

More Smoked CTFs
для
Leet Chicken,
пожалуйста!

1376146800

By
Anton Sapozhnikov
@snowytoxa



Agenda*

/*

- Who am I?
- CTF?!
- Jeopardy
- Classic
- Почему CTF это круто?
- Сервисы
- tips&tricks

*/

*данная презентация выражает только мнение автора

Who am I?

```
/*
```

- penetration tester > 6 yrs
- KPMG
- CTF player MoreSmokedLeetChicken > 6 yrs
 - DEFCON, HITB, CODEGATE, Hack.lu, PHDays, Secuinside, RuCTF, iCTF, UralCTF, ...

```
*/
```

CTF?!

/*

Classic CTF

DEFCON Final

RuCTF Final

* Final

Jeopardy

DEFCON Quals

RuCTF Quals

CODEGATE

* Quals

*/

Jeopardy

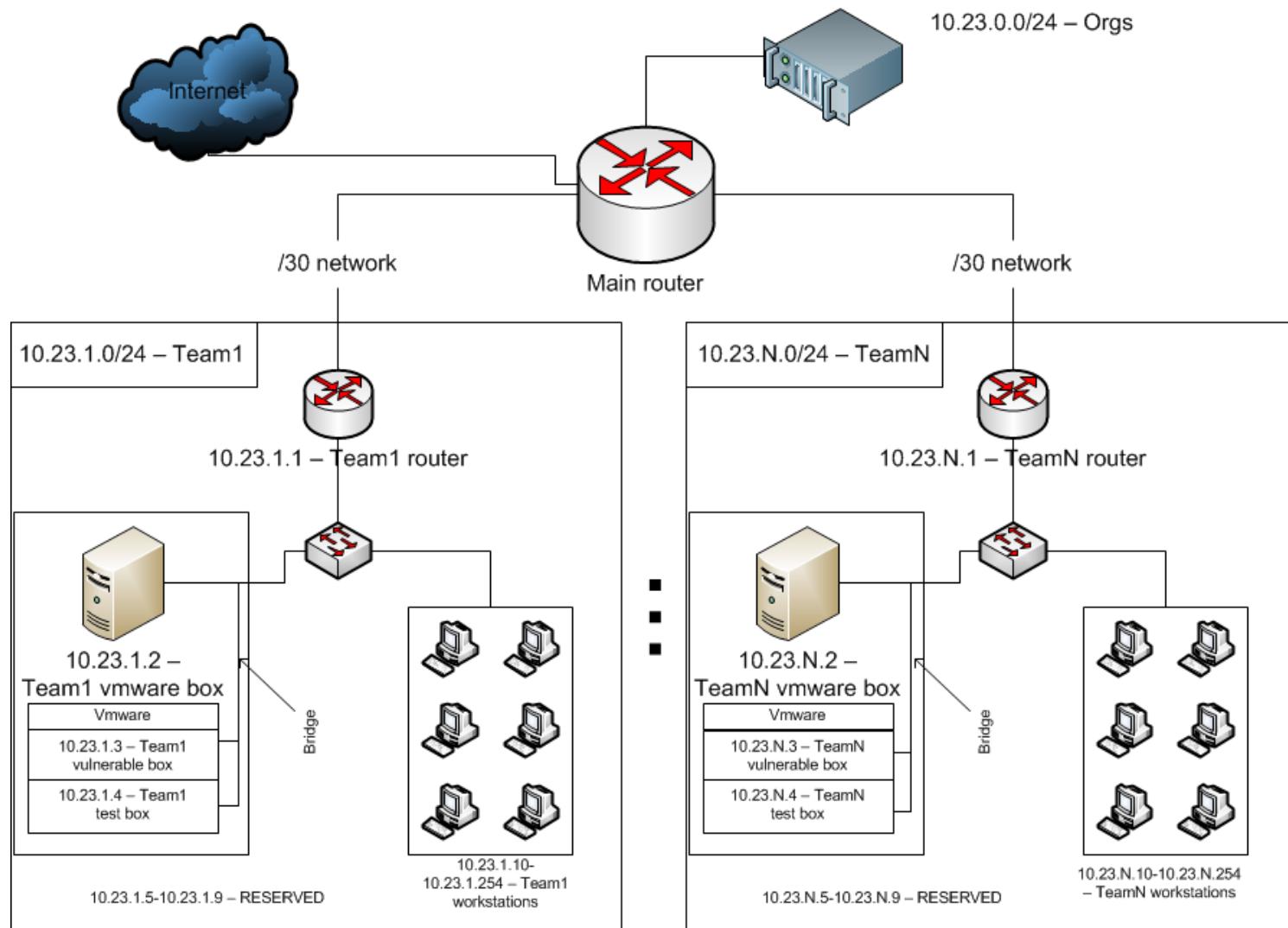
17 июня 2013 г. 4:00:06 <global> WE'RE OVER
 17 июня 2013 г. 3:59:49 <global> go go go go go
 17 июня 2013 г. 3:59:19 <global> IT'S THE FINAL COUNTDOWN
 17 июня 2013 г. 3:59:17 <global> IT'S THE FINAL COUNTDOWN
 17 июня 2013 г. 3:59:17 <global> IT'S THE FINAL COUNTDOWN
 17 июня 2013 г. 3:59:17 <global> IT'S THE FINAL COUNTDOWN

