Девета глава
СИСТЕМИ ЗА ДЕТЕКТИРАНЕ И ПРЕДОТВРАТЯВАНЕ НА ИНТРУЗИЯ

9.1 ОБЩИ СВЕДЕНИЯ

Откриването на атаки е процес на откриване на интрузионни събития, възникващи в процеса на експлоатация на дадена комуникационна система. Наличието на системи за откриване на атаки е задължителен елемент от политиката за сигурност. Аналогично на системите за управление на високоотговорни технологични процеси, в системите за защита на комуникационните системи възниква изискването за детектирането[1] на интрузионните действия в процеса (момента) на тяхното възникване, а не след тяхното реализиране.

Едновременно с **откриването на интрузия** е необходимо да започне функционирането на механизъм за **превантивни действия**. Превантивните действия са свързани с ограничаване или изолиране на действието на интрузионния източник и предприемане на активно противодействие с цел неговото блокиране и привеждане в неработоспособно състояние.

За реализирането на тези действия се прилагат два вида системи:

- **системи за детектиране на интрузия** (intrusion detection systems, IDS) и
- **системи за предотвратяване на интрузия** (intrusion prevention systems, IPS)

Към двата типа системи се предявяват изисквания за работа в реално време и безопасно след отказ поведение.

9.2 СИСТЕМИ ЗА ДЕТЕКТИРАНЕ НА ИНТРУЗИЯ

Система за детектиране на интрузия наричаме *всяко средство, което автоматично регистрира, анализира и сигнализира всяка неоторизирана активност в дадена комуникационна мрежа или крайна система.*

В това определение от съществено значение е правилното разбиране на понятието *детектиране на интрузия.* Употребата на това понятие характеризира свойството на системата за детектиране на интрузия да **регистрира** аномално поведение в трафика (потенциал за интрузия) в дадена комуникационна мрежа и да определи дали това аномално поведение е действително интрузионна дейност. Сами по себе си, системите за детектиране на интрузия не са цялостно решение за сигурността на комуникационна система, а част от политиката за сигурност, защитаваща тази система. Организирането на противодействието на интрузията се реализира от друг елемент на системата за защита.

[1] Може да се ползва и думата „разпознаване”.

Системите за детектиране на интрузия се различават от защитните стени по това, че правилата за филтриране на пакетите се извършват върху цялото съдържание на пакета или поредица от пакети. Анализират се както **заглавните части на пакета**, така **и данните** (полезния товар). В процеса на анализ на данните в тях се търси поредица от символи, които при попадане във вътрешната мрежа могат да предизвикат неоторизирана интрузионна активност.

Системите за детектиране на интрузия се използват за:

- защита от известни заплахи;
- защита от неизвестни заплахи;
- защита от блокиране на мрежа или система.

Защитата от известни заплахи се извършва на базата на търсене на познати модели в съдържанието на трафика и събитията, случващи се в една система.

Защитата от неизвестните заплахи се извършва на основа на изграждане на хипотези за класифициране на детектирани събития като заплаха чрез използване на изкуствен интелект, експертни системи или чрез адаптивно филтриране на трафик от специализиран софтуер.

Защитата от блокиране е насочена срещу детектиране на атаки, предизвикващи претоварване на мрежата или крайното устройство с излишен трафик. Детектирането се извършва посредством анализ на трафика, постъпващ към системата.

Основата на защитата от интрузия е **анализа на пакети**. Използват се два метода за анализ:

- **сигнатурен анализ** – метод за търсене на предварително дефинирани поредици символи (модели) в постъпващите пакети;
- **анализ на аномалиите** – метод за откриване на определени модели от мрежовия трафик (последователност на постъпване на пакетите), предварително дефинирани, като интрузионно опасни.

За да функционират двата метода се нуждаят от *обективен метод за събиране на данни* (регистриране на събития). По отношение на мрежи с комутация на пакети има два начина за събиране на данни:

а/ **огледално копиране на данните от портовете**. Всеки пакет, постъпил на порт в крайната системата се **копира**[2] към друг порт, където подлежи на анализ от работещата там програма. В резултат се класифицира като интрузионен или функционален.

б/ **анализ на данните в реално време.** Всеки пакет се анализира от програма в момента на постъпването му на определени портове. В зависимост от резултата от анализа пакетът или се изпраща в съответното направление или се отхвърля.

9.3 ТИПОВЕ СИСТЕМИ ЗА ДЕТЕКТИРАНЕ НА ИНТРУЗИЯ

Системите за детектиране на интрузия са:

[2] Копирането не спира постъпването на пакета в крайната система

1. Хост базирани;
2. Мрежово базирани;
3. Хибридни системи;

Хост базираните системи (Host-based intrusion detection systems- HIDS), представляват софтуер, стартиран, като резидентен[3] (системен) процес от съответната операционна система, управляваща дадения хост. Този процес сканира *определени системни ресурси*[4] и анализира записите в *определени файлове*[5] (системни, събитийни, трафични) за различни събития. Хост базираните системи регистрират възникналите събития и проверяват дали има съвпадение на регистрираното събитие с предварително дефиниран модел на интрузионна активност.

Мрежово базираните системи (Network-based Intrusion detection systems - NIDS), анализират *мрежовия трафик* (пакети) за наличие на определени поредици от символи (сигнатури) в тях. NDIS получава целия трафик за един мрежов сегмент[6]. След получаване на сегмента става възможно да се анализира целия поток от данни, постъпили или напуснали мрежовия сегмент. По този начин се гарантира възможност да се извърши анализ и да се търси модел на трафична интрузионна активност, резултат на разпределена атака[7].

Мрежовите системи следят за наличие на следните възможни заплахи в трафика:

1. **Опити за провеждане на единична атака** срещу даден комуникационен ресурс или услуга;
2. **Опити за провеждане на разпределена атака** (distributed denial of service[8]) насочена към конкретен хост, целяща предизвикване на отказ, който се изразява в невъзможност за реализиране на дадена услуга.
3. **Наличие на необичайна активност** от определени трафикоизточници (хостове или мрежи). Предполага се, че такава активност е свързана с подготовка на атака. Откриването ѝ дава възможност за предприемане на превантивни действия по отношение на източника и провеждане на действия, защитаващи атакувания обект.
4. **Аномалии в заглавните части** (header) на комуникационните протоколи в анализираните пакети. За разлика от предишните четири заплахи, аномалиите не могат да се определят като директна заплаха. Те могат да се резултат на случайни откази, грешки или умишлени интрузионни действия. Също така е трудно да се определи каква е целта на дадена аномалия, ако е предизвикана умишлено. Информационната неопределеност на една аномалия не дава възможност тя да

[3] Предварително стартиран процес, които стои в паметта непрекъснато.

