SATIN – Sains dan Teknologi Informasi
Journal Homepage : http://jurnal.sar.ac.id/index.php/satin

Network Penetration dan Security Audit Menggunakan Nmap

Dede Sudirman [1], Akma Nurul Yaqin [2]
[1]Universitas Sangga Buana, sudirmandede98@gmail.com, Jl PHH Mustofa (Suci) No.68, Bandung,Indonesia
[2]Universitas Sangga Buana, akmanurul375 @gmail.com, Jl PHH Mustofa (Suci) No.68, Bandung, Indonesia

Informasi Makalah

Submit : Apr 01, 2021
Revisi : May 31, 2021
Diterima : Juni 14, 2021

Kata Kunci :

Jaringan Komputer
Network Penetration
Audit Keamanan jaringan
Nmap

Abstrak

Upaya serangan dari luar pada ekosistem data utama menjadi masalah dalam keamanan jaringan yang terus timbul bagi perusahaan maupun instansi terkait yang telah menyajikan akses datanya secara digital, sejalan mengiringi perkembangan teknologi informasi yang cepat dan terbarukan. 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 berhasil mengisi jajaran 125 Top alat keamanan jaringan teratas bersanding dengan *Wireshark*, *Metasploit*, *Nessus* dan *Nikto* berdasarkan *SecTools.org*. Fleksibel dalam penggunaan di imbangi dengan fitur layanan populer seperti: *port scanning*, identifikasi host, dan *Nmap Scipting Engine* (*NSE*). Penetrasi dilakukan dengan 2 metode pentes yaitu *Black Box Testing dan White Box Testing*, keduanya dipadukan dengan Teknik *Port Scanning* Nmap, hasilnya dapat mengetahui kondisi jaringan SMA ALFA CENTAURI seperti *IP Default gatway*, host aktif, seri perangkat, dan *port* terbuka yang dapat menjadi ancaman.

Abstract

Attempts to attack from outside the main data ecosystem are a problem in network security that continues to arise for companies and related agencies that have provided digital data access in line with the rapid and renewable development of information technology. Administrators can use Nmap to test regional security levels by means of network penetration and security audits on network systems. Nmap is a utility capable of supporting better network security systems by successfully filling in the top 125 top network security tools alongside Wireshack, Metasploit, Nessus and Nikto based on SecTools.org. flexibility in use is offset by popular service features such as port scanning, host identification, and the Nmap Scipting Engine (NSE). Penetration is done with 2 testing methods namely Black Box Testing and White Box Testing, both combined with Nmap Port Scanning Technique, the result can know the condition of ALFA CENTAURI high school networks such as IP Default gateway, active host, device series, and open port that can be a threat.

Dede Sudirman,
Email: sudirmandede98@gmail.com.

SATIN – Sains dan Teknologi Informasi
Vol. 07, No. 01, Juni 2021, pp. 32-44
ISSN: 2527-9114, DOI 10.33372/stn.v7i1.702

1. Pendahuluan

Kebutuhan interaksi perangkat komputer satu dengan lainnya melalui jaringan semakin besar, dukungan terhadapnya menjadi gerbang utama dari pertukaran data pada wilayah lokal maupun akses yang lebih luas melalui internet. sejalan dengan hal itu, SMA Alfa Centauri Bandung telah menggunakan infrastruktur jaringan komputer untuk mendukung kinerja yang lebih cepat dan efektif, seperti dukungan terhadap kebutuhan Administrasi, Sistem Informasi Manajemen (*SIM Alfa*), Portal Informasi (Guru, Siswa, Karyawan), *E-raport* dan Ujian *Online*.

Keamanan jaringan komputer tentunya menjadi masalah yang harus di hadapi ketika memutuskan memulai akses informasi secara *online*, terlebih jika itu berhubungan dengan data sensitif yang dapat mempengaruhi kinerja dan reputasi, beberapa perusahaan besar rela mengeluarkan uang jutaan dolar untuk menangani isu keamanan jaringan di wilayah perusahaannya dengan merekrut tenaga profesional secara khusus atau menjalin kerja sama secara terbuka dengan program *bug bounty*, contohnya seperti Google yang membayar *bug hunter* dengan level kerentanan yang bervariasi, di kutip dari *Google Vulnerability Reward Program* (*VRP*) untuk penemuan kerentanann level bug kualifikasi tertentu di berikan *reward* sampai $100 - $31,337 dan untuk kasus tertentu di hargai juga dengan pantas.

Membangun Sistem Keamananan yang kuat tidaklah mudah dan murah, apalagi jika harus mengamankan setiap lini akses, salah satunya jaringan komputer, kerentanan jaringan dapat terdeteksi dengan bantuan *tools* gratis seperti Nmap, melaluinya Administrator jaringan dapat mendeteksi seluruh informasi dengan *monitoring* salah satunya mengidentifikasi *port* yang terbuka maupun tertutup dari paket layanan, dari informasi ketersediaan tersebut selanjutnya dapat di ketahui bagaimana status dari wilayah jaringannya, apakah memiliki tingkat keamanan yang baik atau sebaliknya.

