CTF: WTF?!

Capture The Flag für Einsteiger

Dr. Hubert 'hubertf' Feyrer
Dezember 2024

38. Chaos Communications Congress (38C3), Hamburg

Zusammenfassung

"Hacken" ist längst nicht mehr nur Hobby. WTF? CTF!

Was ist ein "Capture The Flag", wie passt das in die aktuelle Menge aus Security Buzzwords, welchen Nutzen kann ich daraus ziehen und wie fange ich an?
Es werden ein paar einfache Plattformen und Veranstaltungen zum starten und üben gezeigt. Dem folgen Spielarten, Wege "hacken" zu lernen, und ein Ausblick auf berufliche Möglichkeiten.

Der Vortrag richtet sich an Einsteiger.

hubertf - Dr. Hubert Feyrer

fun	Betriebssysteme (NetBSD), Open Source (pkgsrc), IT-/Information Security, Capture the Flag, Geocaching Erster 3C Congress Vortrag vor 20 Jahren
profit	Cyber Security, Information Security, IT-Security Product Security
contact	EMail: hubertf@gmx.de Others: @hubertf / @huberteff / @hubertf@mastdodon.social

Inhalt

Einführung - Sicherheit, Schutz

Verteidigung - Checklisten, Technik

Angriff - Wozu, wie lernen

CTF - Wo anfangen? - Try Hack Me, Over The Wire, weitere & Veranstaltungen

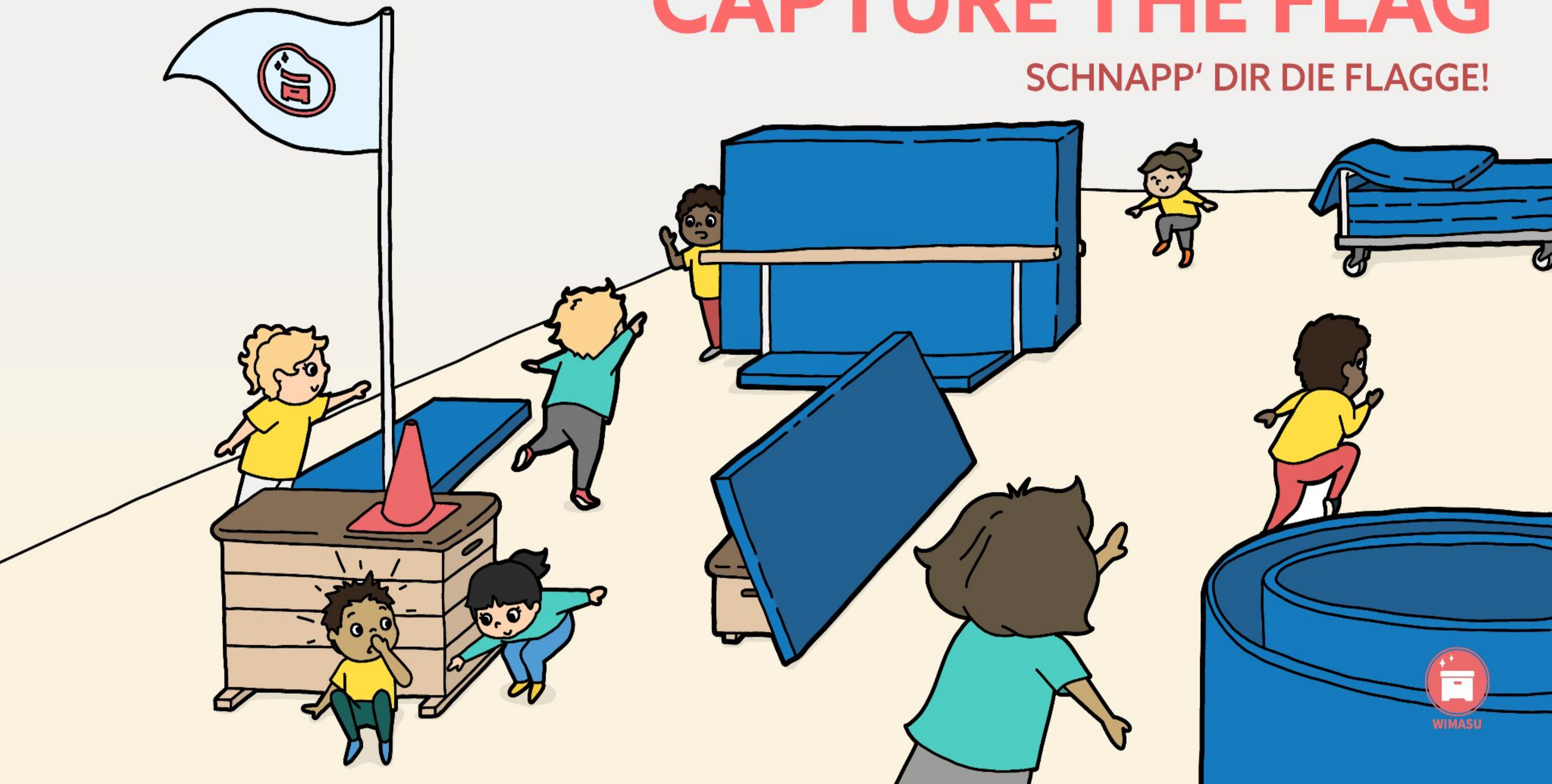
CTF - Arten, Tools

Was kommt dann? - Anfangen, Karrierepfade

Einführung

CAPTURE THE FLAG

SCHNAPP' DIR DIE FLAGGE!



Einführung

Einführung

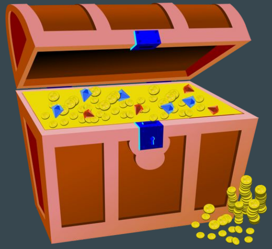
I WANT TO WORK IN CYBER
SECURITY FUNDAMENTALS
SYSTEMS FUNDAMENTALS
NETWORKING FUNDAMENTALS

