ANALISIS *MONITORING* SISTEM KEAMANAN JARINGAN KOMPUTER MENGGUNAKAN *SOFTWARE NMAP* (STUDI KASUS DI SMK NEGERI 1 KOTA SERANG)

Dwi Bayu Rendro[1], Ngatono[2],Wahyu Nugroho Aji[3]
Rekayasa Sistem Komputer, Fakultas Teknologi Informasi, Universitas Serang Raya
Jalan Raya Serang, Cilegon Km. 5 Taman Drangong, Serang-Banten 42116
Telp. : 0254-8235007; Fax. : 0254-8235008
dwibayurendra@gmail.com[1], ngatono077@gmail.com[2], wahyuaji47@gmail.com[3]

Abstrak - Serangan pada jaringan komputer bisa dalam berbagai cara. Aplikasi layanan memiliki kelemahan seperti kesalahan pemrograman, atau versi layanan yang kadaluarsa yang sudah tidak *update*. Kelemahan-kelemahan tersebut memungkinkan *host* yang memiliki layanan dan *port* terbuka tersebut rentan terhadap serangan. Ada baiknya *host* menyediakan layanan yang diperlukan saja umtuk meminimalkan *port* yang terbuka. *Software NMAP* digunakan untuk mendeteksi *port* terbuka, mengetahui perangkat keras dan perangkat lunak yang dipakai dalam jaringan, me-*monitoring* jaringan dengan melakukan *network scanning* dan *port scanning* serta dapa mengeksplorasi sistem keamanan jaringan dan mengaudit keamanan jaringan yang digunakan. Dengan menggunakan *software NMAP* seorang *user* dapat mengetahui *port-port* layanan, versi layanan, perkiraan sistem operasi yang digunakan oleh *host*. Software NMAP mampu melakukan *scanning port* jaringan dengan versi layanan dan mesin pendeteksi sistem operasi. Dengan didapatnya status *port* terbuka (*open*), servis layanan dan informasi layanan, yang dihasilkan oleh pemindaian *Software NMAP*.*Sysadmin* dapat mengetahui informasi yang didapat tersebut.

Kata Kunci: *Software NMAP*, *Network Scanning*, Keamanan Jaringan Komputer

I. PENDAHULUAN

Pengamanan pada jaringan komputer mutlak diperlukan seiring perkembangan teknologi dan internet. Berbagai cara dapat digunakan untuk mendeteksi serangan atau penyusupan, seperti *packet sniffing*, *network scanning*, dan *monitoring* layanan. Dengan teknik-teknik tersebut dapat menolak, memperbolehkan, atau menyaring paket yang mencoba masuk ke dalam jaringan atau ingin mengakses sumberdaya dan layanan tertentu. Jaringan komputer dapat diserang dalam berbagai cara. Aplikasi layanan sendiri mungkin mempunyai beberapa kelemahan seperti kesalahan pemrograman, penggunaan autentikasi atau *password* yang lemah, *sensitive* data tidak terenkripsi atau mengijinkan koneksi dari berbagai alamat IP dan lain sebagainya. Kelemahan-kelemahan tersebut memungkinkan *host* yang menyediakan layanan tersebut rentan terhadap serangan. Oleh karena itu sebaiknya *host* hanya menyediakan layanan yang diperlukan saja, atau dengan kata lain meminimalkan *port* yang terbuka.

Jaringan komputer di SMK Negeri 1 Kota Serang sering mengalami kendala atau kesulitan mengakses Web E-Raport untuk meng-input nilai, padahal akses jaringan internet cukup lancar. Di sini juga pernah mengalami *server down* dimana semua yang akan mengakses Website, E-Raport, Dapodik tidak dapat masuk ke jaringan *server* tersebut, yang selanjutnya dapat berimbas ke semua komputer yang terhubung pada jaringan tersebut.

Hal ini akibat kurangnya perhatian *sysadmin* terhadap jaringan yang digunakan, *sysadmin* kurang rutin dalam melakukan memindai keamanan jaringan server yang terhubung seperti *port* terbuka yang tidak difilter atau ditutup, sehinngga mudahnya lalu lintas data atau paket-paket yang berbahaya yang tidak diizinkan masuk ke dalam jaringan. Sistem keamanan jaringan di SMK Negeri 1 Kota Serang, belum pernah melakukan pemindaian keamanan jaringan dan audit keamanan jaringan sebagai data keamanan jaringan yang digunakan. Sistem keamanan jaringan yang digunakan masih sebatas pengaturan *Modem ISP* dan pengaturan *Router* bawaan, tanpa memiliki keamanan jaringan tambahan.

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. *NMAP* adalah singkatan dari *Network Mapper*, merupakan *tool opensource* yang digunakan khusus untuk eksplorasi jaringan dan audit keamanan jaringan.

II. TINJAUAN PUSTAKA

Penelitian dikembangkan dari beberapa referensi yang telah didapat yang berhubungan dengan objek permasalahan. Telaah penelitian tersebut diantaranya:

Menurut Ade Hendri Hendrawan, Foni Agus Setiawan, Arief Sekto Mulyo (2014). Dalam penelitiannya yang berjudul Analisis Keamanan Jaringan dengan Metode *Security Lifecycle* di Universitas Ibn Khaldun Bogor. Salah satu metode dalam menganalisis keamanan jaringan adalah *Security Lifecycle* (SLC). Metode ini memiliki tahapan mulai dari analisis data potensi ancaman yang mungkin terjadi, kebijakan atas apa yang diperbolehkan dan tidak diperbolehkan dalam menjalankan sebuah sistem, dan spesifikasi mengenai fungsi sistem yang diinginkan, serta hasil implementasi dari sistem keamanan yang diuji. SLC yang diusulkan untuk implementasi sistem keamanan jaringan meliputi 5 tahap, yaitu: *Monitoring*; Analisis; Rekomendasi; Implementasi; dan Evaluasi.

