{elysiumsecurity}

Guide

How to setup Security Onion on a home network with Splunk, email alerts and some basic tuning

Date: April 2015
Version: 3
Author: Sylvain Martinez
Twitter: @__bugs

Website: http://www.elysiumsecurity.com
Twitter: @elysiumsecurity

Document Change Logs

V3 - April 2015
Updated links to new SO GitHub repository
Updated document headers/footers template

V2 - March 2015
Added a Sguil tuning entry in section 4
Added Sguil DB purge info in section 9

V1 - March 2015
Initial release

Security Onion (SO) is a great open source project created by Doug Burks.
It is a Linux Distribution based on Ubuntu and bundled/configured with all the tools you need to get a powerful, and free, Network Security Monitoring system (NSM). It can be used to monitor your network traffic for suspicious activities and malware.

This guide is aimed at people who quickly want to get started with SO with the following basic functionalities:

- Getting an understanding of what Network and Server setup are required
- Going through a basic SO installation
- Getting basic understanding on how to tune Snort and remove false positives
- Getting regular reports and specific signature alerts emailed to you
- Installing Splunk and getting an additional platform to mine information
- How to clean SO data and do some basic maintenance

This guide is NOT aimed at the advanced Security Onion user.

The amount of information and documentation available from the official SO WIKI is very impressive and comprehensive. Therefore this guide has been created mainly to extract and present some key information on installing and running SO in a different light, maybe in a more layman's way. It also combines information from many different sources, hoping to save time for the reader who may be faced with some similar hurdles as the author faced when setting up SO the first time.
There is also a very active support forum, available here , where Doug Burks himself seems to be spending a lot of his time answering questions very quickly and always being very helpful. Please note this guide was written with a Home Network in mind, with only one instance of SO running within a VM and therefore not using any nodes. Some information are still relevant to a commercial environment but the basic SO and Network configuration section would be different.

Installing SO is fairly straight forward, there are also many guides out there on how to configure it. However, getting value out of it takes some time and effort, especially if your network/security/linux skills are a bit rusty.

We have been using SO for some time and found it extremely useful in detecting and understanding risks related to surrounding network activities. It has helped us detect malware, miss-configured applications, ad-aware/monitoring activities, vulnerable clients/servers, etc. Obviously, at the core of it, there is Snort or Suricata, but what SO provides is a nicely bundled framework to quickly and easily deploy those technologies and visualise their results in a meaningful way.

How meaningful and useful SO can be, will depend on 3 factors:

- **Network visibility:** You need to be able to see all traffic from the network(s) you want to monitor
- **Tuned environment:** Unless you can remove most of the false-positives, the alerts you get are meaningless
- **Alert and reporting automation:** You want SO to alert you and inform you when required and/or on a regular basis

In order to achieve the above, this guide will cover the following topics:

1. Define a suitable network infrastructure
2. Define a suitable server configuration
3. Install and configure a basic SO instance
4. Rules Tuning
5. Get automated daily and weekly Snorby report emails
6. Get "live" automated emails sent for specific alerts
7. Install Splunk as a complementary mean to inspect/search data
8. Remotely Connect to Splunk and Snorby
9. How to clean SO data if you want to start afresh whilst keeping your settings
10. How to go further

All the information discussed below is available in some shape or form in the Security Onion WIKI and by doing a few Google searches. Hopefully, having it all centralised into one article/guide will help some of you to go from a nice ISO image sitting in your download folder to a fully functioning NSM providing relevant alerts.

1. Define a suitable network infrastructure

You need to be able to see as much network traffic as possible in order for SO to analyse it. The best, and probably only option!, is to create a network TAP or SPAN port on your router.

A typical home setup is either one of the following environment:

- A. Internet -> (Optional Fibre Router) -> ISP Modem Router also providing WIFI -> Clients (Ethernet and WIFI)
- B. Internet -> (Optional Fibre Router) -> ISP Modem Router -> WIFI Router -> Client (Ethernet and WIFI)

In either case you want to see the network traffic from/to the Internet and the Clients.
In an ideal world you would also want to see traffic between WIFI clients. However, despite all the tests we have done and the different routers we have tested, there were no solutions to see INTRANET Wifi traffic, simply because such traffic is usually going through a dedicated local bridge that is not possible to duplicate. If anyone has managed to do that, we would love to hear from you! And yes, we did play with DD-WRT/Tomato, iptables, mangle rule, etc.
One area to explore would be to use some kind of MiM server pretending to be your WIFI MAC address but that will be for a future article :)

