DINAS KOMUNIKASI DAN INFORMATIKA KOTA TANGERANG
[UNTUK ORANG DALAM]

SECURITY ONION

INSTALLASI, KONFIGURASI, HARDENING, TROUBLESHOOTING

Muhammad Ridwan Na'im

PENGENALAN NETWORK SECURITY MONITORING (NSM)

Network Security Monitoring (NSM) adalah suatu sistem yang dirancang untuk mengawasi jaringan terkait keamanan. NSM sangat berguna dan memungkinkan kita untuk melakukan antisipasi jika terjadi percobaan serangan pada jaringan atau *server*. Bisa juga digunakan sebagai alat untuk mengidentifikasi kerentanan pada sistem jaringan kita serta dimanfaatkan sebagai alat *research* untuk mengetahui model serangan yang terjadi dan *trend* serangan yang terjadi dalam periode tertentu. Data yang diperoleh dari NSM akan dianalisa untuk menentukan langkah selanjutnya.

Beberapa komponen dari NSM:

1. Full Packet Capture via Netsniff (Contoh: Wireshark, NetworkMiner)
2. Network Based dan Host Based Intrussion Detection System (NIDS & HIDS)
3. Analysis Tools (Bro, Squert, Sguild, Kibana, CapMe)

CARA KERJA NETWORK SECURITY MONITORING (NSM)

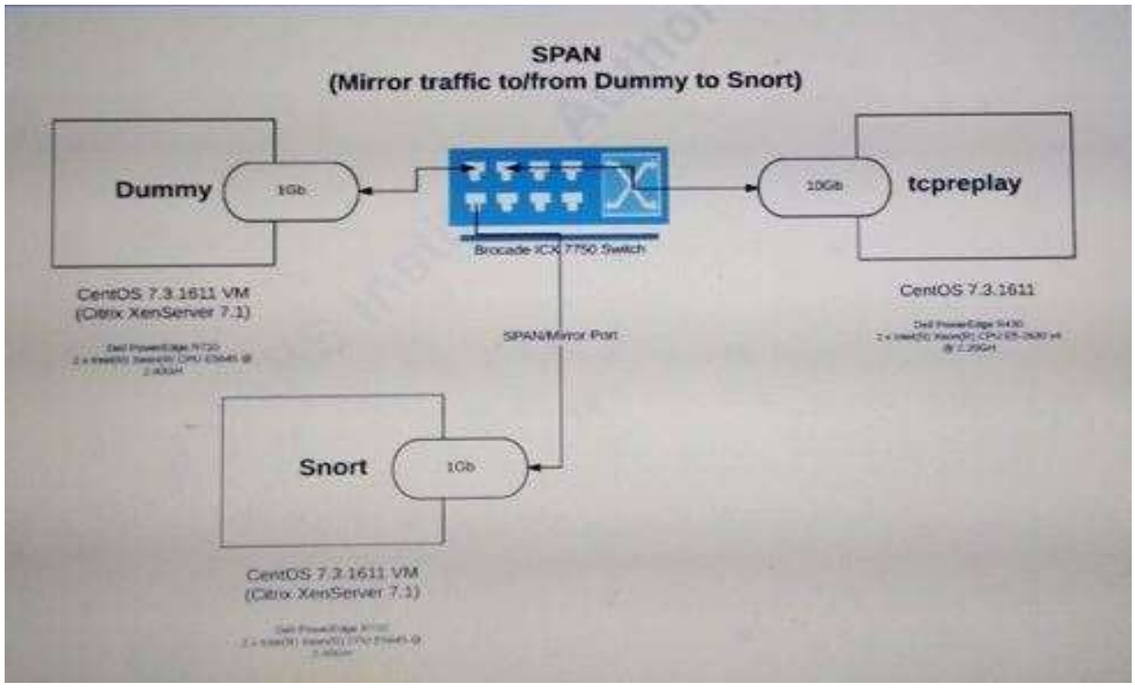
Netsniff menerima semua lalu lintas data yang berada pada jaringan yang sama lalu disimpan oleh NSM *Engine* dalam bentuk *log.* Data yang diterima sangat lengkap, seperti *source* dan *destination address*, kapan waktunya, dan apa yang dibawa oleh *traffic* tersebut. Apakah sebuah *traffic* biasa, atau bahkan sebuah ancaman seperti *exploit, email phishing,* atau *file exfiltration.* Semua akan terbaca secara lengkap.

Log dari netsniff inilah yang kemudian dibaca oleh IDS (*Intrussion Detection System*) dengan cara mencocokkan pola *traffic* tersebut dengan *rule* yang ada. Di antara software IDS yang familiar dan bersifat *open source* adalah *snort* dan *suricata*. IDS memiliki *rule* yang menentukan apakah suatu *traffic* data yang datang adalah suatu ancaman (*Intrussion*) atau bukan. Tentunya ini tergantung dengan konfigurasi IDS. Jika konfigurasi tidak akurat, maka akan terjadi kemungkinan *false-positive* atau *false-negative. False positive* adalah suatu keadaan di mana IDS membaca sebuah *traffic* sebagai ancaman, padahal pada kenyataannya *traffic* tersebut bukanlah ancaman. Sementara *false-negative* adalah suatu keadaan di mana IDS menganggap bahwa sebuah *traffic* bukanlah ancaman, padahal kenyataannya *traffic* tersebut adalah merupakan sebuah ancaman. Hal ini dapat diminimalisir dengan memperbaiki konfigurasi pada *software* IDS atau memodifikasi *rule*-nya –menyesuaikan dengan kebutuhan pada sistem jaringan kita.

Rule IDS inilah yang menentukan nama atau teknik serangan, *severity* (Level Ancaman; *Low, Medium, High*), dan kategori serangan. Semua dicatat dalam bentuk *log.*

Selanjutnya, *log* dari IDS bisa dikelola lebih lanjut. Apakah *log* tersebut akan dikirim ke dalam database atau dikonfersi dalam bentuk JSON dan dikirim oleh *logstash* ke dalam *elasticsearch*. Hal ini dilakukan agar *log* yang ada bersifat *human-readable*. Mudah dibaca oleh manusia dan ditampilkan dalam bentuk *dashboard.* Hal ini juga mempermudah kita dalam menganalisa, membuat laporan, serta mengambil tindakan selanjutnya.

Konsep sederhana peneraapan NSM pada sebuah jaringan seperti yang tergambar pada topologi berikut di mana *Snort* difungsikan sebagai NIDS (*Network Intrussion Detection System)*



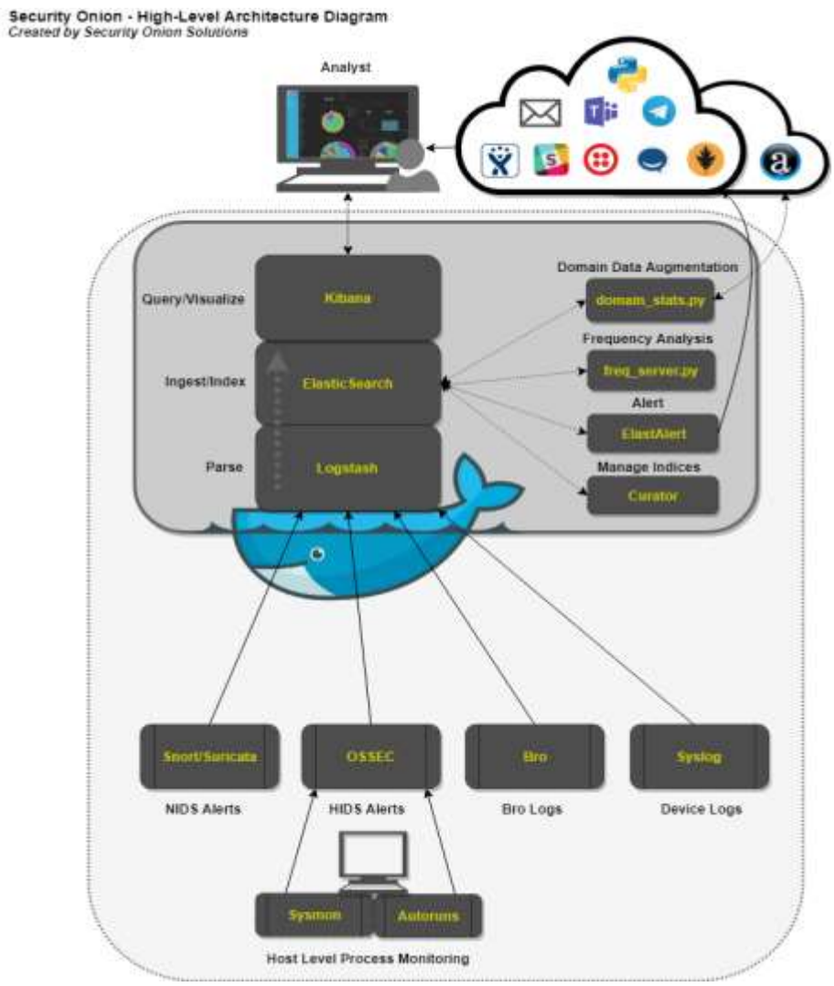
Pada topologi di atas tergambar bahwa *port Dummy* dikonfigurasi secara *mirror* atau *span port* sehingga *traffic* dari dan menuju *port Dummy* akan dikirim juga ke NSM *Engine*.

MENGENAL SECURITY ONION

Security Onion adalah distribusi Linux gratis dan bersifat *open source* khusus untuk memonitor keamanan dan manajemen *log* jaringan berkelas *enterprise*. Security Onion dilengkapi dengan banyak *software* yang sangat berguna seperti *Elasticsearch, Logstash, Kibana, Snort, Suricata, Bro, Wazuh, Sguil, Squert, CyberChef, NetworkMiner,* dan alat keamanan lainnya. Sifatnya yang gratis dan mudah dalam *setup*-nya membuat *Security Onion* banyak digunakan oleh perusahaan-perusahaan bahkan instansi pemerintahan. Bagi anda yang ingin mencobanya, bisa mengunduh di https://github.com/Security-Onion-Solutions/security-onion/blob/master/Verify_ISO.md.

CARA KERJA SECURITY ONION

Berikut adalah diagram yang menggambarkan bagaimana *Security Onion* bekerja. Untuk *flowchart* lebih detail dan penjelasan mengenai *Deployment Types* silahkan kunjungi https://securityonion.readthedocs.io/en/latest/architecture.html



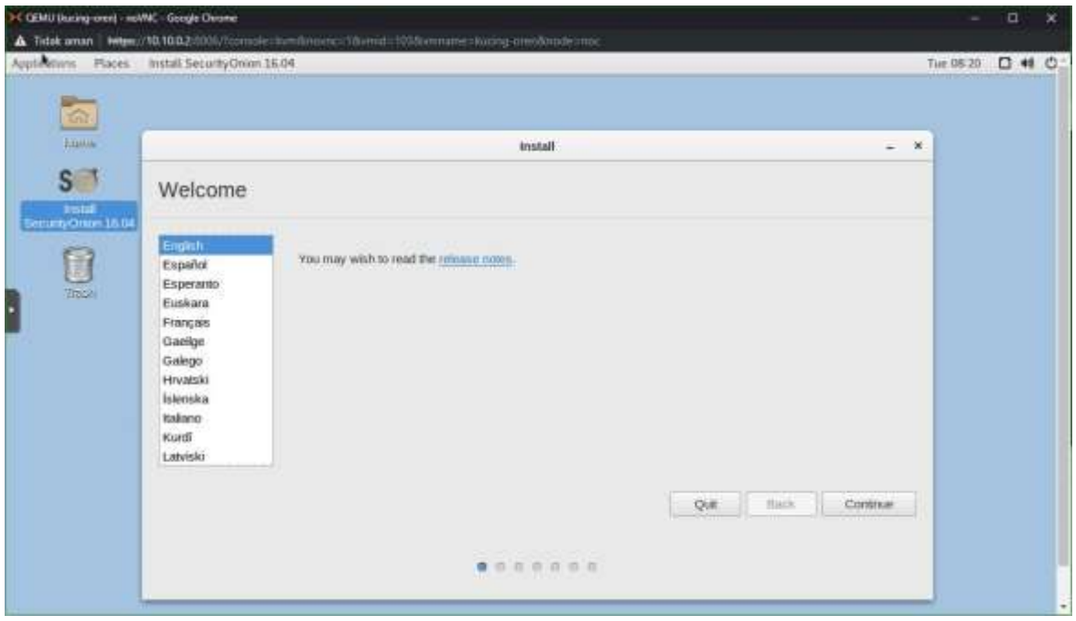
HARDWARE REQUIREMENTS (STANDALONE TYPE)

Berikut adalah tabel rekomendasi *hardware* untuk *Deployement Security Onion* dengan model *Standalone* (Master Server sekaligus *Storage*).

