ANALISIS LOG ROUTER SEBAGAI TOLAK UKUR KEAMANAN PERANGKAT PENGGUNA JARINGAN (STUDI KASUS : IT TELKOM)

Muhammad Riwandeta[1], Niken Dwi C[2], Gandeva Bayu S[3]

Fakultas Teknik Informatika Institut Teknologi Telkom, Bandung

[1]detha.division@gmail.com, [2]nkn@ittelkom.ac.id, [3]gbs@ittelkom.ac.id

Abstrak

Seiring dengan berkembangnya teknologi Internet, semakin banyak situs-situs yang berkembang di dunia maya. Hal ini dapat menyebabkan perangkat user yang terhubung ke jaringan menjadi rentan terhadap serangan (attack). Mulai dari terinfeksi virus, pengiriman spam, hingga bentuk serangan-serangan lainnya. Pada tugas akhir ini akan membahas tentang analisis kebiasaan user yang menyangkut masalah keamanan perangkat komputernya melalui informasi yang dapat digali dari log file. Melalui log file tersebut, dapat diketahui kebiasaan dan perilaku user dalam dalam melakukan tindakan yang akan meningkatkan atau menurunkan tingkat keamanan perangkat komputernya. Hal ini dapat diketahui dengan perhitungan data berdasarkan jumlah IP address yang aktif, yang kemudian diklasifikasikan berdasarkan pemanfaatan update antivirus serta update Operating System MS Windows serta IP yang tidak melakukan update.

Kata Kunci ***: Log file, Internet, Keamanan Komputer, Update***

Abstract

Along with the development of Internet technology, the sites in cyberspace are more developed. This can cause the user device connected to the network becomes vulnerable to attack. Starting from virus infected, sending spam, to other forms of attacks. At the end of this assignment will be discussed on the analysis of user habits regarding computer security devices through which information can be extracted from the log file. Through the log file, can be known about user habits and behavior in taking action that will raise or lower the security level of the computer. This can be determined by calculations of data based on the number of active IP addresses, which are then classified based on utilization and update antivirus update MS Windows Operating System and IP that is not an update.

Key Word : ***Log File, Internet, Computer Security, Update***

1. Pendahuluan

Seiring dengan berkembangnya teknologi Internet, semakin banyak situs-situs yang berkembang di dunia maya. Hal ini dapat menyebabkan perangkat user yang terhubung ke jaringan menjadi rentan terhadap serangan (attack). Mulai dari terinfeksi virus, pengiriman spam, hingga bentuk serangan-serangan lainnya. Akibat fatal yang terjadi adalah dapat mengakibatkan kerusakan pada perangkat yang terserang. Untuk menghindari hal itu, maka diperlukan suatu mekanisme yang digunakan untuk menganalisa perilaku user dalam menjaga keamanan perangkatnya. Hal tersebut dapat dilihat dari pertukaran data (traffic) user yang terjadi di jaringan. Mekanismenya adalah dengan menganalisis log files yang terdapat pada server di jaringan.

Server log files merupakan catatan aktivitas yang terjadi pada web server dalam suatu jaringan. Server log files menyediakan secara terperinci mengenai file request terhadap web server dan respon server terhadap request tersebut. **[1]**

Pada log files dapat dilihat perilaku user dalam melakukan Update operating system dan update anti virus. Updating operating system dan update antivirus secara rutin, merupakan suatu hal yang dapat user lakukan untuk tetap menjaga keamanan perangkatnya. Hal ini memang tampak sepele dan malah terkadang diabaikan oleh user. Seperti yang pernah dikemukakan oleh sales Kaspersky, Jack Chow, tentang kesadaran user dalam melakukan update antivirus. "Masyarakat saat ini memang belum sadar. Padahal antivirus itu sudah seperti obat kalau kita sakit. Terlebih lagi, masyarakat belum terbiasa update antivirus setiap hari. Padahal di dalam antivirus tersebut sudah tersimpan mekanisme update langsung. Sehingga pengguna tidak perlu khawatir terhadap keamanan data dalam perangkatnya." **[2]**

Diharapkan dengan adanya penelitian ini, nantinya dapat diketahui mengenai aktifitas dan perilaku user di jaringan di kampus IT Telkom terhadap kebiasaan mereka dalam melakukan update anti virus serta update operating system, yang bertujuan untuk mengetahui tingkat vulnerability software antivirus dan operating system tersebut terkait tingkat keamanan perangkat yang digunakan.

