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
- 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.

Topics

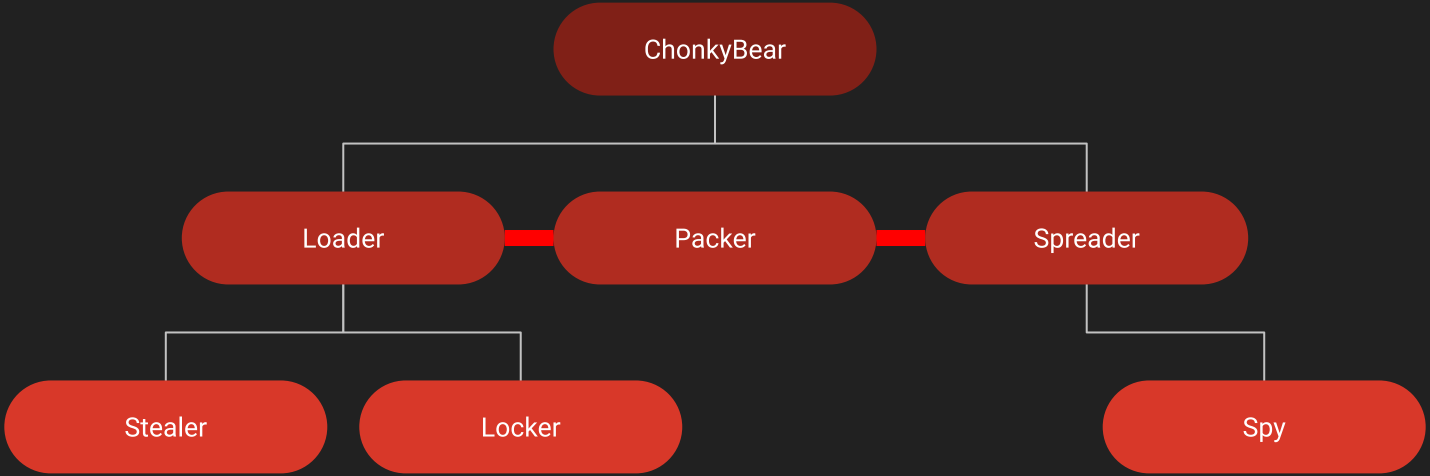
This is the first time we are teaching the class. Depending on how things go, we may cover more or less than what is listed on the syllabus.

Since this is designed to be current, we might also analyze novel malware

Goals of the Course

- Create a safe environment to allow students to explore Infosec.
- Get more people involved with the community, help make everyone here more security literate.

APT ChonkyBear



ChonkyBear

Loader

Packer

Spreader

Stealer

Locker

Spy

Malware Capstone

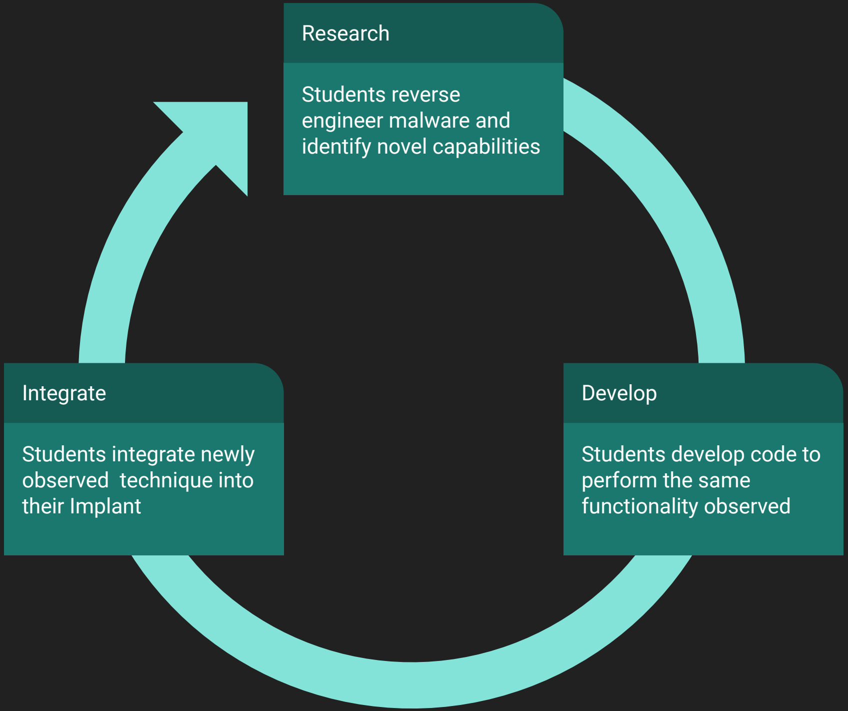
Over the course of a semester, students will reverse engineer and analyse malware, then implement a production ready Remote Administration Tool (RAT) that targets the Windows Operating System.

