Onderzoeksrapport RP1: IDS

Arjan Dekker en Carlos Groen

v1.0 04-02-2005

Inhoudsopgave

1 Voorwoord

In het kader van onze studie System en Netwerkbeheer aan de Universiteit van Amsterdam hebben we vier weken lang onderzoek gedaan naar Intrusion Detection en de toepassingen en beperkingen ervan. Hierbij hebben we ons vooral gericht op detectie verspreid over een aantal netwerken en systemen met de mogelijkheid centraal te registreren en beheren. We hebben gekeken naar aan aantal bekende commerciële en open-source producten, waarbij we dieper zijn ingegaan op de laatste variant.

Onze begeleider in dit project was Fred Mobach, die een bedrijf heeft gespecialiseerd in het ontwerpen en beheren van netwerken en beveiliging. In samenspraak met hem hebben we een lijst van eisen en wensen opgesteld waaraan een gedistribueerd IDS moet voldoen en hij heeft ons gedurende het project begeleid.

2 Intrusion Detection

Intrusion Detection is de benaming voor een set van methoden en technieken die wordt gebruikt voor het detecteren van inbraakpogingen en ongeauthoriseerd gebruik van systemen of netwerken. Met behulp van een Intrusion Detection System (IDS) kan een systeembeheerder de bron en aard van aanvallen detecteren en analyseren. Een IDS is te vergelijken met een inbraaksysteem. Het houdt een inbreker niet tegen maar het geeft wel een waarschuwing bij onraad zodat er maatregelen genomen kunnen worden om de schade te beperken of in de toekomst te voorkomen.

Intrusion detection is gebaseerd op een tweetal technieken. De eerste is gebaseerd op het herkennen van schadelijke activiteiten op basis van bekende eigenschappen, het zogenaamde *signature-based* IDS. De effectiviteit hiervan is geheel afhankelijk van de gebruikte database met signatures, de zogenaamde *ruleset*. Het is van belang dat deze goed wordt geconfigureerd en regelmatig wordt geupdate om het aantal *false-positives* en *false-negatives* te minimaliseren.

Een andere methode is gebaseerd op het herkennen van ongebruikelijke activiteiten. Dit wordt *anomality-based* IDS genoemd. Hierbij wordt gekeken naar wat normaal netwerkverkeer of systeemactiviteit is en wordt er melding gegeven zodra er afwijkingen zijn. Deze methode biedt de mogelijkheid om aanvallen te detecteren die nog niet bekend zijn maar biedt ook een grotere kans op false-positives.

Intrusion Detection Systems zijn grofweg onder te verdelen in twee categorieën: Host-based en Network-based. Beide systemen hebben hun mogelijkheden en hun beperkingen. Een systeem dat beide doet wordt een Hybrid IDS genoemd.

2.1 Network-based Intrusion Detection (NIDS)

De werking van een Network-based IDS is gebaseerd op het analyseren van netwerkverkeer binnen een bepaald netwerksegment. Hierbij werkt een netwerkinterface in *promiscuous* mode, dat wil zeggen dat de interface niet alleen het verkeer ontvangt dat voor hem bedoeld is maar openstaat voor al het netwerkverkeer op het segment. Zowel inkomend als uitgaand verkeer wordt bekeken. Aanvallen komen immers niet alleen van buitenaf, ook binnen het eigen netwerk kunnen virussen of wormen actief zijn of inbraakpogingen worden ondernomen.

Een NIDS kan op diverse plaatsen in het netwerk worden ingezet. Vóór een firewall detecteert het al het verkeer dat voor het netwerk bestemd is, ook het verkeer dat door de firewall wordt tegengehouden. Achter de firewall detecteert het alleen het uitgaande verkeer en het verkeer dat door de firewall wordt doorgelaten. Een toepassing hiervan is het testen van de firewall configuratie.

Een NIDS stelt bepaalde eisen aan de hardware. Des te sneller de verbinding, des te meer dataverkeer het NIDS per tijdseenheid moet bekijken. Indien het NIDS de hoeveelheid data niet bij kan houden slaat het pakketjes over en bestaat de kans dat kwaadaardige verkeer wordt gemist. De minimale hardware (op basis van de x86 architectuur) nodig voor de analyse van een 100Mbit netwerk bestaat uit:

- 1GHz Processor
- Snelheid bus minimaal 266 MHz
- 256 MB intern geheugen
- Snelle harde schijf van minimaal 20 GB (minimaal 7.200 RPM)

Voorbeelden van aanvallen die door een NIDS gedetecteerd kunnen worden zijn:

- Portscans
- Vulnerability scans op services
- Ongewoon of misvormd netwerkverkeer
- Denial of service aanvallen (DOS attacks)
- Verkeer gegenereerd door virussen en worms

Voordelen van een NIDS ten opzichte van een HIDS zijn:

- Er is maar één systeem nodig, dat al het netwerkverkeer in de gaten houdt.
- Realtime: netwerkverkeer wordt direct geanalyseerd wanneer het pakket langskomt.

- Wanneer een persoon toegang heeft verkregen tot een systeem is het mogelijk om de sporen te wissen. Dit lukt niet met behulp van een NIDS.
- Verkeer dat normaal gesproken door de firewall wordt geblokkeerd kan toch nuttige informatie verschaffen. Een NIDS buiten de firewall kan dit verkeer analyseren, een HIDS niet.
- Real-time waarschuwing van de verantwoordelijke persoon op het moment dat een aanval plaatsvindt.
- Het NIDS hoeft geen kennis te hebben van het achterliggende netwerk en de gebruikte besturingssystemen.

Een aantal bekende Network-based Intrusion Detection Systems:

Snort Snort is de meest populaire signature-based NIDS op dit moment. Het is volledig open-source, waardoor er een grote actieve community dit project steunt. Dankzij deze community blijven de rules up to date en zijn er veel uitbreidingen ontwikkeld voor Snort.

