PENERAPAN *NETWORK MANAGEMENT SYSTEM* DENGAN WIRESHARK PADA *PERFORMANCE MANAGEMENT* DATA BADAN SAR NASIONAL

Anton[1], Ibnu Arif[2]
[1]Manajemen Informatika, AMIK BSI Tangerang,
BSD Sektor XIV Blok C1/1, Jl. Letnan Sutopo BSD Serpong-Tangerang Selatan, anton@bsi.ac.id

[2]Teknik Informatika, STMIK Nusa Mandiri
Jl. Damai No.8, Warung Jati Barat (Margasatwa), Pasar Minggu
ibnu.arif12@yahoo.co.id

ABSTRACT:

Network Management System (NMS) is a function to supervise the performance of the network and taking action to control, monitor traffic flow so that the operating capacity on a network can be done optimally. Network Management System is a service that uses tools, applications and devices to help users (user) to monitor, regulate, observe and plan network resources as well as system components in a network. NMS Model includes five conceptual areas, namely Fault Management, Configuration Management, Accounting Management, Performance Management and Security Management (FCAPS). Performance Management is an activity undertaken to assess performance indicators of network operations on an ongoing basis. With the Performance Management expected service levels can be maintained (optimize QoS (Quality of Service)), network conditions can be identified, the possibility of interference can be unpredictable and can make a complete report on the activities of decision-making and planning. Wireshark is a tool Network Analyzer is used for analyze network performance and capture data / information that passes through a network with a graphical display. From the modification and testing the network on the National SAR Agency monitored utilizing wireshark allow the network disruptions can be predicted and the level of service to the user can be maintained.

Keywords: Network management System (NMS), Performance Management, wireshark

PENDAHULUAN

Latar belakang

Perkembangan teknologi informasi saat ini begitu cepat dan memberikan kemudahan bagi manusia dalam mengatasi permasalahan yang dihadapi. Begitu juga dengan penggunaan Internet yang sangat pesat, hal ini membutuhkan pelayanan Quality of service (QoS) yang mumpuni. Keterhubungan setiap user didalam jaringan perlu dijaga performa kenektivitasnya sehingga dapat meningkatkan produktivitas maupun keberlangsungan transaksi yang dilakukan. Untuk meningkatkan kualitas jaringan yang ada, perlu dilakukan pengawasan terhadap kinerja jaringan dan tindakan untuk mengendalikan aliran trafik agar kapasitas pengoperasian pada sebuah jaringan dapat dilakukan secara maksimal.

Permasalahan yang sering timbul pada implementasi manajemen jaringan adalah terkait dengan multivendor, yaitu:

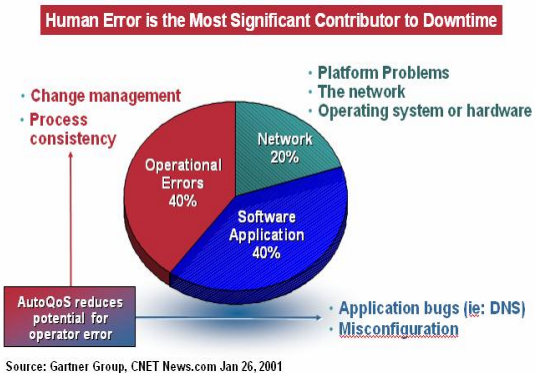
1. Perangkat keras yang digunakan (berbagai macam teknologi dan layanan yang digunakan baik itu voice, video, pesan, maupun data.
2. Perangkat lunak yang digunakan, antara lain sistem operasi, protokol maupun aplikasi digunakan. Masalah yang sering dihadapi dalam protokol jaringan internet yaitu terjadi kerusakan data yang di sebabkan oleh banyak hal yang menyebabkan terjadi permasalahan pada protokol jaringan sehingga kualitas layanan tidak berjalan normal dan terkadang terjadi kerusakan data, padahal setiap kerusakan paket bisa terdeteksi dari nilai error yang dibandingkan dengan data aslinya.

