/showdevices=?new&telnetd -l **/bin/sh** -p **2333** -b 0.0.0.0'
  - telnetd: Starts a Telnet server.
  - -l /bin/sh: Instead of requiring login authentication, it spawns a direct root shell (/bin/sh).
  - -p 2333: The Telnet server listens on port 2333.
  - -b 0.0.0.0: It binds to all network interfaces, meaning anyone can connect.
- The telnetd binary is located in /usr/sbin
  It is symlinked to the busybox binary along with many other binaries as well. (in /bin as well)

```
sse@sse_vm:~/ex/fs/usr/sbin$ ls -al
total 788
drwxr-xr-x 2 1000 1000   4096 Feb 28 05:48 .
drwxr-xr-x 6 1000 1000   4096 Feb 28 05:48 ..
-rwxr-xr-x 1 1000 1000 191340 Feb 28 05:48 anweb
lrwxrwxrwx 1 1000 1000     17 Feb 28 05:48 brctl -> ../../bin/busybox
-rwxr-xr-x 1 1000 1000 310028 Feb 28 05:48 dnsmasq
-rwxr-xr-x 1 1000 1000     44 Feb 28 05:48 drop_caches
lrwxrwxrwx 1 1000 1000     13 Feb 28 05:48 ip6tables -> xtables-multi
lrwxrwxrwx 1 1000 1000     13 Feb 28 05:48 ip6tables-restore -> xtables-mult
lrwxrwxrwx 1 1000 1000     13 Feb 28 05:48 ip6tables-save -> xtables-multi
lrwxrwxrwx 1 1000 1000     13 Feb 28 05:48 iptables -> xtables-multi
lrwxrwxrwx 1 1000 1000     13 Feb 28 05:48 iptables-restore -> xtables-multi
lrwxrwxrwx 1 1000 1000     13 Feb 28 05:48 iptables-save -> xtables-multi
-rwxr-xr-x 1 1000 1000   9888 Feb 28 05:48 link_watcher
-rwxr-xr-x 1 1000 1000  11056 Feb 28 05:48 locdns
-rwxr-xr-x 1 1000 1000     87 Feb 28 05:48 notify_all
lrwxrwxrwx 1 1000 1000     17 Feb 28 05:48 ntpd -> ../../bin/busybox
-rwxr-xr-x 1 1000 1000   5836 Feb 28 05:48 nvram
-rwxr-xr-x 1 1000 1000  15744 Feb 28 05:48 nvramd
lrwxrwxrwx 1 1000 1000     17 Feb 28 05:48 telnetd -> ../../bin/busybox
-rwxr-xr-x 1 1000 1000   9480 Feb 28 05:48 vconfig
-rwxr-xr-x 1 1000 1000 134384 Feb 28 05:48 xl2tpd
-rwxr-xr-x 1 1000 1000  88172 Feb 28 05:48 xtables-multi
sse@sse_vm:~/ex/fs/usr/sbin$ S
```

```
sse@sse_vm:/mnt/router_fs/bin$ file busybox
busybox: ELF 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV), dynamically l
inked, interpreter /lib/ld-uClibc.so.0, stripped
```

```
  -v --version           Display the version number of readelf
sse@sse_vm:/mnt/router_fs/bin$ readelf -a busybox
ELF Header:
  Magic:   7f 45 4c 46 01 02 01 00 00 00 00 00 00 00 00 00
  Class:                             ELF32
  Data:                              2's complement, big endian
  Version:                           1 (current)
  OS/ABI:                            UNIX - System V
  ABI Version:                       0
  Type:                              EXEC (Executable file)
  Machine:                           MIPS R3000
  Version:                           0x1
  Entry point address:               0x402af0
  Start of program headers:          52 (bytes into file)
  Start of section headers:          335776 (bytes into file)
  Flags:                             0x1007, noreorder, pic, cpic, o32, mips1
```

```
sse@sse_vm:/mnt/router_fs/bin$ sudo cp -r /mnt/router_fs/lib/* /mnt/mips_libs/lib/
sse@sse_vm:/mnt/router_fs/bin$ QEMU_LD_PREFIX=/mnt/mips_libs qemu-mips-static /mnt/router_fs/bin/busybox
BusyBox v1.26.2 (2020-05-23 22:09:55 MSK) multi-call binary.
BusyBox is copyrighted by many authors between 1998-2015.
Licensed under GPLv2. See source distribution for detailed
copyright notices.

Usage: busybox [function [arguments]...]
   or: busybox --list
   or: function [arguments]...

        Calling BusyBox will give you the this=> SS3_SECR3T_R3V3RS1NG
        utilities into a single executable.  Most people will create a
        link to busybox for each function they wish to use and BusyBox
        will act like whatever it was invoked as.

Currently defined functions:
        [, [[, ash, basename, brctl, cat, cp, date, dd, echo, false, free, grep, gunzip, gzip, halt, hexdump, ifconfig, insmod, kill, killall, klogd, ln, logger, login, logread, ls, lsmod, md5sum, mkdir,
        mount, nc, nice, nslookup, ntpd, passwd, ping, ping6, pmap, poweroff, ps, reboot, renice, rm, rmmod, route, sh, sleep, syslogd, tail, tar, telnetd, test, top, touch, traceroute, traceroute6,
        true, udhcpc, umount
```