2. Log

Sebuah file log adalah file yang menyimpan semua tindakan dalam urutan yang terjadi dengan Server, perangkat, aplikasi. File log seperti "kotak hitam" di dalam pesawat terbang, tetapi hanya perbedaan adalah bahwa file log dapat digunakan untuk menyimpan crash dari sebuah server dengan mendapatkan rincian tindakan pada server atau perangkat lunak di muka. Log file berisi tentang informasi permintaan, termasuk client alamat IP, permintaan tanggal / Log Server waktu, halaman yang diminta, HTTP kode, byte dilayani, user agent, dan referrer biasanya ditambahkan. Log server biasanya tidak mengumpulkan informasi user tertentu. File-file ini biasanya tidak dapat diakses oleh pengguna internet umum, hanya untuk webmaster atau administrator atau lainnya.**[3]**

3. Analisis Log

Analisis log (atau sistem dan analisis jaringan log) adalah sebuah seni dan ilmu pengetahuan yang berusaha untuk mencari hal/data penting dari catatan yang dihasilkan dari setiap perangkat "cerdas". Proses dalam menciptakan catatan tersebut disebut data logging. Ada beberapa alasan mengapa orang melakukan analisis log, diantaranya adalah:

- Penyesuaian terhadap kebijakan keamanan
- Untuk memecahkan masalah yang tarjadi
- Forensik (selama investigasi)

4. Router

Router adalah sebuah alat yang mengirimkan paket data melalui sebuah jaringan atau Internet menuju tujuannya, melalui sebuah proses yang dikenal sebagai routing. Router berfungsi sebagai penghubung antar dua atau lebih jaringan untuk meneruskan data dari satu jaringan ke jaringan lainnya. Router sangat banyak digunakan dalam jaringan berbasis teknologi protokol TCP/IP, dan router jenis itu disebut juga dengan IP Router. Internet merupakan contoh utama dari sebuah jaringan yang memiliki banyak router IP. **[4]**

5. Prinsip Keamanan Komputer

Seperti yang dikatakan John D. Howard : "*Computer security is preventing attackers from achieving objectives through unauthorized access or unauthorized use of computers and networks. (John D. Howard, An Analysis of Security Incidents on The Internet 1989)*". Dari definisi yang ada, dapat disimpulkan bahwa keamanan komputer adalah: Suatu usaha pencegahan dan pendeteksian penggunaan komputer secara tidak sah atau tidak diizinkan **[5]**

Jika kita berbicara tentang keamanan komputer, maka secara tidak langsung kita berbicara bagaimana mencegah virus untuk masuk dan menjangkit komputer. Ada beberapa cara yang dapat dilakukan agar virus tidak masuk dan menjangkit komputer, diantaranya adalah :

a) Gunakan AntiVirus

Tentu saja ini yang paling penting. Anti virus dapat diibaratkan sebagai sebuah penjaga yang akan mencegah berbagai macam virus yang akan menjangkit komputer kita.

b) Selalu Update

Jangan lupa untuk selalu mengupdate antivirus dan operating system demi keamanan komputer. Tidak ada perangkat lunak atau software yang sempurna. Pasti ada sebuah celah keamanan. Untuk menutup lubang keamanan itu kita harus update dan update. Karena virus internet juga selalu update dan update.

