
go
cyber
COLLECTIVE

October Announcements

- GCC Growth - Very Active Month
- "Community First" - Projects Underway
- November 4th – Threat Intelligence
- November 18th – AI For Management
- November 18th – Governor Visit/Ribbon Cutting

October Announcements – (cont'd)

- November 18-19 – Capture the Flag
- December 16th – Christmas Gathering at Yankee Trace
- GoCyber Collective Business Cards for Distribution
- GoCyber Signal Group
- GoCyber Slack Communication

Cybersecurity Capabilities

Professor Mike Libassi
Sinclair Community College

Agenda

- Cybersecurity Degree Programs.
- NCAE-CD Accreditation & Industry Certification Alignment.
- University Transfer Partnerships.
- Grants & National Leadership.
- Sticker Heist and demo

Cybersecurity Degree Programs

- Cybersecurity Degree Programs focus:
- Cyber Defense (Secure System Administration)
- Cyber Crime & Digital Forensics (Cyber Investigation Technology)
- One-year Technical Certificates
- Short-term Technical Certificates

NCAE-CD Accreditation

- Sinclair is a National Center of Academic Excellence in Cyber Defense (NCAE-CD)
- Through NSA and CISA.
- Only 467 institutions hold this title.

Industry Certification Alignment

- CompTIA Security+
- CompTIA Pen Test+
- CompTIA Net+
- CompTIA A+
- Cisco CCNA
- EC-Council Certified Ethical Hacker
- EC-Council: Certified Hacking Forensics Investigator (DoD recognized)

University Transfer Partnerships

- Our cyber programs transfer seamlessly to:
- Wright State University
- University of Dayton
- University of Cincinnati
- Franklin University
- WGU

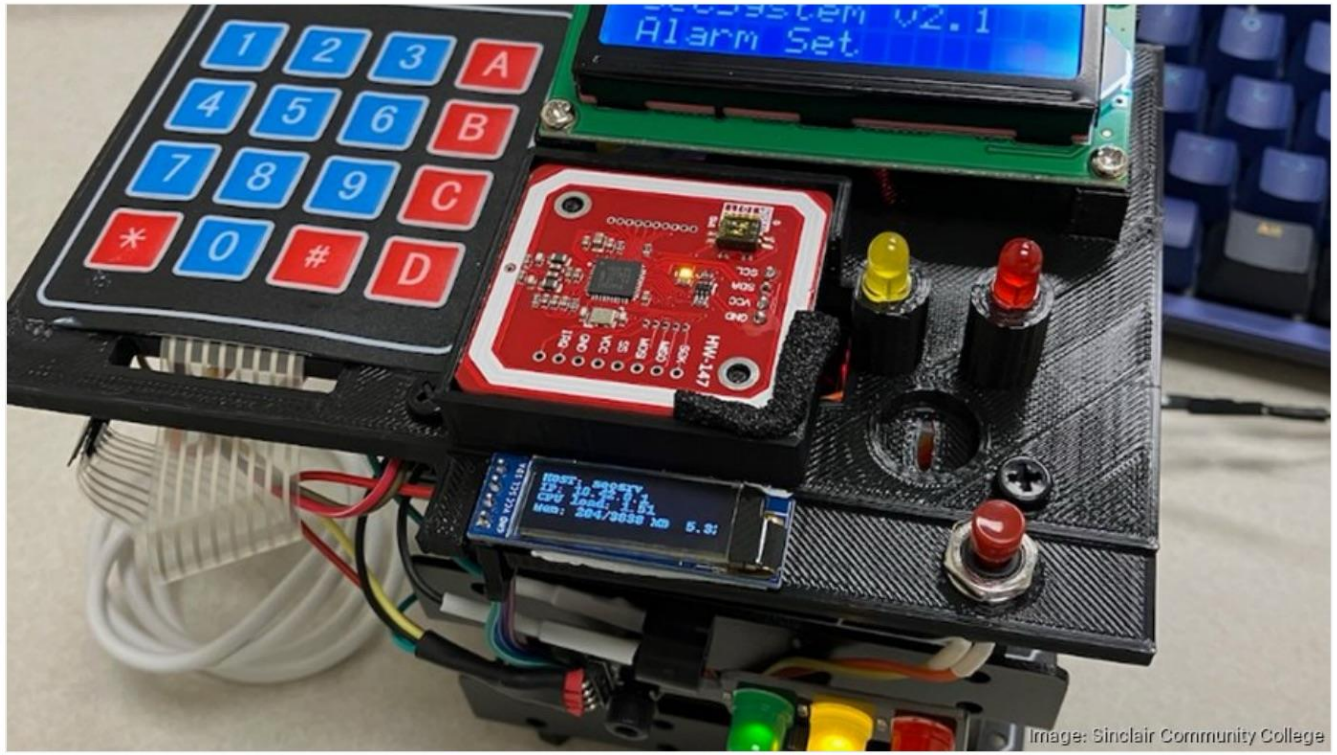
CyAD Conference

- Cross-Disciplinary Cybersecurity Collaboration
- Kyle Jones helped launch CyAD (Cybersecurity Across Disciplines).
- This conference focuses on the intersection of cybersecurity, manufacturing, and IoT and promotes collaboration across these fields.

Grants & National Leadership

- NSF Leadership:
- Kyle Jones serves as Co-PI of the NSF's National Cybersecurity Training and Education Center (NCyTE).
- CyberCorps® SFS:
  - Sinclair was a pioneer in this program, one of the first community colleges to offer it to students, allowing them to serve in cybersecurity roles post-graduation.
- Jumpstart into Cyber (NSF Grant):
  - This grant, highlighted by the White House, helps bring diverse students into cybersecurity careers.
- Sticker Heist (NSF Grant):
  - A gamified learning experience to teach cybersecurity skills through an interactive puzzle box.

Dayton college receives $650K grant to enhance cybersecurity training



A local college in the Dayton region has received more than $646,000 in funding to enhance training within its cybersecurity program.

SINCLAIR COMMUNITY COLLEGE

By Blythe Alspaugh – Staff Reporter, Dayton Business Journal
Oct 3, 2023

News Story

What is Sticker Heist

What is Sticker heist

- Sticker Heist is a cybersecurity challenge that encourages teamwork, communication, while teaching cybersecurity principles.
- Self-contained portable security system protecting a locked box of laptop stickers.
- However, the system is not 100% secure.
- There are several vulnerabilities that challenges students while learning, or practicing, cybersecurity.

