Timm Kennedy B. Sta. Rita **BSIT-4A** **08/12/2025**

Environment: School

1. **Which honeypot/honeynet type will you deploy?**

- To enhance the school's cybersecurity posture, I will deploy a combination of low interaction honeypots alongside a honeynet. These systems will mimic vulnerable services such as student portals, file sharing servers, and IoT devices to attract and analyze malicious activity. The low interaction honeypots will log basic attack attempts, while the honeynet will provide deeper insights into attacker behavior without risking real systems.

2. **Where will it be placed?**

- The honeypots will be strategically placed in two key locations: within the school's DMZ (isolated from the main network) to catch external threats and selectively in internal student lab networks to detect insider threats. The DMZ deployment ensures attackers interact only with decoy systems, while internal honeypots help identify rogue devices or malicious student activity. Network segmentation and VLAN isolation will prevent lateral movement from compromised honeypots to real assets.

3. **How will it integrate with IDS/IPS**

- Integration with the school's IDS and IPS will enable automated threat correlation. Honeypot logs will feed into the IDS to generate alerts when attack patterns match known threats. The IPS will then block offending IPs at the firewall level. Additionally, a SIEM will aggregate honeypot, IDS, and firewall logs for centralized analysis, providing visibility into attack trends.

4. **How will you monitor and respond to alerts?**

- Monitoring and response will follow a structured process: Security staff will receive real time SIEM alerts for honeypot interactions, with high-severity incidents triggering immediate firewall blocks. Daily log reviews will identify recurring threats, while weekly reports will summarize attack trends for IT leadership. If a honeypot detects a serious threat (ransomware probes), the team will conduct a forensic analysis, update IDS/IPS rules, and assess internal systems for exposure. This proactive approach ensures the school stays ahead of emerging threats while minimizing false positives.