HARDWARE	REQUIREMENT
Processor	4-8 Cores
RAM	8-16 GB
Harddisk	100 GB – 1 TB
Ethernet	2 NIC (Untuk netsniff dan manajemen)

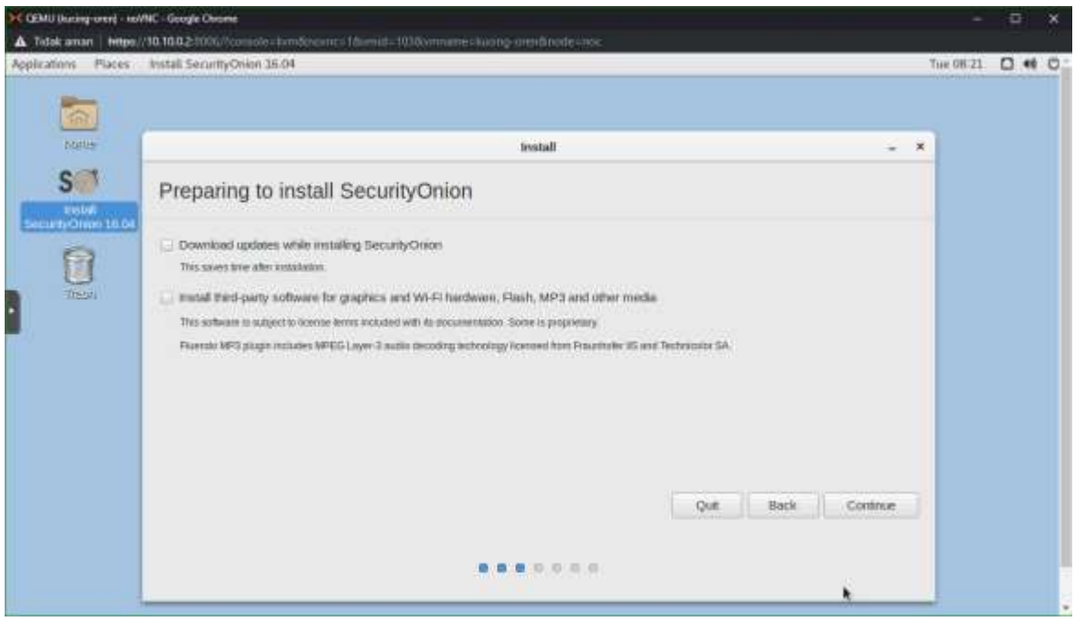
Tabel di atas berisi kebutuhan *hardware* jika *Security Onion* digunakan untuk memonitoring jaringan yang tidak terlalu padat. Jika jaringan padat seperti pada ISP atau *Data Center*, maka *hardware* yang dibutuhkan mungkin akan lebih tinggi. Untuk kelas ISP dengan model *standalone deployment* dibutuhkan *processor* setidaknya 16 core dan RAM 24 GB. Dilengkapi dengan penyimpanan sebesar 1 TB dan *gigabit ethernet.*

INSTALASI

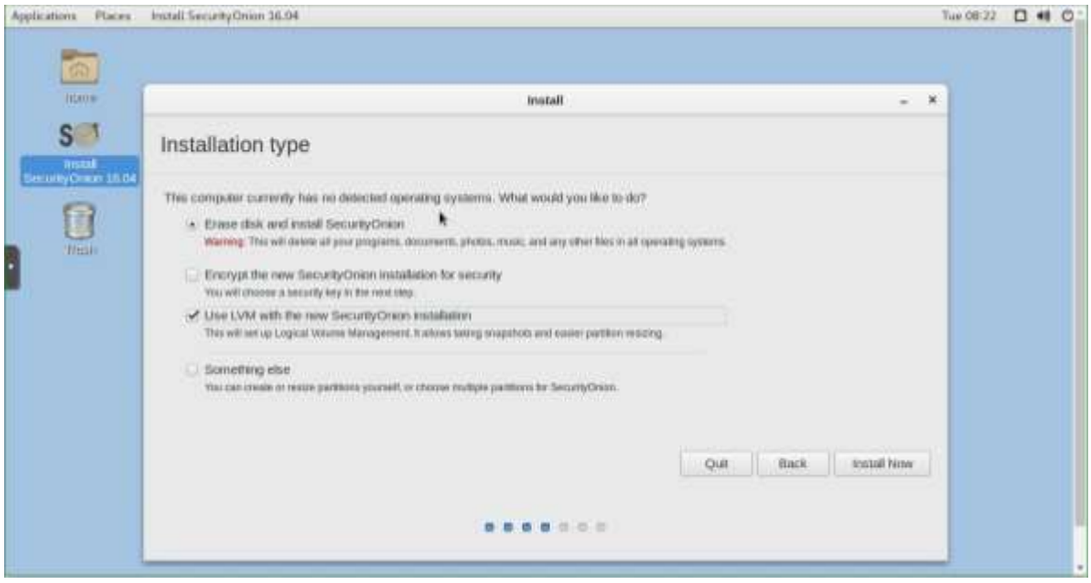


Masukkan installer Security Onion yang sudah diburning ke media installasi. Bisa dengan DVD atau Flashdisk. Atau jika anda melakukan installasi pada sebuah mesin virtualisasi seperti Proxmox atau VMWare, anda hanya butuh ISOnya saja.

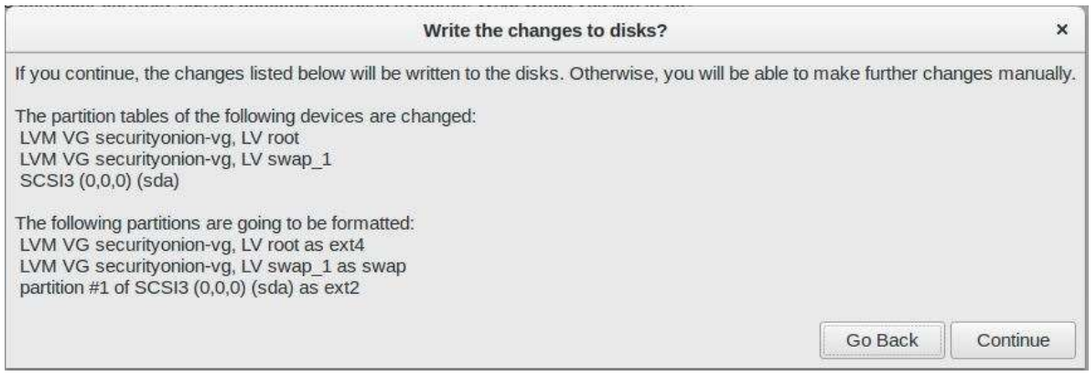
Lakukan booting via media installasi dan tunggu hingga masuk ke mode live. Akan muncul icon Install SecurityOnion 16.xx. Double click icon tersebut maka akan muncul menu pilihan bahasa yang akan digunakan saat installasi. Pilih bahasa lalu klik continue.



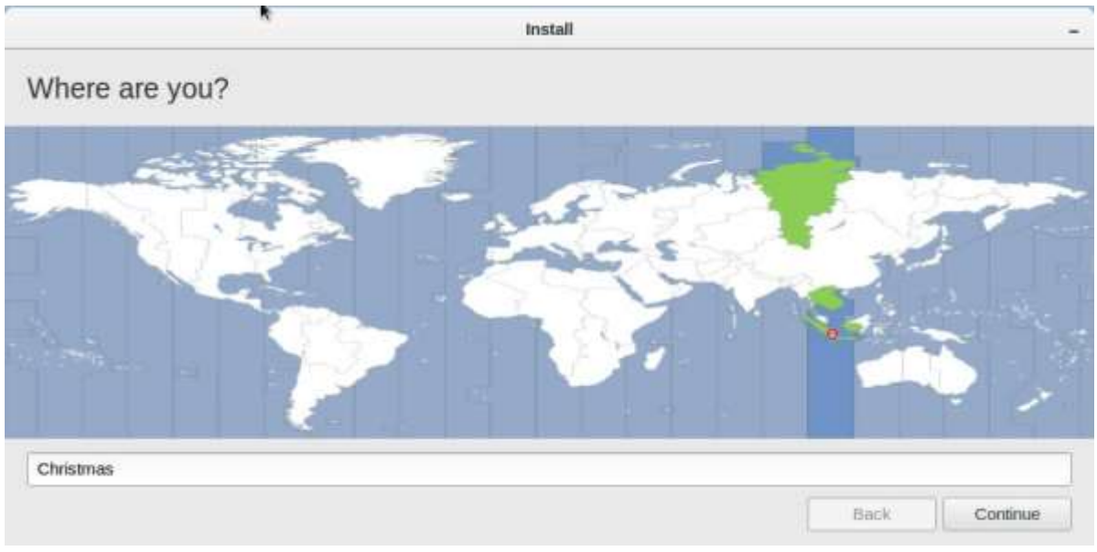
Step selanjutnya, anda akan menentukan apakah anda menghendaki update dan installasi software pihak ketiga saat installasi. Jika anda men-*check list* kedua opsi tersebut, maka anda memerlukan koneksi internet saat installasi. Jika tidak ada koneksi internet, anda bisa *uncheck* atau melewati pilihan tersebut dengan klik continue.



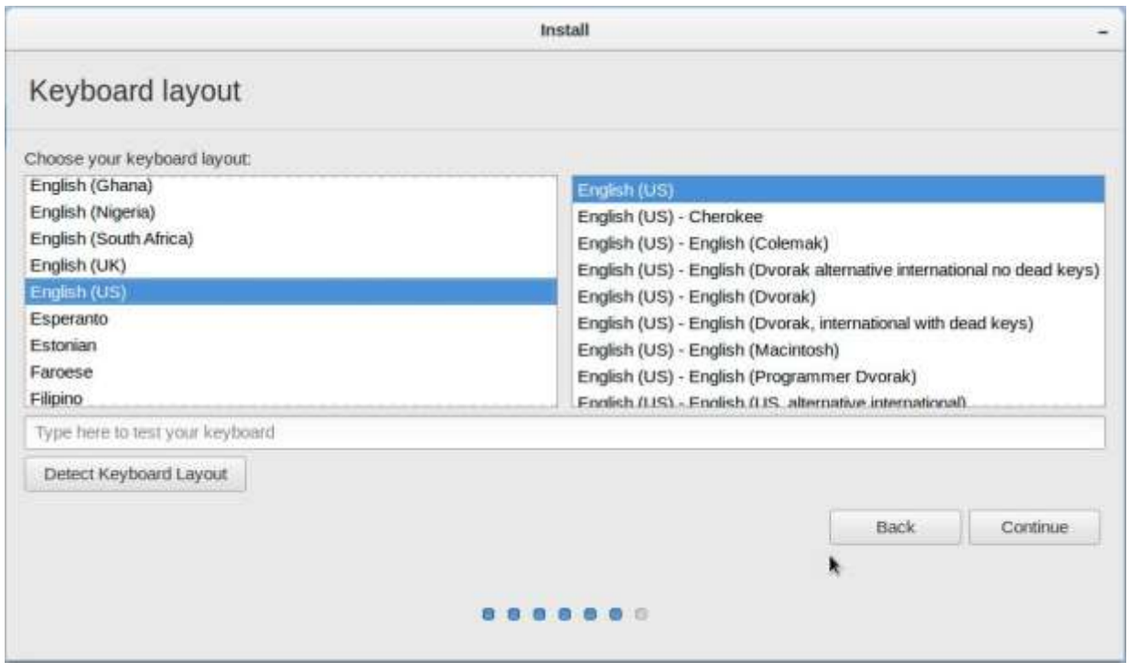
Akan muncul pilihan tipe instalasi. Jika anda memilih pilihan “Use LVM with new SecurityOnion Installation”, maka SecurityOnion akan menentukan sendiri ukuran root, home, swap, atau partisi lainnya secara otomatis. Namun, anda juga bisa memilih “Something Else” dengan mengkonfigurasi ukuran ruang penyimpanan secara manual, seperti menentukan besar space root, home, atau pun swap. Disarankan memilih “Something Else” agar bisa menyesuaikan dengan kebutuhan anda. Minimal, anda hanya perlu mengkonfigurasi berapa space root dan swap yang anda ingingkan. Sebagai asumsi, jika ukuran RAM anda lebih kecil dari 64 GB, anda bisa mengkonfigurasi space swap dua kali ukuran RAM. Jikaa ukuran RAM lebih besar dari 64, anda bisa mengkonfigurasi setengah atau seperempat dari besar RAM yang anda miliki. Sisanya alokasikan ke partisi root (/) .



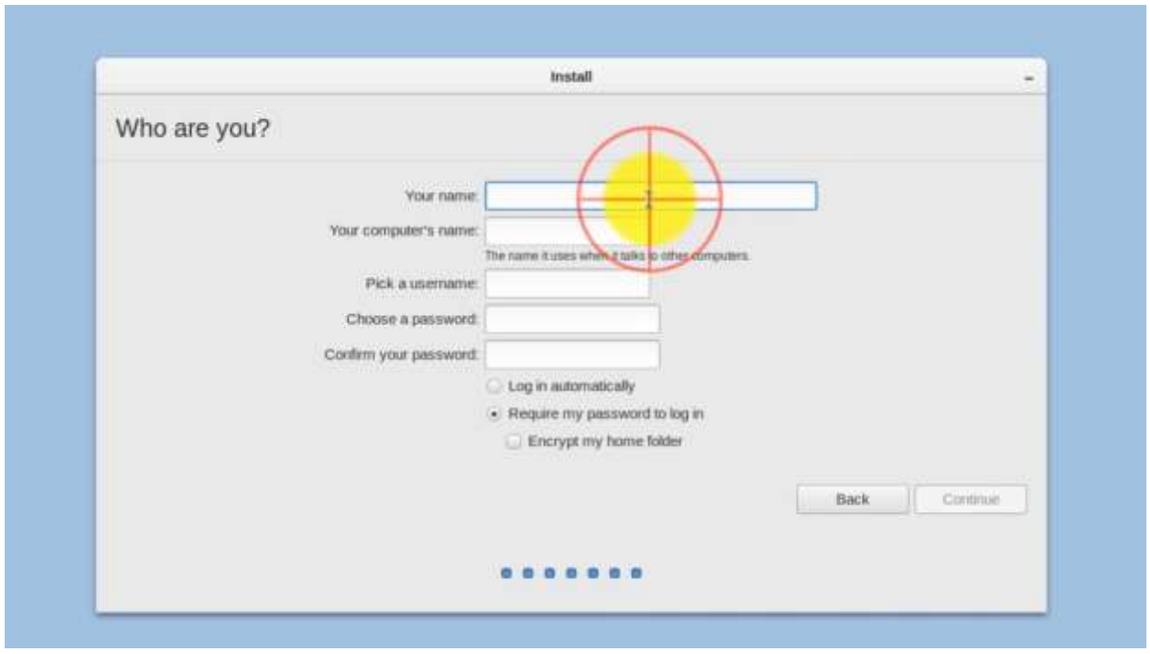
Jika konfigurasi partisi telah selesai dilakukan, maka akan muncul dialog konfirmasi. Klik continue jika anda yakin dengan konfigurasi yang telah anda lakukan.



