

IDS-järjestelmän asennus ja konfigurointi

SECURITY ONION 16.04

Johdanto

Tarkoituksena ladata ja asentaa Security Onionin versio 16.04 virtuaalikoneelle. Liitetään toinen virtuaalikoneen verkkokorteista samaan NAT verkkoon Kalin kanssa, jotta IDS-järjestelmän lokeihin saadaan napattua tietoa verkossa tapahtuvasta liikenteestä.

Sisällysluettelo

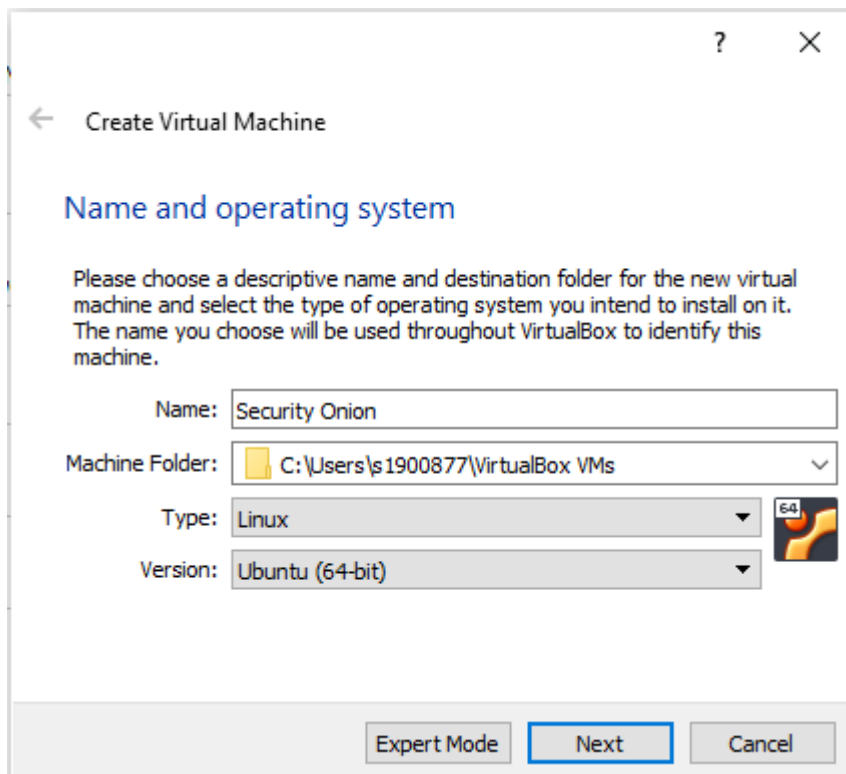
Johdanto	1
Security Onionin lataaminen	2
Uuden virtuaalikoneen luonti.....	2
Verkkokorttien konfigurointi	3
Security Onionin liittäminen virtuaalikoneeseen	3
Security Onionin asennus	3
Setup – sovellus	4
Squid – ohjelma	4

Security Onionin lataaminen

Ladataan Security Onion githubista. (https://github.com/Security-Onion-Solutions/security-onion/releases/tag/v16.04.6.1_20190514).

Uuden virtuaalikoneen luonti

Luodaan uusi virtuaalikone jonka tyyppi on Linux ja versio Ubuntu 64-bit.



?

X

← Create Virtual Machine

Name and operating system

Please choose a descriptive name and destination folder for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name:

Machine Folder:

Type:

Version:

Expert Mode **Next** Cancel

Virtuaalikoneen nimi ja käyttöjärjestelmä

Muistia (RAM) virtuaalikone tarvitsee 8 GB.

Hard disk on tyyppiä VDI, dynamically allocated, kooksi 20 GB.

Verkkokorttien konfigurointi

Verkkokortti 1 = NAT Network.

Verkkokortti 2 = Internal network.

