

Projectverslag
7^{de} semester project: Intrusion Detection Systems

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

8 januari 2004

Voorwoord

Dit rapport bevat het projectmatige deel van de rapportage van het 7^{de} semester project *Intrusion Detection Systems*. Dit project is uitgevoerd door studenten Hogere Informatica aan de Hogeschool van Utrecht.

Lezers geïnteresseerd in het deel van de rapportage welke de technische uitkomsten en het toepassingsvoorstel behandelen worden verwezen naar het Technisch Verslag.

De projectgroep wil in het bijzonder Dhr. L.J.M. van Moergestel en Dhr. A. van Doesburg bedanken voor toestaan van en het ondersteunen bij het zelfstandig opstellen van een projectopdracht.

Inhoudsopgave

1	Inleiding	3
1.1	Uitgangssituatie	3
1.2	Aanleiding	3
1.3	Relevantie	3
1.4	Definities	4
2	Doelstelling en probleemstelling	5
2.1	Doelstelling	5
2.2	Probleemstelling	5
3	Opgeleverde producten	6
3.1	Plan van Aanpak	6
3.2	Demonstratieopstelling	6
3.3	Technisch verslag	6
3.4	Projectverslag	6
4	Projectarchief	7
5	Planning	8
5.1	Opstart fase	8
5.1.1	Inrichting projectruimte	8
5.1.2	Opstellen Plan van Aanpak	8
5.2	Hoofd fase	9
5.2.1	Inwerken in Gebruikte software	9
5.2.2	Bouwen demonstratieopstelling	9
5.3	Afsluitende fase	9
5.3.1	Opstellen Technisch Verslag	9
5.3.2	Opstellen Projectverslag	10
5.3.3	Eind presentatie	10
5.4	Overigen	10
6	Projectorganisatie	11

7	Kostenverantwoording	12
7.1	Uren	12
7.1.1	J.E. Barhorst	12
7.1.2	W. Coene	15
7.1.3	J.C.J. van Dam	18
7.1.4	M.P. Rijkeboer	20
7.2	Faciliteiten	22
8	Evaluatie	23
9	Conclusie	25
A	Versies	26

Hoofdstuk 1

Inleiding

1.1 Uitgangssituatie

Veel bedrijven en instellingen hebben tegenwoordig een open internet verbinding om hun medewerkers en/of servers toegang op en vanaf het internet te geven. Echter, wanneer een dergelijke verbinding niet goed beveiligd is kan dat erg gevaarlijk zijn, aangezien er mogelijk ingebroken kan worden op de systemen van de organisatie en er vitale gegevens op straat kunnen komen te liggen. Een goede oplossing hiervoor is het gebruik van een firewall welke veel ongewenst verkeer buiten het netwerk kan houden. Hiermee zijn al een hoop pogingen tot inbraak op het netwerk af te slaan, maar lang niet alles. Voor dit soort zaken zou een Intrusion Detection Systeem in gebruik genomen kunnen worden. Helaas zijn er nog maar weinig organisaties die gebruik maken van een dergelijk systeem.

1.2 Aanleiding

De aanleiding voor dit project is tweeledig. Ten eerste onze gemeenschappelijke interesse voor netwerken en aan beveiliging gerelateerde zaken. Ten tweede onze onvrede over de slechte beveiliging van een groot aantal netwerken.

1.3 Relevantie

Voor eenieder die een netwerk beheerd waarover hij voor een gedeelte of voor het geheel geen controle bezit, maar wel een afdoende beveiliging wil bieden voor het deel waar hij wel controle over heeft. Een voorbeeld hiervan zijn onderzoeksnetwerken.

1.4 Definities

Beveiliging Het afschermen of monitoren van een geheel met als doel het buitenhouden van ongeautoriseerde personen of organisaties. Beveiliging valt uiteen in twee vormen, zijnde proactieve en reactieve beveiliging.

Intrusion Detection System Een reactief beveiligingssysteem voor losse systemen of een netwerk als geheel verstaan.

