JURNAL ILMIAH FIFO **P-ISSN 2085-4315 / E-ISSN 2502-8332**
DOI: http://dx.doi.org/10.22441/fifo.2024.v16i2.003

Pencegahan Kerentanan Keamanan Jaringan Komputer Mikrotik Menggunakan Metode *Penetration Testing*

Alfian[1], Mardiana Purwaningsih[2*], Fandan Dwi Nugroho Wicaksono[3]

Fakultas Teknologi Informasi, Perbanas Institute[1,2,3]
alfianajjh916@gmail.com[1], mardiana@perbanas.id[2*], fandan.dwi@perbanas.id[3]

*) Corresponding Author

(***received*****:** 24-05-24, ***revised*****:** 19-06-24 ***accepted*****:** 11-09-24)

Abstract

Computer network companies are required to ensure the accessible rights issues. The opportunity for hacking may occur on computer networks in various companies. Apart from that, companies often also use various types of networks or what is usually called multivendor, for example, Cisco, Aruba, Fortinet, F5 Firewall, and Mikrotik, so that the security mechanism becomes more complex. With so many wireless local networks (WLANs) and connected local networks (LANs) available, network security must be a top priority. The routers used by companies today often also lack any type of Internet network protection, allowing any user to connect with relative ease. This condition creates a threat to security, so it is necessary to carry out security testing of the current computer network configuration. The testing method used is Penetration Testing to find out whether the network that has been created is secure, which is then continued by proposing a router configuration to increase network security. Tests and analyses that have been carried out such as Winbox, Putty, and MAC Server were not successful, while Nesuss was successful but can only describe SSL Vulnerabilities and cannot enter the Computer Network.

Keywords*: Microtic, Cybersecurity, Penetration Testing, Hacker, Nessus*

Abstrak

Jaringan komputer perusahaan sangat perlu memperhatikan keamanan hak akses. Saat ini keamanan pada jaringan komputer secara umum di berbagai perusahaan masih memiliki peluang dapat diretas. Selain itu seringkali perusahaan juga memakai berbagai macam jaringan atau biasa disebut multivendor, misal Cisco, Aruba, Fortinet, F5 Firewall serta Mikrotik, sehingga mekanisme pengamanannya menjadi lebih kompleks. Dengan begitu banyak jaringan lokal nirkabel (WLAN) dan jaringan lokal terhubung (LAN) yang tersedia, maka keamanan jaringan harus menjadi prioritas utama. Router yang digunakan oleh perusahaan saat ini seringkali juga tidak memiliki jenis perlindungan jaringan Internet, memungkinkan setiap pengguna terhubung dengan relatif mudah. Kondisi ini membuka ancaman terhadap keamanan, sehingga perlu untuk melakukan pengujian keamanan terhadap konfigurasi jaringan komputer yang ada saat ini. Metode pengujian yang digunakan adalah *Penetration Testing* untuk mengetahui apakah jaringan yang sudah dibuat aman, yang kemudian dilanjutkan dengan mengusulkan konfigurasi router untuk meningkatkan keamanan jaringan. Hasil pengujian dan analisis yang telah dilakukan seperti Winbox, Putty, dan MAC Server tidak berhasil, sedangkan untuk Nesuss berhasil dilakukan tetapi hanya dapat mendeskripsikan Vulnerabilities SSL dan tidak dapat masuk ke dalam jaringan komputer.

Kata Kunci: Mikrotik, Keamanan Siber, *Penetration Testing,* Peretas, Nessus

I. Pendahuluan

Semua pihak yang terlibat dalam sistem terpusat harus mengawasi keamanan jaringan yang digunakan. Jika seorang *hacker* berhasil memasuki sistem dengan niat khusus untuk mencuri informasi sensitif, maka pelanggaran, manipulasi, dan hilangnya data dapat menghancurkan perusahaan dan reputasi personal [1]. Tanpa perlindungan yang tepat, jaringan komputer menjadi sasaran mudah bagi para peretas. Ketika ini terjadi, informasi pribadi orang atau data perusahaan sensitif dapat diakses ke tangan yang salah [2]. Untuk menghindari

hal tersebut maka langkah pertama yang perlu dilakukan oleh organisasi atau perusahaan adalah dengan mengevaluasi keamanan jaringan komputer yang dimilikinya [3], [4]. Evaluasi dilakukan untuk mengurangi risiko kerugian yang disebabkan oleh tindakan peretasan ini, serta mengurangi resiko kerusakan di dalam organisasi [3]. Dan salah satu bentuk evaluasi yang dapat dilakukan adalah dengan pengujian penetrasi.

