PENGESANAN PENCEROBOHAN TRAFIK PENEROWONGAN IPV6 BERASASKAN RANGKAIAN NEURAL PERAMBATAN BALIK

NAZRULAZHAR BIN BAHAMAN

TESIS YANG DIKEMUKAKAN UNTUK MEMPEROLEH IJAZAH
DOKTOR FALSAFAH

FAKULTI TEKNOLOGI DAN SAINS MAKLUMAT
UNIVERSITI KEBANGSAAN MALAYSIA
BANGI

2014

PENGAKUAN

Saya akui karya ini adalah hasil kerja saya sendiri kecuali nukilan dan ringkasan yang setiap satunya telah saya jelaskan sumbernya.

11 September 2014

NAZRULAZHAR BIN BAHAMAN
P 50007

PENGHARGAAN

Syukur Alhamdulillah kepada Allah S.W.T kerana memberikan saya kesihatan yang cukup, masa dan kematangan fikiran untuk menyiapkan penyelidikan ini. Jutaan terima kasih yang rasanya tidak saya mampu untuk balas kembali hingga ke akhir hayat saya kepada penyelia utama Prof. Madya Dr. Anton Satria Prabuwono atas bantuan yang begitu besar, bimbingan, teguran dan nasihat yang begitu berguna sepanjang kajian ini. Tidak lupa juga kepada Prof. Madya Dr. Mohd. Faizal Abdollah dan Dr. Robiah Yusof dengan kepakaran masing-masing yang banyak membantu menguatkan lagi semangat saya untuk menyiapkan kajian ini. Terima kasih juga saya ucapkan kepada pihak KPM dan UTeM atas kebenaran mengikuti pengajian ini serta skim bantuan SLAI yang banyak membantu dari segi kewangan pada kajian ini.

Sumber data bagi penulisan ini telah diperoleh dari trafik rangkaian UTeM. Penulis ingin mengucapkan ribuan terima kasih kepada pegawai-pegawai UTeM khususnya pegawai dari Pusat Komputer kerana membantu saya dari segi pengurusan serta kebenaran dalam proses penyediaan data. Tidak lupa juga pegawai-pegawai dari FTMK, UTeM kerana membenarkan saya menggunakan peralatan dengan semaksimumnya. Begitu juga dengan pegawai yang bertanggungjawab terhadap sumber maklumat di perpustakaan FTSM, UKM. Sekalung penghargaan juga tidak saya lupakan buat NAV6, USM yang telah banyak menyediakan input dari segi data dan maklumat terkini dari luar negara.

Terima kasih yang tidak terhingga juga ditujukan kepada ayahanda serta bonda tercinta Haji Bahaman Kaba dan Hajah Saoma Zakaria yang telah banyak memberi sokongan dan dorongan bagi menyiapkan pengajian ini. Juga kepada isteri serta anak-anak tersayang Elia Erwani Hassan, Muhammad Adeeb Amsyar, Nur Aeen Insyirah dan Nur Aimee Irdyinah atas pengorbanan yang ditempuhi bersama.

ABSTRAK

Setelah melaksanakan mekanisme peralihan IPv6 sebagai pemangkin peralihan protokol Internet, telah memberi kesan terhadap prestasi sebahagian daripada teknik anti pencerobohan. Sistem Pengesanan Pencerobohan (SPP) adalah antara yang amat terkesan di mana kadar janaan penggera palsu yang meningkat ekoran corak ancaman yang berubah. Sebagai tindakan, tesis ini mencadangkan suatu penerbitan corak dan permodelan serangan implikasi penggunaan mekanisme peralihan iaitu penerowongan 6to4. Perolehan maklumat dari permodelan tersebut digunakan bagi mereka bentuk Sistem Pengesanan Pencerobohan Rangkaian Penerowongan (SPP-RP) yang memfokuskan kepada serangan DoS yang tersembunyi di dalam paket kapsul penerowongan yang dikenali sebagai protokol-41. Objektif penyelidikan ini adalah (i) menganalisis tahap keberkesanan SPP semasa terhadap serangan DoS pada model medan uji penerowongan, (ii) menerbitkan corak dan model serangan DoS Alihan Penerowongan (SeDAP), (iii) menggubal kaedah pengelasan corak dengan bantuan algoritma pengelasan RN, dan (iv) menilai serta mengesahkan pembangunan kaedah pengelasan corak mampu meningkatkan pengesanan dan mengurangkan kadar bilangan penggera palsu. Pembangunan medan uji berpandukan model Makmal Lincoln MIT yang melalui beberapa kaedah pengujian bagi memastikan jenis peralatan dan tatarajah tidak mempengaruhi hasil keputusan penyelidikan. SPP-RP terdiri daripada 3 peringkat utama dan setiap darinya terdapat beberapa bahagian. Pertama, peringkat input mengandungi bahagian penangkapan. Kedua, peringkat Pengesanan yang mengandungi bahagian pemprosesan, bahagian pengelasan dan bahagian penggera. Ketiga ialah peringkat output mewakili bahagian tindak balas. Kaedah pengelasan RNPB ini turut disepadukan dengan teknik pengesanan bagi menentukan status data. Tiga jenis algoritma latihan iaitu *Levenberg-Marquardt, Bayesian Regulation* dan *Scaled Conjugate Gradient* dibandingkan bagi memilih yang terbaik. Kesimpulannya, SPP-RP berkebolehan di dalam mengenal pasti trafik penerowongan yang mengandungi paket normal dan anomali dan turut berjaya membantu mengurangkan janaan penggera palsu.