Meerlaags beveiligingssysteem Een systeem waarbij beveiliging van zowel individuele hosts als netwerken aan bod komen.

Netwerkbeveiliging Het fysiek of elektronisch beveiligen van een netwerk, waarbij weinig tot geen rekening wordt gehouden met de individuele computersystemen.

Proactieve beveiliging Het voorkomen van ongeautoriseerde toegang, zoals bijvoorbeeld de gecontroleerde uitgifte van een sleutel tot een ruimte, of het dichtzetten van bepaalde netwerkpoorten.

Reactieve beveiliging Het detecteren en signaleren van ongeautoriseerde toegang, bijvoorbeeld met behulp van een gesloten camerasysteem of het af luisteren en analyseren van netwerkverkeer.

Systeembeveiliging Het fysiek of elektronisch beveiligen van een enkel computersysteem, waarbij weinig tot geen rekening wordt gehouden met de eventuele netwerkverbindingen van dat computersysteem.

Hoofdstuk 2

Doelstelling en probleemstelling

2.1 Doelstelling

Het opbouwen van kennis en het onderzoeken van mogelijkheden op het gebied van Intrusion Detection Systems. Daarnaast het opzetten van een omgeving om eventueel demonstraties te kunnen geven op het gebied van Intrusion Detection Systems.

2.2 Probleemstelling

Hoe en in hoeverre kan een Intrusion Detection System positief bijdragen aan de beveiliging van een netwerk omgeving?

Hoofdstuk 3

Opgeleverde producten

3.1 Plan van Aanpak

Er is een Plan van Aanpak voor het project geschreven, aan de hand van de richtlijnen van de Hogeschool van Utrecht. Dit Plan van Aanpak is gepresenteerd op 9 oktober 2003.

3.2 Demonstratieopstelling

Er is een demonstratieopstelling gebouwd, waarmee verschillende aspecten van Intrusion Detection Systems worden gedemonstreerd. Deze opstelling is op papier uitgewerkt en terug te vinden in het Technisch Verslag.

3.3 Technisch verslag

Aan de hand van bevinding van het project is er een Technisch Verslag voor de implementatie van een Intrusion Detection System voor een klein tot middelgroot onderzoeksnetwerk gemaakt. Dit verslag omvat ondermeer het toepassingsvoorstel.

3.4 Projectverslag

Aan de hand van de bevindingen van het project is dit Projectverslag geschreven. Dit verslag wordt tezamen met het Technisch verslag gepresenteerd.

Hoofdstuk 4

Projectarchief

Alle versies van producten, verslagen en configuratiebestanden zijn in het systeem dossier opgeslagen. Dit systeem dossier is gevormd door een speciaal daarvoor bestemd versiebeheersysteem, te weten CVS. Van dit systeem zijn regelmatig backups gemaakt om verlies van belangrijke gegevens te voorkomen.

Alle beslissingen en andere administrativa welke betrekking hebben op het project zelf zijn opgeslagen in het project dossier, wat gevormd wordt door een Wikisysteem. Zie voor meer informatie het Plan van Aanpak, hoofdstuk Communicatie.

Deze beide dossiers worden aan het einde van het project op een CD-ROM aan de opdrachtgever ter beschikking gesteld.

Hoofdstuk 5

Planning

Wij hebben de opdracht in drie fasen verdeeld. Deze fasen zijn vervolgens weer in subfasen onder verdeeld.

5.1 Opstart fase

5.1.1 Inrichting projectruimte

Resultaten:

- Een werkbare inrichting van de projectruimte conform de wensen van de projectleden en de ARBO¹-wetgeving;
- een computerinfrastructuur waarbinnen het project goed uitgevoerd kan worden;
- onbeperkte toegang tot het Internet aangezien deze wereldwijde informatiebron onmisbaar is voor de correcte uitvoering van het project.

Geplande tijd: \pm 300 uur.

Besteedde tijd: 317 uur.

