Certified Hacking Forensic Investigator

Сертификация EC-Council

Private Eyes for the Digital Age

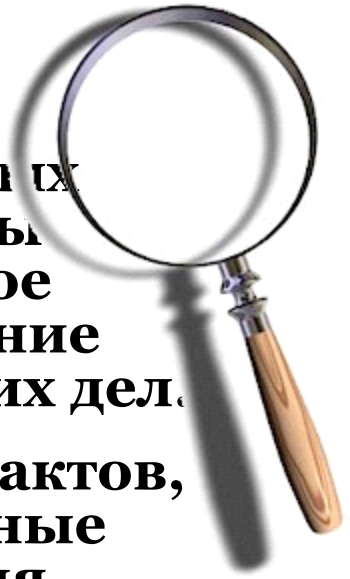
Где-то в Ванкувере...

Стив Роббинс ждет окончания дня, когда, наконец его цель будет достигнута. Когда наступит ночь, Стив и его коллеги пойдут в офис клиента, где главный финансовый директор будет ждать их, чтобы впустить. Оказавшись внутри, команда вскроет несколько стационарных компьютеров, чтобы вытащить жесткие диски и копировать их содержимое на портативные компьютеры. Это не фантастика ... это реальность в эпоху современных цифровых технологий. Стив позже представит свои находки о корпоративном шпионаже в суде и поможет выиграть иск.

Что еще важнее, Стив поможет клиенту в эффективном восстановлении и поможет призвать преступника к ответственности

Добро пожаловать в эпоху цифровых технологий

- **Почему Forensics?**
  - **Достижения в области науки и компьютерных технологий привели к тому, что компьютеры используются во всех областях и техническое расследование приобрело решающее значение для доказательства уголовных и гражданских дел.**
  - **Традиционно источником информации и фактов, касающихся конкретного дела были бумажные документы. Теперь цифровые расследования становятся важнейшим звеном в раскрытии дела и доказательства совершенного преступления.**
  - **В связи с повсеместной задействованностью компьютеров в общении и бизнес-процессах, компьютерная экспертиза стала дисциплиной, которую компании не могут позволить себе игнорировать.**



Оставьте это сыщикам…

- **Почему вас должна интересовать подобная экспертиза?**

  По опросам ИМП / ФБР, кражи конфиденциальной информации и финансовое мошенничество составили ущерб в $ 244 200 000 - сообщается в исследовании 2003 - эта цифра была почти равна общей сумме потерь, перечисленных в этих категориях за предыдущие три года вместе взятые.

- **Нечестные и недовольные сотрудники - это 80% наиболее вероятного источника атаки. 91% сказали, что заметили за инсайдерами злоупотребления при доступе в сеть в течение прошлого года, такие как загрузка порнографии и пиратского программного обеспечения или некорректное использование корпоративных систем электронной почты.**

Подумайте об этом

Готовы ли вы предоставить спасение информации сыщикам, после того как преступление уже совершено?

Какова возможная цена ущерба и какие потери вы способны терпеть, чтобы остаться на плаву?

Дело Роберта Филиппа Ханссена

- Агент Роберт Филипп Ханссен, обвиняется передаче Российским разведчикам строго засекреченных документов и разглашении сведений об американских информационных источниках и электронных операциях за 15-летний период.
- Называя его худшим случаем инсайдерского шпионажа в истории бюро, директор ФБР Луис Фри сказал: «доверенный инсайдер предал его доверие незаметно.»
- ФБР и эксперты в области ИТ безопасности преподносят дело, как суровый урок о растущей угрозе инсайдеров корпоративным данным.

Дело Роберта Филиппа Ханссена

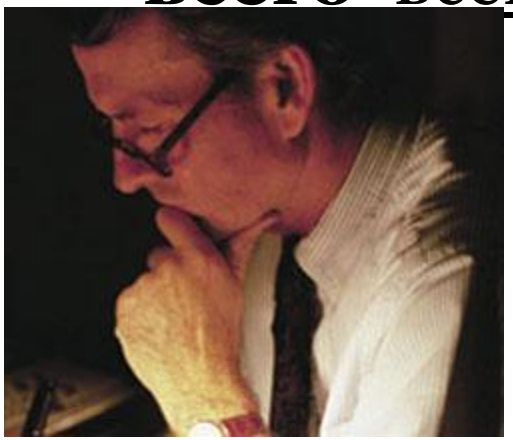
- Он широко использовал компьютерные носители, такие как зашифрованные дискеты, сменные носители и карманный компьютер Palm II, чтобы общаться с русскими офицерами разведки.
- Он передал по крайней мере 26 зашифрованных дискет во время своей шпионской деятельности.
- Это доказывает, что то, что происходит внутри рамок межсетевого экрана, может быть еще более разрушительным из-за степени доступа инсайдеров.