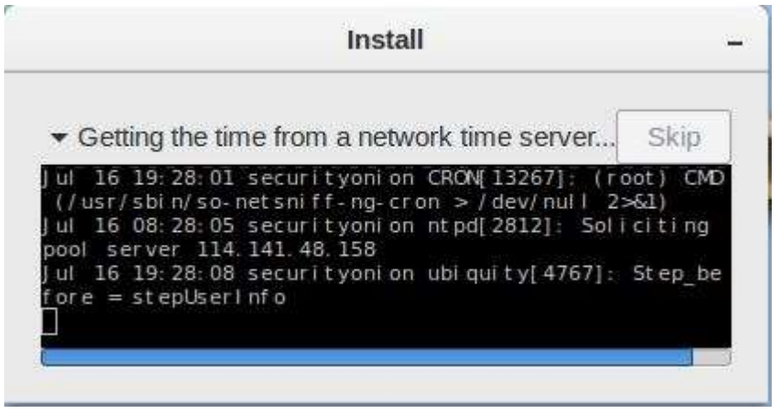
Pilih lokasi untuk menentukan zona waktu anda.



Silahkan pilih keyboard layout anda.



Tentukan username, computer’s name, dan password SecurityOnion anda.



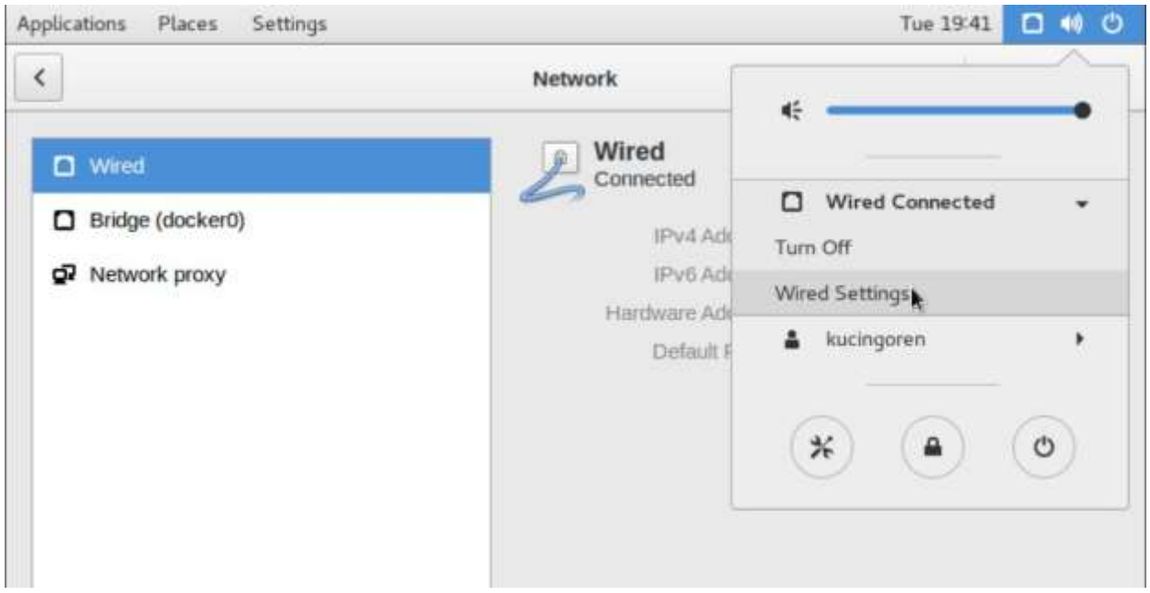
Setelah itu akan muncul jendela proses instalasi. Silahkan menunggu.

Jika proses instalasi telah selesai, anda bisa memilih untuk melanjutkan testing secara live atau melakukan restart.

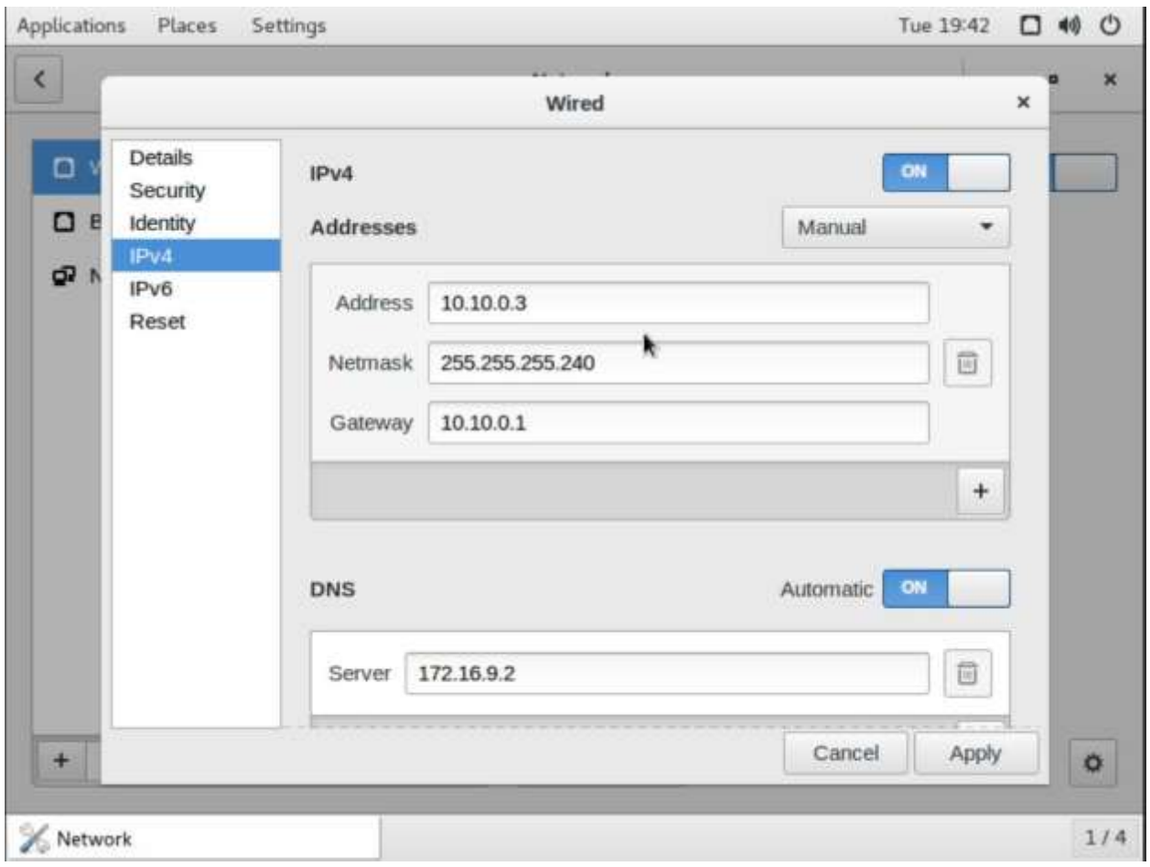
Proses instalasi selesai. Silahkan login dengan username dan password yang telah anda tentukan pada saat proses instalasi.

KONFIGURASI SECURITY ONION

A. KONFIGURASI IP ADDRESS



Klik icon LAN pada pojok kanan atas layar, lalu pilih wired settings.



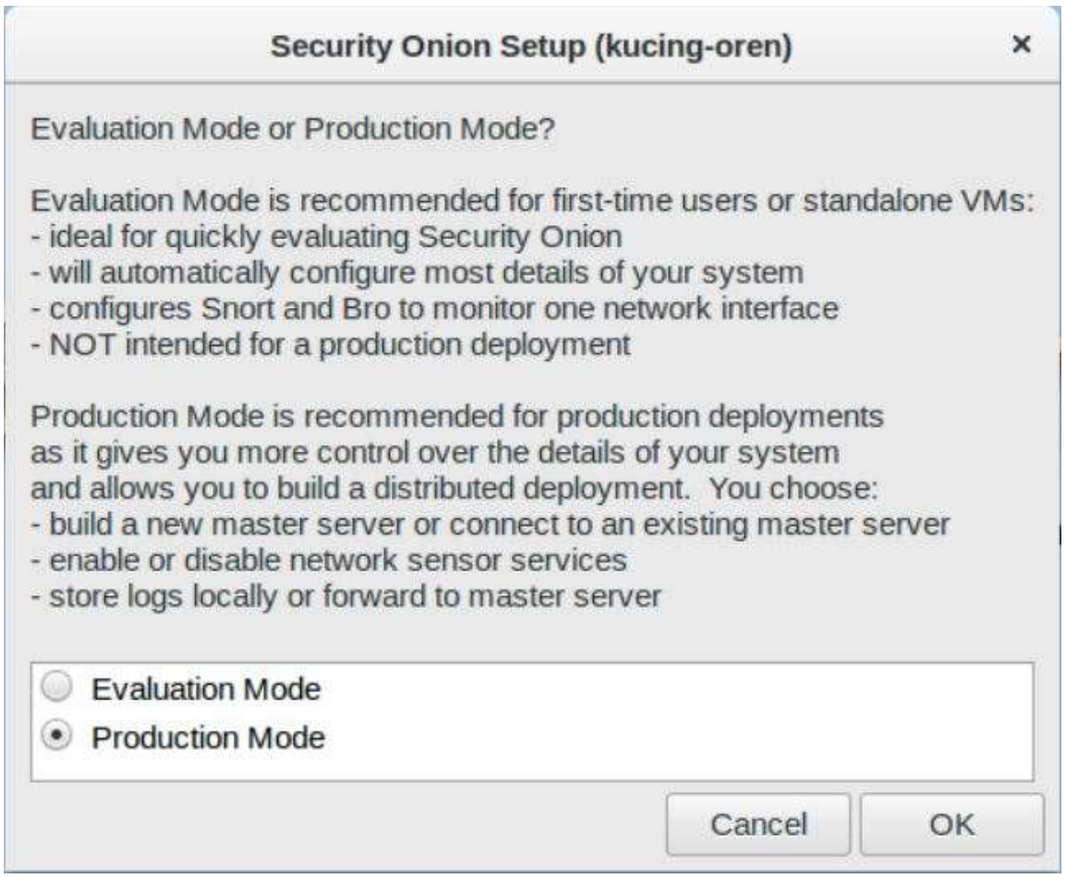
Pilih Ipv4 lalu isikan IP Address, netmask, gateway, dan DNS sesuai kebutuhan anda.

B. KONFIGURASI NMS

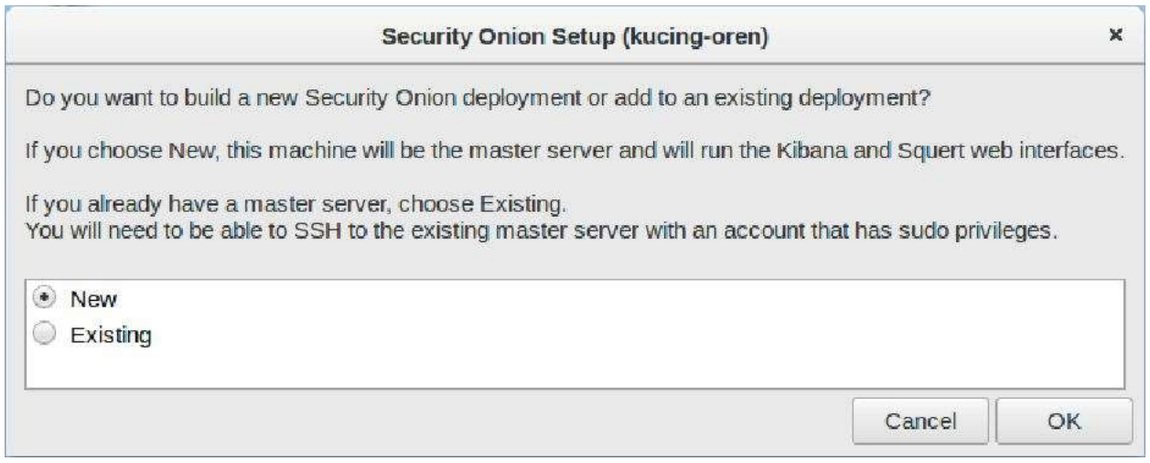
Double klik icon “Setup” pada desktop. Muncul prompt isian password. Masukkan password security onion anda.

Selanjutnya akan muncul dialog konfirmasi service apa saja yang akan diinstall. Klik Yes, Continue!

