Volume 2 No. 4 2025, 529 - 538
DOI : https://doi.org/10.62335

Indonesian Journal of Community Empowerment
https://manggalajournal.org/index.php/maju
E-ISSN 3032-369X

PEMBELAJARAN TEKNOLOGI FIREWALL PADA MIKROTIK UNTUK MENINGATKAN KEAMANAN JARINGAN PT. PROXI JARINGAN NUSANTARA

Nurazizah zahra[1] , Anggun Fergina[2]

[1,2]Program Studi Teknik Informatika, Universitas Nusa Putra Sukabumi, Jawa Barat

E-mail: nurazizah.zahra_ti22@nusaputra.ac.id

ARTICLE INFO

Article history:
Received :29-05-2025
Revised :-20-06-2025
Accepted: 27-06-2025

Key words: *Network Security , Digital Transformation , Mikrotik , Firewall , Industry Collaboration*

DOI: *https://doi.org/10.62335*

ABSTRACT

This service activity presents the results of a practical study regarding network security optimization using Mikrotik at PT Proxi. This research is a practical lesson about firewall technology on Mikrotik to improve network protection. A Mikrotik component that allows network managers to manage data flows according to predetermined guidelines. With a deep understanding of firewalls, the aim is to block potentially harmful access, develop network policies, and strengthen overall security. the services required to use the software are NMAP, to recognize the software used, monitor through network scanning and port scanning, and explore the existing network security system. Thus, it is hoped that this activity will not only increase student capacity, but also provide benefits to the community in gaining more knowledge, in an effective way to strengthen network security technology around them.

ABSTRAK

Kegiatan pengabdian ini menyajikan hasil dari studi praktis mengenai optimasi keamanan jaringan menggunakan Mikrotik di PT Proxi. Penelitian ini merupakan pembelajaran praktis tentang teknologi firewall pada Mikrotik guna meningkatkan perlindungan jaringan. Komponen Mikrotik yang memungkinkan pengelola jaringan untuk mengatur arus data sesuai dengan pedoman yang sudah ditetapkan. Dengan pemahaman yang mendalam mengenai firewall, bertujuan untuk menghalangi akses yang berpotensi merugikan, menyusun kebijakan jaringan, serta memperkuat keamanan secara keseluruhan. layanan yang diperlukan menggunakan perangkat lunak adalah NMAP, untuk mengenali perangkat

lunak yang digunakan, memantau melalui pemindaian jaringan dan pemindaian port, serta menjelajahi sistem keamanan jaringan yang ada. Dengan demikian, kegiatan ini diharapkan tidak hanya meningkatkan kapasitas mahasiswa, tetapi juga memberikan manfaat kepada masyarakat memperoleh pengetahuan yang lebih, dengan cara yang efektif guna memperkuat teknologi keamanan jaringan disekitar.

PENDAHULUAN

PT Proxi Jaringan Nusantara, yang lebih dikenal sebagai Proxinet, merupakan perusahaan di bidang teknologi informasi yang diakui sebagai penyedia layanan internet yang dapat diandalkan di Indonesia. Berbasis di Batam, Proxinet berkomitmen untuk menjawab kebutuhan akses internet yang semakin krusial pada zaman digital ini. Dengan tim yang ahli dan berpengalaman dalam teknologi informasi, Proxinet bertekad untuk menyajikan layanan terbaik bagi konsumennya. Perusahaan ini memprioritaskan pengembangan jaringan yang terpercaya dan inovatif, dengan fokus pada kualitas layanan, keamanan data, serta kepuasan pelanggan.

Proxinet terus berusaha menghadirkan inovasi teknologi dan layanan internet dengan kecepatan terbaik untuk berbagai kebutuhan, mulai dari pengguna pribadi hingga usaha kecil dan perusahaan besar di seluruh Indonesia. Dengan pendekatan yang profesional dan responsif, Proxinet menjamin setiap pelanggan akan mendapatkan pengalaman yang memuaskan.