Ambitious students are encouraged to leverage Porchetta Industries to make productionizing code simpler, and to access sponsorship from the infosec community.

You may also work in a group for the final capstone project.

Capstone Progression

Students will learn about how malware works by reverse engineering malware, 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

Baseline Course Policies

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: don’t submit code that you don’t understand. Staff reserves the right to quiz you on any of the code you submit.

Grading Policies

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

Re: offensive labs / code -
If the code compiles and is a best effort, you’re good (B). If it passes all the tests, automatic A.

Re: technical writing / RE -
all indicators of compromise found and described, clear description of what the code does, and clear definitions of jargon. Attribution analysis (if applicable) is clear. Auto A.

Re: Capstone: If it has all the required capabilities you’re good (B). If the “special” feature works and your presentation is coherent,, automatic A. There is no final exam. .

Breakdown:

Class Participation: 5%

Scrie: 5%

Written Assignments: 20%

Reverse Engineering Assignments: 20%

Coding Assignments 20%

Capstone Project: 30%

Scribe

Each student will be responsible for taking notes and submitting them to the course obsidian.md repository for at least one lecture.

You are welcome to contribute periodically for extra credit (up to an additional 5%)

See https://obsidian.md/

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

DON’T HACK (without express written permission)

WE ARE NOT LAWYERS.

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 used in this class 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 completely illegal, immoral, creepy, and risky, the payout most criminal hackers get is considerably less than if you do the same job but call it “adversary emulation.”

Do not F*ck with the Government

As a remark, 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, and hasn't always been in the past.

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.

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

Use caution when publishing tools that can be misused

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 space, not make script kiddies look good.

Think long and hard about the implications of submitting (for example) a pull request to metasploit or publishing a hooking library.

Be careful

Threat actors use opensource tools. Don’t be the reason that a hospital gets hit with ransomware or a human rights activist 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 course staff. We are happy to provide feedback.

Questions about course / career / industry?

HWK 0: Environment set up + Academic Honesty / NOHACKME agreement

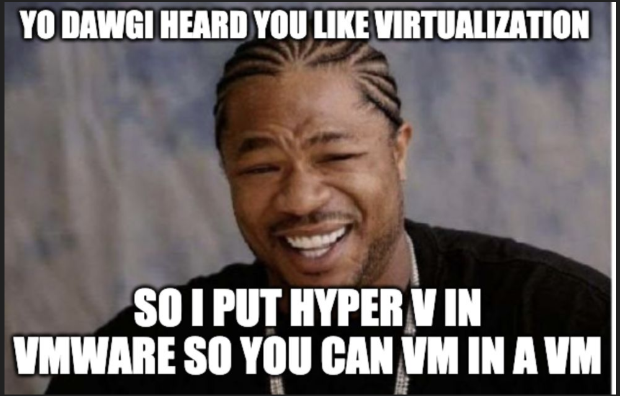
Virtualbox set up

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 DAWGI HEARD YOU LIKE VIRTUALIZATION
SO I PUT HYPER V IN VMWARE SO YOU CAN VM IN A VM

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.

Course Administrative Technology

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

Students are required to join the class Piazza group. This is where all course lectures will be located.

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

Syllabus at a Glance

Remarks about Expertise

Remarks about Mental Health

We want you to succeed and have fun, but at the same time we want to be clear:

- Course staff will only give an incomplete to students who are experiencing extenuating circumstances.
- Mental health emergencies are extenuating circumstances
  - We aren't detectives. If you are are struggling with mental health, all you need to do is contact course staff and we will do our best to accomodate you.
  - **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.

Questions?

Discussion

What is malware?