**YS-5 Kickoff meeting notes**

Red – Network traffic anomaly detection using AI and machine learning approaches

-Make 2-3 modules, then select other cases for at least 5 cases

Showcase attack, potential fixes

Q

Scope of project, like what is the final product that should be turned in.

Are examples of malware needed?

Reports and documentation, what topics it must include.

Limitations of sources?

Preferred coding language if applicable.

Other meeting times for check-in/checkup.

Simple summary of various modules, list links for references

**Network traffic anomaly detection using AI and machine learning approaches 2 modules**

1. **Network Anomaly**
   1. **Overview – Network traffic anomaly caused or found by unusual and/or a substantial change over network traffic. Commonly because it differs from the standard or usual behaviors.**
   2. **Modules**
      1. **DDoS**
         1. **Understanding what DDoS is**
         2. **Different structures of DDoS**
         3. **AI and ML structures to seek DDoS**
      2. **Port scan**
         1. **Understanding what** **Port scan is**
         2. **Different structures of Port scan**
         3. **AI and ML structures to seek Port scan**
   3. Ways to detect network anomaly (Will become the cases/demos)
      1. AI (Databased, as in relies on data to make decision on anomaly) – Uses comparison between usual behavior and abnormal behavior
      2. ML (Uses data to predict anomalies) – Subset of AI, uses different algorithms to detect and predict anomalies, KNN algorithm
      3. Non-AI/ML method
2. **IoT Device Attacks**
   1. **Overview – IoT is internet of things, attack is compromising these devices/systems**
      1. **Types of attacks – Physical Tampering, Eavesdropping, Brute-force, Privilege Escalation, DDoS, Man in the middle, Malicious code injection**
   2. **Citations:** [**https://www.educative.io/answers/what-are-iot-attacks**](https://www.educative.io/answers/what-are-iot-attacks)
3. **Crypto jacking malware**
   1. **Overview –**
4. **AI attacks**
   1. **Overview –**

3 non-AI/ML modules – Source code-based cases so hardcoded solutions

2 AI/ML modules – DDoS and Port Scan in full/deep detail research

**Network Anomaly (Research)**

**DDoS**

**Port Scan**

**References**

**Site module and format example: (**[**https://sites.google.com/view/ml4cs**](https://nam04.safelinks.protection.outlook.com/?url=https%3A%2F%2Fsites.google.com%2Fview%2Fml4cs&data=05%7C01%7Caguo%40students.kennesaw.edu%7C3510a327c12244180aca08da94ec0729%7C45f26ee5f134439ebc93e6c7e33d61c2%7C1%7C0%7C637986038699628176%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=BxFlvTDkvDv1G73GpHuaV8t706k7apoyDZF2siLKlQU%3D&reserved=0)**)**

**Site:** [**https://sites.google.com/d/1Xo0zH-Yr827YKNo220Oiu\_evjQuOT3UR/p/1V1\_kcUKyuszhI9-X7F0TSb-5-K0YoR5D/edit**](https://sites.google.com/d/1Xo0zH-Yr827YKNo220Oiu_evjQuOT3UR/p/1V1_kcUKyuszhI9-X7F0TSb-5-K0YoR5D/edit)