OKTAL : Jurnal Ilmu Komputer dan Science
Volume 1, No. 11, November 2022
ISSN 2828-2442 (media online)
Hal 2091-2099

Pengembangan Keamanan Dan Jaringan Pada *System Windows* Mengunakan Metode *Hardening* (Studi Kasus : PT. Shiva Shakti Steel)

Moh. Triyana Abbas[1], Taswanda Taryo[2*], Murni Handayani[3*]

[1,2,3]Fakultas Teknik, Teknik Informatika, Universitas Pamulang, Jl. Raya Puspiptek No. 46, Kel. Buaran, Kec. Serpong, Kota Tangerang Selatan. Banten 15310, Indonesia
Email: [1]riyanbllz@gmail.com, [2*]dosen02234@unpam.ac.id, [3*]dosen02710@unpam.ac.id
(* : coressponding author)

Abstrak−Di era digital saat ini keamanan dan jaringan merupakan hal yang sangat penting dalam sebuah *system* untuk menunjang seluruh aktivitas di dunia kerja, khususnya untuk perkantoran. Dalam hal ini *system windows* pada PT. Shiva Shakti Steel saat ini yang masih lambat, kinerja aplikasi pendukung terasa lambat, serta keama nan ja rin ga n ya n g ma si h re nta n. PT. Shiva Shakti Steel adalah salah satu perusahaan yang menggunakan teknologi dan informasi, dengan menggunakan jaringan *internet* pada *system windows*, yang diharapkan dapat membantu manajemen untuk mengolah serta menyajikan data dan informasi secara efektif, cepat, dan akurat. Tujuan dari penelitian ini Diharapkan dapat mempercepat kinerja system windows, aplikasi pendukung dan keamanan jaringan. Dalam penelitian ini, teknik analisis data yang peneliti gunakan ialah metode *hardening system. Hardening system* mengacu pada penyediaan berbagai sarana perlindungan dalam sistem komputer. Perlindungan diberikan dalam berbagai lapisan, dan sering disebut sebagai pertahanan mendalam. Melindungi dalam lapisan berarti melindungi pada *level host, level* aplikasi, level system operasi. Menurut John D. Howard dalam bukunya "*An Analysis of security incidents on the internet*" menyatakan bahwa: "Keamanan komputer adalah tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab". Sedangkan Menurut Gollmann pada tahun 1999 dalam bukunya "*Computer Security*" menyatakan bahwa: "Keamanan komputer adalah berhubungan dengan pencegahan diri dan deteksi terhadap tindakan pengganggu yang tidak dikenali dalam *system komputer*". Dari hasil analisis pengujian kerentanan yang dilakukan, yaitu pengujian keamanan system dan jaringan pada *system windows* menggunakan metode *hardening* di PT. Shiva Shakti Steel, maka dapat diambil kesimpulan bahwa, metode hardening system ini dipilih karena ini merupakan pondasi awal untuk system, sehingga dapat menyelesaikan beberapa peramasalahan yang ada di *system*.

Kata Kunci: Sistem Windows, Jaringan, Keamanan, Metode *Hardening.*

Abstract−*In the current digital era, security and network are very important in a system to support all activities in the world of work, especially for offices. In this case the windows system at PT. Shiva Shakti Steel is currently still slow, supporting application performance feels slow, and network security is still vulnerable. PT. Shiva Shakti Steel is a company that uses technology and information, using the internet network on a windows system, which is expected to help management to process and present data and information effectively, quickly, and accurately. The purpose of his research is expected to accelerate the performance of the windows system, supporting applications and network security. In this study, the data analysis technique that the researcher uses is the hardening system method. Hardening system refers to providing various means of protection in a computer system. Protection is provided in multiple layers, and is often referred to as deep defense. Protecting in layers means protecting at host level, application level, operating system level. According to John D. Howard in his book "An Analysis of security incidents on the internet" states that: "Computer security is a preventive measure from attacks by computer users or irresponsible network accessors". Meanwhile, according to Gollmann in 1999 in his book "Computer Security" states that: "Computer security is related to self-prevention and detection of unrecognized intruders in computer systems". From the results of the analysis of vulnerability testing carried out, namely testing system and network security on windows systems using the hardening method at PT. Shiva Shakti Steel, it can be concluded that the hardening system method was chosen because this is the initial foundation for the system, so that it can solve some of the problems that exist in the system.*

Keywords*: Windows System, Network, Security, Hardening Method.*

1. PENDAHULUAN

Pada era teknologi saat ini hampir semua instansi dan perusahaan saling bersaing dalam usaha bisnis. Dengan memanfaatkan perkembangan teknologi dan informasi seperti saat ini, pihak-

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 1, No. 11, November 2022
ISSN 2828-2442 (media online)
Hal 2091-2099

pihak yang bersaing diharapkan dapat menghadapi tantangan dan rintangan dari persaingan bisnis saat ini dan kedepannya. keamanan jaringan merupakan hal yang sangat penting untuk diperhatikan, terutama bagi pelaku bisnis yang menggunakan *system* dan jaringan *internet*.