Einführung - Sicherheit

Wert - Asset

Bedrohung

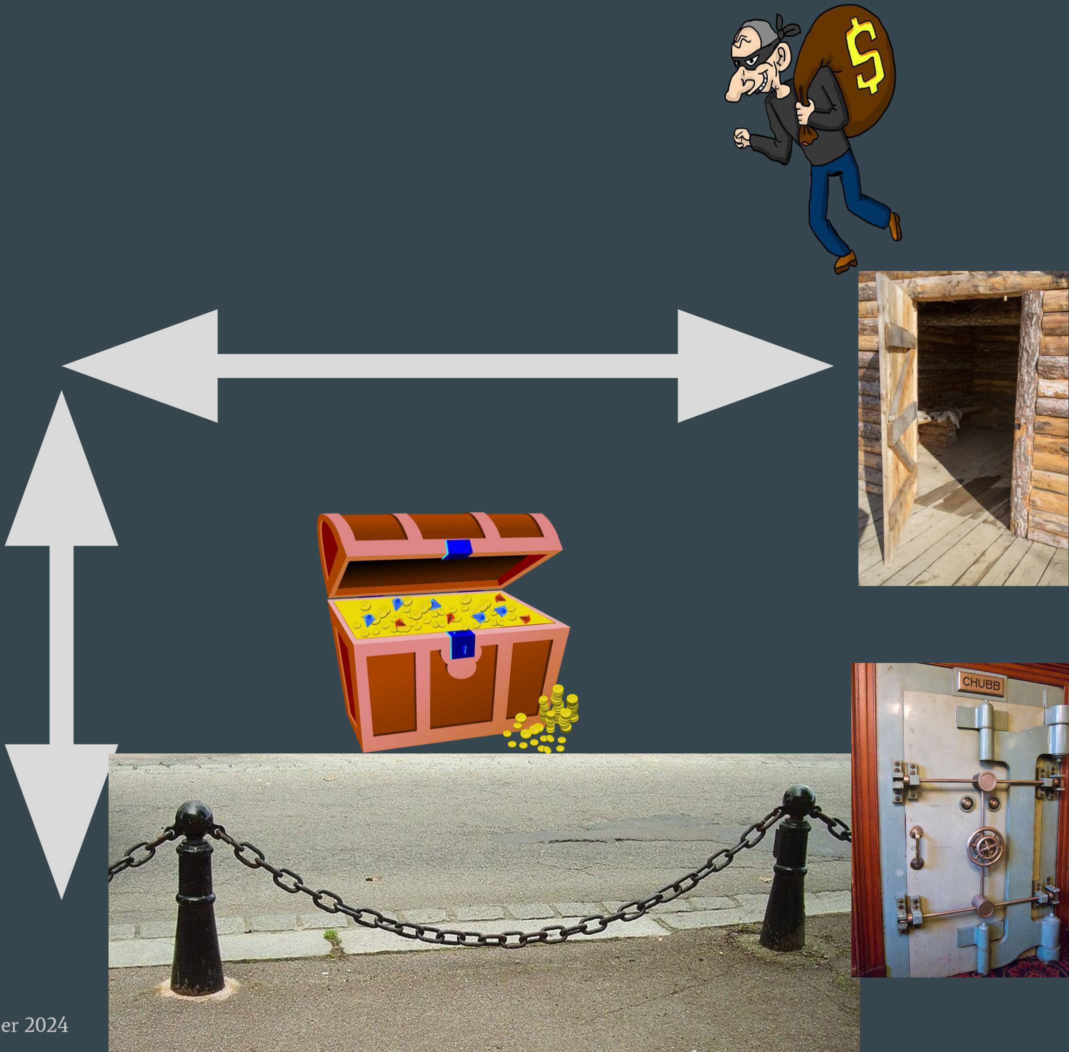
Schutz



Einführung - Schutz

Breite

Tiefe

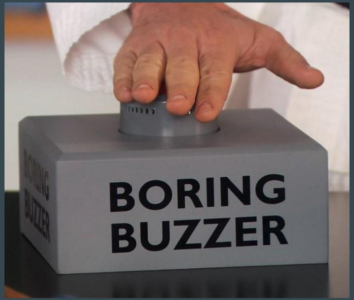


Verteidigung

Verteidigung - Checklisten

Technik & (viel) Organisation

Gesetze	Datenschutz - DSGVO
	Kritische Infrastruktur - NIS-2
	Produkte - Cyber Resilience Act
Standards	National: BSI Grundschutz, US NIST
	International: ISO 27001
	Organisationsintern - "Best Practice"



Verteidigung - Technik

Erkennung - Logfiles

Auswertung & Analyse

Nachverfolgung

=> Cyber Threat Intelligence (TI/CTI)

=> Indicators of Compromise (IoC)

=> Threat Hunting (TH)

=> Incident Response (IR)

=> Security Operations Center (SOC)

NSOC watch floor circa 1985

Angriff

Angriff

- Finden und ausnutzen von Schwachstellen -> Technische Tiefe

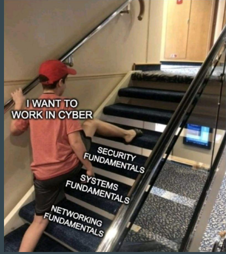
- Wozu?
  - Angriffe erkennen -> Blue Teaming, Threat Hunting
  - Angriffe verhindern / verfolgen -> Sicherheit, Cyber Crime, Attribution
  - Produkte verbessern -> Pentesting

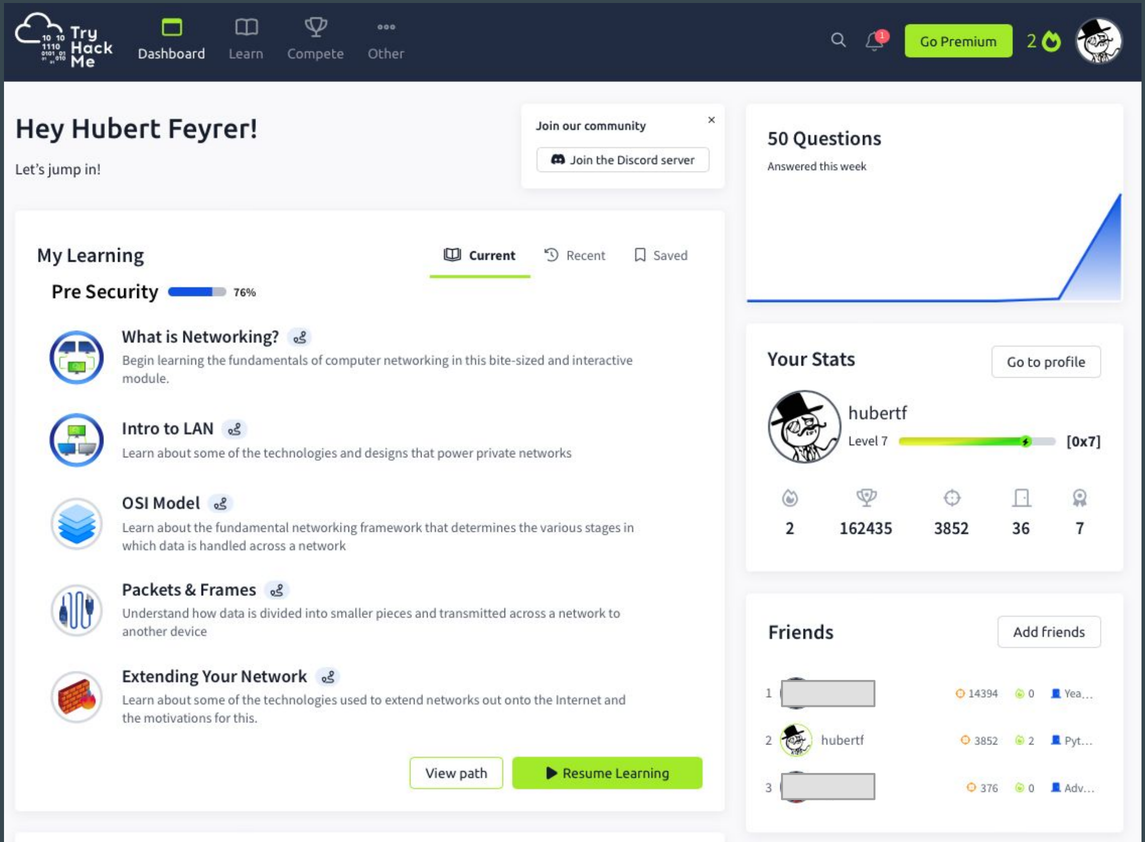
- Wie lernen?[1]
  - Lesen -> passiv,behavioristisches Lernmodell = gut für einfache Themen
  - Üben -> aktiv, konstruktivistisches Lernmodell = gut für komplexe Themen
  - Übungen: Cyber Ranges, Capture The Flag (CTF)

[1] Feyrer: System Administration Training in the Virtual Unix Lab, 2008; https://www.feyrer.de/vulab/

CTF - wo anfangen?

