Onderzoek veiligheid SURFnet IDS

Lourens Bordewijk, Jimmy Macé
lbordewijk, mace@os3.nl

Universiteit van Amsterdam

17 maart 2006

Samenvatting

De instellingen, die aangesloten zijn bij SURFnet, hebben te maken met computer security incidenten die afkomstig kunnen zijn van zowel buitenstaanders als werknemers. SURFnet handelt veel computer security incidenten af van instellingen die bij SURFnet zijn aangesloten. Om inzicht te geven in het aantal van deze security incidenten, heeft SURFnet het Distributed Intrusion Detection System (D-IDS) ontwikkeld als service voor de aangesloten instellingen.

D-IDS is een systeem dat speciaal ontworpen is om kwaadaardig verkeer te detecteren in de netwerken van instellingen die aangesloten zijn bij SURFnet. Het systeem bestaat uit een centrale honeypot die via tunnels gekoppeld wordt aan verschillende sensoren in de netwerken bij SURFnet aangesloten instellingen. De door de honeypot gedetecteerde gegevens worden centraal opgeslagen en geanalyseerd. Vervolgens worden de aangesloten instellingen geïnformeerd over de analyses. Deze oplossing biedt voordelen als het gaat om onderhoud, maar brengt ook een aantal beveiligingsrisico's met zich, omdat de netwerken van verschillende instellingen aan elkaar gekoppeld worden.

Het doel van ons project is om te onderzoeken wat voor beveiligingsrisico's dit kunnen zijn. Het onderzoek start met het identificeren en analyseren van het huidige ontwerp van de SURFnet IDS dienst. De theoretische zwakheden worden onderzocht met behulp van documentatie en van SURFnet medewerkers verkregen informatie. De mogelijke aanvallen worden in kaart gebracht door middel van een aantal scenario's.

Aan de hand van een aantal testen is geprobeerd te achterhalen, hoe de beschikbaarheid, integriteit en vertrouwelijkheid van de IDS dienst onderuit kan worden gehaald. Aan de hand van de onderzoeksresultaten worden een aantal technische en de niet-technische maatregelen aanbevolen. Dit rapport sluit af met een advies over welke maatregelen zouden moeten worden doorgevoerd om de IDS dienst te verbeteren.

Inhoudsopgave

1 Voorwoord

In het kader van onze studie "System en Network engineering" aan de Universiteit van Amsterdam hebben we vier weken onderzoek gedaan naar de veiligheid c.q. beveiliging van de SURFnet IDS dienst. Het onderzoek is uitgevoerd in opdracht van SURFnet [1] onder toezicht van Rogier Spoor. Rogier Spoor is coördinator en oprichter van de SURFnet IDS dienst [2].

2 Inleiding

In hoofdstuk drie wordt het uitgangspunt van het onderzoek beschreven.

Hoofdstuk vier beschrijft kort de doelen, de karakterisatie en de infrastructuur van de IDS dienst. Hier start het onderzoek met het identificeren en analyseren van het huidige ontwerp van de SURFnet IDS dienst. De theoretische zwakheden worden onderzocht met behulp van documentatie en van SURFnet medewerkers verkregen informatie. De mogelijke aanvallen worden in kaart gebracht door middel van een aantal scenario's.

In hoofdstuk vijf wordt de mogelijke reeds beschikbare informatie over de infrastructuur aangevuld, door middel van het uitvoeren van een aantal testen. Door het uitvoeren van deze testen is geprobeerd te achterhalen, hoe de beschikbaarheid, integriteit en vertrouwelijkheid van de IDS dienst onderuit kan worden gehaald.

In hoofdstuk zes wordt eerst het doel van de maatregelen behandelt. Vervolgens komen de technische en de niet-technische maatregelen aanbod.

Ten slotte wordt in hoofdstuk zeven afgesloten met het een conclusie en een advies over welke maatregelen zouden moeten worden doorgevoerd om de IDS dienst te verbeteren.

3 Project

In dit hoofdstuk wordt de achtergrond, het projectdoel en de projectuitvoering behandeld.

3.1 Algemeen

SURFnet is een hoogwaardig computernetwerk speciaal voor hogescholen, universiteiten, academische ziekenhuizen, onderzoeksinstituten en andere wetenschappelijke instellingen. 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. SURFnet is opgericht in 1988 en inmiddels (2006) zijn er ruim 180 instellingen aangesloten. SURFnet is een dochtermaatschappij van de Stichting Surf, een samenwerkingsorganisatie van instellingen voor hoger onderwijs en onderzoek op het gebied van ICT en netwerken.

3.2 Achtergrond

De instellingen, die aangesloten zijn bij SURFnet hebben te maken met vele bedreigingen in hun netwerk, zoals virussen en Trojaanse paarden, denial of service aanvallen, vernietiging en diefstal van gegevens en diverse andere problemen. Deze computer security incidenten kunnen afkomstig zijn van zowel buitenstaanders als werknemers, die de beveiliging al dan niet opzettelijk kunnen compromitteren. SURFnet handelt veel computer security incidenten af van instellingen die bij SURFnet zijn aangesloten. Om inzicht te geven in het aantal van deze security incidenten, heeft SURFnet het Distributed Intrusion Detection System (D-IDS) ontwikkeld als service voor de aangesloten instellingen.

D-IDS is een systeem dat speciaal ontworpen is om kwaadaardig verkeer te detecteren in de netwerken van instellingen die aangesloten zijn bij SURFnet. Het systeem bestaat uit een centrale honeypot die via tunnels gekoppeld wordt aan verschillende sensoren in de netwerken bij SURFnet aangesloten instellingen. De door de honeypot gedetecteerde gegevens worden centraal opgeslagen en geanalyseerd. Vervolgens worden de aangesloten instellingen geïnformeerd over de analyses. Deze oplossing biedt voordelen als het gaat om onderhoud, maar brengt ook een aantal risico's met zich, omdat de netwerken van verschillende instellingen aan elkaar gekoppeld worden.

3.3 Doel van het project

Het doel van dit project is om te onderzoeken wat de beveiligingsrisico's van de SURFnet IDS dienst zijn. De onderzoeksresultaten kunnen een aantal maatregelen opleveren die de risico's verminderen. Het is de bedoeling dat SURFnet met het nemen van de aan te bevelen maatregelen het D-IDS voortaan veiliger kan aanbieden aan de bij SURFnet aangesloten instellingen. De resultaten van het onderzoek worden in een adviesrapport opgeleverd aan het einde van het Research Project 1.

3.4 Projectuitvoering

Het project is uitgevoerd gedurende vier weken en is als volgt ingedeeld:

Week 1 : vooronderzoek;

Week 2 : testen;

Week 3 : maatregelen onderzoeken;

Week 4 : rapporteren.

In de eerste week is het plan van aanpak opgesteld. In het plan van aanpak zijn de hoofdvraag en deelvragen omschreven. De hoofdvraag van het project luidt als volgt:

> *Hoe veilig is de huidige implementatie van de SURFnet Intrusion Detection System dienst en welke maatregelen kunnen er eventueel genomen worden om het systeem veiliger te kunnen inzetten in netwerken van instellingen die aangesloten zijn bij SURFnet?*

De volgende deelvragen kunnen binnen het project worden onderscheiden:

Hoe is de beveiliging gerealiseerd in de huidige situatie en wat zijn de risico's van de huidige implementatie? De SURFnet IDS dienst draait op dit moment als pilot bij verschillende instellingen die aangesloten zijn bij SURFnet. Als de IDS dienst een netwerk van een aangesloten instelling in gevaar kan brengen, kan dit o.a. gevolgen hebben voor de besluitvorming van de instelling om wel of niet gebruik te maken van de IDS dienst.

Hoe kan de beveiliging van SURFnet IDS dienst geoptimaliseerd worden? Hierbij is gekeken of het ontwerp en de implementatie kan worden geoptimaliseerd aan de hand van de onderzoeksresultaten. Bekeken is of extra toepassingen noodzakelijk zijn, zoals hostbased IDS oplossingen?

Na het opstellen van het plan van aanpak, is het vooronderzoek gestart dat bestond uit het bestuderen van de huidige situatie. Vervolgens is nagedacht over de theoretische zwakheden van de IDS dienst. Ten slotte zijn een aantal mogelijke aanvalscenario's onderzocht.

In week twee zijn de eerder vastgestelde aantal aanvalscenario's uitgevoerd. Hierbij is geprobeerd de privacy, integriteit en beschikbaarheid van de dienst onderuit te halen.

In week drie is geprobeerd het ontwerp en de implementatie te optimaliseren aan de hand van de onderzoeksresultaten uit week twee.

De laatste week is gebruikt als uitloop voor het onderzoek, het formuleren van het advies en aanbeveling en voor het adviesrapport.

4 Huidige situatie

Dit hoofdstuk beschrijft kort de doelen, de karakterisatie en de infrastructuur van de IDS dienst. De karakterisatie van de IDS dienst bestaat uit het verzamelen informatie over de IDS dienst.

4.1 Doelen van de IDS dienst

De doelen van de SURFnet IDS dienst zijn o.a. het opzetten van een schaalbare - eenvoudig te beheren en onderhouden - dienst die: de hoeveelheid kwaadaardig verkeer en de verspreiding kan analyseren binnen netwerken van instellingen, die aangesloten zijn bij SURFnet. De gegevens van het kwaadaardige verkeer worden op een overzichtelijke manier beschikbaar gesteld voor de betreffende instellingen. De instellingen kunnen met behulp van deze informatie actie ondernemen en verdere verspreiding van kwaadaardig verkeer tegen gaan.

Het is belangrijk dat de volgende aandachtspunten in stand blijven bij het gebruik van de SURFnet IDS dienst:

- Privacy, vreemden mogen de informatie niet inzien;
- Integriteit,vreemden mogen de informatie niet wijzigen;
- Beschikbaarheid, vreemden moeten de dienst niet uit kunnen schakelen.

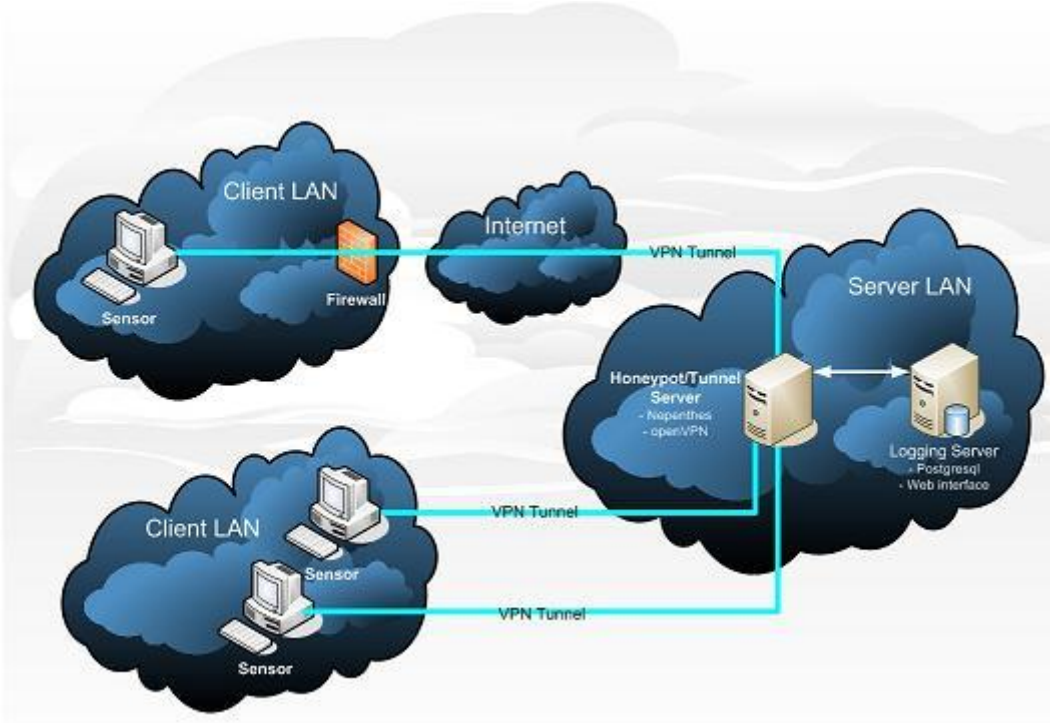
4.2 Karakerisatie van de IDS dienst

In figuur 1 staat een overzicht van de huidige infrastructuur van de IDS dienst. De pilot D-IDS heeft meerdere Knoppix sensoren in de netwerken van de bij SURFnet aangesloten instellingen. Deze sensoren worden opgestart vanaf een USB-stick. Er wordt een layer 2 OpenVPN tunnel opgezet met de centrale Nepenthes honeypot server. Vervolgens wordt door de Honeypot server een DHCP-verzoek gedaan door de tunnel bij de DHCP-server in het netwerk van de aangesloten instelling. Dit verzoek geeft een virtuele interface (tap) van de Honeypot server een IP-adres van de aangesloten instelling. De Honeypot server is hierdoor virtueel aanwezig in het netwerk van de aangesloten instelling. Deze oplossing zorgt ervoor dat er op de sensor fysiek geen honeypot hoeft te draaien.

