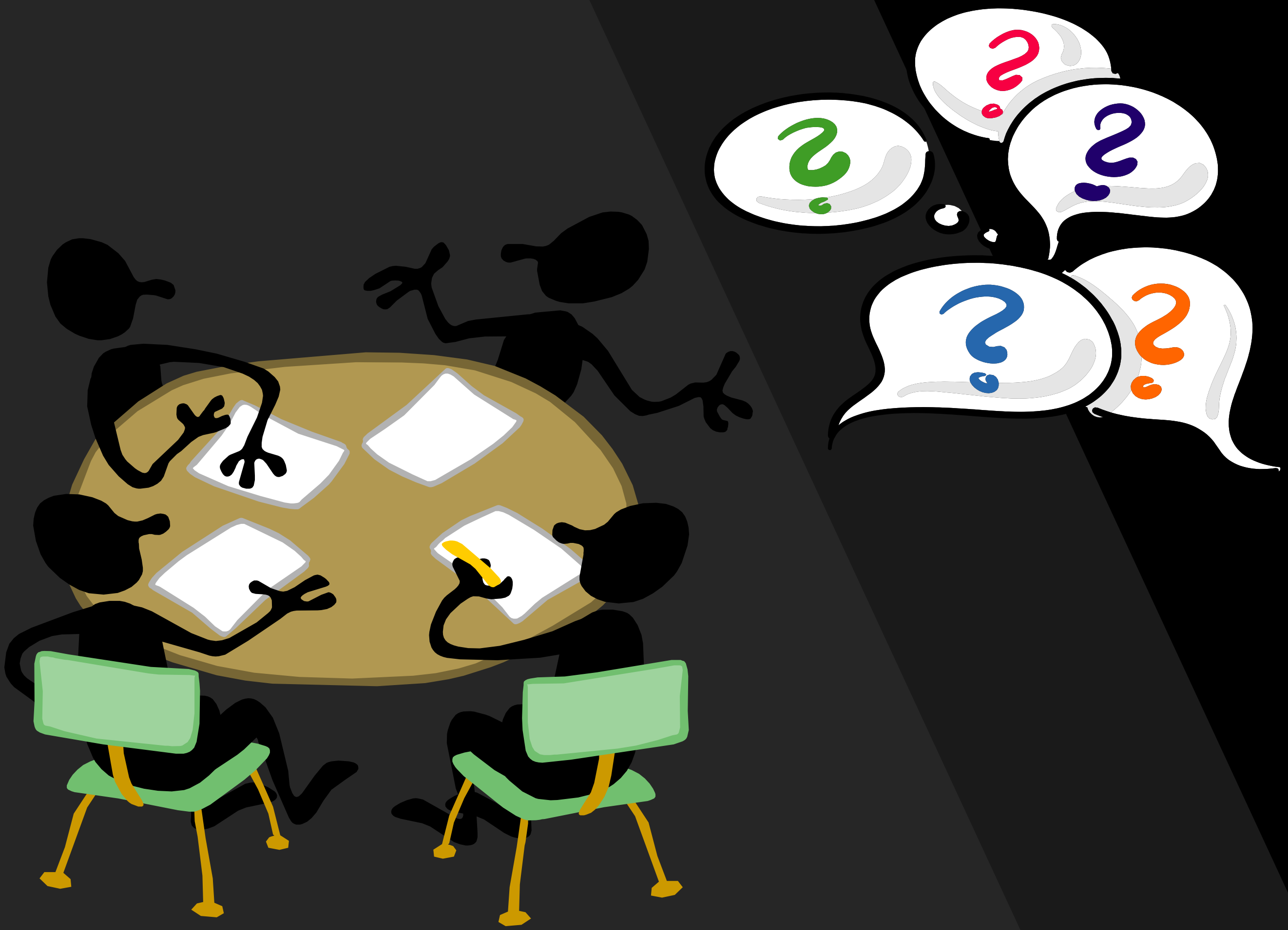
CTF 101

Jose Moruno Cadima
DreamLab Technologies

Y ahora esta charla?



8.8

Jose Moruno Cadima
sniferl4bs@gmail.com

OFFENSIVE® security OSWP

eJPT

www.sniferl4bs.com

sniferl4bs

¿Donde trabajo ?

DREAMLAB
TECHNOLOGIES
DON´T GUESS. KNOW.