PT. Shiva Shakti Steel adalah salah satu contoh perusahaan yang memanfaatkan dari perkembangan teknologi dan informasi, dengan menggunakan jaringan ineternet pada *system windows* yang diharapkan dapat membantu manajemen untuk mengolah dan menyajikan informasi secara efektif, cepat, akurat dan efisien baik dari segi waktu dan biaya. PT. Shiva Shakti Steel memiliki tujuan untuk menjadi mitra bisnis yang baik dengan rekanan bisnis yang saat ini melakukan kerjasama. Diharapkan dengan menggunakan teknologi dan informasi, PT. Shiva Shakti Steel dapat menjaga kualitas pelayanan, baik secara internal perusahaan dan eksternal dengan pihak yang terlibat.

Seiring berjalannya waktu, system yang telah digunakan oleh pengguna di PT. Shiva Shakti Steel masih sering mengalami beberapa kendala dan permasalahan yang kerap kali menghambat proses kegiatan kerja yang berdampak pada tingkat kepuasan pengguna akan *system* tersebut rendah, Salah satu kendala yang terjadi *computer* mengalami kekurangan fungsi dalam menjalankan fungsinya, sehingga tidak bisa di akses dan memberatkan kinerja dari *computer* itu sendiri hal ini di sebabkan oleh adanya serangan DoS. DoS ini merupakan sebuah serangan terhadap komputer atau *server* di dalam jaringan *internet* dengan cara menghabiskan sumber resource yang dimiliki oleh komputer. Sehingga pihak manajemen merasa perlu melakukan evaluasi terhadap *system* yang diterapkan, agar kedepannya system dapat meningkatkan optimalisasi kegiatan kerja dan meningkatkan kepuasan pengguna terhadap system yang digunakan.

Untuk itu perlu dipersiapkan keamanan jaringan untuk mengamankan dan meminimalisir ancaman pada *system computer*. Untuk menangkal ancaman, ada beberapa metode yang bisa diterapkan, dengan menggunakan firewall untuk menghindari serangan yang bertujuan untuk menyerangan data – data yang ada didalam computer. Melakuakan blocking terhadap IP yang terlihat mencurigakan, menolak paket data dan menolak paket service UDP (*user data gram protocol*), menggunakan antivirus yang dapat menangkal serangan data, dan menggunkan metode hardening system pada windows.

Tujuan dari analisis atau evaluasi tingkat keamanan tersebut adalah untuk mengetahui seberapa besar tingkat keamanan system windows yang di gunakan oleh pengguna, terhadap keamanan yang telah di-implementasikan, dengan harapan dapat menjadi acuan manajemen untuk meningkatkan kualitas dari system agar berdampak lebih baik kedepannya bagi pengguna akhir dalam menjalankan proses operasional perusahaan, sehingga dapat mencapai tujuan yang diinginkan perusahaan. Ada beberapa metode yang dapat di gunakan untuk keamanan jaringan, yaitu *Network Intrusion Detection System* (NIDS), *Switch Port Security*, dan metode *hardening*. Metode *hardening system* ini dipilih kareana ini merupakan pondasi awal untuk system, sehingga dapat dijadikan untuk evaluasi system, maka metode *hardening* dipilih dalam riset ini, untuk meningkatkan tingkat keamanan pada *system windows.* Tingkat keamanan dengan metode tersebut dengan maksud dan tujuan untuk mengukur bagaimana tingkat keamanan itu tercipta dari *system* yang digunakan oleh pengguna akhir, sehingga kedepannya hasil daripada pengukuran dengan metode tersebut dapat dijadikan acuan untuk meningkatkan kualitas dari *system* yang telah diimplementasikan saat ini, berdasarkan dengan tingkat kepuasan pengguna dalam menggunakan *system windows.*

2. METODOLOGI PENELITIAN

Peneilitian berjudul Rancang Bangun Sistem Pengukuran Tingkat Keamanan Komputer Pada Jaringan Lan (Riyandi et al., n.d.). 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

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 1, No. 11, November 2022
ISSN 2828-2442 (media online)
Hal 2091-2099

(*Local Area Network*) Sedangkan host secara umum diartikan sebagai komputer yang terkoneksi ke jaringan yang dapat memberikan layanan jaringan (*network service*).

