

## BAB V

### PENUTUP

#### 5.1 Kesimpulan

Berdasarkan penelitian pada PT Adlink Sinemedia setelah dibuatnya sistem keamanan jaringan terhadap *server*, penulis menarik kesimpulan sebagai berikut :

1. Lapisan keamanan yang akan diterapkan terhadap server pada PT Adlink Sinemedia yaitu terdiri dari *Honeypot* yang menggunakan software *HoneyPy*, yang dimana akan berfungsi untuk mengalihkan percobaan koneksi melalui port 21 pada IP, kemudian lapisan keamanan Intrusion Prevention System yang diterapkan terhadap server menggunakan Snort yang berjalan secara *inline* dengan *AFPack* yang dimana diterapkan beberapa *rules* yang mencegah serangan *Bruteforce* FTP, Ping of Death, SYN Flood Attack, dan UDP Flood Attack.
2. *Intrusion Prevention System* mengamankan *server* dengan cara mendeteksi koneksi yang masuk ke jaringan dan menyaring nya menggunakan fitur *filter* yang ada pada *Snort* dengan *AFPack* pada *server* yang telah diterapkan untuk mencegah penyerangan yang berjenis *Bruteforce* FTP, Ping of Death, SYN Flood Attack, dan UDP Flood Attack.
3. Proses implementasi *Honeypot* dimulai dengan instalasi *honeypy* yang kemudian di konfigurasi untuk berjalan pada *port* 21 pada jaringan dan mengubah jalur FTP menjadi *port* 5678, *Honeypy* akan berfungsi untuk mengalihkan penyerang yang melakukan *port scanning* dan melakukan penyerangan melalui *port* 21 yang mengarah ke *Honeypot*. Proses implementasi *Intrusion Prevention System* diawali dengan instalasi software *Snort* versi 2.9.18 yang kemudian akan dilakukan konfigurasi terhadap *server* yang telah diterapkan untuk mencegah serangan yang berjenis *Bruteforce* FTP, Ping of Death, SYN Flood Attack, dan UDP Flood Attack. Dari penelitian didapatkan hasil bahwa *Honeypot* berhasil mengalihkan *port scanning* sebanyak 5 kali yang dilakukan terhadap IP

Muhammad Rizaldi, 2021

**SISTEM KEAMANAN SERVER BERBASIS INTRUSION PREVENTION SYSTEM DAN HONEYPOT PADA PT ADLINK SINEMEDIA**

UPN Veteran Jakarta, Ilmu Komputer, Informatika

[ [www.upnvj.ac.id](http://www.upnvj.ac.id) – [www.library.upnvj.ac.id](http://www.library.upnvj.ac.id) – [www.repository.upnvj.ac.id](http://www.repository.upnvj.ac.id) ]

*server* yang kemudian mengakses *port 21* yang mengarah ke *Honeypot*. IPS pada penelitian ini berhasil mencegah percobaan penyerangan sebanyak 144 *Bruteforce FTP*, serangan *Ping of Death* yang berhasil di *drop* sebanyak 63 packet yang berjumlah 85% dari 74 packet yang dikirimkan, serangan *SYN Flood Attack* yang berhasil di *drop packet* yang berjumlah 142 yang berjumlah 100% dari packet yang dikirimkan. *UDP Flood Attack* yang berhasil di *drop packet* yang berjumlah 289489 packet yang dimana merupakan 52% dari 556710

## 5.2 Saran

Berdasarkan kesimpulan dari penelitian yang telah dibuat oleh penulis, oleh karena itu penulis mengajukan beberapa saran yang mungkin dapat berguna dan diimplementasikan terhadap *server* di PT Adlink Sinemedia maupun berguna sebagai referensi pemakalah lain yang ingin mengimplementasikan sistem yang telah penulis buat. Saran yang penulis berikan sebagai berikut :

1. Melakukan perawatan pada perangkat jaringan yang ada pada perusahaan seperti melakukan *upgrade* terhadap *switch, router, access point*, maupun melakukan *upgrade* terhadap kabel *UTP RJ45* yang digunakan untuk menghubungkan *user* dengan internet maupun dengan *server*.
2. Meningkatkan kualitas terhadap keamanan *server* dengan cara menambahkan *local rules* pada *snort* sesuai dengan kebutuhan yang dibutuhkan dan melakukan *update rules* yang ada pada *snort*.