IPV6 TUNNELING TRAFFIC INTRUSION DETECTION BASED ON BACK PROPAGATION NEURAL NETWORK

ABSTRACT

After implementing of IPv6 transition mechanism (TM) as IP catalyst transition has influences the performance on anti-intrusion system. IDS is one of the greatly affected where there is an increasing rate of false alarms generated due to changing patterns of threat. As an action, this thesis proposes new formulation of attack pattern and model lead by implication of TM named 6to4 tunneling. The outcomes from the model are used to develop SPP-RT that focuses on DoS attack that hiding in encapsulating tunneling packet known as protocol-41. The objectives of the research are (i) analysis the performance of IDS on the testbed model, (ii) formulate SeDAP pattern and model, (iii) ability to extract packet features from IPv4 and IPv6 header, and (iv) capable to increase detection rate and decrease false alarm using BPNN. The development of testbed refers to MIT Licoln Lab model was experimented through several testing methods. This accomplishment was done to ensure that the type of equipment and figure will maintain the accurate results. The SPP-RP formed by 3 major parts containing various modules individually. In first, Information Processing consists of capture module, status labeling module and features extraction module. Secondly, Detection part involved with preprocessing module and classification module. The third part called Output with alert notification module. Furthermore, the BPNN method has been integrated into classification module in determining the normal and anomaly status. Then, this BPNN module applied with 3 dissimilar training algorithms named as Levenberg-Marquardt, Bayesian Regulation and Scaled Conjugate Gradient. As a conclusion the highlighted SPP-RP perform capable to recognize tunneling traffic with normal or anomaly packet and a successful tool in reducing false alarm.

KANDUNGAN

SENARAI JADUAL

SENARAI ILUSTRASI

SENARAI SINGKATAN PERKATAAN

DoS	Serangan Penafian Perkhidmatan
ICMP	*Internet Control Message Protocol*
IETF	*Engineering Task Force*
IPv4	Protokol Internet Versi 4
IPv6	Protokol Internet Versi 6
KB	Kecerdasan Buatan
KDD	*Knowledge Discovery in Database*
MPIPv6	Mekanisme Peralihan IPv6
NGTRANS	*Next Generation TRANSition*
P41	Protokol 41
Palsu$^{(-)}$	Negatif Palsu
Palsu$^{(+)}$	Positif Palsu
RN	Rangkaian Neural
RNPB	Rangkaian Neural Perambatan Balik
SDP	Serangan DoS Penerowongan
SeDAP	Serangan DoS Alihan Penerowongan
SPP	Sistem Pengesanan Pencerobohan
SPPH	Sistem Pengesanan Pencerobohan berasaskan Hos
SPPR	Sistem Pengesanan Pencerobohan berasaskan Rangkaian
SPP-RP	Sistem Pengesanan Pencerobohan Rangkaian Penerowongan
SPR	Sistem Pemantauan Rangkaian
TA	Tembok Api
TCP	*Transmission Control Protocol*
Tulen$^{(-)}$	Negatif Tulen

Tulen$^{(+)}$	Positif Tulen
UDP	*User Datagram Protocol*

BAB I

PENDAHULUAN

1.1 LATAR BELAKANG

Kebergantungan terhadap perkhidmatan berasaskan teknologi maklumat bukan lagi satu fenomena asing. Teknologi ini mendapat kepercayaan oleh pengguna kerana telah terbukti dengan kesahihan dan kejituan perkhidmatan yang ditawarkan. Tambahan pula dengan tersedianya rangkaian komunikasi terkini, telah menjadikannya lebih efisien. Justeru itu, pelbagai pihak telah menjadikan teknologi ini sebahagian besar daripada urusan perkhidmatan harian mereka. Pelbagai maklumat umum mahu pun yang sulit, telah dimuatkan ke alam maya. Oleh itu penglibatan teknologi komunikasi secara tidak langsung turut mendapat perhatian oleh kebanyakan pihak. Keadaan ini telah menjadikan teknologi komunikasi salah satu elemen yang sangat penting dalam era ini.

Sejak awal perkhidmatannya, Protokol Internet Versi 4 (IPv4) merupakan pendukung utama dan tunggal bagi teknologi komunikasi data berinternet. Namun hingga ke hari ini, alamat IP yang tidak terpakai telah mengalami penyusutan amat ketara. Perkara ini diperakui oleh Karpilovsky et al. (2009), di mana menurut beliau dalam beberapa tahun terdekat, permintaan untuk memperoleh alamat IP ini akan terbatas ekoran bilangannya hampir kehabisan. Implikasi daripada kekusutan ini, pengguna Internet telah mula beralih kepada alternatif protokol yang lain iaitu Protokol Internet Versi 6 (IPv6). Sungguhpun IPv6 masih di peringkat asas perlaksanaannya, namun keupayaannya untuk memenuhi keperluan jumlah alamat Internet telah mengatasi kelemahan asas IPv4.