Selain hal-hal yang telah disebutkan diatas sebelumnya, tingkat vulnerability juga mempengaruhi dalam tingkat keamanan perangkat komputer pada end-user. Dalam system security komputer, istilah Vulnerability merupakan suatu kelemahan yang memungkinkan celah untuk masuk dan mendapatkan hak akses kedalam komputer yang dituju(target). Biasanya vulnerability adalah kelemahan yang dikarenakan kesalahan setting ataupun ataupun ketidaktahuan administrator. Semakin rendah vulnerability sebuah perangkat, maka akan semakin aman pula perangkatnya dan begitupun sebaliknya**. [6], [7]**

6. Antivirus

Antivirus adalah sebuah jenis perangkat lunak yang digunakan untuk mengamankan, mendeteksi, dan menghapus virus komputer dari sistem komputer. Antivirus disebut juga Virus Protection Software. Aplikasi ini dapat menentukan apakah sebuah sistem komputer telah terinfeksi dengan sebuah virus atau tidak. Umumnya, perangkat lunak ini berjalan di latar belakang (background) dan melakukan pemindaian terhadap semua berkas yang diakses (dibuka, dimodifikasi, atau ketika disimpan). Antivirus - antivirus terbaru sekarang tidak hanya mendeteksi virus. Program antivirus sekarang juga telah dilengkapi dengan kemampuan untuk mendeteksi spyware, rootkits, dan malware lainnya. **[8].**

7. Microsoft Windows

Microsoft Windows atau yang lebih dikenal dengan sebutan Windows adalah keluarga sistem operasi yang dikembangkan oleh Microsoft, dengan menggunakan antarmuka pengguna grafis. Sistem operasi Windows telah berevolusi dari MS-DOS, sebuah sistem operasi yang berbasis modus teks dan command-line.

Windows 1.0 merupakan perangkat lunak 16-bit tambahan (bukan merupakan sistem operasi) yang berjalan di atas MS-DOS (dan beberapa varian dari MS-DOS), sehingga ia tidak akan dapat berjalan tanpa adanya sistem operasi DOS. Versi 2.x, versi 3.x juga sama. **[11]**

8. Kuisioner

Kuesioner adalah pertanyaan tertulis yang diberikan kepada responden untuk menjawab. Sebelumnya harus dipastikan kebenaran atas responden yang diteliti berdasarkan kriteria respondennya. Tujuan kuesioner adalah untuk memberikan tinjauan tentang ekspresi metafora dalam berbagai macam bahasa di dunia. Semua metode mensyaratkan pencatatan yang detail, lengkap, teliti dan jelas. **[12]**

9. Populasi, Sampel, dan Rumus Slovin

Populasi adalah wilayah generalisasi berupa subjek atau objek yang diteliti untuk dipelajari dan diambil kesimpulan. Sedangkan sampel adalah sebagian dari populasi yang diteliti. Dengan kata lain, sampel merupakan sebagian atau bertindak sebagai perwakilan dari populasi sehingga hasil penelitian yang berhasil diperoleh dari sampel dapat digeneralisasikan pada populasi. **[13]**

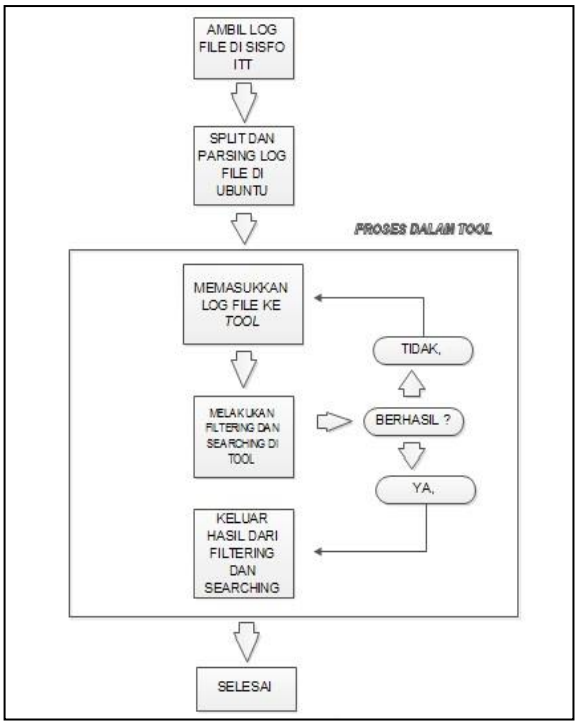
Perhitungan/rumus yang banyak digunakan untuk menentukan ukuran sampel adalah Rumus Slovin.

