Neural Nets in Security Management

Readings: **Strategy Patterns Book, chapters 4 & 5.**

After you experimented with tool #10, imagine you want to propose a solution for one of the security issues at hand in your organization, can you find a Neural Net -based solution for it?

1. Do a quick (2-4 hour long) literature review to see what other organizations have done.

* **Spam and Phishing:** It's an approach based on security that can be improved with neural networks. Spam filters assess the likelihood of your email being spam by comparing it to a database of known spam and phishing emails.Spam filters evaluate emails and attachments based on information, IP addresses, common keywords, file kinds, and linkages, among other things.
* **Intrusion Detection and Prevention Systems:** To monitor network activity and prevent intrusions, intrusion detection and prevention systems employed machine learning techniques or signature-based detection.
* **Entity and User Behaviour Analytics:** Insider threats pose a significant threat to your data security, but they often go unnoticed by traditional security approaches since they originate from internal user accounts that are permitted on your network.
* **Antimalware:** The software prevents viruses and other harmful software (commonly known as malware) by comparing files to a database of known threats to see if they're dangerous

1. Share the top 3 solutions that are based in Neural Nets on this document.

* Natural language processing (NLP) can be used by artificial neural networks to examine the content of an email message. This implies that, rather than scanning an email for specific spam-related keywords, an ANN spam filter reads the message and analyzes its meaning to see if it appears suspect. If you're a native English speaker, for example, an email written in a different language and sent from a foreign IP address is almost certainly spam or phishing. This implies that, rather than scanning an email for specific spam-related keywords, an ANN spam filter reads the message and analyzes its meaning to see if it appears suspect.
* To analyze network data with better accuracy and address other shortcomings of traditional systems, some new IDS and IPS solutions have begun to use neural network technologies, such as deep learning, convolutional neural networks, and recurrent neural networks. Many challenges can be resolved automatically by ANNs without the need for human intervention. As a result, your team will spend less time looking for false positives and dealing with minor threats.
* User and entity behavior analytics (UEBA) solutions use neural networks to monitor user accounts as well as machines like endpoints, routers, and servers, expanding on UBA

technology. UEBA solutions learn the baselines for regular network activity so they can

quickly recognize anomalous or suspicious behavior like long login times or big data transfers. They are typically used in conjunction with security information and event management (SIEM) or other data monitoring and analysis technologies because they require a large quantity of data inputs in order to evaluate your network and build baselines.

* In a couple of unique ways, antimalware systems based on neural networks overcome this issue. To begin, you can use ANNs to monitor systems and networks for any unusual activity that would suggest a malware infestation or breach. Second, neural networks can extrapolate how new malware would behave based on previous infections (or threat signature databases).

1. Find a concrete example of a code written, replicate (fork on GitHub or Kaggle) and make sure you can run it.

https://github.com/dimtics/Network-Intrusion-Detection-Using-Machine-Learning- Techniques

1. In 150-200 words, explain how the code can be modified to help your organization, i.e., what datasets you would need as input, what may you change in the code, what outcomes will you get, and what actions will your organization take.

NSL-KDD dataset has 42 attributes for each connection record including class label

containing attack types. The attack types are categorized into four attac classes:

1. **Denial of Service (DoS)**: is an attack in which an adversary directed a delu e of traffic

g

requests to a system in order to make the computing or memory resource too busy or too full to handle legitimate requests and in the process, denies legitimate users access to a machine.

1. **Probing Attack (Probe)**: probing network of computers to gather information to be used to compromise its security controls.

o

1. **User to Root Attack (U2R)**: a class of exploit in which the adversary starts out with access to a normal user account on the system (gained either by sniffing passwords, a dictionary attack,

or social engineering) and is able to exploit some vulnerability to gain root a system.

c

1. **Remote to Local Attack (R2L)**: occurs when an attacker who has the abilit

y

cess to the

to send packets

to a machine over a netw rk but who does not have an account on that machine exploits

o

some vulnerability to gain local access as a user of that machine.