

O que você precisa saber sobre CTF

By Matheus Vrech a.k.a. abrasax

Roteiro

- O que é CTF e afins
- Tipos de CTF
- CTFtime
- Jeopardy e seus challenges
- Considerações finais
- Alguns challenges!



Capture The Flag

O que é Capture The Flag?

- Qual a importância do CTF para a infosec?
- O que eu preciso saber para jogar um CTF?
- O que são as famosas flags?
 - CTF-BR{3u_s0u_um4_fl4g}
 - actf{wow_ur_a_jinja_ninja}

Jeopardy

Exploitation	100	200	300	300	400	400	500
Reverse Engineering	100	200	300	300	500		
Cryptography	200	300	300				
Forensics	100	200	200	300			
Web	0	300					
Recon	100	100	100				
Networking	100						
Trivia	10	10	10	10	10	10	

Challenge

4 Solves



Implants 'R Us

500

We want to place an implant into the main process cabinet.

Find the cabinet and open it. Once inside, you should see a flashing red button. Press the red button and obtain proof that you succeeded.

PS: Don't get caught, the robots don't take prisoners.

Key

SUBMIT

Attack and Defense



Boot2root



HackTheBox.eu



Arctic



VULNHUB

V U L N E R A B L E B Y D E S I G N

[Home](#) / [CTFs](#) / [Events](#) / [Archive](#)

CTF Events

[All](#) [Upcoming](#) [Archive](#) [Format ▾](#) [Year ▾](#)

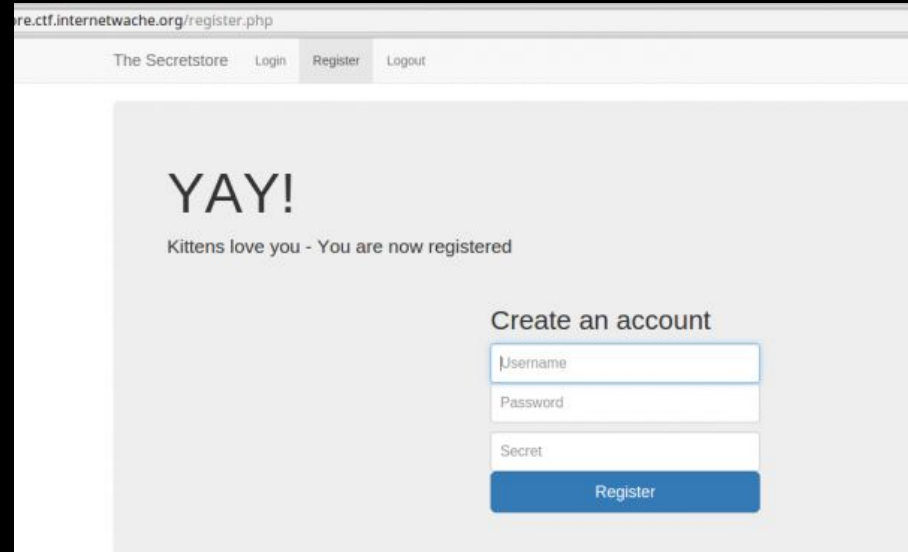
Name	writeup	Date	Format	Location	Notes
RuCTFE 2015	writeup	21 十一月 2015, 18:00 CST — 22 十一月 2015, 03:00 CST	Attack-Defense	On-line	missing the scoreboard
Trend Micro CTF Asia Pacific & Japan 2015 Final	writeup	21 十一月 2015, 12:30 CST — 22 十一月 2015, 14:30 CST	Attack-Defense	Tokyo, Japan	missing the scoreboard
GreHack CTF 2015	writeup	21 十一月 2015, 05:00 CST — 21 十一月 2015, 16:00 CST	Jeopardy		missing the scoreboard
Defcamp CTF Finals 2015	writeup	19 十一月 2015, 21:00 CST — 20 十一月 2015, 21:00 CST	Jeopardy	Bucharest, Romania	missing the scoreboard
Hack Dat Kiwi 2015	writeup	18 十一月 2015, 13:00 CST — 20 十一月 2015, 13:00 CST	Jeopardy	On-line	missing the scoreboard
RCTF 2015 Quals	writeup	14 十一月 2015, 08:00 CST — 15 十一月 2015, 20:00 CST	Jeopardy	On-line	

De volta ao jeopardy..

