

The background of the slide is a dark, textured surface, possibly stone or concrete. A light gray rectangular area in the center has a brick wall pattern. Four gold-colored keys are positioned around the edges of this central area: one on the left, one on the right, and two on the bottom. The keys are oriented vertically, with the top key on the left and right pointing upwards, and the bottom keys pointing downwards.

Offensive security intro meeting

Jarrett Lane

What is offensive security?

- We are the "hackers"
- Our mindset is to look for weaknesses and vulnerabilities, white hat reports these weaknesses grey/black hat exploits them
- We love unexpected behavior from computers
- Offensive covers a wide variety of topics, just like cybersecurity

Before continuing

- Don't be malicious
- There are very serious consequences if you are caught and its not worth it, even if it seems like something minor or harmless
- If curiosity is pushing you, use a secure lab setup for attacking
- If you do use a lab environment, know what you are doing

How I plan to run offensive

- This year I will be taking a different approach from how red team has been traditionally run
- In the past we had a big focus on CTF competitions, I think ctf is awesome and very important, but I also want to do more red team activities that are not competition oriented
- I also want to try out more collaborations with blue team, other groups, and guests

Keeping balance

- This is something new im trying out.
- I want to balance by keeping us competitive at CTF while also diving into the cool red team stuff that is practical
- I also want to always be beginner friendly while also getting into the complex and technical stuff

For beginners

- It is ok if you know nothing, we're here to get you started.
- Its also ok if cyber security isnt your major.
- If something confuses you or you are stuck on something, ask
- Try to learn on your own outside of the club
- Make sure to put school first
- Don't stress about missing meetings
- Talk to others, a lot of people here are very smart and share your interests

Im always open to you all

- If you guys need any help, have questions, or anything from me, you can talk to me whenever, you can talk to me over discord, during/after meetings, or if you see me around the school
- The club is all about community, we plan on creating more opportunity for the club to hang out outside of meetings, whether it be for competitions, projects, or just hanging out and doing hw/studying
- At times I may get busy

What I expect this semester

- I want to get you all familiar with the basics of the technical stuff
- I want to have beginners scoring points in CTF
- I want you all to be comfortable with virtualization/containerization
- For those who are returning, push yourselves more and help newer members

Meeting notes and resources

- Any powerpoint or lab or whatever I make for our meeting I will put here: https://github.com/JarrLane/Offensive_Meeting_Content
- I will also put it in the discord
- I will also have references to anything I use so you all can use those references to learn too
- I may recommend resources too

Competitions

- In offensive we have competitions called "Capture The Flag" or CTF. This is a set of challenges where you try to find a hidden "flag" to score points
- Find the flag by hacking or solving a puzzle
- `flag{w3lc0me_7o_ctf}`
- A lot of these are online but sometimes we go in person
- We try to do this every week
- Don't be intimidated by CTF

Our team

- Anyone can join, if you get really good you get to join the A team
- The A team is for flexing in in-person competitions
- There is no team size limit*, anyone can join ctf
- School first, I don't expect you to compete every weekend

CTF challenges

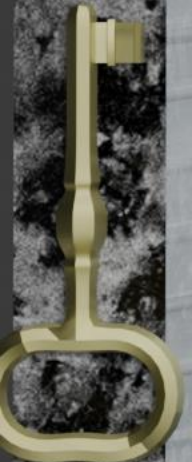
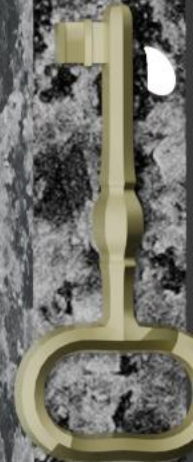
- One competition has many challenges with varying difficulty, and these challenges are unique in how you get the flag
- Common challenge types are:
 - Web
 - Cryptography
 - Forensics
 - Reverse engineering
 - OSINT
 - PWN
 - Miscellaneous
 - Even more depending on the competition

Web

- You are accessing a website, and there is some vulnerability you need to exploit to find the flag
- There are so many possibilities of what the vulnerability is, web security has a lot to it
- Sometimes its multiple vulnerabilities together that you need to exploit
- Do you like web development, are you interested in web security, does it sound cool to you to hack a running web server?



Cryptography

- The flag is encrypted, and you need to decrypt it
 - Many types of cryptography algorithms are used
 - Do you like math, do you like cryptography, are you interested in how we use algorithms to secure data at rest and in transit?
 - I know there are some people in here that love numbers and number puzzles, you will love cryptography
 - If you like word puzzles, that's a form of cryptography, cryptology
- 
- 

Forensics/steganography

- The flag is hidden in plain sight, like maybe an image, pdf, network traffic, memory dumps, and a lot more
- You will be using many tools to find the hidden data, these challenges can get very creative with how they hide the flag
- Do you like ARGs, does it sound cool how information is hidden right in front of our faces, do you like investigating things, do you like diving deep into things?

Reverse engineering

- You need to understand how a program works to find the flag
- You may get a python file, or you might get an executable
- Do you like coding, programming languages, understanding how things work?

OSINT

- You use publicly available information to track down something specific
- You may be given a vague picture and you have to find the exact coordinates of the place, or maybe you have to track down someones social media account
- Do you like ARGs, do you like going down rabbit holes, do you like tracking things down, do you like geoguesser?
- This is generally the easiest category because its not very technical, it's a good starter

PWN/binary exploitation

- These challenges are about exploiting a running executable that is being hosted
- You are usually given the executable, and you can test it locally to see how to hack it, then you apply that to the server running the program containing the flag
- Do you like messing with running programs, getting closer to the hardware, exploiting vulnerabilities?
- This category is challenging
- If you can take these on that's a huge flex

Miscellaneous

- These challenges are for niche things that don't really fit any category, also a lot of general puzzles
- These can be all types of things, like old cellphone communication or knowing a certain data structure
- This stuff is random but if you are an all around tech person or you know a lot of niche cs concepts you may find yourself scoring in these challenges
- If you like puzzles or cool random things you will enjoy misc challenges

Other

- Sometimes there are challenges about AI, video games, mobile, and other things
- Some challenges involve more than one category
- Don't focus on being good at one category

PWN and web

- We need more people into PWN and web
- These challenges lean towards the hacker part of ctf

Recommended general technical skills

- Understand and be able to trace code
- Understand binary and Boolean operations
- Understand foundational concepts of computers and networks
- Understand high/low level computer concepts
- Be able to use python to automate things
- Understand basic command line and running tools
- Its ok if you know nothing, we will teach you

How to get good

- Read writeups (explanations of how someone solved a challenge)
- Have autism (find something cool and spend all day learning how it works)
- Use google
- Use AI to help you understand something unfamiliar, don't ask ai to do the challenge for you that's lame
- Keep competing and coming to meetings
- Talk to people and ask others questions (even professors)
- If you are CS, CE, EE, or cyber eng, pay attention in class



Any questions?

If not, try some pico gym challenges