Andreas Tolnes

N13

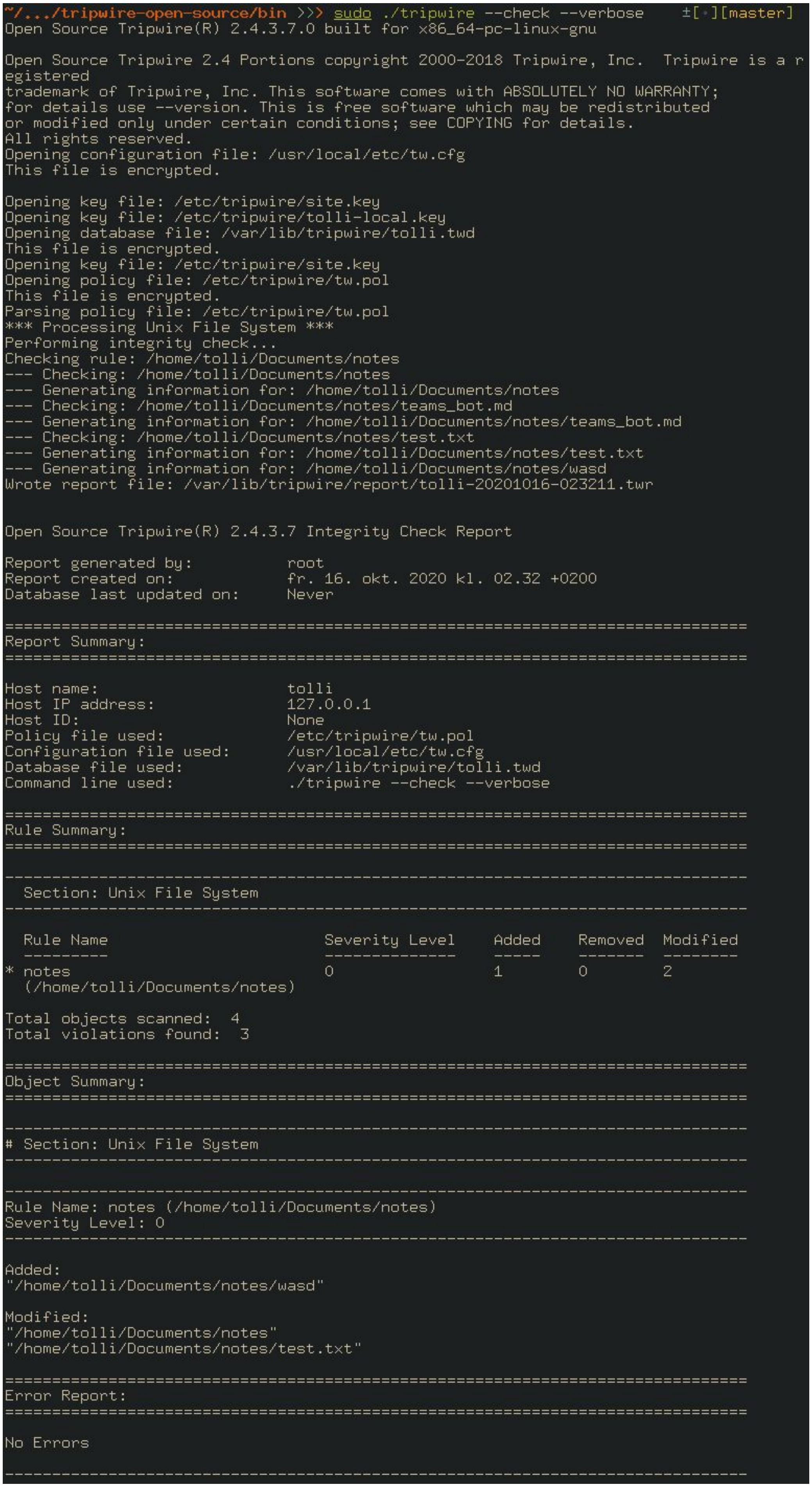
HIDS

Bestemte meg å bruke open source Tripwire.
Fulgte installasjonsguiden, og valgte å beskytte mappen ~/Documents/notes.

Satt regelen “/home/USER/Documents/notes -> $(ReadOnly);
Hver endring i *notes* mappen, burde gi en varsel i Tripwire.

Lagde en ny fil, og endret på en eksisterende fil i mappen. Når kommandoen *tripwire --check* ble kjørt, så sa den ifra at regelen har blitt brutt tre ganger. En gang for å lage ny fil, en gang for å endre den allerede eksisterende filen, og en gang for å endring i mappen.

Bildet under er av utskriften til *check* kommandoen.



