KLIK: Kajian Ilmiah Informatika dan Komputer
ISSN 2723-3898 (Media Online)
Vol 4, No 1, Agustus 2023, Hal 634-641
DOI 10.30865/klik.v4i1.1157
https://djournals.com/klik

Analisis Keamanan Jaringan Menggunakan Metode Security Policy Development Life Cycle (SPDLC)

Yunanri W[1], Yuliadi[1,*], Shinta Esabella[1], Yasinta Bella Fitriana[2]

[1] Fakultas Rekayasa Sistem, Program Studi Informatika, Universitas Teknologi Sumbawa, Indonesia
[2] Program Studi Ilmu Komputer, Universitas Muhammadiyah Papua, Jayapura, Indonesia
Email: [1]yunanri.w@uts.ac.id, [2,*]yuliadi@uts.ac.id, [3]shinta.esabella@uts.ac.id, [4]yasintabella13@gmail.com
Email Penulis Korespondensi: yuliadi@uts.ac.id

Abstrak-Keamanan merupakan sebuah sistem untuk melakukan pencegahan pada jaringan dapat dilakukan dengan berbagai metode, seperti firewall, port scanning, dan DDoS. Firewall adalah sistem keamanan yang dapat membuka atau menutup akses port tertentu melalui firewall pada router sesuai dengan role yang dibangun. Salah satu metode keamanan jaringan yang diterapkan pada Mikrotik Router OS adalah Port Knocking, yaitu membuka atau menutup akses port tertentu melalui firewall pada router sesuai dengan role yang dibangun. namun permasalahan yang umum sering dialami dalam penyediaan layanan internet seperti jaringan keamanan jaringan Kafe Tapangpass adalah masalah hak akses, Beberapa masalah yang dihadapi seperti kebutuhan internet dalam keamanan jaringan, sehingga khawatir terjadinya peretasan pada jaringan mikrotik, maka dari itu peneliti akan melakukan analisis pada keamanan jaringan Kafe Tangpass. Menggunakan metode Security policy development life cycle, kemudian hasil dari analisis ini peneliti menerapkan keamanan jaringan firewall dari serangan port scanning dan denial of service. Hasil pengujian pada jaringan mikrotik kafe tapangpass rentan terhadap celah serangan jadi diperlukan nya keamanan pada firewall rulenya, Setting Secure Routerboard RB941-2nD, Pengujian secara berkala pada jaringan yang digunakan, upgrade Sistem Operasi pada Mikrotik.

Kata Kunci: Analisis; Keamanan; Firewall; Mikrotik; SPDLC

Abstract-Security is a system for carrying out prevention on a network that can be done using various methods, such as firewalls, port scanning, and DDoS. A firewall is a security system that can open or close certain port access through the firewall on the router according to the role that is built. One of the network security methods applied to Mikrotik Router OS is Port Knocking, which opens or closes certain port access through the firewall on the router according to the role that is built. However, a common problem that is often experienced in the provision of internet services such as the security network of the Tapangpass Cafe network is the problem of access rights. Several problems are encountered such as the need for internet in network security, so there is concern about hacking on the proxy network, therefore researchers will conduct an analysis on network security at Tangpass Cafe. Using the Security policy development life cycle method, then the results of this analysis researchers apply firewall network security from port scanning and denial of service attacks. The test results on the Tapangpass Café Mikrotik network are vulnerable to attack gaps, so security is needed on the firewall rules, Secure Routerboard RB941-2nD Settings, Periodic testing on the network used, and Upgrade the Operating System on Mikrotik

Keywords: Analysis; Security; Firewall; Mikrotik; SPDLC

1. PENDAHULUAN

Penggunaan sistem Informasi menjadi sebuah kewajiban bagi setiap individu maupun oraganisasi/ perusahaan. Namun dibalik kemudahan sistem yang ada, terdapat ancaman yang dapat menggangu keberadaan sistem sehingga dapat menyebabkan hilang data atau informasi, bahkan sampai terganggunya proses bisnis didalam suatu organisasi atau perusahaan. Karena hal tersebut Universitas Teknologi Sumbawa, tempat yang saat ini banyak digunakan di Indonesia dalam hal jasa pengiriman barang, Transfer uang masih banyak fitur yang digunakan secara *online*[1][2][3].

Dibutuhkan sebuah keamanan untuk menjaga komputer agar tidak terkena serangan oleh pihak luar yang tidak berwenang. Keamanan jaringan computer sebagai bagian dari sebuah system yang penting untuk menjaga validitas dan integritas data. Jaringan komputer sangat berkaitan erat dengan jaringan nirkabel. Seperti komputer, notebook, handphone dan peripheralnya mendominasi pemakaian teknologi wireless. Penggunaan teknologi wireless dalam suatu jaringan lokal sering dinamakan dengan WLAN (Wireless Local Area Network) dan dibutuhkan IDS untuk menganalisis keamanan jaringan nirkabel. Upaya untuk meningkatkan keamanan jaringan komputer salah satunya adalah dengan firewall. Implementasi dari sistem firewall ini dapat berupa software ataupun hardware yang bersifat aktif dengan melakukan penyaringan paket data yang lewat berdasarkan pengaturan yang diinginkan[3].