Anfangen: Try Hack Me





Hey Hubert Feyrer!

Let's jump in!

Join our community

Join the Discord server

50 Questions

Answered this week

My Learning

Current · Recent · Saved

Pre Security 76%

What is Networking?
Begin learning the fundamentals of computer networking in this bite-sized and interactive module.

Intro to LAN
Learn about some of the technologies and designs that power private networks

OSI Model
Learn about the fundamental networking framework that determines the various stages in which data is handled across a network

Packets & Frames
Understand how data is divided into smaller pieces and transmitted across a network to another device

Extending Your Network
Learn about some of the technologies used to extend networks out onto the Internet and the motivations for this.

View path · Resume Learning

Your Stats

Go to profile

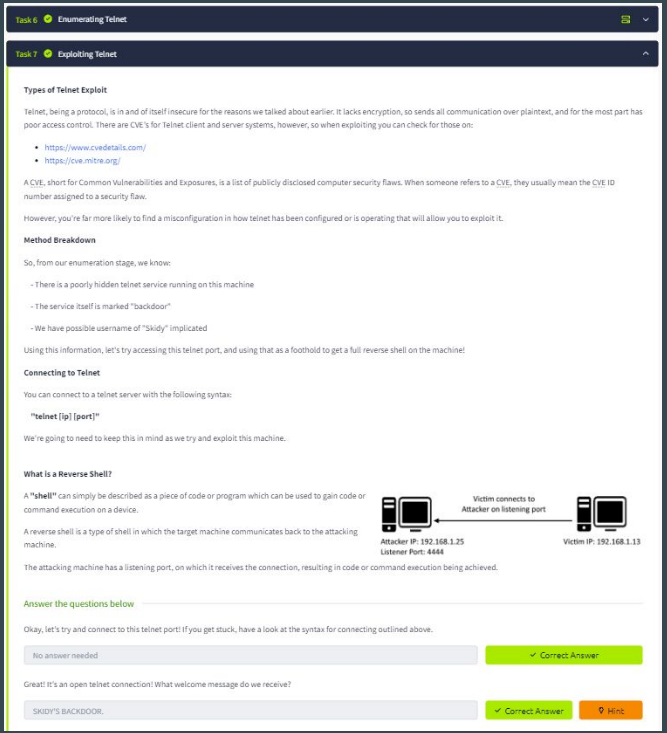
hubertf
Level 7 [0x7]

2 · 162435 · 3852 · 36 · 7

Friends

Add friends

1	[redacted]	14394	0	Yea...
2	hubertf	3852	2	Pyt...
3	[redacted]	376	0	Adv...



Victim connects to Attacker on listening port
Attacker IP: 192.168.1.25
Listener Port: 4444
Victim IP: 192.168.1.13

Task 6 Enumerating Telnet

Task 7 Exploiting Telnet

Types of Telnet Exploit

Telnet, being a protocol, is in and of itself insecure for the reasons we talked about earlier. It lacks encryption, so sends all communication over plaintext, and for the most part has poor access control. There are CVE's for Telnet client and server systems, however, so when exploiting you can check for those on:

- https://www.cvedetails.com/
- https://cve.mitre.org/

A CVE, short for Common Vulnerabilities and Exposures, is a list of publicly disclosed computer security flaws. When someone refers to a CVE, they usually mean the CVE ID number assigned to a security flaw.

However, you're far more likely to find a misconfiguration in how telnet has been configured or is operating that will allow you to exploit it.

Method Breakdown

So, from our enumeration stage, we know:

- There is a poorly hidden telnet service running on this machine

- The service itself is marked "backdoor"

- We have possible username of "Skidy" implicated

Using this information, let's try accessing this telnet port, and using that as a foothold to get a full reverse shell on the machine!

Connecting to Telnet

You can connect to a telnet server with the following syntax:

```
"telnet [ip] [port]"
```

We're going to need to keep this in mind as we try and exploit this machine.

What is a Reverse Shell?

A **"shell"** can simply be described as a piece of code or program which can be used to gain code or command execution on a device.

A reverse shell is a type of shell in which the target machine communicates back to the attacking machine.

The attacking machine has a listening port, on which it receives the connection, resulting in code or command execution being achieved.

Answer the questions below

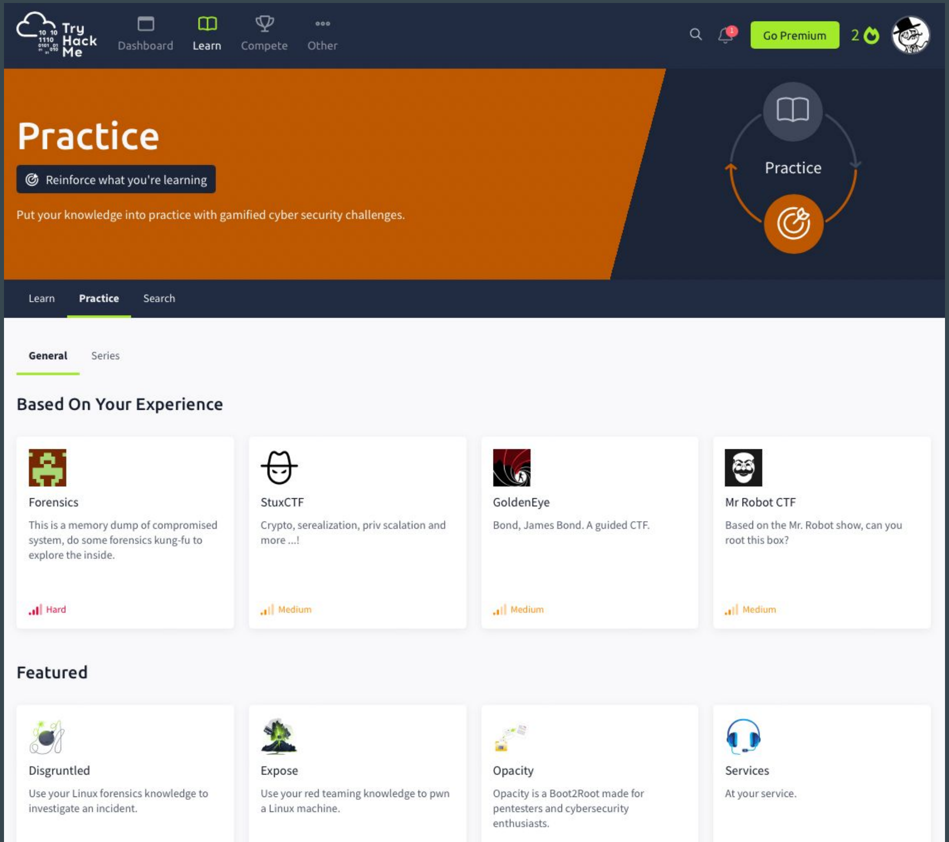
Okay, let's try and connect to this telnet port! If you get stuck, have a look at the syntax for connecting outlined above.

No answer needed ✓ Correct Answer

Great! It's an open telnet connection! What welcome message do we receive?

SKIDY'S BACKDOOR. ✓ Correct Answer Hint

Anfangen: Try Hack Me



Practice

Reinforce what you're learning

Put your knowledge into practice with gamified cyber security challenges.

