**Revisão de literatura sobre ML para D(R)DoS - Rafael Tenfen**

O que desejamos saber dos artigos? (-> questões de pesquisa)

Legenda:

- questões com fundo verde: essenciais
- questões com fundo amarelo: desejáveis
- questões com fundo vermelho: ficam para depois
- Para as questões não essenciais, não custa anotar as respostas para os artigos em que elas forem facilmente encontradas

1. Qual o objetivo do uso de ML?
    a. detecção de ataques DDoS *a posteriori*
        i. estilo dos artigos com o Tiago
    b. detecção precoce de ataques DDoS para alerta e reação
        i. estilo AnubisFlow
    c. para identificação de padrões de ataques/atacantes
        i. e.g., assinaturas de payloads ou outras características do tráfego
    d. para predição de ataques
    e. ?
2. Qual o tipo de ambiente que estas estratégias propõe abordar?
    a. *Tenha em mente que cada caso é um caso. Uma abordagem para identificar ataques DRDoS em ISP (Internet service provider) vai possuir um rumo totalmente diferente de uma abordagem que observa estes dados considerando interações com um honeypot (mesma coisa ao considerar programmable data plane, IoT, ….). Então antes de identificar o lado de ML de um trabalho, você precisa focar em localizar qual é a sua problemática. Por consequência, ao identificar esta informação você vai conseguir classificar adequadamente o trabalho. Recomendo responder estas perguntas:*
        i. Qual o ambiente em que esta estratégia está sendo aplicada? ISP, data plane….
        ii. Qual o tipo de observação e interação existe no ambiente? é um honeypot? é informação de switches (qual a visão deles)?
        iii. Caso eles usem um dataset:
            1. Qual dataset é?
            2. Qual o tipo de visão que existe do ambiente?
            3. Qual o ano do dataset? (*dados antigos geralmente não são mais representativos*)
3. Que técnicas de ML são usadas?
    a. Muitas para enumerar :-)
    b. Além de olhar as técnicas de ML (Random Forest, Multilayer per…), focar em identificar as técnicas de pré-processamento e extração de características. Estas etapas que vão apresentar um diferencial do trabalho.
    c. Também é importante tentar entender qual o tipo de dado que está sendo utilizado. *Por exemplo, para identificar ataques DDoS pode ser utilizado para o treinamento dos modelos dados como flows, pkts (.pcap) .... Então tente responder às seguintes perguntas:*

i. Qual o tipo de dado? pcap, flow?
ii. Como este dado será abordado em relação ao seu tipo? São dados categóricos? São dados numéricos ? São dados textuais?
iii. Qual a técnica de pré-processamento aplicada? Está sendo aplicado algum tipo de filtro nesta etapa?
iv. Qual estratégia para extração de dados está sendo usada? Quais as regras utilizadas para esta extração?
v. Qual algoritmo de ML está sendo utilizado? Como este algoritmo está sendo aplicado (é possível utilizar mais de uma estratégia ao mesmo tempo)?
vi. Por fim, está sendo aplicado algum tipo de estratégia como undersampling ou oversampling? *(Imbalance data é bem comum então precisa ficar de olho neste tipo de informação, já que vai impactar muito no resultado do trabalho e pode prejudicar outras estratégias com diferente conjunto de dados)*

4. Que métricas são usadas na avaliação?
    a. accuracy, precision, recall, F1-score, área da curva ROC, Brier, balanced accuracy
    b. *É importante destacar que as métricas que vão ser responsáveis por apresentar a qualidade do trabalho. Um artigo que só apresenta uma métrica como accuracy não será um bom trabalho, já que esta métrica sozinha não mostra o ambiente por completo. Recomendações de leitura para entender como as métricas se comportam:* https://en.wikipedia.org/wiki/Sensitivity_and_specificity
5. Anotações extras:
    a. *Caso você encontre alguma avaliação de dados diferenciada é legal deixar anotado. Geralmente os trabalhos com estes tipos de avaliação são bons. E no futuro você consegue fazer avaliações similares.*
    b. *Trabalhos "bons" de ML, geralmente irão disponibilizar o conjunto de algoritmos utilizados no experimento, como também o conjunto de dados para reprodução dos experimentos. Então se um trabalho aparenta ser muito bom e não apresenta estes artefatos, desconfie.. Trabalhos que apresentam resultados maravilhosos e são bons irão apresentar estes artefatos.*
6. Leitura Payloads:
    a. https://www.tide-project.nl/papers/cnsm2021.pdf
    b.