ВВЕДЕНИЕ

Развитие компьютерных сетей, интеграция локальных сетей в одну общую сеть приводят к росту происшествий и атак. Для защиты от атак человечество придумывает все новые механизмы, и в то же самое время хакерские атаки становятся все более и более изощренными. Однако основные принципы сетевой защиты сформулированы уже достаточно давно и остаются неизменными. В пособии мы не будем описывать изощренные технологии атак, часть из которых реализована только в теории. Соответственно, не будем приводить и способы защиты от изощренных атак, так как считаем, что, разобравшись с основными принципами защиты от стандартных «классических» атак, читатель с успехом сможет освоить механизмы защиты и от более сложных. В процессе изложения будем предполагать, что защищается небольшая компьютерная сеть, в которой не обрабатывается критичная информация или информация, составляющая государственную тайну, так как требования к защите таких сетей предъявляются существенно более высокие.

Цель пособия — дать возможность читателям на практических примерах изучить способы защиты информации в небольшой компьютерной сети от стандартных сетевых атак.

Системы обнаружения атак (СОА) получили широкое распространение в качестве одного из ключевых средств защиты современных информационных систем (ИС), так как позволяют реализовать многоуровневую стратегию обеспечения информационной безопасности (ИБ), используя активные механизмы защиты от внешних и внутренних угроз, автоматизируя задачи мониторинга и корреляции событий ИБ, а также обеспечить систему управления инцидентами ИБ данными, необходимыми для расследования инцидентов. Длительное время СОА имели лишь исследовательское значение, первые попытки их коммерческого производства были предприняты в 1990 г. компанией Haystack Labs и лишь относительно недавно (2000 г.) было налажено массовое коммерческое производство и крупномасштабное использование СОА для защиты ИС. Не так давно начался широкий переход от концепции обнаружения компьютерных атак к концепции их предотвращения.

Учебное пособие посвящено основным этапам применения СОА: разработке и эксплуатации. В нем описаны математические модели,

используемые в качестве базы для алгоритма обнаружения компьютерных атак. Рассмотрены вопросы эксплуатации распространенных СОА: Snort, Suricata, Cisco IDS Sensor, Cisco MARS. В качестве основы пособия использовались материалы курсов, читаемых авторами в Уральском федеральном университете имени первого Президента России Б.Н. Ельцина.

В учебном пособии рассмотрены вопросы, связанные с применением систем обнаружения компьютерных атак. Порядок изложения охватывает основные этапы применения СОА, включая разработку и эксплуатацию.

В первой главе приведена информация о современных компьютерных атаках. Проанализированы возможные подходы к классификации компьютерных атак.

Во второй главе учебного пособия дается анализ основных типов СОА, применяемых на практике в настоящее время. В этой же главе приводятся сведения о математических моделях, предлагаемых различными авторами в качестве базы для алгоритма обнаружения компьютерных атак. Значительное место в главе уделено рассмотрению существующих методов обнаружения компьютерных атак на основе нечетких множеств и нечеткой логики.

Третья, завершающая глава, посвящена вопросам эксплуатации СОА. В качестве примеров рассмотрены распространенные СОА Snort, Suricata, Cisco IDS Sensor, Cisco MARS. Подробно описывается интерфейс СОА Snort и приводятся примеры правил обнаружения распространенных атак. Дан обзор развертывания СОА Suricata. Рассматриваются технологии обнаружения сетевых компьютерных атак на примере системы Cisco IDS Sensor. Завершается глава описанием технологии обнаружения комплексных сетевых атак с применением комплекса Cisco MARS.

По мере изложения теоретического материала читателям предлагаются практические задания, обозначенные абзацем «**Выполнить!**». Выполнение заданий, а также ответы на содержащиеся в них вопросы являются необходимым условием освоения учебного материала.

1 ВЫЯВЛЕНИЕ СЕТЕВЫХ АТАК ПУТЕМ АНАЛИЗА ТРАФИКА

1.1. Понятие и систематика компьютерных атак

Компьютерная атака — это целенаправленное воздействие программными средствами, в том числе с использованием компьютерных вирусов, на информационно- телекоммуникационную систему (ИТС), ИС или конкретное СВТ, осуществляемое с целью нарушения конфиденциальности, целостности или доступности информации. Назовем *сетевой* компьютерную атаку, использующую сетевую среду для осуществления удаленного доступа к объекту атаки. В целом компьютерная атака рассматривается как любая злоумышленная деятельность, направленная против компьютерной системы.