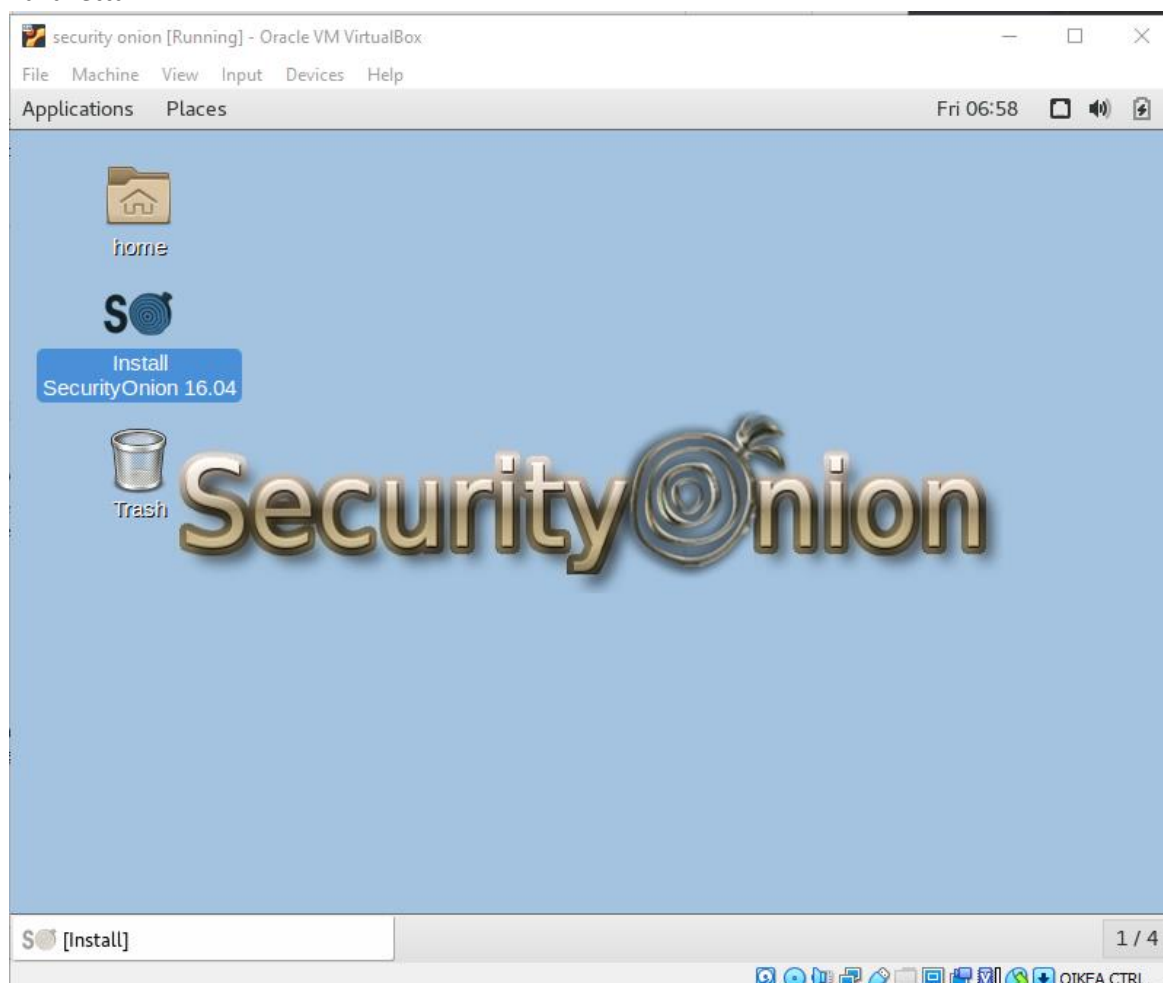
Security Onionin liittäminen virtuaalikoneeseen

Virtuaalikoneen asetuksissa, storage kohdassa "empty" kohtaan valitse ladattu .iso – tiedosto.

