

# 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.

A screenshot of a macOS terminal window with three tabs open at the top: "eric@eric-macbook: ~/Desktop/honeypot", "eric@eric-macbook: /etc/tripwire", and "eric@eric-macbook: ~/Desktop/honeypot". The active tab is the third one. The terminal shows a series of commands and their outputs:  

```
eric@eric-macbook:/etc/tripwire$ ls  
eric-macbook-local.key site.key tw.cfg twcfg.txt tw.pol tw.pol.bak twpol.txt  
eric@eric-macbook:/etc/tripwire$ cd  
eric@eric-macbook:~$ ls  
Desktop Documents Downloads Music no-directory.txt Pictures Public snap Templates testFolder Videos  
eric@eric-macbook:~$ cd Desktop/  
eric@eric-macbook:~/Desktop$ ls  
fuzzing-example honeypot jucipp TDAT3020 test.cpp testFolder  
eric@eric-macbook:~/Desktop$ cd honeypot/  
eric@eric-macbook:~/Desktop/honeypot$ pwd  
/home/eric/Desktop/honeypot  
eric@eric-macbook:~/Desktop/honeypot$ ls  
secretRecipe.txt  
eric@eric-macbook:~/Desktop/honeypot$ cat secretRecipe.txt  
2 tbs of hacking  
eric@eric-macbook:~/Desktop/honeypot$
```

*Innholdet i "secretRecipe.txt" før endring.*

```
eric@eric-macbook: ~/Desktop/honeypot
eric@eric-macbook: ~/Desktop/honeypot
eric@eric-macbook: /etc/tripwire
eric@eric-macbook: ~$ ls
eric-macbook-local.key site.key tw.cfg twcfg.txt tw.pol tw.pol.bak twpol.txt
eric@eric-macbook: /etc/tripwire$ cd
eric@eric-macbook: ~$ ls
Desktop Documents Downloads Music no-directory.txt Pictures Public snap Templates testFolder Videos
eric@eric-macbook: ~$ cd Desktop/
eric@eric-macbook: ~/Desktop$ ls
fuzzing-example honeypot juicpp TDAT3020 test.cpp testFolder
eric@eric-macbook: ~/Desktop$ cd honeypot/
eric@eric-macbook: ~/Desktop/honeypot$ pwd
/home/eric/Desktop/honeypot
eric@eric-macbook: ~/Desktop/honeypot$ ls
secretRecipe.txt
eric@eric-macbook: ~/Desktop/honeypot$ cat secretRecipe.txt
2 tbs of hacking
eric@eric-macbook: ~/Desktop/honeypot$ vim secretRecipe.txt
eric@eric-macbook: ~/Desktop/honeypot$ cat secretRecipe.txt
pwned!
eric@eric-macbook: ~/Desktop/honeypot$ cat secretRecipe.txt
pwned!
eric@eric-macbook: ~/Desktop/honeypot$
```

*Vi endrer på filen "secretRecipe.txt"*

```
eric@eric-macbook: /etc/tripwire
eric@eric-macbook: ~
eric@eric-macbook: /etc/tripwire
eric@eric-macbook: ~/Desktop/honeypot

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

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

Rule Name          Severity Level  Added  Removed  Modified
-----
Other binaries      66             0      0         0
Tripwire Binaries   100            0      0         0
Other libraries      66             0      0         0
Root file-system executables 100            0      0         0
Tripwire Data Files 100            0      0         0
System boot changes 100            0      0         0
(/var/log)          100            0      0         0
Root file-system libraries 100            0      0         0
(/lib)              100            0      0         0
Critical system boot files 100            0      0         0
Other configuration files 66             0      0         0
(/etc)              100            0      0         0
Boot Scripts        66             0      0         0
Security Control     66             0      0         0
Root config files    100            0      0         0
Devices & Kernel information 100            0      0         0
(/dev)              100            0      0         0
* honeypot           100            0      0         2
(/home/eric/Desktop/honeypot)
Invariant Directories 66             0      0         0

Total objects scanned: 52014
Total violations found: 2

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

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

Rule Name: honeypot (/home/eric/Desktop/honeypot)
Severity Level: 100

-----
Modified:
"/home/eric/Desktop/honeypot"
"/home/eric/Desktop/honeypot/secretRecipe.txt"
=====
```

```
eric@eric-macbook: /etc/tripwire
eric@eric-macbook: ~
eric@eric-macbook: /etc/tripwire
eric@eric-macbook: ~/Desktop/honeypot

(/etc)
Boot Scripts        100            0      0         0
Security Control     66             0      0         0
Root config files    100            0      0         0
Devices & Kernel information 100            0      0         0
(/dev)              100            0      0         0
* honeypot           100            0      0         2
(/home/eric/Desktop/honeypot)
Invariant Directories 66             0      0         0

Total objects scanned: 52014
Total violations found: 2

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

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

Rule Name: honeypot (/home/eric/Desktop/honeypot)
Severity Level: 100

-----
Modified:
"/home/eric/Desktop/honeypot"
"/home/eric/Desktop/honeypot/secretRecipe.txt"
=====

Error Report:
=====

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

1. File system error.
   Filename: /root/.bash_history
   No such file or directory

-----
*** End of report ***

Open Source Tripwire 2.4 Portions copyright 2000-2018 Tripwire, Inc. Tripwire is a registered
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.
Integrity check complete.
eric@eric-macbook: /etc/tripwire$
```

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 “honeypot” 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-adresse 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-adresse 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.