Получение достоверных сведений о компьютерных атаках представляет собой достаточно сложную задачу. Не существует единого авторитетного источника информации, посвященного статистике проведения компьютерных атак. Статистика доступна только для вредоносных программ и уязвимостей программного обеспечения. Ясно, что компьютерные атаки, реализуемые вредоносными программами (сетевыми червями, вирусами и пр.), представляют лишь подмножество компьютерных атак. Вместе с тем сетевая активность, создаваемая сетевыми червями, достаточно велика, и в ней могут быть легко замаскированы реализации единичных случаев компьютерных атак. В итоге наблюдается небольшое число разновидностей атак, реализующих несколько уязвимостей, и это никак не отражает степень опасности новых уязвимостей, которые постоянно обнаруживаются в различном программном обеспечении ПО. Кроме того, информация об успешно проведенных атаках скрывается организациями, которые пострадали от них, поскольку это может привести к подрыву доверия потребителей. Информация, доступная по уязвимостям программного обеспечения, в значительной степени отражает потенциальные возможности злоумышленников по совершению компьютерных атак. Использовать статистику обнаружения уязвимостей следует с большой осторожностью, ведь большое число уязвимостей не всегда говорит о высокой опасности использования того или иного ПО, хотя бы в силу того, что эти

уязвимости могут оперативно исправляться производителем путем выпуска соответствующих пакетов обновлений. С другой стороны, одна критическая уязвимость, обнаруженная и использованная хакерами до выпуска пакета обновления может привести к катастрофическим последствиям. Учитывая все это, наиболее достоверные сведения о компьютерных атаках могут быть получены лишь в результате экспертной оценки, выполненной специалистами в области информационной безопасности.

В литературе можно найти значительное число разноплановых классификаций атак на компьютерные системы и сети. Цель любой классификации — объединение объектов в группы, элементы каждой из которых имеют одинаковые свойства. Классификация атак может проводиться по различным признакам в зависимости от решаемой задачи.

Приведем, например, классификацию, которая основана на результатах исследований, проведенных в 1998 г. при разработке первых методик тестирования СОА. Описываемая классификация содержит четыре основных категории, основанные на результатах проведения атаки с точки зрения атакующего: зондирование (probing), атаки типа «отказ в обслуживании» (Denial of Service — DoS), повышение полномочий (User-To-Superuser — U2Su), несанкционированный доступ с удаленного узла (Remote-To-Local — R2L). Недостатком указанной классификации является то, что она не затрагивает таких существенных аспектов, как используемая уязвимость и механизм осуществления атаки. Кроме того, большинство современных атак, использующих одни и те же уязвимости сетевых систем, при атаке на операционную систему (ОС) и ПО различных версий могут приводить к различным результатам. Так, большинство атак, направленных против ОС Microsoft Windows и ставящих целью удаленное получение полномочий администратора, работают лишь в конкретных версиях ОС. Если версия ОС (точнее, отдельных ее библиотек) не совпадает с требуемой, то попытка реализации атаки может приводить лишь к перезагрузке компьютера, т. е. атака повышения полномочий становится атакой на отказ в обслуживании. Причем в обоих случаях действия атакующего, в том числе с точки зрения системы обнаружения атак, могут выглядеть идентично.

Будем использовать следующую систематику компьютерных атак (рис. 1.1). Исходной предпосылкой в ней является то, что *атакующий* (*attacker*) — это человек, преследующий какую-то цель и использующий для ее достижения разнообразные методы. Для любой компьютерной атаки атакующий является отправной точкой.

Рис. 1.1. Систематика компьютерных атак

Будем делить атакующих на шесть различных категорий:

- *хакеры* (*hackers*) — занимаются взломом компьютерных систем из «спортивного интереса» и для самоутверждения;
- *шпионы* (*spies*) — стараются заполучить интересующую их информацию для использования ее в политических целях;
- *террористы* (*terrorists*) — взламывают компьютерные системы для запугивания граждан, т. е. также преследуют политические цели;
- *рейдеры* (*corporate raiders*) — сотрудники одной компании, взламывающие компьютерные системы конкурента для получения финансовой прибыли;

- *профессиональные преступники* (*professional criminals*) — взламывают компьютерные системы для получения финансовой прибыли (не являются рейдерами);
- *вандалы* (*vandals*) — взламывают компьютерные системы для причинения вреда.

Соответственно выделяются четыре основных цели (*objective*), которые преследуют атакующие:

- *самоутверждение* (обычно является целью хакеров);
- *политическая выгода* (цель шпионов и террористов);
- *финансовая выгода* (цель рейдеров и профессиональных преступников);
- *причинение вреда* (цель вандалов).

Для достижения своих целей атакующий должен получить доступ (*access*) к компьютерной системе, а точнее — к информации, которая в ней обрабатывается. Это, может быть сделано через использование *уязвимости* (*vulnerability*) системы. Уязвимости делятся на:

- *уязвимости реализации* (*Implementation Vulnerability*) — ошибки в программном коде или аппаратной реализации (при отсутствии ошибок на этапе проектирования);
- *уязвимости проектирования* (*Design Vulnerability*) — ошибки, допущенные в ходе проектирования;
- *уязвимости конфигурации* (*Configuration Vulnerability*) — ошибки, допущенные при настройке компьютерной системы.