Design Thoughts

- The hands-on heist gives a unique way to learn and practice cybersecurity with:
  - Analyzing how system works.
  - Flexible thinking.
  - Creative Problem solving.
  - Communicating ideas and collaboration.

Design and History on Site

www.stickerheist.com

New - 2024 System

The Sticker Heist Scenario

Scenario

In the not-too-distant future, laptop stickers are the new global currency, and you've just gotten your hands on a safe full of them. The safe is locked for now, but its security system is no match for your team's hacking skills.

Scenario - Mission

Hack into the security system, disable the alarms, and pull off the heist.

Can you pull off the Sticker Heist?

Scenario - Objective

- Find a way to get through the locks and disable the security protecting these valuable stickers.
- Success allows each team member to choose and keep a few stickers.
- This is a mission of stealth. To avoid being caught, we need to follow a few rules...

Scenario - Rules

- You can not unplug power (this will set off alarms at Sticker HQ) or power off any individual systems.
- No resetting the alarm system.
- No destruction of any system components (i.e., clipping wires, rewiring, removing); again, this will set off alarms at HQ. Remember, stealth is key!
- No physical modification of any hardware.

Pentesting

- Objective sets a scope of work.
  - What system(s) are part of the job.
- Rules sets a rules of engagement.
  - ROE very common in a pentesting engagement.

The Sticker Heist Hardware

Components

- The box/safe.
- Printed Circuit Board (PCB)
  - Display
  - RFID
  - LEDs
- Arduino UNO R3
- Raspberry Pi 4 (4 GB) with OLED display
- Wiring for OFF button and alarm sensor

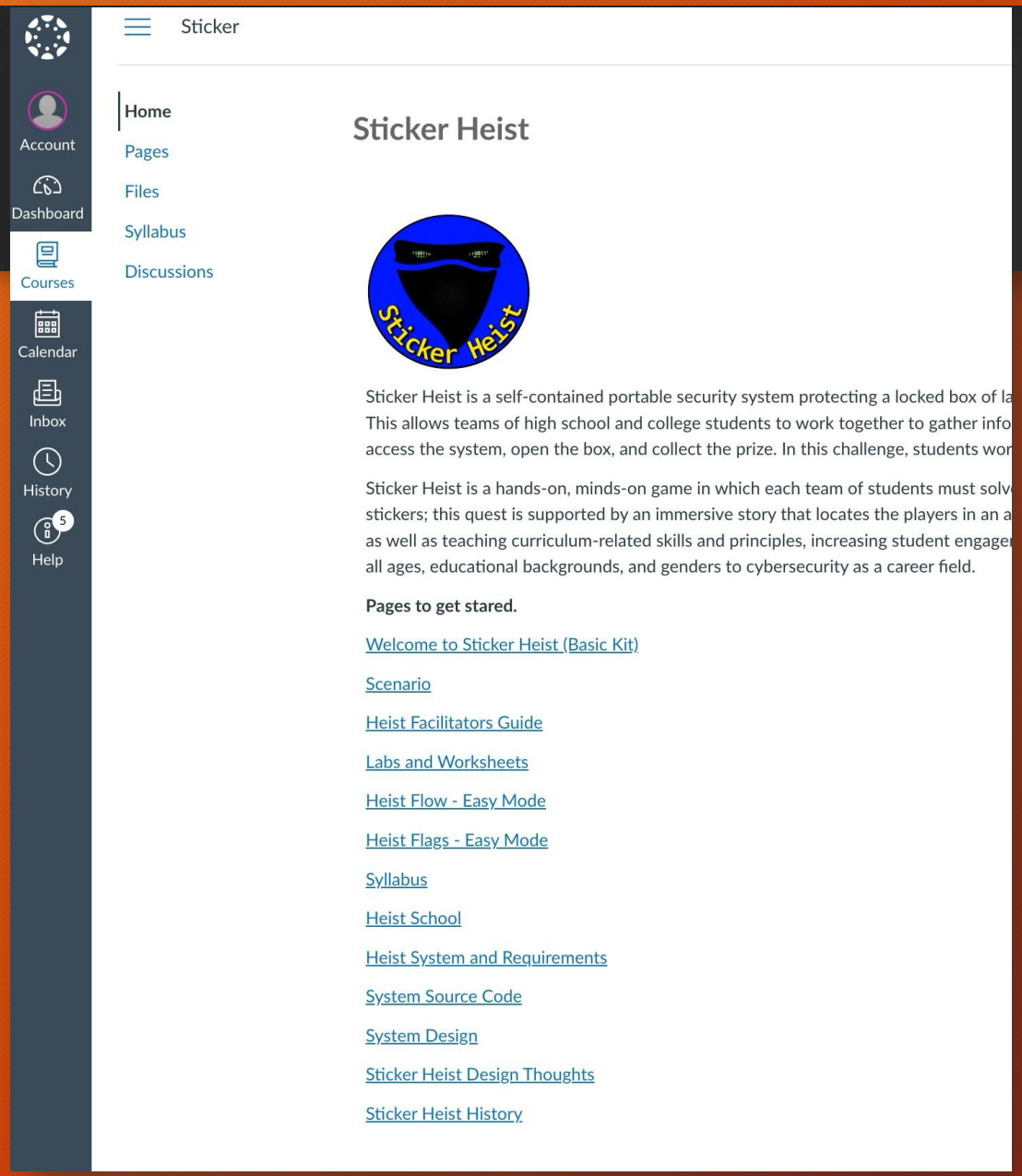
The Sticker Heist Software

Software

- Raspbian OS
  - Custom configured
    - WIFI (NOTE! IT does NOT connect to any external networks)
    - Web Server
    - FTP Server
    - SSH and VNC
    - Arduino IDE and command line tools.
    - Python: *stats.py* to drive the OLED, *shutdown-press-simple.py* for the power off
- Arduino code
  - Installed on the Raspberry Pi.
  - Complies and loads on boot. (Shell script: *unoload.sh*)