5.1.2 Opstellen Plan van Aanpak

Resultaten:

- Plan van Aanpak waarin algemene zaken worden omschreven, zoals de op te leveren producten, randvoorwaarden, succesfactoren, kostenschatting en een globale planning;

¹Arbeids Omstandigheden Wet, ook van toepassing op studenten.

- presentatie van het Plan van Aanpak, waar in de begeleiding er van moet worden overtuigt dat het project voortgezet kan worden.

Geplande tijd: \pm 200 uur.

Besteedde tijd: 224 uur.

5.2 Hoofd fase

5.2.1 Inwerken in Gebruikte software

Resultaten:

- Kennis van het opzetten en configureren van de Gebruikte software.

Geplande tijd: \pm 200 uur.

Besteedde tijd: 208 uur.

5.2.2 Bouwen demonstratieopstelling

Resultaten:

- Een demonstratieopstelling zoals beschreven in het Technisch verslag;
- mogelijkheden en onmogelijkheden van de Gebruikte software onderzoeken;
- een verslag van de bouw van deze opstelling, zie toepassingsvoorstel.

Geplande tijd: \pm 540 uur.

Besteedde tijd: 416 uur.

5.3 Afsluitende fase

5.3.1 Opstellen Technisch Verslag

In het Plan van Aanpak werd gesproken over het Opstellen Toepassingsvoorstel als los onderdeel, echter dit is nu onderdeel geworden van het Technisch Verslag.

Resultaten:

- Een technische verslag waarin onze bevindingen op concrete wijze worden weergegeven en er een toepassingsvoorstel wordt gedaan.

Geplande tijd: \pm 420 uur.

Besteedde tijd: 336 uur.

5.3.2 Opstellen Projectverslag

Resultaten:

- Projectverslag conform de standaard die wordt gehanteerd bij de Hogeschool van Utrecht, afdeling ICIM van de faculteit Natuur en Techniek.

Geplande tijd: \pm 420 uur.

Besteedde tijd: 96 uur.

5.3.3 Eind presentatie

Resultatien:

- Voorbereiden van de presentatie;
- presenteren van resultaten;
- verdedigen van resultaten.

Geplande tijd: \pm 0 uur.

Besteedde tijd: 112 uur.

5.4 Overigen

Tijdens het project zijn er een aantal onvoorziene danwel neven activiteiten geweest. Resultaten:

- Voortgangsbesprekingen;
- presentatie aan eerste jaars TBK (26 september 2003);
- projectruimte schoon- en netjes houden;
- opleveren projectruimte (week 2.8);
- NLUUG Conferentie (6 november 2003);
- KickIT Event 2003 (27 november 2003);
- HCC Dagen 2003 (28 november 2003);

Geplande tijd: \pm 0 uur.

Besteedde tijd: 290 uur.

Hoofdstuk 6

Projectorganisatie

De bedrijfsopdrachtgever van dit project was Dhr. A. van Doesburg en de schoolbegeleider was Dhr. L.J.M. van Moergestel, beiden als docent verbonden aan de Hogeschool van Utrecht, Faculteit Natuur & Techniek.

De projectleider, Martijn P. Rijkeboer, is eerste onder gelijken. De overige projectleden waren:

- Jelmer E. Barhorst;
- Wouter Coene;
- Jesse C.J. van Dam.

Alle projectleden hadden de verantwoordelijkheid voor het correct bereiken van de doelstellingen van dit project.

Hoofdstuk 7

Kostenverantwoording

7.1 Uren

Hieronder volgen de urenverantwoordingen per persoon.