De gegevens van het kwaadaardige verkeer worden gelogd in een PostgreSQL database. Instellingen die gebruikmaken van de IDS dienst kunnen via een webinterface de informatie bezichtigen. Met deze gegevens kunnen beheerders vrij eenvoudig zien welke machines in hun netwerk besmet zijn.

4.3 Identificatie van de dreigingen

De theoretische zwakheden worden onderzocht aan de hand van over dit onderwerp verkregen documentatie [2] en met behulp van medewerkers van SURFnet verkregen informatie. Met de systeem analyse en penetratie techniek, wordt de specificatie en documentatie geanalyseerd om een aantal scenario's met hypothetische zwakheden te creëren. De scenario's worden in het volgende hoofdstuk gebruikt om een aantal testen uit te voeren.



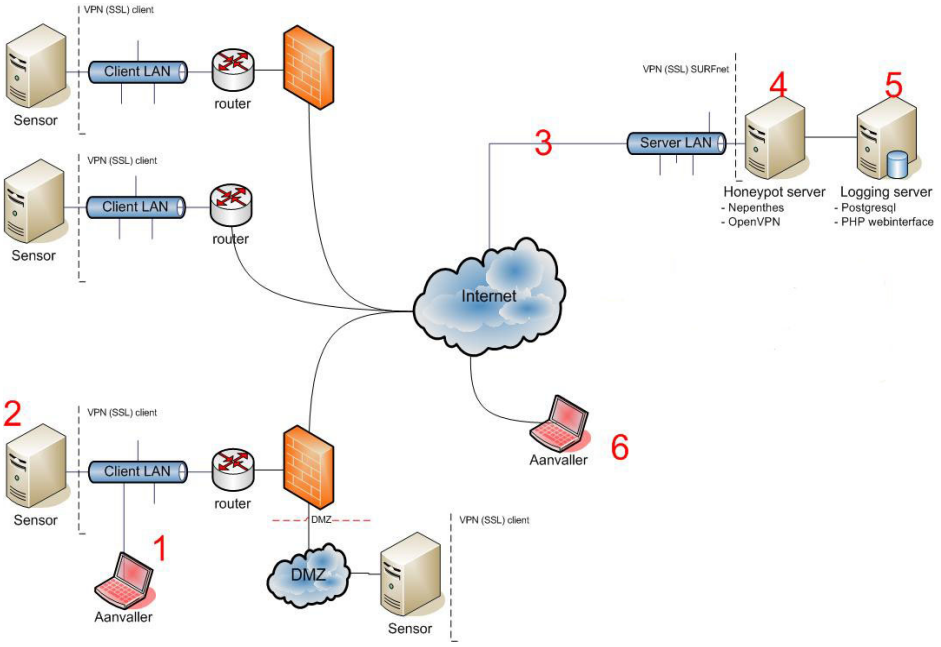
Figuur 1: Overzicht huidige infrastructuur van de IDS dienst

Een sterke beveiliging van een IT infrastructuur bestaat uit lagen. Als een aanvaller één of meerdere lagen van de beveiliging heeft doorbroken, bijvoorbeeld door de firewall te omzeilen. Is het noodzakelijk dat de systemen achter firewall up to date en goed beveiligd zijn.

In de volgende beschreven scenario's worden verschillende lagen van de beveiliging behandeld. Deze scenario's zijn ervoor om de beveiliging vanuit verschillende lagen en posities te onderzoeken.

1. aanval vanuit het client LAN;
2. aanval vanaf de sensor;
3. Man In the Middle (MITM) aanval;
4. aanval vanaf de honeypot;
5. aanval vanaf de logserver;
6. aanval vanaf het Internet.

In figuur 2 zijn de verschillende posities met de scenario's nummers gegeven.



Figuur 2: Overzicht van de verschillende scenario's

4.3.1 Scenario 1 - Aanval vanuit het client LAN

In scenario 1 wordt vanaf een machine in een client netwerk een aanval uitgevoerd op een sensor. De sensor is te benaderen via SSH op poort 22 en DHCP poort 68. Om toegang te krijgen tot het systeem kunnen eventuele kwetsbaarheden in de services worden misbruikt. Veel kwetsbaarheden [1] zijn gebaseerd op een buffer overflow. Een buffer overflow ontstaat op het moment dat er getracht wordt meer informatie naar een buffer te schrijven dan de buffer toelaat. Hierdoor wordt een buffer overschreven, met het gevolg dat een willekeurige code in andere aansluitende buffers kan worden geplaatst. Een aanvaller kan hiermee applicaties laten crashen of bepaalde code laten uitvoeren, en zichzelf op die manier toegang tot het systeem verschaffen.

Als een aanvaller een kwetsbaarheid wil gebruiken om toegang te krijgen moet een bijpassende exploit gezocht worden [2]. Echter wanneer deze niet beschikbaar is, kan men zelf een exploit schrijven voor de gevonden kwetsbaarheid. Met een exploit kan een aanvaller een kwetsbaarheid uitbuiten, om zichzelf van uitgebreidere privileges te verschaffen dan onder normale omstandigheden is toegestaan.

Vanuit het client LAN is via de tunnel de Nepenthes honeypot te benaderen. Nepenthes

[1] Een kwetsbaarheid of vulnerability is een ontwerp- of implementatiefout in een programma die misbruikt kan worden om de integriteit van een systeem aan te tasten of de beveiliging ervan te omzeilen.

[2] Een exploit is stuk code die een gevonden kwetsbaarheid in een applicatie uitbuit om via die weg ongeautoriseerd toegang te verkrijgen tot het doelwit.

simuleert allerlei vulnerability's om virussen mee te vangen. Nepenthes is hoofdzakelijk ontwikkeld en geschreven in C++. Het is goed mogelijk dat Nepenthes buffer overflow kwetsbaarheden bevat. Aangezien het een relatief nieuw product is en de source code nog niet volledig geaudit is, zou Nepenthes dus een zwakheid in het systeem kunnen zijn.

Het TCP/IP protocol ondersteunt een optie voor het specificeren van de exacte route van een pakket. Deze optie heet source routing. Een aanvaller kan deze optie gebruiken om data te verzenden om het doen lijken dat het afkomstig is een andere machine, vaak een meer vertrouwd systeem. Source routing is handig voor het onderzoeken van netwerk fouten, maar aanvallers kunnen het ook misbruiken. De aanvaller zou een source route aan kunnen geven die door de tunnel van de sensor via de honeypot door een andere tunnel naar een ander netwerk gaat.

Een andere mogelijkheid om een sensor te compromitteren, is een brute force aanval op de SSH service. Dit is een luidruchtige aanval, die veel verkeer op het netwerk genereert en snel wordt opgemerkt.

Wanneer een aanvaller erin slaagt via één van deze methodes het systeem te compromitteren is een beveiligingslaag doorbroken, waarna informatie kan worden verzameld om de aanval verder uit te breiden.

4.3.2 Scenario 2 - Aanval vanaf de sensor

In scenario 2 heeft de aanvaller in eerste instantie beperkte toegang op de sensor. De aanvaller zal proberen kwetsbaarheden uit te buiten om meer rechten te krijgen.

Vanaf de sensor zijn de gesimuleerde kwetsbare services van de honeypot te benaderen. Wanneer één van de services verkeerd geïmplementeerd is, zou het mogelijk kunnen zijn om toegang te verschaffen tot het systeem. De services worden gesimuleerd door Nepenthes. Dit programma draait onder de user Nepenthes en heeft beperkte rechten. Wanneer deze software gecompromitteerd, is hangt de beveiliging af van de systeemconfiguratie en van de lokale services.

Vanaf de sensor is de honeypot te benaderen op TCP poort 1194 (OpenVPN), als deze service kwetsbaar is kan dit misbruikt worden. Aangezien de geschiedenis van OpenVPN vrij goed is qua kwetsbaarheden zal dit echter niet waarschijnlijk zijn.

4.3.3 Scenario 3 - MITM aanval

Het zou theoretisch mogelijk kunnen zijn om een Man-In-The-Middle aanval uit te voeren tussen de sensor en de honeypot. De uitgaande pakketten van de sensor gaan in dat geval niet naar de honeypot, maar naar een systeem dat zich als zodanig voordoet. Vervolgens worden deze pakketten, al dan niet in gewijzigde vorm, vanuit het tussenliggende systeem

verzonden naar de honeypot en andersom. Door een dergelijke aanval uit te voeren kan de data onderschept, gedecrypt en gemanipuleerd worden. Deze aanval kan zowel intern als op het Internet gedaan worden.

4.3.4 Scenario 4 - Aanval vanaf de honeypot

In scenario 4 heeft de aanvaller in de eerste instantie beperkte toegang tot de honeypot server. Als de lokale services [3] op de honeypot server kwetsbaar zijn, zal een aanvaller via deze services root toegang proberen te krijgen.

Root toegang op de honeypot server is interessant voor een aanvaller, omdat men vanaf de honeypot server toegang heeft tot alle netwerken die aangesloten zijn op de honeypot. De aangesloten sensoren checken regelmatig bij de honeypot of er updates voor hun beschikbaar zijn. De aanvaller kan zijn eigen geremasterde Knoppix image met rootkit oplaten halen door de sensoren. Als deze aanval succesvol is, zou men controle over alle sensoren kunnen bemachtigen.

In dit scenario is tevens de log server te benaderen. Op de log server draait PostgreSQL op poort 5432. Deze poort kan gebruikt worden om een connectie te maken met de database van de IDS dienst. Vanaf de honeypot is dit eenvoudig omdat het wachtwoord opgeslagen is in */etc/surfnetids/surfnetids-tn.conf*.

4.3.5 Scenario 5 - Aanval vanaf de logserver

In scenario 5 heeft een aanvaller beperkte toegang tot de log server. Hier geldt hetzelfde als bij het vorige scenario's. Als de services op de logserver kwetsbaar zijn, zou een aanvaller via deze services root toegang kunnen krijgen.

Als een aanvaller op de logserver kan inloggen met beheerdersrechten, beschikt de aanvaller over alle informatie betreffende de IDS dienst. Met deze informatie kan een aanvaller zijn aanval verder uitbreiden. Als de honeypot source routing toestaat, zou met de IP-adressen van de aangesloten instellingen een source route aanval uitgevoerd kunnen worden. Met Hping2 [7] kan getest worden of het mogelijk is om pakketten van de log server te routeren naar de klantnetwerken.

