RANCANG BANGUN SISTEM PENGUKURAN TINGKAT KEAMANAN KOMPUTER PADA JARINGAN LAN

Ahmad Riyandi[1], Ade Nurhayati[2]
[1,2]Akademi Teknik Telekomunikasi Sandhy Putra Jakarta
[1,2] Jalan Daan Mogot KM 11, RT.1/RW.4, Cengkareng, Daerah Khusus Ibu Kota Jakarta 1710, Indonesia
Ariyandi1999@gmail.com[1], adenurhayati@akademitelkom.ac.id[2]

Abstrak - Perkembangan teknologi pada jaringan komputer saat ini semakin cepat, dengan meningkatnya kebutuhan akses jaringan yang efesien, stabil serta keamanan komputer yang handal. Penilitian ini berjudul **RANCANG BANGUN SISTEM PENGUKURAN TINGKAT KEAMANAN KOMPUTER PADA JARINGAN LAN** bertujuan untuk mengukur tingkat keamanan komputer dari serangan jaringan pada server/komputer seperti *port scanning* yang tidak diketahui kegunaannya. Salah satu teknik keamanan komputer *scanning port* yang merupakan mekanisme untuk melindungi sistem *internal* menggunakan konfigurasi OS *Linux* dengan tools NMAP pada perangkat *Raspberry Pi,* untuk mengidentifikasi *via telegram* dan tampilan pada WEB bahasa pemograman PHP pada *port* komputer yang terbuka adalah *port* yang sedang di gunakan atau *port* yang tidak di ketahui kegunaannya dari serangan pihak-pihak lain yang ingin memasuki sistem tanpa izin. Dengan adanya sistem ini dapat meminimalasi celah tingkat keamanan pada komputer khususnya di jaringan LAN *(Local Area Network).*

Kata kunci: *Keamanan Komputer, NMAP, PHP, Telegram, Jaringan LAN.*

Abstract - *The development of technology in computer networks is currently getting faster, with the increasing need for network access that is efficient, stable and reliable computer security. This research entitled* ***DESIGN AND DEVELOPMENT OF COMPUTER SECURITY LEVEL MEASUREMENT ON LAN NETWORKS*** *aims to measure the level of computer security from network attacks on servers / computers such as port scanning whose use is unknown. One of the scanning port computer security techniques which is a mechanisme for protecting the internal system using the Linux OS configuration with the NMAP tools on the Raspberry Pi device, to identify via telegram and display on the PHP programming language WEB on the open computer port is the port that is being used or the port which is not known its usefulness from attacks by other parties who want to enter the system without permission. With this system, it can minimize security level gaps on computers, especially in LAN (Local Area Network) networks.*

Keywords: *Computer Security, NMAP, PHP, Telegram, Local Area Network*

1. PENDAHULUAN

Menurut Tanenbaum “Jaringan komputer merupakan kumpulan dari perangkat keras dan perangkat lunak di dalam suatu sistem yang memiliki aturan tertentu untuk mengatur seluruh anggotanya dalam melakukan aktivitas komunikasi satu komputer yang terkoneksi ke jaringan menjadi satu node dari jaringan tersebut. Sedangkan *host* secara umum diartikan sebagai komputer yang terkoneksi ke jaringan yang dapat memberikan layanan jaringan (*network service)”.*

Menurut Ikhwan “Keamanan jaringan sangat vital bagi sebuah jaringan komputer kelemahan-kelemahan yang terdapat pada jaringan komputer jika tidak dilindungi dan dijaga dengan baik akan menyebabkan kerugian berupa kehilangan data, kerusakan sistem *server*, tidak maksimal dalam melayani *user* atau bahkan kehilangan aset-aset berharga institusi”.

Pengukuran tingkat keamanan komputer yang sering dilupakan keamanannya baik dikantor, sekolah, dan tempat umum lainnya yang menggunakan jaringan LAN adalah celah *port* terbuka. Padahal disitulah langkah awal atau pintu pertama penyusup bisa menyerang masuk kedalam jaringan, tentu jika itu terjadi penyusup dapat mengambil data-data dan menggangu kinerja pada jaringan komputer. Mulai dari bug, worm atau virus dan jenis kejahatan lainnya sering ditemukan di *WEB* yang sering tersambung dengan host/client di jaringan internet.

Semakin celah tertutup maka tingkat kejahatan pun semakin sedikit.

