PEMANFAATAN MINI KOMPUTER RASPBERRY SEBAGAI *NETWORK MONITORING TOOL PORTABLE*

Cosmas Eko Suharyanto[1]; Viriyadharma Gopama[2]

[1,2]Program Studi Teknik Informatika
Universitas Putera Batam
www.upbatam.ac.id
[1]cosmas@puterabatam.ac.id, [2]vgopamas@gmail.com

Abstract—*This study aims to design a portable monitoring system using the Raspberry mini computer. As a case study, we conducted this research at Credit Union Tunas Harapan, which is based in Batam, Indonesia. We implemented the system with additional tools to monitor networks, namely Wireshark and Nagios. On the local network we managed to monitor broadcasting from the switch. We have also analyzed several issues on network security. The use of architectural Raspberry mini computers is a very flexible tool.*

Keywords: *Network Security, Raspberry Pi, Network Monitoring, Portable Network Monitoring*

Intisari—Penelitian ini bertujuan untuk merancang sebuah sistem *monitoring* portabel dengan memanfaatkan mini komputer Raspberry. Sebagai studi kasus, kami melakukan penelitian ini di jaringan kantor Credit Union Tunas Harapan, yang berkedudukan di Batam, Indonesia. Kami mengimplementasikan sistem dengan tool tambahan untuk memonitor jaringan, yaitu Wireshark dan Nagios. Pada jaringan lokal kami berhasil memantau adanya broadcasting dari switch. Kami juga telah menganalisis beberapa isu terkait keamanan jaringan. Pemanfaatan komputer mini Raspberry secara arsitektur adalah alat yang sangat fleksibel.

Kata Kunci*: Network Security, Raspberry Pi, Network Monitoring, Portable Network Monitoring*

PENDAHULUAN

Keamanan jaringan adalah segala aktivitas yang dirancang untuk melindungi kegunaan dan integritas jaringan dan data. Oleh karena itu, keamanan jaringan mencakup teknologi perangkat keras dan perangkat lunak. Keamanan jaringan yang efektif mengelola akses ke jaringan; diantaranya bagaimana memantau aktivitas jaringan, mendeteksi ancaman dan mempersiapkan sistem untuk menanggulanginya.

Evolusi *malware* adalah salah satu perkembangan paling signifikan dalam lanskap serangan pada 2017. Munculnya *cryptoworms ransomware* berbasis jaringan menghilangkan kebutuhan akan elemen manusia dalam meluncurkan kampanye *ransomware*. Dan untuk beberapa kasus, "hadiahnya" bukanlah tebusan, tetapi penghapusan sistem dan data, seperti *Nyetya* — *malware* penghapus yang menyamar sebagai *ransomware* (Cisco, 2018).

Perusahaan keamanan Symantec dalam laporannya menyebutkan *ransomware* dan *cryptojacking* digunakan untuk menghasilkan uang bagi para penjahat *cyber*. Tetapi pada tahun 2018 mengalami penurunan untuk pertama kalinya sejak 2013, secara keseluruhan *ransomware* turun 20 %, tetapi naik 12 % untuk target perusahaan. Dengan 90% penurunan nilai *cryptocurrency*, *cryptojacking* turun 52% pada 2018. Namun, *cryptojacking* tetap populer karena *barrier* masuk yang rendah dan *overhead* yang minim; Symantec memblokir empat kali lebih banyak serangan *cryptojacking* pada 2018 dibandingkan tahun sebelumnya (Symantec, 2019).