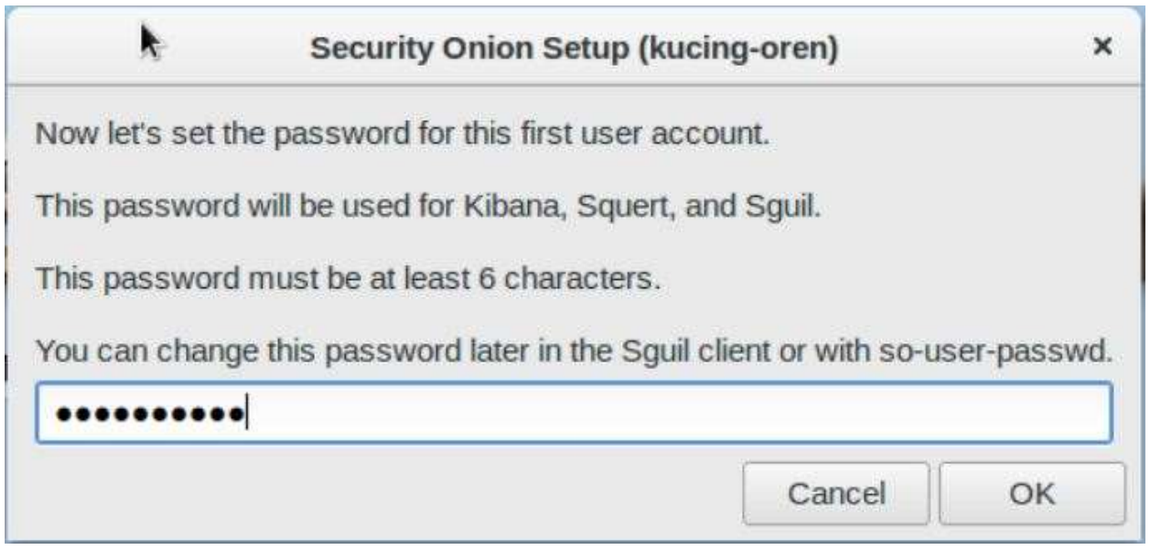
Selanjutnya akan muncul kotak dalog apakah anda ingin mengkonfigurasi interface jaringan sekarang atau tidak. Kita akan melakukannya pada tahap hardening. Pilih No, not right now.



Selanjutnya anda akan menentukan mode installasi. Ada dua mode installasi yakni Evaluation Mode dan Production Mode. Jika anda melakukan installasi hanya untuk mencoba, sialhkan pilih Evaluation Mode. Namun, jika anda menginginkan sistem dan akses secara penuh, silahkan pilih Production Mode.

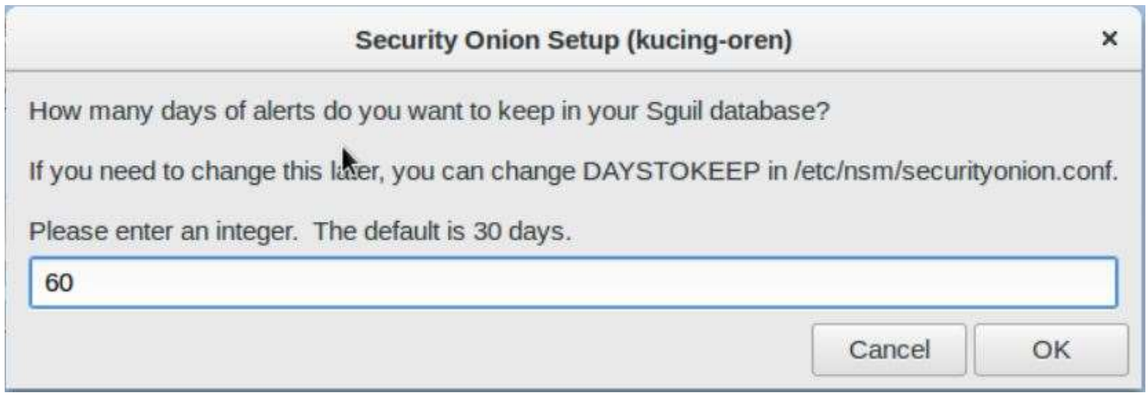


Setelah itu anda harus menentukan apakah Security Onion akan difungsikan sebagai Master Server atau hanya sebagai sensor yang akan mengirimkan data ke master server. Jika anda menginginkn security onion sebagai master server atau anda belum memiliki master server, pilih New. Jika tidak pilih Existing.

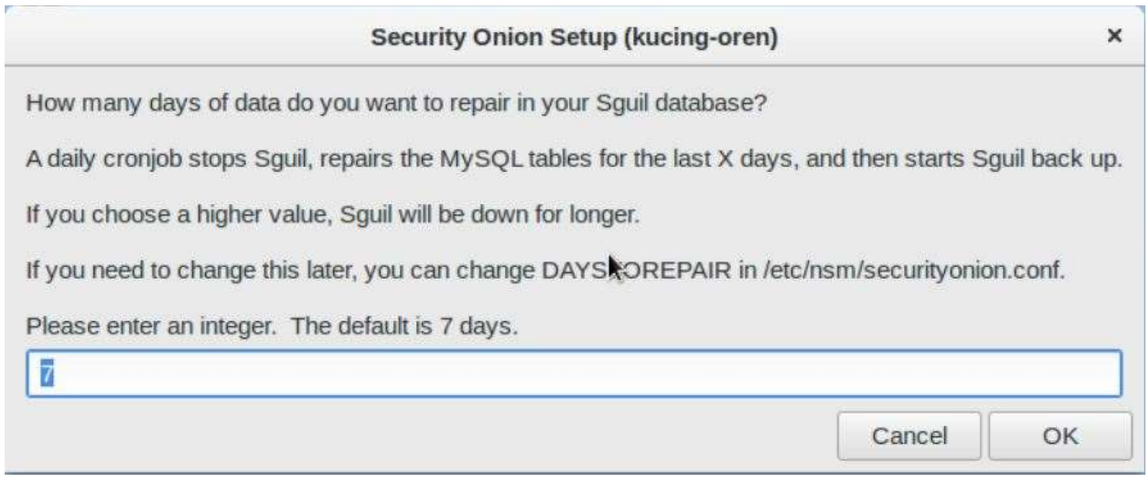


Tentukan username dan password untuk login ke dashboard monitoring security onion.

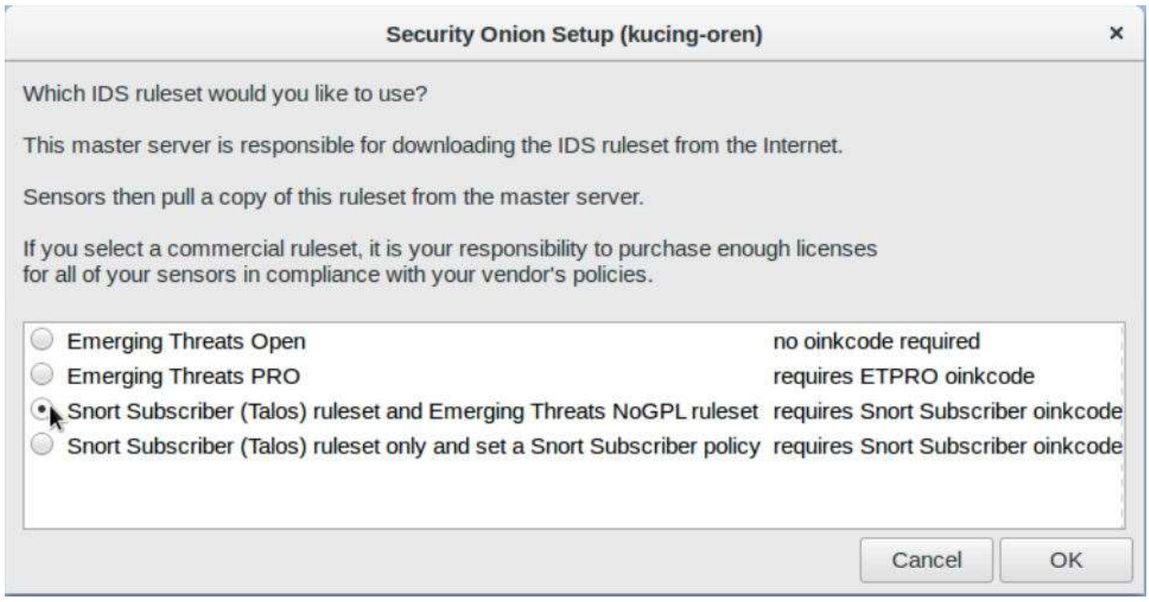
Selanjutnya anda akan memilih ingin melakukan instalasi dengan Best Practices atau Custom. Jika anda memilih Best Practices, sistem akan menentukan konfigurasinya sendiri secara otomatis. Jika custom, anda bisa menentukan sendiri konfigurasi terbaik sesuai dengan kebutuhan pada network yang akan anda monitoring. Rekomendasi pilih Custom.



Tentukan berapa hari anda ingin menyimpan log/alert pada database sguild. Kebutuhan anda mungkin lebih lama atau kurang dari contoh di atas.



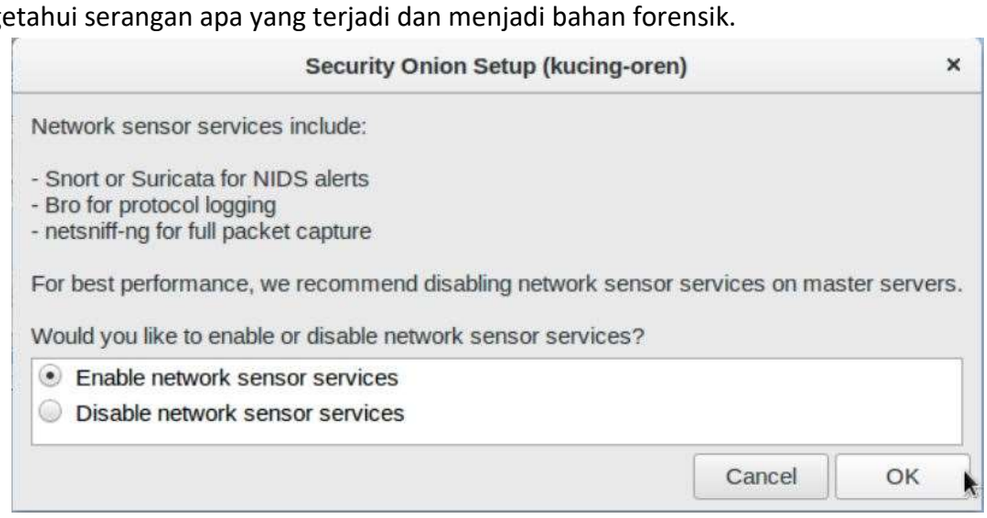
Selanjutnya anda tentukan setiap berapa hari Sguild Database akan merepair datanya. Security Onion akan membuat cronjob yang akan berjalan sesuai hari yang anda tentukan. Default adalah 7. Jangan menentukan jangka waktu repair terlalu lama karena bisa menyebabkan Service Sguil Database down terlalu lama sehingga log tidak tersimpan atau Security Onion tidak bisa memonitoring jaringan anda.



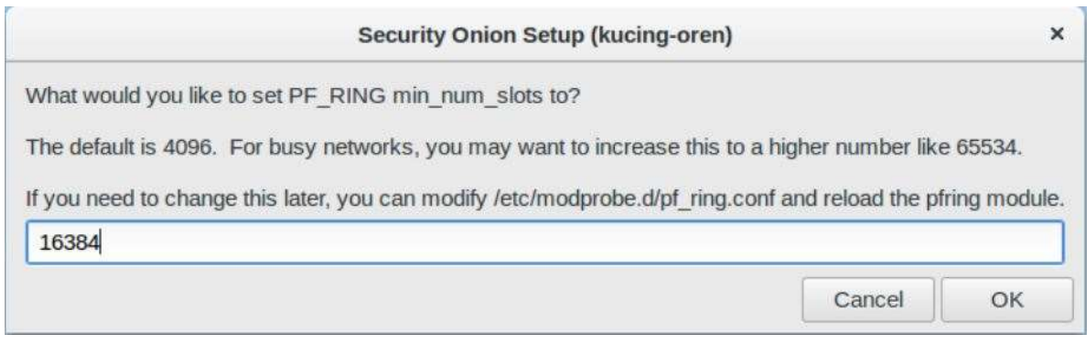
Pilih IDS ruleset sesuai keinginan anda. Jika anda menggunakan IDS Suricata, anda bisa memilih Emerging Threaats Open atau PRO. Namun jika anda memilih Snort sebagai IDS, anda bisa memilih pilihan ketiga dan keempat. Rekomendasi pilih pilihan ketiga namun anda harus mendaftar atau membuat akun di website resmi Snort (https://www.snort.org) untuk mendaapatkan *Oinkcode.*

Kunjungi website snort dan login. Saalin Oinkcode anda lalu tempel di sini setelah anda mengklik Ok pada step sebelumnya.

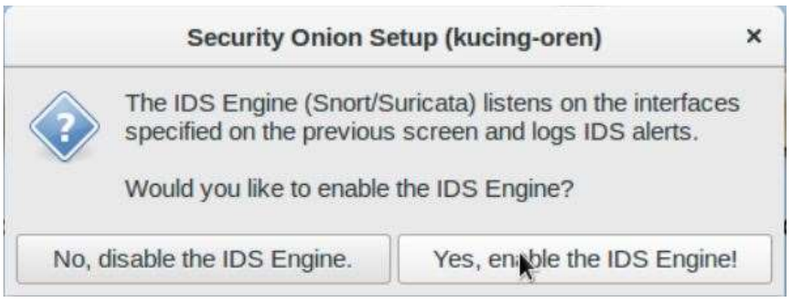
Pilih IDS Engine yang anda perlukan. Karena pada step sebelumnya IDS Ruleset menggunakan Snort Subscriber (Talos) ruleset, maka pilih Snort. Ruleset inilah yang akan menjadi alert ketika terjadi ancaman pada sistem jaringan anda sehingga anda dapat mengetahui serangan apa yang terjadi dan menjadi bahan forensik.