PT Proxi adalah perusahaan yang fokus pada solusi teknologi informasi, terutama dalam pengelolaan jaringan dan terkenal sebagai penyedia layanan internet. Kegiatan pengabdian ini bertujuan untuk masyarakat yang memiliki kesempatan untuk memperoleh pemahaman terkait dalam pembelajaran dalam mengamankan jaringan. PT Proxi Jaringan Nusantara memperlihatkan terhadap kemajuan pendidikan dan pengembangan sumber daya manusia. Upaya ini dapat memberikan dampak baik bagi perusahaan, baik dalam lingkungan akademis, masyarakat, maupun di sektor bisnis lainnya. Perusahaan akan diakui sebagai lembaga yang mendukung proses belajar dan penguatan generasi muda.

Kemajuan dalam dunia teknologi informasi ini sangat penting dan diterima dengan baik oleh masyarakat, karena bisa menjadi jawaban untuk menangani berbagai tantangan di berbagai bidang. Salah satu contoh perkembangan signifikan dalam teknologi informasi adalah adanya internet, sebuah jaringan internasional yang menghubungkan berbagai sistem komputer di seluruh dunia. Internet memberikan kebebasan kepada penggunanya untuk mendapatkan informasi tanpa batas, meskipun tidak semua konten tersebut bersifat positif [Harry Pribadi,2025].

Salah satu cara untuk melindungi pengguna dari risiko tersebut adalah dengan memanfaatkan teknologi firewall. Firewall bisa menjadi solusi untuk menjaga keamanan jaringan yang menghadapi berbagai ancaman baik dari dalam maupun luar. Hal ini memungkinkan pencegahan akses yang tidak sah serta pengendalian arus data yang bisa berbahaya. Oleh sebab itu, penerapan firewall yang tepat sangat

penting sebagai bagian dari usaha untuk mengamankan lingkungan digital secara lebih menyeluruh [Alamsyah, H.,2020].

Keamanan jaringan merujuk pada usaha melindungi sumber daya dari tindakan penyalahgunaan, modifikasi, pembatasan, serta perusakan oleh pihak yang tidak berhak [Putra,P.P., 2016]. Dalam banyak situasi, aliran lalu lintas dalam jaringan komputer seringkali tidak terjamin keamanannya; upaya untuk memperoleh akses ke jaringan tanpa izin bisa terjadi kapan saja, terutama di area publik dan saat ada data yang menarik untuk dieksplorasi. Salah satu aspek penting dalam keamanan adalah pencegahan, yang bertujuan untuk meminimalisir kemungkinan intrusi oleh pengguna yang tidak sah [Harry Pribadi,2025].

Mengenai pembelajaran tentang perlindungan jaringan, kegiatan pengabdian ini bertujuan untuk memahami bagaimana mengamankan jaringan dengan memanfaatkan firewall di perangkat mikrotik. Perangkat yang digunakan meliputi mikrotik, laptop, serta elemen seperti IP, DNS, firewall, dan lain-lain. Mikrotik, yang merupakan router yang banyak dipakai, memiliki sistem firewall yang efektif untuk memfilter lalu lintas jaringan, mencegah ancaman, dan mengatur akses bagi pengguna. Pembelajaran praktis mengenai firewall ini akan membantu pengguna untuk memahami cara menetapkan aturan firewall, memblokir port yang berisiko pada NMAP, serta membatasi akses ke sumber daya jaringan, sehingga dapat meningkatkan keamanan dan kestabilan jaringan.

