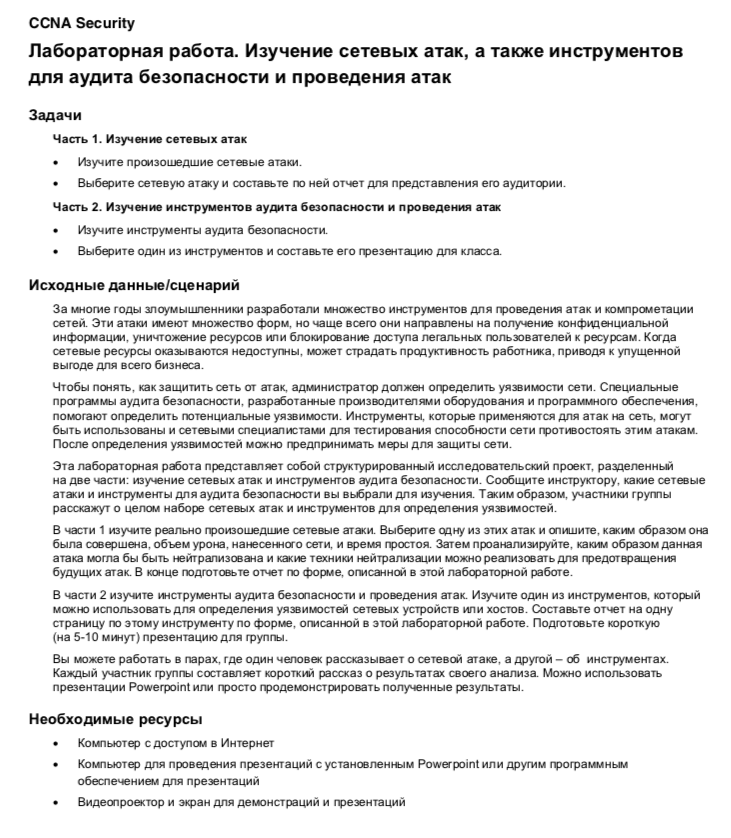
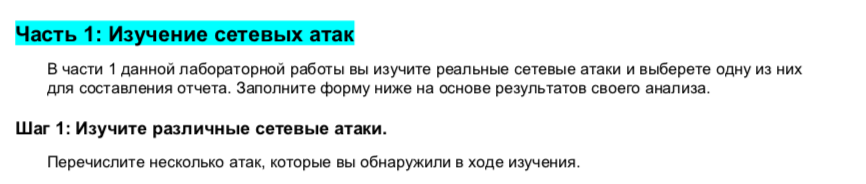
Выхор Александра 303-Кб



1. Stuxnet
2. Ashley Madison
3. взлом Yahoo
4. DDOS против Dyn
5. Melissa
6. база данных Sony PlayStation
7. взлом eBay



**Название атаки:** Ashley Madison

**Тип Атаки:** Сниффинг пакетов - основанный на работе сетевой карты в режиме promiscuous mode («неразборчивый» режим, в котором сетевая плата позволяет принимать все пакеты независимо от того, кому они адресованы). В таком режиме все пакеты, полученные сетевой картой, пересылаются на обработку специальному приложению. В результате злоумышленник может получить большое количество служебной информации: кто, откуда и куда передавал пакеты, через какие адреса эти пакеты проходили.

**Даты проведения атак:** Август 2015

**Пострадавшие компьютеры/ организации:** 40 млн пользователей по всему миру

**Принцип действия и результаты:**

**Ashley Madison** – канадский онлайн-сервис для свиданий, ориентированный на людей, состоящих в браке, был запущен в 2002 году. Хакерская группа, называющая себя The Impact Team, взломала серверы Ashley Madison, клиентские базы, данные кредитных карт пользователей, а также внутренние конфиденциальные документы канадской компании Avid Life Media, которой принадлежат сайты знакомств AshleyMadison, Cougar Life и Established Men.

Вскоре после этого, данные о пользователях стали “всплывать” на различных сайтах и форумах по всему интернету. В начале августа хакеры опубликовали в Сети 10 ГБ данных, скомпрометированных в ходе кибератаки. Сложно подсчитать количество разводов, спровоцированных этими утечками. Что важнее, в некоторых случаях люди кончали жизнь самоубийством после того, как данные об их аккаунте и переписка становились достоянием гласности. Таких случаев было не менее десятка.

Во время атаки взломщики также выяснили, что в Ashley Madison обманывали своих клиентов. На сайте действовал сервис по полному удалению данных за 19 долларов, однако компания продолжала хранить информацию даже после такого «стирания».

**Варианты нейтрализации:** исправить и усовершенствовать следующие проблемы: хранение в исходном коде учетных данных Twitter OAuth, закрытого ключа SSL-сертификата и различные проблемно-ориентированные токены.

Настоятельно рекомендуется всем операторам сайтов более серьезно относиться к проверке исходного кода.

