Raspberry Onion
Hear your network

Snort	www.snort.org
Version show	sudo snort -v
Config file	/etc/snort/snort.conf
Logs file	/var/log/snort
Service start	sudo systemctl start snort
Service stop	sudo systemctl stop snort
Service status	sudo systemctl status snort

Barnyard2	https://github.com/firnsy/barnyard2
Version show	/usr/local/bin/barnyard2 -V
Config file	/etc/snort/barnyard2.conf
Waldo file	/var/log/snort/barnyard2.waldo
Service start	sudo systemctl start barnyard2
Service stop	sudo systemctl stop barnyard2
Service status	sudo systemctl status barnyard2

PulledPork	https://github.com/shirkdog/pulledpork
Version show	/usr/local/bin/pulledpork.pl -V
Config file	/etc/snort/pulledpork.conf
Rules update	sudo pulledpork.pl -c /etc/snort/pulledpork.conf

Aanval	https://adaptive.codes/pages/aanval
BPU run	sudo php /var/www/html/bin/console aanval:bpu:run
BPU start	sudo php /var/www/html/bin/console aanval:bpu:start
BPU stop	sudo php /var/www/html/bin/console aanval:bpu:stop
Status check	ps aux | grep BPU
SMT run	sudo php /smt/smt aanval:smt:run
SMT start	sudo php /smt/smt aanval:smt:start
SMT stop	sudo php /smt/smt aanval:smt:stop
SMT status	ps aux | grep SMT
Web address	localhost
Login	admin
Password	specter

Fail2ban	https://www.fail2ban.org/wiki/index.php/Main_Page
Config file	/etc/fail2ban/jail.conf
Logs file	/var/log/fail2ban.log
Local filters	etc/fail2ban/jail.d/defaults-debian.conf

NIDS rules management	
Local rules	/etc/snort/rules/local.rules
Modified rules	/etc/snort/modifysid.conf
Disabled rules	/etc/snort/disablesid.conf
Enabled rules	/etc/snort/enablesid.conf
Rule threshlods	/etc/rules/threshold.conf
Rule signatures	/etc/snort/sid-msg.map

MySQL database	
Name	snort
Login	snort
Password	ronion

Maltrail	https://github.com/stamparm/maltrail
Service start	Terminal 1 : sudo su && cd ~/maltrail/maltrail && sudo python sensor.py Terminal 2 : sudo su && cd ~/maltrail/maltrail && sudo python server.py
Sensor stop	sudo pkill -f sensor.py
Server stop	sudo pkill -f server.py
Config file	sudo su && cd ~/maltrail/maltrail/maltrail.conf
Logs file	/var/log/maltrail
Web address	localhost:8338
Login	admin
Password	changeme!

Chaosreader	https://github.com/brendangregg/Chaosreader
Service start	cd /tcpdump && sudo chaosreader -D fichierSortie tcpdump.pcap

Tcpdump	https://www.tcpdump.org/
Logs file	/home/pi/tcpdump
Service start	sudo systemctl start tcpdump
Service stop	sudo systemctl stop tcpdump
Service status	sudo systemctl status tcpdump

TrimPCAP	https://www.netresec.com/?page=TrimPCAP
Config file	/etc/cron.d/trimpcap
Logs file	/var/log/trimpcap.log

CyberChef	https://github.com/gchq/CyberChef
Web address	localhost/CyberChef/Cyberchef.html