

# Capture the Flag

GrayHats Cybersecurity Club 10/6/2023



# Who are we and what do we do???

- UW Bothell's cybersecurity club!
- Our mission is to prepare the next generation of cybersecurity professionals
- Meeting topics have included:
  - Networking
  - Working with Active Directory
  - Hacking Tools (Physical and Software)
  - Body Language
- Meeting topics will include
  - Whatever your heart's desire

# Why did we start this club?

- UWB doesn't have a very large cybersecurity curriculum
  - Classes are pretty theoretical, rarely get to practice what you learn
  - So we decided to do something about it! We wanted something where...
- 
- |  |  |  |
|--|--|--|
| <ul style="list-style-type: none"><li>- Learning wasn't bound by a curriculum or textbook - and was actually useful IRL!</li></ul> | <ul style="list-style-type: none"><li>- We could actually put our skills to use!</li></ul> | <ul style="list-style-type: none"><li>- We could try stuff and not worry about it impacting our grades</li></ul> |
|--|--|--|

# Our main focuses...

## General Cybersecurity

- Discuss a cybersecurity topic - usually some concept to attack + defend
- Do some sort of cybersecurity related activity to practice concepts

## Cybersecurity Competitions

- Put our skills to the test in a fast paced, more realistic environment
- Usually, we're defending against professional hackers (really!)
- CCDC, Hivestorm, NCL, CTFs

**Make sure to  
sign up on  
Presence!**



# Marko's Insane Linux Foundations ©

Some might refer to it as MILF

# What is Linux?

- An OS like any other
  - Operating System - The program that controls interaction between your programs and the hardware (desktop.) Although made up of multiple parts, an OS is just software
  - Stuff you take for granted is all controlled by the OS - being able to do multiple things at once
  - Made up of three main parts - resource manager, control program, and the **kernel**
- Why is Linux different from other OS's?
  - Lots of "distributions" - versions of the operating system with different goals in mind
    - **Ubuntu**, Debian, TailsOS, Arch Linux, Kali Linux,
  - Stronger open source community
    - Tools are often released for free online, or are "free" as in freedom
    - The kernel (core) itself is posted on GitHub -> <https://github.com/torvalds/linux>
  - Easier to control
    - Important when we come to Digital Forensics and Incident Response (DFIR)
    - Important because it's not Windows
    - "People who specialize in Windows have my undying respect, since they are sacrificing fun for the greater good (of other people being saved from using it)."

4 hours ago 1,216,231 commits

# Basic Linux Command Line (CLI) Usage

- Every command you run actually refers to an executable file somewhere else on the machine
  - Try it out! Open up a “shell” (command prompt) by searching “Terminal” or by trying Ctrl-Alt-T
  - Here’s some sample commands you can run to travel through the file system
    - `cd /bin/` (Travel to the bin folder, which is inside the `/` directory (root directory))
    - `pwd` (Display what folder you’re currently “operating in”)
      - Notice that this is also shown in your shell prompt
    - `ls` (Display the contents of the current directory AKA present working directory (`pwd`))
- Everything is a file
  - It’s true! Files, processes, connections, data streams, the whole shebang (ha)
  - Folders are groups of files, but to traverse the directory, you access a file
    - Try `cd ~`
      - Home directory for your current user. Usually `/home/<user>`, but can change
    - Try `cd .`
    - Try `cd ..`
- Every user you log in as has a certain amount of permissions that can be changed
  - Users can also belong to groups with special membership permissions
  - The “master” of the Linux computer is the “root” user (not to be confused with the directory)
    - This is why pwnng a box is sometimes referred to as “rooting” a box - when you get root, you win

```
ratchet@ubuntu:/bin$
```



# More CLI Tips

- Depending on a command, sometimes you may need or want to provide extra specification on what you want to do
  - This can be to change the function of the command, provide a file input, or otherwise
  - Try doing ls inside the /bin/ directory
  - Now try ls -l
    - This specifies that you want the ls command to behave differently based on the -l “flag”
    - In this case, -l makes the output more detailed. THIS IS NOT THE SAME FOR ALL CMDs
    - If you want to learn more about a command, try man <command> or <command> -h
  - Now try ls -la
    - This is the same as running ls -l -a
      - Same function as -l, but also shows hidden files with the -a flag
      - Order doesn't typically matter, but some flags may require file input, so typically put those at the end of the command
- Linux distributions (distros) usually use a “package manager” to control software
  - With Ubuntu, try doing sudo apt update ; sudo apt full-upgrade -y
  - With Fedora, try doing sudo dnf update --refresh

The background of the slide is a dark blue color with a white circuit board pattern. The pattern consists of various lines, circles, and dots connected by thin lines, resembling a complex electronic circuit.

# Let's hack CTF TIME!

Form teams of two and  
come up with a team  
name

Go to:  
[https://play.picoctf.org](https://play.picoctf.org/register)  
[/register](#) and make an  
account!

# Walkthrough 1 - Mod 26

Mod 26

| 10 points

Tags:

picoCTF 2021

Cryptography

AUTHOR: PANDU

Hints ?

Description

1

Cryptography can be easy, do you know what ROT13 is?

```
cvpbPGS{arkg_gvzr_V'yy_ge1_2_ebhaqf_bs_ebg13_jd  
JBFOXJ}
```


173,843 solves / 178,910 users attempted  
(97%)


90%  
Liked

picoCTF{FLAG}

Submit Flag


# Walkthrough 2 - Nice netcat...

Nice netcat... 

 | 15 points

Tags: picoCTF 2021 General Skills

AUTHOR: SYREAL

Hints 



Description


1

2

There is a nice program that you can talk to by using this command in a shell: `$ nc mercury.picoctf.net 7449`, but it doesn't speak English...

101,779 solves / 106,125 users attempted  
(96%)

 88%  
Liked 

 picoCTF{FLAG}

Submit Flag