Snort is een pure netwerksensor. Het bekijkt zoveel mogelijk netwerkverkeer en vergelijkt de inhoud van het verkeer met die van zijn rules. Wanneer een rule overeenkomt met de inhoud van een datapakket wordt er een melding gegeven. Deze melding kan worden opgeslagen in de logfiles of in een database. De meldingen kunnen vervolgens met verschillende grafische applicaties worden bekeken, zoals SnortReport en ACID.

Snort kan worden gebruikt onder verschillende besturingssystemen, zoals Windows en alle Unix-achtige distributies. Een nadeel van Snort is dat er standaard geen mogelijkheid aanwezig is om gedistribueerd te werken. Dit kan overigens wel met behulp van een aantal andere applicaties gerealiseerd worden.

Een uitgebreidere beschrijving van Snort en de software die ervoor geschreven is, is te vinden in de appendices.

RealSecure Network RealSecure Network is een commercieël NIDS. Het bestaat uit een sensor en een component dat de gegevens uitwisselt met een centrale server door middel van public key technologie. Installatie, configuratie en het bekijken van de sensoren kan met behulp van een zeer verzorgde GUI worden gedaan. Hierdoor is het beheer van deze IDS eenvoudiger gemaakt.

RealSecure Network gebruikt zijn eigen rules maar heeft ook de mogelijkheid rules van Snort te importeren. Omdat de applicatie niet open-source is, zijn er minder personen die ervoor zorgen dat het product up to date blijft. Uitbreidingen en verbeteringen moeten door de ontwikkelaar worden uitgevoerd, tegen een prijs.

Een nadeel van RealSecure Network is dat er verschillende versies zijn, voor de verschillende netwerksnelheden. Een 100Mbit versie werkt niet op een 1Gbit lijn en andersom, waardoor na een verhoging van de netwerksnelheid weer nieuwe producten moeten worden aangeschaft.

RealSecure Network is verkrijgbaar voor Windows, Linux en Sun Solaris.

Computer Associates eTrust Intrusion Detection eTrust Intrusion Detection is een NIDS met een aantal Intrusion Prevention System (IPS) mogelijkheden. Wanneer gevaarlijk netwerkverkeer gedetecteerd wordt, is het mogelijk de afzender hiervan tijdelijk te blokkeren. De meldingen gegenereerd door eTrust Intrusion Detection worden opgeslagen in een centrale database en kunnen worden bekeken met behulp van een GUI. eTrust Intrusion Detection onderhoudt zijn eigen rules, welke automatisch worden geupdate op vooraf ingestelde tijden.

eTrust Intrusion Detection is alleen verkrijgbaar voor een Windows-omgeving.

2.2 Host-based Intrusion Detection (HIDS)

Een Host-based IDS is actief op een enkel systeem en heeft als functie het detecteren van aanvallen of ongeregeldheden op dat specifieke systeem. Dit doet het door het bekijken en analyseren van logfiles, system calls, veranderingen in policies en bestanden en het netwerkverkeer dat het systeem binnenkomt of uitgaat.

Ongeregeldheden die door een HIDS kunnen worden gedetecteerd zijn:

- Mislukte pogingen om in te loggen
- Het onrechtmatig starten, herstarten of beëindigen van daemons of processen
- Onrechtmatig of overmatig gebruik van system resources
- Ongewone veranderingen in bestanden of het bestandssysteem
- Ongewone wijzigingen in de systeemconfiguratie, policy of wachtwoorden

Voordelen van een HIDS ten opzichte van een NIDS zijn:

- Er is geen extra hardware nodig, een HIDS wordt geïnstalleerd op bestaande systemen.
- Meer informatie beschikbaar over of een aanval gelukt is.
- Detecteert aanvallen op het systeem waarbij een persoon fysiek toegang heeft tot de machine.

- Kan de inhoud van pakketten analyseren die versleuteld worden verstuurd en zo niet door een NIDS kunnen worden bekeken.
- Kan netwerkverkeer analyseren dat voor de host bestemd is en niet bij een NIDS aankomt, bijvoorbeeld in een switched netwerk.
- Geeft ook informatie over het algeheel gebruik van het systeem, zoals system calls en gebruikte system resources.

Een aantal bekende Host-based Intrusion Detection Systems:

Logwatch Logwatch is een open-source applicatie. Logwatch genereert een email op vooraf ingestelde tijden met daarin een samenvatting van de gelogde gegevens. Logwatch haalt dubbele gegevens eruit en onbekende gegevens worden niet geclassificeerd maar wel in de samenvatting opgenomen. Onregelmatigheden zijn door middel van deze samenvatting te ontdekken. Logwatch is gemakkelijk uitbreidbaar en te installeren.

Logwatch is alleen onder Unix-achtige besturingssystemen te gebruiken.

Logcheck Logcheck is een soortgelijke applicatie als Logwatch. Logcheck genereert ook emails met gegevens uit de logfiles. De emails van Logwatch zijn overzichtelijker, maar gebruiken meer system resources om gegenereerd te worden dan die van Logcheck. De emails gemaakt door Logcheck kunnen daarom vaker gegenereerd worden. Het onderhoud van Logcheck gaat op een soortgelijke manier als dat van Logwatch.

Logcheck is ook alleen voor Unix-achtige besturingssystemen beschikbaar.

Samhain De voorgaande HIDS software gebruikte de logfiles voor het verkrijgen van informatie. Samhain werkt op een andere manier. Samhain slaat in een database gegevens op over bestanden en directories, zoals een hash van het bestand, rechten en de grootte. Wanneer na het vergelijken van de gegevens op de schijf en de gegevens in de database veranderingen zijn geconstateerd, wordt een melding gegeven. Samhain bestaat uit een client en een server deel. De gegevens tussen de client en de server worden versleuteld verstuurd. Samhain kan beschikken over een GUI voor het weergeven van meldingen, genaamd Beltane.