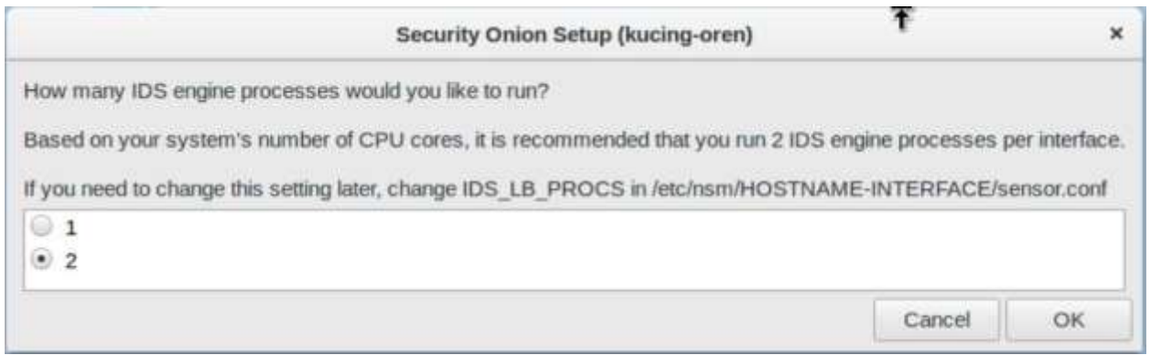
Selanjutnya anda akan menentukan apakah ingin mengaktifkan sensor service atau tidak. Jika Security Onion hanya difungsikan sebagai Master Server, anda bisa menonaktifkan sensor service. Namun jika anda ingin menjadikan Security Onion sebagai Master Server sekaligus Sensor. Jika anda ingin memfungsikan Security Onion sebagai Master sekaligus sensor, maka aktifkan sensor service yang meliputi Snort Engine, Bro, dan netsniff-ng.



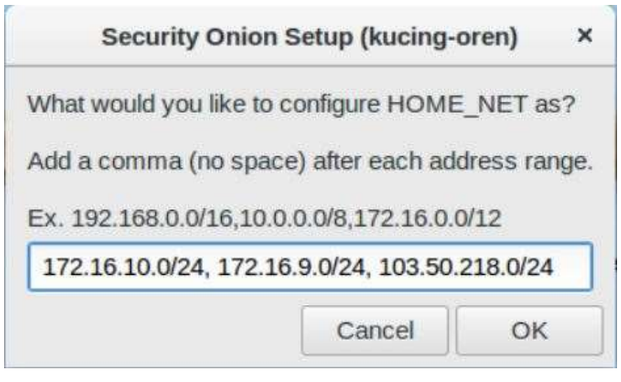
Selanjutnya anda harus menentukan PF_RING min_num_slots. PF-RING bertindak sebagai flow-based Load Balancing yang memungkinkan kami untuk memutar beberapa instance Snort / Suricata / Bro untuk menangani lebih banyak lalu lintas daripada satu instance. Default dari min_num_slots adalah 4096, jika jaringan yang anda ingin monitor adalah jaringan sibuk seperti data center, anda bisa menentukan nilai min_num_slots lebih tinggi agar sensor bekerja dengan maksimal.



Pilih Yes, enable the IDS Engine!

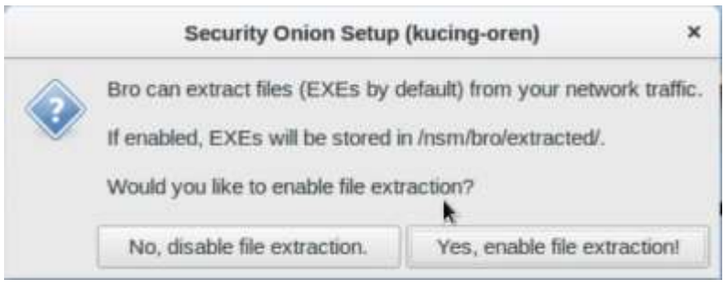


Tentukan berapa Proses IDS Engine yang anda inginkan. Ikuti saja rekomendasi dari sistem atau bisa menyesuaikan dengan kemampuan/jumlah core processor anda.

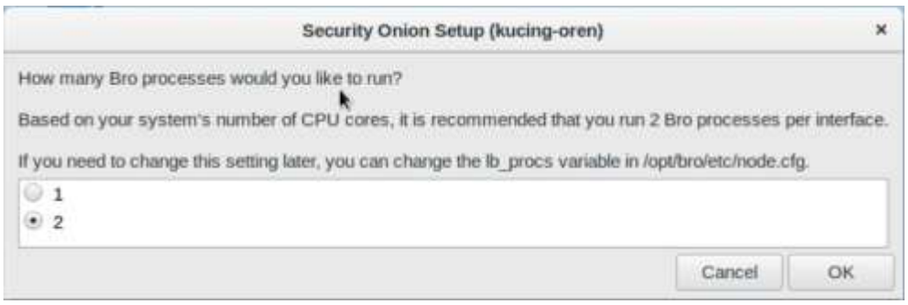


Selanjutnya tentukan blok network mana saja yang akan anda monitoring. Separasi dengan koma.

Apakah anda ingin mengaktifkan Bro sensor atau tidak untuk saat ini. Pilih saja Yes, enable Bro!

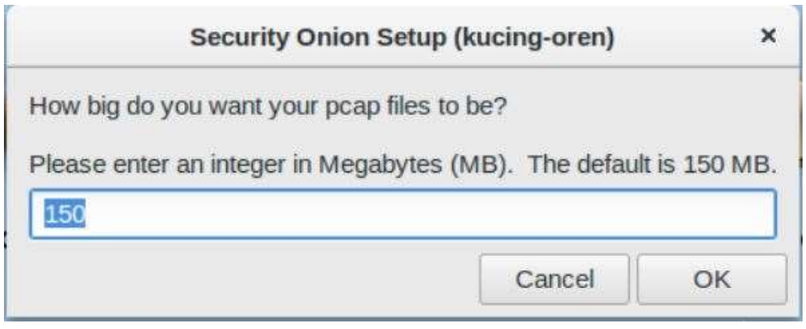


Pilih Yes, enable file extraction!

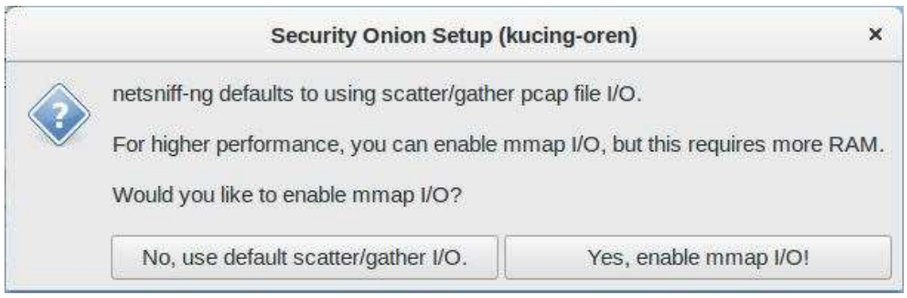


Tentukan berapa Bro proses per interface yang akan anda jalankan. Sistem akan menentukan otomatis sesuai dengan kemampuan/jumlah core processor anda.

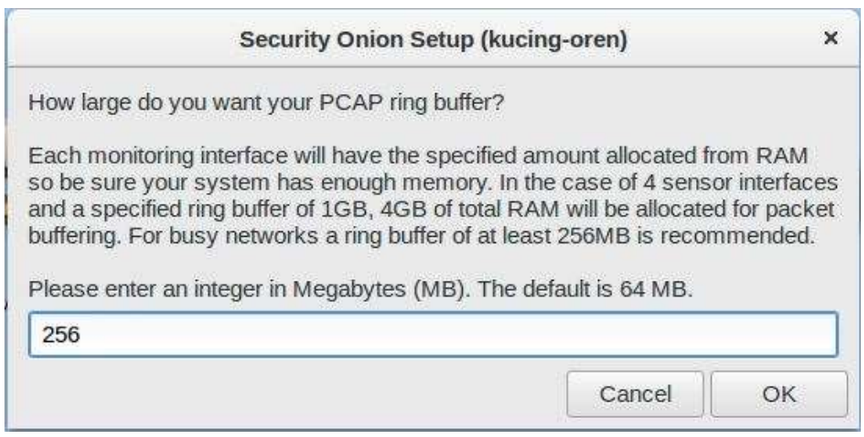
Tentukan apakah anda ingin mengaktifkan mode full packet capture atau tidak. Jika anda menonaktifkan fitur ini, anda akan kurang leluasa dalam melakukan forensik karena pakcet capture yang ada tidak lengkap. Jika anda mengaktifkan fitur ini, anda akan leluasa dalam melakukan forensik namun akan mengkonsumsi ruang penyimpanan lebih besar.



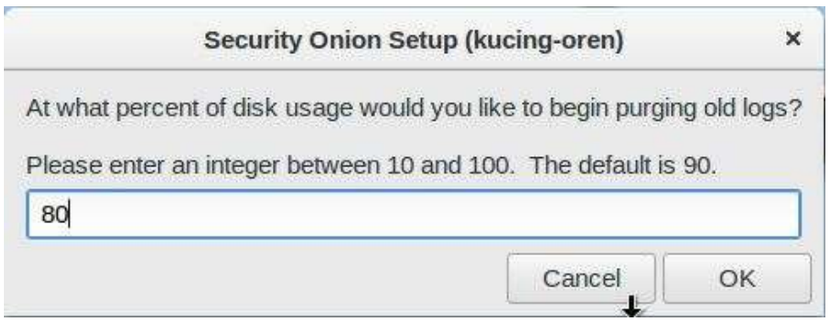
Tentukan besar maksimal pcap (file packet capture) per file yang akan disimpan.



Secara default, netsniff-ng menggunakan scatter/gather pcap file I/O sebagai pcap format. Untuk performa maksimal disarankan mengaktifkan mmap I/O namun memerlukan RAM lebih besar. Jika spesifikasi server anda memili RAM yang cukup besar, silahkan aktifkn mmap I/O sebagai format penyimpanan pcap.

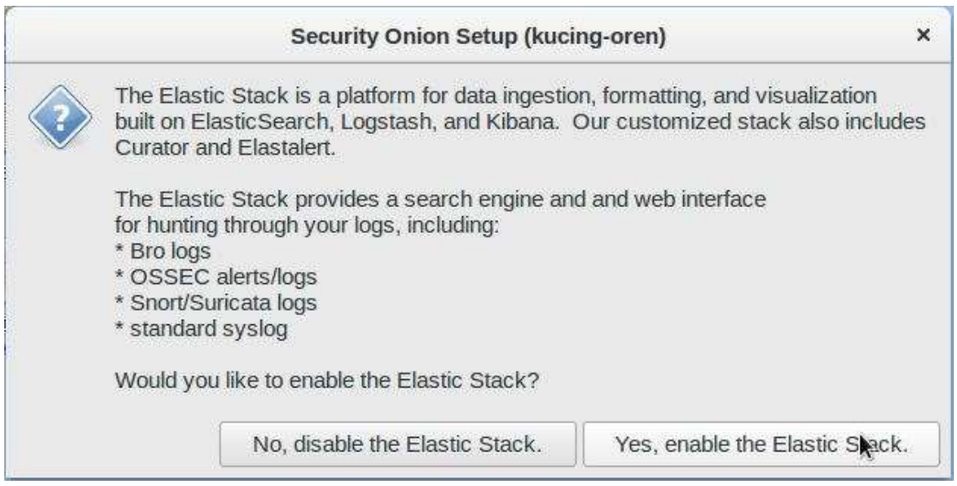


Tentukan besar PCAP Ring Buffer. Pastikan RAM anda cukup dan sesuaikan dengan jumlah sensor yang anda tentukan sebelumnya. Sebagai contoh jika anda memiliki 4 sensor dan PCAP Ring buffer sebesar 1 GB, maka sistem akan mengkonsumsi RAM sebesar 4 GB. Untuk jaringan dengan lalu lintas data yang sibuk, dibutuhkan paling sedikit 256 MB untuk PCAP Ring Buffer. Kebutuhan anda mungkin lebih rendah atau lebih tinggi.

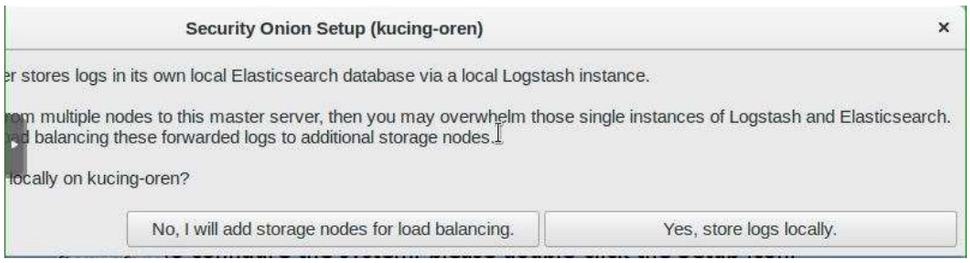


Tentukan sampai berapa persen dari harddisk yang terpakai untuk mulai membersihkan log yang lebih lama.