Implementasi Keamanan Jaringan Komputer *Local Area Network* Menggunakan *Access Control List* pada Perusahaan X (Laksono & Nasution, 2020). Salah satu metode yang digunakan yaitu metode *Virtual Local Area Network* (VLAN) Access Control List (ACL) yang diterapkan pada Perusahaan X. Metode *Vlan Access Control List* merupakan salah satu teknik permintaan suatu akses jaringan internet atau komunikasi data dan pengiriman sejumlah paket data dari satu komputer ke komputer lainnya. Metode ini merupakan metode yang dimana pengumpulan referensi yang berkaitan dengan *Virtual Local Area Network* dan *Access Control List*. dengan menganalisa per topiknya. dan kemudian analisis per topiknya untuk memberikan kesimpulan tiap bagian pembahasan. Tahapan akhir dari metode ini yaitu berupa

pengujian hasil konfigurasi pada tahapan implementasi. pengujian ini dilakukan dengan mencoba melakukan akses dari client atau user yang di blok dengan menggunakan *Access Control List* dari source IP Address (standard ACL) dan dari user yang di blok dari destination IP *address* (extended ACL). Ketika dikonfigurasi *Access Control List* yang ber type hak aksesnya "permit" alamat IP sumber (*Source* IP) dan alamat IP tujuan (Destination IP) dapat saling terhubung dan dapat mengakses service tambahan seperti FTP dan TFTP, ketika *Access Control List* dikonfigurasi dengan type hak akses "deny" dengan alamat IP sumber (Source IP) dan alamat IP tujuan (Destination IP) maka aksesnya akan di filter atau dihentikan akan tetapi dengan menggunakan *Access Control List Extended* dapat menggunakan service contoh menggunakan type hak akses "deny" dengan memfilter sebuah service ftp maka client tidak dibolehkan mengakses FTP dan koneksi terhadap alamat IP tujuan (*Destination* IP) tidak akan terhubung jika menggunakan type (*Outbound*) namun jika menggunakan type (*inbound*) maka client tidak bisa mengakses FTP namun client dapat mengakses koneksi dari alamat IP tujuan (Destination IP) yaitu hanya dapat mengakses *Internet Control Message Protocol* (ICMP) saja.

Keamanan Jaringan Komputer Pada Era Big Data (Munawar et al., 2020). Penelitian ini membahas bentuk dan faktor ancaman keamanan komputer, juga beberapa saran untuk meningkatkan pencegahan dari ancaman keamanan komputer. Ada hal penting yang perlu dilakukan yaitu melakukan pekerjaan dengan baik dalam pencegahan keamanan jaringan komputer, untuk meminimalkan kemungkinan terjadinya kejahatan komputer. Menurut definisi komputer keamanan jaringan oleh Organisasi Internasional untuk Standardisasi, keamanan jaringan komputer mengacu pada perlindungan perangkat keras, perangkat lunak, dan sumber daya data dalam sistem komputer agar tidak dihancurkan, diubah, atau lubang keamanan karena alasan kecelakaan atau berbahaya, sehingga sistem komputer terus beroperasi dengan handal, serta layanan komputer juga teratur. Pengenalan teknologi big data dapat menawarkan organisasi dengan solusi yang dibutuhkan, dengan memberikan kemampuan untuk menganalisis volume data yang lebih besar dengan kecepatan dan akurasi yang lebih besar dari yang sebelumnya mungkin. Dengan jatuh tempo solusi big data, keamanan dan privasi menghadirkan keprihatinan serius bagi berbagai pihak; perorangan, organisasi dan pemerintah, terutama karena banyaknya data pribadi yang dikumpulkan dan dianalisis. Ada empat bentuk utama ancaman terhadap keamanan jaringan komputer: penyalahgunaan informasi *Internet of Things*, penolakan layanan serangan latar belakang, kerusakan pada integritas lingkungan jaringan komputer, dan kebocoran informasi komputer. Hal ini akan menyebabkan bahaya besar yang tersembunyi pada keamanan jaringan komputer, karena setiap situs web, file, tautan dan sebagainya sangat mungkin mengandung virus atau ada file yang disembunyikan serta hal lainnya yan berbahaya, jika tidak ada aplikasi untuk menyaring virus atau file yang tersembunyi, maka dapat menyebabkan kebocoran informasi atau infeksi terhadap komputer.

Simulasi Penggunaan *Intrusion Detection System* (IDS) Sebagai Keamanan Jaringan dan Komputer (Fachri & Harahap, 2020). Simulasi dilakukan untuk menirukan sistem keamanan jaringan nyata yang ada dengan sifat yang lebih mudah untuk diamati daripada sistem aslinya, untuk mengetahui performansi sistem. Pada penelitian ini dibutuhkan sistem yang dapat menanggulangi ancaman yang mungkin terjadi secara optimal dalam waktu yang cepat, hal ini akan mempercepat proses penanggulangan gangguan serta pemulihan sistem atau layanan. Salah satu cara yang dapat digunakan untuk menanggulangi atau mengatasi hal tersebut adalah dengan menggunakan *Intrusion Detection System* (IDS). Salah satu aplikasi yang mendukung *intrusion*

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 1, No. 11, November 2022
ISSN 2828-2442 (media online)
Hal 2091-2099

detection system (IDS) Hal yang mengakibatkan semua komputer yang terhubung ke jaringan komputer sangat rentan terhadap serangan atau kegiatan yang bersifat merugikan yang dilakukan oleh orang lain yang bertujuan untuk mengambil data, memanipulasi data, bahkan merusak data-data berharga untuk tujuan tertentu. Oleh karena itu, dibutuhkan suatu sistem dalam menangani penyalahgunaan disebuah jaringan atau ancaman ancaman dari penyusup yang akan terjadi yaitu dengan menggunakan aplikasi *Intrusion Detection System* (IDS) yaitu Snort dan *vmware (Router OS)* sebagai penindak lanjut terhadap alert Snort yang dihasilkan. Ada beberapa penelitian terdahulu yang menggunakan metode *Intrusion Detection System* dalam mengamankan jaringan dan computer. Program yang digunakan untuk pendeteksian disebut sebagai IDS (*Intrusion Detection System*).

