формационные технологии». Томск, 9-13 ноября 2015 г. – 2016-Томск: Изд-во ТПУ. – Т.1, с. 69 – 70.

3. Кобзарь А.И. Прикладная математическая статистика.–М.: Физматлит, 2006.–816 с.

4. Кацман Ю.Я., Лепустин А.В., Илюхин Б.В. Влияние контекстных факторов на оценку результатов эффективности работы школ томской области [Электронный ресурс] // Современные проблемы науки и образования. – 2014. – №. 6. – С. 1-11. - Режим доступа: http://www.science-education.ru/120-16117

ТИПЫ DDOS-АТАК, МЕТОДЫ ПРОФИЛАКТИКИ И ЗАЩИТЫ ОТ НИХ

Фролов С.Г., Демин А.Ю.
(г. Томск, Томский политехнический университет)

TYPES OF DDOS-ATTACKS, METHODS OF PREVENTING AND DEFENDING AGAINST IT

Frolov S.G., Demin A.U.
(Tomsk, Tomsk Polytechnik University)

DDoS is the most popular type of attack on the company for disabling its service. This article presents classification of the most popular types of DDoS and methods of defending and preventing from it.

Keywords: DoS attack, DDoS attack, defending methods, methods of prevention of DDoS.

DoS-атака или атака типа «отказ в обслуживании» направлена на вычислительную систему с целью создать такие условия, при которых пользователи системы не могут получить данные к определенным ресурсам или сервисам. Одновременная атака с большого числа компьютеров свидетельствует о *DDoS*-атаке – распределенной атаке типа «отказ в обслуживании». Атаки выполняются с помощью зараженных специальными программами компьютеров, которые часто называют «компьютерами-зомби». [1]

Классификация *DDoS*-атак и защита от них. Все *DDoS*-атаки можно классифицировать на три больших типа:

- атаки, направленные на заполнение канала;
- атаки, использующие уязвимости протоколов;
- атаки, использующие уязвимости приложений.

Атаки, направленные на заполнение канала. Этот тип атак направлен на забивание полосы пропускания. Интенсивность данного вида атак измеряется в битах в секунду. В данный тип атак входят такие разновидности флудов, как *UDP* флуд, *ICMP* флуд и прочие направленные потоки фальшивых пакетов.

Существует способ защиты от таких атак — фильтрация паразитного трафика на уровне ЦОД или специализированных сервисов защиты. Для фильтрования остатков паразитного трафика рекомендуется также применять аппаратную защиту.

Атаки, использующие уязвимости протоколов. Эта категория направлена на существующие ограничения различного оборудования или уязвимости сетевых протоколов. Атаки данного типа засоряют ресурсы оборудования сфальсифицированными пакетами, в результате чего система оказывается неспособной обрабатывать полезный трафик. Сила атаки измеряется в пакетах в секунду. К этому типу атак относятся *SYN* флуд, *Ping of Death* и т.д.

Против таких атак самым эффективным средством является аппаратная защита. Специально разработанные устройства для фильтрации трафика помогут отсеять паразитный трафик от полезного.

Атаки на уровне приложений. Атаки данного типа направлены на различные уязвимости, которые присутствуют в программном обеспечении. Они приводят к выходу из строя какого-либо приложения или операционной системы в целом. Типичным представителем

данного вида атак является атака нулевого дня. Сила атаки такого вида измеряется в запросах в секунду.

Такой вид атак наиболее сложен для отражения. Они являются узконаправленнными, из-за чего могут создать глобальные проблемы атакуемому оборудованию при малых затратах ресурсов атакующего. Простой флуд *HTTP*- и *GET*-запросов является самым распространенным видом.

К методам защиты от таких атак можно добавить некоторые программные алгоритмы, которые анализируют запросы и создают правила для брандмауэра по результатам полученного анализа.

Виды *DDoS*-атак. Существует очень много видов *DDoS*-атак, у каждой свой характер и способы борьбы. Наиболее часто встречающиеся виды представлены ниже.

***UDP* флуд.** Тип *DDoS*-атаки, при которой атакующий перегружает случайный порт на хост-машине, используя *UDP*-пакеты. Атакуемое оборудование проверяет, использует ли этот порт какое-либо из запущенных приложений или процессов, и если не находит, то отправляет ответ «*Destination Unreachable*». Так как система получает все больше и больше *UDP*-пакетов и отвечает на них, то в скором времени она становится недоступной для пользователей. Простейшая защита – блокировка *UDP*-трафика.

***ICMP* флуд.** Засорение атакуемого компьютера пакетами *ICMP*. Система должна обязательно ответить на такой пакет, поэтому атакующий стремится создать большое количество пакетов, которые снижают пропускную способность канала. Типичная защита - блокировка *ICMP*-трафика. Сервер будет невозможно пропинговать, однако он будет доступен и одной уязвимостью будет меньше.[2]

***SYN* флуд.** Тип *DDoS*-атаки, которая использует «тройное рукопожатие», присущее *TCP*-соединению, чтобы задействовать все ресурсы атакуемой машины и сделать ее недоступной для окружающих. При *SYN* флуде атакующая сторона посылает запросы на TCP-соединение быстрее, чем атакуемая сторона может их обработать, что забивает сетевой канал и делает недоступным конечное оборудование.