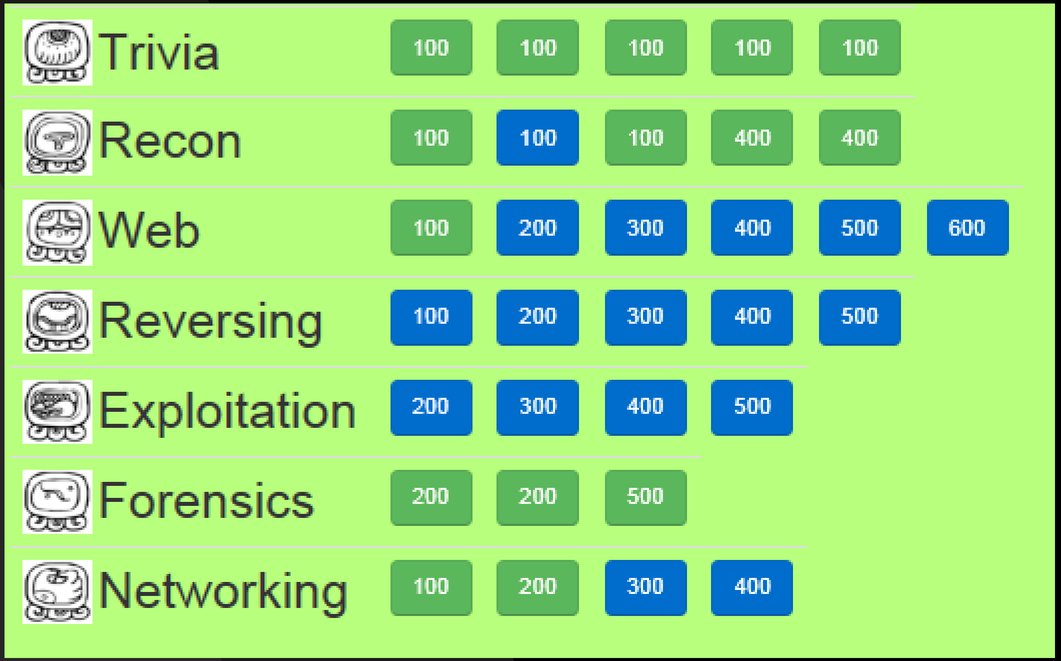
8.8

¿Que es un CTF?

- Jeopardy
- Ataque-defensa
- Mixtos.

CAMINO AL CTF...

Jeopardy



Trivia	100	100	100	100	100	
Recon	100	100	100	400	400	
Web	100	200	300	400	500	600
Reversing	100	200	300	400	500	
Exploitation	200	300	400	500		
Forensics	200	200	500			
Networking	100	200	300	400		

String

Flag [Formato]

8.8

Ataque y defensa

Fix de vulnerabilidades

Flag [Formato]

8.8

DEFCON

Este fue uno de los primeros CTF que se realizaron en el evento

https://www.defcon.org/html/links/dc-ctf.html

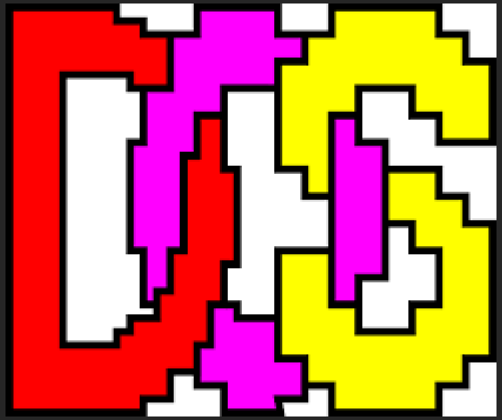
CTF’s Mixtos

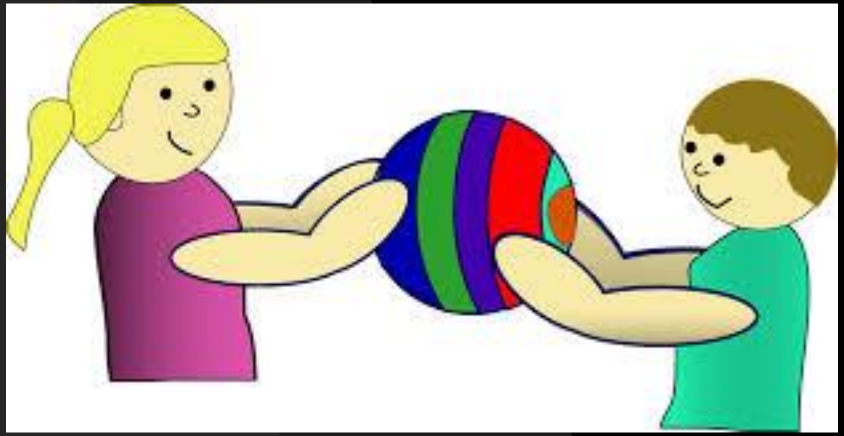
“King of the hill”

Rey de la Colina

Ataque o defensa
Liberan pistas Flags a obtener.

