Безопасность в Web

План лекции

- Отчет с YUT CodeGate 2012, пример задачи
- Hex-editor
- Фаил robots.txt
- .svn - vulnerability
- Toolchain: ping/nslookup/traceroute

Арыков Никита, nikita.arykov@gmail.com

YUT CodeGate 2012

Всего было зарегистрировано 472 команды

Только 182 команды сдало хотя бы одну задачу

Мы заняли 102 место

Разделы задач:

- Vulnerability(SQL-Injection)
- Binary(Disassembly)
- Network
- Forensics(Комп.криминалистика
- Misc

Сдали F100, F200, M300, B100

99		Enforcer	800
100		Kroot	800
101		TwoSixNine	800
102		__bs__	700
103		ColdTiger5	700
104		DigRev	700
105		yoona	700
106		CASPER	700
107		Yeotgarak	700
108		BrooklyntOverfl	700
109		СОБАКА	600
110		test	600
111		PoolC	600
112		guest	600
113		helloworld	600
114		IS_Team1	600
115		kbb_	500
116		InterCEPTeam	500
117		sk8erz	500

Forensics 100

Условие:

Дан «backup» системы(Windows7)

Известно, что с компьютера был украден Excel документ. Необходимо найти полный путь до документа и его размер.

Решение:

Находим фаилы с раширением .xls;

Сразу бросается в глаза фаил

[Top-Secret]_2011_Financial_deals.LNK

Самого фаила в «backup» нету :(

Forensics 100

.LNK — обычный ярлык(shortcut) в windows(аналог в Unix symlink);

Если посмотреть его свойства, то размер исходного фаила не будет виден;

Бинарный формат имеет открытую спецификацию

[MS-SHLLINK]: Shell Link (.LNK) Binary File Format:

http://msdn.microsoft.com/en-us/library/dd871375(v=prot.13).aspx

3.1 Shortcut to a File

msdn

1 out of 2 rated this helpful Rate this topic

This section presents a sample of the Shell Link Binary File Format, consisting of a shortcut to a file with the path "C:\test\a.txt".

The following is the hexadecimal representation of the contents of the shell link.

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xA	xB	xC	xD	xE	xF
0000	4C	00	00	00	01	14	02	00	00	00	00	00	C0	00	00	00
0010	00	00	00	46	9B	00	08	00	20	00	00	00	D0	E9	EE	F2
0020	15	15	C9	01	D0	E9	EE	F2	15	15	C9	01	D0	E9	EE	F2
0030	15	15	C9	01	00	00	00	00	00	00	00	00	01	00	00	00
0040	00	00	00	00	00	00	00	00	00	00	00	00	BD	00	14	00
0050	1F	50	E0	4F	D0	20	EA	3A	69	10	A2	D8	08	00	2B	30
0060	30	9D	19	00	2F	43	3A	5C	00	00	00	00	00	00	00	00
0070	00	00	00	00	00	00	00	00	00	00	00	46	00	31	00	00
0080	00	00	00	2C	39	69	A3	10	00	74	65	73	74	00	00	32

CreationTime: (8 bytes, offset 0x001C) FILETIME 9/12/08, 8:27:17PM.

AccessTime: (8 bytes, offset 0x0024) FILETIME 9/12/08, 8:27:17PM.

WriteTime: (8 bytes, offset 0x002C) FILETIME 9/12/08, 8:27:17PM.

FileSize: (4 bytes, offset 0x0034), 0x00000000.

IconIndex: (4 bytes, offset 0x0038), 0x00000000.

Какой максимальный размер фаила может быть при этих данных?