2. Studi Literatur

Jaringan Komputer adalah sebuah sistem yang terdiri atas komputer-komputer yang di desain untuk dapat berbagi sumber daya (Sabdho & Ulfa, 2018). Secara umum interaksi akan terjadi pada dua atau lebih komputer yang terhubung untuk melakukan komunikasi data dimana jaringan di hubungkan melalui media fisik dan dukungan *software* sebagai fasilitas komputer untuk dapat berkomunikasi. Desain jaringan komputer terintegrasi, harus dimulai dengan perencaaan(Sidabutar, 2020). Infrastruktur pembangun mengikuti standar layaknya skala maupun kualitas layanan. *Client-server* adalah arsitektur jaringan yang memisahkan *client* dengan server (Muzawi et al., 2017). Server menyimpan semua layanan dan data yang dibutuhkan oleh pengguna(Santoso, 2019). Umunya wilayah pusat atau sering di kenal dengan komputer Server sebagai penyedia sumber utama dan lainnya bertindak sebagai klien yang meminta atau menerima data kiriman dari pusat sesuai dengan permintaan.

2.1 Keamanan Jaringan Komputer

Keamanan jaringan didefinisikan sebagai sebuah perlindungan dari sumber daya terhadap upaya penyikapan, modifikasi, utilisasi, perlarangan dan perusakan oleh *person* yang tidak diijinkan (Putra, 2016). Umumnya koneksi lalu lintas pada jaringan komputer tidak ada jaminan selalu aman, upaya percobaan akses jaringan tidak sah dapat saja terjadi kapan saja, terlebih jika telah menyasar pada area jaringan publik dan terdapat ekosistem data yang menggiurkan untuk di tambang. Syarat dari keamanan adalah *Prevention* (pencegahan) yaitu

SATIN – Sains dan Teknologi Informasi
Vol. 07, No. 01, Juni 2021, pp. 32-44
ISSN: 2527-9114, DOI 10.33372/stn.v7i1.702

memperkecil peluang penembusan oleh pemakai yang tak terotorisasi (Alamsyah et al., 2020).

Keamanan Jaringan komputer menjadi hal mutlak untuk di perhatikan oleh perusahaan ketika melihat segudang manfaat dari perencanaan pembangunan jaringan komputer yang akan di dapat, pada umumnya konsep keamanan jaringan diantaranya sebagai berikut:

a. *Risk* atau resiko, merupakan tingkat gangguan yang mungkin saja dapat terjadi, dan mampu memberikan dampak pada ketersediaan dari jaringan komputer secara keseluruhan.
b. *Threat* atau ancaman, adanya kemungkinanan serangan yang dapat menghambat lalu lintas jaringan yang aktif bahkan beberapa peluang ancaman dapat membuat sumber utama mati total.
c. *Vurnability* atau kerentanan, celah keamanan pada sistem yang dapat di kategorikan pada beberapa level, misalnya rendah, menengah sampai tinggi dan menjadi kelemahan yang dapat mengancam ekosistem jaringan utama secara keseluruhan.

Keamanan jaringan sangat vital bagi sebuah jaringan komputer (Ismail & Pramudita, 2020). Memahami konsep keamanan jaringan menjadi upaya pencegahan sejak dini dan perhatian lebih terhadap pentingnya *ethical hacking* pada perusahaan, menanggapi hal itu ada baiknya memperhatikan beberapa hal yang menjadi upaya lebih lanjut dalam mengenali segala bentuk insiden keamanan jaringan.

Insiden keamanan jaringan adalah suatu aktivitas yang memberikan dampak terhadap keamanan sistem yang secara langsung atau tidak bertentangan dengan *security police* sistem tersebut(Juardi, 2017).

Pada umumnya aspek keamanan jaringan meliputi :

1. *Authentication*, memastikan kebenaran pengirim informasi di dapat dari orang yang sebenarnya,
2. *Integrity*, memastikan keaslian informasi sesuai dengan konteks data pengirim dan tidak termodifikasi artinya keaslian terjaga, tidak ada perubahan ketika sampai ke tangan penerima.
3. *Confidentiality*, merujuk pada kerahasian dari Informasi
4. *Privacy*, berkaitan dengan data yang bersifat pribadi artinya bukan konsumsi publik.
5. *Availability*, ketersediaan layanan yang dapat di pantau oleh penggunanya.

Serangan pada kemanan jaringan memiliki variasi dalam praktiknya tersendiri salah satu jenis serangan keamanan populer yang dapat diketahui yaitu *sniffer. Sniffer* adalah sebuah *device* penyadapan komunikasi jaringan komputer dengan metode *premicious* pada *ethernet* (Ariyadi, 2018).

2.2 *Ethical Hacking*

Ethical Hacking adalah disiplin dalam meningkatkan dan menggabungkan kerentanan sistem yang di ketahui (Kelrey & Muzaki, 2019). Umumnya seseorang akan mencari celah keamanan secara legal, selanjutnya melaporkan dan merahasiakan penemuannya untuk di tindak lanjuti.

Melindungi Aset digital sangatlah penting, terlebih bagi instansi pendidikan atau perusahaan yang mengelola dan menyimpan data sensitif dari anggotanya. Pengawasan Data digital (*Digital surveillance*) adalah memantau aktivitas,

SATIN – Sains dan Teknologi Informasi
Vol. 07, No. 01, Juni 2021, pp. 32-44
ISSN: 2527-9114, DOI 10.33372/stn.v7i1.702

prilaku, atau proses bertukar informasi(Jum'ah, 2018). Perhatian khusus dalam menangani kerahasiaan serta privasi dapat berdampak baik pada kinerja dan reputasi. Kesadaran akan adanya ancaman dari luar mampu meningkatkan kewaspadaan terhadap hal yang tidak diinginkan yang mungkin saja dapat terjadi dalam kurung waktu yang cepat atau di kemudian hari.

