Методы и средства защиты информации

ЛЕКЦИЯ 4:

СИСТЕМЫ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ

Тейс Г.Н., 2013

Системы мониторинга сетей

- Системы обнаружения и предотвращения вторжений (IDS/IPS).
- Системы предотвращения утечек конфиденциальной информации (DLP-системы).

Системы обнаружения вторжений

- Система обнаружения вторжений (СОВ, Intrusion Detection System, IDS) — программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими в основном через Интернет. Системы обнаружения вторжений обеспечивают дополнительный уровень защиты компьютерных систем.
- Системы обнаружения вторжений используются для обнаружения некоторых типов вредоносной активности, которая может нарушить безопасность компьютерной системы. К такой активности относятся сетевые атаки против уязвимых сервисов, атаки, направленные на повышение привилегий, неавторизованный доступ к важным файлам, а также действия вредоносного программного обеспечения (компьютерных вирусов, троянов и червей)

Архитектура СОВ

- сенсорная подсистема - сбор событий, связанных с безопасностью защищаемой системы
- подсистема анализа - выявление атак и подозрительных действий на основе данных сенсоров
- хранилище, обеспечивающее накопление первичных событий и результатов анализа
- консоль управления - конфигурирование СОВ, наблюдать за состоянием защищаемой системы и СОВ, просматривать выявленные подсистемой анализа инциденты

Сетевая СОВ
Network-based IDS (NIDS)

- Отслеживает вторжения, проверяя сетевой трафик и ведет наблюдение за несколькими хостами. Сетевая система обнаружения вторжений получает доступ к сетевому трафику, подключаясь к хабу или свитчу, настроенному на зеркалирование портов, либо сетевое TAP устройство.
- Пример – Snort (www.snort.org).

Основанная на протоколе СОВ (PIDS)

- Система (либо агент), которая отслеживает и анализирует коммуникационные протоколы со связанными системами или пользователями. Для веб-сервера подобная СОВ обычно ведет наблюдение за HTTP и HTTPS протоколами. При использовании HTTPS СОВ должна располагаться на таком интерфейсе, чтобы просматривать HTTPS пакеты еще до их шифрования и отправки в сеть.

Основанная на прикладных протоколах СОВ (APIDS)

- Система (или агент), которая ведет наблюдение и анализ данных, передаваемых с использованием специфичных для определенных приложений протоколов. Например, на веб-сервере с SQL базой данных СОВ будет отслеживать содержимое SQL команд, передаваемых на сервер.

Узловая СОВ
Host-based IDS (HIDS)

- Система (или агент), расположенная на хосте, отслеживающая вторжения, используя анализ системных вызовов, логов приложений, модификаций файлов (исполняемых, файлов паролей, системных баз данных), состояния хоста и прочих источников.

- Пример – OSSEC (www.ossec.net).

Гибридная СОВ
Hybrid IDS

- Совмещает два и более подходов к разработке СОВ. Данные от агентов на хостах комбинируются с сетевой информацией для создания наиболее полного представления о безопасности сети.

- Пример – Prelude (www.prelude-ids.org).

Пассивные и активные СОВ

- **Пассивная СОВ** - при обнаружении нарушения безопасности, информация о нарушении записывается в лог приложения, а также сигналы опасности отправляются на консоль и/или администратору системы по определенному каналу связи.
- **Активная СОВ** (Система Предотвращения Вторжений, IPS, Intrusion Prevention system) ведет ответные действия на нарушение, сбрасывая соединение или перенастраивая межсетевой экран для блокирования трафика от злоумышленника. Ответные действия могут проводиться автоматически либо по команде оператора.

Классификация систем предотвращения вторжений

- Сетевые IPS (Network-based Intrusion Prevention, NIPS): отслеживают трафик в компьютерной сети и блокируют подозрительные потоки данных.
- IPS для беспроводных сетей (Wireless Intrusion Prevention Systems, WIPS): проверяет активность в беспроводных сетях. В частности, обнаруживает неверно сконфигурированные точки беспроводного доступа к сети, атаки человек посередине, спуфинг mac-адресов.
- Поведенческий анализ сети (Network Behavior Analysis, NBA): анализирует сетевой трафик, идентифицирует нетипичные потоки, например DoS и DDoS атаки.
- Система предотвращения вторжений для отдельных компьютеров (Host-based Intrusion Prevention, HIPS): резидентные программы, обнаруживающие подозрительную активность на компьютере.

Спуфинг

- Вид хакерской атаки, заключающийся в использовании чужого IP-адреса или MAC-адреса для обмана системы безопасности.
- ARP-спуфинг — техника атаки в Ethernet сетях, позволяющая перехватывать трафик между хостами. Основана на использовании протокола ARP.

DoS-атака

- Атака типа «отказ в обслуживании», от англ. Denial of Service) — атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых легальные (правомерные) пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ затруднён.
- Отказ «вражеской» системы может быть и шагом к овладению системой (если в нештатной ситуации ПО выдаёт какую-либо критическую информацию — например, версию, часть программного кода и т.д.). Но чаще это мера экономического давления: простой службы, приносящей доход, счета от провайдера и меры по уходу от атаки ощутимо бьют «цель» по карману.