[4] Системните ресурси са файлове, оперативна памет, стартирани програми.

[5] Всяка операционна система има специализирани файлове за записване на събитията, случили се по време на експлоатацията на системата.

[6] Група от компютри с една и съща мрежова маска.

[7] Атака, проведена поне от два интрузионни източника едновременно.

[8] Атаките са описани в глава „Видове атаки”.

се класифицира посредством сигнатурен анализ. За правилното й идентифициране е необходимо да се проведе по-сложен анализ от експертна система или изкуствен интелект, разработени за тази цел.

5. Необичайни **събития в мрежата**. За разлика от предните заплахи, които са вградени в трафика, тази заплаха е извън трафика и обобщава всички възможни неоторизирани събития, възникващи в процеса на експлоатация. Такива процеси са, например: промени на данни във файлове, изчезване или създаване на нови файлове-връзки и др.

Основните различия, [40] между двата вида системи за детектиране на интрузия са дадени в таблица 9.1.

Таблица 9.1.

Мрежови системи за детектиране на интрузия	**Хост базирани системи за детектиране на интрузия**
Контрол на цялата мрежова активност	Контрол на активност в рамките на хоста
Лесно инсталиране.	По-трудно инсталиране и настройване
По-добра детекция на атака от външна мрежа.	По-добра детекция на атака тип „от вътре”
По-лесна настройка.	По-трудна настройка.
Детекцията се базира на събития в цялата мрежа	Детекцията се базира на събития в една крайна система – хост.
Изследване на съдържанието на заглавните части на пакетите	Не се изследва съдържанието на заглавните части на пакетите.
Има възможност за реакция в реално време на системата.	Системата реагира само след като намери записано събитие в контролираните файлове.
Независимост от операционните системи в мрежата.	Специално разработени за конкретна операционна система.
Детектира атаките в мрежата, който се в полезния товар на пакетите.	Детектира локалните атаки, преди те да са навлезли в мрежата.
Детектира неуспешните атаки.	Верифицира успеха или неуспеха на дадена атака.

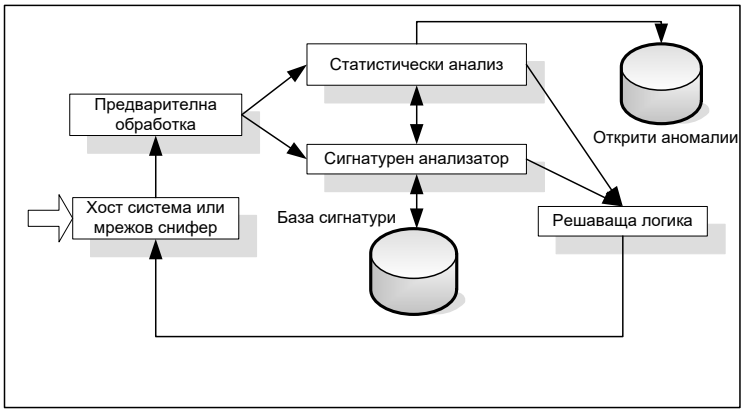
9.4. ПРИНЦИПНА СХЕМА ЗА РАБОТА НА СИСТЕМА ЗА ДЕТЕКТИРАНЕ НА ИНТРУЗИЯ

Начинът за реализиране на система за детектиране на интрузия е даден на Фиг.9.1.

Архитектурата на IDS включва [40] следните елементи:

- Хост система или мрежов снифер.
- Модул за предварителна обработка.
- Модул за статистически анализ.
- Модул за сигнатурен анализ.
- База данни с предварително дефинирани сигнатури.

- База данни с открити аномалии.
- Решаваща логика. Тя определя дали даден пакет или източник на пакети да бъде обявен за интрузионен или не.



Фиг. 9. 1 Принципна схема на система за детектиране на интрузия

Хост системата приема входящият мрежов трафик и го изпраща към модула за предварителна обработка. Този модул има възможност да отдели от трафика определени пакети и да ги изпрати за анализ. Отделянето на пакетите се извършва по предварително определени правила. Отделените пакети се изпращат за статистически анализ или сигнатурен анализ. Модулите за сигнатурен анализ и статистически анализ могат да обменят данни помежду си. Двата модула търсят аномалии в подаденият им за анализ трафик. Откритите аномалии се записват в база данни. В момента, в който се открие аномалия тя се изпраща в решаващата логика, която определя каква да е реакцията на системата за детектиране на интрузия за откритата аномалия. Ако се оцени аномалията като интрузия се предприема действие за нейното неутрализиране, съгласно приетата политика за сигурност. В случая може да се създаде правило за отхвърляне на пакетите. Това правило може да се изпрати към хоста. Ако на него има защитна стена, правилото може да се добави към другите правила и тези пакети да не се допускат в мрежата.

9.5. СИСТЕМИ ЗА ИНТРУЗИОННА ПРЕВАНТИВНОСТ (INTRUSION PREVENTION SYSTEMS - IPS)

Система за превантивна дейност (intrusion prevention systems, IPS) наричаме тази система, която при сигнализиране на интрузия активира мерки за нейното отстраняване. Разликата между тези системи и системите за детектиране на интрузия е, че IPS са активни системи, докато IDS - пасивни.