Wireshark adalah software yang digunakan untuk menganalisa paket data pada jaringan yang disebut juga dengan network packet analyzer dengan fungsi menangkap setiap paket yang lalulalang didalam jaringan dan juga digunakan untuk menampilkan semua informasi paket data secara detail. Semua jenis paket informasi dalam berbagai format protokol akan dengan mudah ditangkap dan dianalisa. Dengan adanya wireshark proses pengawasan didalam jaringan sangat dimudahkan, filterisasi paket dapat sesuai dengan yang diinginkan, kemungkinan gangguan dapat diprediksi dan kondisi jaringan dapat di kenali sehingga tingkat pelayanan dapat dipertahankan.

Konteks penelitian

Network management system (NMS) adalah upaya untuk mengkoordinasikan dan mendistribusikan sumber daya atau *resource* untuk merencanakan, menganalisa, mengevaluasi, mendesain, mengadministrasikan dan mengembangkan jaringan, sehingga memperoleh kualitas pelayanan yang baik pada seluruh waktu dengan biaya yang sesuai dan kapasitas yang optimal. Manajemen jaringan adalah kemampuan menerapkan suatu metode untuk memonitor suatu jaringan, mengontrol suatu jaringan dan merencanakan sumber serta komponen sistem dalam sebuah jaringan komputer. Model NMS mencakup 5 area konseptual yaitu Fault Management, Configuration Management, Accounting Management, Performance Management dan Security Management (FCAPS).

Model NMS adalah upaya untuk meminimalisir gangguan pada elemen jaringan atau keseluruhan jaringan. Gambar berikut beberapa faktor yang menyebabkan terjadinya downtime sebuah jaringan.



Sumber: cisco.com

Gambar 1. Faktor-faktor penyebab network down

Dari gambar terlihat beberapa faktor yang menyebabkan permasalahan didalam jaringan dimana sebanyak 40% permasalahan pada bidang operasional, 40% permasalahan pada software aplikasi dan 20% terkait jaringan. Dari gambaran diatas perlunya dilakukan NMS dan salah satunya adalah dalam Performance management.

Performance management (PM) adalah kegiatan yang dilakukan untuk menilai indikator unjuk kerja dari operasi jaringan secara berkesinambungan. Dengan PM diharapkan gangguan didalam jaringan dapat diprediksi dan QoS dapat terus dipertahankan.

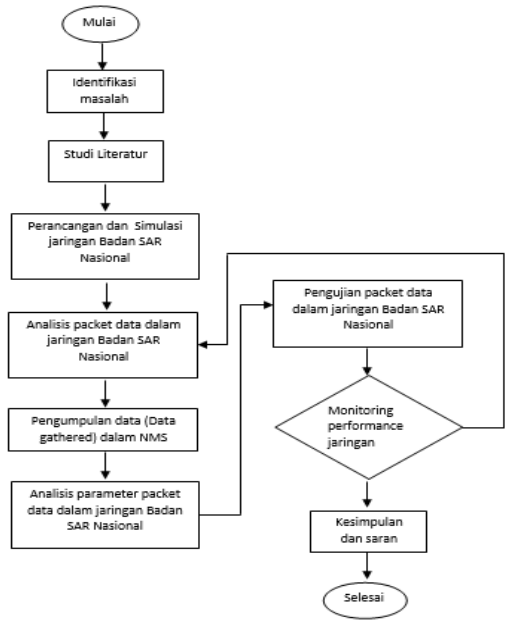
Tujuan penelitian

Tujuan dilakukannya penelitian ini antara lain:

1. Memahami analisis dan proses network forensik terhadap data.
2. Mengidentifikasi permasalahan yang terjadi pada Badan SAR Nasional.
3. Menganalisa paket data jaringan Badan SAR Nasional.