$$n = \frac{N}{1+N(d)^2}$$

Dimana :
n = jumlah sampel
N = Jumlah populasi
d = nilai presisi (0,05 sampai 0,1)

10. Skenario Implementasi Pengujian Data

Dalam proses pengujian data, diperlukan skenario yang terencana dengan baik. Sehingga memudahkan dalam tahapan pengambilan data seta pengujian data, yang nantinya berpengaruh besar pada data yang diperoleh, untuk kemudian dilakukan analisis lebih lanjut. Untuk itu, perlu dibuat sebuah flowchart pengerjaan yang nantinya dipakai sebagai acuan yang membantu dalam proses perancangan. Gambar1 berikut ini adalah flowchart pada skenario pengukuran data.



Gambar 1. flowchart skenario pengukuran data.

11. Skenario Pengujian Data

Ada beberapa tahapan yang dilakukan dalam pengujian data, diantaranya adalah :

1. Memecah log file menjadi beberapa bagian
2. Memasukkan log file ke Ms.Excel
3. Memindahkan log file yang di Ms.Excel ke Ms.Access, kemudian di save dalam format .mdb
4. Buka tool, kemudian open database, lalu pilih file database yang diinginkan
5. Melakukan filterasi IP Source
6. Melakukan proses filtering IP source untuk mengetahui jumpah IP aktif dengan menggunakan tool yang telah dibuat
7. Melakukan proses searching url destination untuk mengetahui proses automatic update antivirus dan automatic update Ms.Windows dengan menggunakan tool yang telah dibuat

12. Pengujian

Pada tahap pengujian dilakukan untuk mencari data dan informasi perilaku user dari log file yang ada serta mencari nilai prosentase untuk mengetahui nilai keamanan perangkat yang digunakan oleh user. Kemudian pada analisis hasil pengujiannya akan dilakukan analisis tentang faktor penyebab besar atau kecilnya nilai prosentase yang didapat dari tahap pengujian yang telah dilakukan.

Parameter filterasi dan searching yang dianalisis pada tugas akhir ini secara garis besar adalah tentang automatic update microsoft windows

dan automatic update antivirus. Alasan pemilihan dua jenis filterisasi ini adalah:

- Mengingat bahwa jenis Operating System windows merupakan salah satu jenis Operating System(OS) yang rentan terhadap serangan yang berasal dari luar, terutama pada saat mengakses internet. Seperti virus, spam, dan lain-lain.
- Salah satu bentuk perlindungan OS windows dari serangan virus ataupun spam dapat digunakan antivirus yang mampu mendeteksi sekaligus menghapus virus ataupun spam tersebut.

Antivirus yang dipakai dalam pengujian ini adalah hasil dari survey yang dilakukan terhadap user yang menggunakan jaringan kampus dan dipilih 3 antivirus teratas. Berdasarkan hasil survey terhadap 155 responden (populasi : 12000, toleransi 8%, reliability 92%), didapat Avira, AVG, dan Avast sebagai 3 antivirus teratas yang paling banyak digunakan. Dengan rincian sebagai berikut :

- Avira : 35 responden
- AVG : 31 responden
- Avast : 24 responden
- Nod32 : 18 responden
- McAfee : 15 responden
- Norton : 13 responden
- Kaspersky : 12 responden
- Lainnya : 9 responden

Survey tidak dilakukan kepada seluruh user jaringan kampus IT Telkom. Survey dilakukan dengan mengambil sampel. Jumlah ukuran sampel didapat dengan menggunakan rumus Slovin.

13. Hasil Pengujian

13.1 Memecah Log File

Fungsi dari memecah kesatuan log file adalah sebagai langkah awal agar log file dapat dibuka dan dimasukkan ke dalam Ms.Excel, yang kemudian nantinya akan dimasukkan ke Ms.Access. Kapasitas jumlah maksimal baris record yang dapat diinputkan ke Ms.Excel hanya sekitar ±1.000.000 untuk setiap kali input. Sedangkan jumlah log files yang didapat dari sisfo IT Telkom adalah sekitar 1,7 GB, yang mana terdapat sekitar ± 7.500.000 record baris log files dalam kurun waktu 4 hari. Oleh karena itu, log files tersebut harus dipecah menjadi 8 files .text, yang mana setiap file text nya terdiri dari 1.000.000 baris record. Pemecahan log files ini dilakukan di Ubuntu 10.11 dan dilakukan di terminal.