Based On Your Experience

Forensics
This is a memory dump of compromised system, do some forensics kung-fu to explore the inside.
Hard

StuxCTF
Crypto, serealization, priv scalation and more ...!
Medium

GoldenEye
Bond, James Bond. A guided CTF.
Medium

Mr Robot CTF
Based on the Mr. Robot show, can you root this box?
Medium

Featured

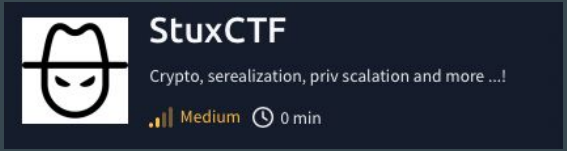
Disgruntled
Use your Linux forensics knowledge to investigate an incident.

Expose
Use your red teaming knowledge to pwn a Linux machine.

Opacity
Opacity is a Boot2Root made for pentesters and cybersecurity enthusiasts.

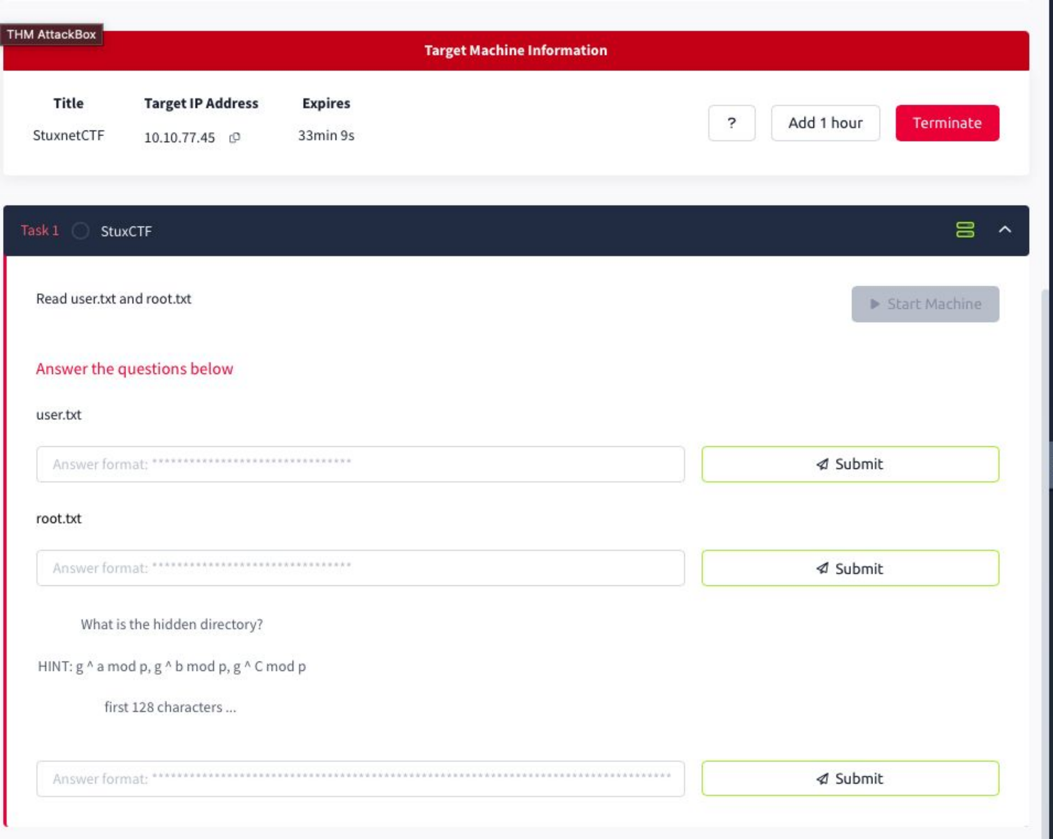
Services
At your service.

Anfangen: Try Hack Me



StuxCTF

Crypto, serealization, priv scalation and more ...!



Target Machine Information

Title	Target IP Address	Expires
StuxnetCTF	10.10.77.45	33min 9s

Task 1 ○ StuxCTF

Read user.txt and root.txt

Answer the questions below

user.txt

Answer format: ********************************

root.txt

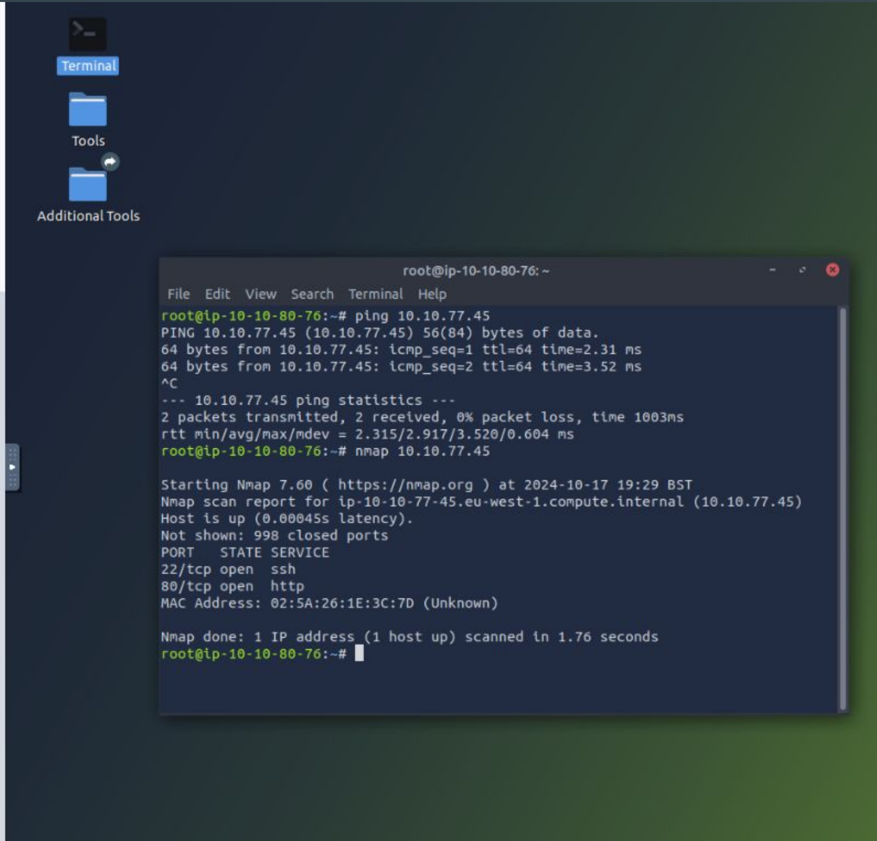
Answer format: ********************************

What is the hidden directory?

HINT: g ^ a mod p, g ^ b mod p, g ^ C mod p

first 128 characters ...

