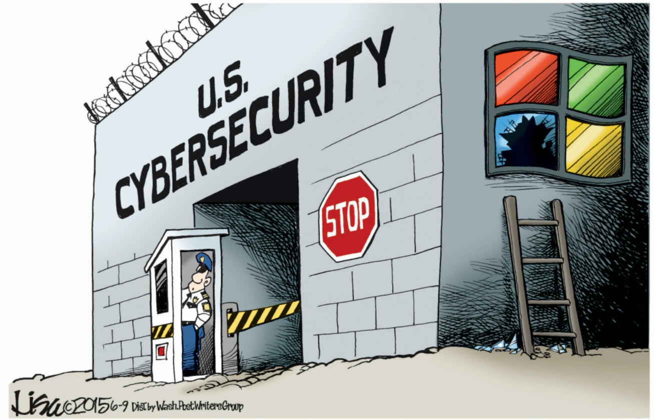
CSIS 641
Advanced Cybersecurity

COLLEGE of CHARLESTON

1770

"The quality or state of being secure—
to be free from danger"

Today, January 11, 2021



- Introductions
- Syllabus
  - Papers, Labs and the Project
- Focus of the Class
- Interlude
- Environment Building

Who am I?

Naval Information Warfare Center

ATLANTIC

Papers

- Each of you will be doing two (2) presentations on research papers
- This is not a ”book report”
- Explain the material in the paper such that your quasi-technical boss could understand it
  - You will have to do the appropriate research to figure out terms you’re not familiar with
- Lead a discussion on the paper
- Everyone is expected to have read and prepared 2 or more questions on the paper that will be used during the discussion