Untuk memperkuat keamanan jaringan, pengujian penetrasi adalah upaya terkontrol dan dibatalkan untuk menemukan dan memanfaatkan kerentanan. Membedakan antara tes penetrasi dan penilaian kerentanan sangat penting. Industri keamanan penuh dengan orang dan vendor yang secara bergantian menggunakan nama-nama ini. Sementara penilaian kerentanan mencari celah keamanan di layanan dan sistem, tes penetrasi menggunakan eksploit dan serangan PoC untuk menetapkan keberadaan cacat. Pengujian penetrasi adalah bentuk analisis keamanan yang lebih menyeluruh daripada pemindaian kerentanan sederhana. Hal ini yang menjadi alasan pemilihan metode penetrasi pada penelitian ini.

Pengujian penetrasi merupakan bentuk analisis keamanan yang lebih menyeluruh, tidak hanya sekedar pemindaian kerentanan sederhana. Alasan pemilihan metode penetrasi pada penelitian ini didasarkan pada hasil beberapa penelitian sebelumnya [2], [5]. Pengujian penetrasi dilakukan untuk mengevaluasi keamanan pada Wireless Local Area Network. Dalam penelitian terdahulu tersebut dinyatakan bahwa metode Penetration Testing merupakan metode yang komprehensif dalam menemukan kerentanan keamanan dalam sistem jaringan WLAN.

Metode Penetration Testing ini sudah dilakukan pada beberapa penelitian sebelumnya [2], [5], terkait dengan evaluasi keamanan Wireless Local Area Network. Dalam penelitian terdahulu tersebut dinyatakan bahwa metode Penetration Testing dapat digunakan untuk menginformasikan keputusan menerapkan tingkat kerentanan yang ditentukan oleh ISSAF dalam mengamankan jaringan WLAN [6]. Pengujian penetrasi merupakan pengujian dengan proses yang komprehensif untuk menemukan kerentanan keamanan dalam sistem. Pengujian penetrasi dapat digunakan untuk mencegah praktik mendapatkan akses yang tidak sah ke jaringan nirkabel dengan menggunakan media yang dilengkapi dengan perangkat lunak dan perangkat keras khusus [5], [8], karena sifat yang tidak aman dari jaringan nirkabel. Dengan dilakukannya pengujian ini maka kerugian keuangan dapat dihindari, hukum industri dapat dipenuhi, pelanggan dan pemegang saham dapat dilindungi, reputasi perusahaan dapat dipertahankan, dan faktor risiko dapat dihilangkan berkat proses ini.

Berdasarkan hal tersebut di atas, PT. SCM yang merupakan perusahaan dalam bidang penyiaran televisi juga merasa perlu untuk melakukan pengujian penetrasi terhadap jaringan komputer yang dimiliki. PT. SCM saat ini telah mengakusisi beberapa perusahaan penyiaran lainnya, serta melakukan transisi dari TV analog ke TV digital. Proses transisi ini melibatkan data dan sumber daya perusahaan yang dilewatkan melalui jaringan komputer. Hasil wawancara dengan Divisi TI dan analisis kondisi keamanan jaringan saat ini menunjukkan masih adanya kerentanan keamanan seperti terjadinya kegiatan mencurigakan. Penggunaan hak akses yang bebas terhadap jaringan komputer menjadi salah satu pemicunya. Hasil analisis secara umum menyatakan bahwa keamanan jaringan di PT. SCM saat ini tidak mencukupi untuk memberikan perlindungan keamanan jaringan. Sehingga perlu ada mekanisme pemantauan jaringan komputer, yang menjadi urgensi dilakukannya pengujian penetrasi di PT. SCM.

Pada saat melakukan pemantauan jaringan komputer tentu dibutuhkan beberapa peralatan. Salah satu alat yang dapat digunakan untuk memantau keamanan jaringan komputer adalah Mikrotik Routeboard. Pengujian penetrasi merupakan praktik mengeksplorasi jaringan untuk mengidentifikasi kerentanan dalam pertahanan terhadap serangan simulasi. Satu-satunya fungsi pengujian penetrasi adalah untuk memastikan keamanan bisnis. Hasil tes penetrasi yang berhasil dapat digunakan oleh organisasi yang berpartisipasi untuk mengidentifikasi dan memperbaiki kerentanan keamanan [2].

Keamanan data dalam jaringan komputer sangat penting sehingga membutuhkan filter keamanan dan sistem yang dapat mengenkripsi data, dengan kehadiran filter keselamatan dan sistem enkripsi informasi pihak yang tidak bertanggung jawab tidak dapat mencuri data dengan mudah karena data tersebut sudah dilindungi oleh penyaringan keamanan dan sistem mengenkripsikan data. Jadi dengan sistem ini tidak ada lagi kehilangan atau kebocoran data di jaringan komputer. Keamanan jaringan yang dibuat sehingga data tidak mudah dibaca atau rusak dan tidak lagi kebocoran data oleh pihak ketiga melalui data pada komputer server dilindungi dengan menggunakan *microtics* dan *password*, *username*, serta data yang dienkripsi [9]. Sistem otentikasi dalam jaringan nirkabel terus menderita kerentanan keamanan seperti serangan penolakan layanan pada titik akses, pembajakan sesi untuk pencurian data, dan penghentian koneksi klien untuk mengambil alih sesi. Administrator jaringan dan pengembang dapat menggunakan rekomendasi penelitian ini sebagai pedoman untuk menyambungkan lubang keamanan yang berpotensi dimanfaatkan di sistem mereka [10].