Als men de honeypot vanaf de logserver wil compromitteren, moet worden bekeken of er kwetsbare services draaien op honeypot. In de documentatie is te vinden dat de poorten 22 (SSH), 1194 (OpenVPN) en 4443 (HTTPS) open staan. De standaard firewall ruleset is te vinden op de website van SURFnet [4]. Dit geeft een goede indruk van de ruleset, maar het is geen garantie dat deze ruleset op de productie systemen hetzelfde is.

4.3.6 Scenario 6 - Aanval vanaf het Internet

In scenario 6 wordt de aanval vanaf Internet uitgevoerd op de IDS dienst van SURFnet. Voor de buitenwereld is webservice (443) beschikbaar. Deze is geschreven in PHP. Een aanvaller kan de webservice aanvallen door middel van SQL injection en cross site scripting [5].

De poorten SSH (22), OpenVPN (1194) en SSL (4443) staan open vanaf Internet. Als deze services niet zijn gepatcht, zijn de services een mogelijke ingang zijn voor aanvallers.

Een aanvaller kan door middel van Denial of Service (DoS) aanvallen de beschikbaarheid van de IDS dienst beïnvloeden . DoS is een type aanval waarbij een systeem of netwerk dusdanig belast wordt, dat ze niet meer in staat zijn om hun diensten naar behoren aan te bieden. De aanval bestaat vaak uit het misbruiken van een tekortkoming in de software van een systeem, waardoor overmatig veel systeem- of netwerkresources verbruikt worden. Een aanval kan ook bestaan uit het verzadigen van het netwerk zelf.

Er zijn een aantal methodes, die een aanvaller kan gebruiken om de beschikbaarheid te beïnvloeden:

Ping flood Dit is het versturen van grote hoeveelheden ping pakketjes (ICMP echo request) naar een systeem, zodat de netwerkfaciliteiten van het aangevallen systeem overmatig belast worden. Deze aanval heeft geen invloed op de honeypot, want Iptables op de honeypot blokkeert ICMP verkeer.

SYN floods Dit zijn een vorm van Denial of Service aanvallen waarbij grote hoeveelheden verzoeken tot het opzetten van een connectie (SYN pakketten) naar een systeem verzonden worden zonder dat deze gevolgd worden door een bevestiging (ACK pakketten). De TCP server reserveert voor ieder verzoek een volgnummer in de queue. Indien de hoeveelheid gereserveerde volgnummers sneller groeit dan dat de volgnummers van de onbeantwoorde connectieverzoeken zal de lijst vollopen en kan het systeem geen nieuwe connecties meer accepteren, waardoor het onbereikbaar wordt.

UDP flood Bij een UDP flood worden er dusdanig veel UDP pakketjes naar het doelwit gestuurd dat deze geen kans meer ziet om andere pakketten te verwerken.

DNS redirectie & Route redirectie Redirectie van DNS-verkeer kan ervoor zorgen dat de webservice niet meer beschikbaar is op het huidige adres. Route redirectie kan ervoor zorgen dat de IDS dienst niet meer beschikbaar is. DNS redirectie en Route redirectie kunnen leiden tot een MITM aanval. Deze methodes hebben niet direct betrekking op de infrastructuur van de IDS dienst, maar vormen wel een dreiging voor de beschikbaarheid van de IDS dienst.

Omweg naar het doelwit

De machines van beheerders van de IDS-systemen die gebruikt worden kunnen interessant zijn voor aanvallers. Als een keylogger of een virus op een van de machine geplaatst wordt, kunnen de SSH en web credentials voor de IDS dienst gelogd worden. Uit het vooronderzoek blijkt dat voor de authenticatie van SSH en de webservice geen tokens worden gebruikt. Via de website van SURFnet IDS zijn de volgende adressen te achterhalen. Jan.vanLith[at]SURFnet[dot]nl, Kees.Trippelvitz[at]SURFnet[dot]nl en projectleider Rogier.Spoor[at]SURFnet[dot]nl. Aanvallers kunnen een lokmail sturen, waarmee de IP-adressen van deze personen te achterhalen zijn. Als deze adressen eenmaal bekend zijn, zou op deze machines een aanval kunnen worden gelanceerd.

4.3.7 Scenario 7 - Fysieke beveiliging

In scenario 7 wordt de fysieke beveiliging van de complete IDS dienst onderzocht. Dit zijn de sensors, honeypot en logserver. De fysieke beveiliging gaat onder andere over de beveiliging van servers en serverruimtes. Wat echter vaak wordt vergeten, is het menselijke aspect. Deze vorm van beveiliging wordt vaak onderschat, toch is de beveiliging tegen social engineering een belangrijke factor, want de beveiliging is zo sterk als de zwakste schakel. Social engineering is een verzamelnaam voor alle methoden om iemand informatie te ontfutselen waarmee men zich ongeoorloofd toegang tot een systeem kan verschaffen. De kern van deze techniek bestaat daaruit dat men het slachtoffer zover weet te krijgen dat deze vertrouwelijke informatie verstrekt aan de dader, in de veronderstelling dat die er recht op heeft.

Servers en server ruimte

Het is mogelijk dat een aanvaller die het gemunt heeft op de honeypot server via social engineering de server ruimtes van SURFnet probeert binnen te komen. Iemand kan zich voordoen als stagiair of schoonmaker om bij SURFnet in het pand te komen. Uiteraard moet de persoon eerst vooronderzoek doen om achter de procedures te komen. Eenmaal binnen kan de persoon zich richten op de serverruimte. Als de servers geen fysieke beveiliging hebben toegepast, kan een aanvaller op verschillende manieren de server systemen voorzien met een rootkit.

Sensor

Als een USB-stick verkeerde handen valt, ontstaan er een aantal hypotetische zwakheden. Een potentiële aanvaller kan een sensor opstarten, het Knoppix-image mounten en vervolgens het root wachtwoord in `/etc/shadow` verwijderen. Om deze verandering permanent te maken kan het Knoppix imagebestand geremastered worden [6]. Het imagebestand moet vervolgens naar de USB-stick worden geschreven. Als een aanvaller in staat is om Knoppix te remasteren kan de image volledig naar wens worden ingericht.

Uit de documentatie blijkt dat het wachtwoord van de sensor 10 karakters, alfanumeriek is en leestekens bevat. Het is opgeslagen als MD5 hash met salt. Het duurt ongeveer 21

miljoen jaar om een wachtwoord zonder salt te kraken. Door gebruik te maken van salt, wordt het de aanvaller lastiger gemaakt een database te bouwen met alle wachtwoorden. De wachtwoorden van de gebruikers staan in het Knoppix-image bestand en worden bij distributie niet gewijzigd. Als het qua rekenkracht mogelijk is om het wachtwoord bestand te brute forcen en de wachtenwoorden te achterhalen, dan is het mogelijk om in te loggen op één van de andere sensoren (mits men de IP-adressen weet). Dit kan omdat de wachtwoorden op elke sensor hetzelfde is.

5 Identificatie van de kwetsbaarheden

De verschillende scenario's zijn onderzocht met behulp van vooraf verkregen schriftelijke en mondelinge informatie. Door middel van testen is geprobeerd te achterhalen, hoe de beschikbaarheid, integriteit en vertrouwelijkheid van de IDS dienst onderuit kan worden gehaald.

Deze open manier van testen, is wordt ook wel de crystal of white box penetratietest genoemd. Bij een black box penetratietest heeft men vooraf geen informatie over het systeem, in tegenstelling tot een crystal box test. Een black box test vergt daarom meer voorbereidingstijd en kent een langere doorlooptijd dan de crystal box penetratietest [1].

De testen hebben geleid tot een lijst met kwetsbaarheden die mogelijke geëxploiteerd kunnen worden. De kwetsbaarheden zijn geïdentificeerd door middel van:

- Fingerprinting;
- Geautomatiseerde en handmatige kwetsbaarheid scan;
- Een kwetsbaarheid analyse;
- Systeem software en security analyses.

Bij fingerprinting wordt gekeken hoe een platform precies reageert op bepaalde pakketten. Hiermee ontstaat een patroon waarmee het onderliggende besturingssysteem te identificeren valt. Dit kan actief gebeuren door misvormde pakketten te versturen naar het systeem, maar ook passief door uitgezonden pakketten met een netwerk monitor af te luisteren. Vervolgens kan een poortscan worden uitgevoerd. Bij een poortscan wordt getracht te detecteren welke TCP of UDP poorten van het gescande systeem actief zijn. Hiermee kan in kaart gebracht worden welke netwerkservices hiervan als potentieel doel kunnen dienen. Zodra bekend is wat voor services en welk besturingssysteem wordt gebruikt, worden de meer gerichte aanvallen opgezet. Fingerprinting en poortscannen is mogelijk met Nmap [7] en Hping2 [8] .

5.1 Scenario 1 - Aanval vanuit het client LAN

In dit scenario is de sensor bereikbaar en de honeypot is te benaderen door de tunnel van de sensor.

5.1.1 Aanval op de honeypot

Vanuit het client LAN zijn via de tunnel de volgende gesimuleerde services van Nepenthes benaderbaar:

```
21/tcp      ftp
42/tcp      nameserver
80/tcp      http
110/tcp     pop3
135/tcp     msrpc
139/tcp     netbios-ssn
143/tcp     imap
220/tcp     imap3
443/tcp     https
445/tcp     microsoft-ds
465/tcp     smtps
993/tcp     imaps
995/tcp     pop3s
1023/tcp    netvenuechat
1025/tcp    NFS-or-IIS
2105/tcp    eklogin
3372/tcp    msdtc
5000/tcp    UPnP
10000/tcp   snet-sensor-mgmt
17300/tcp   kuang2
```

Een aanvaller kan de source code van Nepenthes downloaden en scannen met de Rough Auditing Tool for Security (RATS) [9] om de sourcecode van Nepenthes te onderzoeken. Het resultaat van deze scan meldt dat er een aantal mogelijkheden zijn voor buffer overflows en format string kwetsbaarheden. In totaal zijn er 154 waarschuwingen met een hoge prioriteit en 58 met een medium prioriteit. Het is nog niet duidelijk of het hier gaat om de gesimuleerde kwetsbaarheden van Nepenthes, of echt om kwetsbaarheden in de componenten die Nepenthes gebruikt om kwetsbaarheden te simuleren. Gezien de gelimiteerde onderzoekstijd kan de code van Nepenthes niet verder worden onderzocht.

5.1.2 Aanval op de sensor

De poorten van de sensor zijn met Nmap gescand 8.1.2 om te zien welke versies worden gebruikt. Vervolgens is met behulp van verschillende vulnerability databases bekeken of deze kwetsbaar zijn 8.1.

De volgende services zijn gebonden aan het IP-adres van de sensor SSH (22), Bootpc (68).

- OpenSSH 3.8.1p1 Debian-8.sarge.4 (protocol 1.99)
- dhcpclient/Bootpc

OpenSSH

Na de scan uitgevoerd te hebben is geconstateerd dat er een OpenSSH server draait met versie nummer 3.8.1p1. Op dit moment is OpenSSH versie 4.2 de nieuwste versie. Er is er geen remote kwetsbaarheid geconstateerd voor de OpenSSH versie 3.8.1p1.

Om te kijken of de wachtwoorden sterk genoeg waren op het systeem is er vanaf afstand een woordenboek aanval gedaan op het systeem via SSH. De test was niet succesvol en de aanval is niet onopgemerkt gebleven. Hij is gedetecteerd door de Network Emergency Responder & Detector (NERD) van SURFnet door een behoorlijk aantal connecties op poort 22. Deze aanval heeft alle overige nieuwe connecties op poort 22 vanaf andere machines geblokkeerd. Hiermee is de beschikbaarheid van de SSH dienst dus wel onderuit gehaald.

Dhcpclient/Bootpc

Verder is geconstateerd dat een dhcpclient/Bootpc server draait op poort 68. Op dit moment is deze service niet kwetsbaar.

