Practicum projects in cybersecurity education

Jason Mitchell

Lansing Community College

The need for practicum-based learning

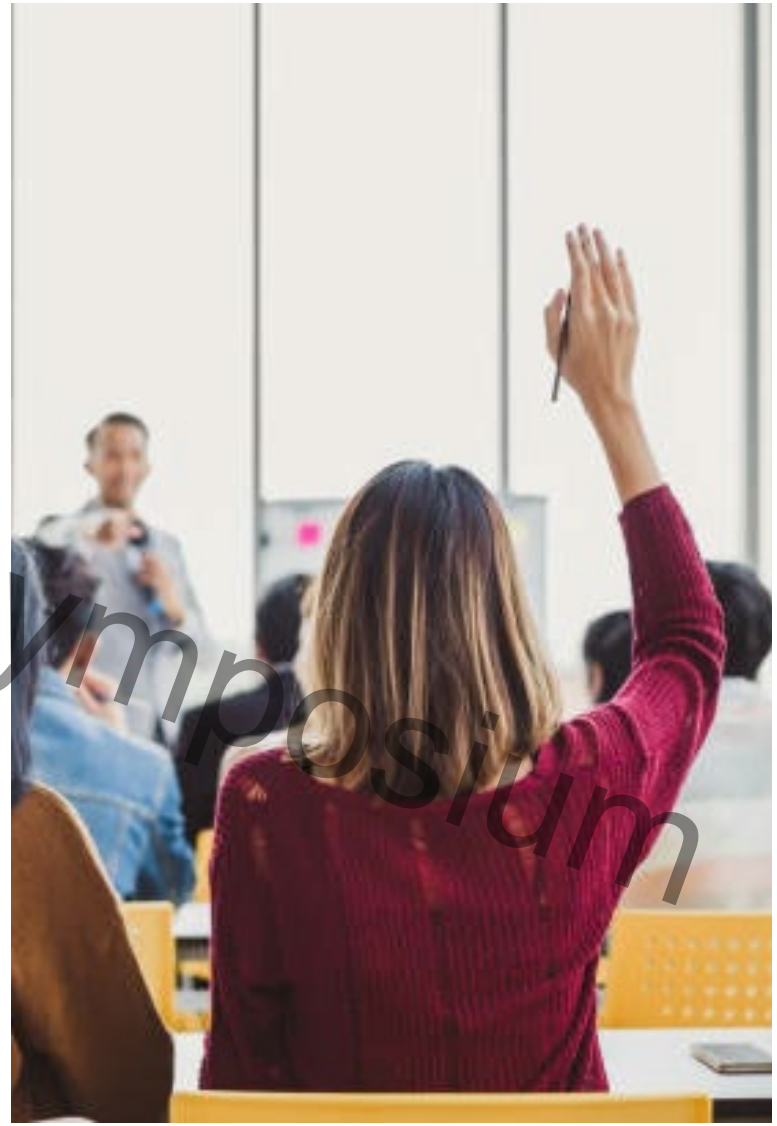
- **The Problem**
  - Many students graduate with theoretical knowledge but lack hands-on experience.
- **Industry Need**
  - Employers seek graduates who can apply cybersecurity concepts in real-world scenarios.
- **Goal**
  - Develop students' technical and soft skills through structured practicum experiences.

What is a practicum?

- **Definition**
  - A practicum is a hands-on learning experience where students apply skills in simulated or real-world environments.

Integration of Practicum in Cybersecurity A.A.S.

