O que você precisa saber sobre CTF

By Matheus Vrech a.k.a. abrasax

Roteiro

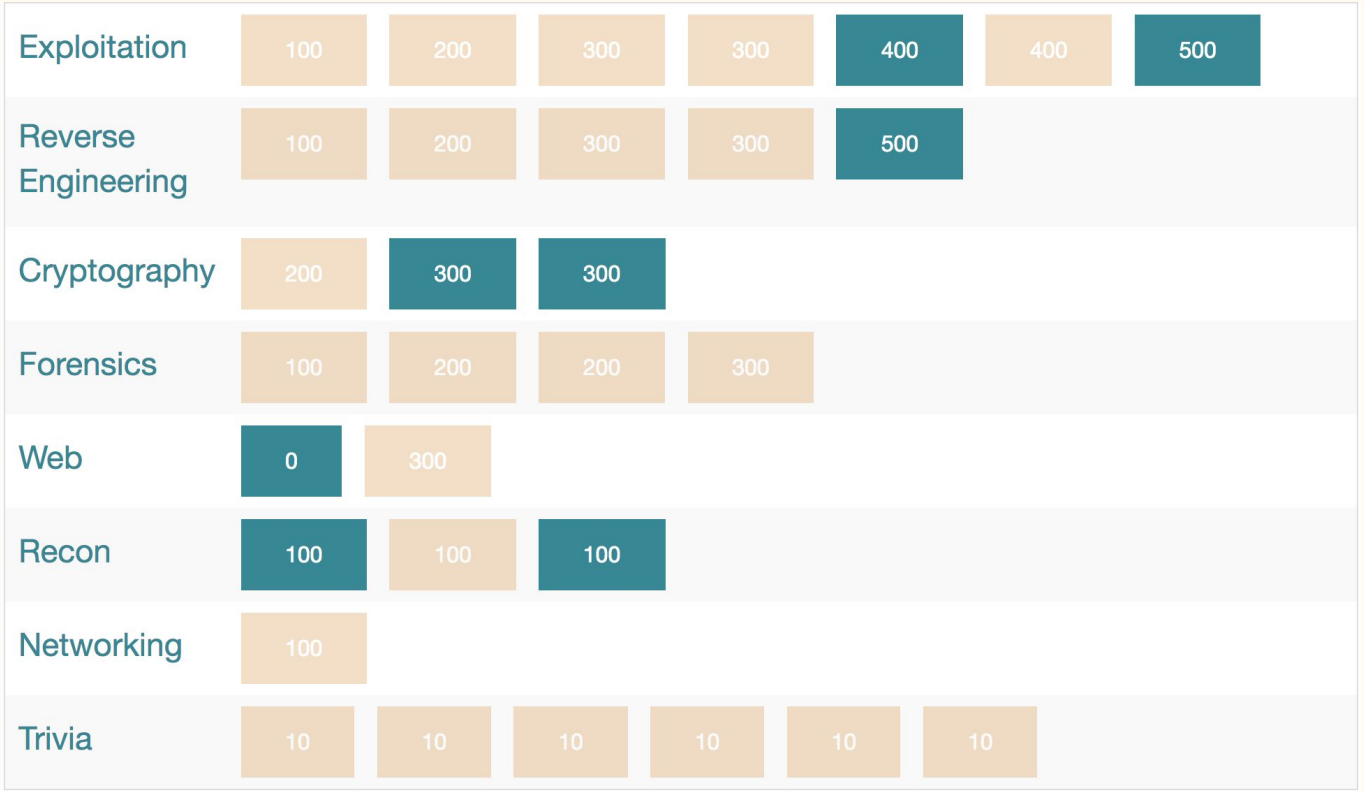
- O que é CTF e afins
- Tipos de CTF
- CTFtime
- Jeopardy e seus challenges
- Considerações finais
- Alguns challenges!

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.

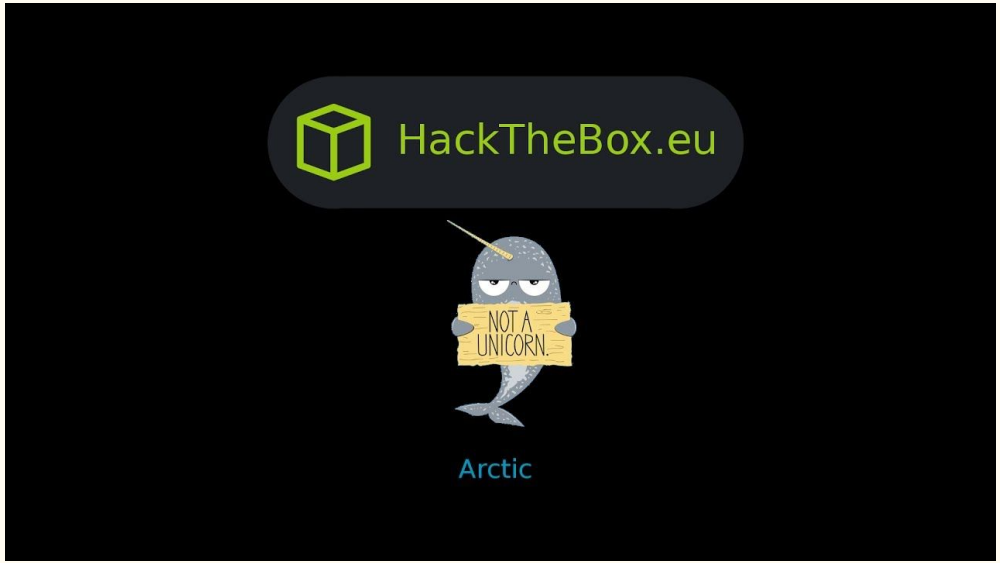
PS: Don't get caught, the robots don't take prisoners.