Изменение исходного кода ресурса Ashley Madison, который содержал токены AWS, базу данных учетных записей, сертифицированные закрытые ключи и другую персональную информацию

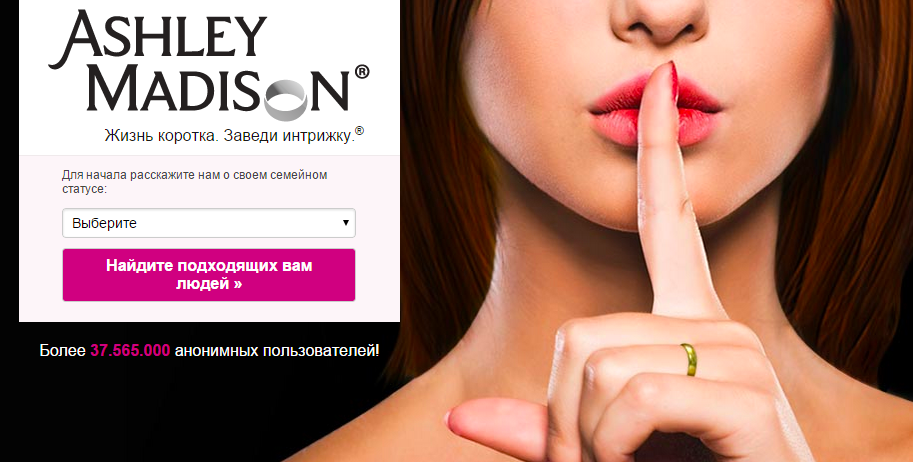
**Справочные данные и ссылки:** в ходе работы использовались следующие ссылки:

1. https://www.securitylab.ru/news/474603.php
2. https://tjournal.ru/tech/55965-ashley-madison-dump
3. https://nv.ua/techno/gadgets/apokalipsis-v-seti-7-krupnejshih-hakerskih-atak-v-istorii-1393066.html
4. https://3dnews.ru/1009634/10-samih-vpechatlyayushchih-kiberatak-v-istorii

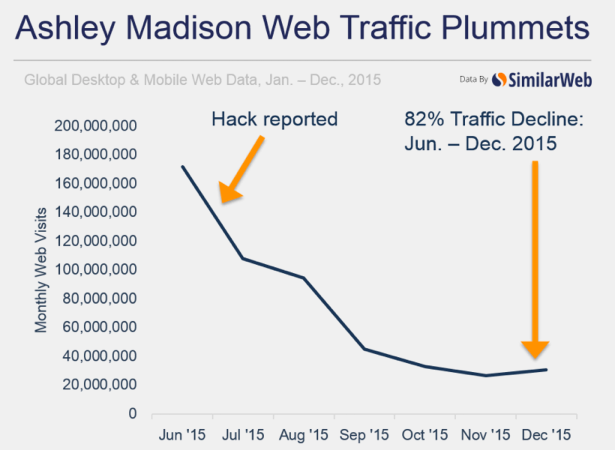
**Графики и иллюстрации (включают ссылки на файл PowerPoint или веб-сайты):**

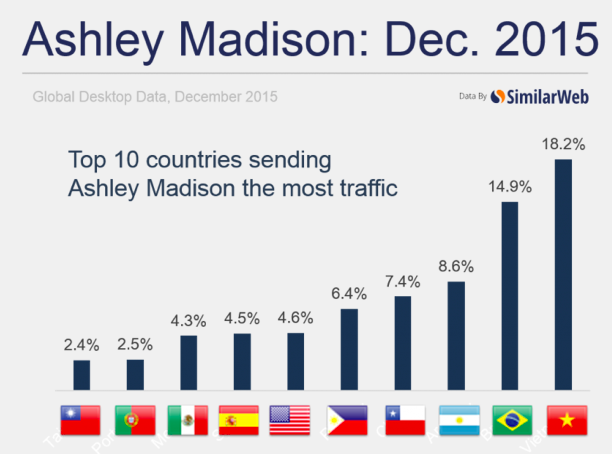
Главная страница:

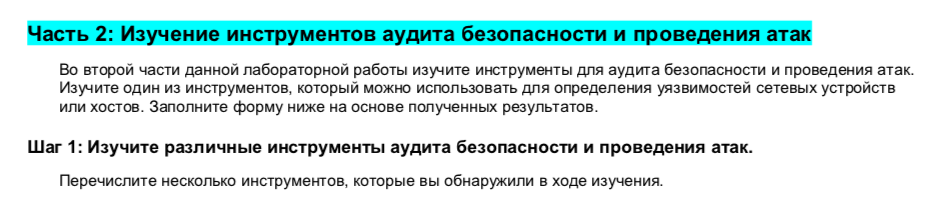




Отчет о посещаемости сайта после взлома:







Для Windows:

1. ADManager Plus (ManageEngine)
2. MBSA — Microsoft Baseline Security Analyzer
3. SekChek Security Auditing

Для Linux:

1. Lynis — auditing system hardening testing
2. Lunar — a UNIX security auditing tool
3. Nix Auditor — a CIS Audit made easier

Для MacOS:

1. Lynis
2. Nmap (Network Mapper)
3. WireShark
4. oclHashcat



**Наименование инструмента:** Lynis

**Разработчик:** Michael Boelen

**Тип инструмента (с интерфейсом или символьно-ориентированный):** с интерфейсом

**Место использования (сетевое устройство или компьютер):** компьютер

**Стоимость:** free

**Описание ключевых особенностей и возможностей продукта или инструмента:**

**Lynis** - это инструмент аудита безопасности с открытым исходным кодом.

Его **основная задача** - аудирование и упрочнение систем на базе Unix и Linux. Он сканирует систему, выполняя многие проверки контроля безопасности. Примеры включают поиск установленного программного обеспечения и определение возможных недостатков конфигурации.

Как только lynis начинает сканировать вашу систему, он выполнит проверку в следующих категориях:

Системные инструменты: системные двоичные файлы

Загрузка и службы: загрузчики, службы запуска

Ядро: уровень запуска, загруженные модули, конфигурация ядра, дампы ядра

Память и процессы: процессы-зомби, процессы ожидания ввода-вывода

Пользователи, группы и аутентификация: идентификаторы групп, sudoers, конфигурация PAM, старение паролей, маска по умолчанию

Файловые системы: точки монтирования, / tmp-файлы, корневая файловая система

Хранилища: usb-хранилище, firewire ohci

Программное обеспечение: службы имен: домен DNS-поиска, BIND

Порты и пакеты: уязвимые/обновляемые пакеты, репозиторий безопасности

Сеть: имена серверов, смешанные интерфейсы, соединения

Принтеры и спулы: cups конфигурации

Программное обеспечение: электронная почта и обмен сообщениями

Программное обеспечение: брандмауэры: iptables, pf

Программное обеспечение: веб-сервер: Apache, nginx

SSH поддержка: SSH конфигурации

SNMP поддержка

Базы данных: MySQL root пароль

LDAP службы

Программное обеспечение: php: php опции

Ненадежные службы: inetd

Баннеры и идентификация

Назначенные задания: crontab/cronjob, atd

Учет: sysstat data, auditd

Время и синхронизация: ntp демон

Криптография: Срок действия сертификата SSL

Виртуализация

Фреймворки безопасности: AppArmor, SELinux, статус безопасности

Программное обеспечение: целостность файла

Программное обеспечение: сканеры вредоносных программ

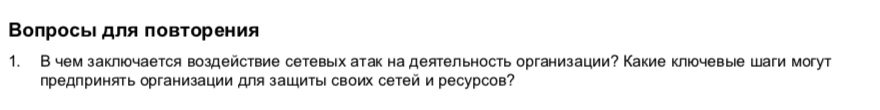
Домашние директории: файлы истории shell

Lynis совместим со многими операционными системами (>18)

Данный инструмент отлично подойдет для специалистов в сфере безопасности, тестировщиков на проникновение, системных аудиторов, системных/ сетевых менеджеров, инженеров по безопасности.

**Справочные данные и ссылки:**

1. https://xakep.ru/2018/10/15/linux-hardening/
2. https://codeby.net/threads/lynis-instrument-dlja-proverki-bezopasnosti-i-provedenija-pentesta-s-otkrytym-isxodnym-kodom-detalnoe-razjasnenie.64501/
3. https://itsecforu.ru/2019/06/03/💻-как-укрепить-безопасность-своих-си/
4. https://spy-soft.net/linux-hardening-tools/



Воздействие: получение доступа к информации, нарушить политику безопасности, нарушить работоспособность, изменить настройки конфигурации, хищение личностных данных, хищение финансовой информации

Ключевые шаги для предотвращения:

Не подключать незнакомые различные устройства к своему компьютеру. На них может храниться вирус или другая вредоносная программа.

Использование более сложных паролей

Использование лицензированных антивирусных программ

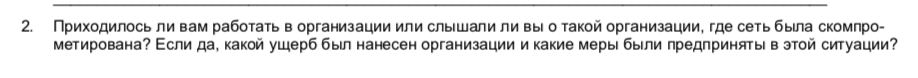
Не оставлять свои устройства без присмотра

Всегда выключать устройства, когда нужно отойти от рабочего места

Не раскрывать информацию компании и личную незнакомым и не проверенным людям

Делать регулярные технические и физические проверки

Настроить резервное копирование



Скомпрометированная сеть в Sony в сети Playstation принесла убытки в сотни тысяч долларов и в несколько миллионов в виде упущенной прибыли.



1. Установка лицензионного ПО
2. Установка лицензионного антивирусного ПО
3. Не подключаться к непроверенным сетям и USB-устройствам
4. Устанавливать надежные пароли и регулярно их менять
5. Не оставлять свои личные данные на непроверенных сайтах