С цел изясняване на връзката между двете системи и защитните стени може да се даде със следния пример:

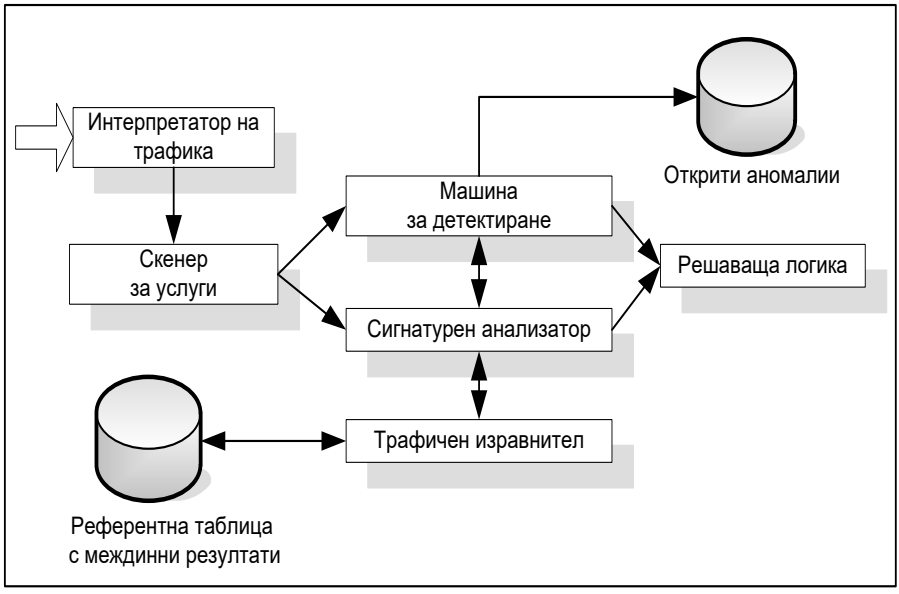
Може да се приеме, че защитната стена (firewalls) е входната врата на една къща, която пропуска само притежателите на ключ за вратата. Системата за детектиране на интрузия е алармата, която се активира, когато вратата (стената) не се отвори коректно (с необходимия ключ). Системата за превантивни действия е тази система, която отстранява проникналия нарушител, който е задействал алармата.

IPS имат възможността да противодействат активно на дадена атака чрез изолиране на източника на атака и/или неговото унищожаване. Дейността на IPS е свързана с понятието „превантивност". В този аспект IPS може да се разгледа като съставена от следните елементи (фиг.9.2):

- интерпретатор на трафика;
- скенер за услуги;
- машина за детекриране;
- изравнител на трафика.

Интерпертаторът на трафика извършва анализ на пакетите, може да реализира деасемблиране на пакетите и притежава блокиращи функции[9]. След интерпретатора, трафикът се насочва към **машината за детекриране.** Тя сравнява заложените в нея модели и взема решение въз основа на резултата от сравнението и данните, записани в поддържаната таблица от интерпретатора.

Скенерът на услуги създава, в процеса на работа, таблица с класификации на интрузии, въз основа на която **изравнителя на трафика** управлява информационния поток.



Фиг. 9. 2 Система за превантивни действия

Сравнението между IDS и ISP е представено [40] в *Таблица 9.2.*

[9] Функция, която определя дали да се блокира действието на даден обект.

Таблица 9.2

IDS	IPS
Инсталира се в мрежов сегмент или на хост	Инсталира се в мрежов сегмент или хост
Активно сканиране	Пасивно сканиране – по сигнал
Не може да обработи криптиран трафик	Обработва криптиран трафик
Централизиран мениджмънт	Централизиран мениджмънт
По-добро детектиране на хакерски атаки	Идеален за блокиране на WWW атаки
Предупреждаващ продукт	Блокиращ продукт

Съвременното ниво на развитие на тези системи предполага постепенно обединяване на функциите на двата типа системи, като по-общото понятие[10] е IDS.

В настоящата книга се разглеждат основно мрежовите системи за детектиране на интрузия.

9.6 АРХИТЕКТУРИ НА СИСТЕМИ ЗА ДЕТЕКТИРАНЕ НА ИНТРУЗИЯ

Архитектурата на конкретната реализация има критично значение за постигането на зададеното ниво на сигурност. Ефективна е тази архитектура, която дава възможност да се наблюдават и колекционират събития и трафик за всеки мрежов компонент или крайна система. Възможни са три архитектурни варианта:

- централизирана архитектура;
- разпределена архитектура;
- архитектура от тип „точка-точка".

Централизирана архитектура (single-tired architecture) е реализация, при която системата за детектиране на интрузия и системата за превантивни действия, колекционират и обработват данни сами за себе си, без да ги изпращат на други компоненти. Пример за такава архитектура е хост базираната. Тя ползва за източник на данни съответните системни файлове за регистриране на събития (sys-, event-log). Получените данни се сравняват с предварително подготвени шаблони (patterns), които представляват предварително дефинирани поредици от символи.

Разпределена архитектура (multi tired architecture) е реализация, която включва използването на специализирани компоненти, обменящи данни помежду си. Компонентите са разположени в различни точки на мрежовия сегмент и събират информация за определени събития в него.

Компонентите могат да се класифицират като:

- сензори;

[10] Отнесено към момента на писане на настоящата книга.

- анализатори (агенти);
- мениджъри.

Сензорите служат за регистриране на събития и аномалии в трафика. Събраната информация се изпраща за анализ.

Анализаторите (агентите) получават данни от сензорите и ги анализират по определени правила. Агентите са предназначени да изпълняват само един тип анализ. Например: един анализатор може да следи единствено TCP трафик. Друг следи единствено FTP (File Transfer Protocol) трафик. При откриването на интрузия (реализирана или започваща), агентът изпраща сигнал до **мениджъра**.

Мениджърът може да предприеме някое от следните действия:

- изпращане на алармено съобщение към конзола;
- позвъняване на пейджър или телефон;
- запис на информация за инцидента в база данни;
- търсене на допълнителна информация, свързана с инцидента;
- изпращане на инструкция до атакувания хост за прекратяване на определени процеси;
- изпращане на команда до защитната стена или рутера на мрежата за промяна на правата за достъп за определени адреси.

Тази архитектурна реализация е по-добра от централизираната понеже:

- осигурява регистрация на събития в целия мрежов сегмент, което дава възможност за събиране на по-добра информационна база за анализ на провежданите атаки;
- дава възможност за по-добра дълбочина на защитата и възможност за разпределяне на функциите на защитата на повече хостове;
- има по-надеждна и отказоустойчива архитектура.