Tidak ada satu pun sistem keamanan yang sempurna, *scanning port* digunakan untuk meminimalisasi celah keamanan pada *port* komputer dan memeriksa *port* yang terbuka adalah *port* yang sedang digunakan atau *port* yang tidak diketahui kegunaannya. Adapun judul yang diangkat oleh penulis adalah **RANCANG BANGUN SISTEM PENGUKURAN TINGKAT KEAMANAN KOMPUTER PADA JARINGAN LAN.**

1.1 Metode Pengujian

Uji coba sistem dan pengukuran

Pada tahap ini merupakan uji coba sistem keamanan *scanning port* untuk mengukur tingkat keamanan komputer standar ISO 27001. Dilakukan sekali pengujian untuk satu komputer atau lebih yang sudah tersambung dengan jaringan bersama *raspberry*, namun untuk mendapatkan hasil yang akurat dilakukan secara berulang-ulang setiap 15 menit sekali dalam sehari, dengan bentuk tabel data monitoring pada *web* dan *notifikasi via telegram* khusus untuk komputer tidak aman beresiko tinggi.

2. DASAR TEORI

2.1 Pengertian Keamanan Komputer

Keamanan komputer adalah tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab. [3]

Keamanan komputer merupakan yang sangat penting, seiring dengan pentingnya informasi yang terkandung pada jaringan. *Port scanning* merupakan langkah awal serangan terhadap komputer. Dari keberhasilan melakukan *port scanning*, penyerang dapat melanjutkan serangan lanjutan ke jaringan komputer. [1]

2.2Port Scanning

Port Scanning merupakan sebuah teknik *hacking* dimana seorang penyerang dapat membobol *website* atau *web server* melalui *port* yang terbuka untuk dieksekusi. Berdasarkan data dari Pemerintah Meksiko, Amerika Serikat dan Rusia pada tahun 1999-2013, yang melakukan *survey* mengenai ancaman *cybercrime* yang sering terjadi pada *Port Scanning*, *carding*, *Hacking Web Site*, dan penyadapan transmisi maka teknik *Port Scanning* adalah *bug* yang kedua paling banyak ditemukan pada *website-website* yang berada di *Internet*. [2]

2.3Jaringan *Local Area Network* (LAN)

LAN adalah bentuk jaringan komputer lokal, yang luas areanya sangat terbatas. Biasanya diterapkan untuk jaringan komputer rumah, laboratorium, perusahaan dimana masing-masing dapat saling berinteraksi, bertukar data dan dapat menggunakan peralatan bersama seperti *printer*, media yang digunakan untuk LAN dapat berupa (UTP atau BNC) maupun *wireless*.

2.4 Raspberry Pi 3 Model B

Raspberry Pi ditemukan pertama kali di *Universitas of Cambridge Laboratory pada tahun 2006, Raspberry Pi* adalah komputer mini yang dirancang dan diproduksi di *Inggris* dengan tujuan awal untuk menyediakan perangkat komputasi yang murah untuk pendidikan. [6]

Raspberry Pi3 ini adalah sebuah jenis *Single Board* untuk komputer. Serta pada dasarnya *Raspberry Pi* ini berfungsi sebagai layaknya sebuah komputer yang mempunyai ukuran lebih kecil, maka dari itu disebut dengan *Single Board Computer*. Sebenarnya jenis *Raspberry Pi3* ini adalah jenis ketiga dan jenis *Raspberry Pi3* ini merupakan penyempurnaan jenis yang *Raspberry Pi2*.

Gambar 1 Raspberry pi 3 model B

alasan penulis menggunakan *raspberry pi* 3 model B, dengan harga yang lebih murah dari *single board computer* yang lain, dilengkapi dengan *support OS linux* dan geany untuk konfigurasi *php* melakukan *scanning port* yang digunakan untuk proyek akhir ini.

2.5 Operating System LINUX

Linus Benedict Torvalds dilahirkan pada 28 desember 1969 di Helsinki, ibu Kota Negara Finland. Beliau telah menciptakan Linux *(LinusUnix) open source kernel* gratis, *kernel* adalah jantung dari sistem operasi yang menangani komunikasi antara pengguna dengan *hardware,* dan kini berperan sebagai pengelola proyek khususnya sistem keamanan. [6]

Adapun *tools* yang digunakan dalam keamanan komputer pada sistem proyek akhir ini adalah:

1. *Firewall* adalah suatu mekanisme untuk melindungi keamanan jaringan komputer dengan menyaring paket-paket data yang keluar dan masuk di jaringan, apabila paket baik (paket memiliki izin) diperbolehkan masuk di jaringan, namun apabila paket jahat (paket tidak memiliki izin) maka tidak diperbolehkan masuk di jaringan. *Firewall* juga berfungsi untuk mengontrol akes terhadap siapa saja yang memiliki akses terhadap jaringan pribadi dari pihak luar, melakukan *autentikasi* terhadap akses dan mencatat semua kejadian di jaringan. [8]

