

В современном информационном обществе, где зависимость от онлайн-сервисов и цифровых платформ стала неотъемлемой частью повседневной жизни, кибербезопасность приобретает все более критическое значение. Одним из наиболее разрушительных и распространенных видов кибератак, угрожающих работоспособности онлайн-ресурсов и организаций, являются атаки типа DDoS (Distributed Denial of Service). DDoS-атаки могут вызвать серьезные последствия, включая простои в работе веб-сервисов, потерю клиентов и нанесение ущерба репутации организации.

Методическое пособие «Путешествие по галактике DDoS: секреты кибербезопасности, или Методы и стратегии обороны от DDoS-атак» создано с целью предоставить заинтересованным лицам полное и всестороннее руководство по глубокому пониманию сути DDoS-атак и их обнаружению, а также предложит надежные методы и стратегии для защиты от таковых: от базовых концепций до продвинутых техник мониторинга и реагирования.

Настоящее пособие позволит организациям быть готовыми к вызовам, которые могут спровоцировать DDoS-атаки, и обеспечить непрерывную и надежную работу онлайн-ресурсов.

Важно понимать, что кибербезопасность – это постоянное противостояние между нападением и защитой, и это пособие является вашим надежным путеводителем в одном из аспектов такого противостояния. Будучи предназначенным для широкого круга читателей, включая специалистов по ИБ и ИТ, бизнес-руководителей, аспирантов и студентов профильных специальностей, оно объединяет лучшие практики и актуальные методы обеспечения надежной защиты вашей организации от этой серьезной киберугрозы.

Введение

Глава 1. Понимание сути DDoS-атак

- 1.1. Цели и мотивы DDoS-атак
- 1.2. Хактивизм и DDoS-атаки
- 1.3. Типы DDoS-атак
 - 1.3.1. Атаки на уровне сети (Network Layer Attacks)
 - 1.3.2. Атаки на сетевое оборудование (Infrastructure Layer Attacks)
 - 1.3.3. Атаки на прикладной уровень (Application Layer Attacks)
- 1.4. Последствия DDoS-атак
 - 1.4.1. Технические последствия DDoS-атак
 - 1.4.2. Финансовые последствия DDoS-атак
 - 1.4.3. Репутационные последствия DDoS-атак
 - 1.4.4. Правовые последствия DDoS-атак

Глава 2. Подготовка к защите от DDoS-атак

- 2.1. Оценка рисков
- 2.2. Выбор правильных инструментов
- 2.3. Разработка стратегии

Глава 3. Основные методы защиты от DDoS-атак

- 3.1. Фильтрация трафика на транспортном уровне
- 3.2. Фильтрация трафика на уровне приложения
- 3.3. Защита от ботов
 - 3.3.1. Методы атак ботов на веб-приложения
 - 3.3.2. Методы и подходы, которые используются для борьбы с ботами
- 3.4. Использование WAF
 - 3.4.1. Подходы к защите от DDoS-атак
 - 3.4.2. Подходы к защите от ботов
 - 3.4.3. Подходы в защите от взлома на основе WAF
- 3.5. Использование Content Delivery Network (CDN)
 - 3.5.1. Использование CDN для защиты от DDoS-атак
 - 3.5.2. Использование CDN для защиты от ботов

- Глава 4. Системы мониторинга и обнаружения DDoS-атак**
 - 4.1. Моделирование DDoS-атак
 - 4.2. Компоненты систем мониторинга и обнаружения DDoS-атак
 - 4.3. Методы обнаружения DDoS-атак
 - 4.4. Типичные признаки DDoS-атак
 - 4.5. Действия при обнаружении DDoS-атаки
- Глава 5. Использование облачных решений для защиты от DDoS-атак**
 - 5.1. Преимущества облачных DDoS-защитных услуг
 - 5.2. Выбор подходящего облачного поставщика
 - 5.3. Настройка и мониторинг облачной защиты
 - 5.3.1. Настройка облачной защиты от DDoS-атак
 - 5.3.2. Мониторинг облачной защиты от DDoS-атак
- Глава 6. Примеры успешных кейсов**
 - 6.1. Реальные DDoS-атаки как исследовательский материал для организации защиты
 - 6.2. Практические случаи защиты от DDoS-атак
 - 6.2.1. Пример №1: правительственный центр обработки данных (ЦОД)
 - 6.2.2. Пример № 2: служба онлайн-бронирования авиабилетов
 - 6.2.3. Пример № 3: агрегатор электронной рассылки
 - 6.2.4. Пример № 4: крупное онлайн-СМИ
 - 6.2.5. Пример № 5: компания космической отрасли
 - 6.2.6. Пример № 6: международная компания электронной коммерции
 - 6.2.7. Пример № 7: оператор связи
 - 6.2.8. Пример № 8: энциклопедия «Руниверсалис»
 - 6.2.9. Пример № 9: крупный российский федеральный банк
 - 6.2.10. Пример № 10: Кубок России по СТФ
 - 6.3. Десять реальных международных кейсов DDoS-атак на компании из разных сфер деятельности
 - 6.4. Уроки, извлеченные из успешных примеров
- Глава 7. Советы по управлению кризисными ситуациями**
 - 7.1. Стратегии управления кризисными ситуациями при DDoS-атаках
 - 7.2. Моделирование нагрузки и ресурсов
 - 7.3. Реагирование на DDoS-атаку
 - 7.4. Сбор и анализ данных после DDoS-атаки
 - 7.5. Разработка плана действий
 - 7.6. Приоритеты действий при DDoS-атаках
 - 7.7. Взаимодействие с провайдерами
 - 7.8. Соблюдение законодательства и взаимодействие с органами правопорядка
 - 7.9. Восстановление после атаки
- Глава 8. Будущее защиты от DDoS-атак**
 - 8.1. Новые технологии и DDoS-атаки
 - 8.2. Тенденции в развитии DDoS-атак
 - 8.2.1. DDoS-атаки на уровне приложения
 - 8.2.2. Целенаправленные атаки на DNS-серверы компаний
 - 8.2.3. Увеличение объемов ботнет-атак
 - 8.2.4. Возрастание продолжительности и мощности DDoS-атак
 - 8.2.5. Использование облачных ЦОДов для организации и монитизации DDoS-атак
 - 8.2.6. Атаки на целые подсети
 - 8.3. Новые методы и технологии защиты

Заключение