NC STATE UNIVERSITY

CSC 405
Computer Security

Aleksandr Nahapetyan
anahape@ncsu.edu

(Slides adapted from Dr. Kapravelos)

Who am I?

- Started undergrad at NC State under exploratory science
- Undergraduate research under Dr. Jennings
- Took this class 6 years ago; was a TA for 3 years after that
- PhD Candidate under Dr. Kapravelos and Dr. Reaves

NC STATE UNIVERSITY

HackPack

Research directions

Systems & software security

- Web security & privacy
  - Emerging web threats
  - Phishing attacks
- Cellular security
  - SMS Phishing
  - Robocalls
- Software supply chain security
- AI security

Logistics

- Class website
  - https://ale0x78.github.io/teaching/csc405-s26/syllabus/
- Ed
  - There should have been an email with a link!
- Panopto
- Discord
  - HackPack (website)

Material

- What material will we be using?
  - Unfortunately, there is no good book on systems security
  - Lecture Slides
  - Related Papers, Readings, and Links
- Useful online books that provide additional information:
  - The Shellcoder’s Handbook: Discovering and Exploiting Security Holes
  - Hacking, The Art of Exploitation
  - The Tangled Web: A Guide to Securing Modern Web Applications

Grading

- Homework Assignments - **75%** of grade
  - Shellcode
  - Buffer Overflows
  - Web Security
- Competing in our Capture The Flag competition - **25%** of grade
  - HackPack CTF

Capture the Flag

There's a flag…

Capture the Flag

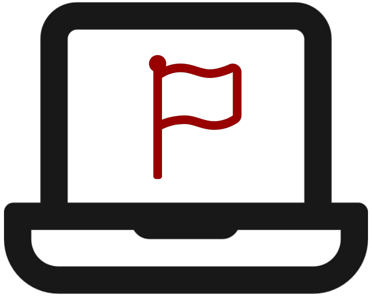
…and you have to capture it.

Capture the Flag

There's a program with a 'flag'

Capture the Flag

- There's a program with a 'flag'
  - The program has an unidentified vulnerability



Capture the Flag

- There's a program with a 'flag'
  - The program has an unidentified vulnerability
    - You need to exploit the vulnerability to get the flag

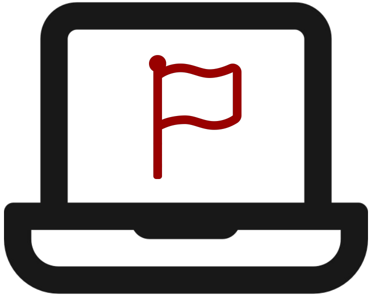
Capture the Flag

There's a program with a 'flag'

The program has an unidentified vulnerability

You need to exploit the vulnerability to get the flag

The flag is typically a secret string / file



Flag:
Drink
More
Ovaltine

HackPack CTF

- Capture the Flag Security Competition
- 48 hours of hacking
- **Friday, April 17th 2026**
- Competing in the CTF is part of your class
  - For the homework-part you will be able to work on the challenges over the weekend
  - Participation is **mandatory** to the CTF event, if you cannot make it you have to inform me beforehand

Assignments

- Individual homework assignments
- These are going to be **hard**!
- Discovering a vulnerability is a frustrating, but very rewarding in the end!

- The assignments have a unique nature
  - They require some **exploration** from you
  - They are **VERY** different from any assignments you had so far
  - Most of them will have two parts:
    - **Identify** the vulnerability
    - **Exploit** the vulnerability

Lectures

- In-person
- Streamed on Panopto if you miss the lecture
- Somewhat flipped
  - watch the lecture before you come to class
  - we discuss/solve a security challenge during class
- You will have to watch the lectures and study any related material
- We will use Ed for any questions