Reglas - Normas





8.8

CONSEJOS…

Donde buscar…

Piensa en lo básico...

Donde encontramos mas retos

http://captf.com/calendar/

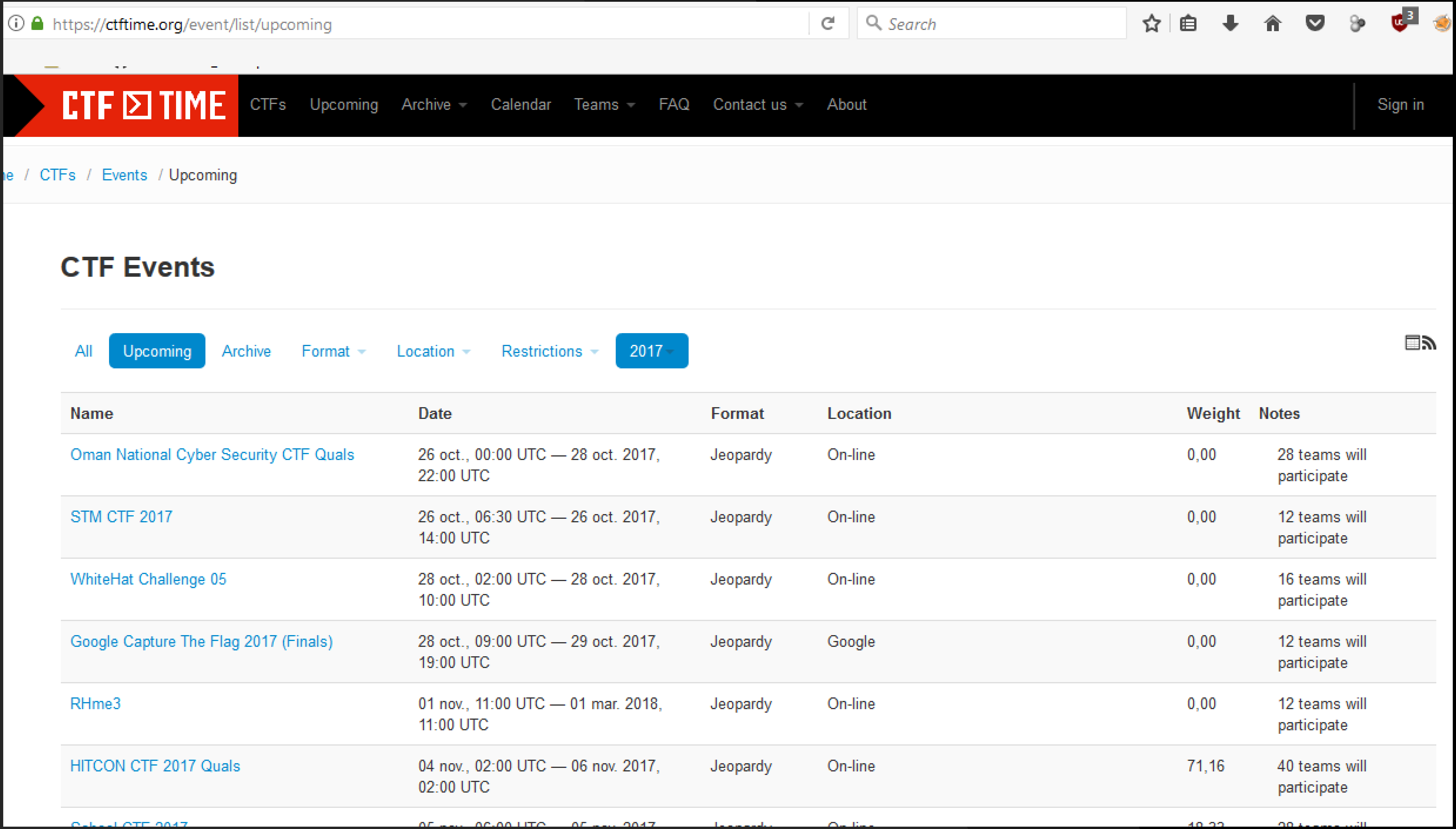
Google :D

DuckDuckGo :D

https://ctftime.org/event/list/upcoming

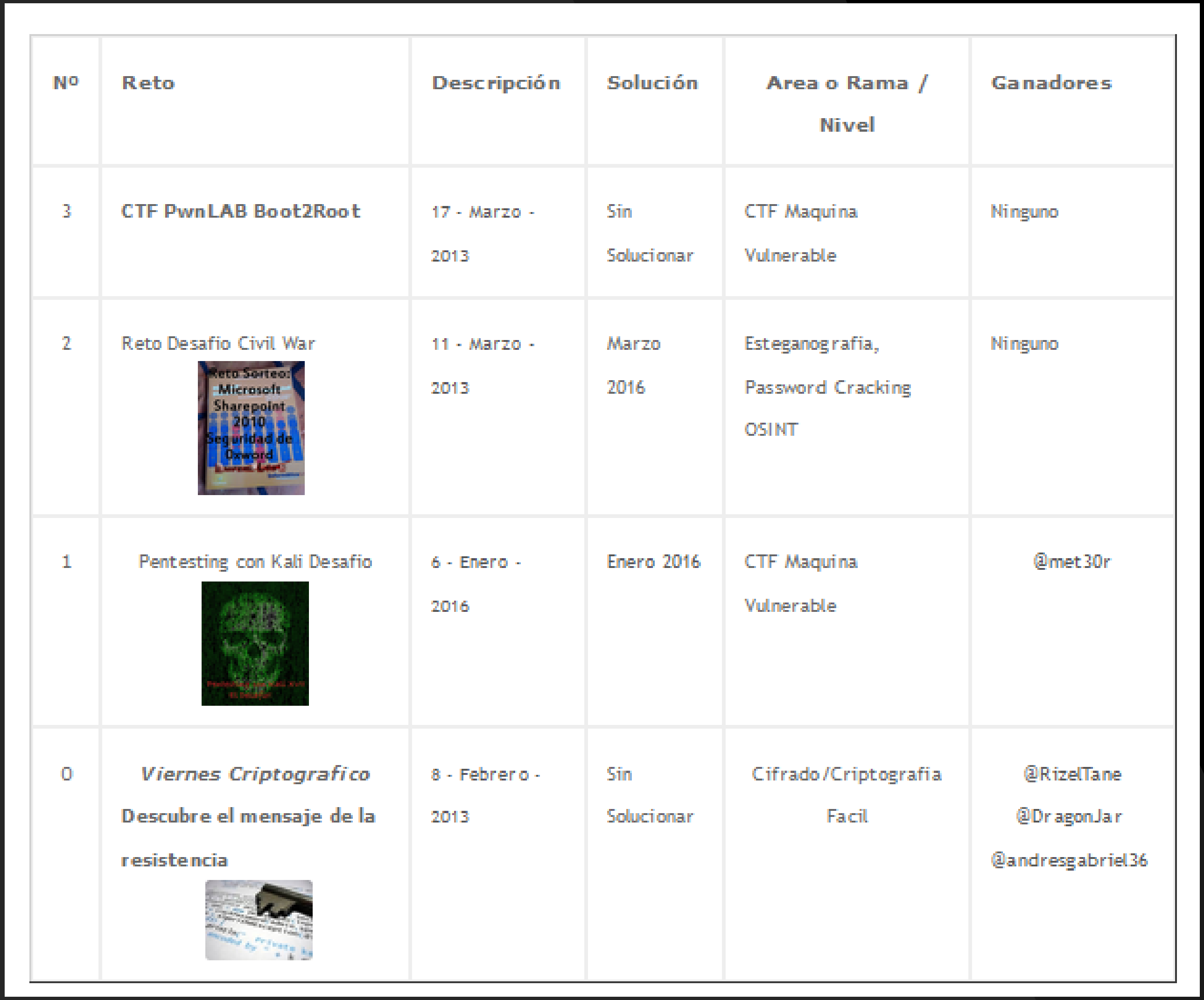
https://www.vulnhub.com/

http://captf.com/practice-ctf/



CTF Events

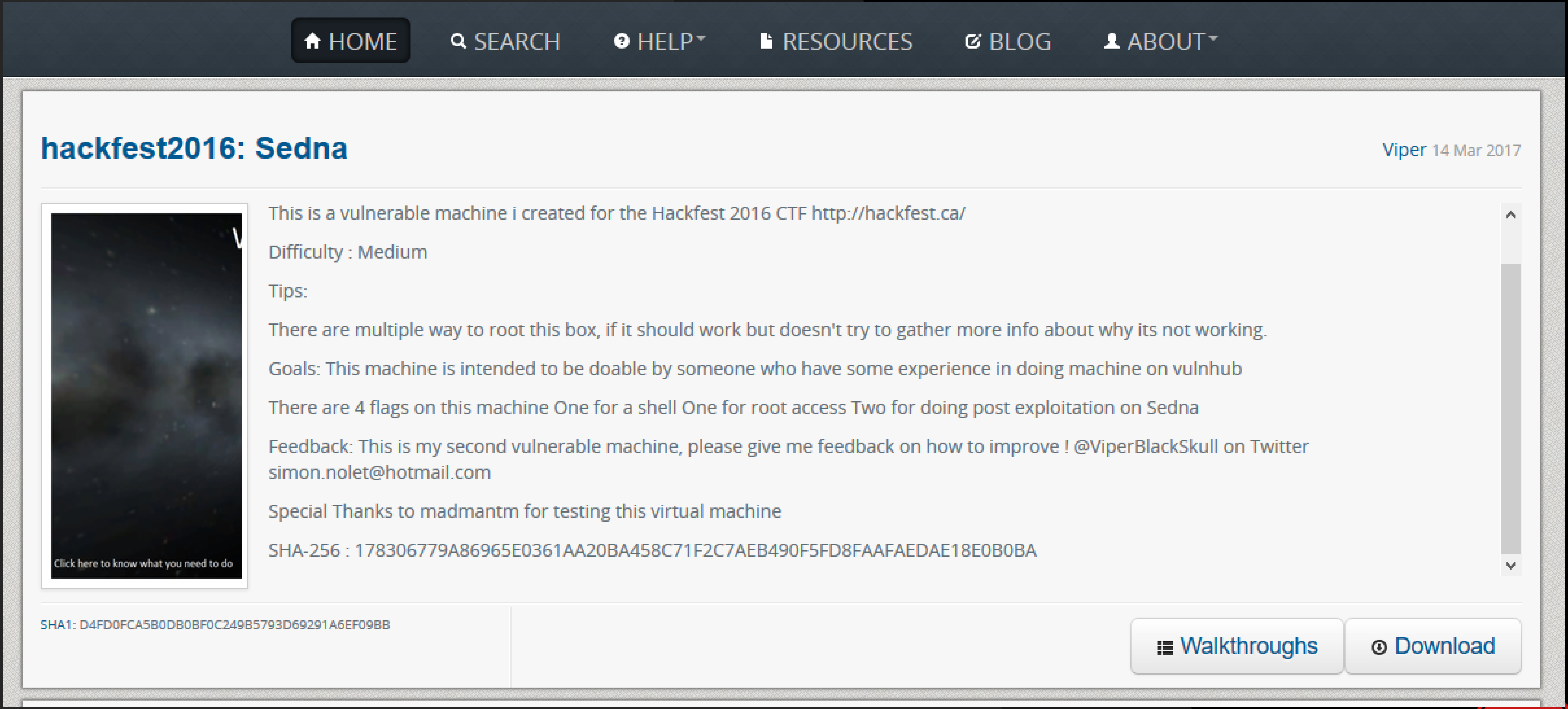
Name	Date	Format	Location	Weight	Notes
Oman National Cyber Security CTF Quals	26 oct., 00:00 UTC — 28 oct. 2017, 22:00 UTC	Jeopardy	On-line	0,00	28 teams will participate
STM CTF 2017	26 oct., 06:30 UTC — 26 oct. 2017, 14:00 UTC	Jeopardy	On-line	0,00	12 teams will participate
WhiteHat Challenge 05	28 oct., 02:00 UTC — 28 oct. 2017, 10:00 UTC	Jeopardy	On-line	0,00	16 teams will participate
Google Capture The Flag 2017 (Finals)	28 oct., 09:00 UTC — 29 oct. 2017, 19:00 UTC	Jeopardy	Google	0,00	12 teams will participate
RHme3	01 nov., 11:00 UTC — 01 mar. 2018, 11:00 UTC	Jeopardy	On-line	0,00	12 teams will participate
HITCON CTF 2017 Quals	04 nov., 02:00 UTC — 06 nov. 2017, 02:00 UTC	Jeopardy	On-line	71,16	40 teams will participate
School CTF 2017	05 nov., 06:00 UTC — 05 nov. 2017,	Jeopardy	On-line	18,33	28 teams will



