Øving - 13 HIDS og NIDS

Eric Younger
Thomas Bakken Moe
Jonas Brunvoll Larsson

HIDS

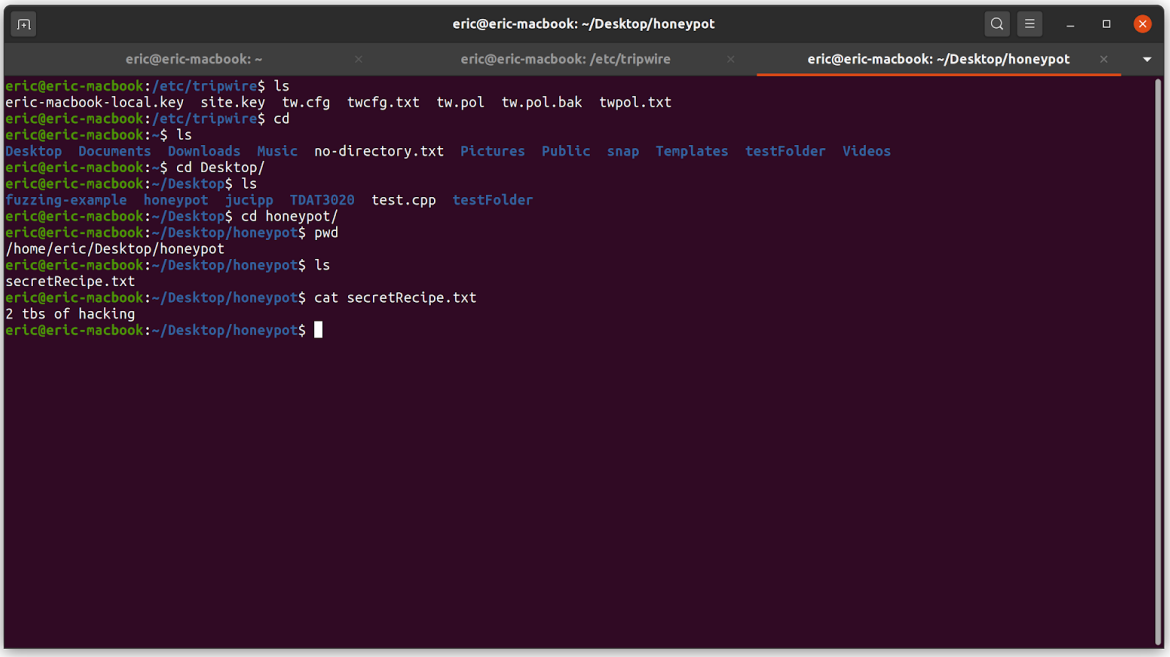
I øvingen benyttet vi programmet Tripwire for Host Intrusion Detection System(HIDS).

Vi har lagd mappen “Honeypot”, og derunder så er det lagd en fil som heter “secretRecipe.txt”. Denne mappen har blitt lagt til som en regel under tripwire som vi ser på skjermbildet under.

