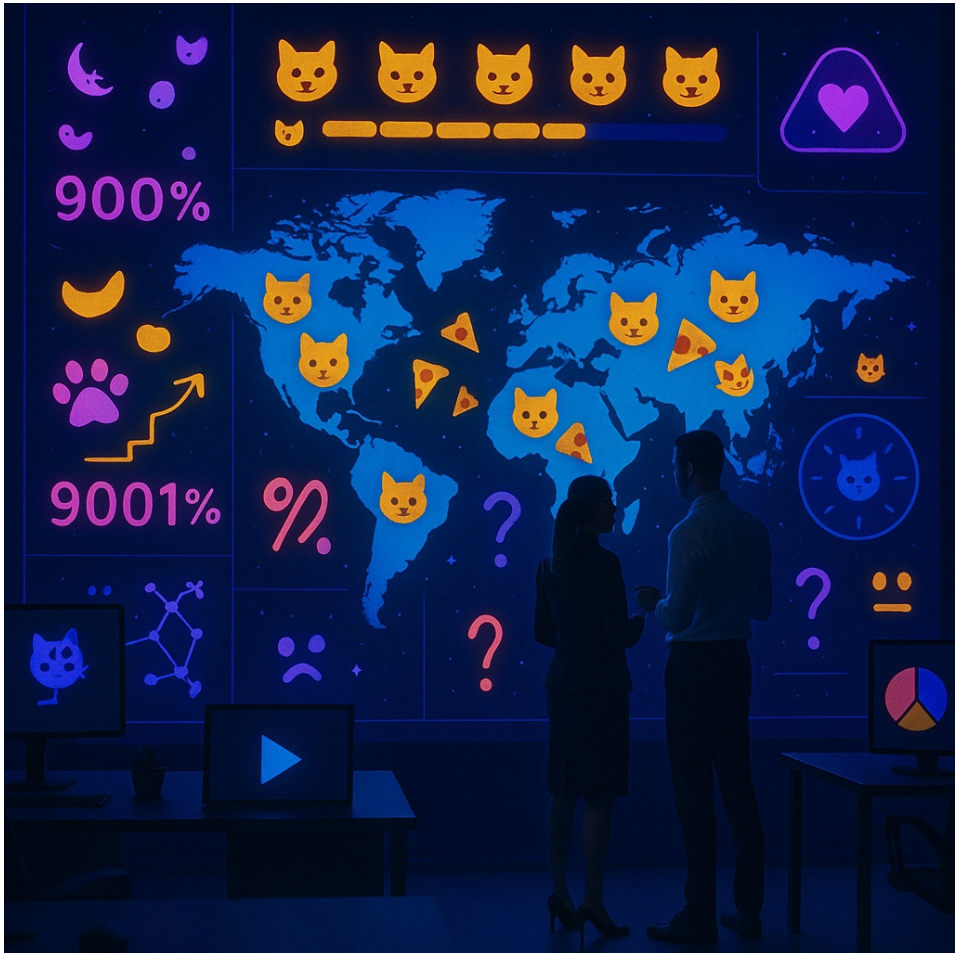
Welcome to Cybersecurity!



Word of the day

HACK VALUE n. Often adduced as the reason or motivation for expending effort toward a seemingly useless goal, the point being that the accomplished goal is a hack. For example, MacLISP had features for reading and printing Roman numerals, which were implemented purely for hack value. Hack value cannot really be explained, only experienced. As Louis Armstrong once said when asked to explain jazz: “Man, if you gotta ask you'll never know.”

About me

- Jeffrey Knockel (call me “Jeff”)
- My research?

About me

- The apps that are running on your phone and laptop, how do you know that they are keeping you safe?
- What if your phone’s keyboard app is phoning home everything you type?
- What if your browser doesn’t properly encrypt your sensitive information and anyone on the Internet can read it?

About me

- I find these instances
- I call them out
- And I get them fixed


SHISEIDO
Nan Xiang Xiao Long
139

Introductions

- What is your preferred name?
- What is a fun fact about yourself?
- Why did you decide to take this class?

In this semester, you will...

- Hack your grades from Fs to As
- Create a self-propagating worm
- Break major encryption algorithms
- Develop a memory exploit that bypasses modern operating system protections
- And more!

Syllabus

- https://tildesites.bowdoin.edu/~j.knockel/csci3330f25/syllabus.pdf

Syllabus highlights

- Grading weekly assignments: scored on completion only. Correctness will be marked but only for your information.

Generative AI Policy

- Don’t be a script kiddie!

Word of the day (bonus)

SCRIPT KIDDIE n. 1. [very common] The lowest form of cracker; script kiddies do mischief with scripts and rootkits written by others, often without understanding the exploit they are using. Used to describe people with limited technical expertise using easy-to-operate, pre-configured, and/or automated tools to conduct disruptive activities against networked systems. Since most of these tools are fairly well-known by the security community, the adverse impact of such actions is usually minimal.

2. Someone who cannot program, but who creates programs by copying routines from other programs. More generally, a script kiddie writes (or more likely cuts and pastes) code without either having or desiring to have a mental model of what the code does; someone who thinks of code as magical incantations and asks only “what do I need to type to make this happen?”

Ask me questions!

- Email
- Slack
- Office hours
- Learning how to ask questions is an important skill in cybersecurity!

