Tutorial

Welcome to SIGPwny!

Thomas made these slides

Oh hey! You're awake, you were trying to join SIGPwny, right?

- Awesome! Welcome, you're in!

What is SIGPwny?

- Computer security Special Interest Group at UIUC

What does SIGPwny do?

- Learn all topics of computer security by learning theory and practical skills
- Participate in CTFs, both internally and externally
- Create a community of security interested students at UIUC, find a network and friend group!

Frequently Asked Questions

When are SIGPwny meetings?

- Typically, they are **Thursdays from 6-7PM CST** (11PM-12AM UTC)
- See #announcements on Discord for any changes (click to join)

Where do I get started?

- The next steps for becoming an awesome hacker are in this presentation.

Where does SIGPwny communicate?

- SIGPwny has a Discord! Join by going to sigpwny.com/discord

Frequently Asked Questions Part 2

I am a UIUC student, how do I prove that?

- We have an authentication bot, go to shib.sigpwny.com to authenticate. Once you do that, you will have access to student-only channels in Discord.

Where do I get started?

- The next steps for becoming an awesome hacker are in this presentation.

Can you teach me to hack someone's _____?

- No, please see our next slide

What you **will learn** and **won't do** in SIGPwny

You Will

- Learn how to think with a security mindset
- Learn how to look find vulns in systems
- Lean about the subcategories of security
- Learn practical security skills
- Find a network of friends and colleagues

You Won't

I had a long list here, but here is the TLDR.

"Don't hack things you don't have permission to hack. When in doubt, ask us if it's ok"

Don't break the law

Acronyms / Common Shortened Words

- SIG - Special Interest Group
- CTF - Capture The Flag
- chal - Challenge
- RE - Reverse Engineering
- PWN - “Pwning”, binary exploitation
- crypto - Cryptography
- OSINT - Open Source Intelligence

What is a CTF?

- Capture The Flag
  - Complete chals (security challenges) of a variety of topics.
  - Upon solving the challenge, you are given a string.
  - That string is your flag, submit the flag to that challenge's page on the CTF website for points!
- Challenge Point Values
  - **WILDLY** Depends on the event, but typically < 100 = Easy, 100-300 = Medium, 301-500 = Hard
- Internal CTF
  - Participate in our internal CTF for PwnyPoints!
- Other CTF's
  - Join SIGPwny's team and participate as much as you can, but there is no pressure*
  - * is CSAW. We go hard on that every year.

SIGPWNY

Cyber?

I’ve been calling this club a computer security club, and not a cybersecurity club.

“Cybersecurity” is also commonly known as “Information Security”, “Infosec”, “Netsec”, “Computer Security”, or “Security”.

- Know your audience, and what they will respond to.
  - Executives & non-technical people like “cyber”
  - Technical people do not
  - When in doubt, say “computer security”

SIGPWNY

More Logistics Slides

We plan to add more slides regarding SIGPwny Logistics. Check back here every few months to see if anything has changed.