***MAC* флуд.** Тип сетевой атаки, при которой атакующая сторона, подключенная к какому-либо порту маршрутизатора, засоряет интерфейс маршрутизатора большим количеством *Ethernet*-пакетов с различными поддельными *MAC*-адресами источников.

Атака нулевого дня. Атака, основанная на использовании уязвимости нулевого дня, то есть применяемая в период, когда данная уязвимость остается неизвестной и против которой пока не разработаны защитные механизмы.

Деградация сервиса. Основной смысл атак данного вида — симуляция действий реальных людей в многократном объеме. Самый простой вариант — бесконечные множественные запросы одной страницы сайта. Защита – временная блокировка страницы с выдачей сообщения об ошибке.

Общий принцип защиты — анализ поведения и отсеивание подозрительных *IP*-адресов на уровне брандмауэра. Чем более сложный алгоритм используется атакующей программой, тем сложнее выявить фальшивый трафик и тем чаще происходят ложные срабатывания, блокирующие доступ к оборудованию реальным пользователям.

Методы профилактики. Самые необходимые меры, которые позволят быстрее и эффективнее отразить *DDoS*-атаку, представлены ниже.

Изучите свою сетевую конфигурацию. У каждого сервиса есть характерные черты использования сети: объём и типы используемого трафика и т.п. Изучите стандартные характеристики и регулярно отслеживайте текущую картину. Вы сможете заранее принять необходимые меры, если будете знать, что атака начинается.

Имейте под рукой необходимые контакты. Вы должны знать с уверенностью, к кому обратиться в случае, если Вы уже находитесь под атакой или ощущаете её приближение.

Искать людей, которые смогли бы Вам помочь в данной ситуации — это последнее, что необходимо, когда атака уже началась.

Имейте четкий план действия при атаке. Необходимо иметь краткую инструкцию, что делать в случае атаки, по аналогии с планом эвакуации. Она должна быть прописана на бумаге и висеть на видном месте. В момент атаки рядом может оказаться администратор без практического опыта решения текущей проблемы, и чрезвычайно важно, чтобы у него не возникла заминка, и не было потраченного времени на поиск решения.

Тренируйтесь на учебных тревогах. *DDoS* — такая же чрезвычайная ситуация, как и пожар. Поэтому необходимо устраивать периодические проверки навыков оперативной обработки незапланированных ситуаций. Это поможет усвоить и закрепить навыки и обнаружить слабые места в процедурах.

Заранее блокируйте неиспользуемые порты. Заблаговременно заблокируйте на брандмауэре всё лишнее, что таким образом уменьшит поле для атаки. Если Вы имеете узкий круг проверенных, важных клиентов, добавьте их адреса в белый список, чтобы не отсеивать их запросы.

Определитесь с тем, где блокировать. Отсеивать ненужный трафик на брандмауэре или на маршрутизаторе? Подключать собственный аппаратный или сервис внешней фильтрации трафика? Решите эти важные вопросы заранее. Исключите метод проб и ошибок тогда, когда на него определенно нет времени.

ЛИТЕРАТУРА

1. DDoS-атаки. Причины возникновения, классификация и защита от DDoS-атак [Электронный ресурс]. URL: http://efsol.ru/articles/ddos-attacks.html
2. Флёнов М. Linux глазами хакера. - СПб.: БХВ-Петербург, 2010. - 480 с.

МОДЕЛИРОВАНИЕ АЗОТИРОВАНИЯ МЕТАЛЛОВ С УЧЕТОМ ФАЗОВЫХ ПЕРЕХОДОВ

Чан Ми Ким Ан

(г. Томск, Национальный исследовательский Томский политехнический университет)

e-mail: tranmykiman@gmail.com

MODELING OF NITRIDING INCLUDING METALLIC PHASE TRANSITIONS

Tran My Kim An

(Tomsk, National Research Tomsk Polytechnic University)

Abstract: This paper deals with ion nitriding in metallic environment including phase changes. It contains mathematical model, analytical calculation, computer simulation and analysis received results from analytic and experiments.

Key words: plasma nitriding, nitrogen concentration profile, mathematical model, diffusion, layer growth kinetic.

Введение

Одним из наиболее распространенных и эффективных методов модификации поверхности является метод азотирования. При азотировании повышаются прочность, твёрдость, износостойкость, сопротивление усталости и коррозии сталей и сплавов [1-6]. Ионно-плазменное азотирование широко применяется в промышленности, однако, из-за большого числа факторов, влияющих на окончательный результат, имеется необходимость в совершенствовании условий проведения процесса азотирования [6].