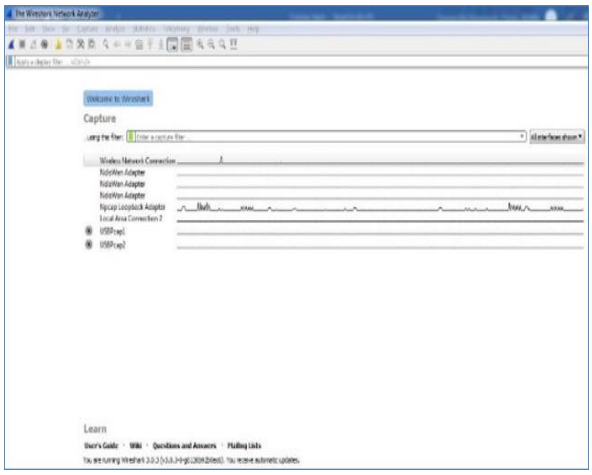
Selain isu keamanan yang semakin berkembang, tren mini komputer juga menjadi pilihan baru bagi pecinta teknologi. Raspberry Pi, komputer mungil seukuran kartu kredit, telah menangkap imajinasi para mahasiswa, pendidik, dan pemikir di seluruh dunia sejak muncul pertama pada 2012 (Samuel Gibbs, 2015; The New York Times, 2014).

Raspberry Pi, dapat digunakan untuk mengembangkan berbagai arsitektur karena memiliki koneksi dengan kamera, pemindai sidik jari, dan lain sebagainya melalui port USB (Halfacree & Upton, 2012). Selain itu juga memiliki port Ethernet untuk konektivitas Internet atau dapat dihubungkan ke *hotspot* Wi-Fi melalui *USB Wi-Fi adapter*. Raspberry Pi memiliki kemampuan untuk berinteraksi dengan dunia luar, dan telah digunakan dalam beragam proyek digital, mulai dari bidang seni musik hingga detektor utama untuk stasiun cuaca. Dalam tulisan ini, Raspberry Pi digunakan sebagai alat *portable* untuk memonitor jaringan. Sebagai studi kasus, kami melakukan implementasi di Credit Union Tunas Harapan, yang berkedudukan di Batam, Indonesia.

BAHAN DAN METODE

Implementasi dibagi dalam beberapa tahapan proses, diataranya, persiapan dan instalasi Raspberry Pi dengan *aplikasi network monitoring* Nagios dan *packet monitoring* Wireshark, penempatan perangkat, implementasi sistem, evaluasi temuan, analisis keamanan dan pelaporan.

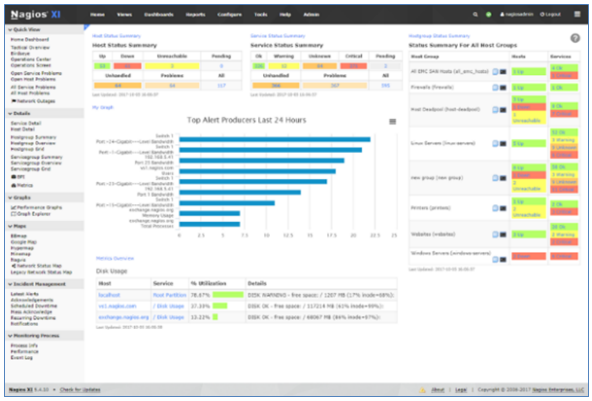
1) Wireshark, adalah penganalisa protokol jaringan yang terkemuka dan banyak digunakan dalam berbagai analisis jaringan. Wireshark memungkinkan kita melihat apa yang terjadi di jaringan pada tingkat mikroskopis dan merupakan standar *de facto* (dan sering *de jure*) di banyak perusahaan komersial dan nirlaba, lembaga pemerintah, dan lembaga pendidikan. Pengembangan Wireshark dilakukan berkat kontribusi sukarela para pakar jaringan di seluruh dunia dan merupakan kelanjutan dari proyek yang dimulai oleh Gerald Combs pada tahun 1998 (Wireshark Foundation, 2019). Pada penelitian ini Wireshark kami gunakan untuk memonitor paket data terkait aktivitas pengguna dan keamanan komputer dengan menggunakan *update* terakhir versi 3.