13.2 Input ke Ms.Excell

Sebelum dimasukkan ke Ms.Aceess, log file terlebih dahulu dimasukkan ke dalam Ms.Excel. Ini bertujuan untuk bertujuan untuk meratakan dan membuat baris dan kolom pada log file agar lebih mudah dimasukkan ke Ms.Access.

13.3 Transfer dari Ms.Excell ke Ms.Access

Proses transfer log files dari Ms.Excel ke Ms.Access bertujuan agar dapat menyaring dan mencari data-data yang dinginkan dari log file tersebut dengan mudah menggunakan query-query database yang ada di Ms.Access.

13.4 Filtrasi IP Source

Proses filterasi IP source bertujuan untuk mencari dan mengetahui jumlah IP aktif yang ada dari ± 7.500.000 baris record log file. Dari ± 7.500.000 baris record log file, terdapat banyak IP yang sama didalamnya. Maka dari itu, dilakukanlah penyaringan/filter untuk mendapatkan semua IP aktif selama 4 hari tersebut. Filterasi IP source dilakukan pada tool yang telah dibuat. Caranya dengan klik button "Total IP Keseluruhan" pada tool. Setelah klik button "Total IP Keseluruhan", proses penyaringan IP pada kolom IpSource sedang dilakukan.

Didalam button "Ip Aktif" tersebut terdapat query yang digunakan untuk mencari IP aktif. Query tesebut adalah :

```
SELECT distinct IpSource
FROM Table1;
```

Setelah klik button "Ip Aktif", dan menunggu, maka didapatlah IP aktif nya. Jumlah IP aktif yang didapat dari log file tersebut adalah **1274** IP aktif dari ± 7.500.000 baris log file yang ada. Gambar 4.6 dibawah ini adalah printscreen hasil running tool untuk filtering IP.

13.5 Searching Update Ms.Windows

Langkah ini bertujuan untuk mengetahui jumlah IP yang melakukan update Ms.Windows. Pencarian update Ms.Windows dilakukan pada tool yang telah dibuat. Caranya dengan klik button "MS.WINDOWS" pada kotak cek update yang ada pada tool. Setelah klik button tersebut, maka proses pencarian sedang dilakukan.

Didalam button "MS.WINDOWS" tersebut terdapat query yang digunakan untuk mencari update Ms.Windows. Query tesebut adalah :

```
SELECT distinct IpSource
FROM Table1
WHERE Url Destination LIKE
'*windowsupdate*';
```

Berdasarkan hasil dari pengujian yang dilakukan, maka didapatkan jumlah IP yang melakukan automatic update Ms.Windows. jumlah IP yang melakukan update Ms.Windows ada **137** IP dari 1274 IP aktif yang ada. Pada gambar 4.7 berikut adalah hasil printscreen hasil running tool untuk pencarian jumlah IP yang melakukan update Ms.Windows.

13.6 Searching Update Antivirus

a). Avira

Pencarian update antivirus avira dilakukan pada tool yang telah dibuat. Caranya dengan klik button "AVIRA" pada kotak cek update yang ada pada tool. Setelah klik button tersebut, proses pencarian sedang dilakukan.

Didalam button "AVIRA" tersebut terdapat query yang digunakan untuk mencari update avira. Query tesebut adalah :

```
SELECT distinct IpSource
FROM Table1
WHERE UrlDestination LIKE '*.vdf*';
```

Berdasarkan hasil dari pengujian yang dilakukan, maka didapatkan jumlah IP yang melakukan update avira. Jumlah IP yang melakukan update avira ada **51** IP dari 1274 IP aktif yang ada.

b). AVG

Pencarian update AVG antivirus dilakukan pada tool yang telah dibuat. Caranya dengan klik button "AVG" pada kotak cek update yang ada pada tool. Setelah klik button tersebut, proses pencarian sedang dilakukan.

