
Intrusion Detection/Intrusion Prevention

Etter å ha fullført modulen, forventes det at studenten har oppnådd følgende læringsmål:

- Ha kunnskap om forskjellen mellom en innbruddsdeteksjon og innbruddsforebygging.
- Forstå hvordan vertsbaserte innbruddsdeteksjonssystemer (HIDS) fungerer.
- Forstå hvordan nettverksbaserte innbruddsdeteksjonssystemer (NIDS) fungerer.
- Forstå begrepet misbruksdeteksjon og anomali-deteksjon.
- Forklare mulige utfall av innbruddsalarm:
 - Falske positive
 - Sanne positive
 - Falske negative
 - Sanne negative
- Kunne analysere og tolke alarmer fra HIDS (OSSEC).
- Kunne analysere og tolke alarmer fra NIDS (Snort).

DEFINISJONER:

- Inntrenging
 - En rekke hendelser som har som mål å kompromittere sikkerheten, nemlig:
 - Integritet, konfidensialitet og tilgjengelighet
- Intrusjonsdeteksjon/Intrusjonsforebygging
 - Prosessen med å identifisere og respondere/blokke inntrengingsaktivitet

IDS og IPS er to typer sikkerhetsteknologier som brukes for å beskytte datasystemer og nettverk mot uautorisert tilgang, inntrengninger og angrep. Her er en kort forklaring av begge:

1. IDS (Intrusion Detection System) - Inntrengningsdeteksjonssystem:

- IDS er et sikkerhetssystem som overvåker nettverkstrafikk eller systemaktivitet for å oppdage potensielle trusler eller uautoriserte aktiviteter.

- Det analyserer trafikken i sanntid og genererer varsler når det oppdager mistenkelige mønstre eller avvik fra normen.
- IDS er vanligvis passivt og varsler bare om mulige trusler uten å gripe inn i selve nettverket eller systemet.

2. IPS (Intrusion Prevention System) - Inntrengningsforebyggelsessystem:

- IPS er en videreutvikling av IDS og går et skritt videre ved å ikke bare oppdage trusler, men også ta aktive skritt for å forhindre dem.
- Når en trussel oppdages, kan IPS ta umiddelbare handlinger, for eksempel å blokkere trafikk fra en skadelig kilde, begrense tilgang eller stanse en angripende handling.
- IPS er derfor mer proaktivt enn IDS og kan bidra til å beskytte systemene mot potensielle trusler i sanntid.

Begge IDS og IPS spiller en viktig rolle i nettverkssikkerhet ved å oppdage og respondere på angrep og inntrengninger. De brukes ofte sammen for å gi en omfattende sikkerhetsløsning.