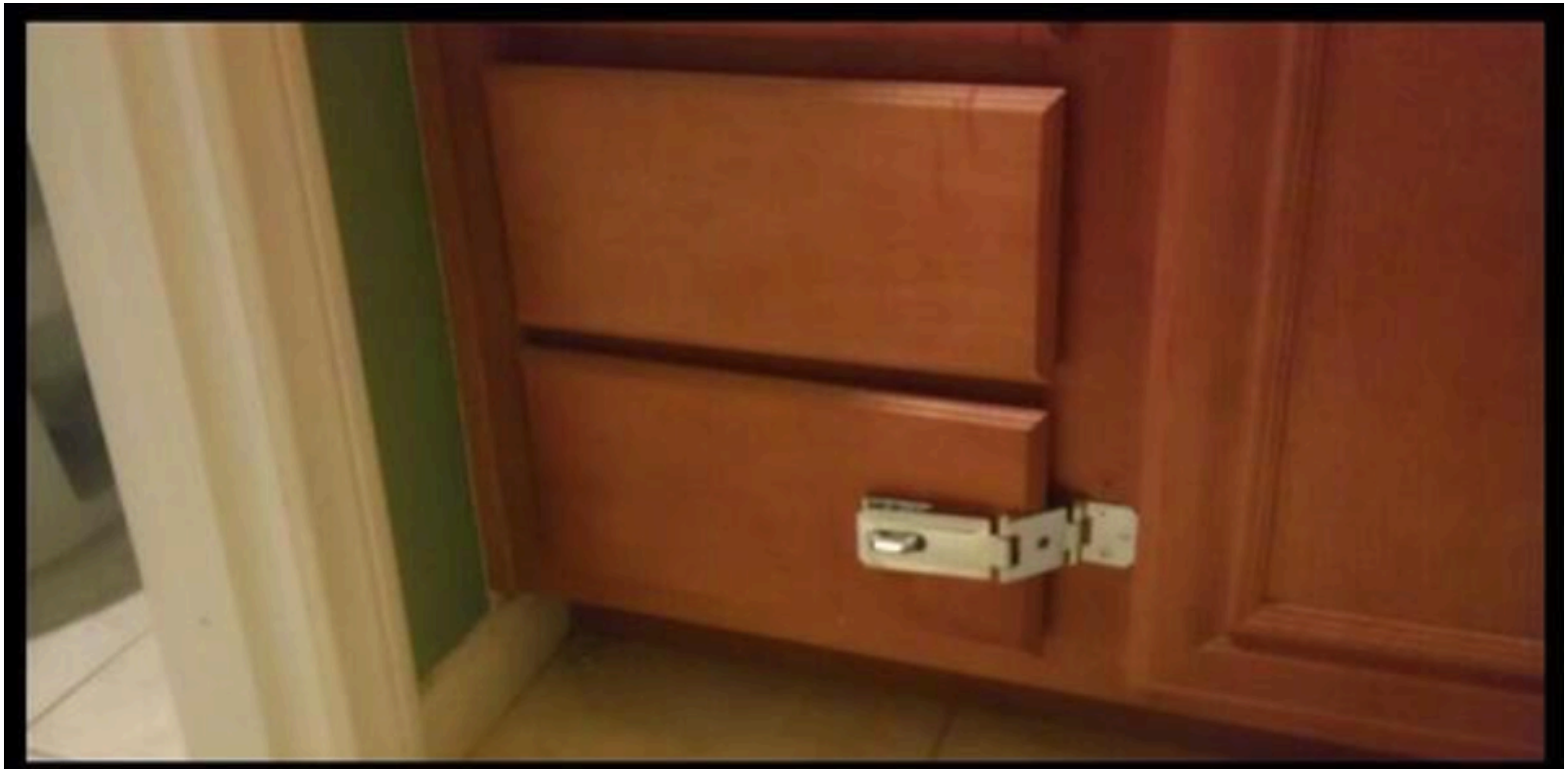
Labs

- There will be multiple parts to each lab.
- Produce a report detailing:
  - What the lab is intended to accomplish
  - The process you followed
    - A chronological log is a good way to do this
  - Issues and problems encountered during the process
  - The results obtained from the lab
    - Include screen shots, excerpts from console logs, etc. as part of the report, not separate files.
  - Analysis and conclusions can can be drawn from the lab
  - Any references (e.g. web resources) you used.
- Report will be submitted to Oaks in PDF (and only PDF) format.

