Øving 13 - IDS

HIDS

Her ble *tripwire* brukt på Ubuntu 20.04 LTS.

Regel

Følgende regel ble lagt inn i *etc/tripwire/twpol.txt*:

```
(
  rulename = "Test Ruleset",
  severity= $(SIG_HI)
)
{
        /hakon/home/test   -> $(ReadOnly);
}
```

Mappen */hakon/homw/test* skal altså kun kunne leses, ikke skrives til.

Regelbrudd

For å framprovosere feil opprettet jeg en .txt fil i */hakon/home/test* mappen:

```
echo "ikke lov" > test.txt
```

Kjørte deretter en sjekk med *tripwire*, som resulterte i følgende output:

```
 Rule Name                 Severity Level    Added    Removed  Modified
  ---------                 --------------    -----    -------  --------
* Test Ruleset                    100            1        0        1
  (/home/hakon/test)

Total violations found:  2

Added:
"/home/hakon/test/test.txt"

Modified:
"/home/hakon/test"
```

Her ble det funnet to regelbrudd. Den første var at *test.txt* ble lagt til i */home/hakon/test* mappen. Den andre var at */home/hakon/test* mappen ble modifisert. Dette viser at HIDS-et fungerer som ønsket.

NIDS

Her ble *snort* brukt på Ubuntu 20.04 LTS.

Regel

Følgende regel ble lagt inn i */usr/local/etc/rules/local.rules*:

```
alert icmp any any -> $HOME_NET any (msg:"Ping-flood"; sid:1000001;
detection_filter:track by_dst, count 500, seconds 3;)
```

Regelen sier at dersom en maskin mottar over 500 ICMP-pakker i løpet av tre sekunder, skal et varsel sendes (logges). *Snort* vil se på pakker som sendes fra alle IP-adresser (*any*) og alle porter (*any*), til hjemmenettet (*$HOME_NET*) på alle porter (*any*). Hjemmenettet er i dette tilfellet satt til 192.168.1.0/24.

Regelen ble verifisert med *snort* slik:

```
snort -c /usr/local/etc/snort/snort.lua -R
/usr/local/etc/rules/local.rules
```

Regelbrudd

For å framprovosere feil ble det kjørt en ip-flood fra en annen maskin i samme nettverk:

```
sudo ping -f 192.168.1.139
```

Snort produserte følgende output i *alert_fast.txt* filen:

```
09/27-22:40:17.885826 [**] [1:1000001:0] "Ping-flood" [**] [Priority: 0]
{ICMP} 192.168.1.142 -> 192.168.1.139
09/27-22:40:17.885831 [**] [1:1000001:0] "Ping-flood" [**] [Priority: 0]
{ICMP} 192.168.1.139 -> 192.168.1.142
09/27-22:40:17.885836 [**] [1:1000001:0] "Ping-flood" [**] [Priority: 0]
{ICMP} 192.168.1.142 -> 192.168.1.139
...
```

Her kan vi se at regelen “Ping-flood” har blitt trigget, som tiltenkt. Ser at angrepet gikk fra maskin med IP 192.168.1.142 til maskin med IP 192.168.1.139. Snort reagerte ved å skrive dette til loggen. NIDS-et fungerer med andre ord som ønsket.