Menurut Devi Christiani Angir, Agustinus Noertjahyana, Justinus Andjarwirawan (2015). Dalam penelitiannya yang berjudul *Vulnerability Mapping* pada Jaringan Komputer di Universitas X. *Vulnerability* adalah suatu kelemahan yang mengancam nilai *integrity*, *confidentiality*, dan *availability* dari suatu aset. *Penetration testing* atau yang lebih dikenal dengan sebutan *pentest* adalah salah satu metode yang dapat digunakan untuk melakukan evaluasi terhadap suatu jaringan komputer. Selain itu, *mapping* terhadap *vulnerability* juga perlu dilakukan. Keamanan jaringan ini dapat bertujuan untuk agar pemilik sistem informasi dapat menjaga sistem informasinya tidak ditembus atau disusupi oleh orang lain yang pada akhirnya dapat merusak sistem. Adapun tipe dari penyusup ini dapat berupa: *the curious*, *the malicious*, *the high-profile intruder*, dan *the competition*. Jenis-jenis segi keamanan jaringan yang ada antara lain: *confidentiality*, *integrity*, *availability*, *non-repudiation*, *authentication*, dan *accountability*. *Digital Signature* adalah salah satu teknologi yang digunakan untuk meningkatkan keamanan jaringan dan berfungsi untuk memastikan bahwa tidak ada data yang berubah.Cara kerja *digital signature* dilihat telah memenuhi salah satu syarat keamanan jaringan, yaitu *Non-repudiation*.

Menurut Egi Widya Yachya (2016). Dalam penelitiannya yang berjudul Analisis Keamanan Jaringan *Server Web* dan *Hotspot* Menggunakan *Tool Nmap* dan *Nessus* di Pusat Penelitian Limnologi LIPI. Salah satu cara dalam menganalisis keamanan jaringan yaitu menggunakan *tool Nmap* dan *Nessus*, dimana *tool Nmap* berfungsi untuk melihat *port-port* dari jaringan local yang terbuka, dan *tool Nessus* akan menghasilkan *output* berupa *Vulnerabilities* dari IP *scan target* yang akan dianalisis. Dengan teknik-teknik tersebut dapat menolak, memperbolehkan, atau menyaring paket yang mencoba masuk ke dalam jaringan atau ingin mengakses sumberdaya atau layanan tertentu. *Scan* jaringan menggunakan *Nmap* menampilkan *host-host* dan *port* yang terbuka serta *host* detail dari port yang di-*scan*, selain itu akan terlihat topologi dari *IP target* yang di-*scan*. *Scan* jaringan menggunakan *Nessus* menampilkan *vulnerabilities* dari IP target yang di *scan*, selain itu setelah hasil dari *vulnerabilities* tersebut didapat maka *Nessus* akan menampilkan detail dari *vulnerabilities IP* yang di-*scan* beserta solusi untuk mengatasi *vulnerabilities* tersebut. Dari hasil analisis yang dilakukan setiap harinya *vulnerabilities* semakin bertambah jika tidak ada divisi khusus yang menangani masalah keamanan jaringan. Hasil rekomendasi yang disarankan untuk mengatasi *vulnerabilities* diantaranya meningkatkan kinerja dan performa sistem keamanan jaringan.

Menurut Ino Anugrah, R.Hengki Rahmanto (2017). Dalam penelitiannya yang berjudul Sistem Keamanan Jaringan *Local Area Network* Menggunakan *Teknik De-Militarized Zone*. *De-Militarized Zone* (DMZ) merupakan mekanisme untuk melindungi sistem internal dari serangan *hacker* atau pihak-pihak lain yang ingin memasuki sistem tanpa mempunyai hak akses. DMZ terdiri dari semua *port* terbuka, yang dapat dilihat oleh pihak luar sehingga jika *hacker* menyerang dan melakukan *cracking* pada *server* yang mempunyai DMZ, maka *hacker* tersebut hanya dapat mengakses *host* yang berada pada DMZ dan tidak pada jaringan internal. Selain itu dengan melakukan pemotongan jalur komunikasi pada jaringan internal, *virus*, *trojan* dan sejenisnya sehingga tidak dapat lagi memasuki jaringan. Untuk itu diperlukan teknik keamanan jaringan yang dapat menangkal ancaman serangan tersebut atau meminimalisir ancaman serangan yang bisa memasuki sistem jaringan. Dalam penelitian ini dilakukan implemetasi teknik DMZ pada sistem keamanan jaringan lokal di Universitas Islam 45 (Unisma) Bekasi. Penelitian ini dilakukan dalam beberapa tahap: 1) Analisis Kebutuhan: Tahap ini merupakan identifikasi masalah dari sistem keamanan jaringan di Unisma. Dari masalah yang ada kemudian diselesaikan dengan implementasi metode DMZ pada jaringan *local*. 2) Perancangan: Dalam tahap perancangan dilakukan penentuan topologi dan konfigurasi jaringan. 3) Implementasi: Tahap implementasi merupakan tahap yang melakukan *setting* layanan DMZ pada *server*. 4) Pengujian: Tahap pengujian dilakukan untuk mengetahui sejauh mana implementasi dilakukan. Dalam penelitian dilakukan 2 pengujian yaitu pengujian tanpa menggunakan DMZ dan pengujian dengan menggunakan DMZ.