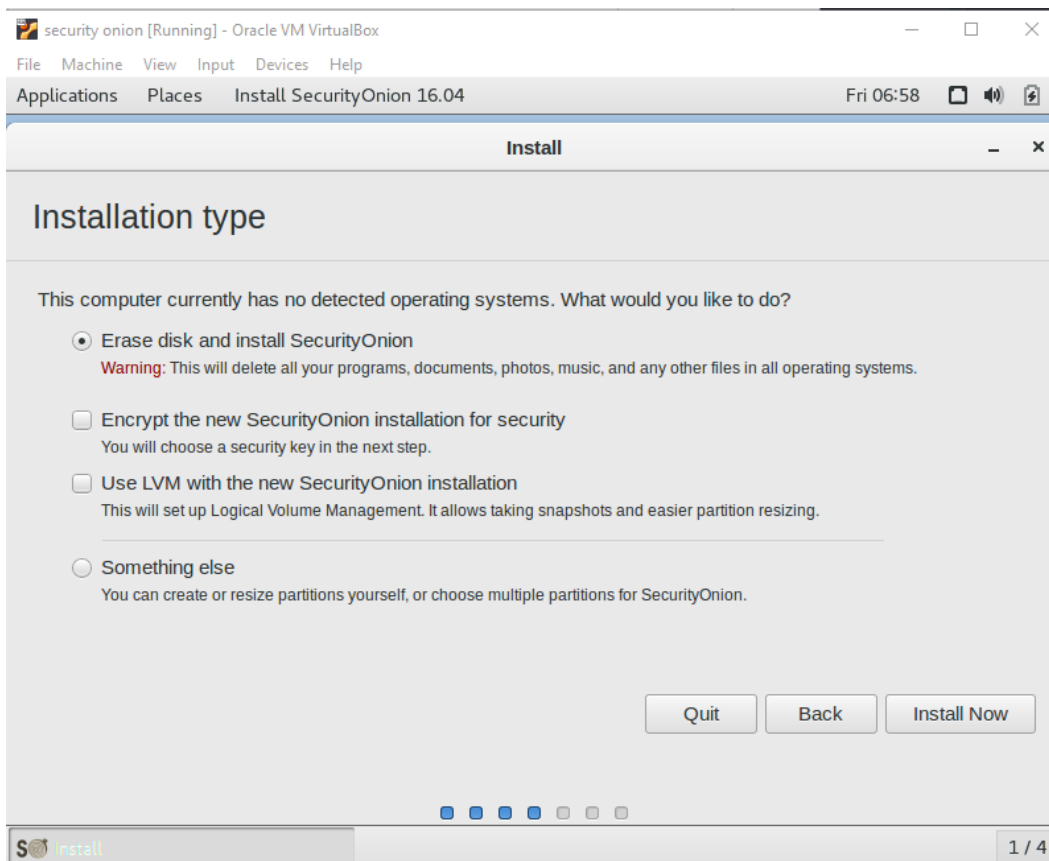
Jos "optical disk – selector" kohdassa ei näy ladattua .iso tiedostoa, täytyy se lisätä painamalla "add" painiketta vasemmassa yläreunassa.

Security Onionin asennus

Kun virtuaalikone on käynnistetty, tuplaklikataan työpöydällä näkyvää "Install SecurityOnion 16.04"-kuvaketta.



Install SecurityOnion 16.04



Asennustyyppi

Asennustyyppi on yllä olevan kuvan mukainen, tyhjennä levy ja asenna SecurityOnion.

Asennuksen yhteydessä kysytään sijaintia, näppäimistön asettelua ja käyttäjän luontia.

Näppäimistön asettelu = QWERTY (suomalainen perusasettelu)

Sijainti = Helsinki

Käyttäjänimi = noa

Salasana = salasana

Tiedot voi täyttää haluamallaan tavalla.

Setup – sovellus

Käynnistetään työpöydältä setup – sovellus, annetaan salasana ja valitaan ylempi verkkokortti vaihtoehdoista. Annetaan sille ip-osoite 192.168.1.1. Subnet mask = 255.255.255.0.

