**Analisis SNMP Menggunakan Wireshark and Monitoring menggunakan orange**

ADRIAN AJISMAN (09011281520133)

Sistem Komputer 2015

Simple Network Management Protocol (SNMP)

merupakan [protokol](https://id.wikipedia.org/wiki/Protokol_Internet%22%20%5Co%20%22Protokol%20Internet) standard industri yang digunakan untuk memonitor dan mengelola berbagai perangkat di jaringan [Internet](https://id.wikipedia.org/wiki/Internet) meliputi [hub](https://id.wikipedia.org/wiki/Hub), [router](https://id.wikipedia.org/wiki/Router), [switch](https://id.wikipedia.org/w/index.php?title=Switch&action=edit&redlink=1), [workstation](https://id.wikipedia.org/wiki/Workstation) dan sistem manajemen jaringan secara jarak jauh (remote). Baru-baru ini (pertengahan Februari 2002) [Oulu University Secure Programming Group](https://id.wikipedia.org/w/index.php?title=Oulu_University_Secure_Programming_Group&action=edit&redlink=1), sebuah group riset keamanan jaringan di [Finlandia](https://id.wikipedia.org/wiki/Finlandia), telah menemukan adanya kelemahan pada SNMP v1.

Kelemahan tersebut memungkinkan seorang [cracker](https://id.wikipedia.org/w/index.php?title=Cracker&action=edit&redlink=1) memasang [back door](https://id.wikipedia.org/w/index.php?title=Back_door&action=edit&redlink=1) 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](https://id.wikipedia.org/wiki/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](https://id.wikipedia.org/w/index.php?title=Vendor&action=edit&redlink=1) sehingga diperlukan patch/update dari berbagai vendor yang peralatannya menggunakan SNMP v1.

Untuk mengatasi kelemahan pada SNMP ini [CERT Coordination Center](https://id.wikipedia.org/w/index.php?title=CERT_Coordination_Center&action=edit&redlink=1), 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](https://id.wikipedia.org/wiki/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.

Simple Network Management Protocol (SNMP) merupakan suatu protokol berbasis internet yang digunakan untuk memonitor perangkat pada jaringan. Berbagai perangkat yang dapat dimonitor oleh SNMP di antaranya router, switch, server, client, printer dan sebagainya.

Dalam SNMP, perangkat jaringan dibagi menjadi dua, agent dan manager. Agent adalah perangkat yang dimonitor dan manager adalah perangkat yang memoniotrnya. Adapun protokol ini menggunakan UDP.

Komponen SNMP terdiri atas Structure of Management Information (SMI) dan Management Information Base (MIB). SMI berperan dalam penamaan object, menentukan tipe object dan menunjukkan bagaimana meng-encode object untuk dikirim. Sedangkan MIB berfungsi memberikan informasi mengenai perangkat yang dimonitor.

Untuk mengetahui informasi suatu perangkat, SNMP bekerja dengan dua pendekatan :

1. Polling, disebut juga dengan pendekatan aktif. SNMP akan mengirimkan pesan kepada agent misalkan apakah suatu agent mengalami masalah. Polling dikirimkan kepada agent melalui port 161.

2. Notifikasi, disebut juga dengan pendekatan pasif. Pada pendekatan ini, trap (laporan event yang tidak diminita yang dikirim oleh agent) akan dikirimkan kepada manager, misal ada gangguan pada perangkat. Notifikasi ini dikirimkan kepada manager melalui port 162.

 Berikut adalah hasil pengcapturean snmp pada wifi @UNSRI di wilayah perpustakaan Unsri.



Screenshot dari apps orange

1. 
2. 

References :

[1] R. S. Saputra, Perancangan Dan Implementasi Aplikasi Sistem Monitoring Jaringan Berbasis Web ( Studi Kasus Telkom University), Bandung, 2016.

[2] <https://searchnetworking.techtarget.com/definition/SNMP>

[3] Esad Saitovic and Ivan Ivanovic , Network Monitoring and Management, Produced by AMRES led working group on network monitoring , February 2011.