ANALISA SIMPLE MANAGEMENT NETWORK PROTOCOL

****

THERIO ANGGARA

09011281520112

SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2018

**Simple Network Management Protocol (SNMP)**

SNMP) merupakan protokol standard industri yang digunakan untuk memonitor dan mengelola berbagai perangkat di jaringan Internet meliputi hub, router, switch, workstation dan sistem manajemen jaringan secara jarak jauh (remote). Baru-baru ini (pertengahan Februari 2002) Oulu University Secure Programming Group, sebuah group riset keamanan jaringan di Finlandia, telah menemukan adanya kelemahan pada SNMP v1.

Kelemahan tersebut memungkinkan seorang cracker memasang back door pada peralatan yang menggunakan SNMP v1 sehingga bisa menyusup ke jaringan dan melakukan apa saja terhadap jaringan. Kelemahan ditemukan pada SNMP trap and request facilities yang memungkinkan penyusup memperoleh akses ke dalam sistem yang menjalankan SNMP dan melakukan serangan Denial of Service (DoS) yang membuat sistem tidak berfungsi (down) atau tidak stabil.

SNMP v1 telah dipakai sejak awal tahun 1980-an. Terdapat berbagai usaha untuk memperbaiki standard SNMP yaitu dengan munculnya SNMP v2 dan SNMP v3 pada tahun 1998. Namun usaha ini tidak begitu berhasil. Sebagian besar jaringan saat ini masih menggunakan SNMP v1.

Masalah ini cukup merepotkan karena tidak hanya menyangkut satu jenis peralatan dari satu vendor melainkan menyangkut perangkat dari berbagai banyak vendor sehingga diperlukan patch/update dari berbagai vendor yang peralatannya menggunakan SNMP v1.

Untuk mengatasi kelemahan pada SNMP ini CERT Coordination Center, suatu pusat pengembangan dan riset keamanan Internet, merekomendasikan untuk sementara menutup jalan masuk (ingress filtering) trafik SNMP pada port 161/udp dan 162/udp. Jika hal ini tidak mungkin dilakukan, CERT menyarankan untuk membatasi trafik SNMP hanya pada Virtual Private Network (VPN) atau mengisolasi sistem manajemen jaringan dari jaringan publik. Penutupan port dilakukan sementara sambil menunggu dikeluarkannya pacth/update dari pihak vendor yang membuat perangkat yang menggunakan SNMP v1 tersebut.

**SNMP Versi 1**

SNMP versi 1 adalah standar protokol SNMP yang pertama kali dibuat, SNMP dibuat untuk digunakan sebagai alat manajemen jaringan untuk jaringan dan mengoperasikan internetworking TCP/IP. (Stallings, 2007,p761). SNMP sebenarnya digunakan untuk merujuk kepada kumpulan spesifikasi manajemen jaringan yang mencakup protocol itu sendiri, definisi database, dan konsep-konsep yang terkait. Model manajemen jaringan yang digunakan untuk SNMP mencakup elemen-elemen utama sebagai berikut:

1. Management station atau Manager
2. Agent
3. Management Information Base
4. Network Management Protocol

**SNMP Versi 2**

SNMPv2 menyediakan framework dimana dapat dibangun aplikasi manajemen jaringan dan menyediakan infrastruktur untuk manajemen jaringan. (Stallings, 2007, p765). Fungsi-fungsi pada SNMP v1 masih sama dengan yang digunakan pada SNMP v2, namun ada fungsi-fungsi yang dikembangkan, seperti pada fungsi trap. SNMP v2 juga memperkenalkan 2 protokol baru yaitu GetBulk dan inform. GetBulk digunakan oleh NMS untuk mendapatkan data yang berukuran besar dengan efisien. Operasi Inform memungkinkan NMS untuk saling mengirimkan informasi trap. Dari segi keamanan SNMP v2 juga dikembangkan sehingga lebih aman dibanding SNMP v1.

**SNMP Versi 3**

SNMPv3 menyediakan 3 layanan penting yaitu authentication, privacy, dan access control, Authentication dan privacy adalah bagian dari User-Based Security Model (USM) dan access control didefinisikan dalam View-Based Access Control Model (VACM). (Stallings, 2007, p769).

**Management Information Base (MIB)**

Management information base (MIB) adalah koleksi dari objek-objek atau variable data-data yang merupakan salah satu aspek dari managed agent. (Stallings, 2007, p762). Setiap perangkat memiliki unique object identifier (OID) yang terdiri dari angka – angka yang dipisahkan oleh titik. OID secara alami akam membentuk tree. MIB menghubungkan setiap OID dengan label dan parameter lain yang berhubungan dengan objek yang bersangkutan. MIB kemudian bertindak sebagai kamus atau buku kode ang digunakan untuk menghubungkan dan menerjemahkan SNMP.