Konsep Dasar Jaringan

Jaringan komputer adalah kumpulan beberapa komputer (dan perangkat lain seperti *router*, *switch* dan sebagainya) yang saling terhubung satu sama lain melalui media perantara. Media perantara ini

bisa berupa media kabel ataupun media tanpa kabel (Iwan Sofana, 2013).

Jaringan komputer (jaringan) adalah jaringan telekomunikasi yang memungkinkan antar komputer untuk saling berkomunikasi dengan bertukar data. Tujuan dari jaringan komputer adalah agar dapat mencapai tujuannya, setiap bagian dari jaringan komputer dapat meminta dan memberikan layanan (*service*). Pihak yang meminta/menerima layanan disebut klien (*client*) dan yang memberikan/mengirim layanan disebut peladen (*server*). Desain ini disebut dengan sistem *client-server*, dan digunakan pada hampir seluruh aplikasi jaringan komputer (curlie.org, 2019).

Sistem Keamanan Jaringan Komputer

Dalam bukunya "*An Analysis of security incidents on the internet*", menurut John D. Howard (1997), yang menyatakan bahwa Keamanan komputer merupakan suatu tindakan pencegahan perangkat dari agresi pengguna personal komputer atau pengakses jaringan yang bukan bertanggung jawab.

Menurut Gollmann pada tahun 1999 dalam bukunya yang berjudul "*Computer Security*" menyatakan bahwa: Keamanan suatu komputer merupakan berhubungan dengan pencegahan diri dan deteksi terhadap tindakan yang mengganggu yang tidak dikenali di dalam sistem komputer. Pada keamanan sistem komputer yang harus dilakukan adalah untuk mempersulit orang lain mengganggu sistem yang sedang digunakan, baik menggunakan komputer yang sifatnya pribadi, jaringan lokal ataupun jaringan global. Harus dimastikan sistem dapat berjalan dengan baik atau lancar serta kondusif, selain itu program dari aplikasinya masih dapat dipakai tanpa adanya suatu masalah.

Menurut (Garfinkel dan Spafford, 2018), seorang ahli dalam *computer security*, menyatakan bahwa "*A computer is secure if you can depend on it and its software to behave as you expect (intend). Trust describes our level of confidence that a computer system will behave as expected. (intended)*" yang dapat diartikan bahwa komputer dikatakan aman apabila dapat diandalkan serta perangkat lunaknya bekerja sesuai dengan apa yang diharapkan.

Dalam menjaga kemanan jaringan, diterapkan konsep atau hukum dasar yang biasa disebut dengan *CIA* yang merupakan, *Confidentiality* (kerahasiaan), *Integrity* (integritas),dan *Availability* (ketersediaan). *Confidentiality* adalah seperangkat aturan yang membatasi akses ke informasi. *Integrity* adalah jaminan bahwa informasi itu dapat dipercaya dan akurat, serta *Availability* yang merupakan konsep dimana informasi tersebut selalu tersedia ketika dibutuhkan oleh orang-orang yang memiliki akses atau wewenang.

Aspek dan Ancaman Terhadap Security

Adapun aspek dan ancaman terhadap *security* diantaranya yaitu:

1. *Privacy* adalah sesuatu yang sifatnya rahasia atau *private*. Intinya adalah suatu pencegahan supaya informasi tersebut tidak dapat diakses oleh orang yang tidak dikenal atau tidak berhak. Contohnya adalah, e-mail atau file-file lain yang tidak boleh dibaca orang lain meskipun ia adalah administrator.
2. *Confidentiality* adalah data yang diberikan kepada pihak lain dengan tujuan khusus namun tetap dijaga penyebarannya. Contohnya adalah data yang bersifat pribadi seperti: Nama, Alamat, No KTP, Telepon dan lain sebagainya.
3. *Integrity* atau penekanannya adalah suatu informasi tidak boleh diubah terkecuali oleh pemilik informasi tersebut. Terkadang data yang sudah terenskripsi pun tidak terjaga integritasnya karena adanya suatu kemungkinan *chaper text* dari enkripsi tersebut yang berubah. Contoh: Penyerangan integritas pada saat sebuah e-mail dikirimkan di tengah jalan kemudian disadap dan diganti isinya, sehingga e-mail tersebut yang sampai ketujuan telah berubah.
4. *Authentication* ini akan dilakukan sewaktu *user login* dengan menggunakan nama *user* serta *password*-nya. Hal ini biasanya akan berhubungan dengan hak akses seseorang, apakah dia pengakses yang sah atau bukan.
5. *Availability*, dalam aspek ini berkaitan dengan apakah suatu data tersedia ketika dibutuhkan atau diperlukan oleh pengguna. Jika sebuah data ataupun informasi terlalu ketat pengamanannya maka akan menyulitkan dalam akses data tersebut. Selain itu akses yang lambat juga dapat menghambat terpenuhinya aspek *availability*. Serangan yang sering dilakukan pada aspek ini adalah *Denial of Service* (DoS), yaitu merupakan penggagalan dari *service* sewaktu adanya permintaan data sehingga komputer tidak dapat melayaninya. Contoh lain dari *Denial of Service* ini adalah mengirimkan suatu *request* yang berlebihan sehingga dapat menyebabkan komputer tidak dapat lagi menampung beban tersebut dan hingga pada akhirnya komputer *down*.

