Технически университет – София

ПГ по Компютърни Технологии и Системи - Правец

Упражнение - 4

СИСТЕМИ ЗА СИГУРНОСТ

Тема: Работа със система за откриване и защита от проникване

Изготвил:

Доц. д-р Румен Трифонов

Общи сведения за IPS и IDS (IDPS)

Общ преглед

Целта на защитната стена в мрежата е точно дефинирана. Тя предпазва една част от мрежата от друга нейна част, като разрешава или забранява определен трафик на базата на редица избрани критерии. По отношение на сигурността обаче винаги имаме определени съмнения. Откъде знаем, дали защитната стена изпълнява нейните функции? Как да разберем, че защитната стена е конфигурирана правилно? Сигурни ли сме, че през нея не преминава трафик от кибернетични атаки, които не са били предвидени, когато за първи път сме я конфигурирали? Устройството, което е проектирано да ни отговори на тези въпроси се нарича *система за откриване на нарушители (IDS - Intrusion Detection System)*.

Ако защитната стена е ключалката на вашата врата, то IDS е алармата срещу проникване с взлом. Защитната стена е мрежовия елемент осигуряващ защитата. В случай че защитата е преодоляна, IDS включва алармата.

Това, което IDS се опитва да прави, е оценка на всеки от милионите пакети които наблюдава в режим на нормална работа. За всеки пакет, който се разглежда, логиката на IDS определя дали пакетът е „добър" (с други думи такъв, какъвто нормално се среща в мрежата) или „лош" пакет. В този случай „лош" може да означава виртуално всякакъв, но обикновено се приема, че това е пакет, който независимо поради какви причини, не трябва да се среща в мрежата. Това дори може да означава, че пакетът нормално е „добър", но е видян в „лошо" време.

Дейностите, които IDS предприема, когато види добър или лош пакет могат да бъдат най-различни. Понеже предполагаме, че голяма част от трафика в мрежата е добър, нормално IDS обръща внимание само на лошите пакети. IDS може да избере да игнорира напълно лошия пакет, да регистрира този пакет в дневника като предложение за по-късен анализ от страна на администратора, или да включи аларма и да извести всички определени за целта лица, че такъв пакет е открит в мрежата.

Определянето на това, какво е „добър" и „лош" пакет е обект на безкрайни дискусии и множество патенти и продукти. За да разберем какъв избор трябва да направим при разделянето на добрите от лошите пакети, нека се опитаме да създадем своя собствена IDS.

В основата си, една IDS не е нищо повече от програма специално обучена да разпознава пакети (sniffer). Тази програма наблюдава преносната среда и записва всички пакети за допълнителен анализ. Засега ние ще разглеждаме IDS като прост анализатор на пакети. Къде да бъде той поместен в мрежата, за да бъде максимално ефективен, с това ще се занимаем по-нататък. На този етап ние ще включим нашата IDS към някой концентратор.

Като начало, ние прихващаме всички пакети от преносната среда и ги записваме в дневник (log). След няколко дни ще забележим, че разполагаме с гигабайтов файл съдържащ текстови данни, който трябва да бъде сортиран. За да си улесним работата, ще се опитаме да филтрираме

данните в известна степен. Това можем да направим по няколко начина. Първото нещо което ни идва на ум е да въведем всички видове „добри" пакети. Няма да направим и няколко крачки и ще осъзнаем, че съществува голямо разнообразие от много и различни видове добри пакети. Затова трябва бързо да променим курса. Трябва да се опитаме да намерим някакви отличителни характеристики на лошите пакети, като направим преглед на специализираната литература и наличната информация за различните видове мрежови атаки. За всяка атака, за която намерим информация, създаваме съответен филтър на нашата IDS. Например ако сме сигурни, че никога в нашата мрежа не трябва да се появяват пакети с IP адрес на източника 0.0.0.0, ние създаваме съответен филтър и причисляваме такива пакети към лошите.

Въпреки че такъв подход може да отнеме много време, все пак броят на видовете лоши пакети е значително по-малък от броя на видовете добри пакети. Доволни от работата си, ние инсталираме нашата IDS и я включваме. Веднага ще забележим, че нещо не е в ред. IDS ни алармира за голямо количество „лоши" пакети, макар че работим в идеални условия, в мрежа, която не е подложена на атаки. Започваме да търсим източника на тези лоши пакети. Ще открием, че много от тях удивително приличат на добрите пакети, които използваме в нашата мрежа. За да отстраним проблема, ние прекарваме дни и седмици в настройка на нашата IDS. Всеки път когато открием лоши пакети ние извършваме разследване дали тези пакети са наистина лоши, или са част от нормалния трафик на мрежата. С течение на времето ентусиазмът ни за чисто нова IDS започва да намалява. Можем дори, поради непрекъснатия тормоз от фалшиви лоши пакети, да вземем решението за цялостно изключване на алармената система.

Ако все пак до това не се стигне и ние упорито продължим работата си по създаване на нови филтри в нашата IDS, в определен момент ща забележим, че броят на фалшивите сигнали драстично намалява. Това е, което ни доставя удоволствие от нашата работа, и ние най-вероятно ще продължим да добавяме нови и нови правила за нашата IDS.

Това щастие ще продължи до момента, когато с ужас разберем, че нашата защита е била разбита, и че имаме инсталирани троянски коне върху сървърите. Тогава ще започнем процеса на възстановяване на всичко от последния добър архив с който разполагаме, но понеже не знаем кога е извършена атаката, най-вероятно ще трябва да възстановим системата от оригиналните носители. Това е депресиращ процес. Ще си задаваме въпроса къде сгрешихме? Нашата защитна стена работеше, а IDS не ни алармира за лоши пакети. Едва на следващия ден ще открием, че е измислена нова атака, и че последствията от нея са точно такива, каквито ние сме открили при себе си. Затова трябва стриктно да следваме политиката непрекъснато да инсталираме новите правила за откриване на атаки. Проблемът е, че ние можем да сваляме тези правила от сайтовете на специализираните фирми по сигурността, но тази информация ще дойде при нас, когато може би вече е твърде късно за нашата мрежа.

До тук ние научихме по трудния начин, че така изградената наша IDS страда от голям недостатък. Ако в системата не сме въвели информация за определен вид атака, то системата няма да ни сигнализира за нейната наличност. По същество нашата IDS е реактивна. Ние знаем

само за атаки с които някой друг е бил нападнат, той е забелязал това и е известил Интернет общността за случката.

Можем ли да използваме друг подход? Например вместо да мислим за поведението на добрите и лошите пакети, да помислим за поведението на потребителите. Идеята е, че обикновените потребители са доста предсказуеми. Те използват мрежата по един и същи начин всеки ден. Сървърите ни са едни и същи. При предишния си опит за създаване на IDS ние научихме, че в нашата мрежа има неща, които се случват постоянно. Затова решаваме да категоризираме потребителския трафик като „нормален" и „ненормален". Задачите, които потребителите и мрежовите компютри изпълняват непрекъснато определяме като „нормални". Трафикът, който не е част от „нормална" задача се счита за „ненормален". Този вид трафик генерира аларми и се записва в дневника.

Основният момент при този подход е, че вместо да преминаваме през трудния процес на регистрация на нормалния и ненормален трафик, след което да го въвеждаме в IDS, ние позволяваме на IDS сама да научи кое е нормално и ненормално. Чрез наблюдение на трафика, ние можем да предскажем статистически какъв вид трафик се очаква между всеки две устройства в мрежата. Колкото повече наблюдаваме, толкова по-точни са нашите оценки. За ограничаване на настройките, които трябва да направим, ние дефинираме като нормален за IDS малък набор от възможности. Това означава, че даваме на IDS свобода на преценка какво е нормално и какво не. Не е необходимо когато потребителите направят нещо малко по-различно, веднага да се събира групата по сигурността. Това което се счита за нормално всъщност е малък прозорец на поведение на двете страни, който се определя статистически от IDS.

Този подход може да ни защити в бъдеще от нови атаки. Както може да се предполага, новата атака ще използва специфичен, различен вид трафик, който не е бил използван досега. Следователно той няма да бъде част от базата данни с образци на нормален мрежов трафик, ще бъде регистриран като ненормален и ще задейства алармената система.

Така че след инсталирането и конфигурирането на новия тип IDS, ние сме уверени в своята възможност да откриваме нови атаки срещу мрежата ни и да им противодействаме. Това е така докато не проведем сериозен разговор с експерт по сигурността. Той ще ни убеди, че нашите определения за нормалност и ненормалност са въз основа на наблюдаваното поведение на мрежовия трафик. Има две причини, които трябва да ни накарат сериозно да се замислим. Първата от тях е, как да разберем, че нашата мрежа действително не е била атакувана преди да сме инсталирали IDS? Трафикът от такива атаки би могъл да се счита вече за нормален. Освен това, кое ни гарантира, че някой няма постепенно и много внимателно да променя вида на трафика, така че да тренира IDS да не разпознава тези изменения като ненормален трафик. Ако поведението се променя достатъчно бавно, то трафикът винаги ще бъде разпознаван като нормален. Такива атаки биха останали напълно незабелязани от новата ни система.

