CS-501

Introduction to Malware, Threat Hunting
& Offensive Capabilities Development

Course Developers

- Winnona DeSombre (Defensive Security)
- Kai Bernardini (Offensive Security)

$ whoami

- Kai
- Security Consultant
- Vulnerability Researcher / Red teamer
- Lecturer @ BU
- Malware Developer / Threat Hunter
- Allergic to cats
- Totally harmless

$ whoami

- Winnona DeSombre
- Harvard Kennedy School / Georgetown Law
- Women in Security & Privacy Board member
- Former Google TAG (hunting nation state threats)

Course Overview

Abstract

CS501 is an introduction to the wild world of malware analysis and offensive capabilities development. Students will work to analyze, and emulate a simulated APT: APT-Chonky-Bear. In order better defend against attackers, this course takes the stance that it is essential to think like an attacker. Therefore, students will learn the basics of malware reverse engineering, threat hunting and malware development.

Why get into Infosec

- It’s fun :D.
- There is no shortage of interesting work.
- You’ll become really fun at parties.
- The impact you can have is massive
- $$$$

On a serious note, there is nothing wrong with pursuing a career in infosec for the sole purpose of securing economic stability.

Topics

This is the **Third** time the class is being taught.

Depending on how things go, we may cover more or less than what is listed on the syllabus.

Since this is designed to be current, topics might shift according to current events.

ME WHENEVER SOMETHING IN CLASS GOES WRONG
OL' RELIABLE
IT'S THE NTH TIME TEACHING THE CLASS

Goals of the Course

- Create a safe environment to allow students to explore malware
- Create clear paths for students to enter the security community
- Help make everyone here more security literate.
- Get your hands dirty reversing and writing malware

You read that right. In this class you will be writing malware

Malware Capstone

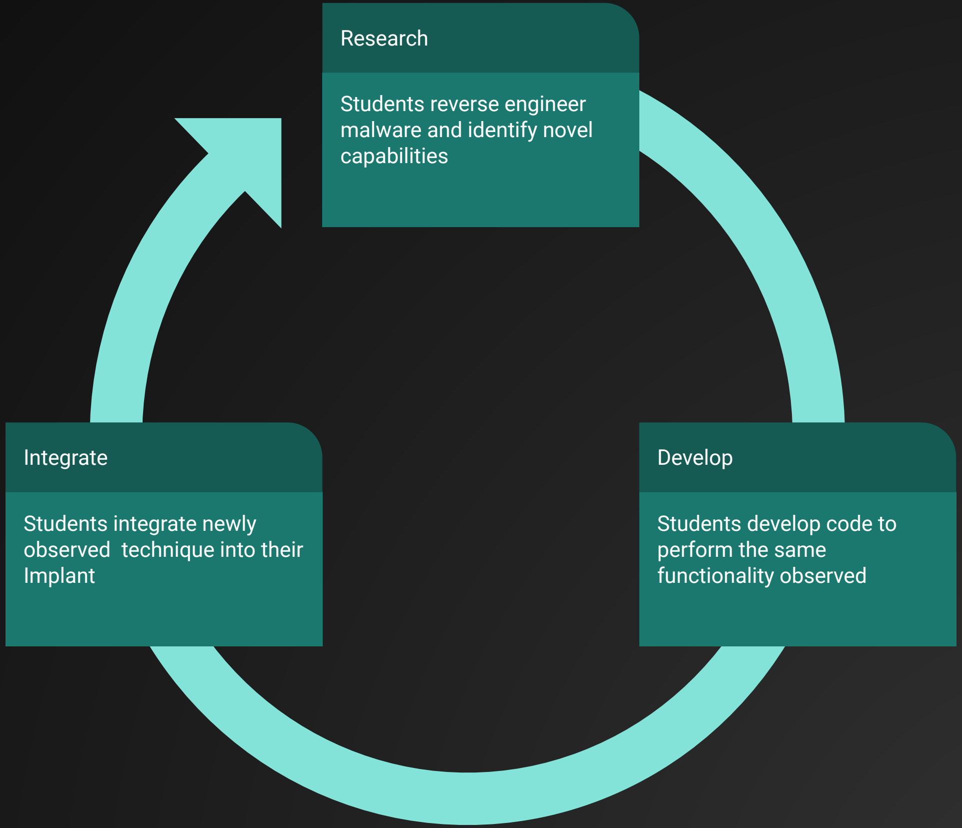
Over the course of a semester, students will reverse engineer and analyze malware, then implement a production ready Remote Administration Tool (RAT) that targets the Windows Operating System.

