Защита от современных угроз Технологии и методы

Введение

ТТХ

- Где и когда
  - понедельники в 18:00 в 523
- Кто
  - Андрей Петухов (petand@seclab.cs.msu.su)
  - Иван Новиков (aka Владимир @d0znpp Воронцов, oxod@onsec.ru)
  - Денис Гамаюнов (gamajun@cs.msu.su)
- WWW
  - страница курса http://course.secsem.ru/lections
  - http://lists.secsem.ru/cgi-bin/mailman/listinfo/course

Зачем этот курс aka Мотивация

- Мы наблюдаем, как несистемно воспринимают люди ИБ
- В головах путаница, что от чего защищает и не защищает
  - i.e. мой сайт нельзя взломать. т.к. он работает по HTTPS
- Взаимосвязь между угрозами, атаками и уязвимостями куда более хитрая, чем можно себе представить
- Мы постараемся сделать обзор системной области системно, интересно и актуально

Workflow курса

- Тенденции развития технологий и ИБ
- Безопасность пользователей aka End-point security
- Безопасность приложений aka Application security
- Безопасность инфраструктур aka Infrastructure security
- Безопасность организаций aka Business security

«And now for a taste of things to come» (c) Mortal Kombat

Антивирусы

- Зачем нужны (от чего защищают) антивирусы?
- Какие методы заложены в АВ?
- Назовите угрозы, против которых методы АВ защитить не могут?
- Как защищаться?

Сетевые системы обнаружения атак

- Зачем нужны (от чего защищают) IDS/IPS?
- Какие методы заложены в IDS/IPS?
- Назовите угрозы, против которых методы IDS/IPS защитить не могут?
- Как защищаться?

Утечки данных из организаций

- От продажи базы на «Горбушке» до Сноудена
- Как защищаться?

Недостатки в ПО

- Недостатки в своем ПО: как защищаться?
- Недостатки в чужом ПО: как защищаться?

Вопросы?