PENGGUNAAN NMAP DAN HPING 3 DALAM MENGANALISA KEAMANAN JARINGAN PADA B2P2TO2T

(Karanganyar, Tawangmangu)

Makalah

Diajukan oleh :

Nama : ***Yunan Arie Prabowo***
Pembimbing 1 : ***Muhammad Kusban, S.T., M.T***
Pembimbing 2 : ***Hernawan Sulistyanto, S.T, M.T***

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS KOMUNIKASI DAN INFORMATIKA
UNIVERSITAS MUHAMMADIYAH SURAKARTA
2014

HALAMAN PENGESAHAN

Publikasi Ilmiah dengan judul :

PENGGUNAAN NMAP DAN HPING 3 DALAM MENGANALISA KEAMANAN JARINGAN PADA B2P2TO2T

(Karanganyar, Tawangmangu)

Yang dipersiapkan dan disusun oleh :

YUNAN ARIE PRABOWO
L 200 080 173

Telah disetujui pada :

Hari : SENIN

Tanggal : 23 JUNI 2014

Pembimbing I	Pembimbing II
Muhammad Kusban, S.T., M.T	Hernawan Sulistyanto, S.T, M.T
NIK: 663	NIK : 882

Publikasi ilmiah ini telah diterima sebagai salah satu persyaratan

Untuk memperoleh gelar sarjana

Tanggal ....

Mengetahui,

Ketua Program Studi

Teknik Informatika

Dr. Heru Supriyono, M.Sc.

NIP: 100.970

UNIVERSITAS MUHAMMADIYAH SURAKARTA
FAKULTAS KOMUNIKASI DAN INFORMATIKA
PROGRAM STUDI TEKNIK INFORMATIKA
Jl. A Yani Tromol Pos 1 Pabelan Kartasura Telp. (0271)717417, 719483 Fax (0271) 714448
Surakarta 57102 Indonesia. Web: http://informatika.ums.ac.id Email: informatika@fki.ums.ac.id

SURAT KETERANGAN LULUS PLAGIASI

/A.3-II.3/INF-FKI/VII/2014

Assalamu'alaikum Wr. Wb

Biro Skripsi Program Studi Teknik Informatika menerangkan bahwa :

Nama	:	YUNAN ARIF PRABOWO
NIM	:	L200080173
Judul	:	PENGGUNAAN NMAP DAN HPING3 DALAM MENGANALISA KEAMANAN JARINGAN PADA B2P2TO2T (KARANGANYAR,TAWANGMANGU)
Program Studi	:	Teknik Informatika
Status	:	**Lulus**

Adalah benar-benar sudah lulus pengecekan plagiasi dari Naskah Publikasi Skripsi, dengan menggunakan aplikasi Turnitin.

Demikian surat keterangan ini dibuat agar dipergunakan sebagaimana mestinya.

Wassalamu'alaikum Wr. Wb

Surakarta, 12 Juli 2014

Biro Skripsi
Teknik Informatika

Fauzan Natsir, S.Kom

Turnitin Originality Report

GUNAAN NMAP DAN HPING 3
M MENGANALISA KEAMANAN
GAN PADA B2P2TO2T
nganyar, Tawangmangu) by Yunan
rabowo

Similarity Index	Similarity by Source	
28%	Internet Sources:	23%
	Publications:	0%
	Student Papers:	8%

September 2014 (publikasi maret

sources:

ocessed on 07-Jul-2014 06:06 WIT
: 438186040
ord Count: 2661

1 12% match (Internet from 16-Apr-2014)
http://budi.insan.co.id/courses/ec5010/projects/thomas-t.pdf

4% match (student papers from 17-Feb-2014)
Class: publikasi maret 2014
Assignment:
r ID: 397168759

2% match (Internet from 08-Dec-2012)
http://www.madhi.web.id/2011/11/tips-membuat-jaringan-komputer-lanlocal.html

1% match (Internet from 16-Dec-2013)
http://www.unisbank.ac.id/ojs/index.php/fti1/article/view/33

