

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

C:\WINDOWS\system32\cmd.exe

```
D:\>nmap -A -T4 iit.csu.ru
```

```
Starting Nmap 5.51 ( http://nmap.org ) at 2011-05-04 01:00 ЧЕРНЫЕЪЮХ ТЕХЪ <чшьр
>
Nmap scan report for iit.csu.ru (195.54.14.120)
Host is up (0.00090s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
22/tcp   open  ssh      OpenSSH 5.1 (protocol 2.0)
|_ ssh-hostkey: 1024 b6:90:3c:97:1f:ef:5b:c5:1b:04:9c:f4:a8:a6:80:bf (DSA)
|_ 1024 74:df:18:4d:a7:7e:2e:46:e7:d8:e0:ce:83:dc:f1:a7 (RSA)
80/tcp   open  http     Apache httpd 2.2.10 ((Linux/SUSE))
|_ http-title: \xD0\x93\xD0\xBB\xD0\xB0\xD0\xB2\xD0\xBD\xD0\xB0\xD1\x8F : \xD0\x9
8\xD0\xBD\xD1\x81\xD1\x82\xD0\xB8\xD1\x82\xD1\x83\xD1\x82 \xD0\x98\xD0\xBD\xD1\x
84\xD0\xBE\xD1\x80\xD0\xBC\xD0\xB0\xD1\x86\xD0\xB8\xD0\xBE\xD0\xBD\xD0\xBD\xD1\x
8B\xD1\x85...
|_ http-methods: No Allow or Public header in OPTIONS response (status code 200)
|_ http-favicon:
|_ http-robots.txt: 36 disallowed entries (15 shown)
|_ /includes/ /misc/ /modules/ /profiles/ /scripts/
|_ /sites/ /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
|_ /INSTALL.pgsql.txt /install.php /INSTALL.txt /LICENSE.txt
|_ /MAINTAINERS.txt
113/tcp  closed auth
Device type: general purpose!broadband router!router!firewall!WAP
Running (JUST GUESSING): Linux 2.6.X (96%), Linksys embedded (94%), Asus Linux 2
.6.X (94%), Gemtek embedded (92%), Siemens embedded (92%), Aastra embedded (91%)
, D-Link Linux 2.4.X (91%), Netgear Linux 2.4.X (91%)
Aggressive OS guesses: Linux 2.6.13 - 2.6.31 (96%), Linux 2.6.24 - 2.6.28 (96%),
Linux 2.6.15 - 2.6.27 (96%), Linux 2.6.27 (Ubuntu 8.10) (96%), Linux 2.6.24 (Ub
untu 8.04) (95%), Linux 2.6.22 - 2.6.23 (95%), DD-WRT v24 SP2 (Linux 2.6.24) (95
%), Linux 2.6.18.8 (openSUSE 10.2) (95%), Linux 2.6.18.8 (openSUSE 10.2, SMP) (9
5%), Linksys WRT54GX2 WAP (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 12 hops
```

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-зс 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

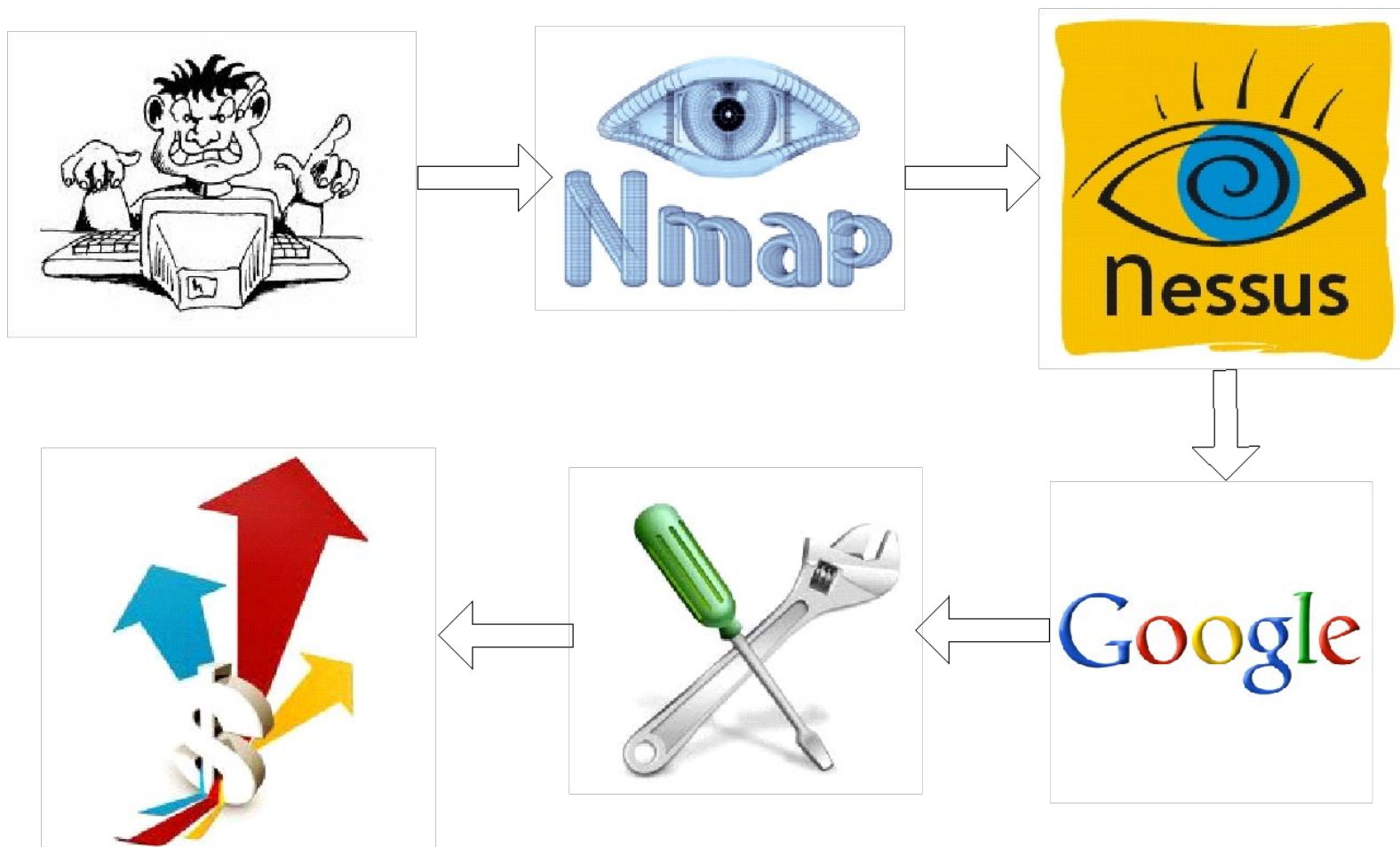


Уязвимости

- Внедрение (Injection)
 - Внедрение SQL
 - Внедрение команд
- Межсайтовые сценарии (Cross Site Scripting, XSS)
- Неправильная аутентификация и управление сессиями
- 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
 - Бесплезные 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