Canvas

Canvas


Account
Dashboard
Courses
Calendar
Inbox
History
5
Help
Sticker
Home
Pages
Files
Syllabus
Discussions
Sticker Heist
Sticker Heist
Sticker Heist is a self-contained portable security system protecting a locked box of la
This allows teams of high school and college students to work together to gather info
access the system, open the box, and collect the prize. In this challenge, students wor
Sticker Heist is a hands-on, minds-on game in which each team of students must solv
stickers; this quest is supported by an immersive story that locates the players in an a
as well as teaching curriculum-related skills and principles, increasing student engage
all ages, educational backgrounds, and genders to cybersecurity as a career field.
Pages to get stared.
Welcome to Sticker Heist (Basic Kit)
Scenario
Heist Facilitators Guide
Labs and Worksheets
Heist Flow - Easy Mode
Heist Flags - Easy Mode
Syllabus
Heist School
Heist System and Requirements
System Source Code
System Design
Sticker Heist Design Thoughts
Sticker Heist History


Sticker Heist

Canvas

- Each instructor will get access to the Canvas site.
- Site has:
  - Facilitators Guide
  - Lab Documents
  - Presentations
  - Heist flow-chart and answers
  - All source code and libraries
  - Backup of all Operating Systems (Easy, Medium and Hard)
  - Other supporting information and material

Heist Facilitators Guide

- Guide to help you run a heist.
- Scenario, recommendations and tips.
- The answer key for Easy, Medium and Hard mode.

Worksheets and Labs

- Lab Worksheets can help guide the participants.
  - Give hints on next steps
- Add graded tasks that map to course syllabus and industry standards.
- Students create own vulnerability listing and ranking (scoring with industry CVSS score).
- Students create security policies on how to secure their findings.

Worksheets

Sticker Heist Worksheet
Level 1 – Part 1

Name:
Date:

A crucial pa
essential. Co
that will hel
with tips and

Phase 1 –
An importan
- The sc
- The ru

Review the

Scope of wo

Rules of eng

Phase 2 –
Since you ha
controls, ind

List all you

Question 1

Sticker Heist Worksheet
Level 1 – Part 2

Name:
Date:

A crucial part of securi
target. Look at everyth
See www.stickerheist.c
and see the rules for th
essential the Rules of E

Pre-step: Share any f

Phase 1 – Networ
Since you have found t
services are open is a g
nmap.org). Inspect any
web server found point
you go is part of the ga

Question 1: List the n

Question 2: What is t

Question 3: List the p
the ports?

Phase 2 – Check

Sticker Heist Worksheet
Level 1 – Part 3

Name:
Date:

A crucial part of secur
target. Look at everyt
See www.stickerheist.c
and see the rules for th
essential the Rules of E
Share any findings w
vulnerabilities found

Phase 1 – Back t
Now you have gained
the security server star
contain? If it's assume
great value. (Hint: Yo

Question 1: Record h
port(s) were used. (1

Question 2: List any

Question 3: Research
Capability Core Baseli
findings (3 points)

Phase 2 – The H

Sticker Heist Worksheet
Level 1 – Final/CHORD Lab 4

Name:
Date:

Preforming a penetration test, security assessment or vulnerability scan is only part of securing a system. Documenting, reporting, and creating policies to secure the system is critical.

As a last step. (50 Points) *Use in place of original CHORD Lab #4*

- **Document all vulnerabilities found into Table 1 (use the table to list findings and assignee a severity as Hight, Medium, Low or Info) with any justification and notes. (10 points)**
- **Select the top three findings and create a Security Policy for each using an edited** SANS Institute Information Security Policy Template **(Three policies at 10 points each)**
  - **Company name to use is Sticker Security Inc.**
  - Edit the policy to add and remove any parts as needed.
- **Develop Plan to Disseminate and Evaluate Policies (10 points)**
  - Create an information security policy implementation and dissemination plan. Include specific tasks and events that Sticker Security Inc will use to make sure that all employees involved are aware of the information security policies that pertain to them.
  - The plan should include any specific departments that need to be involved. Sticker Security Inc must also be able to assess whether individuals have the proper knowledge of the policies that pertain to their job responsibilities.
    - A one-page description of the plan and tasks will be the deliverable.