Ask me questions!

- I strive for max 24 hour turnaround on class questions (often 24 minutes).
- Tips for email success:
  - Use plain text: no HTML, no weird encoding
  - Don't attach files casually – cut and paste ***selected*** parts as needed.
  - Be as specific as you can.
  - Be sure actually to ask a question!

Less successful question

- Subject: My code doesn’t work?
- Attachments:
  - PreviousVersion.c
  - Copy of assignment (2).c
  - AnOldShoe.c

Less successful question

- Subject: Today’s lecture

  Today’s lecture was confusing. Could you explain it?

Successful question

- Subject: string equality comparison

```
Isn't it okay to use == on Strings?  I tried this:

   String s1 = "foo", s2 = "foo";

   if (s1 == s2) System.out.println("equal");

and it printed 'equal'.  So isn't '==' as good as
s1.equals(s2)?

Thanks.
```

Syllabus highlights

- Bring your laptop to class!

Syllabus highlights

- Anonymous feedback:
- https://cryptpad.fr/form/#/2/form/view/tiBld9vIC14L1gX5238y5-2lxZ9TaCwKSA+J0zfS92k/

Syllabus highlights

- Questions?

What is Cybersecurity?


AVX:
Enabled
ST Mode
Enabled
xT Mode
Disabled
Attributes:
Sector S3
Local Attributes:
View
Data
Settings
Connections
Connections
Tracking
Advanced Monitoring
Activity:
Up time 27:14:27:53
Signal
Frequency:
12.75 G
Trackers:
51260
Utilisation:
85 %
Data Compre
1/72

What is Cybersecurity?

- The science of keeping people digitally safe

What is Cybersecurity?

- The science of keeping people digitally safe
- A better name for this class is cyber***in***security
- Attacks and defenses

What does “hack” mean?

- It depends!

What does “hack” mean?

- It depends!
- A quick job that produces what is needed, but not well.
- An incredibly good, and perhaps very time-consuming, piece of work that produces exactly what is needed.

What does “hack” mean?

- It depends!
- To break security on a system.

The essence of this class

- I want you to learn to think like a hacker.

A story of a recent hack of mine

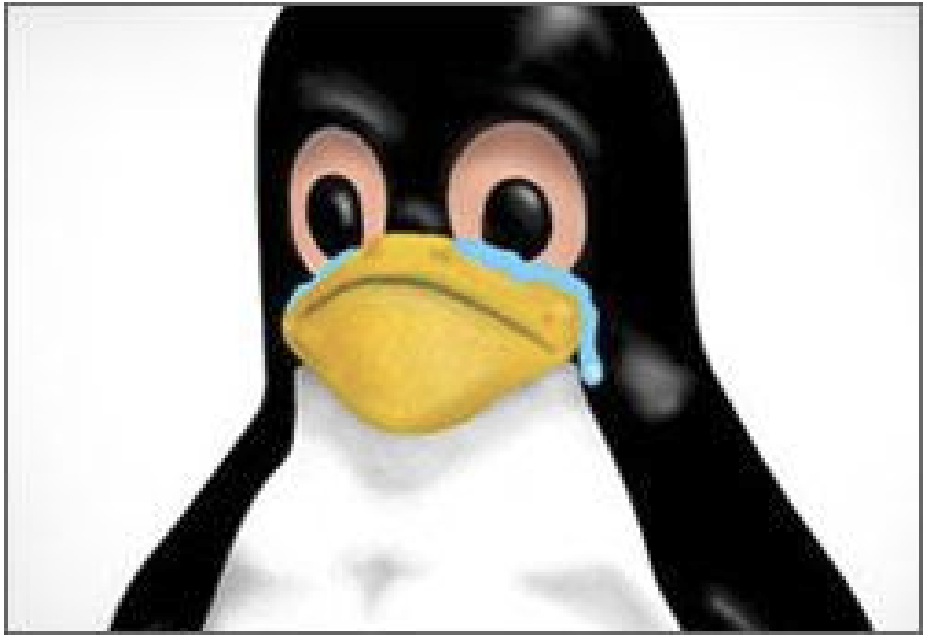
- Not my most glorified
- But that’s why I like it
- Because it emphasizes the everyday lifestyle of being a hacker