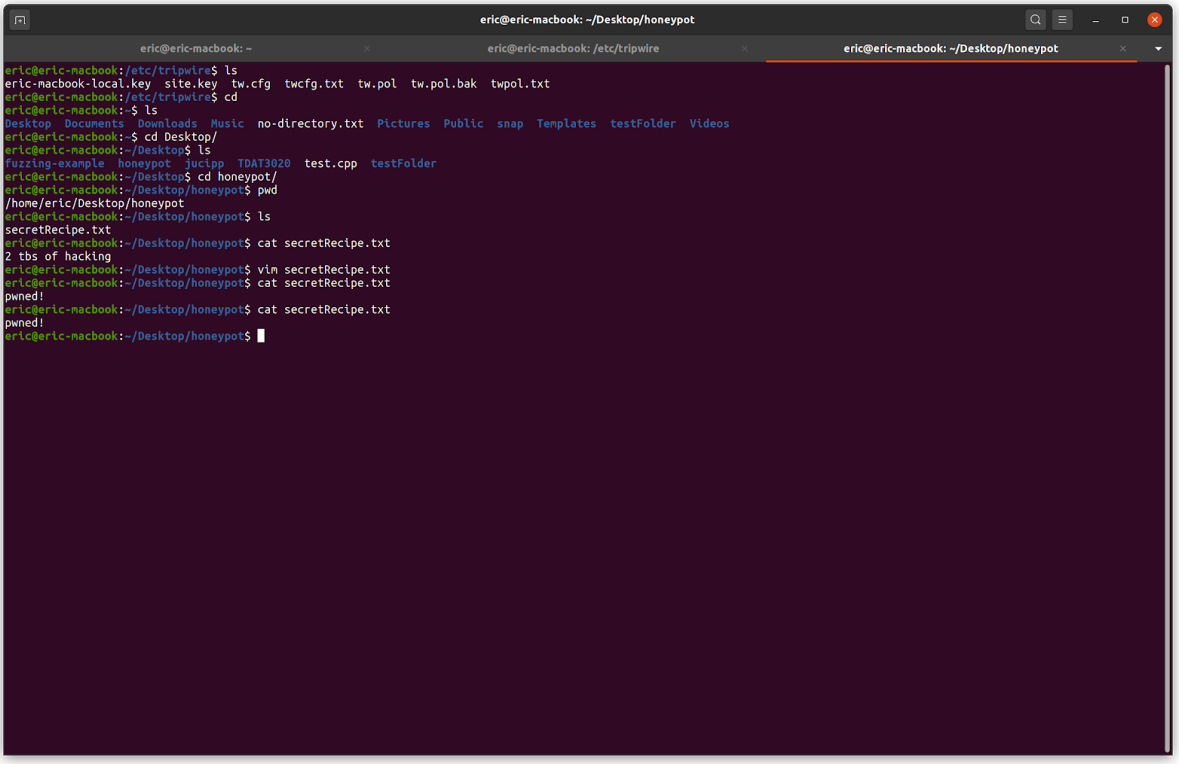
```
# Ruleset for honeypot
(
  rulename = "honeypot",
  severity= $(SIG_HI)
)
{
        /home/eric/Desktop/honeypot         -> $(SEC_CRIT);
}
"twpol.txt" 287L, 6220C
```

Etter å ha lagt til regelen så kjørte vi kommandoen: “sudo twadmin -m P /etc/tripwire/twpol.txt” som regenerer config filen til tripwire.

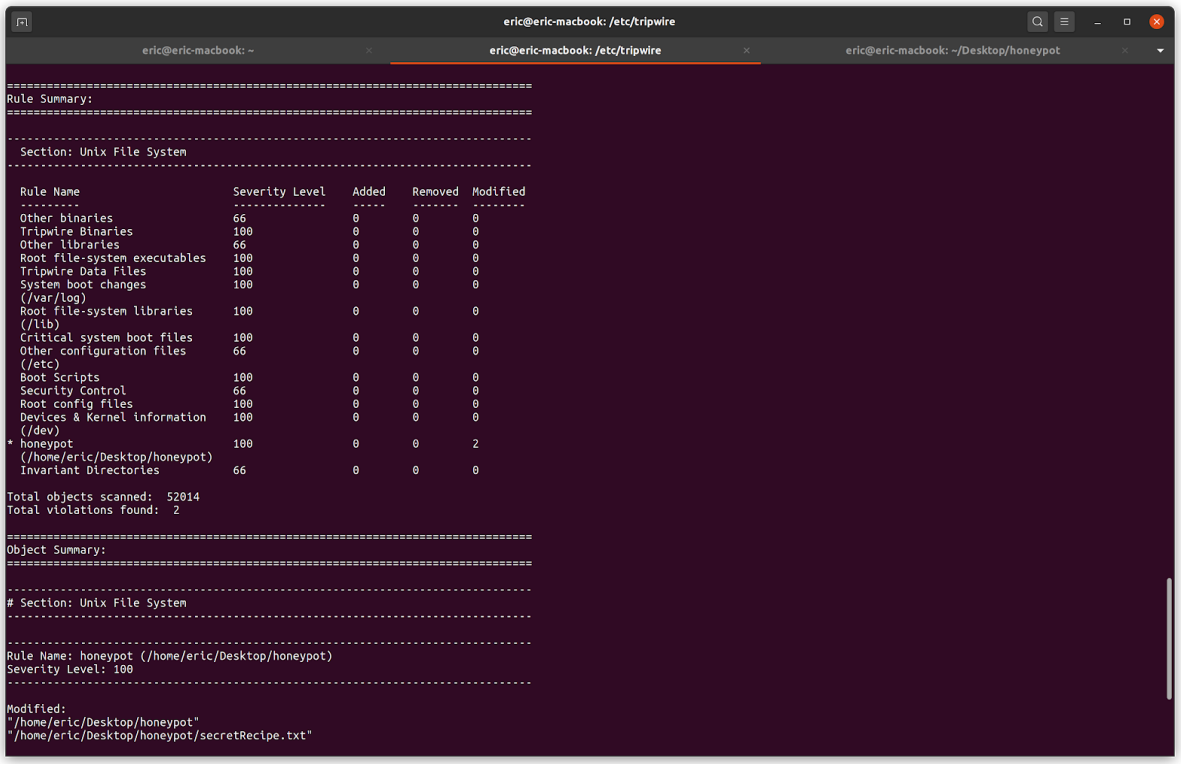
Så kjører vi kommandoen: “sudo tripwire --init” som initialiserer databasen med satte sjekksummer for filene som er satt regler for.