There are different ways to create such TAP/SPAN, below are two possible examples:

- A. Internet -> (Optional Fibre Router) -> ISP Modem Router with WIFI DISABLED -> TAP: Switch/HUB -> WIFI Router with NAT Disabled -> Clients (Ethernet and WIFI)
- B. Internet -> (Optional Fibre Router) -> TAP: Modem Router-> WIFI Router with NAT Disabled -> Clients (Ethernet and WIFI)

The 2 key elements are for your NAT to be disabled on your WIFI router and for you TAP to be installed between your WIFI router and the Internet. The TAP will, of course, have to be connected to your SO instance.
The reason we need NAT disabled is to see individual IP from your WIFI network rather than just the WIFI gateway IP (likely to be 192.168.X.1)

We have had some success with option A by using the Netgear GS-105E as a TAP, it can easily be configured to duplicate its ethernet ports to a dedicated SPAN Ethernet port and cost only about £20. Note that if you are using an Apple TimeCapsule/Router it implements a slightly different version of NAT and you should be able to keep NAT ON and still see individual WIFI client IP addresses. It is the only router we witnessed this behaviour.

With Option B, the best Modem Router we found is the Mikrotik RB2011Ui . It is an amazing router which has an incredible array of options, it might be a bit daunting for some as it requires quite a few tweaks and manual configuration but at around £80 it is still quite cheap. Did we mentioned it has a touch screen too? ;)
You can configure that router to duplicate an ethernet port to a SPAN port which you would have to connect to your SO instance.

With such setup you should be able to see individual traffic from/to the internet and your network clients, as well as being able to see each individual IP.

2. Define a suitable server configuration

Although you can run SO on a dedicated server, it is quite convenient to actually run it on a Virtual Machine and this is what we will be doing for this guide, using VMWARE.
Whatever environment you choose, the hosting server must have 2x network interfaces:
1x for Management (i.e: WIFI connection) and 1x for monitoring (i.e.: Ethernet connection).
For better efficiency, and less packet drops, the monitoring interface should not have any IP addresses assigned to it. On a MAC this means turning off IPv4 configuration.
Further Hardware requirements information is available on the Security Onion Wiki

We assume your hosting environment is connected to the Internet via a WIFI connection and that you have an ethernet port which is enabled but not setup (no IP configuration)
In VMware, the steps required are:

- Create a new Machine and select Install from disc or image
- Select the Security Onion ISO (which you can download from here)
- VMWare should automatically detect the OS to be Ubuntu 64-bit, if not this is the OS you should select
- Go to "Customize settings" and set the following:
- If you have a multicore CPU, select 2 cores
- 4Gb minimum of Memory
- 40Gb minimum of Disk Space
- Configure you network to be Bridged on WIFI (this can always be changed later to NAT if you have issues getting an IP address)
- Add a new Network Device, Ethernet and Bridged (this interface must NOT be set to NAT)
- Setup some Shared folders if you need to.

3. Install and configure a basic SO instance

If you have time and want more detailed information, the following 3x links will explain all the steps you need to install and configure SO:

- https://github.com/Security-Onion-Solutions/security-onion/wiki/Installation
- https://github.com/Security-Onion-Solutions/security-onion/wiki/IntroductionWalkthrough
- http://www.drchaos.com/ultimate-guide-to-installing-security-onion-with-snort-and-snorby/

If you are in a hurry, below is a summary of the steps we used to install SO version 12.04.5.1:

- In the VMware virtual machine you created previously, run the image in LIVE MODE
- click the install Link on the Security Onion Desktop
- Select "Download update while installing" and "Install third Party Software"
- Reboot your VM when prompted to do so, and press ENTER if asked to remove the install disc
- Log on to your SO instance once the reboot is completed and run the following command as root:
- apt-get update; apt-get upgrade
- Some updates may not install through the command line (i.e. new kernel). By now you should see a red exclamation mark on the top right VM toolbar
- Click on the exclamation mark and select "show updates" then click on install updates
- Reboot your VM once more to ensure the updates have been applied correctly (and probably load a new linux kernel too)

You should also Install VMWARE Tools, with more details available in this install guide

Below is a summary of the steps we used to install VMwaretools on SO:

- Select the option to install the VMWARE tools from the VMWARE "Virtual Machine" menu (note this menu is outside your VM)
- This will mount the VMWARE Tools disc
- Open a command prompt, and as root, do the following commands:
- Copy the tar.gz from /media/VMware Tools/ to /tmp
- Go to the /tmp directory
- unmount /media/VMware Tools
- decompress the file using tar -xvzf filename.tar.gz

NOTE that you are very likely to get an error message when trying to compile the VMwaretools and enabling host file sharing. Look out for error messages involving the vmhgfs.ko file. If this occurs, interrupt the installation and then follow the instructions from a previous post we recently published explaining how to fix that problem.