Връзка от тип „точка-точка" (peer-to-peer architecture). Тази архитектура дава възможност за обмен на информация между две системи за детектиране на интрузия, изпълняващи сходни функции. Много често тя се използва за обединение на дейността на няколко системи за детектиране на интрузия и превантивни действия. При разпознаване на ново интрузионно събитие в дадена система, тя изпраща данните[11] за него до друга системата (с която е свързана). Последната променя контролните си функции и базата данни (access list), с която разполага. По този начин тя може да разпознае тази нова атака в момента на възникването й.

Основното предимство на този метод е простотата. На практика се формира група от системи, които обменят данни помежду си, без да е необходимо специализирано централно управление.

9.6.1. Сензори

Сензорите са критичните точки в системите за детектиране на интрузия. Функциите, които те изпълняват са прости и са свързани със събиране на определени типове данни от постъпващия трафик в мрежата.

[11] Правилото за разпознаване на атаката.

Сензорите са два типа:

- мрежови сензори;
- хост-базирани сензори;

Мрежовите сензори са по-често използваните от двата типа. Те представляват програми или специализирани мрежови устройства, които прихващат трафика в локалната мрежа или в мрежов сегмент. Сензорите са специализирани за прихващане на определени типове трафик. Използването на един сензор за следене на целия трафик е неправилно и може да се допуска само в краен случай. Сензорите не трябва да внасят закъснения в мрежата, породени от допълнителната обработка на пакетите.

Прихващането на данните се извършва по следния начин:

Всяка мрежова карта получава данните от мрежата. След като ги получи, тя ги изпраща на операционната система. Операционната система премахва Ethernet header-a и декодира с протоколния си стек получения пакет, с цел предаването на данните на съответния протокол от мрежовия слой. Най-често това е Internet Protocol. В IP header-a се прочита следващия протокол (от транспортния слой), за който са предназначени данните. На това ниво могат да се анализират данните, доставени от дейтаграмата и нейната заглавна част. В транспортния слой се анализира неговата заглавна част и номера на порта, за който са предназначени доставените данни. Така се достига до Application Layer, след който остават само данните оформящи полезния товар на пакетите. Тук данните могат да се анализират като отделни пакети или като цял файл.

Хост-базираните сензори следят пакетите, постъпили в мрежовия интерфейс. За целта мрежовата карта се поставя в режим на работа – promiscuous mode. В този режим се прихващат всички постъпили пакети от порта на мрежовото устройство (switch, hub). Колекционираните данни се изпращат към анализаторите.

За осигуряване на най-голямото покритие на регистрирането на събитията в мрежата, сензорът се конфигурира да приема данни, отнасящи се не само до него, но и за всеки друг хост в мрежата.

Следващите фактори въздействат на поведението на сензора:

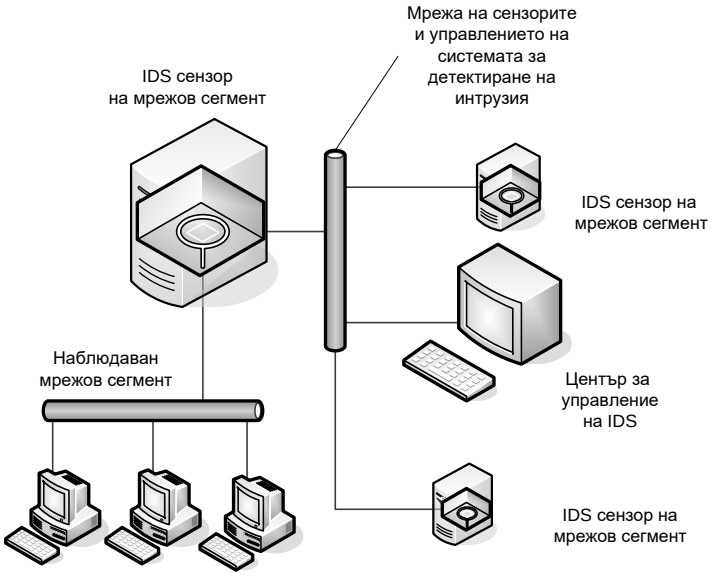
- местоположение;
- производителност;
- възможност за запис;
- мрежова конфигурация.

Местоположението на сензора зависи от това, какъв трафик трябва да се следи, и силно зависи от мрежовата конфигурация на дадения сайт. Основната структура на мрежа се състои от защитна стена (firewall), демилитаризирана зона (DMZ), една или няколко вътрешни и външни мрежи. Дизайнът на мрежата е планиран така, че да изолира различните услуги в отделни зони. Всяка от тях носи уникален вид трафик и товар и към всяка една от тях могат да се очакват различни опити за атаки.

За да се обхване пълната картина от събития в рамките на една мрежа, се поставят няколко сензора в различни части от мрежата. Потокът от данни от ня-

колко сензори е по-цялостен от този, постъпващ от един единствен сензор и помага да се намери корелацията между данните във фазата *анализ*.

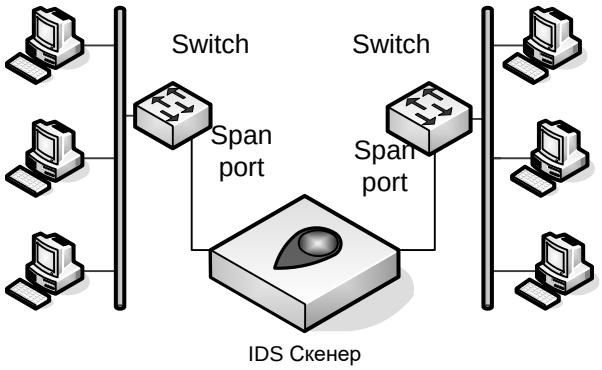
Сензорите се конфигурират така, че да наблюдават събитията в определен мрежов сегмент. Реализацията на сензора (Фиг 9.3), изисква използването на двуинтерфейсен хост (с две мрежови карти). Единият от интерфейсите е свързан към наблюдавания мрежов сегмент, а другият се използва за комуникация с мрежата на анализиращата система (мрежа за управление на сензорите). Конфигурацията, с два интерфейса има по-добра *производителност*[12] и *сигурност* на сензора.