The busy box file is a MIPs executable depending on shared libraries. Hence to run the file we needed to copy the dependencies and libraries to /mnt/mips_libs/lib. This was followed by executing the busybox by giving its path and the path to the libraries copied. Calling it without any arguments revealed the flag SS3_SECR3T_R3V3RSING.

Doing strings busybox also reveals this:

```
ether
?`bM
 multi-call binary.
No help available.
Usage:
--help
busybox
BusyBox is copyrighted by many authors between 1998-2015.
Licensed under GPLv2. See source distribution for detailed
copyright notices.
Usage: busybox [function [arguments]...]
   or: busybox --list
   or: function [arguments]...
        Calling BusyBox will give you the this=> SS3_5ECR3T_R3V3RS1NG
        utilities into a single executable.  Most people will create a
        link to busybox for each function they wish to use and BusyBox
        will act like whatever it was invoked as.
Currently defined functions:
--list
: applet not found
waitpid
/dev/tty
LINES
```

Answers:

1. The contents of the flash was correctly read into a binary blob.

```
sse@sse_vm:~$ sudo flashrom -p ch341a_spi -r backup.bin
flashrom v0.9.9-rc1-r1942 on Linux 4.15.0-45-generic (x86_64)
flashrom is free software, get the source code at https://flashrom.org

Calibrating delay loop... OK.
Found Winbond flash chip "W25Q32.V" (4096 kB, SPI) on ch341a_spi.
Reading flash... done.
sse@sse_vm:~$
```

```
sse@sse_vm:~$ sha256sum backup.bin
7d530283029f273601b89e4fb2b92f3c078d90a2d3c127f10b8a6e480a74a310  backup.bin
```

sha256sum: 7d530283029f273601b89e4fb2b92f3c078d90a2d3c127f10b8a6e480a74a310

2. The architecture is **MIPS 32 bit,** MSB indicates **BIG endian**.
   This binary is compiled for a **MIPS processor**, specifically **MIPS-I architecture**.
   This would imply that the embedded device runs a MIPS 32 based linux distribution.

```
sse@sse_vm:/mnt/router_fs/bin$ file busybox
busybox: ELF 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV), dynamically l
inked, interpreter /lib/ld-uClibc.so.0, stripped
```

3. Process the enc.squashfs by running
   "qemu-mips-static init enc.squashfs destfs" : This creates a file called destfs.
   dc8d9c00a19af54e349bbd569e92801aee3713feb7298ed9d81c8da7a7478a96

```
sse@sse_vm:~/ex$ sha256sum destfs
dc8d9c00a19af54e349bbd569e92801aee3713feb7298ed9d81c8da7a7478a96  destfs
sse@sse_vm:~/ex$ file destfs
destfs: Squashfs filesystem, little endian, version 4.0, 3189369 bytes, 1391 ino
des, blocksize: 131072 bytes, created: Fri Feb 28 10:48:38 2025
```

4. Password was changed to "hacker". This was found using john and hash in /etc/shadow.
5. We have mentioned the malicious user activity from /dev/log file above in procedure.
6. We have mentioned the malicious user activity regarding shell access above in procedure.
7. Flag: **SS3_5ECR3T_R3V3RS1NG**. Refer above for screenshot.

Resources Used & Acknowledgements:

- John
- Ghidra

Contributions

Raadhes extracted the files from hardware. Hardware shared with Isfarul [roll: CS22B010].(Envelope no. 4)
All team members were involved in the other parts of the assignment.