3dub	0x41414141	\xFF\xE4\xCC	OMGACM	gnireenigne
1	1	1	1	1
2	2	2	2	2
3	3	3	3	3
4	4	4	4	4
5	5	5	5	5

0:00:00 left

PPP	75
European NOPSled Team	70
More Smoked Leet Chicken	70
blue-lotus	64
Routards	61
Shell Corp	61
Shellphish	60
WOWHACKER-B10S	60
WHAT_Mafia	59
9447	59
Men in Black Hats	58
clgt	58
Samurai	54
sutegoma2	54
pwnningyeti	54
APT8	54
Alternatives	53
int3pids	52
Robot Mafia	51
[TechnoPandas]	51

Classic



Почему CTF это круто?

Яндекс

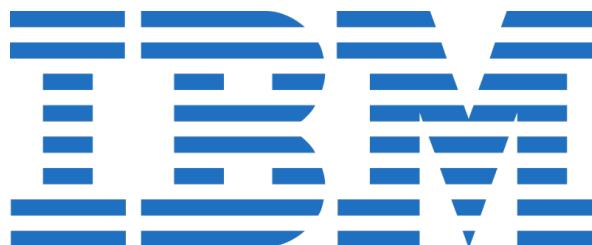
Найдётся всё



лаборатория
КЛ(ПЭР)(КОГО)



Информзащита
Системный интегратор



DECON XXI Final

```
/*
 - Legitimate Business Syndicate
 - ARM
 - IPv4
 - Linux ourteam 3.8.13.2 #15 SMP PREEMPT Wed Jul 31 22:58:59 PDT 2013 armv7l
 GNU/Linux.

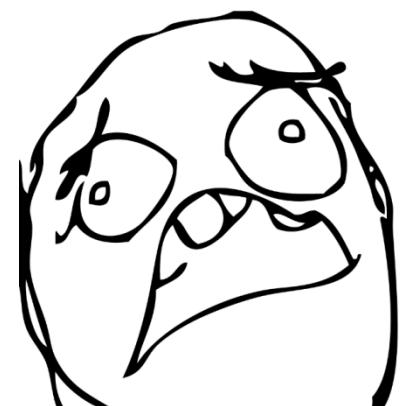
 */
```

眞の会社

+



=



**more smoked
leet chicken**

DEF CON CTF 2013
Ultimate Business Syndicate

reeses

```
/*
```

- получает по сети VM
- проверяет целостность
- запускает

- переполнение в VM под MIPS
- лик в хост машине

```
    syscall_rand(){  
        if( !initialized ){  
            srand(time(0)^printf);  
            initialized = 1;  
        }  
        return rand();  
    }
```

- bof в хост машине через syscall_read()/syscall_write()
- ```
*/
```

# trouver

```
/*
-эм뮬атор шелла
-вход по паролю, листинг файлов, создание файлов,
etc

- 1 byte overflow by '\n'
- утечка адреса возврата
- спрей rop system('cat flag')
*/
```

# lonetuna

```
/*
```

- Принимает 3 команды:

- 1 ) Change display text.\n2 ) Upload a new font.\n3 ) Exit.\n-->

- Биндит случайный порт и отрисовывает в него текст (до 5 символов) по шрифтом из п.2

- DoS

- bof+libc+rop

```
*/
```

# tips&tricks

```
/*
```

- мониторить сетевой трафик
- защищать свою сеть
- хакать другие команды\*
- изучать логику игры
- делать домашние заготовки
- have fun

```
*/
```

/\*  
**Final**  
**Scoreboard**  
\*/

|   | Team                      | Score |
|---|---------------------------|-------|
| 1 | PPP                       | 15002 |
| 2 | men in black hats         | 7924  |
| 3 | raon_ASRT                 | 7107  |
| 4 | more smoked leet chicken  | 4160  |
| 5 | routards                  | 2503  |
| 6 | sutegoma2                 | 1540  |
| 7 | shellphish                | 1223  |
| 8 | Alternatives              | 1095  |
| 9 | The European Nopsled Team | 859   |
| A | 9447                      | 506   |
| B | blue lotus                | 441   |
| C | Samurai                   | 12    |
| D | APT8                      | 0     |
| D | clgt                      | 0     |
| D | pwnies                    | 0     |
| D | pwningyeti                | 0     |
| D | Robot Mafia               | 0     |
| D | shell corp                | 0     |
| D | [Technopandas]            | 0     |
| D | WOWHacker-BIOS            | 0     |

/\*  
СПАСИБО!  
\*/



Антон @snowytoxa Сапожников

10 августа 2013 г.



```
/*
TEXT
*/
```