Key

SUBMIT

Attack and Defense

Boot2root



VULNHUB

VULNERABLE BY DESIGN

CTF Events

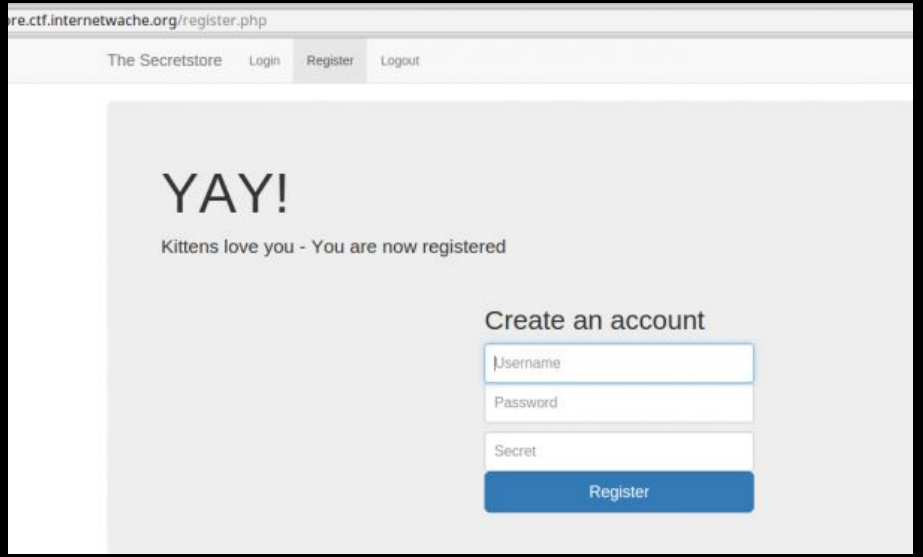
All | Upcoming | Archive | Format | Year

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

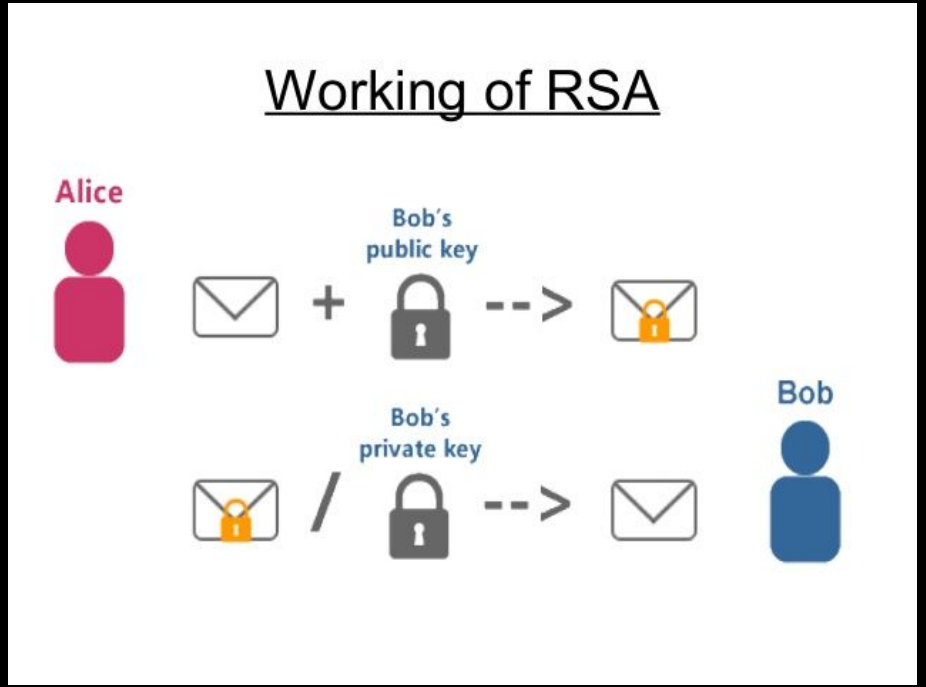
- Quanto mais se conhecer as aplicações web, melhor
- Ajuda muito com a realização de pentests



