Implementasi dan analisis kinerja WIDS (wireless intrusion detection system) untuk monitoring keamanan jaringan wireless terdistribusi berbasis kismet = Implementation and performance analysis of WIDS (wireless intrusion detection system) for kismet based distributed wireless network security monitoring

Rika Febita, author

Abstrak

Banyak pihak yang berusaha memanfaatkan kerentanan dari jaringan WLAN sehingga dibutuhkan suatu WIDS yang user friendly dapat mendeteksi adanya serangan dalam jaringan ini. Implementasi WIDS menggunakan Kismet sebagai aplikasi WIDS, Sagan sebagai penghubung Kismet dengan Snorby, dan Snorby sebagai frontend. Metode pengujian menggunakan functionality test untuk spoofed AP, brute force WPS, dan de-authentication flood dan response time untuk de-authentication flood saja. Pengujian de-authentication flood akan dilakukan 10 kali untuk membandingkan nilai alert, frame, dan response time berdasarkan banyaknya serangan dan peletakan sensor terhadap penyerang.
Untuk penyerang1 pada banyaknya serangan, pada 1, 2, dan 3 serangan, rata-rata alert adalah 12 alert, 3,8 alert, dan 2,3 alert, persentase false negative frame deotentikasi yang mengacu kepada 1 serangan adalah 28,43% (2 serangan) dan 44,47% (3 serangan), dan response time adalah 0,015 detik, 0,056 detik, dan 0,087 detik. Untuk peletakan sensor, pada ruang yang sama (ruang 1), ruang yang berbeda 1 ruangan (ruang 2), dan ruang yang berbeda 2 ruangan (ruang 3) dari penyerang, rata-rata alert-nya adalah 10,6 alert, 7,9 alert, dan 7,8 alert, persentase false negative frame de-otentikasi yang mengacu kepada frame de-otentikasi yang terdeteksi pada ruang 1 adalah 72,48% dan 77,17%, dan rata-rata response time adalah 0,018 detik, 0,046 detik, dan 0,111 detik.
Seiring bertambahnya serangan dan semakin banyak dinding pembatas, alert penyerang1 semakin sedikit, dan false negative frame de-otentikasi dan response time penyerang1 semakin banyak. Oleh karena itu, banyaknya trafik dan peletakan sensor berpengaruh terhadap kinerja WIDS. WIDS dapat bekerja optimal jika berada dalam 1 ruangan dengan AP yang ingin dimonitor dan tidak terlalu banyak trafik. Hal ini untuk menghindari adanya interferensi dan terlalu banyaknya frame yang lalu lalang di udara.
<hr><i>Many people that try to exploit the vulnerability of WLAN so it is needed a user friendly WIDS that can detect attacks in these networks. WIDS implementation is using Kismet as WIDS application, Sagan which connects Kismet and Snorby, and Snorby as a frontend. Method of testing for functionality test is using spoofed AP, WPS brute force, and de-authentication flood and the response time for the de-authentication flood. De-authentication flood testing will be performed 10 times to compare the value of alerts, frames, and response time based on the number of attacks and the laying of the sensor against the attacker.
For attacker1 on the number of attacks, at 1, 2, and 3 attacks, the average alert is 12 alerts, 3,8 alerts, and 2,3 alerts, the percentage of de-authentication frame false negative that refers to 1 attack is 28,43 % (2 attacks) and 44,47% (3 attacks), and response time is 0,015 seconds, 0,056 seconds and 0,087 seconds. For sensor placement, in the same room (room 1), a different 1 room (room 2), and different 2 rooms (room 3) from the attacker, the average alert is 10,6 alert, 7, 9 alerts, and 7,8 alerts, the percentage of de-authentication frame

false negative are referring to the de-authentication frame that are detected in the room 1 is 72,48% and 77,17%, and the average response time is 0,018 seconds, 0,046 seconds and 0,111 seconds.
As we get more and more attacks and the dividing wall, the less alert from attacker1, and de-authentication frames's false negative and response time from attacker1 is bigger than before. Therefore, the amount of traffic and the placement of the sensors affect the performance of WIDS. WIDS can work optimally if it is in a room with the AP would like to be monitored and not too much traffic. This is to avoid interference and that too many frames passing through the air.</i>