Intro to CTF

Motivation

- Great for learning practical (security) skills
- Can win money / prizes
- Can be used to get a job
- Fun !

What is CTF

- Capture-the-Flag
- Solve a challenge or problem and get a flag
  - A flag is a proof-of work to show that the challenge has been completed: CCSC{Th1s_is_a_Fl4g_f0r_r3al}
- Two main types: Jeopary and Attack / Defence
  - We will focus only on the first !
  - CCSC / ECSC competitions are (mostly) Jeopardy-style CTFs

Jeopardy CTFs

- Like the popular American television show
- Multiple challenges across different categories, mainly:
  - Web: web application security
  - Reverse engineering: reversing programs
  - Binary exploitation: exploiting vulnerabilities in binary files (also known as ***pwn***)
  - Forensics: analyzing files
    - Multiple sub-categories, e.g. network forensics, steganography etc
  - Crypto: cryptography

How to be Successful

- Passion (!)
  - If someone doesn’t enjoy this they shouldn’t waste their time
- Perseverance / hard work
  - A lot of failure will occur because challenges involve practical aspects
  - Being able to study and learn on your own
- Hacking doesn’t discriminate and is for **everyone**

“Without the element of enjoyment, it is not worth trying to excel at anything.”
Magnus Carlsen, World Chess Champion

Key (Beginner) Technical Skills

- Familiarity with a Linux distribution
  - A lot of the tools used during CTFs require a working linux distribution
  - Encourages familiarization with the command line
- Good reading (and writing) English (!)
  - A lot of information is only available in English
  - Incentive to improve your English
- Programming
  - Reading code is more important than writing code
  - Writing code is also important
  - At least on scripting language recommended
    - Python
    - Javascript

CTF Resources

Resource Pack – Linux Distros

- Kali Linux (specifically for penetration testing)
  - Has a lot of tools / libraries installed
  - https://www.kali.org/
- Linux Mint (Ubuntu-based, very friendly; I use this)
  - https://linuxmint.com/
- Manjaro Linux (Arch-based, maybe more advanced but more flexible; for those feeling a bit more daring)
  - https://manjaro.org/

Resource Pack – Linux Distros

- Kali Linux (specifically for penetration testing)
  - Has a lot of tools / libraries installed
  - https://www.kali.org/
- Linux Mint (Ubuntu-based, very friendly; I use this)
  - https://linuxmint.com/
- Manjaro Linux (Arch-based, maybe more advanced but more flexible; for those feeling a bit more daring)
  - https://manjaro.org/

Resource Pack – YouTube Channels

- LiveOverFlow
  - https://www.youtube.com/channel/UClcE-kVhqyiHCcjYwcpfj9w
- John Hammond
  - https://www.youtube.com/channel/UCVeW9qkBjo3zosnqUbG7CFw
- ippsec
  - https://www.youtube.com/channel/UCa6eh7gCkpPo5XXUDfygQQA

Platforms for Learning

- Hack The Box
  - https://hackthebox.eu
- TryHackMe (beginner-friendly)
  - https://tryhackme.com/
- CyberRanges (Cyprus company)
  - https://app.cyberranges.com/
- PicoCTF (CTF for highschoolers, although some challenges are hard)
  - https://picoctf.com

Resource Pack – Web

- PortSwigger Academy
  - https://portswigger.net/web-security
- Web Application Hacker’s Handbook
  - https://www.amazon.de/-/en/Dafydd-Stuttard/dp/1118026470

Resource Pack – Crypto

- Cryptopals
  - https://cryptopals.com/
- CryptoHack
  - https://cryptohack.org/
- https://id0-rsa.pub/
- https://mysterytwister.org/home/welcome/

Resource Pack – Binary Exploitation

- Curated beginner’s guide to pwn
  - https://www.notion.so/MSc-CTF-Pwn-9ecbafd7791a413dae7d37a24ec27fb9

Resource Pack – General CTF

- Beginner CTF guide
  - http://trailofbits.github.io/ctf/
  - https://ctf101.org/
  -

Resource Pack – Academic Papers / Talks

- **Academic papers**
  - Google Scholar “Capture the Flag Search”
  - CTF: State-of-the-Art and Building the Next Generation
    - https://www.usenix.org/system/files/conference/ase17/ase17_paper_taylor.pdf
  - Order of the Overflow Proposal:
    - https://oooverflow.io/ooo-dc-cfo-proposal.pdf

- **Talks**
  - Building a Competitive Hacking Team
    - https://www.youtube.com/watch?v=-r-B1uOj0W4

Final Note

- Skills acquired from CTFs can potentially be used to carry out ***criminal*** activities
- You should remember that doing anything to other systems can and will result in criminal prosecution
  - Example: Joshua Epiphaniou
- There is no need to do anything illegal because of so many learning platforms
- Good career prospects instead of becoming a criminal

Thank You