

Eindpresentatie

J.E. Barhorst

W. Coene

J.C.J. van Dam

M.P. Rijkeboer

19 januari 2004

7^{de} semester project: Intrusion Detection Systems

Inhoud

- Algemeen
- Host Intrusion Detection
- Network Intrusion Detection
- Alerting
- Conclusie

Aanleiding

- Gemeenschappelijke interesse in beveiliging
- Onvrede over beveiliging bestaande netwerken

Definitie Beveiliging

- Proactief
- **Reactief**
- Fysiek
- **Electronisch**

Host Intrusion Detection

Monitoren?

Wel:

- Programmatuur, libraries
- Configuratiebestanden

Niet:

- Logbestanden
- Gebruikersdirectories

AIDE

Voordelen:

- Werkt op alle Unices
- Vrij beschikbaar

Nadelen:

- Recursie niet apart aan te zetten

mtree

Voordelen:

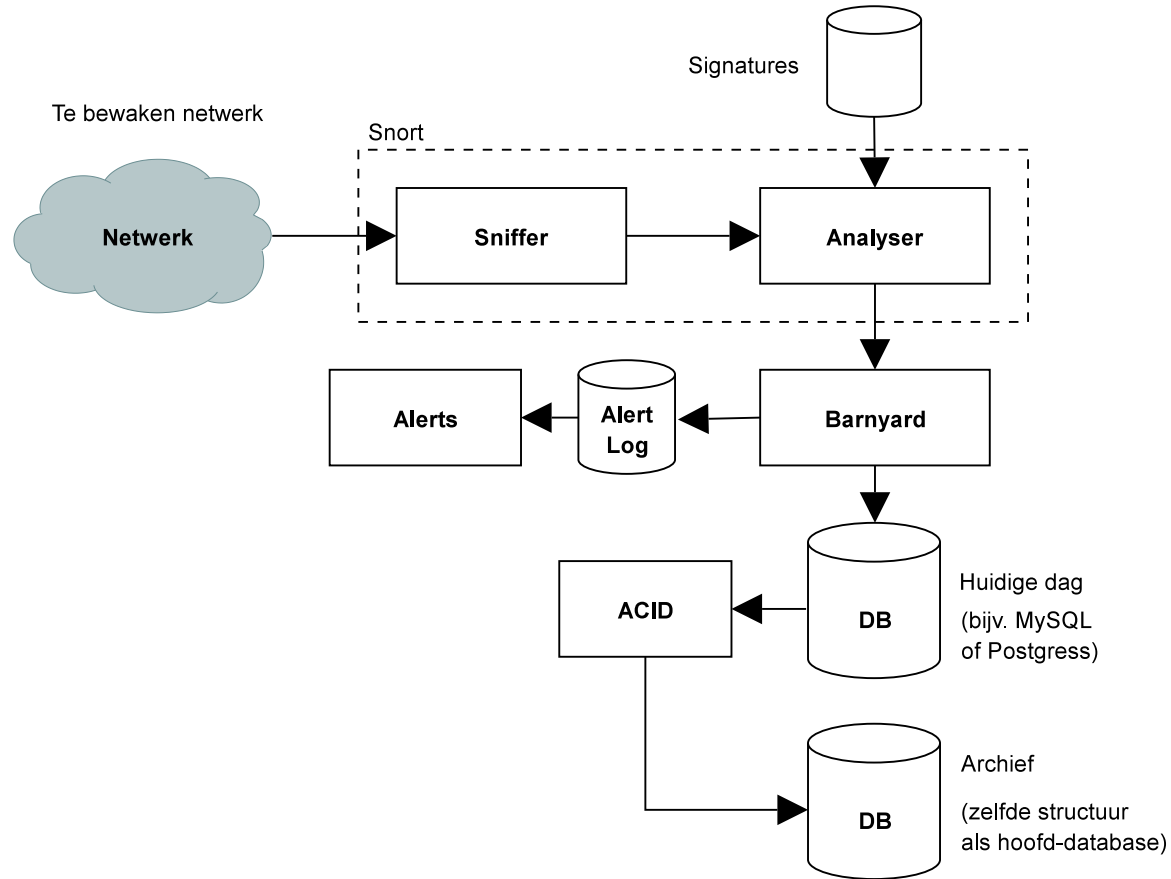
- Standaard in veel Unices

Nadelen:

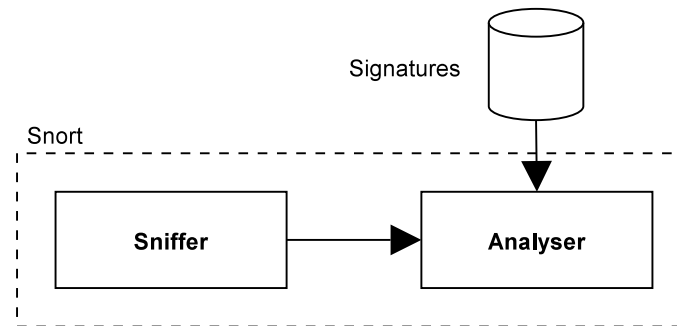
- Recursie niet te stoppen
- Voor nuttig gebruik, scripts nodig

Network Intrusion Detection

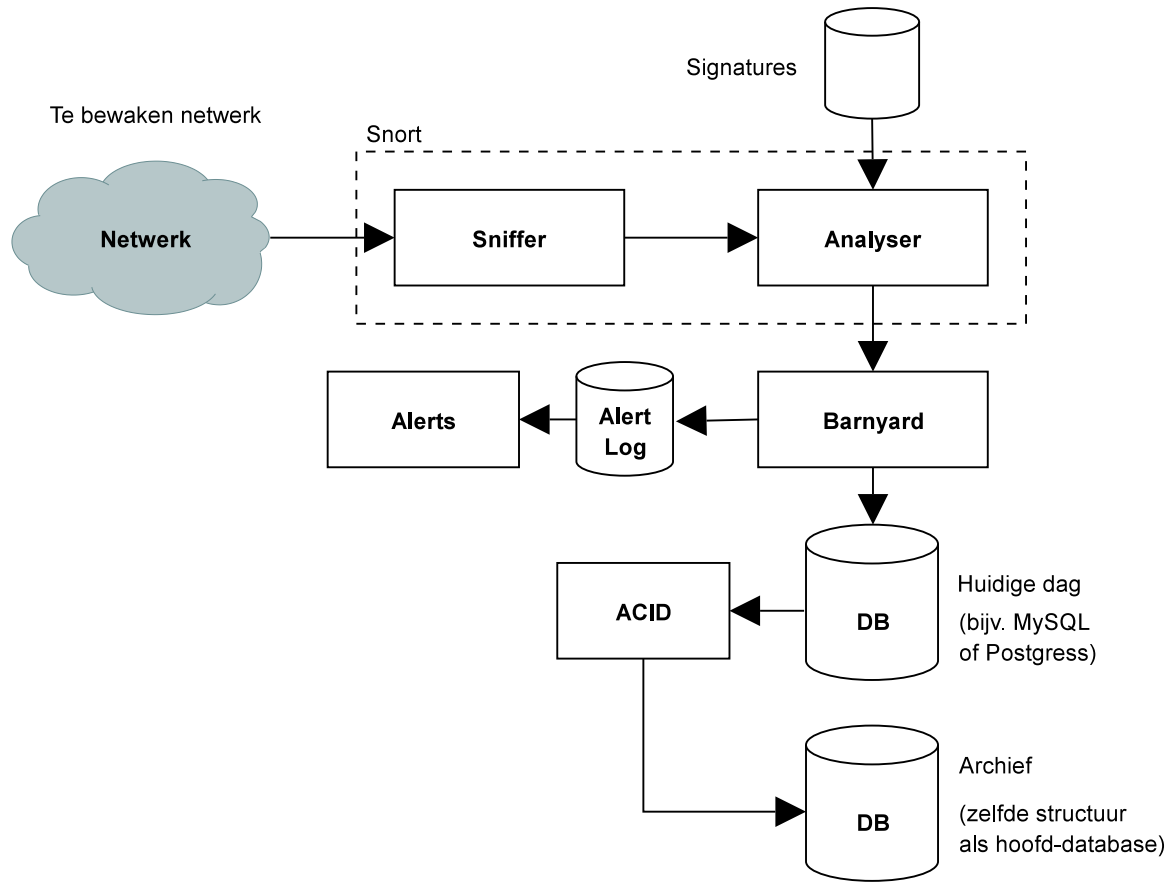
Snort, Barnyard & ACID



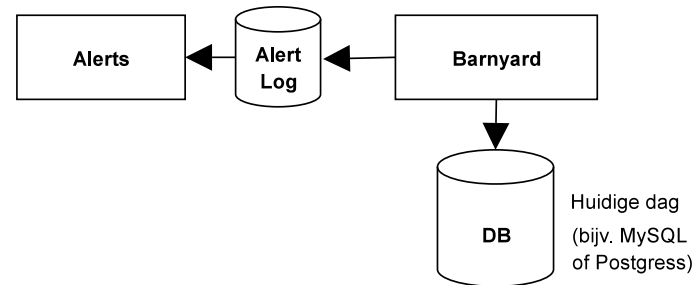
Snort



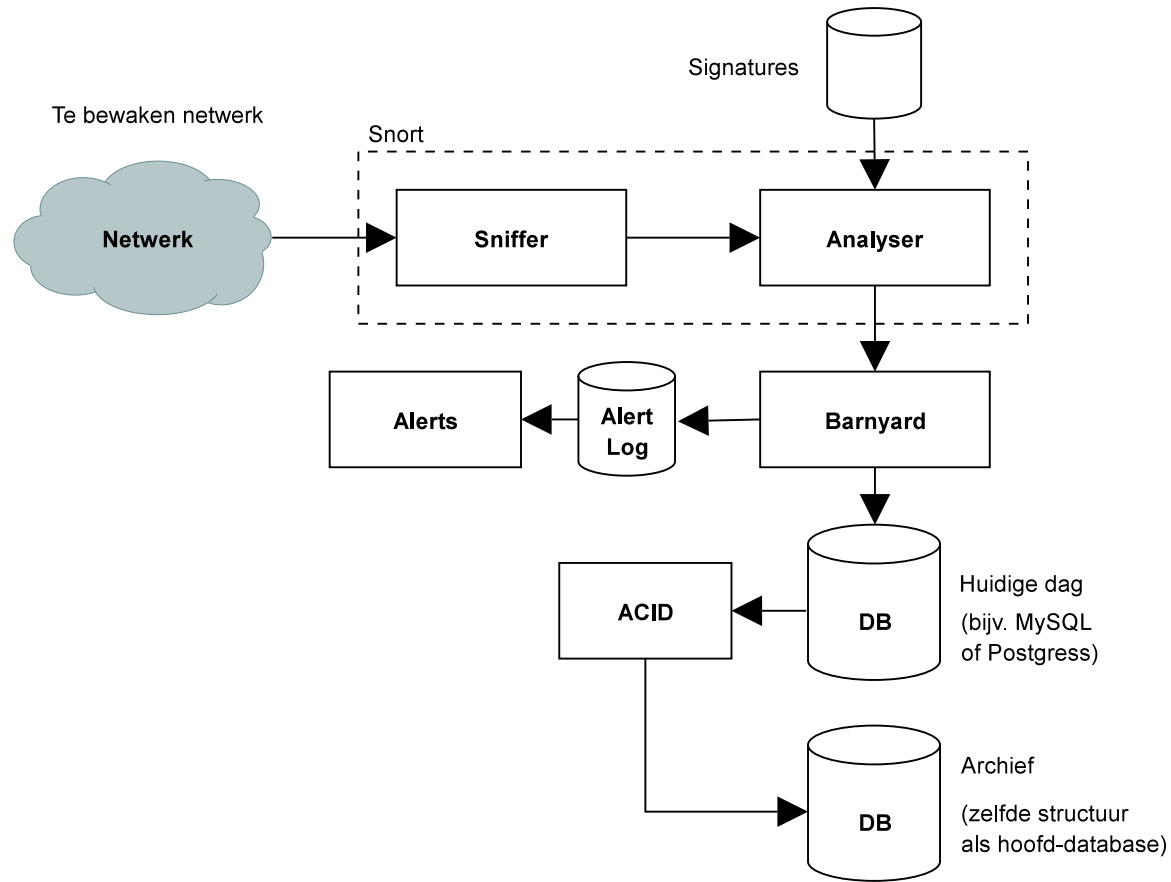
- Sniffer: netwerkverkeer doorsluizen naar Analyser
- Analyser: eventueel eerst door een preprocessor, daarna vergelijken met *signatures*



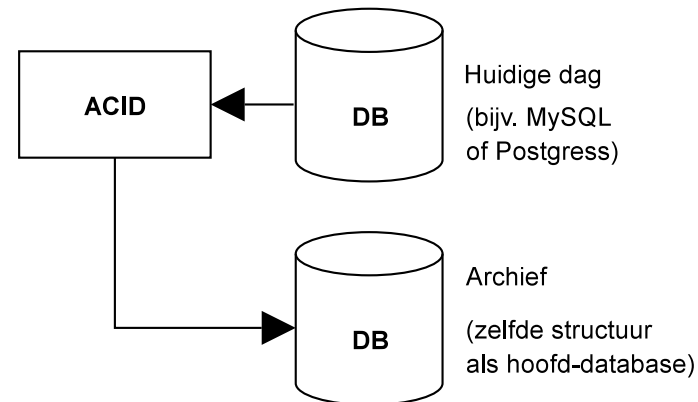
Barnyard



- Verwerkt de resultaten van de Analyser
- Slaat verdacht netwerkverkeer op in een database
- Alerts worden in een aparte database opgeslagen