1% match (Internet from 31-Jan-2011)
http://laurasaragih85.wordpress.com/2009/04/27/pertemuan-3/

1% match (Internet from 16-Jun-2014)
http://dwiawan081.blogspot.com/

1% match (student papers from 19-Jun-2013)
Submitted to Universitas Muhammadiyah Surakarta on 2013-06-19

1% match (Internet from 15-Jun-2013)
http://derivil.blogspot.com/

1% match (Internet from 10-Apr-2014)
http://alexbucely.blogspot.com/2013/07/makalah-keamanan-jaringan-komputer.html

1% match (Internet from 12-Aug-2012)
http://jagadilmu.com/component/content/article/74.html

PENGGUNAAN NMAP DAN HPING 3 DALAM MENGANALISA KEAMANAN JARINGAN PADA B2P2TO2T

(Karanganyar, Tawangmangu)

Teknik Informatika, Fakultas Komunikasi dan Informatika

Universitas Muhammadiyah Surakarta

E-Mail : yunanarie@ymail.com

ABSTRAK

Sistem keamanan jaringan komputer yang terhubung ke internet harus direncanakan dan dipahami dengan baik agar dapan melindungi sumber daya yang berada dalam jaringan tersebut secara efektif. Model-model penanganan keamanan yang terjadi pada masing-masing lapis pada teknologi wireless tersebut dapat dilakukan antara lain yaitu dengan cara menyembunyikan SSID, memanfaatkan kunci WEP, WPA-PSK atau WPA2-PSK, implementasi fasilitas MAC *filtering*, pemasangan infrastruktur *captive portal.*

Tujuan dari penelitan yaitu mengetahui kelemahan dari suatu jaringan, dengan mengunakan NMAP dan HPING3 sehingga dengan mengetahui kelemahan yang terdapat pada jaringan maka langkah-langkah untuk mengatasi kelemahan ini dapat dilakukan.

Metode yang digunakan yaitu ekperimen dengan lokasi penelitian di yaitu di Balai Besar Penanaman dan Penelitian Tanaman Obat Dan Obat Tradisional (B2P2TO2T) Tawangmangu, Karanganyar. Metode pengumpulan data dilakukan dengan cara hasil implementasi pada Nmap dan Hping.

Kesimpulan hasil penelitian yaitu jaringan komputer internet yang sifatnya publik dan global pada dasarnya kurang aman. Untuk meningkatkan keamanan jaringan internet dapat menggunakan beberapa metode, dua metode diantaranya menggunakan Nmap dan Hping3. Keunggulan-keunggulan yang dimiliki oleh Nmap, antara lain *powerful* Nmap dapat digunakan untuk men-*scan* jaringan yang besar, *portable*, Nmap dapat berjalan di berbagai macam system, operasi seperti Linux, Windows, FreeBSD, OpenBSD, Solaris, dan sebagainya, mudah untuk digunakan, dan free. Kelebihan Hping3, yaitu untuk pengecekan kondisi komputer dan port-portnya, paket yang dikirimkan dapat berupa TCP, UDP, atau ICMP, dan aplikasi ini berukuran kecil sehingga ringan dijalankan.

Kata Kunci: Keamanan Jaringan Komputer, Nmap, Hping

PENDAHULUAN

Balai Besar Penanaman dan Penelitian Tanaman Obat dan Obat Tradisional (B2P2TO2T) Tawangmangu, Karanganyar merupakan salah satu lembaga pertanian yang memberikan informasi kepada masyarakat mengenai hasil penelitian yang telah dilakukan.

B2P2TO2T memiliki aset informasi (*hardware, software*, sistem, informasi dan manusia) untuk mendukung pelaksanaan pemberian informasi ke masyarakat. Aset informasi tersebut merupakan aset yang perlu dilindungi dari risiko keamanannya baik dari pihak luar dan dalam organisasi.