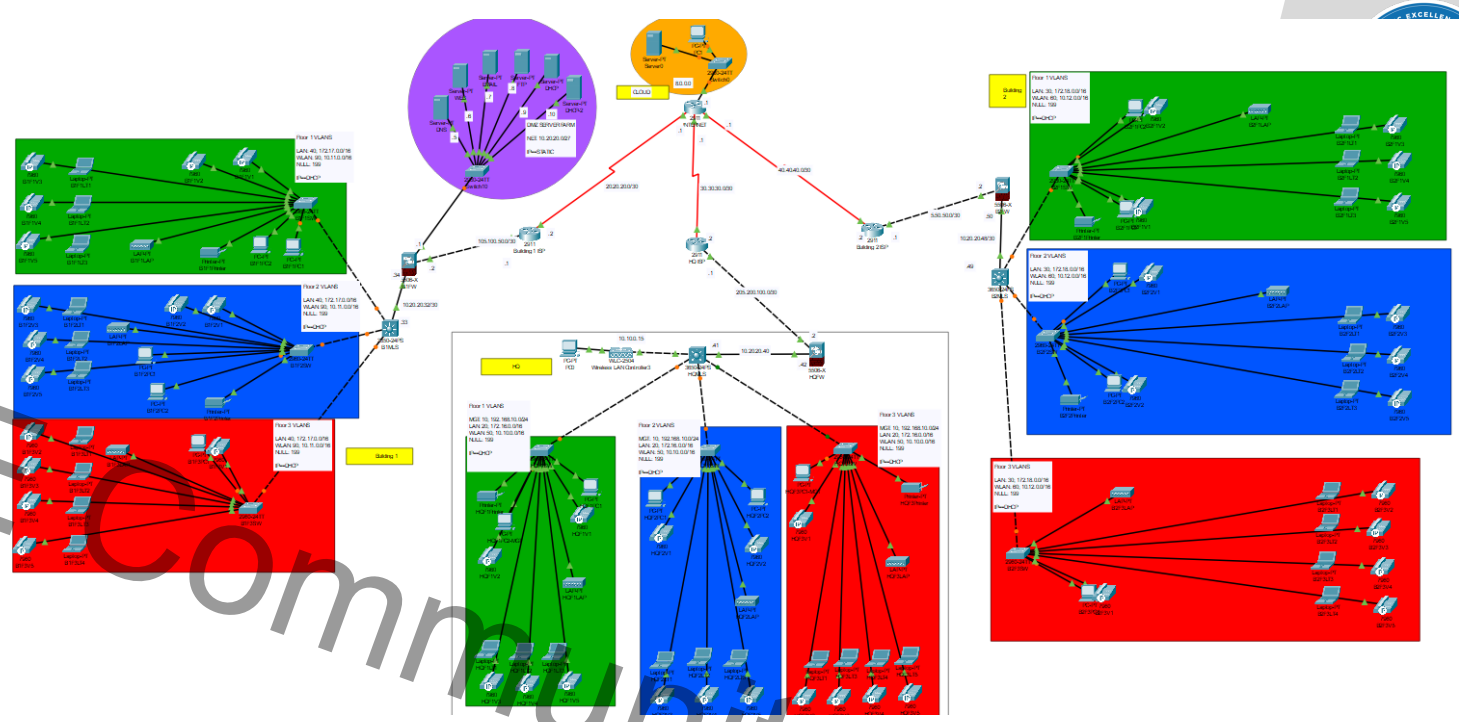
- **Program Design**
  - Practicum projects are embedded throughout the curriculum. 12 out of 20 courses have them.
- **Employer Engagement**
  - The Business Industry and Leadership Team (BILT) provides feedback and ensures industry relevance.
- **Student Benefits**
  - Increased job readiness, problem-solving skills, and exposure to industry expectations.