Ambitious students are encouraged to leverage Porchetta Industries to access sponsorship from the infosec community.

You will also work in a groups for the final capstone project.

Capstone Progression

You will learn how malware works by reverse engineering samples, then reimplementing the capabilities observed.



Research

Students reverse engineer malware and identify novel capabilities

Develop

Students develop code to perform the same functionality observed

Integrate

Students integrate newly observed technique into their Implant

This is a new field. All concepts learned in this class are directly applicable to industry.

Course Success Stories

- Free trip to DefCon
- Introduction to folks from industry
- Jobs lined up for high performers in the course

Baseline Course Policies

Read the Syllabus

Attendance

Attendance is mandatory. Unless cleared with me, you may not asynchronously take the course.

While I record lectures, they are released 2-4 days after they are recorded.

I do not take attendance, but if I notice you missing class, it will affect your grade.

If you need to miss class for any reason, please just shoot me an email, make a private post on piazza, or DM me on discord

Class Comms

- We have a dedicated Discord room on a public server
- I will also respond to email, but will be slower there
- If you have a personal question about course administration, job stuff, or anything else that you don’t think your fellow classmates can benefit from, you may DM
- If someone else can benefit from the question, please ask it publicly.
- If you need help, Ask

Academic Honesty

TLDR: Don’t cheat. Thnx

Cheating and plagiarism of any kind will not be tolerated. Any such incident will result in the very least an automatic zero and could lead to further disciplinary actions. It is your responsibility to know and understand the provisions of the CAS Student Academic Conduct Code.

Students are encouraged to to collaborate on homework assignments but must clearly identify collaborators. You are also welcome to Google answers, but must cite all sources, include all licenses...etc

Rule of Thumb: <u>don’t submit code that you don’t understand</u>. Staff reserves the right to quiz you on any of the code you submit.

Academic Honesty (cont)

- If you submit code that is identical to another classmates, you will fail the assignment.
- If you collaborate when it is expressly forbidden, you will fail the assignment.
- If you copy and paste code in the real world, you are incurring a lot of personal and institutional risk.
- If you would like to work in a group for homework assignments you can where permitted, but you can’t both submit the exact same code. You also need to clearly identify who you worked with and where your sources came from.

Academic Honesty (cont)

- Cheating robs you of the experience of writing your own code, and in turn is a waste of your time and money.
- I will not tolerate anything that compromises your ability to learn in this class.
- Whenever you fail an assignment due to an academic honesty violation, you risk incurring further sanctions.
- You’re all adults, and know the drill.

Academic Honesty (cont)

- I am not a cop.
- You are paying a lot of money to be here.
- It is my job to make sure you get your monies worth

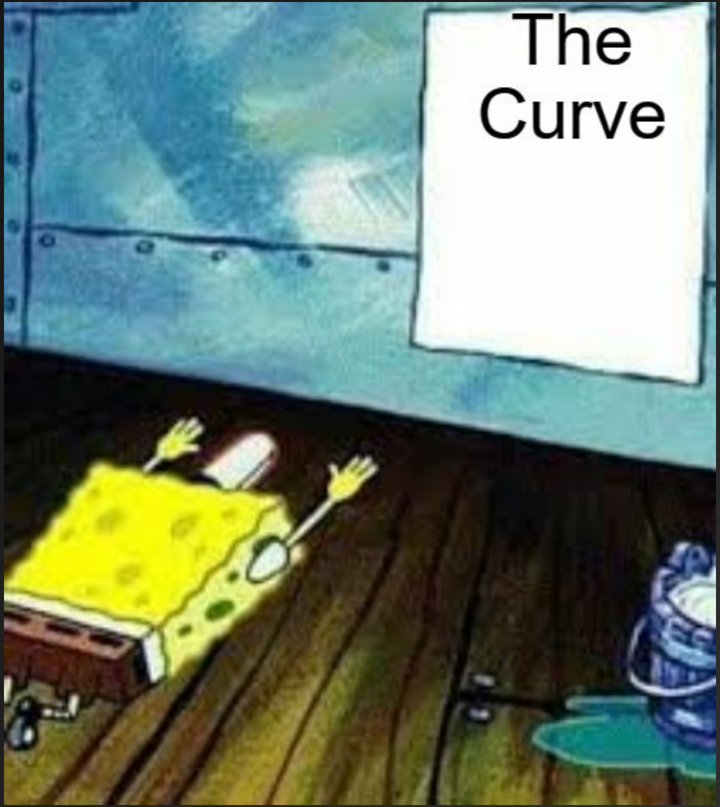
Grading Policies

This is not a weed out course. You get what you put in, use the time to learn and try new things.