С други думи трябва да си припомним основното правило на сигурността – няма перфектно решение. Дайте ми време, пари и мотивация, и всяка система за сигурност може да бъде компрометирана.

Можем да започнем да мислим за евентуално комбиниране на елементи от двата изложени до тук подхода. Да отбележим, че повечето атаки се основават на незаконно използване на мрежови протоколи. Например, нормално няма да видите URL GET заявка (заявка за уеб страница), която да съдържа дълъг низ от ../../../../ в нея. Това може да се получи, когато някой се опитва да достигне до определена директория, като премине през множество други. Ако се върнем към нашата оригинална идея и просто дефинираме всички нормални начини, по които искаме протокола да действа, то можем да заключим, че появата на горната форма е необичайно поведение и представлява някакъв вид атака.

Тъй като има много големи различия в протоколите, трябва да се обърнем към писмените стандарти на протоколните правила. Трябва да научим IDS какво представляват нормалните операции на даден протокол съгласно RFC документа и да конфигурираме системата да ни предупреждава за всички пакети които нарушават това поведение. Веднага след инсталирането на нова IDS, ние ще бъдем засипани от множество алармени сигнали от всякакъв вид. При това нашата мрежа не е изложена на атака в този момент. Естествено трябва да предвидим определен период за настройка към спецификата на конкретната мрежа, но количеството на алармите които получаваме почти винаги значително надхвърля очакванията ни.

Системите за откриване на нарушители, които в момента съществуват, са несъвършени и много често са непълни. Нито един модел на функциониране на IDS не е в състояние да открие всички атаки. Тези системи изискват значителни ресурси при първоначалното инсталиране и настройка. Независимо от продукта и начина, по който той се опитва да открие атаките, такава система винаги ще се нуждае от определен обучителен период за разпознаване на специфичните нужди на мрежата. Въпреки недостатъците, тези устройства са основен инструмент в модерните мрежи и спадат към някой от видовете, описани подробно по-долу.

Принципи на откриване и защита от проникванията

Откриването на проникванията е процес на наблюдение на настъпващите събития в компютърната система и/или мрежа. Това се прави с цел да се анализират всички признаци за възможни инциденти, които са нарушения или непосредствена заплаха от нарушения на политиките за компютърна сигурност, политики за приемлива употреба и/или стандартни практики за употреба. Причините за инцидентите са разнообразни по характер, те може да са предизвикани от:

- Зловреден софтуер (червей, софтуер за шпиониране на лична информация);
- Нарушителят получава неоторизиран достъп до системата през интернет;
- Упълномощено лице, което злоупотребява с привилегиите си или се опитва да се сдобие с допълнителни привилегии, за които не е оторизиран.

Системите за открива на прониквания (Intrusion Detection System - IDS) са софтуер, който автоматизира процеса за откриване на проникванията. Системите за защита от прониквания (Intrusion Prevention System - IPS) е софтуер, който има всички възможности на IDS, но освен това предлага възможност да предприеме действия срещу възможните инциденти. Администраторът може да изключи функциите за защита от прониквания, което ще накара IPS да функционира като стандартна IDS. Съответно, за кратност терминът система за откриване и защита от прониквания (Intrusion Detection and Protection System - IDPS), ще бъде използван за позоваване на IDS и IPS технологиите.

Основна терминология

- ***Burglar Alert/Alarm*** – сигнал за уведомяване за протичаща/протекла атака
- ***Detection Rate*** – дефинира се като броят на проникванията, засечени от система, разделен на общия брой на прониквания в тестовия набор;
- ***False Alarm Rate*** – дефинира се като броят на нормалните шаблони, които са възприети като атаки, разделен на общия брой на шаблоните;
- ***True Positive*** – легитимни атаки, които предизвикват задействане на алармата на IDS системата;
- ***False Positive*** – *събитие, което стимулира IDS да генерира аларма в случайна несъществуващи атаки;*
- ***False Negative*** – не се генерира аларма въпреки наличието на атака;
- ***True Negative*** – събитие, в което не се извършва атака, не се изпълнява изследване на такива;
- ***Noise*** – данни или външна намеса, които могат да предизвикат false positive или да прикрият true positive атака;
- ***Site Policy*** – упътвания в рамките на една организация, за контрол на правилата и контролиране на IDS;
- ***Site Policy awareness*** – способността на IDS динамично да променя правилата и конфигурациите в отговор на променящите дейности.
- ***Confidence value*** – стойност, с която организацията оценява IDS , базирано на производителност в минало и способността да анализира ефективно атаките;
- ***Alarm filtering*** –способност да се групират алармите за атаки с цел да се отделят false positive събитията от реалните атаки;
- ***Attacker / Intruder*** – обект, който се опитва да получи неоторизиран достъп до информация, да нанесе конкретна щета и да участва в злонамерени действия;
- ***Masquerader*** – потребител, който се опитва да се сдобие с неоторизиран достъп до информация, представяйки се за оторизирано лице(принципно това са външни лица);
- ***Misfeasor*** – разделят се на два типа, като принципно са вътрешни лица:
  ** оторизиран потребител с ограничени възможности;
  ** потребители с неограничен достъп, които злоупотребяват със своите правомощия;
- ***Clandestine user*** – човек, който заема ръководна роля и използва поста си за да избегне да бъде поднесен под отговорност

Приложение на IDPS технологията

IDPS се фокусират върху откриването на възможни инциденти. Например: IDPS може да засече кога извършителят е успешно компрометирал системата с цел използване на уязвимост. IDPS може да докладва за инцидента на администраторите, с цел да се предприемат ответни мерки, целящи минимизиране на щетите. IDPS може да запише информацията в дневник (log), който се използва от устройствата за борба с атаки. Тези системи могат да бъдат конфигурирани да засичат нарушения в политиките за сигурност. Например: Много IDPS могат да бъдат конфигурирани с набор от настройките на защитната стена (firewall), с цел идентифициране на мрежовия трафик, който нарушава политиките за сигурност и правилата за приемливо функциониране на организацията. IDPS може да наблюдава трансфера на файлове и да определи подозрителните от тях.

Много от IDPS могат да идентифицират разузнавателни дейности, които подсказват за предстоящи атаки или продължителни такива. IDPS блокира тези дейности и уведомява администратора, който може да предприеме ответни действия (промяна на контролите за сигурност). Поради честотата и разнообразието на такъв тип атаки, защитата от тях се извършва преди всичко върху защитени вътрешни мрежи.

Освен изброените до тук приложения, IDPS също спомага за:

- **Откриване на проблем с правилата за сигурност** – може да подсигури качествен контрол над правилата за сигурност, алармиране в случай на откриване на мрежови трафик, който би трябвало да бъде блокиран от защитната стена, но е пропуснат поради грешка в конфигурацията.
- **Документиране на съществуващите заплахи** – създават се дневник (log) с информация за откритите опасности. Чрез анализиране на честотата и отличителните им характеристики се изграждат планове за противодействие. Документацията може се използва за запознаване на ръководството с атаките, с които се сблъсква организацията.
- **Възпиране на външни/вътрешни лица от нарушаване на политиките за сигурност** – ако дадено лице е наясно, че действията му се наблюдават с цел предпазване от нарушения, има възможност да се откаже от намеренията поради опасността да бъде заловен.

Ключова функционалност

Има голямо разнообразие на IDPS технологии, които се разделят в зависимост от типа на събития, които могат да разпознаят, и вида на методологията, която ще използват за откриването на инцидента. В допълнение към наблюдението и анализа на събития, всички видове IDPS предлагат следната функционалност:

- **Записване на информацията свързана с изследваното събитие** – информацията се записва локално или в отделни централизирани сървъри за log файлове, за система за управление на събитията и за информационна сигурност.

- **Уведомява администратора за важни събития, които са обект на наблюдение** – алармирането е под формата на: електронно писмо, съобщения в IDPS потребителски интерфейс, Syslog съобщения, потребителски дефинирани скриптове и програми. Алармата съдържа само основната информация за събитието, за допълнително подробности администраторът трябва да провери в IDPS.
- **Генерира доклади** – създава доклади, които обобщават информацията за наблюдаваното събитие или предоставят конкретни детайли за него.

Някои системи също могат да променят своя профил на сигурност, когато се открие нова заплаха. Например: Възможно е сдобиването с по-детайлна информация за сесията, едва след като бъде обект на атака. IDPS може да прецени кога да се използват различните видове аларми и какви приоритети да бъдат предадени към повдигнатите сигнали.