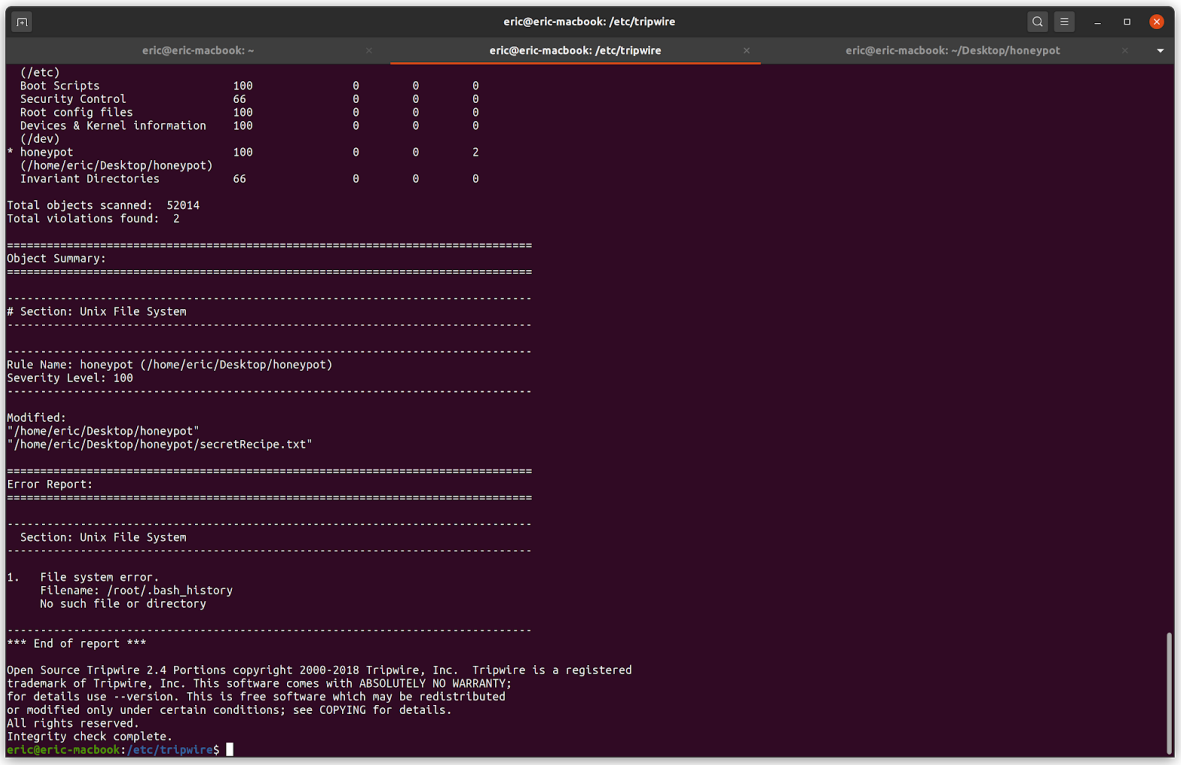


Innholdet i “secretRecipe.txt” før endring.