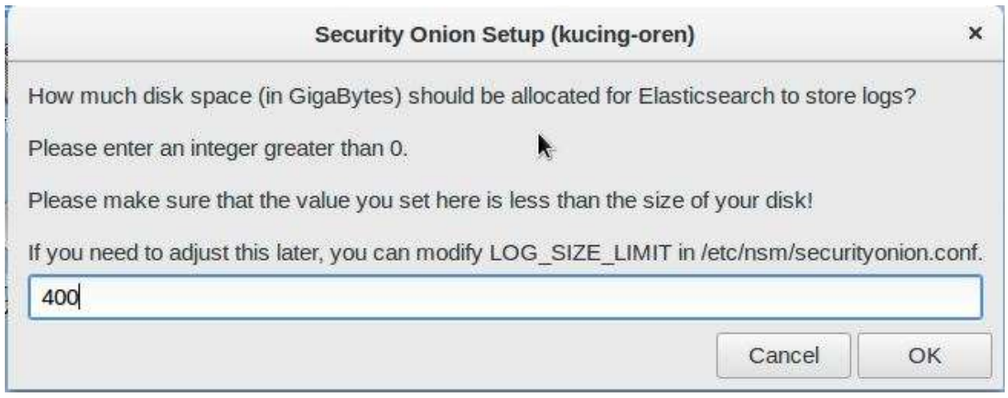
Pilih Yes, enable Salt!



Apakah anda ingin mengaktifkan Elastic Stack atau tidak. Mengaktifkan Elastic Stack memungkinkan anda menampilkan data atau traffic jaringan dalam bentuk visualisasi grafik yang menarik pada dashboard kibana. Rekomendasi pilih Yes, enable the Elastic Stack.



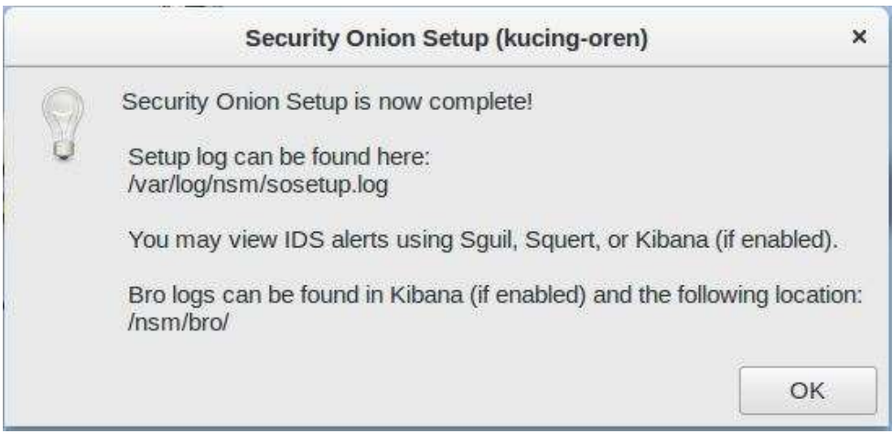
Tentukan di mana anda ingin menyimpan log. Jika anda memiliki storage node sebagai penyimpanan log, anda bisa menambahkannya dengan memilih No, I will add Storage nodes for load balancing. Namun jika anda tidak memiliki storage nodes, anda bisa menyimpan log pada penyimpanan lokal.



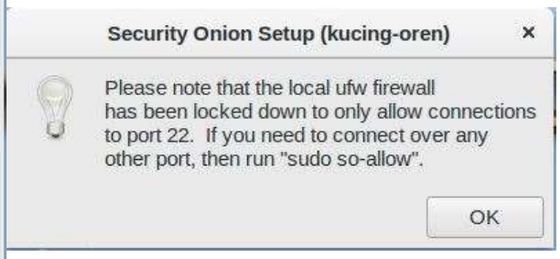
Tentukan alokasi penyimpanan untuk log elasticsearch dalam satuan gigabyte.

Selanjutnya akan muncul ringkasan dari konfigurasi yang telah anda lakukan. Jika anda yakin dengan konfigurasi yang anda lakukan, maka klik Yes, proceed with the changes!

Silahkan tunggu sementara sistem sedang melakukan setup sesuai konfigurasi yang telah anda tentukan.



Jika muncul dialog box seperti di atas, maka proses setup sudah selesai. Selanjutnya akan muncul dialog box berisi tips. Anda bisa melewatinya dengan mengklik OK.

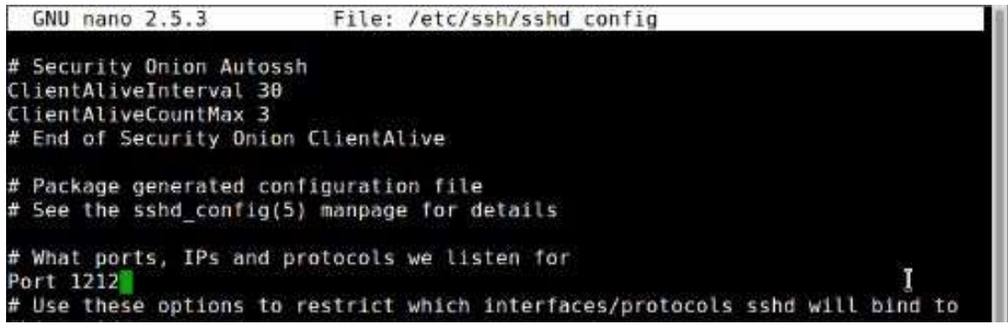


C. KONFIGURASI SSH

```
$ sudo nano /etc/ssh/sshd_config
```

Disarankan mengubah port default ssh demi keamanan. Silahkan ubah port default anda dengan port unused. Contoh : 1212

```
$ sudo systemctl restart sshd
```



Lalu lakukan allow untuk koneksi dengan dst port 1212 melalui firewall

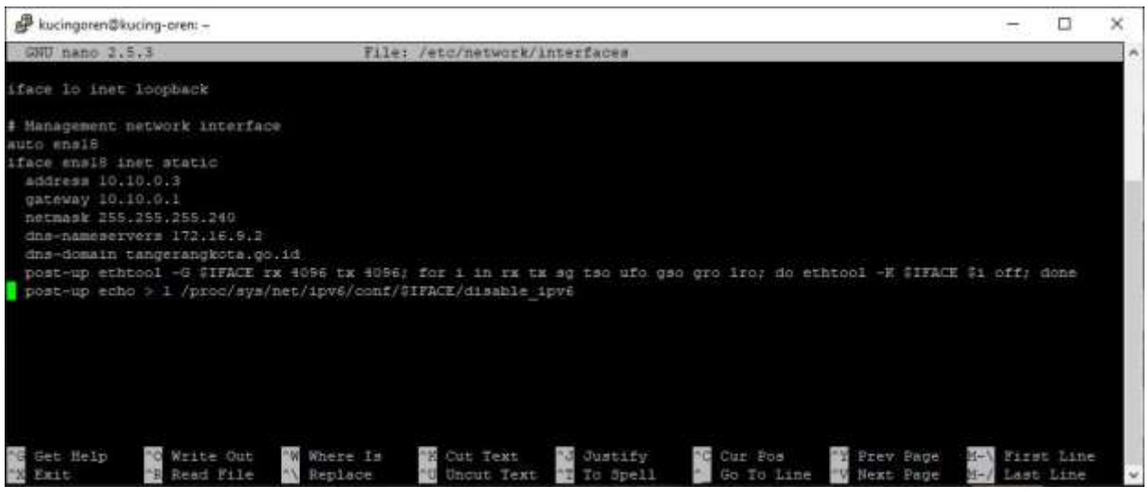
```
$ sudo ufw allow 1212
```

Atau jika anda ingin menentukan IP tertentu saja yang bisa terhubung dengan ssh, bisa jalankan perintah berikut

```
$ sudo ufw allow from xxx.xxx.xxx.xxx to any port 1212
```

D. IP ADDRESS (No NetworkManager)

```
$ sudo systemctl stop NetworkManager

$ sudo systemctl disable NetworkManager

$ sudo nano /etc/network/interfaces
```



Contoh di atas adalah konfigurasi network dengan Port Management sekaligus Sensor. Jika anda memiliki lebih dari satu network interface, anda bisa mengkhususkan misal Port 1 sebagai management dan Port 2 khusus berfungsi sebagai sensor.

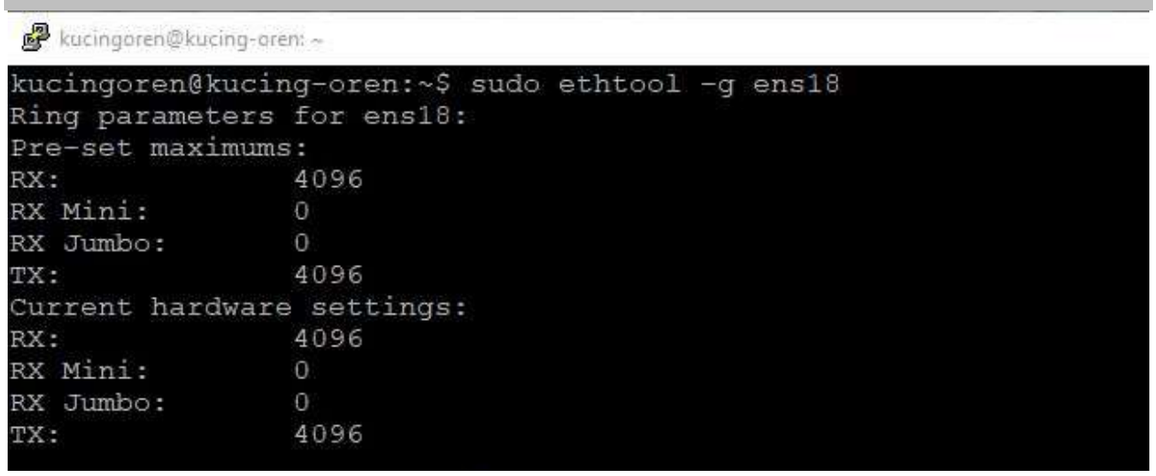
Untuk jaringan yang sibuk, sangat disarankan Security Onion anda memiliki Gigabit ethernet interface agar traffic dapat diterima oleh sensor dengan maksimal. Juga untuk meminimalisir *bottleneck*.

PERHATIKAN BARIS BERIKUT

```
post-up ethtool -G $IFACE rx 4096 tx 4096; for i in rx tx sg tso ufo \
gso gro lro; do ethtool -K $IFACE $i off; done \
post-up echo > 1 /proc/sys/net/ipv6/conf/$IFACE/disable_ipv6
```

Dalam konfigurasi IP Address, anda bisa menambahkan script di atas agar NIC Sensor mendapatkan traffic yang akurat dengan menonaktifkan *offloading function*. Angka 4096 hanya contoh, NIC Anda mungkin memiliki ukuran rx maksimum yang berbeda. Anda bisa mengetahui pengaturan default tx/rx maksimum NIC anda dengan menjalankan perintah:

```
$ sudo ethtool -g interface_name
```




```
$ sudo systemctl restart networking
```

Cek apakah NIC offloading function sudah berhasil dinonaktifkan dengan menjalankan perintah berikut

```
$ sudo ethtool -k interface_name | grep off
```

COMPATIBILITY ISSUE

Setelah menjalankan `sudo soup` Di SecurityOnion 16.04, Anda tidak dapat menggunakan ethtool dan akan mendapatkan kesalahan seperti ini karena modul yang tidak kompatibel

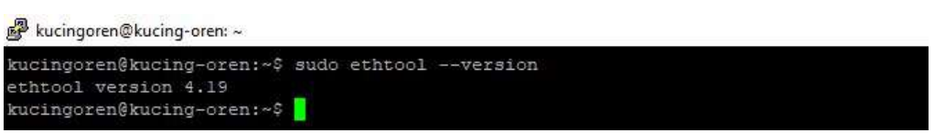
```
$ sudo ethtool -K ens18 gso off

Cannot get device udp-fragmentation-offload settings: Operation not supported
Cannot get device udp-fragmentation-offload settings: Operation not supported
```

Solusinya adalah men-*upgrade* ethtool dari 3.16 ke 4.19

```
$ sudo apt-get install autoconf automake debhelper
$ git clone https://salsa.debian.org/kernel-team/ethtool.git
$ cd ethtool
$ git checkout debian/1%4.19-1
$ dpkg-buildpackage -uc -us -tc -b
$ ls -al ../ethtool_4.19-1_amd64.*
$ cd..
$ sudo dpkg -i ethtool_4.19-1_amd64.deb
```

Setelah selesai, silahkan cek versi ethtool dengan perintah di bawah

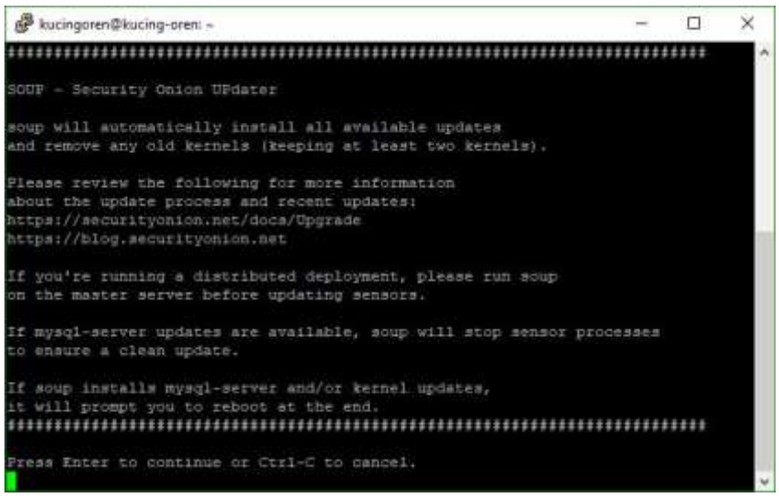
```
$ sudo ethtool --version
```



E. UPGRADE SECURITY ONION

Anda dapat melakukan upgrade sistem security onion anda dengan menjalankan perintah berikut. Perhatian: Sangat tidak disarankan menjalankan perintah `apt-get upgrade` untuk melakukan upgrade sistem.