BAHAN DAN METODE

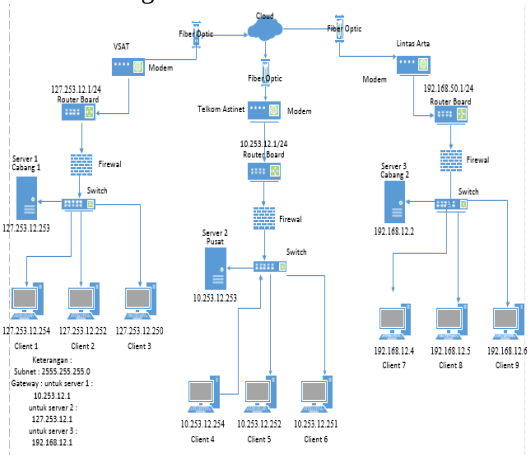
Untuk menganalisa sebuah system jaringan komputer di Badan SAR Nasional digunakan aplikasi wireshark, wireshark memungkinkan pengguna mengamati data dari jaringan yang sedang beroperasi. Simulasi jaringan menggunakan aplikasi virtual Box, komputer server, komputer client dan perangkat keras jaringan berupa switch sebagai penghubung. Metode penelitian yang dilakukan dengan menggunakan eksperimen secara langsung, dengan diagram alur sebagai berikut:



Gambar 2. Diagram alur penelitian

Analisa dan perancangan

Pada Badan SAR Nasional memiliki jaringan komputer dalam mendukung kinerja perusahaan dengan menggunakan topologi star, pada topologi ini semua node yang terhubung secara individual untuk satu switch umum. Topologi jaringan dimana stasiun transmisi yang terhubung sedemikian rupa kesimpul pusat menyerupai bentuk bintang.



Sumber: Badan SAR Nasional

Gambar 3. Skema jaringan SAR Nasional

Provider internet yang digunakan dilingkungan Badan SAR Nasional menggunakan 3 provider yaitu dari Telkom Astinet, VSAT dan Lintas Arta. Pada gambar 3, terlihat skema jaringan terdiri dari tiga cord, yang akan didistribusikan ke gedung masing-masing. Terdapat beberapa firewall sebagai pengaman jaringan baik untuk koneksi kedalam maupun keluar, sebagai upaya melindungi jaringan dan pembatasan hak akses bagi para client.

Keamanan Jaringan

Komponen yang paling penting dalam membangun sebuah jaringan komputer yaitu firewall. Celah-celah keamanan dapat terbuka dikarenakan perangkat komputer di instal dengan lebih dari satu program aplikasi, seperti aplikasi pengolah dokumen, aplikasi email client, aplikasi anti virus, aplikasi server client dan lain sebagainya.

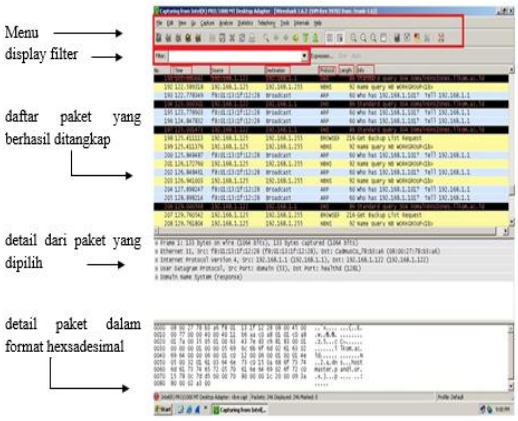
Dilingkungan Badan Sar Nasional dilengkapi dengan Cisco 2811, layanan keamanan berkinerja tinggi, termasuk firewall aplikasi, SSL dan IPS (*Internet Protocol Security*), VPN (*Virtual Private Network*), IPS (*Internet Protocol Security*) dengan korelasi global dan cakupan jaminan, antivirus, anti spam, anti phising, dan layanan web filtering. Dikombinasikan dengan teknologi reputasi real-time, teknologi ini memberikan jaringan dan sangat efektif keamanan aplikasi-aplikasi, kontrol akses, perlindungan malware, meningkatkan produktivitas karyawan, instant messaging dan aman bagi pengguna konektivitas situs.