Keamanan Jaringan Menggunakan Teknik *Network Intrusion Detection System* (NIDS) Di Kantor Setwan Kepulauan Meranti (Ari Setiawan & Tria Putra Abza, 2020). Gangguan keamanan yang terjadi pada tempat yang menjadi studi kasus ini terjadi dari pihak internal yang ingin menjatuhkan sistem kerja jaringan dan ingin mencoba ketahanan dan keamanan jaringan yang ada pada tempat tersebut. Untuk mendeteksi setiap gejala serangan tersebut, sistem menggunakan pola pengenalan terhadap source yang didapat dari pihak yang dianggap ancaman dalam sistem jaringan komputer. Penulis menggunakan Snort, Barnyard dan BASE yang diimplementasikan pada mesin sensor berbasis open source. Keseluruhan sistem dibangun dalam sistem LAN yang merepresentasikan sistem produksi. Tujuan dari penelitian ini adalah meningkatkan sistem keamanan jaringan dengan merancang dan mengimplementasikan Network Instrusion Detection System berbasis open-source dan memahami teknik- teknik cara kerja serangan *Man-In-The-Middle Attack* (MITM) pada jaringan lokal dan mekanisme NIDS dalam usaha pendeteksian terhadap serangan tersebut. teknik *Network Instrusion Detection System* (NIDS) yang akan digunakan dalam keamanan sistem jaringan computer .Kepulauan Meranti ditemukan beberapa permasalahan yang dihadapi diantaranya adalah sering masuknya malware ke dalam personal komputer yang terhubung ke dalam jaringan dan Penyadapan pada jalur komunikasi (*Man-in the- Mid-dle Attack*) yang dapat dilakukan lebih mudah. Karena Sistem jaringan di Kantor Setwan tidak menggunakan pengamanan enkripsapti dan otentikasi, atau menggunakan enkripsi. Hardening Komputer dalam hal ini bukan berarti mengeraskan komputer dalam arti fisik. Dalam hal ini penulis menggunakan Metode *Network Base Intrusion Detection system* untuk mengamankan komputer dalam jaringan yang terdapat di Kantor Setwan Kab. Snort bertugas mendeteksi berbagai aktifitas intrusi dan penyerang yang terjadi pada jaringan komputer dan akan menampilkan alert bila terjadi aktifitas intrusi. Dalam penelitian ini, menggunakan simulasi LAN sebagai representasi sistem jaringan lingkungan produksi.

Metode Penetration Testing pada Keamanan Jaringan *Wireless Wardriving* PT. Puma Makmur Aneka Engineering Bekasi (Ismail, 2020). *Wardriving* adalah suatu kegiatan diamana seseorang maupun sekelompok orang yang dibekali alat dan keahlian untuk mengakses sebuah jaringan *Wireless* secara gratis atau tanpa melakukan login. Tujuan penelitian untuk mengetahui seberapa kuat keamanan jaringan *Wireless* pada PT. Puma Makmur Aneka *Engineering* Bekasi. Pengujian Kondisi Infrastruktur Jaringan setelah ditemukannya masalah yang ada pada jaringan *wireless* PT. Puma Makmur Aneka Engineering, maka adapun pengujian perhitungan nilai kerentanan yang dilakukan yaitu Perhitungan Nilai Kerentanan. Setelah pengujian dilakukan pada access point target, maka setelah itu dilakukan perhitungan tingkat kerentanan menggunakan CVSS. Berikut hasil dari nilai kerentanan pada *Access Point* jaringan PT. Puma Makmur Aneka *Engineering*. Pada proses perhitungan nilai kerentanan ini didapatkan hasil sebagai berikut a) WPA2 *Cracking*, berdasarkan hasil perhitungan yang telah dilakukan, dampak kerentanan dari serangan WPA2 *Cracking* untuk tingkat kerentanan sedang karena *password* yang digunakan belum menggunakan karakter yang unik dan kuat minimal 15 karakter. b) DoS, berdasarkan hasil perhitungan yang telah dilakukan dampak kerentanan dari serangan DoS untuk tingkat kerentanan tinggi karena proses memutuskan koneksi *Client* dalam *access point* sangat mudah karena hanya membutuhkan MAC Address dan SSID dari Access Point. c) *Password Router Wireless Cracking*, berdasarkan hasil perhitungan yang telah dilakukan dampak kerentanan dari serangan *Password Router Wireless Cracking* untuk tingkat kerentanan tinggi karena access point hanya menggunakan password default. d) *Access Point Isolation*, berdasarkan hasil perhitungan yang telah dilakukan dampak kerentanan dari serangan *Access Point Isolation* untuk tingkat kerentanan sedang karena