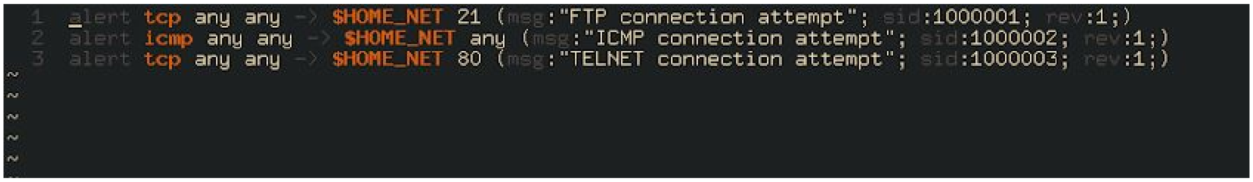
```
~/.../tripwire-open-source/bin >>> sudo ./tripwire --check --verbose    ±[•][master]
Open Source Tripwire(R) 2.4.3.7.0 built for x86_64-pc-linux-gnu

Open Source Tripwire 2.4 Portions copyright 2000-2018 Tripwire, Inc.  Tripwire is a r
egistered
trademark of Tripwire, Inc. This software comes with ABSOLUTELY NO WARRANTY;
for details use --version. This is free software which may be redistributed
or modified only under certain conditions; see COPYING for details.
All rights reserved.
Opening configuration file: /usr/local/etc/tw.cfg
This file is encrypted.

Opening key file: /etc/tripwire/site.key
Opening key file: /etc/tripwire/tolli-local.key
Opening database file: /var/lib/tripwire/tolli.twd
This file is encrypted.
Opening key file: /etc/tripwire/site.key
Opening policy file: /etc/tripwire/tw.pol
This file is encrypted.
Parsing policy file: /etc/tripwire/tw.pol
*** Processing Unix File System ***
Performing integrity check...
Checking rule: /home/tolli/Documents/notes
--- Checking: /home/tolli/Documents/notes
--- Generating information for: /home/tolli/Documents/notes
--- Checking: /home/tolli/Documents/notes/teams_bot.md
--- Generating information for: /home/tolli/Documents/notes/teams_bot.md
--- Checking: /home/tolli/Documents/notes/test.txt
--- Generating information for: /home/tolli/Documents/notes/test.txt
--- Generating information for: /home/tolli/Documents/notes/wasd
Wrote report file: /var/lib/tripwire/report/tolli-20201016-023211.twr


Open Source Tripwire(R) 2.4.3.7 Integrity Check Report

Report generated by:          root
Report created on:            fr. 16. okt. 2020 kl. 02.32 +0200
Database last updated on:     Never

===============================================================================
Report Summary:
===============================================================================

Host name:                    tolli
Host IP address:              127.0.0.1
Host ID:                      None
Policy file used:             /etc/tripwire/tw.pol
Configuration file used:      /usr/local/etc/tw.cfg
Database file used:           /var/lib/tripwire/tolli.twd
Command line used:            ./tripwire --check --verbose

===============================================================================
Rule Summary:
===============================================================================

-------------------------------------------------------------------------------
  Section: Unix File System
-------------------------------------------------------------------------------

  Rule Name                       Severity Level    Added    Removed  Modified
  ---------                       --------------    -----    -------  --------
* notes                           0                 1        0        2
  (/home/tolli/Documents/notes)

Total objects scanned:  4
Total violations found:  3

===============================================================================
Object Summary:
===============================================================================

-------------------------------------------------------------------------------
# Section: Unix File System
-------------------------------------------------------------------------------

-------------------------------------------------------------------------------
Rule Name: notes (/home/tolli/Documents/notes)
Severity Level: 0
-------------------------------------------------------------------------------

Added:
"/home/tolli/Documents/notes/wasd"

Modified:
"/home/tolli/Documents/notes"
"/home/tolli/Documents/notes/test.txt"

===============================================================================
Error Report:
===============================================================================

No Errors

-------------------------------------------------------------------------------
```

Andreas Tolnes

NIDS

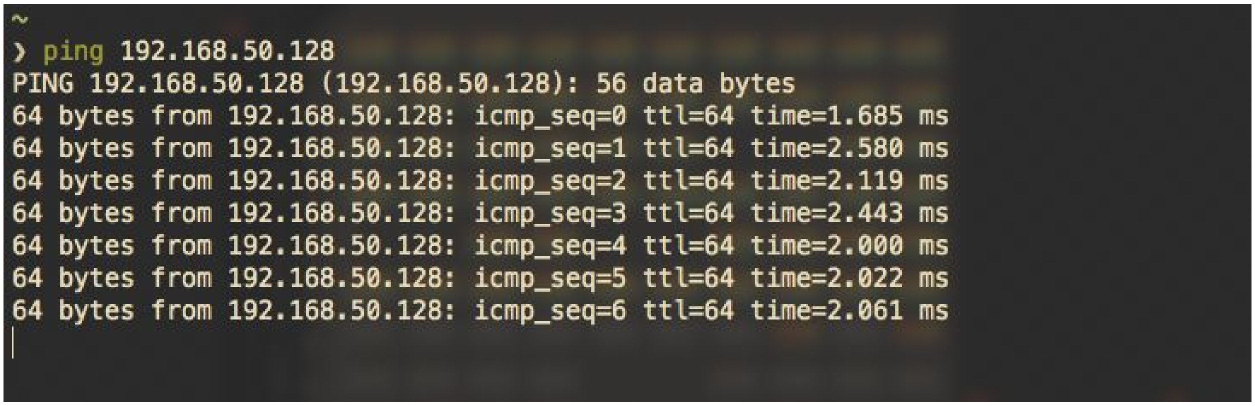
Valgte å bruke Snort, fulgte denne artikkelen for å få til installasjonen av programvaren.