Een aanvaller kan door middel van een ICMP flood, Syn flood en DDoS 4.3.6 de beschikbaarheid van de sensor wel beïnvloeden.

5.2 Scenario 2 - Aanval vanaf de sensor

In dit scenario is eerst onderzocht wat een aanvaller op de sensor kan doen met beperkte rechten. Hierna is gekeken wat er mogelijk is met root toegang.

5.2.1 Beperkte toegang

OpenSSH is kwetsbaar voor een lokale SCP Shell exploit. Een applicatie fout zorgt ervoor dat - gebruikers commando's - niet gevalideerd worden voordat er een system call wordt uitgevoerd. Deze fout staat toe dat lokale aanvallers willekeurige commando's met

de privilege van gebruikers uit te voeren op de kwetsbaarheidbare versies van OpenSSH met SCP ingeschakeld.

De sensor is gescand met de Tiger audit tool wat heeft geleid tot 428 meldingen van verkeerde veiligheidsinstellingen, hoofdzakelijk verkeerde bestands permissies. Verder meldt Tiger dat er 515 packages niet up to date zijn. Het rapport is te lang voor de bijlage. Voor een volledig overzicht van de meldingen moet Tiger worden uitgevoerd op de sensor.

Hier volgen nog een paar opmerkelijke berichten:

```
# Checking network configuration
--FAIL-- The system is configured to answer to ICMP broadcasts
--FAIL-- The system is not protected against Syn flooding attacks
--FAIL-- The system permits the transmission of IP packets with invalid addresses
--FAIL-- The system permits source routing from incoming packets
--WARN-- The system is not configured to log suspicious (martian) packets

# Checking listening processes
--WARN-- The process 'pump' is listening on socket bootpc is run by root.
--WARN-- The process 'sshd' is listening on socket ssh is run by root.
```

Het systeem maakt gebruik van OpenSSH versie 3.8.1p1. Deze versie blijkt een lokale kwetsbaarheid te bevatten. Het biedt geen mogelijkheid om root rechten te bemachtigen, maar het kan wel de beschikbaarheid onderuit halen [10].

5.2.2 Root toegang

De certificaten om een OpenVPN verbinding op te zetten, worden via een SSL (4443) verbinding opgevraagd. In het bestand `/cdrom/script/wgetrc` staat de gebruikersnaam en wachtwoord om de SSL verbinding te maken. Wanneer men is ingelogd op de sensor kan men met `wget` certificaten aanvragen op de honeypot. Dit gebeurd door een PHP script te triggeren en maakt het mogelijk om oneindig veel certificaten aan te vragen en de database te vervuilen.

Het is mogelijk om informatie over potentiële doelwitten te verzamelen uit het known_host bestand. Als gebruik wordt gemaakt van de SSH client op de sensor, wordt in de home directory door de SSH client een lijst bij gehouden met de namen en IP-adressen van elk host waarmee verbinding gemaakt is [11].

5.3 Scenario 3 - Man in the Middle (MITM) aanval

Wanneer de sensor (USB-Stick) wordt geleverd aan de aangesloten instelling bij SURFnet, dan wordt deze geleverd met het CA certificaat. Als de sensor voor de eerste keer

wordt aangesloten en opgestart wordt beschikt deze nog niet over de sensor.key en sensor.crt. Deze sleutels zijn nodig voor de client om een OpenVPN tunnel op te zetten met de honeypot. De sleutels worden met wget via HTTPS verkregen, met de optie –no-check-certificate. Door deze optie mee te geven wordt er tijdens de HTTPS sessie niet gekeken of het certificaat echt van de server afkomstig is. Dat de certificaten niet gecheckt worden, komt door wget. Bij de laatste versie bestaat de mogelijkheid van het ontvangen van self sign certificaten niet meer.

Door dat er niet gecheckt wordt of de certificaat werkelijk afkomstig is van de server tijdens de HTTPS sessie is het mogelijk om een HTTPS MITM aanval te doen om de server.key en server.crt te bemachtigen. Als de aanvaller het voor elkaar krijgt de CA.crt van de sensor te halen, door in te breken of fysieke toegang te krijgen tot sensor, dan wordt het mogelijk om een tunnel op te zetten met de honeypot.

Nu kan er nog steeds geen OpenVPN MITM aanval worden uitgevoerd, omdat de aanvaller niet in het bezit is van de privé sleutel van de server. Er kan geconcludeerd worden dat een OpenVPN MITM niet mogelijk is, zonder de sensor en de honeypot te hacken.

5.4 scenario 4 - Aanval vanaf de honeypot

In scenario 4 heeft de aanvaller in de eerste instantie beperkte rechten op de honeypot. Vervolgens worden de mogelijkheden beschreven wanneer root toegang is verkregen.

5.4.1 Beperkte toegang

In het geval de aanvaller beperkte toegang heeft tot de honeypot server, zijn de volgende lokale componenten op de honeypot server kwetsbaar voor misbruik:

- Imagemagick's libmagick bibliotheek
- PHP
- Midnight Commander

Imagemagick's libmagick bibliotheek

In de imagemagick's libmagick bibliotheek worden onder sommige omstandigheden, tijdelijke bestanden aangemaakt met de verkeerde beveiligingsmaatregelen. De kwetsbaarheid kan door een lokale gebruiker misbruikt worden door bestanden te overschrijven met privileges van een programma van een andere gebruiker die dezelfde bibliotheek gebruikt.

PHP4

Er zitten twee kwetsbaarheden PHP4: de memory_limit functionaliteit in PHP 4.x t/m 4.3.7 en 5.x up t/m 5.0.0. Als register_globals is ingeschakeld staat het aanvallers vrij om willekeurige code uit te voeren door een memory_limit abort te triggeren tijdens de uitvoering van de zend_hash_init functie.

Midnight Commander

Midnight Commander is een file manager. Als een malicious archief (zoals een .tar file) door Midnight Commander wordt geopend, kan Midnight Commander ervoor zorgen dat willekeurige code wordt uitgevoerd.

Meer informatie over deze kwetsbaarheden is te vinden in de bijlage 8.2.

De honeypot is met Tiger, een audit tool, gescand. Zie volgend scenario 5.5.1 voor uitgebreide de resultaten.

Logserver

Vanaf de honeypot is de logserver te benaderen poort 5432. De PostgreSQL tool Pgsql, kan gebruikt worden om een connectie te maken met de database van de IDS dienst. Het wachtwoord om in te loggen is namelijk opgeslagen in /etc/surfnetids/surfnetids-log.conf. In hetzelfde configuratie bestand staat overigens ook het GNUpg mail wachtwoord.

In de tabel login van de database staan de volgende gegevens:

rogier	098f6bcd4621d373cade4e832627b4f6	rosp@SURFnet.nl	test
os3	d63ec68b0b5236e450473145c24ae0fd	lbordewijk@os3.nl	
SURFnet	098f6bcd4621d373cade4e832627b4f6		test
admin	e4a24c98a8d482747ac52383d57f2b22		
kees	098f6bcd4621d373cade4e832627b4f6	kees.trippelvitz@SURFnet.nl	test
markjonel	d47ed3a0696db95f5f9f6e9a51a9d373	mark@os3.nl	
jan	cc03e747a6afbbcbf8be7668acfebee5	jan.vanlith@SURFnet.nl	test123

Tabel 1: Login tabel

Het is mogelijk om de hashes te kraken door middel van brute force aanval. Dit is vaak een tijdrovende aangelegenheid. Als men 100.000 wachtwoorden per seconde kan proberen, levert dit tabel 2 op.

lengte	**26 (alleen letters)**	**36 (letters&cijfers)**	**52 (case sensetive)**	**96 (all printable)**
4	0	0	1 minuten	13 minuten
5	0	10 minuten	1 uur	22 uren
6	50 minuten	6 uren	2.2 dagen	3 maanden
7	22 uren	9 dagen	4 maanden	23 jaar
8	24 dagen	10.5 maanden	17 jaar	2287 jaar
9	21 maanden	32.6 jaar	881 jaar	219,000 jaar
10	45 jaar	1159 jaar	45,838 jaar	21 miljoen jaar

Tabel 2: Overzicht tijden brute force aanval met 100.000 wachtwoorden per seconde

Er wordt geen gebruikt gemaakt van salt, waardoor een aantal van deze MD5 hashes zijn te achterhalen door middel van online Rainbowtables [12]. De anderen zijn lastiger,

omdat de wachtwoorden meer characters, leestekens en cijfers bevatten. Op dit moment zijn er een aantal grote Rainbowtable projecten online [13]. Het opzoeken van de andere hashes is een kwestie van tijd.

Om op de webservice als admin in te loggen kan een aanvaller met beperkte rechten `checklogin.php` aanpassen en de bovenstaande MD5 hash meegeven. Als admin heeft de aanvaller volledige toegang tot de webservice. Als een aanvaller volledige toegang heeft tot de webservice, kan hij in de webapplicatie het admin wachtwoord veranderen zonder het oude wachtwoord op te geven.

Er is geprobeerd om de admin MD5 hash uit de login tabel van testmachine door te sturen naar `checklogin.php` de pilot productiemachine om te kijken of dezelfde admin wachtwoorden zijn gebruikt. Er is geconstateerd dat op de test- en pilot productiemachines niet dezelfde admin wachtwoorden worden gebruikt.

5.4.2 Root toegang

Wanneer een aanvaller door een van de lokaal gevonden kwetsbaarheden op de honeypot root toegang heeft verkregen, zal een aanvaller waarschijnlijk als eerste een rootkit installeren. Vanaf de honeypot server kunnen de aangesloten instellingen door de tunnels worden aangevallen. Er kan geSSH'ed worden via die tunnels met `ssh -b 'bind adres' 'sensor adres'`. Uit de logfiles blijkt dat er regelmatig geSSH'ed wordt vanaf de honeypot. Met root toegang is het eenvoudig voor een aanvaller om de inloggegevens te onderscheppen.

In de known_host file op de honeypot staan een aantal IP-adressen. Met deze informatie zijn de adressen van de productiemachines te achterhalen, zoals `xxx.SURFnet.nl` en `xxx.SURFnet.nl`.

5.5 Scenario 5 - Aanval vanaf de logserver

De logserver heeft dezelfde kwetsbaarheden als de honeypot, omdat deze qua services en geïnstalleerde packages vrijwel identiek zijn.

Meer informatie over deze kwetsbaarheden is te vinden bijlage 8.2

5.5.1 Beperkte toegang

Met beperkte toegang is de database op de logserver lokaal te bereiken. Pgsql kan gebruikt worden om de database van de IDS dienst uit te lezen. Het wachtwoord is opgeslagen in `/etc/surfnetids/surfnetids-log.conf`.

De logserver is met Tiger gescand, de volgende packages zijn niet up to date:

```
gzip kernel-headers-2.4.27-2-686
perl-modules kernel-image-2.4.27-2-686
perl kernel-source-2.4.27
libperl5.8 libgtk2.0-common
perl-base libgtk2.0-bin
imagemagick libgtk2.0-0
libmagick6 mc
clamav-docs perl-doc
clamav-testfiles perlmagick
libcurl3-dev sudo
libcurl3 unzip
curl libapache2-mod-auth-pgsql
kernel-headers-2.4.27-2
```

Hier volgen een aantal opmerkelijke berichten, waarvan een aantal ook van toepassing waren bij de sensor:

```
# Checking network configuration
--FAIL-- The system is configured to answer to ICMP broadcasts
--FAIL-- The system is not protected against Syn flooding attacks
--FAIL-- The system permits source routing from incoming packets
--WARN-- The system is not configured to log suspicious (martian) packets

--WARN-- The process ‘apache’ is listening on socket webcache is run by root.
--WARN-- The process ‘apache-ss’ is listening on socket 4443 is run by root.
--WARN-- The process ‘apache-ss’ is listening on socket 4443 is run by www-data.
--WARN-- The process ‘dhclient3’ is listening on socket bootpc is run by root.
```

Op dit moment zijn Apache en Dhclient3 niet kwetsbaar. Het is niet verstandig om Apache en Dhclient3 als root te draaien, want wanneer in toekomst een kwetsbaarheid wordt misbruikt, kan willekeurige code via deze kwetsbaarheid met root rechten worden uitgevoerd. De volledige uitvoer van Tiger is te lang en daarom deze niet opgenomen in dit rapport.