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 1, No. 11, November 2022
ISSN 2828-2442 (media online)
Hal 2091-2099

disebabkan *Client* dapat menyerang *Client* atau *Client to Client* hanya dengan menyamakan workgroup client saja. Berdasarkan pengujian kerentanan yang dilakukan yaitu pengujian keamanan jaringan wireless wardriving menggunakan metode Penetration Testing pada PT. Puma Makmur Aneka Engineering, maka dapat diambil kesimpulan bahwa pengujian keamanan jaringan internal dan publik telah dilakukan dengan menggunakan metode Penetration Testing dan mendapatkan kerentanan seperti WPA2 Cracking, Dos,

Paswword Router Wireless Cracking, dan AP *Isolation Testing* sehingga diketahui kerentanan pada jaringan internal dan publik. Setiap kerentanan yang ditemukan telah dilakukan perbaikan sehingga resiko dapat diturunkan. Penghitungan kerentanan telah dilakukan menggunakan CVSS *Calculator Version* 2 sehingga didapatkan hasil nilai kerentanan disetiap perangkat jaringan yang dimiliki oleh perusahaan. Kerentanan yang ditemukan juga telah diatasi kemudian dilakukan perhitungan nilai kerentanan setelah proses perbaikan. Hasil perhitungan setelah perbaikan didapatkan penurunan resiko yang baik sehingga dapat dinyatakan bahwa jaringan perusahaan memiliki tingkat keamanan yang lebih baik. Dengan pengujian standar keamanan jaringan *wireless* ini, diharapkan aktivitas di PT. Puma Makmur Aneka Engineering dapat lebih efektif dan lebih efisien.

3. ANALISA DAN PEMBAHASAN

Analisa kebutuhan adalah suatu rincian penjelasan kebutuhan dalam proses pengumpulan data yang diperlukan untuk dijadikan bahan acuan, Data yang digunakan untuk proses pengembangan keamanan jaringan ini didapatkan dengan cara *scaning System* (mengumpulkan) data dari perushaan. Maka akan didapatkan hasilnya setelah melalui beberapa tahapan dengan variabel yang sudah ditentukan, sehingga proses identifikasi antar tahapan pada metode hardening dapat lebih akurat dan informatif hasilnya.

Dalam penelitian ini digunakan spesifikasi *hardware* dan *software* sebagai alat bantu pada penelitian yaitu terdapat pada tabel berikut:

Tabel 1. Spesifikasi *Software* dan *Hardware*

Hardware	***Software***
CPU : Intel Core i3 Gen 5	*System Windows*
Memory : Ram 4Gb	*whireshrk*
Hdd : 500 Gb	*Windows Resource Monitor, Winbox, hping3, nmap, Virtual box*

Windows adalah sebuah sistem operasi (operating system) yang diciptakan oleh Microsoft guna mengakomodasi kebutuhan pengguna awam.

Wireshark digunakan untuk melakukan analisis dan pemecah masalah jaringan. Hal ini memungkinkan kamu untuk mengetahui masalah yang terjadi pada jaringan. *Wireshark* adalah program penganalisa jaringan yang sangat populer saat ini. Aplikasi *Wireshark* sendiri merupakan salah satu dari *tool Network Analyzer* yang biasa digunakan oleh *Network Administrator* pemecahan masalah jaringan, analisis, perangkat lunak dan pengembangan protokol komunikasi, dan pendidikan.

Resource monitor adalah fitur dimana kita bisa melihat informasi tentang penggunaan hardware (CPU, memory, disk dan network) dan software (file handle dan module) dari proses dan service secara real time di Windows 7 dan Windows 8, 10, 11.

Winbox adalah salah satu aplikasi untuk konfigurasi Mikrotik Router OS menggunakan GUI. Aplikasi Winbox bisa berjalan pada windows berbentuk portable binary, tapi bisa juga berjalan pada Linux dan MACOS (OSX) menggunakan Wine. Semua fungsi pada aplikasi Winbox hampir sama persis dengan fungsi konsol (*command line*).

Hping 3 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).\

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 1, No. 11, November 2022
ISSN 2828-2442 (media online)
Hal 2091-2099

Network Mapper adalah sebuah aplikasi atau tool yang berfungsi untuk melakukan *port scanning.* Nmap dibuat oleh *Gordon Lyon*, atau lebih dikenal dengan nama Fyodor Vaskovich. Aplikasi ini digunakan untuk meng-audit jaringan yang ada.

