РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ДОКЛАД

на тему Провайдеры типа Cloudflare и защита от DDoS и Brute Force атак

дисциплина: Администрирование сетевых подсистем

Студент: Бакулин Никита 1032201747

Группа: НПИбд-01-20

МОСКВА

2022 г.

Содержание

Введение.....3

Виды атак.....3

DDoS атаки.....3

Brute force атаки.....4

Средства защиты.....5

Iptables.....5

Fail2ban.....5

Nginx.....6

Cloudflare.....6

О компании.....6

CDN.....6

Turnstile.....7

Anti-DDoS.....7

Настройка средств защиты.....7

Iptables.....7

Fail2ban.....8

Заключение.....9

Список литературы по теме.....9

Введение

Сетевым администраторам довольно часто приходится сталкиваться с внешними атаками со стороны злоумышленников.

Атаки бывают разных типов, различного уровня сложности, поэтому в задачи сетевого администратора входит заранее обезопасить систему от вторжения, а также в случае атаки вовремя обнаружить подозрительную активность и устранить проблему.

Защиты от сетевых атак – актуальная проблема в современном мире, существует множество популярных инструментов для противодействия им, а на рынке широко представлены решения от крупных технологических компаний.

Виды атак

DDoS атаки

Изначально DoS атака - атака злоумышленников на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых добросовестные пользователи системы не смогут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ будет 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: потеря простой службы, приносящей доход, счета от провайдера и меры по уходу от атаки ощутимо бьют по карману «цели». В настоящее время DoS и DDoS-атаки наиболее популярны, так как позволяют довести до отказа практически любую плохо написанную систему, не оставляя юридически значимых улик. [1]

Если атака выполняется одновременно с большого числа компьютеров, говорят о DDoS-атаке (Distributed Denial of Service, распределённая атака типа «отказ в обслуживании»). Такая атака проводится в том случае, если требуется вызвать отказ в обслуживании хорошо защищённой крупной компании или правительственной организации.

Злоумышленникам гораздо легче осуществить DoS-атаку на систему, чем получить полный доступ к ней. Существуют различные причины, из-за которых

может возникнуть DoS-условие, то есть такая ситуация, при которой пользователи не могут получить доступ к ресурсам, которые предоставляет сервер, либо доступ к ним существенно затруднен:

- Насыщение полосы пропускания (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
- Недостаток ресурсов (тяжелые запросы) - Атакующий посылает серверу пакеты, которые не насыщают полосу пропускания (канал обычно довольно широкий), но тратят всё его процессорное время. Процессор сервера, когда будет их обрабатывать, может не справиться со сложными вычислениями. Из-за этого произойдёт сбой, и пользователи не смогут получить доступ к необходимым ресурсам.
- Ошибки программирования (эксплойт) – использование ошибок в программном коде. Профессиональные реализаторы DoS-атак не используют такой примитивный способ атаки, как насыщение полосы пропускания. Полностью разобравшись в структуре системы жертвы, они пишут программы (эксплойты), которые помогают атаковать сложные системы коммерческих предприятий или организаций. Чаще всего это ошибки в программном коде, приводящие 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 адресу.

Также атаки разделяют по уровням модели OSI, например, если идет флуд на http – то это Layer 7 атака

Brute force атаки

Brute force атака – атака методом полного перебора, например взлом пароля путём перебора всех возможных вариантов ключа. Её особенностью является возможность применения против любого практически используемого шифра.

Однако такая возможность существует лишь теоретически, зачастую требуя нереальные временные и ресурсные затраты. Если пространство решений слишком большое, то данный вид атаки может не дать результатов в течение нескольких лет или даже веков. Наиболее оправдано использование атаки методом «грубой силы» в тех случаях, когда не удается найти слабых мест в системе шифрования, подвергаемой атаке (либо в рассматриваемой системе шифрования слабых мест не существует). При обнаружении таких недостатков разрабатываются методики криптоанализа, основанные на их особенностях, что способствует упрощению взлома. [2]

Средства защиты

Iptables

Iptables – это утилита командной строки, является стандартным интерфейсом управления работой межсетевого экрана (брандмауэра) netfilter для ядер Linux.

Функционирование фаервола определяется набором правил, каждое из которых состоит из условия и действия (например DROP или ACCEPT), применяемого к пакетам, подпадающим под это условие. Iptables при обработке отдельных пакетов использует информацию о соединениях в целом, позволяя делать выводе не только на основе заголовков пакетов [3]

Fail2ban

Fail2ban – это программа для защиты серверов от атак методом грубой силы, написанная на Python, может работать на POSIX-системах имеющих встроенный менеджер пакетов и брандмауэр.

