CYB102 | Intermediate Cybersecurity

University-Cybersecurity-Spring-2023 (@ Northern Michigan University)
Personal Member ID#: **74191**

Course Overview

🏗 Unit Structure

Each 1-week unit will consist of:

- **2 Hours of In-Class Time**, consisting of:
  - **Interactive Lecture.** An instructor-led discussion of this week's topics, assignments, and how they relate to real-world Cybersecurity.
    Estimated time: 30-60 minutes (synchronous)
  - **Labs.** In weekly class sessions, students will follow guides to learn new concepts through hands-on interaction with real Cybersecurity tools.
    Estimated time: 60-90 minutes (synchronous)
- **Unit Projects:**
  - For units 1-7, a Cybersecurity challenge is assigned to each student as an individual project. This is the student's chance to demonstrate what they have learned that week!
  - For units 8-10, students will be divided into teams of 3-4 students to work on a Group Capstone. Groups will showcase their work on *demo day* during the final week.
  - *Estimated time: 2-4 hours / unit (asynchronous)*

📚 Unit Topics

Unit	Topic	Project
1	**Lab:** Logging **Project:** Log analysis and correlation of events	• Wireshark • EInspect PCAP files • Inspect email traffic
2	**Lab:** Host instrusion prevention / detection systems **Project:** File integrity validation	• Wazuh • Integrity monitoring • Identify modification

Unit	Topic	Project
3	**Lab:** Endpoint networking (SSH) **Project:** Endpoint networking (FTP)	• FTP • Directory traversal attack • Detect directory traversal attack
4	**Lab:** Enterprise networking (SSL Proxy) **Project:** Enterprise networking (DoS)	• DoS attack • Proxy server • nginx
5	**Lab:** Security Events **Project:** SIEM CTF	• SIEM • Event log correlation • Malware event timeline
6	**Lab:** Incident Response **Project:** Incident Response	• Catalyst • NIST IR Framework • Incident analysis
7	**Lab:** Threat Intel **Project:** Threat Hunting	• MISP • Threat Feeds • TTPs
8	**Group Capstone:** Milestone 1	• HUNT • Log event analysis • Threat Intel
9	**Group Capstone:** Milestone 2	• SOAR • Demonstrating skills
10	**Group Capstone:** Demo Day!	• Sharing learning • Celebrating accomplishments

🧩 Individual Projects

Each unit, students will complete a project in order to apply the concepts they have learned. These projects will take around 5-7 hours outside of class session times to complete, so plan accordingly!

Click the titles below to view details on each Project:

▼ 📋 Logging

In this project, you'll look at emails and try to identify the BEC activity that is occurring. You will inspect PCAP files and try to figure out which emails are legitimate and which ones are fraudulent. Hopefully, this will allow you to stop the bad guy from sending a large wire transfer to a fictitious company!

Close Section

▼ ⛔ Host Instrusion Prevention

In this project, you will configure files that have been modified on a host and use some file integrity validation to see if you can detect which files were modified and how.

Close Section

▼ 👀 Endpoint Networking (SSH)

In this project, you'll install an exploitable version of an ftp server, and perform a directory traversal attack against it. You will then look at the logs from another attack and see if you can figure out what the attacker was able to access!

Close Section

▼ ⚡ Enterprise Networking (SSL Proxy)

In this project, you'll get a sense of what a DoS attack looks like and what you can do to both detect and respond to one! We'll even try running our own DoS attack against our proxy server, then design rules to mitigate the attack.

Close Section

▼ 🖱️ Security Events

In this project, you'll be tested on your ability to search, analyze, and visualize data using Splunk. Demonstrate your ability to look through logs and write queries to find and communicate key data in a real SIEM system.

Close Section

▼ 🧰 Incident Response

In this project, you'll simulate an incident response workflow: First using Splunk to detect and explore a malware attack, and then using Catalyst to document your response to the attack. What happened, why did it happen, and how can it be prevented next time?

Close Section

▼ 🔎 Threat Hunting

In this project, you'll take on the role of digital detective, using the tools and techniques we've learned to hunt for threats. First, you'll do some on-the-ground investigative work and search for IOCs, sifting through clues and artifacts to discern what type of attack might be in progress. Next, you'll use tools like MISP and Splunk to analyze log data and piece together the story of a potential network compromise.

Close Section