ABSTRACT

LOCAL AREA NETWORK SECURITY ANALYSIS THAT USES CISCO-BASED DHCP SERVER USING PENETRATION TESTING METHOD

Medianto
1531014

The writing of this scientific paper aims to solve the problem of DHCP Rogue network attack method using DHCP Snooping which is a network security feature that is rarely used by people, because the lack of knowing the importance of network security causes the network to be given less attention on the security matter. For this reason, this scientific paper will discusses how to counteract DHCP Rogues with DHCP Snooping and how to implement these security features on the network. Apart from that, to prove whether using the DHCP Snooping feature is able to counteract Rogue DHCP attacks. The research method used by the author by conducting a study that uses simulation networks. Because of the author is using Cisco-based DHCP Snooping, the authors will conduct research where network simulation will be made in Cisco Packet Tracer simulation applications specifically for simulating with Cisco hardware. From the results of the comparison and conclusions of the study, the authors stated that ordinary networks that do not use the DHCP security feature of Snooping have the potential to be exposed to DHCP Rogue attacks. DHCP Rogue attacks causes hackers to be able to control the entire network by only spreading IP from hackers DHCP server to the network. On the other hand, networks that use the DHCP Snooping network security feature are able to completely ward off IP that is spread from hackers and the client only gets IP from the company's official DHCP Server, so the network is safe and protected from the control of hackers.

Keywords : DHCP Snooping, DHCP Rogue, Cisco Packet Tracer, how DHCP Snooping works, network security.