Основы безопасности информационных технологий

Инструментальные средства: сканеры портов, уязвимостей

Содержание лекции

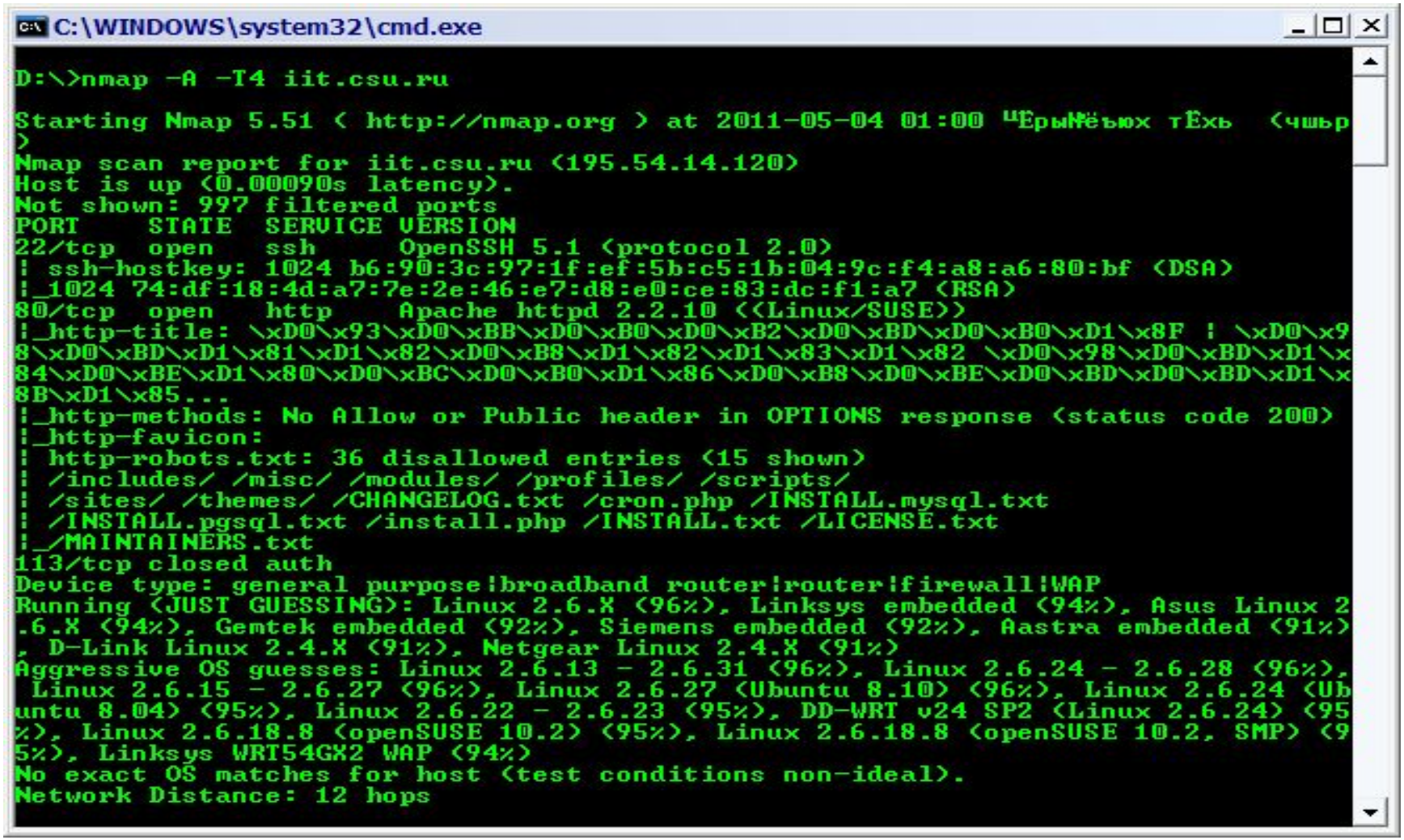
- Серверные порты
- Сканирование портов
- Nmap: сканер портов
  - Типы сканирования
  - Анализатор логов
- Уязвимости
- Анатомия взлома
- Nessus: сканер уязвимостей