2. IDS *(Intrusion Detection System)* merupakan *software* ataupun dapat berbentuk *hardware* yang dapat melihat pola dari serangan-serangan yang terdapat pada jaringan komputer khusus nya jaringan LAN. Pola tersebut berupa paket data yang lewat terindentifikasi oleh IDS sebagai paket yang mengandung serangan ataupun ancaman pada sebuah jaringan. *Snort,* Martin Roesch merupakan orang yang pertama kali menulis *snort* dan sekarang dikelola oleh Sourcefire, Roesch bertindak sebagai pendiri dan CTO *(Chief of Technical officer). Snort* merupakan sebuah alat yang berfungsi untuk mencegah sebuah instruksi atau serangan pada jaringan. Dalam pratiknya *snort* sangat handal dalam membentuk *logging* paket-paket dan analisis trafik-trafik secara *real time* dalam jaringan yang berbasis TCP/IP. [9]

3. Nmap *(Network Mapping)* adalah alat yang digunakan untuk mengetahui *service* yang diberikan oleh suatu komputer melalui *scanning port.* Nmap banyak digunakan penyerang untuk mengetahui *port* komputer korban yang aktif, kemudian menggunakan *port* yang aktif tersebut untuk masuk ke sistem komputer korban. Namun untuk sistem penulis ini Nmap digunakan untuk mengetahui *port* yang aktif sebagai parameter tingkat keamanan komputer.

2.6 PHPMyadmin

PHPMyadmin Adalah Aplikasi untuk mengolah basis data yang berbasis web.

Aplikasi ini sangat membantu untuk mengelolah database dalam pembuatan aplikasi bersama PHP. [10]

2.6 Telegram

Gambar 2 Logo Telegram
(Sumber: https://telegram.org)

Telegram merupakan aplikasi pengirim pesan berbasis internet yang dibuat oleh Nikoali dan Pavel Durov. Aplikasi chatting ini tersedia untuk android, Ios, windows Phone, Windows NT, macOS, dan Linux. Pengguna pun dapat mengirim pesan dan bertukar foto, video, stiker, audio dan file jenis apapun. Telegram dapat dijalankan pada beragam perangkat dari sistem operasi, telepon genggam, komputer dan perangkat pintar komputer serupa lainnya. Cara mendaftar telegram sangat mudah, cukup dengan mengisi nomor HP aktif dan melakukan verifikasi code melalui SMS atau panggilan telepon.
Bot adalah sebuah mesin program komputer yang melakukan pekerjaan tertentu secara otomatis. Bot dibuat untuk meningkatkan pekerjaan manusia, dalam kaitannya bot dengan telegram tinggal menulis kata kunci yang kita ingin cari, maka secara otomatis akan keluar pada aplikasi telegram. Khusus pada penelitian ini bot telegram di pakai untuk hasil notifikasi tingkat keamanan komputer yang sudah dilakukan *scanning port* dengan tingkat keamanan komputer dibawah 50%.

2.7 PHP

PHP *(Personal Home Page Tools)* dikembangkan oleh Rasmus Lerdofr, merupakan bahasa pemrograman pada sisi *server* yang memperbolehkan *programmer* menyisipkan perintah – perintah perangkat lunak *web server* akan diproses sebelum perintah itu dikirimkan *client*, kemudian diproses oleh *server* dan akan ditampilkan dalam bentuk *web*. Sesuai dengan fungsinya yang berjalan disisi server maka PHP adalah bahasa pemrograman yang digunakan untuk membangun teknologi *web application*. [11]

2.8 MySQL

MySQL adalah tampilan salah satu program *database* gratis yang cukup terkenal dan handal. MySQL merupakan *software database* yang popular di OS Linux maupun *Windows*. MySQL dapat dikatakan lebih unggul dibanding perangkat lunak *database* lainnya, MySQL merupakan perkembangan dari SQL *(Structured Query Language)*. SQL adalah sebuah konsep pengoperasian *database*, terutama untuk pemilihan atau seleksi dan pemasukan data, yang memungkinkan pengoperasian data dikerjakan dengan mudah secara otomatis. [11]

2.9 Client Server

Client adalah komputer-komputer yang menerima atau menggunakan fasilitias yang disediakan *server* dan *server* adalah sebuah perangkat yang mampu menyediakan data atau layanan dapat di akses oleh *client* dalam jaringan*. Client Server* adalah pembagian tugas antara *server* dan *client, client* mempunyai izin akses menuju *server* yang saling berkomunikasi ketika hendak mengakses server untuk suatu jaringan. [12]

