

Presentatie Plan van Aanpak

J.E. Barhorst W. Coene J.C.J. van Dam
M.P. Rijkeboer

9 oktober 2003

7^{de} semester project: Intrusion Detection Systems

Aanleiding

- Gemeenschappelijke interesse in beveiliging
- Onvrede over beveiliging bestaande netwerken

7^{de} semester project: Intrusion Detection Systems

1

Definitie beveiliging

- **Proactief**
(voorkomen; bijv. uitgifte van sleutels)
- **Reactief**
(administreren; bijv. camera's, actie ondernemen)

7^{de} semester project: Intrusion Detection Systems

2

Typen beveiliging

- Host beveiliging
 - Fysiek
 - **Electronisch**
- Netwerk beveiliging
 - Fysiek
 - **Electronisch**

7^{de} semester project: Intrusion Detection Systems

3

Relevantie

- Netwerkbeheerders
- Beleidsmedewerkers
- Beveiliging van netwerken

Uitgangssituatie

- Openheid en relatieve anonimiteit van het Internet
- Behoeftte voor beveiliging
- Firewall is niet de volledige oplossing

Wat is een IDS?

Intrusion Detection System:

- Detecteren van inbraken
- Loggen van verdachte activiteiten
- Inlichten van beheerders

Hoe werkt een IDS?

- Analyseren van activiteiten
- Bewaren van relevante oude data

Gekozen software

- **Server OS:** OpenBSD
- **Network IDS:** Snort
- **Host IDS:** AIDE

Waarom OpenBSD?

- Open Source & gratis
- Focus op beveiliging
- Bruikbaar op veel platformen

Waarom Snort?

- Open Source & gratis
- Veel toegepast
- Flexibel
- Uitgebreid

Waarom AIDE?

- Open Source & gratis
- Vrij standaard
- Makkelijk te integreren

De opdracht

“Onderzoek en test de mogelijkheden van een Intrusion Detection System op individuele hosts en binnen een netwerk infrastructuur.”

- Meerlaags beveiligingssysteem
- Toepassingsvoorstel

Doelstelling

- Opbouwen van kennis
- Ontwikkelen van een demonstratieomgeving

Reikwijdte

Wat valt er binnen?

- Algemene oplossingen om inbraken te detecteren op netwerken en hosts
- Demonstratieomgeving opbouwen

Reikwijdte

Wat valt er buiten?

- Beveiligen van individuele software pakketten
- Adviezen over beveiliging schoolnetwerk
- Installatiehandleidingen opstellen voor besturings-systemen

Producten

- Plan van Aanpak
- Demonstratieomgeving
- Toepassingsvoorstel
- Projectverslag

Methoden, technieken en standaarden

- Typesetting: \LaTeX
- Versiebeheer: CVS
- Backupstrategie

Projectmanagementmethodiek

Extreme Programming:

- Programmeermethode
- *“Pair Programming”*
- Kwaliteit

Meer info: <http://www.extremeprogramming.org/>

Fasering en planning

Onderdeel	Tijdsduur
Inrichting projectruimte	± 300 uur
Opstellen PvA	± 200 uur
Inwerken gekozen software	± 200 uur
Opzetten demonstratieomgeving	± 540 uur
Opstellen toepassingsvoorstel	± 420 uur
Opstellen projectverslag	± 420 uur

Samenwerking en taakverdeling

- Gezamenlijke verantwoordelijkheid
- Projectruimte
- Veel face-to-face communicatie

Communicatie en rapportage

- Wiki
- Werkoverleg
 - onderling
 - met begeleider
- Verslagen

Einde presentatie

Zijn er nog vragen?