Nº	Reto	Descripción	Solución	Area o Rama / Nivel	Ganadores
3	**CTF PwnLAB Boot2Root**	17 - Marzo - 2013	Sin Solucionar	CTF Maquina Vulnerable	Ninguno
2	Reto Desafio Civil War	11 - Marzo - 2013	Marzo 2016	Esteganografia, Password Cracking OSINT	Ninguno
1	Pentesting con Kali Desafio	6 - Enero - 2016	Enero 2016	CTF Maquina Vulnerable	@met30r
0	***Viernes Criptografico*** **Descubre el mensaje de la resistencia**	8 - Febrero - 2013	Sin Solucionar	Cifrado/Criptografia Facil	@RizelTane @DragonJar @andresgabriel36

http://www.sniferl4bs.com/p/blog-page_25.html

Vulnhub



hackfest2016: Sedna

Viper 14 Mar 2017

This is a vulnerable machine i created for the Hackfest 2016 CTF http://hackfest.ca/

Difficulty : Medium

Tips:

There are multiple way to root this box, if it should work but doesn't try to gather more info about why its not working.

Goals: This machine is intended to be doable by someone who have some experience in doing machine on vulnhub

There are 4 flags on this machine One for a shell One for root access Two for doing post exploitation on Sedna

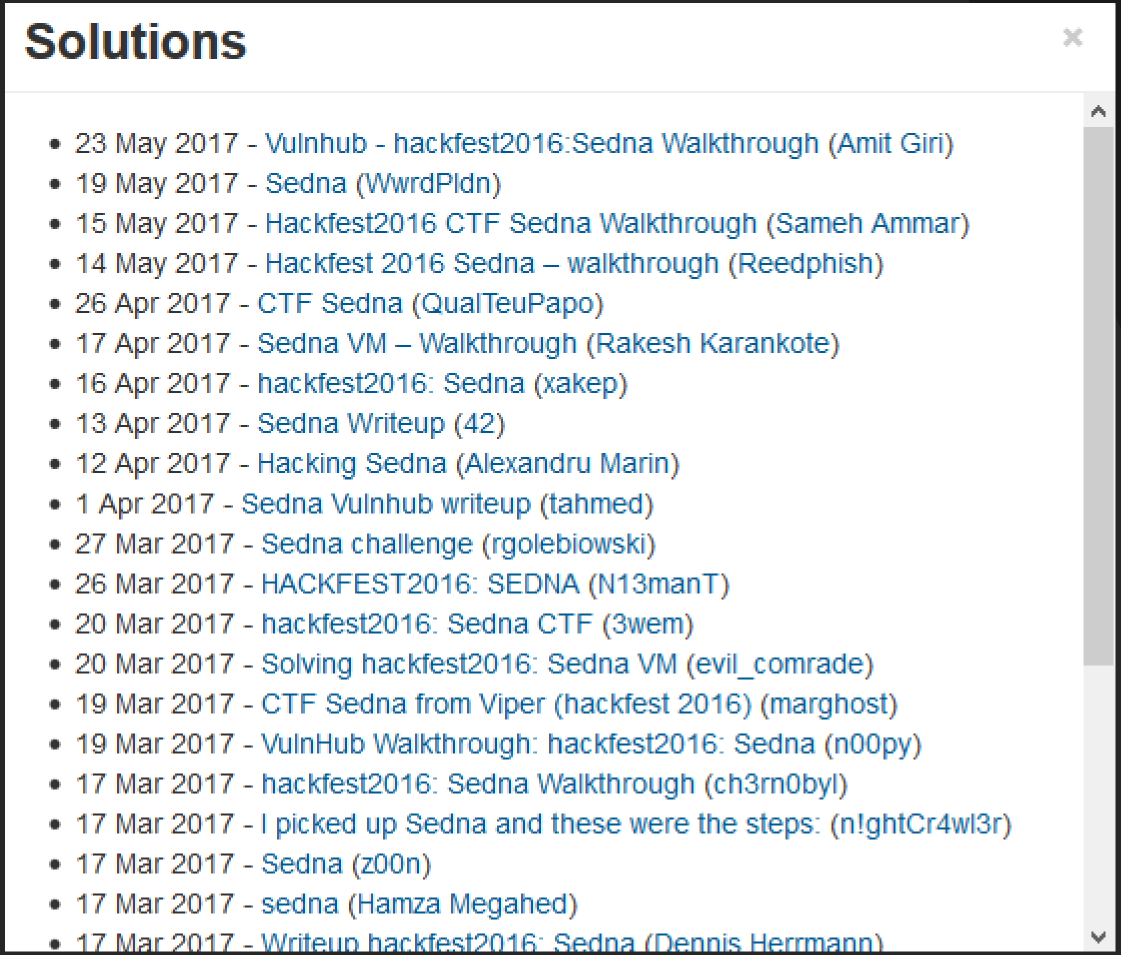
Feedback: This is my second vulnerable machine, please give me feedback on how to improve ! @ViperBlackSkull on Twitter simon.nolet@hotmail.com