Didalam button "AVG" tersebut terdapat query yang digunakan untuk mencari update AVG. Query tesebut adalah :

```
SELECT distinct IpSource
FROM Table1
WHERE UrlDestination LIKE '*.ctf*';
```

Berdasarkan hasil dari pengujian yang dilakukan, maka didapatkan jumlah IP yang melakukan update AVG. Jumlah IP yang melakukan update AVG ada **22** IP dari 1274 IP aktif yang ada.

c). Avast!

Pencarian update antivirus avira dilakukan pada tool yang telah dibuat. Caranya dengan klik button "AVAST" pada kotak cek update yang ada pada tool. Setelah klik button tersebut, proses pencarian sedang dilakukan.

Didalam button "AVAST" tersebut terdapat query yang digunakan untuk mencari update avast. Query tesebut adalah :

```
SELECT distinct IpSource
FROM Table1
WHERE UrlDestination LIKE '*.vpx*';
```

Berdasarkan hasil dari pengujian yang dilakukan, maka didapatkan jumlah IP yang melakukan update avast. Jumlah IP yang melakukan update avast ada **16** IP dari 1274 IP aktif yang ada.

13.7 Prosentase Hasil Update

a). Prosentase Update Ms.Windows

Berdasarkan hasil yang didapat dari pengujian update Ms.Windows, kita telah mengetahui jumlah IP yang melakukan update Ms.Windows. jumlah IP yang melakukan proses update Ms.Windows adalah 137 IP dari 1274 IP aktif yang ada. jika dihitung dalam prosentase dengan rumus 1 :

$$\frac{Jumlah\ IP\ Update\ Ms.Windows}{Jumlah\ IP\ Aktif}\ x\ 100\%$$

$$\frac{157}{1274}\ x\ 100\% = 10.75\ \%$$

Dari hasil perhitungan tersebut didapatkan 10.75 % dari jumlah IP yang aktif melakukan update Ms.Windows.

b). Prosentase Update Antivirus

Berdasarkan hasil yang didapat dari pengujian update Antivirus, kita telah mengetahui jumlah IP yang melakukan update Antivirus. jumlah IP yang melakukan proses update AntiVirus diantaranya adalah :

Avira	:	51 IP
AVG	:	22 IP
Avast!	:	16 IP
_____		+
Total	:	89 IP

Pemilihan jenis antivirus ini sangat tergantung oleh beberapa faktor, seperti : free atau tidaknya antivirus tersebut, kemampuan antivirus tersebut untuk melawan virus, dan fitur-fitur yang ditawarkan oleh antivirus tersebut.

Ada 89 IP yang update Antivirus dari 1274 IP aktif yang ada. jika dihitung dalam prosentase dengan rumus 2 :

$$\frac{Jumlah\ IP\ Update\ Antivirus}{Jumalh\ IP\ Aktif}\ x\ 100\ \%$$

$$\frac{89}{1274}\ x\ 100\ \% = 6.98\ \%$$

Dari hasil perhitungan tersebut didapatkan 6.98 % dari jumlah IP yang aktif melakukan update antivirus.

14. Analisis Hasil Pengujian

Hasil dari dua prosentase yang didapat terbilang kecil, atau dengan kata lain user yang melakukan update antivirus dan update Ms.Windows jumlahnya sedikit, dan user yang tidak melakukan update AntiVirus dan update Ms.Windows jumlahnya banyak. Jadi, dapat disimpulkan bahwa software antivirus dan operating system Ms.Windows yang digunakan oleh mayoritas user di jaringan kampus IT Telkom memiliki tingkat vulnerability yang tinggi. Melihat dari mayoritas user memiliki tingkat vulnerability software antivirus dan operating system Ms.Windows yang tinggi, maka dapat dikatakan bahwa perangkat komputer yang digunakan oleh mayoritas user tersebut memiliki tingkat keamanan yang rendah.

