

# Ethical Student Hackers

---



# The Legal Bit

- The skills taught in these sessions allow identification and exploitation of security vulnerabilities in systems. We strive to give you a place to practice legally, and can point you to other places to practice. These skills should not be used on systems where you do not have explicit permission from the owner of the system. It is VERY easy to end up in breach of relevant laws, and we can accept no responsibility for anything you do with the skills learnt here.
- If we have reason to believe that you are utilising these skills against systems where you are not authorised you will be banned from our events, and if necessary the relevant authorities will be alerted.
- Remember, if you have any doubts as to if something is legal or authorised, just don't do it until you are able to confirm you are allowed to.



# Code of Conduct

- Before proceeding past this point you must read and agree to our Code of Conduct - this is a requirement from the University for us to operate as a society.
- If you have any doubts or need anything clarified, please ask a member of the committee.
- Breaching the Code of Conduct = immediate ejection and further consequences.
- Code of Conduct can be found at  
<https://shefesh.com/downloads/SESH%20Code%20of%20Conduct.pdf>



# How to Play a CTF

## What is a CTF?

- A **Capture the Flag** hacking competition
- You will solve various challenges and look for a flag, usually a string related to the challenge such as `SESH{F4k3_fl4g_her3}`
- Sometimes the flag won't have the `SESH{ }` wrapper, and you'll have to add it yourself
- Challenges require some creative thinking, but many of them should be doable if you've attended SESH sessions!

## What will we cover today?

- Introduce you to some common challenge categories
- Tips, tricks, and tools
- Where to look for flags in certain challenge types
- Not all of this will be relevant for our CTF - but some of it might be...



# General Challenge Categories

Web: Anything web application-hacking related!

Crypto: Cryptography-based challenges - often finding the flaw in a badly implemented algorithm (RSA is a usual favourite) but sometimes you may find some more basic ciphers to decode

Reversing: Reverse Engineering challenges, usually finding secrets in a compiled binary or looking at how to break a vulnerable function

Pwn: Usually binary exploitation challenges

- You will usually get an IP + port that hosts the vulnerable binary
- You may get access to the source code

Forensics: usually searching through log files, pcap files, and machine memory images to find secrets or evidence of malware



# General Challenge Categories

Boot2Root: go from an IP address to full root/SYSTEM access!

- Usually multiple stages: foothold (likely via a web app or file sharing services), initial shell, then privilege escalation - similar to things like HackTheBox

Other:

- Steganography
- Cloud-based challenges
- Hacking Kubernetes/Docker
- Challenges hidden *on* the platform itself!
- OSINT challenges where you have to find public information on the internet
- Automation/scripting-based challenges e.g. scraping a website



# What Skills Might you Need?

GOOGLE!! Google, google, google - if it exists, someone will have a CTF writeup about it

Web hacking skills:

- LFI, SQLI, XSS are common challenges!
- You may need to analyse Javascript code and look for secrets, functions that are vulnerable, obfuscated passwords, etc
- Common paths to flags and things to remember: check page source, robots.txt
- Always worth running SQLMap - but usually brute force is not the answer
- Some Challenges require Remote Code Execution - once you have the flag, you shouldn't attack the underlying infrastructure for the CTF!
- Remember your basics! Check version numbers, try admin:admin and default creds...

Crypto:

- Know your basic substitution ciphers (Caesar, Vigenere) and how to attack them with frequency analysis
- Know some common pitfalls in RSA! E.g. small primes



# What Skills Might you Need?

Other quick web hacking checks:

- Nikto and wpscan
- Check for obvious paths like /admin, /wp-admin

Pwn: we've not taught you buffer overflows this year, but we have [a session from last year](#)

Steganography:

- Information hidden in files, such as images
- Useful commands: strings, hexdump, binwalk
- <https://fareedfauzi.gitbook.io/ctf-checklist-for-beginner/steganography>

