

PERANCANGAN SISTEM MONITORING AKTIF BERBASIS ANDROID PADA INTRUSION PREVENTION SYSTEM (IPS) SURICATA

Kholiq
(11.04.1.1.1.00059)

Pembimbing I : Cucun Very Angkoso, S.T., M.T.
Pembimbing II : Dwi Kuswanto, S.Pd., M.T.

ABSTRAK

Intrusion Prevention System (IPS) merupakan sistem yang dapat diterapkan untuk melakukan pengawasan terhadap jaringan untuk memberikan keamanan pada *server*. Salah satu sistem *IPS* yang digunakan adalah *IPS Suricata*. Namun terkadang seorang *administrator* jaringan bekerja dengan lebih dari satu *IPS Suricata*. Hal ini dapat membuat *administrator* jaringan tersebut mengalami kesulitan dalam melakukan pengawasan. Sehingga dibutuhkan suatu perangkat yang dapat melakukan pengawasan secara *realtime*, dan akan memberikan *alert* jika *IPS Suricata* mendeteksi adanya serangan.

Android merupakan sistem operasi berbasis *Linux* yang dikembangkan untuk perangkat *smartphone* dan *tablet*. Dalam penelitian ini, sistem *monitoring* yang dibangun menggunakan perangkat berbasis *Android*. Jika terjadi serangan maka *Monitoring Agent* pada *IPS Suricata* akan memblokir penyerang dan mengirimkan informasi serangan kepada *Web Server*, untuk kemudian akan menjadi *notification* pada perangkat *Android*. Sistem *monitoring* yang akan dibangun juga dapat melakukan *monitoring* lebih dari satu *IPS Suricata*.

Setelah dilakukan uji coba 50 kali serangan menggunakan *Port Scanning* dengan *Nmap* dan *SuperScan*, *SQL Injection* dengan *Havij*, dan *Vulnerability Web Scanner* dengan *Nikto*. Terbukti aplikasi *Monitoring Agent* yang mengkombinasikan *IPS Suricata* dengan *IPTables* mampu mendeteksi dan memblokir penyerang. *Monitoring Agent* juga dapat mengirimkan informasi serangan ke *Web Server*, dan dapat diterima oleh *Android Client* sebagai *notification*.

Kata kunci : *Android, Intrusion Prevention System (IPS), Suricata, Monitoring, IPTables.*

ACTIVE MONITORING SYSTEM DESIGN BASED ON ANDROID FOR INTRUSION PREVENTION SYSTEM (IPS) SURICATA

Kholiq
(11.04.1.1.1.00059)

Adviser I : Cucun Very Angkoso, S.T., M.T.

Adviser II : Dwi Kuswanto, S.Pd., M.T.

ABSTRAK

Intrusion Prevention System (IPS) is a system that can be applied to conduct monitoring of the network to provide security on the server. One of the IPS system used is IPS Suricata. But sometimes a network administrator to work with more than one IPS Suricata. It can make the network administrators have difficulty in doing monitoring. So it needs a device that can perform real-time monitoring, and will provide alerts if IPS Suricata detected an attack.

Android is a Linux-based operating system that was developed for smartphones and tablets. In this study, a monitoring system that is built using Android-based devices. If there is an attack, the Monitoring Agent on IPS Suricata will block the attacker and sends information to the Web server attacks, and then will be notification on Android devices. The monitoring system to be built also can monitor more than one IPS Suricata.

After testing 50 times attacks using Port Scanning with Nmap and SuperScan, SQL Injection with Havij, and Web Vulnerability Scanner with Nikto. Proven applications that combine IPS Monitoring Agent Suricata with IPTables able to detect and block attackers. Monitoring Agent can also send information to the Web server attacks, and can be accepted by the Client as Android notifications.

Keywords : Android, Intrusion Prevention System (IPS), Suricata, Monitoring, IPTables.