Analisis Simple Network Management Protocol (SNMP) Menggunakan Wireshark dan Visualisasi Traffic Data Menggunakan Orange

Ridho Ilham Renaldo
09011181520021@students.ilkom.unsri.ac.id
Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Abstrak

Jaringan merupakan suatu kebutuhan penting sekarang ini. Semakin besar jaringan maka sangatlah penting untuk menjaga keamanannya. Monitoring merupakan salah satu cara untuk menjaga keamanan jaringan. Dalam jaringan modern sekarang yang menggunakan TCP/IP dikenal sebuah protocol yang dapat melakukan manajemen jaringan yang dikenal dengan *Simple Network Management Protocol* (SNMP) dengan memanfaatkan software bernama Wireshark yang dapat membaca hampir semua paket yang ada dan menyeleksi data tersebut sedetail mungkin. Visualisasi Traffic Data yang dihasilkan oleh Wireshark dapat memanfaatkan *open source learning machine* yang bernama Orange. Sehingga data yang ada dapat dimengerti dengan mudah.

Kata Kunci: *Network Management System, Simple Network Management Protocol, Traffic Data, Wireshark, Orange*

I. PENDAHULUAN

Jaringan Internet (*Internet Network*) sangatlah penting pada jaman sekarang untuk mempermudah kegiatan sehari-hari. Dalam jaringan internet kita dapat berinteraksi kapan saja, dimana saja dan dengan siapa saja. Semakin besar jaringan semakin banyak juga data dan informasi yang terdapat didalamnya.

Jaringan yang besar tentunya harus memiliki *security* yang baik untuk menjaga seluruh data yang ada dalam jaringan agar tidak terjadi pencurian dari luar. Pengamatan (*monitoring*) adalah salah satu tindakan waspada yang sangat ampuh untuk memperhatikan segala proses yang berjalan pada server sebagai tonggak dari suatu jaringan

Monitoring jaringan adalah salah satu kegiatan dari *system administrator* agar dapat mengetahui kinerja dari peralatan jaringan yang dimiliki. Setiap perangkat memiliki spesifikasi yang khusus dan membutuhkan penanganan tersendiri, untuk itulah dibutuhkan sebuah perangkat lunak yang mampu melakukan pengumpulan data sehingga *system administrator* bisa melakukan analisa dari data yang terkumpul tersebut.

Dalam jaringan modern sekarang yang menggunakan protokol TCP/IP, dikenal sebuah protokol yang dapat melakukan monitoring dan manajemen jaringan (*Network Management System*) yaitu SNMP (*Simple Network Management Protocol*). Protokol ini berfungsi untuk melakukan manajemen dan monitoring dari peralatan jaringan, mulai dari server, router, switch dan peralatan server lain. SNMP sendiri dapat dilakukan dengan berbagai macam *tools* salah satunya adalah Wireshark. Wireshark sangatlah popular karena memiliki tampilan GUI yang *user friendly* dan dapat membaca

hampir semua paket yang lewat serta menyeleksi dan menampilkan data tersebut sedetail mungkin [3].

II. TINJAUAN PUSTAKA

a. *Simple Network Management Protocol* (SNMP)

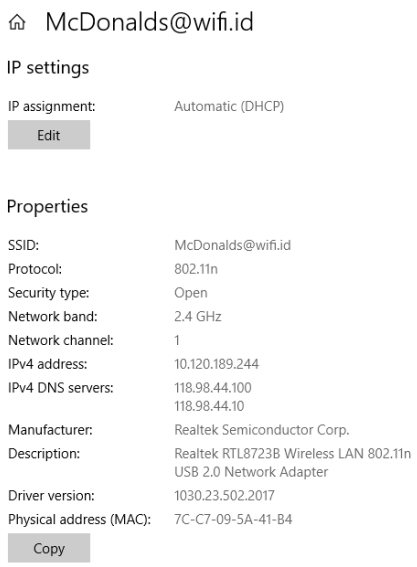
Secara sederhana, SNMP merupakan sebuah protokol yang didesain untuk memberikan kemampuan kepada pemakai untuk mengelola jaringan komputernya dari jarah jauh atau remote. Pengelolaan ini dilaksanakan dengan cara melakukan polling dan setting variabel-variabel elemen jaringan yang dikelolanya. [1]

b. *Network Management System* (NMS)

Network Management System merupakan software yang dapat memantau keadaan di dalam jaringan. Software NMS mempunyai sejumlah besar fitur yang sangat menarik. NMS dapat dimanfaatkan oleh ISP untuk meningkatkan dan menjaga kualitas layanan yang diberikan kepada pelanggannya [4].

