Merancang Keamanan Jaringan Internet Menggunakan Program Network Mapper Di Linux Ubuntu

Teuku Rizky Chairil, Jenih
Program Studi Ilmu Komputer
Fakultas Teknologi Informasi, Universitas Respati Indonesia
Email : subuhtime@gmail.com, jenih@fti.urindo.ac.id

ABSTRAK

Upaya serangan dari luar pada ekosistem data utama menjadi masalah yang terus timbul bagi P.T Solusi Penjaminan Aman maupun instansi terkait yang telah menyajikan akses datanya secara digital, sejalan mengiringi perkembangan teknologi informasi yang cepat dan terbaru. Administrator dapat menggunakan Nmap untuk menguji tingkat keamanan wilayah dengan cara Network Penetration dan Security audit pada sistem jaringannya. Nmap merupakan utilitas yang mampu mendukung sistem keamanan jaringan yang lebih baik dengan fitur layanan populer seperti: port scanning, identifikasi host, dan Nmap Scipting Engine (NSE). Penetrasi dilakukan dengan metode pentes yaitu Teknik Port Scanning Nmap, hasilnya dapat mengetahui kondisi port jaringan P.T Solusi Penjaminan Aman seperti IP Default gateway, host aktif, seri perangkat, dan port terbuka yang dapat menjadi ancaman dan merancang keamanan jaringan dengan menggunakan IDS untuk P.T Solusi Penjaminan Aman.
Kata kunci : Keamanan, Jaringan, Penetrasi,pengujian, nmap.

ABSTRACT

Attempts to attack from outside on the main data ecosystem have become a problem that continues to arise for PT Solusi Penjaminan Aman and related agencies that have provided digital access to their data, in line with the fast and latest developments in information technology. Administrators can use Nmap to test the level of regional security by means of Network Penetration and Security audits on their network systems. Nmap is a utility capable of supporting a better network security system with popular service features such as: port scanning, host identification, and the Nmap Scipting Engine (NSE). Penetration is carried out using the pentest method, namely the Nmap Port Scanning Technique, the results can determine the condition of the P.T network port Secure Guarantee Solution such as Default IP gateway, active host, device series, and open ports that can be a threat and design network security using IDS for P.T Guarantee Solution Safe.
Keywords: Security, Network, Penetration, testing, nmap.

PENDAHULUAN

P.T Solusi penjaminan aman adalah perusahaan penyedia solusi terbaik untuk memastikan keabsahan suatu dokumen, baik surat jaminan, dokumen lelang, kontrak dan lainnya. Menyediakan layanan dari berbagai platform untuk dapat dengan mudah digunakan oleh para stakeholder dalam dunia lelang atau pengadaan dengan nama-nama produk Penjaminan Online,Portal e-Polis dan ePonten. Walaupun PT ini sudah berjalan dengan baik diera digilitallisasi dengan melakukan kerja sama dengan banyak perusahaan terutama untuk masalah keamanan lalu lintas jaringannya dengan peruri code menggunakan standar audit dengan ISO 27001 yang merinci tugas manajerial seperti penilaian risiko dan meninjau keamanan.Tetapi masih saja ada celah keamanan jaringan untuk di eksploitasi.

Website P.T Solusi Penjaminan Aman sering mengalami gangguan dari luar seperti DDos, Malware dan Phising, sehingga kinerja website terganggu.Dalam hal ini pengecekan keamanan akan dilakukan port scanning untuk pemetaan secara langsung, melihat keamanan jaringan website PT.Solusi Penjaminan Aman menggunakan Network Mapper(Nmap) dan merancang topologi arsitektur keamanan jaringan.