- Run the install script from the directory you just decompressed
- Keep all the default settings (keep an eye for any compiling errors)
- Follow the post install instructions by running the command:
- /usr/bin/vmware-user
- log out and log back on

Configure your installation

- From a terminal, check which interface has an IP: ifconfig -a
- Only one should have an IP, the other one (WIRED) should not and will be used to sniff traffic
- Run setup from the link on the desktop
- Select eth0 for management (Assuming this is the one which has an IP - WIFI)
- select eth1 for monitoring (Assuming this is the one which has no IP - ETHERNET)
- You will be prompted to reboot
- Once the reboot is completed, run setup again, you can skip the network configuration this time
- Select Quick Setup, click on all default settings offered to you as well as setting a userID/email/password for the different SO applications

You may want to also check the post installation recommendation from the SO WIKI

Customise your network settings (needs root access)

- These steps are optional, in case you want to restrict the number of IP ranges that are expected to be local to your network
- Edit the following 3 files in /etc/nsm/yourMONITORINGinterface/ (likely eth1)

snort.conf
suricata.yaml (in case you use it later)
prads.conf

- For each of those files change the HOME_NET ip range to reflect your network IP range, ie.: 192.168.2.0/24
- You will also need to apply the same changes in the following file: /opt/bro/etc/networks.cfg
- To apply the changes run: nsm_sensor --restart

To quickly and visually confirm your installation is working, from a terminal as root run the following command: etherape (to install: apt-get install etherape)
Select the Capture interface to be eth1, and you should see network traffic from all the active clients on your network.
etherape value is limited, but it has a nice eye candy feel to it, and provides a very visual cue as to how much activity is occuring on your network.

4. Rules Tuning

The best place to tune your IDS alerts is to read the relevant SO WIKI Section

Snort tuning

The key for SO to be effective is to eventually remove as much false positives as possible and only get alerted of new or real warnings. To do so, you need to update the following file: /etc/nsm/rules/threshold.conf

- Let security onion run for a few days
- Check the most noisy rules
- Suppress those noisy/false positive rules by adding some "suppress lines" to the threshold.conf file

You can suppress those rules in different ways:

- Disable the rule for every client:

```
suppress gen_id 1, sig_id 2002334
```

- Disable the rule for a specific IP (by_src or by_dst)

```
suppress gen_id 1, sig_id 2002334, track by_src, ip 192.168.2.45
```

- Disable the rule for an ip range (by_src or by_dst)

```
suppress gen_id 1, sig_id 2002334, track by_src, ip [192.168.2.45, 192.168.2.56]
```

You can also use a subnet such are 192.168.2.0/24

Note that for the changes to take effect you need to run the following command:

```
$ sudo rule-update
```

- Finally, to test you can detect and alert when signatures are triggered, you can create a local rule which will generate a warning if a ping traffic is detected originating from SO:
- Edit the file /etc/nsm/rules/local.rules, and add the following line where SO_IP is the IP of your SO instance:

```
alert icmp SO_IP any -> any any (msg:"ICMP test"; sid:10000001;)
```

To trigger the alert, from your SO machine, ping google.com or any other external IP address (remember you are unlikely to see internal WIFI traffic, so pinging another WIFI client would not be detected)

Sguil tuning

You should inspect and manage the events in Sguil everyday, its database doesn't grow too big.

- To do that you need to log on the Sguil Portal using the shortcut on the desktop and categorise the different events using your Function keys.
- For more information on Sguil and the different function keys (F1-F7 = prioritise events 1 to 7 and F8 = Expire it), look at this page

Another way is to autocategorize events:

- Edit the file: /etc/nsm/securityonion/autocat.conf
- For example, if you want to autocategorize PADS event, add the following line to specify no further action is required (the "1" at the end of the line)

```
noneIIANYIIANYIIANYIIANYIIANYIIANYII%%REGEXP%%^PADSII1
```

More information and examples are available in this article.