Hacking merupakan teknik kejahatan dimana pelaku melakukan pembobolan suatu sistem (Taufiqurrohman et al., 2017). Umumnya penyusupan menyerang pada celah keamanan pada sistem jaringan, aplikasi atau sistem komputer lainnya, yang selanjutnya dapat mengekploitasi sumber daya utama, upaya penyusupan kebanyakan lebih mengarah pada hal yang dapat merugikan bagi korban yang di serang (*Black hat*) walau ada juga beberapa *hacker* (orang yang melakukan *hacking*) dengan tujuan yang baik seperti menginformasikan celah keamanan yang dapat di susupi atau bug dari sebuah program (*White hat*).

Umumnya prinsip keamanan informasi menjadi upaya perlindungan terhadap aspek yang berkaitan seperti:

a. *Confidentiality* (kerahasiaan), memastikan informasi tersampaikan langsung pada penerima dengan aman tanpa adanya kebocoran informasi yang dapat merugikan seperti penyalahgunaan data dari akses luar seperti pesaing bisnis.
b. *Integrity* (Integritas), Informasi dari pengirim harus konsisten sampai di tangan penerima, artinya tidak ada perubahan apapun.
c. *Availability* (ketersediaan), menjadi aspek yang menjamin bahwa data tersedia saat dibutuhkan.

Adapun aspek ancaman keamanan jaringan yang meliputi:

1. *Interuption* (perusakan, penghapusan data komputer), perubahan data yang terjadi tanpa sadar bahkan tidak di inginkan menjadi ancaman yang sangat mengkhawatirkan terlebih jika sampai data penting hilang.
2. *Interception* (penyadapan), upaya pengawasan ilegal dapat memonitoring seluruh aktivitas yang akan berhubungan dengan kerahasiaan.
3. *Modification* (Merubah informasi tanpa ijin pada lalu lintas pengiriman), terjadi perubahan informasi ketika proses pengiriman terjadi, sehingga penerima akan mendapatkan informasi yang sudah di rubah dari informasi aslinya, hal itu dapat menimbulkan kerugian besar terutama persoalan yang sensitif.
4. *Fabrication*, merupakan ancaman terhadap integritas.

Serangan dapat terjadi dari mana saja, salah satunya melalui koneksi pada jaringan utama, para peyusup akan senang ketika telah berhasil memasuki lalu lintas target dan mendapakan kontrol penuh, penanaman *virus*, *worm*, *Trojan* atau *script* komputer yang aktif dalam kurun waktu tertentu sangat mungkin untuk dilakukan.

Virus, *Worm* dan *Trojan Hourse*, juga bisa membuat *Back Door* yang dapat melakukan pencurian informasi pribadi (Setia et al., 2019).

Protokol keamanan seperti penerapan *Firewall* dapat di padukan dengan pengetahuan pentes. *Firewall* adalah suatu cara untuk membatasi informasi yang dibolehkan masuk dan keluar dari jaringan lokal(Gani, 2014)

SATIN – Sains dan Teknologi Informasi
Vol. 07, No. 01, Juni 2021, pp. 32-44
ISSN: 2527-9114, DOI 10.33372/stn.v7i1.702

Pengetahuan tentang bagaimana serangan terjadi akan sangat membantu untuk meracik sistem yang lebih kuat. Umunya Serangan pada jaringan yang biasa terjadi seperti :

1. *Scanning*, yang akan menggali seluruh informasi melalui *Network* korban,
2. *Brute-force*, yang akan membongkar kata kunci dari keamanan sistem secara acak untuk bisa di tebak.
3. *Rootkit*, sebagai alat penghilang jejak setelah melakukan penyusupan.

Melakukan audit pada keamanan jaringan tidak hanya sebagai seni tersendiri pada pelaporan administratif malainkan sebagai upaya pemeliharaan, pencegahan dan pengamanan pada sistem jaringan, berdasarkan standar keamanan yang di keluarkan oleh Kementrian Depkominfo (Departemen Komunikasi dan informasi Indonesia) yang di kenal dengan Indeks Keamanan Informasi atau disingkat KAMI. Indeks KAMI adalah instrumen pertimbangan untuk penilaian tingkat ketersediaan dan kematangan untuk mengukur implementasi dari manajemen keamanan informasi (Yunella et al., 2020).

Adapun langkah yang dapat dilakukan untuk audit keamanan jaringan secara mandiri, diantaranya :

1. Identifikasi, mengidentifikasi pada ruang lingkup untuk di evaluasi dapat di sesuaikan dengan kepentingan yang ingin di capai oleh kepentingan terkait.
2. Peran, Peran disini merupakan peran dari kepentingan dari penggunaan Teknologinya.
3. Area pengamanan, yang dapat di kelompokan menjadi 3 kategori, yaitu kerangka kerja, efektivitas dan peningkatan kinerja pada pengamanan.
4. Mengkaji ulang kelengkapan dan hasil yang telah di lakukan untuk proses evaluasi.

Standar Audit dapat dilakukan dengan Standar keamanan sistem informasi ISO 20072:2005 sebagai upaya keamanan untuk masa depan yang lebih baik dan terdokumentasi. ISO 20072 merupakan salah satu standar keamanan informasi yang di terbitkan oleh ISO dan IEC (Setiono et al., 1979). Audit akan sangat membantu dalam menggambarkan kesiapan sistem dan jaringan komputer ketika memasuki area publikasi yang lebih luas seperti internet.

2.3 *Penetration Test* atau Pentes

Pentes adalah sebuah metode untuk melakukan evaluasi terhadap keamanan dari sistem dan jaringan komputer (Samsumar et al., 2017). Administrator dapat mengetahui bagaimana upaya perbaikan yang di perlukan untuk memperkuat sistem yang telah ada dengan melakukan *penetration testing*.