IPS технологиите се различават от IDS технологиите с това, че предлагат възможност за отговор на откритата заплаха. В пасивните IDS сензорите откриват потенциално нарушаване на сигурността, записват информацията и алармират в конзолата. При реактивните системи, познати като системи за предотвратяване на проникване (IPS), автоматично се предприемат действия към подозрителните дейности. Действията, които могат да се предприемат са:

- **IPS спира атаката без чужда намеса** –
    - Терминира мрежовата връзка или потребителската сесия, която е използвана за атаката;
    - Блокира достъпа до целта (или вероятни мишени на атаката) от агресивния потребител, IP адрес или други атрибути на агресора;
    - Блокира целия достъп до терминала, услугата, приложението или други ресурси.
- **IPS променя средата за сигурност –** променя конфигурацията на различни контроли с цел да прекъсне атаката. Например: Конфигуриране на мрежови устройства с цел да блокират достъпа от агресора или към мишената, настройване на терминално-базираната защитна стена да блокира атаките, предизвикване на обновяване на терминал, ако бъдат открити уязвимост.
- **Промяна на съдържанието на атаката –** премахване на зловредната част от атаката. Например: IPS премахва инфектираният файл от електронното писмо и допуска писмото до получателя.

IDPS не предлагат 100 % точност на откритите заплахи. Когато безобидно действие бъде определено като атака, се създава аларма от вида false positive, а когато зловреден софтуер не бъде засечен се създава аларма от вида false negative. Не е възможно да бъде елиминирана напълно появата на тези два вида събития. Намаляване на честотата на единия, увеличава честотата на другия.

Повечето IDPS технологии предлагат функционалност, която да компенсира за използването на техники за укриване. Тези техники променят формата или времето на дадено

зловредно действие, като по този начин действието изглежда различно, но ефекта се запазва. Този подход се предприема от агресора с цел затрудняване на IDPS системите.

Методи за укриване от IDS

- Фрагментация – пращайки фрагментирани пакети, зловреднят код ще премине без да бъде засечен;
- Избягване на настройки по подразбирането – използването на допълнително конфигурации на настройки на портовете, които ще позволят на атакуващият да премине през защитата;
- Координирани нискочестотни атаки – IDS изпитва затруднение да координира анализа си сред множество нападатели, като всеки от тях има собствен порт и терминал.
- Address spoofing/proxying - препращане на пакетите през грешно конфигуриран proxy сървър затруднява проследяването.

Ограничения

- Шумовете могат значително да намалят ефективността на системата;
- Пакети с лошо качество, генерирани от грешки в софтуера, повредени DNS данни и локални пакети, които се губят, може да предизвикат сравнително високо ниво на фалшиви аларми;
- Стандартно броят на фалшивите атаки превишава броят на реалните, което понякога води до това реалните атаки да бъдат игнорирани или пропускани;
- Повечето атаки са насочени към остарели версии на специфичен софтуер;
- Необходимо е често подменяне на библиотеки с подписи в база данните.
- Съдържателно претърсващите системи имат забавяне между откриването на нова заплаха и прилагането й към IDS, през това време системата не може да открие други щети;
- Системата не подлежи на отговорност при слаба реализация на автентикацията и оторизацията;
- Криптираните пакети не се обработват от системата;
- Невалидни данни и TCP/IP атаки могат да предизвикат преустановяване на работа в NIDS;
- NIDS (Network IDS) са податливи на същите протоколни атаки, на които са податливи мрежата.

Какви възможности предлага IDS:

IDS не може да разреши всички проблеми свързани със сигурността.

IDS предлага:

- По-високо ниво на интегритет на инфраструктурата;
- Може да проследи действията на потребител от момента на влизането му до момента на промяната;
- Разпознава и докладва изменението в данните;
- Автоматизира търсенето на информация за най-новите видове атаки;
- Разбира кога системата ви е атакувана;

- Открива грешки в системните конфигурации;
- Подпомага администратора за оформяне на политики при работа с компютърните данни;
- Прави възможно управлението на системата от персонал, който не е експерт в областта.

IDS не предлага:

- Компенсация за слаба автентикация и оторизация;
- Изпълнение на разследване без намесата на човек;
- Компенсация за слаби точки в мрежата;
- Компенсация за проблеми с качеството и интегритета на информацията, която се предоставя от системата;
- Анализ на целият трафик при претоварена мрежа;
- 100% възможност да се справи с атаки използващи пакети;
- Възможност да работи с някои модерни устройства и функционалности.

Първи стъпки при избор на IDPS

Преди определянето на вида на IDPS всяка организация трябва да:

- Определи какви цели си поставят чрез използването на IDPS;
- Прегледа фирмените правила за сигурност;
- Зададе определени изисквания към :
    - Възможности за сигурността – събиране на информация, създаване на дневник , откриване и предпазване.
    - Производителност – максималните възможности за функционална производителност
    - Управление – дизайн, имплементация, опериране, поддръжка, документация за обучение,жизнен цикъл и цена за поддръжка.

Зависимости на IDS от други компоненти

IDS не е независима, тя трябва да е съвместима със следните компоненти:

- Операционна система - функционалност за генериране на дневник и проверка
- Услуги (Services) – функционалност за генериране на дневник и проверка
- Защитна стена – трябва да има способност да открива прониквания
- Мрежова платформа – да поддържа възможност за алармиране

Свързване на IDS система

Ефективността на IDS зависи до голяма степен от начина му на свързване.

- В среди с отдалечен достъп;
- Между сървъра и потребителските машини, за да може да открие вътрешни атаки;
- В близост до intranet среда,ftp среда или база данни;

- Между вашата мрежа и extranet среда;
- Между защитната стена и мрежата, за да открива опасности, които са преминали през стената.

Обвързани лица в процеса на комуникация с IDS

- Лицата отговарящи за информационната сигурност;
- Мрежовия администратор;
- Администратор на база данните;
- Главен управител;
- Администратора на операционната система;
- Собственика на данните.

Действия след успешна инсталация на IDS

Трябва да се назначи персонал, който да администрира IDS. Дневникът (log) трябва да се преразглежда периодично. Трафикът трябва да се пригоди да отговаря на нуждите на компанията. IDS трябва да бъде поддържан и конфигуриран. Трябва да се обучи квалифициран персонал. Процедурата за аварийни ситуации трябва да бъде съобразена с политиката на фирмата. В тази процедура се настройва списъка на лица за контакти, който включва:

- Кой да бъде алармиран първи;
- Списък на всички хора, които трябва да бъдат уведомени;
- Човекът, който отговаря за решението - как да се справят с възникналия проблем;
- Човекът, който ще бъде отговорен за разследването;
- Кой ще се оправя с медиите в случай, че стане публично;
- Как да се използва информацията за инцидента.

Основни методи за откриване на проникванията

Има различни методи за откриване на проникванията. Повечето IDPS използват няколко метода – по отделно или заедно, с цел да осигурят по –широк обхват на защита и по- голяма точност при откриване на проникванията. В следващите няколко страници ще разгледаме четири от най-използваните:

- Съдържателно претърсващи (signature-based)
- Статистически
- Базирани на откриване на аномалии (anomaly -based)
- Динамично защитни протоколни анализи

Съдържателно претърсващи

Това са едни от най-разпространените IDS. При тях образци на пакети, с които са направени опити за атака, се въвеждат в базата данни на IDS, след което IDS проверява дали всеки новооткрит пакет съвпада с някой от въведените й в базата данни образци. Пакетите, които съвпадат с образците, се маркират за по-нататъшна проверка. Този вид IDS е широко

разпространен, разбираем и лесно се имплементира. Той обаче страда от два недостатъка: липса на информация за определена атака и липса на образци на пакетите от такава атака. Тези недостатъци произхождат от начина, по който IDS работи. За да се открие определен вид атака някой трябва да положи усилия и да премине през процедурата за дефиниране как тази атака изглежда и през процедурата за конфигуриране на IDS с тази информация. Разбира се, никой не може да знае как една атака изглежда, докато някой не е бил атакуван, не е открил атаката по някакъв начин, и не е информирал Интернет обществото за нея. Този процес на неизвестност може да трае от няколко часа до няколко дни след реализиране на атаката, в зависимост от това какво е естеството на атаката, нейния обхват, както и какво внимание обръщаме на този проблем. Обикновено на атаките които нанасят големи поражения и са с широк параметър на действие се обръща по-голямо внимание и те се обработват по-бързо. Това едва ли е някаква утеха, тъй като вашата мрежа често е подложена на такъв тип атаки.Методът е много ефективен срещу познати заплахи, но не може да се справя с неизвестни атаки, замаскирани атаки с техники за преминаване през защитата и различни версии на познати злоупотреби.