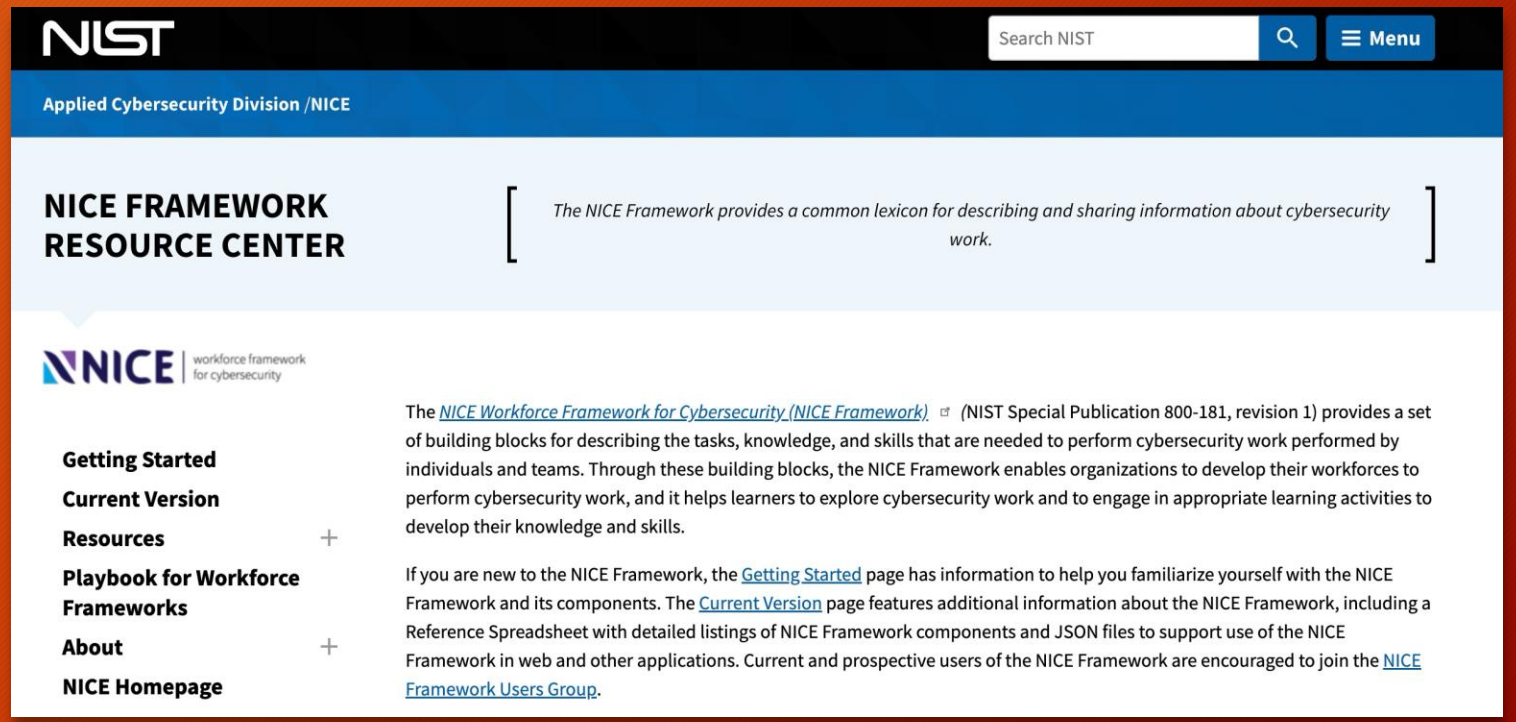
Finding Severity Justification / Notes

Mapping to Security + Course

WEEK	TOPICS	CHAPTERS | NETLAB | TASK	Sticker Hest Mapping
1	General Security Concepts and Trends	Chapter 1: General Security Concepts and Trends NETLABs: • Lab 17: Capturing Network Traffic Start Research Project	
2	Operational, Organizational and Physical Security	Chapter 4: Role of People in Security—**Operational and Organizational Security** **Chapter 7: Physical Security** NETLABs: • Lab 08: Analyze and Differentiate Types of Malware & Application Attacks	**Level 1 Phase 1**
3	Basic Cryptography	Chapter 15: Cryptography NETLABs: • Lab 19: Cryptography Concepts Project: Topic Due	
4	Public Key Infrastructure	Chapter 16: Public Key Infrastructure NETLABs: • Lab 14: Implementing **Common Protocols and Services** for Basic Security Practices Start CHORD Lab #1	**Level 1 Phase 2**
5	Networking and Server Attacks	Chapter 9: Attacks Chapter 10: Network Attacks NETLABs: • Lab 07: Analyze and Differentiate Types of Attacks and Mitigation Techniques • Lab 09: Analyzing Types of Web Application Attacks	
6	Network Fundamentals and Infrastructure Security	Chapter 2: Network Fundamentals and Infrastructure Security NETLABs: • Lab 11: Configuring a Network-Based Firewall • Lab 13: Secure Network Administration Principles Log Analysis CHORD Lab #1 Draft Submission Due	**Level 1 Phase 3**
7	Email, Instant Messaging, and Web Components	Chapter 12: Email, Instant Messaging, and Web Components NETLABs: • Lab 16: Connecting to a Remote System	
8	Midterm Presentation	Research Project: Outline Due CHORD Lab #1: Report and Presentation Due	
9	Wireless and Intrusion Detection System Network Security	Chapter 3: Wireless and Intrusion Detection System Network Security NETLABs: • Lab 06: Wireless Networking Attack and Mitigation Techniques • Lab 12: Identifying & Analyzing Network/Host Intrusion Detection System (NIDS/HIDS) Alerts **Start CHORD Lab #4**	**Level 1 Phase 4** **Tie in with CHORD 4 (r three security policies training plan for Sticke System Inc)**

NIST / NICE Framework

The NICE Workforce Framework for Cybersecurity (NICE Framework) … provides a set of building blocks for describing the tasks, knowledge, and skills that are needed to perform cybersecurity work performed by individuals and teams.



NIST/NICE Mapping

Level	Skills Learned/Used	NICE Competences (NICE Table 3)	Tools
Easy	. a) Physical recon . b) Mapping the network . c) Discovering misconfigured web server . d) Accessing system find source code	. a) Collection operations . b) Target network analyst . c) Vulnerability assessment analyst . d) Exploitation analyst	. a) Physical/visual . b) Nmap . c) Web browser . d) VNC or SSH
Medium	. a) Physical recon . b) Mapping the network . c) Discovering misconfigured web server . d) Analyzing PCAP file . e) Accessing system find source code	. a) Collection operations . b) Target network analyst . c) Vulnerability assessment analyst . d) Target network analyst . e) Exploitation analyst	. a) Physical/visual . b) Nmap . c) Browser/ recon-ng . d) Wireshark . e) SSH
Hard	. a) Physical recon . b) Mapping the network . c) Discovering unpatched FTP . d) Exploiting FTP . e) Discovering PCAP . f) Accessing system find source code	. a) Collections operations . b) Target network analyst . c) Vulnerability assessment analyst . d) Exploitation analyst . e) Target network analyst . f) Exploitation analyst	. a) Physical/visual/ kismet? . b) Nmap . c) Vulnerability scanner . d) Metasploit . e) Wireshark . f) SSH
Demo	. a) Physical recon . b) Mapping the network . c) Discovering misconfigured web server	. a) Collection operations . b) Target network analyst	. a) Physical/visual . b) Nmap . c) Web browser

