Important Files

Configuration Files	
Configuration	**File**
General Settings	/etc/nsm/securityonion.conf
Sensor Settings	/etc/nsm/<sensor>/sensor.conf
Maintenance Scripts	/etc/cron.d/
Snort	/etc/nsm/<sensor>/snort.conf
Suricata	/etc/nsm/<sensor>/suricata.yaml
Bro	/opt/bro/
Bro Config	/opt/bro/etc
Bro Local Policy	/opt/bro/share/bro/site/local.bro
ELSA Web UI	/etc/elsa_web.conf
ELSA Node	/etc/elsa_node.conf
Syslog-NG	/etc/syslog-ng/syslog-ng.conf
OSSEC	/var/ossec/etc/ossec.conf
Sguil	/etc/nsm/securityonion/sguild.conf
E-Mailed Alerts	/etc/nsm/securityonion/sguild.email

Log Files	
Service	**Log File**
Bro	/nsm/bro/logs/current/stderr.log
ELSA	/nsm/elsa/data/elsa/log
OSSEC	/var/ossec/logs/ossec.log
Sensor Logs	/var/log/nsm/<sensor>/snortu-n.log, barnyard2-n.log, suricata.log, netsniff-ng.log

Rule Management	
Configuration	**File**
IDS Rules (Downloaded)	/etc/nsm/rules/downloaded.rules
IDS Rules (Custom)	/etc/nsm/rules/local.rules
Rule Thresholds	/etc/nsm/rules/threshold.conf
Disabled Rules	/etc/nsm/pulledpork/disablesid.conf
Pulled Pork Config	/etc/nsm/pulledpork/pulledpork.conf
Modified Rules	/etc/nsm/pulledpork/modifysid.conf
OSSEC Rules (Default)	/var/ossec/rules/
OSSEC Rules (Custom)	/var/ossec/rules/local_rules.xml

Packet Filtering	
Scope	**BPF File**
Server	/etc/nsm/rules/bpf.conf
Sensor Specific	/etc/nsm/<sensor>/bpf.conf
Component Specific	/etc/nsm/<sensor>/bpf-bro.conf,bpf-ids.conf,etc

Data

Sensor Data Directories	
Data	**Directory**
Packet Capture	/nsm/sensor_data/<sensor>/dailylogs/
Alert Data	/nsm/sensor_data/<sensor>/
Bro (Archived)	/nsm/bro/logs/yyyy-mm-dd
Bro (Current Hr)	/nsm/bro/logs/current
Bro Extracted Files	/nsm/bro/extracted

Common Tasks

General Maintenance	
Task	**Command**
Check Service Status	service nsm status
Start/Stop/Restart All NSM Services	service nsm start|stop|restart
Start/Stop/Restart Server	nsm_server_ps-start|stop|restart
Start/Stop/Restart Sensor	nsm_sensor_ps-start|stop|restart
Add Analysis (Sguil, etc) User	nsm_server_user-add
Add Firewall Rule	so-allow
Update Ubuntu and SO	soup
Update Rules	rule-update
Generate SO Statistics	sostat
Create a Remote Backup	rysnc –av <source> <user>@<server>:<path>

Salt Commands (from Master Server)	
Task	**Command**
Execute Command	salt '*' cmd.run 'command'
Verify Sensors Up	salt '*' test.ping
Update Minions	salt '*' state.highstate
Update Sensors	soup && salt '*' cmd.run 'soup –y'

Support
Mailing List https://groups.google.com/forum/#!forum/security-onion
Wiki http://securityonion.net/wiki
Blog http://blog.securityonion.net/
Enterprise Support https://securityonionsolutions.com/

Designed by: Chris Sanders – http://www.chrissanders.org - @chrissanders88
Security Onion Version: 14.04.5.2
Last Modified: 8.7.2017