Sumber: Peneliti, 2019

Gambar 1. Interface Wireshark Versi 3

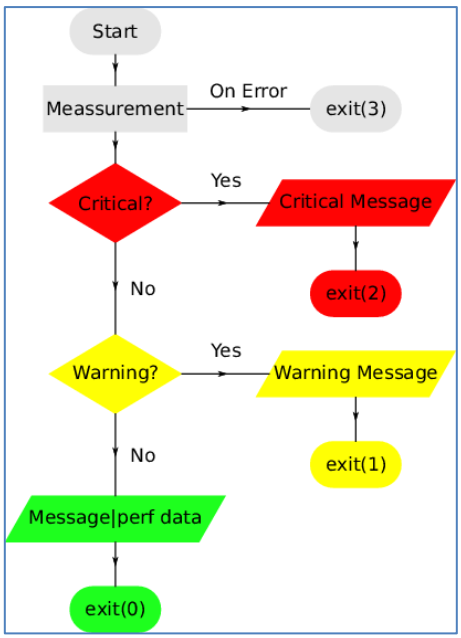
2) Nagios, adalah alat monitor jaringan; Nagios memantau seluruh infrastruktur TI untuk memastikan sistem, aplikasi, layanan, dan proses bisnis berfungsi dengan baik. Jika terjadi kegagalan, Nagios memiliki sistem *alert*, yang memungkinkan proses perbaikan sebelum memengaruhi proses bisnis, pengguna akhir, atau pelanggan (Nagios Enterprises, 2019; Renita & Elizabeth, 2018). Pada penelitian ini, kami menggunakan Nagios untuk memantau sumber daya yang tersedia sesuai dengan studi kasus yang kami lakukan.



Sumber: www.nagios.com, 2019

Gambar 2. Tampilan Dashboard Nagios Enterprise

Tugas utama nagios sebagai alat monitor dicapai melalui penggunaan *plugin*, program kecil yang bertanggung jawab untuk melakukan tes dan memproses *output*, karena sistem inti tidak melakukan tes apa pun. Status tes dijelaskan oleh satu dari empat status: *OK, WARNING, CRITICAL* atau *UNKNOWN* (Rafiullah Khan, 2018). Bagan alur tipikal dari *plugin* Nagios ditunjukkan pada Gambar 3.



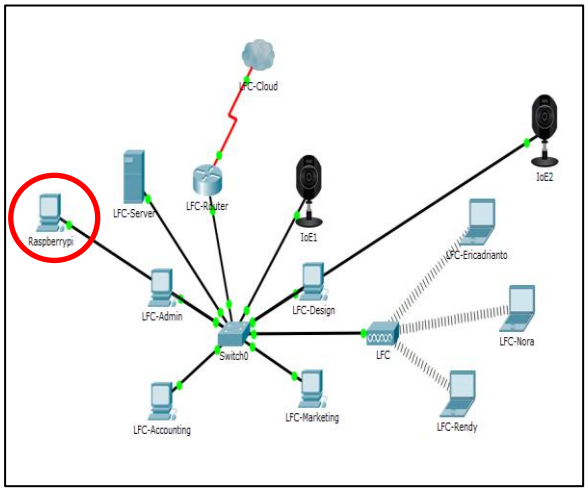
Sumber : Fernández, Pazos, Saborido, & Seco (2014)

Gambar 3. Basic flowchart generic Nagios plugin

Pada tahap awal *plugin*, jika perlu, menetapkan ambang batas untuk status *CRITICAL* dan *WARNING* baik dari argumen baris perintah atau dari serangkaian *default*. Langkah kedua adalah melanjutkan dengan pengukuran yang sebenarnya. Jika langkah ini gagal, sensor mengakhiri eksekusi dengan kode keluar 3. Hasilnya kemudian diperiksa terhadap rentang kritis dan peringatan

dan, tergantung pada hasilnya, *plugin* mencetak pesan yang tepat dan selesai dengan status keluar yang sesuai (Fernández, Pazos, Saborido, & Seco, 2014).

3) Penempatan Raspberry, Setelah kami melakukan analisis topologi jaringan di kantor Credit Union Tunas Harapan sebagaimana terlihat di Gambar 4, kami menempatkan perangkat pada switch utama dengan mengaktifkan *mode mirroring* pada interface port-port lainnya. *Port Mirroring* adalah mengonfigurasi *mirror port* untuk meng-c*opy* paket-paket dari satu *port* atau dari beberapa *port* ke antarmuka lokal untuk pemantauan lokal atau ke VLAN untuk pemantauan jarak jauh (Jian & Moore, 2007).