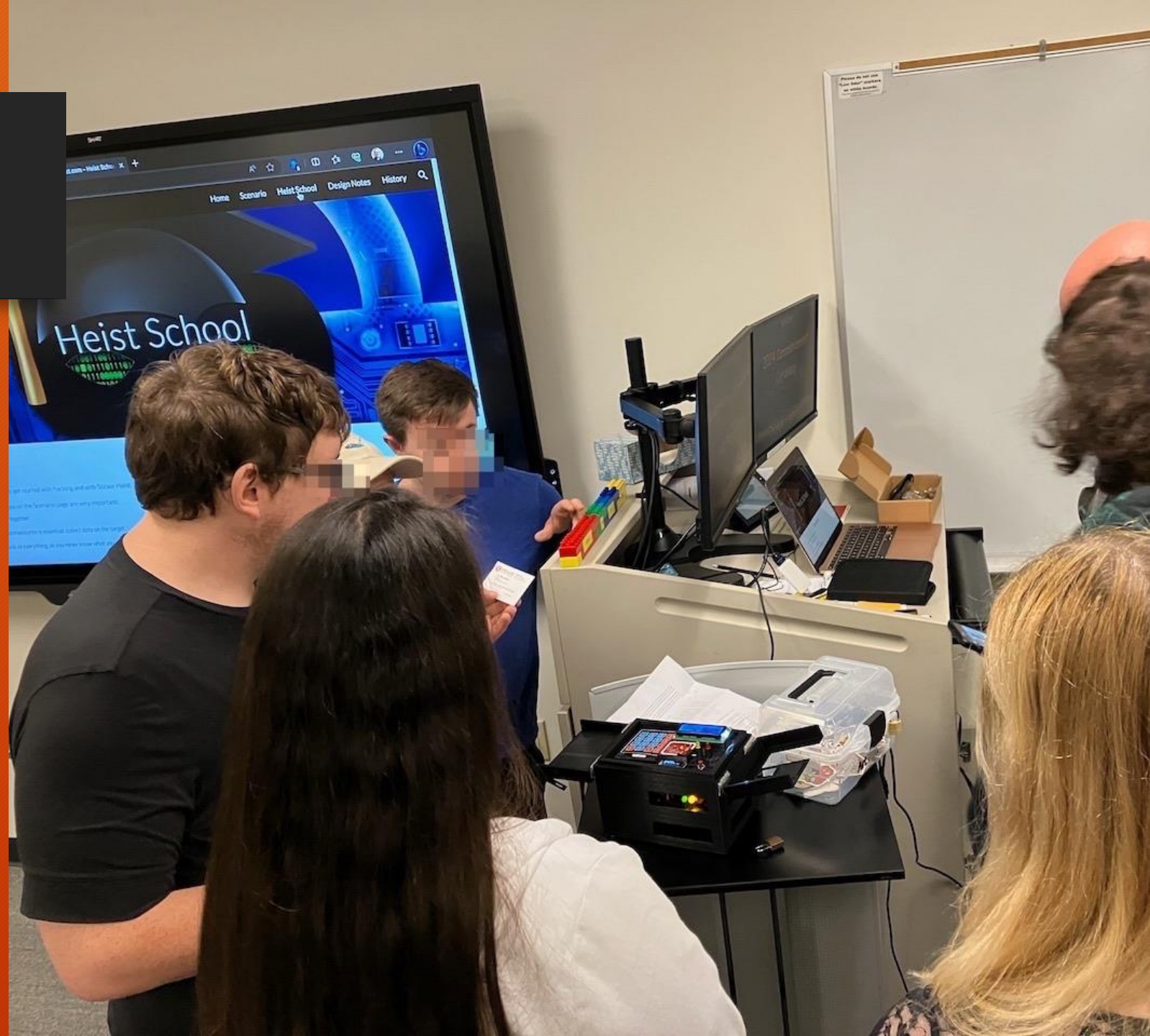
Running the Heist

General

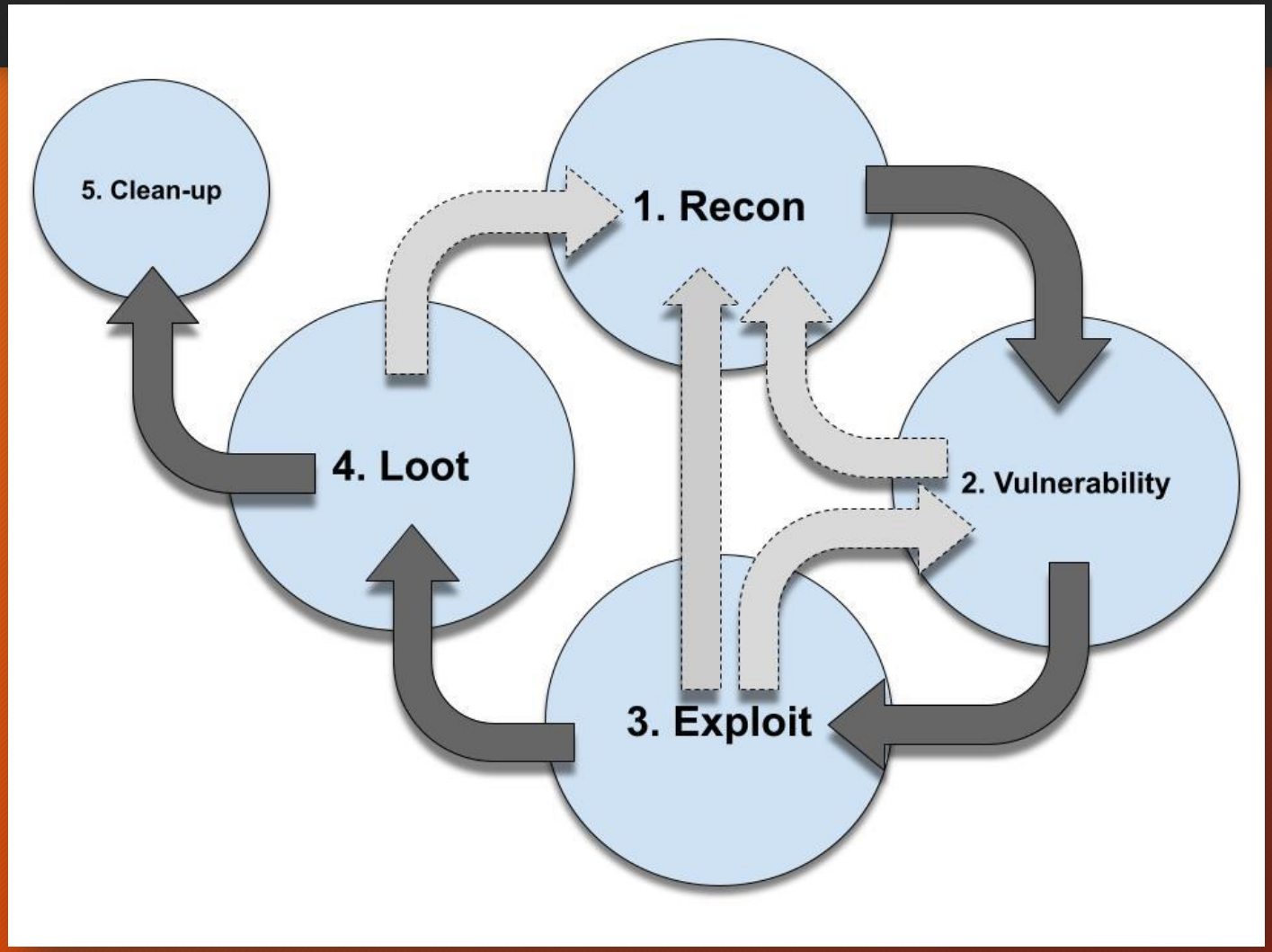
- Start off with the scenario and rules.
- Break larger class into groups of four to five.
  - It can be cooperative or competitive.
- The facilitator is the most important part of running the heist.
- They know:
  - The class experience levels (empower the power students)
  - Time per exercise and total number of heist sessions
  - What labs you plan to use (if any)
- They can drop hints to help move it along.