There is a curve, and the average is a B+

If you are on the border of a letter grade, I will probably bump it.

I do not curve grades down



Difficulty

- This class is not easy
- The capstone will be very time consuming and will require you to work in a group
- You will get out what you put in!
- Many students have received job offers based on the work they did for the capstone!

Difficulty (cont)

- Coding assignments will require you to read the documentation
- Reading the documentation can feel tedious but is a valuable skill in and of itself.
- Part of reverse engineering is being exposed to techniques you have not seen before
- Assignments will regularly have content that has not been previously covered

There are no stupid questions but I might ask you to Google it :-)

Difficulty (cont)

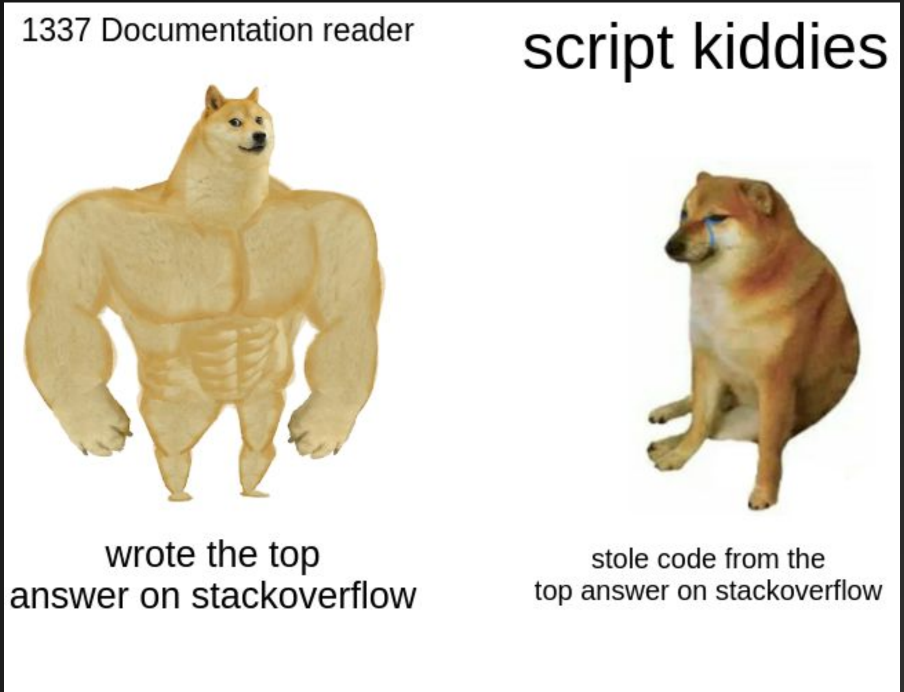
<rant>

Most of this content is simple in hindsight

Simple != easy

Getting comfortable being lost and working out what is happening is an essential skill for hacking

</rant>


1337 Documentation reader
script kiddies
wrote the top answer on stackoverflow
stole code from the top answer on stackoverflow

No Jail plz

DON’T HACK (without express **written** permission)

I AM NOT LAWYER.(IANL)

The Computer Fraud and Abuse Act 1986: bans “intentionally accessing a computer without authorization or in excess of authorization”.

BU will not protect you if you conduct operations or deploy any malware / tools outside your approved lab environment.

We will not bail you out of jail. Do not piss off anybody who has more time and money than you. The laws are intentionally vague, and the **judges are technically illiterate.** You will lose and be made an example of. When in doubt, ask course staff but always error on the side of caution!

Seriously, Don’t Hack Without Permission

Aside from it being illegal, immoral, creepy, and risky, you will fail the class.

Plus, the payout most criminal hackers get is considerably less than if you do the same job but call it “adversary emulation” or run a threat intel company.

Do not F*ck with the Government

The current geopolitical climate is hot.

Countries haven’t regularly resorted to kinetic action in response to hacking, but that isn’t a hard and fast rule. It is a norm that might not be respected tomorrow

Do not, under any circumstances, hack a foriegn or domestic government. They have all the time, all the money, and capabilities that you cannot hope to compete with.

If you really want to do this kind of work, go get a clearance.

Oh and by the way, *kinetic* is a euphemism for killing people.

Use caution when publishing tools

Plenty of researchers publish offensive security tools

Some advance the field, some are published for clout. Be careful with especially sophisticated, easy to use, and low detection tools.