Sumber: Peneliti, 2019

Gambar 4. Penempatan Perangkat pada Topologi Jaringan

HASIL DAN PEMBAHASAN

Untuk dapat memberikan gambaran kinerja dari alat yang sudah dirancang, maka tahap selanjutnya eksperimen dilakukan dengan mengaktifkan *packet monitoring* atau *packet sniffing* Wireshark pada interface LAN dan mengaktifkan *network monitoring* Nagios secara bersamaan. *Packet sniffing* adalah proses menangkap setiap paket yang dikirim melalui jaringan dan menganalisis isinya. Seringkali, *packet sniffing* digunakan untuk memecahkan masalah jaringan atau untuk mengumpulkan statistik jaringan. *Network Monitoring* merupakan penggunaan sistem yang secara *continue* memonitor jaringan komputer, mampu mendeteksi komponen yang lambat atau gagal dan sistem akan memberi tahu administrator jaringan (melalui email, SMS atau alarm lainnya) jika terjadi kegagalan atau masalah lain. Pemantauan jaringan adalah bagian dari manajemen jaringan. Alat ini memudahkan seorang *network engineer* dalam melakukan manajemen jaringan yang besar terutama dengan *traffic* jaringan yang tinggi.

Proses *capture* dilakukan selama kurang lebih satu bulan pada kondisi jaringan sesuai pada studi kasus. Pemilihan waktu pada saat lalu-lintas jaringan tinggi menjadi pilihan utama. Data-data *packet-captured* yang telah dilakukan disimpan per hari untuk kemudian dilakukan analisis protokol dan paket data.

Sumber: Peneliti, 2019

Gambar 5. Network Monitoring Tool Portable

Analisis paket data dan monitoring jaringan menjadi acuan dalam analisis keamanan jaringan. Terutama aktivitas terkait autentikasi dan performa jaringan. Beberapa sampel dilakukan terkait analisis protokol jaringan yang populer juga terkait lalu-lintas.

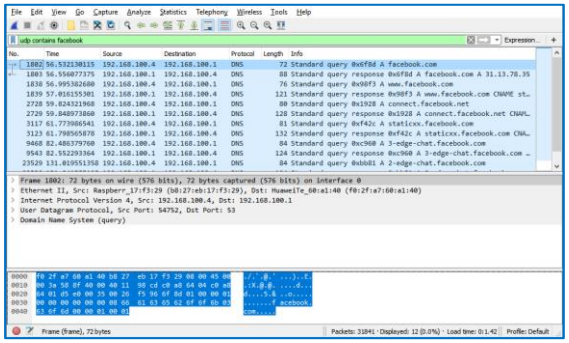
Dalam melakukan analisis, dua pendekatan utama yaitu *Packet Capture Monitoring* dan *Network Monitoring* menjadi bahan utama untuk selanjutnya melakukan analisis keamanan.

Topologi jaringan yang telah dibangun di kantor Credit Union Tunas Harapan menggunakan jaringan LAN dan memiliki sebuah switch dan router yang berfungsi untuk mengatur dan mengendalikan keseluruhan sistem fungsi jaringan dan juga bertindak sebagai penguat aliran data. IP Address lokal yang digunakan adalah kelas C dengan *network* 192.168.100.0/24. Sistem komunikasi antar pengguna menggunakan *client-server*.

A. Packet Caputure Monitoring

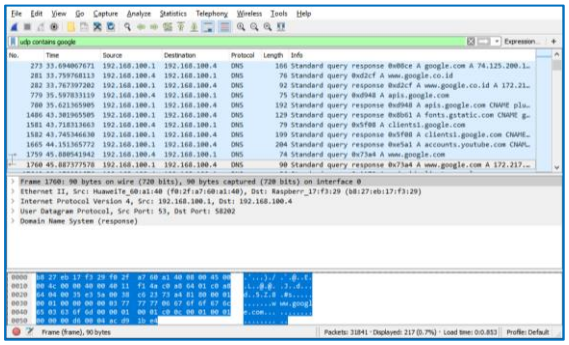
Packet Captured Monitoring merupakan hasil tangkapan Wireshark terhadap lalu lintas data pada jaringan. Sebagai sampel, berikut ini disajikan beberapa tangkapan *filter* data; Facebook, Google, Youtube, Credential. Pada Gambar 6 terpantau paket yang ter-*captured* pada jaringan sedang melakukan aktivitas yang berhubungan dengan Facebook. *Filter* yang kedua memperlihatkan *client* dalam jaringan membuka Google dapat dilihat pada Gambar 7 dan *filter* ketiga mengetahui adanya komputer client sedang

