ABSTRAK

Dalam keamanan data dan informasi pada suatu teknologi informasi akan terus diperbaharui setiap waktu, dengan perkembangan teknologi informasi pada masa ini yang akan selalu berkembang, sehingga menyebabkan kemanan menjadi sebuah prioritas utama. Penggunaan prosedur penelitian metode *Network Development Life Cycle* (NDLC) dimulai dengan *Analysis, Deisgn, Prototype, Implementation, Monitoring,* dan *Management*. Oleh karena itu dengan semakin banyaknya serangan yang dilakukan oleh oknum yang tidak bertanggung jawab sehingga menyebabkan kerusakan terhadap *server*. Serangan tersebut seringkali dilakukan melalui suatu *port* yang tersedia pada *server* dan menyebabkan pengguna yang mempunya akses maupun tidak berkepentingan dapat masuk pada port yang tersedia. Salah satu metode keamanan jaringan yang digunakan pada *port* adalah metode *port knocking* bertujuan memberi lapisan keamanan pada *port* yang tersedia dan menyamarkan *port* yang akan di akses. Sehingga tidak terdeteksi *port* awal yang harus diakses terlebih dahulu agar perangkat masih tetap bisa diakses, dan pengguna yang tidak memiliki akses dapat diblokir pada perangkat. Hasil penelitian ini yaitu dapat mengamankan perangkat pada saat akan di akses dan setiap aktifitas akses perangkat tersebut akan dihubungkan pada aplikasi telegram yang terhubung secara *online* kepada *administrator* jaringan dan akan mendapatkan notifikasi melalui *bot* telegram.

Kata kunci : Keamanan jaringan, NDLC *(Network Depelopment life Cycle), Port Knocking*.

ABSTRACT

In data and information security, information technology will continue to be revamped from time to time, with the development of information technology this time which will always develop, thus causing security to become a top priority. The use of research procedures using the Network Development Life Cycle (NDLC) method begins with Analysis, Design, Prototype, Implementation, Monitoring and Management. Therefore, with the increasing number of attacks carried out by irresponsible persons, causing damage to the server. These attacks are often carried out through an available port on the server and cause users who have access and are not authorized to enter the available port. One of the network security methods used on ports is the port knocking method, which aims to provide a layer of security on available ports and disguise the ports to be accessed. So that the initial port is not detected which must be accessed first so that the device can still be accessed, and users who do not have access can be blocked on the device. The results of this study are that it can secure the device when it will be accessed and every activity of accessing the device will be connected to the telegram application which is connected online to the network administrator and will get notifications via telegram bot.

Keyword *: Network Security,NDLC (Network Depelopment life Cycle), Port Knocking.*