Heist Steps

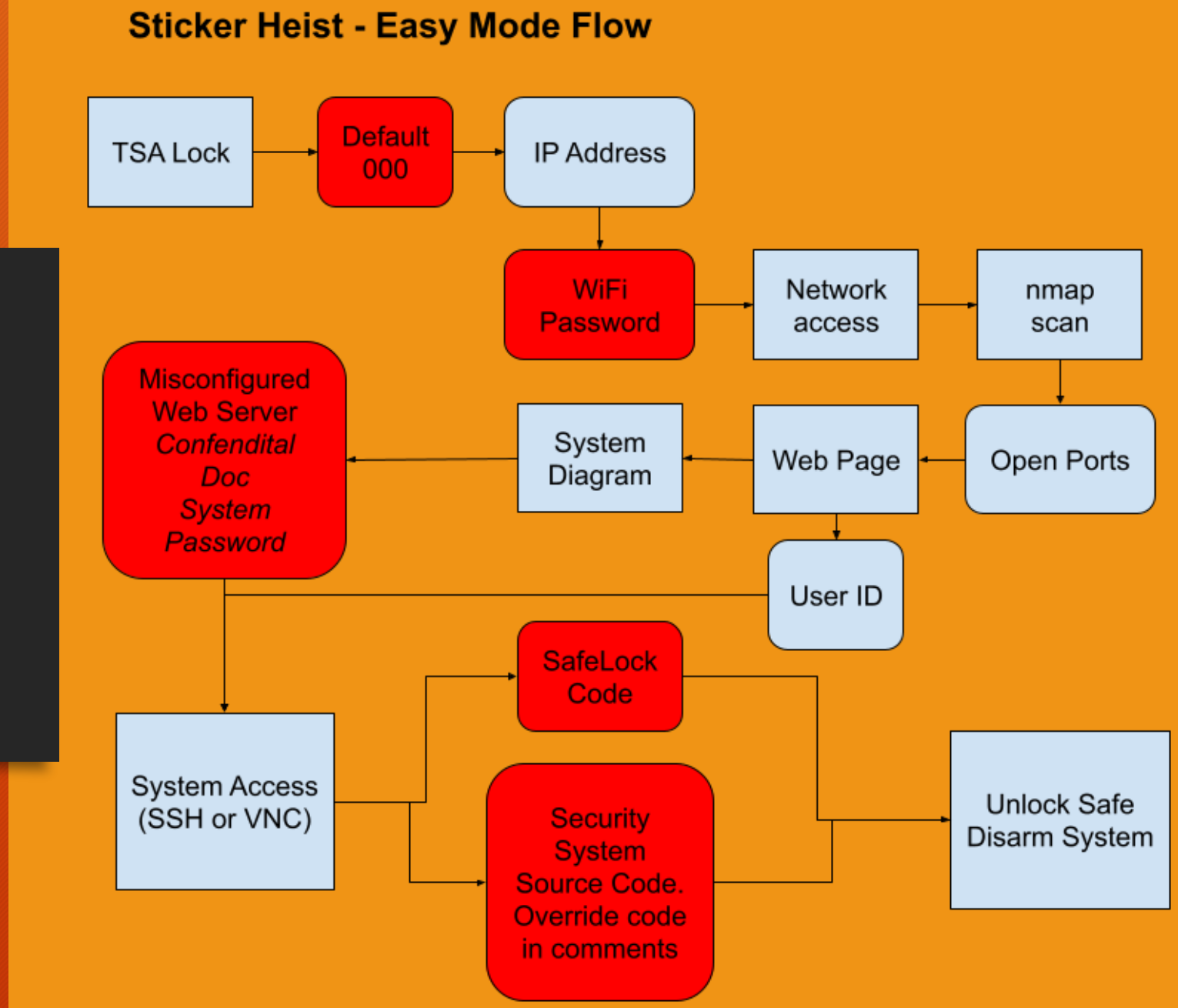
- Physical
- Network
- Application
- Code



