

# WTF CTF

Vasilij Schneidermann

June 2019

# Outline

## 1 WTF CTF

# Section 1

## WTF CTF

# About

- Vasilij Schneidermann, 26
- Software developer, bevuta IT GmbH
- mail@vasilij.de
- <https://github.com/wasamasa>
- Played a few CTFs and helped organizing one
- Chanop on #wargames at OverTheWire IRC network

# What is a CTF?

- Hacker contest
- Task: Capturing flags for points
- Timeboxed
- Competitive

# Why should I care?

- It's fun
- Mess compete with the best
- Great learning opportunity
- Entry gateway to the infosec world

# How do they look like?

- Attack and Defense
  - Defend your own boxes, attack other boxes
  - Not as popular, requires admin skills
- Jeopardy
  - Many tasks that can be completed independently
  - Categorized into web/pwn/rev/forensic/stego/crypto/misc/...
  - Very popular

# Where/when do they happen?

- All over the world
- Often it's online
- Sometimes it's local or requires admission
- <https://ctftime.org>



# What stuff do they do at a Jeopardy event?

- Web
- Binary Exploitation
- Reverse Engineering
- Forensics
- Steganography
- Cryptography
- Miscellaneous

# What do they do during a Jeopardy event?

- Register user/team
- Solve challenges and submit flags
- Report bugs

# What do they do after a Jeopardy event?

- Figure out how challenge XYZ was supposed to work
- Celebrate
- Vote on <https://ctftime.org>
- Publish writeups
- Look for the next CTF to compete in

# How do I learn this stuff?

- Learn basics (your OS, programming, ...)
- Online labs (wargames, <http://wechall.net>)
- Set up a lab (<https://vulnhub.net>)
- Play an entry-level or highschool CTF
- Learn from your mistakes
- Study writeups

- Learn to use your browser effectively
- Intercepting proxy (Burp)
- OWASP Top 10
- OverTheWire: Natas
- WebGoat
- Random stuff found on <https://vulnhub.net>

# Binary Exploitation

- Classic Phrack articles
- [Jon Erickson] Hacking: The Art of Exploitation
- LiveOverflow YouTube channel
- <https://microcorruption.com>
- OverTheWire (everything after Bandit/Natas/Krypton/Leviathan)
- <http://io.netgarage.org/>
- <http://smashthestack.org/>

# Reverse Engineering

- Know your OS and toolchain (binutils) well
- Learn IDA/Ghidra/Hopper/Binary Ninja/radare2
- [Dennis Yurichev] Reverse Engineering for Beginners
- angr is pretty cool

- It's either packet analyzer captures or (broken) file systems
- Learn Wireshark
- binwalk is OK for carving
- radare2 was originally developed for this purpose



# Steganography

- Lots of guessing
- Common tools:
  - strings
  - binwalk
  - exiftool
  - steghide
  - zsteg

# Cryptography

- <https://cryptopals.com>
- Lots of RSA/ECC/linear algebra
- Some (sage) math may be required
- Sometimes they just throw classic ciphers at you. . .

# Miscellaneous

- Programming challenges (typically involving the network)
- Knowing trivia about your OS/toolchain
- Grab bag