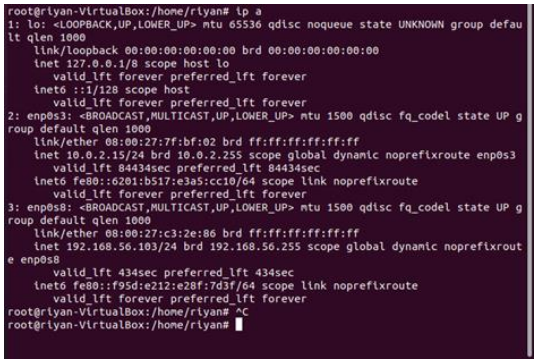
VirtualBox adalah aplikasi open source yang berkaitan dengan Virtualisasi. Virtualisasi yang dimaksud adalah membuat mesin PC virtual yang bisa berjalan secara independen di atas sistem operasi utama. Segala bentuk hardware yang berkaitan dengan mesin virtual semuanya disimulasikan oleh host pc. Sehingga semua sumber daya perangkat keras tidak bisa melebihi sumber daya aslinya.

4. IMPLEMENTASI

Penelitian dilakukan dengan kombinasi metode atau melakukan scaning terhadap system windows yang berjalan . Tujuan dari proses scaning system ini agar memudahkan untuk menganalisa kelemahan keamanan pada system. Disamping itu untuk memastikan keamanan jaringan. Tahap analisis ini akan memunculkan beberpa kelemahan yang ada pada system windows.

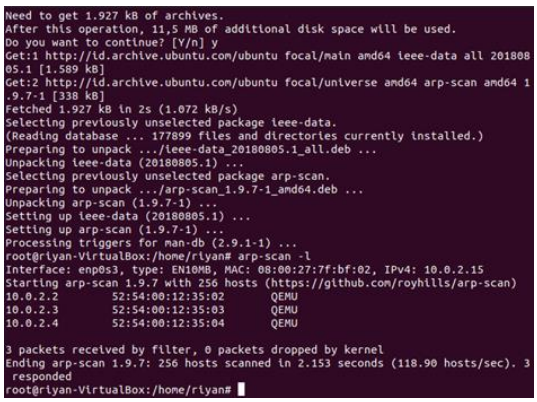
Penelitian ini dilakukan dengan menggunakan *tools Hping*3, *nmap,* dan *whireshark.* pada tahap persiapan ini data yang digunakan adalah hasil scaning port. Sacning Networks- port dan *service discovery* menggunakang *Hping*3 Port dan *service discovery* merupakan tahapan dalam pentest untuk melakukan pemeriksaan port dan layanan yang open pada sebuah host. Salah satu *tools* yang dapat di gunakan dalam hal ini dalah Haping3. Dengan menggunakan tools ini kita dapat melihat port dan services yang terdapat pada sebuah host. Pada penelitian ini saya menggnakan hping3 dengan menggunakan sisitem ubuntu 20.

Sebelum melakukan port scaning kita akan melakukan host discovery. Untuk mengetahui network addres makan printah nya ip a pada terminal yang sudah terbuka, dan terlihat ip padres yang saya gunakan adalah 192.168.56.103/24. Ini menandakan saya di network 192.168.56.103/0.



Gambar 1. Ip a Network addres

Berikutnya saya menggunakan printah arp-scan -I untuk mengetahui host aktif



Gambar 2. Host Aktif

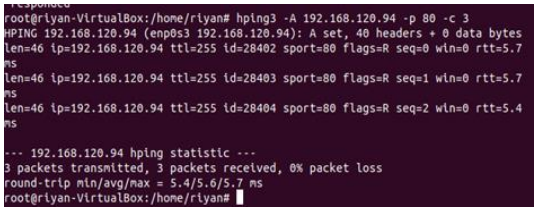
OKTAL : Jurnal Ilmu Komputer dan Science
Volume 1, No. 11, November 2022
ISSN 2828-2442 (media online)
Hal 2091-2099

Selanjutanya saya mengunakan Hping3 untuk memeriksa apakah PORT 80 (HTTP) tersedia.

-A: digunakan untuk setting ACK flag.

-P: digunakan untuk port scanning, dalam hal ini yang di scan adalh port 80 (HTTP)

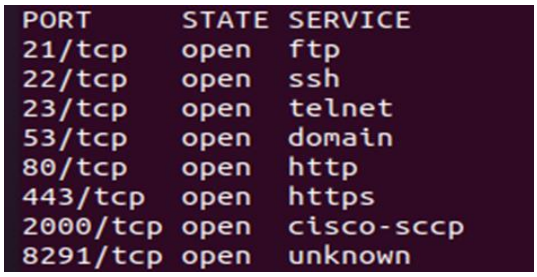
-C: digunakan untuk membatasi jumlah packet yang di kirim, dalam hal ini 3. Hasil dapat dilihat bahwa paket direspon. Artinya port 80 tersedia.



Gambar 3. Port 80 tersedia

Port tersebut tersedia namun belum tentu ada ato terbuka. Kita dapat melakukan pemeriksaan port yang aktif dengan perintah berikut: hping3 -8 0-100 –s

192.168.120.94 –v. -8: digunakan untuk scan spesifik port dalam hal ini 0-100 artinya port 0-100 kita bisa melihat service name mana yang ada dan kita dapat melihat juga port yang open aktif dari nilai kolom win yang tersedia.