Vi endrer på filen “secretRecipe.txt”





Som vi kan se fra å kjøre kommandoen: “sudo tripwire --check” som sjekker igjennom filene opp mot indekserte verdier, så har en fil blitt endret inni mappa “honepot” og det gir en Violation.

NIDS

Oppsett for å teste ut NIDS:

Jonas sin datamaskin var koblet mot Eric sin datamaskin gjennom en Ethernet kabel.
Vi benyttet oss av programmet Snort for NIDS (Network Intrusion Detection System) for å løse oppgaven.

Vi endret på **etc/snort/snort.conf** til å peke mot default gateway med CIDR /24 på maskinen som skulle detektere inntrengere med linjen: *ipvar HOME_NET 10.42.0.1/24*

Deretter la vi inn en regel i filen **etc/snort/rules/local.rules** som skulle fange opp og gi en Alert når det ble kjørt PING eller NMAP kommandoen mot nettverket.

```
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.
#
alert icmp any any -> $HOME_NET any (msg:"ICMP test"; sid:1000001; rev:1; classtype:icmp-event;)
eric@eric-macbook:/etc/snort/rules$
```

Kjører så Snort med kommandoen: “sudo snort -A console -c /etc/snort/snort.conf -i ens9 -K ascii”.

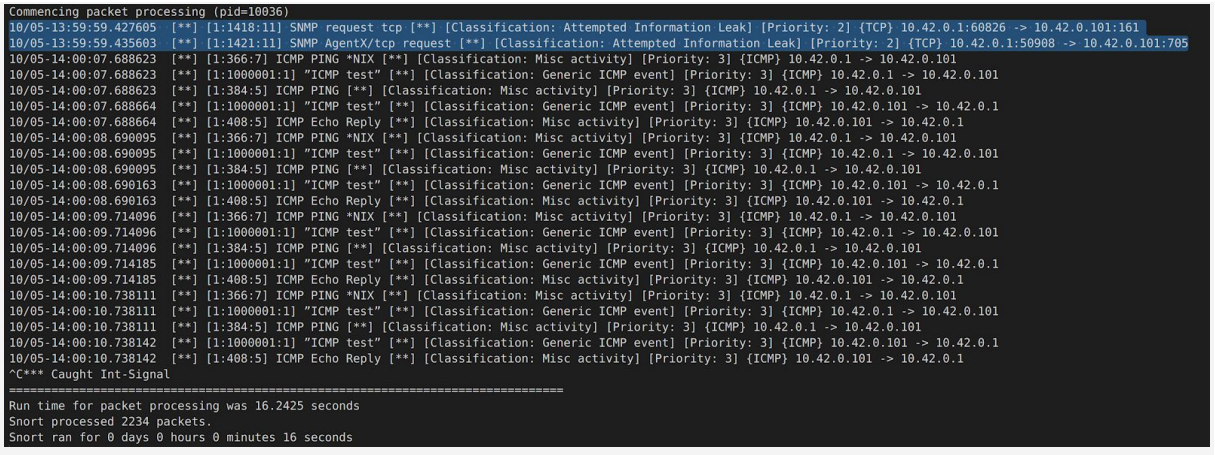
Vi utløste Alerts ved å først kjøre kommandoen ‘nmap -A [ip-addresse til maskinen med Snort]’,

```
jonasbl@jonasbl-MacBookAir: ~
jonasbl@jonasbl-MacBookAir:~$ nmap -A 10.42.0.101
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-05 13:51 CEST
Nmap scan report for 10.42.0.101
Host is up (0.0046s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
25/tcp open  smtp    Postfix smtpd
|_smtp-commands: eric-macbook.wlan.ntnu.no, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES
, 8BITMIME, DSN, SMTPUTF8, CHUNKING,
| ssl-cert: Subject: commonName=ubuntu
| Subject Alternative Name: DNS:ubuntu
| Not valid before: 2020-08-28T18:28:47
|_Not valid after:  2030-08-26T18:28:47
|_ssl-date: TLS randomness does not represent time
Service Info: Host:  eric-macbook.wlan.ntnu.no
```