Examples

Course	Industry Certification	Practicum
CITS 125 – Computer Support A+ Cert Prep	CompTIA A+	Students enter the classroom to find individual computer parts laid out. They must assemble the computer, install an operating system, set up a wireless network, connect a network printer, and complete three maintenance tasks—all while demonstrating the process in front of the BILT Team/Peer Group.
CITS 225 – Networking for PC Technicians	CompTIA Network+	Students take on the role of network consultants and are given a scenario to design and build a network from scratch using Cisco Packet Tracer. They present their final design to their peers and the BILT Team, discussing their design choices, challenges faced, solutions implemented, and security measures applied. Example Scenario: A school campus network including:1 HQ, 2 buildings, 30 laptops (10 per building), 15 desktops (5 per building), 5 servers in HQ, Multiple wireless access points (one per building), 6 printers (2 per building), 45 VoIP telephones (15 per building), Underground fiber/Ethernet connections to buildings, Internet access for each building through a firewall
CITN 280 – IT Security Foundations	CompTIA Security+	Students are provided with a network containing outdated and vulnerable devices. Their task is to conduct a full risk assessment by inventorying devices, performing a vulnerability assessment, prioritizing risks, and implementing risk mitigation strategies. They document their findings in a comprehensive report and present their recommendations to the BILT Team and Peer Group.
CITC 282 – Ethical Hacking	CompTIA Pentest+	Students are given VPN access to a network containing 23 vulnerable machines. They must conduct a black box penetration test using the methodology and tools covered in the course. After identifying all the machines, they select one for an in-depth penetration test. The machines include both Windows and Linux systems, varying in difficulty from easy to hard. Students document their findings in a detailed report and present their assessment to the BILT Team and Peer Group.
CITC 285 – System Defense	CompTIA CySA+	Students are given a network where several machines have been compromised. Their task is to identify indicators of compromise and conduct a full incident response process, including identification, containment, eradication, recovery, and a lessons learned analysis. Students document their findings and response actions in a report and present their conclusions to the BILT Team and Peer Group.
CITC 287 – Cybersecurity Incident Response	EC-Council ECIH	Students are provided with a disk image and a scenario based on a cybercrime. They must analyze the image, document their findings in an examiner's note, and compile a comprehensive report based on the evidence acquired. The final report is presented to the BILT Team and Peer Group.

Examples – Networking



Security Implementation

- Port Shutdown for Unused Ports
- Access Control List (ACLs)
- Wireless Security with WPA2

Port Shutdown
Unused Ports

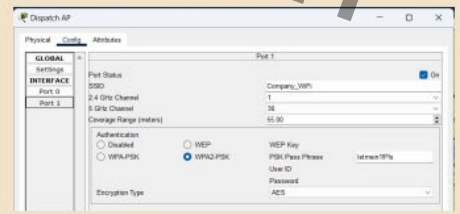
```
DispatchSwitch>enable
DispatchSwitch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
10   Dispatch                         active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
99   Unused_Ports                     active    Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                Gig0/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
DispatchSwitch#show interfaces status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1                        connected    trunk      auto    auto  10/100BaseTX
Fa0/2                        connected    10         auto    auto  10/100BaseTX
Fa0/3                        connected    10         auto    auto  10/100BaseTX
Fa0/4                        connected    10         auto    auto  10/100BaseTX
Fa0/5                        connected    10         auto    auto  10/100BaseTX
Fa0/6                        notconnect   10         auto    auto  10/100BaseTX
Fa0/7                        connected    10         auto    auto  10/100BaseTX
Fa0/8                        connected    10         auto    auto  10/100BaseTX
Fa0/9                        notconnect   10         auto    auto  10/100BaseTX
Fa0/10                       disabled     99         auto    auto  10/100BaseTX
Fa0/11                       disabled     99         auto    auto  10/100BaseTX
Fa0/12                       disabled     99         auto    auto  10/100BaseTX
Fa0/13                       disabled     99         auto    auto  10/100BaseTX
Fa0/14                       disabled     99         auto    auto  10/100BaseTX
Fa0/15                       disabled     99         auto    auto  10/100BaseTX
Fa0/16                       disabled     99         auto    auto  10/100BaseTX
Fa0/17                       disabled     99         auto    auto  10/100BaseTX
Fa0/18                       disabled     99         auto    auto  10/100BaseTX
Fa0/19                       disabled     99         auto    auto  10/100BaseTX
Fa0/20                       disabled     99         auto    auto  10/100BaseTX
Fa0/21                       disabled     99         auto    auto  10/100BaseTX
Fa0/22                       disabled     99         auto    auto  10/100BaseTX
Fa0/23                       disabled     99         auto    auto  10/100BaseTX
Fa0/24                       disabled     99         auto    auto  10/100BaseTX
Gig0/1                       disabled     99         auto    auto  10/100BaseTX
Gig0/2                       disabled     99         auto    auto  10/100BaseTX
DispatchSwitch#
```