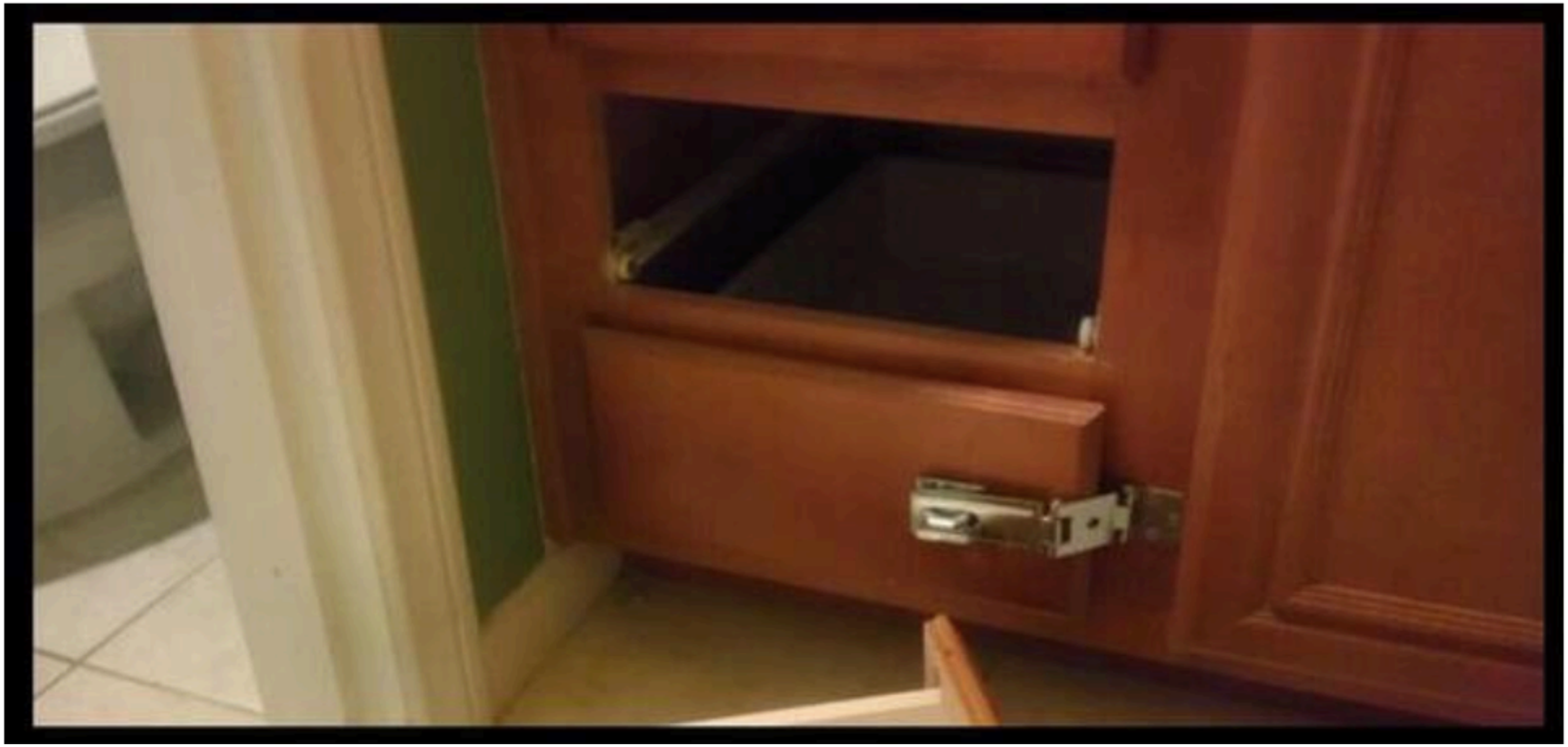
Project

- The project will be presented to the class during the Finals slot
- The expectation is that you will produce a report as well as a 15-20 minute presentation
- Each student will be responsible for selecting the topic
- There will be two other checkpoints along the way
  - Topic selection
  - Project outline

What is wrong with this picture?



What is wrong with this picture?



The Security "mindset"

- Think critically
- Challenge assumptions
- Be curious
- Think about weaknesses
- Be neurotic

Why it's important

- Technology changes, so learning to think like a security person is more important than learning specifics of today
- Will help you design better systems/solutions
- Interactions with broader context: law, policy, ethics, etc.

What is Security?

- “The quality or state of being secure—to be free from danger”
- A successful organization should have multiple layers of security in place:
  - Physical security
  - Personal security
  - Operations security
  - Communications security
  - Network security
  - Information security

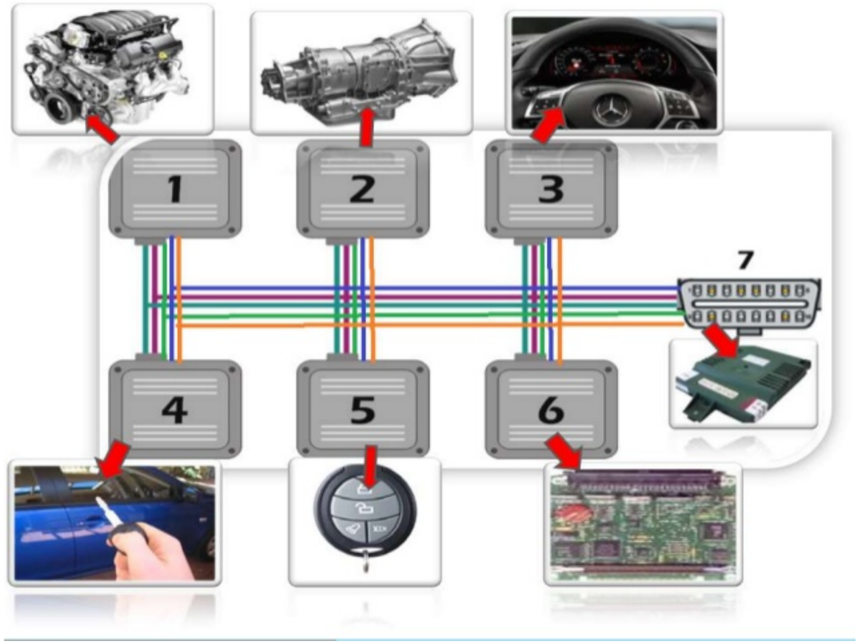
Definitions

- Penetration Testing
- Black Hat/White Hat
- Attack Surface
- Trust (as it pertains to Cyber)
- Data and Metadata