7.1.1 J.E. Barhorst

Diversen

Datum	Uren	Omschrijving
juni 2003	16	Voorbereidend overleg

September 2003

Datum	Uren	Omschrijving
woensdag 3	8	Verkrijgen en inrichten/opruimen projectruimte
donderdag 4	8	Overleg met v. Doesburg en v. Moergestel over project en middelen Desktop voorzien van Windows XP installatie Configuratie Baystack switch
woensdag 10	8	Desktop voorzien van Debian installatie (dual-boot) Intern overleg: inleiding door Martijn in Snort bepalen wat er in het PvA komt te staan
donderdag 11	8	Debian installatie verfijnd
vrijdag 12	8	Wavelan d.m.v. accesspoint bridging proberen op te zetten
woensdag 17	8	Plan van aanpak opstellen
donderdag 18	8	PvA verder uitwerken overleg i.v.m. internet verbinding

September 2003

Datum	Uren	Omschrijving
vrijdag 19	8	PvA versie 1 afgemaakt
woensdag 24	8	Permanente internet aansluiting geregeld PvA versie 1 gecorrigeerd
donderdag 25	12	Inlezen in Snort
vrijdag 26	12	Presenteren aan 1e jaars TBK PvA doorlezen
zaterdag 27	5	PvA doorlezen + herzien

Oktober 2003

Datum	Uren	Omschrijving
woensdag 1	8	Inlezen in Snort
donderdag 2	8	Overleg met Dhr v. Doesburg en Dhr v. Moergestel betreffende PvA PvA herzien
woensdag 8	8	PvA + presentatie herzien
donderdag 9	8	PvA presenteren
vrijdag 10	8	SUN's voorzien van OpenBSD
woensdag 22	8	Inlezen Snort
donderdag 23	8	Proef setup Snort op sun + OpenBSD
vrijdag 24	8	Proef setup Snort op Sun + OpenBSD
dinsdag 28	8	Proef setup Snort op Intel + Linux
woensdag 29	8	Ilse met Blaster virus geïnfecteerd
donderdag 30	8	zie de 29e + lange stroomuitval

November 2003

Datum	Uren	Omschrijving
dinsdag 4	8	Diverse andere virussen en trojans geprobeerd
woensdag 5	8	Switch werkend gemaakt
donderdag 6	10	NLUUG conferentie
woensdag 12	8	Voortgangsbespreking + hele middag stroomuitval
donderdag 13	8	testen met Snot, MySQL proberen te versnellen
vrijdag 14	8	Database server voorzien van SCSI schijf Verder testen met Snot
woensdag 19	8	2e sensor op judith, printers FCJ opgezocht, webcam
donderdag 20	8	SMS als alert aan de praat proberen te krijgen
vrijdag 21	8	Opruimen, voorbereiding opendag, webcam
woensdag 26	8	UVIS ALV, eerste aanzet Projectverslag
donderdag 27	8	KickIT evenement, printers FCJ opgezocht
vrijdag 28	8	HCC Dagen

December 2003

Datum	Uren	Omschrijving
dinsdag 2	2	Projectverslag
woensdag 3	8	Projectverslag
donderdag 4	8	Projectverslag
vrijdag 5	8	Projectverslag
woensdag 10	8	Techverslag
donderdag 11	8	Techverslag
vrijdag 12	8	Techverslag
dinsdag 16	8	Techverslag
woensdag 17	8	Techverslag
donderdag 18	8	Techverslag
vrijdag 19	8	Techverslag
maandag 29	8	Doorlezen

Januari 2004

Datum	Uren	Omschrijving
dinsdag 6	8	Projectverslag afmaken
woensdag 7	8	Presentatie maken
donderdag 8	8	Presentatie maken
vrijdag 9	8	Presentatie maken
zondag 18	4	Presentatie voorbereiden
maandag 19	8	Presentatie + projectruimte ontmantelen
dinsdag 20	8	Projectruimte opleveren