Pertimbangan menggunakan mikrotik sebagai alat untuk memantau suatu jaringan komputer serta merawat jaringan adalah karena mikrotik lebih tahan lama, lebih murah biaya yang digunakan, serta lebih mudah untuk diimplementasikan pada pengamanan akses jaringan saat ini, sehingga dikatakan belum sepenuhnya aman [6]. Akibatnya sering terjadi penyalahgunaan hak akses user ke dalam jaringan dan juga hak akses terhadap file. Selain itu seringkali perusahaan juga memakai berbagai macam jaringan atau biasa disebut multivendor, misal Cisco, Aruba, Fortinet, F5 Firewall serta Mikrotik, sehingga mekanisme pengamanannya menjadi lebih kompleks. Solusi untuk masalah di atas adalah melakukan pengujian penetrasi, yang merupakan pengujian jaringan dengan simulasi serangan jaringan [7]. Hasil pengujian jaringan digunakan untuk meningkatkan hak akses user, hak akses terhadap jaringan, dan meningkatkan keamanan jaringan komputer secara keseluruhan. Metode evaluasi dengan pengujian penetrasi menggunakan mikrotik ini walaupun biayanya murah, akan tetapi dapat memberikan hasil pengujian yang komprehensif pada jaringan Wireless LAN PT. SCM, sehingga menjadi pertimbangan utama dalam penelitian ini.

II. Metodologi Penelitian

Untuk memperkuat keamanan jaringan, pengujian penetrasi adalah upaya terkontrol untuk menemukan dan memanfaatkan kerentanan. Pengujian penetrasi adalah bentuk analisis keamanan yang lebih menyeluruh daripada pemindaian kerentanan sederhana [11]. Pengujian penetrasi adalah teknik untuk mengukur ketahanan keamanan jaringan dengan meneliti celah yang dapat dimanfaatkan oleh penyerang, menemukan area yang rentan, mengatur firewall, serta membangun jaringan nirkabel [12]. Kedua jaringan lokal dan eksternal digunakan untuk simulasi dan identifikasi. Tujuannya adalah untuk mempelajari tentang potensi bahaya yang terkait dengan kerentanan keamanan dalam sistem komputer atau jaringan dan bagaimana melindungi terhadap mereka [13], [14]. Uji penetrasi adalah serangkaian kegiatan yang dilakukan untuk mengidentifikasi dan mengeksploitasi kerentanan keamanan. Ini membantu mengkonfirmasi efektivitas atau ketidakefektifan langkah-langkah keamanan yang telah dilaksanakan [6]. Dampak dan kemungkinan kerentanan juga dapat diukur melalui pengujian penetrasi. Akibatnya, perusahaan akan dapat memprioritaskan memperbaiki kerentanan yang diketahui dan mengambil tindakan [6].

Setelah risiko kerentanan diperoleh dari hasil uji penetrasi, maka tahap berikutnya adalah proses pencegahan penetrasi yang telah dilakukan pada beberapa penelitian sebelumnya. Beberapa tindakan yang dapat diambil oleh organisasi dalam mencegah adanya penetrasi dalam jaringan komputer adalah dengan menyusun SOP terkait dengan hak akses dan etika keamanan dalam organisasi [14]. Administrator jaringan juga tidak hanya sekedar menggunakan konfigurasi router yang disediakan secara default saja, tetapi juga meningkatkan konfigurasi menjadi lebih aman [8].

Metode evaluasi atau pemantauan jaringan dilakukan dengan pengujian penetrasi menggunakan mikrotik. Alasan pemilihan metode ini adalah walaupun biayanya murah, akan tetapi pengujian penetrasi menggunakan mikrotik dapat memberikan hasil pengujian yang komprehensif pada jaringan Wireless LAN PT. SCM. Tahapan pengujian penetrasi dilakukan mengikuti tahapan yang disampaikan oleh [15]. Tahapan pengujian penetrasi meliputi:

1. *Reconnaissance* (Pengintaian) yaitu pengumpulan informasi target yang akan diuji;
2. *Scanning* yaitu melakukan pemindaian pada sistem untuk mengindentifikasi layanan yang aktif, port yang terbuka dan kerentanan yang mungkin ada;
3. *Gaining Access* yaitu mencoba mendapatkan akses ke dalam sistem target;
4. *Maintaining Access* yaitu mempertahankan akases kedalam sistem target; serta
5. *Analysis WAF Configuration* yaitu menganalisis hasil dari serangkaian langkah sebelumnya. WAF di sini adalah *Web Application Firewall* yang biasanya digunakan untuk memproteksi aplikasi web dari berbagai serangan atau injeksi.