Това е най-простият метод, тъй като просто сравнява данните за конкретното устройство със списък от шаблони, използвайки операция за сравнение на низове. Тази технология няма задълбочени познания за мрежата и протоколът на приложението, не може да проследи или да разчете сложна комуникация между устройства. Тя не помни предишните си заявки в момента на проверката на текущата, което създава ограничение свързано с липсата на умение да залови атаки, състоящи се от повече от едно събитие, ако нито едно от тях не съдържа индикация за злоупотреба.

Броят на актуализациите на базата данни също трябва да се има предвид. Някои компании имат образци от всяка регистрирана в Интернет атака. Размерът на базата данни непрекъснато нараства. Въпреки че това звучи положително, то забавя действието на IDS. В другия край на спектъра са компании, които ползват малко подмножество от образци на „най-често срещаните” в Интернет атаки. Това подмножество обикновено ви защитава само от елементарните, скриптови атаки. По-рафинираните ще останат незабелязани във вашата мрежа. В идеалния случай можем да използваме един компромис между двете крайности. Въпреки наличието на голям набор от образци, ние можем да изградим библиотека и да включим в нея само специфични за нашите нужди образци. Там могат да присъстват например образци от атаки от типа отказ на услуга, но не и на атаки срещу FTP сървър, понеже ние нямаме такъв сървър в нашата мрежа. Ще инсталираме и конфигурираме само тези правила, които имат някакво отношение към нашето мрежово обкръжение.

Предимства:

- Агресорът не може да тества IDS предварително и да провери какво би довело да аларма, тъй като профилите се генерират от администратор;
- За новите потребители и групи може да се редактират профилите;
- Може да открие нови атаки;
- Може да открие атаки в рамките на мрежата от служители.

Недостатъци:

- Конфигурирането му е продължително;
- Задължително трябва да се обновят профилите за новите потребители и групи;
- Трябва периодично да се реконфигурира дефиницията за нормален трафик;
- След инсталацията IDS трябва да бъде трениран да разпознава нормален трафик.

Откриване на аномалии

Вторият основен вид IDS продукти се категоризират като статистически IDS. Вместо да разчитат на образци от предишни атаки, статистическите IDS се опитват да разберат нормалното поведение на мрежата и да класифицират като ненормален всеки трафик, който нарушава това нормално поведение. В продължение на много години статистическите IDS бяха просто лабораторни експерименти. Идеята със сигурност не отговаряше на нуждите на промишлените мрежи. В последно време обаче започна производство на такива статистически IDS, които в известна степен допълват съдържателно претърсващите IDS приложения. Например статистическият продукт научава образеца на пакета за регистриране на потребител и генерира сигнал когато получи пакет за регистрация отличаващ се значително от научения вече образец.

Статистическите IDS страдат от няколко недостатъка. Първият е необходимостта да научат нормалното поведение на мрежата. Тук съществува възможност да сметнат нещо необичайно като нормално. Освен това, за да се намали броя на лъжливите аларми в повечето от този тип IDS се въвежда ниво на чувствителност, което може да се регулира. Ако направим сензорите прекалено чувствителни ще се генерират прекалено много фалшиви алармени сигнали, и това ще доведе до затормозяване на потребителите и администраторите. Намалението на чувствителността пък ще увеличи вероятността за неоткрита злоупотреба с ресурсите на мрежата.

IDPS създава различни профили за поведението на потребителите, мрежовите връзки, хоста или приложението. Тези профили се създават като за определен период се наблюдава нормалното функциониране на събитието. IDPS използва статистически методи за сравнение характеристиките на текущата дейност. Профилите могат да се отнасят към поведението на конкретни атрибути, например:

- брой e-mails, които се изпращат от потребител;
- брой неуспешни опити за автентикиране пред системата;
- процент на използване на процесор от даден хост в определен момент.

Най-голямото предимство от тази технология е че е ефективна срещу неизвестни заплахи. Начален профил се генерира през определен период от време (принципно в рамките на няколко дни, възможно е и през няколко седмици). Профилите могат да бъдат статични и динамични. Веднъж след като бъде генериран статичен профил, той остава непроменен докато не бъде зададена команда за промяна към IDPS. Динамичните профили се изменят в зависимост от наблюдаваното събитие. Тъй като системите и мрежите се променят постоянно, очакваното поведение също претърпява промени, което изисква пресъздаване на профила през определени периоди, ако използваме статични настройки. Динамичните профили от своя страна нямат такива

проблеми, но са податливи на техниките за преодоляване на защита (evasion). Например: Ако скоростта на промяна в следствие на атаката е прекалено ниска, IDPS може да приеме злонамерения софтуер за нормално поведение и да го включи към профила. В процеса на създаване на профила могат да бъдат наблюдавани и откривани злонамерени програми. Не са редки ситуациите, в които източникът на атака е включен към профила, възприет за шаблон. Администраторът може да модифицира профила с цел да премахне такива злонамерени компоненти. Друго предизвикателство при създаването на профили е сложността на постигане на висока точност. IDPS, използващи метода с аномалии, често генерират false positive. Това се получава когато добронамерени действия се отклоняват значително от приетият профил на поведение в разнообразни или динамични среди. Други затруднения от използването му е факта, че е много трудно при анализа да се определи причината за алармиране и дали алармата е действителна, поради сложността на събитията, които могат да я генерират.

Предимства:

- Използва данни със сигнатури на известни атаки;
- IDS може да почне да работи моментално след инсталацията;
- Лесно се конфигурира и има интуитивно използване;
- Всяка сигнатура си има идентификационен номер и име за да може администратора да посочи кои атаки трябва да се прихващат.

Недостатъци:

- Трябва да се обновява база данните със сигнатури;
- Новите атаки може да не присъстват база данните;
- С минимални промени на атаките, агресора може да избегне намиране на съответствие в база данните;
- Изисква място за съхранение на база данните.

Динамична защита чрез протоколен анализ

Това е процес на сравняване на предварително изготвен профил от основните протоколи, които са приети безопасни, със наблюдаваното събитие. За разлика от методът, базиран на аномалии, тук не се използват профили, които са специфични за хоста или мрежата. Тук се използват профили, които се създават от продавача, който е изготвил универсален профил, съдържащ правила как трябва и не трябва да се използват конкретни протоколи. IDPS може да проследява и разбира мрежовите, транспортните протоколи и протоколите на приложението. Например: Когато един потребител стартира сесия за прехвърляне на файл (File Transfer Protocol - FTP), при стартирането сесия се установява в неоторизирано състояние. Потребителят, които не е влезнал в системата, трябва да има правото да изпълнява ограничено количество операции, като да достъпва информация за помощ или да предоставя потребителско име и парола. Заявката и отговорът към нея се предават заедно на IDPS, като по този начин когато бъде подадена заявка, може да се установи дали тя е успешна по кодът на състоянието в съответният отговор. Така се определя кое поведение е подозрително и кое не. Например: Връщаме се към горният пример,

ако лице, което неуспешно е влезнало в системата все пак има достъп до всички операции, това би се възприело като съмнителни действия. В случай, че заявката е успешна това е нормално протичане на комуникацията между потребител и система.

Тази технология може да открие неочаквано използване на команди, като извикването й няколкократно или извикването й без използването на командата, от която зависи текущата. IDPS може да следи опитите за влизане в системата за всички сесии и да ги записва с цел проследяване на съмнителните дейности. Също така IDPS може да използва информация от компонента за оторизиране на достъп, с цел определяне на приемливо поведение за група потребители или конкретен потребител.

Този метод използва протоколни модели, които се използват в зависимост от стандартите на продавачите на софтуера или общо утвърдени стандарти. Този модел взема в предвид разликите в реализацията на протоколите. Много от стандартите не са напълно изчерпателни в детайлите за протокол, което позволява да съществуват различия при реализацията им. Също така много от разпространителите нарушават стандартите или добавят собствена функционалност, която може да измести стандартни функции. За индивидуалните протоколи често няма пълно описание, което затруднява анализа. Протоколните модели трябва да се обновяват с цел добавянето на протоколните промени към тях.

Основният недостатък на този анализ е, че използва прекалено много ресурси поради сложността си. Друг недостатък е, че не може да засече атаки, които не нарушават поведението на протоколите, възприето като допустимо, като изпълнение на много позволени операции с цел предизвикване на претоварване (Denial of service). Друг проблем , който може да възникне, е вероятността от конфликт между протоколната реализация на приложението и операционната система или комуникацията между клиент и сървър.