Fail2ban считывает логи (например, /var/log/apache2/error.log) и блокирует IP-адреса, активность которых является подозрительной (например, большое количество попыток войти с неправильно введенным паролем, выполнение опасных или бессмысленных действий). В случае обнаружения подобных действий программа обновляет правила брандмауэра для блокировки такого IP-адреса на определенный промежуток времени. Программа может быть настроена и для выполнения другого действия (например, отправки электронного письма).

Конфигурация по умолчанию содержит фильтры для Apache, Lighttpd, sshd,

vsftpd, qmail, Postfix, Courier Mail Server, Asterisk и других популярных серверных приложений. В фильтрах используются регулярные выражения, которые могут быть легко изменены и настроены в случае необходимости. [4]

Nginx

Nginx - это HTTP-сервер и обратный прокси-сервер, почтовый прокси-сервер, а также TCP/UDP прокси-сервер общего назначения. Его широко используют в качестве балансировщика нагрузки, перенаправляя трафик с сервера nginx на внутренний контур.

Правильные настройки кэша позволяют снять с сервера рутинную нагрузку, разгрузить процессорные мощности и сеть для обработки целевого трафика и противостояния вредоносным DDoS-запросам.

Для защиты от DDoS (тяжелые запросы) в Nginx есть возможность выставить тайм-ауты, которые не позволят соединениям висеть слишком долго.

Cloudflare

О компании

Cloudflare — американская компания, предоставляющая услуги CDN, защиту от DDoS-атак, безопасный доступ к ресурсам и серверы DNS. Продукт Cloudflare — это глобальная сеть, предназначенная для обеспечения безопасности, конфиденциальности, быстродействия и надежности всего, что вы подключаете к Интернету.

CDN

CDN - географически распределённая сетевая инфраструктура, позволяющая оптимизировать доставку и дистрибуцию содержимого конечным пользователям в сети Интернет. Использование контент-провайдерами CDN способствует увеличению скорости загрузки интернет-пользователями аудио-, видео-, программного, игрового и других видов цифрового содержимого в точках присутствия сети CDN.

На скорость загрузки веб-страницы и её содержимого сильно влияет то, насколько далеко пользователь находится от сервера. Это происходит из-за того, что при использовании технологии TCP/IP, применяемой для распространения информации в сети Интернет, задержки при передаче информации зависят от

количества маршрутизаторов, находящихся на пути между источником и потребителем содержимого. Размещение содержимого на нескольких рассредоточенных серверах средствами CDN сокращает сетевой маршрут передачи данных и делает загрузку сайта быстрее с точки зрения пользователя.

CDN от Cloudflare позволит защититься от атак. Из-за мощности и распределённой архитектуры сама CDN устойчива к DDoS-атакам. Центральные серверы можно защитить на уровне CDN, если их адреса закрыты или засекречены. При DDoS атаке на один URL сервера Cloudflare будут возвращать кешированный ответ, не перегружая тем самым сервера приложения. [5]

Turnstile

Капча – это компьютерный тест, используемый для того, чтобы определить, кем является пользователь системы: человеком или компьютером. Одни из самых популярных решений – reCAPTCHA от Google и Turnstile от Cloudflare

Turnstile полезен при борьбе с DDoS атаками, при обнаружении однотипных запросов он позволит не перенаправлять трафик на сервера приложения, а блокировать их на серверах Cloudflare до ручного решения капчи. [6]

Anti-DDoS

Anti-DDoS – это сервис мониторинга и фильтрации трафика, защиты от DDoS-атак

CloudFlare DDoS Protection — сервис, предоставляющий услуги по защите веб-сайтов от DDoS-атак. Решение выполняет фильтрацию трафика через свои центры перед тем, как он будет направлен на сайт заказчика, позволяет защитить его данные благодаря надежной инфраструктуре CloudFlare и очень компетентной команде специалистов. [7]

Настройка средств защиты

Iptables

Iptables – одно из самых простых по настройке средств, для блокировки нужно оперировать правилами, которые задаются командами. Пример лога при блокировке запроса приведен на Рисунок 1

Пример команд:

- iptables -A INPUT -p tcp --dport 22 -m state --state NEW -m recent --name

BLOCK -set – добавляем ip в таблицу

- iptables -A INPUT -p tcp --dport 22 -m state --state NEW -m recent --name BLOCK --update --seconds 60 --rttl --hitcount 3 -j DROP – разрешаем с одного адреса до 3 запросов на соединение в минуту, блокировка применяется после третьего запроса и длится минуту.