Rebootin jälkeen setup – sovellus ajetaan toisen kerran, skipaten internetin uudelleen konfiguroimisen. Modeksi valitaan evaluation mode ja tulevat ikkunat täytetään haluamallaan käyttäjätunnus + salasana kombolla.

Squid – ohjelma

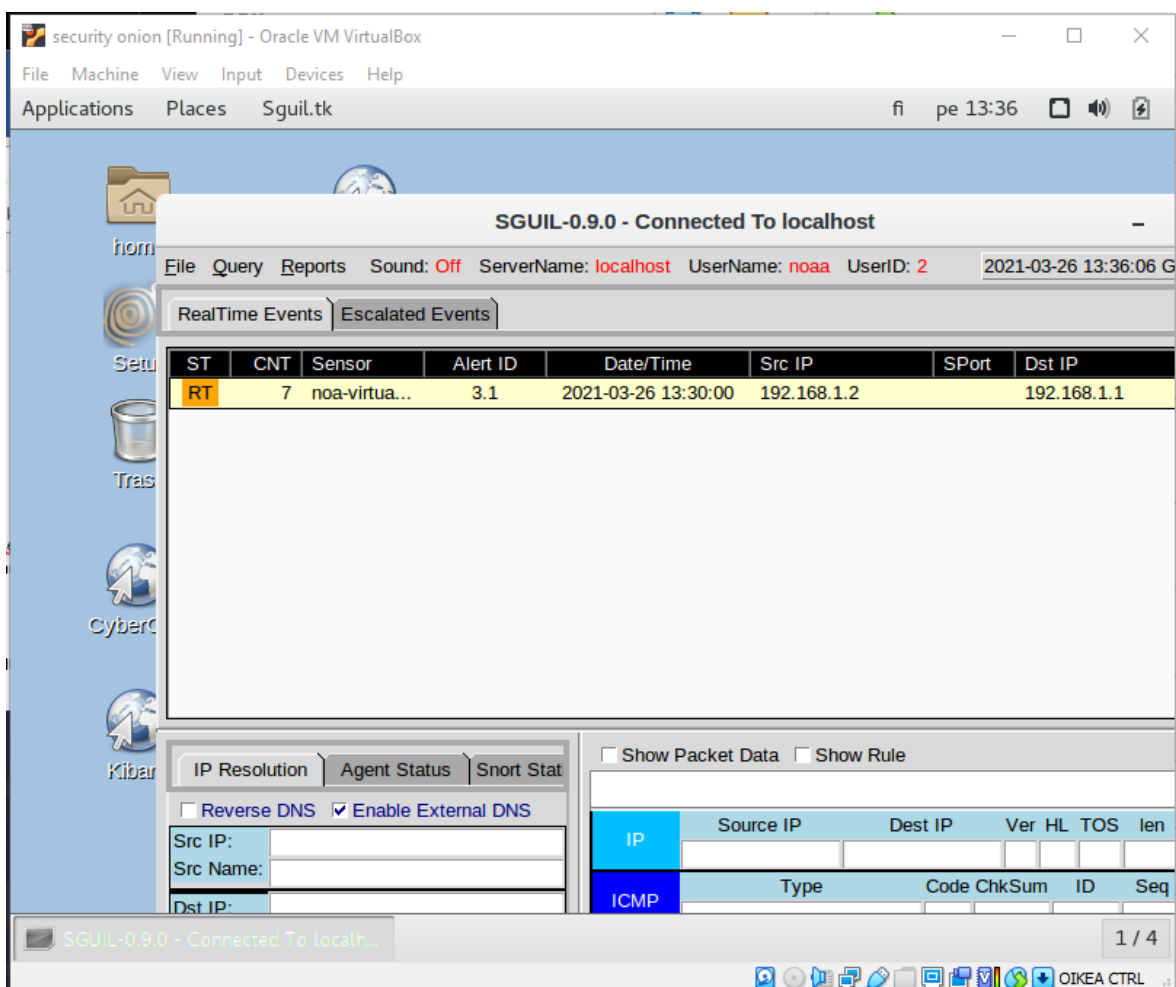
Kirjaudutaan squid – ohjelmaan (avataan se työpöydältä tuplaklikkaamalla) setup – sovelluksen toisella kierroksella asetetuilla tiedoilla. Kun Squid on käynnissä, pingataan kalilla security onionia.

```
(noa@noa)-[~]
$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.606 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.426 