Workshop Time

Cryptography

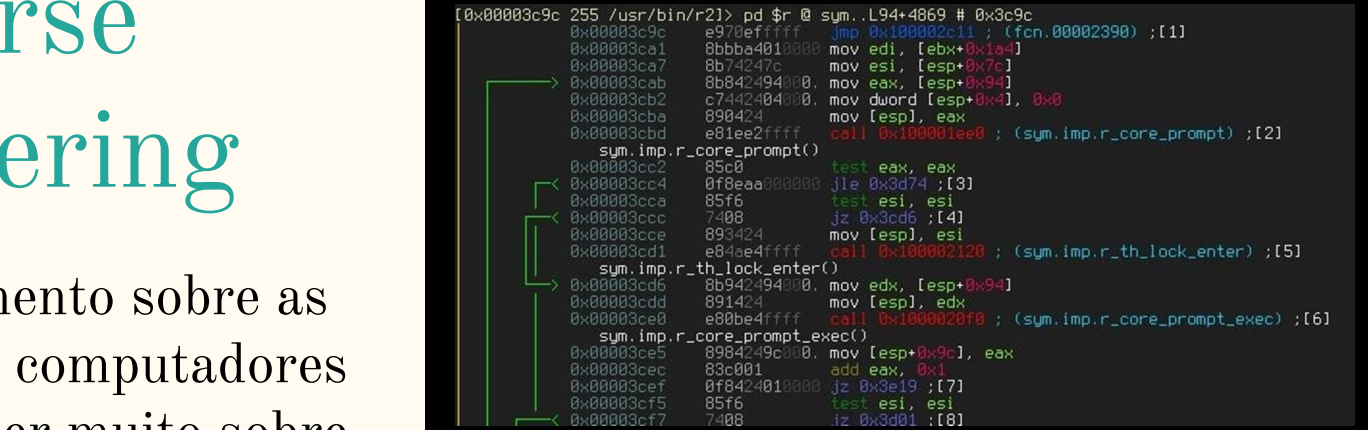
- Aborda os principais ataques conhecidos a criptografias
- É ótimo para quem gosta de matemática e programar soluções



Workshop Time

Reverse Engineering

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



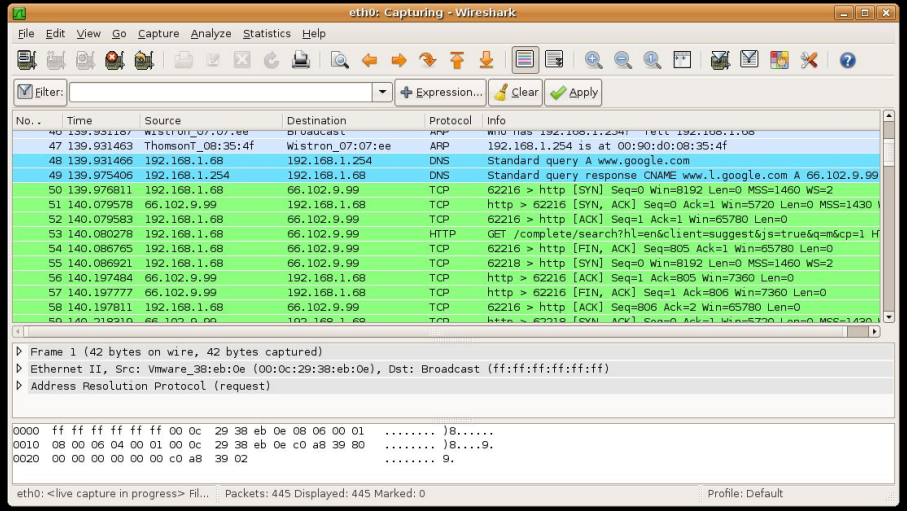
Workshop Time

Pwn

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

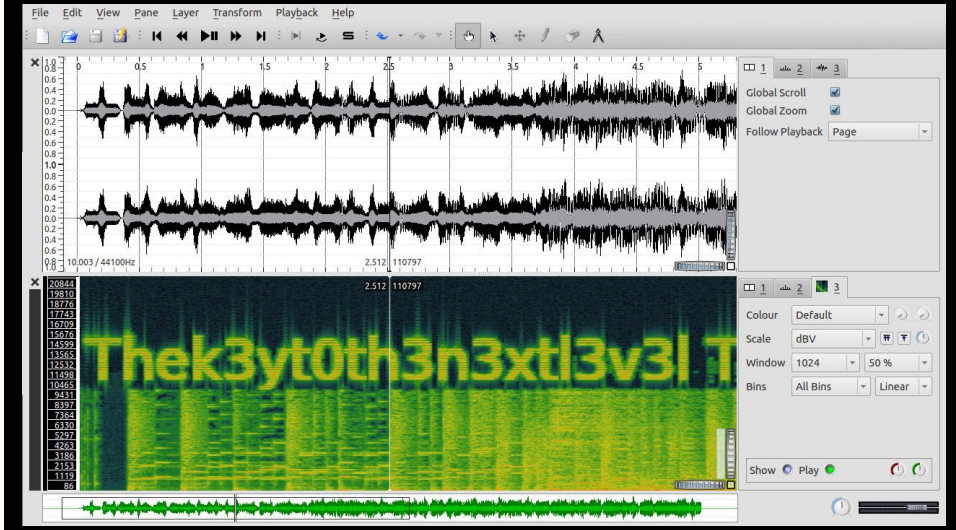
Network

- 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!