5. Get automated daily and weekly Snorby report emails

Snorby generates great and easy to read reports: daily/weekly/monthly. They provide a quick overview of your top IDS signatures as well as your source and destination addresses.

- To enable this feature, you need to edit: /opt/snorby/config/initializers/mail_config.rb
- The ruby file has a template for gmail built-in, you just need to enter your gmail account credentials and uncomment the relevant lines by removing the "#"
- Once this is done, you need to run the following 2 commands:

```
$ sudo pkill -f delayed_job
$ sudo su www-data -c "cd /opt/snorby; bundle exec rake snorby:update RAILS_ENV=production"
```

6. Get "live" automated emails sent for specific alerts

In addition to receiving daily/weekly/monthly report, you may want to receive an email alert when a specific signature is found on your network. This can be very useful in helping identify what triggers an alert by being notified when it happens.
The following steps will allow you to configure the same GMAIL account used in the previous Snorby section. The information has been taken from this runabove article and this SO WIKI article

- Start by installing the required packages

```
$ sudo apt-get install postfix mailutils
```

- Edit the file: /etc/postfix/main.cf, and add/modify the following lines:

```
relayhost = [smtp.gmail.com]:587
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl/sasl_passwd
smtp_sasl_security_options = noanonymous
smtp_tls_CAfile = /etc/postfix/cacert.pem
smtp_use_tls = yes
```

- Validate Certificate & Open/Create sasl_passwd:

```
$ sudo cat /etc/ssl/certs/Thawte_Premium_Server_CA.pem >> /etc/postfix/cacert.pem
```

- Edit /etc/postfix/sasl/sasl_passwd. And add following line, replacing USERNAME and PASSWORD with your gmail credentials.
- *(If you have enabled 2-Step-Verification, use a Google App password for PASSWORD)*

```
[smtp.gmail.com]:587 USERNAME@gmail.com:PASSWORD
```

- Set sasl_passwd file permission and update postfix config to use sasl_passwd file:

```
$ sudo chmod 400 /etc/postfix/sasl/sasl_passwd
$ sudo postmap /etc/postfix/sasl/sasl_passwd
```

- Reload postfix config for changes to take effect:

```
$ sudo /usr/sbin/postfix reload
```

- To confirm everything is working, send a test email

```
$ echo "Test mail from postfix" | mail -s "Test Postfix" you@example.com
```

- For troubleshooting any problems you should run the following command and review any errors

```
$ tail -f /var/log/mail.log
```

If the above file is empty, it is because you have ELSA enabled. So instead, launch ELSA, click in the left-menu on "Host Logs -> Syslog-NG (program) -> postfix/smtp"
If you really want to get logs (duplicated) in /var/log/ then you should read this article

You can also read the runabove article which contains further information and is where the above steps were taken from.

You can now forward local emails
Following instructions from this webpage, lets forward all emails sent to root@localhost to your gmail account:

- Edit /etc/aliases and add the following line:

```
root: yourexternalemailaddress@gmail.com
```

- Then run the following commands:

```
$ sudo newaliases
$ sudo service postfix restart
```

- Test sending emails to root@localhost get forwarded:

```
echo test | mail -s "test message" root
```

Configure Sguil to send emails against specific detected signatures

- Change the following in the /etc/nsm/securityonion/sguild.email file, from a default install you should only need to update the lines highlighted in bold

```
set EMAIL_EVENTS 1
set SMTP_SERVER smtp.example.com
set EMAIL_RCPT_TO "root@localhost"
set EMAIL_FROM "root@localhost"
set EMAIL_CLASSES "successful-admin trojan-activity attempted-admin attempted-user"
set EMAIL_PRIORITIES "0"
set EMAIL_DISABLE_SIDS "0"
set EMAIL_ENABLE_SIDS "10000001"
```

- Add the following line in /etc/hosts smtp.example.com   localhost
- Restart sguild:

```
sudo nsm_server_ps-restart
```

- Check you see a reference to "Email Configuration" and no errors:

```
sudo head -20 /var/log/nsm/securityonion/sguild.log
```

The SID "10000001" is the test rule we created earlier and generated with a ping
You can also specify different classes and priorities (1 to 5) if you want broader email alerts

Note that emails will only be sent for new *type* of events in Sguil.
Thus if you notice you don't receive any emails but the signature do get logged: logon into Sguil, locate the event you were expecting an email for, select it and press F8.
This will expire the event, basically clearing it from Sguil which means next time it occurs it will generate an email. You have to repeat this "F8" step if you want to receive further emails on a specific event.