Фиг.9. 3 Двуинтерфейсна конфигурация на мрежовите сензори

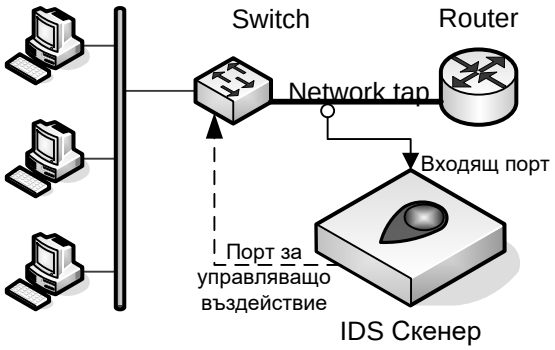
При използване на сензори в Ethernet мрежи, реализирани с комутатори (switch), е необходимо използване на специализиран порт (span port) за включване на сензора (фиг 9.4). На този порт се копира всеки пакет, постъпил в мрежовия комутатор от който и да е негов друг порт. По този начин сензора на мрежовия сегмент получава достъп до всеки постъпил пакет в тази част на мрежата.

[12] Скорост на обработване на пакетите. Ако е малка, се внася закъснение в работата на охранявания мрежов сегмент.



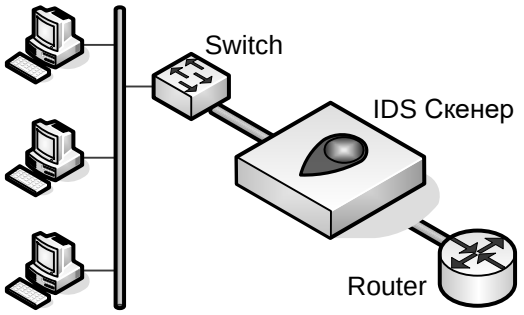
Фиг. 9. 4 Сканиране на трафик, чрез Span Port

За директно сканиране на трафика се използва метода представен на Фиг.9.5.



Фиг.9.5 Сканиране на трафик чрез Network tap

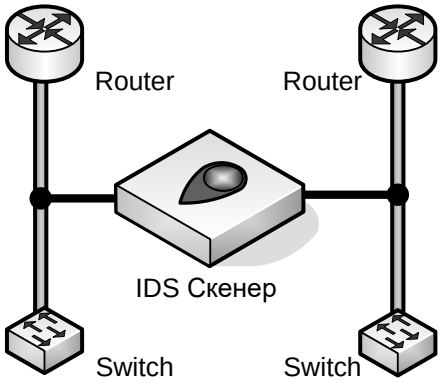
Друг възможен вариант е директното включване на сензора в мрежата.



Фиг. 9. 6 Сканиране чрез директно включване на скенер.

В този случай се използват два интерфейса за пропускане на трафика между рутера и комутатора (switch). Обвързването на скенера (сензора) със системата за анализ става чрез трети мрежов интерфейс.

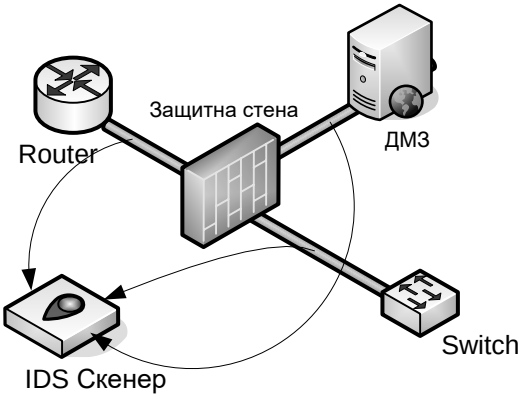
Един сензор може да се свърже с няколко мрежови сегмента. По този начин се получава комплексна картина на протеклите събития в няколко мрежови сегмента и може да се получи по-ясна представа за различните атаки, проведени в дадена мрежа.



Фиг. 9. 7 Метод за вграждане на сензора чрез многопортово сканиране

На фиг. 9.8 е даден вариант за включване на сензора, така че да получава данни от:

- входящия трафик от външната мрежа, идващ от рутера;
- трафика, филтриран от защитната стена, който постъпва във вътрешната мрежа;
- трафика, отклоняван към демилитализираната зона.



Фиг. 9. 8 Включване на скенер за пълен контрол на постъпващия трафик

Получената информация дава възможност да се анализират данните преди и след защитната стена. При регистриране на атака въз основа на тази ин-

формация може да се променят динамично правилата за филтриране на стената и да се локализира обекта на атака – дали е обект на вътрешната мрежа (след комутатора) или е обект от демилитализираната зона – най-вероятно сървър за публични услуги (електронна поща, файлов трансфер и др.).

Производителността зависи от способността на сензорите да прихващат целия трафик на сегмента и възможността да го записват. Като се има предвид, че локалните мрежи използуват 100 Mbit Ethernet, количеството записани данни става огромно дори при слабо натоварване. При установяване, че сензорът изпуска пакети, той се заменя с по-производителен такъв, или се конфигурира така, че да пропуска регистрацията на ненужните събития и записва само предварително дефинирани.

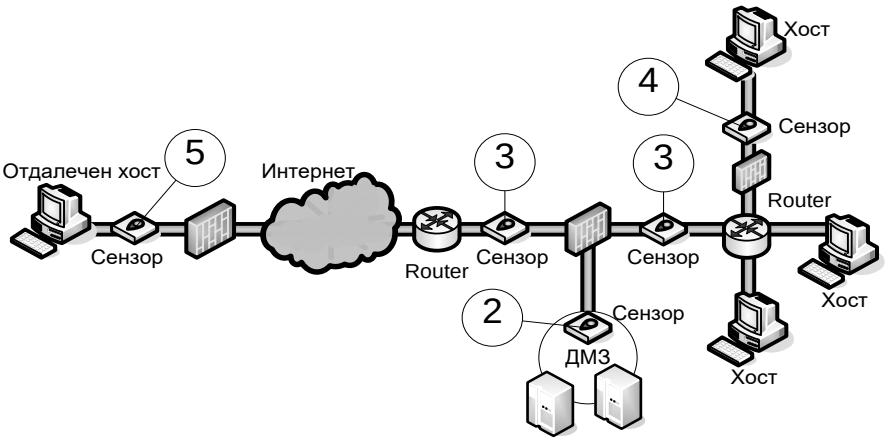
По време на работа на сензорите трябва да се следят параметрите, с които са стартирани. Всеки процес в операционните системи има определени привилегии по отношение на останалите компоненти. Част от процесите притежават големи права и привилегии. Такива са и програмите, използвани за сензори. В процеса на работа трябва да им се гарантира възможността да реконфигурират мрежовите устройства и да записват постъпилата от тях информация там, където други процеси нямат права на файлови операции.