Серверные порты

- Internet Assigned Numbers Authority (IANA)
- http://www.iana.org/assignments/port-numbers

Номер порта	Протокол	Сервис
21	FTP	Протокол передачи файлов (управляющий порт)
22	SSH	Защищенный shell
23	Telnet	Telnet
25	SMTP	Почтовый сервис
53	DNS	Разрешение доменных имен
79	Finger	Finger
80	HTTP	Web-сервис
135-139	NetBIOS	Сетевые коммуникации Windows
443	SSL	Защищенный web-сервис

Сканирование портов



Применение сканеров портов

- Инвентаризация сети
- Оптимизация сети/сервера
- Выявление шпионского ПО, "троянских" программ и сетевых "червей"
- Поиск неавторизованных или запрещенных сервисов

Nmap: сканер портов

Достоинства:

- множество опций
- легкий
- прост в использовании

http://nmap.org/download.html

Nmap cmd

nmap *параметры IP-диапазон*

Example:

nmap -A -T4 example.com

Типы сканирования в Nmap

- SYN (-sS)
- TCP-соединение: Connect (-sT)
- Эхо-тестирование: Ping Sweep (-sP)
- UDP-сканирование: UDP Scan (-sU)
- FIN-сканирование: FIN Stealth (-sF)
- NULL-сканирование: NULL Scan (-sN)
- XMAS-сканирование: XMAS Tree (-sX)
- Сканирование через отражатель: Bounce Scan (-n FTP_HOST)
- RPC-сканирование: RPC Scan (-sR)
- Window-сканирование: Window Scan (-sW)
- Реактивное сканирование: Idle Scan (-sI хост-зо
  используемый_порт)

Nlog: log analyzer for NMap

- http://seclists.org/nmap-hackers/1998/81

Расширения:

- Nlog-rpc.pl
- Nlog-smb.pl
- Nlog-dns.pl
- Nlog-finger.pl

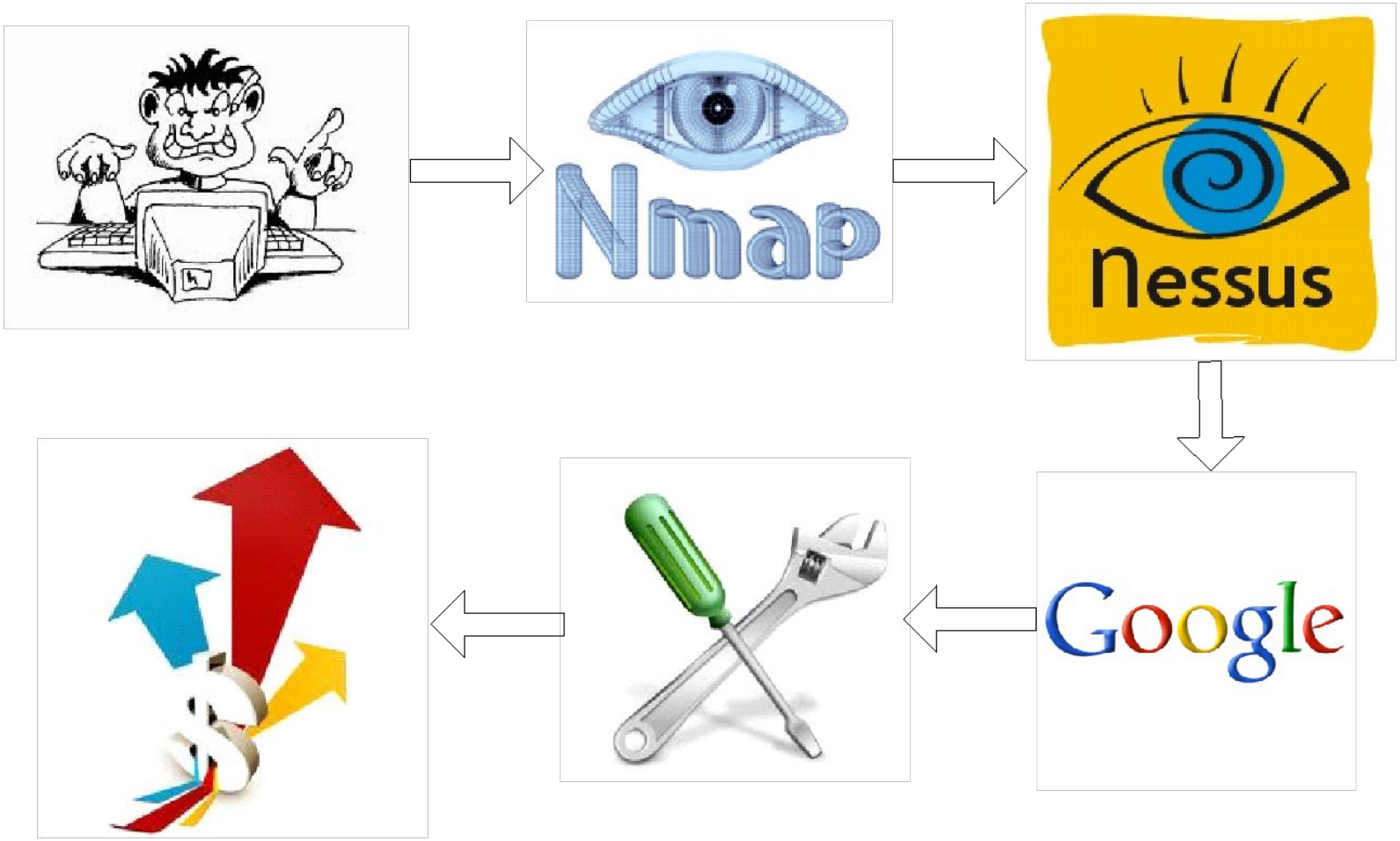
Применение Nlog и Nmap

- Выявление малоупотребительных сервисов
- Охота на незаконные/неизвестные Web-серверы
- Сканирование с целью выявления серверов, выполняющихся на настольных системах
- Охота на "троянские" программы
- Проверка внешнего представления сети

Уязвимости

- Внедрение (Injection)
  - Внедрение SQL
  - Внедрение команд
- Межсайтовые сценарии (Cross Site Scripting, XSS)
- Неправильная аутентификация и управление сеансами
- Подделка межсайтовых запросов (Cross Site Request Forgery, CSRF, XSRF)
- Небезопасное управление конфигурацией
- Хранение незащищенных данных
- Переполнение буфера
- …

Анатомия взлома



Nessus: сканер уязвимостей

Категории тестов:

- Потайные входы
- Ненадлежащее использование CGI
- Cisco
- Атаки на доступность
- Ненадлежащее использование Finger
- Удаленный доступ к командному интерпретатору
- Удаленное получение прав суперпользователя
- Общие
- Прочие
- NIS
- Сканеры портов
- Удаленный доступ к файлам
- RPC
- Настройки
- SNMP
- Непроверенные
- Бесполезные сервисы
- Windows

- http://www.tenable.com/products/nessus/nessus-download-agreement

Nessus: сканер уязвимостей

- Архитектура клиент-сервер
- Независимость
- Встроенный язык сценариев атак
- Интеграция с другими средствами
  - Nmap
  - Nikto, Whisker
  - Hydra
- Интеллектуальное тестирование
- База знаний
- Множество форматов отчетов

Что не находит тестирование уязвимостей?

- Логические ошибки
- Необнаруженные уязвимости
- Индивидуальные приложения
- Безопасность персонала