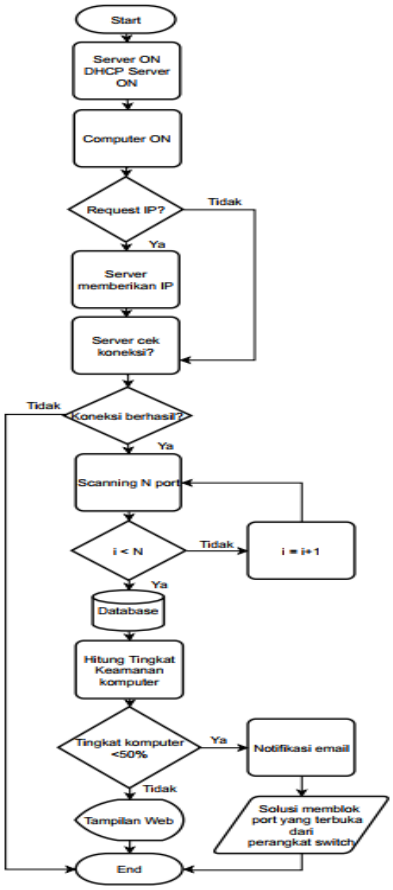
2.10 Web Server

Web server adalah sebuah perangkat lunak *server* yang berfungsi melayani koneksi *transfer* data dalam bentuk prorokol *Hyper Text Transfer Protocol* atau *Hyper Text Transfer Protocol Secure* dari *client* melalui *web browser* dan

mengirimkan kembali hasilnya dalam bentuk halaman-halaman *web* yang umumnya berbentuk dokumen PHP/HTML. [2]

Khusus pada penilitian ini *client* meminta permintaan hasil data monitoring tingkat keamanan komputer, apakah komputer yang sedang digunakan aman atau tidak, hasilnya ditampilkan pada tampilan *web* setelah di *scanning port*.

3. PERANCANGAN SISTEM



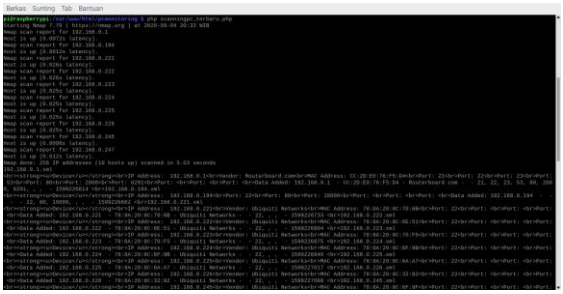
Gambar 3 Flowchart Perancangan Sistem

Pada *flowchart* di atas dapat dijelaskan mulai dengan kondisi *server ON* dan DHCP *server ON* setelah itu memastikan *computer on sebagai input* untuk mengecek *computer* mana yang akan di *scan,* sebelum terhubung dan diproses oleh *server* tentu harus meminta *request* IP *address* secara *dynamic* atau secara *static,* jika menggunakan *dynamic, server* langsung memberikan IP address untuk dapat terkoneksi dalam jaringan, jika menggunakan *static, server* langsung cek koneksi karena IP tersebut sudah terdaftar secara *permanent.* Setelah itu server mengecek koneksi *computer* yang telah diberikan IP *dynamic*, maksud dari *server* cek koneksi adalah apabila komputer yang tidak terkoneksi dengan jaringan maka tidak dapat melakukan *scanning port* dan jika komputer sudah bisa terkoneksi dengan jaringan maka komputer tersebut dapat melakukan *scanning port.*

Jika komputer sudah terkoneksi dalam sebuah jaringan, maka akan dilakukan proses *scanning port* yang diminta oleh *client (admin/user),* I < N nilai index kurang dari N=100 *port* yang akan discan secara berulang-ulang untuk mendapatkan hasil yang lebih akurat terhadap *port* terbuka yang tidak diketahui kegunaannya, setelah proses *scanning* selesai maka data akan diproses dan disimpan ke dalam *database* dengan parameter aman, dengan bantuan *tools scanning port, firewall,* IDS *snort* yang sudah terpasang pada jaringan akatel setelah itu sistem akan menghitung tingkat keamanan komputer apakah komputer keadaan aman atau tidak aman, dari *server* hasil *output* itu akan di tampilkan dalam bentuk data monitoring dan tingkat keamanan komputer pada *web* dan *notifikasi* telegram ke *administrator,* namun hanya komputer yang tingkat keamanannya <50% saja masuk ke dalam *notifikasi telegram* dan solusinya akan memblok atau menutup *port* yang tidak diketahui kegunaannya disitulah sistem ini berjalan untuk memastikan pengukuran tingkat keamanan komputer.