Hex-editor

1 Byte — 8 bit, может принимать одно из 2^8 = 256 значений.

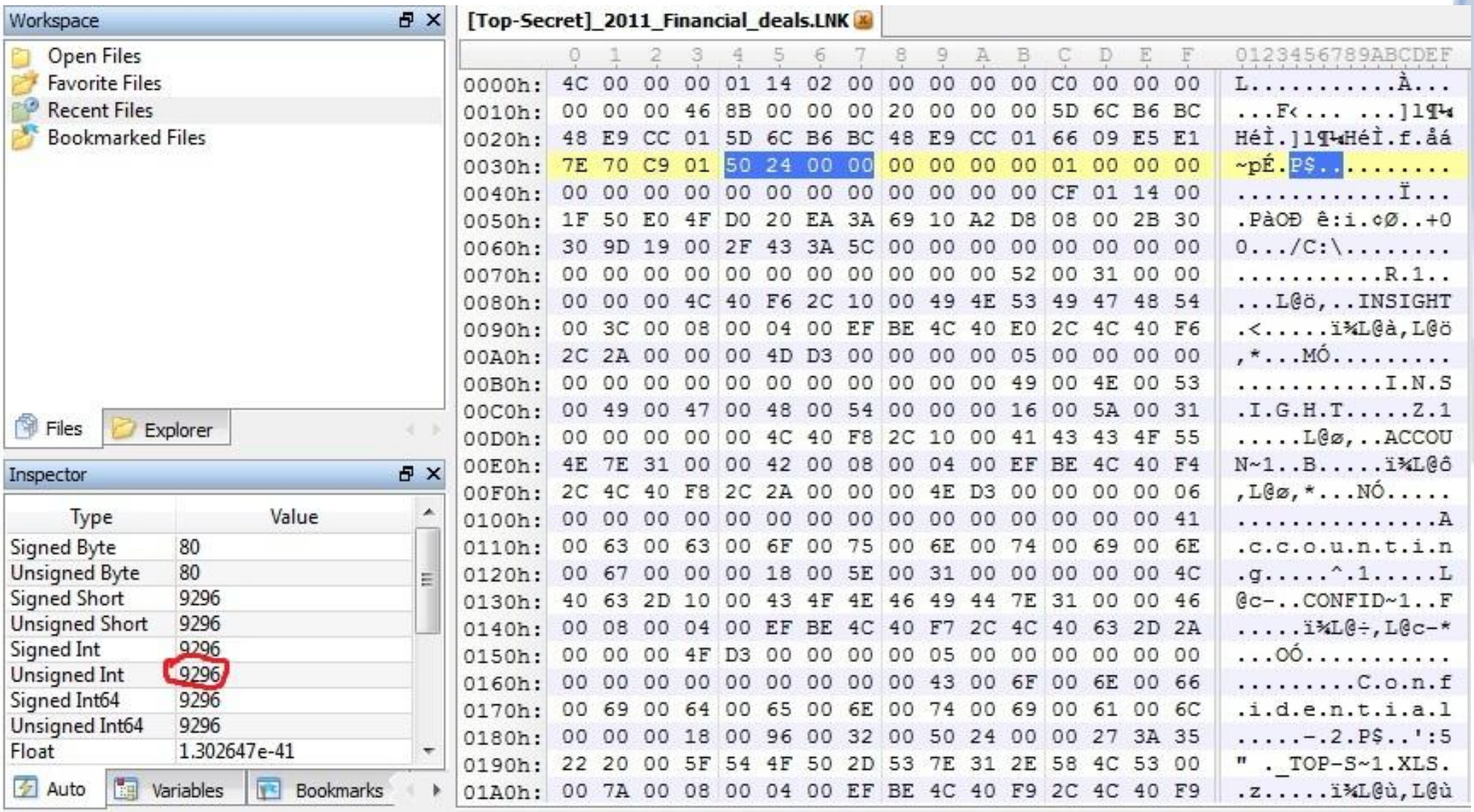
1 Byte ~ $[0x00, 0xFF]_{hex} = [0,255]_{dec}$

2 Byte ~ $[0x0000, 0xFFFF]_{hex} = [0,65535]_{dec}$

Hex-editor — приложение для редактирования данных, в котором данные представлены в «сыром виде»(raw) — как последовательность байтов.