Analisa trafik dengan Wireshark

Trafik data yang ada didalam jaringan akan mengalami fruktuasi selama proses digunakan. Pada jam kerja/jam-jam sibuk trafik data akan sangat padat sehingga proses pengiriman data akan terganggu, hal ini dikarenakan antrian data yang akan dikirim maupun yang akan datang komputer pengguna. Keterlambatan pengiriman data akan sangat mengganggu proses bisnis yang berjalan. Perlu upaya yang menjamin ketersediaan informasi yang dibutuhkan oleh seorang network administrator dalam mengelola jaringan.

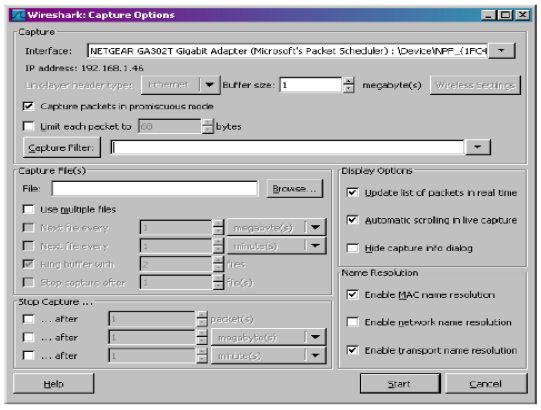
Struktur dari wireshark adalah sebagai berikut:

a. Baris menu
b. Display filter: untuk memfilter packet data
c. Daftar paket yang berhasil ditangkap
d. Detail dari paket yang dipilih
e. Detail dari paket dalam format hexadesimal



Sumber: Pribadi

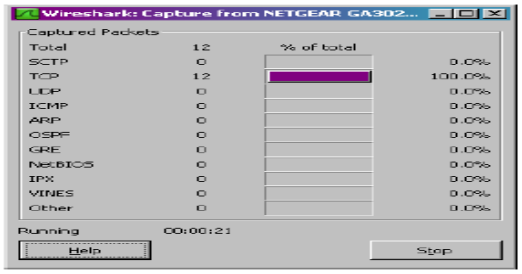
Gambar 4. Struktur wireshark



Sumber: Pribadi

Gambar 5. Pemilihan interface card

Pemilihan interface LAN Card ini diperlukan untuk pemantauan paket data yang lalu lalang di jaringan. Proses Capture dilakukan setelah tombol star di tekan.



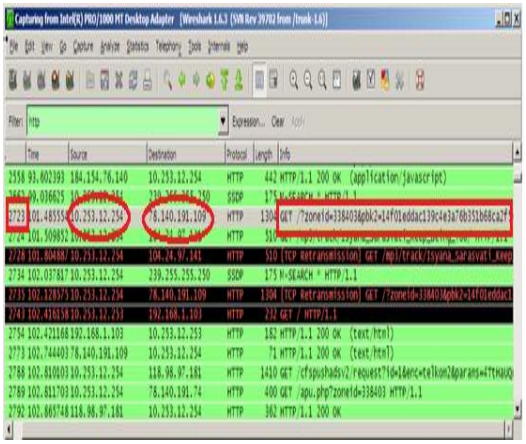
Sumber: Pribadi

Gambar 6. Proses capture paket data

Pengamatan paket data yang berjalan dijaringan mulai dilakukan. Wireshark mampu melihat dan menganalisa paket data baik secara online maupun offline.