IDS/IPS-klassifisering

Klassifisering basert på beskyttelsesomfang eller plassering

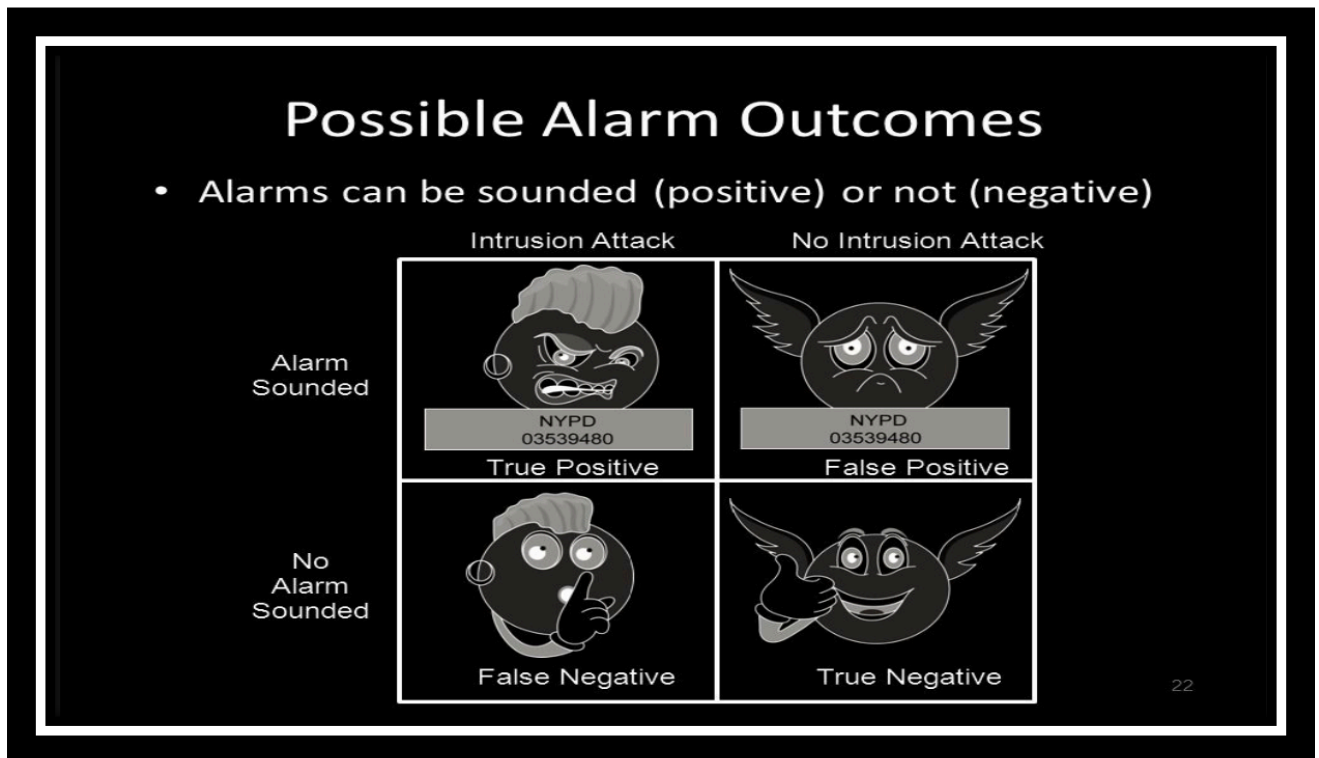
- Vertsbasert IDS
 - Overvåker aktiviteten på en datamaskin for å oppdage forsøk på eller vellykkede inntrengninger
 - Krever agenter på alle maskiner i en organisasjon
- Nettverksbasert IDS
 - Frittstående nettverksenhet som overvåker nettverkstrafikk for å oppdage angrep

Klassifisering basert på deteksjonsmodell

- Misbruk deteksjon
 - Sammenlikner «mønstre/signaturer» fra ukjente angrep
 - Rapporterer hvis det er match
 - Oppdager ikke nye type angrep
- Anomalideteksjon
 - Bygger matematisk/statistisk modell med akseptbar oppførsel
 - Gyldig, mistenkelig og ukjent
 - Rapporterer uvanlig/ukjent oppførsel

UTFORDRINGER VED Å BRUKE IDS

- Masse trafikk
- IDS forhindrer ikke angrep med mindre det er inntrengings forhindring egenskaper også
- Sender mange alarmer
 - o Falske positiver