Data dikumpulkan melalui metode observasi untuk mengamati dan mencatat secara sistematik jaringan komputer yang sedang diselidiki di sebuah perusahaan televisi nasional yang selanjutnya disebut SCM. Perangkat lunak yang digunakan meliputi: 1) Cisco Paket Tracer yang digunakan untuk melakukan simulasi jaringan Wireless LAN; 2) Aplikasi Nessus, digunakan untuk pengujian *scanning* dan mengaudit keamanan sebuah sistem, seperti *vulnerability*, *misconfiguration*, *security patch* yang belum diaplikasikan, *default password*, dan *denial of service*; 3) Nessus berfungsi untuk monitoring lalu-lintas jaringan; 4) *Virtual Box* (KaliLinux) yaitu OS yang digunakan untuk pengujian jaringan komputer; serta 5) Windows 11 – 64 bit, digunakan untuk mengelola fungsi dasar sistem, seperti meluncurkan aplikasi. Tahap selanjutnya ada analisis, setelah proses eksploitasi (menentukan target dan jenis serangan) selesai maka selanjutnya adalah melakukan

evaluasi hasil tes dan menyusun laporan. Teknik analisis yang digunakan adalah analisis dinamis, dimana pengecekan dilakukan ketika jaringan sedang berjalan sehingga diperoleh hasil yang nyata.

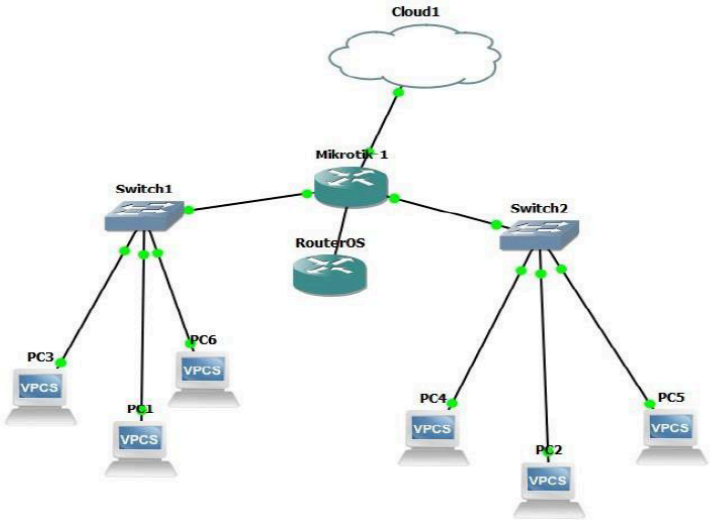
III. Hasil dan Pembahasan

Pengujian penetrasi diawali dengan merancang usulan konfigurasi jaringan di PT. SCM. Konsep ini mencakup pengembangan sistem manajemen *bandwidth* serta penggunaan fitur Mikrotik Routerboard yang ada, yang diharapkan berdampak positif pada sistem keamanan. Pada saat melakukan pemantauan keamanan jaringan komputer, Mikrotik Routeboard adalah salah satu alat yang paling berguna yang tersedia saat itu. Pengujian penetrasi adalah praktik mengeksplorasi jaringan untuk mengidentifikasi kerentanan dalam pertahanan terhadap serangan simulasi. Satu-satunya fungsi pengujian penetrasi adalah untuk memastikan keamanan bisnis. Hasil tes penetrasi yang berhasil dapat digunakan oleh organisasi yang berpartisipasi untuk mengidentifikasi dan memperbaiki kerentanan keamanan.

Sebuah jaringan dianggap aman, harus mematuhi beberapa kondisi, yang paling penting adalah memastikan bahwa data sensitif hanya dapat diakses oleh pihak yang berwenang. Kemudia Integritas yang menjamin bahwa data yang diterima tidak telah diubah, duplikat, atau ditransmisikan kembali dengan cara apa pun. Semua pengguna yang terhubung melalui jaringan yang aman harus terlebih dahulu diautentikasi sebelum tiga pilar keamanan lainnya, yaitu penolakan perlindungan layanan, pemantauan ketersediaan, dan kontrol akses dapat diimplementasikan.

A. Validasi Usulan Jaringan Komputer pada SCM

Rancangan konfigurasi jaringan komputer dilakukan validasi ke pakar yaitu dari Karyawan PT. SCM sebanyak empat orang. Teknik validasi yang digunakan adalah *Face Validity*. *Face Validity* menekankan pada apakah usulan jaringan komputer secara umum telah memenuhi kecukupan untuk sebuah jaringan komputer. Gambar 1 adalah usulan jaringan komputer yang menurut para karyawan PT. SCM sudah cukup bagus untuk sebuah topologi jaringan dengan menambahkan Router OS sebagai alat untuk pemantauan keamanan jaringan komputer. Rancangan jaringan komputer PT. SCM menggunakan Mikrotik Routeboard dengan Router OS sebagai Router yang mengatur Routing melalui ISP berkecepatan 100 Mbps. Pakar yang dipilih untuk *Face Validity* dapat dilihat pada Tabel 1.



