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.

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

© © 2013 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

www.netacad.com

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.

SANS NewsBites – это аннотированный, выходящий два раза в неделю краткий обзор самых последних и важных новостей в сфере кибербезопасности.

@RISK предоставляет надежную еженедельную сводку о недавно обнаруженных векторах атак, уязвимостях с активными новыми эксплойтами, подробные объяснения того, как работали недавние атаки, и другие ценные данные.

OUCH! – это ведущая в мире ежемесячная рассылка новостей по безопасности, предназначенная для обычных пользователей компьютеров. Как всегда, переведено на более чем 25 языков и бесплатно для сообщества.

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.

Злоумышленники всегда пытаются найти новые способы доставки вредоносного ПО жертвам. Недавно они начали отправлять файлы Microsoft OneNote в ходе масштабных фишинговых кампаний[1]. Файлы OneNote (с расширением, заканчивающимся на «.one») автоматически обрабатываются компьютерами, на которых установлен пакет Microsoft Office. Вчера мой honeypot поймал первый образец. Это хорошая возможность взглянуть на эти файлы. Файл под названием «delivery-note.one» был доставлен в виде вложения к классическому фишинговому письму.

Ретрансляция NTLM уже много лет является проблемой в средах Windows, и мы стали свидетелями множества эксплойтов, основанных на возможности ретрансляции попыток аутентификации NTLM различным целевым службам.Хотя здесь есть много потенциальных целей, в большинстве случаев Red

© © 2013 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco
www.netacad.com

Team я и мои коллеги передаем учетные данные другим службам SMB, LDAP или HTTP(S) (особенно на сервере AD CS, используемом для выдачи сертификатов). Поэтому одним из обязательных действий по «проверке работоспособности» должно быть подтверждение того, действительно ли в ваших системах включена подпись. Вот два *очень простых* способа, как я это делаю, когда сталкиваюсь с большим количеством внутренних активов.

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.

https://www.kaspersky.ru/resource-center/preemptive-safety/cyber-security-trends

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

1. Риски кибербезопасности при удаленной работе

2. Развитие интернета вещей

3. Рост количества программ-вымогателей

4. Совершенствование многофакторной аутентификации

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.

© © 2013 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

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

Имя атаки:	**DDoS**
Тип атаки:	DDoS
Даты атак:	2 ноября 2024 года
Пострадавшие компьютеры или организации:	новосибирский интернет-провайдер «Сибсети»
Механизм атаки и ее последствия:	
Зафиксирована хакерская атака на инфраструктуру компании — злоумышленники направляют на наши сервисы и сайты огромное количество запросов. Серверы не выдерживают нагрузки и перестают отвечать. .Компании пришлось приостановить работу	
Способы устранения:	
Блокировка IP-адресов атакующих	
Источники и ссылки на информационные ресурсы:	
URL	

Шаг 2. Следуйте указаниям инструктора и закончите презентацию .

Вопросы для повторения

1. Какие меры можно предпринять для защиты собственного компьютера?

   Не скачивать подозрительные сайты, не посещать подозрительные сайты

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

   Совершенствовать безопасность своих систем. Делать их более отказоустойчивыми

© © 2013 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

www.netacad.com