7.1.2 W. Coene

Diversen

Datum	Uren	Omschrijving
juni 2003	10	Voorbereiden project

September 2003

Datum	Uren	Omschrijving
woensdag 3	8	Inrichten Projectruimte
donderdag 4	8	Inrichten Projectruimte
vrijdag 5	8	Inrichten Projectruimte
woensdag 10	8	Inrichten Projectruimte
donderdag 11	8	Inrichten Projectruimte
vrijdag 12	8	Inrichten Projectruimte
dinsdag 16	5	Boek over projectmanagement gelezen
woensdag 17	8	Plan van Aanpak
donderdag 18	8	Plan van Aanpak
vrijdag 19	8	Aan presentatie PvA gewerkt
dinsdag 23	7	Aan presentatie PvA gewerkt (thuis)
woensdag 24	8	Aan presentatie PvA gewerkt
donderdag 25	8	Aan presentatie PvA gewerkt
vrijdag 26	8	Systeemonderhoud
zaterdag 27	12	Ingelezen in Snort
zondag 28	7	Ingelezen in Snort
maandag 29	3	Ingelezen in Snort
dinsdag 30	5	Ingelezen in Snort

Oktober 2003

Datum	Uren	Omschrijving
woensdag 1	8	Systeemonderhoud
donderdag 2	8	Plan van Aanpak
vrijdag 3	8	Plan van Aanpak
zaterdag 4	6	Plan van Aanpak (thuis)
maandag 6	4	Plan van Aanpak (thuis)
dinsdag 7	9	Plan van Aanpak (eerst op school, thuis verder)
woensdag 8	8	Plan van Aanpak
donderdag 9	8	Plan van Aanpak gepresenteerd
vrijdag 10	8	Systeemonderhoud
woensdag 22	8	Ingewerkt in AIDE
donderdag 23	8	Systeemonderhoud

Oktober 2003

Datum	Uren	Omschrijving
vrijdag 24	8	Ingewerkt in AIDE
dinsdag 28	8	Ingewerkt in mtree
woensdag 29	8	Aan AIDE gesleutelt
donderdag 30	8	Stroomuitval, systeemonderhoud

November 2003

Datum	Uren	Omschrijving
dinsdag 4	8	Systeemonderhoud
woensdag 5	8	Systeemonderhoud / mtree
donderdag 6	10	Conferentie beveiliging NLUUG
vrijdag 7	12	Aan AIDE gesleutelt (thuis)
woensdag 12	8	Stroomuitval
donderdag 13	8	Assistentie bij NIDS deel
vrijdag 14	8	Assistentie bij NIDS deel / Systeemonderhoud
woensdag 19	8	Lekke printers proberen te misbruiken
donderdag 20	8	SMS alerting
vrijdag 21	8	Systeemonderhoud
woensdag 26	8	Systeemonderhoud
donderdag 27	8	KickIT
vrijdag 28	8	HCC Dagen

December 2003

Datum	Uren	Omschrijving
woensdag 3	8	Technisch Verslag
donderdag 4	8	Projectverslag / Technisch Verslag
vrijdag 5	8	Technisch Verslag
dinsdag 9	12	Boek over rapportagetechnieken gelezen
woensdag 10	8	Technisch Verslag
donderdag 11	8	Technisch Verslag
vrijdag 12	8	Technisch Verslag
zaterdag 13	12	Boek over rapportagetechnieken gelezen
dinsdag 16	8	Technisch Verslag
woensdag 17	8	Technisch Verslag
donderdag 18	8	Technisch Verslag
vrijdag 19	8	Technisch Verslag

Januari 2004

Datum	Uren	Omschrijving
zaterdag 3	5	Technisch Verslag (thuis)
dinsdag 6	8	Technisch Verslag / Projectverslag
woensdag 7	8	Gewerkt aan eindpresentatie
donderdag 8	8	Gewerkt aan eindpresentatie
vrijdag 9	8	Gewerkt aan eindpresentatie
zaterdag 18	3	Eindpresentatie voorbereiden
maandag 19	8	Eindpresentatie / Projectruimte Opruimen
dinsdag 20	8	Projectruimte Upruimen

7.1.3 J.C.J. van Dam

Diversen

Datum	Uren	Omschrijving
juni 2003	15	Voorbereidend overleg + andere voorbereidingen