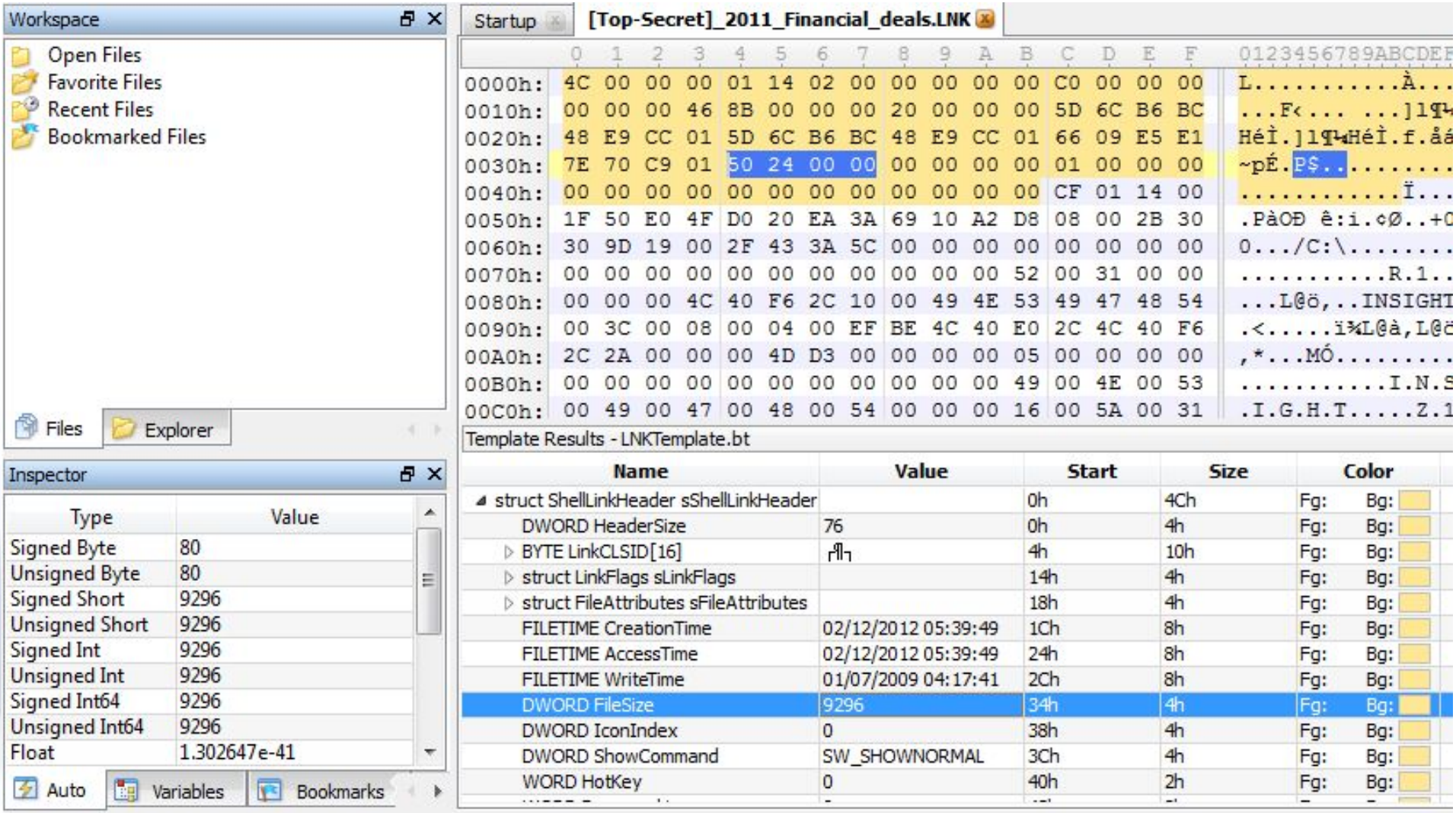
Мы использовали 010 editor, так же есть и другие, например, достаточно популярный WinHEX

Forensics 100



FileSize(4 bytes, offset 0x0034), 0x00000000;
0x00002450=9296 — размер фаила(запись байтов в обратном порядке)

Forensics 100



Есть плагин который понимает формат .LNK
LNK Template http://blog.didierstevens.com/2010/08/08/quickpost-2-lnk-tools/

Фаил robots.txt

Стандарт исключений для роботов (robots.txt) — файл ограничения доступа к содержимому поисковым роботам на http-сервере. Файл должен находиться в корне сайта (то есть иметь путь относительно имени сайта /robots.txt).

