Analisa perbandingan man in the middle attack arp spoofing untuk protocol IPV4 dan IPV6 di software defined network = Comparing analysist for man in the middle attack arp spoofing for protocol IPV4 and IPV6 in software defined network / Utama Prillianto Putra

Utama Prillianto Putra, author

Abstrak

ABSTRAK
Address Resolution Protocol (ARP) mempunyai sejarah panjang akan kelemahannya terhadap spoofing attack dikarenakan sifat statelessness nya dan kurangnya mekanisme autentikasi untuk memverifikasi dari pengirim paketnya. ARP spoofing terkadang merupakan titik awal untuk terbentuknya serangan LAN yang lebih canggih seperti denial of service, man in the middle and session hijacking. Metode deteksi saat ini menggunakan pendekatan pasif, memantau trafik ARP dan mencari inkonsistensi didalam Ethernet ke alamat IP yg ter mapping. Kelemahan utama dari pendekatan pasif ini adalah jeda waktu antara mempelajari dan mendeteksi serangan spoofing. Ini kadang-kadang menyebabkan serangan yang ditemukan sudah terlanjur lama berjalan setelah serangan itu direncanakan. Dalam tulisan ini, teknik aktif untuk mendeteksi ARP spoofing di arsitektur SDN untuk protocol IPv4 dan IPv6 dianalisis. Permintaan ARP dan TCP SYN paket dikirimkan ke jaringan untuk menyelidiki inkonsistensi pada jaringan tersebut. Teknik ini lebih cepat, cerdas, terukur dan lebih handal dalam mendeteksi serangan daripada metode pasif. Hal ini juga dapat mendeteksi tambahan pemetaan nyata MAC ke alamat IP untuk tingkat akurasi yang adil dalam hal serangan yang sebenarnya. Saat serangan DOS dengan paket ARP yang tidak berbahaya atau normal, kontroler menggunakan port monitor untuk mencegah beban apapun. Hasilnya cukup mengesankan menunjukkan hasil minimal atau tidak ada overhead pada controller sama sekali. Arsitektur SDN menghasilkan bandwidth lebih bagus dari pada jaringan tradisional. Ini dikarenakan utilisasi bandwidth dari SDN lebih baik daripada jaringan tradisional. Performansi SDN lebih bagus 7,2% dari pada jaringan tradisional. Begitu juga untuk untuk IPv6 performansi SDN lebih bagus 8,1% dari pada jaringan tradisional.
<hr>
ABSTRACT
The Address Resolution Protocol (ARP) due to its statelessness and lack of an authentication mechanism for verifying the identity of the sender has a long history of being prone to spoofing attacks. ARP spoofing is sometimes the starting point for more sophisticated LAN attacks like denial of service, man in the middle and session hijacking. The current methods of detection use a passive approach, monitoring the ARP traffic and looking for inconsistencies in the Ethernet to IP

address mapping. The main drawback of the passive approach is the time lag between learning and detecting spoofing. This sometimes leads to the attack being discovered long after it has been orchestrated. In this paper, we analyze active technique to detect ARP spoofing in SDN architecture for IPv4 and IPv6 protocol. We inject ARP request and TCP SYN packets into the network to probe for inconsistencies. This technique is faster, intelligent, scalable and more reliable in detecting attacks than the passive methods. It can also additionally detect the real mapping of MAC to IP addresses to a fair degree of accuracy in the event of an actual attack. When DOS attack with ARP packets that are not harmful or normal are produced, the controller uses a monitor port to prevent any burden to the controller server. The result is quite impressive show results minimal or no overhead on the controller altogether. SDN architecture produces better bandwidth than traditional networks. This is because the bandwidth utilization of SDN better than traditional network. SDN performance 7.2% better than in traditional networks. Likewise for SDN to IPv6 performance 8.1% better than in traditional networks.Keywords: Man in the middle, ARP, Spoofing, IPv4, Ipv6, SDN