Gambar 4. Port Terbuka

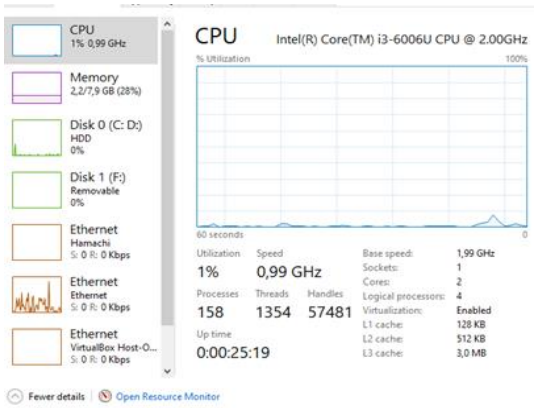
Untuk Menseleksi port dari banyaknya port yang tersedia kita dapat mengunakan printah hping3 –scan 0-100 –S 192.168.120.94

--scan: digunakan untuk scanning port dalam hal ini port 0-100

-S: digunakan untuk setting Synflag.

Dalam list ini hanya port open dan aktif saja yang akan ditampilkan. Penelitian ini dilakukan dengan menggunakan tools Hping3, nmap dan whireshark versi 3.6.2 pada tahap persiapan ini data yang digunakan adalah Scanning yang dilakukan

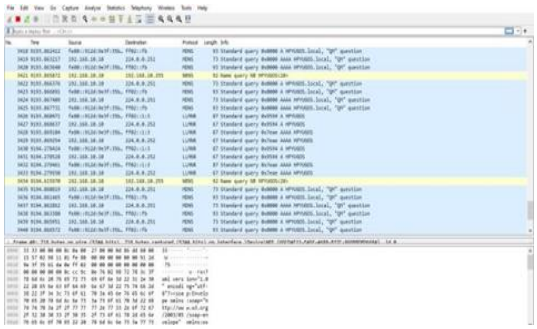
menggunakan Nmap pada objek 192.168.120.94 menunjukan bahwa system memiliki beberapa port yang terbuka. Nmap menggunakan DNS dari objek untuk mendapatkan port apa saja yang terbuka.



Gambar 5. CPU dalam keadaan normal

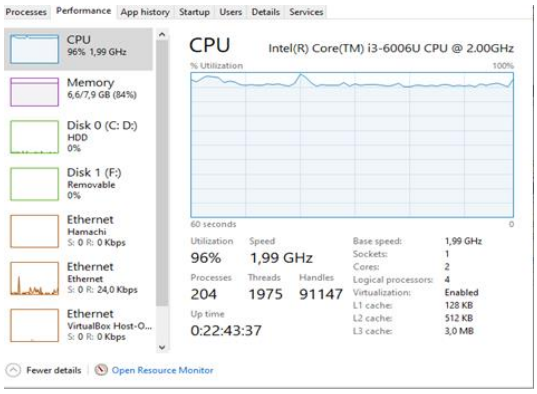
OKTAL : Jurnal Ilmu Komputer dan Science
Volume 1, No. 11, November 2022
ISSN 2828-2442 (media online)
Hal 2091-2099

Pengujian dilakukan menggunakan hping3 dalam proses ini system akan di uji dengan melakukan serangan berupa Ddos attack. Ddos sendiri merupakan jenis serangan terhadap sebuah computer atau server di dalam jaringan internet dengan cara menghabiskan sumber resource yang di miliki oleh computer sampai computer tidak dapat menjalankan fungsinya dengan benar.



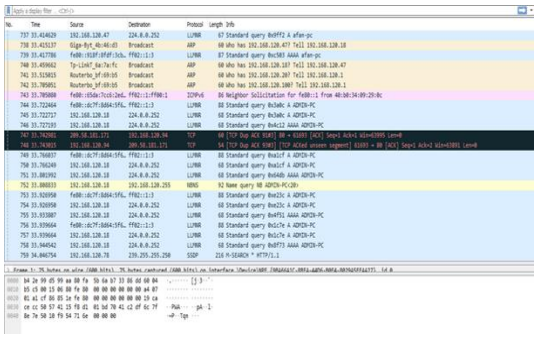
Gambar 6. Perjalanan Paket di Wireshark

Sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan computer yang diserang. Dalam hal ini penyerang melakukan ping of death. Serangan ini dilancarkan dengan menggunakan utility ping pada sebuah system oprasi.