Topics

Computer Security Basics

Software Security

Web Security

Goals

Learn how an attacker takes control of a system

Learn to defend and avoid common exploits

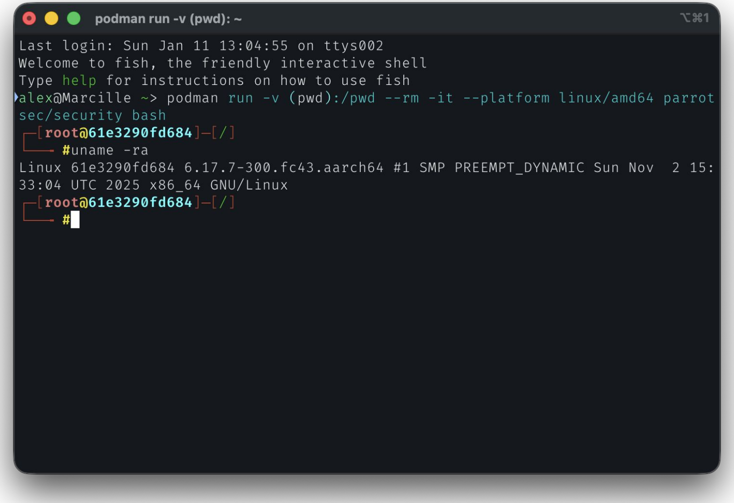
Learn how to architect secure systems

You need to understand

- Networks and Operating Systems
- Basics of systems theory and implementation
  - file systems, distributed systems, networking, operating systems, …
- You will build stuff. I expect you to:
  - know how to code (in language of your choice*)
  - I will use mix of pseudocode, Python, Assembly, JavaScript, PHP and C
  - be(come) comfortable with Linux/UNIX

What do you need

- Access to an x86 Linux system
  - You can use the ParrotOS VCL image
  - Docker/Podman (especially on M-series macOS)
  - Virtualbox/UTM
  - Checkout other solutions in the reading: Linux Setup
- **Do not use EOS/WSL (Windows Subsystem Linux)**
- If you do not have access to any x86 machine, email me!



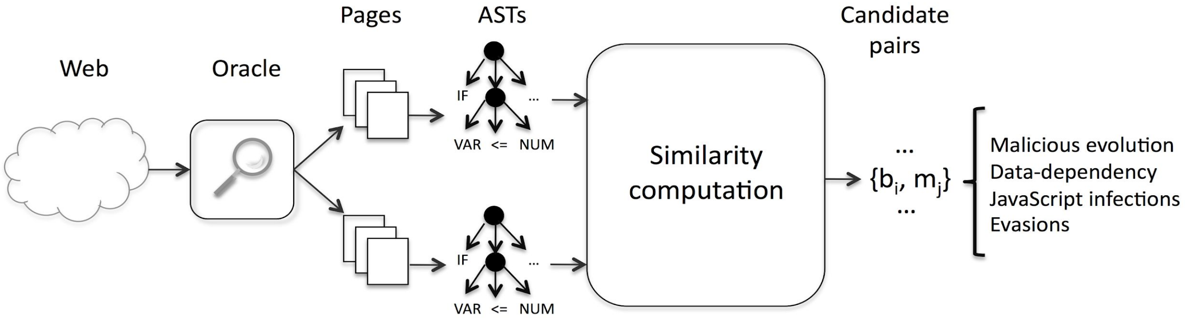
```
Last login: Sun Jan 11 13:04:55 on ttys002
Welcome to fish, the friendly interactive shell
Type help for instructions on how to use fish
alex@Marcille ~> podman run -v (pwd):/pwd --rm -it --platform linux/amd64 parrot
sec/security bash
┌─[root@61e3290fd684]─[/]
└──╼ #uname -ra
Linux 61e3290fd684 6.17.7-300.fc43.aarch64 #1 SMP PREEMPT_DYNAMIC Sun Nov  2 15:
33:04 UTC 2025 x86_64 GNU/Linux
┌─[root@61e3290fd684]─[/]
└──╼ #
```

Readings

- There is a large amount of readings in this course covering various topics:
  - Support the lectures in the course (provide clarity)
  - Augment the lectures and provide a broader exposure to security topics
- **Students are required to go through the readings**
  - Some of the material is **really helpful** in solving the homework assignments

Cheating

- Cheating is not allowed
- We run tools
  - Prior instructor worked with Senior Design to make more
- If you cheat you will probably get caught and get a failing grade in the course
- All academic dishonesty incidents will be reported without exception



Ethics

With great power comes great responsibility

- Topics will cover technologies whose abuse may infringe on the rights of others
- When in doubt, please contact us for advice
- Do not undertake any action which could be perceived as technology misuse anywhere and/or under any circumstances unless you have received explicit written permission from the instructor.

Extra Credit Policy

- Anyone who finds a security vulnerability (on any site/program) during the semester will receive extra credit (bonus points)
- **YOU MUST USE RESPONSIBLE DISCLOSURE**
  - You are responsible for your own actions
  - If you are unsure, come speak with us
  - Do not attack servers you do not own, do not destroy data

questions?