Firewall adalah elemen penting dalam menjaga keselamatan jaringan, memungkinkan pengelolaan paket IP dengan cara yang efektif untuk mengenali host yang tersedia dalam jaringan. Sering dipakai untuk evaluasi keamanan, banyak pengelola sistem dan jaringan juga menyadari keuntungan untuk kegiatan seperti pencatatan jaringan, mengelola jadwal pembaruan layanan, dan memeriksa ketersediaan host atau layanan. Teori ini telah dipelajari dan diterapkan dalam situasi nyata, serta memberikan pengalaman berharga yang dapat meningkatkan keterampilan profesional. Selain itu, program pengabdian ini juga bertujuan untuk membangun jaringan profesional dan memahami budaya kerja di sektor teknologi informasi, yang sangat penting untuk perkembangan karier di masa depan.

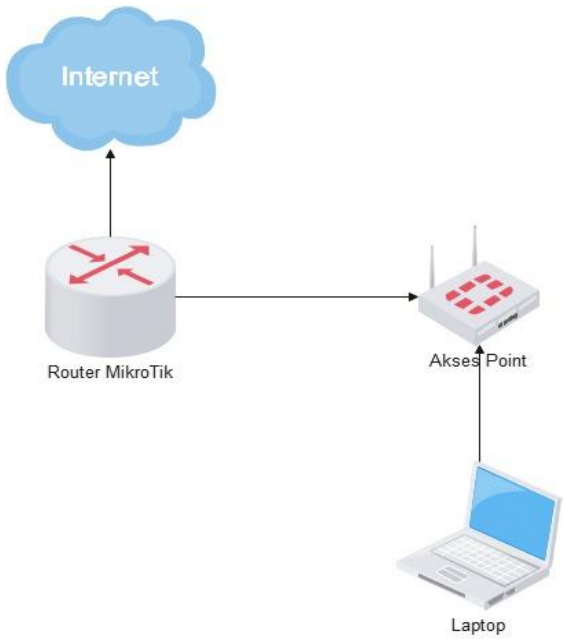
Kegiatan ini dirancang untuk membantu mahasiswa, terutama pada masyarakat dan ahli dalam bidang keamanan jaringan melalui kerja sama dengan PT Proxi. Melalui pembelajaran ini yang berfokus pada strategi keamanan jaringan, Mahasiswa diharapkan mampu memberikan pemahaman dalam menerapkan solusi keamanan jaringan sesuai kebutuhan masyarakat. Hasil dari pembelajaran ini diharapkan dapat diaplikasikan pada jaringan menggunakan mikrotik, guna meningkatkan perlindungan terhadap ancaman dan mendukung transformasi yang lebih aman.

METODE PELAKSANAAN

Dalam Kegiatan pengabdian ini, ada beberapa metode yang dilakukan untuk menjaga keamanan jaringan dengan menerapkan firewall pada bagian metode penerapan ini, sebelum di uraikan harus mengetahui terlebih dahulu topologi yang digunakan dan konfigurasi yang dilakukan. Topologi ini bertujuan untuk memahami

struktur jaringan secara menyeluruh, agar langkah-langkah selanjutnya dapat dilakukan secara efektif dan efisien [Sukma, D.,2023].

Topologi ini dibuat sederhana oleh penulis yang terdiri dari router mikrotik dan laptop untuk konfigurasi firewall keamanan jaringan. Langkah awal dalam topologi jaringan firewall ini, yaitu router mikrotik pada internet yang akan dihubungkan dengan akses point untuk mengelola jaringan. Hal ini bertujuan untuk meningkatkan keamanan dan mengetahui traffic jaringan. Dalam hal ini penulis pengabdian bersama dengan mitra yaitu PT Proxi melakukan penerapan firewall untuk keamanan jaringan menggunakan mikrotik, Tools yang digunakan untuk pengetesan adalah NMAP [Hairun, A. N.,2023]. Adapun langkah yang dilakukan yaitu sesuai topologi berikut.



