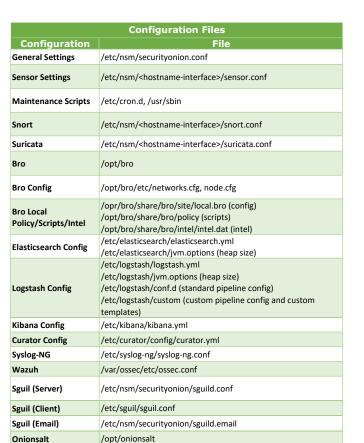
IMPORTANT FILES



Log Files		
File		
/nsm/bro/logs/current/stderr.log (errors), reporter.log (errors/warnings), loaded_scripts.log (loaded scripts)		
/var/log/elastalert/elastalert_stderr.log		
/var/log/elasticsearch/ <hostname>.log</hostname>		
/var/log/logstash/logstash.log		
/var/log/kibana/kibana.log		
/var/ossec/logs/ossec.log		
/var/log/nsm/ <hostname-interface>/snortu-n.log, barnyard2-n.log, suricata.log, netsniff-ng.log</hostname-interface>		
/var/log/nsm/securityonion/sguild.log		

Performance Tuning		
Target	Parameter/File	
Bro	lb_procs in /opt/bro/etc/node.cfg	
Snort/Suricata	IDS_LB_PROCS in /etc/nsm/ <hostname-interface>/sensor.conf</hostname-interface>	
PF_RING	min_num_slots in /etc/modeprobe.d/pfring.conf	
Netsniff-NG	PCAP_OPTIONS, PCAP_SIZE, PCAP_RING_SIZE in /etc/nsm/ <hostname-interface>/sensor.conf</hostname-interface>	



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
Modified Rules	/etc/nsm/pulledpork/modifysid.conf
PulledPork Config	/etc/nsm/pulledpork/pulledpork.conf
Wazuh Rules	/var/ossec/rules
Wazuh Rules (Custom)	/var/ossec/rules/local_rules.xml
Elastalert	/etc/elastalert/rules

Packet Filtering	
Scope	File
Server (Entire Deployment)	/etc/nsm/rules/bpf.conf
Sensor-Specific	/etc/nsm/ <hostname-interface>/bpf.conf</hostname-interface>
Component-Specific	/etc/nsm/ <hostname-interface>/bpf-bro.conf, bpf-ids.conf, etc.</hostname-interface>

DATA

Data Directories	
Data	Directory
Packet Capture (Sensor)	/nsm/sensor_data/ <hostname-interface>/dailylogs</hostname-interface>
Alert Data (Sensor)	/nsm/sensor_data/ <hostname-interface></hostname-interface>
Alert Data (Master)	/var/lib/mysql/securityonion_db
Bro (Archived) (Sensor)	/nsm/bro/logs/yyyy-mm-dd
Bro (Current Hr) (Sensor)	/nsm/bro/logs/current
Bro Extracted Files (Sensor)	/nsm/bro/extracted (only EXEs extracted, by default)
Elasticsearch (Master/Heavy/Storage)	/nsm/elasticsearch/nodes/x/indices

Originally Designed by: Chris Sanders - http://www.chrissanders.org - @chrissanders88 Updated by: Wes Lambert - https://securityonion.net - @therealwlambert Security Onion Version: 16.04.5.6 Last Modified: 02.05.2019

COMMON TASKS

General Maintenance	
Task	Command
Check Service Status	so-status
Start/Stop/Restart All Services	so-start stop restart
Start/Stop/Restart Server Services	so-sguild-start stop restart
Start/Stop/Restart Sensor Services	so-sensor-start stop restart
Start/Stop/Restart Docker	docker start stop restart
Start/Stop All Docker Containers	so-elastic-start stop
Start/Stop Specific Container/Service	so- <noun>-verb Ex: so-logstash-start stop</noun>
Add Analyst (Sguil/Squert/Kibana) User	so-user-add
Change Analyst User Password	so-user-passwd
Add/View Firewall Rules (Analyst, Beats, Syslog, etc.)	so-allow so-allow-view
Update SO (and Ubuntu)	soup
Update Rules	rule-update
Generate SO Statistics	sostat
Check Redis Queue Length	redis-cli 'llen logstash-redis'

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'	

Port/Protocols/Services (Distributed Deployment)		
Port/Protocol	Service/Purpose	
22/tcp (Sensor/Master)	SSH access/AutoSSH tunnel from sensor(s) to Master	
4505-4506/tcp (Master)	Salt comm from sensor(s) to Master	
7736/tcp (Master)	Sguild comm from sensor(s) to Master	

Support Mailing List https://groups.google.com/forum/#!forum/securityonion Reddit https://www.reddit.com/r/securityonion/ Wiki https://securityonion.net/wiki Blog https://blog.securityonion.net Enterprise Support https://securityonionsolutions.com