Story of how Jeff printed some documents

Chapter 1: Jeff needs a state license

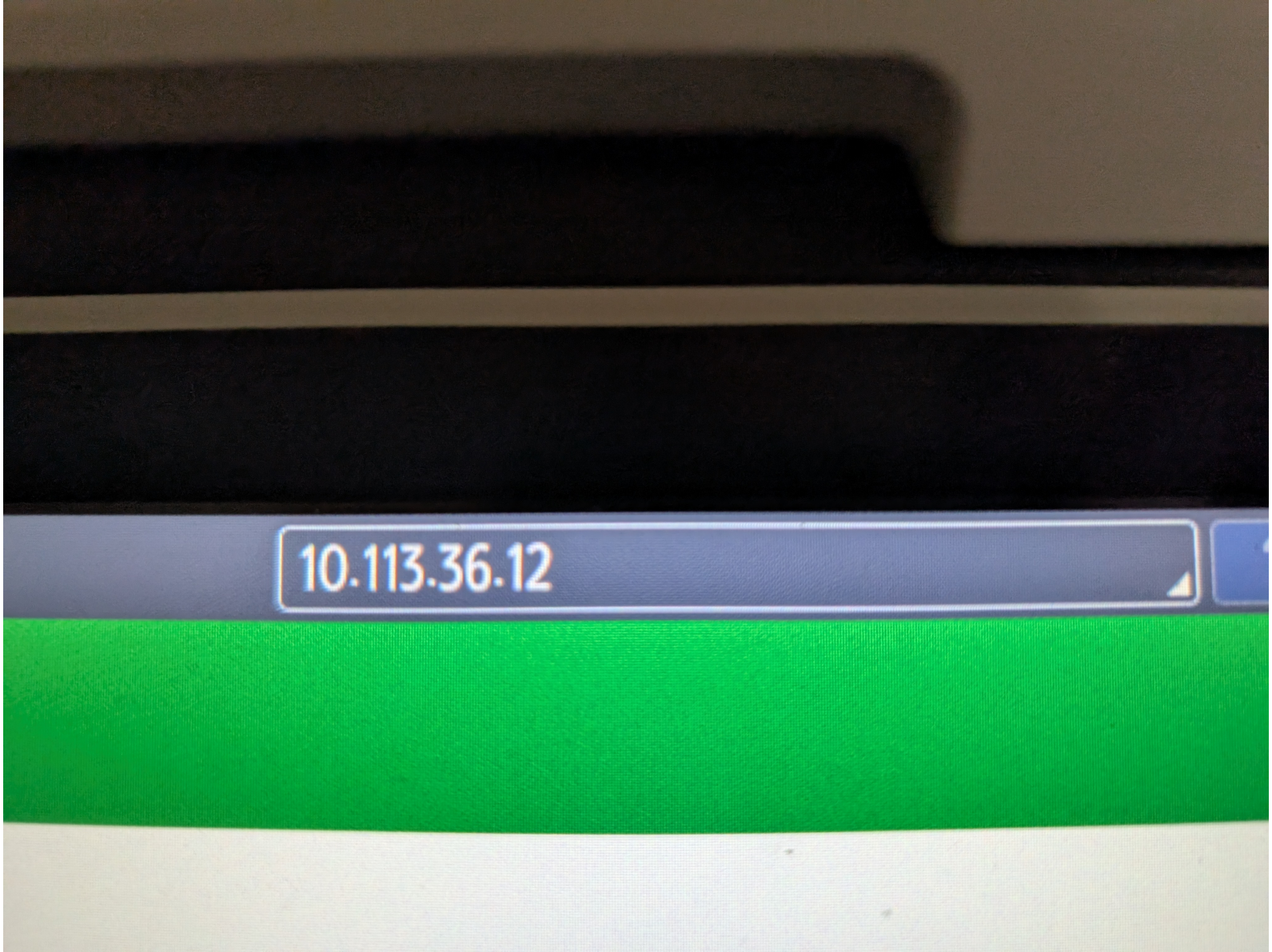
- I moved here, need a state license
- Needed documents establishing residency, etc.
- My printer is somewhere in Canada still
- PaperCut!?