Bentuk-Bentuk Ancaman dari Sistem Komputer

Adapun bentuk-bentuk ancaman dari sistem komputer diantaranya yaitu:

1. Interupsi (*Interruption*), Interupsi merupakan bentuk ancaman terhadap

ketersediaan, yang mana data rusak sehingga tidak dapat diakses bahkan digunakan lagi. Perusakan Fisik, contohnya: Perusakan pada Hardisk, Perusakan pada media penyimpanan yang lainya, serta pemotongan kabel jaringan. Perusakan Non fisik, contohnya: Penghapusan suatu file-file tertentu dari sistem komputer.

2. Intersepsi (*Interception*), Intersepsi merupakan bentuk sebuah ancaman terhadap kerahasiaan atau *secrecy*, yang mana pihak yang tidak berhak berhasil mendapatkan hak akses untuk membaca suatu data atau informasi dari suatu sistem komputer. Tindakan yang dilakukan dapat berupa melalui penyadapan data yang ditrasmisikan melalui jalur *public* atau umum yang dikenal dengan istilah *Writetapping* dalam *Wired Networking*, yang merupakan jaringan yang menggunakan kabel sebagai media dari transmisi data.
3. Modifikasi (*Modification*), Modifikasi merupakan sebuah bentuk dari ancaman terhadap integritas (*integrity*), yang mana pihak yang tidak berhak berhasil mendapatkan hak akses dalam mengubah suatu data ataupun informasi dari suatu sistem komputer. Data atau informasi yang diubah tersebut berupa *record* dari suatu tabel yang terdapat pada file *database*.
4. Pabrikasi (*Fabrication*), Pabrikasi adalah suatu bentuk ancaman terhadap integritas. Tindakan yang dilakukan adalah dengan meniru dan juga memasukkan suatu objek ke dalam sistem komputer. Objek yang dimasukkan biasanya berupa suatu *file* ataupun *record* yang disisipkan atau diletakkan pada suatu program aplikasi.

NMAP (*Network Mapper*)

Nmap ("*Network Mapper*") adalah sebuah *tool open source* untuk eksplorasi dan audit keamanan jaringan. *Nmap* menggunakan paket *IP raw* untuk mendeteksi *host* yang terhubung dengan jaringan dilengkapi dengan layanan (nama aplikasi dan versi) yang diberikan, sistem operasi (dan versi), apa jenis *firewall/filter* paket yang digunakan, dan sejumlah karakteristik lainnya.

Output Nmap adalah sebuah daftar target *host* yang diperiksa dan informasi tambahan sesuai dengan opsi yang digunakan. Hal kunci diantara informasi itu adalah "tabel *port* menarik". Tabel tersebut berisi daftar angka *port* dan protokol, nama layanan, dan status. Statusnya adalah terbuka (*open*), difilter (*filtered*), tertutup (*closed*), atau tidak difilter (*unfiltered*). Terbuka berarti bahwa aplikasi pada mesin target sedang mendengarkan (*listening*) untuk koneksi/paket pada *port* tersebut. Difilter berarti bahwa sebuah *firewall*, filter, atau penghalang jaringan lainnya memblokir port sehingga Nmap tidak dapat mengetahui apakah ia terbuka atau tertutup. Tertutup port tidak memiliki aplikasi yang sedang mendengarkan, meskipun mereka dapat terbuka kapanpun. Port digolongkan sebagai tidak difilter ketika mereka menanggapi *probe* Nmap, namun Nmap tidak dapat menentukan apakah mereka terbuka atau tertutup. Nmap melaporkan kombinasi status *open|filtered* dan *closed|filtered* ketika tidak dapat menentukan status manakah yang menggambarkan sebuah *port*. Tabel *port* mungkin juga menyertakan detil versi *software* ketika diminta melakukan pemeriksaan versi. Ketika sebuah pemeriksaan protokol IP diminta (-sO), Nmap memberikan informasi pada protokol IP yang didukung alih-alih *port-port* yang mendengarkan.

Fungsi utama dari Nmap adalah sebagai *port scanning*, menurut definisinya *port 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, https dan lain-lain) dan mencatat respon dari komputer target. Dengan cara seperti ini, *user* program *scanner* dapat memperoleh informasi yang berharga dari *host* yang mejadi target (Rosenelly dan Pulungan, 2011).

III. METODE PENELITIAN

Penelitian ini penulis menggunakan metode Analisis Monitoring dengan teknik *port scanning*. Tempat penelitian dilakukan di SMK Negeri 1 Kota Serang.

Pengumpulan data

Pengumpulan data dilakukan dengan tiga metode yaitu: Studi pustaka, dengan mengumpulkan data dari berbagai buku, artikel, jurnal, dan sebagainnya yang berhubungan dengan penelitian sebagai pendukung pembuatan penelitian. Observasi, dengan mengamati objek yang dianalisis monitoring secara langsung. Wawancara dengan memberikan pertanyaan kepada petugas SMK Negeri 1 Kota Serang yang bertanggung jawab di bidangnya.