7. Install Splunk as a complementary mean to inspect/search data

SPLUNK is a great log management tool, it does not come with SO but installing it is a great addition. It will allow you to search/mine data further against a specific IP address you might be interested in, as a result of a Snort/Suricata alert.
It has an SO module that integrates really well to an SO instance
To download Splunk you will need to register first, but that's free!

Below are the steps required to install Splunk on SO:

- Download the 64 bit Debian version (.deb) of Splunk ENTERPRISE from the SPLUNK Webpage
- You can also check this YOU TUBE INSTALLATION VIDEO which will provide further information
- Go to the folder you downloaded Splunk and run the following commands:

```
$ sudo dpkg -i splunk*.deb
$ cd /opt/splunk/bin
$ sudo ./splunk start —accept-license
$ sudo ./splunk enable boot-start
```

Installing Flash

To get some of the nice (but maybe pointless) animation in the Security Onion App for Splunk, you need to install Flash and use Firefox
The reason you need to use Firefox is because there isn't a flash version for Chrome in 64 bits available.

- Start Firefox
- Download Flash (Select APT for Ubuntu 64 bits)
- You will need to select UBUNTU Software Center to install flash when prompted and "run from this source"

Installing the Splunk Security Onion App

Before configuring Splunk, we are also going to download a few "apps" for it, remember where you save those files as we will be using them later.

- Download Sideview (Requires registration)
- Download Reporting and Management for OSSEC
- Download geo location lookup maxmind
- Download google maps
- Download splunk visualisations
- Download security onion

- Start your browser and go to localhost:8000
- Login spunk and change your admin password when prompted
- Go to the Apps menu (top left)
- Click on "Install App from file" and install each .tar.gz file you downloaded earlier. Only accept to restart Splunk after having installed all the apps:

Sideview, OSSEC, Maxmind, Google, Visualisations and finally, Security Onion
Log back in Splunk by going to http://localhost:8000 in a FIREFOX browser. You can use Chrome but the Flash animation will not work, especially the nice SOStats data flow. If the SOStats dashboard is empty, it is easy to recreate an impressive one by creating 4 splitters and daisy chain them: (traffic flow) -> src_port -> src_ip -> dst_ip -> dst_port
If you click on the Splunk logo on the top left corner of your browser, on the left you will see the Security Onion App with all your network data ready to be inspected!

Set retention policy

The default retention time is 6 years with a default index size of 500Gb.
This is not fit for our VM configuration, we will therefore change it to 32 days and 10Gb

- To do that, you need to edit the file: /opt/splunk/etc/system/default/indexes.conf
- Change the value of the first instance of "frozenTimePeriodInSecs" to 2764800 (you can ignore the other instances)
- Near that variable, you will also need to change "maxTotalDataSizeMB" to 10240

For more information on data retention you can read the Splunk documentation

- For the changes to take effect, you will need to run the following command:

/opt/splunk/bin/splunk restart

Upgrading Splunk

From time to time you might want to install new Splunk versions. You will be notified of new versions when you logon to the Splunk Web Interface
When you see such an upgrade notice:

- Download the latest version as instructed above during the first installation (Debian 64bit version)
- use dpkg -i splunk*.tar.gz
- then restart spunk and accept the new license with the following command: /opt/splunk/bin/splunk start

- If you ever get a problem with geoip after an upgrade, complaining it cannot find GeoLiteCity.dat, you can do the following:
- Edit the geo file: $SPLUNK_HOME/etc/apps/maps/default/geoip.conf
- Change the line: database_file = GeoLiteCity.dat
- To: database_file = /opt/splunk/etc/apps/maps/bin/GeoLiteCity.dat
- Restart splunk: /opt/splunk/bin/splunk start

We only witnessed this error once when upgrading from a previous version of Splunk. The newer version should not have that problem.

8. Remotely Connect to Splunk and Snorby

The following instruction were taken from this EyeIS article and will allow you to remotely connect to the Splunk, SO Home and Snorby Web Interface from a different system (computer, tablet, or even phone!)