membuka Youtube, dapat dilihat pada Gambar 8. Hal ini perlu disajikan memastikan bahwa perangkat yang terpasang mampu melakukan monitoring pada semua client dengan diaktifkannya *mode monitoring* pada *manageable switch* kantor.



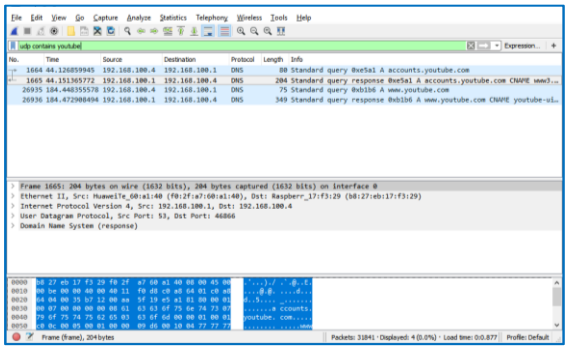
Gambar 6. Capture Filter Facebook

Pada Gambar 6 terpantau dalam trafik jaringan aktivitas node client dengan halaman Facebook. Dalam aktifitas yang di-*filter* dengan *filter* UDP terlihat *query Domain Name Service* (DNS) ketika jaringan lokal mengakses server Facebook melalui *gateway* jaringan kantor.



Gambar 7. Capture Filter Google

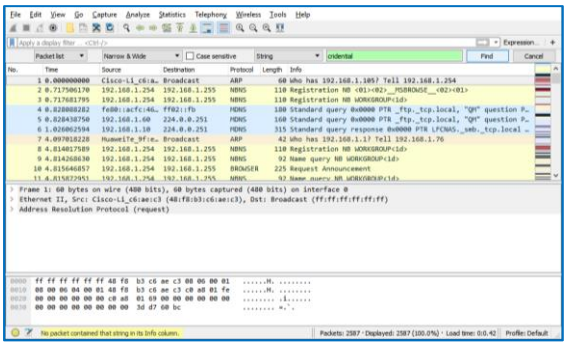
Demikian juga pada Gambar 7, Wireshark memantau aktivitas *query* DNS komputer client ketika mengakses *server* Google melalui *gateway* jaringan lokal.



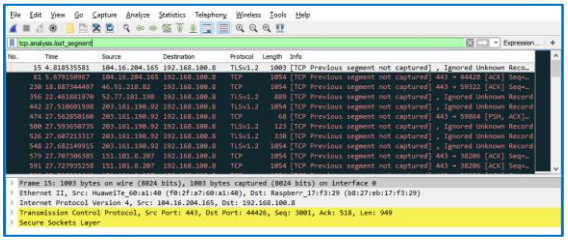
Gambar 8. Capture Filter Youtube

Pada Gambar 8 terlihat filter yang dilakukan dengan protokol UDP pada aktivitas *query* DNS komputer *client* yang berinteraksi dengan *node/ server* Youtube.

Filter selanjutnya menggambarkan paket data aktivitas *credential* pada Gambar 9. *Credential* adalah sertifikat *login* yang mencantumkan konten identitas (ID) dan *password* pengguna.