Gambar 1. Usulan Konfigurasi Jaringan Komputer

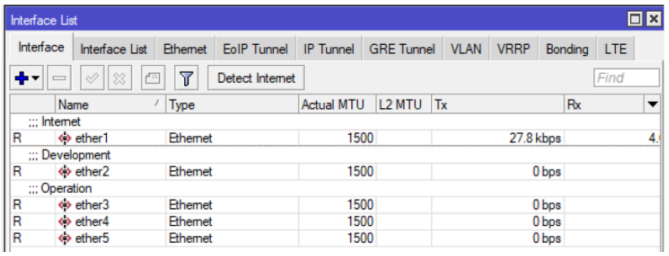
Hasil validasi usulan konfigurasi jaringan bahwa Pakar 1, 2, 3, dan 4 menyatakan secara umum usulan jaringan komputer pada PT. SCM dan ruangan jaringan sudah memenuhi kebutuhan dalam mengatur jaringan komputer.

Tabel 4.1 Demografi Pakar Validasi Usulan Jaringan Komputer

Aktor	Kode	Pendidikan	Pengalaman	Kepakaran
Karyawan	Pakar 1	S2	> 10 tahun	Knowledge Sharing
Karyawan	Pakar 2	S2	> 10 tahun	Network Admin
Karyawan	Pakar 3	S2	> 5 tahun	System Network
Karyawan	Pakar 4	S1	> 5 tahun	Bussines Analys

Setelah menyusun konfigurasi jaringan, maka selanjutnya adalah melakukan beberapa konfigurasi, yaitu:

1. Konfigurasi Router
   Konfigurasi Interface bertujuan agar *interface* dapat lebih mudah dikenali, tahap ini dapat dilihat pada Gambar 2. Gambar 2 merupakan hasil konfigurasi yang telah dilakukan pada mikrotik, yang menampilkan Internet menggunakan ether1, Development menggunakan ether2, dan Operation menggunakan ether3.



Gambar 2. Konfigurasi Router Mikrotik

2. Konfigurasi IP Address Jaringan Komputer
   Konfigurasi IP Address pada Router adalah menambahkan IP 192.168.56.254/24 pada ether1 (sebagai penghubung antara Router dengan modem internet). IP 192.168.1.10/24 pada ether2 (sebagai penghubung antara Router dengan Acces Point 1 pada ruangan development), dan menambahkan IP 192.168.2.10/24 pada ether3 (sebagai penghubung antara Router dengan Access Point 2 pada ruangan operasional).
3. Konfigurasi DHCP Server Jaringan Komputer
   Konfigurasi DHCP Server dilakukan untuk memberikan IP secara otomatis kepada setiap komputer yang terhubung pada jaringan serta selalu diperhatikan mengenai IP Address dan juga DNS server.
4. Konfigurasi Firewall NAT Jaringan Komputer
   Konfigurasi Firewall NAT merupakan suatu protokol yang digunakan mikrotik untuk mentranslasikan IP publik ke IP privat agar IP privat dapat tersambung dengan IP publik dalam penggunaan internet. Konfigurasi ini diperlukan agar komputer yang terhubung di jaringan tersebut dapat memperoleh akses ke internet.
5. Konfigurasi Keamanan Router Jaringan Komputer
   Konfigurasi keamanan router dilakukan untuk mengamankan router dari pihak yang tidak diberikan atau memiliki akses untuk masuk menggunakan jaringan komputer yang ada.

B. Pengujian Jaringan Komputer

Pengujian jaringan komputer dilakukan untuk mengetahui apakah sistem serta keamanan yang digunakan sudah cukup baik serta apabila terdapat celah keamanan dapat segera diperbaiki. Pengujian jaringan menggunakan *penetration testing* dengan Winbox, Putty, MAC Server, dan Nessus sebagai alat untuk melakukan pengujian dan mengetahui apakah pengujian berhasil atau tidak, serta melakukan pengamanan dari serangan terhadap jaringan komputer.

1. Winbox

Pengujian jaringan komputer yang pertama dilakukan menggunakan aplikasi Winbox untuk melakukan konfigurasi jaringan pada Mikrotik. Gambar 3 dan 4 adalah konfigurasi Winbox dan terlihat bahwa setelah *port default* Winbox diubah maka pengguna lain yang akan mengakses menggunakan *port default* Winbox tidak akan dapat masuk meskipun *user* dan *password* login yang digunakan sudah benar.