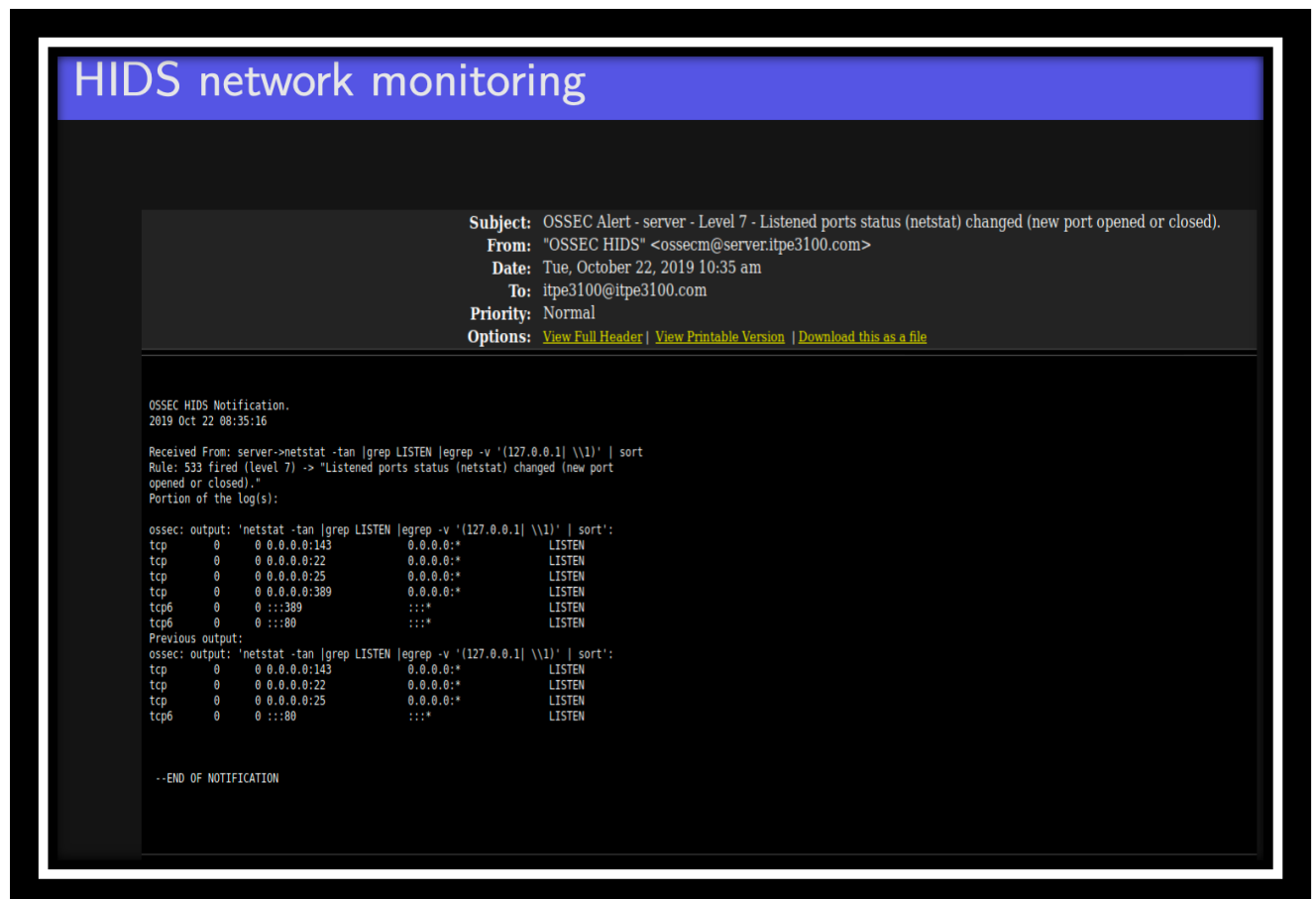
FALSK/SANN/POSITIV/NEGATIV

- Falsk positiv
 - o En autorisert aktivitet er feil identifisert som en inntrenger. Systemet sender en falsk alarm. Dette er uønsket.
- Sann positiv
 - o En autorisert aktivitet er riktig identifisert. Systemet sender en legitim alarm. Dette er ønsket.
- Falsk negativ
 - o En autorisert aktivitet er ikke identifisert. Systemet sender ikke en alarm. Dette er uønsket og veldig farlig.
- Sann negativ

- Autorisert aktivitet riktig identifisert. Alt er normalt, og systemet sender ikke en alarm. Dette er ønsket.

HOST INTRUSION DETECTION SYSTEM (HIDS)

- HIDS overvåker filsystemer, loggfiler, nettverkstilkoblinger og bruekraktivitet.
 - Eksempel: når en fil overvåket av IDS endres, sammenlikner HIDS hashverdien til den nye filen med hashverdien til den gamle filen for å se om den har endret seg eller ikke. Hvis det er en forskjell sendes en varsling til system administrator.



The screenshot shows an email alert from OSSEC HIDS titled "HIDS network monitoring". The email header includes the subject "OSSEC Alert - server - Level 7 - Listened ports status (netstat) changed (new port opened or closed)", from "OSSEC HIDS" <ossecm@server.itpe3100.com>, date "Tue, October 22, 2019 10:35 am", to "itpe3100@itpe3100.com", and priority "Normal". The body of the email contains the following text:

```
OSSEC HIDS Notification.
2019 Oct 22 08:35:16

Received From: server->netstat -tan |grep LISTEN |egrep -v '(127.0.0.1|\\1)' | sort
Rule: 533 fired (level 7) -> "Listened ports status (netstat) changed (new port
opened or closed)."
```