От друга страна, е необходимо да се следи обема на заеманото дисково пространство. При записването на трафика сензорът може да изчерпи дисковото пространство и така да наруши работоспособността на операционната система.

При разполагането на сензорите е необходимо да се имат в предвид следните особености [57]:

1. Хост базираните сензори са по-добър източник на информация, понеже предоставят данни за конкретния хост, докато мрежовите сензори дават целия трафик в мрежата;
2. Хост базиранте сензори от своя страна имат ограничен поток от данни за анализ, което ограничава сканиращите им способности, докато мрежовите сензори могат да проведат сканиране върху целия обем от данни и да получат по-добри кореалционни характеристики.
3. Скоростта на пропускане (сканиране) на пакети е критична за сензорите. При трафик със скорост 350-400 MBps част от сензорите, могат да излязат от работоспособно състояние.
4. При използване на сензори в комутируеми мрежи има проблем с прихващането на целия трафик. За целта е необходимо ползването на комутиращи устройства от тип switch с наличие на порт, към който се копират всички постъпили пакети (spanning port).
5. При наличие на криптиран трафик е необходимо сканирането да се извършва в точката на получаване на трафика, където може да бъде декриптиран и анализиран.
6. При инсталиране на сензори предварително е необходимо да се определи, от гледна точка на транспортните протоколи, типа на следения от тях трафик. Целта е да се раздели трафика за филтриране от този, които няма да се допуска в мрежата.

Местата за разполагане на сензори са дадени на Фиг. 9.9.



Фиг. 9. 9 Приоритети при разполагане на сензори

Задължително се разполага сензор зад защитната стена разделяща вътрешната от външната мрежа. (1) Този сензор има възможност, както да анализира трафика преминал през стената, така и да прекрати преминаването на трафик към вътрешната мрежа при подаване на команда от съответния мениджър.

Целта на сензорите в демилитализираната зона (DMZ) е да следят трафика в зоната на сървърите. Между екраниращия рутер и защитната стена на мрежата се разполага сензор, който сканира трафика, постъпващ в стената. Така се организира контрол на входа и на изхода на стената. На базата на тази информация, впоследствие мениджърът на системата може да определи при детекриране на интрузия, какво ново правило да състави за защитната стена, което да не даде възможност за повторно провеждане на атаката. Събирането на такава информация дава възможност на системите да изпълняват „интелигентен анализ" и да работят в режим на самообучение.

Целта на сензорите преди вътрешната мрежа е да защитават специализираните сървъри, до които няма публичен достъп. Такива са сървърите за организиране на фирмената дейност (ERP), счетоводните сървъри и др.

Отдалечените офиси се намират в зоната на риска. Предполага се, че всеки от тях има система за детектиране на интрузия, аналогична на централния офис. Следенето на този трафик от специални сензори се прави с цел събиране на максимален обем информация за заплахите, касаещи бизнес дейността на фирмата. Колкото е по-пълен обемът от информация, толкова е по-голяма възможността за провеждане на „интелигентен" анализ и самообучение на системата за детектиране на интрузия.

9.6.2. Агенти

Агентите са следващото ниво в системите за детектиране и превантивни действия. Функциите на агентите са систематизирани още през 1990 година. Основната тяхна функция е **анализ на колекционираните данни от сензорите.** По принцип агентите могат да се представят като група от процеси, които се стартират независимо един от друг и имат за цел анализирането на възникналите системни събития. Всеки процес по принцип се проектира да търси определено поведение в получената колекция от данни. Независимостта на агентите е необходима, за да се гарантира устойчивостта на системата за детектиране на интрузия, насочена срещу нея. Предполага се, че такава интрузия може да е успешна срещу един агент, но останалите продължават да функционират. От друга страна, независимостта на агентите позволява изборното им включване в зависимост от вида на желания анализ.

Добре е агентите да се стартират на отделни хостове, като не се отнема възможността им да се кооперират помежду си посредством обмяна на съобщения. При откриването на опит за атака от един от агентите, той уведомява останалите, с които е свързан. По този начин се постига възможност за изолиране на атакувания мрежов сегмент, с което се предотвратява разпространението на интрузията в мрежата.

Взаимодействието между агентите дава възможност за предотвратяване на фалшиви аларми. Всеки агент, преди да обяви аларма, може да иска решението на други агенти за същия проблем. След получаването на данните от тях, може да се вземе решение на базата на организиране на кворум функция на принцип N от M.

Характеристики на агентите:

- **Агентите са адаптивни**. Те могат да работят в режим на самообучение.
- **Ефективност на агентите**. По-добре е да се работи с много на брой малки агенти. Така за всеки могат да се дефинират строго специализирани функции и вероятността за грешно разпознаване на интрузия да се сведе до минимум.
- **Гъвкавост**. Агентите могат да се възстановят след отказ или при отказ на източника им на данни. Това се дължи на възможността им периодично да записват състоянието си и при възстановяване да започнат работа при натрупана история до момента.
- **Независимост**. Агентите могат да се стартират независимо и при пропадане на един агент, останалите не губят функционалността си.
- **Мащабируемост**. Агентите могат да работят еднакво в големи и малки системи за детектиране на интрузия.
- **Мобилност.** Част от агентите могат да се преместват от една система в друга и да променят част от функциите си при тази миграция.