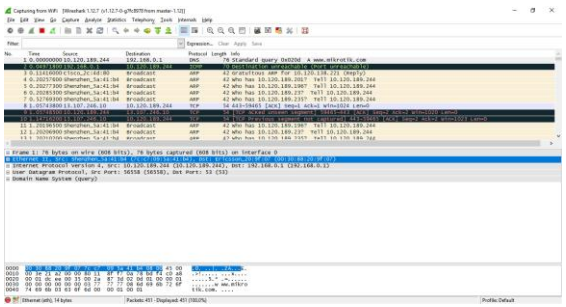
III. PERCOBAAN

Percobaan yang dilakukan pada analisis SNMP ini merupakan jaringan public yang terdapat pada Mc Donald Jalan R. Sukamto Palembang yang merupakan salah satu restoran *fast food* paling ramai yang ada di kota Palembang. Pada percobaan ini pertama-tama dilakukan dengan menghubungkan koneksi terhadap jaringan internet milik Mc Donald yang dapat dilihat perinciannya pada gambar 3.1 dibawah ini:



Gambar 3.1

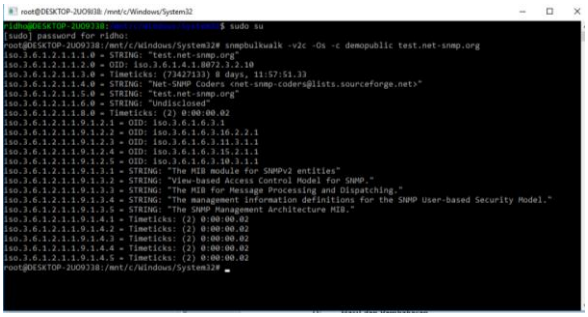
Setelah mendapatkan data-data diatas lalu buka software Wireshark, pada halaman utama terbuka pilih **Interface List** lalu centang **WIFI** setelah itu pilih **Start**. Maka tampilan yang ada akan terlihat seperti gambar 3.2.



Gambar 3.2

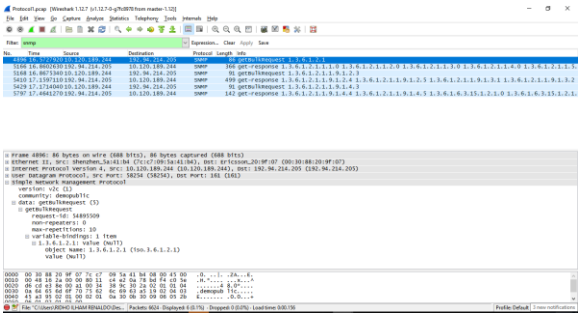
Setelah itu pastikan computer anda telah terinstall Ubuntu. Ubuntu merupakan system operasi berbasis linux yang tersedia secara bebas, fungsinya pada percobaaan kali ini adalah menjalankan perintah Bash pada command prompt. Bash ini berfungsi untuk menjalankan perintah **sudo su** yang fungsinya adalah untuk melakukan root sebagai superuser sehingga dapat menguasai

system yang sedang dipakai. Tampilan yang dihasilkan ketika menjalankan fungsi root tersebut dapat dilihat pada gambar 3.3.



Gambar 3.3

Setelah langkah-langkah diatas dilakukan, kita akan tiba pada langkah terakhir yaitu kembali pada Wireshark dan ketikan **snmp** pada kolom Filter yang fungsinya adalah mefilter protocol yang ada sehingga yang ditampilkan hanyalah protocol yang SNMP saja, seperti pada gambar 3.4 dibawah ini.

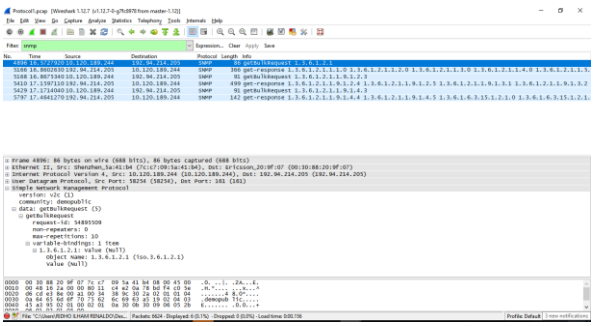


Gambar 3.4

Sekarang kita telah mendapatkan protocol SNMP yang kita butuhkan untuk analisis yang akan dilakukan.

