|  |  |  |
| --- | --- | --- |
| **Name: Adam Mesewicz** | **Contact Info:** [**adam.mesewicz@covington.kyschools.us**](mailto:adam.mesewicz@covington.kyschools.us) | **Date: 7/4/2018** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Lesson Title : Is this Normal?** | **Unit #:**  **1** | **Lesson #:**  **2** | **Activity #:**  **3** |
| **Activity Title: Anomaly Detection Challenge** |

|  |  |
| --- | --- |
| **Estimated Lesson Duration:** | **20min** |
| **Estimated Activity Duration:** | **30min** |

|  |  |
| --- | --- |
| **Setting:** | **Classroom** |

|  |
| --- |
| **Activity Objectives: I will determine whether or not an attack is about to occur based on statistics calculated from intervals of network traffic.** |

|  |
| --- |
| **Activity Guiding Questions:**   * **How do you think computers communicate with each other?** * **With such a large amount of data available in PCAP files, what are some methods we can use to summarize all of it?** * **How can we use knowledge of “normal” network traffic to identify malicious users.** * **What would happen if we made a mistake when identifying hackers?** |

| **Next Generation Science Standards (NGSS)** | |
| --- | --- |
| **Science and Engineering Practices (Check all that apply)** | **Crosscutting Concepts (Check all that apply)** |
| ☒ Asking questions (for science) and defining problems (for engineering) | ☐ Patterns |
| ☐ Developing and using models | ☐ Cause and effect |
| ☒ Planning and carrying out investigations | ☐ Scale, proportion, and quantity |
| ☒ Analyzing and interpreting data | ☒ Systems and system models |
| ☒ Using mathematics and computational thinking | ☐ Energy and matter: Flows, cycles, and conservation |
| ☐ Constructing explanations (for science) and designing solutions (for engineering) | ☒ Structure and function. |
| ☐ Engaging in argument from evidence | ☐ Stability and change. |
| ☒ Obtaining, evaluating, and communicating information |  |

| **Ohio’s Learning Standards for Science (OLS)** |
| --- |
| **Expectations for Learning - Cognitive Demands (Check all that apply)** |
| ☐ Designing Technological/Engineering Solutions Using Science concepts **(T)** |
| ☒ Demonstrating Science Knowledge **(D)** |
| ☒ Interpreting and Communicating Science Concepts **(C)** |
| ☐ Recalling Accurate Science **(R)** |

| **Ohio’s Learning Standards for Math (OLS) and/or**  **Common Core State Standards -- Mathematics (CCSS)** | |
| --- | --- |
| **Standards for Mathematical Practice (Check all that apply)** | |
| ☒ Make sense of problems and persevere in solving them | ☒ Useappropriate tools strategically |
| ☐ Reason abstractly and quantitatively | ☒ Attendto precision |
| ☐ Construct viable arguments and critique the reasoning of others | ☐ Look for and make use of structure |
| ☐ Model with mathematics | ☐ Look for and express regularity in repeated reasoning |

|  |
| --- |
| **Unit Academic Standards (NGSS, OLS and/or CCSS):**  Constructing and interpreting graphical displays of distributions of univariate data (dotplot, stemplot, histogram, cumulative frequency plot)  Summarizing distributions of univariate data  The Normal Distribution  1 . Properties of the normal distribution  2 . Using tables of the normal distribution  3 . The normal distribution as a model for measurements  Type I and Type II Error  Describe key protocols and underlying processes of Internet-based services (e.g., http/https and SMTP/IMAP, routing protocols) |

|  |
| --- |
| **Materials**:   * Anomaly Detection Challenge Worksheet * Anomaly Detection Challenge PCAP File * Calculators |

|  |
| --- |
| **Teacher Advance Preparation:**   * Teachers must have fundamental knowledge of the Network Traffic as well as a fundamental understanding for how DDOS attacks are carried out. A video series produced by code.org can be found at <https://www.youtube.com/playlist?list=PLzdnOPI1iJNfMRZm5DDxco3UdsFegvuB7> to prepare teachers who are unfamiliar with these concepts. |

|  |
| --- |
| **Activity Procedures:**   * The teacher should start by reviewing information about the internet and data transfer covered during the first lesson. * After the necessary background information is reviewed, split students up into groups of 4. * When students are split into their teams, pass out the challenge worksheet, as well as the PCAP file. * Students must work through the challenge as a team, splitting up responsibilities, or they will not be able to finish the challenge in time. * The teacher should circulate during the activity, making sure all students are participating in the challenge. |

**Formative Assessments:** None

**Summative Assessments:** Anomaly Detection Challenge

|  |
| --- |
| **Differentiation:** Grouping – Students will be grouped homogeneously so when circulating, I will be able to focus my attention on the groups that are struggling. |

|  |
| --- |
| **Reflection:** This activity started out rougher than I had hoped. When students were given the paper PCAP file, many of them had no idea what the different numbers and phrases meant, and it took almost an entire day just explaining what statistic they were trying to calculate. However, after an explanation of packets, and packet frequencies, students picked up on the idea quickly and ultimately had the process of calculating z-scores reinforced. |