Какво е мрежова сигурност

1. Какво е сигурност

В българския език терминът “сигурност” означава две различни неща, които могат лесно да се обяснят през английския език – security и reliability. Първото представлява в по-голямата си част защита от неправомерни действия на индивиди или групи от такива, докато второто представлява защита срещу различни видове природни проблеми и проблеми с хардуера. Този курс обръща внимание повече на първият вид сигурност.

Сигурността е процес, а не единично действие.

- security и reliability
- Сигурността е процес, а не единично действие
- Security through obscurity
- Разделение на секретната (пароли) и несекретна информация (алгоритми), информация, която е безсмислено да се крие
- Описание на термина reliability

2. Какви са рисковете

- Атакуващи - в едно общество винаги има определен процент хора с "лоши" намерения. Интернет е едно такова огромно общество, което има достъп до вас.
  Пример – червеи

- Потребителски - винаги се допускат същите стандартни грешки (buffer overflows, sql injections)
- Много често се допускат грешки и от незнание
- По тези причини винаги ще има security рискове, поради хората, които пишат софтуер, и поради тези, които го използват
- Разпространение на информацията за нов проблем

3. Малко информация за лошите хора

- Изясняване на терминологията
  Хакер
  Кракер
  Phreaker
  Лоши хора - ще се използва по-нататък в курса за по-ясно
  История на термините

- Разделение по намерения - white/black hat
- Етични хакери/кракери

- Какво целят, защо го целят, как можем да пострадаме, каква е опасността
  Крадене на лична информация - кредитни карти, адреси, използване (например за направа на фалшиви документи, или за social engineering)
  Използване на лични ресурси
  Текущи примери за използването за спам, DDoS
  Използване на незаконни цели, storage

- Защо точно нас?
  Защото интернет е огромен, и лесно може да се "преслушва" от лишите хора. На тях им е нужен един човек, а могат да проверят милиони.
  Пример за глобално сканиране, и скорост на разпространение на червеи.
  Разбира се, може някой директно да се интересува от вас, има и много такива случаи.

4. Разлика между инструменти и намерения

- Какви инструменти има
- Защо тези инструменти са важни за администраторите и потребителите
  Проверка, patch-ване - много инструменти за проверка дали са сложени подходящите patch-ове правят грешки
  ! Всеки е администратор на личната си машина

- Не оръжията убиват хора, хората убиват хора
- Вредни" инструменти - autoroot-ери, червеи и т.н., нямащи реално приложение

В много случаи са зле написани ... :)

- Почти всеки инструмент може да се използва по лош начин - пример с ping

- Няколко морални въпроса
  Да можеш не значи да го направиш
  IRC войни, най-добрия пример за грешно използване на инструменти