Недостатъци:

- **Заеман ресурс**. Агентите заемат функционални ресурси на операционната система и намаляват функционалността ѝ;
- **Фалшиви аларми**. Агентите генерират фалшиви аларми, които могат да доведат до нарушаване на работоспособността на операционните системи.
- **Настройване**. Агентите трябва периодично да се настройват и модифицират, с цел минимизиране на алармите. На практика това е вид обучение, което отнема време и изисква специализирани човешки ресурси.

9.6.3. Мениджъри

Мениджърите са *управляващата част* на системите за детектиране на интрузия.

По принцип сензорите и агентите могат да работят самостоятелно. При тази си работа те генерират голямо количество от данни. Възниква необходимост от периодичното архивиране и индексиране (класифициране по дадена схема) на това количество от данни. Правилният вариант за управление на данните е поддържането на RAID-масиви (Redundant Array of Inexpensive Disks). По този начин данните се записват върху голямо количество дискове под управление на една програма. Обикновено на един файл с данни се правят няколко копия. Така се постига висока надеждност на съхранение на натрупаната информация. Освен съхраняването на информацията мениджърите организират и методите за достъп до нея, така че да е гарантиран бърз достъп до поискан информационен ресурс.

Друга важна функция на менджмънта е *генериране на алармени съобщения* при откриване на интрузия и предприемане на действия по отношение на нейното неутрализиране. Най-често тези действия се изразяват в активиране на дадена система за превантивни действия и изпращане на съобщение посредством електронна поща, SMS или друг начин.

Мениджърите изпълняват *анализ върху настъпилите събития* за дълъг период от време с цел определяне на наличност на интрузионни действия, посредством търсене на корелации.

Част от мениджърите анализират проведените атаки стъпка по стъпка с цел локализиране на слабата част на избраната политика за сигурност. Целта е да се определи мястото на пробива и при какви условия е реализиран. Въз основа на този анализ могат да се получат правила за фино настройване на защитните компоненти и сензорите. Средствата за провеждане на тези анализи се основават на използване на невронни мрежи или експертни системи.

Освен анализ на данните, мениджърите изпълняват задачи по *мониторинг на отделните сензори и агенти.* Целта на мониторинга е да се установи готовността на сензора или агента и каква в вероятността да генерира фалшива аларма или да пропусне интрузия. Мониторингът се тества, като се провежда на фалшива атака от мениджъра и се анализира реакцията на агента или сензора.

9.7. АНАЛИЗ ЗА ОТКРИВАНЕ НА ИНТРУЗИЯ

Понятието „анализ" в контекста на детектиране на интрузия представлява процес на организиране и класифициране на събраните данни според техните връзки (релативни отношения) с цел идентифициране на аномална активност. Анализът може да се провежда в реално време, докато данните преминават през мрежата (real-time analysis). Той се разделя на четири фази: *предварителна обработка, анализ; отговор; пренастройване (фина настройка)*.

Предварителната обработка е ключова функция, която се извършва след като данните са регистрирани от сензорите. Тя има за задача да представи събраните данни в подходяща форма за анализ. Възможностите са две – или да се опишат в някаква канонична форма (мета език) или да се запишат в предварително структурирана релационна база данни.

Анализът може да се проведе чрез: *търсене на шаблони (сигнатурен анализ), детекция на трафична (или системна) аномалност и търсене на промени в определени обекти*.

Откриването на атаки, базирано на **сигнатурен анализ**, е сравнителен метод. Сигнатурата дефинира или описва образец, който се търси впоследствие в трафика. Сигнатурите могат да се отнесат както към протоколната заглавна част, така и към полезния товар. Изборът, какво да се анализира, зависи от специфичната IDS и от фокуса на политиката за сигурност. Създаването на сигнатури изисква детайлни познания за мрежи и сигурност.

В процеса на анализ на мрежовия трафик се търси интрузионна активност не само в отделните пакети. За целите на анализа системите за детектиране на интрузия могат да реасемблират дейтаграмите и да възстановят постъпилия трафик в целия мрежов сегмент. Това се прави с цел обхващане на цялостната трафична активност, постъпваща или отиваща към дадена мрежа. Анализирането само на отделни пакети се счита за ниско надежден метод за детекция на интрузия.

За да се реализира **анализ на аномалия в трафика** се използва предварителна подготовка на статистически профили, характеризиращи нормална или интрузионна трафична активност. Всяко отклонение или съвпадение със създадения модел се счита за аномалия. Мрежовият трафик има няколко характерни черти, които могат да бъдат използвани да се откриват аномалии в "нормалния" трафик: товар, ping времена, информация за достъп до портовете, брой на връзките, уникалност на сокетите и т.н.

Едно от предимствата на вторият тип анализ е възможността за анализ на криптирани данни и работа с тунели. Използването на метода *"сравняване на сигнатури"* при криптирани канали е почти безполезно, но използването на статистически анализ, дава метод за откриване на поведение, което може да е интрузионно. Такива събития могат да бъдат, например, необикновено висок брой връзки, необичайно високи нива на трафика за дадена връзка или необичайно „накъсване" на трафика. Принципно, инструментите за съставяне на статистика, събират информация на всеки един час, ден, седмица, а възможно е и на месец, в зависимост от това какъв период е приложим в случая.

Анализ на промяната е метод за детектиране на интрузия, основан на следене на състоянието на предварително зададени обекти. Целта е да се открие неоторизирана модификация (системна аномалност). По принцип следеният обект е файл, понеже това е основната градивна единица на операционните системи. За всеки наблюдаван файл се пресмята контролната му сума и стойността се криптира. Периодично това пресмятане се повтаря и се сравнява резултата от предишното. При откриване на разлика се генерира алармен сигнал, който се подава към системата за превантивни действия.

