**Abstract :**

Port scanning represents a sizable portion of today's internet traffic. An attacker performs port scans of IP addresses to find vulnerable hosts to compromise. Port scanning detection has received a lot of attention by researchers. However a slow port scan attack can deceive most of the existing Intrusion Detection Systems (IDS). In this project, we present a new, simple, and efficient method for detecting slow port scans.

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 of our approach classified as suspicious are kept and their destination ports for the next (K) time windows for further examination to decide whether they represent scanners or legitimate users. A small Local Area Network was put together to test our proposed method. The experiments show the effectiveness of our proposed method in correctly identifying malicious scanners when both normal and slow port scan were performed using the three most common TCP port scanning techniques(TCP SYN, Half connect, FIN ).

Keywords- Intrusion Detection System, Port Scanning

**ملخص**

مسح المنافذ تمثل جزءا لايستهان به في حمولة شبكة الانترنت في يومنا هذا. المخترق يقوم بعملية مسح المنافذ لمختلف عناوين IP للعثور على ثغرات امنية للحواسيب المستهدفة من اجل اختراقها. اكتشاف عملية مسح منافذ الحواسيب استقطب اهتمام كبير من الباحثين. لكن هجوم مسح المنافذ البطيء استطاع تظليل معظم انظمة كشف التطفل الموجودة.

في هذا المشروع نقترح طريقة جديدة وبسيطة وفعالة لكشف مسح المنافذ البطيء. وهته الطريقة مكونة من مرحلتين:(1) مرحلة جمع الميزات التي تمثل المعلومات المحملة في شبكة الانترنت وتستخرج الميزات التي نحتاجها لتصنيف عنوانين معينة على انها خبيثة او لا. (2) مرحلة التصنيف التي تقسم العناوين المستندة على المعلومات المجمعة الى مجموعتين: عناوين مشبوهة و عناوين خبيثة .والعناوين المصنفة كمشبوهة يحافظ عليها مع منافذ وجهتها من اجل فحصها ن مرة اضافية لتقرير ما اذا كانت تمثل ماسح منافذ او مستخدم عادي.

نربط شبكة محلية مع بعضها لاختبار الطريقة المقترحة. التجارب توضح فاعلية هذه الطريقة لكشف التحليل الخبيث سواء في الفحص العادي او البطيء والتي اجريت باستعمال الطرق الاكثر شيوعا في مسح المنافذ .

(TCP SYN, Half connect, FIN )

الكلمات المفتاحية : نظام كشف التطفل ، فحص المنافذ