Gambar 1 Topologi Jaringan firewall

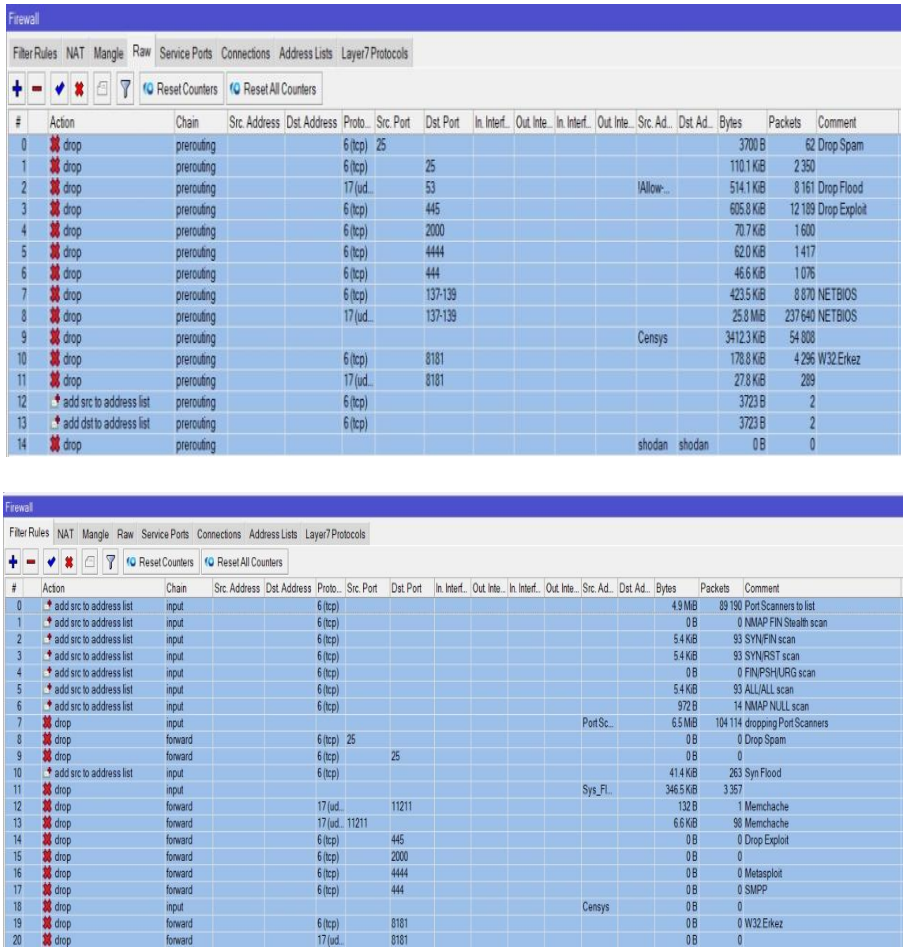
HASIL DAN PEMBAHASAN

Pengabdian kepada masyarakat ini merupakan upaya untuk memberikan ilmu, teknologi, dan seni kepada masyarakat. Aktivitas ini harus bisa memberikan manfaat tambahan bagi masyarakat, baik dalam aspek ekonomi, kebijakan, maupun perubahan sosial. Hasil dan pembahasan memanfaatkan pembelajaran dan pemahaman ini bentuk pengembangan kompetensi mahasiswa di bidang keamanan jaringan dengan metode studi pustaka sebagai sarana untuk memperoleh data dan informasi pendukung.

Yang dimana dilaksanakan pada tanggal 10 Februari 2025 yang berkolaborasi dengan PT Proxi Jaringan Nusantara Sukabumi, Jawa Barat.

Kegiatan ini melibatkan mahasiswa dengan tujuan memberikan pemahaman, pembelajaran dan pengalaman praktis mengenai pentingnya keamanan jaringan. Dengan menggunakan perangkat milik PT Proxi, penulis diberikan pembelajaran dengan mengenalkan perangkat pendukung teknologi firewall pada mikrotik untuk keamanan jaringan. Hasil dari pengabdian ini adalah memberikan pelayanan dan

pemahaman dalam keamanan jaringan kepada masyarakat. Firewall yang dilakukan mampu menangani keamanan dan informasi pada jaringan mikrotik. Adapun contoh Hasil konfigurasi firewall berikut ini.