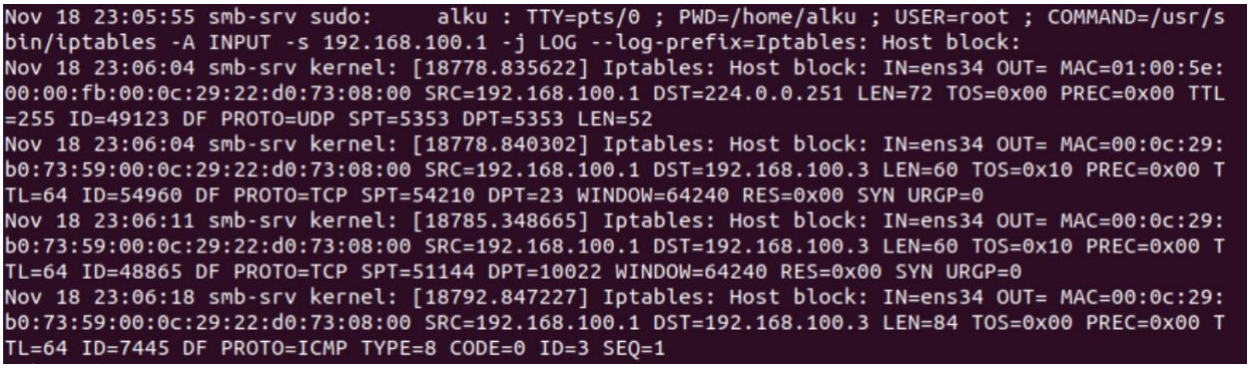

Рисунок 1 Пример лога при блокировке

Fail2ban

Настройка Fail2ban также оперирует правилами блокировки, но уже для конкретных систем

Конфигурационные файлы создаются по пути - /etc/fail2ban/jail.d/NAMEFILE.local. Примеры конфигурации правил представлены на Рисунок 2. На примерах задается время блокировки (bantime), блокировка адреса (ignoreip), включаются правила для ssh ([sshd]) на защиту от перебора пароля, apache веб сервера ([apache]) на защиту от ботов, почтового сервер ([postfix], [dovecor]) на защиту от спама

Команды:

- fail2ban-client status <JAIL> - проверить статус клиента или правила
- fail2ban-client set <JAIL> maxretry <RETRY> - задать максимальное количество нарушений правила перед блокировкой

Рисунок 2 Пример конфигурационных файлов

Заключение

Борьба с DDoS и Brute force атаками сейчас актуальна как никогда. Таким атакам могут подвергнуться как частные сервисы, так и государственные.

Для работы системного администратора по защите от таких атак существует множество утилит разного уровня сложности и степени защиты, например Iptables и Fail2ban. В борьбе с атаками также используются услуги провайдера Cloudflare – CDN, Turnstile, Anti-DDoS

Список литературы по теме

1. DoS-атака // Википедия. [2022]. Дата обновления: 17.12.2022. URL: https://ru.wikipedia.org/?curid=9722&oldid=127313491 (дата обращения:

17.12.2022).
2. Полный перебор // Википедия. [2022]. Дата обновления: 14.04.2022. URL: https://ru.wikipedia.org/?curid=360053&oldid=121425766 (дата обращения: 14.04.2022).
3. Iptables Tutorial 1.1.19 // OpenNet [2022] URL: https://www.opennet.ru/docs/RUS/iptables (дата обращения: 27.12.2022)
4. Fail2ban // Fail2ban wiki [2022] URL: https://www.fail2ban.org/wiki/index.php/Main_Page (дата обращения: 27.12.2022)
5. What is a CDN? | How do CDNs work? // Cloudflare Learning Center [2022] URL: https://www.cloudflare.com/learning/cdn/what-is-a-cdn (дата обращения: 27.12.2022)
6. Turnstile // Cloudflare Docs [2022] URL: https://developers.cloudflare.com/turnstile (дата обращения: 27.12.2022)
7. DDoS Prevention: Protecting The Origin // The Cloudflare Blog [2022] URL: https://blog.cloudflare.com/ddos-prevention-protecting-the-origin (дата обращения: 27.12.2022)