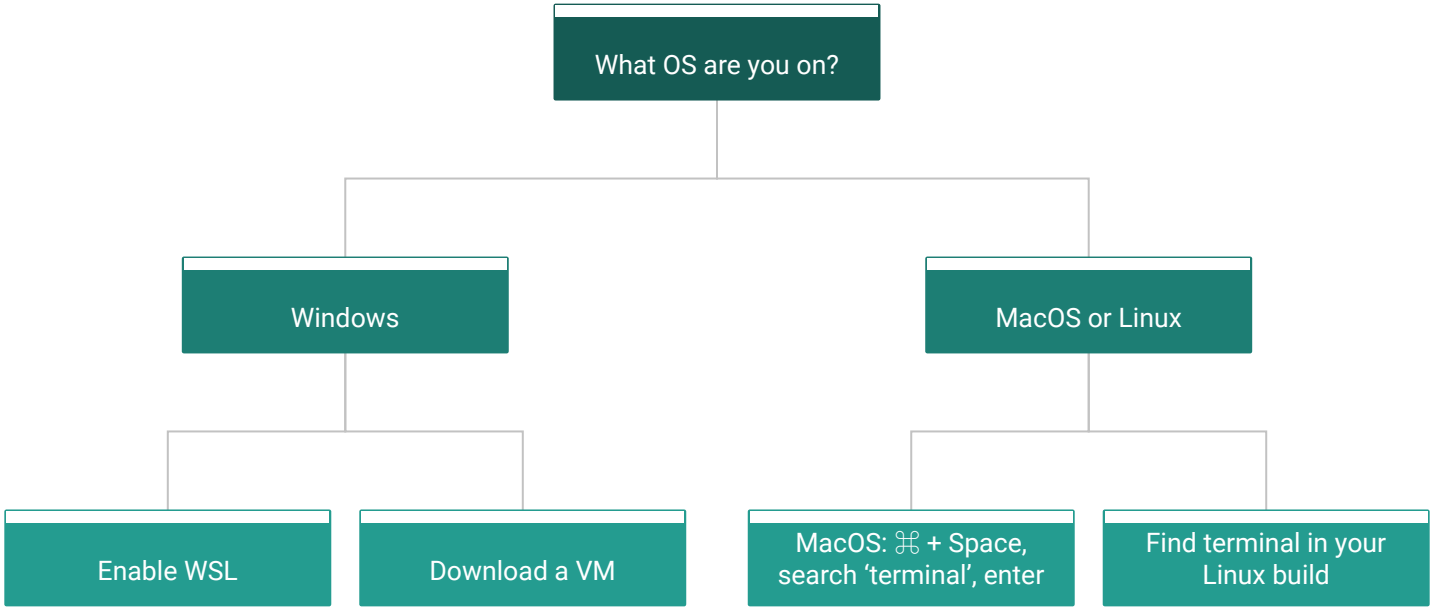
If any major changes happen, we will probably drop an announcement in Discord.

Tutorial

From here on in this presentation, we will cover

1. How to get into a terminal (WSL)
2. How to use basic terminal commands
3. Introduction to the security mindset
4. Subcategories of computer security
5. How to run a SIGPwny meeting!

1. Getting into a Terminal



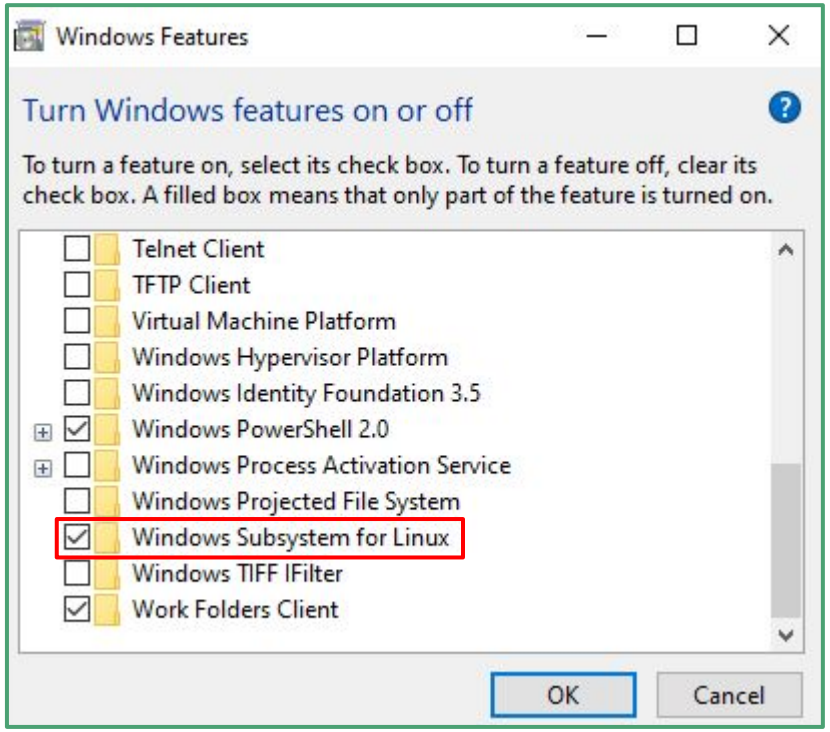
Enabling WSL (Be prepared to restart your PC)

https://docs.microsoft.com/en-us/windows/wsl/install-win10

That link is the fastest way. But there are lots of different ways to do so.