Adapun beberapa metode yang dapat digunakan untuk melakukan pentes pada umumnya:

a) *Black Box Testing*, penguji atau orang yang melakukan pentes tidak memiliki informasi dan gambaran apapun tentang sistem yang akan di uji.
b) *Grey Box Testing*, berperan sebagai orang luar yang melakukan langkah menguji sistem keamanan yang lebih terpokuskan.
c) *White Box Testing*, Penguji telah mengetahui informasi dan gambaran sistem yang akan di uji secara menyeluruh.

2.4 Nmap (*Network Mapper*)

Nmap adalah sebuah *Tools Open Source* untuk ekplorasi dan audit keamanan jaringan (Rendro et al., 2020). Nmap di kenal sebagai

SATIN – Sains dan Teknologi Informasi
Vol. 07, No. 01, Juni 2021, pp. 32-44
ISSN: 2527-9114, DOI 10.33372/stn.v7i1.702

salah satu *Tool* yang dapat melakukan ekplorasi pada jaringan dengan cepat sekalipun itu pada ekosistem jaringan yang besar, tak hanya digunakan untuk menemukan celah keamanan dengan teknik *port scanning*, identifikasi host, dan Nmap *Scipting Engine* (*NSE*), namun para administrator jaringan membuatnya lebih dapat melakukan banyak hal, misalnya seperti inventori jaringan, pengelolaan jadwal pembaharuan pada layanan, dan monitoring ketersediaan host serta layanannya untuk memastikan agar tetap aktif. Metode yang dapat digunakan Nmap yaitu melalui teknik *port scanning* atau memasuki lalu lintas jaringan lalu mencari *port* yang terbuka maupun tertutup untuk di ekplorasi.

Teknik *Port scanning* adalah bug yang kedua paling banyak di temukan di website yang ada di internet (Rusydianto et al., 2017).

Port yang terbuka akan menandakan bahwa koneksi serta pertukaran layanan dapat di lakukan sedangkan tertutup akan memberikan informasi bahwa terdapat protokol jaringan penghalang seperti *firewall* atau pemblokir lainnya, teknik *port scanning* akan melibatkan pengetahauan tentang jaringan *IP Address* sebagai protokol standar dalam komunikasi jaringan, dari sana informasi perangkat dapat di peroleh misalnya nama *DNS*, Sistem Operasi, jenis atau tipe perangkat dan *MAC Address*, adapun enam status *port* yang di kenali oleh Nmap berdasarkan *nmap.org*, diantaranya :

a. *Open* (terbuka), menerima koneksi secara aktif melaui paket koneksi *TCP/UDP*, informasi jalur terbuka dapat memberitahukan layanan yang dapat di gunakan pada jaringan terkoneksi, namun hal ini juga dapat membuat pemikiran terbuka bagi penyerang terhadap celah yang dapat di susupi.
b. *Closed* (tertutup), akses dapat diterima serta di tangapi oleh Nmap, namun aplikasi tidak dapat mendengarnya karena terhalang oleh pelindung *firewall* yang terpasang pada jaringan.
c. *Filtered* (filter), Nmap tidak dapat mengetetahui informasi lengkap *port* terbuka karena terhalang oleh *firewall*, keamanan *Router* atau *software* tambahan yang terapasang pada *host*, membuat komunikasi tidak dapat di lakukan secara administratif.
d. *Unfiltered* (tidak di filter), *Port* tersebut dapat di akses, namun Nmap tidak dapat mengenali termasuk kedalam *port* terbuka atau tertutup, sehingga perlu tambahan pemeriksaan lain, salah satunya menggunakan teknik *windows scan*.
e. *Open Filtered*, Terjadi ketika *port* terbuka tidak memberikan respon atau tanggapan dengan kata lain terpadat paket filter yang mendrop, sehingga Nmap tidak dapat mengenali apakah *port* tersebut terbuka atau telah di filter.
f. *Closed Filtered*, Nmap tidak dapat memastikan apakah protokol jaringan tersebut menggunakan *port* tertutup atau yang telah di filter.

Penerapan teknik *port scanning* pada Nmap tidaklah sulit, dokumentasi penggunaan tersedia secara lengkap pada halaman website *nmap.org* ketika pengguna ingin mempelajarinya, dan tidak terbatas untuk salah satu sistem operasi, keluarga Windows, Linux maupun MacOS dapat memasang dan menjalankannya, dari banyaknya baris perintah berikut yang popular untuk melakukan *port scanning* menggunakan Nmap:

SATIN – Sains dan Teknologi Informasi
Vol. 07, No. 01, Juni 2021, pp. 32-44
ISSN: 2527-9114, DOI 10.33372/stn.v7i1.702

a. –sS (*TCP SYS Scan*)
   Merupakan scan baku yang popular, keunggulannya akan membuka seluruh koneksi *TCP* dan dapat melakukan proses dengan cepat dimana mampu memeriksa ribuan *port* per detik ketika tidak di halangi oleh *firewall* pada jaringan target.
b. –sT (*TCP Connect scan*)
   Termasuk salah satu scan baku yang di gunakan ketika *Scan SYS* tidak bisa di lakukan karena masalah *privilege* atau hak akses untuk paket tertentu.
c. –sU (*UDP Scan*)
   Walau sering di abaikan karena kebanyakan lebih banyak menggunakan protokol *TCP*, namun sebagai salah satu upaya untuk menscan layanan *DNS*, *SNMP* dan *DHCP* yang berada pada masing-masing *port* (53,161/162 dan 67/68).
d. –sW (*TCP Windows scan*)
   Windows scan akan memberitahukan perbedaan *port* terbuka dan *port* tertutup.
e. –sO (*IP Protocol Scan*)
   Perintah tersebut memberitahukan protokol alamat IP yang di dukung oleh mesin target apakah *TCP*, *ICMP*, dan lainnya.