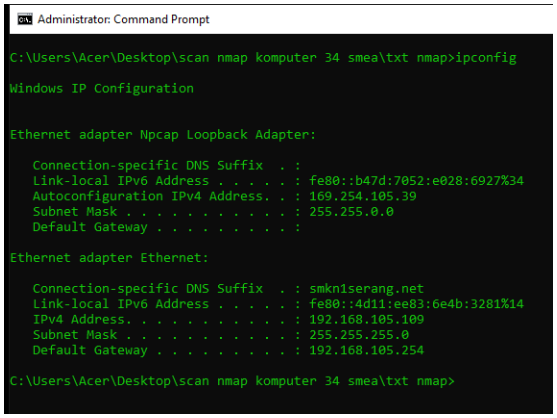
Peralatan Pendukung

Alat dan peralatan yang mendukung penelitian ini adalah sebagai berikut: Laptop, Komputer Client, OS Windows 7, *Software* Nmap.

IV. HASIL DAN PEMBAHASAN

Pengujian Jaringan Awal

Disini *user* menggunakan komputer yang telah terhubung pada jaringan sekolah di Lab. MM dengan komputer terkoneksi jaringan LAN. Setelah terhubung pada jaringan LAN *user* harus mencari *host* target untuk dilakukan *scanning* jaringan menggunakan *software* Nmap. Berikut ini gambaran hasil dalam mencari host target dengan menggunakan CMD :



Gambar 1. Mencari *Host* Target pada Komputer *User*

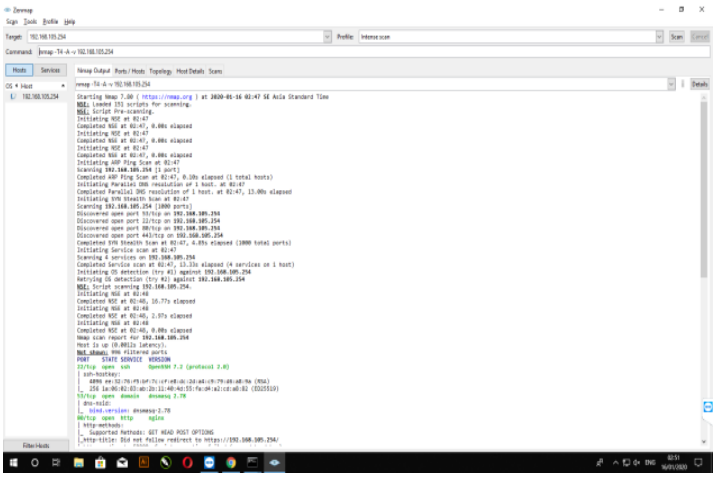
Pada gambar di atas *user* dapat mengetahui *host* target yang akan dilakukan *scanning* jaringan menggunakan *software* Nmap dengan melihat hasil dari *Ethernet adapter Ethernet*. Berikut daftar pada hasilnya:

a. Default Gateway: IP Address 192.168.105.254
   Default Gateway adalah gerbang jaringan pada perangkat Komputer user yang terhubung dengan jaringan LAN.
b. Subnet Mask: IP Address 255.255.255.0
   Subnet Mask dengan alamat kelas C. Sub prefinya yaitu /24
c. Ipv4: IP Address 192.168.105.109
   Merupakan alamat IP Address Laptop user dengan protocol IP versi 4.

Default Gateway IP 192.168.105.254 akan menjadi host target yang akan dilakukan scanning jaringan menggunakan software Nmap.

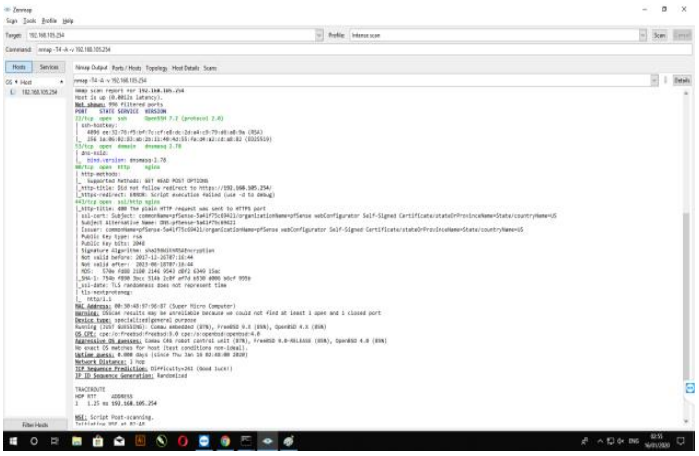
Pengujian Jaringan Akhir

1. Pengujian *Host* Target Jaringan pada Komputer *User*



Gambar 2. Pengujian Host Target Jaringan Pada Komputer User

Pada gambar di atas menggunakan perintah nmap –T4 –A –v 192.168.105.254. *User* melakukan *scanning* pada *host* target berupa IP Default Gateway jaringan LAN milik SMK Negeri 1 Kota Serang yang digunakan di Lab MM. User menggunakan perintah flag –T4 untuk mempercepat hasil scanning, flag –A untuk melakukan Aggresive Detection dan flag –v untuk menampilkan hasil Nmap lebih detil.