Chapter 2: A block in the road



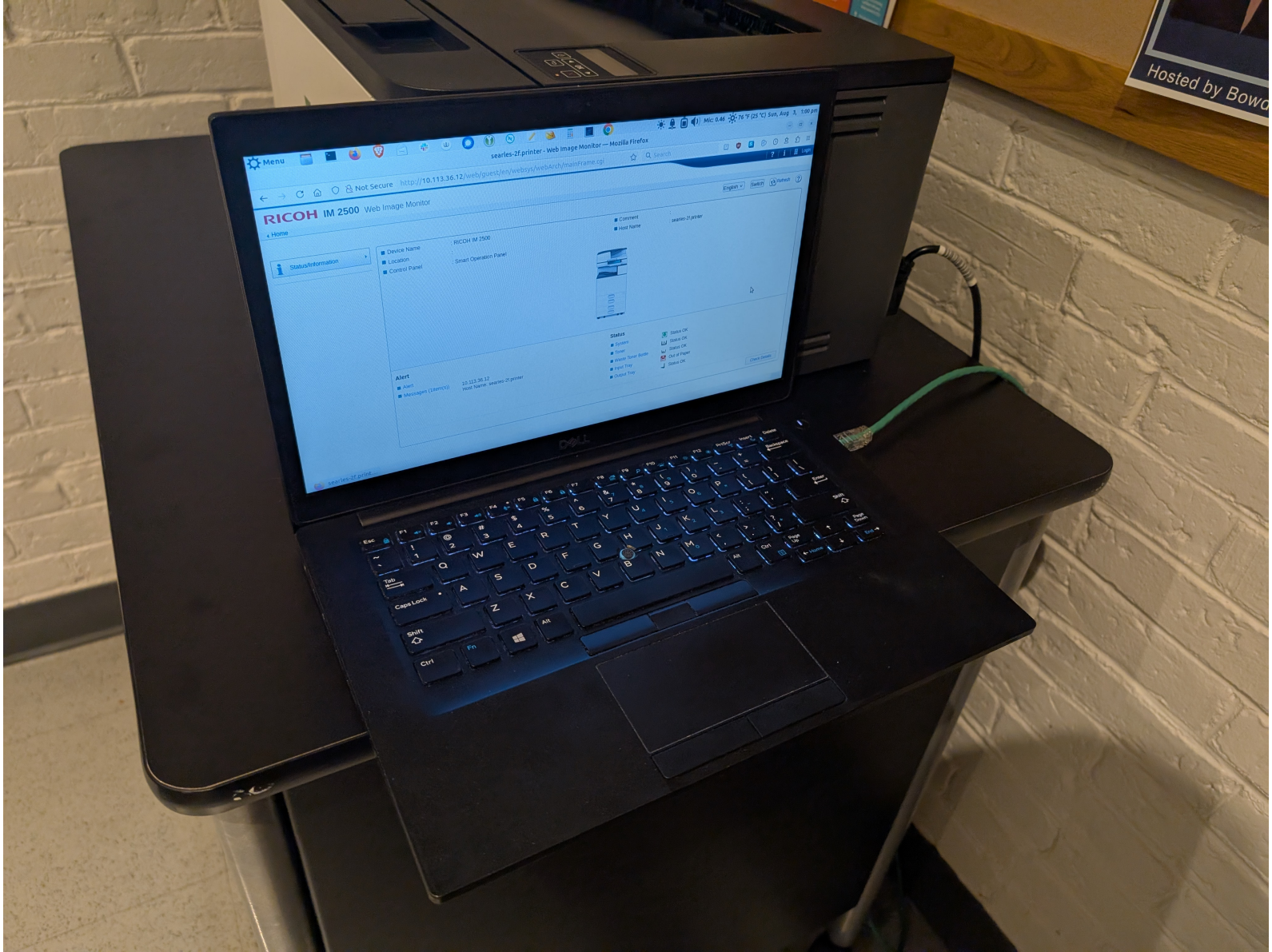
Chapter 3: Jeff does some poking around

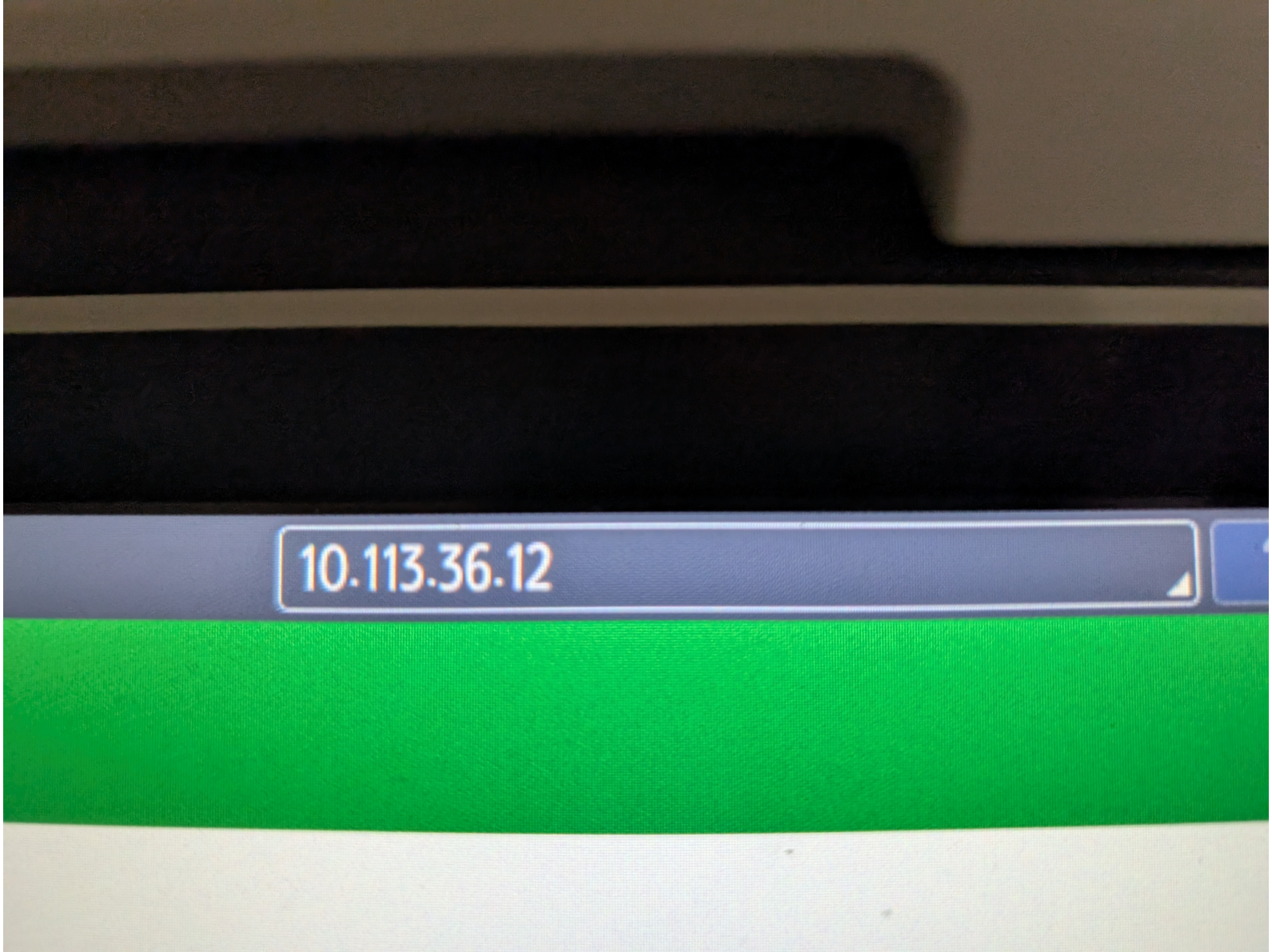

Status
10.113.36.6
OK


10.113.36.12

IP address?