Nmap memberikan fitur ekplorasi audit keamanan jaringan yang lengkap, tak salah jika di sandingkan dengan *tools* penetrasi keamanan jaringan serupa seperti *Wireshark*, *Metasploit*, *Nessus* dan *Nikto* serta berhasil masuk kedalam jajaran 125 Top alat keamanan jaringan teratas berdasarkan informasi di *SecTools.org*, penggunaannya telah banyak di sadari oleh banyak praktisi termasuk para golongan hitam atau *black hat*, Nmap juga dapat menjadi ancaman ketika berada di tangan yang salah, oleh karenanya mengenal seperti apa karakter Nmap menjadi salah satu upaya bagaimana merumuskan pencegahannya.

3. Metode Penelitian

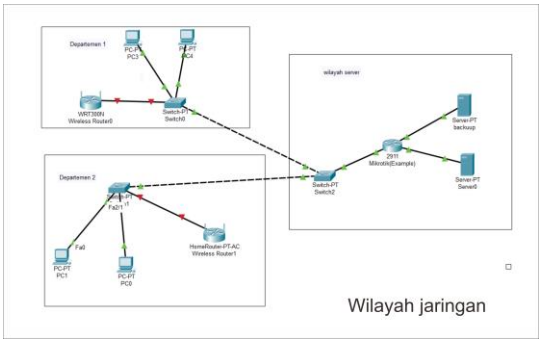
Metode pelitian yang digunakan dalam melakukan Teknik *Penetration testing* dalam pengujian ini adalah sebagai berikut:

1. Metode *Black Box Testing*, demo yang akan di simulasikan oleh pengakses luar dengan tujuan jahat,
2. Metode *White Box Testing*, dilakukan langsung oleh penguji yang memiliki akses sah dan berupaya untuk mencari kerentanan untuk memperbaikinya.

Setelah berhasil memasuki wilyah jaringan, selanjutnya metode *port scanning* dengan Nmap yang dijalankan pada keduanya.

3.1 Gambaran simulasi pentes

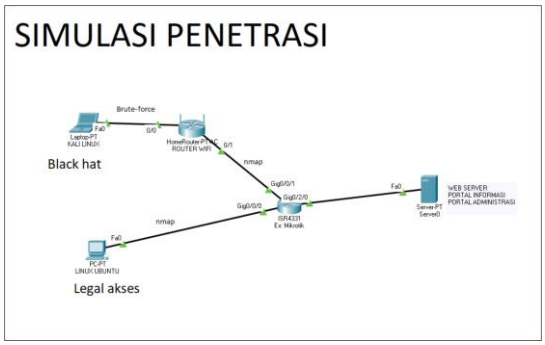
Pada wilayah jaringan sebenarnya terdapat komputer server, Mikrotik, *Switch*, perangkat komputer klien dan Router Wifi dengan jumlah unit lebih dari 1.



Gambar 1. Wilayah jaringan

Gambar 1, memuat informasi medan wilayah jaringan yang akan di lakukan pentes. Selanjutnya di sederhanakan dalam dengan konsep simulasi pentes di bawah.

SATIN – Sains dan Teknologi Informasi
Vol. 07, No. 01, Juni 2021, pp. 32-44
ISSN: 2527-9114, DOI 10.33372/stn.v7i1.702



Gambar 2. Simulasi penetrasi

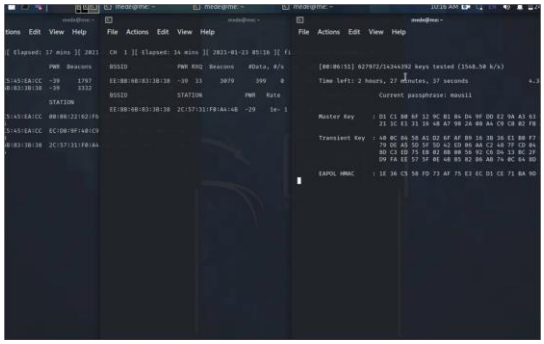
Gambar 2, menjelaskan terdapat satu pengakses (*black hat*) yang menggunakan metode *Black Box Testing*, masuk melalui jaringan wifi dengan teknik *Brute-force*, lainnya dilakukan pengakses legal dengan metode *White Box testing*, mengakses dari komputer, masing-masing selanjutnya melakukan teknik *port scanning Nmap* untuk mengetahui detail lengkap sistem pada wilayah jaringan.

3.2 Perlengkapan Dukungan

Sebagai upaya terhadap dukungan pada penelitian, adapun peralatan yang digunakan selain perangkat pada ekosistem jaringan yaitu perangkat PC (laptop dan Komputer) dengan masing-masing terpasang sistem operasi Linux Ubuntu versi 20.04 dan Kali Linux yang telah di bekali *Tools* Nmap pada perangkat tersebut.

3.3 Pengujian dengan *Black Box Testing*

Pada simulasi ini, pengakses *Black hat* menggunakan perangkat dengan sistem operasi *Kali Linux* untuk mecoba masuk pada jaringan target melalui koneksi jaringan *wireless* yang di pancarkan oleh perangkat *WIFI* yang tersedia pada lalu lintas jaringan target dengan menggunakan teknik *Brute-force*, yang akan membongkar kata kunci dari keamanan *WIFI* secara acak untuk mendapatkan sandi yang pas berdasarkan *wordlist* yang memuat ribuan kata kunci. Paket *tools* penetrasi yang digunakan adalah *aircrackng*.