HASIL DAN PEMBAHASAN

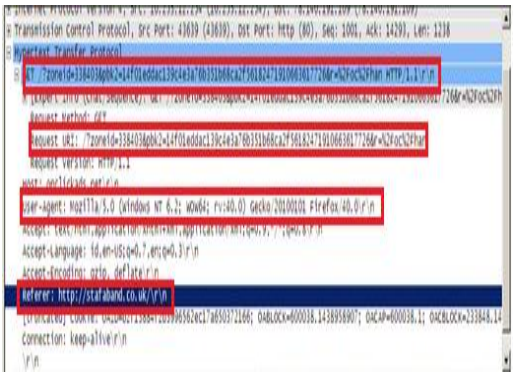
Hasil pengujian berikut ini adalah pengujian dalam proses capture yang dilakukan menggunakan wireshark baik berupa waktu capture, informasi sumber pengiriman, dan tujuan protokol.



Sumber: Pribadi

Gambar 7. Capture 2723 protokol HTTP

Pada Gambar 7 yang diberi tanda lingkaran merah terlihat bahwa *source* beralamatkan IP 10.253.12.254 dan *destination* beralamatkan IP 78.140.191.109 disana terjadi proses *request* data dari *source* kepada *destination*. *Source* berubah menjadi alamat *destination* awal dan *destination* berubah menjadi *source* awal yang dimana proses pengiriman data *request* dari *source* awal telah terkirim

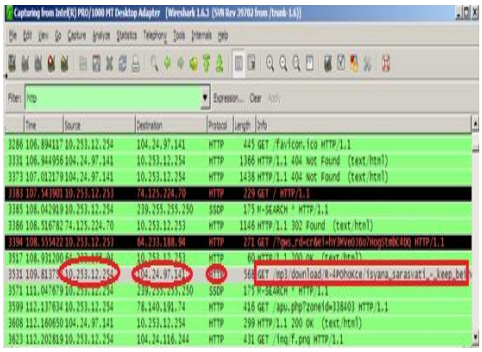


Sumber: Pribadi

Gambar 8. Paket yang di analisis

Gambar 8 menjelaskan bagaimana wireshark dapat menangkap aktifitas yang dilakukan oleh user didalam jaringan, yaitu:

a. Protokol yang digunakan : HTTP (HyperText Transfer Protokol)
b. Versi protokol HTTP/1.1
c. Pada bagian host terdapat goclickads\r\n yang merupakan alamat yang diketik pada address bar.
d. File yang direquest adalah /zoneid
e. Pada bagian user agent terdapat : Firefox/40.0 yang merupakan aplikasi browser yang digunakan beserta versinya.
f. Pada bagian user agent terdapat juga (windows NT 6.2).



Sumber: Pribadi

Gambar 9. Capture no.3531

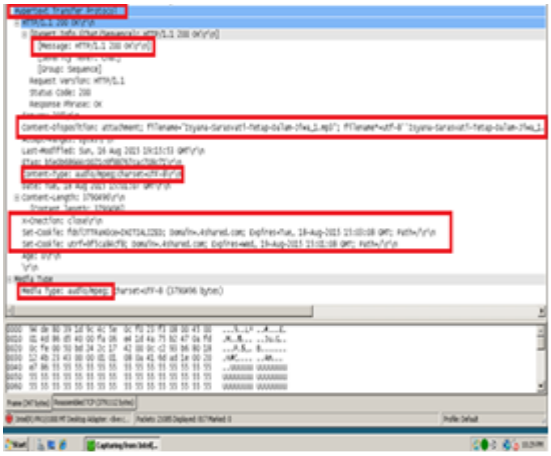
Gambar 9 dapat dilihat kembali IP source 10.253.12.254 dan destination 104.24.97.141 (IP berubah dikarenakan mirror). Source berubah menjadi alamat destination awal dan destination berubah menjadi alamat source awal yang dimana proses pengeriman data request dari source awal telah dikirim oleh destination yang bertindak sebagai source kedua karena mengirimkan data yang direquest oleh source awal. Sehingga dapat disimpulkan bahwa disini terjadi komunikasi half duplex karena proses pengiriman data terjadi secara bergantian setelah source awal bertindak sebagai pengirim request data dan destination sebagai penerima request data lalu kemudian destination tadi berubah menjadi source yang mengirimkan data request dari source awal tersebut.