5.5.2 Root toegang

Een aanvaller met root rechten heeft volledige controle over de database. Op de logserver staan ook in de known_host file een aantal IP-adressen. Uit de logfiles blijkt dat er regelmatig geSSH’ed wordt vanaf de logserver. Het is eenvoudig voor de een aanvaller om de inloggegevens te onderscheppen.

Vanaf de logserver is geen een andere firewall ruleset van toepassing dan vanaf Internet. Een kwetsbaarheid aanval vanaf de logserver is daarom gelijk aan scenario 6 (aanval vanaf Internet).

5.6 Scenario 6 - Aanval gehele IDS dienst

In dit scenario is een aanval uitgevoerd op de honeypot en de logserver. De poorten zijn met Nmap gescand om te kijken wat voor versies gebruikt worden en/of deze kwetsbaar zijn.

De volgende services zijn beschikbaar vanaf Internet: webservice (443), SSH (22), OpenVPN (1194), SSL (4443). OpenVPN 2.0-1sarge2 bevat op het moment van schrijven geen bekende vulnerability's. Apache httpd 1.3.33 wordt nog steeds onderhouden en wordt op dit moment veilig verondersteld.

De volgende kwetsbaarheden zijn aangetroffen op het honeypot systeem:

- OpenSSL 0.9.7e-3sarge1
- PHP & PGSQL
- HTTP TRACE

OpenSSL 0.9.7e-3sarge1

OpenSSL 0.9.7e-3sarge1 bevat de ASN.1 Parsing kwetsbaarheden. Deze kwetsbaarheden kunnen worden gebruikt om een Denial of Service te veroorzaken of om willekeurige code uit te voeren. De volgende proof-of-concept brute force exploit is voor gedragen door Bram Matthys [10].

PHP & Pgsql

De mod_auth_pgsql0.9.12.1 versie staat een SQL insertion attack toe, waarmee aanvallers arbitrary SQL commando's kunnen uitvoeren.

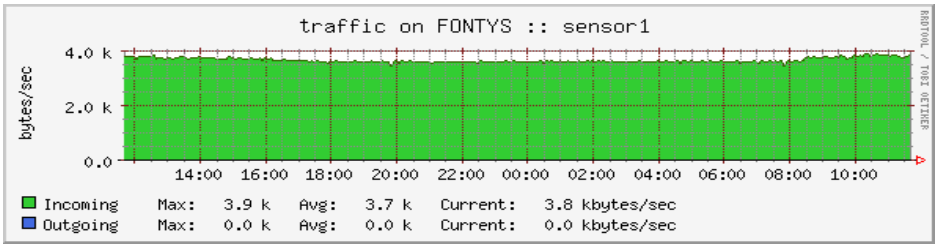
Er zitten twee kwetsbaarheden PHP4: de memory_limit functionaliteit in PHP 4.x t/m 4.3.7 en 5.x up t/m 5.0.0. Als register_globals is ingeschakeld staat het aanvallers vrij om willekeurige code uit te voeren door een memory_limit abort te triggeren tijdens de uitvoering van de zend_hash_init functie.

HTTP TRACE

De HTTP TRACE option is ingeschakeld op de webserver. Gevoelige header informatie kan door aanvallers gelezen worden. Aanvallers kunnen HTTP TRACE misbruiken om toegang te verschaffen tot informatie in HTTP headers, zoals cookies en authenticatie data.

De webaplicatie is gescand, met Nikto. Deze lijst met kwetsbaarheden staat in bijlage 8.2.3.

De volgende directories zijn beschikbaar vanaf Internet: backup, cgi-bin, doc, include, icons, images. Er kunnen onder andere afbeeldingen betreffende de loganalyse bekeken worden. Hier volgt een afbeelding:



Figuur 3: Overzicht van het verkeer op de sensor van Fontys van één dag

Uit de afbeeldingen kan afgeleid worden dat onder andere Fontys, VU, KNMI, LUMC, OnsNET, Philips-GP, UVT, RUG, Roc-nijmegen, Govcert en RIVM sensoren draaien in hun netwerk.

Verder kan een aanvaller door middel van verschillende DoS aanvallen de beschikbaarheid beïnvloeden, zoals Syn flood, DDoS.

5.7 Scenario 7 - Fysieke beveiliging

In scenario 7 is de fysieke beveiliging van de IDS dienst onderzocht. Dit zijn de sensors, honeypot en logserver.

5.7.1 Radboudburcht

De eerste ingang van het kantoor van SURFnet op de Radboudburcht is beveiligd met een elektronisch slot. De pincode (****) makkelijk af te lezen wanneer een andere persoon deze intypt. Men kan meelopen met een persoon die de code intypt. Ook de tweede ingang heeft een elektronisch slot op de deur. Een aanvaller kan hier aanbellen en zeggen dat hij stagiair, schoonmaker of monteur is. Na werktijd rond zeven/acht uur is het vaak vrij rustig in het SURFnet kantoor, op dit tijdstip heeft een aanvaller vermomt als schoonmaker alle tijd om rustig rond te kijken.

SURFnet heeft voor de dienstontwikkeling een testlab server ruimte. In deze server ruimte draaien geen operationele diensten. Wanneer een aanvaller eenmaal binnen is, kan de deze server ruimte vrij gemakkelijk gevonden worden. Om bij de testlab server ruimte te komen, moet men eerst door de mediakamer, waar enkele beheerders pc's staan. De testlab server ruimte heeft geen speciale vorm van toegangsbeveiliging, behalve een slot dat niet wordt gebruikt. Het is vrij eenvoudig deze ruimtes binnen te komen en enkele machines te voorzien van een rootkit en/of een keysnooper te installeren. Nu kan een aanvaller op beheerders pc's en testmachines interessante informatie, zoals wachtwoorden van productiemachines verzamelen.

De echte server ruimte op het SURFnet kantoor bevat echter wel speciale toegangscon-

trole, dit maakt het scenario voor een aanvaller een stuk lastiger, maar niet onmogelijk.

6 Maatregelen

In dit hoofdstuk wordt het doel van de maatregelen behandelt. Vervolgens komen de technische en de niet-technische maatregelen aanbod.

Het is aan te bevelen dat SURFnet door het uitvoeren van maatregelen, de risico's vermindert, waardoor de veiligheid van de IDS dienst toeneemt. Maatregelen kunnen geïmplementeerd worden door middel van technische middelen, zoals computer hardware of software, encryptie, extra IDS mechanismen, identificatie en authenticatie van subsystemen. Andere middelen die kunnen worden geïmplementeerd, zoals security policies, administratieve acties, en fysieke en omgevingsmechanismen, worden beschouwd als niet-technische middelen. Beide technische en niet-technische middelen kunnen verder geclassificeerd worden als preventieve of detective middelen.

Welke maatregelen genomen worden, is onder andere afhankelijk van de classificatie van het netwerk. In Nederland onderscheidt de overheid de volgende categoriën security classificaties: Stg (staatsgeheim) zeer geheim, Stg geheim, Stg confidentieel. Het bedrijfsleven krijgt hier niet vaak mee te maken. In het bedrijfsleven worden de volgende categoriën gehanteerd: gevoelig, vertrouwelijk, privé en publiek. Hoe strenger de categorie, hoe strenger de maatregelen moeten worden. De sensoren draaien op dit moment in netwerken met de classificatie vertrouwelijk, privé en publiek. De aan te bevelen maatregelen in dit hoofdstuk zijn op deze classificaties afgestemd.

6.1 Doel van de maatregelen

Het voornaamste doel van de maatregelen is het geven van informatie voor het veilig implementeren van de SURFnet IDS dienst. De maatregelen zijn gebaseerd op een defense-in-depth-benadering van het beveiligingsontwerp. Dit type ontwerp richt zich op de hypothetische zwakheden en op methoden van risicobeperking. De implementatie van de maatregelen moeten resulteren in een gelaagde aanpak van beveiliging waarbij het onwaarschijnlijk is dat de uitval van één beveiligingssysteem er toe leidt dat de Privacy, Integriteit en Beschikbaarheid gevaar lopen.

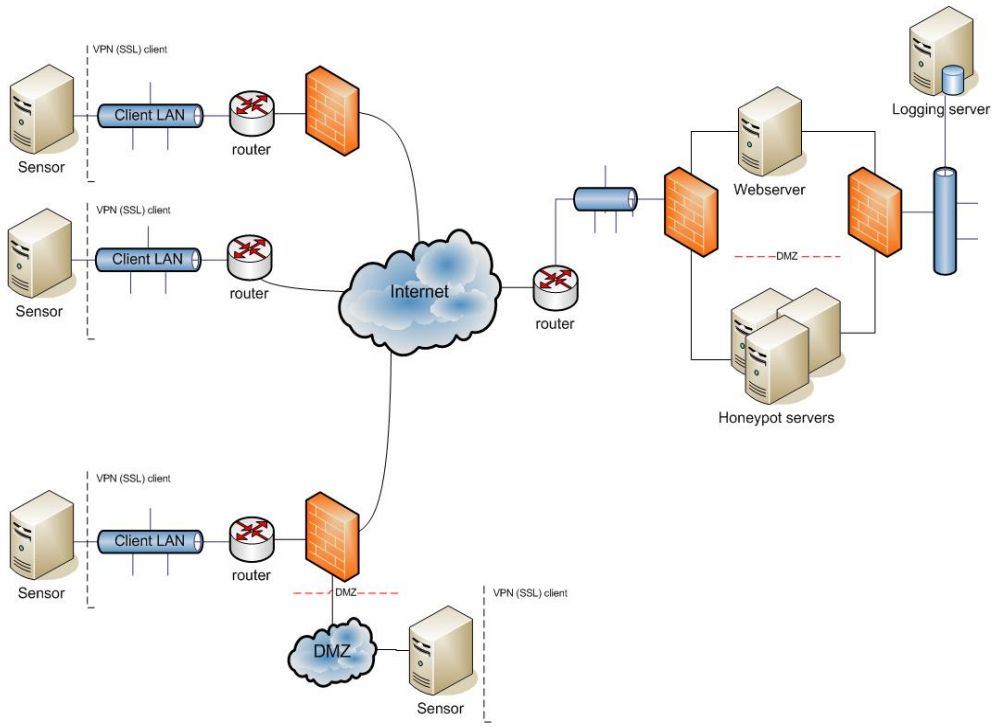
6.2 Technische maatregelen

In deze paragraaf worden de te nemen technische maatregelen behandeld. Als eerst komt kort de keuze van de infrastructuur aanbod. Vervolgens worden maatregelen voor de verschillende componenten uit de infrastructuur beschreven.

6.2.1 Infrastructuur

Sommige bedrijfspolicies staan het niet toe om te tunnelen door de firewall van het bedrijf. Hierdoor is het niet mogelijk om de infrastructuur uit figuur 4 te gebruiken. Als men toch gebruik wil maken van deze IDS oplossing, zou de complete IDS dienst achter de bedrijfs firewall moeten worden geplaatst. Als voor deze oplossing wordt gekozen is er geen communicatie mogelijk met de centrale SURFnet dienst. Als de communicatie met SURFnet wenselijk is, is versleutelde email een alternatief. De gewenste informatie kan via een interne mail server binnen een bedrijf naar SURFnet worden gestuurd. Om de mail te versleuten kan uitstekend gebruik worden gemaakt van de SURFnet PKI certificaten [14].