Видове IDPS технологии

- **Мрежово базирани (Network- based IDS - NIDS)-** IDS за мрежа са устройства, които работят в един мрежови сегмент. Функциониращи в т.н. хаотичен (promiscuous) режим, тези устройства записват целия трафик в дадения сегмент. Това им дава предимство спрямо ICS за хост, защото могат от едно място да откриват атаки насочени към много хостове. Освен това една или две ICS за мрежа могат много по-лесно да бъдат наблюдавани, отколкото десетки или стотици IDS за хостове. Тези системи имат и редица недостатъци. Първият от тях е, че повечето мрежи са комутируеми (switched). За да могат IDS за мрежа да функционират правилно, те трябва да имат достъп до целия мрежови трафик. Това може да се осигури като комутаторите се конфигурират с пренасочване на портовете (port forwarding), известно също като огледално копие на портовете (port mirroring). Пренасочването на портовете е възможност за препращане на трафика между различните портове към специално отделен порт за наблюдение. Не всички комутатори, особено по-

евтините, поддържат тази възможност. Освен това, дори да позволяват пренасочване на портовете, те не винаги поддържат възможността да наблюдават едновременно предаваните и приеманите пакети от тези портове. Увеличението на скоростта на предаване в мрежата увеличава проблемите с този вид IDS. Производителите могат да твърдят, че техните устройства откриват всички атаки при гигабитови скорости, но трябва да се обърне специално внимание на специализираната литература и да бъдат консултирани лаборатории провеждащи независими изпитания. В лабораторни условия може и да се постигне откриване на нарушения при гигабитови скорости, но в реалния свят горната граница е 300 Mbps. Причините за това широко разминаване се крият в разпалената реклама и в методите на провежданите тестове. В лабораторията имаме ограничен брой наблюдавани връзки и ограничен брой портове, като при това се използват максимални дължини на пакетите. Този начин на тестване позволява всеки продукт да работи в близост до максималните си теоретични възможности. Реалната производителност на IDS зависи от редица фактори на обкръжаващата среда, включително от броя на активните сесии, размерът на пакетите, а също така и от това, дали пакетите, които обработваме са валидни. Един валиден пакет създава много по-малко работа отколкото пакет, в който се опитваме да открием някакви непоследователни фрагменти от повече от няколко милиона активни връзки. За да се компенсират намалените възможности за откриване на проникванията при по-високи скорости на мрежата, можем да приложим няколко метода. Всички те по някакъв начин са свързани с разпределение на натоварването на високоскоростните връзки между множество IDS сензори. Трябва да използваме балансиране на мрежовия трафик или трафика на приложенията, като разделим този трафик на няколко ниско скоростни потока и към всеки един от тях да свържем отделен IDS сензор, който да наблюдава трафика в рамките на своите възможности. При това препоръчително е трафикът да се разделя на потоци към отделни дестинации или за отделни сесии, а не по кръгова схема (round-robin), каквато се използва при балансиране на натоварването в мрежовите устройства. Важно е пакетите от един поток да са свързани смислово, така че IDS да имат възможност да открият свързани пакети като част от една атака. Друг начин, който е много по-трудно управляем, но е значително по-евтин, е да разположим IDS сензорите по-близо до хостовете и по-далеко от гръбнака на мрежата, където се използват високоскоростни връзки. Макар че все по-често срещаме малки мрежи да използват Gigabit Ethernet връзки, много сегменти на мрежата работят на по-ниски скорости. Като поместим IDS сензорите в области, в които сме принудени да работим на по-малки скорости поради различни причини, можем да изградим добре работещи IDS без да прилагаме скъпи балансирания на приложенията или хардуерни гигабитови IDS.

- **Безжични (Wireless IDS - WIDS)** - наблюдава трафика по безжичните мрежи и анализира мрежовите протоколи с цел откриване на съмнителни действия, свързани със самите протоколи. Не може да открие атаки в приложните протоколи или мрежови протоколи от по-висок слой (TCP,UDP).
- **Анализ на мрежовото поведение (Network Behavior Analysis - NBA)** - изследва мрежовия трафик за да открие заплахи, които генерират нестандартен трафик, като разпространено

отказване на обслужване (Distributed Denial Of Service), някой видове злонамерени програми и престъпване на правила (клиентската система предлага услуги на други системи)

- **Терминално базирани (Host-based IDS - HIDS)** - работи за единичен терминал или устройство в мрежата. Тя следи за входните и изходните пакети на устройството и алармира потребителя или администратора при наличие на подозрителни дейности. Прави копие на съществуващите системни файлове и ги сравнява с предишните им версии. Ако основните файлове са модифицирани или изтрити , се изпраща аларма към администратора за допълнително разследване. Предимството на системата е, че можем да имаме голяма степен на доверие в нея, както и информация за всяка атака предприета към дадения хост. Обикновено трафикът към даден хост е подмножество на трафика в цялата мрежа, което ни позволява ефективно да изградим система от разпределени IDS с по-голяма вероятност на откриване на атаките именно поради малкия и специфичен трафик към конкретните хостове. Независимо от това предимство, тези системи имат и редица недостатъци. На първо място, те са зависими от операционната система на хоста. За хетерогенните мрежи това означава множество различни IDS, което води до по-големи административни разходи. Това е особено вярно в случая, когато искаме да покрием с този тип системи всички потребителски работни станции в мрежата. Възникват и проблеми със самото наблюдение на тези разпределени IDS. Ще има ли централно регистриране на събитията, или всеки един от тези хостове трябва периодично да бъде анализиран за своевременно откриване на прониквания? Поради тези недостатъци, IDS за хост обикновено се използват за защита само на особено чувствителни устройства, като например мрежови сървъри.
- **IDS Add-on –**
    - Потвърждаване на интегритета на системата (SIV – System Integrity Verifier) Наблюдава критични файлове в системата (системни файлове и други) с цел да провери дали са променяни. Следи системните регистри за да проследи основните сигнатури. Може да засече ако нормален потребител придобие администраторски права по непозволен начин.
    - Наблюдаване на log файлове (LFM – Log File Monitor) – създава запис с log файловете и след това ги анализира.
    - Honeypots - Направено е да изглежда като податлива на атака система с цел да се открият методите и инструментите използвани за атака. Важно е къде ще бъде позиционирано за да не застраши сигурността на мрежата : DMZ зона или зад защитната стена.

Компоненти и архитектура на IDPS

Типични компоненти

Основните компонентите в едно IDPS решение са:

- **Сензор или агент –** сензорите или агентите наблюдават и анализират дейностите. Терминал сензори обикновено се използва за IDPS, които наблюдават мрежи - мрежово базирани, безжични и анализ на мрежовото поведение. Терминал агент се използва единствено за терминално базираната технология.
- **Мениджмънт сървър –** това е централно устройство, което получава информация от сензорите и агентите. Сървърът е отговорен за тяхното управляване. Някой от сървърите извършват анализ на данните от събитието и имат възможност да открият събития, които самостоятелния агент или сървър не биха могли. Сравняването на информацията от множество сензори и агенти се нарича *корелация* . Повечето IDPS реализации използват такъв сървър, но не е изключена липсата на такъв за малка група от IDPS. В по-големите системи има повече от един сървър, като е възможно реализирането му в двуслойна структура.
- **Сървър на база данните –** това е хранилище за информацията, която се записва от сензорите, агентите и/или мениджмънт сървъра. Огромна част от IDPS поддържат база данни.
- **Конзола –** програма, която подсигурява интерфейс за потребителите и администраторите. Конзолната програма обикновено се инсталира на стандартен стационарен компютър или лаптоп. Някои от конзолите се използват единствено и само от администратора – конфигуриране на агенти и сензори, добавяне на софтуерни обновления. Други конзолни приложения се използват стриктно само на анализ и наблюдение. Някои от IDPS конзолите предлагат както администраторски възможности и възможности за наблюдение.

Мрежова архитектура

Компонентите могат да се свържат един с друг през стандартните мрежи на фирмата или през отделна стриктно проектирана мрежа, която се използва за управление на софтуера и се нарича мениджмънт мрежа. Ако използваме мениджмънт мрежа всеки от сензорите и агентите получава допълнителен мрежови интерфейс. Освен това всеки сензор или агент не може да праща трафик между защитената мрежа и която и да било друга мрежа. Останалите компоненти се свързват само към защитената мрежа. Този подход успешно изолира мениджмънт мрежата от производствената мрежа, това позволява да се прикрие наличието на IDPS от нарушителя, да се защитим от атакуващи и подсигурява сигурност, че IDPS има достатъчно широка честотна лена за да работи при неблагоприятни условия. Недостатъка на този подход е разходите за оборудване и неудобството за потребителите и администраторите от използването на различни машини за управление и наблюдение. В случай че не използваме допълнителен сървър можем да подобрим сигурността чрез създаване на виртуална мрежа в рамките на стандартната мрежа.

