

Лабораторная работа. Изучение угроз безопасности сети

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 к Интернету
- Компьютер для презентации с установленной программой PowerPoint или другой программой для презентаций.

Инструкции

Часть 1. Изучение веб-сайта SANS

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

Шаг 1. Найдите ресурсы SANS.

Задайте поиск в Интернете - SANS. На домашней странице SANS нажмите на **БЕСПЛАТНЫЕ ресурсы**.

Назовите три доступных ресурса. Reading Room, Webcasts, Newsletters, Blogs, Top 25 Software Errors, 20 Critical Controls, Security Policies

Шаг 2. Найдите ссылку на CIS основные средства контроля безопасности.

Список **CIS 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). Документ CIS Critical Security Controls размещается на веб-сайте Центра безопасности в Интернете (CIS) и требует бесплатной регистрации для доступа. На странице «Контроли безопасности CIS» в сети SANS имеется ссылка для загрузки информации «Критические средства управления безопасностью SANS 2014», в котором содержится краткое описание каждого элемента управления.

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

Шаг 3. Выберите меню **Newsletters** (Новостные рассылки).

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

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).

Перечислите некоторые недавние уязвимости. При необходимости просмотрите несколько последних выпусков рассылки.

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.

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

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:	WannaCry ransomware
Тип атаки:	Крипточервь
Даты атак:	июль 2001 г. май 2017 г.
Пострадавшие компьютеры или организации:	Приблизительно 200 000 компьютеров в 150 странах.
Механизм атаки и ее последствия:	
Способы устранения:	
Примените исправления, выпущенные Microsoft для операционной системы Windows.	
Источники и ссылки на информационные ресурсы:	
Wikipedia CSO Online	

Шаг 2. Следуйте указаниям инструктора и закончите презентацию .

Вопросы для повторения

1. Какие меры можно предпринять для защиты собственного компьютера?
2. Какие важные меры могут предпринимать компании для защиты своих ресурсов?