Look at writeups: <https://ctftime.org/> and useful tools: <https://github.com/apsdehal/awesome-ctf>





# What Skills Might you Need?

Forensics & Reversing (often some overlap):

- Know how to analyse a pcap file with Wireshark
  - wireshark [file.pcap]
  - Look for interesting requests (e.g. to /login) or leaked secrets in handshakes
  - Right Click > Follow TCP Stream to see the full request rather than the individual packets
  - Practice: <https://tryhackme.com/room/wireshark> + <https://tryhackme.com/room/c2carnage>
- Interact with a machine image using [volatility](#)
  - `volatility imageinfo -f [file.mem]` to get machine details and pick a profile e.g. Win7SP1x64
  - `volatility -f [file.mem] -- profile=[PROFILE] pslist` to list processes
- Analysing word documents: [oletools](#) -> `olevba [FILE]`
- Have a read of the following to see the range of possible challenges in Forensics + Reversing!  
<https://darkdefender.medium.com/write-up-memory-forensics-in-the-def-con-dfir-ctf-c2b50ed62c6b>  
and <https://yan1x0s.medium.com/htb-x-uni-ctf-writeup-forensics-d3d122a71e36>



# What Skills Might you Need?

## Automation:

- Using Web Scraping to visit websites and fill out forms or scrape sites for information in a short amount of time.
  - Web Scraping tools include:
    - Selenium [\[Link to previous session slides\]](#)
    - BeautifulSoup [\[Link to previous session slides\]](#)
  - When Web Scraping also remember to use **XPaths** in order to easily select items on a webpage.
  - If a site does have a captcha this can be counteracted by having the program wait until you press enter etc, and then letting it launch the scraping program. [Maybe also include a delay so you don't get blocked for too many requests]
  - When web scraping an import thing to remember is that website cookies will in most cases need to be preserved.



# What Skills Might you Need?

Remember your common ports:

- 20 + 21 (FTP)
- 22 (SSH)
- 80 (HTTP)
- 443 (HTTPS)
- 139 + 445 (SMB)
- 8080 (Often a web proxy)
- 3000 (Often for Node/Express servers)
- 3306 (MySQL)

This is useful if you're port scanning, but that's only usually required on a Boot2Root Challenge - most challenges will give you an IP and specific port to attack, please don't scan the rest of the ports on the machine unless you are certain it's required for the challenge!



# Reversing Checklist

Commands to run:

- file [BINARY]
- Strings [BINARY]
- Oletools
- Trace

Run the binary to see what it does!

Live debug with gdb/ollydbg - Dynamic Analysis

Reverse with Ghidra - Static Analysis

- Get Ghidra [here](#)
- Try to label functions and variables that you find



# Useful Links

[CTFs Github site] <https://ctfs.github.io/resources/> :

- Cryptography
- Steganography

[CTF101] <https://ctf101.org/>

- Web Exploitation

CTF Command Cheat Sheet <https://dvd848.github.io/CTFs/CheatSheet.html>



# Practise

You can practise and improve your skills via a variety of websites such as TryHackMe, Hackthebox and a variety of others, For today's session to give a more authentic ctf experience before we run ours, we'll be doing the:

- [Google CTF] <https://capturetheflag.withgoogle.com/beginners-quest>
- [TryHackMe Advent of Cyber] <https://tryhackme.com/room/adventofcyber3>
- [TryHackMe Steganography] <https://tryhackme.com/room/ccstego>



# Upcoming Sessions

What's up next?

[www.shefesh.com/sessions](http://www.shefesh.com/sessions)



**GroceryTF**

THIS WEEKEND!!! 31st - 2nd

Prizes will include Hack the Box vouchers, Try Hack Me codes, and more to be announced!

<https://shefesh.com/grocerytf>

After Easter:

- Tor & Cryptocurrency + AGM: 25/04/22
- Rest of sessions TBC

# Any Questions?



[www.shefesh.com](http://www.shefesh.com)  
Thanks for coming!

