**Networking and Cybersecurity Competency Assessment**

**1. Introduction to Networking and Cybersecurity**

In my MS-CISBA coursework, two courses significantly advanced my understanding of digital security and forensic technologies:

* **CIDM 6340 – Network Management and Information Security (Dr. Jennex, Spring 2025)**
* **CIDM 6356 – Digital Forensics and Fraud Detection (Dr. Humpherys, Spring 2024)**

These courses provided both conceptual grounding and hands-on experience in cybersecurity, network protocols, digital forensics, and fraud detection. More than anything, **being introduced to Jupyter Notebooks** in CIDM 6356 was transformative. As someone who often struggles with configuring development environments, working in Jupyter made it easy to focus on the learning objectives, experiment with code, and understand concepts interactively. It was the single most impactful tool I was introduced to across the program.

**2. What I Know (Strengths)**

Through these courses, I built skills in:

* **Network Mapping and Analysis**: Using Nmap to identify open ports and understand attack surfaces.
* **Packet Inspection**: Applying Wireshark to observe traffic flows, identify vulnerabilities, and troubleshoot network behavior.
* **Vulnerability Scanning**: Utilizing tools like ShieldsUp and Nessus to evaluate firewall behavior, detect exposed services, and measure risk.
* **Ransomware Response Planning**: Understanding how to prepare and recover from major breaches through incident planning, containment, and auditing.
* **Machine Learning for Fraud Detection**: CIDM 6356 introduced fraud modeling using Python, scikit-learn, and natural language processing.
* **Digital Forensics Reporting**: I wrote forensic reports based on fake news, phishing, steganography, and internal employee fraud detection scenarios.

**3. Where I Am Weak**

Areas that remain challenging include:

* **Advanced Malware Analysis**: CIDM 6340 covered ransomware and malware behaviors, but detailed reverse engineering or sandboxing was not part of the coursework.
* **Network Protocol Deep Dive**: Though I used Wireshark, memorizing all protocol structures (e.g., TCP flags, handshake sequences) remains a challenge.

**4. What I Wish I Knew**

In hindsight, I would have benefited from:

* **Cloud Security Training**: Exposure to AWS/GCP security features like IAM, cloud firewalls, or auditing tools would expand my understanding of modern deployments.
* **Automation Tools**: I’d like to explore how to automate routine scans or audit logs using PowerShell, Bash, or Python scripting.

Again, **Jupyter Notebooks** made the learning process smoother and more approachable. I could code, document, visualize, and analyze all in one place, which demystified machine learning and security-focused analytics.

**5. Supporting Evidence**

Key projects and deliverables include:

* **Nmap and Wireshark Reports** (CIDM 6340): Hands-on reports analyzing live traffic and system vulnerabilities.
* **ShieldsUp and Nessus Scan Results**: Interpreted firewall status, open ports, and scan visibility.
* **Ransomware Recovery Plan**: Proposed an organizational response to a simulated ransomware event.
* **Jupyter Notebook Projects** (CIDM 6356): Fraud detection models using scikit-learn, text classification, and visual analytics.
* **Capstone-Ready Security Audit**: Conducted a security review of a home or small business environment.

These documents are located in the CN folder in my Capstone GitHub repository.

**6. Capstone Readiness and Integration**

Cybersecurity plays an important supporting role in my Capstone project by promoting awareness of risks and applying responsible data handling practices. While my prototype does not include application-layer authentication or audit logging, I applied principles learned throughout my Networking & Cybersecurity coursework to minimize risks in the design and sharing of the project.

Specifically:

* I ensured that no sensitive personal data or real banking information was ever collected, stored, or shared in the prototype
* I raised awareness of the risks associated with opening and managing multiple online bank accounts (attack surface expansion)
* I emphasized the use of personal cybersecurity practices such as two-factor authentication (2FA), strong passwords, password managers, and account separation to mitigate risk
* I promoted these same cybersecurity principles to friends, family, and the broader churning community to help others minimize risk

This focus on secure thinking supports:

* **Software Systems**, by guiding the design of a safe prototype with no unnecessary data exposure
* **Data Management**, by ensuring responsible collection, cleaning, and storage of only non-sensitive public data
* **Data Analytics**, by safeguarding the accuracy and integrity of the dataset without introducing privacy concerns

**7. Conclusion**

These two courses taught me to think like both a hacker and a defender. I’ve gained technical skill in reconnaissance, vulnerability assessment, and response planning—and paired it with hands-on machine learning and forensics. The tools and thinking frameworks I encountered, especially in Jupyter Notebooks, gave me confidence that I can handle data security responsibly and ethically in my Capstone project and beyond.