**Komponen utama dalam proses manajemen jaringan TCP/IP terdiri dari tiga elemen, yaitu:**

1. **MIB (Management Information Database)**

MIB Adalah struktur basis data variabel dari elemen jaringan yang dikelola. Pada kelompok interface terdapat variabel objek MIB yang mendefinisikan karakteristik interface diantaranya : *ifInOctets* mendefinisikan jumlah total byte yang diterima, *ifOutOctets* mendefinisikan jumlah total byte yang dikirim, *ifInErrors* mendefinisikanjumlah paket diterima yang dibuang karena rusak, *ifOutErrors* mendefinisikan jumlah paket dikirim yang dibuang karena usak, dan variable objek lainnya yang juga berkaitan dengan paket internet.

1. **Agen**

Merupakan software yang dijalankan di setiap elemen jaringan yang dimonitor.

Agen bertugas mengumpulkan seluruh informasi yang telah ditentukan dalam MIB.

1. **Manajer**

Merupakan software yang berjalan di sebuah host di jaringan. Bertugas meminta informasi ke SNMP Agen. Manajer biasanya tidak meminta semua informasi yang dimiliki oleh agen, tetapi hanya meminta informasi tertentu saja yang akan digunakan untuk mengamati unjuk kerja jaringan. Manager biasanya menggunakan komputer yang memiliki tampilan grafis dan berwarna sehingga selain dapat menjalankan fungsinya sebagai Manager, juga untuk melihat grafik unjuk kerja dari suatu elemen jaringan yang dihasilkan oleh proses monitoring.

**SNMP terdiri dari dua jenis yakni:**

* Network Management Station, yang berfungsi sebagai pusat penyimpanan untuk pengumpulan dan analisa dari data manajemen jaringan.
* Peralatan yang dimanage menjalakan SNMP agent, yaitu proses background yang memonitor peralatan tersebut dan mengkomunikasikannya ke network management station.

**PDU SNMPv1**

* *GetRequest*

Adalah jenis PDU yang dikirimkan dari manager kepada agent. PDU ini bertujuan untuk me-request data pada agent.

* *GetNextRequest*

Adalah jenis PDU yang dikirimkan dari manager kepada agent. Operasi ini hampir

sama dengan operasi GetRequest, hanya saja, GetNextRequest ini meminta data

setelahnya dari OID yang dispesifikasikan dalam paket GetNextRequest.

* *SetRequest*

Adalah jenis PDU yang dikirimkan dari manager kepada agent. PDU ini bertujuan untuk mengubah data pada agent.

* *GetResponse*

Adalah jenis PDU yang dikirimkan dari agent kepada manager. PDU ini bertujuan untuk me-reply data kepada manager sebagai response atas data yang diminta oleh manager melalui operasi GetRequest, GetNextRequest, dan SetRequest.

* *Trap*

Adalah jenis PDU yang dikirimkan dari agent kepada manager. SNMP trap ini adalah sebuah pesan yang diprakarsai oleh suatu elemen dalam jaringan (agent) dan dikirimkan kepada manager untuk memberitahu atau memberikan informasi kepada manager bahwa terjadi suatu event tertentu pada objek yang di-manage (managed device).

**Struktur MIB ()**

* Setiap object mempunyai ID unik (OID).
* MIB mengasosiasikan setiap OID menggunakan label dan parameter lain.
* MIB bertindak sebagai kamus data yang digunakan untuk menyusun terjemahan pesan SNMP.

**Object Identifier (OID)**

* Object Identifier (OID) merupakan sebuah pengenal yang digunakan untuk menamakan sebuah objek yang terdapat dalam MIB.
* OID bersifat unik untuk masing-masing objek.
* Secara struktural, sebuah OID terdiri dari sebuah node dalam namespace yang

ditetapkan secara hirarki, yang didefinisikan secara formal menggunakan standar ASN.1.

OID dapat didefinisikan dalam dua format, yaitu :

1. Textual OID

Pendefinisian OID berdasarkan nama tiap node mulai dari root, dengan dipisahkan oleh titik (.) .

