World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:9, No:05, 2015

Packet Fragmentation Caused by Encryption and Using It as a Security Method

Authors : Said Rabah Azzam, Andrew Graham

Abstract : Fragmentation of packets caused by encryption applied on the network layer of the IOS model in Internet Protocol version 4 (IPv4) networks as well as the possibility of using fragmentation and Access Control Lists (ACLs) as a method of restricting network access to certain hosts or areas of a network.Using default settings, fragmentation is expected to occur and each fragment to be reassembled at the other end. If this does not occur then a high number of ICMP messages should be generated back towards the source host indicating that the packet is too large and that it needs to be made smaller. This result is also expected when the MTU is changed for certain links between devices.When using ACLs and packet fragments to restrict access to hosts or network segments it is possible that ACLs cannot be set up in this way. If ACLs cannot be setup to allow only fragments then it is a limitation of the hardware's firmware holding back this particular method. If the ACL on the restricted switch can be set up in such a way to allow only fragments then a connection that forces packets to fragment should be allowed to pass through the ACL. This should then make a network connection to the destination machine allowing data to be sent to and from the destination machine. ICMP messages from the restricted access switch and host should also be blocked from being sent back across the link which will be shown in an SSH session into the switch.

Keywords : fragmentation, encryption, security, switch
Conference Title : ICWIST 2015 : International Conference on Internet Technology and Secured Transactions
Conference Location : London, United Kingdom
Conference Dates : May 25-26, 2015