METODE PENELITIAN

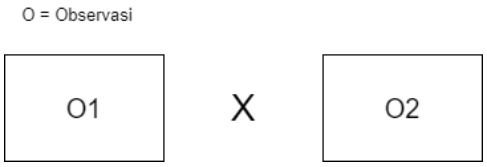
Dengan memperhatikan cakupan kegiatan penelitian dari aspek kurun waktu pelaksanaan kegiatan penelitian, cara memperoleh informasi yang dibutuhkan, tujuan penelitian dan merujuk lebih lanjut kepada referensi serta ahli jaringan komputer, sehingga penelitian ini bersifat deskriptif, karena tujuan dari penelitian ini adalah bagaimana meminimalisir vulnerabilitas keamanan jaringan komputer. Pada bab metode penelitian ini akan dijelaskan tentang pendekatan penelitian yang memang menggunakan metode penetration testing.

a. Metode R&D (Research and Development)

Metode penelitian yang digunakan dalam penelitian ini adalah metode R&D (Research and Development). Metode penelitian dan pengembangan adalah metode penelitian yang digunakan untuk menghasilkan produk tertentu, dan menguji keefektifan produk tersebut. Menurut Amile and Reesnes (2015:297), Research and Development (R&D) adalah metode penelitian yang digunakan untuk menghasilkan produk tertentu, dan menguji keefektifan produk tersebut. Berdasarkan definisi di atas dapat dijelaskan bahwa metode R&D adalah metode penelitian yang digunakan untuk menghasilkan produk tertentu dan untuk menyempurnakan suatu produk yang sesuai dengan acuan dan kriteria dari produk yang dibuat sehingga menghasilkan produk yang baru melalui berbagai tahapan dan validasi atau pengujian. Peneliti melakukan penelitian terlebih dahulu untuk mengumpulkan sejumlah data yang dibutuhkan selanjutnya dilakukan pengembangan sistem dan melakukan pengujian dan evaluasi terhadap sistem yang dibuat.

b. Eksperimental

Eksperimen dapat dilakukan dengan cara membandingkan dengan keadaan sebelum dan sesudah memakai sistem baru (before-after) atau dengan membandingkan yang tetap menggunakan sistem yang lama. Dalam hal ini ada kelompok eksperimen dan kelompok kontrol.



Gambar 1 Logika Eksperimental

Berdasarkan gambar 1 tersebut dapat diberikan penjelasan sebagai berikut. Eksperimen dilakukan dengan membandingkan hasil observasi O1 dan O2. O1 adalah nilai sistem keamanan jaringan yang lama, yang belum memiliki monitoring dari keamanan jaringan tersebut. Karena hanya menggunakan

ISO27001 untuk mengandalkan sistem keamanan jaringannya. Sedangkan O2 adalah sistem keamanan jaringan yang sudah diaudit menggunakan program Network Mappper (Nmap) dan memonitoring sistem keamanan jaringan menggunakan Snort IDS. Sistem keamanan yang baru akan lebih efektif jika nilai O2 lebih besar dari nilai O1.

c. Tahapan Pengujian

Berikut ini adalah penjelasan tahapan-tahapan yang dilakukan pada penelitian ini:

1) Ruang Lingkup (Scope)

Tahapan awal adalah menentukan batasan terhadap website yang menjadi target yaitu Web penjaminan-online.id Penulis hanya akan melakukan vulnerability scanning dan tidak melakukan eksploitasi terhadap website tersebut.

2) Reconnainsance (Footprinting dan Information Gathering)

Tahapan ini dilakukan untuk mendapatkan informasi sebanyak-banyaknya terkait dengan perangkat apa saja yang digunakan, versi OS dan lain-lain.

3) Vulnerability Scanning

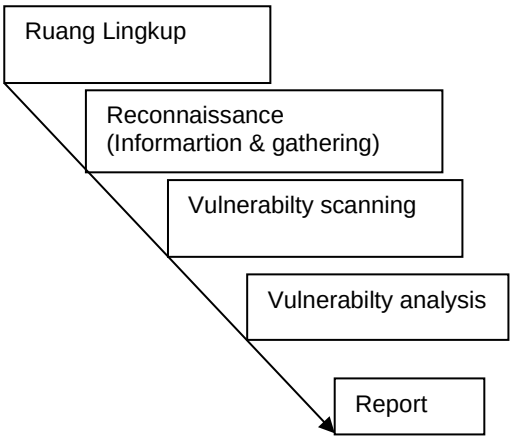
Tahapan ini melakukan scanning dengan memanfaatkan tools yang ada, agar mendapatkan informasi seperti daftar port yang terbuka,host,O.S dan lain-lain.