Portion of the log(s):

```
ossec: output: 'netstat -tan |grep LISTEN |egrep -v '(127.0.0.1|\\1)' | sort':
tcp      0      0 0.0.0.0:143      0.0.0.0:*        LISTEN
tcp      0      0 0.0.0.0:22       0.0.0.0:*        LISTEN
tcp      0      0 0.0.0.0:25       0.0.0.0:*        LISTEN
tcp      0      0 0.0.0.0:389      0.0.0.0:*        LISTEN
tcp6     0      0 :::389          :::*             LISTEN
tcp6     0      0 :::80           :::*             LISTEN

Previous output:
ossec: output: 'netstat -tan |grep LISTEN |egrep -v '(127.0.0.1|\\1)' | sort':
tcp      0      0 0.0.0.0:143      0.0.0.0:*        LISTEN
tcp      0      0 0.0.0.0:22       0.0.0.0:*        LISTEN
tcp      0      0 0.0.0.0:25       0.0.0.0:*        LISTEN
tcp6     0      0 :::80           :::*             LISTEN
```

--END OF NOTIFICATION

HIDS user activity monitoring

Subject: OSSEC Alert - server - Level 8 - New group added to the system
From: "OSSEC HIDS" <ossecm@server.itpe3100.com>
Date: Mon, October 21, 2019 9:43 am
To: itpe3100@itpe3100.com
Priority: Normal
Options: [View Full Header](#) | [View Printable Version](#) | [Download this as a file](#)

```
OSSEC HIDS Notification.
2019 Oct 21 07:43:37

Received From: server->/var/log/auth.log
Rule: 5901 fired (level 8) -> "New group added to the system"
Portion of the log(s):

Oct 21 09:43:37 server useradd[957]: new group: name=sysadmin, GID=1002

--END OF NOTIFICATION

OSSEC HIDS Notification.
2019 Oct 21 07:43:37

Received From: server->/var/log/auth.log
Rule: 5902 fired (level 8) -> "New user added to the system"
Portion of the log(s):

Oct 21 09:43:37 server useradd[957]: new user: name=sysadmin, UID=1002, GID=1002,
home=/home/sysadmin, shell=/bin/bash

--END OF NOTIFICATION
```

HIDS user activity monitoring

Subject: OSSEC Alert - server - Level 4 - First time user logged in.
From: "OSSEC HIDS" <ossecm@server.itpe3100.com>
Date: Mon, October 21, 2019 9:41 am
To: itpe3100@itpe3100.com
Priority: Normal
Options: [View Full Header](#) | [View Printable Version](#) | [Download this as a file](#)

```
OSSEC HIDS Notification.
2019 Oct 21 07:40:52

Received From: server->/var/log/auth.log
Rule: 10100 fired (level 4) -> "First time user logged in."
Src IP: 10.175.102.1
User: itpe3100
Portion of the log(s):

Oct 21 07:40:52 server sshd[4101]: Accepted password for itpe3100 from 10.175.102.1
port 37184 ssh2

--END OF NOTIFICATION
```

FILSYSTEMET SOM EN DATAKILDE

- Linux, unix og Windows er operativsystemer som har viktige filsystem attributter
- I unix/Linux filsystem vil de følgende attributtene/tidsstemplingene være av interesse til HIDS:
 - o Tilgang: Sist en kilde er aksessert
 - o Modifiser: Sist innholdet til en kilde er endret
 - o Endre: Sist meta dataen til en fil var modifisert (for eksempel filrettigheter)

FILSYSTEM INTEGRITET OVERVÅKING

- integritet overvåking involverer å sjekke nøkkel filsystem attributter for endringer
- HIDS tar vanligvis en 'snapshot' av en MD5/SHA1 checksum av filene for å merke endringer til en fil på et senere tidspunkt
- Noen kjente programmer for overvåking av integriteten av filer er:
 - o EXAMPLE
 - OSSEC
 - AIDE
 - Samhaim
 - TripWire
 - Den mest populære i HIDS i åpenkilde, men har blitt commercialized