Функционалности за защита

- **Функционалност за събиране на информация** – събиране на информация от терминали и мрежи за различни събития.
- **Функционалност за създаване на log файлове** – IDPS генерирала логове с данни за откритите събития. Тези данни могат да се използват за потвърждаване на различни видове аларми, разследване на събитие или откриване на връзка между IDPS и останалите източници на информация. Основните полета, които се попълват са дата на събитието,време на събитието, тип на събитието, приоритет на събитието и предотвратяване на извършваните дейности.Обикновено логовете трябва да се съхраняват както локално, така и централно, с цел поддържане на интегритета и достъпа до данните. Освен това IDPS трябва да синхронизират времето си чрез мрежовия протокол (NTP – Network Time Protocol) и чрез честотна манипулация с цел достоверност на посочената информация в логовете спрямо време на възникване и други.
- **Функционалност за откриване на пробив** – обикновено се предлага широки функционални възможности за откриване на пробив. Точността на откриването изцяло зависи от типа на използваната технология, като се допуска използването на комбинирани стратегии. Повечето IDPS изискват настройване и персонализиране с цел подобряване на точността, употребата и ефективността. Например: Настройване на мерки за предотвратяване на събитие предизвикано от конкретен тип атаки. Някой основни възможности за персонализиране са:
    - **Прагове** – това е стойност, която поставя лимит между нормалното и анормалното поведение. Принципно установява максималното приемливо ниво. Най-често се използва при метода базиран на аномалии и при динамичната защита чрез протоколен анализ.
    - **Черен списък и бял списък** – черният списък съдържа информация за терминали, TCP или UDP портове, ICMP типове и кодове, приложения, потребители, URL сайтове, имена на файлове, разширения на файлове, които на някакъв етап са били определени като обвързани с конкретна злонамерена дейност. Те се използват за да се разпознават и блокират събития, които биха могли да са злонамерени, и за да може да се установява по –висок приоритет на аларми, които отговарят на запис в този списък. Белият лист съдържа информация за събития, които са известни като безопасни. Използват се за да се намали броя на false positive алармите свързани с дейности от сигурен източник. Обикновено тези два списъка се използват при метода базиран на шаблони и при динамичната защита чрез протоколен анализ.

Настройки на IDS

Когато първоначално инсталираме едно IDS устройство, то обикновено се нуждае от някакъв вид настройка. Това е така, защото първоначално нормалния трафик на мрежата е в известна степен подозрителен и наподобява някаква атака. Броят на настройките може да бъде значителен, в зависимост от това какви правила се проверяват и от вида на трафика в мрежата. Обемът на работата, свързана с настройката на IDS е толкова голям, че понякога се използва като

мощен аргумент при маркетинга на такива продукти. Производителите рекламират продуктите си и претендират, че не се изисква почти никаква настройка и едва ли не след включване на IDS в мрежата, устройството веднага започва да функционира нормално.

Заедно с появата на фалшиви сигнали, свързани с валидните пакети на нормалния трафик, съществува и проблема с невалидните пакетите, които не задействат системата за предупреждение, т.е. пакети които са част от неоткрита атака. Такива пакети създават даже много по-голям проблем на администраторите, понеже, по дефиниция, те не знаят за тяхната поява. Ето защо инсталирането дори на най-великите и мощни IDS продукти кара администраторите да се чувстват неуютно и несигурно.

В процеса на настройката трябва да решим какво да правим с информацията, която IDS произвежда. Една такава система обикновено има възможност да уведомява администраторите за алармени състояния по много различни начини. Използва се изпращане на SMS, електронна поща, или разпечатка на екран. Въпреки различията между отделните производители, IDS информацията или генерира сигнали за аларма, или се записва в регистрационни дневници.

Сигналите за аларма съобщават за събития, на които мрежовият администратор трябва веднага да обърне внимание. Например, една атака, която IDS класифицира като отваряне на вратичка за проникване (backdoor attack) е нещо, за което мрежовият администратор иска да научи незабавно. Сканирането на определен порт пък е нещо, което носи по-малък риск, и може да бъде само регистрирано и оставено за разглеждане на един по-късен етап.

Най-голямата грешка, която правят мрежовите администратори, когато конфигурират една IDS система, е тя да алармира мрежовия администратор всеки път, когато някой сензор регистрира някоя аномалия. В този случай алармените сигнали стават толкова много, че не смогваме с тяхното анализиране и в крайна сметка изключваме системата напълно. Ето защо, за да можем да използваме системата ефективно, на алармите трябва да зададем различни приоритети.

Най-разпространения начин за приоритизиране на IDS сигналите, е да използваме метод, много подобен на анализа на риска, като задаваме различна тежест на информацията, която прихваща IDS. Всеизвестно е в мрежовите среди, че вашата мрежа може да бъде атакувана или чрез случайно сканиране (цифровия еквивалент на натискане на дръжката на входната врата докато вие се намирате в хола), или чрез насочена „атака” (някой се опитва да разбие вратата и да офейка с каквото набързо отвлече). Понеже повечето IDS позволяват на мрежовия администратор да настройва различни нива на регистриране на сигналите от различни устройства, то има смисъл да се направи задълбочена инвентаризация на мрежовите активи преди всяка настройка на IDS. Ако имаме изградена правилна политика за сигурност, то голяма част от тази работа вече е била извършена по време на анализа на риска.

След инвентаризацията на мрежовите услуги следва да се създаде списък с техния относителен приоритет. Някои системи и приложения са по-важни от останалите. Например системата за планиране на ресурсите (Enterprise Resource Planning – ERP) или

системата за връзка с клиентите (Customer Relationship Management – CRM) са с много по-голям приоритет от системата на сървъра за печат. Пощенският сървър може да се разглежда като по-важен от файл сървъра, или обратното. На базата на тази информация, администраторът може да реши да бъде алармиран при предполагаема атака на ERP, а при атака на сървъра за печат да се извърши само регистриране на събитията и те да бъдат анализирани по-късно.

Заедно с приоритетите на ресурсите трябва да обмислим и приоритетите на атаките. Например, ако сте убедени, че вашите ERP сървъри са сравнително защитени срещу DoS атаки (какъвто е случаят при съвременните операционни системи след използването на множество кръпки), то такива атаки могат само да се регистрират. От друга страна, ако в публичното пространство са се появили нови заплахи и вие подозирате, че вашите сървъри не са подходящо защитени за тях, то би трябвало при поява на такъв тип активност в мрежата да бъдете незабавно алармирани.

В мрежите, в които са взети всички необходими мерки, естествено няма 100% гарантирана сигурност, но такива мрежи са сравнително добре защитени и са устойчиви на широко разпространените скриптови атаки. Такъв тип атаки трябва да се разглеждат като атаки с нисък приоритет. Те трябва да бъдат само регистрирани до достигането на определен праг, след което може да се издаде сигнал за аларма. От друга страна, всяка атака, която потенциално дава на нападателя достъп като администратор на системата, следва да се счита за атака с най-висок приоритет.

При определянето на относителния приоритет на алармите трябва да се има предвид и мястото на IDS сензора, който прихваща трафика. Сигналите от сензор, който се намира в сегмента на сървърите естествено са с много по-висок приоритет, отколкото сигналите идващи от сензор, който следи Интернет трафика извън защитната стена.

И накрая, работата по приоритетите на алармените сигнали значително се опростява, ако самата мрежа е в добро състояние от гледна точка на сигурността. А това означава всички операционни системи и приложения да бъдат осигурени с необходимите последни кръпки, всички процеси да бъдат документирани и потребителите да използват разумно криптиране и автентикация. Това ще позволи голям брой от атаките да бъдат само регистрирани и ще намали времето на администраторите за анализиране на атаки, които и без това вече са се провалили.

Работата по настройката на IDS може да отнеме много време. Системата трябва да бъде научена да игнорира фалшивите сигнали от валидни пакети и само да регистрира алармените сигнали с нисък приоритет. Крайният резултат от тази работа е кратък и сигурен преглед на заплахите, на които е изложена вашата мрежа, и които с малко късмет, са успешно отблъснати.

Разполагане на IDS в мрежата

Местата, където се поставят IDS в мрежата, зависят от броя на устройствата с които разполагаме. Например, ако имаме само една IDS система, най-разумно е да я поставим между външните маршрутизатори и защитната стена. Такова разположение ни гарантира, че целият

трафик ще бъде проверяван за атаки преди да бъде филтриран от защитната стена. Надяваме се IDS да служи като система за ранно предупреждение, която да ни показва пред какви заплахи е изправена защитната стена. Винаги е хубаво да се знае, когато някой се опитва да се промъкне в мрежата.

Основният недостатък на тази конфигурация е, че тя ще генерира голям брой аларми. Понеже нямаме метод, с който да установим със сигурност, кои атаки ще успеят и кои не, броят на атаките увеличава чувствителността на мрежовите администратори и те изразходват много време за анализ на генерираните от IDS доклади.

Някои привеждат различни разумни аргументи да разположите IDS в самата защитна стена. Логиката на тази позиция е, че управлението на IDS тогава ще бъде много по-лесно, тъй като голяма част от подозрителния трафик ще бъде блокиран от защитната стена. Така разположена вътре във вашата мрежа, IDS извършва и важна проверка на правилното конфигуриране и функциониране на самата защитна стена. Това ни позволява да научаваме за проведени срещу мрежата успешни атаки.