Berdasarkan National Institute of Standards and Technology (NIST), standard tingkat keamanan dapat ditinjau dari Security Category (SC)/kategori keamanan jenis informasi yang dimiliki oleh user (user dalam hal ini adalah para pengguna jaringan kampus IT Telkom). Pengguna jaringan kampus IT Telkom adalah mereka yang memiliki hak untuk mengakses VPN, salah satunya adalah mahasiswa yang notabene memiliki knowledge tentang dasar-dasar keamanan komputer dan experience dalam aktivitas berselancar di dunia maya. Berdasarkan kategori keamanan jenis informasi tersebut, user mahasiswa masuk ke dalam user dengan kategori jenis informasinya adalah public information. NIST juga menjelaskan bahwa public information merupakan tipe informasi dengan tingkat security objective(Confidentiality, Integrity, Availability) yang berada pada level moderate. Jika prosentase hasil pengujian adalah nilai range antara 0% sampai 100%, maka level moderate berada pada range nilai prosentase 33.33% sampai 66.66%. oleh karena itu, tingkat keamanan dapat dikatakan baik apabila nilai prosentase yang didapat adalah lebih dari 33.33%. **[15]**

Dari hasil perhitungan nilai prosentase yang kecil tersebut, maka akan muncul pertanyaan : "Mengapa jumlah user yang melakukan update sedikit?" atau "Mengapa prosentase yang dihasilkan memiliki nilai yang kecil?". Berdasarkan kuisioner yang dibuat dan disebarkan dilingkungan kampus IT Telkom pada tanggal 26 Mei 2012 kepada 155 responden pengguna jaringan kampus IT Telkom, didapatkan hasil sebagai berikut :

1. Pentingkah peranan antivirus dalam menjaga keamanan perangkat komputer anda?
   Yang menjawab :
   - Ya : 143 responden = 92.26 %
   - Tidak : 12 responden = 7.74 %

2. Apakah merk sotftware antivirus yang anda gunakan untuk mengamankan perangkat komputer anda?
   Yang menjawab :
   - Avast! : 24 responden = 15.48 %
   - Avira Antivir : 35 responden = 22.48 %
   - AVG : 31 responden = 20 %
   - BitDeff : 2 responden = 1.29 %
   - Eset Nod32 : 17 responden = 10.96 %
   - Kaspersky : 12 responden = 7.74 %
   - McAfee : 14 responden = 9.03 %
   - Norton : 13 responden = 8.38 %
   - Symantec : 2 responden = 1.29 %
   - VBA32 : 0 responden = 0 %
   - Lainnya : 9 responden = 5.80 %

3. Apakah anda tahu cara malakukan automatic updates pada software antivirus yang anda gunakan?
   Yang menjawab :
   - Ya : 141 responden = 90.96
   - Tidak : 14 responden = 9.04 %

4. Apakah anda mengaktifkan layanan/fitur automatic updates pada software antivirus yang anda gunakan?
   Yang menjawab :
   - Ya : 121 responden = 78.06 %
   - Tidak: 34 responden = 21.94 %

5. Pernahkah anda melakukan proses automatic update software antivirus menggunakan jaringan kampus IT Telkom?
   Yang menjawab :
   - Ya : 108 responden = 69.67 %
   - Tidak : 47 responden = 30.33 %

6. Pernahkah anda melakukan proses automatic update Microsoft Windows menggunakan jaringan kampus IT Telkom?
   Yang menjawab :
   - Ya : 40 responden = 25.80 %
   - Tidak : 115 responden = 74.2 %
   -

7. Apakah pernah ada kendala dalam hal teknis saat melakukan automatic update software antivirus dan Microsoft Windows di jaringan kampus IT Telkom? (Seperti : VPN putus, koneksi gagal, koneksi putus, update gagal, dll)
   Yang menjawab :

- Ya : 82 responden = 52.90 %
- Tidak : 73 responden = 47.1 %

Pengguna jaringan kampus IT Telkom adalah mereka yang memiliki hak untuk mengakses VPN, salah satunya adalah mahasiswa yang notabene memiliki *knowledge* tentang dasar-dasar keamanan komputer dan *experience* dalam aktivitas berselancar di dunia maya.

