Jurnal Antarabangsa (Teknologi Maklumat) 2(2002): 1-13

FTSM WATCH: Pendekatan Berasaskan-petua Untuk Mengesan Pertelingkahan dan Pencerobohan Alamat IP/ETHERNET

AZIZI ABDULLAH & KHAIRUDDIN OMAR

ABSTRAK

Dalam persekitaran terbuka seperti Universiti dan organisasi penyelidikan, pengalamatan IP biasanya diumpukan secara statik. Pengalamatan berkenaan memberi peluang berlakunya fenomena pertelingkahan dan pencerobohan IP/MAC. Aplikasi FtsmWatch direka bentuk untuk menangani pencerobohan salahguna yang menggunakan teknik rajah peralihan keadaan berasaskan-petua. Satu set petua yang saling berhubung kait dengan nilai ambang direka bentuk untuk membuat keputusan. Keputusan yang dijalankan dalam persekitaran sebenar menunjukan corak pertelingkahan dan pencerobohan IP/MAC berjaya dikesan secara masa-nyata menggunakan FtsmWatch.

Kata kunci : pertelingkahan dan pencerobohan IP, keselamatan rangkaian, pengesanan pencerobohan berasaskan-rangkaian, rajah keadaan berasaskan-petua.

ABSTRACT

In the open environment like University and research organization the IP address is regularly assigned statically. This type of address provides the opportunity of conflict and violation of IP/MAC phenomenon to occur. The application of FtsmWatch was created to handle misuse violation which uses the rule-based state diagram technique. A set of rules corresponding with the appropriate thresholds was designed for intrusion decision. The decision that was implemented in the real environment shows that the conflict and violation of IP/MAC pattern can be detected in real-time using FtsmWatch.

Keywords : IP conflict and intrusion, network security, host-based intrusion detection system, rule-based state diagram.

Sistem pengesanan pencerobohan atau *intrusion detection system* (IDS) merupakan sistem automasi untuk mengesan pencerobohan komputer. Secara umumnya matlamat IDS untuk mengenalpasti sebarang salah guna, penganiayaaan sistem komputer dan penggunaan tidak sah oleh kedua-dua pencerobohan dalaman atau luaran pada masa nyata [1]. Terdapat dua domain utama mengesan pencerobohan dalam rangkaian iaitu: pengesanan salah guna dan pengesanan anomali. Pengesanan salah guna adalah lebih kepada cubaan menyalahgunakan kelemahan yang diketahui terdapat dalam perisian atau sistem komputer. Sesuatu pencerobohan salah guna mengesan anasir pencerobohan berdasarkan padanan corak atau tanda tangan. Setiap tandatangan serangan terhadap kelemahan sistem komputer atau perisian mangsa adalah berbeza di antara satu sama lain. Sementara pengesanan anomali adalah berdasarkan kepada mengenalpasti kelakuan luarbiasa terhadap operasi pada perisian atau sistem komputer mangsa. Kelakuan mungkin berbentuk penggunaan sumber bahan komputer dan operasi terhadap sistem fail yang luar biasa. Kelakuan anomali juga dapat dikesan dengan mengkuantitikan kelakuan biasa atau normal dengan kelakuan yang luar biasa yang berpontensi sebagai penceroboh [2].