Gambar 2 Konfigurasi Firewall

Membangun sistem keamanan yang tangguh adalah tantangan yang tidak sederhana dan juga memerlukan biaya yang tidak sedikit, terutama ketika harus melindungi setiap jalur akses, termasuk jaringan komputer. Kerentanan dalam jaringan bisa ditemukan dengan bantuan alat gratis seperti Nmap. Dengan alat ini, administrator jaringan mampu mengawasi semua informasi, termasuk mengidentifikasi port yang aktif maupun yang tidak aktif dari berbagai layanan. Dari informasi mengenai ketersediaan ini, kemudian dapat menganalisis status jaringan, apakah memiliki tingkat keamanan yang memadai atau sebaliknya [Sukma, D.,2023].

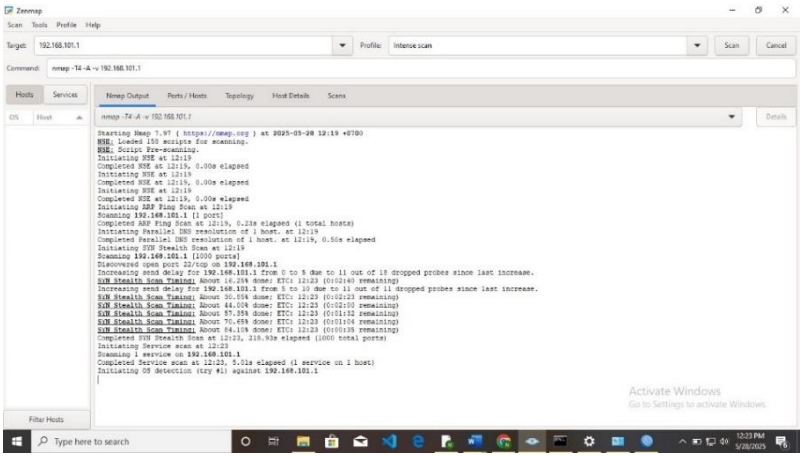
Dengan topologi yang dibuat, penulis dan tim PT Proxi memperoleh pemahaman mengenai pentingnya dalam menjaga keamanan jaringan. Oleh karena itu, penulis mencoba menerapkan firewall untuk keamanan jaringan menggunakan mikrotik, Tools yang digunakan untuk pengetesan adalah NMAP.

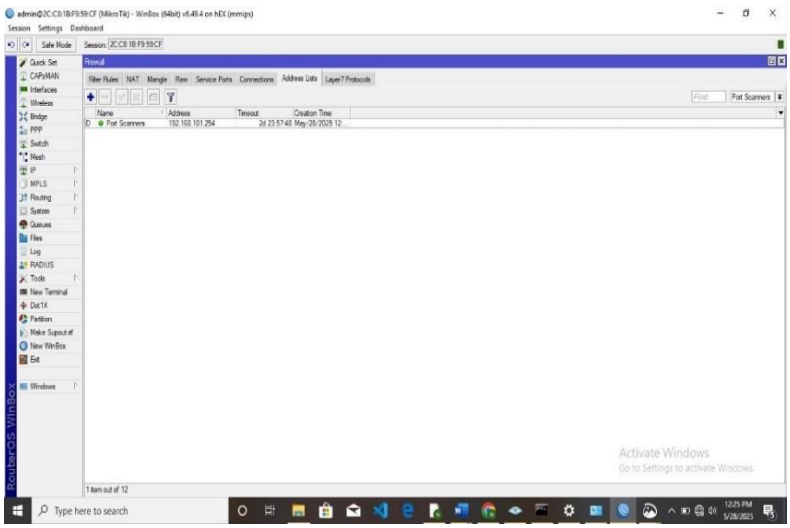
Network Mapper, lebih dikenal sebagai Nmap, merupakan perangkat lunak sumber terbuka yang dimanfaatkan untuk mengaudit dan menyelidiki keamanan

