Auditing tools lecture plan

1. Защо се ползват (цели и намерения)

2. Видове auditing tools
   - Скенери - получаване на информация за системата
     - Отворени портове
     - Предоставяни услуги
     - Версия на сървърният софутер
     - Известни уязвимости
   - IDS - откриване на опити за пробиви
     - Следене на мрежов трафик
     - Следене за промени във файловата система
   - Log Auditing - откриване на пробиви след като са се случили
   - Password Crackers - откриване на слаби пароли

2. Скенери
   - Network scanners
     - Използват се главно за събиране на информация за отдалечена система
     - Сканират се TCP/UDP портове
     - Специални видове сканиране (SYN, XMAS, Idle scan, etc)
     - Откриване на версиите на OS-ите отдалечено
     - Софтуер
       - nmap
       - paketto keiretsu
       - hping
   - Vulnerability scanners
     - Използват се за откриване на конкретни пробиви във предоставяните услуги
     - Разполагат с бази данни със известни уязвимости и тестове за тях
     - Някой скенери имат възможност да тестват за неизвестни все още уязвимости
     - Софтуер
       - Nessus
       - Retina
       - ISS
       - X-probe

3. IDS - откриване на опити за пробиви
   - Следене на мрежата (Network IDS)
     - За да работи ефективно в дадена мрежа, IDS трябва да може да вижда целият трафик преминаващ през мрежата. По същество Network IDS е подслушваща програма, която следи за определени последователности в мрежовият трафик.
   - Софтуер
     - Snort
     - PreludeIDS
   - Следене на файловата система
     - Целта е откриване на промени във файлове и права за достъп до тях.
   - Софтуер
     - tripwire
     - samhain
     - AIDE

4. Log Auditing
   - Следене на системните събития
   - Отдалено записване на събитията (remote logging)
   - Софтуер
     - Syslog
     - EventLog

Logwatch

5. Password crackers

- Целта е откриване на слаби пароли на потребители

- Отдалечено откриване (brute force)
  Лесно се забелязва при преглед на log файловете

- Локални атаки
  При повечето OS, паролите се държат хеширани
  Ако нормален потребител има достъп до хешовете обикновено това е знак, че има и друг проблем в системата
  Тъй като паролите са хеширани откриването на clear text паролата може да бъде доста времеотнемащ процес
  Полезно за непозволяване на слагане на слаби пароли от потребителите

- Софтуер
  John the ripper
  L0pht Crack
  cracklib