INTISARI

ANALISIS PENGGUNAAN DHCP *SNOOPING* PADA *CUSTOMER PREMISES EQUIPMENT* DI LAYANAN INTERNET PT INDONESIA COMNETS PLUS

Besarnya konsumsi data yang meningkat di Indonesia sejajar dengan meningkatnya jumlah pelanggan internet. Pada tahun 2018 PT Indonesia Comnets Plus (ICON+) telah menarik lebih dari 2000 pelanggan. Meningkatnya jumlah *client* yang menggunakan layanan internet, diperlukan adanya kemudahan dalam pendistribusian IP kepada pengguna, salah satunya dengan menggunakan protokol DHCP. Namun protokol ini memiliki kelemahan di segi keamanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab seperti adanya serangan DHCP *server rogue*. Terdapat banyak kasus pada perangkat sisi *client* mengalami *reboot* karena adanya pemadaman, perangkat bermasalah, atau gangguan jaringan yang memberikan kesempatan *server rogue* masuk ke jaringan. Dalam mewujudkan integritas informasi maka diperlukan adanya pencegahan terhadap masuknya DHCP *server rogue* dengan penerapan DHCP *snooping* pada *Customer Premises Equipment* (CPE) di layanan internet PT Indonesia Comnets Plus.

Penelitian dilakukan menggunakan *server* I-WON pada tiga skenario yaitu dengan penerapan tanpa penerapan DHCP *snooping* dan tanpa serangan, tanpa penerapan DHCP *snooping* dan adanya serangan, serta penerapan DHCP *snooping* dan adanya serangan. Analisis dilakukan dengan pengujian terhadap parameter alokasi IP, *discover response time*, *elapsed time*, dan *request response time* pada masing-masing skenario. Hasil yang didapatkan adalah adanya alokasi IP yang berasal dari DHCP *server rogue* ketika tidak dilakukan implementasi DHCP *snooping.* Ketika DHCP *snooping* diterapkan, tidak ada alokasi IP DHCP *server rogue* yang diterima oleh *client.* Sedangkan adanya DHCP *server rogue* dan DHCP *snooping* mempengaruhi waktu yang dibutuhkan oleh *elapsed time, discover response time,* dan *request response time.* Rata-rata waktu yang dibutuhkan *elapsed time* skenario kedua memiliki perbedaan 7,57 dari skenario pertama, *discover response time* skenario ketiga perbedaan waktu 1,76 detik dari skenario pertama dan *request response time* skenario ketiga perbedaan waktu 5,72 dari skenario pertama.

Kata Kunci:
DHCP *snooping*, *server rogue*, *Customer Premises Equipment*, DHCP, internet

ABSTRACT

ANALYSIS OF DHCP SNOOPING USAGE IN CUSTOMER PREMISES EQUIPMENT FOR INTERNET SERVICE PT INDONESIA COMNETS PLUS

The high number of data usage in Indonesia is equivalent with the increasing number of internet users. In 2018 PT Indonesia Comnets Plus has captivated more than 2000 clients. The increasing number of clients in using internet service needs easier method in distributing IP to users, the most common method is using DHCP protocol. The weakness of this protocol is the security itself that can be used by attacker like rogue DHCP server attack. There are cases the devices in client side do reboot because of several causes like power outage, error device, or network error so could give opportunity to rogue DHCP server do attack. In order to create the integrity of information, the prevention of rogue DHCP server attack is needed with the implementation of DHCP snooping in Customer Premises Equipment (CPE) in internet service PT Indonesia Comnets Plus.

This research was conducted use I-WON as DHCP server for three scenarios; first without either rogue DHCP server attack or implementation of DHCP snooping; second, attack from rogue DHCP server but without DHCP snooping; third, attack from rogue DHCP server and implementation of DHCP snooping. This study analyzed to the previous scenarios on several parameters; IP allocation, discover response time, elapsed time, and request response time in each scenario. The result of this study shows that client get IP allocation from rogue DHCP server while DHCP snooping is disabled. But if DHCP snooping is enabled, there was no IP allocation from rogue DHCP server. While the presence of rogue DHCP server and DHCP snooping influenced the time that needed by elapsed time, discover response time, and request response time. The different of average time that needed by elapsed time in second scenario is 7.57 seconds from first scenario, while discover response time in third scenario has 1.76 seconds difference from first scenario and request response time has 5.72 seconds difference from first scenario.

Keywords:
DHCP snooping, server rogue, Customer Premises Equipment, DHCP, internet