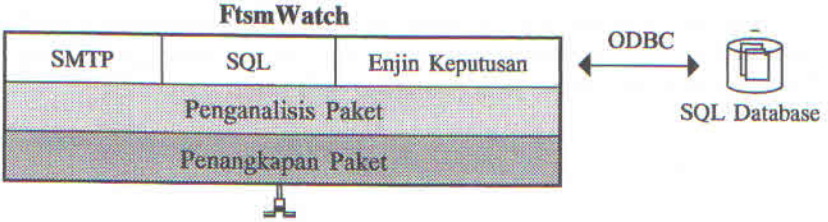
Penyelidikan mengenai pengesanan pencerobohan semakin meningkat selari dengan kadar pencerobohan ke atas komputer yang semakin bertambah. Terdapat dua kategori IDS iaitu berasaskan sistem pengesanan berasaskan-hos dan berasaskan-rangkaian. Suatu IDS berasaskan-hos adalah menjalankan jejak audit ke atas sistem pengoperasian yang merupakan input utama pada satu hos yang berisiko. Sistem pengoperasian yang berlainan memerlukan corak pengesanan yang berbeza. Aplikasi IDS adalah tertanam pada hos tersebut dan boleh mengesan sebarang pencerobohan berbentuk salah guna dan anomali. Kekangan terhadap pemantauan pada satu komputer berisiko sahaja memberi motivasi kepada pembangunan IDS berasaskan-rangkaian. Sementara IDS berasaskan-rangkaian akan memantau sebarang hos yang berada dalam suatu segmen rangkaian. Terdapat satu komputer yang berfungsi untuk mengaudit jejak trafik rangkaian pelbagai hos untuk mengenalpasti corak atau tanda tangan serangan oleh penceroboh. Ianya tidak bergantung kepada sistem pengoperasian kerana corak trafik rangkaian keluar-masuk adalah seragam.

Penyelidikan dan penggunaan IDS sebagai suatu sistem yang dapat mengesan dan memaklum sebarang aktiviti pencerobohan semakin meningkat. Ini memandangkan sistem pencegahan pencerobohan yang sudah "matang" seperti perisian *firewall* masih mempunyai kelemahan. Fungsi *firewall* secara umumnya bertindak sebagai pelindung sistem komputer daripada ancaman keselamatan daripada risiko luaran. Kebanyakan *firewall* hanya memberi tumpuan kepada pencerobohan berdasarkan kepada *security event* berbanding

dengan IDS yang lebih dinamik dan berdasarkan kepada *security event* dan *alarm* [3]. Pengesanan pencerobohan rangkaian adalah dipilih bukan sahaja dapat menghalang aktiviti pencerobohan tetapi boleh memberi peringatan awal amaran terhadap fenomena pengodaman komputer.

SENIBINA FTSMWATCH

Setiap komponen FtsmWatch dilaksanakan menggunakan teknik bebenang (threading) dengan komponen lain tanpa bimbang dengan semafor. Setiap komponen tidak akan menghalang proses pada komponen lain. Secara ringkasnya senibina FtsmWatch terbahagi kepada tiga komponen iaitu: Penangkapan paket, Penganalisis paket, dan Enjin keputusan FtsmWatch. Senibina komponen FtsmWatch boleh digambarkan seperti Rajah 1.



RAJAH 1. Senibina FtsmWatch

Komponen utama FtsmWatch terdiri daripada komponen penangkapan data (paket), penganalisis data rangkaian dan enjin keputusan berasaskan-petua. Komponen sampingan adalah seperti SMTP dan SQL bertindak sebagai automasi dan memaklumkan sebarang pertelingkahan dan pencerobohan IP/MAC menerusi e-mail.

TEKNIK BERASASKAN-PETUA

Terdapat banyak pendekatan untuk mengesan pencerobohan telah dicadangkan [4]. Kaedah yang berbeza akan beroperasi dengan cara yang berbeza. Pelbagai teknik telah dicadangkan dan digunakan untuk mengesan pencerobohan tetapi tiada satu penyelesaian terbaik yang dapat menghadangi semua serangan. Sesetengah teknik adalah efisyen untuk mengesan satu corak tunggal tetapi tidak sesuai untuk meramal corak yang dinamik walaupun jenis serangannya adalah sama. Teknik mengesan corak tunggal adalah amat berkesan jika corak atau tanda tangan serangan atau penceroboh adalah statik dan tidak akan mengalami sebarang perubahan pada masa hadapan. Contohnya teknik berasaskan-petua sesuai mengesan sebarang pertelingkahan IP/MAC dan

pencerobohan IP/MAC pada suatu sumber komputer. Tanda tangan pencerobohan biasanya dikelaskan dengan mengenalpasti *perhubungan* di antara entiti. Kaedah berasaskan-petua adalah disepadukan kepada sistem cerdas dalam kepintaran buatan [5]. Setiap perhubungan menentukan proses pembelajaran melalui perwakilan kelas *petua if-then*. Jika keputusan mesti dibuat dengan maklumat tertentu, secara logikal sesuai menggunakan petua keputusan *first-order if-then* seperti petua berikut :

Tentukan ω_1 *IF* $f(\omega_1) > f(\omega_2)$; selainya tentukan ω_2.