Reglene som er satt, vil gi en advarsel når maskinen blir TCP pinget. Dette kan gjøres ved å bruke *ping* kommandoen uten noen flagg.



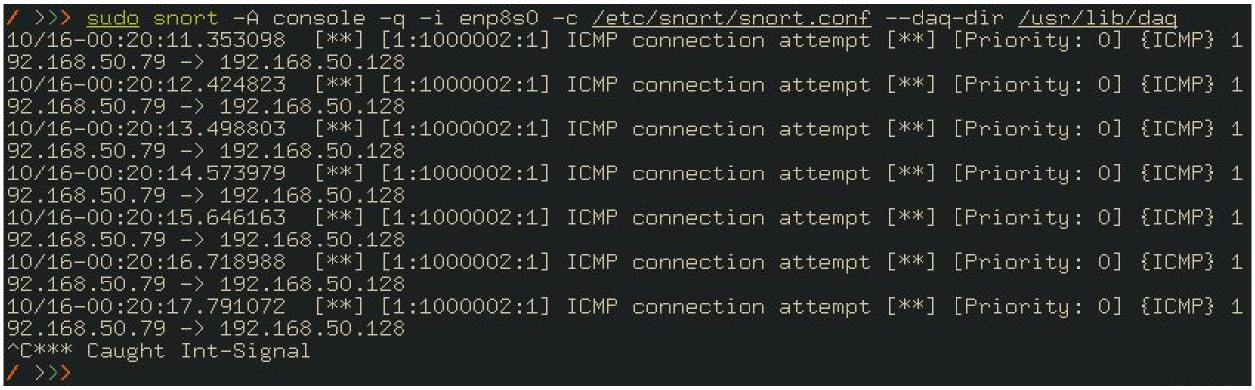
```
alert tcp any any -> $HOME_NET 21 (msg:"FTP connection attempt"; sid:1000001; rev:1;)
alert icmp any any -> $HOME_NET any (msg:"ICMP connection attempt"; sid:1000002; rev:1;)
alert tcp any any -> $HOME_NET 80 (msg:"TELNET connection attempt"; sid:1000003; rev:1;)
~
~
~
~
~
```

Her pinges det fra en annen maskin, til maskinen som har snort installert.



```
~
❯ ping 192.168.50.128
PING 192.168.50.128 (192.168.50.128): 56 data bytes
64 bytes from 192.168.50.128: icmp_seq=0 ttl=64 time=1.685 ms
64 bytes from 192.168.50.128: icmp_seq=1 ttl=64 time=2.580 ms
64 bytes from 192.168.50.128: icmp_seq=2 ttl=64 time=2.119 ms
64 bytes from 192.168.50.128: icmp_seq=3 ttl=64 time=2.443 ms
64 bytes from 192.168.50.128: icmp_seq=4 ttl=64 time=2.000 ms
64 bytes from 192.168.50.128: icmp_seq=5 ttl=64 time=2.022 ms
64 bytes from 192.168.50.128: icmp_seq=6 ttl=64 time=2.061 ms
```

Og her er varslene som oppstår når maskinen blir pinget.



```
/ >>> sudo snort -A console -q -i enp8s0 -c /etc/snort/snort.conf --daq-dir /usr/lib/daq
10/16-00:20:11.353098  [**] [1:1000002:1] ICMP connection attempt [**] [Priority: 0] {ICMP} 1
92.168.50.79 -> 192.168.50.128
10/16-00:20:12.424823  [**] [1:1000002:1] ICMP connection attempt [**] [Priority: 0] {ICMP} 1
92.168.50.79 -> 192.168.50.128
10/16-00:20:13.498803  [**] [1:1000002:1] ICMP connection attempt [**] [Priority: 0] {ICMP} 1
92.168.50.79 -> 192.168.50.128
10/16-00:20:14.573979  [**] [1:1000002:1] ICMP connection attempt [**] [Priority: 0] {ICMP} 1
92.168.50.79 -> 192.168.50.128
10/16-00:20:15.646163  [**] [1:1000002:1] ICMP connection attempt [**] [Priority: 0] {ICMP} 1
92.168.50.79 -> 192.168.50.128
10/16-00:20:16.718988  [**] [1:1000002:1] ICMP connection attempt [**] [Priority: 0] {ICMP} 1
92.168.50.79 -> 192.168.50.128
10/16-00:20:17.791072  [**] [1:1000002:1] ICMP connection attempt [**] [Priority: 0] {ICMP} 1
92.168.50.79 -> 192.168.50.128
^C*** Caught Int-Signal
/ >>>
```