Gambar 3. Kali linux, aircrakng

Gambar 3, menjelaskan dokumentasi tools *aircrackng* dengan informasi bahwa penetrasi di lakukan sebagai upaya untuk terhubung ke jaringan dengan mengidentifikasi *SSID* dari perangkat target berada pada *channel* 1, 2 atau lainnya, setelah di ketahui, perangkat penguji akan melakukan jabat tangan untuk dapat terhubung dan selanjutnya mencoba menebak kata kunci yang sesuai dengan kata sandi perangkat *WIFI* dan setelah berhasil masuk penetrasi *Port scanning Nmap* di lakukan untuk menggali informasi perangkat yang tersambung dalam jaringan tersebut.

3.4 Pengujian dengan *White Box Testing*

Peran kedua, penetrasi di lakukan dari akses legal menggunakan perangkat dengan sistem operasi Ubuntu, dimana gerbang informasi jaringan sudah di ketahui, selanjutnya teknik *port scanning* Nmap di aktifkan untuk melakukan pentes.

Tabel 1. *Network* yang digunakan untuk *port scanning*

Protokol	**Network**
	Value
IP address	192.168.77.5
Netmask	255.255.255.0
Gateway	192.168.77.1

Simulasi *Network* untuk *port scanning*

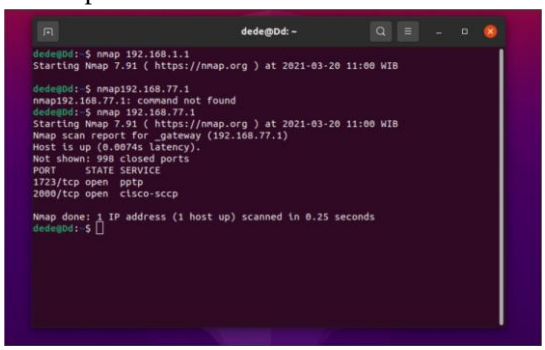
SATIN – Sains dan Teknologi Informasi
Vol. 07, No. 01, Juni 2021, pp. 32-44
ISSN: 2527-9114, DOI 10.33372/stn.v7i1.702

Table 1, memuat informasi dari Jaringan target yang sudah di ketahui *seperti IP gateway* salah satu *port* yang aktif pada router miktorik 192.168.77.1 dengan Netmask 255.255.255.0, sehingga perangkat penetrasi dari *white hack* hanya menyesuaikan IP Address perangkatnya yaitu 192.168.77.5 dengan netmask yang sama 255.255.255.0. proses penetrasi *port scanning* dengan Nmap dapat dilakukan setalahnya.

3.5 Script pengujian

Kedua metode penetrasi menggunakan *Script Nmap* yang sama dalam percobaannya, yaitu :

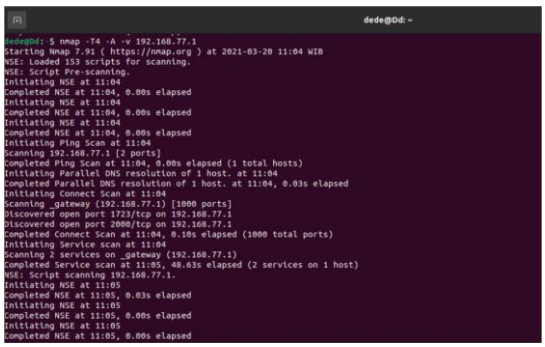
1. nmap 192.168.77.1



Gambar 4. *Ports scanning* standar nmap

Gambar 4, Perintah tersebut merupakan baris umum untuk menggali sedikit informasi dari *port* layanan pada jaringan seperti *open port*, serta informasi *host* yang aktif.

2. nmap -T4 –A –v 192.168.77.1



Gambar 5. Nmap nse

Gambar 5, memuat baris perintah kedua, bertujuan untuk menggali informasi lebih dalam, dengan menggunakan baris perintah tingkat lanjut yang menggunakan fitur *NSE* pada Nmap. Baris perintah tersebut dapat memberikan informasi yang lebih mendetail jika dibandingkan dengan perintah umum yang langsung menargetkan IP Address dari *network*, yang dapat di ketahui diantaranya : *IP default getaway*, jumlah host aktif, open port, spesifikasi perangkat, sistem operasi.

4. Hasil dan Pembahasan

4.1 Hasil audit penetrasi

Upaya penetrasi yang telah di lakukan dengan dua metode akses yang berbeda namun sama dalam melakukan penetrasi akhir dengan nmap, dengan menggali informasi seluruh jaringan tersaji dalam tabel berikut:

Tabel 2. Hasil Penetrasi Nmap pada jaringan target

Protokol	**Hasil Audit Port Scanning Nmap**
	Value
IP address	192.168.77.1
Port TCP Open	1723,2000,
Port UDP open	67,16
Router	Mikrotik RB951Ui-2Hnd
Sistem Operasi	Linux_karnel
MAC Address	E4:8D:8C:A1:8B:xx

Hasil audit dari penetrasi nmap pada target

Tabel 2, memuat informasi hasil penetrasi menggunakan teknik *port scanning* Nmap, terdapat alamat IP address 192.168.77.1 sebagai alamat jaringan lokal utama, terdapat 2 *port TCP* yang terbuka 1723 yang

SATIN – Sains dan Teknologi Informasi
Vol. 07, No. 01, Juni 2021, pp. 32-44
ISSN: 2527-9114, DOI 10.33372/stn.v7i1.702

merupakan *port* dari *access point* dan wifi router, *port* 2000 yang menjadi perhatian khusus karena diindikasikan *trojan* pada *protocol TCP*, *port* 67 untuk *BOOTP* atau *DHCP* Server, artinya sistem tersebut memiliki paket alamat distribusi otomatis, *port* 16 *UDP* menjadi kerentanan yang patut di waspadai dimana penyerang dari jarak jauh dapat mengekplorasi dan membuat sistem aplikasi macet, di lengkapi dengan informasi seri perangkat yang di gunakan untuk Router yaitu Mikrotik dengan detail MAC Addressnya.