Our job is to advance the security industry, not make script kiddies look good.

Think long and hard about the implications of submitting (for example) a pull request to metasploit or open sourcing a RAT.

Be Thoughtful

Threat actors use open source tools. Don’t be the reason that a hospital gets hit with ransomware or a journalist gets assasinated.

If you do decide to publish tools, make sure to also include countermeasures that defenders can use to combat your tool.

For questions about licenses, responsible disclosure, or advice on whether or not to publish a tool, please contact us! We are happy to provide feedback.

Grading Policy

Late Policy

You are allocated 3 late days for the semester, and may use them at your discretion.

You may ask for more late days for extenuating circumstances. I am usually pretty reasonable when it comes to providing extensions.

Late days may only be used on reverse engineering assignments, or coding assignments.

I will drop the lowest homework grade.

No reverse engineering assignments will be dropped.

There are no late days for the capstone project or exercises.

Assignment Philosophy:

The questions on homework assignments will increase in difficulty.

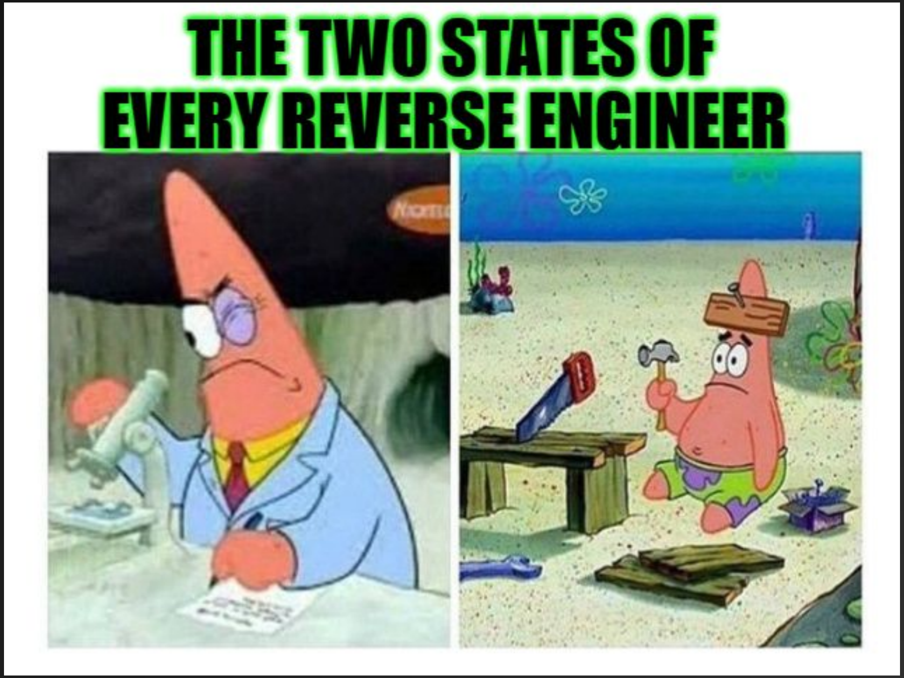
Difficulty should be a spectrum

Often times the solution is *simple*

Simple != easy

RE: Reverse Engineering HW

- Automatically graded for the most part.
- Will be time consuming.
- You are encouraged to to collaborate with classmates
- There are easter eggs for you to find
- Easter eggs (flags) can be submitted for points in the class CTF



Re: Offensive Labs/code

Assignments are automatically graded according to a handful of test cases.

Partial credit is given on a case by case basis, but due to the size of the class, it is not guaranteed anywhere outside of the capstone.

RE: Coding Assignments

- Coding assignments are auto graded.
- Unless otherwise stated, you may NOT work in groups for coding assignments.
- You may only collaborate unless it is explicitly stated.
- **Coding assignments are meant to be completed solo!**

RE: Exercises

- Exercises are weekly, quick turn around homework, and in class assignments
- They are designed to be sanity checks for topics as the course progresses
- They are questions that should take between 5 and 10 minutes
- Questions will always be based on recent material, but topics build on each other
- Bring your laptop to class.

CTF

Stay tuned for details on the semester long competition

There will be a prize and that prize might be an interview at a top tier security firm.

