Lab - Research Network Security Threats

# Цели

Часть 1: Изучите веб-сайт SANS

Часть 2: Выявление недавних угроз безопасности сети

Часть 3: Подробное описание конкретной угрозы безопасности сети

# Предыстория/Сценарий

Чтобы защитить сеть от атак, администратор должен определить внешние угрозы, которые представляют опасность для сети. Веб-сайты безопасности могут использоваться для определения возникающих угроз и предоставления вариантов смягчения для защиты сети.

Один из самых популярных и надежных сайтов для защиты от угроз компьютерной и сетевой безопасности — SysAdmin , Audit, Network, Security (SANS). Сайт SANS предоставляет множество ресурсов, включая список 20 лучших критических элементов управления безопасностью для эффективной киберзащиты и еженедельный бюллетень @Risk: The Consensus Security Alert. В этом бюллетене подробно описываются новые сетевые атаки и уязвимости.

В этой лабораторной работе вы перейдете на сайт SANS и изучите его, воспользуетесь сайтом SANS для выявления недавних угроз безопасности сети, изучите другие веб-сайты, выявляющие угрозы, а также изучите и представите сведения о конкретной сетевой атаке.

# Требуемые ресурсы

* Устройство с доступом в Интернет
* Презентационный компьютер с установленным PowerPoint или другим программным обеспечением для презентаций

# Инструкции

## Изучение веб-сайта SANS

В Части 1 перейдите на сайт SANS и изучите доступные ресурсы.

### Найдите ресурсы SANS.

Поищите в интернете SANS. На домашней странице SANS нажмите на БЕСПЛАТНЫЕ **ресурсы** .

#### Вопрос:

Перечислите три доступных ресурса.

Введите свои ответы здесь.

### Найдите ссылку на критические меры безопасности CIS.

Критические **элементы управления безопасностью CIS** , ссылки на которые размещены на сайте SANS, являются кульминацией государственно-частного партнерства с участием Министерства обороны (DoD), Ассоциации национальной безопасности, Центра интернет-безопасности (CIS) и Института SANS. Список был разработан для определения приоритетов элементов управления кибербезопасностью и расходов для DoD. Он стал центральным элементом эффективных программ безопасности для правительства США. В меню « **Ресурсы»** выберите **«Критические элементы управления безопасностью»** или аналогичный. Документ «Критические элементы управления безопасностью CIS» размещен на сайте Центра интернет-безопасности (CIS) и требует бесплатной регистрации для доступа. На странице «Контроль безопасности CIS» на сайте SANS есть ссылка для загрузки плаката «Критические элементы управления безопасностью SANS 2014», в котором дается краткое описание каждого элемента управления.

#### Вопрос:

Выберите один из элементов управления и перечислите предложения по реализации этого элемента управления.

Введите свои ответы здесь.

### Найдите меню «Информационные бюллетени».

#### Вопрос:

Выделите меню **Ресурсы** , выберите **Информационные бюллетени** . Кратко опишите каждый из трех доступных информационных бюллетеней.

Введите свои ответы здесь.

## Определите недавние угрозы сетевой безопасности

В части 2 вы изучите последние угрозы сетевой безопасности с помощью сайта SANS и определите другие сайты, содержащие информацию об угрозах безопасности.

### Найдите архив бюллетеня @Risk: Consensus Security Alert.

На странице **Newsletters** выберите **Archive** для @RISK: The Consensus Security Alert. Прокрутите вниз до **Archives Volumes** и выберите последний еженедельный информационный бюллетень. Просмотрите разделы **Notable Recent Security Issues и Most Popular Malware Files** .

#### Вопрос:

Перечислите некоторые недавние уязвимости. Просмотрите несколько последних информационных бюллетеней, если необходимо.

Введите свои ответы здесь.

### Определите сайты, предоставляющие актуальную информацию об угрозах безопасности.

#### Вопросы:

Помимо сайта SANS, найдите еще несколько веб-сайтов, которые предоставляют последнюю информацию об угрозах безопасности.

Введите свои ответы здесь.

Перечислите некоторые из недавних угроз безопасности, подробно описанных на этих веб-сайтах.

Введите свои ответы здесь.

## Подробно опишите конкретную атаку на безопасность сети

В Части 3 вы исследуете конкретную сетевую атаку, которая произошла, и создадите презентацию на основе ваших выводов. Заполните форму ниже на основе ваших выводов.

### Заполните следующую форму для выбранной сетевой атаки.

|  |  |  |  |
| --- | --- | --- | --- |
| Название атаки | Тип атаки | Даты нападений | Компьютеры / Организации, пострадавшие |
| Пустой | пустой | пустой | пустой |
| Как это работает и что сделано: | | | |
| Пустой | | | |
| **Варианты смягчения последствий:** | | | |
| Пустой | | | |
| **Ссылки на источники и информацию:** | | | |
| Пустой | | | |

Пустая строка, нет дополнительной информации

Пустая строка, нет дополнительной информации

### Следуйте указаниям преподавателя, чтобы завершить презентацию.

# Вопросы для размышления

* 1. Какие шаги вы можете предпринять, чтобы защитить свой компьютер?

Введите свои ответы здесь.

* 1. Какие важные шаги могут предпринять организации для защиты своих ресурсов?

Введите свои ответы здесь.

Конец документа