4) Vulnerability Analysis

Tahapan ini melakukan analisis terhadap informasi yang ditemukan setelah dilakukan scanning terhadap website target.

5) Report

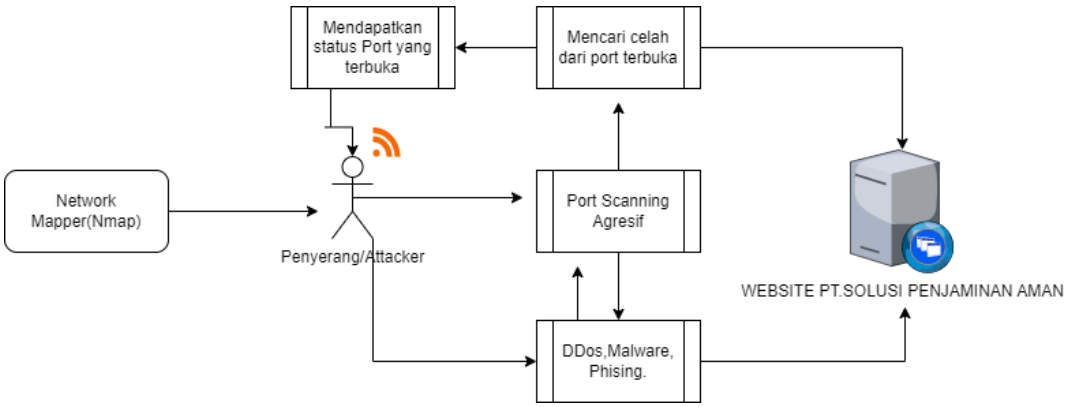
Tahapan ini adalah hasil analisa dari celah keamanan website target yang akan diberikan kepada pengelola website target untuk mengetahui apa saja kelemahan yang ada dalam website tersebut.



Gambar 2 Tahapan pengujian

d. Analisa Kerentanan

Dalam alur serangan port scanning ini akan diceritakan bagaimana terjadinya serangan.



Gambar 3 Alur Port Scanning Menggunakan Nmap

e. Port Scanning (Pemetaan)

website yang sudah terkoneksi dengan internet umumnya rentan dengan keamanan jaringan dari hosting tersebut. Maka dari itu penulis akan menjalankan teknik port scanning yang biasa di lakukan untuk pengujian pemetaan, untuk melihat celah port mana saja yang bisa disusupi oleh para cracker yang cerdas membobol sistem keamanan jaringan. Contoh dari port scanning itu seperti layaknya sebuah rumah yang sedang di pantau oleh para pencuri untuk mendapatkan celah keamanan dari rumah tersebut agar para pencuri bisa mendapatkan apa yang mereka mau. Port port ini , ibaratnya seperti sebuah jendela dan pintu awalan dari hal pertama terjadinya pencurian. Maka dari itu penulis akan melakukan teknik ini, melakukan pemetaan terhadap website penjaminan-online.id.

f. Perancangan Sistem Jaringan

Risiko masalah keamanan jaringan semakin besar seiring meningkatnya popularitas penggunaan jaringan nirkabel.

Kendala yang biasanya sering terjadi pada sebuah sistem atau jaringan yaitu akses ilegal, pembajakan, dan aktivitas mencurigakan lainnya. IDS adalah sebuah teknologi untuk mengatasi masalah tersebut. IDS memiliki peran cukup penting sebagai basis pertahanan dalam jaringan. Sistem ini mampu menangkal berbagai jenis ancaman berbahaya terutama masalah yang berkaitan dengan *intrusion* atau akses ilegal. Oleh sebab itu, mempelajari dan menerapkan IDS sudah selayaknya diberi perhatian lebih guna membangun sistem keamanan jaringan untuk website ataupun server.