Petua keputusan *first-order if-then*

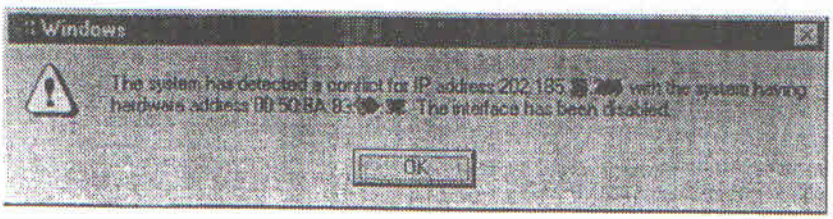
Untuk kes pertelingkahan dan pencerobohan IP/MAC petua keputusan *first-order if-then* digunakan memandangkan sebarang keputusan dipengaruhi oleh parameter (w) yang dinamik dalam trafik rangkaian. Parameter w boleh digambarkan sebagai peristiwa atau *event* yang akan memetakan fungsi atau kelakuan dengan keputusan yang ditetapkan oleh petua.

METODOLOGI

Perkara pertama yang perlu difikirkan untuk menjejak pertelingkahan, dan pencerobohan IP/MAC iaitu (a) Ciri pertelingkahan dan pencerobohan IP/MAC, (b) Mengaudit data untuk menentukan tanda pertelingkahan dan pencerobohan, dan (c) QoS iaitu mengesan dan memaklum kelakuan dengan efisyen dengan situasi serangan sebenar.

PERTELINGKAHAN DAN PENCEROBOHAN IP/MAC

Pertelingkahan IP bermaksud satu alamat IP cuba dikongsi oleh dua komputer rangkaian dalam satu persekitaran sama. Apabila fenomena ini berlaku komputer yang mengesan pertelingkahan memaparkan mesej ralat seperti yang ditunjukkan dalam Rajah 2 (untuk sistem pengoperasian Windows/NT):



RAJAH 2. Mesej pertelingkahan IP

Pengesanan alamat yang duplikasi merupakan satu perkara penting. Bila timbunan (stack) diawalkan ataupun alamat IP baru ditambah dalam rangkaian, protokol ARP (Address Resolution Protocol) akan disiarkan (broadcast) untuk alamat IP bagi hos tersebut. Jika terdapat hos lain yang respon ARP tersebut, bermakna alamat IP sedang digunakan. Apabila ini berlaku dan hos yang melanggar masih *boot;* antara muka rangkaian tidak berupaya untuk mencapai sumber rangkaian dan log sistem akan dijanakan dan ralat seperti yang Rajah 2 dipaparkan pada skrin hos. Jika hos yang mempertahankan alamat IP adalah berasaskan Windows, log sistem akan dijanakan, dan mesej ralat dipaparkan pada hos tersebut. Untuk membaiki kerosakan yang disebabkan oleh ARP *cache* pada hos lain, hos yang melanggar menyiarkan semula ARP lain, meletak-semula nilai sebenar dalam ARP *cache* pada hos yang dilanggar.

Pencerobohan IP/MAC berlaku apabila tiada sahutan (respond) daripada hos lain. Pencerobohan dikesan dengan membina suatu pangkalan data yang memetakan alamat IP dengan alamat MAC pada hos yang memasuki rangkaian. Secara umumnya pencerobohan IP/MAC tidak dapat dikesan oleh protokol ARP secara automatik, perlu ada suatu teknik yang perlu untuk mengatasi masalah tersebut. Contoh pangkalan data yang direka bentuk untuk menangani masalah pencerobohan alamat IP/MAC seperti Jadual 1 di bawah.