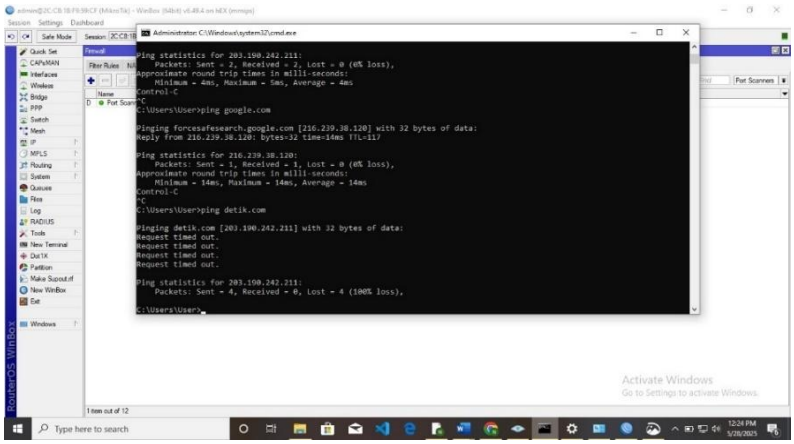
jaringan. Nmap dikembangkan oleh Gordon Lyon, yang sering disebut Fyodor Vaskovich, pada bulan September tahun 1997. Gordon Lyon adalah seorang pakar di ranah komputer, terutama dalam hal keamanan sistem komputer, serta seorang pengembang perangkat lunak open source.

Nmap (Network Mapper) adalah alat sumber terbuka untuk menganalisis dan memeriksa keamanan jaringan. Nmap memanfaatkan paket IP mentah untuk menentukan host yang terhubung ke jaringan, sekaligus memberikan informasi tentang layanan (termasuk nama aplikasi dan versinya), sistem operasi (beserta versinya), jenis firewall atau filter paket yang diterapkan, beserta berbagai ciri-ciri lainnya [Rendro, D. Bayu,2020].

Hasil keluaran dari Nmap berupa daftar host yang telah diperiksa beserta informasi tambahan sesuai dengan pilihan yang diterapkan. Salah satu informasi penting dalam daftar tersebut adalah "tabel port menarik". Tabel ini menampilkan daftar nomor port dan protokol, nama layanan, serta keadaan dari setiap port. Keadaan tersebut bisa berupa terbuka, difilter, tertutup, atau tidak difilter. Apabila keadaannya terbuka, ini menunjukkan bahwa aplikasi pada komputer tujuan sedang menunggu sambungan atau paket di port. Adapun contoh Hasil Pengetesan Keamanan Jaringan menggunakan NMAP







Gambar 3 Hasil Keamanan NMAP

Nmap merupakan alat sumber terbuka yang digunakan untuk menjelajahi dan memeriksa keamanan jaringan [Rendro, D. Bayu,2020]. Nmap terkenal sebagai salah satu alat yang mampu mengeksplorasi jaringan dengan cepat, bahkan dalam ekosistem jaringan yang sangat besar. Selain dipakai untuk mendeteksi potensi kekurangan dalam sistem keamanan jaringan dengan metode pemindaian port, identifikasi host, dan Mesin Pemrograman Nmap (NSE), para pengelola jaringan juga memanfaatkannya untuk berbagai keperluan, seperti pencatatan inventaris jaringan, pengelolaan jadwal pembaruan layanan, serta pemantauan ketersediaan host dan layanannya agar tetap berfungsi. Teknik yang dapat diterapkan oleh Nmap adalah melalui pemindaian port atau dengan mengakses lalu lintas jaringan untuk menemukan port yang terbuka maupun tertutup untuk dieksplorasi [Sudirman,2021].