ACL

```
Router#show running-config | include access-list
access-list 1 permit 192.168.10.0 0.0.0.255
access-list 1 permit 192.168.20.0 0.0.0.255
access-list 1 permit 192.168.30.0 0.0.0.255
access-list 1 permit 192.168.40.0 0.0.0.255
access-list 1 permit 192.168.50.0 0.0.0.255
access-list 100 permit icmp any any
Router#
```

Wireless
WPAS Security



Examples – Ethical Hacking

Executive Summary

This penetration test*(see glossary) is required for the completion of Lansing Community College course Ethical Hacking. It is to demonstrate what I have learned throughout the course to find any security weaknesses that may negatively impact the organization. For the pen test, I was given PwnTillDawn* website that has a server and multiple virtual machines* that I could choose from to attack. After scanning for available machines on the server, I choose to focus on a Linux box with an IP address of 10.150.150.166.

While performing the penetration test on this box, here are two ports that I discovered:

- Port 22 which is SSH or Secure Shell* is open
- Port 8089 which is ssl/http* is open

As I continued to work through the box, I was able to remote into it and find the first flag out of three. I was also able to use a password cracking tool to uncover the user's password to find flags two and three.

Finally, there are some applications that are installed which could be concerning.

- Sudo*
- base-passwd
- openssh
- openssl
- telnet*

Recommendations:

- One main recommendation I would make is to make sure the organization has a strict password policy in effect for all users. This will add a layer of security so hackers will have to work harder in order to gain access to the system.
- Another recommendation is for the organizations security department to be constantly aware of what ports on their network are open. When using ssh, change the default port number.
- Make sure that all installed applications are up to date and any patches rolled out.

1. Project Scope Description

The scope of this project is to do penetration test against one PwnTillDawn virtual machine. As the pen tester, I am allowed to attempt to access the PwnTillDawn network at anytime from October 21st 2024 to December 16th 2024 when the penetration test hands on final is due.

1.1 Objectives

1. Document vulnerabilities* that you are able to successfully exploit* on the server. Describe in detail what you did and what level of access you were able to obtain. If you obtain a user account with limited privileges, document whether you were able to escalate the privileges to root. Document each exploit that you are able to successfully launch.

2. Document potentially sensitive information that you are able to obtain from the server. These could include user files or web, database, or other server files.

3. For both 1 and 2 above, argue for methods that could protect the vulnerabilities and sensitive information from > exploitation.

1.2 Authorization

You are hereby authorized to perform the agreed-upon vulnerability assessment of the Pwn Till Dawn network and virtual machine within the IP address range 10.150.150.10-10.150.150.254.
Your scope of engagement is exclusively limited to the single Pwn Till Dawn Interview network and asset.

You may:

- Access the server through any technological means available.

You may not:

- Social engineer any Pwn Till Dawn employees.
- Carry out activities that may crash the server.
- Sabotage the work of any other person hired or being interviewed by Pwn Till Dawn.
- Disclose to any other party any information discovered on the asset.