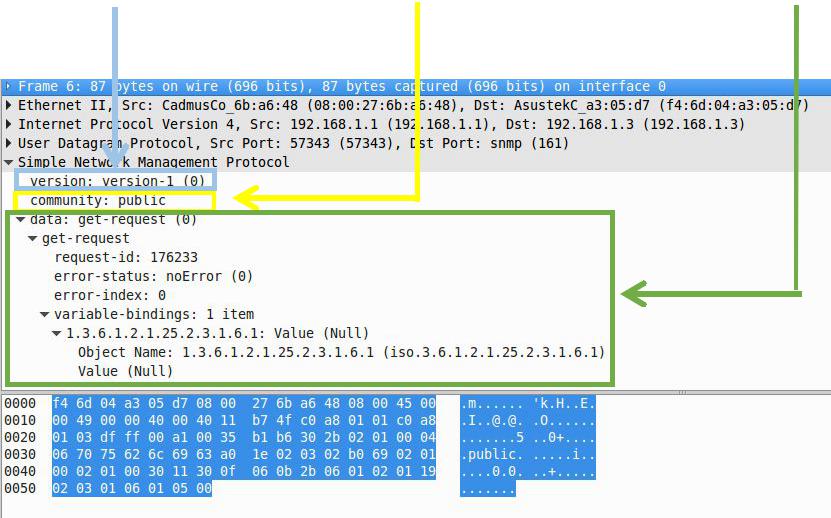
Contoh : .iso.org.dod.internet.mgmt.mib.system.sysDescr

1. Numerical OID

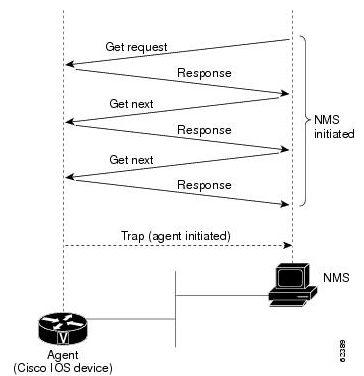
Pendefinisian OID berdasarkan angka integer sebagai pengganti nama, juga dipisahkan dengan titik (.) .