Wanneer de policies toestaan, dat er door de firewall getunneld mag worden, is het voor de IDS dienst veiliger om de webserver en logserver te scheiden in de huidige infrastructuur. Hierdoor wordt de infrastructuur veiliger en is het efficiënter te schalen in de toekomst. De nieuwe infrastructuur is gegeven in figuur 4.



Figuur 4: Overzicht van de nieuwe infrastructuur

De webserver staat apart en is puur en alleen voor de webservice. Wanneer de IDS groeit kan de honeypot in deze opstelling eenvoudig en veilig gedupliceerd worden. De honeypot en de webserver zijn via een privé subnet gekoppeld aan de logserver. Dit is ervoor om te voorkomen dat onnodige open poorten beschikbaar zijn vanuit andere publieke

netwerken. Deze te nemen maatregel zorgt voor een extra laag in de beveiliging

Er moet een veilig gateway\admin systeem in het privé subnet komen te draaien. Deze machine wordt als gateway gebruikt om in te loggen op de verschillende backend systemen. Het beveiligingsniveau kan verhoogd worden door het authenticatie mechanisme van de gateway te versterken. Een veilige oplossing is two factor authenticatie om in te loggen op de gateway. Hiervoor zou onder andere een Cryptocard RB1 challenge/respone [15] token of een SecurID token [16] kunnen worden gebruikt. Het voordeel van SecurID is dat het centraal gemanaged kan worden. De centrale server maakt de oplossing een stuk duurder dan wanneer men kiest voor een Cryptocard RB1 oplossing. Als een men gebruik wil maken van een voordelige two factor authenticatie voor OpenSSH, is de cryptocard een goede keus.

Verder moeten de systemen waarop ingelogd wordt TCP-wrappers inschakelen. Middels TCP wrappers kan men de toegang tot het systeem beperken, door alleen toegang voor bepaalde IP-adressen toe te staan. TCP wrappers biedt de mogelijkheid de toegang specifiek tot de daemons te beperken. Services zoals SSH bieden ook een dergelijke optie, vanuit beheerdersoogpunt is het beter zijn om de toegang tot de systemen centraal door TCP wrappers te regelen.

Om de technische maatregelen zo overzichtelijk mogelijk weer te geven, worden de maatregelen per component van de IDS dienst beschreven. De volgende componenten worden onderscheiden:

- Sensor
- Webserver
- Logserver
- Honeypot

6.3 Algemene maatregelen

Hier volgen een aantal maatregelen die van toepassing zijn op alle componenten. Voor een juiste basis moet een veilig besturingssystemen worden gekozen. Security staat vaak op gespannen voet met functionaliteit voor de gebruiker van een computersysteem. Linux biedt voor een breed scala aan toepassingen een oplossing die daar goed tussenin zit. Maar voor extreme security is OpenBSD geschikt.

Om de beveiliging verder te optimaliseren moeten de gebruikte systemen gehardened en gestript worden. Filesysteem Integriteits tools moeten geïnstalleerd worden (Tripwire of Aide). Er moet regelmatig geaudit worden. Voor een automatische kwetsbaarheid identificatie zijn een lokale Nessus en Tiger scan geschikt. Om dit regelmatig uit te voeren kunnen de scans in een cronjob geplaatst worden. De audit trails moeten regelmatig geanalyseerd worden en de fysieke beveiliging moet op orde zijn.

6.3.1 Sensor specifieke maatregelen

In deze paragraaf worden de specifieke maatregelen voor de sensor beschreven.

Besturingssysteem:

OpenBSD is in de standaard installatie veiliger als Knoppix, maar de ontwikkelaars hebben gekozen voor Knoppix. Knoppix is vrij eenvoudig te remasteren en te onderhouden. Het systeem is bovendien erg stabiel. Dit komt doordat tijdens de ontwikkeling zorgvuldig naar dit systeem wordt gekeken. Dat zorgvuldig naar het systeem wordt gekeken is tevens ook een nadeel, omdat het meestal langer duurt voordat er nieuwe security fixes uitkomen.

Uit de testen is gebleken dat de huidige Knoppix variant van de sensor een aantal kwetsbaarheden bevat. Deze moeten gepatcht worden. Het systeem moet gehardened worden. Als eerste moeten de gedetecteerde issues van Tiger opgelost worden. De netwerk problemen, zoals Syn flooding en verdachte (martian) pakketen kunnen opgelost worden door een aantal waardes in pseudo `/proc` files uit te schakelen [17].

OpenBSD is een veiliger alternatief, maar lastiger in onderhoud. Het is de vraag of OpenBSD de benodigde functionaliteit kan bieden. Voor een optimale veiligheid raden we OpenBSD aan om te onderzoeken of OpenBSD geschikt is als sensor.

Software:

Hier worden een aantal specifieke sofware maatregelen behandeld om de beveiliging te optimaliseren. Als eerste wordt de firewall behandeld, vervolgens een aantal maatregelen voor OpenSSH, SSL, OpenVPN en een aantal overige zaken.

In totaal zijn er een behoorlijk aantal software packages en hardware devices die niet gebruikt worden. De niet gebruikte software packages moeten als eerste verwijdert worden. De packages die wel gebruikt worden, moeten geupdate worden.

Firewall

Om het netwerk van de aangesloten instellingen te beschermen tegen aanvallen vanaf de honeypot door de tunnel, kan een host-based firewall met IP-tables op de sensors geïnstalleeerd worden. Indien dit realiseerbaar is door de werking van Nepethens niet onmogelijk te maken, zorgt de firewall voor een extra laag in beveiliging. Hoe de firewall exact geconfigureerd moet worden om Nepenthes correct te laten werken moet nader worden onderzocht. Wanneer een sessie vanuit het client LAN naar de Nepenthes wordt opgezet, mag de bijbehorende sessie die terug naar het client LAN gaat alleen door de firewall, dus nieuwe verbindingen vanaf de honeypot mogen niet door de tunnel naar clients in het LAN. Wanneer een honeypot gecompromitteerd wordt kan niet direct het client LAN van een aangesloten instelling worden aangevallen.

OpenSSH

Op dit moment wordt versie 3.8.1.p1 van OpenSSH. Het is aan te raden om de nieuwste versie van SSH versie 4.2 te installeren. Bij deze versie is het niet meer mogelijk IP-adressen uit het known_host bestand te halen.

Het is veiliger als SSH is uitgeschakeld op de sensor. Met behulp van een extra menu optie op de sensor, zou de aangesloten instelling SSH kunnen activeren wanneer het nodig is. Een andere oplossing is port knocking. Met deze techniek, is de TCP poort 22 standaard gesloten. Door een reeks pakketen op verschillende poorten naar de sensor te sturen, wordt de SSH poort opengezet.

Een andere mogelijkheid is `fwknop` [18]. Hiermee kan de SSH poort alleen door middel van een speciaal versleutelt pakket de SSH poort geopend worden. Dit beschermt de service tegen aanvallen, omdat de service eerst geactiveerd moet worden voordat deze reageert.

Een wat duurdere oplossing is het gebruik van tokens.

6.3.2 Webserver

In deze paragraaf worden de specifieke maatregelen voor de webserver beschreven.

Besturingssysteem

De enige functie van de webserver is de PHP webservice beschikbaar stellen via HTTPS. Vanuit beveiligingsoogpunt adviseren we om OpenBSD als besturingssysteem te gebruiken voor de webserver.

Als SURFnet niet kiest om over te stappen op OpenBSD, moeten het besturingssysteem gehardened en geupdate worden. Voor een uitgebreide omschrijving van de hardening van Debian kan de volgende website [20] geraadpleegd worden.

Software

Hieronder komen de eerder genoemde begrippen hardening, strippen en authenticatie als eerste aanbod. Vervolgens worden enkele configuratie aspecten behandeld.

Alle onnodige pakketen moeten verwijderd worden van het systeem (strippen) en de packages als moeten geüpgrade worden naar de nieuwste versie. Zie de testresultaten van de webserver voor een overzicht van de packages 5.5.1. De resultaten van Tiger moeten verwerkt worden [19].

Configuratie webservice

De directory structuur moet worden aangepast en beter beveiligd. Op de website [7] staat een uitgebreide omschrijving met instructies voor de optimalisatie van de beveiliging van de structuur. Verder staat op deze website een interessante beschrijving van een challenge/response implementatie voor PHP, dat de veiligheid van de authenticatie verbeterd.

Om cross-site scripting [5] tegen te gaan moet de TRACE Methode uitgeschakeld worden op de webserver. Dit kan door het volgende in `httpd.conf` te plaatsen:

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^TRACE
RewriteRule .* [F]
```

Authenticatie webservice

De veiligste oplossing tegen een MITM aanval, is de gebruikers van de IDS webservice te voorzien van certificaten van de SURFnet PKI, zodat de gebruikers zich ook kunnen identificeren tegenover de webserver. De certificaten kunnen uitgedeeld kunnen worden door de Root CA van SURFnet. Het scheelt veel tijd en werk als gebruik gemaakt kan worden van een bestaande infrastructuur. Een integratie van een PKI omgeving geeft vertrouwen tegenover de gebruiker.

6.3.3 Honeypot

In deze paragraaf worden de specifieke maatregelen voor de honeypot beschreven.

Besturingssysteem

OpenBSD is in de standaard installatie veiliger als Debian, maar de ontwikkelaars van D-IDS hebben gekozen voor Debian. Debian is vrij eenvoudig onderhouden, maar het duurt gemiddeld langer bij Debian, voordat nieuwe patches uitkomen.

Uit de testen is gebleken dat de gebruikte Debian versie een aantal kwetsbaarheden bevat. Deze moeten gepatcht worden. Het systeem moet worden gehardened. Als eerste moeten de gedetecteerde issues van Tiger opgelost worden. De netwerk problemen, zoals Syn flooding en verdachte (martian) pakketen kunnen opgelost worden door een aantal waardes in pseudo `/proc` files uit te schakelen [17]. Voor een uitgebreide omschrijving van de hardening van Debian kan de volgende website [20] geraadpleegd worden.

OpenBSD is een veiliger alternatief, maar lastiger in onderhoud. Het is de vraag of OpenBSD de benodigde functionaliteit en performance kan bieden. Voor een optimale veiligheid raden we net zoals bij de andere systemen OpenBSD aan om te onderzoeken of OpenBSD geschikt is als sensor.

Software

SSL

Vanaf de sensor worden sleutels via HTTPS aangevraagd bij de honeypot om de OpenVPN verbinding op te zetten. Hiervoor wordt gebruik gemaakt van een gebruikersnaam en wachtwoord, dat in plain text op de USB-stick staat. Op dit moment, is de gebruikersnaam en wachtwoord voor elke aangesloten instelling hetzelfde.

Het zou veiliger zijn om bij de initialisatie van de sensor de gebruikersnaam en wachtwoord handmatig op te geven, dan hoeft deze niet op de USB-stick bewaart te worden. Dit brengt het nadeel met zich mee, dat de gebruiker van de sensor een extra handeling moet uitvoeren bij de initialisatie van de sensor.

Een betere en veiligere maar duurdere oplossing is de certificaten mee te leveren op een USB-token van bijvoorbeeld Aladin [21]. Met deze oplossing is het niet meer mogelijk om een HTTPS MITM aanval uit te voeren.

OpenVPN

Een van de herhaalde spreuken van netwerkveiligheid is dat men nooit vertrouwen in een enkel veiligheidscomponent moet plaatsen. Een fout in een component zou het meteen een rampzalige veiligheidsbreuk kunnen veroorzaken. OpenVPN verzorgt enkele mechanismen om bijkomende veiligheidslagen toe te voegen en het systeem zo beter te beveiligen.

Bij het bestuderen van de configuratie file van de Sensor is er wel degelijk wat gedaan aan security door middel van certificaten en public keys. Om OpenVPN te beveiligen zijn er meer mogelijkheden van beveiliging, zodat als één van de beveiligingslagen wordt doorbroken, er nog meer beveiligingslagen doorbroken moeten worden, om het systeem eigen te maken. Hieronder vindt u verschillende mogelijkheden die toegepast kunnen worden:

- Proto udp
- Tls-auth
- Chroot

Proto UDP OpenVPN 2.0 biedt meer mogelijkheden dan OpenVPN 1.x. Door het aanbieden van een schaalbare client/server dienst, is het mogelijk om met meerdere clients te verbinden op één TCP of UDP poort [22].

OpenVPN kan zowel TCP als de UDP protocol gebruiken, om een OpenVPN verbinding op te zetten. Een veiligheids voordeel ten opzichte van TCP, is dat UPD protocol beter beschermt tegen DoS aanvallen en poort scans. Het wordt daarom aangeraden om gebruik te maken van UDP.

TLS-auth De TLS-auth [22] voegt een bijkomende HMAC handtekening toe aan alle SSL/TLS handshake pakketjes voor de integriteits controle. Elk UDP pakket dat niet de correcte HMAC handtekening draagt, vervalt zonder verdere verwerking.

De TLS-auth HMAC handtekening voegt een bijkomend beveiligingsniveau toe. Het biedt bescherming tegen:

- DoS aanvallen of port flooding op de OpenVPN UDP poort;
- Poort scannen om vast te stellen welke server UPD poorten in luister mode staan;

- Buffer overflow kwetsbaarheden in de SSL/TLS implementatie.

Chroot Chroot zorgt ervoor dat OpenVPN in een zogenaamde chroot gevangenis wordt opgesloten. Eenmaal ingesloten kan de OpenVPN service geen toegang krijgen tot de rest van het systeem bestandsysteem, behalve zijn eigen aangewezen directory.

Het toepassen van chroot brengt veel voordelen met zich op het gebied van security, maar het heeft ook zijn nadelen. Zo moeten de bestanden die OpenVPN gebruikt voor de initialisatie ook in de chroot directory staan om goed te functioneren. Er wordt geadviseerd om te onderzoeken of het past in de structuur van het IDS project.

Man-in-the-Middle Om een mogelijke MITM aanval te vermijden waar een gemachtigde client verbinding probeert te maken met een andere aanvaller, die de server imiteert, is het belangrijk dat een server certificaat controle wordt afgedwongen door de clients. Deze server certificaat controle zorgt voor de verificatie van de identiteit van de server. Om beter bestand te zijn tegen een MITM aanval en om het systeem veiliger te maken, moet er van 'build-key-server [23] gebruik gemaakt worden in plaats van "build-key". Hier volgen een aantal andere mogelijkheden:

- gebruik van TLS-remote;
- gebruik van TLS-verify script;

Zie voor meer uitleg de OpenVPN configuratie [23] [25];

Nepenthes

Nepenthes is een relatief nieuw product waardoor de source code waarschijnlijk nog niet volledig geaudit is. De test resultaten van Nepenthes beschrijven een aantal mogelijkheden voor buffer overflows en format string kwetsbaarheden. Hierdoor kan de Nepenthes een zwak punt in beveiliging van de IDS dienst zijn. We raden aan om de source code van het product zelf of te laten auditen, om de risico's te kunnen vaststellen en beoordelen.

6.4 Fysieke beveiliging machines

Deze paragraaf beschrijft de algemene preventieve beveiligingsmaatregelen voor alle componenten van IDS dienst.

De bootloaders en de BIOS moeten met een wachtwoord beveiligd worden. De harde schijf mag het enige apparaat zijn waarvan opgestart kan worden, zodat er niet vanaf een ander medium geboot kan worden. De behuizingen moeten goed worden afgesloten, zodat de bios niet snel gereset kan worden.

Een dure oplossing is het gebruik van safeboot met tokens om de schijven te versleutelen. Dit is op dit moment een goede oplossing om schijven te versleutelen, omdat deze oplossing de privacy garandeert van de gegevens wanneer het systeem niet is opgestart.

6.5 Niet-technische maatregelen

6.5.1 Taken voor beheer

Het is belangrijk dat de beheerders van de IDS dienst dagelijks verschillende mailinglijsten, nieuwsgroepen en websites monitoren om continu op de hoogte te blijven van de nieuwste kwetsbaarheden in de gebruikte besturingssystemen en software. Dit lijkt vanzelfsprekend maar wordt vaak vergeten door systeembeheer.

7 Conclusie

Dit adviesrapport beschrijft het beveiligingsonderzoek van de SURFnet IDS dienst. Het onderzoek beantwoordt de vraag hoe veilig de huidige implementatie van de SURFnet IDS dienst is en welke maatregelen er genomen moeten worden om het systeem veiliger te kunnen inzetten in netwerken van instellingen die aangesloten zijn bij SURFnet.

SURFnet biedt een mooie schaalbare en eenvoudig te beheren en onderhouden IDS dienst. De IDS dienst is op moment nog relatief jong en vrij complex waardoor het lastig is om alle punten exact te verifiëren die kunnen leiden tot beveiligingsproblemen.

Na dit onderzoek kunnen we concluderen dat de IDS dienst enkele beveiligingsproblemen kent. De meest belangrijke problemen hebben te maken met updates, configuratie/hardening, encryptie en implementatie fouten.

Het totale beveiligingspakket van de IDS moet op orde zijn om niet alleen de gebruikelijke hackpogingen de baas te blijven, maar ook social engineering de kop in te kunnen drukken. In het onderzoek zijn bij de SURFnet D-IDS dienst een aantal beveiligingsrisico's geconstateerd. Om deze risico's te verminderen, is het belangrijk de in dit rapport opgesomde maatregelen consequent door te voeren. Wel moet gerealiseerd worden dat risico's nooit volledig geëlimineerd kunnen worden. Bij het doorvoeren van de aanbevolen maatregelen moet onder andere gekeken worden naar de kosten van implementatie. Deze kosten moeten opwegen tegen de voordelen die deze maatregelen met zich brengen. Afhankelijk van het budget en de classificatie van de data zullen de duurdere maatregelen afvallen. Daarnaast kan gebruiksgemak voor de afnemers van de dienst en gebruiksgemak voor de beheerders van de dienst doorslaggevend zijn bij de door SURFnet te maken keuzes. Mogelijk zal dit rapport SURFnet kunnen helpen bij het kiezen van een best-effort oplossing.

7.1 Toekomst

Uit het is onderzoek is gebleken dat een aantal zaken nader onderzocht moeten worden. Geadviseerd wordt om een audit op Nepenthes te laten uitvoeren om er zeker van te kunnen zijn dat de software veilig veronderstelt kan worden.

Een juiste implementatie van IP-tables op de sensoren en OpenBSD als vervanging van de besturingssystemen op de sensor, honeypot en logserver moet nog nader worden onderzocht.

Alle maatregelen moeten gereflecteerd worden in een security checklist voor de beheerders.

Ten slotte moeten policies worden opgesteld voor: het beheer van de dienst, voor de wachtwoorden, de veiligheid en het maken nieuwe sensoren. Het naleven van de policies verlaagt het risico op compromitteringen en verhoogt het beveiligingsniveau van de IDS dienst.

8 Bijlage I - Overzicht kwetsbaarheden machines van SURFnet IDS

In deze bijlage worden van alle machines betreffende het SURFnet IDS de kwetsbaarheden beschreven.

8.1 Sensor

8.1.1 Nessus scan

Problems regarding : ssh (22/tcp)

Security warnings :

- The remote SSH daemon supports connections made
  using the version 1.33 and/or 1.5 of the SSH protocol.

  These protocols are not completely cryptographically
  safe so they should not be used.

  Solution :
   If you use OpenSSH, set the option 'Protocol' to '2'
   If you use SSH.com's set the option 'Ssh1Compatibility' to 'no'

  Risk factor : Low

Security note :

- An ssh server is running on this port
- It was possible to log into the remote host using the supplied
   password
  The output of "uname -a" is :
  Linux Knoppix 2.6.11 #2 SMP Thu May 26 20:53:11 CEST 2005 i686
   GNU/Linux

  The remote Debian system is :
  3.1

  Local security checks have been enabled for this host.
- Remote SSH version : SSH-1.99-OpenSSH_3.8.1p1 Debian-8.sarge.4

```
Remote SSH supported authentication :
 publickey,password,keyboard-interactive
```

- The remote SSH daemon supports the following versions of the SSH protocol :

  . 1.33
  . 1.5
  . 1.99
  . 2.0

```
SSHv1 host key fingerprint :
 f6:04:d2:ab:52:de:1d:23:82:8e:6e:0f:04:41:5a:b5
SSHv2 host key fingerprint :
 04:92:db:b6:20:9c:9c:d1:4b:9f:bf:a4:bf:36:34:6b
```

Problems regarding : bootpc (68/tcp)

Security note :

- The service closed the connection after 0 seconds without sending any data
  It might be protected by some TCP wrapper

Problems regarding : general/icmp

Security note :

- Synopsis :

  It is possible to determine the exact time set on the remote host.

  Description :

  The remote host answers to an ICMP timestamp request. This allows an

```
 attacker
to know the date which is set on your machine.

This may help him to defeat all your time based authentication
 protocols.

Solution : filter out the ICMP timestamp requests (13), and the
 outgoing ICMP
timestamp replies (14).

Risk factor :

None / CVSS Base Score : 0
(AV:R/AC:L/Au:NR/C:N/A:N/I:N/B:N)
CVE : CVE-1999-0524
```

Security note :

- The remote host is running Linux Kernel 2.6
-

```
Information about this scan :

Nessus version : 3.0.1
Plugin feed version : 200602031215
Type of plugin feed : Registered (7 days delay)
Scanner IP : 192.xxx.xxx.xxx
Port scanner(s) : nessus_tcp_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Max hosts : 20
Max checks : 4
Scan Start Date : 2006/2/3 20:12
Scan duration : 163 sec
```

8.1.2 Nmap scan

```
nmap -A -T4 -P0 -F 192.xxx.xxx.xxx
```

```
PORT   STATE SERVICE     VERSION
22/tcp open  SSH         OpenSSH 3.8.1p1 Debian-8.sarge.4 (protocol 1.99)
68/tcp open  dhcpclient?

Device type: general purpose
Running: Linux 2.4.X|2.5.X|2.6.X
OS details: Linux 2.4.18 - 2.6.7
Uptime 0.008 days (since Tue Jan 24 15:51:06 2006)

Nmap finished: 1 IP address (1 host up) scanned in 5.123 seconds
```

8.1.3 National vulnerability database

Kernel

```
Original release date: 3/9/2005
Last revised: 10/20/2005
Source: US-CERT/NIST


Overview

Integer overflow in sys\_epoll\_wait in eventpoll.c for Linux kernel 2.6 to
2.6.11 allows local users to overwrite kernel memory via a large number of events.