- CIDR notation?
- 10.0.0.0/8
- 192.168.0.0/16
- 192.168.xxx.0/24


searles-2f.printer - Web Image Monitor — Mozilla Firefox
Not Secure http://10.113.36.12/web/guest/en/websys/webArch/mainFrame.cgi
RICOH IM 2500 Web Image Monitor
Home
Status/Information
Device Name
Location
Control Panel
RICOH IM 2500
Smart Operation Panel
Alert
Status
Hosted by Bowa


10.113.36.12

searles-2f.printer - Web Image Monitor — Mozilla Firefox

Not Secure http://10.113.36.12/web/gue

Search

RICOH IM 2500 Web Image Monitor

Login

Home

English Switch Refresh

Status/Information

Device Name	: RICOH IM 2500	Comment	:
Location	:	Host Name	: searles-2f.printer
Control Panel	: Smart Operation Panel		

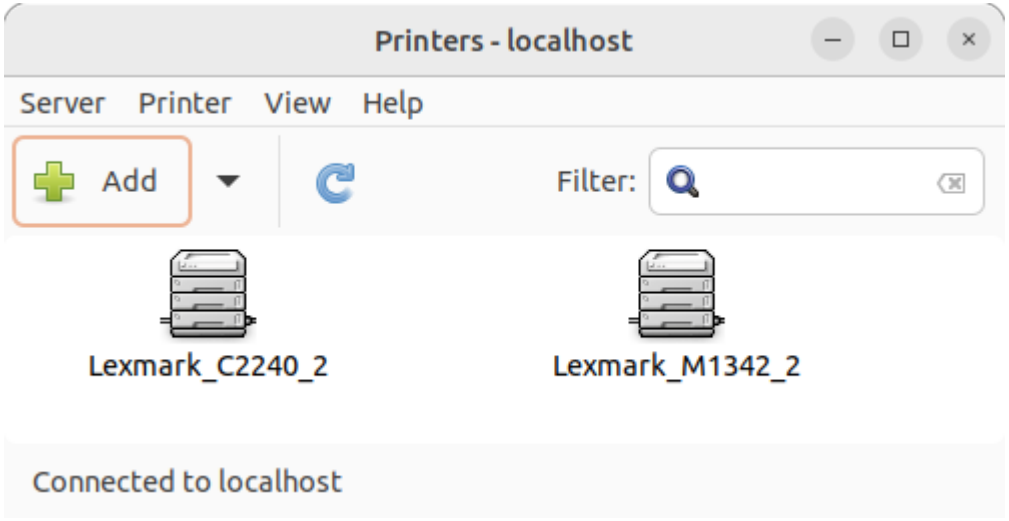
Alert

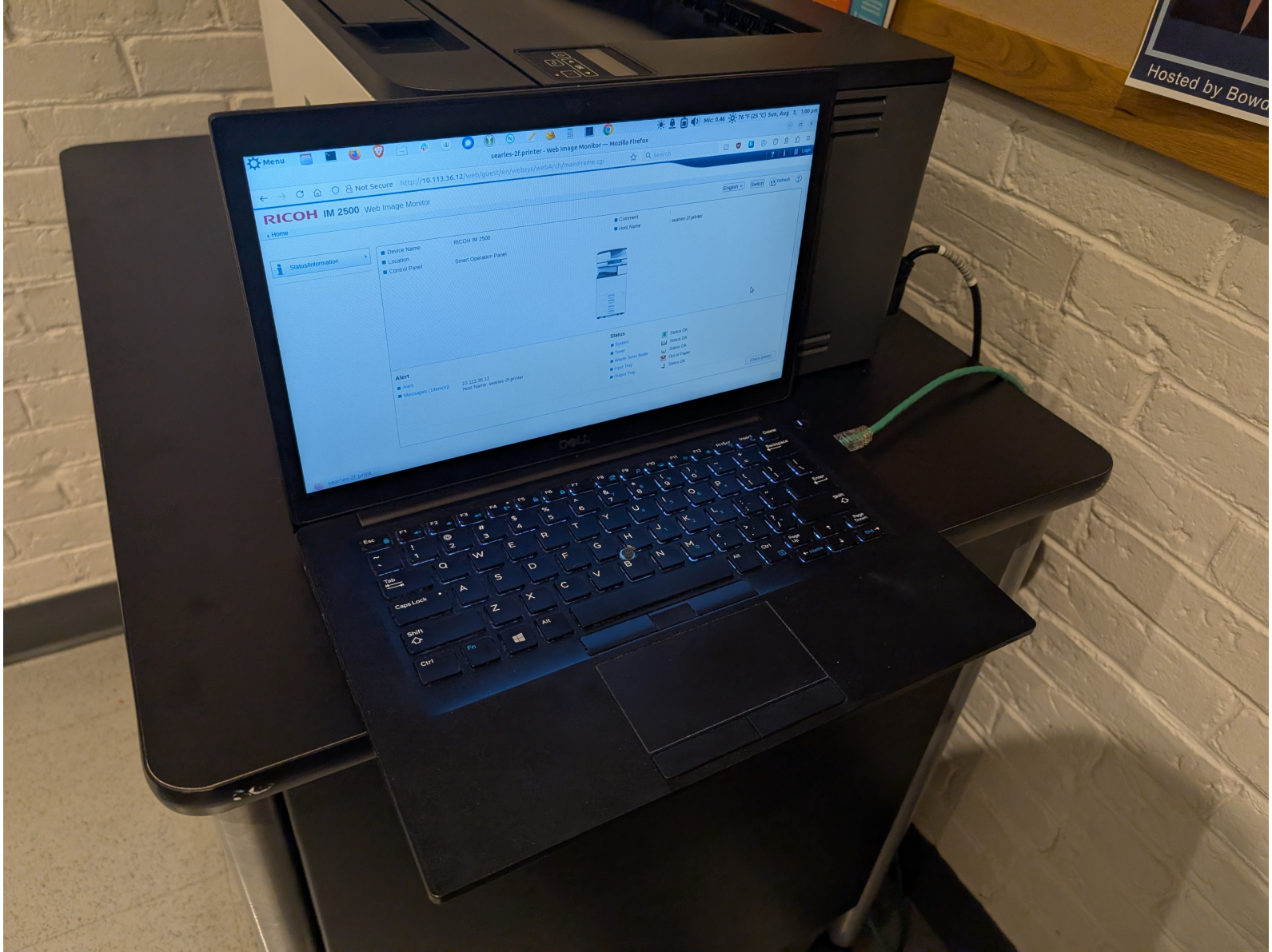
Alert	
Messages (1item(s))	10.113.36.12 Host Name: searles-2f.printer