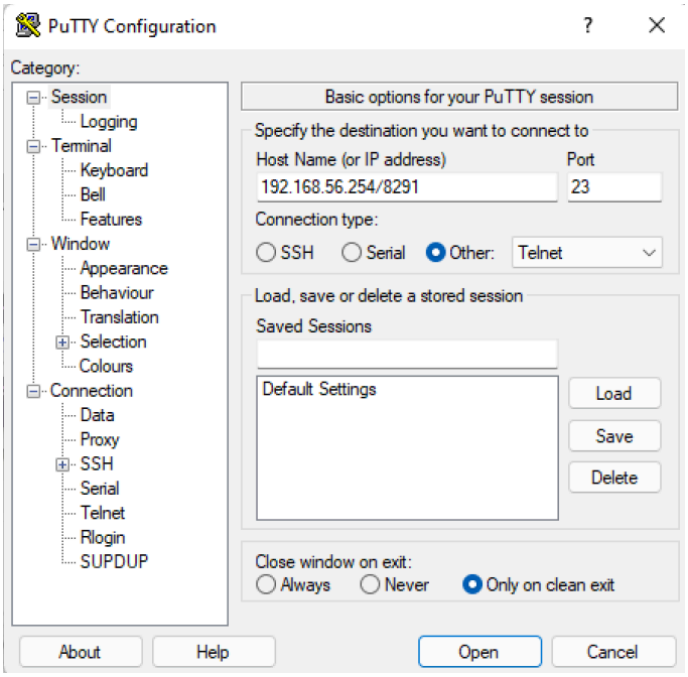
Gambar 3. Tampilan Interface Login pada Winbox dengan menggunakan port default

DOI: http://dx.doi.org/10.22441/fifo.2024.v16i2.003

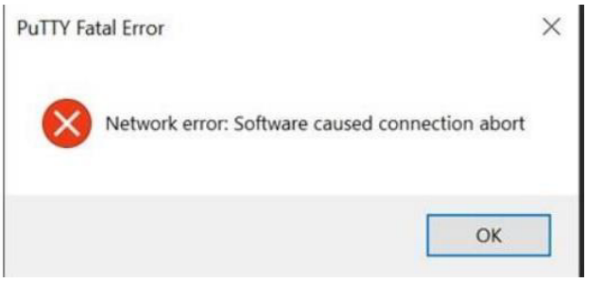
Gambar 4. Tampilan Erorr Login menggunakan port default Winbox

2. Putty

Pengujian jaringan komputer kedua menggunakan Telnet pada Aplikasi Putty yang biasa digunakan untuk akses jarak jauh terhadap jaringan. Gambar 5 dan 6 adalah konfigurasi Putty dan dapat terlihat bahwa setelah memasukkan IP Address serta *port default* Telnet diubah maka pengguna lain yang akan mengakses tidak dapat mengakses, karena sudah diubah meskipun telah memasukkan IP Address serta Port dengan benar.



Gambar 5. Tampilan Erorr Login menggunakan port default Winbox



Gambar 6. Tampilan Erorr Login menggunakan port default Telnet

3. Menonaktifkan atau Mengubah Fitur MAC Server

Dengan melakukan *disable* pada Discovery Interface bukan berarti router tidak dapat diakses jarak jauh menggunakan MAC Address Router. Jika menginginkan router untuk tidak dapat diakses jarak jauh menggunakan MAC Address melalui Winbox atau Telnet maka perlu menonaktifkan fitur MAC Server di Router. Untuk melakukan penonaktifan dapat ke menu Tools lalu pilih MAC Server.

4. Menonaktifkan Btest Server

Pengujian dapat memverifikasi tautan yang ditetapkan dengan fungsi Btest Server yang tersedia di Router Mikrotik. Namun, jika kemampuan ini tidak terduga digunakan oleh pihak ketiga, router dapat mencapai batasan bandwidth atau melihat kenaikan tiba-tiba dalam penggunaan CPU jika dipaksa untuk menciptakan lalu lintas atau menerima trafik untuk tes bandwith. Dalam beberapa kasus administrator sistem tidak menginginkannya sehingga pengujian menonaktifkan fungsi ini.

5. Mengaktifkan Bootloader Protector

Fitur Bootloader Protector digunakan untuk proteksi terhadap gangguan fisik yang dapat saja terjadi pada Routerboard terutama proteksi terhadap tombol reset yang ada di Router Mikrotik.

6. Mengamankan Fisik Router

Ada beberapa cara untuk mengamankan Fisik Router, yaitu: 1) melakukan proteksi kabel power agar jangan terlalu sering dicabut dan dicolok; 2) meletakkan Router pada ruangan dengan suhu yang cukup dingin agar dapat menjaga suhu perangkat Router Mikrotik; serta 3) memberikan perlindungan terhadap lonjakan listrik mengggunakan UPS atau yang melewati POE sebaiknya menggunakan Arester.

