Security Onion Management

PREFACE:
You can get most all of this info from google or from https://github.com/Security-Onion-Solutions/security-onion/wiki

Create a Bridge Interface when using a half-duplex Tap:

- Run Initial Setup as normal and select the 2 interfaces coming from the TAP as monitoring for the initial interface setup. When setup is completed it will prompt you to make final changes before rebooting the host. Open a terminal as root as add the following to the interfaces file.

- Edit /etc/network/interfaces
  - sudo nano /etc/nsm/rules/bpf.conf
- Add the following at the bottom of the file:

```
auto br0
iface br0 inet manual
  bridge_ports eth1 eth2
  up ip link set br0 promisc on arp off up
  down ip link set br0 promisc off down
  post-up ethtool -G br0 rx ; for i in rx tx sg tso ufo gso gro lro; do ethtool -K br0 $i off; done
  post-up echo 1 > /proc/sys/net/ipv6/conf/br0/disable_ipv6
```

- Save the file and exit
- Reboot the Computer/Server
- After Reboot Verify that the new br0 interface shows up with ifconfig.
- Now you can run the second setup to configure the onion.
- When it prompts you for sniffing interfaces…deselect the 2 half duplex sniffing interfaces and simply leave the br0 interface as the only interface to sniff on.

Suppress a Rule:

- edit the /etc/nsm/rules/threshold.conf
  - sudo nano /etc/nsm/rules/threshold.conf

- to suppress GID here is an example Example:
  - sudo suppress gen_id 1, sig_id 10000007
    OR
  - sudo suppress gen_id 1, sig_id 10000007, track by_src, ip 172.16.42.109

- restart snort alert and snort agent
  - sudo service nsm_sensor_ps-restart --only-snort-alert

Disabling a Rule Category:

- Edit the /etc/nsm/pulledpork/diablesid.conf
  - sudo nano /etc/nsm/pulledpork/diablesid.conf

- Add the following for each rule:
  - 1:<rule_id>
    FOR EXAMPLE:
  - 1:2812045

- Run rule update
  - sudo rule-update

Disabling a Rule Category:

- If using ET Pro rules remove the emerging threats tar.gz from the /tmp
  - cd /tmp
  - sudo rm -f emerging*tar.gz

- Ensure the ET PRO RULES tar.gz is in the /tmp directory.

- Run this one liner that will go and scrap the downloaded.rules for all the category names, then dump then all to a file in your current directory
  - sudo lz /tmp/*.gz | egrep '\.rules' | cut -d'/' -f3 | sort -u | perl -lne '/(.*)'.rules/ && print $1' > rules.`date +%F`

- Now copy and paste the contents of the file created (IE: rules.<date>) to the disablesid.conf
  - sudo cat rules.2070308 >> /etc/nsm/pulledpork/disablesid.conf

- Now you need to edit disablesid.conf and comment in the categories of rules sets you want to keep active and leave the ones you want to disable uncommented.

- Then run rule-update
  - sudo rule-update

- **Alternative Command to get rules categories
  - sudo cut -d\" -f2 /etc/nsm/rules/downloaded.rules | awk '{print $1, $2}'|sort |uniq -c |sort -nr

Adding Local Rules:

- Navigate to your home directory
  - cd ~

- Make a copy of the local.rules
  - sudo cp /etc/nsm/rules/local.rules

- Rename the file so you don't get confused
  - sudo mv local.rules test_local.rules

- Make this directory for log entries during testing
  - sudo mkdir -p /var/log/snort

- Create all your variables and rules in the test_local.rules. You will need to copy and paste your custom variables in to each snort.conf once you put these rules in production and delete from the local.rules. You put them in local.rules just for testing purposes. Some examples are below for variables.
  - ipvar SERVERS [192.168.1.0/16, 192.5.3.5]
  - portvar HIGH_PORTS [1024:65535]
  - var WHITE_LIST_PATH /etc/nsm/rules

- Once you're done creating all your rules you need to test that your test_local.rules with the following syntax to ensure there are no issues with the file.
  - sudo snort –c test_local.rules –T

- If errors populate, fix the errors. Snort will tell you what's wrong. You can also look in the log file if it generates an error
  - sudo tail -n 50 /var/log/snort/<file_that_is_here>

- Once the file is good to go, add the contents to the real local.rules
  - sudo cat test_local.rules >> /etc/nsm/rules/local.rules

- Add your custom variables (if any) to the snort.conf's for each sniffing interfaces

- Do a rule update and ensure there are no errors generated during the rule update. Make sure the ET PRO rules tar ball is in the /tmp for the rule-update
  - sudo rule-update

- Check the sid-msg.map file to ensure your rules were added to this file.
  - sudo less /etc/nsm/rules/sid.msg.map

Applying Berkeley Packet Filters (BPF):

- Edit bpf.conf
  - sudo nano /etc/nsm/rules/bpf.conf

- Add networks or IP addresses
  - #Nothing from src host to dst port
  - !(src host xxx.xxx.xxx.xxx && dst port 161) &&

  - #Nothing from src host to dst host and dst port
  - !(src host xxx.xxx.xxx.xxx && dst host xxx.xxx.xxx.xxx && dst port 80) &&

  - #Nothing to or from:
  - !(host xxx.xxx.xxx.xxx) &&

  - #Last entry has no final &&
  - !(host xxx.xxx.xxx.xxx)

- #BPF A Network
- !(net xxx.xxx.xxx.xxx/24)

- Restart nsm
  - sudo nsm_sensor_ps-restart

Setting Variables (HOME_NET)in snort.conf:

- Edit each snort.conf for each interface and add the appropriate HOME_NET IP's for example:
  - ipvar HOME_NET [192.168.1.0/16, 192.5.3.5/25]