Keamanan informasi tidak bisa hanya disandarkan pada *tools* atau teknologi keamanan informasi, melainkan perlu adanya pemahaman dari organisasi tentang apa yang harus dilindungi dan menentukan secara tepat solusi yang dapat menangani permasalahan kebutuhan keamanan informasi). Untuk itu butuh pengelolaan keamanan informasi yang sistemik dan komprehensif.

Selama ini B2P2TO2T menggunakan tools keamanan *nessus*. Pada kenyataan sistem keamanan *nessus* yang dipergunakan tersebut belum optimal karena terjadi kelemahan jaringan wireless, Hal ini mengganggu keamanan sistem informasi. Keamanan sistem informasi berbasis internet harus sangat diperhatikan, karena jaringan komputer internet yang sifatnya publik dan global pada dasarnya tidak aman.

Guna mengatasi permasalahan kelemahan pada jaringan wireless B2P2TO2T tersebut, peneliti mencoba mengunakan NMAP dan HPING3. Oleh sebab itu, tujuan penulisan dari proyek akhir ini adalah untuk membahas mengenai analisa keamanan jaringan internet dan bagaimana untuk mengetahui *vulnerability* dari suatu jaringan, dengan

mengunakan NMAP dan HPING3 sehingga dengan mengetahui kelemahan yang terdapat pada jaringan maka langkah-langkah untuk mengatasi kelemahan ini dapat dilakukan.

TINJAUAN PUSTAKA

Jaringan Komputer

Sulistyo (2011) menyatakan bahwa jaringan komputer adalah sebuah kumpulan komputer, *printer* dan peralatan lainnya yang terhubung dalam satu kesatuan. Informasi dan data bergerak melalui kabel-kabel atau tanpa kabel sehingga memungkinkan pengguna jaringan komputer dapat saling bertukar dokumen dan data, mencetak pada *printer* yang sama dan bersama-sama menggunakan *hardware/software* yang terhubung dengan jaringan.

Tujuan dari jaringan komputer adalah : (1) Membagi sumber daya: contohnya berbagi pemakaian *printer*, CPU, memori, *Hard-Disk*.. (2) Komunikasi: contohnya surat elektronik, *instant messaging*, *chatting.* (3) Akses informasi: contohnya *web browsing* (Andrian, 2010).

Apabila ingin mengamankan suatu jaringan maka harus ditentukan terlebih dahulu tingkat ancaman (*threat*) yang harus diatasi, dan resiko yang harus diambil maupun yang harus dihindari seperti mengenai ancaman (*threat*), kelemahan, dan *Policy* keamanan (*security policy*) jaringan.

Insiden keamanan jaringan adalah suatu aktivitas terhadap suatu jaringan komputer yang memberikan dampak terhadap keamanan sistem yang secara langsung atau tidak bertentangan dengan *security policy sistem* tersebut (Amin, 2012).

NMAP (ZENMAP)

Rosnelly dan Pulungan (2011) menjelaskan bahwa Nmap (*Network Mapper*) adalah sebuah program *open source* yang berguna untuk mengeksplorasi jaringan. Nmap didesain untuk dapat melakukan *scan* jaringan yang besar, juga dapat digunakan untuk melakukan *scan* host tunggal. Nmap

menggunakan paket IP untuk menentukan host-host yang aktif dalam suatu jaringan port-port yang terbuka, sistem operasi yang dipunyai, tipe *firewall* yang dipakai.

Fungsi utama dari Nmap adalah sebagai *port scanning*, menurut definisinya *scanning* adalah kegiatan probe dalam jumlah yang besar dengan menggunakan tool secara otomatis, dalam hal ini adalah Nmap. Sebuah scanner sebenarnya adalah scanner untuk *port* TCP/IP, yaitu sebuah program yang menyerang port TCP/IP dan servis-servisnya (telnet, ftp, http, dan lain - lain) dan mencatat respon dari komputer target. Dengan cara ini, user program scanner dapat memperoleh informasi yang berharga dari *host* yang menjadi target (Rosnelly dan Pulungan, 2011).