7. Nessus

Pengujian kali ini menggunakan salah satu IP yang digunakan oleh pengguna untuk mencari adanya kelemahan pada jaringan komputer di PT. SCM. Dari pengujian ini ditemukan ada beberapa *hosts* yang sedang terkoneksi dengan jaringan komputer. Dari koneksi ini kemudian ditemukan memiliki beberapa kelemahan mulai dari yang Critical, High, Medium sampai Low. Untuk beberapa kelemahan yang ditemukan kebanyakan berasal dari SSL yang pada terdapat celah. Hasil pengujian dan analisis jaringan komputer PT. SCM dapat dilihat pada Tabel 2.

Tabel 2 Hasil Pengujian dan Analisis

Pengujian dan Analisis	Hasil
Winbox	Tidak Berhasil
Telnet	Tidak Berhasil
MAC Server	Tidak Berhasil
Nessus	Berhasil

Untuk pengujian dan analisis menggunakan Telnet tidak berhasil karena port default Telnet yang digunakan sudah diubah yang menyebabkan tidak dapat lagi diakses atau erorr pada saat mencoba melakukan login menggunakan Telnet. Untuk pengujian dan analisis menggunakan MAC Server tidak berhasil karena tampilan MAC Server untuk Winbox dan Putty dimatikan oleh karena itu tidak dapat masuk ke jaringan komputer. Untuk pengujian dan analisis menggunakan Nessus berhasil mengetahui hosts yang sedang menggunakan jaringan internet dan juga terdapat beberapa kelemahan tentang SSL. Hasil ini mendukung beberapa penelitian sebelumnya terkait penggunaan pengujian penetrasi yang dapat membantu melakukan evaluasi konfigurasi jaringan komputer.

Akan tetapi hasil pengujian dan inalisis pada penelitian ini telah sampai pada tahap diskusi yang mana beberapa dari pengujian dengan penetration testing yang digunakan tidak berhasil karena masing–masing dari *port default* sudah diubah dengan *port* baru. Sedangkan untuk pengujian menggunakan Nessus berhasil untuk mengetahui apa saja kelemahan-kelemahan yang ditemukan. Selain itu juga dijelaskan mengapa dapat terjadi serta bagaimana cara untuk mengamankan jaringan komputer di PT. SCM. Pengujian juga menemukan beberapa IP Address yang digunakan pada saat melakukan proses *scanning* menggunakan Nessus. Namun, penelitian sebelumnya yang digunakan sebagai referensi pada penelitian ini belum ada yang menjelaskan bahwa dengan menggunakan Nessus, hasil pengujian dan analisis dapat meningkatkan keamanan jaringan, infrastruktur jaringan yang digunakan, dan bagaimana cara mencegah serangan yang dapat melumpuhkan sistem keamanan suatu jaringan komputer.

Ada beberapa keterbatasan yang ditemui selama pengujian, seperti tidak dapat bebas menggunakan IP Address untuk dilakukan pengujian dan analisis karena dapat mengganggu jalannya produksi oleh pengguna serta Mikrotik yang digunakan juga terbatas. Keterbatasan ini dijadikan sebagai dasar untuk usulan penelitian ke depan. Satu, pengujian dapat menyediakan pemindaian jaringan yang menyeluruh untuk menemukan perangkat yang terhubung, layanan yang berjalan, atau *port* yang terbuka. Data ini dapat digunakan untuk menemukan titik

masuk potensial bagi penyerang. Dua, hasil pengujian dan analisis ini harus diikuti dengan rekomendasi yang spesifik dan praktis untuk meningkatkan keamanan jaringan. Rekomendasi perbaikan ini dapat mencakup perbaikan kebijakan keamanan yang lebih baik, perubahan konfigurasi perangkat [8], pembaruan perangkat lunak, atau penerapan lebih banyak solusi keamanan. Tiga, hasil dari pengujian dan analisis yang dilakukan harus didokumentasikan dalam laporan yang lengkap yang mencakup ancaman yang teridentifikasi, dan rekomendasi dari perbaikan pada jaringan komputer SCM. Dan empat, keamanan jaringan komputer sangat penting sehingga perlu selalu melakukan pemeliharaan serta memperbaharui keamanan jaringan komputer yang sudah ada.