Impact

CVSS Severity: 2.3 (Low) Approximated
Range: Locally exploitable
Impact Type: Allows unauthorized modificatio
```

OpenSSH

```
1

Original release date: 1/25/2006
Last revised: 1/25/2006
```

```
Source: US-CERT/NIST
 Overview
scp in OpenSSH 4.2p1 allows attackers to execute arbitrary commands via filenames
that contain shell metacharacters or spaces, which are expanded twice.
 Impact

CVSS Severity: 4.9 (Medium)
Range: Locally exploitable
Authentication: Not required to exploit
Impact Type: Provides user account access
 References to Advisories, Solutions, and Tools
External Source:  SECUNIA (disclaimer)
Name: 18595
Type:  Advisory , Patch Information
Hyperlink: http://secunia.com/advisories/18595
 External Source: (disclaimer)
Hyperlink: https://bugzilla.redhat.com/bugzilla/show\_bug.cgi?id=174026
 External Source:  BID (disclaimer)
Name: 16369
Hyperlink: http://www.securityfocus.com/bid/16369
 External Source:  FRSIRT (disclaimer)
Name: ADV-2006-0306
Type:  Advisory
Hyperlink: http://www.frsirt.com/english/advisories/2006/0306
 External Source:  SECUNIA (disclaimer)
Name: 18579
Hyperlink: http://secunia.com/advisories/18579

Vulnerable software and versions

OpenSSH, OpenSSH, 3.8.1 p1
OpenSSH, OpenSSH, 3.8.1
OpenSSH, OpenSSH, 3.9
OpenSSH, OpenSSH, 3.9.1 p1
OpenSSH, OpenSSH, 3.9.1
OpenSSH, OpenSSH, 4.0 p1
OpenSSH, OpenSSH, 4.1 p1
OpenSSH, OpenSSH, 4.2 p1

Technical Details

CVSS Base Score Vector: (AV:L/AC:L/Au:NR/C:P/I:P/A:P/B:N) (legend)
```

```
Vulnerability Type: Input Validation Error

CVE Standard Vulnerability Entry:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0225


2

Original release date: 8/23/2005
Last revised: 10/20/2005
Source: US-CERT/NIST

Overview

SSH, as implemented in OpenSSH before 4.0 and possibly other implementations,
stores hostnames, IP addresses, and keys in plaintext in the known\_hosts file,
which makes it easier for an attacker that has compromised an SSH user's account
to generate a list of additional targets that are more likely to have the same
password or key.

Impact

CVSS Severity: 2.3 (Low) Approximated
Range: Locally exploitable
Impact Type: Allows unauthorized disclosure of information

References to Advisories, Solutions, and Tools

External Source:  MIT (disclaimer)
Name: Protecting SSH from known\_hosts Address Harvesting
Type:  Patch Information
Hyperlink: http://nms.csail.mit.edu/projects/SSH/

External Source:  EWEEK (disclaimer)
Name: Researchers Reveal Holes in Grid
Hyperlink: http://www.eweek.com/article2/0,1759,1815795,00.asp

Vulnerable software and versions

OpenSSH, OpenSSH, 3.8
OpenSSH, OpenSSH, 3.8.1 p1
OpenSSH, OpenSSH, 3.8.1
OpenSSH, OpenSSH, 3.9
```

```
OpenSSH, OpenSSH, 3.9.1 p1
OpenSSH, OpenSSH, 3.9.1

Technical Details

CVSS Base Score Vector: (AV:L/AC:L/Au:NR/C:C/I:N/A:N/B:N)

Vulnerability Type: Design Error

CVE Standard Vulnerability Entry:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-2666
```

8.2 Honey.spoor.nu

8.2.1 Nessus scan

Problems regarding : SSH (22/tcp)

Security note :

- An SSH server is running on this port
- It was possible to log into the remote host using the supplied password
  The output of "uname -a" is :
  Linux honey 2.4.27-2-686 #1 Mon May 16 17:03:22 JST 2005 i686 GNU/Linux

  The remote Debian system is :
  3.1

  Local security checks have been enabled for this host.
- Remote SSH version : SSH-2.0-OpenSSH_3.8.1p1 Debian-8.sarge.4

  Remote SSH supported authentication : publickey,keyboard-interactive

- The remote SSH daemon supports the following versions of the SSH protocol :

  . 1.99
  . 2.0

```
SSHv2 host key fingerprint :
 6f:36:47:a7:30:e2:6e:c9:75:60:39:8a:dc:c1:84:aa
```

Problems regarding : http-alt (8080/tcp)

Security note :

- A web server is running on this port
- Synopsis :

  Debugging functions are enabled on the remote HTTP server.

  Description :

  The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK
  are HTTP methods which are used to debug web server connections.

  It has been shown that servers supporting this method are subject to
  cross-site-scripting attacks, dubbed XST for "Cross-Site-Tracing", when
  used in conjunction with various weaknesses in browsers.

  An attacker may use this flaw to trick your legitimate web users to give
  him their credentials.

  Solution :

  Disable these methods.

  See also :

  http://www.kb.cert.org/vuls/id/867593

  Risk factor :

  Low / CVSS Base Score : 2
  (AV:R/AC:L/Au:NR/C:P/A:N/I:N/B:N)

```
Plugin output :


Solution :
Add the following lines for each virtual host in your configuration
 file :

    RewriteEngine on
    RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
    RewriteRule .* - [F]


CVE : CVE-2004-2320
BID : 9506, 9561, 11604
```

- The following directories were discovered:
  /backup, /cgi-bin, /doc, /include, /icons, /images

  While this is not, in and of itself, a bug, you should manually
   inspect
  these directories to ensure that they are in compliance with company
  security standards

  Other references : OWASP:OWASP-CM-006

- The remote web server type is :

  Apache/1.3.33 (Debian GNU/Linux) PHP/4.3.10-16
   mod_auth_pgsql/0.9.12.1

  Solution : You can set the directive 'ServerTokens Prod' to limit
  the information emanating from the server in its response headers.

Problems regarding : general/tcp

Security holes :

- A vulnerability was discovered in Midnight Commander, a file manager,
  whereby a malicious archive (such as a .tar file) could cause
  arbitrary code to be executed if opened by Midnight Commander.
  For the current stable distribution (woody) this problem has been

fixed in version 4.5.55-1.2woody2.
For the unstable distribution (sid) this problem has been fixed in
version 1:4.6.0-4.6.1-pre1-1.
We recommend that you update your mc package.

Solution : http://www.debian.org/security/2004/dsa-424
Risk factor : High
The package mc is vulnerable in Debian 3.1.
Upgrade to mc_1:4.6.0-4.6.1-pre1-1

CVE : CVE-2003-1023
BID : 8658
Other references : DSA:424

- Two vulnerabilities were discovered in php4:
  The memory_limit functionality in PHP 4.x up to
  4.3.7, and 5.x up to 5.0.0RC3, under certain conditions such as
  when register_globals is enabled, allows remote attackers to
  execute arbitrary code by triggering a memory_limit abort during
  execution of the zend_hash_init function and overwriting a
  HashTable destructor pointer before the initialization of key data
  structures is complete.
  The strip_tags function in PHP 4.x up to 4.3.7, and
  5.x up to 5.0.0RC3, does not filter null (\0) characters within tag
  names when restricting input to allowed tags, which allows
  dangerous tags to be processed by web browsers such as Internet
  Explorer and Safari, which ignore null characters and facilitate
  the exploitation of cross-site scripting (XSS) vulnerabilities.
  For the current stable distribution (woody), these problems have been
  fixed in version 4.1.2-7.
  For the unstable distribution (sid), these problems have been fixed in
  version 4:4.3.8-1.
  We recommend that you update your php4 package.

  Solution : http://www.debian.org/security/2004/dsa-531
  Risk factor : High
  The package php4 is vulnerable in Debian 3.1.
  Upgrade to php4_4:4.3.8-1

  CVE : CVE-2004-0594, CVE-2004-0595
  Other references : DSA:531

- imagemagick's libmagick library, under certain circumstances, creates temporary files without taking appropriate security precautions. This vulnerability could be exploited by a local user to create or overwrite files with the privileges of another user who is invoking a program using this library.
  For the stable distribution (woody) this problem has been fixed in version 4:5.4.4.5-1woody1.
  For the unstable distribution (sid) this problem has been fixed in version 4:5.5.7-1.
  We recommend that you update your imagemagick package.

  Solution : http://www.debian.org/security/2003/dsa-331
  Risk factor : High
  The package imagemagick is vulnerable in Debian 3.1.
  Upgrade to imagemagick_4:5.5.7-1

  CVE : CVE-2003-0455
  BID : 8057
  Other references : DSA:331

8.2.2 National vulnerability database

PostgreSQL

Vulnerability Summary CVE-2006-0410
Original release date: 1/24/2006
Last revised: 1/25/2006
Source: US-CERT/NIST

Overview

SQL injection vulnerability in ADOdb before 4.71, when using PostgreSQL, allows remote attackers to execute arbitrary SQL commands via unspecified attack vectors involving binary strings.

Impact

CVSS Severity: 2.3 (Low)
Range: Remotely exploitable

```
Authentication: Not required to exploit
Impact Type: Allows unauthorized modification

CVE-2005-1410      OVAL1086
Summary: The tsearch2 module in PostgreSQL 7.4 through 8.0.x declares the (1)
dex_init, (2) snb_en_init, (3) snb_ru_init, (4) spell_init, and (5) syn_init
functions as "internal" even when they do not take an internal argument, which
allows attackers to cause a denial of service (application crash) and possibly
have other impacts via SQL commands that call other functions that accept
internal arguments.

Published: 5/3/2005

CVSS Severity: 2.3 (Low) Approximated


CVE-2005-0227
Summary: PostgreSQL (pgsql) 7.4.x, 7.2.x, and other versions allows local users
to load arbitrary shared libraries and execute code via the LOAD extension.

Published: 5/2/2005

CVSS Severity: 4.9 (Medium) Approximated

CVE-2004-0977  The make_oidjoins_check script in PostgreSQL 7.4.5 and earlier
allows local users to overwrite files via a symlink attack on temporary files.

PostgreSQL LOAD Extension Local Privilege Escalation Vulnerability,
http://www.securityfocus.com/bid/12411
```

8.2.3 Nikto - Web server scanner

```
code//webinterface/include/nusoap.php:6983: High: eval
Argument 1 to this function call should be checked to ensure that it does not
come from an untrusted source without first verifying that it contains nothing
dangerous.

code//webinterface/include/functions.inc.php:30: High: fopen
code//webinterface/include/nusoap.php:3277: High: fopen
code//webinterface/include/nusoap.php:4276: High: fopen
Argument 1 to this function call should be checked to ensure that it does not
come from an untrusted source without first verifying that it contains nothing
```

```
dangerous.

code//webinterface/whois.php:21: Medium: fsockopen
code//webinterface/include/nusoap.php:2123: Medium: fsockopen
code//webinterface/include/nusoap.php:2125: Medium: fsockopen
Argument 1 to this function call should be checked to ensure that it does not
come from an untrusted source without first verifying that it contains nothing
dangerous.
```

Referenties

[1] Website penetratie test http://www.penetration-testing.com

[2] Website van de SURFnet IDS dienst , http://ids.SURFnet.nl

[3] Packages op honeypot server http://ids.surfnet.nl

[4] SURFnet IDS website http://ids.SURFnet.nl/server/iptables.php

[5] Cross site scripting http://www.secguru.com

[6] Knoppix Remastering http://www.knoppix.net/wiki/Knoppix_Remastering_Howto

[7] Nmap http://www.insecure.org/nmap/

[8] Hping Hping http://www.hping.org/

[9] Rough Auditing Tool for Security http://www.securesoftware.com/resources/download_rats.html

[10] Exploit lokale SSH kwetsbaarheid http://downloads.securityfocus.com

[11] Omschrijving known_host bestand http://nms.csail.mit.edu/projects/ssh/

[12] Rainbow Crack Home http://rainbowcrack.com/

[13] Rainbow Crack online http://www.rainbowcrack-online.com/

[14] PKI http://pki.surfnet.nl

[15] Cryptocard RB1 token http://www.cryptocard.com

[16] SecurID en OpenSSH http://www.omniti.com

[17] Linux netwerk gerelateerde protecties http://www.hackinglinuxexposed.com

[18] Fwknop http://www.cipherdyne.org

[19] Tiger Tool http://www.nongnu.org/tiger/

[20] Harden Debian http://www.debian.org

[21] Aladin E-token http://www.aladdin.com

[22] Proto udp http://www.imped.net/oss/misc/openvpn-2.0-howto-edit.html#security

[23] Man in the middle security how to http://www.imped.net

[24] OpenVPN howto http://openvpn.net/howto.html

[25] VPN-Configs http://www.batcom-it.net