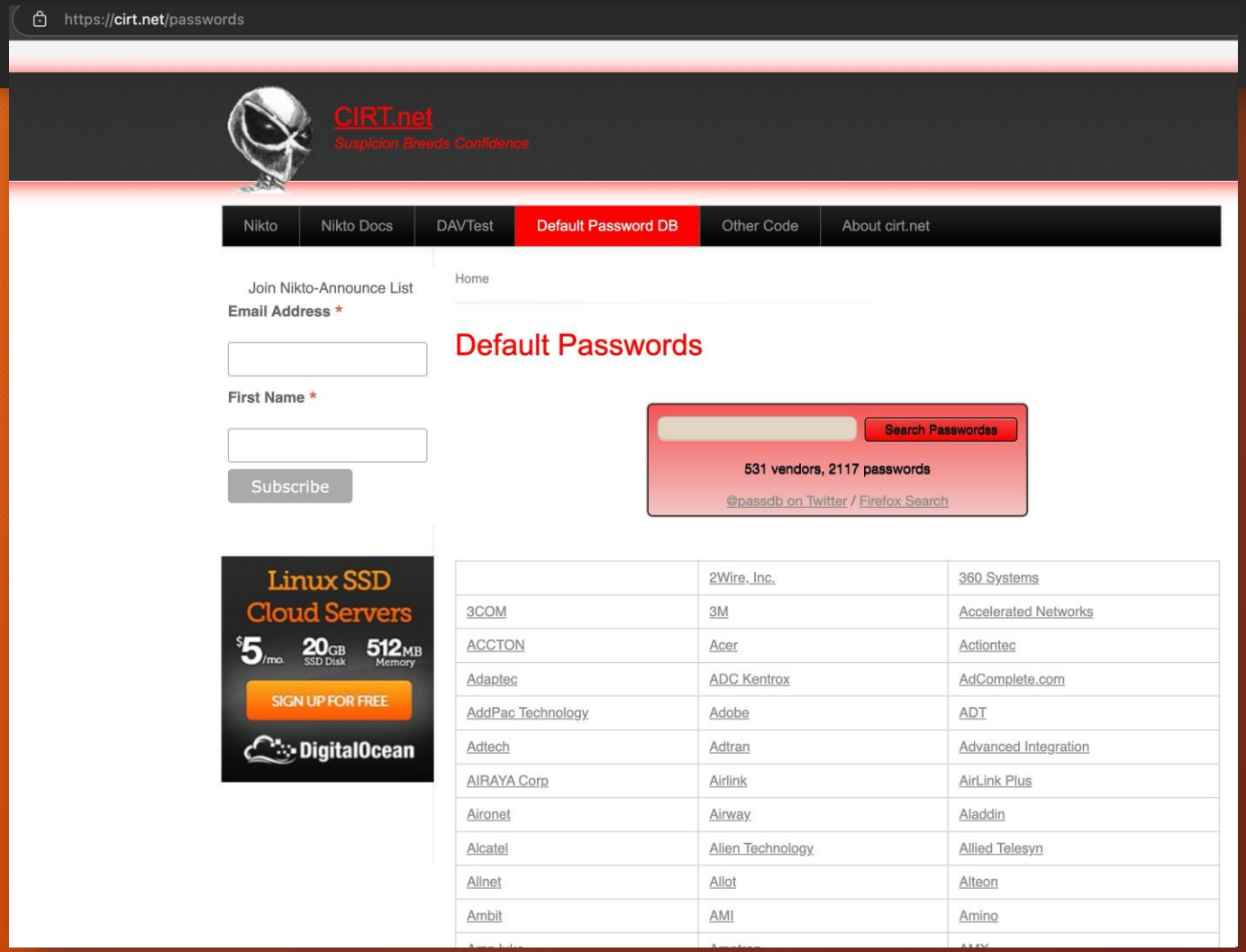
Using Common Pentesting Workflow



Heist Steps


Sticker Heist - Easy Mode Flow
TSA Lock
Default 000
IP Address
WiFi Password
Network access
nmap scan
Misconfigured Web Server *Confendital Doc System Password*
System Diagram
Web Page
Open Ports
User ID
SafeLock Code
System Access (SSH or VNC)
Security System Source Code. Override code in comments
Unlock Safe Disarm System

Default Password / Passcode



Written Down / Exposed Password

Hawaii's missile alert agency stored its passwords on Post-it Notes

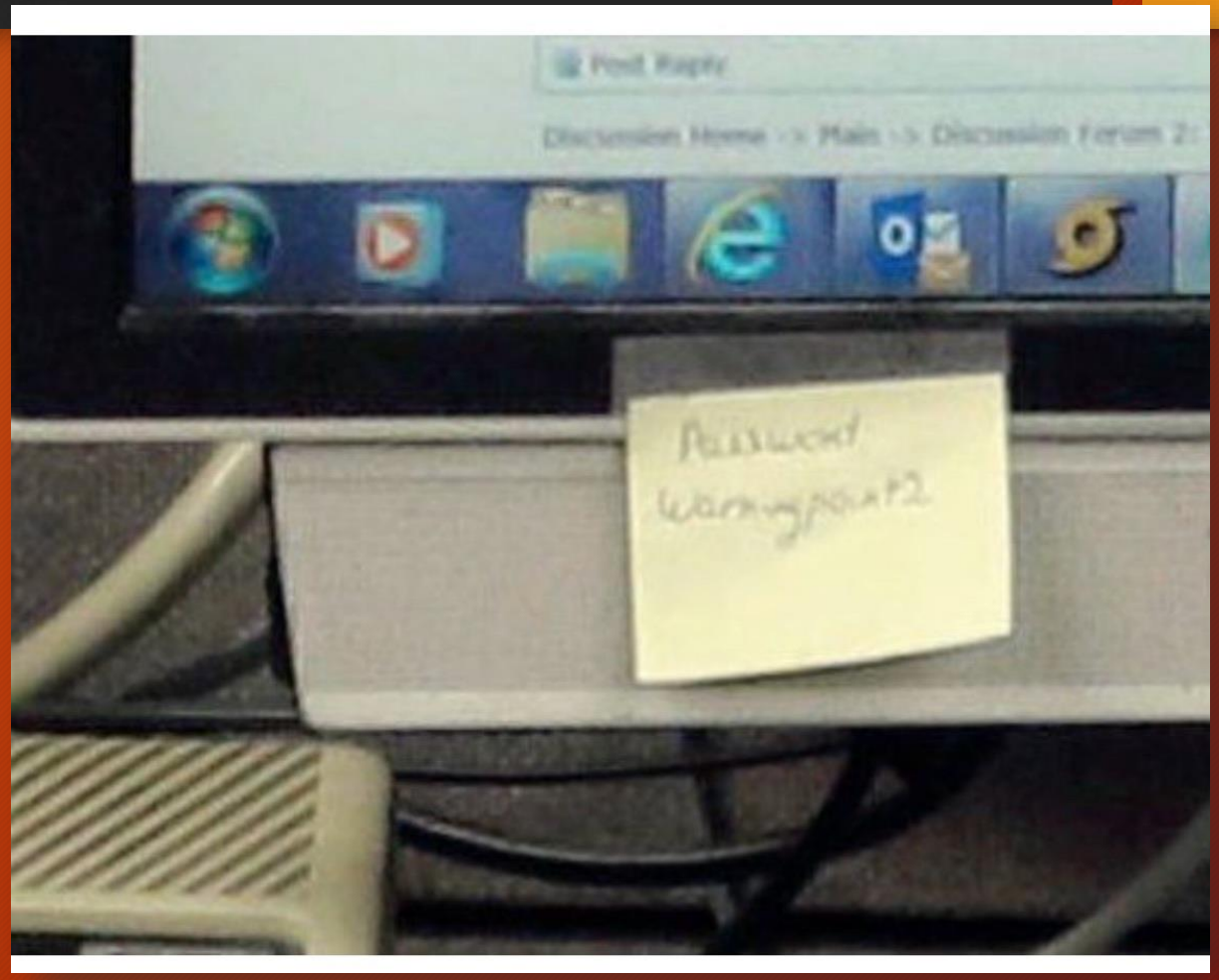
By Mark Coppock
January 17, 2018

SHARE

Listen to article 3 minutes

AP

It's bad enough that North Korea continues to pursue its nuclear weapons program and the country is developing missiles capable of delivering those