4. HASIL DAN PEMBAHASAN

4.1 Proses Scanning Port



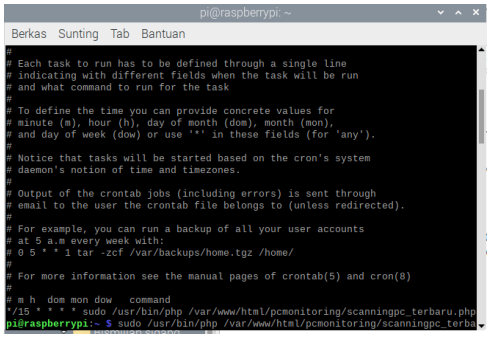
Gambar 4 proses scanning port pada terminal raspberry

Pada gambar 4 merupakan tampilan saat melakukan scanning port dengan peritah **php.scanningpc_terbaru.php.** Penulis menggunakan perintah “nmap –sP” (PING Scan) pada *geany raspberry pi* untuk mengetahui IP

atau komputer mana saja yang tersambung dan keadaan hidup untuk dilakukan scanning port, apabila komputer mati dan tidak tersambung dengan jaringan maka tidak dilakukan scanning. Ditemukan 10 host yang tersambung dengan ip jaringan 192.168.0.0/24 dan 192.168.1.0/24 akan di parsing dan disimpan ke dalam *database.*

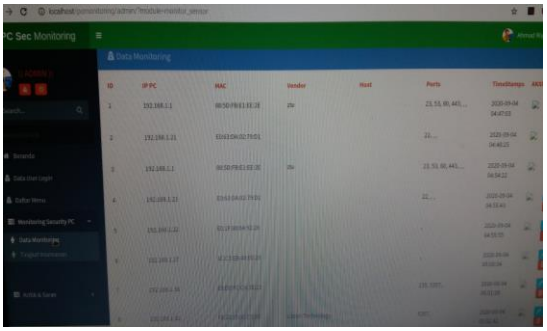
4.2 Menjadwalkan Cron jobs

Cara kerja *cron jobs* untuk menjadwalkan skrip dan program basis waktu pemberitahuan secara berulang dengan tata letak entri enam komponen setiap menit, jam, hari dalam sebulan, bulan, hari dalam seminggu seperti yang ditunjukkan pada gambar 4.17. proses untuk mengatur berapa kali melakukan *scanning por*t dengan otomatis, jalankan perintah **$ crontab –e** pada terminal *raspberry*, lalu pilih editor **nano** seperti yang ditunjukkan pada gambar 4.15. penulis mengatur setiap 15 menit dapat melakukan *scanning* pada port komputer aktif yang tersambung dengan jaringan.



Gambar 5 Pengaturan Waktu Perintah Cronjob

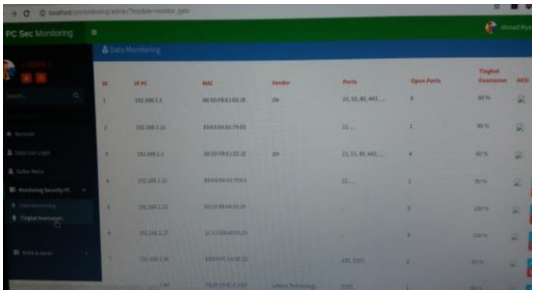
Sebagai contoh penelitian ini dilakukan *scanning port* setiap 15 menit dengan perintah seperti yang penulis contohkan **15 * * * * /usr/bin/php/var/www/html/pcmonitoring/scanningpc_terbaru.php**. Skrip dan program ditulis di bawah **# m h dom mon dow command**. Jika ingin membuka file tanpa mengedit jalankan **$ crontab –l.**



Gambar 6 Data Monitoring Komputer

1. Buka pada menu **monitoring security pc**, lalu buka **data monitoring** yang akan melihat hasil *scanning* port mulai dari IP, MAC address, Vendor, host, port yang terbuka, dan tahun-tanggal-bulan serta waktu hasil scanning port yang dilakukan setiap 15 menit setelah *scanning* pertama. Seperti yang ditunjukkan pada gambar 6.