JADUAL 1. Maklumat Individu dan IP/MAC

Alamat_IP	Alamat_MAC	Tarikh/Masa	E-mail	Nama	Lokasi

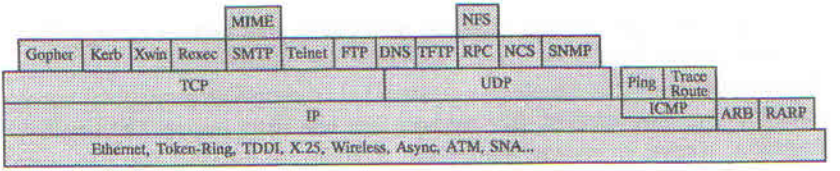
Di dalam reka bentuk pangkalan data, kesetaraan maklumat terutama pemetaan **Alamat_IP** dan **Alamat_MAC** mestilah setara iaitu **Alamat_IP** ⇔ **Alamat_MAC.**

MENGAUDIT DATA

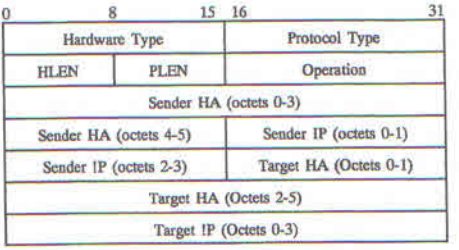
Proses mengaudit audit data adalah untuk mencari ciri-ciri dan hubungan mengenai data yang dikaji. Setiap paket yang mengalir dalam mod bercamuran *(promiscous)* disemak. Pengaudit data dilakukan ke atas *arpdump* untuk melihat kelakuan yang bersifat salah guna dalam trafik rangkaian. Ia merupakan input asas untuk pengesanan berasaskan-petua terhadap pertelingkahan dan pencerobohan rangkaian. Rajah 3 menunjukan format protokol ARP yang perlu dikeluarkan daripada protokol TCP/IP untuk menentukan perhubungan dengan ciri-ciri dalam data yang dikaji.

Corak pertelingkahan dan pencerobohan IP/MAC perlu ditentukan daripada *arpdump.* Medan berikut adalah disaring daripada kepala ARP:

1. Sumber alamat perkakasan (*sender hardware address – Sender HA).*
2. Sumber alamat IP (*sender protocol address – Sender IP).*



(a)



(b)

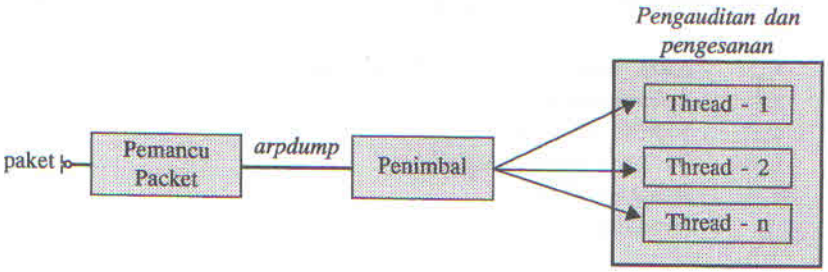
RAJAH 3. Format ARP dalam model TCP/IP. (a) Lapisan TCP/IP (b)Datagram ARP

3. Destinasi alamat perkakasan (*target hardware address – Target HA).*
4. Destinasi alamat IP (*target protocol address – Target IP).*
5. Operasi (*operation).*

Proses mengaudit data *arpdump* dilakukan jika timbunan (*stack*) diawalkan atau bila alamat IP baru ditambah dalam rangkaian. Alamat IP yang perlu dianalisis untuk mengesan pencerobohan perlulah berada dalam domain atau *subnet mask* rangkaian. Alamat IP yang lain perlulah diabaikan. Ia adalah perlu memandangkan *arpdump* yang dianalisis adalah dalam mod *promiscous* dan mempengaruhi kualiti penggera pertelingkahan atau pencerobohan IP/MAC.