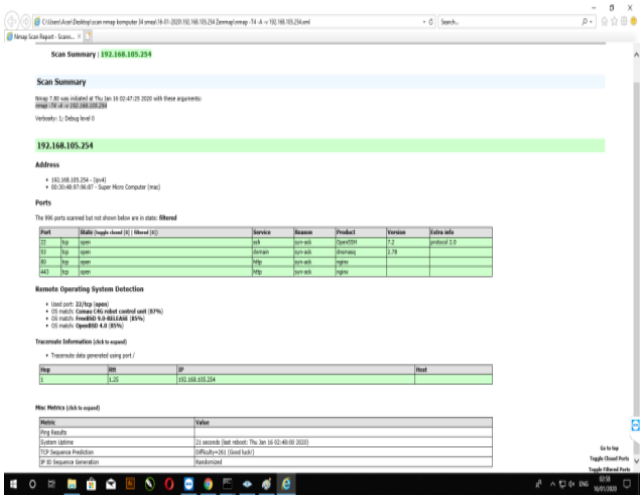
Gambar 3. Hasil Port Scanning 192.168.105.254 Zenmap

Pada gambar di atas merupakan hasil dari *scanning* yang dilakukan oleh Nmap pada host target IP 192.168.105.254 jaringan LAN milik SMK Negeri 1 Kota Serang. Pada hasil menunjukkan beberapa *port* yang terbuka (*open*). *Port* tersebut diantaranya port 22 tcp ssh, port 53 tcp domain, port 80 tcp nginx dan port 443 tcp nginx. *User* dapat mengetahui port-port, layanan dan versi layanan yang digunakan pada host target tersebut.

Pada gambar di atas mendapatkan informasi tentang Mac Address, perkiraan sistem operasi dan traceroute. Berikut hasilnya, Alamat MAC: 00: 30: 48: 97: 96: 87 (*Super Micro Computer*) yang

ISSN : 2406-7733
e-ISSN :2597-9922

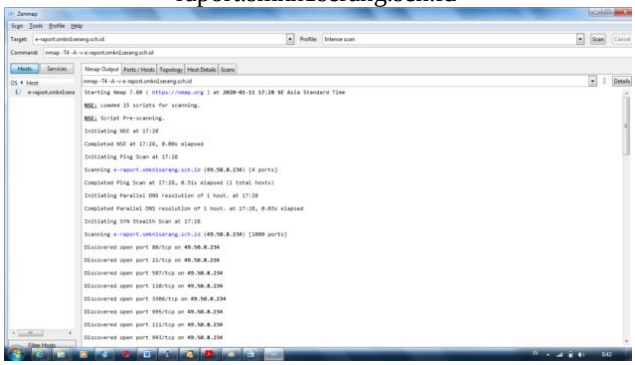
digunakan oleh host target 192.168.105.254, OS CPE: cpe: / o: freebsd: freebsd: 9.0 cpe: / o: openbsd: openbsd: 4.0 pada OS CPE dihasilkan field value type: o, yang mengidentifikasi bahwa sistem operasi yang digunakan pada host target menggunakan vendor freebsd, produk freebsd dan versi 9.0 dan atau sistem operasi vendor openbsd, produk openbsd dan versi 4.0. Aggressive OS guesses: Comau C4G robot control unit (87%), FreeBSD 9.0-RELEASE (85%), OpenBSD 4.0 (85%). TRACEROUTE 1.1.25 ms 192.168.105.254.



Gambar 4. Laporan Dalam Bentuk xml 192.168.105.254 Zenmap

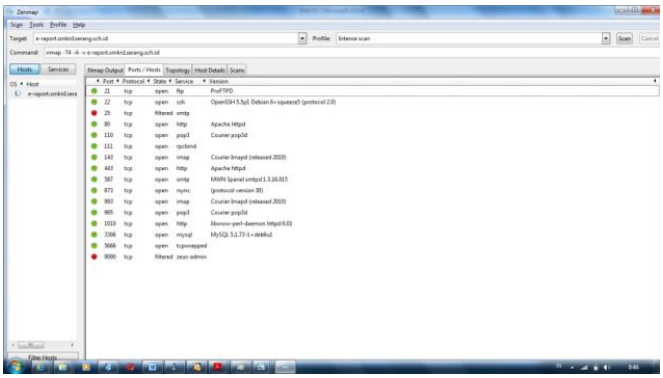
Bentuk output atau laporan dalam file xml yang dapat dibuka pada browser internet explorer. Ini merupakan bentuk ringkasan hasil dari pemindaian yang telah dilakukan oleh software Zenmap.Pada hasil ini user lebih mudah untuk melihat informasi yang didapat ketimbang melihat outputnya pada Zenmap. Terdapat info Scan Summary, Address, Ports, Remote Operation System Detection, Traceroute Information dan Misc Metrics.

2. Tahap Pengujian Host Target Web e-raport.smkn1serang.sch.id



Gambar 5. Pengujian Nmap e-raport.smkn1serang.sch.id zenmap

Pada gambar di atas menggunakan perintah nmap –T4 –A –v e-raport.smkn1serang.sch.id.user melakukan *scanning* pada *host* target berupa website milik SMK Negeri 1 Kota Serang. User menggunakan perintah flag –T4 untuk mempercepat hasil scanning, flag –A untuk melakukan Aggressive Detection dan flag –v untuk menampilkan hasil Nmap lebih detail.



Gambar 6. Hasil Port Scanning e-raport.smkn1serang.sch.id Zenmap

Pada gambar di atas merupakan hasil dari *scanning* yang dilakukan oleh nmap pada website e-raport.smkn1serang.sch.id milik SMK Negeri 1 Kota Serang. Pada hasil menunjukkan beberapa port yang terbuka (*open*) dan ter-*filtered*. Port tersebut diantaranya port 21 tcp ftp, 22 tcp ssh, 80 tcp http, 110 tcp pop3, 111 tcp rcpbind, 143 tcp imap, 443 tcp https, 587 tcp smtp, 873 tcp rsync, 993 tcp imap, 995 tcp pop3, 1010 tcp http, 3306 tcp mysql, 5666 tcp wrapped merupakan port yang terbuka dan por 25 tcp smtp dan 9090 tcp zeus-admin merupakan port yang ter-*filtered*. User dapat mengetahui port-port, layanan dan versi layanan yang digunakan pada website tersebut.