Contoh : .1.3.6.1.2.1.1.1

**Pesan SNMPv1**

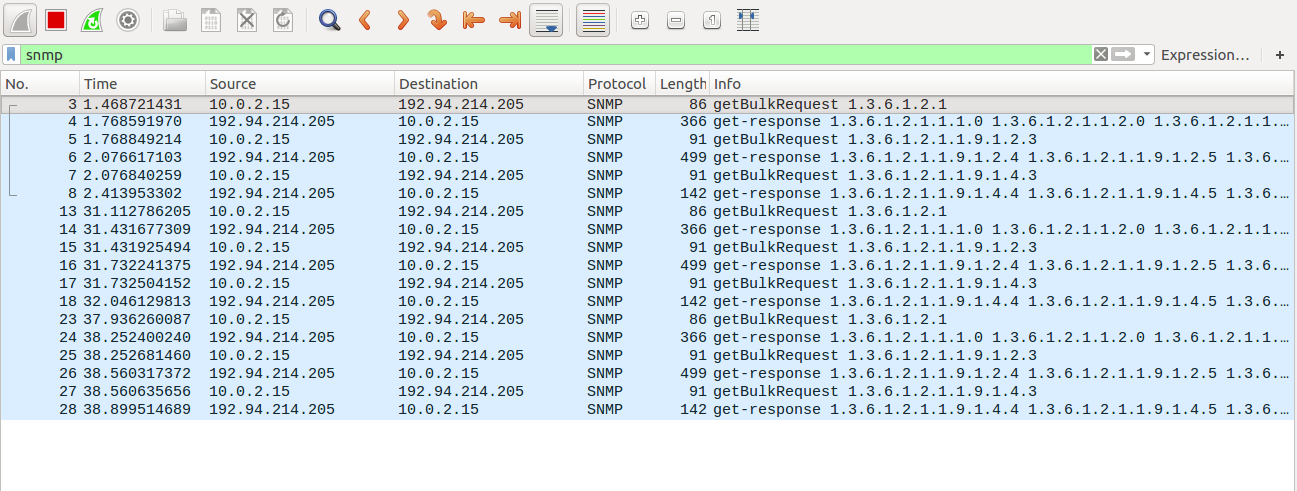
****

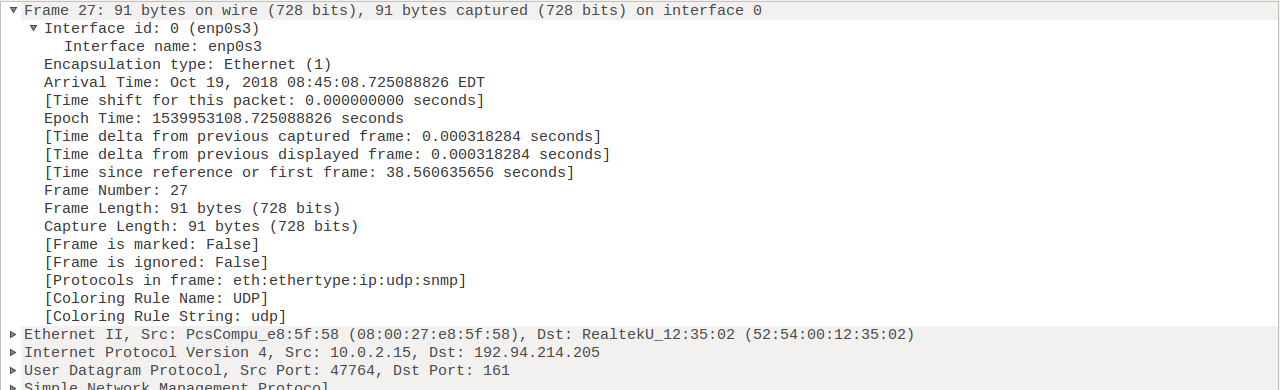
**SNMP Event Interaction and Timing**

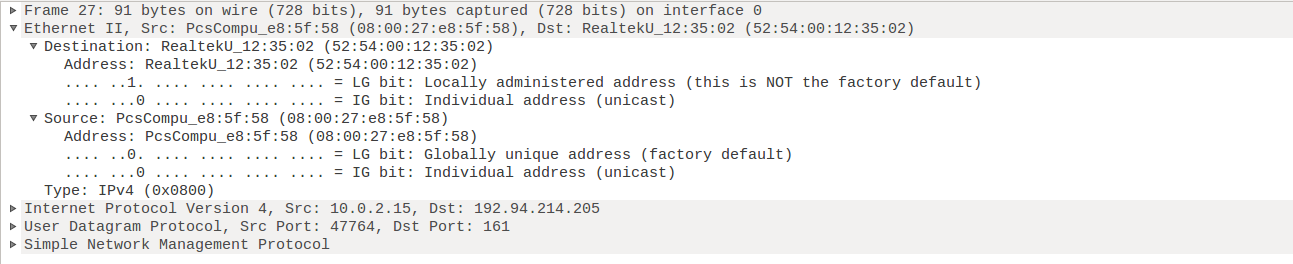
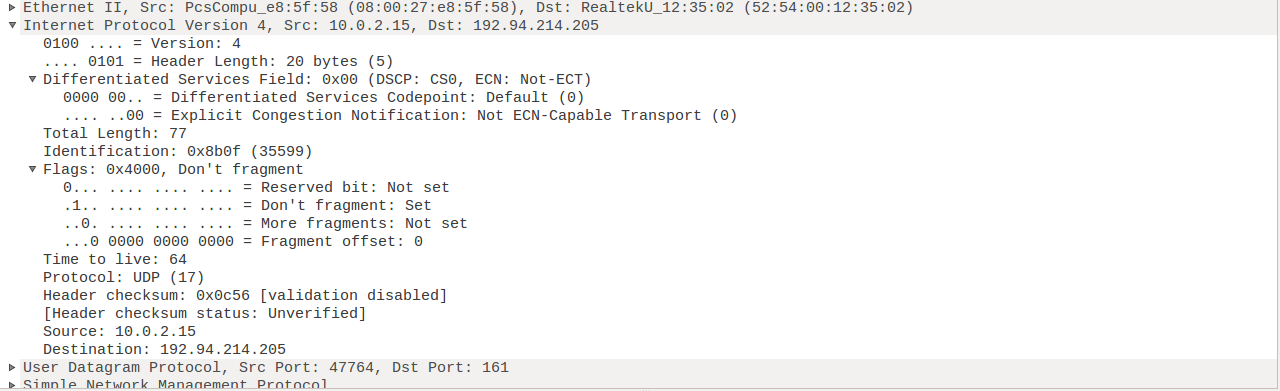
****