QoS

Sebuah sistem pencerobohan yang baik dapat mengesan dan memaklum kejadian dengan cepat dan betul. Ia bergantung kepada senibina IDS dan adalah penting. Untuk mengatasi masalah tersebut, suatu penimbal dicipta yang dilaksanakan serentak bersama-sama dengan pengauditan, pengesanan, dan tindak balas. Fungsi penimbal adalah untuk menyimpan paket yang berkaitan dengan protokol ARP. Saiz penimbal sepatutnya dinamik dan bergantung kepada trafik rangkaian semasa. Jika saiz penimbal sifar iaitu setiap paket ARP dianalisis secara masa-nyata dalam mod *promiscous* boleh menjejaskan prestasi keseluruhan sistem komputer. Rajah 4 menunjukkan senibina pengauditan dan pengesanan pertelingkahan dan pencerobohan IP/MAC.

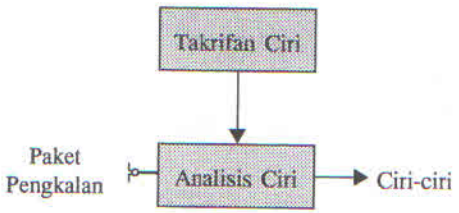


RAJAH 4. Senibina pengauditan dan pengesanan paket ARP FtsmWatch.

Sebarang keputusan pengesanan adalah bergantung kepada saiz penimbal. Berdasarkan pengalaman FtsmWatch, saiz penimbal yang dinamik dapat membantu proses dan operasi yang sedang berjalan dengan cekap.

PEMILIHAN PETUA

Tugas utama enjin keputusan ialah mengesan corak pertelingkahan dan pengawalan alamat IP baru dalam rangkaian. Ia cuba menyaring parameter penting daripada paket rangkaian. Parameter yang dikaji menggunakan medan kepala protokol ARP seperti yang dibincangkan di atas. Struktur komponen pemilihan petua adalah seperti Rajah 5 berikut :



RAJAH 5. Komponen pemilihan petua.

Berdasarkan takrifan ciri yang dikenal pasti, paket akan dianalisis untuk menentukan hubungan di antara parameter yang dikaji. Fitur tertakrif oleh protokol ARP REQUEST (F_{arp}) adalah dalam format 5 parameter tuple. Ciri-ciri yang ditakrifkan oleh sistem adalah (S_HA, S_IP, T_HS, T_IP, Op) seperti berikut:

$$F_{arp} = (\text{S\_HA}, \text{S\_IP}, \text{T\_HA}, \text{T\_IP}, \text{Op}).$$

Setiap parameter mempunyai maksud berikut :

F_{arp} : paket yang terdiri daripada *arpdump.*
S_HA : Sumber alamat perkakasan.
S_IP : Sumber alamat IP.
T_HA : Destinasi alamat perkakasan.
T_IP : Destinasi alamat IP.
Op : Parameter Operasi.

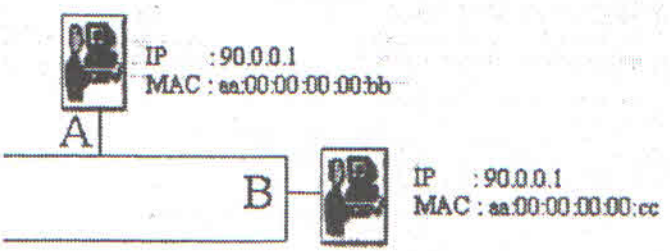
Berdasarkan kepada parameter di atas, enjin keputusan seterusnya dibina. Ciri-ciri yang perlu diambil perhatian ialah terhadap ARP REQUEST.

ENJIN KEPUTUSAN

Enjin keputusan adalah sebahagian daripada sistem. Ia menganalisis peristiwa dengan set petua pengesanan dan mengenal pasti sebarang salah-guna rangkaian. Untuk mengenalpasti corak pencerobohan, jujukan paket mestilah mematuhi beberapa keadaan. Berikut adalah fitur yang disaring daripada paket yang melibatkan pertelingkahan dan pengawalan alamat IP baru rangkaian:

$$F_{arp} = (S\_HA, S\_IP, T\_HA, T\_IP, Op).$$

Untuk menentukan pertelingkahan alamat IP boleh dirujuk dalam Rajah 6. Hos B cuba melanggar alamat IP pada hos A.