September 2003

Datum	Uren	Omschrijving
woensdag 3	8	Regelen van faciliteiten
donderdag 4	8	Inrichten en opruimen projectruimte
vrijdag 5	8	Installeren workstation
woensdag 10	12	Inwerken snort
vrijdag 12	8	Uitzoeken snort en gerelateerde sites
zaterdag 13	10	Uitzoeken snort en communities
woensdag 17	12	Snort documentatie lezen
donderdag 18	8	Maken pva en presentatie pva
vrijdag 19	8	Maken pva en presentatie pva
woensdag 24	8	installeren snort
donderdag 25	10	Uitzoeken snort en bekijken blaster meldingen
vrijdag 26	8	Snort code bekijken en bewerken

Oktober 2003

Datum	Uren	Omschrijving
woensdag 1	8	Onderzoeken snort en de snort code
donderdag 2	8	werken aan snort code en werken aan pva
vrijdag 3	8	bespreken en verbeteren pva
woensdag 8	8	Verbetering presentatie
donderdag 9	12	Presentatie + uitzoeken snort
vrijdag 10	8	SUN's voorzien van OpenBSD voor Snort
woensdag 22	8	Zoeken sparc versie snort + installeren ilse
donderdag 23	8	Zoeken trojans en virussen
vrijdag 24	6	Proef snort op sun + OpenBSD → *fail*
dinsdag 28	8	Proef snort virussen en snort logging
woensdag 29	8	Proef Blaster virus
donderdag 30	8	zie 29e + lange stroomuitval

November 2003

Datum	Uren	Omschrijving
dinsdag 4	8	Diverse andere virussen/trojans geprobeerd

November 2003

Datum	Uren	Omschrijving
woensdag 5	8	Snort preprocessor porstscan
donderdag 6	10	NLUUG conferentie
woensdag 12	8	Voortgangsbespreking + hele middag, stroomuitval
donderdag 13	8	testen met Snot, MySQL proberen te versnellen
vrijdag 14	8	bekijken code barnyard
woensdag 19	8	2e sensor op judith, printers FCJ opgezocht
donderdag 20	8	2e sensor op judith, bekijken resultaten
vrijdag 21	8	SMS alerting niet standaard telefoon
woensdag 26	8	afronden snort
donderdag 27	8	KickIT evenement, printers FCJ opgezocht
vrijdag 28	8	HCC Dagen

December 2003

Datum	Uren	Omschrijving
woensdag 3	8	techverslag indeling maken
donderdag 4	8	techverslag probleem domein
vrijdag 5	8	techverslag NIDS
woensdag 10	8	techverslag NIDS
donderdag 11	8	techverslag NIDS
vrijdag 12	8	techverslag NIDS en verbeteringen
dinsdag 16	8	techverslag verbeteringen
woensdag 17	8	techverslag toepassings voorstel
donderdag 18	8	techverslag toepassings voorstel
vrijdag 19	8	techverslag verbeteringen
maandag 29	6	Doorlezen verslag + verbeteringen

Januari 2004

Datum	Uren	Omschrijving
maandag 5	8	Urenstaat maken + presentatie
dinsdag 6	8	Presentatie
woensdag 7	8	Presentatie
donderdag 8	8	Inleveren verslag + presentatie
maandag 19	8	Presentatie
dinsdag 20	8	Ruimte opleveren

7.1.4 M.P. Rijkeboer

Diversen

Datum	Uren	Omschrijving
juni 2003	16	Voorbereiden project
zomer 2003	80	Lezen boek "Netwerk Intrusion Detection using Snort"

September 2003

Datum	Uren	Omschrijving
woensdag 3	8	Regelen van faciliteiten
donderdag 4	8	Inrichten en opruimen projectruimte
vrijdag 5	8	Installeren workstation + opbouwen netwerk
woensdag 10	8	Installeren server
donderdag 11	8	Regelen internet verbinding
woensdag 17	4	Begin maken voor pva
donderdag 18	8	Werken aan het pva
vrijdag 19	8	Werken aan het pva
woensdag 24	8	Regelen internet verbinding
donderdag 25	8	Werken aan het pva
vrijdag 26	8	Werken aan de presentatie pva