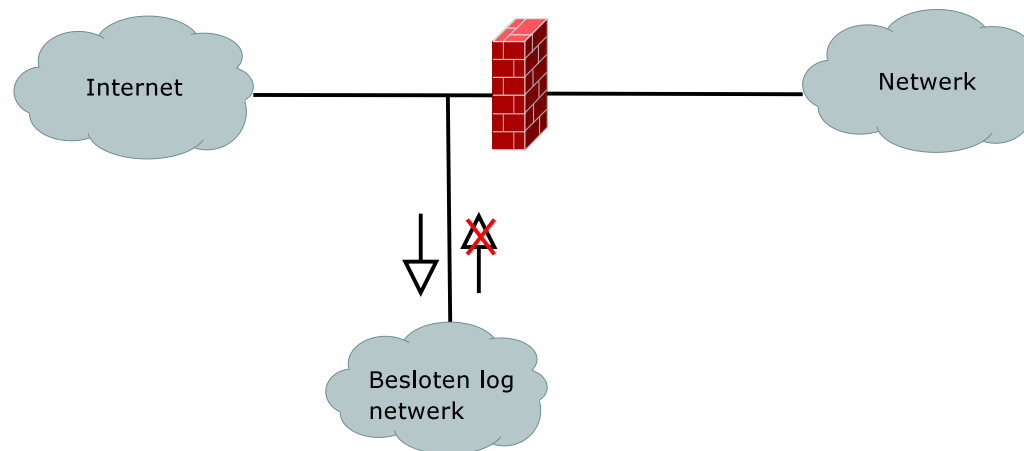


ACID



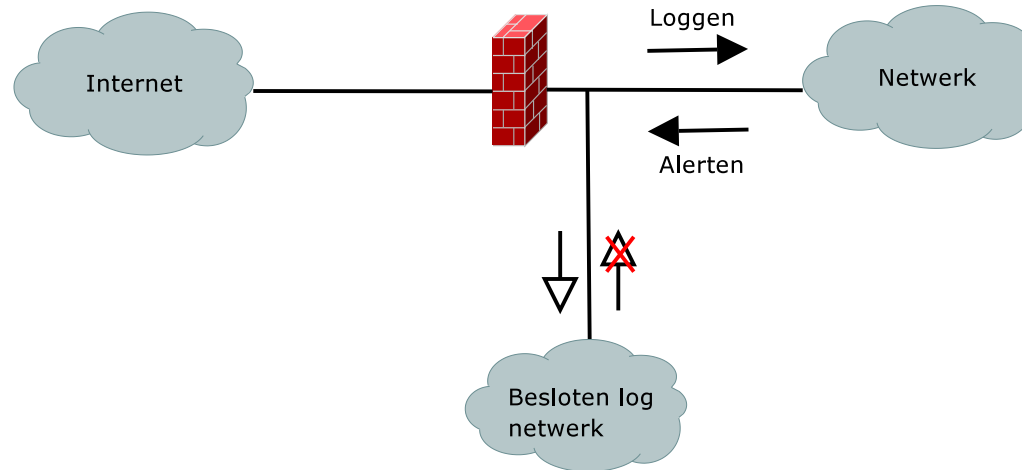
- "Analysis Console for Intrusion Databases"
- Doorzoeken & verwerken logbestanden
- Tevens inzetbaar voor diverse firewalls

Hoe het beste toe te passen



- NIDS voor firewall
- Snot

Hoe het beste toe te passen



- NIDS achter firewall
- Loggen ingaand verkeer, alerten uitgaand verkeer
- Combinatie HIDS

Communitie en updates

- Founder: Martin Roesch
- Signatures
- Update
 - Performance
 - Exploits
 - Verminderen false positives

Alerting

Wat is een alert?

- Kort bericht
- Belangrijk
- Niet kunnen tegenhouden

E-mail

Voordelen:

- Makkelijke integratie
- Standaard hardware

Nadelen:

- Plat te leggen
- Bericht moet gelezen worden

SMS

Voordelen:

- Apart netwerk
- Komt direct aan (met geluidssignaal)

Nadelen:

- Extra hardware (GSM) nodig
- Beperkte lengte bericht

Resultaten

- Zowel E-mail als SMS voor- en nadelen
- Combinatie van beiden

“*Cry Wolf*”-probleem

- Te veel alerting
- Alleen bij concrete dreiging

Conclusie

Conclusie

- Goede aanvulling op proactieve beveiliging
- Niet makkelijk op te zetten
- Beveiliging is een continu-proces

Einde Presentatie

Zijn er nog vragen?