—

Web

- Quanto mais se conhecer as aplicações web, melhor
- Ajuda muito com a realização de pentests

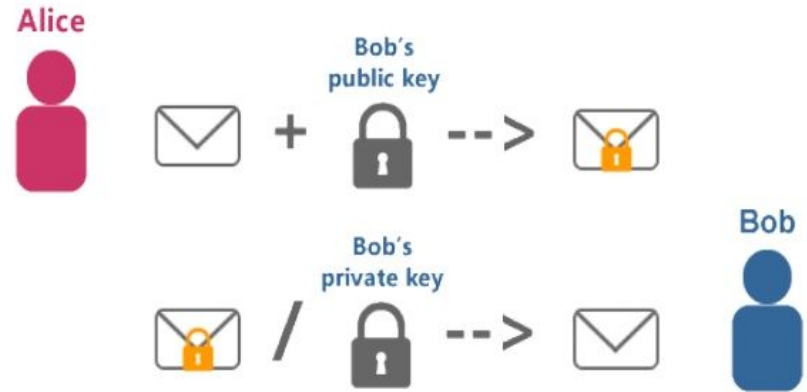


Workshop Time

Cryptography

- Aborda os principais ataques conhecidos a criptografias
- É ótimo para quem gosta de matemática e programar soluções

Working of RSA



Workshop Time

Reverse Engineering

- Exige conhecimento sobre as arquiteturas de computadores
- Ajuda a entender muito sobre como os programas funcionam nos “bastidores”

```
[0x00003c9c 255 /usr/bin/r2]> pd $r @ sym..L94+4869 # 0x3c9c
0x00003c9c e970efffff jmp 0x100002c11 ; (fcn.00002390) ;[1]
0x00003ca1 8bbba4010000 mov edi, [ebx+0x1a4]
0x00003ca7 8b74247c mov esi, [esp+0x7c]
0x00003cab 8b8424940000 mov eax, [esp+0x94]
0x00003cb2 c74424040000 mov dword [esp+0x4], 0x0
0x00003cba 890424 mov [esp], eax
0x00003cbd e81ee2ffff call 0x100001ee0 ; (sym.imp.r_core_prompt) ;[2]
    sym.imp.r_core_prompt()
0x00003cc2 85c0 test eax, eax
0x00003cc4 0f8eaa000000 jle 0x3d74 ;[3]
0x00003cca 85f6 test esi, esi
0x00003ccc 7408 jz 0x3cd6 ;[4]
0x00003cce 893424 mov [esp], esi
0x00003cd1 e84ae4ffff call 0x100002120 ; (sym.imp.r_th_lock_enter) ;[5]
    sym.imp.r_th_lock_enter()
0x00003cd6 8b9424940000 mov edx, [esp+0x94]
0x00003cdd 891424 mov [esp], edx
0x00003ce0 e80be4ffff call 0x1000020f0 ; (sym.imp.r_core_prompt_exec) ;[6]
    sym.imp.r_core_prompt_exec()
0x00003ce5 8904249c0000 mov [esp+0x9c], eax
0x00003cec 83c001 add eax, 0x1
0x00003cef 0f8424010000 jz 0x3e19 ;[7]
0x00003cf5 85f6 test esi, esi
0x00003cf7 7408 jz 0x3d01 ;[8]
```

Workshop Time

Pwn

- É como um “algo a mais” dos exercícios de rev
- É bom para quem quer começar a desenvolver os próprios exploits

pwntools - CTF toolkit



PWNTOOLS

[docs](#) [stable](#) [pypi](#) [v3.0.1](#) [build](#) [passing](#) [coverage](#) [53%](#) [twitter](#) [pwntools](#) [license](#) [MIT](#)