Samhain is alleen beschikbaar voor Unix-achtige omgevingen, maar met behulp van Cygwin (een Unix emulator) kan het ook onder Windows worden gebruikt.

Tripwire Tripwire is van oorsprong een commercieële applicatie die een vergelijkbare werking heeft als Samhain. De makers van Tripwire hebben een open-source versie vrijgeven, met beperkte mogelijkheden. De commercieële versie ondersteunt een client en server-architectuur, de open-source

versie niet. De Enterprise versie van Tripwire heeft ook de mogelijkheid om netwerkapparatuur te ondersteunen.

De commercieële versie van Tripwire is beschikbaar voor Windows, Linux en Sun Solaris. De open-source versie is alleen te gebruiken onder Linux.

AIDE AIDE is een open-source alternatief voor Tripwire. Dit project staat nog in de kinderschoenen, vandaar dat het nog niet alle functionaliteit van Tripwire biedt. De bedoeling is echter dat het , naarmate de ontwikkeling vordert, meer functionaliteit dan Tripwire bevat.

PortSentry PortSentry is een HIDS toevoeging. PortSentry maakt het mogelijk om portscans op het systeem te detecteren en daarvan melding te geven. Het is ook mogelijk om de bron van de portscan te blokkeren.

PortSentry is alleen geschikt voor Unix-achtige platforms.

2.3 Hybrid Intrusion Detection (HyIDS)

Een Hybride IDS bestaat uit zowel NIDS als HIDS componenten en combineert daarmee de mogelijkheden van beide.
Voorbeeld van een Hybride IDS:

Prelude Prelude is een Hybride IDS met distributed mogelijkheden. Het bestaat uit diverse netwerk- en host-based componenten. Deze componenten sturen hun informatie naar een centrale manager die de meldingen registreert. Doelstelling van Prelude is om een compleet, alles in één IDS te zijn. Prelude kan worden gekoppeld met andere IDS applicaties, zoals Samhain en Snort.

Prelude is open-source en kan worden gebruikt op alle Unix-achtige besturingssystemen.

3 Het project

Om de doelstellingen van het project duidelijk te maken geven we eerst een overzicht van de huidige situatie. Vervolgens geven we een opsomming van de eisen en wensen die we in samenspraak met de heer Mobach hebben opgesteld. In het volgende hoofdstuk gaan we dieper in op deze eisen en wensen en kijken we met welke tools hieraan voldaan kan worden. Uitgangspunten zijn hierbij Snort en Prelude.

3.1 De huidige situatie

De heer Mobach beheert de netwerken en beveiliging van een aantal klanten. Deze klanten zitten verspreid over Nederland en hebben diverse servers en subnetten. Op elke locatie bevinden zich, door de heer Mobach ingerichte, firewalls

die ongewenst verkeer tegenhouden. Om dit zo goed mogelijk te doen haalt hij met regelmaat de logfiles van bijvoorbeeld Apache en Sendmail van de diverse servers op en analyseert deze met behulp van een aantal zelfgemaakte scripts. Met de verkregen informatie kan hij vervolgens besluiten preventief bepaalde systemen of subnetten te blokkeren in bijvoorbeeld de mailserver of voor het gehele netwerk.

3.2 Gewenste situatie

In de gewenste situatie wordt er naast logfiles ook gekeken naar netwerkverkeer en wordt het proces van analyse verder geautomatiseerd. Er zijn meerdere sensoren, zowel Host-based als Network-based, die hun meldingen op een centrale plaats registreren. Het configureren en updaten van de rulesets op de verschillende sensoren wordt gecentraliseerd en deels geautomatiseerd. Hiermee kunnen rulesets eenvoudig en overzichtelijk worden beheerd en kunnen false-positives en false-negatives worden geminimaliseerd.

Ook zijn er aanknopingspunten voor het automatiseren van het preventief blokkeren van verkeer vanaf bepaalde netwerken.

De voorkeur gaat uit naar open-source. Naast de lagere kosten is het hiermee mogelijk om zelf aanpassingen te doen en uitbreidingen te schrijven. Ook is er met open-source meer inzicht in de precieze werking van de software.

3.3 Eisen en wensen

De eisen en wensen zoals we deze hebben gedefinieerd zijn:

Zowel Network- als Host-based Intrusion Detection Momenteel wordt er alleen informatie over aanvallen verkregen uit het analyseren van logfiles. Dit zou aangevuld moeten worden met eventueel andere Host-based en Network-based Intrusion Detection Systemen om zoveel mogelijk informatie te vergaren die nuttig kan zijn bij het beveiligen van de netwerken.

Centrale registratie van meldingen Meldingen, door de verschillende verspreide sensoren gegenereerd, moeten centraal worden geregistreerd. Centrale registratie maakt het mogelijk om de alerts van de diverse sensoren met elkaar te vergelijken om zo trends te ontdekken. Ook wordt het mogelijk om preventief te blocken op andere netwerken dan degene waar de melding vandaan komt, eventueel via een IPS systeem.

De heer Mobach heeft aangegeven dat centrale registratie in zijn situatie niet real-time hoeft te gebeuren.

Centrale configuratie en updates Het up-to-date houden van de sensoren en de gebruikte rules is van belang om nieuwe aanvallen tijdig te kunnen detecteren en false-positives en negatives te minimaliseren. Ook minimaliseert een goed geconfigureerde sensor de load op het systeem. Verschillende netwerken en IDS systemen kunnen verschillende eisen stellen aan hun configuratie en rules. Hierdoor is het vaak niet mogelijk om deze rules

automatisch te installeren en naarmate het aantal sensoren groeit gaat het up-to-date houden steeds meer tijd kosten. Hiervoor is het wenselijk dat dit centraal kan, waarbij per sensor of groep van sensoren aangegeven kan worden wat de gewenste configuratie en rules zijn.