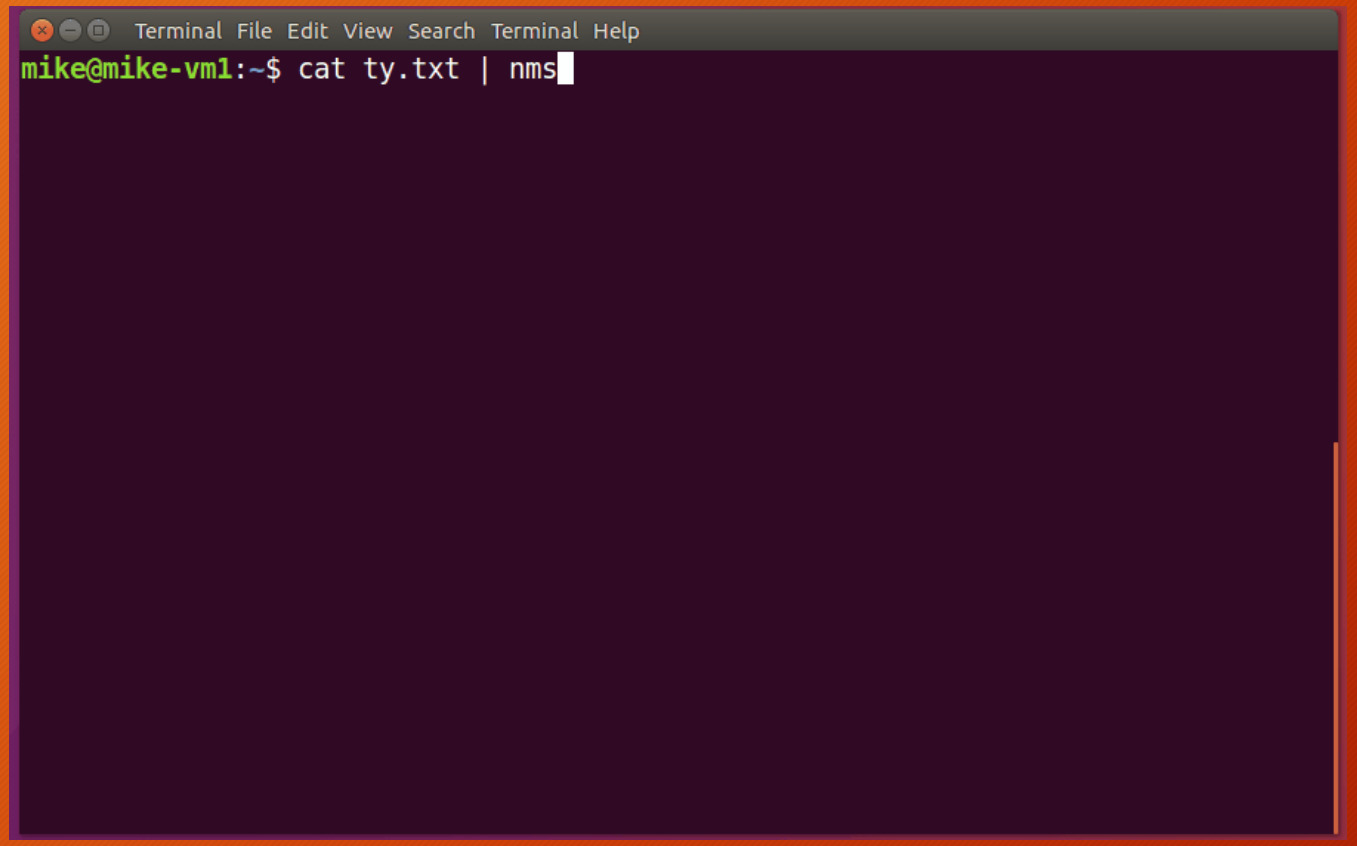


Vulnerabilities

- **We can introduce best practices and industry guideline (NIST, CISA, OWASP, SANS). Example:**

- Risks of Default Passwords on the Internet | CISA
- Insecure Passwords and Default Credentials | OWASP Foundation
- A05 Security Misconfiguration - OWASP Top 10:2021
- A04 Insecure Design - OWASP Top 10:2021
- NIST IoT IR 8259A, IoT Device Cybersecurity Capability Core Baseline | CSRC (nist.gov)

Demo


Terminal File Edit View Search Terminal Help
mike@mike-vm1:~$ cat ty.txt | nms

Thank You

October Threat Briefing

Something Shaping the World Breaches & Regs

- Australia's First Cyber Bill Proposals Standards and Ransom Disclosure
- Marriott/Starwood Settlements
- Fidelity 77k+ Breach Notification

Something to Cautious of: Critical Infrastructure Attacks

- False-Flag: China says U.S. Made up Volt Typhoon
- Salt Typhoon Breaching U.S. Broadband Providers
- Water Works: Wayne County, IN & Richardson, TX

Something to Cautious of: Critical Infrastructure Attacks

- EY Piotr Ciepiela "82% (of Organizations) Cannot Provide a Full Inventory of OT Assets."
- MITRE EMB3D Framework Adds Mitigations https://ebm3d.mitre.org

What's Evolving
AI Challenges/Threats

- OpenAI Observes and Bans Threat Actors- Abuse of Prompts/Prompt Engineering
- CISA'S Chief AI Officer: AI Tools Need to be Accompanied by Human Processes – Over Trust in This Technology

I'm Not All Mr. Doom and Gloom Guy

- INL Chief Power Grid Scientist Emma Stewart: "No Cyber Event That Caused the Lights to Go Out in the U.S. to Date." - Black Hat 2024 Session

Information

Feel free to email us at Admin@gocybercollective.org.

If you have a suggestion on meeting topics, special interest groups, breakfast menu, or anything else we want to hear from you.

You can register and download past presentations from the website.

- GoCyberCollective.org

Event Sponsors