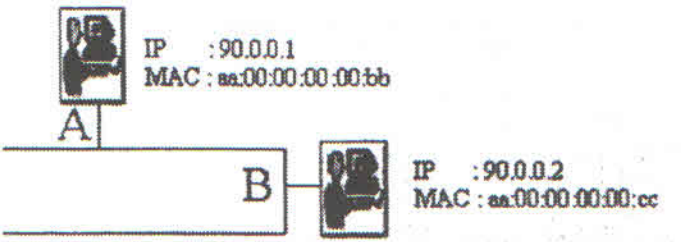


RAJAH 6. Pertelingkahan alamat IP

Fitur pertelingkahan (jika hos A dan B mempunyai alamat IP sama) berdasarkan fitur di bawah :

F_{arp} = (aa:00:00:00:00:bb, 90.0.0.1, aa:00:00:00:00:cc, 90.0.0.1, 2). (1)

Untuk menentukan pengawalan alamat IP baru rangkaian boleh dirujuk dalam Rajah 7. Hos B memasuki rangkaian menggunakan alamat IP baru.



RAJAH 7. Pengawalan alamat IP baru rangkaian

Pengawalan IP baru berdasarkan fitur di bawah :

F_{arp} = (aa:00:00:00:00:cc, 90.0.0.2, 00:00:00:00:00:00, 90.0.0.1, 1). (2)

Berdasarkan kepada kes (1) dan (2) di atas, perwakilan set petua pengesanan dapat ditentukan. Di bawah adalah petua yang boleh dibina untuk mengesan pertelingkahan dan Pengawalan IP baru rangkaian :

Petua 1 : Mengesan Pertelingkahan

```
IF ( TCP-IP PACKET = = ARP PACKET ) THEN
    IF ( S_IP = = T_IP AND Op = = 2 ) THEN
            Pertelingkahan = TRUE
    ELSE
            Pertelingkahan = FALSE
    ENDIF
END IF
```

Petua 2 : Mengesan Pengawalan IP baru

```
IF ( TCP-IP PACKET = = ARP PACKET ) THEN
    IF ( S_IP = = T_IP AND Op = = 1 ) THEN
            IP_Baru = TRUE
    ELSE
            IP_Baru = FALSE
    ENDIF
END IF
```

Daripada petua 2, pencerobohan alamat IP/MAC dapat ditentukan. Di bawah adalah petua 3 yang dibina untuk mengesan pencerobohan alamat IP/MAC :

Petua 3 : Mengesan pencerobohan MAC asing

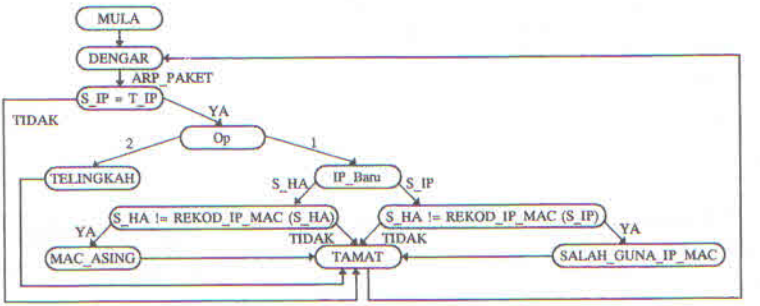
```
IF ( TCP-IP PACKET = = ARP PACKET ) THEN
    IF ( S_IP = = T_IP AND Op = = 1 ) THEN
        IF ( S_HA != Rekod_IP_MAC(S_HA) ) THEN
                MAC_Asing = TRUE
        ELSE
                MAC_Asing = FALSE
        ENDIF
    ENDIF
END IF
```

Rekod_IP_MAC merujuk kepada pangkalan data yang memetakan alamat IP kepada alamat MAC yang sah. Julat alamat MAC disemak berdasarkan parameter S_HA dari protokol ARP. Dengan mengubah petua 3, pengesanan terhadap pencerobohan IP atau salah guna IP dalam rangkaian dapat ditentukan menggunakan petua berikut :

