Hardware Exploitation Cheat-sheet

COMMANDS

UART Interface (Universal Asynchronous Receiver-Transmitter)

Identify buad rate run buadrate,py script in tools folder

```
#> ./baudrate.py
```

```
#> screen /dev/ttyUSB# <baudrate>
```

Common Baudrate – 9600, 115200, 57600, 38400

Flash Memory Dump – SPI - https://www.flashrom.org/

```
#> flashrom -p ft2232_spi:type = <HW>
```

HW - FT232H or FT2232H

Debuggers

```
#> openocd -f interface/<dev.cfg> -f target</target.cfg>
```

Cfg- files you can find on internet or search /usr/local

OpenOCD - https://openocd.org/pages/about.html

```
telnet localhost:4444
halt – to halt the CPU
reset – to reset the CPU
flash info bank <bankid>
flash dump_image <file> <addr><size>
flash write_image erase <file> <addr>
```

GDB - https://sourceware.org/gdb/

```
gdb-multiarch
set arch <arch – arm/mips>
target remote localhost:3333
```

Read Data from Flash Memory Address - https://docs.u-boot.org/en/latest/usage/cmd/sf.html

probes SPI flash memory connected to SPI bus 0

```
# > sf probe 0
```

Command to read data from SPI flash memory

```
#> sf read <destination address> <source address> <length>
```

Communication Interfaces PINs

UART	SPI	I2C	JTAG
TX	SCK	SCK	TCK
RX	MOSI	SDA	TDI
	MISO	SDA	TDO
	CS		TMS

JTAG – 20 PINs		JTAG – 10 PINs		ST-Link – 10 PINs	
VCC	VCC	RST	SCK	VCC	SWD/TMS
TRST	GND				
TDI	GND	SWIM	SWD	GND	SCK/TCK
SWD/TMS	GND				
SCK/TCK	GND	GND	GND	GND	SWO/TDO
RTCK	GND				
SWO/TDO	GND	3.3V	3.3V	KEY	TDI
RESET	GND				
NC	GND	5V	5V	GND	nRESET
NC	GND				

Attify OS - https://www.attify.com/attifyos

Flashrom - https://www.flashrom.org/