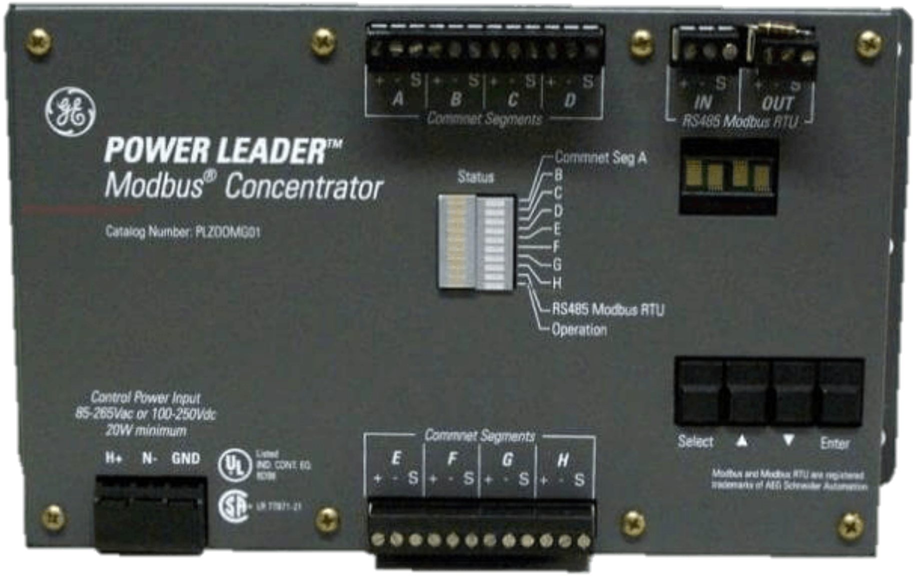
Security in Organizations

Origins

- CAN Bus



- Modbus



Activities

- Espionage
  - Nation States
  - Industrial
- Criminal Activity
  - Extortion
  - Theft
- Insurrection
  - Political Movements
  - Resistance to Authority
- Anarchy
  - Just to prove it can be done

Pen Testing Phases

- Reconnaissance
    - What can be learned about the target?
- Scanning
    - How can we get access to the target?
- Exploitation
    - OK, what do we want to do now that we’re here?
- Follow-on activities
    - Retaining access

Attacks (OWASP)

- Abuse of Functionality
- Data Structure Attacks
- Embedded Malicious Code
- Exploitation of Authentication
- Injection
- Path traversal
- Probabilistic techniques
- Protocol Manipulation
- Resource Depletion
- Resource Manipulation
- Sniffing
- Spoofing

Critical Characteristics of Information

- The value of information comes from the characteristics it possesses:
  - Availability
  - Accuracy
  - Authenticity
  - Confidentiality
  - Integrity
  - Utility
  - Possession

Balancing Information Security and Access

- Impossible to obtain perfect security—it is a process, not an absolute
- Security should be considered balance between protection and availability
- To achieve balance, level of security must allow reasonable access, yet protect against threats

Interlude

Deplatforming

- Rogers, Richard. "Deplatforming: Following extreme Internet celebrities to Telegram and alternative social media." *European Journal of Communication* (2020): 0267323120922066.
- Jardine, Eric. "Online content moderation and the Dark Web: Policy responses to radicalizing hate speech and malicious content on the Darknet." *First Monday* (2019).
- Urman, Aleksandra, and Stefan Katz. "What they do in the shadows: examining the far-right networks on Telegram." *Information, communication & society* (2020): 1-20.

Basics

- Obsfucation
  - TOR
  - DuckDuckGo
- Personal protection
  - Private browsing (ha ha)
  - Firewalls
- Tools of the Trade
  - Best equipment you can afford
  - Cloud services

Environment Building

- Virtual Box
- Kali Linux
- Ubuntu Server

For Next Time

- Download .iso files for
  - Kali Linux
  - Ubuntu Server
- Build VMs for
  - Kali Linux
  - Two or more Ubuntu server VMs