Gambar 7. Hasil Pendeteksi OS dan Traceroute e-raport.smkn1serang.sch.id

Pada gambar diatas mendapatkan perkiraan hasil sistem operasi yang dipakai oleh website smkn1serang.sch.id. berikut hasilnya, Tebakan OS

Agresif: HP Integrated Lights-Out 2 (89%), firewall Endian 2.3 atau IPCop 1.4.10 - 1.4.21 (Linux 2.4.31 - 2.6.22) (89%), Linux 2.6.32 (89%) , Netopia 3386 ADSL router (89%), Linux 2.6.18 - 2.6.22 (88%), Beat MIB MusicButler (87%), firewall Huawei Secospace USG6680 (87%), Panasonic WV-SP300 atau webcam WV-SF330 (87%), IPCop 2.0 (Linux 2.6.32) (87%), modem Motorola 2210-02 ADSL (87%). Terdapat catatan "Tidak ada OS yang cocok dengan host (kondisi pengujian tidak ideal)" ini menunjukan tidak ada perkiraan sistem operasi yang cocok pada host target. Info Layanan: Host: spanel-42224-ssl.maintenis.com, server42224.maintenis.com; OS: Linux; CPE: cpe: / o: linux: linux_kernel. TRACEROUTE (menggunakan port 80 / tcp), 1.9.00 ms 10.107.0.1; 2.6.00 ms 245.subnet125-160-11.speedy.telkom.net.id (125.160.11.245); 3. 6,00 ms remetuk.n.maintenis.com (49.50.8.234).

Gambar 8. Laporan Dalam Bentuk xml e-raport.smkn1serang.sch.id

V. PENUTUP

Kesimpulan

Dari hasil penelitian "Analisis Sistem Keamanan Jaringan Komputer Menggunakan Software NMAP" (Studi Kasus di SMK Negeri 1 Kota Serang). Didapat bahwa seorang sysadmin mampu melakukan *scanning* jaringan secara mudah untuk mendapatkan informasi yang ada pada jaringan. Seperti pemindai *port* jaringan dengan versi layanan dan mesin pendeteksi sistem operasi. User Nmap juga dapat melihat rute jaringan yang dilewati dalam mengakses sumber host target, seperti host jaringan dan host website.

Pada tahap pengujian menggunakan Nmap, penulis memakai beberapa host target untuk di analisis. Host target diantaranya adalah IP 192.168.0.1 (IP dari *Access Point*) dilakukan pengujian menggunakan Laptop penulis, IP 192.168.105.254 (ip dari koneksi LAN) dilakukan pengujian menggunakan Komputer User Lab MM, Host smkn1serang.sch.id dilakukan pengujian dengan Laptop penulis, dan Host e-raport.smkn1serang.sch.id dilakukan pengujian dengan menggunakan Laptop penulis.

Kesimpulan seputar penelitian berdasarkan pada pengujian dan analisis sistem keamanan jaringan komputer menggunakan *software Nmap* dengan melakukan tahap uji coba dan dapat ditarik kesimpulan diantaranya.

1. Software Nmap dapat digunakan untuk melakukan *scanning* jaringan pada host target berupa IP Address dan Website. Mampu melakukan pemindaian port jaringan dengan versi layanan dan mesin pendeteksi sistem operasi. Dapat membuat hasil nmap dengan bentuk file xml.
2. Dengan didapatnya status *port* terbuka (*open*), servis layanan dan informasi layanan, yang dihasilkan oleh pemindaian Nmap dengan beberapa macam teknik *scanning*. Sysadmin dapat mengetahui informasi yang didapat tersebut, sehingga kedepannya dapat melakukan tindakan-tindakan preventif dalam melakukan pencegahan keamanan jaringan baik terhadap keamanan jaringan router maupun pada website yang digunakan.
3. Sysadmin dapat menggunakan *software* Nmap untuk melakukan pemindaian jaringan dengan hasil secara realtime sesuai dengan keadaan yang terjadi.

Saran

Software Nmap merupakan perangkat lunak *open source* yang bisa terus berkembang dan demi terciptanya sebuah aplikasi yang mampu mendeteksi *port* jaringan, informasi layanan jaringan, perkiraan sistem operasi yang digunakan dan script NSE yang digunakan untuk *Network Discovery*, *Version Detection System*, *Vulnerability Detection*, *Backdoor Detection* dan *Vulnerability Exploitation*.*Software Nmap* bertujuan untuk memudahkan *sysadmin* dalam menemukan informasi jaringan dan kerentanan keamanan jaringan yang ada. Ada beberapa saran yang dapat dijadikan pertimbangan diantaranya:

1. Banyak *software* sejenis yang dapat digunakan, mulai dari versi *pro* berbayar, *Free* gratis dan *Open Source* dengan kemampuan berbeda dan teknik yang berbeda pula, sehingga dalam penelitian dapat memilih *software* sesuai yang dibutuhkan dan diinginkan.
2. Untuk pengembangan penelitian kedepannya bisa dengan menggunakan sistem operasi selain windows, kerena software Nmap dapat berjalan pada berbagai platform termasuk Unix, Linux, BSD, Windows, dan Mac OS.
3. Untuk penelitian ke depannya bisa dilakukan penginstallan di bagian *server*.