Специалисты утверждают...

- "Самым важным уроком, который следует извлечь из этого случая, является то, что большинство нарушений безопасности вызывают инсайдеры, не аутсайдеры", - сказал Ричард Хантер, аналитик по вопросам безопасности в Stamford, Conn.-based Gartner Group Inc.
- "Этот инцидент не связан с киберпреступностью или взломе как таковыми, но исторически, подавляющее большинство киберпреступлений совершаются инсайдерами", - сказал Хантер, бывший аналитик Агентства национальной безопасности.
- "Поскольку компании несут всё большие потери, мы начинаем представлять себе, как преступление будет выглядеть в веке информационных технологий", сказал Ричард Пауэр - директор редакции опросов ИМП / ФБР

Статистика не лжёт…

- **ИМП/ФБР утверждают, что группа всего 34 респондентов сообщили о более чем $ 151 млн. потерь от краж проприетарных данных, а в среднем $4.5 миллиона на компанию. И** $92.9 миллиона **финансовых потерь вызвали всего** всего 21 **респондент.**



Вам следует задать вопрос:

“Можете ли вы сделать что-либо для подтверждения своих подозрений, опираясь только на своё шестое чувство?”

Куда вы хотите отправиться сегодня?

- 91% респондентов сказали, что заметили за инсайдерами злоупотребления при доступе в сеть в течение прошлого года, такие как загрузка порнографии и пиратского программного обеспечения или некорректное использование корпоративных систем электронной почты.
- Хотя 38% компаний, опрошенных в ФБР / ИМП, сообщили о об 1-5 случаях инсайдерских злоупотреблений, 37% компаний заявили, что не знают, сколько нарушений в системе безопасности, связанны с инсайдерами.

Куда вы хотите отправиться сегодня?

- "Следующим шагом в эволюции сетевой безопасности будет обнаружение внутренних угроз, нежели вторжения", - Эрик Фридберг, бывший координатор телекоммуникационных и киберпреступлений в офисе прокурора США в Нью-Йорке.
- Идея «в том, что компании стремятся получить ложное чувство безопасности с помощью высокой безобасности периметра»
- "Нынешняя необходимость компьютерной экспертизы такова, что большинство экспертов говорят, что есть три или больше профессии, нуждающиеся в каждом квалифицированном профессионале и дальнейший рост ожидается в будущем." - Ред Титтель, Президент, LANWrights, Inc

Чему учит компьютерная экспертиза?

- **Программно-техническая экспертиза обращает ваше внимание на информацию, которая поможет вам в обнаружении внутренних угроз и проверке на наличие компьютерных преступлений.**

1. **Настройки времени и даты компьютера**
2. **Операционная система и управление версиями**
3. **Разделение жёсткого диска**
4. **Целостность данных и операционной системы**
5. **Вычисление компьютерного вируса**
6. **Лицензирование программного обеспечения**
7. **Каталогизация файлов**
8. **Сохранение ПО, входящих и исходящих файлов**

Итак,

Программно-техническая экспертиза является сбором, сохранением, анализом, извлечением и представлением компьютерных доказательств

Как ПРИМЕНИТЬ CHFI на практике?

Используя знания, содержащиеся в курсе CHFI, вы сможете ответить на такие вопросы, как:

- **Было ли совершено преступление?**
- **Есть ли основания для судебного преследования?**
- **Есть ли возможность реституции?**
- **Как расследовать преступление?**
- **Кого следует информировать о течении дела?**
- **Можете ли вы определить, что информация под угрозой?**
- **Какие доказательства нужно собирать и как?**
- **Будет ли иметь место негативное влияние на ваших клиентов, и что можно предпринять для реабилитации?**

Being Forewarned is being Forewarned!

Being Forewarned is being Forewarned!

Предупреждён - значит вооружён!