Лабораторная работа. Изучение угроз сетевой безопасности

Задачи

Часть 1. Изучение веб-сайта SANS

Часть 2. Определение новых угроз безопасности сети

Часть 3. Подробное описание отдельной угрозы безопасности сети

Общие сведения/сценарий

Чтобы защитить сеть от атак, администратор должен определить, какие внешние угрозы представляют опасность для сети. Для определения возникающих угроз и способов их устранения можно пользоваться специализированными веб-сайтами.

Одним из наиболее известных и проверенных ресурсов для защиты компьютера и сети является веб-сайт института SANS (Институт системного администрирования, сетей и безопасности). На веб-сайте SANS доступны несколько разных ресурсов, включая список 20 основных средств контроля безопасности для эффективной киберзащиты и еженедельную новостную рассылку по вопросам безопасности @Risk: The Consensus Security Alert. В рассылке подробно рассказывается о новых сетевых атаках и уязвимостях.

В этой лабораторной работе вам необходимо открыть и изучить веб-сайт SANS, определить новые угрозы сетевой безопасности с его помощью, посетить другие аналогичные веб-ресурсы и подготовить подробное описание отдельной сетевой атаки.

Необходимые ресурсы

- Устройство с доступом в Интернет
- Компьютер для презентации с установленной программой PowerPoint или другой программой для презентаций.

Часть 1: Изучение веб-сайта SANS

В части 1 вам нужно открыть веб-сайт SANS и изучить доступные ресурсы.

Шаг 1: Найдите ресурсы SANS.

Перейдите по ссылке www.SANS.org. На главной странице наведите указатель мыши на меню **Resources** (Ресурсы).

Назовите три доступных ресурса.

Webcasts, Free Cybersecurity Events, Focus Areas

Шаг 2: Найдите основные средства контроля безопасности.

Список **основных средств контроля безопасности** на веб-сайте SANS был составлен в результате совместной работы государственных и частных компаний при участии Министерства обороны, Ассоциации национальной безопасности, Центра интернет-безопасности и Института SANS. Его задачей было определить приоритетность средств контроля кибербезопасности и связанных с ними расходов для Министерства обороны. На основе этого списка правительство США разработало эффективные программы обеспечения безопасности. В меню **Resources** (Ресурсы) выберите пункт **Critical Security Controls** (Основные средства контроля безопасности) (название может отличаться).

Выберите одно из средств контроля и назовите три предложения по его реализации.

Превентивное средство контроля безопасности:
Аутентификация пользователей
Сегментация сети
Проведение аудитов безопасности

Шаг 3: Выберите меню Newsletters (Новостные рассылки).

Откройте меню **Resources** (Ресурсы) и выберите пункт **Newsletters** (Новостные рассылки). Кратко опишите каждую из трех предлагаемых рассылок.

NewsBites - полуеженедельник, содержащий информацию о самых важных новостях в сфере кибербезопасности, которые были недавно опубликованы, с комментариями от экспертов общества сайта SANS

@RISK - еженедельный сборник обнаруженных атак и уязвимостей с эксплоитами, объяснением работы атак, и прочими данными

OUCH! Newsletter - бесплатные рассылки, предназначенные для увеличения осведомлённости о безопасности, публикуются каждый месяц на нескольких языках

Часть 2: Определение новых угроз безопасности сети

В части 2 вам нужно изучить новые угрозы сетевой безопасности, пользуясь веб-сайтом SANS, и узнать, на каких других сайтах можно найти информацию по этой теме.

Шаг 1: Выберите раздел Archive (Архив) новостной рассылки @Risk: Consensus Security Alert.

Откройте страницу **Newsletters** (Новостные рассылки) и выберите раздел **Archive** (Архив) рассылки @Risk: Consensus Security Alert. Прокрутите страницу вниз до раздела **Archives Volumes** (Тома архива) и выберите последний выпуск еженедельной новостной рассылки. Ознакомьтесь с информацией в разделах **Notable Recent Security Issues (Последние важные проблемы безопасности) и Most Popular Malware Files** (Наиболее распространённые файлы вредоносных программ).

Назовите некоторые из последних атак. При необходимости просмотрите несколько последних выпусков рассылки.

DNS Reflection Update and Odd Corrupted DNS Requests
Fake GitHub Site Targeting Developers
Phishing links with @ sign and the need for effective security awareness building

Шаг 2: Найдите веб-сайты, которые содержат информацию о новых угрозах безопасности.

Выясните, на каких еще сайтах, помимо SANS, можно ознакомиться с информацией о новых угрозах сетевой безопасности.

CVE, OWASP, Threatpost, Malwarebytes Labs, Kaspersky

Назовите некоторые новые угрозы безопасности, подробно описанные на этих веб-сайтах.

Walmart customers scammed via fake shopping lists, threatened with arrest
Malicious Npm Packages Tapped Again to Target Discord Users

Часть 3: Подробное описание отдельной угрозы безопасности сети

В части 3 вы займетесь изучением отдельной сетевой атаки, а затем на основе полученной информации подготовите презентацию. Используя полученные результаты, заполните приведенную ниже форму.

Шаг 1: Заполните приведенную ниже форму для выбранной сетевой атаки.

Имя атаки:	DDoS
Тип атаки:	Denial of Service
Даты атак:	2018, 2020, 2021
Пострадавшие компьютеры или организации:	Github, Amazon Web Services, Яндекс
Механизм атаки и ее последствия:	
DDoS-атака осуществляется путем одновременного отправления огромного количества запросов на сервер с множества зараженных устройств (ботнет), что приводит к перегрузке сервера. Последствия могут включать временные простои, финансовые потери, ущерб репутации.	
Способы устранения:	
Использование систем защиты от DDoS-атак (Cloudflare, Akamai). Настройка фильтрации трафика. Увеличение пропускной способности сети.	
Источники и ссылки на информационные ресурсы:	
CISA - DDoS Attacks (https://www.cisa.gov/), Cloudflare - What is a DDoS Attack?(https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/)	

Шаг 2: Следуйте указаниям инструктора и закончите презентацию.

Вопросы для повторения

1. Какие меры можно предпринять для защиты собственного компьютера?

   Постоянное обновление ПО, установка антивируса, включенный сетевой экран, делать бэкапы, ставить сложные пароли на профиль админа, настроить блокировку экрана по паролю, не скачивать пиратское ПО

2. Какие важные меры могут предпринимать компании для защиты своих ресурсов?

   Физический контроль доступа (турникеты, камеры и пр.), фильтрование трафика, обучение сотрудников, проведение аудитов безопасности, разрабатывать планы реагирования на потенциальные инциденты