Gambar 7. Traffic Monitor Tinggi

Serangan *Syn Flooding* dilakukan dengan cara memanfaatkan kelemahan protocol pada saat terjadinya proses handshake. Saat dua buah computer memutuskan untuk memulai melakaukan komunikasi, computer penyerang dalam hal ini akan mengirimkan sync kepada kompter penerima, (target) akan menjawab dengan mengirimkan sync ack kepada computer pengirim. Setlah menerima syn ack dari penerima pengirim mengirimkan ack kepada penerima untuk melakukan proses handshake. Dalam hal ini pengirim justru mengirimkan banyak paket syn, kepada penerima yang mengakibatkan penerima harus terus menjawab permintaan dari pengirim, serangan seperti ini tentunya akan menghambat penerima memberikan pelayanan kepada user yang sah.



Gambar 8. Serangan Syn Flooding ke port 80

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 1, No. 11, November 2022
ISSN 2828-2442 (media online)
Hal 2091-2099

Bagaimana untuk mengatasi masalah keamanan agar masalah tersebut tidak mengangu proses kerja system, dalam hal ini metode *hardening system* sangat penting untuk mengokohkan sebuah system ada bebrapa tahap proses *hardening system.*

5. KESIMPULAN

Berdasarkan analisis pengujian kerentanan yang dilakukan, yaitu pengujian keamanan system dan jaringan pada system windows menggunakan metode hardening pada PT. Shiva Shakti Steel, maka dapat diambil kesimpulan bahwa, metode hardening system ini dipilih karena ini merupakan pondasi awal untuk system, sehingga dapat menyelesaikan beberapa peramasalahan yang ada.

1. Kondisi system windows PT. Shiva Shakti Steel saat ini yang masih lambat. Dapat diselesaikan dengan metode, *hardening* dengan membuat akun non-admin, *disable automatic loogin*, membuat *password* untuk *screen server*,
2. Kinerja aplikasi pendukung masih lambat. Dapat di selesaikan dengan mengaktifkan firewall, mengaktifkan windows security, menonaktifkan remote akses, mengaktifkan *windows update*, serta menutup port yang tidak di gunakan.
3. St rate gi unt uk me n gem ba n gkan keama na n ja ri n ga n PT . Shi va Sha kti Steel secar a o ptimal , den gan men am bah kan tambahan aplikasi ke aman an d ari l uar , m enam ba hka n a nti vir u s, serta an ti mal ware te rbai k.

Pengujian keamanan jaringan internal telah dilakukan dengan menggunakan scaning port pada system dan mendapatkan kerentanan pada system, yaitu berupa serangan DDos, *syn flooding.* Setiap kerentanan yang ditemukan telah dilakukan perbaikan dengan metode hardening system sehingga resiko system lambat, aplikasi pendukung lambat, dan keamanan jaringan dapat di selesaikan. Sehingga pengoprasian system dapat berjalan dengan optimal Dan dapat dinyatakan bahwa jaringan perusahaan memiliki tingkat keamanan yang lebih baik dan optimal. Dengan adanya analisa serta pengujian keamanan jaringan pada *system windows* ini, diharapkan aktivitas di PT. Shiva Shakti Steel dapat lebih efektif dan lebih efisien.

REFERENCES

Aditya, Y. S., Yunan, U., Septo, K., & Fathinuddin, M. (2021). PENGAMANAN DATA CLOUDFRI MENGGUNAKAN METODE SECURITY HARDENING. 8(5), 9428–9438.

Ari Prayoga Hutabarat, & H. (2020). Analisa Dan Perancangan Keamanan Jaringan End User Dari Serangan Exploit Menggunakan Metode Penetration. *Journal of Information System and Technology.*

Ari Setiawan, C., & Tria Putra Abza, A. (2020). Keamanan Jaringan Menggunakan Teknik Network Intrusion Detection System (NIDS) Di Kantor Setwan Kepulauan Meranti. *Jurnal Intra Tech*, 4(2), 35–46. https://www.journal.amikmahaputra.ac.id/index.php/JIT/article/view/82

Bina, K., Jl, W., Soebrantas, H. R., & Baru, S. (2019). Pengaruh serangan keamanan pada vanet terhadap performansi jaringan. 6, 1–6.

Bustami, A., & Bahri, S. (2020). Ancaman, Serangan dan Tindakan Perlindungan pada Keamanan Jaringan atau Sistem Informasi: *Systematic Review. Unistek, 7*(2), 59–70. https://doi.org/10.33592/unistek.v7i2.645

Cosmas Eko Suharyanto. (2016). Analisis Komparatif Sistem Keamanan Windows 7 Dan Windows 8. *JIF (Jurnal Ilmiah Informatika).*

Dewi, S. (2020). Keamanan Jaringan Menggunakan VPN (Virtual Private Network) Dengan Metode PPTP (Point To Point Tunneling Protocol) Pada Kantor Desa Kertaraharja Ciamis. *EVOLUSI: Jurnal Sains Dan Manajemen, 8*(1), 128–139.

Fachri, B., & Harahap, F. H. (2020). Simulasi Penggunaan Intrusion Detection System (IDS) Sebagai Keamanan Jaringan dan Komputer. *Jurnal Media Informatika Budidarma, 4*(2), 413. https://doi.org/10.30865/mib.v4i2.2037.