Grading Breakdown

Malware Writeup: 10%

Exercises: 10%

Capture the Flag (CTF): 10%

Reverse Engineering Assignments: 20%

Coding Assignments: 20%

Capstone Project: 30*-50% (if you do really well on the capstone project, I will weight it more)

Bonus Points:

Class Participation: 2.5%

Remarks about Mental Health

- I give incompletes to students who have extenuating circumstances: usually medical emergencies.
- Mental health emergencies are medical emergencies.
  - **No questions asked, no details necessary.**
- There will be some sections that discuss material that may be triggering to some.
- Warnings will be given at the start of such lectures, and attendance is completely optional.

To Reiterate

I give incompletes.

If you say the words “I am having a mental health emergency and need an incomplete” you will get one, zero questions asked.

Please refer to CAS as to what an incomplete entails

Course Lab Environment

Malware = Bad

In this class you will be analyzing and running real malware

In order to reduce the risk of infecting your machine, all suspicious binaries should be run in a *malware sandbox*

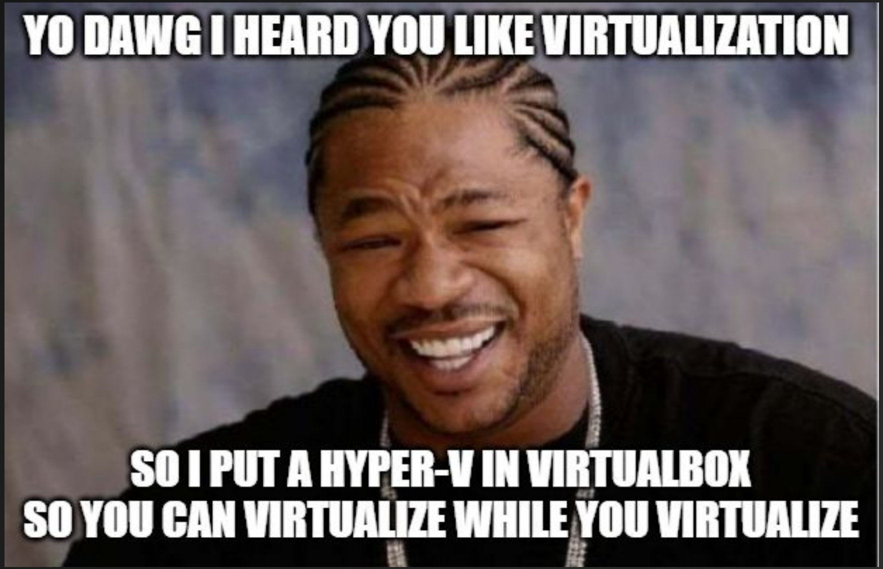
Virtualbox set up

VMWare/Virtualbox: hypervisor software.

Hypervisor: runs virtual machines.

Virtual Machine: software that lets you run a computer on top of your computer

VDI Environment: Hosted environment that hosts virtual machines

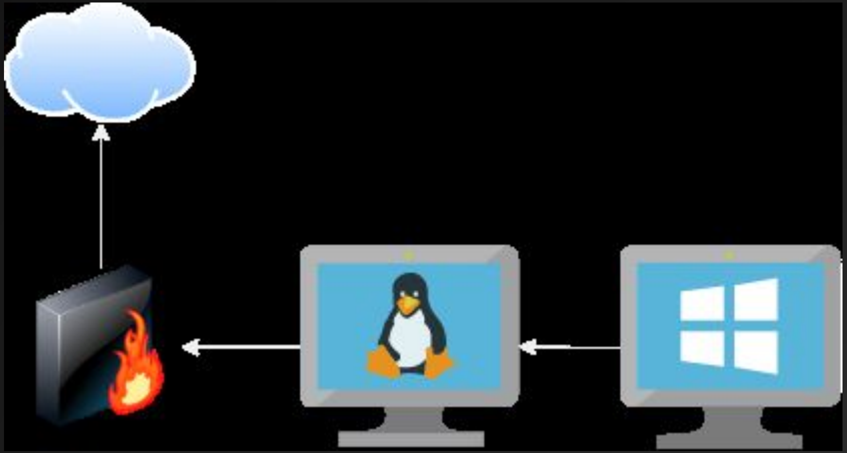

YO DAWG I HEARD YOU LIKE VIRTUALIZATION
SO I PUT A HYPER-V IN VIRTUALBOX
SO YOU CAN VIRTUALIZE WHILE YOU VIRTUALIZE

Course Technology

Your first assignment is to create A malware analysis sandbox.

To accomplish this, you will make use of

- Virtualbox (hypervisor)
- Windows x1-2 (analysis and development)
- Remnux x1 (Think Kali linux but for malware analysis)



Course Lab Environment

You are free to use any lab setup that you like, but the course staff will only provide technical assistance for VMs and Virtualization software officially supported by the class.