DAFTAR PUSTAKA

Abdullah. (2016). *Kung-Fu Hacking Dengan Nmap (Automatic Vulnerability Scanning) Nmap Scanning Report*. Yogyakarta: Penerbit Andi.

Amalia, Dina. (2018). *Pengertian Jaringan Komputer dan Manfaatnya*. [Online]. Tersedia: https://idwebhost.com/blog/pengertian-jaringan-komputer-dan-manfaatnya/ [12 Agustus 2019]

Angir, Devi C, *et al*. (2015). "Vulnerability Mapping pada Jaringan Komputer di Universitas X". *Jurnal Infra*. Vol. 3. No. 2. Surabaya: Universitas Kristen Petra.

Anugrah, Ino., Rahmanto, RH. (2017). "Sistem Keamanan Jaringan Local Area Network Menggunakan Teknik De-Militarized Zone". *Jurnal Penelitian Ilmu Komputer, Sistem Embedded & Logic*. Vol. 5. No. 2. Bekasi: Universitas Islam 45.

Febriyandra, Danang. (2019). "Enkripsi dan Deskripsi: Pengertian, Jenis, Macam dan Contoh". [Online] Tersedia: https://www.mastekno.com/id/pengertian-enkripsi-deskripsi/. [13 Januari 2020]

Garfinkel dan Spafford. (2018). Information Security. Dalam *CSE870 - Advanced Software Engineering : Security Intro, spring 2018*. Michigan USA: Michigan State University. Tersedia: http://www.cse.msu.edu/~cse870/Lectures/Notes/10-security-intro-2018-notes.pdf.

Gollmann, Dieter. (1999). *Computer Security*. Chichester, West Sussex, PO19 8SQ England: John Wiley & Sons Ltd.

Hendrawan, Ade, *et al*. (2014). "Analisis Keamanan Jaringan Dengan Metode Security Lifecycle Di Universitas Ibn Khaldun Bogor". *Jurnal Teknik Informatika*. Vol. 2. No. 2. Bogor: Unversitas Ibn Khaldun Bogor.

Howard, John D. (1997). "An Analysis Of Security Incidents On The Internet". *Disertasi* pada Carnegie Mellon University Pittsburgh, Pennsylvania 15213 USA.

Isnanto, Burham. (2015). "Prototipe SMS Gateway Pemantau Jaringan LAN Dan Network Pada PT Bangka Pesona Media". *Jurnal Teknologi Informatika Dan Komputer Atma Luhur*. Vol. 2 No. 1. Maret 2015 ISSN : 2406-7962. Pangkal Pinang: STMIK Atmaluhur Pangkal Pinang.

Itgid.org. (2019). "5 Langkah Mudah Melakukan Audit Keamanan Jaringan (Network Security Audit)". [Online] Tersedia: https://www.itgid.org/5-langkah-mudah-melakukan-audit-keamanan-jaringan-network-security-audit/. [13 Januari 2020]

Kim, Peter. (2014). *The Hacker Playbook Practical Guide To Penetration Testing*. South Carolina: Secure Planet LLC.

Kuperman, Idan. (2018). "Conducting Network Security Audits in a Few Simple Steps". [Online] Tersedia: https://www.portnox.com/blog/network-security/conducting-network-security-audits-in-a-few-simple-steps/. [13 Januari 2020]

Lyon, "Fyodor" Gordon. (2009). *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*. California: Insecure, insecure.org., nmap.org

Lyon, Gordon. (2009). *Nmap Network Scanning (Nmap Reference Guide)*. [Online]. Tersedia: https://nmap.org/book/man.html [12 Maret 2019]

Maxmanroe. (2016). *Topologi Jaringan: Pengertian, Jenis, dan Gambar Topologi Jaringan*. [Online]. Tersedia: https://www.maxmanroe.com/vid/teknologi/komputer/topologi-jaringan.html [12 Agustus 2019]

Mulyawan, Rifqi. (2018). "Mengenal Pengertian Sistem Keamanan Komputer: Menurut Para Ahli, Sejarah dan Jenis Ancamannya". [Online] Tersedia: https://rifqimulyawan.com/pengertian-sistem-keamanan-komputer.html [13 Januari 2020]

Muniz, Joseph & Aamir Lakhani. (2013). *Web Penetration Testing with Kali Linux*. Birmingham : Packt Publishing Ltd.

Rosnelly, Rika & Pulungan, Reza. (2011). Membandingkan Analisa Trafik Data Pada Jaringan Komputer Antara Wireshark Dan Nmap. *Konferensi Nasional Sistem Informasi*. Yogyakarta

Sibero, Alexander FK. (2011). *Kitab Suci Web Programing*. Yogyakarta: MediaKom.

Sofana, Iwan. (2013). *Membangun Jaringan Komputer (Wire & Wireless) untuk Pengguna Windows dan Linux*. Bandung: Penerbit Informatika.

Syafrizal, Melwin. (2005). *Pengantar Jaringan Komputer*. Yogyakarta: Penerbit Andi.

Text.co.id. (2019). "Sistem Keamanan Komputer : Pengertian, Lingkup, Aspek Dan Bentuknya". [Online]. Tersedia: https://teks.co.id/sistem-keamanan-komputer/ [13 Januari 2020]

Yachya, Egi W. (2016). "Analisis Keamanan Jaringan Server Web dan Hotspot Menggunakan Tool Nmap dan Nessus di Pusat Penelitian Limnologi LIPI". Depok: Universitas Gunadarma.