Hping3

Hping adalah sebuah TCP/IP assembler dan juga merupakan command-line yang berorientasi pada pemrosesan paket TCP/IP. Hping dapat digunakan untuk membuat paket IP yang berisi TCP, UDP atau ICMP *payloads*. Semua *field header* dapat dimodifikasi dan dikontrol dengan menggunakan baris perintah (*command line*). Pemahaman yang cukup baik tentang IP, TCP atau UDP wajib diketahui untuk menggunakan dan memahami *tool* ini (http://www.hping.org).

Setiawan (2004) menjelaskan bahwa Hping3 merupakan versi terbaru dari Hping, dan Hping2 adalah aplikasi pendahulunya yang paling signifikan. Hping3 merupakan aplikasi yang berdiri sendiri (*standalone*), sedangkan Hping2 dalam beberapa kasus masih memerlukan aplikasi dari pihak ketiga, seperti *scapy* (*tools* memanipulasi paket) dan *idswakeup* (sebuah aplikasi untuk sistem pendeteksian *intrutions* / penyusup). Hping3 hadir dengan mesin baru TCL *scripting*, sehingga lebih kuat pada perintah *command line* yang sederhana.

METODE PENELITIAN

Penelitian ini penulis menggunakan metode experimental. Tempat penelitian dilakukan di Balai Besar Penelitian dan Pengembangan Tanaman Obat dan Obat Tradisional,

Tawangmangu, Karanganyar. Peralatan utama dan pendukung.

Alat dan perangkat lunak yang mendukung penelitian ini adalah sebagai berikut: Laptop, Komputer *Server*, Komputer *Client*, OS LINUX, *Software* NMAP dan HPING3.

HASIL PENELITIAN

1. PC Router sebagai Firewall

a. Pengujian Menggunakan Nmap

Digunakan Nmap TCP Connect Scan () untuk melakukan port scan/sweep terhadap *web server cloud* dan melihat hasilnya apakah *firewall* berfungsi dengan baik. Nmap telah melakukan *Port Scan* pada *web server* selama 17,48 detik dan layanan (*service*) yang ada pada *web server cloud* adalah untuk http (port 80), https (port 443) dan DNS (port 53). Tetapi yang dalam keadaan terbuka (open/tersedia pada *web server* tersebut) adalah layanan untuk http dan https (port 80 dan 443), sedangkan untuk layanan DNS (port 53), walaupun pada *web server* ada layanan untuk DNS tetapi *web server* tidak menyediakannya untuk client karena dalam keadaan tertutup (*closed*). Ketika dilakukan scan nmap kembali kepada *web server private cloud*, paket yang di-log oleh *Iptables* bertambah dari yang asalnya 2006 paket, menjadi 4012 paket. Dengan kata lain, setiap nmap TCP *Connect Scan Iptables* dapat melakukan *log paket* 1990-2020 paket

b. Pengujian menggunakan Hping3

Didapatkan hasil bahwa hping3 telah melakukan *ICMP Flood* dengan mengirimkan paket sebanyak 4381686 paket, tetapi paket yang di-log oleh *Iptables* hanya berjumlah 64 paket. Terjadinya perbedaan jumlah paket yang dikirim dan di-log oleh *firewall ini* karena keterbatasan kemampuan seberapa cepat *Iptables* menghasilkan sebuah pesan log.