Nmap menawarkan kemampuan untuk memeriksa dan mengevaluasi keamanan jaringan secara menyeluruh, dan berhasil masuk ke dalam daftar 125 alat keamanan jaringan terbaik menurut *SecTools.org,* Banyak praktisi, termasuk yang berorientasi negatif, semakin menyadari penggunaannya. Selain itu, Nmap dapat menjadi bahaya jika digunakan oleh orang yang tidak bertanggung jawab, sehingga mengenali karakteristik Nmap dengan langkah penting dalam merancang pencegahannya.

Fungsi utama Nmap adalah melakukan pemindaian port, yang didefinisikan sebagai aktivitas melakukan pemeriksaan dalam jumlah besar secara otomatis menggunakan alat, dalam hal Nmap. Pemindaian ini pada dasarnya adalah alat untuk mengecek port TCP/IP, yaitu sebuah aplikasi yang menyerang port TCP/IP dan layanan-layanannya (seperti telnet, ftp, http, https, dan lainnya) serta mencatat dari komputer yang ditargetkan. Dengan metode ini, pengguna pemindai dapat mengumpulkan informasi dari host yang menjadi sasaran [Rosnelly,2016].

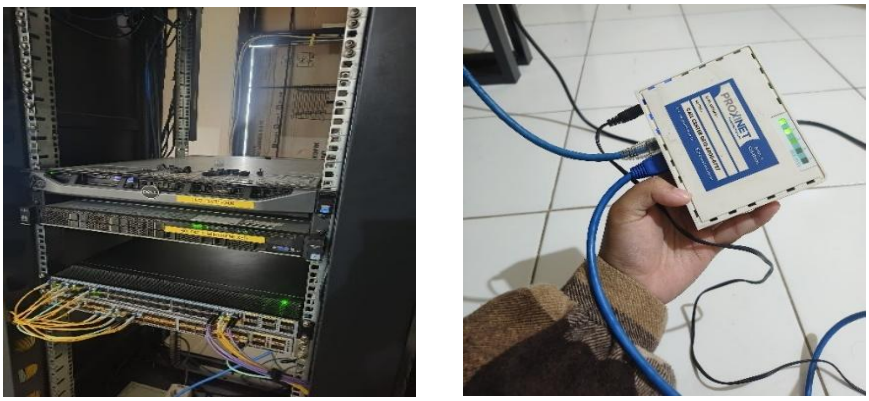
Nmap merupakan sebuah alat yang sangat berharga dan berguna dalam manajemen dan perlindungan jaringan. Dengan kemampuannya untuk memetakan jaringan serta mengidentifikasi perangkat yang aktif, Nmap membantu pengelola jaringan dalam memahami struktur jaringan secara mendalam. Fitur ini memfasilitasi deteksi awal terhadap potensi kekurangan dalam sistem keamanan yang dapat

dieksploitasi oleh individu yang tidak bertanggung jawab, sehingga memungkinkan tindakan pencegahan yang diperlukan sebelum terjadinya serangan.

Di samping itu, Nmap juga menyediakan fleksibilitas dalam penggunaannya, baik untuk skala kecil maupun besar, dan mendukung berbagai protokol yang umum di jaringannya. Dengan berbagai fitur canggih yang dimiliki, Nmap bukan hanya alat yang kuat untuk analisis jaringan tetapi juga sangat penting dalam membangun pertahanan jaringan yang kokoh. Nmap menjadi pilihan utama para profesional keamanan siber untuk mempertahankan integritas dan perlindungan jaringan mereka. Adapun Hasil pada Nmap.

Hasil dan Gambar

Gambar 4 Pengenalan firewall dengan NMAP



Gambar 5 Sistem Jaringan proxy pada (Mikrotik)

KESIMPULAN

Kegiatan pengabdian pada masyarakat ini melibatkan mahasiswa dan PT Proxi yang telah berkerja sama berhasil mencapai tujuan utama, yaitu meningkatkan kompetensi dalam bidang keamanan jaringan, melalui rangkaian yang dilakukan secara langsung, khususnya konfigurasi firewall pada mikrotik dengan memanfaatkan tools NMAP. Mahasiswa tidak hanya belajar tentang teori, tetapi juga mendapatkan pemahaman, pembelajaran dan pengalaman praktis yang lebih nyata.