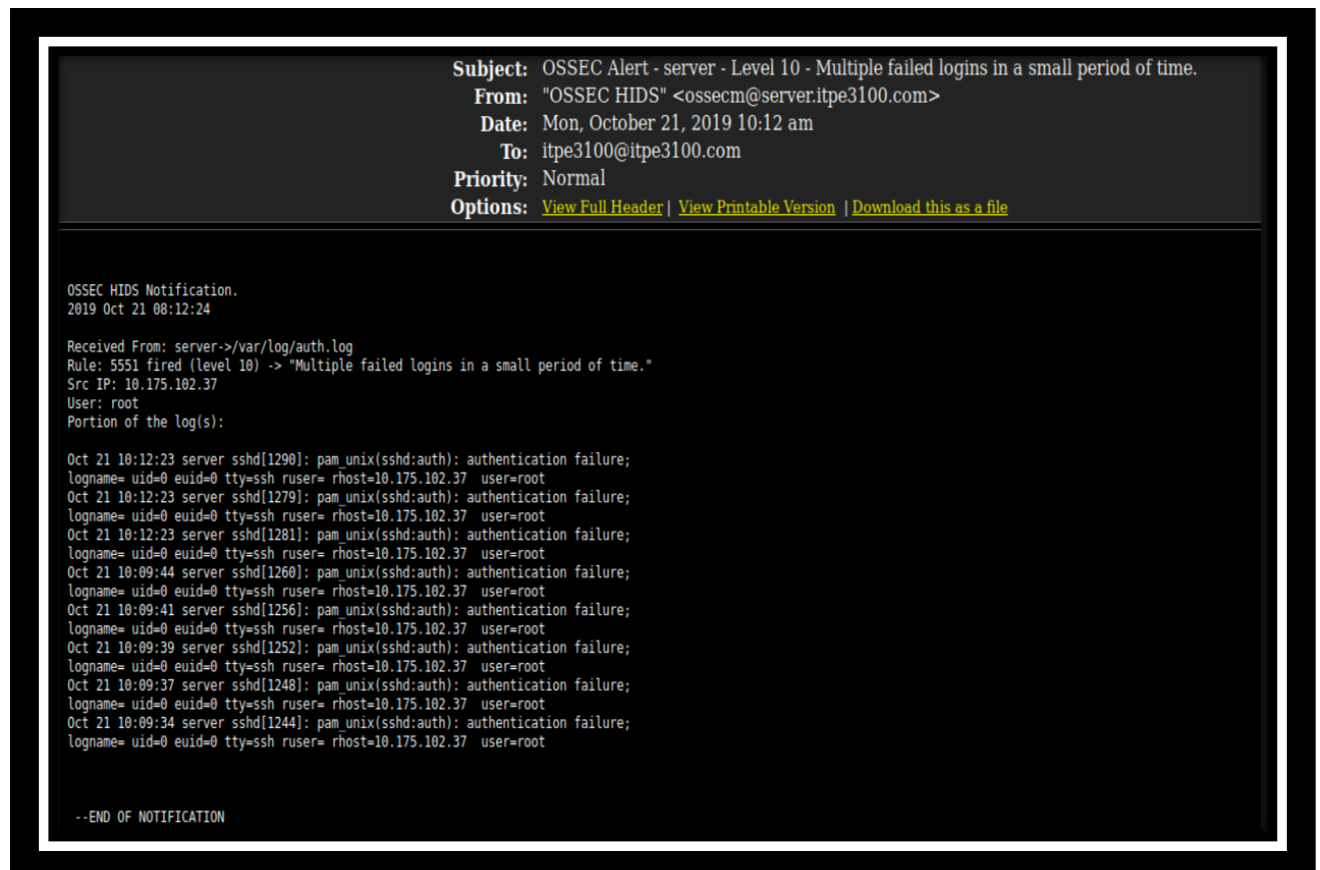
HIDS FILSYSTEM INTEGRITET ANALYSE



LOGGFILER SOM EN DATAKILDE

- Loggfil overvåking forsøker å følge inntrengere bed å tolke loggfiler
- Logg overvåkings programmer er tilgjengelige for Linux/unix
- Eksempel:
 - o OSSEC: overvåking unix loggfiler og tillater administrator å ta spesifikke valg som å sende varsling ved epost
 - o Swatch: overvåker unix loggfiler og kan informere administratører gjennom epost eller konsoll
 - o LogWatch: hjelper spot problemer og sikkerhetsbrudd i dine loggfiler automatisk og vil sende resultatene det tas opp til deg på mail

