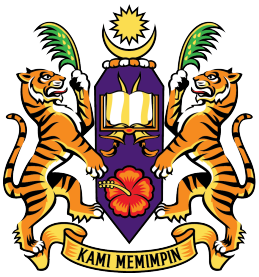

UNIVERSITI SAINS MALAYSIA

CST334 : NETWORK MONITORING AND SECURITY
CST338 : NETWORK AND COMMUNICATION SECURITY

Project - Port Scanning Detection System
Project Proposal

Daniel Hergast
Simon Alix

Date: 22.12.2022

Contents

1 Project Proposal

1.1 Introduction

To protect computer networks from attack, it is helpful to first understand an attacker's approach to compromising networks. The attacker's approach is roughly illustrated in figure ??.

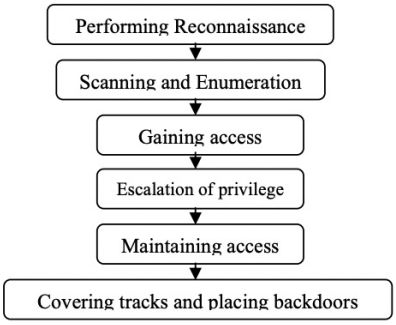

Figure 1: Attackers Methodology [**1**]

Reconnaissance forms the first action in this process. In addition to passive open source intelligence techniques (OSINT), which are very difficult to detect, active measures to gather information, determine network reach, identify active hosts, find open ports and access points, OS fingerprinting, service fingerprinting, and network mapping also form a large part of the reconnaissance phase [**1**, **2**].

Since port scans are usually performed before an actual attack, identifying network scan attempts gives a precautionary indication that attacks may follow in the near future. By identifying these patterns, it is possible to predict the occurrence of attacks in the near future. This represents a non-negligible advantage in defending against cyberattacks [**1**].

Much research has been done in this regard in the past, and the various detection solutions can be broadly classified into the following categories, according to a recent study [**6**]:

- rule-based/threshold-based.
- machine learning-based
- anomaly-based
- frame-based
- connection-based
- distributed processing-based

Based on initial findings, threshold-based systems have emerged as leaders [**3**]. Despite further broad research that may reveal other promising systems as possibly superior, we intend to devote ourselves to the development of a rule-based/threshold-based recognition system based on simple pattern recognition that takes advantage of recent advances.

1.2 Objectives

Our goals are to achieve an executable program that will roughly consist of 2 parts:

- **Network Capturing Mechanism** and storage of network traffic data.
- **Pattern Recognition Engine** for effective detection of port scanning methods in the network traffic data based on rules and thresholds

The Pattern Recognition Engine includes scan detection of the following strategies:

- SYN scan
- TCP connection scan
- ACK scan
- FIN scan
- NULL scan
- XMAS scan
- UDP scan
- ICMP scan

As well as the development of strategies for detecting:

- Fragmentation, Decoy and Coordinated Scanning
- Slow and Distributed Scanning
- Ident and Proxy Scanning

1.3 Intervention Design and Strategy

Extensive research has been done on scanning recognition in recent years, including machine learning, deep learning, and support vector machine techniques. Since we are focusing on a simple rule-based approach, our foundation will be a 2000 [**7**] paper on scanning detection. We will seek to refine this approach and evolve it to include new features to enable better and more accurate detection. This includes thoughts and ideas on slow scanning and backbone scanning detection from recent work (4, 5), but are not limited to those.

1.4 Activities and Timeline

Our approximate timeline is shown in figure **??**.

We will collaborate on theoretical and practical decisions to achieve these goals. We will refine our program based on incremental test results that will help us improve our product.

1.5 Evaluation Indicators

Our assessment will be short and quick. Are we able to detect certain scanning techniques with a high probability or not? This will depend on our test cases and results.

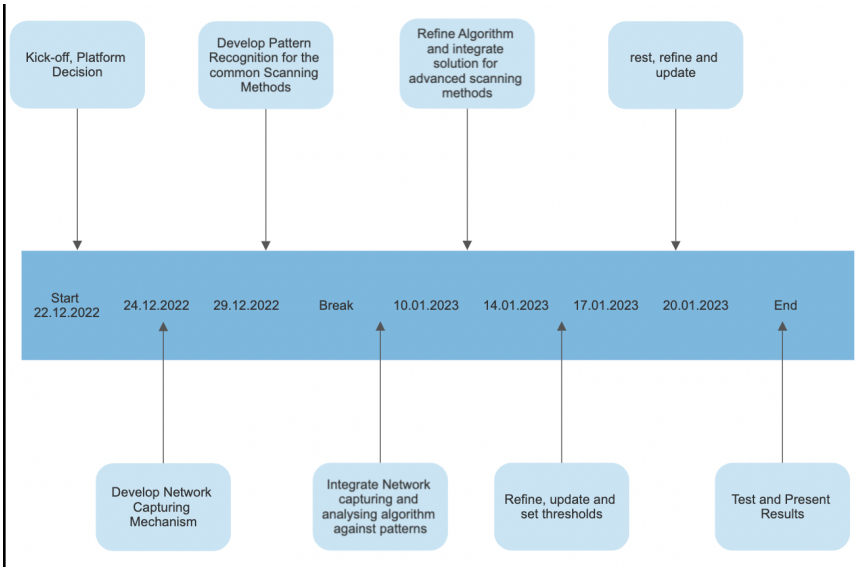

Figure 2: Development Timeline

References

[1] J. Gadge and A. A. Patil, "Port scan detection," 2008 16th IEEE International Conference on Networks, 2008, pp. 1-6, doi: 10.1109/ICON.2008.4772622.

[2] D. Aksu and M. Ali Aydin, "Detecting Port Scan Attempts with Comparative Analysis of Deep Learning and Support Vector Machine Algorithms," 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT), 2018, pp. 77-80, doi: 10.1109/IBIGDELFT.2018.8625370.

[3] Monowar H. Bhuyan, D.K. Bhattacharyya, J.K. Kalita, Surveying Port Scans and Their Detection Methodologies, The Computer Journal, Volume 54, Issue 10, October 2011, Pages 1565–1581, https://doi.org/10.1093/comjnl/bxr035

[4] M. u. Nisa and K. Kifayat, "Detection of Slow Port Scanning Attacks," 2020 International Conference on Cyber Warfare and Security (ICCWS), 2020, pp. 1-7, doi: 10.1109/ICCWS48432.2020.9292389.

[5] Majed, H., Noura, H.N., Salman, O., Chehab, A., Couturier, R. (2021). Efficient and Secure Statistical Port Scan Detection Scheme. In: Bouzefrane, S., Laurent, M., Boumerdassi, S., Renault, E. (eds) Mobile, Secure, and Programmable Networking. MSPN 2020. Lecture Notes in Computer Science(), vol 12605. Springer, Cham. https://doi.org/10.1007/978-3-030-67550-9_ 6

[6] Ijaz Ul Haq, Muhmmad. (2021). Survey of Port Scanning Detection Techniques.

[7] U. Kanlayasiri, S. Sanguanpong, and W. Jaratmanachot, "A rule-based approach for port scanning detection," 2000