Answer format: **

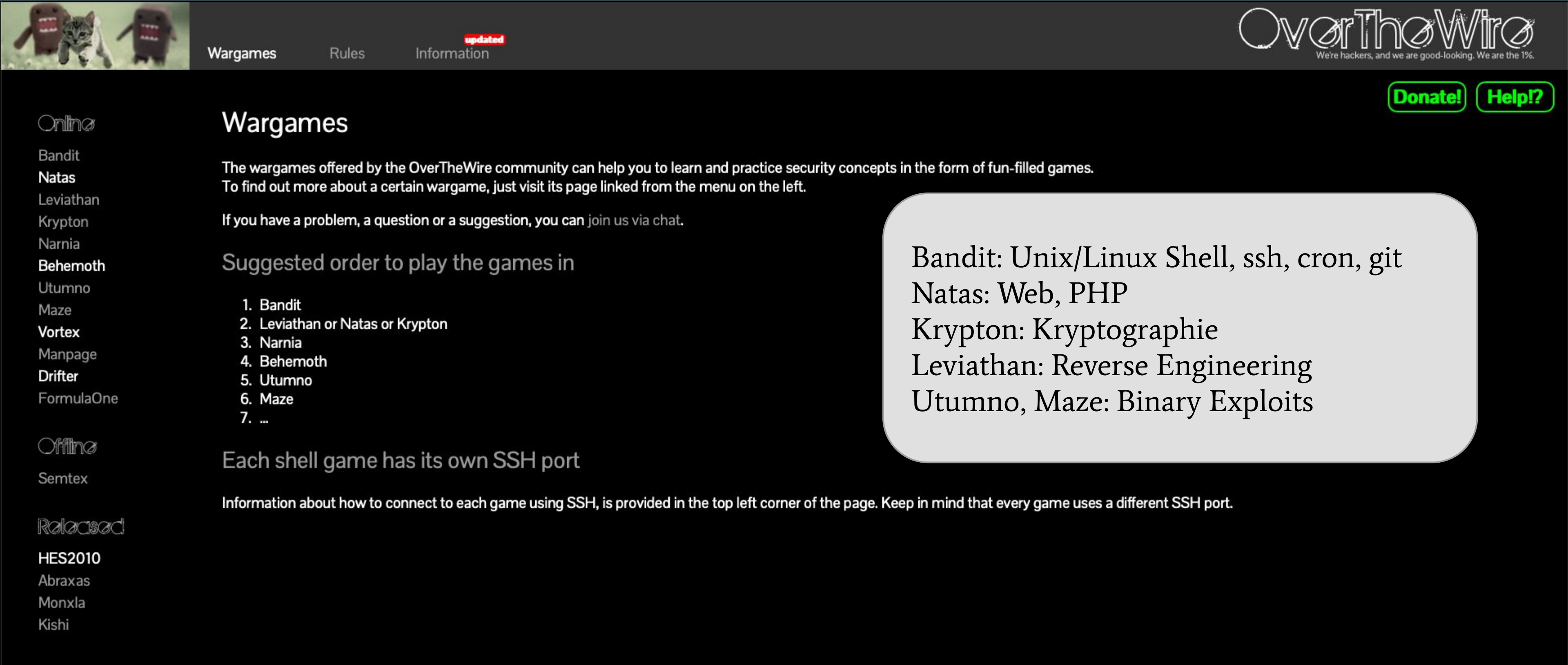


```
root@ip-10-10-80-76:~# ping 10.10.77.45
PING 10.10.77.45 (10.10.77.45) 56(84) bytes of data.
64 bytes from 10.10.77.45: icmp_seq=1 ttl=64 time=2.31 ms
64 bytes from 10.10.77.45: icmp_seq=2 ttl=64 time=3.52 ms
^C
--- 10.10.77.45 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 2.315/2.917/3.520/0.604 ms
root@ip-10-10-80-76:~# nmap 10.10.77.45

Starting Nmap 7.60 ( https://nmap.org ) at 2024-10-17 19:29 BST
Nmap scan report for ip-10-10-77-45.eu-west-1.compute.internal (10.10.77.45)
Host is up (0.00045s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 02:5A:26:1E:3C:7D (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.76 seconds
root@ip-10-10-80-76:~#
```

Anfangen: Over The Wire



Wargames

The wargames offered by the OverTheWire community can help you to learn and practice security concepts in the form of fun-filled games.
To find out more about a certain wargame, just visit its page linked from the menu on the left.

If you have a problem, a question or a suggestion, you can join us via chat.

Suggested order to play the games in

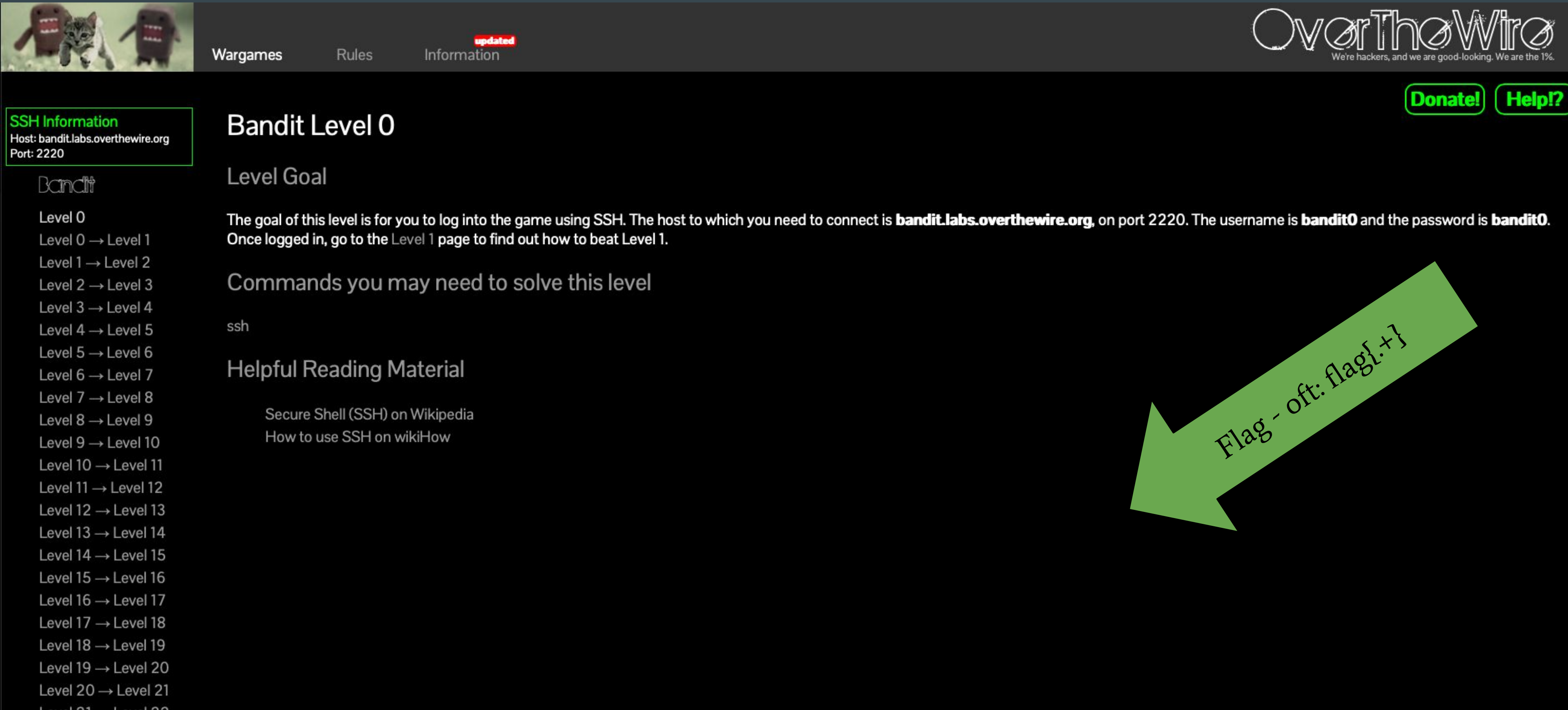
1. Bandit
2. Leviathan or Natas or Krypton
3. Narnia
4. Behemoth
5. Utumno
6. Maze
7. ...