g. Intrusion detection system

intrusion Detection System atau IDS adalah sebuah sistem yang memonitor trafik jaringan untuk mendeteksi aktivitas-aktivitas mencurigakan. Jika aktivitas mencurigakan tersebut ditemukan, IDS akan melaporkannya dalam bentuk peringatan. Dengan kata lain, IDS bisa dibilang sebagai perangkat lunak pemindai sistem jaringan guna terhindar dari kegiatan yang melanggar kebijakan. Secara teknis, IDS pada dasarnya dibuat untuk mendeteksi upaya-upaya serangan siber. Sistem ini tidak memiliki fungsi merespon atau memblokir upaya serangan tersebut. Segala bentuk aktivitas berbahaya biasanya dilaporkan ke pihak administrator atau diteruskan ke Security Information and Event Management (SIEM) secara terpusat. Selanjutnya SIEM akan mengintegrasikan output dari sejumlah sumber sekaligus memfilter setiap aktivitas.

h. Cara kerja IDS

Cara kerja IDS adalah mendeteksi dan menemukan ancaman. dimana sistem akan mendeteksi aktivitas berbahaya. IDS memantau dan mencocokan trafik dengan pusat data intrusi yang menyimpan kumpulan data berbagai jenis penyusupan atau serangan. Jika terdapat kecocokan, selanjutnya IDS akan mengidentifikasi sekaligus mengirimkan peringatan. IDS juga dapat bekerja menggunakan

metode lain, yakni memantau berkas sistem operasi. Cara ini memungkinkan IDS mendeteksi aktivitas yang berpotensi merubah file tertentu pada operating system, terutama log file. Selanjutnya IDS akan mengirimkan peringatan bilamana sebuah aktivitas diidentifikasi sebagai suatu ancaman.

i. SNORT Mode

Snort dapat dikonfigurasi menggunakan tiga mode utama: sniffer, packet logger, dan network intrusion detection.

1. Mode Sniffer : pada mode ini, snort bertugas untuk menangkap paket-paket pada lalu lintas jaringan serta menampilkannya ke layar dalam bentuk aliran yang bersifat continuous pada sebuah layar
2. Mode Logger : pada mode ini, snort akan mencatat log dari paket-paket pada lalu lintas jaringan dan menyimpannya ke dalam disk.
3. Mode Intrusion Detection : snort akan memonitor semua traffic yang lewat dan membandingkan dengan rule yang di definisikan oleh user. Snort IDS mirip dengan *tcpdump/wireshark* , tetapi memiliki outpu tyang lebih bersih dan bahasa aturan yang lebih fleksibel. Sama seperti tcpdump / wireshark, snort akan mendengarkan antarmuka tertentu, atau membaca jejak paket dari sebuah file.

HASIL DAN PEMBAHASAN

a. Filtering Port

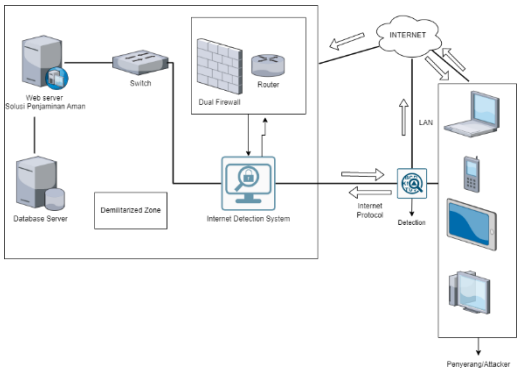
Pada screened subnet gateway digunakan dua buah screened host gateway, yang meng-isolir LAN dari internet, dan menciptakan sebuah wilayah yang disebut Demilitarized zone(DMZ), keamanan jaringan lokal yang berfungsi melindungi sistem dari peretas yang ingin mencoba memaksa masuk ke

dalamnya tanpa memiliki izin akses. Nantinya, saat peretas menyerang server yang disimpan di dalam DMZ ini, maka dia hanya dapat mendapatkan akses host yang berada di DMZ, bukan pada jaringan internal.

Penulis mengkonfigurasi DMZ yang paling banyak dipakai dengan dual firewall yang dapat diperluas untuk pengembangan sistem yang lebih kompleks.

