

ABSTRAK

Hutasoit, DF. 2022. *Implementasi Port Knocking dan Honeypot Sebagai Keamanan Jaringan Pada Server Virtual Ubuntu*, Skripsi. Tanjungpinang: Jurusan Teknik Informatika, Fakultas Teknik, Univeristas Maritim Raja Ali Haji. Pembimbing I: Muhammad Radzi Rathomi, S.Kom., M.Cs. Pembimbing II: Nola Ritha, S.T.,M.Cs.

Keamanan suatu *server* merupakan hal yang sangat krusial mengingat *server* sebagai penyedia layanan dan menampung banyak data penting tentang pengguna, dan hal ini lah yang membuat *server* sering dijadikan target penyerangan. oleh karena itu penelitian ini difokuskan pada sistem keamanan *server* yang sering dijadikan sebagai percobaan penyerangan oleh attacker, yaitu layanan *SSH* dan *Telnet*. untuk mengantisipasi serangan yang datang peneliti menerapkan metode keamanan *port knocking*, *honeypot*, dan *IP tables*. *port knocking* merupakan teknik autentikasi yang mengharuskan *client* untuk memasukkan urutan ketukan *port* tertentu sebelum bisa melakukan koneksi *ssh* ke *server*, dan setelah *client* selesai mengakses *server*, maka *firewall* akan menutup kembali akses ke *server* sehingga *server* tidak bisa diakses kembali, *Honeypot* berfungsi untuk mengalihkan *port server* utama ke *port server* tiruan dan sengaja terbuka untuk mengetahui apa saja upaya yang dilakukan untuk memasuki *server*. dan *IP tables* berfungsi untuk menggantikan peran *firewall*, untuk menentukan aturan *port* mana yang akan di *filter*, sehingga setiap paket yang masuk pada *filtered port* akan di *refused*.

Kata kunci: Sistem Informasi, *Port Knocking*

ABSTRACT

Hutasoit, DF. 2022. *Implementasi Port Knocking dan Honeypot Sebagai Keamanan Jaringan Pada Server Virtual Ubuntu*, Skripsi. Tanjungpinang: Jurusan Teknik Informatika, Fakultas Teknik, Univeristas Maritim Raja Ali Haji. Pembimbing I: Muhammad Radzi Rathomi, S.Kom., M.Cs. Pembimbing II: Nola Ritha, S.T.,M.Cs.

The security of a *server* is very crucial considering the *server* as a service provider and holds a lot of important data about its *users*, and this is what makes the *server* often used as a target for attacks. therefore, this research is focused on *server security systems* that are often used as attack attempts by attackers, namely *SSH* and *Telnet* services. in anticipation of the oncoming attacks researchers applied security methods of *port knocking*, *honeypots*, and *IP tables*. *port knocking* is an authentication technique that requires the *client* to enter a certain sequence of *port* taps before it can make an *ssh* connection to the *server*, and after the *client* finishes accessing the *server*, the *firewall* will *close* access to the *server* again so that the *server* cannot be accessed Again, *Honeypot* serves to switch the main *server port* to the dummy *server port* and deliberately *opens* to find out what attempts are made to enter the *server* and *IP tables*. serves to replace the role of the *firewall*, to determine which *port rules* will be *filtered*, so that any packets that enter on the *filtered port* will be refused.

Keywords: *Information System, Port Knocking*