Berdasarkan hasil kuisioner terhadap 155 respoden diatas, dapat disimpulkan bahwa : Mahasiswa/i IT Telkom secara mayoritas mengakui pentingnya peranan antivirus dalam menjaga keamanan perangkat komputer mereka. Mereka juga mengerti cara melakukan dan mengaktifkan automatic update terhadap software antivirus yang mereka gunakan. Lebih dari 50% hasil dari kuisoner menyebutkan bahwa mahasiswa/i IT Telkom pernah melakukan update terhadap software antivirus yang mereka gunakan, walaupun secara mayoritas banyak pula yang mengalami kendala dalam melakukan update, seperti koneksi gagal, update gagal, ada kuota dalam melakukan download file, dll. Kendala-kendala ini yang mungkin menyebabkan para user jaringan kampus gagal dalam proses updating Ms.windows dan updating antivirus, sehingga menyebabkan rendahnya nilai prosentase yang didapat dari pengujian yang dilakukan sebelumnya.

15. Kesimpulan

1. Jumlah IP aktif yang didapat dari filterasi IP source sebanyak 1274 IP aktif dan total IP yang melakukan update Ms.Windows sebanyak 137 IP, serta total IP yang melakukan update antivirus sebanyak 89 IP.
2. Dari hasil perhitungan didapatkan 10.75 % jumlah IP yang aktif melakukan update Ms.Windows dan 6.98 % jumlah IP yang aktif melakukan update antivirus.
3. Software antivirus dan operating system Ms.Windows yang digunakan oleh mayoritas user memiliki tingkat vulnerability yang tinggi. Setelah mengetahui mayoritas user memiliki tingkat vulnerability software antivirus dan operating system Ms.Windows yang tinggi, maka dapat dikatakan bahwa perangkat komputer yang digunakan oleh mayoritas user tersebut memiliki tingkat keamanan yang rendah.
4. Kendala-kendala teknis pada jaringan yang dialami user saat melakukan update dapat meningkatkan tingkat vulnerability software antivirus dan operating system Ms. Windows yang berakibat pada menurunnya keamanan perangkat user yang terhubung ke jaringan.

Daftar Pustaka

1. Kurniawan, Wiharsono. Januari 2007.Computer Starter Guide :Jaringan Komputer. Yogyakarta: PenerbitAndi.
2. http://tekno.kompas.com/read/2011/11/05/10174079/Harga.Antivirus.Original.Semakin.Murah
3. Tec-Ed, inc. Assessing Web Site Usability from Server Log Files, Michigan.
4. Setiawan, Deris. 2003. Mengenal Infrastruktur Jaringan Komputer..November 15, 2003.
5. http://www.scribd.com/abang_kiky/d/92362445-Jurnal-Keamanan-Komputer-Dan-Jaringan
6. http://ahmad-prayitno.com/2009/12/pengertian-vulnerability/
7. http://publikasi.kominfo.go.id/bitstream/handle/54323613/119/Panduan%20Penerapan%20Tata%20Kelola%20KIPPP.pdf?sequence=1
8. http://wartawarga.gunadarma.ac.id/2012/01/pengertian-antivirus-dan-macam-%E2%80%93-macam-antivirus/
9. http://www.pdii.lipi.go.id/wp-content/uploads/2011/08/Prasetya-TP.-2010.-Pengelolaan-Sarana-Jaringan-Komputer-TI.pdf
10. http://jurnal.pdii.lipi.go.id/admin/jurnal/51085258.pdf
11. http://windows.microsoft.com/en-ID/windows/explore/get-to-know
12. http://www.tukiran.com/2012/05/cara-membuat-kuesioner-penelitian.html
13. Supranto, J. 1998. Teknik Sampling untuk Survei dan Eksperimen. Jakarta: Rineka Cipta.
14. http://opensource.telkomspeedy.com/wiki/index.php/IP
15. Standards for Security Categorization of Federal Information and Information Systems, National Institute of Standards and Technology Gaithersburg, MD 20899-8900February 2004 U.S.