Visuele rapportage Meldingen van sensoren worden opgeslagen in een database of in logfiles. Om als beheerder iets met deze meldingen te doen is het van belang dat ze op basis van bepaalde criteria kunnen worden geselecteerd, gegroepeerd en getoond. Dit kan handmatig met behulp van database queries of regular expressions, maar een aantal voorgedefinieerde rapportages en eventuele visuele representatie kunnen helpen om inzicht te krijgen in verbanden en trends.

Notificatie Afhankelijk van de impact van een melding kan het handig zijn om deze direct te melden aan de verantwoordelijke persoon. Zo kan deze tijdig maatregelen nemen om schade te beperken. Hiervoor is een notificatiemethode nodig die bijvoorbeeld een mailtje of sms bericht stuurt zodra er een melding komt die voldoet aan bepaalde criteria.

Het delen van informatie Er zijn diverse personen en bedrijven die zich bezighouden met beveiliging en Intrusion Detection. Net zoals bij het centraal registreren van meldingen door de eigen sensoren kan het nuttig zijn om meldingen uit te wisselen met anderen. Zo kan er een beter beeld worden gevormd van aanvallen en bronnen hiervan, ook als deze op de eigen netwerken en systemen nog niet zijn gedetecteerd.

Basis voor Intrusion Prevention Intrusion Prevention is het automatisch nemen van maatregelen op basis van gegevens uit een IDS systeem. Hoewel er bij de heer Mobach nog geen plannen zijn om op korte termijn IPS te implementeren is het wel nuttig om te kijken hoe de stand van zaken is met betrekking tot IPS op dit moment.

4 Onderzoek/uitwerking

In dit deel kijken we naar de eisen en wensen zoals die zijn gedefinieerd en geven we per item aan wat er bij komt kijken en hoe het gerealiseerd kan worden met de huidige tools of combinatie van tools.

4.1 Zowel Host- als Network-based Intrusion Detection

Voor een zo compleet mogelijke informatievergaring is het van belang dat er zowel gebruik kan worden gemaakt van Host-based als Network-based Intrusion Detection.

Aandachtpunten hierbij zijn:

Plaatsing van NIDS Wordt het NIDS buiten de firewall geplaatst om zo al het netwerkverkeer richting het netwerk te analyseren of wordt het NIDS

binnen de firewall geplaatst, om zo intern netwerkverkeer en verkeer dat door de firewall wordt doorgelaten te analyseren.

Verschillende besturingssystemen Host-based IDS'en zijn afhankelijk van het besturingssysteem op de hosts. In heterogene netwerken moeten er dus voor alle verschillende besturingssystemen specifieke HIDS'en worden geïnstalleerd.

Verschillende HIDS soorten Om een compleet beeld van alle systeemacitiviteiten te geven moet een HIDS op diverse manieren het systeem in de gaten houden. Logfiles bekijken, veranderingen in files, policies en system calls. Hiervoor zijn verschillende componenten nodig.

Snort is puur een NIDS en heeft geen HIDS mogelijkheden. Er moeten dus andere oplossingen worden bedacht voor HIDS. Prelude heeft al wel HIDS mogelijkheden maar deze zijn standaard beperkt tot het parsen van logfiles. Voor andere HIDS varianten is het nog nodig om externe applicaties in te zetten, eventueel als Prelude plugin.

4.2 Centrale registratie van meldingen

Bij centrale registratie worden alle meldingen van de sensoren verzameld op een centrale server. Aandachtspunten hierbij zijn:

Opslag alleen centraal of ook lokaal ? Als er alleen centraal wordt opgeslagen is het van belang dat er een constante verbinding is met de centrale server. Als deze verbinding wegvalt kan de sensor zijn data niet kwijt en gaan er meldingen verloren.

Waar vindt de filtering plaats ? Er kan voor gekozen worden om alle meldingen of zelfs gehele logfiles naar de centrale server te sturen. Voordeel hiervan is dat er meer wordt gelogd, ook meldingen die in eerste instantie als onbelangrijk zouden zijn bestempeld maar later nuttige informatie blijken te bevatten. In een situatie met veel sensoren en veel meldingen kan dit er echter voor zorgen dat er grote hoeveelheden data tegelijk naar de server worden verstuurd, waardoor de verbinding kan verstoppen of de server zelf overbelast raakt.

Filteren kan ook worden gedaan door de sensoren. Hierbij worden alleen belangrijke meldingen doorgestuurd waardoor bovenstaand probleem wordt voorkomen. Dit houdt echter wel in dat de sensor goede rules moet bevatten die up-to-date worden gehouden.

Realtime verzending of met een regelmatige interval Meldingen kunnen realtime of op vastgestelde tijdstippen naar de centrale server worden gestuurd. Realtime heeft als voordeel dat de meldingen direct op de centrale server beschikbaar zijn waardoor er snel gereageerd kan worden. Mocht een aanval succesvol zijn en de host of het netwerk buiten werking raken, dan is een log hiervan opgeslagen op de centrale server.

Nadeel is dat er een constante verbinding met de server moet zijn.

Beveiliging Meldingen kunnen voor een aanvaller nuttige informatie bevatten. Ook kan een aanvaller met behulp van valse meldingen een verkeerd beeld geven van aanvallen en bronnen. Door veel false-positives te genereren kan hij stimuleren dat op den duur bepaalde rules worden uitgezet of subnetten worden geblokkeerd.

Het is dus van belang dat de communicatie tussen de sensor en de centrale server wordt versleuteld, waarbij de identiteit van de zender (de sensor) wordt gewaarborgd.

Prelude is ontworpen met het oog op distributie. Filtering vindt plaats in de sensor zelf op basis van de rulesets. Meldingen worden in principe realtime doorgegeven maar worden gecached op het moment dat er geen verbinding is. Communicatie gebeurt middels een standaard protocol, met ondersteuning voor SSL en authenticatie op basis van een gebruikersnaam en wachtwoord.