Въпреки че поставянето на самостоятелна IDS вътре в мрежата позволява на администраторите да се концентрират само върху заплахите, които са успели да заобиколят защитната стена, то тези администратори имат вече само ограничен поглед върху това, което се случва извън тяхната мрежа. Те няма да узнават например за атаките, които се провеждат срещу самата защитна стена.

Понеже една самостоятелна станция за управление може да обработва сигналите от много сензори, то често се използва конфигурация, при която се поставят сензори от двете страни на защитната стена. Това ни позволява да сравним информацията си за това на какви атаки е подложена мрежата и доколко защитната стена ни предпазва от тях. Ако ресурсите ни позволяват, IDS могат да бъдат разположени и на други стратегически места в мрежата. Най-честите вторични места на разполагане са демилитаризираната зона (DMZ) и сегментите, където са разположени сървърите. Когато искаме максимално наблюдение на трафика, можем да разположим IDS и в сегментите с работни станции на крайните потребители. Както е при всяко решение засягащо сигурността, броят и разположението на IDS сензорите следва да отразява приоритетите за сигурност на самата организация.

Във всички случаи IDS следва да се конфигурират в „невидим" режим. Невидим режим означава да не задаваме IP адрес на мрежовия контролер, който наблюдава трафика. Конфигурирането на IDS без IP адрес не позволява на никого извън мрежата да открие устройството и дори да научи за неговото съществуване. По този начин IDS сензорът е предпазен от мрежови сканирания и от атаките, които той се опитва да открие.

Премахването на IP адреса на сензора пречи и на администраторите да наблюдават и управляват процеса (когато използват TCP/IP). Това е от особено значение, когато в една мрежа са разположени няколко сензора и една централна станция събира информацията от тях. За да защитим IDS сензорите, и едновременно с това да извършваме тяхното дистанционно управление,

най разумно е да имаме два мрежови интерфейса. Единият интерфейс се използва като сензор и е конфигуриран без IP адрес. Вторият интерфейс обикновено се свързва в отделна локална мрежа, чиято единствена цел е събирането на информация и управлението на различните IDS устройства.

Реактивни IDS

IDS обикновено е пасивно устройство в мрежата. То тихо прослушва трафика и генерира изход, който се анализира от системния администратор. Устройството има големи възможности за алармиране на администратора при появата на значителни заплахи. Като имаме предвид обаче времето на отговор на компютрите сравнено с това на хората, човекът реално би могъл да реагира на атака тогава, когато тя вече е завършила. Най- доброто нещо което администраторът може да направи е да анализира дневника и да определи дали атаката е била успешна.

С течение на времето системните администратори започват да осъзнават, че в някои случаи IDS системата може да отговори на атаките вместо тях. Това е различно от защитната стена, където най-общо имаме статична конфигурация. Там пакетите се филтрират на базата на адреси, протоколи и портове. Ако желаете да позволите достъп на отдалечен хост до уеб сървър, трябва да позволите трафик през защитната стена с местоназначение порт 80. За да се защитим от атаки срещу уеб сървъра, ние можем да забраним трафика към порт 80, но тогава ще блокираме целия законен трафик към сървъра. Разбира се имаме възможност да блокираме трафика на основата на IP адреса на източника, но това може да стани само, ако ние вече знаем, че някой е използвал определен адрес за нападение , т.е. вече е имало успешна атака.

Много ще е хубаво, ако IDS сама може да организира защитата срещу атаки, които току що е открила. Това би премахнало бавната човешка реакция от затворения кръг. Ако някой се опита да атакува нашият хипотетичен уеб сървър като използва добре познатото прекосяване на директории, IDS би могла да изпрати към източника на атаката пакет за преустановяване на TCP сесията от името на уеб сървъра, след което да преконфигурира защитната стена така, че трафикът от този адрес да бъде блокиран. Нападателят ще бъде спрян от IDS, а останалите потребители могат да продължат да използват мрежата. Това звучи твърде хубаво, за да бъде истина.

Идеята за „реактивна” IDS, макар и не нова, не среща широко разпространение. От първостепенно значение е това, че пакети с подменени IP адреси на източника (spoofed IP packets) могат да бъдат използвани за провеждане на атаки от типа отказ на услуга (DoS). Ако например искам да попреча да използвате определен мрежов ресурс, мога просто за създам пакет, който да изглежда като че ли идва от ваш компютър и е начало на атака. По този начин вашият достъп до мрежовите ресурси ще бъде ограничен вследствие на мои действия. Представете си тази ситуация в много по-голям мащаб, с десетки хиляди пакети и ще разберете, че възможността от злоупотреба е голяма.

Независимо от това, идеята за реактивни IDS е твърде добра, за да умре от такива „малки” технически пречки. Някои от предложените възможности за реактивни IDS включват, както беше споменато по-горе, възможността активно да възстановяват TCP връзки, като сами изпращат

пакети с подменени IP адреси и динамично преконфигурират правилата на защитната стена, в отговор на заплаха, като това става в почти реално време. Други възможности включват спиране на изпълнението на процес в хост, заключване на потребителски акаунти, и изпращане на SNMP съобщения от типа “trap” към устройствата.

Интегриране на защитната стена с IDS устройство

Като имаме предвид взаимно допълващите се роли, които играят защитната стена и IDS, не трябва да се изненадваме, че производителите са създали устройства „всичко в едно”. Този тип устройства със сигурност улесняват интеграцията между реактивните IDS приложения и приложенията на защитната стена, тъй като и двете устройства използват един и същ хардуер.

Защитната стена може да бъде интегрирана и с VPN шлюз. Изобщо при интегрирането на няколко различни по своите функции устройства за сигурност в едно устройство, винаги получаваме определени предимства и недостатъци. От една страна, когато всички защитни функции се намират в едно устройство, сигурността на мрежата може по-лесно да бъде тествана, наблюдавана, конфигурирана и управлявана. Тъй като основна заплаха за информационната сигурност е твърде сложната конфигурация на мрежовите услуги, то очевидно е, че колкото е по-голяма е интеграцията на защитната стена с IDS, толкова по-лесно и безпроблемно те ще бъдат конфигурирани.

От друга страна, уповаването на само едно устройство за мрежова сигурност е рисковано предложение. IDS служи и за проверка на конфигурацията на защитната стена, а системата за регистриране служи за проверка на дейността на мрежата след определени събития. Ако всички тези системи бъдат поставени в едно единствено устройство, достатъчна е само една успешна атака към това устройство, и това да се окаже опустошително за цялата мрежа. Не само че вашата защитна стена ще бъде компрометирана, което само по себе си е сериозен инцидент, но вие ще загубите и способността да разберете за това.

Макар че разделянето на услугите по сигурността между различни устройства увеличава усилията за управление на системите , то също така и дава възможност за гарантиране на целостта и работоспособността на различните системи – дори и след като мрежата е била изложена на риск.

Няма еднозначен отговор на въпроса дали да използвате устройство, в което са интегрирани двете функции. Решението трябва да вземете вие, и то само след като сте наясно с последиците от него и как то ще повлияе върху вашата политика за сигурност.

Други видове IDS

„Традиционната” концепция на използване на IDS не е единственото оръжие в арсенала за мрежова защита. Ако вашата политика по сигурността го изисква, има и други мрежови елементи, които могат да бъдат включени като част от цялостната IDS стратегия.

Системите за откриване на нарушители са полезни, тъй като те предупреждават за съмнителна мрежова активност. Проблем обаче е да определим, дали откритата атака е била успешна. Най-добре е дейността по регистрирането на достъпа да се извършва на отделен хост, който от своя страна да бъде сигурен. От гледна точка на сигурността обаче, почти никога не знаем със сигурност дали вашата система, вашата IDS или системата за регистриране е сигурна. IDS системите за мрежа или хост само откриват атаки и други аномалии на мрежово поведение. Те обаче не дават информация за това, дали са направени легитимни промени в хостовете по мрежата и дали някой е получил физически достъп до хоста чрез локален терминал или флаш памет. Повечето IDS за мрежа не са в състояние да разберат за такива злоупотреби или промени. Ако искаме да знаем за тези събития, задължително е да използваме проверка на целостта на файла (file integrity checker).

Проверката на целостта на файла е софтуерна програма, която изчислява MD5 хеш суми на всички програми на даден хост. За всеки файл се изчислява индивидуална хеш сума. Тази сума се записва. Целта на програмата за проверка на целостта на файла е да позволи на мрежовия администратор да следи измененията в хиляди файлове и изпълними програми, които се намират на даден хост. Периодично, или когато мрежовият администратор подозира за някакъв вид компрометиране на мрежата, се стартира тази програма. Ако новата стойност на MD5 хеша е различна от старата стойност, то е ясно, че са настъпили някакви промени във файла.

