Summary

This paper proposes a comprehensive framework for passive OS fingerprinting to countermeasure attacks in network systems. First of all, a passive OS fingerprinting tool is integrated with efficient honeypot system to lure attackers in the system. Thereafter, the collected data from the attacker undergoes an efficient filtration algorithm to reduce the congestion in the network as well as make fast analysis. Finally, the filtered data is sent out to an analysis tool to grasp as much information as possible about the attacker in a short time. Experimental results demonstrate the effectiveness of our proposed framework in identifying the vulnerabilities in the network system as well as the ability to countermeasure attacks through identifying their OS, and thus, escalating their further actions.

قمنا في هذا البحث ببناء نظام حماية كامل لحماية الأنظمة من خطر المخترقين و لتجنب أي مخاطر على الأنظمة المتعلقة بالتجارة والأنظمة الحساسة و الحكومية. مبدأ عمل هذا المشروع قائم على جذب انتباه المخترقين الى نظام وهمي بهدف استدراجه, ومن ثم القيام باستخراج البيانات من هذا المخترق عن طريق تحليل الرسائل التي يرسلها المخترق لإتمام التواصل بينه وبين النظام الوهمي. بعد ذلك نقوم بعمل فلترة لهذه البيانات التي حصلنا عليها بهدف جعل قرائتها اسهل للنظام الخاص بنا. ومن ثم تأتي المرحلة النهائية وهي مرحلة تحليل البيانات واستخراج جداول واحصائيات لدراسة المخترق. هذا المشروع سوف يساهم بمساعدة المتخصصين في الأمن على القيام بحماية أنظمتهم ومعرفة المخاطر الموجودة في نظامهم , ومعرفة الطرق المستخدمة من المخترق لاختراق النظام .