deretter ved hjelp av ‘ping [ip-addresse til maskinen med Snort]

```
jonasbl@jonasbl-MacBookAir:~$ ping 10.42.0.101
PING 10.42.0.101 (10.42.0.101) 56(84) bytes of data.
64 bytes from 10.42.0.101: icmp_seq=1 ttl=64 time=0.308 ms
64 bytes from 10.42.0.101: icmp_seq=2 ttl=64 time=0.348 ms
64 bytes from 10.42.0.101: icmp_seq=3 ttl=64 time=0.369 ms
64 bytes from 10.42.0.101: icmp_seq=4 ttl=64 time=0.275 ms
^C
--- 10.42.0.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3049ms
rtt min/avg/max/mdev = 0.275/0.325/0.369/0.036 ms
jonasbl@jonasbl-MacBookAir:~$
```

Alertsene som er markert i blått under er når Jonas kjørte NMAP kommandoen mot nettverket. Mens de under der igjen er ifra PING kommandoen.



```
Commencing packet processing (pid=10036)
10/05-13:59:59.427605  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 10.42.0.1:60826 -> 10.42.0.101:161
10/05-13:59:59.435603  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 10.42.0.1:50908 -> 10.42.0.101:705
10/05-14:00:07.688623  [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [Priority: 3] {ICMP} 10.42.0.1 -> 10.42.0.101
10/05-14:00:07.688623  [**] [1:1000001:1] "ICMP test" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.42.0.1 -> 10.42.0.101
10/05-14:00:07.688623  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 10.42.0.1 -> 10.42.0.101
10/05-14:00:07.688664  [**] [1:1000001:1] "ICMP test" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.42.0.101 -> 10.42.0.1
10/05-14:00:07.688664  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 10.42.0.101 -> 10.42.0.1
10/05-14:00:08.690095  [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [Priority: 3] {ICMP} 10.42.0.1 -> 10.42.0.101
10/05-14:00:08.690095  [**] [1:1000001:1] "ICMP test" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.42.0.1 -> 10.42.0.101
10/05-14:00:08.690095  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 10.42.0.1 -> 10.42.0.101
10/05-14:00:08.690163  [**] [1:1000001:1] "ICMP test" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.42.0.101 -> 10.42.0.1
10/05-14:00:08.690163  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 10.42.0.101 -> 10.42.0.1
10/05-14:00:09.714096  [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [Priority: 3] {ICMP} 10.42.0.1 -> 10.42.0.101
10/05-14:00:09.714096  [**] [1:1000001:1] "ICMP test" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.42.0.1 -> 10.42.0.101
10/05-14:00:09.714096  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 10.42.0.1 -> 10.42.0.101
10/05-14:00:09.714185  [**] [1:1000001:1] "ICMP test" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.42.0.101 -> 10.42.0.1
10/05-14:00:09.714185  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 10.42.0.101 -> 10.42.0.1
10/05-14:00:10.738111  [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [Priority: 3] {ICMP} 10.42.0.1 -> 10.42.0.101
10/05-14:00:10.738111  [**] [1:1000001:1] "ICMP test" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.42.0.1 -> 10.42.0.101
10/05-14:00:10.738111  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 10.42.0.1 -> 10.42.0.101
10/05-14:00:10.738142  [**] [1:1000001:1] "ICMP test" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.42.0.101 -> 10.42.0.1
10/05-14:00:10.738142  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 10.42.0.101 -> 10.42.0.1
^C*** Caught Int-Signal
===============================================================================
Run time for packet processing was 16.2425 seconds
Snort processed 2234 packets.
Snort ran for 0 days 0 hours 0 minutes 16 seconds
```

Logg fra kjøring av programmet:

Se vedlagt “log.txt” for full rapport fra kjøring av programmet Snort.