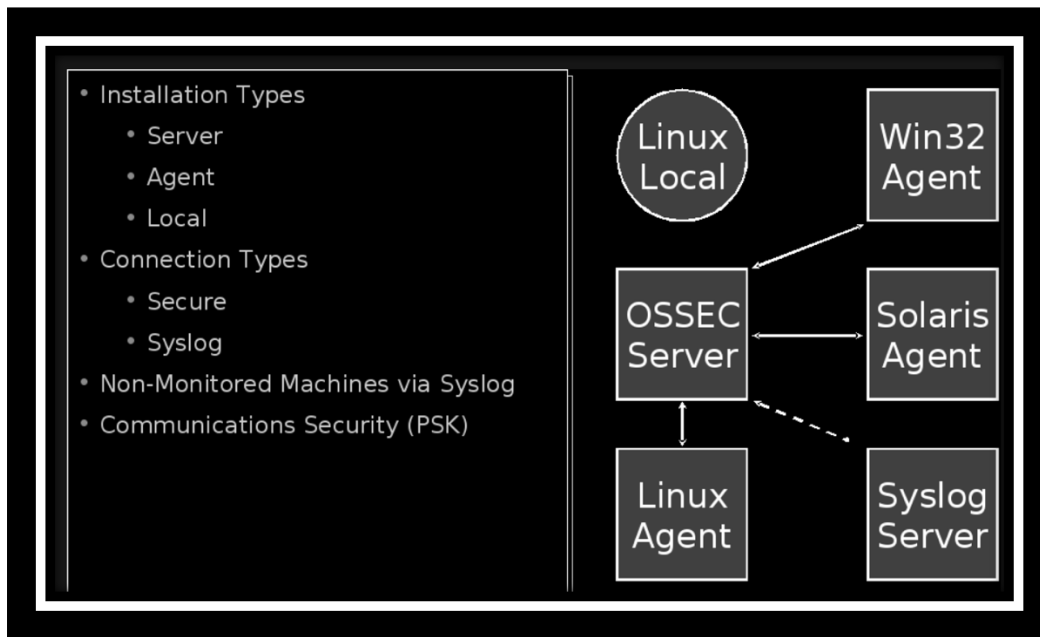
HIDS LOGGFIL OVERVÅKING



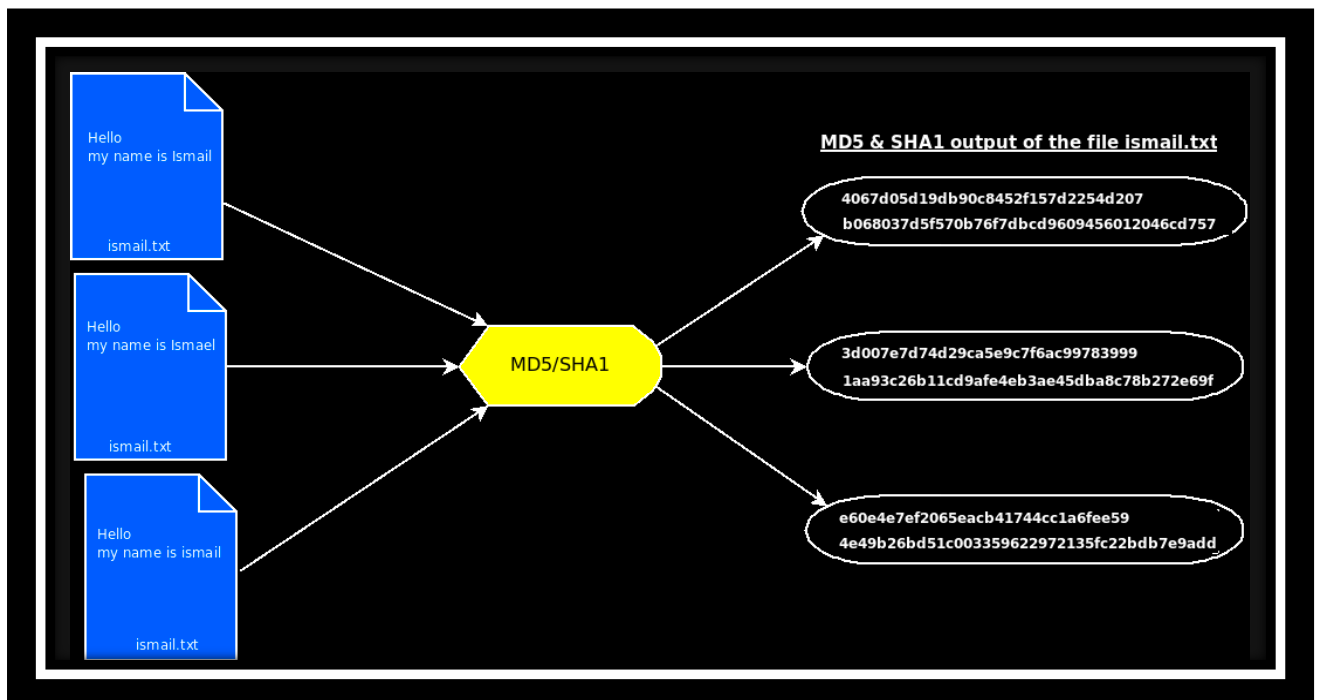
OSSEC

- En åpenkilde HIDS. Utfører logganalyse, integritetssjekk, Windows registrerings overvåking, sanntid varslinger og aktive respons. Kjøres på fleste os (Linux, Open BSD, FreeBSD, solaris, Windows, MacOS)