Petua 4 : Mengesan salah-guna IP

```
IF ( TCP-IP PACKET = = ARP PACKET ) THEN
    IF ( S_IP = = T_IP AND Op = = 1 ) THEN
        IF ( S_HA != Rekod_IP_MAC (S_IP) ) THEN
            Salah_guna_IP_MAC = TRUE
        ELSE
            Salah_guna_IP_MAC = FALSE
        ENDIF
    ENDIF
END IF
```

Kesatuan di antara S_HA dan S_IP dapat diuji dengan menggunakan fungsi Rekod_IP_MAC. Fungsi tersebut menerima parameter S_IP dan menukarkan kepada alamat MAC sebenar IP tersebut. Daripada petua dan keadaan di atas, gambarajah pengesanan keadaan seperti ditunjukan dalam Rajah 8 .



RAJAH 8. Rajah pengesanan keadaan

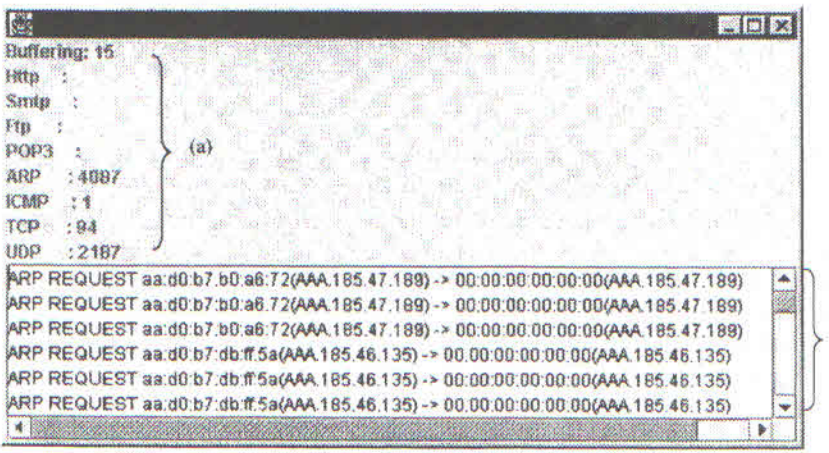
Alat perisian rangkaian FtsmWatch yang dibangunkan, diuji dalam persekitaran rangkaian kawasan setempat (LAN). Ia mampu mengesan sebarang pertelingkahan atau pencerobohan IP/MAC dan memaklum fenomena tersebut kepada beberapa pihak tertentu. Dalam kes di Fakulti Teknologi dan Sains Maklumat di antara pihak yang dimaklumkan ialah :

- Penceroboh.
- Mangsa penceroboh.
- Pentadbir sistem.

Antaramuka yang dibangunkan adalah ringkas dan terhad kepada beberapa perkara berikut :

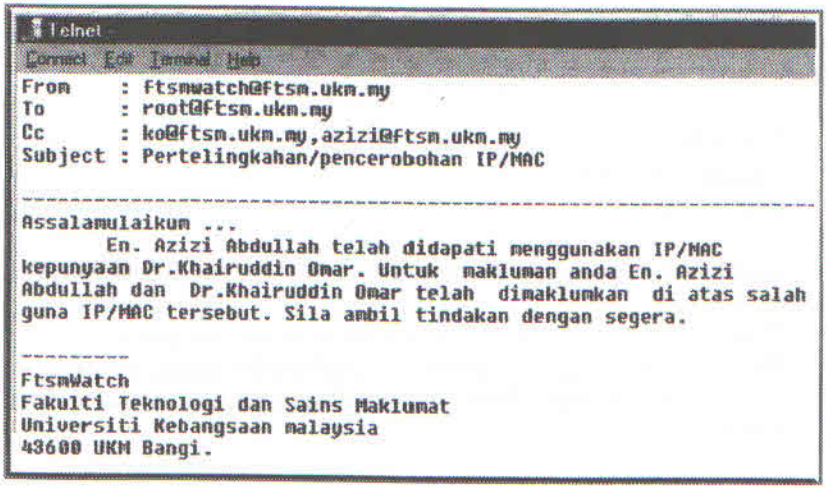
- Memantau perjalanan paket protokol TCP/IP secara masa-nyata
- Mengesan dan memaparkan paket ARP yang berkaitan dengan pengawalan IP baru dan sebarang fenomena pertelingkahan dan pencerobohan IP/MAC.