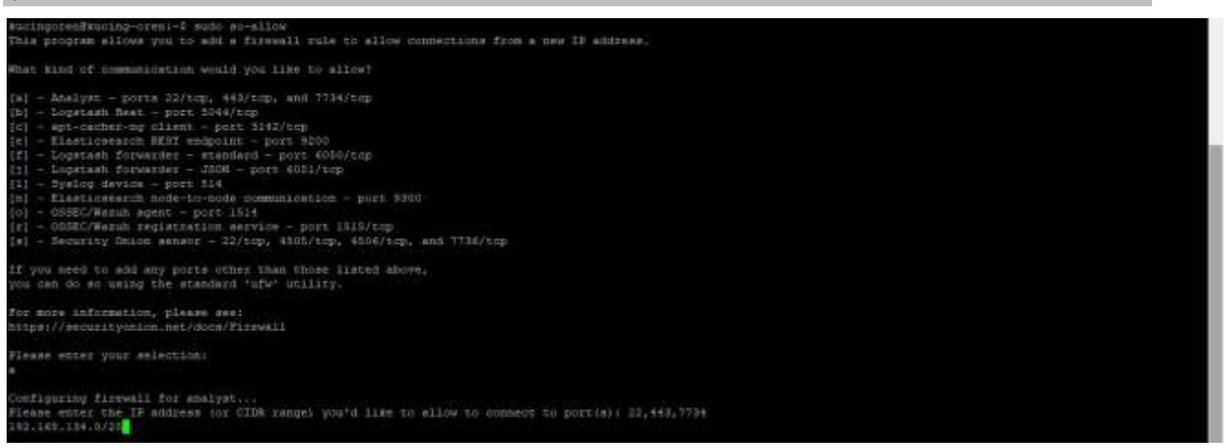
```
$ sudo soup
```



F. ALLOW REMOTE USER

Anda bisa menentukan komputer mana saja yang bisa mengakses dashboard monitoring anda.

```
$ sudo so-allow
```

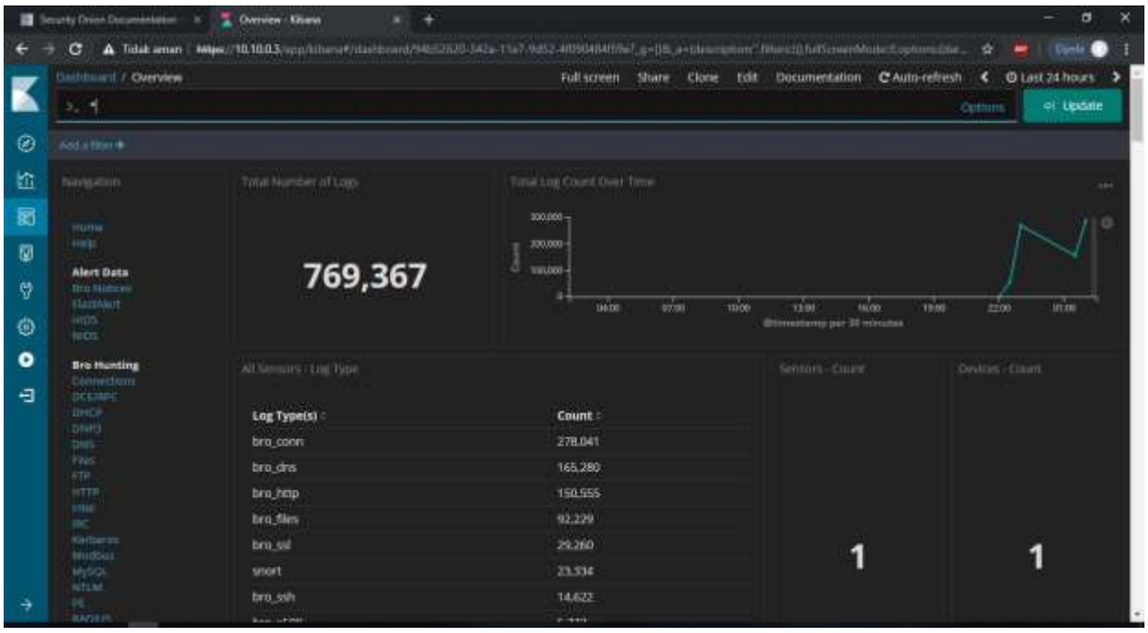


Tekan tombol [a] lalu masukan IP yang ingin anda whitelist. Anda juga bisa memasukkan blok Network sekaligus.

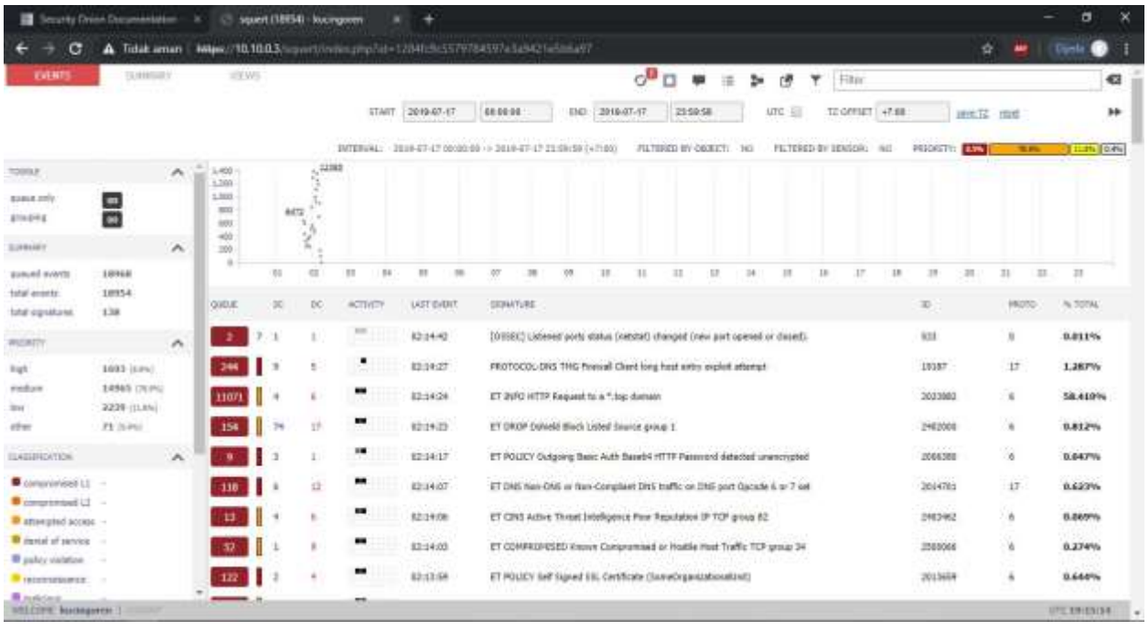
Dengan menjalankan perintah di atas, anda secara tidak langsung menambahkan rule pada ufw firewall security onion. Anda bisa melihat rule firewall anda dengan menjalankan perintah berikut.

```
$ sudo so-allow-view

$ sudo ufw status
```

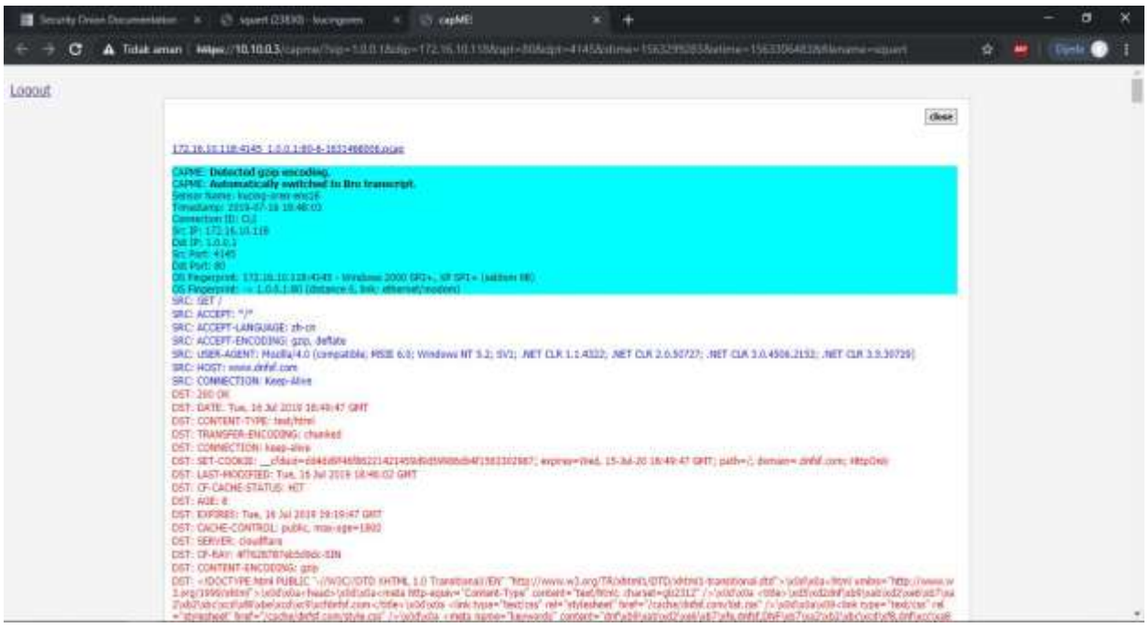
Anda bisa mengakses Kibana Dashboard, Squert, atau Capme di:
https://your-nsm-ip/app/kibana
https://your-nsm-ip/squert



KIBANA DASHBOARD



SQUERT DASHBOARD



CAPME TRAFFIC TRANSCRIPT

G. HIGH PERFORMANCE TUNING

Beberapa service di security onion mengkonsumsi banyak sumber daya memori (RAM). Anda bisa meminimalisir konsumsi RAM dengan menonaktifkan beberapa service yang tidak diperlukan seperti bluetooth atau dekstop mode.

Disable bluetooth service

```
$ sudo systemctl stop bluetooth
$ sudo systemctl disable bluetooth
```

Disable GUI:

```
$ sudo nano /etc/default/grub
```

Cari baris berikut:

```
GRUB_CMDLINE_LINUX_DEFAULT="quiet splash"
```

Ubah menjadi:

```
GRUB_CMDLINE_LINUX_DEFAULT="text"
```

```
$sudo update-grub
```

Untuk security onion 16.x jalankan perintah berikut untuk memberitahu systemd agar tidak me-*load* graphical login manager:

```
$ sudo systemctl enable multi-user.target –force
$ sudo systemctl set-default multi-user.target
$ sudo reboot
```

H. MANAJEMEN RULE

Beberapa rule pada snort terkadang sangat mengganggu dan menimbulkan flood pada database sguild. Beberapa bahkan merupakan alert false positive. Snort memungkinkan anda melakukan suppress terhadap rule yang mengganggu atau mendisable rule tersebut.

```
$ sudo nano /etc/nsm/hostname-iface/threshold.conf
```

Pergi ke baris paling bawah dan berikut contohnya :

```
# POST W/O CONTENT-LENGTH OR CHUNKS

suppress gen_id 119, sig_id 28
```

Suppress rule ke destinasi ip tertentu:

```
#Suppress PostgreSQL TO 10.0.0.9

suppress gen_id 1, sig_id 2010939, track by_dst, ip 10.0.0.9
```

Jika anda ingin mendisable rule tersebut anda bisa menambahkannya pada:

```
$sudo nano /etc/nsm/pulledpork/disablesid.conf

# POST W/O CONTENT-LENGTH OR CHUNKS

119:28
```

```
$ sudo rule-update
```

I. REKONFIGURASI NSM

Security Onion memungkinkan anda untuk mengkonfigurasi ulang nsm anda. Seperti contoh pada modul ini, diasumsikan port ssh yang digunakan pada jaringan anda adalah 1212. Maka anda bisa mengubah konfigurasi IDS engine anda dengan menyesuaikan port ssh yang anda gunakan. Semua konfigurasi snort IDS engine ada pada file berikut.

```
$ sudo nano /etc/nsm/hostname-iface/snort.conf

Line 93 : portvar SSH_PORTS 1212

Line 438 : preprocessor ssh: server_ports { 1212 } \

$ sudo nsm_sensor_ps-restart
```

Selain itu anda juga bisa mengkonfigurasi pengaturan umum dari security onion pada file berikut.

```
$ sudo nano /etc/nsm/securityonion.conf
```

MERUBAH DAYSTOKEEP SGUIL DATABASE:

Cari baris berikut (Contoh: Simpan database selama 60 hari. Setelah 60 hari, database akan dikosongkan):

```
DAYSTOKEEP=60
```

CHANGE SECURITY ONION DATABASE REPAIR SCHEDULE

Cari baris berikut (Contoh: Lakukan Repair terhadap database setiap 7 hari):

```
DAYSTOREPAIR=7
```

KONFIGURASI PENGGUNAAN RUANG PENYIMPANAN

Cari baris berikut (Contoh: Ingatkan jika penggunaan ruang penyimpanan mencapai 70% dari kapasitas):

```
WARN_DISK_USAGE=70
```

Cari baris berikut (Contoh: Hapus data lama jika penggunaan ruang penyimpanan mencapai 80% dari kapasitas total):

```
CRIT_DISK_USAGE=80
```