OSSEC ARKITEKTUR



HASH FEATURES OG INTEGRITETS SJEKKING



AKTIV SVAR (INNTRENGER FORHINDRING)

Aktiv respons gir deg muligheten til å automatisk utføre kommandoer eller svar når en bestemt hendelse eller en serie hendelser blir utløst.

OSSEC KAN TRIGGE BRANNMUREN TIL Å STOPPE ET ANGREP!

NETWORK INTRUSION DETECTION SYSTEM (NIDS)

- Nettverksbasert IDS (NIDS) overvåker trafikk på bestemte punkter på ett eller flere nettverk
- NIDS undersøker all trafikk (alle pakker) i sanntid eller så likt som mulig sanntid, for å prøve å oppdage alle innbruddsmønstre
- Med økt bruk av kryptering utover TLS/SSL, SSH IPsec(VPN), har NIDS mistet tilgang til innholdet av pakkene, som hindrer deres evne til å fungere ordentlig
 - o NIDs har fremdeles en viktig rolle å spille og kan være en del av IDS løsning for en organisasjon

SNORT

- Snort er en åpenkilde NIDS
- Snort er signatur basert og bruker regler til å analysere nettverkstrafikken
- Snort kan funksjonere som en IPS gjennom snort inline
- Snort kan kjøres i fire modus henholdsvis:
 - o Sniffer

► Using the following command, Snort will be put in sniffer mode:

Eksempel

```
snort -vde
```

- v Prints to the screen (default just the header)
- e Adds the data link layer header with MAC-addresses (red/boldface font)
- d Adds the content of the packet (blue/emphasized font)

```
=====
05/14-11:31:20.118697 0:0:C:5A:CD:90 -> 1:0:5E:0:1:16 type:0x800 len:0x62
158.36.146.200:427 -> 224.0.1.22:427 UDP TTL:30 TOS:0x0 ID:1792 IpLen:20 DgmLen:84
Len: 56
01 01 00 38 00 00 65 6E 00 03 92 FA 00 00 00 28 ...8 .en.....(
42 69 6E 64 65 72 79 2E 4E 6F 76 65 6C 6C 2F 2F Bindery NovelW/
28 53 56 43 4E 41 4D 45 2D 67 53 3D 3D 50 35 32 (SVCNAME:WS==P52
=====
```

- o Packet Logger

- If you provide a directory as an option, Snort will log all packages in this directory and create a directory hierarchy:

Eksempel

```
snort -l /var/log/snort
```

```
ls -l /var/log/snort
```

```
drwx--S--- 2 root  snort  4096 May 19 12:01 128.39.89.10
drwx--S--- 2 root  snort  4096 May 19 12:01 129.241.92.150
drwx--S--- 2 root  snort  4096 May 19 12:01 158.36.161.202
```

```
ls -l /var/log/128.39.89.10
```

```
-rw----- 1 root  snort  3793 May 19 12:04 TCP:38293-2003
-rw----- 1 root  snort  1489 May 19 12:04 UDP:2049-790
-rw----- 1 root  snort  2010 May 19 12:04 UDP:2049-791
```

- NIDS

Bruker alle snort fraser og plug-ins for å analysere nettverkstraffik for begge misbruks oppdagelse

Snort i NIDS modus kan: port-skanne, IP defragmentere, TCP stream, reassembly, applikasjons layer analysere og normalisere, etc..

- IPS

Snort i NIDS modus vil bare logge til nettverkstrafikk og sende asvarsel hvis et angrep er oppdaget, men med snort inline vil det også være kunne mulig å blokkere angrepet grunnet regler satt opp av administratorer gjennom Linux brannmunerer (iptables).

Bruker iptables isteder for libpcap for å fange pakker

Bruker spesielle regler for å blokkere trafikk gjennom iptables