- On the computer you want to connect from, run: ssh-keygen
- This will generate a ~/.ssh/id_rsa.pub file
- Copy/export it to your SO instance, i.e.: in the /tmp directory
- Open a terminal on your SO instance, as a normal user, NOT root.
- Run the following command:
- cd ~; mkdir .ssh
- cd .ssh; touch authorized_keys
- chmod 644 authorized_keys
- cat /tmp/id_rsa.pub >> authorized_key

- Edit the /etc/ssh/sshd.conf and enable the following:
- RSAAuthentication yes
- PubkeyAuthentication yes
- PasswordAuthentication no
- UsePAM no

- Restart the SSH service with the command: sudo service ssh restart

The approach uses an SSH tunnel and is really easy to setup. On your Security Onion/ Splunk server you'll want to make sure SSH is enabled in Uncomplicated Firewall (ufw).

- The following commands should all be run **as root**

ufw status

- You should see 22/tcp ALLOW in the results. If it says DENY, then enable it:

sudo ufw allow 22/tcp

- Next configure ufw to block (yes I said block) Snorby, Squert and Splunk ports

ufw deny 443/tcp; ufw deny 444/tcp; ufw deny 8000/tcp

- From a remote Linux host with openssh-client installed:

sudo ssh username@securityonion.example.com -L
443:localhost:443 -L 444:localhost:444 -L 8000:localhost:8000

- You will then be able to remotely access Splunk, SO Home and Snorby:

http://localhost:8000 – Splunk
https://localhost:443 – SO Home/Squert
https://localhost:444 – Snorby

9. How to clean SO data if you want to start afresh whilst keeping your settings

Database wipe (This is quite a drastic option)

To wipe most of the traffic/log data you just need to restart the setup procedure, by clicking on the SETUP icon on the desktop.
You can use all the default options and skip the initial network setup.
This process will keep your Snort rules, Sguil and Snorby email settings.

Sguil data wipe

Edit the file: /etc/nsm/securityonion.conf
Change the value of DAYSTOKEEP to a low number (i.e. 1 or 7, for 1 or 7 days)

```
$ sudo sguil-db-purge
```

Change back the DAYSTOKEEP in /etc/nsm/securityonion.conf to whatever value you had

Snorby data wipe

You will only save a bit of disk space by doing that after doing the previous steps.
This will also remove any custom configuration you may have had in Snorby, including asset names.
The command to run as root is: so-snorby-wipe

Splunk data wipe

- Locate spunk folder by running the following command:

```
$ whereis spunk
```

- Go to the binary folder of spunk (most likely /opt/splunk/bin)

```
$ sudo ./splunk stop
$ sudo ./splunk clean eventdata
```

10. How to go further

Add Asset names to Snorby

When looking at your local network traffic in Snorby it is easier to see hostnames rather than just IP addresses.
You have 2 options to do this, either use static IP addresses for each of your clients on your network, or reserve DHCP addresses.
Whatever option you choose, you should maintain a text file with the following format for each entry/line:
IP,Hostname
i.e.: 192.168.0.5, Laptop_son
You can import that list in Snorby by going to Administration -> Asset Manager -> Upload Name Data -> Choose File -> Upload CSV
Alerts will now display the hostnames, if known, rather than just an IP. On a local network you should know each active IP, making it easier to investigate alerts. And if you detect a local IP without a hostname, this may be the sign of a rogue device (or guest!)

Add Asset names to /etc/host

You can also add an IP to hostname mapping at the OS level, this may be useful with etherape and other network tools.
The format for the /etc/host file is:
IP (tab) Hostname
i.e.: 192.168.0.5	Laptop_son

Other useful tools/commands provided by SO (and from the post setup screen)

- sostat (lot of info on the setup)
- sostat-quick (explanation)
- rule-update (update IDS rules, Rules will be updated every day at 7:01 AM UTC. anyway)
- Rules downloaded by Pulledpork are stored in: /etc/nsm/rules/downloaded.rules
- Local rules can be added to: /etc/nsm/rules/local.rules
- To get PulledPork modify the downloaded rules edit: /etc/nsm/pulledpork/

Random useful unix commands

- Finding space left:

```
df -h (disk)
du -h (folder)
```

- Listing the top 10 biggest directories:

```
du -hsx * | sort -rh | head -10
```