1. (Windows) + S => “Turn windows features on or off” (search this)
2. Scroll down to “Windows Subsystem for Linux”
3. Enable it
4. Restart your PC
5. Download linux cli (Just download Ubuntu) from the Microsoft Store

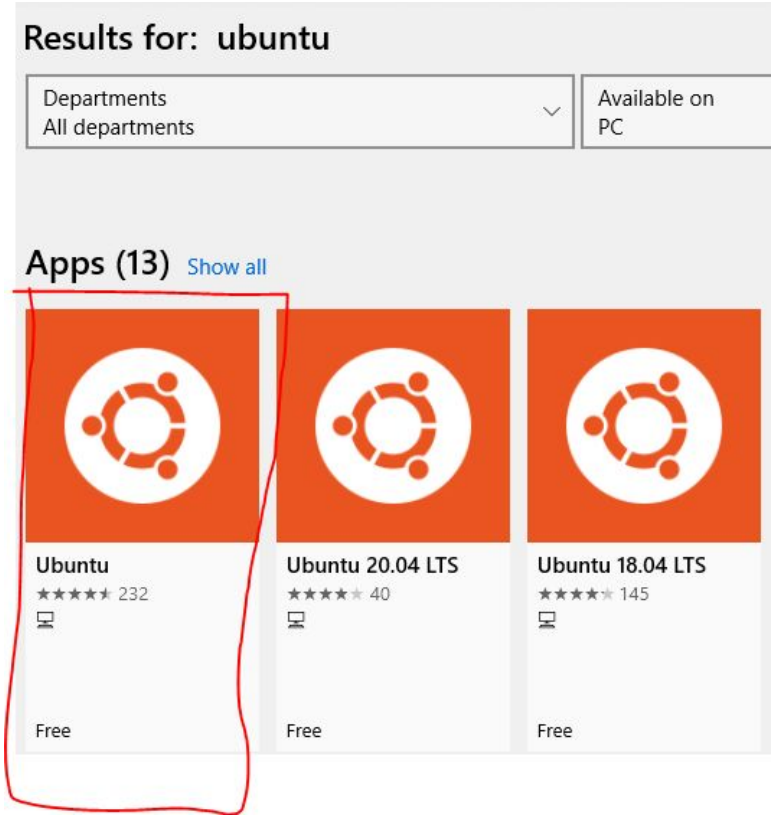
Enabling WSL



RESTART

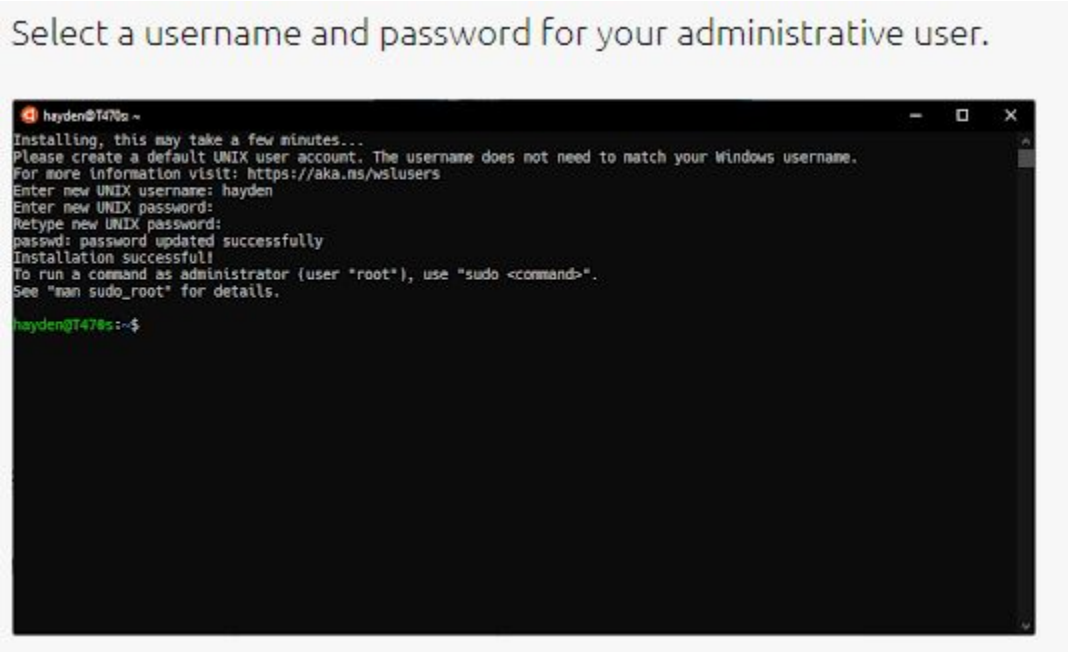
SIGPWNY

Installing Ubuntu



SIGPWNY

Setting up ubuntu



When you type in the password, no *’s will show up. That is normal

Filesystem (FS) Navigation

What is a Filesystem?

A filesystem is the underlying system in which your files are stored, it can be navigated in many different ways. In filesystem terminology, Folders = Directories

Path, Absolute, Relative, Home, Root, what do they mean?

Path: the location of a file within the filesystem. I.E. “/Users/Thomas/Desktop/spaghetti.png”
Absolute Path: The full path of the file, relative to root I.E. “/home/Thomas/music/oop.mp3”
Relative Path: Where a file is relative to what directory you are currently in. I.E. “./music/oof.mp3”
Home: The current user’s directory, signified by ~,the absolute path varies.
Root: The lowest possible directory, signified by /, basically everything is in this one.

SIGPWNY

We will be using the Linux filesystem, please dont use Windows standards...

Terminal Commands - Filesystem

ls: list all files in your current directory (do ‘man ls’ for the manual, this applies with many commands)

cd [*new_directory*]: changes your current directory to *new_directory*

mv [*source]* [*dest*]: renames file from *source* to *dest*, if *dest* is a directory, move *source*

rm [*file*]: removes *file*, **NOT REVERSIBLE**

cat [file]: prints the contents of *file*. (Sometimes it prints gibberish, think about why that might happen)

./file: executes whatever is at *file*

Terminal Commands - Permissions

chmod [*perms*] [*file*]: changes the (read, write, execute) permissions *file* to *perms*

The website slides will have more commands here

Terminal Commands - Networking

nc [ip] [port]: netcat, connect to *ip* on port *port*.

ssh user@ip: secure shell, run an instance of terminal as *user* at *ip*. Often a server.

ping [ip]: see if a *ip* is up, but could be firewalled (Windows by default)

The website slides will have more commands here

Next Steps (Bandit)

Try out bandit by overthewire (https://overthewire.org/wargames/bandit/)

Great set of challenges to get introduced to terminal, and the security mindset.

After challenge 20, it gets pretty guessy, so stop at 20.

The security mindset? (Open to floor)

