INTISARI

RANCANGAN DAN IMPLEMENTASI KEAMANAN WEB SERVER DENGAN TEKNIK HARDENING DALAM KASUS WORDPRESS

Nur Fauzi
18/431575/SV/15546

Data merupakan hal yang sangat penting dan sensitif di era sekarang ini dikarenakan antara data yang satu dengan lainnya mempunyai keterikatan atau saling terkoneksi sehingga dapat mengakses ke berbagai hal yang menunjang kebutuhan hidup seseorang, data menjadi sebuah konfirmasi pemilik akun seseorang. Keamanan merupakan hal yang terpenting dalam menjaga kebenaran dan keutuhan data, serta menjamin ketersediaan layanan kepada penggunanya. Berkembangnya sistem keamanan terutama pada keamanan *server*, menuntut sistem keamanan menjadi lebih baik, terlebih dalam keamanan *web server*. Di era saat ini, teknologi memudahkan banyak hal terutama dalam pembuatan dan memanajemen konten yang di publish di *website* dengan menggunakan *Content Management System*, contohnya yaitu *wordpress*. Namun, masih terdapat kelemahan atau celah pada *web server*, sehingga akan lebih mudah dalam melakukan eksploitasi dengan berbagai macam teknik penyerangan.

Pada pengujian ini, penerapan sistem keamanan jaringan terdiri dari dua buah *server*, yaitu *server gateway* dan *web server*. *Server gateway* merupakan *server* yang mengamankan *web server* dari berbagai teknik penyerangan yang berasal dari jaringan atau terhubung ke luar. Kemudian *web server* merupakan *server* yang digunakan untuk *Content Management System* berjenis *wordpress* dan lebih mengarah untuk mengamankan aplikasinya. Pada *server gateway* dipasang tools seperti *Firewall, port knocking, IDS, honeypot, reverse proxy* dan *network analyzer* sedangkan pada *web server* mengkonfigurasi *htaccess* dan memasang *plugins* pada *wordpress*. Pada *Firewall* menggunakan iptables, *port knocking* menggunakan knockd, *IDS* dan *monitoring* menggunakan maltrail, *honeypot* menggunakan endlessh. Semua penyerangan yang mengarah kepada *website* dengan *ip server gateway* akan terdeteksi oleh *IDS* dan di visualkan pada *browser* secara *real-time*. Sedangkan penyerangan melalui *remote* atau *ssh*, *port ssh* asli dipindah dengan *port* yang lebih tinggi (22222) dan dipasang *port knocking* kemudian pada *port default ssh* (22) diteruskan ke *port* (2222) yang dipasang dengan *honeypot*. Dari penelitian ini akan mendapatkan informasi tentang keberhasilan dalam melakukan *penetration testing* kepada keamanan *server*. Sehingga, dengan hadirnya sistem keamanan pada *web server* ini dapat menjadi alat untuk mengamankan *server* dengan *tools* yang simple tetapi *powerful* dalam hal pengamanan dan juga *server* tidak keberatan dalam menjalankan *tools* tersebut sehingga kinerjanya menjadi optimal.

Kata kunci *: Firewall, Honeypot, IDS, Keamanan Webserver, Port knocking*

ABSTRACT

Web Server Security Design and Implementation with Hardening Techniques In Case Of Wordpress

Nur Fauzi
18/431575/SV/15546

Data is very important and sensitive in today's era because data is related to one another or connected to each other so that it can access various things that support one's life needs, data becomes confirmation of one's account owner. Security is the most important thing in maintaining the truth and integrity of data, as well as ensuring the availability of services to its users. The development of security systems, especially on servers, demands a better security system, especially in web server security. In the current era, technology makes things easier, especially in the creation and management of content published on websites using a Content Management System, for example, WordPress. However, there are still weaknesses or gaps in the web server, so it will be easier to exploit with various attack techniques.

In this test, the application of the network security system consists of two servers, namely the gateway server and the web server. The gateway server is a server that secures the web server from various attack techniques originating from the network or connecting to the outside. Then the web server is a server that is used for the wordpress Content Management System and is more directed to securing the application. On the gateway server, tools such as Firewall, port knocking, IDS, honeypot, reverse proxy and network analyzer are installed, while the web server configures htaccess and installs plugins on WordPress. Firewall uses iptables, port knocking uses knockd, IDS and monitoring uses maltrail, honeypot uses endlessh. All attacks that lead to websites with the gateway server ip will be detected by the IDS and visualized on the browser in real-time. While the attack is via remote or ssh, the original ssh port is moved to a higher port (22222) and port knocking is installed then on the default ssh port (22) is forwarded to the port (2222) which is installed with a honeypot. From this research, you will get information about the success of doing penetration testing on server security. So, with the presence of a security system on this web server, it can be a tool to secure servers with simple but powerful tools in terms of security and also the server does not mind running these tools so that its performance is optimal.

Keywords: Firewall, Honeypot, IDS, Port knocking, Web server Security