See Course Documentation for a walkthrough.

Remember, take lots of Snapshots. VMs can sometimes be bit unstable.

Mac M1 Users

For folks who only have access to computers that have ARM based CPUs (eg Mac M1/M2) please contact me and I will get you setup on the VMware Learn platform but it is not as smooth as using an a computer with an Intel/AMD CPU

More Elaborate Setups

This lab setup is not sufficient for a real world triage environment

For those of you who are interested, I will publish a bonus lecture that details how to use QEMU with KVM/HAXM to create a more robust malware sandbox complete with a Firewall, analysis env…etc

Course Administrative Technology

Students are encouraged to join the class Discord generously hosted by Porchetta Industries.

All assignments are to be submitted through GradeScope

Classes will be recorded, but attendance is mandatory

Course Notes will use Obsidian.md and Google slides

Requirements: Courses/Topics

- CS-131/Combinatorics
- CS-237/Probability (recommended)
- CS-210/Computing systems : familiarity with memory management, c programming, reading assembly, using debuggers and compiler toolchains.
- CS-357/Basic cryptography: familiarity with Ciphers, MACs and Hash functions. Ideally also the idea behind asymmetric cryptography
- Recommended: CS-460 (TCP/IP/UDP/HTTP/TLS)

Requirements: Courses/Topics

- CS-131/Combinatorics
- CS-237/Probability (recommended)
- CS-210/Computing systems : familiarity with memory management, c programming, reading assembly, using debuggers and compiler toolchains.
- CS-357/Basic cryptography: familiarity with Ciphers, MACs and Hash functions. Ideally also the idea behind asymmetric cryptography
- Recommended: CS-460 (TCP/IP/UDP/HTTP/TLS)

Requirements: Tools

- GDB/experience debugging native binaries
- Experience with compiler toolchains (compilers, linkers)
- Wireshark is a plus
- As is Ghidra/ some other SRE framework

Requirements: Programing/scripting

- Python 3: you need to be very proficient with python.
- c/c++/some other systems programming language: you should be able to write simple C programs, know the difference between Stack and Heap memory, and how to manage memory
- intel x86 assembly: you should be able to read x86 assembly.
- Being able to write assembly is a plus!

Requirements: Protocols

- IP: you should know the difference between a private and public IP, the basics of addressing, and know the relationship between a domain name, DNS and an IP address
- TCP: More so the basics of socket programming, less so the internals of how reliability is achieved or what the handshake process looks like.
- DNS: You don't need to understand **how** DNS works, but you need to know what it does.
- TLS: You need to understand what a Certificate Authority is, a TLS cert is, and the basics of establishing secure tunnels
- HTTP(s): HTTP verbs, request structure, and error codes

Requirements: Computer

- Ability to run 1 heavy VM and 1 lighter vm simultaneously.
- For that, you probably need a minimum of 8GB of RAM, a decent CPU, at least 100GB of storage
  - If your computer is low on space, you can install the VM in an external SSD connected via USB3. You can find these at microcenter for around $50-100
  - Ideally, you should have 16GB of ram and should separate your development environment from your sandbox
- Intel based CPU.
- Internet connection

Remarks about pre-requisite

Is Infosec for me?

Short answer: yes

Long answer: also yes

Do I have the right background for this class?

- Take a look at HW 0.
- If you are lost, it might be a good idea to take this course next semester! You are welcome to stick it out but you might need to put in extra work.

Course Livestream

The course will be streamed via zoom

Office Hours

T/Thr after class in my office.

Where is my office?

Good question. I don’t know :D

Bonus/Guest Lectures

Experts from industry, some of which are hiring, will periodically swing by to give a bonus lecture

You should come if you can make it!

Questions?

Homework

- Join Discord
  - https://porchetta.industries/ join the discord
- Join Gradescope (Do it.).
  - You should receive an email to join Gradescope
- Download the VMs and setup your development environment
  - You will need very good internet connection for this.
  - Coffee shop internet will not cut it.
  - This will take a LONG time. Do not do this the night before
  - Remnux takes ~1-2 hours to set up if built from scratch
  - Windows takes ~1-2 hours to set up
  - In both cases, you can kick it off then go AFK
  - You should carve out some time in case you need to debug.

Homework (Continued)

The first assignment will be released later tomorrow

It will require a working Lab environment

It may or may not have some easter eggs :-)

Discussion

What is malware?