Oktober 2003

Datum	Uren	Omschrijving
woensdag 1	8	Installeren Sun machine
donderdag 2	8	Vergaderen over pva
vrijdag 3	8	Aanpassen pva
dinsdag 7	2	Aanpassen pva
woensdag 8	8	Suns ombouwen
donderdag 9	8	Presentatie + Suns ombouwen
vrijdag 10	8	Netwerk + Suns
woensdag 22	8	Inwerken in AIDE
donderdag 23	8	Inwerken in AIDE + Ipv6
vrijdag 24	8	Beginnen met AIDE
dinsdag 28	8	Beginnen met AIDE
woensdag 29	8	Configureren + testen AIDE
donderdag 30	8	Inwerken in Mtree + Stroomuitval

November 2003

Datum	Uren	Omschrijving
dinsdag 4	8	Prutsen met Mtree
woensdag 5	8	Prutsen met Mtree
donderdag 6	8	NLUUG
woensdag 12	8	Voortgangs vergadering + Stroomuitval
donderdag 13	8	NIDS + mysql
vrijdag 14	8	Snort + mysql
woensdag 19	8	Printers geexploited
donderdag 20	8	SMS alerting
vrijdag 21	8	Opruim + management dag
woensdag 26	8	Afronden alerting + voorlichting
donderdag 27	8	KickIT + printers geexploited
vrijdag 28	8	HCC

December 2003

Datum	Uren	Omschrijving
woensdag 3	8	Projectverslag
donderdag 4	8	Projectverslag
vrijdag 5	8	Projectverslag
woensdag 10	8	Techverslag
donderdag 11	8	Techverslag
vrijdag 12	8	Techverslag
dinsdag 16	8	Techverslag
woensdag 17	8	Techverslag
donderdag 18	8	Techverslag
vrijdag 19	8	Techverslag

Januari 2004

Datum	Uren	Omschrijving
maandag 5	8	Techverslag nakijken
dinsdag 6	8	Projectverslag afmaken
woensdag 7	8	Presentatie maken
donderdag 8	8	Presentatie maken
vrijdag 9	8	Presentatie maken
zaterdag 17	4	Presentatie voorbereiden
maandag 19	8	Presentatie + projectruimte ontmantelen
dinsdag 20	8	Projectruimte opleveren

7.2 Faciliteiten

Een aantal personen en/of instanties hebben faciliteiten beschikbaar gesteld voor dit project, te weten:

- Hogeschool van Utrecht, Faculteit Natuur & Techniek:
 - Projectruimte;
 - meubilair;
 - werkstations;
 - internet verbinding;
 - bekabeling;
 - stroomvoorziening.
- Dhr. L.J.M. van Moergestel:
 - Sun UltraSPARCs;
 - SiteCom 10/100Mbit Switch.
- Dhr. A. van Doesburg:
 - PrePaid GSM Simkaart;
- J.C.J van Dam:
 - Server;
 - Nortel Baystack 450 10/100Mbit managed switch.
- W. Coene:
 - IBM 9,1GB SCSI disk;
 - Symbios Logic 53c875J SCSI controller.

Hoofdstuk 8

Evaluatie

Tijdens de uitvoering van het project zijn we een aantal externe obstakels tegen gekomen welke ons in de uitvoering belemmerden. Verder hebben we ook een aantal problemen met onze projectaanpak ontdekt. Dit hoofdstuk benoemt en bespreekt deze problemen in de hoop deze bij toekomstige projecten te kunnen vermijden.

Een van de belangrijkste obstakels was het verkrijgen van een Internet aansluiting. Wij hebben enige tijd om het ontbreken hiervan heen kunnen werken door gebruik te maken van een laptop en een WaveLAN verbinding, maar hierin en in het regelen van de uiteindelijke Internetverbinding is erg veel tijd in gaan zitten.

