**Master’s Capstone Project Guide: Cybersecurity Engineering**

**1. Setting Up Your Capstone Project**

**A. Virtualization and Infrastructure**

To simulate real-world environments, you will need multiple machines or virtual environments. Options include:

* **Virtualization Software:** VirtualBox, VMware, Proxmox
* **Cloud Services:** AWS, Azure, Google Cloud for scalable environments
* **Bare Metal Servers:** If using physical hardware, set up a secure lab environment with multiple OS installations

**B. Lab Setup**

* **Operating Systems:** Windows, Linux (Ubuntu, Kali, Debian), macOS (if applicable)
* **Security Tools:** Kali Linux, Metasploit, Wireshark, Snort, Splunk, Suricata, SIEM solutions
* **Networking Components:** Routers, firewalls, VLAN configurations, IDS/IPS solutions

**2. Cybersecurity Capstone Project Ideas**

**A. Penetration Testing Framework**

* Conduct ethical hacking on a simulated enterprise environment.
* Perform vulnerability scanning using Nessus or OpenVAS.
* Develop an in-depth security assessment report.

**B. Intrusion Detection System (IDS) Analysis**

* Implement and test Snort or Suricata IDS.
* Analyze real-world attack patterns and evaluate detection accuracy.

**C. Incident Response & Digital Forensics**

* Simulate a cyberattack and document response procedures.
* Use forensic tools like Autopsy, Volatility, and FTK to analyze artifacts.

**D. Cloud Security Research**

* Deploy and secure virtual machines in AWS, Azure, or Google Cloud.
* Evaluate misconfigurations and present mitigation strategies.

**E. Securing IoT Devices**

* Assess vulnerabilities in smart home or industrial IoT devices.
* Implement security solutions and test effectiveness.

**3. Documenting and Showcasing Your Work**

**A. Writing a Detailed Report**

Your capstone report should include:

* **Abstract:** Overview of the project and key findings.
* **Introduction:** Problem statement and objectives.
* **Methodology:** Tools, techniques, and setup process.
* **Results & Findings:** Data, analysis, and security recommendations.
* **Conclusion:** Summary and future improvements.

**B. Creating a Demo or Presentation**

* **Screen Recording:** Use OBS Studio or Camtasia to document demonstrations.
* **GitHub Repository:** If applicable, upload scripts, reports, and notes.
* **Live Presentation:** Showcase findings via PowerPoint or a live security demo.