2. PC Router sebagai Firewall dan Log Analysis

a. Pengujian Menggunakan Nmap

Dalam laporan ada bagian yang kosong atau bernilai [*NONE*] yaitu pada bagian iptables auto-blocked IPs. Ini dikarenakan fitur IDS pada Psad tidak diaktifkan (*OFF*) sehingga apabila suatu Alamat IP melakukan serangan yang

melebihi batas toleransi yang diijinkan oleh sistem keamanan (*Danger Level/DL*), tidak akan dilakukan pemblokiran alamat IP. Ketika dilakukan pengujian nmap scan kembali, hasil data *log Iptables* bertambah dari yang asalnya 2006 menjadi 4012 paket. Dari hasil yang didapat tersebut tidak berbeda jauh dengan pengujian sebelumnya (*PC Router* sebagai *Firewall*), dimana ketika dilakukan nmap scan kembali setelah percobaan pertama paket yang di-log oleh *Iptables* bertambah sekitar 1990-2010 paket.

b. Pengujian menggunakan Hping3

Hasil laporan tidak berbeda jauh dengan pengujian yang sebelumnya dilakukan pada laporan Psad dijelaskan secara detil mengenai serangan/scan yang terjadi tetapi pada bagian Top 50 signatures mantches terdapat suatu keterangan terhadap serangan/scan yang terjadi yaitu "*ICMP PING*".

3. PC Router Sebagai Firewall, Log Analysis dan IDS

a. Pengujian Menggunakan Nmap

Psad telah memasukkan/membuat alamat IP 90.10.1.100 untuk di-blok secara otomatis karena telah melebihi Danger Level yang sebelumnya telah ditentukan (DL=2). Dapat dilihat pada bagian *iptables auto-blocked IPs*: terdapat keterangan bahwa alamat IP 90.10.1.100 telah di-blok dan waktu yang tersisa *Rules block IP* tersebut berlaku tinggal 2276 detik (dari yang sebelumnya 3600 detik).

b. Pengujian menggunakan Hping3

Menjelaskan secara detil serangan apa saja yang terjadi terhadap *web server*. Hasil laporan yang dihasilkan tidak berbeda jauh dengan hasil pengujian yang sebelumnya dilakukan. Hanya, pada pengujian ini, keterangan *iptables auto-blocked IPs*:, terisi dengan alamat IP 90.10.1.100, ini menandakan bahw a *IDS Psad* bekerja dalam melakukan blok alamat IP. Serangan yang terjadi terhadap *web server*. Hasil laporan yang dihasilkan tidak berbeda jauh dengan hasil pengujian yang sebelumnya dilakukan. Hanya, pada pengujian ini, keterangan *iptables auto-blocked IPs*:, terisi dengan

alamat IP 90.10.1.100, ini menandakan bahw a IDS Psad bekerja dalam melakukan blok alamat IP.

4. PC Router Tanpa Firewall, Log Analysis dan IDS

a. Pengujian Menggunakan Nmap

Terlihat hasil laporan Psad tidak melaporkan sama sekali terhadap nmap scan yang dilakukan. Ini dikarenakan karena *Iptables* sama sekali tidak melakukan log paket atau *PC Router* tidak menggunakan fungsi *Iptables* sebagai *firewall* dan log paket serta men-drop-nya kemudian. Dan karena *Iptables firewall* dalam keadaan tidak berfungsi sehingga otomatis fitur IDS pada Psad tidak berfungsi.

b. Pengujian Menggunakan Hping3

Sistem keamanan yang paling aman/baik adalah pada pengujian ketiga yaitu PC Router Sebagai *Firewall, Log Analysis* dan *IDS*. Dikarenakan adalah ketika Attacker PC melakukan serangan *Port Scan* (percobaan 1) terhadap *web server Private Cloud*, serangan tersebut menyebabkan IDS bekerja secara otomatis mem-blok alamat IP yang melakukan serangan. Sehingga ketika *Attacker PC* melakukan *Port Scan* kembali (percobaan 2), pada hasil port scan-nya port-port pada web server tidak terlihat dan tertutup untuk *Attacker PC*. Serta jumlah paket yang di-log *Iptables* sama seperti sebelumnya, yaitu 25 paket. Ditambah waktu yang diperlukan nmap dalam menyelesaikan scan lebih lama apabila dibandingkan dengan pengujian yang sebelumnya. Ini artinya bahwa IDS sukses melakukan blok alamat *IP Attacker* PC. Sedangkan yang paling tidak aman/baik adalah pada pengujian 2 (PC Router Tanpa Firewall, Log Analysis dan IDS). Karena pada pengujian 2, ketika port scan dilakukan. Didapatkan hasil bahwa port yang terbuka dan terlihat oleh *Attacker PC* selain Port-port yang secara umum terbuka (port 80, 443), *port-port* vital pun terlihat dari luar seperti port 135, 139, 445, dan 3306 sehingga menambah resiko keamanan *Web Server* itu sendiri. Karena pada pengujian 4 Sistem keamanan tidak diaktifkan, maka hasilnya sama sekali tidak ada paket yang di-log oleh *firewall*