9.8. МОДЕЛ НА ПРОЦЕСА НА ОТКРИВАНЕ НА АТАКИ

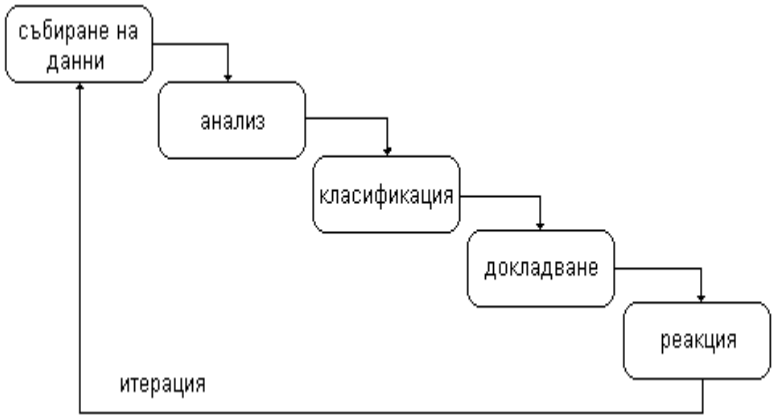
Процесът за откриване на атаки се състои от няколко стъпки:

1. събиране на данни,
2. анализ
3. класификация,
4. сигнализиране (докладване) на атаката,
5. предприемане на ответна реакция.

Тези пет стъпки на процеса на откриване на атаки, оформят каскада както е показано на Фиг. 9.10. Способността за автоматизиране на процеса по откриване на атаки е силно зависима от първите две фази:

- способността за събиране на качественни данни и
- способността за извличане на полезна информация от тях.

Фазите *класификация* и *сигнализиране* са свързани със способността на оператора (автоматичен или човек) да преработва данните с цел модифициране на правилата за откриване на интрузия.



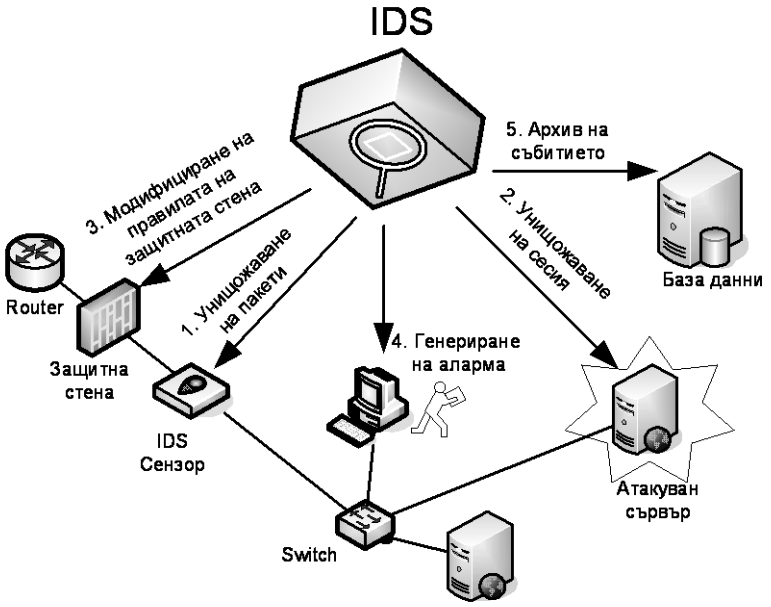
Фиг. 9. 10 Процес на откриване на атаки

Качеството на записаните данни за събитията, възникващи в системата по време на нормална работа и при интрузия, влияе на методите за извличане на полезна информация от тях. За целта е необходимо:

- Наблюдението да покрива *цялата система.* В случай на невъзможност да се обхване пълната гама от системни събития, се определят ключовите зони за наблюдение и съответно, точките, в които да се осъществи наблюдение. Ключовите зони се определят при оценката на риска и анализ на сигурността по време на съставянето на политиките за сигурност.
- Системата за запис трябва да регистрира успешно събитията, които се случват. Някои системи са проектирани да взимат само отделни проби[13] от случващите се събития. Това се прави с цел предпазване на системата от препълване на ресурсите и с голям обем от данни.

9.9. ПРЕВАНТИВНИ ДЕЙСТВИЯ ПРИ ДЕТЕКТИРАНЕ НА АТАКА

Превантивните действия са свързани с прекратяването или изолирането на атаката. Пример за такова действие е даден на Фиг.9.11.



Фиг. 9. 11 Детектиране и прекратяване на атака

В случая, системата за детектиране на интрузия е открила начало на атака към определен сървър в защитаваната мрежа. За да прекрати интрузията IDS предприема следните действия 40,57]

1. Изтрива пакетите постъпващи от източника на интрузия. За целта е необходимо да има вграден поне един сензор след защитната стена.

[13] Случаен набор от записи в определени системни файлове

2. Подава команда към атакувания сървър да прекратява установените сесии с източника на интрузия.
3. Модифицира или създава нови правилата за филтриране на защитната стена и ги зарежда в конфигурационните й файлове, така че тя да предотврати постъпването на нови пакети в мрежата.
4. Генерира алармено съобщение (в реално време) и го изпраща към централния мениджър по сигурността.
5. Създава файл с история на събитието и го записва в база данни или в определена директория.

КОНТРОЛНИ ВЪПРОСИ ПО ДЕВЕТА ГЛАВА

1. Избройте разликите между защитна стена и система за детекриране на интрузия?
2. Как бихте използвали система за предотвратяване на интрузия за да защитите сървър предоставящ публични услуги (например електронна поща)?
3. Избройте действията на мениджъра на система за детектиране на интрузия при регистриране на опасно събитие?
4. Предложете алгоритъм за работа на IDS при следене на трафика в даден мрежов сегмент? Какво е необходимо да се следи?
5. Предложете алгоритъм за откриване на интрузионни събития в мрежова конфигурация с два гейтуея.
6. Дадена е мрежа с двадесет хоста, един гейтуей и два рутера. Мрежата е разделена на две подмрежи, всяка от които има по 10 хоста. Разполагате с три сензора. Предложете възможна конфигурация на мрежата и разположете сензорите в нея. Аргументирайте решението си.
7. Какви са възможните предимства и недостатъци при разполагане на сензорите показани от фиг. 9.3 до фиг. 9.8 включително. При какви условия ще ползвате тези схеми на включване.
8. Какви правила за откриване на атаки ще предложите по отношение на TCP протокола? Опитайте се да докажете функционалността им.
9. Какви правила за откриване на атаки ще предложите по отношение на IP протокола? Опитайте се да докажете функционалността им.
10. Каква схема за събиране на данни ще предложите за дадена локална мрежа?
11. Как се променя решението, ако мрежата от предната задача се промени в три подмрежи?