Special Thanks to madmantm for testing this virtual machine

SHA-256 : 178306779A86965E0361AA20BA458C71F2C7AEB490F5FD8FAAFAEDAE18E0B0BA

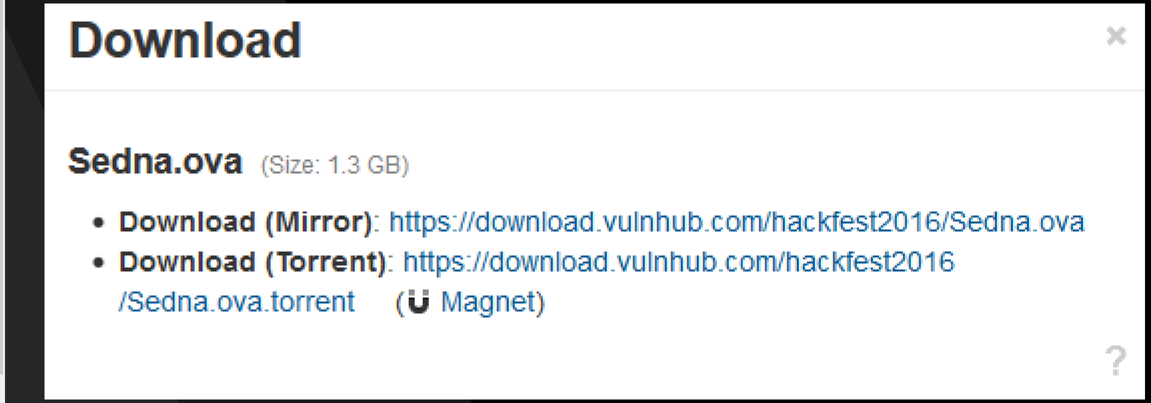
SHA1: D4FD0FCA5B0DB0BF0C249B5793D69291A6EF09BB

Vulnhub



Solutions

- 23 May 2017 - Vulnhub - hackfest2016:Sedna Walkthrough (Amit Giri)
- 19 May 2017 - Sedna (WwrdPldn)
- 15 May 2017 - Hackfest2016 CTF Sedna Walkthrough (Sameh Ammar)
- 14 May 2017 - Hackfest 2016 Sedna – walkthrough (Reedphish)
- 26 Apr 2017 - CTF Sedna (QualTeuPapo)
- 17 Apr 2017 - Sedna VM – Walkthrough (Rakesh Karankote)
- 16 Apr 2017 - hackfest2016: Sedna (xakep)
- 13 Apr 2017 - Sedna Writeup (42)
- 12 Apr 2017 - Hacking Sedna (Alexandru Marin)
- 1 Apr 2017 - Sedna Vulnhub writeup (tahmed)
- 27 Mar 2017 - Sedna challenge (rgolebiowski)
- 26 Mar 2017 - HACKFEST2016: SEDNA (N13manT)
- 20 Mar 2017 - hackfest2016: Sedna CTF (3wem)
- 20 Mar 2017 - Solving hackfest2016: Sedna VM (evil_comrade)
- 19 Mar 2017 - CTF Sedna from Viper (hackfest 2016) (marghost)
- 19 Mar 2017 - VulnHub Walkthrough: hackfest2016: Sedna (n00py)
- 17 Mar 2017 - hackfest2016: Sedna Walkthrough (ch3rn0byl)
- 17 Mar 2017 - I picked up Sedna and these were the steps: (n!ghtCr4wl3r)
- 17 Mar 2017 - Sedna (z00n)
- 17 Mar 2017 - sedna (Hamza Megahed)
- 17 Mar 2017 - Writeup hackfest2016: Sedna (Dennis Herrmann)