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=0.348 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=0.827 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=0.372 ms
64 bytes from 192.168.1.1: icmp_seq=6 ttl=64 time=0.347 ms
64 bytes from 192.168.1.1: icmp_seq=7 ttl=64 time=0.970 ms
^Z
zsh: suspended ping 192.168.1.1

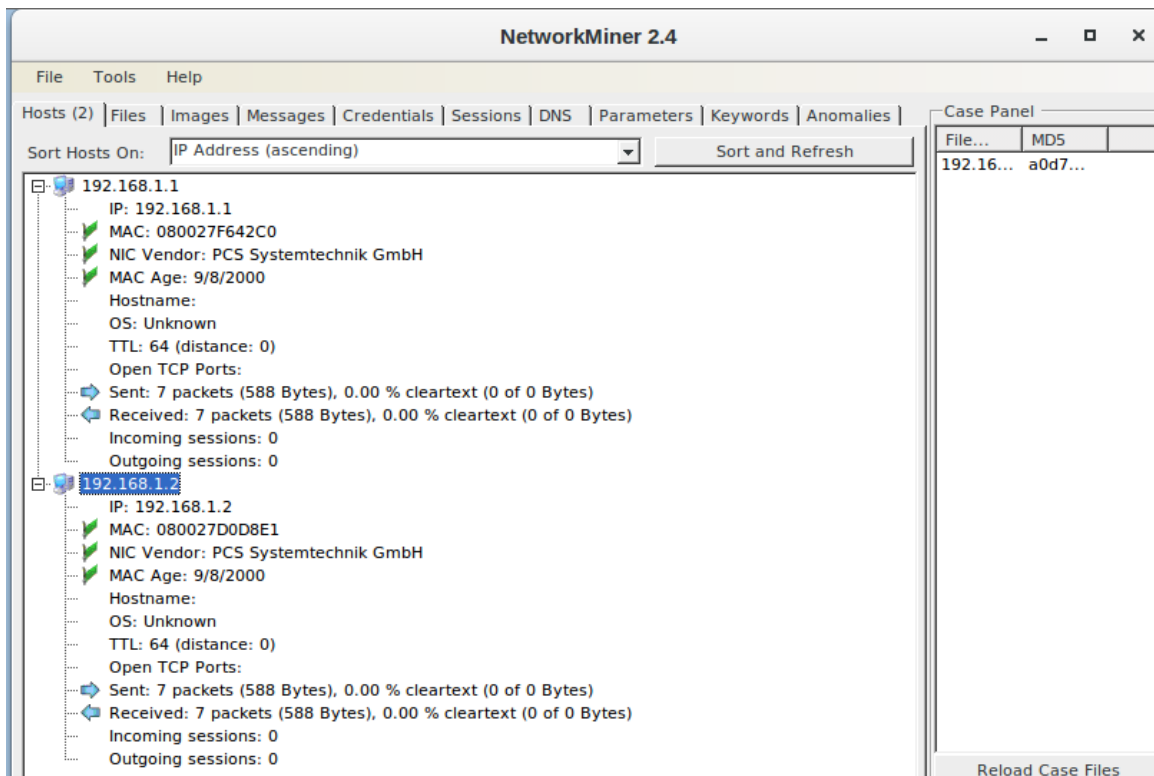
(noa@noa)-[~]
$
```

Pingaus Kalilta

Squilissa tapahtuma näyttää seuraavanlaiselta :



Pingaus Squilissa



Pingauksen jälki NetworkMinerissa

Yllä olevasta kuvasta huomataan lähetävä ja vastaanottava kone. Pakettien määrä ja koko.