Each shell game has its own SSH port

Information about how to connect to each game using SSH, is provided in the top left corner of the page. Keep in mind that every game uses a different SSH port.

Bandit: Unix/Linux Shell, ssh, cron, git
Natas: Web, PHP
Krypton: Kryptographie
Leviathan: Reverse Engineering
Utumno, Maze: Binary Exploits

Anfangen: Over The Wire - Bandit



SSH Information
Host: bandit.labs.overthewire.org
Port: 2220

Bandit Level 0

Level Goal

The goal of this level is for you to log into the game using SSH. The host to which you need to connect is **bandit.labs.overthewire.org**, on port 2220. The username is **bandit0** and the password is **bandit0**. Once logged in, go to the Level 1 page to find out how to beat Level 1.

Commands you may need to solve this level

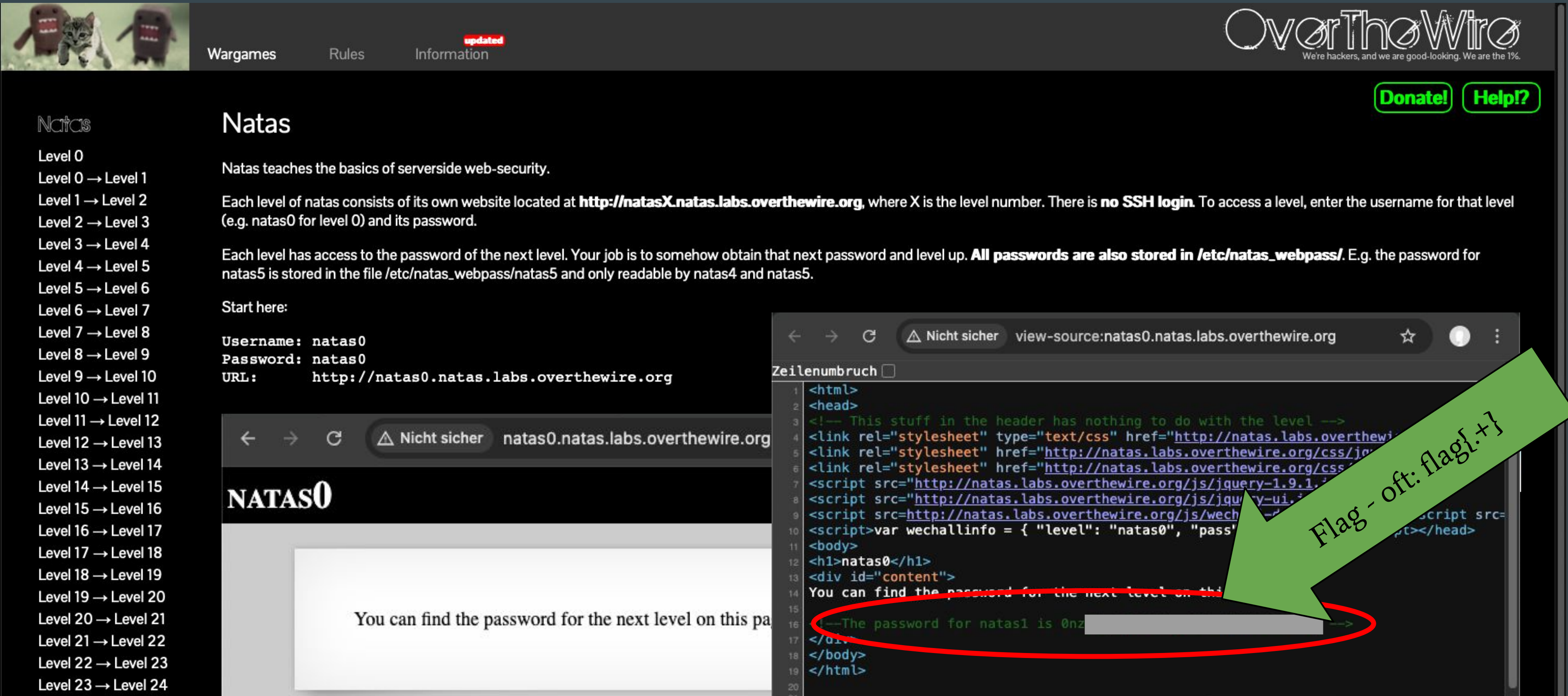
ssh

Helpful Reading Material

Secure Shell (SSH) on Wikipedia
How to use SSH on wikiHow

Flag - oft: flag{.+}

Anfangen: Over The Wire - Natas



Natas

Natas teaches the basics of serverside web-security.

Each level of natas consists of its own website located at **http://natasX.natas.labs.overthewire.org**, where X is the level number. There is **no SSH login**. To access a level, enter the username for that level (e.g. natas0 for level 0) and its password.

Each level has access to the password of the next level. Your job is to somehow obtain that next password and level up. **All passwords are also stored in /etc/natas_webpass/**. E.g. the password for natas5 is stored in the file /etc/natas_webpass/natas5 and only readable by natas4 and natas5.

Start here:

```
Username: natas0
Password: natas0
URL:      http://natas0.natas.labs.overthewire.org
```

NATAS0

You can find the password for the next level on this pa

```
<html>
<head>
<!-- This stuff in the header has nothing to do with the level -->
<link rel="stylesheet" type="text/css" href="http://natas.labs.overthewi
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jq
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css
<script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.
<script src="http://natas.labs.overthewire.org/js/jquery-ui.
<script src=http://natas.labs.overthewire.org/js/wech                    script src=
<script>var wechallinfo = { "level": "natas0", "pass"                    t></head>
<body>
<h1>natas0</h1>
<div id="content">
You can find the password for the next level on thi

<!--The password for natas1 is 0nz[redacted] -->
</div>
</body>
</html>
```

Flag - oft: flag{.+}

Plattformen

Kommerziell:

- Try Hack Me, Hack The Box -> "Premium" Content
- Kommerzielle Cyber Ranges - Ueberblick
- SANS, ISC2, ISACA -> viel Organisatorisches, Zertifizierungen

Weitere CTF Plattformen:

- PicoCTF.org -> Lernen & üben
- Pwn.college -> Binary Exploits

Verwandte:

- HackerOne, YesWeHack, Intigriti -> Bug Bounty (und Pentests etc.)
- LetsDefend.io -> Blue Teaming

Veranstaltungen

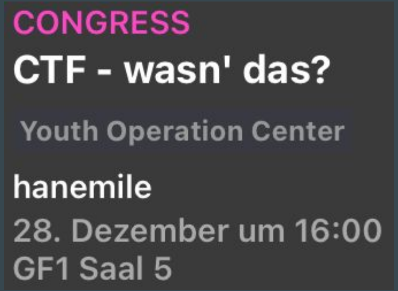
Wochenende:

- Meist, z.B. Hack.lu/CTF
- hxp 38C3 CTF - https://2024.ctf.link/

Längere Einzelveranstaltungen:

- Try Hack Me: Advent of Cyber
- Hasso Plattner Institut: Potsdam Cyber Games
- SANS: Holiday Hack Challenge