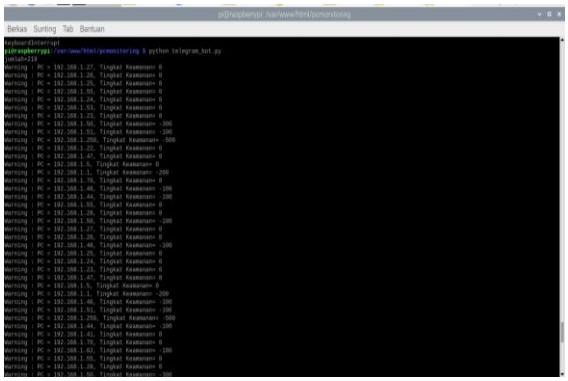
2. Buka pada menu **monitoring security pc**, lalu buka tampilan **tingkat keamanan**, seperti yang ditampilkan pada gambar 7 mulai dari IP, MAC address, vendor, *port*, jumlah *port* terbuka dan *presentase* tingkat keamanan komputer. Hasil *scanning port* dapat dimonitoring pada *web* ini yang sudah dibuat konfigurasi pada *raspberry pi.*



Gambar 7 Tingkat Keamanan Komputer

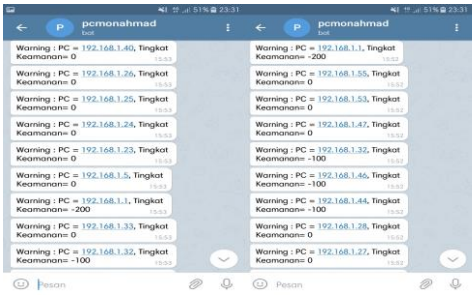
4.3 Notifikasi Kondisi Tingkat Keamanan Komputer

Pada gambar 8 Proses pengiriman notifikasi dari raspberry dengan perintah **$ pyhhon telegram_bot.py** yang dikirim notifikasi via telegram dari hasil *scanning port* setiap 15 menit.



Gambar 8 Proses Notifikasi Telegram

Notifikasi *via telegram* hanya komputer yang tingkat keamanannya di bawah 50%, dari hasil perhitungan yang sudah dilakukan *scanning port* dan tersimpan ke dalam *database* pada jaringan yang tersambung dengan *raspberry*, secara otomatis notifikasi masuk ke *bot telegram* yang sudah dibuat oleh penulis dengan nama **pcmonahmad**. Seperti yang ditunjukkan pada gambar 9



Gambar 9 Tingkat Keamanan Komputer

4.4 Analisa Kondisi Tingkat Keamanan Komputer

Perhitungan persentase kondisi tingkat keamanan komputer dapat dilihat pada tabel 1 Dimana tabel berisikan IP perangkat, jumlah port yang terbuka, jumlah port target yang ditentukan, dan tingkat keamanan komputer merupakan analisa proses pada pengukuran tingkat pengukuran berdasarkan standar ISO 27001.

Tabel 1 Pengukuran Tingkat Keamanan Komputer

IP Perangkat	Jumlah Port Terbuka	jumlah Port Target	Port Terbuka	Tingkat Keamanan
192.168.1.1	4	10	23,53,80,443	60%
192.168.1.21	1	10	22	90%
192.168.1.22	0	10	'	100%
192.168.1.27	0	10	'	100%
192.168.1.36	2	10	135, 5357	80%
192.168.0.1	7	10	21,22,23,53,80,2000,8291	30%
192.168.0.194	3	10	22,80,10000	70%
192.168.0.221	1	10	22	90%
192.168.0.222	1	10	22	90%
192.168.0.223	1	10	22	90%

Pengujian sebelumnya penulis menentukan jumlah *port* target sebanyak 1000 *port* dan 100 port, karena jaringan akatel terbilang aman diantaranya ada parameter aman seperti *firewall*, IDS Snort dan jenis keamanan yang lain sudah memenuhi standar pada umumnya membuat tingkat keamanan komputer tidak ada di bawah 50%. Sehingga untuk melakukan notifikasi dibawah jumlah *port* target, penulis menurunkan jumlah *port* target menjadi 10 *port* untuk menampilakan hasil *notifikasi via telegram* seperti yang ditunjukkan pada gambar 9.

Setelah hasil pengukuran selesai maka setiap port memiliki kerentanan yang terjadi apabila tidak dilakukan pemeliharaan keamanan yang baik, seperti contohnya yang tinjukkan pada tabel 2 Setiap masalah pasti memiliki solusi untuk menyelesaikannya, keamanan seperti firewall yang berfungsi memblok apabila alamat IP dipindai melebihi waktu yang ditentukan secara otomatis terblokir, Port Knocking berfungsi untuk membuka port eksternal pada *firewall* jarak jauh, untuk membuka port harus mengetuk (di knock) port lain secara urut yang valid jika urutan gagal maka port yang di incar tidak akan terbuka.