2. Targets of Assessment

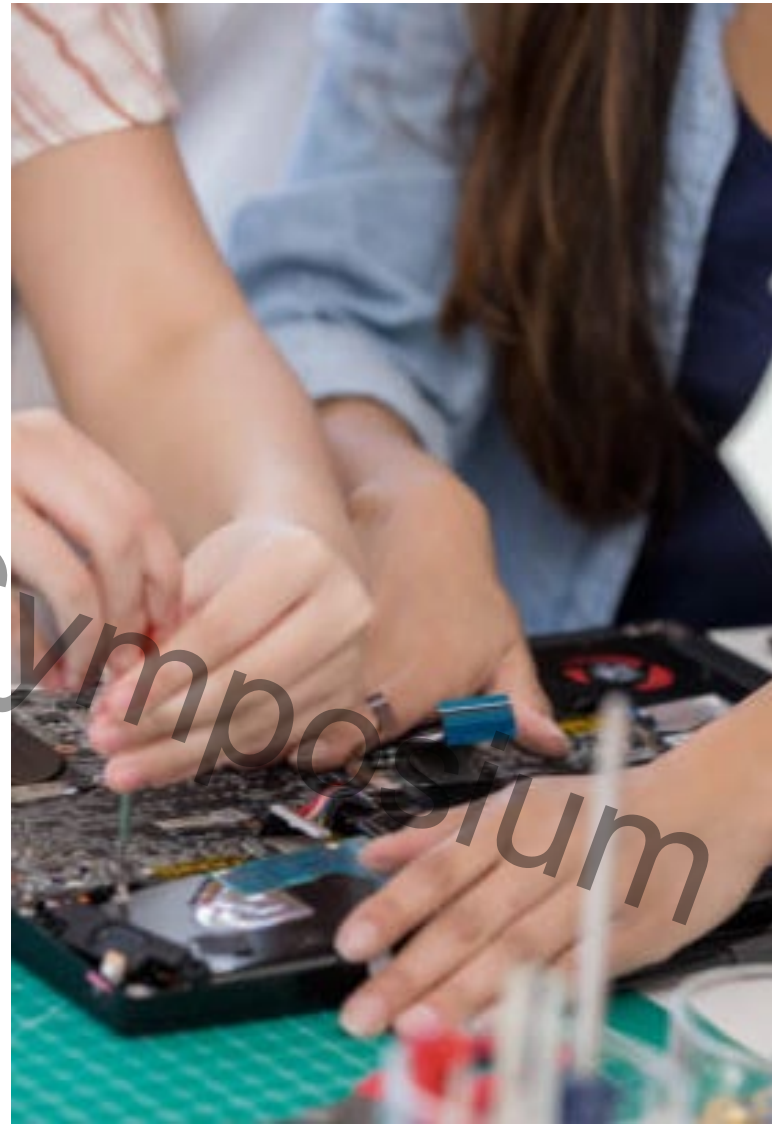
The operating system of the victim machine is Linux Ubuntu. The main user account that I focused on was mike, however, there are additional user accounts that will be provided in a screen shot later in section 4.

Table – Node Description

Key	Value
Operating system	Linux/Ubuntu 18.04.4 LTS (Bionic Beaver)
MAC Address	00:0c:29:d5:a1:e7
User Accounts	Mike
Services running	Below is a brief description of the running services:

How Practicum Enhances Workforce Readiness

- **Technical Skills**
  - Hands-on experience with cybersecurity tools and techniques.
- **Soft Skills**
  - Communication, teamwork, problem-solving, and adaptability.
- **Industry Certifications**
  - Practicum projects align with A+, Network+, Security+, and other credentials.



Lessons Learned & Best Practices

- **Challenges**
  - Time constraints, resource needs, student anxiety.
- **Solutions**
  - Structured project timelines, employer engagement, and iterative learning.

Conclusion & Call to Action

- **Summary**
  - Practicum projects prepare students for real-world cybersecurity roles.
- **Engagement**
  - Invite industry professionals to evaluate student work.
- **Next Steps**
  - Institutions should embed practicum experiences in cybersecurity education.
- **Thank You!**
  - Jason Mitchell, mitch24@lcc.edu