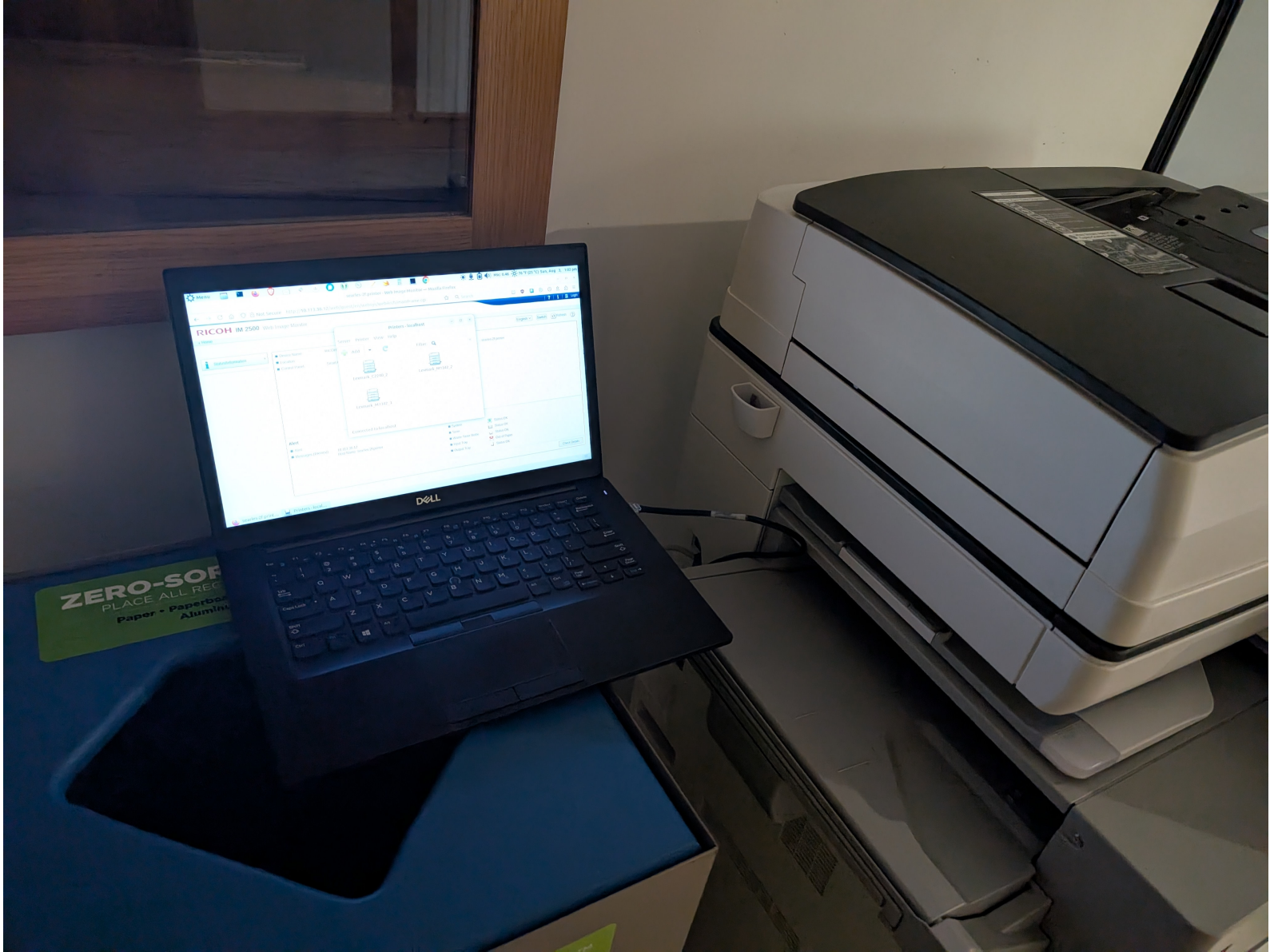
Status

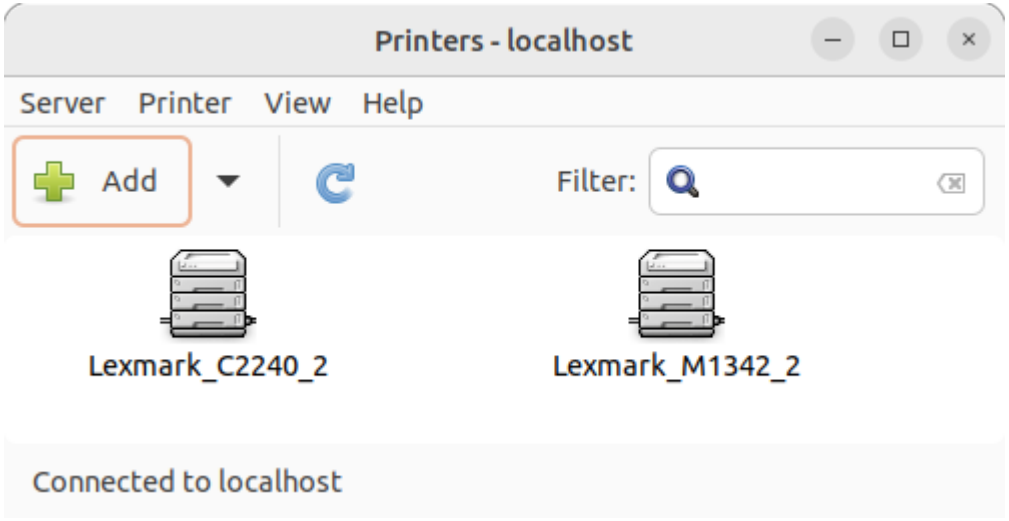
System	Status OK
Toner	Status OK
Waste Toner Bottle	Status OK
Input Tray	Out of Paper
Output Tray	Status OK

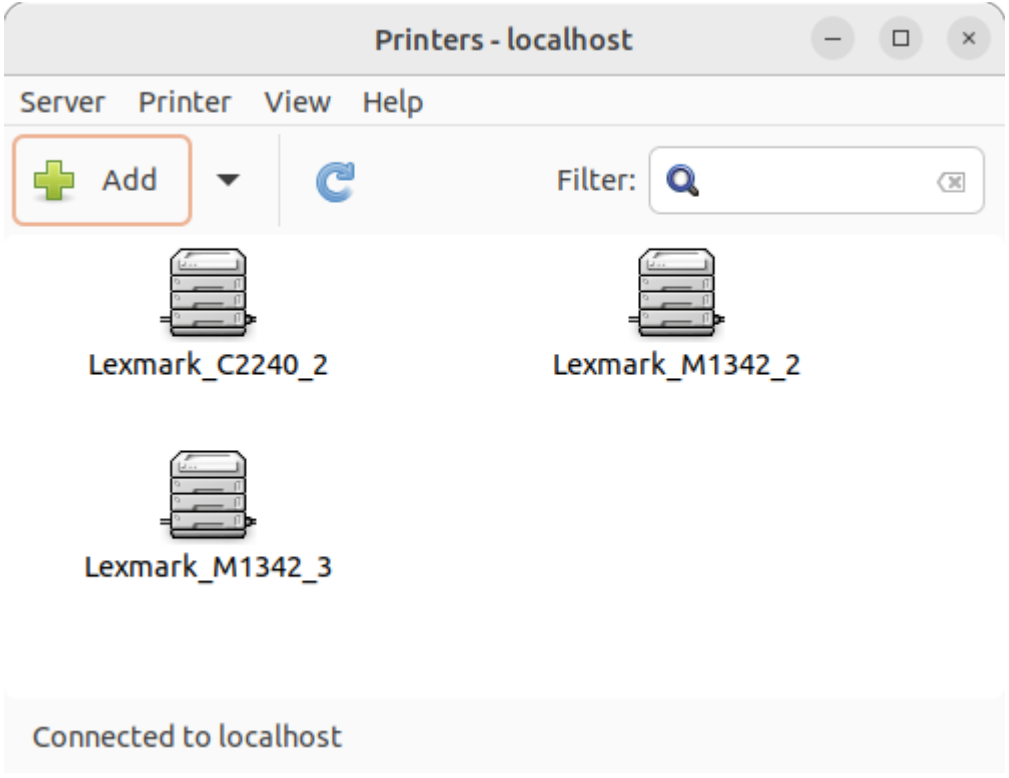
Check Details


Printers - localhost
Server
Printer
View
Help
Add
Filter:
Lexmark_C2240_2
Lexmark_M1342_2
Connected to localhost


searles-2f.printer - Web Image Monitor — Mozilla Firefox
Not Secure http://10.113.36.12/web/guest/en/websys/webArch/mainFrame.cgi
RICOH IM 2500 Web Image Monitor
Home
Status/Information
Device Name
Location
Control Panel
RICOH IM 2500
Smart Operation Panel
Alert
Status
Hosted by Bowa


