Logo

Description automatically generated

Capstone Project – Intrusion Detection using AI

Craig Perkins – [perkins.cr@northeastern.edu](mailto:perkins.cr@northeastern.edu)

Northeastern University

January 2023 – EAI6980

Capstone Project – Intrusion Detection using AI

For the capstone project, I will be using artificial intelligence to develop an intrusion detection system. Over the last few decades, more and more companies have been relying on technology to host mission critical applications that keep industry running. In the last decade, cloud computing has emerged as an enormous field where small companies can leverage the same infrastructure as major technology companies like Microsoft, Google and Amazon. In addition to cloud services, many large companies also host applications on-premise in a data center that is managed by the same company or co-located in a data center. When securing a physical location like a data center, companies can install cameras to monitor for unauthorized entry to restricted locations to detect intrusions. It’s also important to monitor the digital infrastructure inside the data center which is connected to the internet and accessible by the outside world. There are many methods for securing servers like protecting the server with username and password, restricting traffic to certain ports and adding a firewall to block traffic. Even with all of the security measures in place, hackers can still find methods to exploit to remotely takeover machines. There have been prominent examples of zero-day vulnerabilities that allow attackers to remotely execute code on a vulnerable application server. Examples include heartbleed and log4shell.

In this project, I seek to find a solution for automated monitoring for intrusion detection to determine anomalous behavior within a cluster that should trigger a security alert. I will be examining network traffic to determine if and when a machine was compromised.

**Dataset**

For this project I will be examining raw network packets from the UNSW-NB 15 (University of New South Wales) dataset. The dataset can be located here: <https://research.unsw.edu.au/projects/unsw-nb15-dataset>. The dataset has nine types of attacks:

1. Fuzzers
2. Analysis
3. Backdoors
4. DoS
5. Exploits
6. Generic
7. Reconnaissance
8. Shellcode
9. Worms

References

1. The Heartbleed Bug - <https://heartbleed.com/>
2. Log4Shell a year on - <https://usa.kaspersky.com/blog/log4shell-still-active-2022/27531/>
3. UNSW-NB15 Dataset - <https://research.unsw.edu.au/projects/unsw-nb15-dataset>