DDoS-атака

- Если атака выполняется одновременно с большого числа компьютеров, говорят о DDoS-атаке (от англ. Distributed Denial of Service, распределённая атака типа «отказ в обслуживании»).
- В некоторых случаях к фактической DDoS-атаке приводит непреднамеренное действие, например, размещение на популярном интернет-ресурсе ссылки на сайт, размещённый на не очень производительном сервере (слэшдот-эффект). Большой наплыв пользователей приводит к превышению допустимой нагрузки на сервер и, следовательно, отказу в обслуживании части из них.

Виды DoS атак [ч.1]

- **Ошибка в программном коде**, приводящая к обращению к неиспользуемому фрагменту адресного пространства, выполнению недопустимой инструкции или другой необрабатываемой исключительной ситуации, когда происходит аварийное завершение программы-сервера — серверной программы. Классическим примером является обращение по нулевому (null) адресу.
- **Недостаточная проверка данных пользователя**, приводящая к бесконечному либо длительному циклу или повышенному длительному потреблению процессорных ресурсов (вплоть до исчерпания процессорных ресурсов) либо выделению большого объёма оперативной памяти (вплоть до исчерпания доступной памяти).

Виды DoS атак [ч.2]

- **Флуд** — атака, связанная с большим количеством обычно бессмысленных или сформированных в неправильном формате запросов к компьютерной системе или сетевому оборудованию, имеющая своей целью или приведшая к отказу в работе системы из-за исчерпания системных ресурсов — процессора, памяти или каналов связи.
- **Атака второго рода** — атака, которая стремится вызвать ложное срабатывание системы защиты и таким образом привести к недоступности ресурса.

Эксплойт

- От англ., - эксплуатировать.
- Компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему.
- Целью атаки может быть как захват контроля над системой (повышение привилегий), так и нарушение её функционирования (DoS-атака).

Виды эксплойтов

- Эксплойты для операционных систем
- Эксплойты для прикладного ПО (проигрыватели, офисные пакеты и т. д.)
- Эксплойты для браузеров
- Эксплойты для интернет-продуктов (IPB, WordPress, VBulletin, phpBB)
- Эксплойты для интернет-сайтов (facebook.com, hi5.com, livejournal.com)
- Прочие эксплойты

Выявление DoS-атак [ч.1]

- **Предотвращение**. Профилактика причин, побуждающих тех или иных лиц организовывать и предпринять DoS-атаки. (Очень часто кибератаки вообще являются следствиями личных обид, политических, религиозных и иных разногласий, провоцирующего поведения жертвы и т.п.)
- **Фильтрация и блэкхолинг**. Блокирование трафика, исходящего от атакующих машин. Эффективность этих методов снижается по мере приближения к объекту атаки и повышается по мере приближения к атакующей машине.
- **Обратный DDoS** - перенаправление трафика, используемого для атаки, на атакующего.
- **Устранение уязвимостей**. Не работает против флуд-атак, для которых «уязвимостью» является конечность тех или иных системных ресурсов.

Выявление DoS-атак [ч.2]

- **Наращивание ресурсов**. Абсолютной защиты, естественно, не дает, но является хорошим фоном для применения других видов защиты от DoS-атак.
- **Рассредоточение**. Построение распределённых и дублирование систем, которые не прекратят обслуживать пользователей, даже если некоторые их элементы станут недоступны из-за DoS-атаки.
- **Уклонение**. Увод непосредственной цели атаки (доменного имени или IP-адреса) подальше от других ресурсов, которые часто также подвергаются воздействию вместе с непосредственной целью атаки.

Выявление DoS-атак [ч.3]

- **Активные ответные меры**. Воздействие на источники, организатора или центр управления атакой, как техногенными, так и организационно-правовыми средствами.
- **Использование оборудования для отражения DoS-атак**. Например, DefensePro® (Radware), SecureSphere® (Imperva), Периметр (МФИ Софт), Arbor Peakflow®, Riorey, Impletec iCore и от других производителей.
- **Приобретение сервиса по защите от DoS-атак**. Актуально в случае превышения флудом пропускной способности сетевого канала.

Ботнет

- (от ro**bot** и **net**work) — это компьютерная сеть, состоящая из некоторого количества хостов, с запущенными ботами — автономным программным обеспечением. Чаще всего бот в составе ботнета является программой, скрытно устанавливаемой на устройство жертвы и позволяющей злоумышленнику выполнять некие действия с использованием ресурсов заражённого компьютера. Обычно используются для нелегальной или неодобряемой деятельности — рассылки спама, перебора паролей на удалённой системе, атак на отказ в обслуживании.

СОВ и Межсетевой экран

- Межсетевой экран отличается тем, что ограничивает поступление на хост или подсеть определенных видов трафика для предотвращения вторжений и не отслеживает вторжения, происходящие внутри сети.
- СОВ, напротив, пропускает трафик, анализируя его и сигнализируя при обнаружении подозрительной активности. Обнаружение нарушения безопасности проводится обычно с использованием эвристических правил и анализа сигнатур известных компьютерных атак.

Ваши вопросы

?