Sistem keamanan yang paling baik, adalah sistem keamanan yang digunakan pada pengujian 2 (PC Router sebagai Firewall, Log Analysis dan IDS). Karena ketika dilakukan ICMP Flood pada percobaan 1, Attacker PC yang melakukan serangan, di-blok alamat IP-nya oleh IDS sehingga menyebabkan ketika Attacker PC melakukan serangan kembali sistem keamanan pada PC Router memblok paket-paket yang berasal dari Attacker PC. Ini dibuktikan dengan jumlah paket yang di-log sesudah percobaan 1 dan 2 berjumlah sama (80 paket). Pengujian 1 dan 2 jumlah paket yang di-log setelah percobaan 1 dan 2 mengalami kenaikan.

Tabel Ringkasan Hasil Nmap

No	Pengujian	Status	Jumlah paket yang di log		Hasil Port Scan Nmap	
			Percobaan 1	Percobaan 2	Percobaan 1	Percobaan 2
1	PC Router Sebagai Firewall	OFF	2006	4012	53 (closed), 80 (open), 443 (open)	53 (closed), 80 (open), 443 (open)
2	PC Router Sebagai Firewall dan Log Analysis	OFF	2006	4012	80 (open), 443 (open)	53 (closed), 80 (open), 443 (open)
3	PC Router Sebagai Firewall, Log Analysis dan IDS	ON	25	25	53 (closed), 80 (open), 443 (open)	NONE (BLOCKED)
4	PC Router Tanpa Firewall, Log Analysis dan IDS	OFF	0	0	80 (open), 135 (open), 139 (open), 443 (open), 445 (open), 3306 (open)	80 (open), 135 (open), 139 (open), 443 (open), 445 (open), 3306 (open)

Tabel Ringkasan Hasil Hping3

No	Pengujian	Status	Jumlah Paket dikirim Hping3		Jumlah paket yang di log	
			Percobaan 1	Percobaan 2	Percobaan 1	Percobaan 2
1	PC Router Sebagai Firewall	OFF	4381686	4467485	64	130
2	PC Router Sebagai Firewall dan Log Analysis	OFF	4479887	4505001	66	132
3	PC Router Sebagai Firewall, Log Analysis dan IDS	ON	4473024	4482804	80	80
4	PC Router Tanpa Firewall, Log Analysis dan IDS	OFF	4489364	4491140	0	0

Kesimpulan

Pengujian Nmap menggunakan perintah Nmap –sT 192.168.1.10 dan Hping3 menggunakan perintah hping3 –p 80 --flood –-icmp 192.168.1.10. Pengujian-pengujian Nmap dan hping3 menggunakan 4 kriteria yaitu: (1) PC *Router* sebagai *Firewall (Iptables)*, (2) *PC Router* sebagai *Firewall (Iptables)* serta *Log Analysis (Psad)*, (3) *PC Router* sebagai *Firewall (Iptables)* serta *Log Analysis* and IDS (Psad), dan (4) *PC Router* tanpa *Firewall*, *Log Analysis* dan ID. Hasil yang diperoleh, sebagai berikut:

1. *PC Router* sebagai *Firewall (Iptables)*, Nmap telah

melakukan *Port Scan* pada web server selama 17,48 detik dan layanan *(service)* yang ada pada web *server cloud* adalah untuk http (port 80), https (port 443) dan DNS (port 53). Sedangkan hping3 telah melakukan ICMP *Flood* dengan mengirimkan paket sebanyak 4381686 paket, tetapi paket yang di-log oleh *Iptables* hanya berjumlah 64 paket.