Gambar 9. Capture Filter Credential



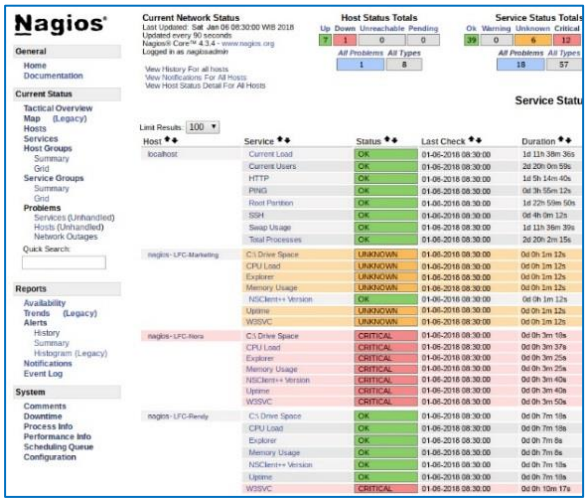
Gambar 10. Capture Filter Bad TCP

Sedangkan pada Gambar 10 adalah contoh *Bad TCP*. Ada dua faktor yang mempengaruhi terjadinya *Bad TCP* yang pertama adalah saat terjadi pencarian alamat, tetapi alamat yang dicari tidak dapat ditemukan, dan yang kedua terjadi pada jaringan lokal dalam kondisi *down* sehingga terjadinya *Bad TCP* atau bisa dapat disebut sebagai *packet loss.*

B. Network Monitoring

Tool Network Monitoring Nagios yang telah aktif, mampu melakukan monitor jaringan. Pada Gambar 11 dapat kita temukan bahwa terpantau adanya *user* yang tidak terkoneksi dalam jaringan; Nagios memberikan kode dengan *background* warna merah. Ada juga yang berwarna jingga dengan notifikasi *service* dan muncul kata "*unknown*". Secara umum ada dua kemungkin atas masalah tersebut, yang pertama adalah setelah konfigurasi aplikasi Nagios dalam Raspberry belum 100% jalan sempurna perlu *restart*, dan kemungkinan kedua adalah pada PC *client* tidak membuka atau memberi akses program Nagios berjalan dalam jaringan. Dalam kasus ini adalah

anti virus pada PC client mem-*block* program Nagios.



Sumber: Peneliti, 2019

Gambar 11. Status Monitoring Nagios

Gambar 11 selain menunjukkan status monitoring, juta memberikan gambaran secara rinci aktivitas protokol yang sedang berjalan pada setiap komputer *client.*

Status lengkap dalam pengujian selama lima hari dapat dilihat pada Tabel 1 di bawah ini.

Tabel 1. Status Monitoring Nagios

TGL	User	Sesi1	Sesi2	Sesi3	Sesi 4	Sesi5
6 Mei	Client 1	OK	OK	OK	OK	OK
	Client 2	OK	OK	OK	OK	OK
	Client 3	OK	OK	OK	OK	OK
	Client 4	OK	OK	OK	OK	OK
	Client 5	*UNKNOWN*	OK	OK	OK	OK
	Client 6	*CRITICAL*	*CRITICAL*	*CRITICAL*	OK	OK
	Client 7	OK	OK	OK	OK	OK
7 Mei	Client 1	OK	OK	OK	OK	OK
	Client 2	OK	OK	OK	OK	OK
	Client 3	*CRITICAL*	*CRITICAL*	OK	OK	OK
	Client 4	OK	OK	OK	OK	OK
	Client 5	OK	OK	OK	OK	OK
	Client 6	OK	OK	OK	OK	OK
	Client 7	OK	OK	OK	OK	OK
8 Mei	Client 1	OK	OK	OK	OK	OK
	Client 2	OK	OK	OK	OK	OK
	Client 3	OK	*CRITICAL*	*CRITICAL*	OK	OK
	Client 4	OK	OK	OK	OK	OK
	Client 5	OK	OK	OK	OK	OK
	Client 6	*CRITICAL*	*CRITICAL*	OK	OK	OK
	Client 7	OK	OK	OK	OK	OK
9 Mei	Client 1	OK	OK	OK	OK	OK
	Client 2	OK	OK	OK	OK	OK
	Client 3	OK	OK	OK	OK	OK
	Client 4	OK	OK	OK	OK	OK
	Client 5	OK	OK	OK	OK	OK
	Client 6	OK	OK	OK	OK	OK
	Client 7	OK	OK	OK	OK	OK

Sumber: Peneliti, 2019

C. Network Security Analysis

Berdasarkan hasil monitor baik dari *tool packet monitoring* Wireshark maupun *tool network monitoring* Nagios, kedua aplikasi tersebut yang telah di-*embed* dalam Raspberry dapat berjalan dengan lancar. *Network Monitoring tool* mampu melakukan monitoring *packet* data dalam lalu lintas jaringan, demikian juga mampu melakukan pemantauan status jaringan secara menyeluruh. Tabel 2 menunjukkan total *packet loss* yang terjadi pada jaringan selama periode waktu tersebut.

