COURSE MAP TEMPLATE

Fill out the template with learning objectives, resources, assignments, and assessments for two learning modules in your course (this template includes 2 pages, one for each learning module)

Course Title:Network Forensics

Course Number: CSCI 546-

List of All **Course** level Outcomes:

1. Students will analyze data from common network protocols to enhance the accuracy and reliability of forensic investigations.
2. Students will evaluate network architectures to identify potential sources of additional evidence that can contribute to cybersecurity investigations.
3. Students will dissect network traffic patterns using standard protocols to pinpoint unusual activities or actions that require deeper investigation.
4. Students will apply methods to integrate historical log data into ongoing analytic processes to address and fill in knowledge gaps.
5. Students will extract files from network packet captures and proxy caches for subsequent malware analysis or to determine the extent of data loss definitively.
6. Students will analyze historical NetFlow data to identify past network events, facilitating precise incident scoping and understanding of the attack's breadth.
7. Students will apply their accumulated knowledge in a comprehensive capstone lab, simulating real-world cyber intrusion scenarios by nation-state actors and threat groups, to create a detailed investigation report.

Topic: What Is Network Security Monitoring	**PACING/LENGTH: 1 week**	**Essential concepts OR terminology:** **Intrusion detection system, network data capture, SolarWinds breach**

Course Level Outcome(s) addressed in this module

1. Students will analyze data from common network protocols to enhance the accuracy and reliability of forensic investigations.

Module 1 OBJECTIVES: students will be able to	**RESOURCES/COURSE MATERIAL (Existing or Needed)**	**ASSIGNMENTS (Existing or Needed)**	**Assessment(s) (Existing or Needed)**
A. Identify the basics of network forensics (course outcome 1)	Kaltura lecture quiz Google slides (for escape room)	● Escape room style assessment	embedded in lecture and in-class quiz assignment

B. Compare historic network forensic techniques to modern-day techniques and tools (course outcome 1)	Kaltura lecture quiz Google slides (for escape room)	- Escape room style assessment	in lecture quiz in-class quiz assignment
C. Explain the vulnerabilities and exploits of a modern-day breach (course outcome 1)	Google ChatGPT Google Sheets	- Spreadsheet with questions about recent breach that students need to research	lab

Topic: HTTP Protocol	**PACING/LENGTH: 1 week**	**Essential concepts OR terminology:** **pcap, https status code, user-agent, capinfos, editcap, tshark**

Course Level Outcome(s) addressed in this module

1. STUDENTS WILL ANALYZE DATA FROM COMMON NETWORK PROTOCOLS TO ENHANCE THE ACCURACY AND RELIABILITY OF FORENSIC INVESTIGATIONS.

3. STUDENTS WILL DISSECT NETWORK TRAFFIC PATTERNS USING STANDARD PROTOCOLS TO PINPOINT UNUSUAL ACTIVITIES OR ACTIONS THAT REQUIRE DEEPER INVESTIGATION.

Module 2 OBJECTIVES: **students will be able to**	**RESOURCES/COURSE MATERIAL (Existing or Needed)**	**ASSIGNMENTS (Existing or Needed)**	**Assessment(s) (Existing or Needed)**
A. Recognize HTTP status codes (course outcome 1)	Kaltura lecture quiz Canvas quiz (used as a lab) VMWare image of SIFT hosted on the class server	lab	quiz lab (gives immediate feedback if the correct answer is given)

B. Identify HTTP "User-Agent" data (course outcome 1)	Kaltura lecture quiz Canvas quiz (used as a lab) VMWare image of SIFT hosted on the class server	lab	quiz lab (gives immediate feedback if the correct answer is given)
C. Interpret PCAP files (course outcome 3)	Kaltura lecture quiz Canvas quiz (used as a lab) VMWare image of SIFT hosted on the class server	lab	quiz lab (gives immediate feedback if the correct answer is given)
D. Articulate the features of the tools capinfos, editcap, and tshark (course outcome 3)	Kaltura lecture quiz Canvas quiz (used as a lab) VMWare image of SIFT hosted on the class server	lab	quiz lab (gives immediate feedback if the correct answer is given)