Snort biedt standaard geen ondersteuning voor centrale registratie. Toch kan dit met behulp van een aantal technieken worden gerealiseerd. In het volgende hoofdstuk geven we hiervoor een paar oplossingen.

4.3 Centrale configuratie en updates

Configuratie van de sensoren en gebruikte rulesets wordt gedaan vanuit een centrale locatie.

Aandachtspunten hierbij zijn:

Verschillende typen sensoren Er zijn verschillende typen host-based en network-based sensoren. Deze hebben elk hun eigen configuratiemethoden en rulesets. Host-based sensoren monitoren en analyseren bijvoorbeeld logfiles van zeer uiteenlopende applicaties, die alle een eigen formaat en bijbehorende rulesets hebben. Hierdoor wordt het heel lastig om met één centrale applicatie al deze configuraties en rules te beheren.

Verschillende policies per host, netwerk of groepen van hosts en netwerken Elke host, netwerk of groep van hosts en/of netwerken heeft z'n eigen policy. Hierdoor is het niet mogelijk om geautomatiseerd rules vanaf een centrale locatie op te halen: rules moeten per sensor worden geïnstalleerd en geconfigureerd.

Beveiliging Ook bij het op afstand configureren van de sensoren en updaten van de rulesets is beveiliging van groot belang. Een kwaadwillend persoon kan kennis van configuratie en rulesets gebruiken om sensoren te omzeilen en deze eventueel deels uit te schakelen. Hiervoor is het nodig dat de data versleuteld wordt en de authenticiteit van de sensor en de manager gewaarborgd zijn.

Snort heeft SnortCenter voor het centraal beheren van zijn sensoren. Hiermee is het mogelijk om middels een webinterface per sensor of groep van sensoren de rules te bekijken, te updaten en te activeren/deactiveren. SnortCenter communiceert hiervoor middels SSL met een SnortAgent op het systeem van de sensor. Deze SnortAgent kan rules toevoegen en verwijderen en Snort vervolgens herstarten om de wijzigingen te activeren.

Prelude biedt standaard geen remote management faciliteiten. Hiervoor moet dus eigen software worden ontwikkeld.

4.4 Visuele rapportage

Voor een visuele rapportage haalt de rapportagetool de meldingen op uit de database of logfiles en geeft deze gestructureerd weer.

Aandachtspunten hierbij zijn:

Verschillende opslagmechanismen en formaten De verschillende IDS systemen slaan hun meldingen op, op verschillende manieren. Meldingen kunnen in een database staan of in logfiles, in verschillende tabellen en verschillende formaten. Omdat de aard van meldingen van Host- en Network-based systemen erg van elkaar verschillen is het groeperen van deze resultaten en het weergeven in één overzicht lastig.

Beveiliging Indien de rapportage wordt bekeken op een ander systeem van dat waarop de meldingen staan opgeslagen is het van belang dat de communicatie versleuteld is. Dit kan in het geval van een webbased presentatie met behulp van SSL. Ook moet er een toegangscontrole zijn met behulp van bijvoorbeeld een gebruikersnaam/wachtwoord combinatie om misbruik door onbevoegden te voorkomen.

Een visuele rapportagetool voor Prelude is Piwi. Dit is een in Perl geschreven webbased GUI waarin diverse overzichten kunnen worden gegenereerd en weergegeven. Voorbeelden zijn de tien meest voorkomende meldingen, de tien meest voorkomende aanvallers en de laatste meldingen. Piwi is nog in ontwikkeling en biedt verder nog niet veel functionaliteit. Wel kunnen zowel de meldingen van de host-based als de network-based sensoren in één overzicht worden weergegeven. Er is geen beveiliging op basis van gebruikersnaam/wachtwoord ingebouwd in Piwi, maar door middel van htacces is dit wel mogelijk. Het versleuten kan via standaard https.

Voor Snort zijn meerdere grafische front-ends beschikbaar die verder zijn uitgewerkt en meer rapportagemogelijkheden bieden dan Piwi. Voorbeelden zijn ACID en SnortReport. Beiden kunnen alleen overweg met meldingen uit een database. Voor het weergeven van meldingen uit logfiles kan SnortALog worden gebruikt. Ook kunnen hiermee logs van Fw-1, Netfilter en IPFilter worden geparsed en weergegeven. Bij alle genoemde front-ends voor Snort kan gebruik worden gemaakt van gebruikersnaam/wachtwoord authenticatie en https.

4.5 Notificatie

Afhankelijk van de ernst van een melding kan het nodig/handig zijn om een notificatie te versturen naar de verantwoordelijke persoon.

Aandachtspunten hierbij zijn:

Notificatiemethoden Notificatie kan plaatsvinden via bijvoorbeeld mail, SMS of een SMB popup (in het geval de beheerder een Windows machine gebruikt). Welke methode gebruikt wordt is afhankelijk van de configuratie en eventueel de ernst van de melding. Zo kan gekozen worden voor mail of een SMB popup voor minder ernstige en SMS voor de zeer ernstige meldingen. Ook een combinatie is mogelijk waarbij eerst via mail/SMB wordt gemeld en vervolgens bij geen reactie via SMS.

Notificatieinterval Ernstige meldingen zouden direct een notificatie moeten kunnen triggeren. Hierbij moeten herhalingen worden afgevangen zodat er per tijdseenheid maar een beperkt aantal notificaties wordt verzonden met betrekking tot een zelfde type melding. Minder ernstige meldingen kunnen worden samengebundeld en bijvoorbeeld eens per dag worden verzonden.

Classificatie van meldingen Een goede classificatie van meldingen is nodig voor het automatisch verzenden van notificaties. Alleen meldingen die voldoen aan bepaalde voorwaarden moeten direct een notificatie triggeren. Als de drempel te laag ligt worden er onnodig notificaties verstuurd waardoor de betreffende persoon deze op een gegeven moment gaat negeren.