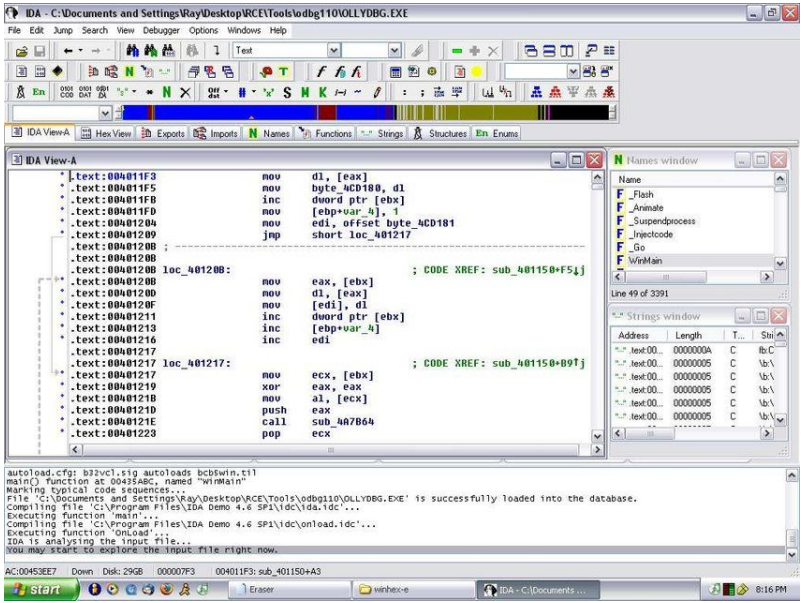
How would you break into Siebel or ECEB?

SIGPWNY

Sub-topics of Computer Security

Topics of Security: RE (Reverse Engineering)

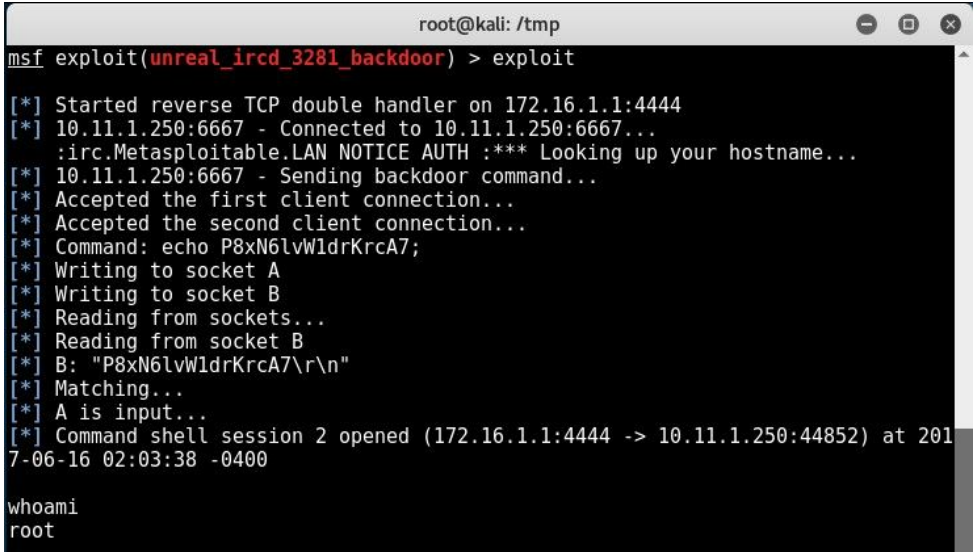
- What is it?
  - Analyzing an app without its source code
- What are some examples?
  - TikTok privacy issues and Antivirus
- Where can I go to learn this?
  - Ghidra, IDA, Old But Gold PowerPoint
- Who can I talk to to learn this?
  - @Chris



SIGPWNY

Topics of Security: PWN

- What is it?
  - Exploiting ane executable to achieve some goal.
- What are some examples?
  - Buffer Overflow to execute shellcode. Reverse shells. Printf exploits
- Where can I go to learn this?
  - Stick around in SIGPwny
  - http://hackthebox.eu (hard!)
- Who can I talk to to learn this?
  - @Ravi



SIGPWNY

Topics of Security: Web

- What is it?
  - Exploiting services or platforms that are based on the web.
- What are some examples?
  - SQL Injection, CRSF, XSS (Those are big 3)
- Where can I go to learn this?
  - Natas by OverTheWire,
- Who can I talk to to learn this?
  - @kuilin