Port spoof membuat interprestasi hasil pemindaian port menjadi sulit, membuat keluar tugas mengindentifikasi port yang terbuka menjadi pekerjaan yang sangat lambat, port spoof menjawab kembali dengan SYN-ACK untuk semua upaya koneksi masuk oleh pemindai port. Port spoof juga dapat menyetel deskripsi layanan port TCP palsu, port spoof akan meniru layanan yang berjalan disemua port terbuka dilaporkan, tetapi deskripsi ini akan dibuat secara acak dari *database* tanda tangan deskripsi layanan validnya sendiri. Hasilnya menipu mereka, karena mereka berfikir bahwa port tersebut terbuka dan layanan tertentu sedang berjalan diatasnya, padahal kondisi ini tidak benar.

Tabel 2 Solusi Pengukuran Tingkat Keamanan Komputer

Port	Fungsi Port	Rentan Terjadi (Bahaya)	Solusi
21	File Transfer Protocol berfungsi untuk tukar menukar file dalam satu network.	Pemindaian port	Pemfilteran Firewall, Port Spoof dan Port Knocking
22	Secure Shell (SSH) berfungsi untuk melakukan tugas yang bisa diakses dari jarak jauh.	Pemindaian port	Pemfilteran Firewall, Port Spoof dan Port Knocking
23	Telnet	Pemindaian port	Pemfilteran Firewall, Port Spoof dan Port Knocking
25	SMTP (Simple Mail Transfer Protocol)	Pemindaian port	Pemfilteran Firewall, Port Spoof dan Port Knocking
53	Domain Name System berfungsi untuk menerjemahkan alamat IP berupa angka menjadi huruf	Pemindaian port	Pemfilteran Firewall, Port Spoof dan Port Knocking
80	Hypertext Transfer Protocol untuk terhubung ke internet.	Pemindaian port	Pemfilteran Firewall, Port Spoof dan Port Knocking
110	POP3 (Post Office protocol)	Pemindaian port	Pemfilteran Firewall, Port Spoof dan Port Knocking
135	Windows RPC (Remote Procedure Call) untuk mengakses prosedur yang berada di komputer lain	Pemindaian port	Pemfilteran Firewall, Port Spoof dan Port Knocking
443	Hypertext Transfer Protocol Scurre untuk men-enkripsi dan analisa keamanan data melalui internet	Pemindaian port	Pemfilteran Firewall, Port Spoof dan Port Knocking
445	file sharing printer dan sharing resources.	Worm dan virus	Memasang software anti virus pada pc yang tersambung dengan printer
2000	Layanan atau aplikasi untuk meremote anywhere	Pemindaian port	Pemfilteran Firewall, Port Spoof dan Port Knocking
3306	Mysql Server	Pemindaian port	Pemfilteran Firewall, Port Spoof dan Port Knocking
5357	Layanan web untuk perangkat WSDAPI hanya disediakan Windows Vista, Windows 7 dan server 2008	Trojan	Peletakkan Portr harus benar dengan Menggunakan windows firewall
8291	Winbox Mikrotik untuk remote setting mikrotik Bik local maupun internet	Pemindaian port	Pemfilteran Firewall, Port Spoof dan Port Knocking
8080	Http-Proxy untuk layanan internet	Pemindaian port	Pemfilteran Firewall, Port Spoof dan Port Knocking
10000	WebMin untuk layanan pengelolaan web	Pemindaian port	Pemfilteran Firewall, Port Spoof dan Port Knocking. Apabila tidak dibutuhkan cukup meremove WebMin.

Tabel 3 Persentase Pengukuran Tingkat Komputer

persentase (%)	Kategori
0-20	Tidak Aman
21-40	Tidak Aman
41-49	Tidak Aman
50-80	Aman
81-100	Sangat Aman

Pada tabel 3 diatas bahwa nilai persentase dan kategori keamanan berdasarkan hasil dari data **((10 – port terbuka) / 10 * 100)** *scanning port* yang sudah dilakukan, maka secara otomatis setelah proses *scanning*

selesai langsung disimpan ke dalam *database* dan langsung di tampilkan pada *web monitoring security pc* dan *notifikasi via telegram*. Khusus *telegram* apabila tingkat keamanan komputer di bawah 50 %.

5.1 Kesimpulan

Kesimpulan dari penelitian ini adalah sebagai berikut.

