Implementasi sensor WIDS dan analisa trafik RTT pada pendeteksian rogue access point = Implementation WIDS sensor and RTT traffic analysis on rogue access point detection

M. Adhitya Akbar, author

Abstrak

Perkembangan jaringan wireless internet sangat mengagumkan selama beberapa dekade ini. Hal ini mendorong pertumbuhan hotspot di tempat-tempat umum. Dibalik kemudahannya, terdapat ancaman yang sangat berbahaya, salah satu bentuk ancaman terbesarnya adalah Rogue Access Point (RogueAP). Evil-twin-attack merupakan sebuah proof-of-concept ancaman dari RogueAP. User biasa akan mudah tertipu dan terhubung ke akses poin palsu tersebut. Ketidakpahaman mendalam mengenai network oleh user semakin mempermudah aktifitas hacker. Dibutuhkan suatu sistem yang tepat untuk mengetahui keberadaan RogueAP ini. Metode yang diusulkan juga bermacam-macam seperti pendekatan wired-side, wireless-side dan gabungan keduanya. Pada tulisan ini akan memberikan gambaran dua metode tersebut yaitu analisa trafik RTT dan WIDS sensor. Pada skenario 1 dan 2, kenaikan RTT Ping berkisar rata-rata 7.5% dari RTT Legitimate Access Point. Response time pendeteksian RAP di WIDS sensor tergantung pada jarak dan kekuatan sinyal antara WIDS dengan RogueAP. Pendeteksian WIDS Sensor mencapai keakuratan hingga 100% mendeteksi RogueAP dalam jangkauannya akan tetapi masih berbasiskan identitas mac address. Pada Area 1 dan 2 rata-rata response time berkisar 1-2 detik sedangkan pada Area 3 sebesar 3.7 detik dan Area 4 (1%-24%) sekitar 10.4 detik. Analisa trafik RTT sangat berpotensi menjadi alternatif pendeteksian Rogue Access Point.

<hr>

The development of wireless data networks are very impressive for several decades. This encourages the growth of hotspots in public area. Behind the simplicity, there is a very dangerous threat, one of the greatest threats is the Rogue Access Point. Evil-twin-attack is a proof-of-concept threat of RogueAP. Regular user would be easily fooled and wil be connected to the fake access point. Not understanding the depth of the network by the user enhances the threat from hackers. Therefore we need a proper system for the presence of Rogue Access Point. The proposed method as well as a variety approaches of wired-side, wireless-side and a combination of both (hybrid). In this paper will provide an overview of two methods, namely the analysis of RTT traffic and WIDS sensor. In scenario 1 and 2, average increasing ranged Ping RTT is 7.5% of the RTT Legitimate AP. Response time detection of RAP in WIDS sensor depends on the distance and signal strength between the WIDS with Rogue Access Point. WIDS detection sensor reaches up to 100% accuracy in detecting RogueAP range but still based on the identity of the mac address. Average response time Area 1 and 2 ranges from 1-2 seconds while in Area 3 of 3.7 seconds and Area 4 (1% -24%) at about 10.4 seconds. RTT traffic analysis is a potential alternative to Rogue Access Point detection.