Setelah melakukan audit dengan bantuan penetrasi upaya pencegahan dilakukan dengen cara berikut:

1. Mikrotik mendukung upaya pencegahan pada aktifitas *port scanning* oleh karenanya upaya perbaikan keamanan dapat di tingkatkan dengan Metode *Port Knocking* pada Mikrotik, metode tersebut memberikan gambaran keamanan yang cukup kuat dengan dua gerbang keamanan, walaupun pengakses mengetahui kombinasi user dan sandi untuk login tapi tidak mengetahui jalur ping permintaannya maka tidak dapat masuk, hal itu akan membantu mencegah pengakses yang tidak diinginkan untuk mengeksplorasi lebih dalam ketika berhasil masuk pada gerbang pertama di lalu lintas jaringan.
2. Mencegah aktivitas penetrasi *aircrackng* dengan menggunakan kombinasi sandi yang tidak umum, dapat menggunakan kombinasi angka dan karakter unik
3. Mengatur kembali paket layanan *port* yang terbuka, jika tidak digunakan ada baiknya menutup akses tersebut.
4. Monitoring lebih lanjut pada sistem perangkat, melakukan pembersihan, *backup* atau *restore* pada router ketika terindikasi aktivitas tidak wajar.

4.2 Perbaikan lebih lanjut

Upaya jangka Panjang dalam perbaikan keamanan jaringan dapat dilakukan dengan menggunakan metode ISO 27002:2005, adapun poin bahasan utama yang dapat diketahui diantaranya:

Klausul 1, Instansi sangat mengedepankan upaya keamanan yang lebih baik karena hal itu menyangkut kerahasiaan data internal dari anggotanya, namun pada sektor jaringan kesadaran akan keamanan masih kurang karena sebelumnya tidak ada teanaga ahli khusus, perangkat usang dan belum ada kasus yang merugikan secara material maupun moril.

Klausul 2, dokumentasi tujuan keamanan sudah ada, namun lebih banyak pada sisi *database*, website dan dengan format yang standar.

Klausul 3, dokumentasi aset sudah ada, namun terus di upayakan untuk terus di perbaiki dengan mengupgrade perangkat baru yang di lengkapi dengan fitur keamanan yang lebih baik.

Klausul 4, Kebijakan kemanan sudah ada namun belum di dokumentasikan secara tertulis baru sekedar ucapan melalui lisan.

Klausul 5, Hak akses telah terdokumentasikan dengan baik dimana, perangkat server dan jaringan utama tidak sembarangan orang untuk menyentuhnya, di tempatkan di ruangan khusus dan diizinkan pihak IT saja, tanpa terkecuali.

Klausul 6, sudah ada prosedur untuk *backup* namun belum ada dokumentasinya, sepenuhnya dilakukan berdasarkan kebutuhan dan pengakses tertentu.

Klausul 7, *privilege* pengguna pada departemen IT sudah ada namun belum ada dokumentasinya, sehingga pembagian tugas masih tercampur pada beberapa bagian sektor.

SATIN – Sains dan Teknologi Informasi
Vol. 07, No. 01, Juni 2021, pp. 32-44
ISSN: 2527-9114, DOI 10.33372/stn.v7i1.702

Klausul 8, Aktivitas data sensitif seperti transaksi keuangan sudah terdokumentasikan, dan departemen keuangan yang memiliki akses untuk hal itu.
Klausa 9, Penyerang pada jaringan belum terdokumentasikan, Adapun jika terjadi upaya pelaporan langsung ke pada kepala IT yang selanjutnya di cari solusi bersama anggota timnya.
Klausul 10, prosedur ini menjadi perhatian khusus mengingat manfaat jangka Panjang Ketika terjadi hal yang tidak diinginkan.
Klausul 11, anggota intansi lainnya cenderung tidak mengetahui pentingnya keamanan jaringan, namun edukasi pada temuan kasus di lapangan sering di lakukan untuk penyesuaian bertahap sebagai kepedulian seluruh anggota pada instansi. Upaya tambahan audit tersebut dapat menjadi langkah perubahan pada sistem yang lebih baik .

5. Simpulan

Nmap merupakan *tools* audit keamanan jaringan gratis yang dapat di gunakan pada *multi-platform* (Windows, Linux dan MacOS), fitur yang di sajikan dapat membantu Administrator jaringan untuk mengecek kesiapan sistem sebelum publikasi secara luas dengan mencari celah keamanan secara mandiri sebagai perhatian terhadap *Ethical Hacking* pada perusahaan, teknik penetrasi yang dapat di kombinasikan seperti *port scanning*, identifikasi *host*, dan *NSE* (*Nmap Scipting Engine*), Hasil yang di peroleh dengan penetrasi *port Scanning* menggunakan Nmap pada jaringan target dapat membuka informasi lalu lintas pada jaringan, seperti jumlah host pada perangkat terhubung, *IP Address*, *Network*, perangkat *Router*, *Port TCP/UDP* terbuka dan tertutup.