Использование:

Запрет доступа робота googlebot к каталогу /private/:

```
User-agent: googlebot
Disallow: /private/
```

Запрет доступа всех роботов ко всему сайту:

```
User-agent: *
Disallow: /
```

Фаил robots.txt

Следующий пример дает явную подсказку хакеру

User-agent: *

Disallow: /admin/

Disallow: /secret/

Эксплуатация

- http://mail.ru/robots.txt
- http://en.wikipedia.org/robots.txt

Фаил .htaccess/.htpasswd

.htaccess (от. англ. hypertext access) — файл дополнительной конфигурации веб-сервера Apache, а также подобных ему серверов. Позволяет задавать большое количество дополнительных параметров и разрешений для работы веб-сервера в отдельных каталогах (папках), таких как управляемый доступ к каталогам, переназначение типов файлов и т.д., без изменения главного конфигурационного файла.

!!!Аналог robots.txt(использовать аналогично)

.svn - vulnerability

В силу особенностей архитектуры, Subversion хранит в каждой директории проекта свои метафайлы, аккуратно сложенные в скрытую директорию .svn.

Там находится информация о расположении репозитория, размере файлов, даты их изменения и логины пользователей, работающих над проектом.

Эксплуатация

http://site.com/.svn/entries

http://site.com/.svn/text-base/index.php.svn-base

.svn - vulnerability

Немного статистики:

- Просканировано доменов: 2253388
- Уязвимых: 3320
- В их числе сайты Yandex, Rambler, Opera...

Причина

- Используется svn checkout вместо svn export, в следствие чего пользователь извне обладает правами доступа к фаилам

!!!Можно добавить в наш Filter безопасности

Ссылка

http://habrahabr.ru/blogs/infosecurity/70330/

ping

ping — утилита для проверки соединений в сетях на основе TCP/IP;

Практическое использование

- Можно узнать IP-адрес по доменному имени.
- Можно узнать, работает ли сервер.

```
C:\Users\daredevil>ping ya.ru

Pinging ya.ru [87.250.250.3] with 32 bytes of data:
Reply from 87.250.250.3: bytes=32 time=240ms TTL=51
Reply from 87.250.250.3: bytes=32 time=273ms TTL=51
Reply from 87.250.250.3: bytes=32 time=248ms TTL=51
Reply from 87.250.250.3: bytes=32 time=246ms TTL=51

Ping statistics for 87.250.250.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 240ms, Maximum = 273ms, Average = 251ms
```

Ping of Death

Ping of death — тип сетевой атаки, при которой компьютер-жертва получает особым образом подделанный эхо-запрос (ping), после которого он перестает отвечать на запросы вообще (DoS);

По стандарту RFC 791 IPv4 суммарный объем пакета не может превышать 65 535 байт;

Пример

```
ping -l 65500 example.com
```

http://en.wikipedia.org/wiki/Ping_of_death

DNS

DNS (Domain Name System) — компьютерная распределённая система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста.

Записи тип A (A RECORDS)

Запись типа A позволяет установить соответствие между именем хоста в домене и его IP-адресом. Например, если Вы хотите, чтобы mycomputer.yourdomain.com указывала на Ваш домашний компьютер (который имеет адрес, например, 192.168.0.3);

DNS

Записи сервера имён (NS)

Записи типа NS (Name Server - сервер имен) описывают authoritative DNS-серверы для данного домена.

