

General Conclusion

In this project we propose a simple and efficient approach for detecting slow port scanning. Our method processes the captured traffic in a small time window and therefore overcomes the disadvantages of the previous approaches that work on a large time window, thus requiring a lot of processing which causes degradation in the QoS and might become a target for a DoS attack. Our approach divides the IPs into two categories: scanner IPs, suspicious IPs which is different than the traditional IDS that classify the IPs into either scanners or legitimate users. These traditional IDS can't detect slow port scanning. On the other hand, our method adds this IP with its destination port to the suspicious list to further examine its behaviour. If the IP isn't classified as suspicious in the following (K) time windows, it is removed from the suspicious list. Otherwise, an alarm is sent to the administrator since this continuous suspicious behaviour represents a slow port scanning and blocks scanner IPs directly while suspicious IPs are monitored in the upcoming time windows and either cleared or blocked.

The experimental results show the effectiveness of our approach in correctly classifying IPs and in correctly detecting normal and slow port scanning. For future work, we plan to implement our method on larger traffic data and determine the probability of false detection for our method. We also plan to apply our detection method into horizontal scan detection which is the second stealthy technique after vertical port scanning that is used by attackers to hide the scanning activity.