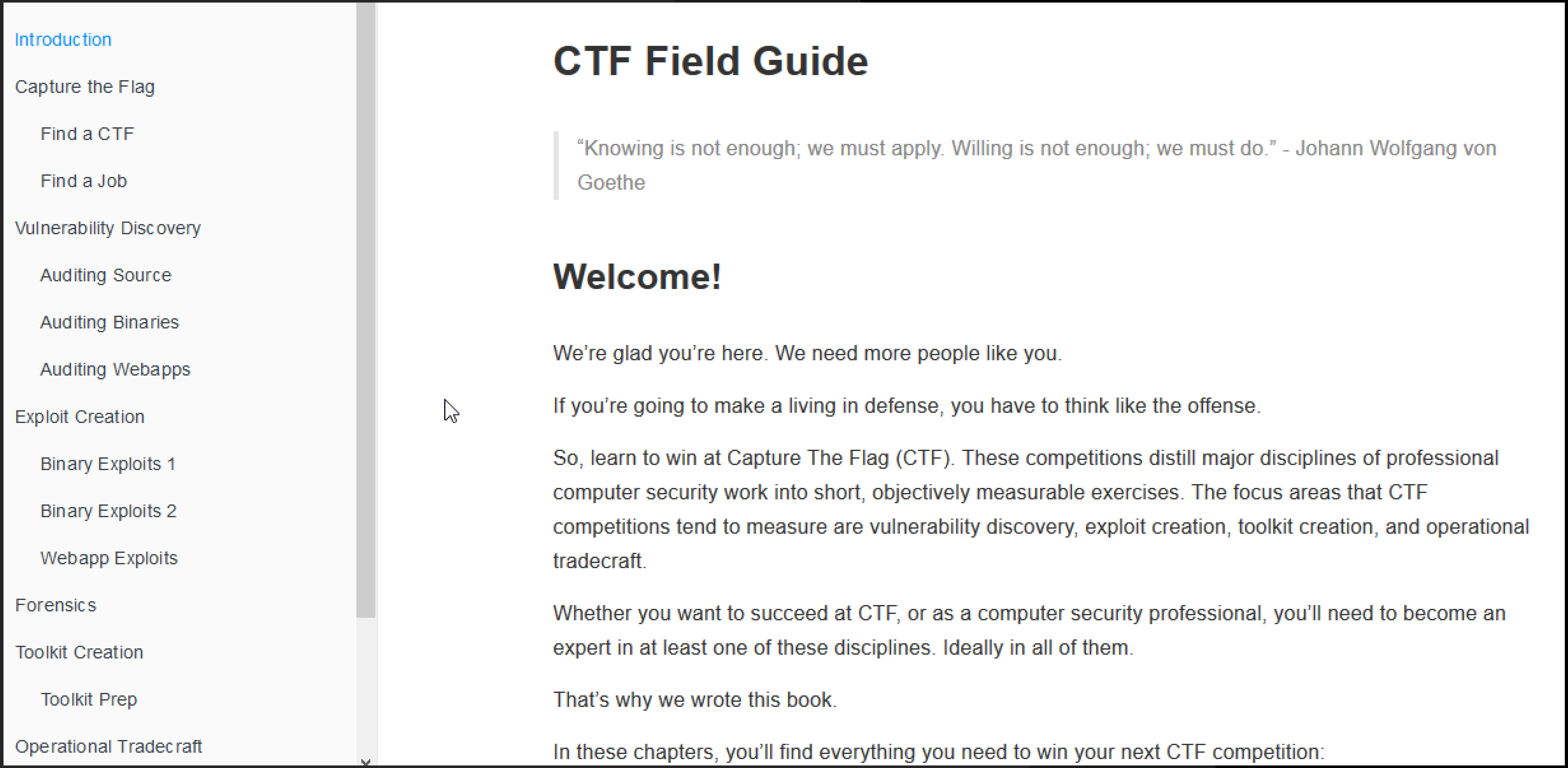
Download

Sedna.ova (Size: 1.3 GB)

- **Download (Mirror)**: https://download.vulnhub.com/hackfest2016/Sedna.ova
- **Download (Torrent)**: https://download.vulnhub.com/hackfest2016/Sedna.ova.torrent (Magnet)

CTF Field Guide

https://trailofbits.github.io/ctf/



CTF Field Guide

> “Knowing is not enough; we must apply. Willing is not enough; we must do.” - Johann Wolfgang von Goethe

Welcome!

We’re glad you’re here. We need more people like you.

If you’re going to make a living in defense, you have to think like the offense.

So, learn to win at Capture The Flag (CTF). These competitions distill major disciplines of professional computer security work into short, objectively measurable exercises. The focus areas that CTF competitions tend to measure are vulnerability discovery, exploit creation, toolkit creation, and operational tradecraft.

Whether you want to succeed at CTF, or as a computer security professional, you’ll need to become an expert in at least one of these disciplines. Ideally in all of them.

That’s why we wrote this book.

In these chapters, you’ll find everything you need to win your next CTF competition:

La teoría es buena, pero con práctica es mucho mejor!