Prelude biedt op dit moment nog geen automatische notificatie. Hiervoor zou een script moeten worden gebouwd dat meldingen uit de database haalt en notificatie verzorgt.

Voor Snort zijn er diverse notificatietools beschikbaar. Deze werken echter niet met een database, slechts met logfiles. Ook hiervoor geldt dat er een script zou moeten worden gebouwd dat meldingen uit de database haalt.

4.6 Sharing Information

Delen van informatie met collega's is vooral een kwestie van vertrouwen. Hoe zeker ben je van de juistheid van de verkregen meldingen. Zeker als je van plan bent om op basis van uitgewisselde gegevens actie te gaan ondernemen is deze juistheid erg belangrijk.

Mocht je besluiten meldingen van een bepaalde partij te vertrouwen dan is het van belang dat je zeker weet dat de gegevens van die partij afkomstig zijn. Hiervoor is versleuteling en signing van gegevens met public key technologie uitermate geschikt. Data versleuteld met jouw public key kan alleen door jezelf worden ontsleuteld en data gesigned met iemands private key kan alleen van die partij afkomstig zijn.

Afhankelijk van de mate van vertrouwen in een partij kan ervoor gekozen worden om meldingen direct voor 100% te vertrouwen of om eerst te wachten tot er een soortgelijke melding van een ander partij komt.

Ook meldingen die door een partij indirect zijn verkregen (dus weer van een andere partij) kunnen zo worden geclassificeerd en worden opgeteld tot er een bepaalde drempel is bereikt.

Ook een centrale uitwisseling is mogelijk. Hierbij is er niet direct contact tussen partijen onderling maar worden meldingen naar een centrale server gestuurd. Dit kan eventueel ook op basis van trustlevels, bijvoorbeeld volgens het CACert principe. Het trustlevel van een partij, en dus zijn meldingen, wordt hierbij bepaald aan de hand van het vertrouwen dat andere partijen in hem hebben getoond.

Er is op dit moment al een initiatief in deze richting, namelijk DShield.org. Hier worden meldingen van Snort en firewall logs geregistreerd welke vervolgens voor de hele wereld inzichtelijk zijn. Er is nog geen authenticatie op basis van de genoemde principes, dus de betrouwbaarheid van de geregistreerde gegevens valt de betwijfelen. Prelude biedt nog geen mogelijkheden tot uitwisseling maar een koppeling met DShield is in ontwikkeling.

4.7 Basis voor IPS

Op basis van de met IDS verkregen gegevens kan met behulp van IPS automatisch verkeer vanaf een host of subnet worden geblocked in de firewall. Dit blocken kan grote gevolgen hebben voor het eigen netwerk, bijvoorbeeld het niet bereikbaar zijn van een DNS server of een veel geraadpleegde webserver. IPS is erg gevoelig voor DOS attacks. Daarom is het van belang dat er zorgvuldig wordt nagedacht over de criteria waarop wordt geblocked. Wordt er bijvoorbeeld geblocked op het ip-adres van een host of wordt er geblocked op subnet. Hoeveel hosts moeten er binnen een subnet meldingen genereren en hoe vaak moeten meldingen herhaald worden voordat tot blocken wordt overgegaan ? Hoe lang moet er worden geblocked ? Het is verstandig om te werken met whitelists om bereikbaarheid van bepaalde adressen te garanderen.

Standaard IPS biedt geen bescherming tegen DDOS attacks. Omdat verkeer al over de internetlijn loopt kan er niets aan gedaan worden. Een ideale oplossing zou zijn een signaal te geven naar de router die het verkeer vanaf de bronnen naar het doel blocked. Als deze dit dan door zou kunnen geven aan de router die het verkeer naar hem stuurt en die het ook blocked etc..

Prelude heeft een countermeasure component in ontwikkeling, maar op het moment is hier nog geen werkend prototype van.

Er zijn een aantal tools die op basis van Snort logs firewall rules kunnen aanpassen. Deze tools werken niet op een database. Wanneer alles naar syslog wordt gelogd, is het mogelijk om Blockit of Gaurdian te gebruiken. Deze kijken naar een whitelist, staat dat ip-adres er niet op, dan wordt hij tijdelijk geblocked. Er zijn op dit moment nog geen distributed mogelijkheden, maar door middel van SSH en aanpassingen aan de scripts van Gaurdian is dit wel te realiseren. Hierbij behoren wel alle Snort logfiles zich op één locatie te bevinden.

5 Mogelijke implementaties

We zullen hier een aantal mogelijke implementaties op basis van zowel Prelude als Snort bespreken.

5.1 Prelude

Prelude biedt standaard alle functionaliteit voor het gedistribueerd rapporteren van meldingen door sensoren. Real-time doorgave, een eigen protocol, beveiliging met behulp van SSL en authenticatie. Er zijn zowel host-based als network-based sensoren voor. Prelude-LML werkt op basis van pattern matching in logfiles van diverse server applicaties, Prelude-NIDS werkt ongeveer hetzelfde als Snort en op basis van Snort rules.

Om aan alle eisen te voldoen moet Prelude nog wel uitgebreid worden. Er is nog geen functionaliteit voor het analyseren van de logs van Apache, Bind, Sendmail en/of Postfix en MySQL. Om dit te realiseren kunnen er applicatiespecifieke regels geschreven worden voor Prelude-LML.

Voor het checken van de integriteit van bestanden is het verder nog nodig om bijvoorbeeld Samhain als Prelude plugin te installeren. Hiervoor is een patch beschikbaar, die echter nog niet werkt met de meest recente versie van Samhain.

Gedistribueerd configureren en updaten van rules is nog niet mogelijk. Hiervoor moet een set van scripts worden gebouwd die deze functionaliteit verzorgt. Voor de Prelude-NIDS moet dit een script zijn dat via een SSH tunnel de betreffende Snort rules naar de juiste directory op de server kopiëert, een conversiescript start en vervolgens de sensor herstart. Voor de host-based componenten van Prelude moeten diverse configfiles worden gewijzigd. Dit kan op een vergelijkbare manier als met Prelude-NIDS.