1. Sistem pengukuran tingkat keamanan komputer berbasis *linux debian* dari perangkat *raspberry pi 3 model B* dapat dibangun menggunakan *scanning port* menggunakan *tools* nmap dengan tampilan *web* dan *notifiikasi via telegram.*
2. *Tools* nmap menggunakan program php cukup efektif dapat dilakukan secara otomatis baik di terminal raspberry dan cronjob untuk *scanning port* yang terbuka dari komputer yang aktif, merupakan langkah awal penyusup bisa masuk ke jaringan.
3. Penggunaan hasil *scanning port* pada *web* dan *notifikasi telegram* sangat membantu *administrator* dalam mengetahui tingkat keamanan komputer dari jumlah *port* yang terbuka, *notifikasi* akan memberikan informasi perangkat komputer yang tingkat keamanan dibawah 50%, sehingga *administrator* dapat mengambil tindakan lebih lanjut dan solusi sesuai dari hasil tingkat pengukuran komputer tersebut.

5.2 Saran

Saran diajukan dari penelitian ini dengan sifatnya membangun adalah sebagai berikut.

1. Selalu mengaktifkan *firewall* pada perangkat yang digunakan, agar dapat mengurangi celah *port* terbuka.
2. Selalu melakukan peninjauan keamanan komputer sebelum menggunakannya, karena port terbuka adalah pintu utama bagi penyusup untuk masuk ke sistem jaringan.
3. Dapat dikembangkan *tools* keamanannya, tambahan notifikasi telegram pada client setiap komputer dan diterapkan pada perusahaan, kampus, sekolah dan dimanapun selagi masih di jaringan LAN, karena sudah dikonfigurasi dimanapun letak *raspberry* apabila sudah tersambung dengan jaringan yang sama, maka proses *scanning* pun dapat digunakan.

DAFTAR PUSTAKA

[1] M. Anif, S. Hws, and M. D. Huri, “Penerapan Intrusion Detection System (IDS) dengan metode Deteksi Port Scanning pada Jaringan Komputer di Politeknik Negeri Semarang,” *J. TELE, Vol. 13 Nomor 1*, vol. 13, no. 1, pp. 25–30, 2015, doi: 10.1155/2017/3680758.

[2] M. R. Rusydianto, E. Budiman, and H. J. Setyadi, “Implementasi Teknik Hacking Web Server Dengan Port Scanning Dalam Sistem Operasi Kali Linux,” *Pros. Semin. Nas. Ilmu Komput. dan Teknol. Inf. e-ISSN*, vol. 2, no. 2, 2017.

[3] M. S. Hasibuan, “Keylogger pada Aspek Keamanan Komputer,” *Teknovasi*, vol. 3, no. 1, pp. 8–15, 2016.

[4] H. Arifin, *Kitab Suci Jaringan Komputer*. Yogyakarta: MediaKom, 2011.

[5]A. Goeritno and A. H. Hendrawan, “Implementasi Iso / Iec 27001 : 2013 Untuk Sistem Manajemen Keamanan Informasi (Smki) Pada Fakultas Teknik Uika-Bogor,” *Semin. Nas. Sains dan Teknol. Fak. Tek. Univ. Muhammadiyah Jakarta*, vol. 8, no. November, pp. 1–5, 2016, [Online]. Available: https://media.neliti.com/media/publications/174077-ID-none.pdf.

[6] M. F. Wicaksono, *Mudah Belajar Raspberry Pi*. Bandung: INFORMATIKA, 2018.

[7] UMM, “Pengertian Raspberry Pi 3.” Di Akses Pada 20 Februai 2020, [Online]. Available: http://eprints.umm.ac.id/40879/3/BAB II.pdf.

[8] N. Suryana, D. D. Saputra, T. Informatika, S. Tinggi, and T. Indonesia, “Perancangan Penggunaan Firewall Dan Proxy Server Untuk,” vol. 8, no. 1, pp. 44–53, 2018.

[9] D. Stiawan, “Sistem Keamanan Jaringan Komputer,” pp. 1–165, 2005.

[10] K. Aryanto and K. Mahendy, *Jaringan Komputer*. Yogyakarta: Graha Ilmu.

[11] E. Z. Henry Februariyanti, “Rancang Bangun Sistem Perpustakaan untuk Jurnal Elektronik,” *J. Teknol. Inf. Din.*, vol. 17, no. 2, pp. 124–132, 2012.

[12] G. W. Uke Kurniawan Usman, Agus Ganda Permana, *Jaringan Teleomunikasi dan Teknologi Informasi*. Bandung: INFORMATIKA, 2018.