2. *PC Router* sebagai *Firewall (Iptables*) serta *Log Analysis (Psad),* nmap menyelesaikan *port scan* dengan waktu sekitar 17,98 detik. mendeteksi ada 3 port yang terlihat dari luar jaringan *privete cloud* yaitu http (port 80), https (port 443) dan DNS (port 53) dan ICMP Flood dengan Hping3 selama 30 detik adalah sebanyak 4479887 paket
3. *PC Router* sebagai *Firewall (Iptables)* serta *Log Analysis and IDS (Psad),* nmap menyelesaikan port scan-nya selama 1158,09 detik. Sedangkan ICMP PING pada Hping3 untuk memblok suatu alamat IP yang melakukan serangan selama 3600 detik.
4. *PC Router t*anpa *Firewall Log Analysis dan ID*, Nmap TCP Connect Scan () terhadap web server private cloud dapat terdeteksi port 80 (http), dan 443 (https) dalam keadaan terbuka, *port-port vital* seperti port 135 (msrpc), 139 (netbios-ssn), 445 (microsoft-ds), dan 3306 (mysql) pada web. Sedangkan Hping3 menunjukkan *Attacker* PC mengirimkan paket ICMP_ECHO_REQUEST pada *web server private cloud* selama 30 detik sebanyak 4489364 paket.

Saran

Mengingat jaringan *wireless* di B2P2TO2T masih ada kelemahan, maka bagi B2P2TO2T sebagai lembaga publik disarankan untuk menggunakan menggunakan jaringan *wireless* lain, sehingga dapat melindungi data-data penting bagi lembaga.

Bagi lembaga B2P2TO2T diharapkan di masa mendatang dapat menggunakan teknologi yang lebih

baik untuk menjaga keamanan jaringan. Adanya teknologi baru yang dimanfaatkan oleh B2P2TO2T, maka lembaga dapat memanfaatkan jaringan *wireless* baru untuk kepentingan lembaga.

DAFTAR PUSTAKA

Amin, Ziad. 2012. Analisis Vulnerabilitas Host Pada Keamanan Jaringan Komputer di PT. Sumeks Tivi Palembang (PALTV) Menggunakan Router Berbasis UNIX. *Jurnal Teknologi dan Informatika*. Vol. 2, No. 3.

Andrian, Henry Rossi. 2010. *Implementasi Radio Kampus pada Jaringan Lokal Politeknik Telkom*. Bandung: Program Studi Teknik Komputer Politeknik Telkom Bandung.

Rosnelly, Rika dan Pulungan, Reza. 2011. Membandingkan Analisa Trafik Data Pada Jaringan Komputer antara Wireshark dan NMap. *Konferensi Nasional Sistem Informasi*. Yogyakarta.

Setiawan, Thomas. 2004. *Analisis Keamanan Jaringan Internet Menggunakan Hping, Nmap, Nessus, dan Ethereal*, Bandung, Departemen Teknik Elektro Fakultas Teknologi Industri Institut Teknologi Bandung.

Sulistyo, Haryo Budi. 2011. Implementation And Local Area Network (Lan)-Based Wireless Network. *Skripsi*. Jakarta: Universitas Gunadarma.

BIODATA PENULIS

Nama : Yunan Arie Prabowo

Tempat dan Tanggal Lahir : Surakarta, 18 Juni 1989

Jenis Kelamin : Pria

Agama : Islam

Perguruan Tinggi : Universitas Muhammadiyah Surakarta

Fak/Jur : Komunikasi & Informatika / T.informatika

Alamat Rumah : Joho Kidul RT 01 RW 04 Mojolaban Sukoharjo

No. HP : 085642475574

Alamat e-mail : yunanarie@ymail.com