Sumber: Pribadi

Gambar 10. Hasil capture wireshark

a) Pada gambar diatas dijelaskan sebagai berikut:
b) Protokol yang digunakan : TCP (Transmission Control Protokol)
c) Header yang diberikan berbentuk IP address
d) Protokol yang digunakan : HTTP (Hypertext Transfer Protokol)
e) Versi protokol HTTP/1.1
f) Pada bagian host terdapat www.stafaband.co.uk\r\n yang merupakan alamat yang diketik pada address bar.

g) File yang di request adalah mp3/download/R-4pohKce/isyana_saravasti_-_keep_being_you/.
h) Pada bagian user agent terdapat: firefox/40.0\r\n yang merupakan aplikasi browser yang digunakan beserta versinya



Sumber: pribadi

Gambar 10. Hasil capture wireshark

Hasil capture gambar 10, dapat dianalisa sebagai berikut:

i) Protokol yang digunakan yaitu HTTP (Hypertext Transfer Protokol)
j) Pesan : HTTP/1.1 200 ok yang berarti telah selesai.
k) Content-position: attachment; filename=“ Isyana-Sarasvati-Tetap-Dalam-Jiwa_1.mp3
l) Content-type: dalam bentuk audio/mpeg.
m) Dalam content-length terlihat adanya x-cnectio yaitu close dan dibawahnya terdapat cookie (berkas).
n) Media type berbentuk audio/mpeg.

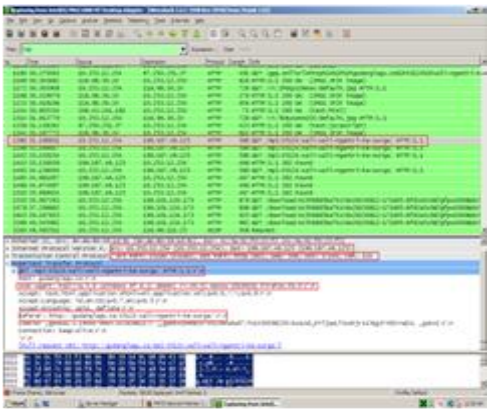
Dalam pengujian akhir server memantau kerusakan data pada client saat mengakses data.

1. Protokol Hypertext Transfer Protokol (HTTP)
   Protokol HTTP dapat dikatakan protokol yang sering digunakan terutama pada aplikasi browser untuk berinternet. Karena sering digunakan, peluang terjadinya kerusakan atau kegagalan pada protokol ini besar.

Sumber: Pribadi

Gambar 11. Paket data no 1360

Keterangan dari gambar 11 ip dari *client* yaitu 10.253.12.254 yang akan melakukan download, sedangkan ip dari situs yang akan di*download* 192.167.46.125 dari info diatas ip *client* sudah mendapatkan dengan kata Get.

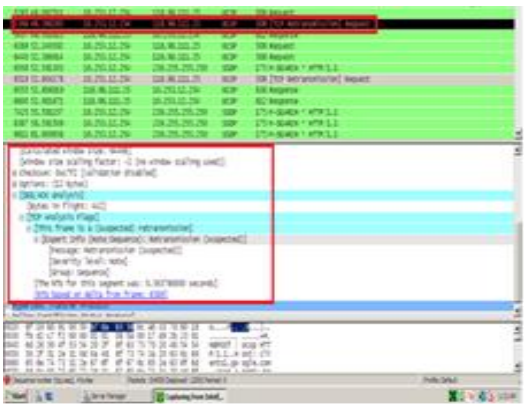


Sumber: pribadi

Gambar 12. Capture paket data no 1360

Dari gambar 12 dapat di analisa sebagai berikut:

a. Gambar kotak pertama menjelaskan no.1360, time: 31.196831 source 10.253.12.254 dan destination 199.167.46.125, info yang diatas adalah Get (yang artinya meminta)/mp3/45124/wali-wali-ngantri-ke-surga/ HTTP/1.1
b. Kotak kedua menjelaskan ip version 4 dimana *client* 10.253.12.254 dan tujuan 199.167.46.125
c. Kotak ketiga menjelaskan tentang *port*, *port client* 45810, *destination port* http (80), sequence 508, acknowledgement 37140, len 520.
d. Pada kotak keempat ketika klik hypertext Protokol akan keluar lebih detail penjelasan arah *client*.
e. Kotak kelima *client* membuka aplikasi melalui mozila firefox.
f. Kotak ke enam arah client menunjukan http://gudang lagu.co//wali-ngantri-ke-surga



Sumber: pribadi

Gambar 13. Penjelasan Request time Out

Pada gambar diatas kotak pertama ip client dan ip tujuan dengan protokol OSCP (*Online Certificate Status Protokol*) dengan info [TCP

Retransmission] Request. Dalam kotak yang kedua sebagai berikut

1. Ukuran kalkulasi window : 64466
2. Skala faktor ukuran window : -2 (tidak skala dalam window bekas)
3. Checksum : 0xc7f2 (pengesahan gagal)
4. SEQ/ACK (mengakui data yang diterima) analysis, bytes in flight : 422
5. *Frame ini adalah suspected (tersangka)* retransmission (pengiriman ulang sebuah paket data jika data diterima terdapat kesalahan.
6. Severity level (tingkat keparahan) : note (kode error HTTP)
7. RTO segment adalah : 0.363786000
8. RTO based on delta from frame (berdasarkan delta dari frame) :63891

Dalam pengujian akhir dapat disimpulkan bahwa pengujian akhir ini mengalami request time out dikarenakan client mendownload tanpa selesai dengan masalah jaringan internet.

KESIMPULAN

Dari penelitian yang telah dilakukan, maka dapat diambil kesimpulan sebagai berikut:

1. Sistem wireshark dapat menjalankan fungsi forensik (identifikasi) terhadap lalu lintas data sehingga dapat terus di identifikasi setiap saat.
2. Lebih mempermudah kerja administrator jaringan dalam melihat kondisi client-client yang sedang mengakses data dikantor pusat maupun dikantor cabang.
3. Pada jaringan komputer digunakan metode komunikasi half duplex dibuktikan pada proses penerimaan dan pengiriman paket dilakukan satu per-satu antara source dan destination

UCAPAN TERIMAKASIH

Penulis menyampaikan terimakasih kepada Bapak Didit Permana, S.Kom. dan seluruh staf dan karyawan BASARNAS, atas masukkan dan kerjasamanya.

DAFTAR PUSTAKA

International journal of advanced research in computer science and software engineering, vol 2, issue 11

Kurniawan, A. 2012. Network Forensics: Panduan analisis & invenstigasi paket data jaringan menggunakan wireshark, Andi: Yogyakarta.

Muamar kadafi & Khusnawi (2015), Analisis Rogue DHCP Packets menggunakan wireshark Network protocol analyer. Citec Journal. Vol 2 No.2

M. Ferdy Adrian & Is Mardianto (2015), Implementasi wireshark untuk penyadapan (sniffing) paket data jaringan. Seminar nasional Cendekiawan 2015.

Rika Rosnelly & Reza pulungan (2011), Membandingkan analisa trafik data pada jaringan komputer antara Wireshark dan NMAP. Konferensi nasional Sistem informasi.

Shilpi Gupta & Roopal Mamtora (2012). Intrusion Detection System using wireshark.

Subramanian, Mani. 2000. Network Management: Principles and Practice

Sofana. 2012. Cisco CCNP dan Jaringan Komputer. Informatika: Bandung.

Tengku Mohd Diansyah (2015), Analisa pencegahan aktivitas ilegal didalam jaringan menggunakan Wireshark. Jurnal Times, vol IV No.2: 20-23