Perancangan dan analisis mekanisme mitigasi di layer 3 terhadap serangan blacknurse pada jaringan berbasis wireless = Design and analysis of mitigation's mechanism in layer 3 against blacknurse attack on wireless based network

Muhamad Harist Refian Anwar, author

Abstrak

Serangan Denial of Service DoS merupakan salah satu serangan yang sering terjadi dalam jaringan internet. Dampak yang dihasilkan mulai dari memperlambat kinerja suatu perangkat keras hingga mematikannya. Selain itu, serangan ini terus berkembang dengan munculnya metode-metode terbaru dalam melakukan penyerangan. Pada tahun 2016, telah ditemukan jenis serangan DoS terbaru dengan kemampuan dalam mematikan sistem pertahanan suatu perangkat keras dalam hal ini yaitu firewall yang diberi nama BlackNurse.
Bekerja seperti serangan ICMP flooding, serangan BlackNurse ini dapat dilakukan oleh siapapun dengan menggunakan suatu jaringan yang memiliki ukuran bandwidth minimal yaitu 15-18 Mbit/s untuk menghasilkan suatu volume paket berukuran 40.000 hingga 50.000 paket ICMP palsu per detik. Serangan ini telah banyak dilakukan untuk menguji ketahanan suatu perangkat keras jaringan dalam menghadapi suatu serangan, seperti router.
Dalam peneilitian ini, digunakan perangkat keras jaringan yang akan diuji berupa layer 3 wireless router. Ditambah dengan pemasangan perangkat lunak bernama Snort dan Wireshark yang berguna untuk menganalisis tingkah laku serta dampak yang dihasilkan dari serangan BlackNurse tersebut kepada perangkat keras yang ditargetkan. Pada bagian akhir penelitian ini, akan disimpulkan langkah mitigasi terbaik yang mampu mengurangi serangan Blacknurse yang dapat terjadi, sehingga kinerja suatu perangkat keras jaringan tetap maksimal.
<hr>Denial of Service (DoS) attack is one that often occurs in the world of internet. The resulting impact ranging from slow performance of a hardware device until turning it off. In addition, these DoS attacks continue to evolve with the emergence of the latest methods for assault. In 2016, a newest type of DoS attack was found with capabilities to turned down the defence system of a hardware device in this case it called firewall which is named BlackNurse.
Works like ICMP flooding attack, the BlackNurse attack can be done by anyone using a network that has a size of minimum bandwidth which is 15 18 Mbit s to generate a volume of packages sized up to 40,000 until 50,000 fake ICMP packets per second. This attack has been widely carried out to test the resilience of a network hardware to face this type of attack, such as a router.
In this research, the network hardware that will be tested is a layer 3 wireless router. With the installation of a software called Snort and Wireshark, researcher can analyze the behavior and the impact resulting from BlackNurse attack which is done to the targeted hardware. At the end of this essay, there will be conclusion on which best mitigation measures that will be able to reduce the Blacknurse attack that can occur, so that the performance of a fixed maximum of network hardware.