Hasil yang didapatkan dari penerapan pembelajaran teknologi firewall pada mikrotik untuk meningkatkan keamanan jaringan menunjukan efektivitas yang

signifikan, sehingga secara langsung bekerja sama terhadap peningkatan keamanan jaringan yang dikelola oleh komunitas PT Proxi.

Kegiatan pengabdian ini, diharapkan dapat menjadi langkah awal sebagai pengalaman dan pembelajaran dalam menciptakan solusi keamanan jaringan yang dapat diterapkan secara luas terutama kepada masyarakat, dan berbagai komunitas atau organisasi. Selain itu, mahasiswa bekerja sama dengan PT Proxi untuk menekankan pentingnya menjalin erat antara akademisi dan industri. Kolaborasi ini tidak hanya memberikan manfaat secara langsung, tetapi meningkatkan dampak positif yang lebih luas dalam pengetahuan dan berkelanjutan bagi masyarakat secara keseluruhan.

Oleh karena itu, kegiatan ini diperluas dalam membantu meningkatkan ekosistem keamanan jaringan yang lebih responsif terhadap perkembangan teknologi. Dengan demikian, dapat memastikan bahwa masyarakat memiliki kemampuan dan wawasan yang dibutuhkan untuk mengatasi tantangan serta risiko dalam bidang teknologi informasi.

UCAPAN TERIMA KASIH

Penulis mengucapkan penghargaan kepada PT Proxi yang telah mendukung kegiatan pengabdian ini. Kolaborasi dan kerja sama ini terjalin memberikan banyak manfaat dalam pengetahuan teknologi terutama bagi masyarakat.

Terimakasih kepada tim PT Proxi yang telah memberikan pemahaman, pembelajaran dan pengalaman dan aktif berpatisipasi dengan memberikan dukungan. Harapan kami adalah agar kerja sama ini dapat terus berjalan dan memberikan manfaat yang baik bagi masyarakat di masa depan.

Penulis juga mengucapkan terima kasih kepada semua pihak yang telah berkolaborasi dalam pelaksanaan program pengabdian ini. Semoga apa yang telah didapatkan bermanfaat dan dapat menginspirasi kegiatan selanjutnya.

DAFTAR PUSTAKA

Fitrian, Harry Pribadi, et al. "IMPLEMENTASI MIKROTIK FIREWALL SEBAGAI SOLUSI FILTERING SITUS JUDI ONLINE DALAM JARINGAN." JATI (Jurnal Mahasiswa Teknik Informatika) 9.1 (2025): 1685-1691.

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.v5i1.1 240

Sukma, D., Mitro, S. S., kunci -Kemanan Jaringan, K., & Komputer, J. (n.d.). Penerapan Internet Positif Di SMK N 3 Pandeglang Berbasis Mikrotik Dengan Packet Filtering. Jurnal POLEKTRO: Jurnal Power Elektronik, 12(3), 2023. www.facebook.com

Hairun, A. N., Katili, M. R., Takdir, R., & Tuloli, M. S. (2023). Penerapan firewall di router OS mikrotik pada aplikasi e-rapor.Jambura Journal of Informatics, 5(2), 108–119. https://doi.org/10.37905/jji

Sudirman, Dede, and Akma Nurul Yaqin. "Network Penetration dan Security Audit Menggunakan Nmap." SATIN-Sains dan Teknologi Informasi 7.1 (2021): 32-44.

Rendro, D. Bayu, and W. Nugroho Aji. "Analisis Monitoring Sistem Keamanan Jaringan Komputer Menggunakan Software Nmap (Studi Kasus Di Smk Negeri 1 Kota Serang)." Jurnal Prosisko (2020): 108-115.

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

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.