Verder is tijdens de loop van het project tot twee keer toe de stroom uitgevallen, waardoor beide keren meer dan de helft van de dag niet gewerkt kon worden en onze server stabiliteitsproblemen ontwikkelde. Gelukkig maakten we gebruik van een backup-strategie, waardoor eventuele risico's tot een minimum waren beperkt.

Maar ook in de organisatie van het project zelf is het een en ander fout gegaan. Zo hadden we van te voren niet echt een duidelijk idee wat we nu als resultaten wilden opleveren en zijn deze resultaten ook te onduidelijk in het Plan van Aanpak gespecificeerd. Dit leidde tijdens de uitvoering van het project tot verwarring en lichte demotivatie.

Ook was de opdracht te uitgebreid opgezet. We hebben ons in zowel Netwerk- als Host Intrusion Detection verdiept, terwijl beperking tot een van beiden waarschijnlijk meer diepgang in de uiteindelijke resultaten had opgeleverd.

Tot slot heeft het opstellen van het Plan van Aanpak veel te veel tijd in beslag genomen. We hadden namelijk in eerste instantie aan de hand van richtlijn van de school het Plan van Aanpak opgesteld, wat resulteerde in een vrij onduidelijk document. Later hebben we bij een werkoverleg en aan de hand van een boek

over projectmanagement¹, besloten tot het grotendeels herschrijven van het Plan van Aanpak.

Mogelijk ligt een factor in de problemen die we ervonden hebben bij de opzet en uitvoer van het project in het feit dat het hier ging om een onderzoeksproject, terwijl wij nooit enige scholing in onderzoeksmethodologie hebben gehad. Wellicht had enige kennis op dit gebied tot een duidelijker Plan van Aanpak geleid, en daarmee tot een beter resultaat.

¹R. Grit, *Project Management: Projectmatig werken in de praktijk*, tweede druk, Wolters Noordhoff, 1997

Hoofdstuk 9

Conclusie

Het project is heel redelijk verlopen. De resultaten zijn op tijd af, de wrijving tussen de projectleden was niet buitensporig hoog en er is een hoop van geleerd.

Zoals in de evaluatie al besproken is de reikwijdte van het project eigenlijk te groot geweest om diep op bepaalde interessante onderwerpen in te gaan. Daarom lijkt het ons handig aan de hand van de resultaten van dit project een of meerdere vervolgonderzoeken op te zetten. Deze kunnen zich onder andere richten op:

- schaalbaarheid van Snort: hoe veel verkeer kan Snort aan met betrekking tot het aantal ingeladen verkeersdefinities;
- de voor- en nadelen van het gebruik van andere database-systemen voor de opslag van de resultaten;
- evaluatie van in hardware geïmplementeerde Network Intrusion Detection systemen;
- de mogelijkheden om Snort in te zetten als een filter;
- analyse van het gebruik van systeembronnen in het kader van Host Intrusion Detection.

Bijlage A

Versies

Hieronder volgt een lijst van de CVS versies van alle \LaTeX bronbestanden.

Bestand	Versie	Laatste wijziging
projectverslag.tex	1.12	2004-01-09 09:46
voorwoord.tex	1.11	2004-01-08 13:23
inleiding.tex	1.4	2004-01-08 12:42
doelstelling.tex	1.1	2003-12-03 11:42
producten.tex	1.5	2003-12-05 13:21
archieff.tex	1.5	2004-01-08 13:23
planning.tex	1.6	2004-01-08 13:23
organisatie.tex	1.4	2003-12-04 11:07
kosten.tex	1.10	2004-01-08 13:23
jelmer.tex	1.6	2004-01-08 13:23
wouter.tex	1.10	2004-01-08 13:23
jesse.tex	1.6	2004-01-08 13:23
martijn.tex	1.8	2004-01-08 13:23
evaluatie.tex	1.7	2004-01-09 10:02
conclusie.tex	1.2	2004-01-09 10:02