Ook voor notificatie, delen met collega's en IPS zijn er nog geen oplossingen. Hiervoor moet dus zelf iets worden ontwikkeld.

Ook is de visuele rapportage nog zeer beperkt.

5.2 Snort

Snort is de standaard open-source NIDS. Er worden met grote regelmaat nieuwe rules voor uitgegeven en er zit een grote community achter. Er zijn oplossingen voor het gedistribueerd configureren en updaten van rules en voor notificatie, delen van meldingen en visuele rapportage.

Snort biedt echter weinig tot geen ondersteuning voor Host-based IDS en voor gedistribueerde rapportage. Daarom moet het worden gecombineerd met een aantal Host-based applicaties met elk hun eigen oplossingen voor distributie, centrale configuratie en notificatie en rapportage.

Oplossingen voor het distribueren van meldingen van Snort:

Snort met remote syslog

Snort kan zijn meldingen remote loggen via syslog over een SSH tunnel of SSL. Hierbij wordt realtime gelogd en SSH en SSL bieden de functionaliteit voor versleuteling en authenticatie. Als echter de verbinding met de server wegvalt kan Snort zijn data niet kwijt en gaan er meldingen verloren. Door het gebruik van remote syslog komen alle belangrijke gegevens bij elkaar, waardoor de NIDS en delen van HIDS gegevens in één bestand staan. Ook moeten de meldingen op de server nog verwerkt en in een database worden gezet, iets dat extra serverload met zich meebrengt.

Benodigde software:

- **Lokaal:** Snort
- **Remote:** Syslog server (bijvoorbeeld Syslog-ng) en scripts om de centrale syslog te parsen, zoals Logwatch of Logcheck en eventueel Snort-specifieke scripts
- **Verbinding:** Stunnel en een SSH-implementatie, bijvoorbeeld openSSH of openSSL

Snort via een MySQL tunnel

Hierbij is er sprake van een directe databaseverbinding met de server. De lokale MySQL poort kan worden getunneld naar de MySQL database op de centrale server met behulp van SSH. Hierbij draagt SSH zorg voor de versleuteling en authenticatie. Nadeel van deze methode is dat er geen lokale opslag is, waardoor bij het wegvallen van de verbinding meldingen verloren gaan. Voordeel is dat de visuele rapportagetools de gegevens uit de database kunnen gebruiken. Voor een HIDS moet een andere oplossing worden gebruikt.

Benodigde software:

- **Lokaal:** Snort en MySQL-client
- **Remote:** MySQL-server
- **Verbinding:** Stunnel en een SSH-implementatie, bijvoorbeeld openSSH

Snort met lokale opslag en scripts

Bij deze methode slaat Snort zijn meldingen op in een lokale logfile of database. Een script leest deze meldingen met een bepaalde interval uit en stuurt ze via een tunnel naar de database op de centrale server. Hierbij gaan er geen meldingen verloren als er tijdelijk geen verbinding is, maar het is ook niet geheel realtime. De visuele tools voor Snort kunnen gebruikt worden. Wanneer realtime geen belangrijk punt is kunnen de gegevens ook alleen 's avonds worden verstuurd om overdag bandbreedte te besparen.

Benodigde software:

- **Lokaal:** Snort, zelfgeschreven scripts voor het ophalen en doorsturen van de gegevens en eventueel een MySQL-server
- **Remote:** MySQL-server
- **Verbinding** Stunnel en een SSH-implementatie, bijvoorbeeld openSSH

Host-based oplossingen die samen met Snort zouden moeten worden geïmplementeerd:

Logfile parsing Hiervoor moeten applicatiespecifieke scripts worden geschreven. Logwatch en Logcheck is ook mogelijk. Hierbij moet wel worden gedacht aan distributie en centrale onderhoudsmogelijkheden.

Filechanges Hiervoor kan Samhain of Tripwire worden gebruikt. Ook hierbij moet er iets verzonnen worden voor distributie en centrale configuratie. Indien voor Samhain wordt gekozen, kan de mogelijkheid worden gebruikt om een Samhain server te plaatsen. Dit kan eventueel dezelfde machine zijn die ook de centrale Snort gegevens ontvangt.

6 Conclusie en aanbevelingen

Het concept van Prelude is veelbelovend en biedt veel mogelijkheden voor het gedistibueerd opzetten van zowel host-based als network-based Intrusion Detection. De ontwikkeling ervan vordert gestaag maar het is op dit moment nog niet volwassen genoeg om in een bedrijfssituatie te worden ingezet. Snort biedt op het gebied van NIDS de meeste mogelijkheden en ondersteuning, mede door de grote community er achter. Het biedt echter standaard geen mogelijkheden voor centrale opslag. Om dit toch te realiseren kan er gebruik worden gemaakt van MySQL tunneling, remote syslog of custom made scripts. Wij adviseren de laatste optie omdat dit de meeste mogelijkheden biedt en er geen verlies van meldingen optreedt op het moment dat de verbinding met de centrale server wegvalt. Voor een complete IDS oplossing moet Snort nog worden aangevuld met een of meerdere Host-based Intrusion Detection methoden, waaronder centrale opslag en analyse van logfiles en integriteitscontrole van bestanden.

Op het gebied van IPS is meer onderzoek nodig naar de verschillende manieren van Intrusion Prevention en de problemen die hierbij een rol spelen. Wij raden dan ook aan om in een vervolgonderzoek hierin verder te gaan.