- Edit each snort.conf for each interface and edit the EXTERNAL_NET variable to:
  - ipvar EXTERNAL_NET !$HOME_NET

- Edit each snort.conf for each interface and add any additional custom variables you want for snort for example:
  - portvar HIGH_PORTS [1024:65535]
  - var WHITE_LIST_PATH /etc/nsm/rules

- Restart snort
  - sudo nsm_sensor_ps-restart –only-snort-agent
  - sudo nsm_sensor_ps-restart –only-snort-alert

Changing Sguil Database Archive and Repair Date Settings:

- Edit the securityonion.conf
  - sudo nano /etc/nsm/securityonion.conf

- Edit the following variables:
  - DAYSTOKEEP=7
  - DAYSTOREPAIR=1

- Restart NSM:
  - sudo nsm_sensor_ps-restart

Settings Network Variables for Bro:

- Open the bro network file
  - sudo nano /etc/bro/etc/networks.cfg

- Add the HOME_NET Subnets here as follows:
  - 10.0.0.0/8
  - 207.133.0.0/16
  - 130.16.100.0/24
  - 130.16.101.0/24
  - 134.11.199.0/24

- Restart Bro
  - sudo nsm_sensor_ps-restart --only-bro

Adding scripts to Bro:

- To enable VLANs and SMB scripts for Bro, edit local.bro and restart bro
  - sudo nano /opt/bro/share/bro/site/local.bro

- Uncomment the following @load scripts
  - @load policy/protocols/conn/vlan-logging
  - @load policy/protocols/smb

- Restart Bro
  - sudo nsm_sensor_ps-restart --only-bro

Using Salt to Manage Sensors:

- The salt commands must be ran from the Master Onion Server

- To verify all your sensors are up:
  - sudo salt '*' test.ping

- To execute a command on all your sensors at once:
  - sudo salt '*' cmd.run 'InsertYourCommandHere'
  - sudo salt '*' cmd.run 'nsm_sensor_ps-restart --only-bro'

Run Away Alert:

- Sometimes there is a custom rule that is written wrong and generates millions of alerts. The following is the process take care of this.

- Disable and Suppress the rule IAW the steps in this document

- Stop some services first
  - sudo nsm_server_ps-stop
  - sudo service nsm_sensor_ps-stop --only-snort-alert
  - sudo service nsm_sensor_ps-stop --only-snort-agent
  - sudo service nsm_sensor_ps-stop --only-barnyard2

- Navigate to where the alerts are written to disk initially
  - cd /nsm/sensor_data/<interface_name>/<worker_number>

- Delete the files
  - sudo rm -f snort.unified.*

- Do this for all sniffing interfaces and their corresponding dedicated workers (CPU Cores)
- Now go to mysql and delete the rules manually
  - sudo mysql

- Show databases available
  - show databases;

- Get into the right database for alerts
  - use securityonion_db;

- Show available tables
  - show tables;

- Show the event details
  - describe event;

- Delete the run away rule by signature_id (AKA:sid)
  - delete from event where signature_id="100007";

- If you can afford to purge and repair the DB do it now otherwise you can now restart. You may want to change the Days to keep and repair days located in the securityonion.conf. Instructions for this is in another section in this document.
  - sudo sguil-db-purge

- Start the services back up and then check the overall status of the services
  - sudo nsm_server_ps-start
  - sudo service nsm_sensor_ps-start --only-snort-alert
  - sudo service nsm_sensor_ps-start --only-snort-agent
  - sudo service nsm_sensor_ps-start --only-barnyard2
  - sudo nsm_server_ps-status

Replaying PCAP:

- Navigate to the directory when there is PCAP to replay. Security Onion ships with plenty of sample PCAP to replay.
  - cd /opt/samples

- Use tcpreplay command to replay the desired pcaps:
  - sudo tcpreplay -i eth1 -M10 /opt/samples/*.pcap

Firewall Commands – Uncomplicated Firewall (UFW)

- There is a command that will walk you through the firewall changes. Follow the prompt.
  - sudo so-allow

Running Setup with ET PRO Rules:

- Copy the ET pro tar.gz into the /tmp directory

- When running setup, select ET PRO and enter a random oink code when prompted (12345)

- If setup has already been run, then edit the pulledpork.conf and uncomment the ET PRO rules line and add a fake oinkcode.

- Make sure the ET pro tar.gz is in the /tmp directory and then run a sudo rule-update

Daily Sensor Status Reports:

- Execute this command to check the status of the sensor:
  - sudo sostat | less

- CPU Utilization looking the load average [round up and divide x/12= percentage]
  - cpu_usage= 50%

- # For pcap loss go to "PCAP LOSS STATS" and divide the dropped by the RX packets to get your %:
  - pcap loss= .001%

- #Stats for IDS (snort) it will be in "IDS Engine":
  - IDS snort Loss= 0%

- #for bro packet loss go to the section below IDS engine called BRO:
  - Bro Packet Loss= .02%

- # for storage information go to "Log Archive"
  - Pcap storage for today= 3 tb
  - bro logs for today= 1 gb

Important Standard File Locations:

- Bro logs
  - /nsm/bro/logs

- PCAP
  - /nsm/sensor_data/<interface_name>/dailylogs/

- Snort.conf
  - /etc/nsm/<interface_name>/snort.conf

- Rules
  - /etc/nsm/rules

- Threshold.conf
  - /etc/nsm/rules

- Diasblesid.conf
  - /etc/nsm/pulledpork/

- Bpf.conf

- /etc/nsm/rules

- Unified2 files
  - /nsm/sencor_data/<interface_name>/<snort_worker_number>

- Local.bro
  - /opt/bro/share/bro/site

- Intel.dat for bro
  - /opt/bro/share/bro/intel