RICOH IM 2500
DELL


Printers - localhost
Server
Printer
View
Help
Add
Filter:
Lexmark_C2240_2
Lexmark_M1342_2
Connected to localhost


Printers - localhost
Server
Printer
View
Help
Add
Filter:
Lexmark_C2240_2
Lexmark_M1342_2
Lexmark_M1342_3
Connected to localhost

Story of how Jeff printed some documents

- You see an obstacle in the system
- You think about *how does this really work*
- You get around the roadblock
- Hackers are often motivated by getting around BS, bureaucracy, injustice, etc.

Factors

- Ethics
- Laws
- Other policies

Ethics

- Don’t harm real users
- Don’t “pivot”
- If you find vulnerabilities in software, privately disclose them to someone who can fix them
- Give time to fix (45/90/etc. days) before pubicly disclosing
- Responsible/coordinated disclosure process

If no response is received to this disclosure, we will publish details regarding the security vulnerability on its website after 15 calendar days from the date of this communication. In other words, where there is no response from you, we will publish details regarding the vulnerability after [15 days from now].

If a substantive response is received (which excludes, for example, an auto reply) to this disclosure within 15 calendar days from the date of this communication, we will provide you with 45 calendar days from the date of this communication to fix (whether in whole or in part) the vulnerability before publicly disclosing the issue. In other words, where we do receive a substantive response from you, we will publish details regarding the vulnerability after [45 days from now].

We reserve the right to publish details regarding the vulnerability to the general public before the expiry of the 45 calendar days set out above in the following situations: (1) you have disclosed the vulnerability to the general public, (2) you have patched the vulnerability, (3) you have taken the position that there is no security vulnerability, or (4) we observe the vulnerability is under active exploitation.

Laws

- Depends on your jurisdiction
- USA:
  - CFAA (Computer Fraud and Abuse Act)
  - DMCA (Digital Millennium Copyright Act)

CFAA

- USA federal law
- Most general purpose law
- Illegal to access computer systems without authorization

CFAA

- Security research unclear
- Department of Justice announced it will not prosecute security researchers (2022)
- But this is not promised by the law

DMCA

- Illegal to circumvent copyright-protecting systems
- DMCA exemptions renewed every three years
- Historically exempts security research

KrebsonSecurity
In-depth security news and investigation

Missouri Governor Vows to Prosecute St. Louis Post-Dispatch for Reporting Security Vulnerability

October 14, 2021

How Safe is SafeConnect?

By: Carib Guerra Mar 29, 2012

Other policies

- Computer and Network Usage Policy Authority

Users of College information resources must respect copyrights and licenses, respect the integrity of computer-based information resources, refrain from seeking to gain unauthorized access, and respect the rights of other information resource users.

In-band signal

- Control information sent over the same channel as the data

In-band signal

- Earliest form: phreaking
- Notable phreaks:

2600 hz signal – stopped billing

2600 hz signal – stopped billing

- https://www.youtube.com/watch?v=gJDEqIzkBHg

In-band signal

- In-band signals are ***everywhere*** in computer systems
- What about a file name? “kitten.jpeg”

In-band signal

- In-band signals are ***everywhere*** in computer systems
- What about a file name? “kitten.jpeg”
- Most APIs that take file names actually take file ***paths***
- “/home/jeffrey/allmysecrets.db”

Directory traversal attacks

- Often have to guess file paths
  - No way to list directories
- Some useful files to probe for:
  - /etc/passwd: user accounts
  - /etc/shadow: their (hashed) passwords

Directory traversal attacks

- download?name=kitten.jpeg
- => download?name=/etc/passwd
- readfile($name)
- => readfile(‘/etc/passwd’)

Directory traversal attacks

- download?name=kitten.jpeg
- => download?name=/etc/passwd
- But this might fail…
- readfile(‘images/’ . $name)
- => readfile(‘images//etc/passwd’)

Directory traversal attacks

- “..”: on UNIX a link to the parent directory(*)
- download?name=../etc/passwd
- download?name=../../etc/passwd
- download?name=../../../etc/passwd
- How many ‘../’? Depends on your CWD

Directory traversal attacks

- /var/www/html/download.php
- CWD: /var/www/
- readfile(‘images/’ . ‘../../../etc/passwd’)
- download?name=../../../etc/passwd

In class challenge

- Go to https://brainhammer.com/dt/
- Can you get the machine's accounts and passwords?
- Minimum: https://brainhammer.com/dt/
- Expected: https://brainhammer.com/dt/expected.php
- Cool: https://brainhammer.com/dt/cool.php

Assignment 0

- Deadline: September 9, 2025, 10:00pm
- Set up Slack, read Syllabus, etc.
- https://tildesites.bowdoin.edu/~j.knockel/csci3330f25/assignment0.pdf