Meta-Info: https://ctftime.org



CONGRESS

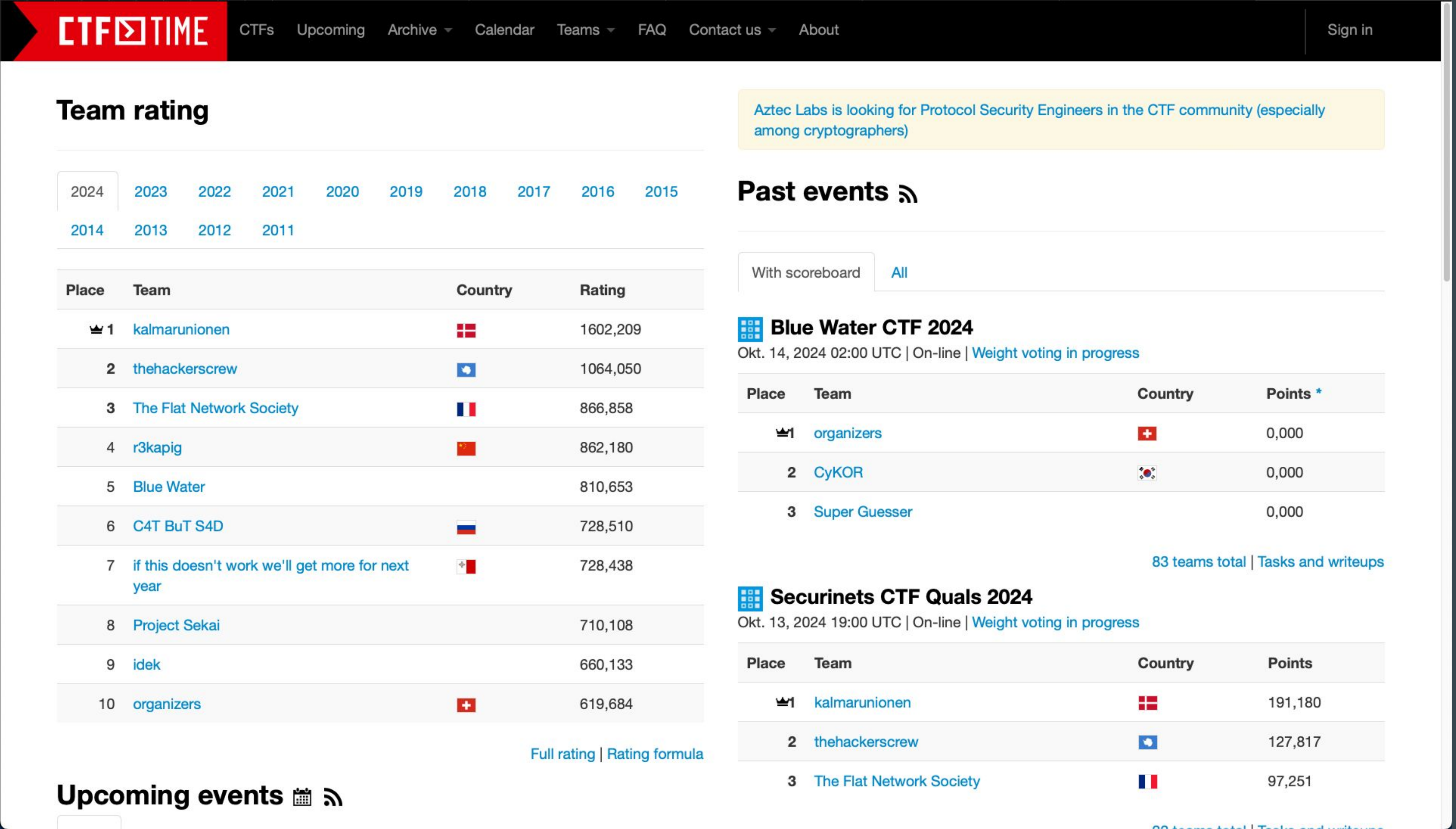
CTF - wasn' das?

Youth Operation Center

hanemile

28. Dezember um 16:00

GF1 Saal 5



Team rating

2024 | 2023 | 2022 | 2021 | 2020 | 2019 | 2018 | 2017 | 2016 | 2015 | 2014 | 2013 | 2012 | 2011

Place	Team	Country	Rating
👑 1	kalmarunionen	🇩🇰	1602,209
2	thehackerscrew	🇦🇶	1064,050
3	The Flat Network Society	🇫🇷	866,858
4	r3kapig	🇨🇳	862,180
5	Blue Water		810,653
6	C4T BuT S4D	🇷🇺	728,510
7	if this doesn't work we'll get more for next year	🇲🇹	728,438
8	Project Sekai		710,108
9	idek		660,133
10	organizers	🇨🇭	619,684

Full rating | Rating formula

Upcoming events

Aztec Labs is looking for Protocol Security Engineers in the CTF community (especially among cryptographers)

Past events

With scoreboard | All

Blue Water CTF 2024

Okt. 14, 2024 02:00 UTC | On-line | Weight voting in progress

Place	Team	Country	Points *
👑1	organizers	🇨🇭	0,000
2	CyKOR	🇰🇷	0,000
3	Super Guesser		0,000

83 teams total | Tasks and writeups

Securinets CTF Quals 2024

Okt. 13, 2024 19:00 UTC | On-line | Weight voting in progress

Place	Team	Country	Points
👑1	kalmarunionen	🇩🇰	191,180
2	thehackerscrew	🇦🇶	127,817
3	The Flat Network Society	🇫🇷	97,251

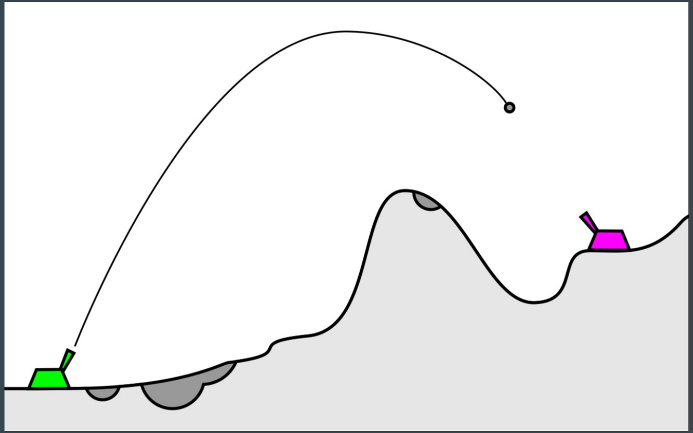
CTF - Arten, Tools

CTF Arten

- Jeopardy - Kategorien: Web, OSINT, Reverse Engineering, Binary Exploits, ...