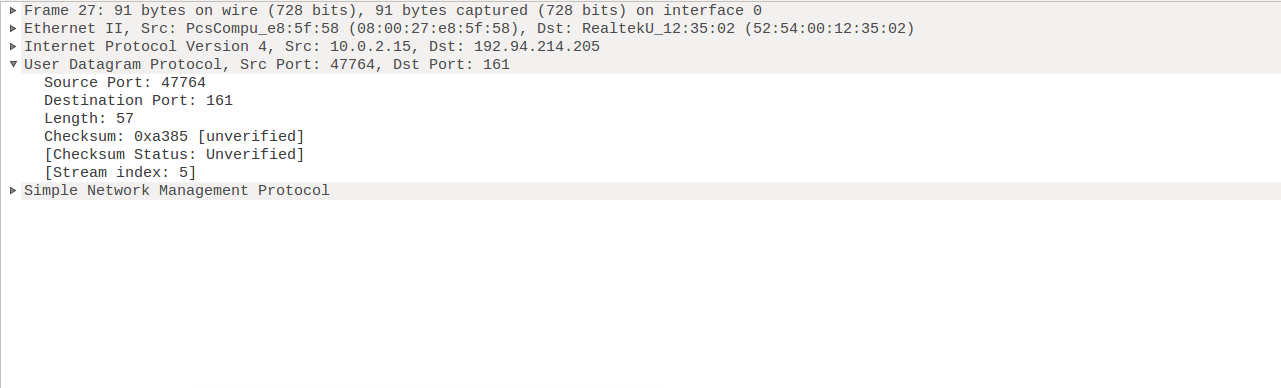
**Analisa Packet Capture Pada Wireshark**

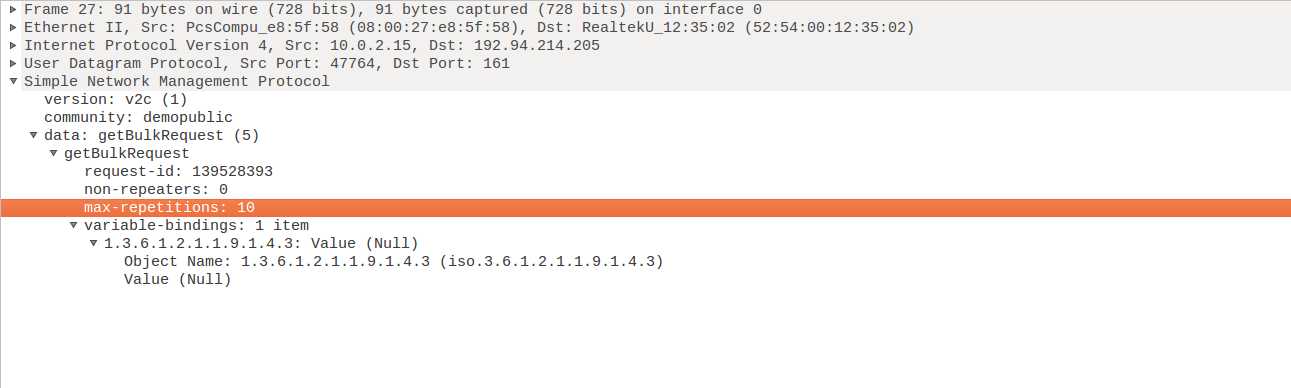
Hasil capture packet dengan “Wiresharks”



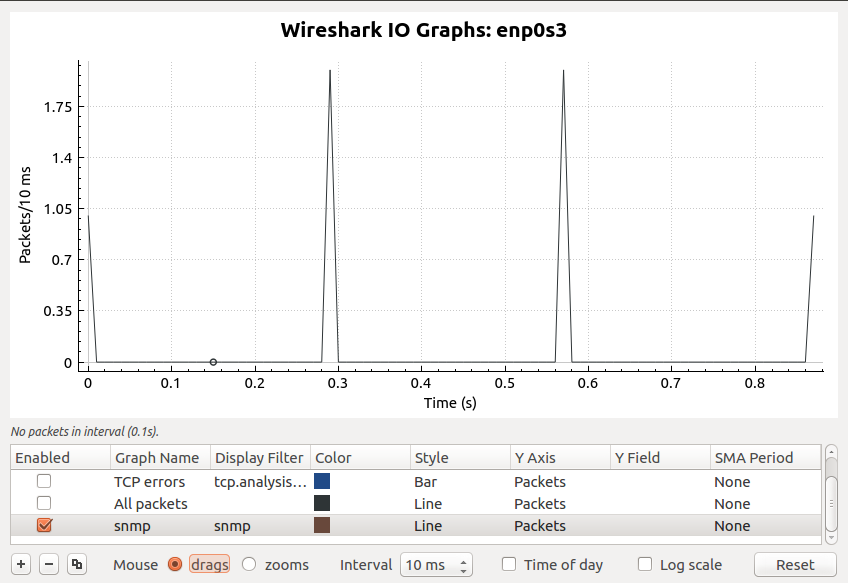








Trafic Percobaan



Visualisasi Pada Rumint