DISABLE/ENABLE OSSEC HIDS AGENT

Cari baris berikut (Set to yes/no):

```
OSSEC_AGENT_ENABLED=yes
```

ELASTICSEARCH LOG SIZE LIMIT

Cari baris berikut (Contoh: Mengatur batas ukuran log elasticsearch sebesar 450 GB):

```
LOG_SIZE_LIMIT=450
```

CURATOR CLOSE DAYS

Cari baris berikut (Contoh: Tutup elastic indices lebih lama dari 30 hari)

```
CURATOR_ENABLED="yes"

CURATOR_CLOSE_DAYS=30
```

J. REKONFIGURASI SENSOR DAN PCAP

Anda bisa merekonfigurasi pengaturan sensor dan pcap pada file securityonion.conf:

```
$ sudo nano /etc/nsm/securityonion.conf
```

MERUBAH SENSOR INTERFACE

Cari baris berikut:

```
SENSOR_INTERFACE="inface-name"
```

MERUBAH UKURAN FILE PCAP

Cari baris berikut: (Contoh: konfigurasi ukuran pcap dan ukuran pcap ring)

```
PCAP_SIZE=160MiB

PCAP_RING_SIZE=512MiB
```

AKTIFKAN MEMORY-MAPPED IO

Cari baris berikut: (Contoh: Jika anda ingin emngaktifkan pcap memory mapped)

```
PCAP_OPTIONS="--mmap"
```

TRIM/MEMPERKECIL UKURAN PCAP (SNORT LOG) MENGGUNAKAN TRIMPCAP.PY

Install pip, dpkt, and repoze.lru

```
$ sudo apt-get install python-pip

$ pip install dpkt

$ pip install repoze.lru

$ sudo wget -O /opt/trimpcap.py \
https://www.netresec.com/?download=trimpcap
```

MENJALANKAN TRIMPCAP.PY (MEMPERKECIL UKURAN FILE MENJADI 819200 BYTES/FILE)

```
python trimpcap.py <max_bytes_per_flow> <pcap_file(s)>

$ sudo python trimpcap.py 819200 \
/nsm/sensor_data/kucing-oren-ens18/dailylogs/yyyy-mm-dd/*
```

Kemudian kita dapat menjalankan TrimPCAP, sebagai berikut (menentukan ukuran 102KB per aliran, iterasi semua PCAP dari semua periode, di semua direktori):

```
$ sudo /usr/bin/find /nsm/sensor_data/ -name "snort.log.??????????" \
-type f -exec sudo python trimpcap.py 102400 {} \;
```

Jika anda ingin melakukan trim untuk PCAP lebih dari 3 hari, anda bisa menjalankan perintah berikut:

```
$ sudo /usr/bin/find /nsm/sensor_data/ -name "snort.log.??????????" \
-mmin +$((60*72)) -type f -exec sudo python trimpcap.py 102400 {} \
```

- Tindakan ini akan memakan waktu lama tergantung pada jumlah file yang akan dipangkas.

Anda juga bisa mengotomatisasi trimPcap menggunakan cronjob, sehingga PCAP anda diperiksa setiap hari.

```
$ sudo nano /etc/cron.d/trimpcap

#/etc/cron.d/trimpcap

#

#crontab entry for TrimPCAP



TRIMPCAP="/locate_of_trimpcap_py_file/trimpcap.py"

LOG="/var/log/trimpcap.log"

SHELL=/bin/sh

PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin



# Trim after 3 days

0 1 * * * root echo $(date) >> $LOG; /usr/bin/find /nsm/sensor_data/ -
name   "snort.log.??????????"   -mmin   +$((60*72))   -type   f   -exec
/usr/bin/python

$TRIMPCAP 1000000 {} \; >> $LOG 2>&1;
```

Untuk mengkonfigurasi PCAP secara otomatis agar dipangkas pada interval yang direkomendasikan di atas, anda dapat melakukan hal berikut:

```
$ sudo wget \
https://raw.githubusercontent.com/weslambert/misc/master/trimpcap_inst
all && sudo chmod +x ./trimpcap_install && sudo ./trimpcap_install

$ sudo so-restart
```

K. MANAJEMEN DATABASE SECURITY ONION

Anda hanya bisa mengakses database security onion anda dengan menjalankan perintah berikut:

```
$ sudo mysql --defaults-file=/etc/mysql/debian.cnf -Dsecurityonion_db
```

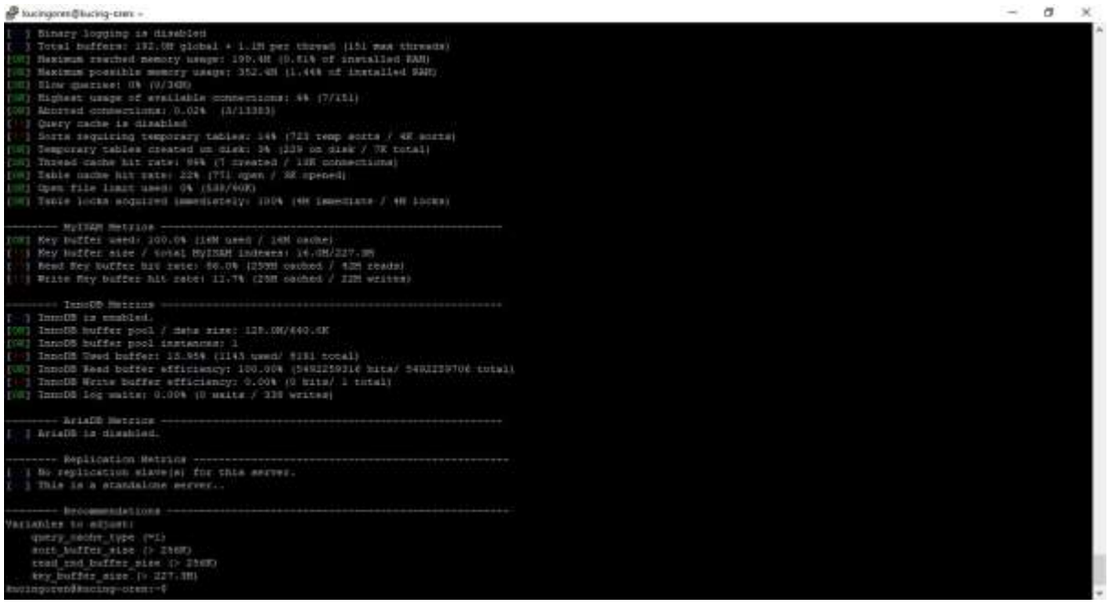
CONTOH : Jika anda ingin melihat 20 EVENT teratas:

```
mysql> SELECT COUNT(*) AS cnt, signature, signature_id FROM event
WHERE status=0 GROUP BY signature ORDER BY cnt DESC LIMIT 20;
```

TUNING MYSQL

```
$ sudo apt update && sudo apt install mysqltuner

$ sudo mysqltuner
```

Implementasikan rekomendasi yang diberikan mysqltuner di `/etc/mysql/my.cnf` atau buat sebuah file baru di `/etc/mysql/conf.d/.` Direkomendasikan membuat file konfirguasi tersendiri di `/etc/mysql/conf.d/` agar konfigurasi anda tidak tertimpa ketika upgrade MySQL Server.



Berikut adalah beberapa variabel umum yang mungkin perlu disetel untuk sistem Anda:

1. open-files-limit
2. table_cache
3. key_buffer
4. max_connections

Setelah mengubah konfigurasi MySQL, Anda harus merestart service MySQL:

```
$ sudo systemctl restart mysql
```

REPAIR MYSQL TABLE

```
$ sudo mysqlcheck -A -u readonly -p
```

```
Password: securityonion
```

OPTIMASI MAX ALLOWED PACKET MySQL DAN AKTIVASI MySQL LOG

```
$ sudo nano /etc/mysql/conf.d/mysql.cnf
```

```
max_allowed_packet = 256M

general_log_file = /var/log/mysql/mysql.log

general_log = 1
```

```
$ sudo systemctl restart mysql
```

L. TROUBLESHOOTING CAPME : ERROR CONNECTION TO SGUILD FAILED

1. **Make sure your system date based on UTC Standard**

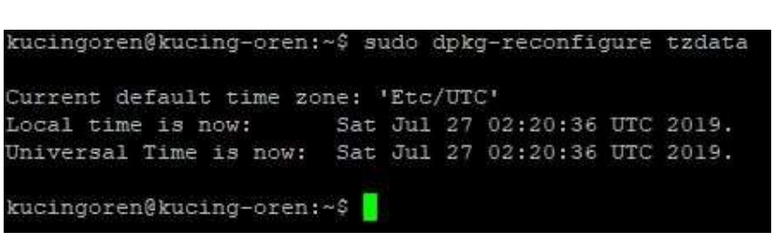
   ```
   $ date
   ```

   Set system date to UTC:

   ```
   $ sudo dpkg-reconfigure tzdata
   ```

   Chose non of the above -> UTC

   ```
   $ sudo nsm_server_ps-restart && sudo nsm_sensor_ps-restart
   ```

2. **Repair or Purging database's tables**

   ```
   $ sudo mysqlcheck -u readonly -p securityonion_db
   ```

   (Password: securityonion) atau

   ```
   $ sudo nsm_server_ps-stop && sudo nsm_sensor_ps-stop

   $ sudo sguild-db-purge

   $ sudo nsm_server_ps-start && sudo nsm_sensor_ps-start
   ```

3. **Modify squert database config file**

```
$ sudo nano /var/www/so/squert/.inc/config.php
```

Ubah baris berikut :

```
$dbHost = "127.0.0.1"; to $dbHost = "localhost";

$ sudo nsm_server_ps-restart
```

4. **Database Corruption Issue : Try to update table event manually and Update Package**

```
$ sudo nsm_server_ps-stop && sudo nsm_sensor_ps-stop

$ sudo mysql --defaults-file=/etc/mysql/debian.cnf
```

```
mysql> UPDATE event SET status=1, last_modified='2019-07-
27 00:00:01', last_uid='sguil' WHERE event.status=0 and
event.signature LIKE '%';
```

Catatan : Atur last_modified menjadi hari itu juga.

```
$ sudo nsm_server_ps-start && sudo nsm_sensor_ps-start

$ sudo soup
```

Reboot Server setelah update

M. TROUBLESHOOTING MDADM

```
$ sudo nano /etc/mdadm/mdadm.conf
```

Tambahkan baris berikut di bagian paling bawah file:

```
ARRAY devices=/dev/sda
```

SECURITY ONION CHEATSET

IMPORTANT FILES

Configuration Files	
Configuration	**File**
General Settings	/etc/nsm/securityonion.conf
Sensor Settings	/etc/nsm/<hostname-interface>/sensor.conf
Maintenance Scripts	/etc/cron.d, /usr/sbin
Snort	/etc/nsm/<hostname-interface>/snort.conf
Suricata	/etc/nsm/<hostname-interface>/suricata.yaml
Bro	/opt/bro
Bro Config	/opt/bro/etc/networks.cfg, node.cfg
Bro Local Policy/Scripts/Intel	/opt/bro/share/bro/site/local.bro (config) /opt/bro/share/bro/policy (scripts) /opt/bro/share/bro/intel/intel.dat (intel)
Elasticsearch Config	/etc/elasticsearch/elasticsearch.yml /etc/elasticsearch/jvm.options (heap size)
Logstash Config	/etc/logstash/logstash.yml /etc/logstash/jvm.options (heap size) /etc/logstash/conf.d (standard pipeline config) /etc/logstash/custom (custom pipeline config and custom templates)
Kibana Config	/etc/kibana/kibana.yml
Curator Config	/etc/curator/config/curator.yml
Syslog-NG	/etc/syslog-ng/syslog-ng.conf
Wazuh	/var/ossec/etc/ossec.conf
Sguil (Server)	/etc/nsm/securityonion/sguild.conf
Sguil (Client)	/etc/sguil/sguil.conf
Sguil (Email)	/etc/nsm/securityonion/sguild.email
Onionsalt	/opt/onionsalt

Log Files	
Scope	**File**
Bro	/nsm/bro/logs/current/stderr.log (errors), reporter.log (errors/warnings), loaded_scripts.log (loaded scripts)
Elastalert	/var/log/elastalert/elastalert_stderr.log
Elasticsearch	/var/log/elasticsearch/<hostname>.log
Logstash	/var/log/logstash/logstash.log
Kibana	/var/log/kibana/kibana.log
OSSEC	/var/ossec/logs/ossec.log
Sensor Logs	/var/log/nsm/<hostname-interface>/snortu-n.log, barnyard2-n.log, suricata.log, netsniff-ng.log
Sguild	/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
PF_RING	min_num_slots in /etc/modprobe.d/pf_ring.conf
Netsniff-NG	PCAP_OPTIONS, PCAP_SIZE, PCAP_RING_SIZE in /etc/nsm/<hostname-interface>/sensor.conf

Security Onion

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
Component-Specific	/etc/nsm/<hostname-interface>/bpf-bro.conf, bpf-ids.conf, etc.

DATA

Data Directories	
Data	**Directory**
Packet Capture (Sensor)	/nsm/sensor_data/<hostname-interface>/dailylogs
Alert Data (Sensor)	/nsm/sensor_data/<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: Security Onion Solutions - https://securityonion.net - @securityonion
Security Onion Version: 16.04.6.1
Last Modified: 05.14.2019

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
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 Minions Up	salt '*' test.ping
Sync Minions	salt '*' state.highstate
Update Entire Deployment	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://securityonion.net/docs/mailinglists
Reddit https://www.reddit.com/r/securityonion/
Docs https://securityonion.readthedocs.io
Blog https://blog.securityonion.net
Training, Professional Services, Hardware Appliances https://securityonionsolutions.com