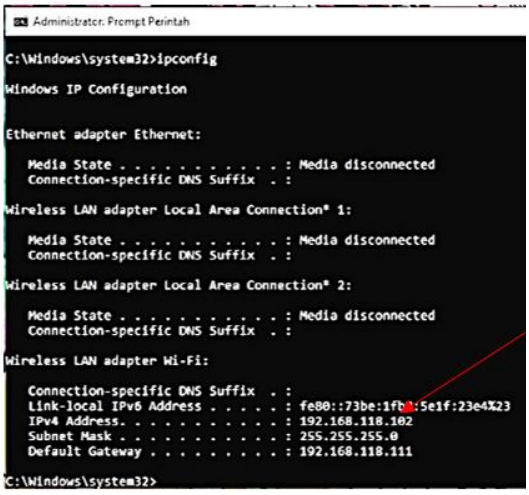
Karena menggunakan dua firewall, DMZ tersedia pada kedua firewall untuk keamanan yang lebih baik dibanding single firewall. Firewall yang pertama hanya akan mengizinkan trafik eksternal menuju DMZ, sedangkan yang kedua mengizinkan trafik yang berasal dari DMZ menuju jaringan internal. Peretas harus dapat melewati kedua firewall untuk mendapatkan otorisasi jaringan lokal (LAN).

Kontrol keamanan juga dapat disempurnakan untuk beberapa jenis jaringan, yang berarti IDS (intrusion detection system) dalam DMZ dapat dikonfigurasi untuk memblokir permintaan trafik selain HTTPS menuju TCP port 443.



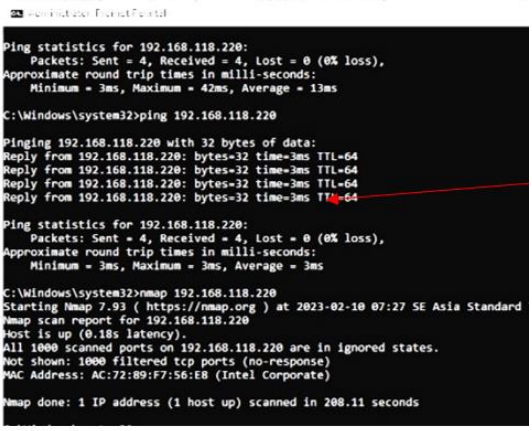
Gambar 4 Topologi Keamanan Jaringan Solusi Penjaminan Aman

b. Intrusion Detection System



Gambar 5 Command Prompt Administrator

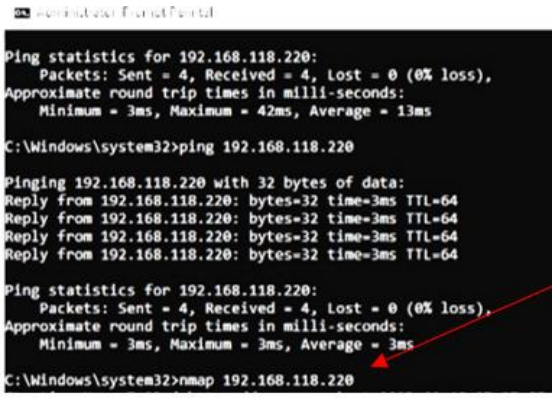
Penulis melakukan port scanning menggunakan operasi sistem windows 10, dengan alamat ip 192.168.118.102.



Gambar 6. Ping

Penjelasan dari gambar 6.

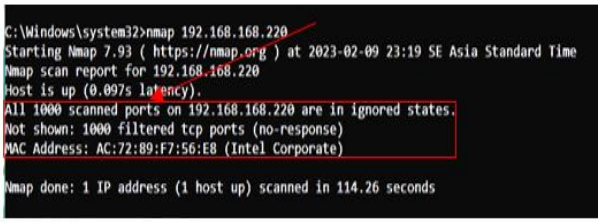
Snort IDS memberi peringatan bahwa terdapat port scanning menggunakan Nmap dengan alamat ip 192.168.118.102.