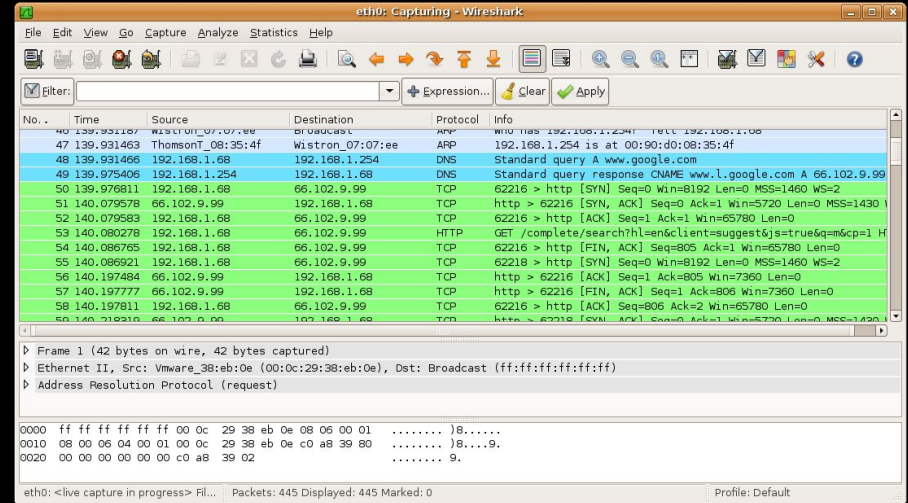
pwntools is a CTF framework and exploit development library. Written in Python, it is designed for rapid prototyping and development, and intended to make exploit writing as simple as possible.

```
from pwn import *
context(arch = 'i386', os = 'linux')

r = remote('exploitme.example.com', 31337)
# EXPLOIT CODE GOES HERE
r.send(asm(shellcraft.sh()))
r.interactive()
```

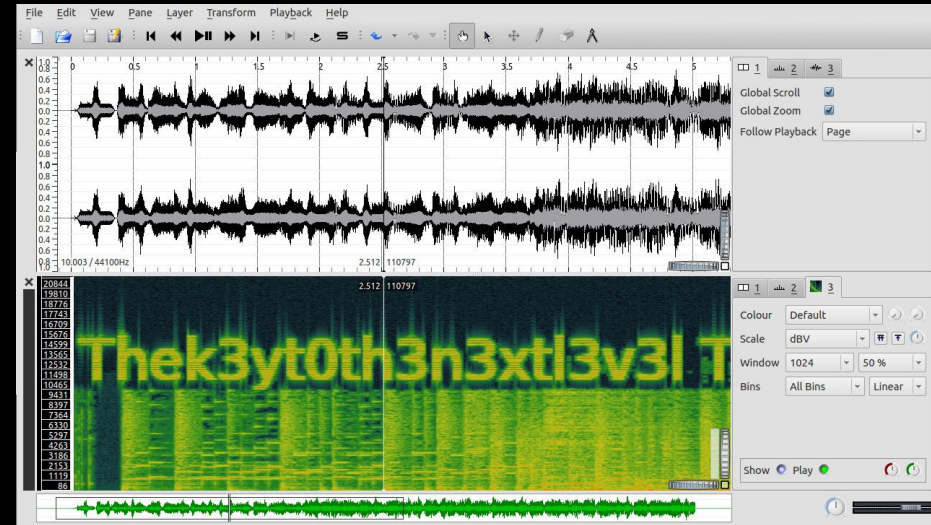
Network

- Envolvem conhecimentos de redes
- São ótimos para quem gosta de realizar ataques em redes locais e analisar o tráfego



Steganography

- Costuma exigir habilidades com multimídias
- É perfeito para quem gosta de tratar imagens e vídeos



Sugestões

- Se especializar em menos áreas com um time diversificado é uma boa ideia
- Ler writeups é uma ótima forma de aprender
- Pessoas diferentes criam soluções diferentes
- Trabalho em equipe faz toda a diferença

Como posso continuar essa jornada?

- <https://shellterlabs.com/>
- <https://www.hackthebox.eu/>
- <https://ctftime.org/>
- <https://ctf-br.org/docs/>
- @pomboufscar
- @UniverSecBrasil
- @vrechson
- abrasax@cocaine.ninja

Challenges!

—