Computer security project

Use machine learning algorithm in network flows to detect the incoming scanning actions.

Emmanuel Anta Aliou

African Institute for Mathematical Science

February 15, 2019

Overview

Introduction

Problems

Objectives

Methodology

Results

Conclusion

References

Introduction

Scan detection methods range from monitoring for simple thresholds and patterns,such as number of ports connected to a single origin over a period of time, to probabilistic models based on expected network behavior.

Kali Linux is offensive tool aimed at advanced Penetration Testing and Security Auditing in network system.

Wireshark is a free and open-source packet analyzer, it might help you figure out what is really going on in network.

Problems

- Footprinting generally refers to one of the pre-attack phases; tasks performed prior to doing the actual attack. Some of the tools used for Footprinting are Sam Spade, nslookup, traceroute, Nmap and neotrace.
- Vulnerability scanning is a method used to discover known vulnerabilities of computing systems available on a network.

Objectives

1. Classification of packets in network system.
2. Detect suspicious incoming network flows.
3. Prevention of attacking action before it happen.

Methodology

- Generate data of network traffic flow using wireshark.
- Python analysis tool for data manipulation.
- K mean algorithm for data clustering.
- Logistic regression for classification.
- K-Nearest Neighbors (K-NN) model for classification.
- Support Vector Machine model.
- Visualization and analyze of the results.

Results

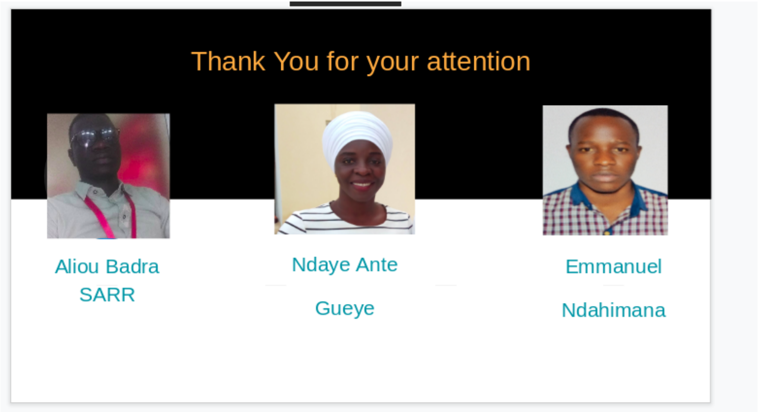
`Let’s take a look on demo`

Conclusion

The detection of slow port scans is challenging due to the large amount of network traffic in company networks. In this paper, we propose three models for detecting slow port scans within flow-based network data. All these approaches reduce the amount of data due to the transformation of flows to network events which simultaneously minimizes the analysis effort for security experts.

References

[1]Lamping, U., Sharpe, R., Warnicke, E. (2014). Wireshark User's Guide for Wireshark 2.1.
[2]Wang, K., Stolfo, S. J. (2004, September). Anomalous payload-based network intrusion detection. In International Workshop on Recent Advances in Intrusion Detection (pp. 203-222). Springer, Berlin, Heidelberg.



Thank You for your attention

Aliou Badra
SARR

Ndaye Ante
Gueye

Emmanuel
Ndahimana