Gambar 7 Menjalankan Nmap

Penjelasan dari gambar 6.5:

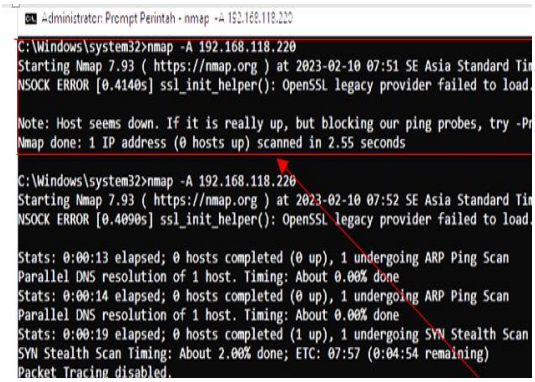
Penulis melakukan port scanning terhadap alamat ip server 192.168.118.220



Gambar 8 Output port scanning di command prompt administrator

Penjelasan dari gambar 8:

Snort IDS memfilter 1000 port, keluaran status no-response, yang artinya Snort IDS menutup celah atau telah memfilter port scanning yang telah di lakukan nmap.



Gambar 9 Mode agresif scanning nmap

Penjelasan dari gambar 9:
Nmap tidak dapat melakukan scanning dengan alamat ip 192.168.118.220, walaupun dalam mode agresif.

SIMPULAN

Dari hasil penelitian yang telah penulis lakukan dengan banyak pertimbangan dimana website penjaminan-online.id masih dalam mode pengembangan maka dapat ditarik kesimpulan dari diri penulis, yaitu:

1. Tingkat keamanan website P.T Solusi Penjaminan Aman masih perlu ditingkatkan. Hal ini dibuktikan dengan penyerangan port scanning pada gambar 4.1.
2. Dengan menggunakan nmap dan snort telah di ketahui adanya celah keamanan port yang terbuka.
3. Dengan dibangunnya topologi jaringan keamanan lebih efektif untuk mengendalikan serangan dari luar.

DAFTAR PUSTAKA

Hartono & Onno W.Purbo (2022). Membangun dan Menguji Keamanan Website. Network Mapper(Nmap), 9(9), 111-118.

Iwan Sofana & Rifkie Primartha (2019). Network Security dan Cyber Security. Byod(Bring Your Own Device),VPN(Virtual Private Network), 4(4), 160-172.

Rusydianto, M. R., Budiman, E., & Setyadi, H. J. (2017). Implementasi Teknik Hacking Web Server Dengan Port Scanning Dalam Sistem Operasi Kali Linux. Prosiding Seminar Nasional Ilmu Komputer Dan Teknologi Informasi E-ISSN, 2(2).

Kelrey, A. R., & Muzaki, A. (2019). Pengaruh Ethical Hacking Bagi Keamanan Data Perusahaan. CyberSeccurity Dan Forensik Digital, 2(2), 77–81.

Setia, T. P., Aldya, A. P., & Widiyasono, N. (2019). Reverse Engineering untuk Analisis Malware Remote Access Trojan. Jurnal Edukasi Dan Penelitian Informatika (JEPIN), 5(1), 40.

Sidabutar, J. (2020). Desain Jaringan Komputer Terintegrasi Menggunakan Arsitektur Campus LAN. Jurnal Jaring SainTek, 2(1), 25–32.

Rendro, D. B., Ngatono, & Aji, W. N. (2020). Analisis Monitoring Sistem Jaringan Komputer Menggunakan Software Nmap. PROSISKO: Jurnal Pengembangan Riset Dan Observasi Sistem Komputer, 7(2), 108–115.

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

Wahid, Aceng Abdul. Perancangan Konsep Smart Campus Menggunakan Jaringan Internet of Things (IOT). Jurnal Ilmu Informatika dan Manajemen STMIK, 2019.

Prof. Dr.Sugiyono. Metode Penelitian Kuantitatif, Kualitatif dan R&D. Metode Penelitian Pengembangan, (4)16, 297-313.