

# General Introduction

---

## 1.1 Context:

As a result of the large usage of computers and computer networks all over the world, computer network security has become an international priority. A significant challenge for today's network engineers and security administrators is to develop techniques capable of detecting attempts to compromise the integrity and availability of the network. This area of research is called Intrusion Detection Systems (IDS). Port scanning is regarded as a dangerous network intrusion method for discovering exploitable communication channels. It is considered as the most popular reconnaissance technique attackers use to discover services they can break into. Port scanning consists of probing a network host for open ports. Port scanning is a more targeted form of information gathering that attempts to profile the services that are run on a potential target. [1]

## 1.2 Statement of the Problem:

There are a lot of security tools that will scan a wide range of ports and IP addresses. Intrusion Detection Systems (IDS) will generally catch this type of broad scanning and shut it down by blocking the source IP address or alerting someone to the multiple log entries that are created by a broad, quick scan for open ports.

However a slow port scan attack can deceive most of the existing Intrusion Detection Systems (IDS).

The problem treated in this report may be stated as follows:

*Is it possible to detect efficiently a slow port scanning in computer network?*

## 1.3 Objectives:

### 1.3.1. General Objectives:

The general objective of this study is developing an efficient tool for network intrusion detection systems, to detect port scan attempts.

### **1.3.2. Specific Objectives:**

The specific objectives of this research are the following:

The realization of a new, simple, and efficient method for detecting slow port scans.

## **1.4 Research Approach and Methodology:**

We study in our project two approaches, port scanning detection and slow port scanning detection, using the three most common TCP port scanning techniques: the connect scan, the half-connect scan and the FIN scan. These two approaches is the most popular reconnaissance technique attackers use to discover services they can break into. There are many types to scan ports we focus in our study to vertical scans and detect it.

A new detection technique is proposed in this project focus on the destination port values. Since the most attackers scan the well known services port or consecutive ports.

Our proposed method is mainly composed of two phases: (1) a feature collection phase that analyzes network traffic and extracts the features needed to classify a certain IP as malicious or not. (2) A classification phase that divides the IPs, based on the collected features, into two groups: suspicious IPs and scanner IPs. The IPs our approach classify as suspicious are kept for the next (K) time windows for further examination of destination port to decide whether they represent scanners or legitimate users.

## **1.5 Previous work:**

### **1.5.1 Port Scan Detection:**

Zhang et.al. Published in 2008 a paper called Scan Attack Detection Based on Distributed Cooperative Model. They propose a distributed cooperative model for intrusion detection. This model consists of five layers; (i) sensor, (ii) event generator, (iii) event detection agent, (iv) fusion center and (v) control center. The model describes three different way of detecting an intrusion; (i) feature-based, (ii) scenario-based and (iii) statistics-based. The fusion center analyzes the results from the three detection mechanisms and may generate alerts up to the control center.

Ertöz et al. published in 2004 a paper named The MINDS - Minnesota Intrusion Detection System. This paper presents a new IDS model using machine learning techniques. The MINDS is a data mining based system for detecting malicious traffic/network intrusions.

They use NetFlow to filter out traffic for further analyzing. The detection mechanism consists of both anomaly and misuse/pattern matching techniques in their detection model. The anomaly processing is based on an unsupervised learning technique.

Jung et.al. Published in 2004 a paper called "Fast Portscan Detection Using Sequential Hypothesis Testing". Initial they discuss the problem with anomaly NIDS and false positives. They further use captured network traffic data and manage to find a connection with this data and the theory of sequential hypothesis testing. This data is captured by using Bro. With their research they purpose a new algorithm:

TRW (Threshold Random Walk), an online detection algorithm that identifies malicious remote hosts. This method was proved to be 4-5 times more efficient than previous methods.

[2]

### **1.5.2 Slow Port Scan Detection:**

Staniford et.al. Published in 2002 a paper called "Practical automated detection of stealthy portscans". This paper goes deep into how network scans are performed and show examples from logs. They look at several previous works. They introduce SPICE (Stealthy Probing and Intrusion Correlating Engine), which consists of two components; (i) an anomaly sensor and (ii) a correlator. They collect traffic pattern that is defined as anomaly for later analysis. They use simulated annealing algorithm to cluster anomaly network traffic pattern. They also have adapted SPICE into the Snort plugin SPADE (Statistical Packet Anomaly Detection Engine).

Kim et.al. published in 2008 a paper: "A Slow Port Scan Attack Detection Mechanism Based on Fuzzy Logic and A Stepwise Policy". This paper purpose a way of detecting slow port scanning by using fuzzy logic and a stepwise policy. Kim et.al. have developed an Abnormal Traffic Control Framework (ATCF) that consists of the following elements; (i) an intrusion detection module (with packet analyzing (PA) and intrusion analysis (IA) module, (ii) an intrusion prevention module (with packet filtering (PF) and queuing assignment (QA) module) and (iii) a control module. If anomaly traffic and/or an attack is detected, the PF alerts the QA and blocks this traffic. A slow port scan is handled by using stepwise shaping; (i) if classified as suspicious - bandwidth is reduced to minimum, (ii) if classified as attack - traffic is blocked. The decision regarding a port scan is normal, suspicious or an attack is done by an fuzzy logic rule table.

Malmedal finished his master thesis in 2005 called "Using Netflows for slow portscan detection". Malmedal challenge Netflow, Snort and Network Flight Recorder (now CheckPoint IPS-1) regarding slow port scanning. He sat up a network flow (netflow) analysis system using Argus, PostgreSQL, php and jgraph. This netflow system stored all network data

in a database for non real-time analyzing. Network Flight Recorder is Cisco Corp.'s IDS/IPS (a commercial product). Malmedal chose NMAP to perform slow port scan using port range 0-1000 and scan interval 60 sec. [2]

## **1.6 Thesis Outline:**

To meet this objective this paper is structured as follows:

The First chapter consider the context of our work. First of all provides an overview of port scan categories: single source, distributed, that' where the first one is divides into four types: vertical, horizontal, strobe and block. Then it presents a panorama of the most commonly techniques used in scanning with famous tool Nmap. Finally it summarizes these techniques in table.

The Second chapter will focus on some of the methods which aim to detect port scanning. Then describe the techniques used by attackers to make port scanning stealthier and difficult to detect. Finally comparing the methods discussed.

The third chapter suggest a simple and efficient method for detecting slow port scanning the idea behind our detection method is monitoring traffic every time window, then classifying the IPs into scanner IPs, suspicious IPs based on extracted features from the traffic. The behaviour of suspicious IPs and its destination port is monitored in the following time windows in order to decide whether they represent scanners or legitimate users, which allows the detection of slow port scanning. Also highlight in this chapter how our method is different from the traditional detection approaches. Finally present a detailed description of detection algorithm.

In the fourth chapter we will present the implemented detector and we will present screen shots of the results obtained when running the scanner Nmap and our scan port detector.

We conclude this memory by a general conclusion and perspectives.