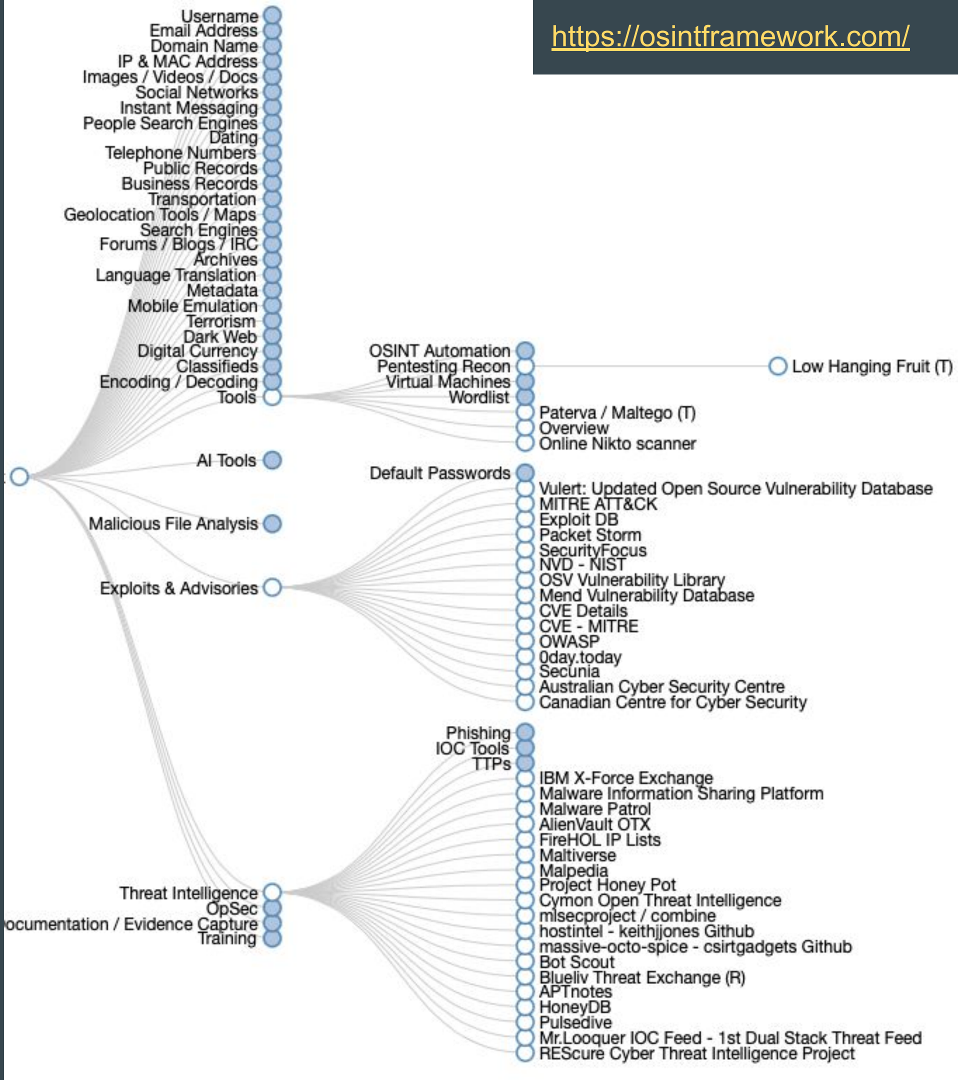
- Attack & Defense, King of the Hill

THE DINOSAURS	NOTABLE WOMEN	OXFORD ENGLISH DICTIONARY	NAME THAT INSTRUMENT	BELGIUM	COMPOSERS BY COUNTRY
$200	$200	$200	$200	$200	$200
$400	$400	$400	$400	$400	$400
$600	$600	$600	$600	$600	$600
$800	$800	$800	$800	$800	$800
$1000	$1000	$1000	$1000	$1000	$1000



CTF - Tools

- Kali Linux
- Unendlich viel mehr:
  - Windows, Linux Bordmittel
  - Netzwerk - nmap, nessus, wireshark
  - Web - curl, burpsuite
  - SQL Injections - sqlmap
  - Reverse Engineering - ghidra, cutter
  - Binary Exploits - pwntools



https://osintframework.com/

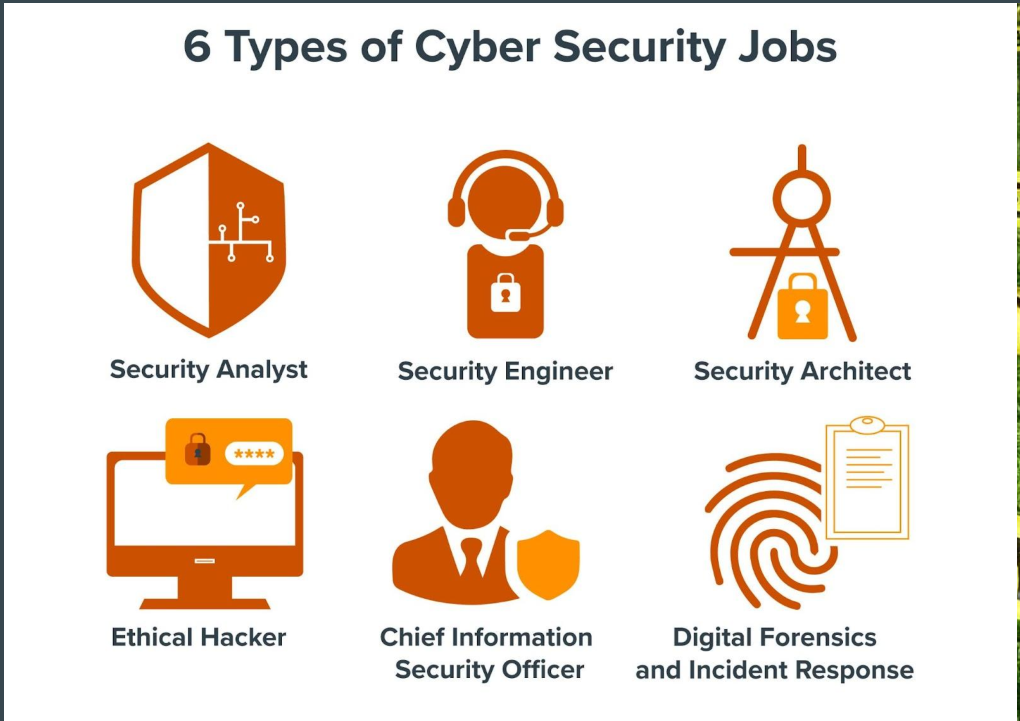
CTF - Lernen

- Das übliche - Bücher, Videos, Internet, Vorlesungen, MOOCs, Studium
  z.B. Jon Erickson: Hacking- The Art of Exploitation (2nd ed. 2008)

- Writeups
  - https://ctftime.org/writeups
  - Google: ctf site:medium.com

Was kommt dann?

Karrierepfade


6 Types of Cyber Security Jobs
Security Analyst
Security Engineer
Security Architect
Ethical Hacker
****
Chief Information Security Officer
Digital Forensics and Incident Response

CTF - machen

Anfangen!

-> OverTheWire.org

-> Bandit (Linux)

-> Natas (Web/PHP)

-> Leviathan (Rev. Engineering)

-> Maze, Narnia (Binary Exploit

-> TryHackMe.com

Üben, üben, üben!

Zusammenfassung

Einführung - Sicherheit, Schutz

Verteidigung - Checklisten, Technik

Angriff - Wozu, wie lernen

CTF - Wo anfangen? - Try Hack Me, Over The Wire, weitere & Veranstaltungen

CTF - Arten, Tools

Was kommt dann? - Anfangen, Karrierepfade

Danke! Fragen?

Danke & Grüsse an

- die Maschinenfabrik Reinhausen
- das Mad Monday CTF Team :-)

Kontakt: EMail: hubertf@gmx.de
Others: @hubertf / @huberteff / @hubertf@mastodon.social