Filter key tcp contains pada sistem mampu untuk mendapatkan filter paket aktivitas website yang perlu dianalisis, seperti *tcp contains* Facebook atau Google atau Youtube. Aktivitas autentikasi misalnya *user login* ke suatu website pun bisa terpantau melalui aktivitas *sniffing* yang mampu dilakukan Wireshark, sehingga dapat dilakukan evaluasi terkait kebijakan keamanan yang akan diterapkan.

Sistem juga mampu memantau atau memonitor *resource* jaringan. Hal ini sangat penting terkait isu keamanan sistem agar proses mitigasi keamanan cepat dilakukan.

Tabel 2. *Packet Loss*

Minggu	*Total Paket*	*Paket Loss*	*Paket Loss %*
Minggu 1	2587	27	1.044%
Minggu 2	1969	62	3.149%
Minggu 3	31841	747	2.346%
Minggu 4	2340	0	0%

Sumber: Peneliti, 2019

KESIMPULAN

Pemanfaatan mini computer Raspberry Pi dalam rancang bangun arsitektur *Network Monitoring Portable* mampu diimpelementasikan dan dapat berjalan dengan baik. Sistem mempunyai keunggulan mobilitas dan portabilitas dapat dipindah tempat kan sesuai kondisi topologi suatu jaringan.

Portabilitas sistem memampukan implementasi tanpa harus mengganggu sistem yang sedang berjalan bila akan dilakukan evaluasi atau audit keamanan jaringan.

REFERENSI

Cisco. (2018). *Cisco 2018 Annual Cybersecurity Report*. San Jose.

Fernández, V., Pazos, A., Saborido, J., & Seco, M. (2014). Arduino and Nagios integration for monitoring. *Journal of Physics: Conference Series*, *513*(TRACK 6). https://doi.org/10.1088/1742-6596/513/6/062015

Halfacree, G., & Upton, E. (2012). *Raspberry Pi User Guide*. https://doi.org/10.1007/s13398-014-0173-7.2

Jian, Z., & Moore, A. (2007). Traffic trace artifacts due to monitoring via port mirroring. *Fifth IEEE/IFIP Workshop on End-to-End Monitoring Techniques and Services, E2EMON'07*, (May 2014). https://doi.org/10.1109/E2EMON.2007.375317

Nagios Enterprises, L. (2019). Overview Nagios. Retrieved July 31, 2019, from https://www.nagios.org/about/overview

Rafiullah Khan, S. U. (2018). Design and implementation of an automated network monitoring and reporting back system. *Journal of Industrial Information Integration*, *9*, 23–34. https://doi.org/https://doi.org/10.1016/j.jii.2017.11.001

Renita, J., & Elizabeth, N. E. (2018). Network's server monitoring and analysis using Nagios. *Proceedings of the 2017 International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2017*, *2018-January*(March), 1904–1909. https://doi.org/10.1109/WiSPNET.2017.8300092

Samuel Gibbs. (2015). Raspberry Pi becomes best selling British computer | Technology | The Guardian. Retrieved June 19, 2017, from https://www.theguardian.com/technology/2015/feb/18/raspberry-pi-becomes-best-selling-british-computer

Symantec. (2019). *2019 Internet Security Threat Report*. Mountain View.

The New York Times. (2014). Creativity Unleashed, With the Help of a Little Pi. Retrieved July 31, 2019, from https://www.nytimes.com/2014/06/26/technology/personaltech/a-breakdown-of-the-raspberry-pi-computer.html

Wireshark Foundation. (2019). *Wireshark User's Guide Version 3.1.0*. Retrieved from x