Referenties

[1] De officiële website van het Prelude Project,
http://www.prelude-ids.org/

[2] De officiële website van het Snort Project,
http://www.snort.org/

[3] De officiële website van het Samhain Project,
http://la-samhna.de/samhain/

[4] De officiële website van het Swatch Project,
http://swatch.sf.net/

[5] De officiële website van de open-source versie van Tripwire,
http://www.tripwire.org/

[6] De officiële website van de commerciele Tripwire Versie,
http://www.tripwire.com/

[7] De officiële website van het Logcheck Project,
http://sourceforge.net/projects/logcheck/

[8] De officiële website van het Logwatch Project,
http://sourceforge.net/projects/sentrytools/

[9] De officiële website van het PortSentry Project,
http://sourceforge.net/projects/sentrytools/

[10] De officiële website van het RealSecure Network product,
http://www.iss.net/

[11] De officiële website van het eTrust Intrusion Detection Product,
http://www3.ca.com/Solutions/Product.asp?ID=163

[12] De officiële website van het AIDE Project,
http://www.cs.tut.fi/~rammer/aide.html/

[13] De officiële website van het SnortReport Project,
http://www.circuitsmaximus.com/download.html

[14] De officiële website van het ACID Project,
http://acidlab.sourceforge.net/

[15] De officiële website van het SnortCenter Project,
http://users.pandora.be/larc/

[16] De officiële website van de Snort Bleeding Edge Rules,
http://snort.infotex.com/

[17] De officiële website van het Guardian Project,
http://www.chaotic.org/guardian/

[18] De officiële website van het BlockIt Project,
http://www.teknofx.com/

[19] De officiële website van het Cygwin Project,
http://www.cygwin.com/

[20] Een website met een verzameling van verschillende links naar IDS tools,
http://www.forinsect.de/ids/ids-tools.html

[21] Boek: Sams, Intrusion Detection with Snort
Auteur: Jack Koziol

[22] Boek: Snort for Dummies
Auteurs: Charlie Scott, Paul Wolfe en Bert Hayes

[23] Boek: Syngress, Snort 2.0 Intrusion Detection
Auteurs: Jay Beale en James C. Foster

[24] Boek: Prentice Hall, Intrusion Detection Systems with Snort
Auteur: Rafeeq Ur Rehman

[25] Artikel: Distributed NIDS: A How-To Guide
Auteur: Alan McCarty

[26] Artikel: Using Snort For a Distributed Intrusion Detection System
Auteur: Michael P. Brennan

A Snort

Snort is de onbetwiste standaard voor open-source NIDS. Geheel open-source, gratis, meerdere platformen etc.

De volgende software is ontwikkeld voor Snort:

Barnyard Barnyard ontlast de Snort sensor door de koppeling met de database op zich te nemen.

Snortcenter Grafische tool voor het centraal beheren van de rulessets op verschillende remote sensoren. Hiervoor communiceert Snortcenter met een Snort Agent die op het betreffende systeem is geinstalleerd.

SnortReport Grafische tool voor de weergave van Snort alerts uit een database.

ACID Grafische tool voor de weergave van Snort alerts uit een database.

Snorter Grafische tool voor het weergeven van Snort alerts uit een database.

SnortALog Grafische tool voor het weergeven van Snort alerts uit logfiles. Kan naast Snort logs ook Fw-1, Netfilter en IPFilter logs parsen.

Blockit Tool die met behulp van de output van Snort ervoor kan zorgen dat de bron van problemen geblokkeerd kan worden. Dit gebeurd met behulp van het dynamisch aanpassen van de firewall.

Guardian Tool die met behulp van de output van Snort ervoor kan zorgen dat de bron van problemen geblokkeerd kan worden. Dit gebeurd met behulp van het dynamisch aanpassen van de firewall.

Snortsam Tool die met behulp van de output van Snort ervoor kan zorgen dat de bron van problemen geblokkeerd kan worden. Dit gebeurd met behulp van het dynamisch aanpassen van de firewall.

Snort-inline Tool die ervoor kan zorgen dat gevaarlijke datapakketten van het netwerk verwijderd worden. Dit gebeurd door de gevaarlijke pakketten niet door te sturen.

Oinkmaster Tool voor het automatisch updaten van Snort-rules. Deze tool haalt automatisch de nieuwste rules vanaf het internet.

Loghog Tool dat aan de hand van de ouput van Snort acties kan ondernemen, zoals het blokkeren en emailen.

IDScenter Tool voor het beheren van Snort, zowal rules als instellingen. Alleen beschikbaar voor het Windows-platform.

B Prelude

Prelude is een hybrid IDS. Dat wil zeggen dat het zowel Network-based als Host-based Intrusion Detection elementen bevat.

De componenten van Prelude zijn:

Prelude-Manager is de centrale manager applicatie. Deze luistert naar sensoren en slaat de verkregen informatie op in een database (MySQL of PostgreSQL).

Prelude-NIDS is de sensor voor het netwerkverkeer. Prelude-NIDS heeft nagenoeg dezelfde functionaliteit als Snort en maakt ook gebruik van Snort rules.

Prelude-LML omvat de host-based componenten. Prelude-LML analyseert de logfiles van een flink aantal bekende server applicaties.

Libsafe is een applicatie die buffer underrun protectie biedt en zelf ook als sensor kan dienen.

Piwi is de grafische front-end waarin alerts van de Prelude sensoren kunnen worden weergegeven.

Prelude-LML kan standaard overweg met logfiles van de volgende applicaties:

- IPFW
- NetFilter
- IPChains
- Cisco routers
- Cisco VPN Concentrator
- Cisco PIX
- Nagios
- Zyxel Routers
- WuFtpd
- ProFtps
- SSHD
- Squid
- Qpopper
- GRSecurity

- UnixSecurity
- Checkpoint FW-1

Prelude biedt de mogelijkheid diverse bestaande softwareapplicaties te patchen zodat ze gebruik kunnen worden als sensor voor de Prelude-Manager. Er zijn op dit moment patches voor de volgende programma's:

- Snort
- Nessus
- Nagios
- Argus
- HoneyD
- LibSafe
- Samhain
- SysTrace
- Bro IDS