**Capstone Assignment Assessing Networking & Cybersecurity by Masyn Grisel**

**1. What Do I Know? (Competencies, Skills, and Knowledge)**

* Understanding of network technologies and communication protocols (TCP/IP, HTTP, HTTPS)
* Basic knowledge of cybersecurity principles, including risk management and vulnerability assessment
* Familiarity with network security policies and best practices
* Exposure to contingency planning and business continuity strategies
* Understanding of web application security threats and common attack methods

**2. Where Am I Weak? (Least Confident and Proficient)**

* Hands-on experience with penetration testing and ethical hacking
* Implementing advanced cryptographic security measures
* Deep knowledge of security governance, compliance, and regulations
* Advanced incident response and forensic analysis
* Designing and managing enterprise-level security policies
* Awareness of encryption methods and cryptographic techniques

**3. What Do I Wish I Knew or Might Be Missing?**

* Best practices for securing cloud-based networks and hybrid environments
* Hands-on experience with firewall configurations
* More practice with cybersecurity best practices
* Real-world exposure to cyber risk assessments in corporate environments
* Advanced network penetration testing tools and techniques

**4. Examples of My Work & Knowledge Sources**

* Examples of Work:
  + Conducted a basic vulnerability assessment on a simulated network
  + Researched common cyber threats and risk mitigation strategies
  + Developed a business continuity plan for a case study scenario
  + Analyzed network security threats and recommended best practices for a real business
* Knowledge Sources:
  + Course materials from CIDM 6340 & CIDM 6341
  + Online resources on network security and cyber risk management
  + YouTube videos on software setup and uses
  + Labs and case studies on cyber threat assessment and security policies

**5. Summary of Capabilities and Preparedness**

Through my coursework, I have developed a strong foundation in network security, risk assessment, and cybersecurity principles. I understand network protocols, security threats, and best practices for risk mitigation, and I have applied this knowledge through vulnerability assessments and business continuity planning. My research on cyber threats and security policies has given me insight into real-world security challenges and the strategies used to mitigate them.

However, I recognize that my hands-on experience in penetration testing, encryption methods, and security compliance frameworks is still developing. While I understand the theoretical aspects of cyber risk management, firewall configurations, and forensic analysis, I need more practical experience in applying these concepts to real-world cybersecurity scenarios.

Moving forward, I aim to strengthen my technical skills in network security by gaining hands-on practice with firewall configurations, cryptographic security, and penetration testing tools. I also want to improve my understanding of cloud security, cybersecurity governance, and compliance standards to enhance my ability to assess and manage security risks in professional environments.

For my Capstone portfolio and prototype project, I plan to incorporate network security principles and cyber risk assessment methodologies to demonstrate my ability to identify vulnerabilities, analyze threats, and implement security measures. This will not only reinforce my technical skills but also showcase my ability to apply cybersecurity concepts to real-world business challenges.