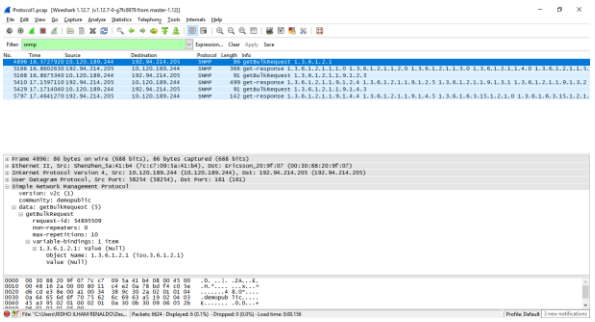
IV. HASIL DAN PEMBAHASAN

Setelah langkah-langkah pada bab Percobaan dilakukan maka kita akan mendapatkan tampilan seperti pada gambar 4.1



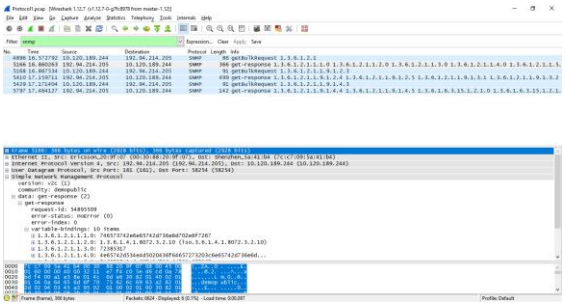
Gambar 4.1

Gambar 4.1 menjelaskan beberapa Protocol SNMP yang sedang melakukan traffic data, manakah yang sedang melakukan request dan melakukan response.



Gambar 4.2

Pada gambar 4.2 menunjukkan tentang IP melakukan request dengan penjelasan GetBulkRequest yang berguna untuk *retrieve data* dari suatu table dalam SNMP dalam jumlah besar yang tidak bisa dilakukan oleh GetNextRequest. IP Source 10.120.189.244 dan IP Destination 192.94.214.205 melakukan traffic data dengan panjang data (length) 86 bytes dan waktu 16.5727920 seconds dengan request-id 54895509 terdapat 1 variable binding yaitu 1.3.6.1.2.1: Value (Null) dan Object Name 1.3.6.1.2.1 (iso.3.6.1.2.1).



Gambar 4.3

Jika pada gambar 4.2 menunjukkan request protocol, maka gambar 4.3 menunjukkan response protocol dimana IP Source 192.94.214.205 dan IP Destination adalah 10.120.189.244 dimana request-id adalah 54895509 dan variable bindings tterdapat 10 items, namun sebagai contoh satu saja yaitu 1.3.6.1.2.1.1.1.0 dengan penjelasan angka 1 adalah ISO, 3 merupakan identification ISO, 6 US dod, 1 merupakan angka internet, 2 merupakan management, 1 merupakan MIB, kemudian 1 lagi merupakan protocol SNMP dan 0 merupakan datagram dari SNMP, dari variable-variable tersebut terbentuklah satu kesatuan variable saat IP meminta request.

Dengan informasi yang ditampilkan oleh Wireshark tersebut maka visualisasi traffic yang ada dapat dilihat dengan menggunakan software yang disebut *Orange*. Hasil dari data visualization tersebut dapat dilihat pada gambar 4.4.

Gambar 4.4

Gambar 4.4 menampilkan Scatterplot Diagram dari Orange dimana data tersebut berasal dari software Wireshark yang kita gunakan pada percobaan ini. Dari gambar tersebut dapat dilihat 6 label yang merupakan IP Source yang terletak berdasarkan Length dan Time masing-masing label. Warna yang dibedakan tersebut berdasarkan dengan IP Destination, dimana biru menunjukkan IP Source yang IP Destination-nya adalah 192.94.214.205 dan merah menunjukkan IP Source yang memiliki IP Destination 10.120.189.244.

V. KESIMPULAN

Kesimpulan yang didapatkan pada percobaan ini berdasarkan data yang tersedia adalah semua data yang merupakan request tidak lebih dari 100 bytes dengan keterangan GetBulkRequest yang berarti *retrieve data* dari SNMP dalam jumlah besar dimana semua IP Source nya adalah 10.120.189.244 dan IP Destination nya adalah 192.94.214.205, sedangkan data response memiliki Length lebih dari 100 bytes dan semua IP Source nya adalah 192.94.214.205 dan IP Destination nya adalah 10.120.189.244.

DAFTAR PUSTAKA

[1] Indarto, W., Wijaya, S., & Zukhri, Z. (2005). Simple Network Management Protocol Untuk Pemantauan Jaringan Dengan Pelaporan SMS.

[2] Moko, P.H., dkk. 2011. Studi Kasus Pemanfaatan Software Network Management System Oleh ISP di Jakarta

[3] Muchlis, *Meretas DC*, Pengertian dan Fungsi Wireshark, Sisi Hacker vs Administrator Jaringan, 2015,

http://www.meretas.com/wireshark-adalah/
[diakses 19 Oktober 2018].

[4] Wikipedia, Ubuntu, 25 September 2018, https://id.wikipedia.org/wiki/Ubuntu
[diakses 19 Oktober 2018].