Abstrak

Pada tunnel IPv6 over IPv4 masih bisa terjadi *spoofing*. Seorang penyerang mengirim paket ke alamat tertentu dengan alamat yang dipalsukan melewati sistem tersebut atau bahkan memang salah satu node dari sistem tersebut yang dituju. Alamat IPv4 yang digunakan untuk *spoofing* merupakan salah satu dari ujung-ujung tunnel. Tunnel IPv6 over IPv4 menggunakan dua jenis IP, IPv4 dan IPv6, yang header IPv6 beserta payloadnya akan dibungkus dengan header IPv4 sehingga bisa melewati infrastruktur IPv4. Untuk mengurangi dampak dari serangan *spoofing* tersebut direkomendasikan penggunaan protokol keamanan yang beroperasi di level IP, yaitu *IP Security* (IPSec). Ada dua protokol yang bisa digunakan. Protokol tersebut adalah *Authentication Header* (AH) dan *Encapsulating Security Payload* (ESP). Setiap protokol tersebut bisa menggunakan mode transport atau mode tunnel. Menurut RFC4891, mode transport akan melindungi paket yang didefinisikan dengan (alamat IPv4 sumber, alamat IPv4 tujuan, protokol=41), sedangkan mode tunnel melindungi paket yang didefinisikan (alamat IPv6 sumber, alamat IPv6 tujuan). Penggunaan mode transport direkomendasikan karena protokol 41 masih ada. Protokol tersebut merupakan penanda bahwa paket yang dibawa adalah paket IPv6.

Skenario tunneling yang digunakan adalah *host-to-host*. Sistem utama yang dibangun ada dua, yaitu tunnel tanpa IPSec dan tunnel dengan IPSec. Masing-masing sistem akan dikirimi dengan sejumlah paket *spoofing* yang kemudian akan diamati jumlah paket yang diproses oleh korban maupun node lain yang terkena akibatnya (tersangka). Selain itu, akan diamati pula utilitas yang diakibatkan oleh paket *spoofing* yang dikirimkan tersebut pada kedua host. Pada sistem yang menerapkan IPSec akan dilakukan pengujian tentang pengaruh umur hidup IPSec terhadap paket yang diproses oleh keduanya pula beserta utilitasnya.

Setelah itu, hasil dari sistem yang tidak menggunakan IPSec akan dibandingkan dengan hasil dari sistem yang menerapkan IPSec kemudian didapat kesimpulan bahwa paket yang diproses pada sistem dengan IPSec jauh lebih sedikit daripada sistem yang tanpa IPSec. Sebelum menerapkan IPSec, korban memproses paket sebanyak tiga kali jumlah paket *spoofing* yang dikirim (paket dengan flag SYN, SYN/ACK, dan RST), sedangkan tersangka memproses dua kalinya (paket dengan flag SYN/ACK dan RST). Setelah menerapkan IPsec, hanya korban saja yang menerima paket dengan flag SYN dari penyerang yang kemudian paket tersebut tidak akan diproses lagi dengan mengirim SYN/ACK ke tersangka. Hal ini disebabkan paket *spoofing* yang masuk ditolak di level IPSec. Utilitas yang diakibatkan oleh paket *spoofing* tersebut juga mengalami penurunan karena tidak ada paket yang diproses. Umur hidup IPSec tidak terlalu berpengaruh pada paket yang diproses maupun utilitas yang dihasilkan oleh paket *spoofing* tersebut. Hal ini juga disebabkan oleh paket *spoofing* yang ditolak di level IPSec sehingga tidak ada paket yang diproses lagi.

Kata Kunci: IPv6-*over*-IPv4, tunn*el*, *spoofing*, IPv4, IPv6, level IP, IPSec, AH, ESP, mode transport, mode tunnel, paket, utilitas, umur hidup IPSec