SURFnet Intrusion Detection System (IDS)

Inleiding over SURFnet

SURFnet is een hoogwaardig computernetwerk speciaal voor het hoger onderwijs en onderzoek in Nederland. Studenten en medewerkers van aangesloten organisaties kunnen via SURFnet communiceren met andere internetgebruikers. Door voortdurende innovatie heeft SURFnet één van de meest geavanceerde netwerken ter wereld met filevrije verbindingen naar de belangrijkste Nederlandse, Europese en transatlantische netwerken. Naast snelheid staan ook de betrouwbaarheid en veiligheid van het netwerk hoog in het vaandel.

Aangesloten instellingen bij SURFnet zijn universiteiten, hogescholen, research instellingen, academische ziekenhuizen en overige onderwijsinstellingen. In totaal heeft SURFnet 150 instellingen aangesloten.

SURFnet b.v. is een not-for-profit bedrijf dat voortdurend werkt aan het verbeteren van de netwerkinfrastructuur en het ontwikkelen van nieuwe toepassingen, waardoor gebruikers snellere en betere toegangsmogelijkheden krijgen tot nieuwe internetdiensten

Inleiding over het project Intrusion Detection System
SURFnet heeft binnen het SURFworks Next Generation jaarplan 2005 een project geformuleerd waarin SURFnet een Intrusion Detection System (IDS) van sensornetwerken gaat opzetten. Dit IDS zal uit verschillende sensoren bestaan die verspreid kunnen worden binnen de netwerken van de aangesloten instellingen. Door deze verspreiding kan er een duidelijke analyse worden opgesteld over een bepaald type kwaadaardig verkeer zich heeft verspreid binnen SURFnet en welke aangesloten instellingen er in meer of mindere mate hinder van ondervinden. Vervolgens zullen de aangesloten instellingen geïnformeerd worden over de analyses.

Doelstellingen

• Het opzetten van een schaalbare infrastructuur waarbinnen SURFnet bij aangesloten instellingen sensoren kan plaatsen.
• Het ontwikkelen van een sensor die onderhoudsvrij is en die SURFnet eenvoudig bij aangesloten instellingen kan installeren.
• Het ontwikkelen van een centrale analyse tool die per aangesloten instelling onder andere statistieken laat zien.

Stage en/of afstudeer mogelijkheden

De eerste fase van het project bestaat uit het ontwerpen en ontwikkelen van de vereiste sensorsoftware. De volgende fases bestaan uit de ontwikkeling van de centrale analyse tool en het testen van het IDS. Voor alle fases zoekt SURFnet naar studenten die bereid zijn als stageopdracht hiermee aan de slag te gaan.

In de eerste fase moet er een ontwerp gemaakt worden voor de sensor. Deze sensor moet voldoen aan de volgende criteria:
-zero maitenance, zodat de sensor eenvoudig bij elke bij SURFnet aangesloten instelling geïnstalleerd kan worden
-schaalbaarheid moet in orde zijn. Het moet mogelijk zijn om meer dan 100 sensoren te gebruiken
-de sensor moet de optie hebben om ruwe netwerkdata te verzamelen
-de sensor moet de netwerkdata doorsturen naar de centrale server

In eerste kwartaal van 2005 is er door SURFnet onderzocht of "standaard" applicaties niet ingezet kunnen worden als sensor. De uitkomst van dit onderzoek was dat dit niet het geval was. Wel is het naar verwachting mogelijk om componenten van pakketten zoals snort, tcpdump en acid in te zetten. Daarnaast lijkt Knoppix, een van cd bootable linux OS, een interessante oplossing om als sensor in te richten.

Zoals hierboven staat vermeld is er bij SURFnet b.v. nader gekeken naar de wijze waarop een IDS ingericht kan worden, maar op dit moment staat de daadwerkelijke invulling nog geheel open. Een student krijgt dan ook de mogelijkheid om met eigen ervaring en inzicht tot een werkbare oplossing te komen.

Benodigde ervaring student

Een student dient ervaring te hebben met linux en scripting onder linux.
Ervaring met tools zoals snort, acid, argus en tcpdump is een pré.