Kerentanan yang di ketahui dapat menjadi upaya perbaikan dalam meracik sistem keamanan jaringan yang lebih kuat sehingga dapat menyakinkan seluruh pengguna yang mengakses pada wilayah jaringan tetap aman dan privasi terjaga. Nmap mampu memberikan perluasaan keamanan jaringan yang murah dengan mengedepankan teknik yang mudah pada baris kode perintah, menjadi panduan yang sangat cocok untuk di implementasikan pada wilayah tingkat dasar sampai menengah.

5.1 Saran

Adapun saran dalam melakukan penetrasi testing menggunakan Nmap ini :

1. Aktifitas penetrasi dapat membahayakan sistem jika di lihat pada beberapa kasus, oleh karennya perlu di sadari akan kebutuhan dan resikonya jika metode yang digunakan *White Box Testing*.
2. Sistem operasi Linux di rekomendasikan untuk melakukan penetrasi keamanan jaringan, misalnya seperti Kali linux, Ubuntu, atau turunan *Debian* lainnya.
3. Ketika melakukan panetrasi dengan metode *Black Box Testing*, memaksimalkan fungsi *aircrackng* dapat mengunakan perangkat wifi ekstender agar tangkapan bar signal lebih bagus dan stabil.

6. Referensi

Alamsyah, H., -, R., & Al Akbar, A. (2020). Analisa Keamanan Jaringan Menggunakan Network Intrusion Detection and Prevention System. JOINTECS (Journal of Information Technology and Computer Science), 5(1), 17. https://doi.org/10.31328/jointecs.v5i1.1240

Ariyadi, T. (2018). Mitigasi Keamanan Dynamic Host Control Protocl (DHCP) Untuk Mengurangi Serangan Pada Local Area Network (LAN).

INOVTEK Polbeng - Seri Informatika, 3(2), 147. https://doi.org/10.35314/isi.v3i2.455

Gani, A. G. (2014). Konfigurasi Sistem Keamanan Jaringan. Jurnal Sistem Informasi Universitas Suryadarma, 6(1), 134–149. https://doi.org/10.35968/jsi.v6i1.280

Ismail, R. W., & Pramudita, R. (2020). Metode Penetration Testing pada Keamanan Jaringan Wireless Wardriving PT . Puma Makmur Aneka Engineering Bekasi. Jurnal Mahasiswa Bina Insani, 5(1), 53–62.

Juardi, D. (2017). Kajian Vulnerability Keamanan Jaringan Internet Menggunakan Nessus. Syntax Jurnal Informatika, 6(1), 11–19. https://journal.unsika.ac.id/index.php/syntax/article/view/1148/Kajian Vulnerability Keamanan Jaringan Internet Menggunakan Ness

Jum'ah, M. N. Al. (2018). Analisa Keamanan dan Hukum untuk Pelindungan Data Privasi. CyberSecurity Dan Forensik Digital, 1(2), 39–44. http://ejournal.uin-suka.ac.id/saintek/cybersecurity/article/view/1370

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

Muzawi, R., -, R., & -, A. (2017). Perancangan Aplikasi Berbasis Client Server dalam Mengupload File-File Ujian pada Laboratorium Komputer STMIk Amik Riau. SATIN - Sains Dan Teknologi Informasi, 3(1), 10. https://doi.org/10.33372/stn.v3i1.210

Putra, P. P. (2016). Pengembangan Sistem Keamanan Jaringan Menggunakan Rumusan Snort Rule (HIDS) untuk Mendeteksi Serangan Nmap. SATIN - Sains Dan Teknologi Informasi, 2(1), 15–21.

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.

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).

Sabdho, H. D., & Ulfa, M. (2018). Analisis Keamanan Jaringan Wireless Menggunakan Metode Penetration Testing Pada Kantor PT. Mora Telematika Indonesia Regional Palembang. Semhavok, 1(1), 15–24.

Samsumar, L. D., Gunawan, K., Program, D., Manajemen, S., Program, D., & Komputerisasi, S. (2017). Analisis Dan Evaluasi Tingkat Keamanan Jaringan Komputer Nirkabel (Wireless Lan); Studi. Ilmiah Teknologi Informasi Terapan, IV(1), 73–82.

Santoso, J. (2019). Uji Kerentanan Keamanan Server Menggunakan Scada Shodan. Teknokom, 2(2), 1–4. https://doi.org/10.31943/teknokom.v2i2.38

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. https://doi.org/10.26418/jp.v5i1.28214

Setiono, M., Willyanto, L., & Noertjahyana, A. (1979). Audit Sistem Keamanan Jaringan Pada PT TRIAS SENTOSA TBK. 5.

Sidabutar, J. (2020). Desain Jaringan Komputer Terintegrasi Menggunakan Arsitektur Campus LAN. Jurnal Jaring SainTek, 2(1), 25–32. https://doi.org/10.31599/jaring-

saintek.v2i1.64

Taufiqurrohman, I., Widiyasono, N., & Mubarok, H. (2017). Pemanfaatan Raspberry Pi untuk Hacking dan Forensic dengan metode NIST (National Institute of Standards and Technology). Jurnal Teknik Informatika Dan Sistem Informasi (JUTISI), 3, 231–244.

Yunella, M., Herlambang, A. D., & Putra, W. H. N. (2020). Evaluasi Tata Kelola Keamanan Informasi pada Dinas Komunikasi dan Informatika Kota Malang Menggunakan Indeks Kami. … Teknologi Informasi Dan …, 3(10), 9552–9559. http://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/6521