В някои случаи промените във файла са очаквани. Такива са файловете, които се пазят в кеш или временни директории. Други файлове се променят при нормално използване, например файловете на база данни или файловете в потребителските директории. Изпълнимите файлове обаче се променят рядко, ако изобщо трябва да се променят. Системният администратор е този, който трябва да определи кои промени във файловете са допустими и легитимни и кои не. Всички програми за проверка на целостта на файл, които се намират в търговската мрежа, позволяват конфигуриране, така че мрежовият администратор да не подлага на проверка някои често използвани файлове.

Програмата за проверка на целостта на файл не ви позволява да определите каква промяна е настъпила. Тя само ще потвърди, че файлът е променен. Успехът на тази програма се дължи на интегритета на MD5 хеша, поради което не е препоръчително стойностите на хеша да се пазят на хоста, който се опитвате да защитите. Ако в този хост вече има вирус от типа „троянски кон”, то той може да модифицира хеш стойностите по такъв начин, че те да отговарят на направените промени. В идеалния случай хеш стойностите могат да бъдат записани на CD и да се съхраняват на сигурно място до следващата проверка.

Програмите за проверка на целостта на файловете са от съществено значение при определянето дали са правени промени в даден хост. Мрежовите администратори могат да се опитат ръчно да наблюдават тези хостове, но това се оказва непосилна и в крайна сметка безполезна задача. Типичните UNIX системи имат около 60 000 файла и дори да отстраним всички ненужни файлове, то пак ще останат над 15 000 файла. Неприемливо е използването на времето на администратора за търсене на промени в самите файлове или във времената за достъп до тях.

Много програми от типа „троянски кон” могат да прикриват промените в програмите, а понякога да скриват и цели приложения от типа „задна вратичка”, при претърсване на директориите и преглед на списъка от изпълняващите се процеси. В този случай дори и най-проницателните и способни мрежови администратори няма да могат да определят дали техните системи са били компрометирани просто като проверяват сами файловете.

Докато програмите за проверка на целостта на файловете може да се разглеждат като необходимост в хост машините, то има и друг инструмент на мрежовата сигурност, който е информативен, но някои го смятат за изключително важен.

Инструментите, които нападателите използват срещу мрежовите системи, са в непрекъснато развитие. Старите инструменти, които се възползват от миналогодишни уязвимости, вече не са актуални, тъй като са направени системни кръпки. Разработват се нови инструменти, които да се възползват от новооткрити уязвимости. За професионалистите по мрежова сигурност, проблемът е да се определи какви са новите атаки преди те да бъдат използвани срещу мрежата и да причинят вреди или да компрометират поверителна информация. Един нов подход към решаването на този проблем е да създадем отделна система, чиято единствена цел е да бъде атакувана и разбита. Това е известно като използване на капан наречен “honeypot”.

Honeypot, както подсказва превода на името му (гърне с мед), е привлекателно изглеждащ сървър в мрежата, който е разположен там само за да примамим някой да разбие неговата защита. Отделно от него е разположена една IP-невидима система, която действа като мрежов анализатор и която записва всички пакети към и от този сървър. След разбиването на сървъра, пакетите се изследват, за да определим метода, който е използван за компрометиране на системата. Един път разбрали същността на метода, вече не е трудно всички реално действащи сървъри в мрежата да бъдат защитени срещу тази нова заплаха.

Honeypot е много полезен срещу често срещаните скриптови атаки в Интернет. Използвайки прекомпилирани заготовки, много хакери с ограничени технически умения, са в състояние да нанесат големи щети в мрежите. При този клас атаки има голяма вероятност за компрометиране на всеки достъпен сървър. Това не означава, че honeypot не може да се използва за записване на действията на по-опитни хакери. Просто групата на високо квалифицираните хакери е по-проницателна при проучване на целите си и се стреми да завладее хостове, които да бъдат използвани в последствие за постигане на крайните цели, а не разбиване на всяко нещо, което изглежда интересно и с което могат да се справят.

Има honeypot продукти, които могат да емулират няколко операционни системи. Ако ви трябва например сървър, който емулира Apache Web Server с Red Hat Linux 6.0, то трябва само да изберете това като опция при конфигурирането. Ако искате да го промените на IIS сървър, избирате друга опция. Понеже honeypot е преди всичко средство за обучение, то най-добре е да използвате реален сървърен софтуер. Едновременно с обучението ви по често срещани атаки в Интернет, вие ще увеличавате и своите умения за защита на сървърите срещу такива атаки. Най-простият honeypot е просто един сървър, който е създаден и не предоставя никакви реални

услуги. Тъй като сървърът не обслужва мрежови ресурси, всеки достъп да него ще изглажда подозрителен. Акаунтът на администратора може да бъде променен от “Administrator” на някакъв друг, и всеки опит за достъп до сървъра като администратор автоматично ще генерира предупреждение.

За да увеличим максимално неговата ефективност, honeypot трябва да бъде конфигуриран с известна степен на сигурност. Това преследва две цели. Първата е, че нищо няма да научим от атаки, за които знаем всичко. Има достатъчно документация как да защитим мрежата си в значителна степен. Тази документация трябва да бъде използвана, а не отново да я преоткриваме. Ако сте положили достатъчно усилия за създаването на honeypot, то вие ще искате да извлечете и максимална полза от него. Втората причина е, че напълно незащитен сървър ще изглежда подозрително. Въпреки че броят на незащитените сървъри в Интернет все още е отчайващо голям, хакерите знаят за honeypot, и могат да бъдат подозрителни от съществуването на голяма мрежа с намиращ се в нея напълно незащитен сървър.

Honeypot може да бъде разположен на различни места в мрежата, в зависимост от целите на сървъра. Повечето организации го поставят извън обичайната си защитна стена. Това позволява лесен достъп до сървъра, като едновременно с това не подлага на риск истинската мрежа. Не е рядко явление обаче, да поставите honeypot във вътрешната мрежа, за да заловите служители, които могат да бъдат по-любознателни, отколкото корпоративната политика за сигурност им позволява.

И при двете местоположения трябва да имаме включен мрежов анализатор или даже IDS, който да следи целия трафик към honeypot. Както при нормалното разполагане на IDS, интерфейсът на сензора не трябва да бъде конфигуриран с IP адрес. Устройството ще подслушва трафика, но ще остава невидимо от гледна точка на мрежовия слой. Разпечатването на дневниците на хартиен носител или на CD може да достави много полезна информация за действията на атакуващия хакер.

Използването на механизъм за сигурност като honeypot може да се окаже понякога доста сложно от юридическа гледна точка. Някои организации създават honeypot като капан за примамване, заклещване и последващо преследване на лица и групи, опитващи се да компрометират техните сървъри. Границата между примамването (enticement) и заклещването (entrapment) може да бъде доста тънка. Примамването е законно, но със заклещването не е така. Простото поставяне на атрактивен сървър с няколко уязвимости в мрежата е пример за примамване. От атакуващите зависи дали ще открият примамката и ще се възползват от ситуацията. Заклещването от друга страна, би било действие на „издърпване” на потребителя към сървъра, за да се регистрира неговата дейност. Например рекламирането на пиратски софтуер в една дискусионна група с последващ запис на действията на всички, които са влезли да търсят такива файлове, ще се разглежда като заклещване.

Активното привличане на внимание в Интернет може да доведе и до други неприятни последствия. Въпреки че се надявате да заловите и преследвате атакуващите лица, в

действителност може да откриете, че тези лица са извън вашата юрисдикция и са недосегаеми за правоприлагащите органи според законите на тяхната страна. Като резултат от многото усилия за проследяване на нападателите, можете да откриете група гневни хора в другия край на света, върху която администраторът не може да упражни никакво въздействие. Освен това администраторите могат да открият, че са привлекли много голямо внимание и са подложени на допълнителни хакерски атаки към производствените мощности на корпорацията и атаки от типа отказ на услуга в мрежата като цяло.

Honeypot е интересно устройство за обучение по мрежови атаки и защита на мрежови ресурси; то със сигурност не е най-подходящото средство за залавяне на нападатели. С негова помощ можем да намерим необходимата информация за начина на атаката, но използването на нормалните процедури за сигурност ще ни снабдят с тази информация по един или друг начин.

Задачи за изпълнение

1) Дефинирайте основните принципи на IPDS системите за откриване (IDS) и защита от проникване (IPS).

2) Посочете приложенията и ключовите за функционалности на системите за откриване и защита от проникване IPDS.

3) Опишете основните методи за откриване на проникванията при системите за отриване на проникване IDS.

4) Анализирайте видовете технологии на системи за откриване и защита от проникване IDPS.

5) Избройте компонентите и съставете архитектура на система за откриване и защита от проникване IDPS.