В результате использования той или иной уязвимости атакующий получает возможность осуществить несанкционированный доступ к процессу (*process*), функционирующему на атакуемой компьютерной системе, или несанкционированно (неправильно) использовать его. Этот процесс, в свою очередь, получает доступ к файлам или передаваемым данным. Результатом осуществления доступа атакующего к компьютерной системе может стать:

- *повреждение информации* (*Corruption of Information*) — несанкционированная модификация хранимых файлов или данных, передаваемых по сети;
- *разглашение информации* (*Disclosure of Information*) — получение информации лицами, не имеющими прав на доступ к ней;
- *«кража службы»* (*Theft of Service*) — несанкционированное использование локальной или сетевой службы, не ведущее к ухудшению качества услуг, оказываемых другим (законным) пользователям;

- *отказ в обслуживании* (*Denial-of-service*) — целенаправленное блокирование или ухудшение качества работы компьютера или сетевых служб (ресурсов).

Последним звеном систематики является инструмент (*tool*), которым пользуется атакующий, чтобы осуществить доступ к компьютерной системе. Предполагаются следующие инструменты:

- *пользовательские команды* (*User Command*) — атакующий вводит команды с использованием командной строки или графического интерфейса;
- *сценарий или программа* (*Script or Program*) — сценарий или программа, запускаемые для проникновения в атакуемую систему с использованием имеющихся в ней уязвимостей. Пример: программа-эксплоит или троянская программа, размещаемая атакующим в компьютерной системе;
- *автономный агент* (*Autonomous Agent*) — активизируемые атакующим программа или фрагмент программы, которые функционируют независимо, самостоятельно выбирают объект для атаки и проникают в систему, используя ее уязвимости. Пример: компьютерные вирусы и черви;
- *инструментарий* (*Toolkit*) — атакующий использует пакет, который может включать сценарии, программы или автономных агентов, и предназначенный для проникновения в атакуемую компьютерную систему путем использования ее уязвимостей. Пример: программный пакет, состоящий из перехватчика паролей и троянской программы, совместно устанавливаемых на атакованной системе;
- *распределенный инструмент* (*Distributed Tool*) — атакующий распределяет инструмент на множество сетевых узлов, которые затем синхронизируются для одновременного начала атаки на выбранную цель. Пример: программы для организации распределенной атаки на отказ в обслуживании;
- *утечка информации* (*Data tap*) — перехват побочных электромагнитных излучений сетевого кабеля или компьютера.

Главной задачей данной систематики является упрощенное изображение «пути», который необходимо проделать атакующему, чтобы достичь выбранной цели. Не исключается возможность существования нескольких путей для достижения одной и той же цели. Кроме того, в процессе осуществления атаки несколько путей могут использоваться одновременно.

В качестве несомненного достоинства предложенной систематики следует отметить наглядность и логичность, позволяющие, с од-

ной стороны, рассматривать компьютерную атаку как последовательность отдельных этапов, каждый из которых может быть выполнен несколькими возможными способами, с другой — классифицировать атаки по семи различным признакам (атакующий, используемый инструмент, тип уязвимости, тип доступа, объект доступа, результат атаки, цель атаки). Внимания заслуживают разделение результата и цели компьютерной атаки. Действительно, нарушение конфиденциальности информации сложно назвать целью компьютерной атаки. Целью может быть, например, получение финансовой прибыли в результате использования добытых конфиденциальных сведений.

В литературе вводится понятие простой и комплексной атак. Будем считать, что *простая атака* включает в себя действия, выполняемые в рамках одного этапа *комплексной атаки* (*complex cyber attack*). В целом простая атака реализует один из следующих этапов комплексной атаки на ИС: разведка (*Probe*), проникновение (*Penetrate*), закрепление (*Persist*), распространение (*Propagate*) и парализация (*Paralyze*). Данная модель называется моделью 5P.

На этапе разведки злоумышленник осуществляет сбор информации о потенциальной цели и направлении атаки. На данном этапе могут реализовываться действия типа сканирования сетевого диапазона, сканирования портов, идентификации сервисов и ОС, выявление их уязвимостей.

На этапе проникновения уязвимости ИС используются для получения доступа к ее ресурсам или для ее компрометации.

Этап закрепления характеризуется тем, что злоумышленник производит некоторые действия, позволяющие ему в будущем проникать в систему без необходимости использовать уязвимость, с помощью которой произошло проникновение. На этом этапе злоумышленник может, например, установить программное обеспечение удаленного администрирования или создать нового пользователя. Кроме того, на этом этапе злоумышленник может уничтожить следы своего проникновения и своей активности.

После проникновения и закрепления на отдельных компонентах ИС злоумышленник может расширять область своего присутствия на другие части ИС, используя атакованные ресурсы. Этот этап называется распространение.

Парализация представляет этап, на котором реализуются деструктивные действия, такие как атака на отказ в обслуживании, кража и уничтожение информации.