Лекция 12

Обнаружение вторжений - это еще одна задача, выполняемая сотрудниками, ответственными за *безопасность* информации в организации, при обеспечении защиты от атак. Обнаружение вторжений - это *активный процесс*, при котором происходит обнаружение хакера при его попытках проникнуть в систему. В идеальном случае такая система лишь выдаст сигнал тревоги при попытке проникновения. Обнаружение вторжений помогает при превентивной идентификации активных угроз посредством оповещений и предупреждений о том, что *злоумышленник* осуществляет сбор информации, необходимой для проведения атаки. В действительности, как будет показано в материале лекции, это не всегда так. Перед обсуждением подробностей, связанных с обнаружением вторжений, давайте определим, что же это в действительности такое.

Системы обнаружения вторжений (*IDS*) появились очень давно. Первыми из них можно считать ночной дозор и сторожевых собак. Дозорные и сторожевые собаки выполняли две задачи: они определяли инициированные кем-то подозрительные действия и пресекали дальнейшее проникновение злоумышленника. Как правило, грабители избегали встречи с собаками и, в большинстве случае, старались обходить стороной здания, охраняемые собаками. То же самое можно сказать и про ночной дозор. Грабители не хотели быть замеченными вооруженными дозорными или охранниками, которые могли вызвать полицию.

Сигнализация в зданиях и в автомобилях также является разновидностью системы обнаружения вторжений. Если *система оповещения* обнаруживает событие, которое должно быть замечено (например, взлом окна или открытие двери), то выдается сигнал тревоги с зажиганием ламп, включением звуковых сигналов, либо сигнал тревоги передается на пульт полицейского участка. *Функция* пресечения проникновения выполняется посредством предупреждающей наклейки на окне или знака, установленного перед домом. В автомобилях, как правило, при включенной сигнализации горит красная лампочка, предупреждающая об активном состоянии системы сигнализации.

Все эти примеры основываются на одном и том же принципе: обнаружение любых попыток проникновения в защищенный периметр объекта (*офис*, здание, автомобиль и т. д.). В случае с автомобилем или зданием периметр защиты определяется относительно легко. Стены строения, ограждение вокруг частной собственности, двери и окна автомобиля четко определяют защищаемый периметр. Еще одной характеристикой, общей для всех этих случаев, является четкий критерий того, что именно является попыткой проникновения, и что именно образует защищаемый периметр.

Если перенести концепцию системы сигнализации в компьютерный мир, то получится *базовая* концепция системы обнаружения вторжений. Необходимо определить, чем в действительности является периметр защиты компьютерной системы или сети. Очевидно, что периметр защиты в данном случае - это не стена и не ограждение. Периметр защиты сети представляет собой виртуальный периметр, внутри которого находятся компьютерные системы. Этот периметр может определяться межсетевыми экранами, точками разделения соединений или настольными компьютерами с модемами. Данный периметр может быть расширен для содержания домашних компьютеров сотрудников, которым разрешено соединяться друг с другом, или партнеров *по* бизнесу, которым разрешено подключаться к сети. С появлением в деловом взаимодействии беспроводных сетей периметр защиты организации расширяется до размера беспроводной сети.

Сигнализация, оповещающая о проникновении грабителя, предназначена для обнаружения любых попыток входа в защищаемую область, когда эта область не используется. Система обнаружения вторжений *IDS* предназначена для разграничения авторизованного входа и несанкционированного проникновения, что реализуется гораздо сложнее. Здесь можно в качестве примера привести ювелирный магазин с сигнализацией против грабителей. Если кто-либо, даже владелец магазина, откроет дверь, то сработает сигнализация. Владелец должен после этого уведомить компанию, обслуживающую сигнализацию, о том, что это он открыл магазин, и что все в порядке. Систему *IDS*, напротив, можно сравнить с охранником, следящим за всем, что происходит в магазине, и выявляющим несанкционированные действия (как, например, пронос огнестрельного оружия). К сожалению, в виртуальном мире "огнестрельное оружие" очень часто остается незаметным.

Вторым вопросом, который необходимо принимать в расчет, является *определение* того, какие события являются нарушением *периметра безопасности*. Является ли нарушением попытка определить работающие компьютеры? Что делать в случае проведения известной атаки на систему или *сеть*? *По* мере того как задаются эти вопросы, становится понятно, что найти ответы на них не просто. Более того, они зависят от других событий и от состояния системы-цели.

**Определение типов систем обнаружения вторжений**

Существуют два основных типа *IDS*: узловые (*HIDS*) и сетевые (*NIDS*). Система *HIDS* располагается на отдельном узле и отслеживает признаки атак на данный узел. Система *NIDS* находится на отдельной системе, отслеживающей сетевой трафик на наличие признаков атак, проводимых в подконтрольном сегменте сети. На [рисунке 13.1](https://intuit.ru/studies/courses/102/102/lecture/2995?page=1#image.13.1) показаны два типа *IDS*, которые могут присутствовать в сетевой среде.



**Рис. 13.1.**Примеры размещения IDS в сетевой среде

**Узловые IDS**

Узловые *IDS* (*HIDS*) представляют собой систему датчиков, загружаемых на различные сервера организации и управляемых центральным диспетчером. Датчики отслеживают различные *типы событий* (более детальное рассмотрение этих событий приводится в следующем разделе) и предпринимают определенные действия на сервере либо передают уведомления. Датчики *HIDS* отслеживают события, связанные с сервером, на котором они загружены. *Сенсор* *HIDS* позволяет определить, была ли *атака* успешной, если *атака* имела *место* на той же платформе, на которой установлен датчик.

Как будет показано далее, различные типы датчиков *HIDS* позволяют выполнять различные *типы задач* *по* обнаружению вторжений. Не каждый тип датчиков может использоваться в организации, и даже для различных серверов внутри одной организации могут понадобиться разные датчики. Следует заметить, что система *HIDS*, как правило, стоит дороже, чем сетевая система, так как в этом случае каждый *сервер* должен иметь лицензию на датчик (датчики дешевле для одного сервера, однако общая *стоимость* датчиков больше *по* сравнению со стоимостью использования сетевых *IDS*).

С использованием систем *HIDS* связан еще один вопрос, заключающийся в возможностях процессора на сервере. Процесс датчика на сервере может занимать от 5 до 15 % общего процессорного времени. Если датчик работает на активно используемой системе, его присутствие отрицательно скажется на производительности и, таким образом, придется приобретать более производительную систему.