Записи MX

Запись типа MX (Mail Exchange - почтовый сервер) определяет почтовый сервер - машину, которая обрабатывает почту для вашего домена.

nslookup

nslookup (name server lookup) — утилита, предоставляющая пользователю интерфейс командной строки для обращения к системе DNS

```
C:\Users\daredevil>nslookup
Default Server:  UnKnown
Address:  192.168.43.1

> set q=NS
> ya.ru
Server:  UnKnown
Address:  192.168.43.1

Non-authoritative answer:
ya.ru   nameserver = ns1.yandex.ru
ya.ru   nameserver = ns5.yandex.ru
> set q=MX
> ya.ru
Server:  UnKnown
Address:  192.168.43.1

Non-authoritative answer:
ya.ru   MX preference = 10, mail exchanger = mx.yandex.ru
> set q=A
> ya.ru
Server:  UnKnown
Address:  192.168.43.1

Non-authoritative answer:
Name:    ya.ru
Addresses:  87.250.250.3
          77.88.21.3
          213.180.204.3
          213.180.193.3
          93.158.134.203
          93.158.134.3
          87.250.251.3
          87.250.250.203
```

IP-адресов уже
больше чем с помощью ping

nslookup

```
C:\Users\daredevil>nslookup
Default Server:  UnKnown
Address:  192.168.43.1

> set q=A
> set d2
> mail.ru
Server:  UnKnown
Address:  192.168.43.1

------------
SendRequest(), len 25
    HEADER:
        opcode = QUERY, id = 2, rcode = NOERROR
        header flags:  query, want recursion
        questions = 1,  answers = 0,  authority records = 0,  additional = 0

    QUESTIONS:
        mail.ru, type = A, class = IN

------------
------------
Got answer (89 bytes):
    HEADER:
        opcode = QUERY, id = 2, rcode = NOERROR
        header flags:  response, want recursion, recursion avail.
        questions = 1,  answers = 4,  authority records = 0,  additional = 0

    QUESTIONS:
        mail.ru, type = A, class = IN
    ANSWERS:
    ->  mail.ru
        type = A, class = IN, dlen = 4
        internet address = 94.100.191.204
        ttl = 46 (46 secs)
    ->  mail.ru
        type = A, class = IN, dlen = 4
        internet address = 94.100.191.201
        ttl = 46 (46 secs)
    ->  mail.ru
        type = A, class = IN, dlen = 4
        internet address = 94.100.191.202
        ttl = 46 (46 secs)
    ->  mail.ru
        type = A, class = IN, dlen = 4
        internet address = 94.100.191.203
        ttl = 46 (46 secs)

------------
Non-authoritative answer:
Name:    mail.ru
Addresses:  94.100.191.204
          94.100.191.201
          94.100.191.202
          94.100.191.203
```

set d2 - включает дополнительную отладочную информацию

traceroute

Traceroute — это служебная компьютерная программа, предназначенная для определения маршрутов следования данных в сетях TCP/IP;

В windows называется tracert

```
C:\Documents and Settings\Administrator>tracert ru.wikipedia.org

Трассировка маршрута к rr.esams.wikimedia.org [91.198.174.2]
с максимальным числом прыжков 30:

1     1 ms    <1 ms    <1 ms  vpn4.kras.gldn [10.10.1.14]
2     2 ms    <1 ms    <1 ms  C7604-BRAS4-FTTB.ranetka.ru [80.255.150.41]
3     1 ms     1 ms     4 ms  C76-External.ranetka.ru [80.255.128.162]
4     1 ms    <1 ms    <1 ms  pe-1.Krasnoyarsk.gldn.net [195.239.173.37]
5    79 ms    79 ms    98 ms  cat01.Stockholm.gldn.net [194.186.157.62]
6   131 ms   131 ms   132 ms  ams-ix.2ge-2-1.br1-knams.wikimedia.org [195.69.145.176]
7   131 ms   131 ms   131 ms  te-8-2.csw1-esams.wikimedia.org [91.198.174.254]
8   133 ms   134 ms   133 ms  rr.esams.wikimedia.org [91.198.174.2]

Трассировка завершена.
```

Литература

Календарь CTF http://capture.thefl.ag/calendar/

Большая часть решений(eng) http://eindbazen.net/

Часть решений(rus)
http://darkbyte.ru/2012/35/codegate-2012-writeup/

http://blog.0x01000000.org/2010/08/10/lnk-parsing-you re-doing-it-wrong-i/