Antaramuka alat perisian FtsmWatch boleh digambarkan seperti rajah 9.



RAJAH 9. (a) Pemprosesan protokol TCP/IP masa nyata oleh FtsmWatch. Setiap paket dalam penimbal akan diproses apabila mencapai nilai ambang 100. (b) Kotak mesej yang mengesan sebarang pertingkahan dan pengawalan IP/MAC baru dalam persekitaran rangkaian kawasan setempat.

Apabila berlaku fenomena pertelingkahan atau pencerobohan IP/MAC mesej seperti yang digambarkan dalam rajah 10 akan dipaparkan. Antaramuka yang dipaparkan adalah berupaya mesej e-mail yang dihantar oleh FtsmWatch.



RAJAH 10. Contoh antaramuka mesej yang dimaklumkan kepada pengguna yang terlibat jika berlaku pertelingkahan atau pencerobohan IP/MAC menggunakan perisian pine.

KESIMPULAN

Kertas ini cuba menunjukan FtsmWatch boleh digunakan bukan sahaja untuk mengesan pertelingkahan atau konflik alamat IP, tetapi juga sebagai alamat sistem pengesan pencerobohan berdasarkan IP/MAC. Aplikasi FtsmWatch telah diuji dengan rapi ke atas pelbagai jenis rangkaian yang mempunyai kelajuan berbeza. Penggunaan penimbal (*buffer*) dapat menentukan kualiti prestasi ke atas FtsmWatch. Saiz penimbal sebanyak (100 * SizeOf (Packet)) byte diuji ke atas Ethernet 10 Mbit. Saiz berkenaan adalah sudah memadai untuk FtsmWatch berfungsi dengan normal.

RUJUKAN

Biswanath, M., Heberlein, L.T & Karl, N.L. 1994. *Network Intrusion Detection*: IEEE Network.

Kumar, S. 1995. *Classfication and Detection of Computer Intrusion*. Ph.D. Thesis, Department of Computer Science, Purdue University, W.Lafayette, IN

Jordan, C. 2001. *Analyzing IDS Data*. http://www.securityfocus.com/focus/ids/articles/analyzeids.html.

Debar H., Dacier M. & Wespi A. 1999. *Towards a Taxonomy of Intrusion Detection System*. Computer Network.

Richard O.D., Peter E.H. & David G.S. 2001. *Pattern Classification*. 2nd Edition John Wiley & Sons.

Dave M.D. 1996. Microsoft Windows NT 3.5/3.51/4.0: *TCP/IP Implementation Details and TCP/IP Protocol Stack and Services, Version 2.0*. A White Paper from Enterprise Technical Support and the Personal and Business Systems Division.

Joe N. 2000. *Automating IP host Data Collection on a LAN*.
ftp: //ftp.ssc.com/pub/lj/listings/issue67/3517.tgz

Stuart M.C., Joel S. & George K. 2001. Hacking Expose: *Network Security Secretes and Solutions*. 3rd Edition. McGrawHill.

David J.M. 2001. Computer Intrusion Detection and Network Monitoring: *A Statical Viewpoint*. Springer-Verlag.

Richard S.W. 1994. TCP/IP Illustrated Volume 1: *The Protocols*. Addision-Wesley.

Michael N. 2002. Artifical Intelligence: *A Guide to Intelligent Systems*. Addision Weseley.

Rebecca G.B 2000. *Intrusion Detection*. MacMillan Technical Publishing

MAKLUMAT PENGARANG
Azizi Abdullah & Khairuddin Omar
Jabatan Sains Komputer
Fakulti Teknologi dan Sains Maklumat
Universiti Kebangsaan Malaysia
43600 UKM Bangi, Selangor D.E, Malaysia.
azizi@fsm.um.my; ko@ftsm.ukm.my