IV. Kesimpulan

Berdasarkan pengujian dan analisis yang telah dilakukan pada jaringan komputer PT. SCM secara keseluruhan dapat disimpulkan bahwa pengujian yang telah dilakukan seperti Winbox, Putty, dan MAC Server dinyatakan tidak berhasil. Hal ini disebabkan karena masing–masing dari port default sudah diubah dengan port baru pada saat konfigurasi. Hal ini menunjukkan bahwa untuk meningkatkan keamanan jaringan maka administrator jaringan tidak lagi menggunakan port default. Sedangkan untuk Nesuss berhasil dilakukan tetapi hanya dapat mendeskripsikan kelemahan SSL dan tidak dapat masuk ke dalam jaringan komputer. Selain itu usulan validasi dengan *Face Validity* berdasarkan hasil serta masukan dari beberapa pakar menyatakan secara umum usulan jaringan komputer SCM sudah memenuhi kebutuhan untuk sebuah jaringan komputer. Penggunaan Mikrotik Ruterboard pada jaringan komputer di SCM dapat memudahkan dalam melakukan monitoring serta dapat mengontrol jaringan komputer yang ada. Penggunaan fitur keamanan jaringan yang ada pada Mikrotik Routeboard dengan mengubah *user admin default*, menonaktifkan *service*, mengubah *port* Winbox, serta menonaktifkan *Neighbor's Discovery* cukup aman untuk jaringan komputer PT. SCM. Penggunaan *Management Bandwidth* dengan memanfaatkan fitur *Simple Queue* yang terdapat pada Mikrotik Routeboard membuat pembagian jaringan Internet tidak saling mengganggu terhadap divisi Development dan Operasional pada SCM.

Daftar Pustaka

[1] Baihaqi, Y. Yanti, and Zulfan, "Implementasi Sistem Keamanan WPA2-PSK pada Jaringan WiFi," *J Serambi Eng*, vol. 3, no. 1, pp. 248–254, 2018.
[2] I. K. Bayu, M. Yamin, and L. F. Aksara, "Analisa Keamanan Jaringan Wlan Dengan Metode Penetration Testing (Studi Kasus: Laboratorium Sistem Informasi dan Programming Teknik Informatika UHO," *SemanTIK*, vol. 3, no. 2, pp. 69–78, 2017.
[3] P. Panggabean, "Analisis Network Security Snort Metode Intrusion Detection System Untuk Optimasi Keamanan Jaringan Komputer," *Jursima*, vol. 6, no. 1, p. 1, 2018.
[4] D. M. Sari, M. Yamin, and L. B. Aksara, "Analisis Sistem Keamanan Jaringan Wireless (WEP, WPAPSK/WPA2PSK) Mac Address, Menggunakan Metode Penetration testing," *SemanTIK*, vol. 3, no. 2, pp. 203–208, 2017.
[5] M. Z. Hussain, M. Z. Hasan, M. Taimoor, and A. Chughtai, "Penetration Testing In System Administration," *Int J Sci Technol Res*, vol. 6, no. 6, pp. 275–278, 2017.
[6] B. V. Tarigan, A. Kusyanti, and W. Yahya, "Analisis Perbandingan Penetration Testing Tool Untuk Aplikasi Web," *J Pengemb Teknol Inf dan Ilmu Komput*, vol. 1, no. 3, pp. 206–214, 2017.
[7] N. A. Santoso, M. Ainurohman, and R. D. Kurniawan, "Penerapan Metode Penetrasion Testing Pada Keamanan Jaringan Nirkabel," *J Responsif Ris Sains dan Inform*, vol. 4, no. 2, pp. 162–167, 2022.
[8] H. Haeruddin and A. Kurniadi, "Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus: TP-Link Archer A6)," *Comb Manag ...*, vol. 1, no. 1, pp. 508–515, 2021.
[9] A. H. Harahap, C. Difa Andani, A. Christie, D. Nurhaliza, and A. Fauzi, "Pentingnya Peranan CIA Triad Dalam Keamanan Informasi dan Data Untuk Pemangku Kepentingan atau Stakholder," *J Manaj dan Pemasar Digit*, vol. 1, no. 2, pp. 73–83, 2023.
[10] F. Ulum and Amarudin, "Desain Keamanan Jaringan Pada Mikrotik Router Os Menggunakan Metode Port Knocking," *Teknoinfo*, 2018.
[11] K. Kaushik and A. Bhardwaj, "Perspectives on Ethical Hacking and Penetration Testing," 2023. [Online]. Available: https://www.igi-global.com/book/perspectives-ethical-hacking-penetration-testing/312214.
[12] I. G. A. S. Sanjaya, G. M. A. Sasmita, and D. M. S. Arsa, "Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF," *J Ilm Merpati (Menara Penelit Akad Teknol Informasi)*, vol. 8, no. 2, p. 113, 2020.
[13] U. Ravindran and R. V. Potukuchi, "A Review on Web Application Vulnerability Assessment and Penetration Testing," *Rev Comput Eng Stud*, vol. 9, no. 1, pp. 1–22, 2022.

[14] H. M. Z. Al Shebli and B. D. Beheshti, "A study on penetration testing process and tools," *2018 IEEE Long Isl Syst Appl Technol Conf LISAT 2018*, pp. 1–7, 2018.
[15] A. Borg, H. Klintskog, and I. Technology, "'What if someone steals it?' Hands-on evaluation of the software security work of a networked embedded system," 2022.