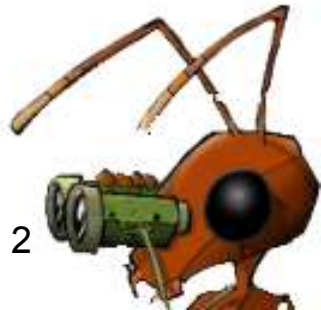
Welkom

Intrusion Detection Systems:
Snort & Prelude

Arjan Dekker en Carlos Groen

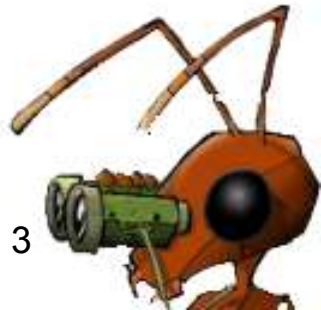
Inhoud

- Intrusion Detection
- IDS tools
- Eisen en wensen
- Bevindingen
- Implementaties
- Conclusie en aanbevelingen
- Vragen



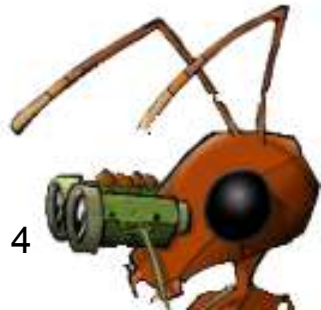
Intrusion Detection

- Inbraakpogingen detecteren
- Zien wat er speelt (virussen etc)
- Reactief maatregelen nemen
- Proactief maatregelen nemen



Intrusion Detection

- Network-IDS (NIDS)
  - Netwerkverkeer sniffen en pakketinhoud vergelijken met rules.
- Host based-IDS (HIDS)
  - Loganalyse
  - File integriteit
  - Connecties
  - Processen



IDS Tools

NIDS

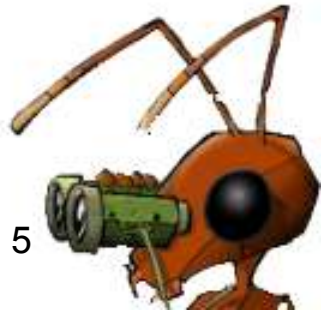
- Snort

HIDS

- Logwatch, Logcheck
- Samhain, Tripwire
- PortSentry

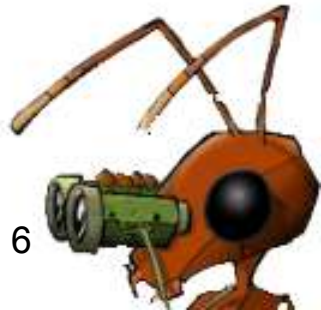
HyIDS

- Prelude



Eisen en Wensen

- Network- en Host-based IDS
- Centrale registratie
- Centrale configuratie
- Rapportage
- Notificaties
- Informatie delen
- Aanknopingspunten IPS

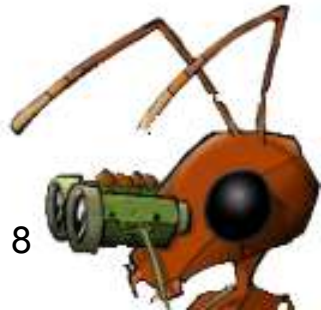


NIDS en HIDS

- Waarom:
  - Vullen elkaar aan
  - Meer detectie
- Punten:
  - Plaatsing
  - Besturingssystemen
  - Typen
- Snort/Prelude

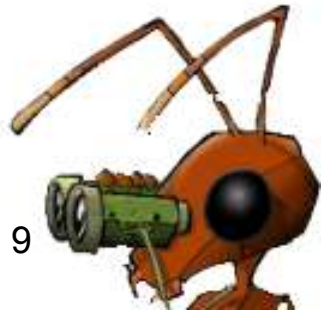
Centrale registratie

- Waarom:
  - Verbanden
  - Early warning
- Punten:
  - Centraal/Lokaal
  - Waar filteren
  - Realtime
- Snort/Prelude



Centrale configuratie

- Waarom:
  - Sneller/eenvoudiger
  - Overzicht
- Punten:
  - Verschillende sensoren
  - Verschillende policies
- Snort/Prelude



Rapportage

- Waarom:
  - Overzicht
  - Verbanden
- Punten:
  - Verschillende formaten
  - Wat rapporteren
- Snort/Prelude

Notificatie

- Waarom:
  - Waarschuwen
- Punten:
  - Methoden
  - Classificatie
  - Interval
- Snort/Prelude

Informatie delen

- Waarom:
  - Beeldvorming
  - Proactief
- Punten:
  - Web of trust
  - Decentraal
  - Centraal
- Snort/Prelude

Aanknopingspunten IPS

- Waarom:
  - Automatisch blokkeren
- Punten:
  - Criteria
  - Whitelists
  - Methodes
- Snort/Prelude

Implementaties

- Prelude
- Snort met externe HIDS tools
  - Met remote Syslog
  - Met remote MySQL
  - Met lokale opslag en scripts

Conclusie

- Prelude nog te onvolwassen
- Snort met externe HIDS tools
- IPS verder onderzoeken

Vragen ???