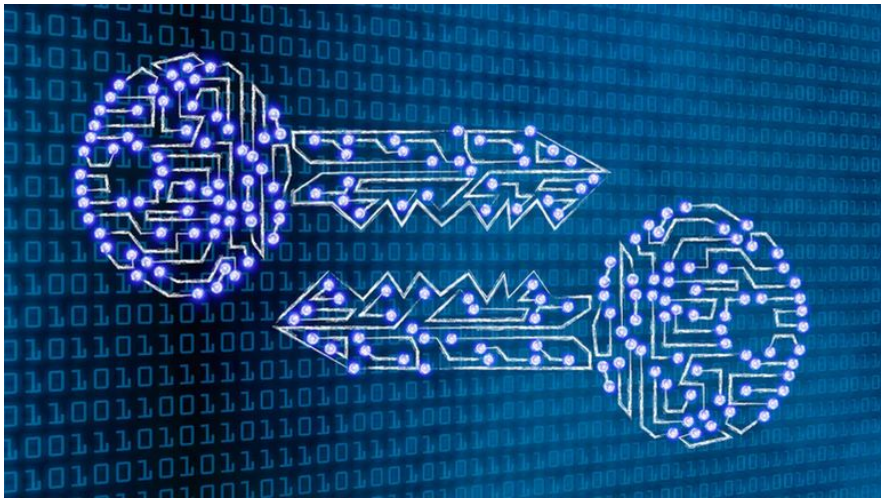
I Googled “Web Hacking” and found this image, how could I NOT use it?

SIGPWNY

Topics of Security: Crypto

- What is it?
  - Secret ~~tunnel~~ communication
- What are some examples?
  - Caesar cipher, Password hashing, HTTPS/TLS protocols
- Where can I go to learn this?
  - Crypto Chals, Python Library for Crypto
- Who can I talk to to learn this?
  - @Jesse / @potatoboy69#1337

“wait, CS 173 is useful for something?”



SIGPWNY

Topics of Security: Forensics

- What is it?
  - Investigating digital content to gather information about various stuff
- What are some examples?
  - Disk, memory, network forensics
- Where can I go to learn this?
  - Practical Packet Analysis
  - Art of Memory Forensics
- Who can I talk to to learn this?
  - @Thomas, @Dillon

SIGPWNY

Topics of Security: Networking

- What is it?
  - Breaking the assumptions of secure communication between two hosts.
  - Hosts can be in a user - user relationship, or a client - server relationship.
- What are some examples?
  - Man in the middle attacks
  - Off path attacks
  - Packet analysis
- Where can I go to learn this?
  - Watch Wireshark Packets, Take CS438, tutorialspoint.com
- Who can I talk to to learn this?
  - @Thomas, @Dillon

SIGPWNY

Topics of Security: OSINT

- What is it?
  - OSINT, or Open Source INTelligence, is gathering information about people through public or semi-public *legal* sources. This information can then be used later when doing another part of a pentest.
- What are some examples?
  - Looking on Linkedin => personal website => personal email
  - Determining information about a person you can use to generate a password list
- Where can I go to learn this?
  - https://osintframework.com/, https://ctf.cybersoc.wales/ (great OSINT CTF), UIUC OSINT Chals
- Who can I talk to to learn this?
  - @Thomas, @Dillon

SIGPWNY

Topics of Security: Everything Else

- What is it?
  - Social Engineering, Physical Security, Hardware Hacking, Phishing, OS Hacking, Password Cracking
- What are some examples?
  - Lock Picking, Hacking a FPGA, Phishing Ravi, Changing an OS to your preferences, Cracking Passwords...
- Where can I go to learn this?
  - Stick around for SIGPwny meetings!
- Who can I talk to to learn this?
  - @Thomas (All Except Hardware and OS), @Ravi (Hardware & OS)

SIGPWNY

How to run a SIGPwny Meeting

We ran a meeting last year on how to run a SIGPwny meeting. If you are interested, go to this link (https://docs.google.com/presentation/d/1bZrHXo6ex-EhHpA9GXj4wJuvVTpzF-xm9Uus4wPLEeo/edit?usp=sharing)

We would love it if you ran a meeting!!!

Questions

Please reach out to any @Helper's on discord,

or email sigpwny@gmail.com