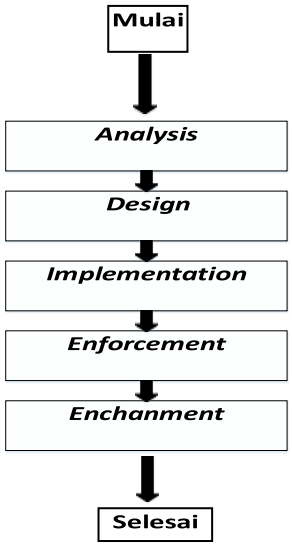
Kedai Tapangpass yang berlokasikan di Jl. Hasanudin No.95, Bugis, Kec. Sumbawa, Kabupaten Sumbawa, Nusa Tenggara Barat. Merupakan suatu usaha kafe yang bergerak pada bidang kuliner yang dilengkapi dengan layanan fasilitas internet kepada pelanggan[4][5]. Saat ini, kedai tersebut sudah memiliki teknologi jaringan, yakni Wireless *Local Area Network* (WLAN). Namun permasalahan yang umum sering dialami dalam penyediaan layanan internet seperti jaringan keamanan *mikrotik* Kafe Tapangpass adalah masalah hak akses, seperti yang diketahui bukan tidak mungkin dalam suatu keamanan jaringan akan terdapat pengguna yang tidak diinginkan mencoba untuk mengakses koneksi jaringan mikrotik Kafe Tapangpass tersebut seperti orang yang mengakses jaringan internet tanpa izin dengan melakukan scanning dan *denial of service* (DOS) untuk membobolnya. Peneliti melakukan observasi untuk menganalisis permasalahan pada keamanan jaringan kadang muncul masalah *user* yang tidak dikenal, pemilik kafe dan pengguna pastinya menginginkan akses layanan internet yang aman dan stabil[6].

Perkembangan teknologi dan telekomunikasi semakin berkembang dengan pesat, seiring makin modern maka pemanfaatan teknologi harus memberikan kemudahan, kenyamanan, keamanan dan lain sebagainya, ilmu komputer

banyak memeberikan kemudahan atau fiture-fiture menarik dan canggih, agar dimanfaatkan oleh masyarakat luas di Indonesia salah satunya, pengguna *wifi* pada sektor usaha UMKM, Adanya kendala yang menyebabkan menurunnya performa akses internet, maka dibutuhkan langkah-langkah menganalisa kendala, faktor utama yang menyebabkan, menurunya performa akses internet di Café Tapangpass resto[7]. Keamanan jaringan komputer adalah langkah untuk mencegah dan mengidentifikasi penggunaan yang tidak sah pada jaringan komputer. Fungsi untuk mengantisipasi ancaman baik fisik maupun logik yang dapat mengganggu aktifitas atau data yang ada dalam sistem pada jaringan komputer [8].

2. METODOLOGI PENELITIAN

Metode penelitian menggunakan metode kualitatif yang merupakan penelitian yang mendeskripsikan suatu berdasarkan permasalahan yang akan diteliti. Adapun metode kegiatan yang dilakukan diantaranta, yakni Observasi, Wawancara dan Studi Pustaka. Berdasarkan referensi definisi sejumlah model pengembangan sistem yang ada, dalam penelitian ini peneliti menggunakan metode pengembangan keamanan jaringan dengan metode *Security Policy Development Lifecycle* (SPDLC). Berikut penjelasan tahapan-tahapan dalam pada metode *Security Policy Development* [9] :



Gambar 1. Diagram Metodologi SPDLC

Gambar 1. menjelaskan tahapan-tahapan yang dilakukan dalam penelitian ini yang menggunakan metodologi SPDLC diantaranya adalah [10]:

a. *Analysis*

Tahap ini melakukan Pengumpulan data berupa informasi tentang kondisi objek penlitian saat ini seperti hasil wawancara, observasi, studi pustaka serta kebutuhan sebagai peningkatan keamanan jaringan mikrotik pada kedai Tapangpass.

b. *Design*

Pada tahap ini peneliti membuat perancangan berupa simulasi topologi jaringan susuai objek tempat penelitian yang akan di lakukan pengujian dengan menggunakan *software* GNS3.

c. *Implementation*

Kemudian tahap ini akan dilakukan implementasi dari rancangan topologi jaringan yang telah dibuat dari awal yaitu dengan melakukan instalasi dan menkonfigurasi dengan *software winbox*, seperti membuat *IP address list, dhcp, route, firewall* pada keamanannya *mikroti*knya.

d. *Enforcement*

Pada tahap ini, peneliti melakukan pengujian sistem keamanan pada *firewall mikrotik* yang bertujuan untuk mengetahui serangan yang dilakukan yaitu *Denial of Service* serta port *scanning yang digunakan oleh attacker.*

e. *Enchnmet*

Pada tahap ini, peneliti melakukan perbaikan system keamanan yang telah dibangun karean sebelumnya masih ada celah untuk serangan. yaitu membuat keamanan dari serangan *port scanning* dan *denial of service* pada *firewall mikrotik* dan hasil perbandingan dari sistem jaringan sebelumnya.

3. HASIL DAN PEMBAHASAN

Adapun dari penerapan hasil pengumpulan data dan metode pengembangan keamanan jaringan S*ecurity Policy Development Life Cycle* (SPDLC) yang telah diterapkan dan pada penelitian ini dibagi atas hasil dan pembahasan.

3.1 *Analysis*

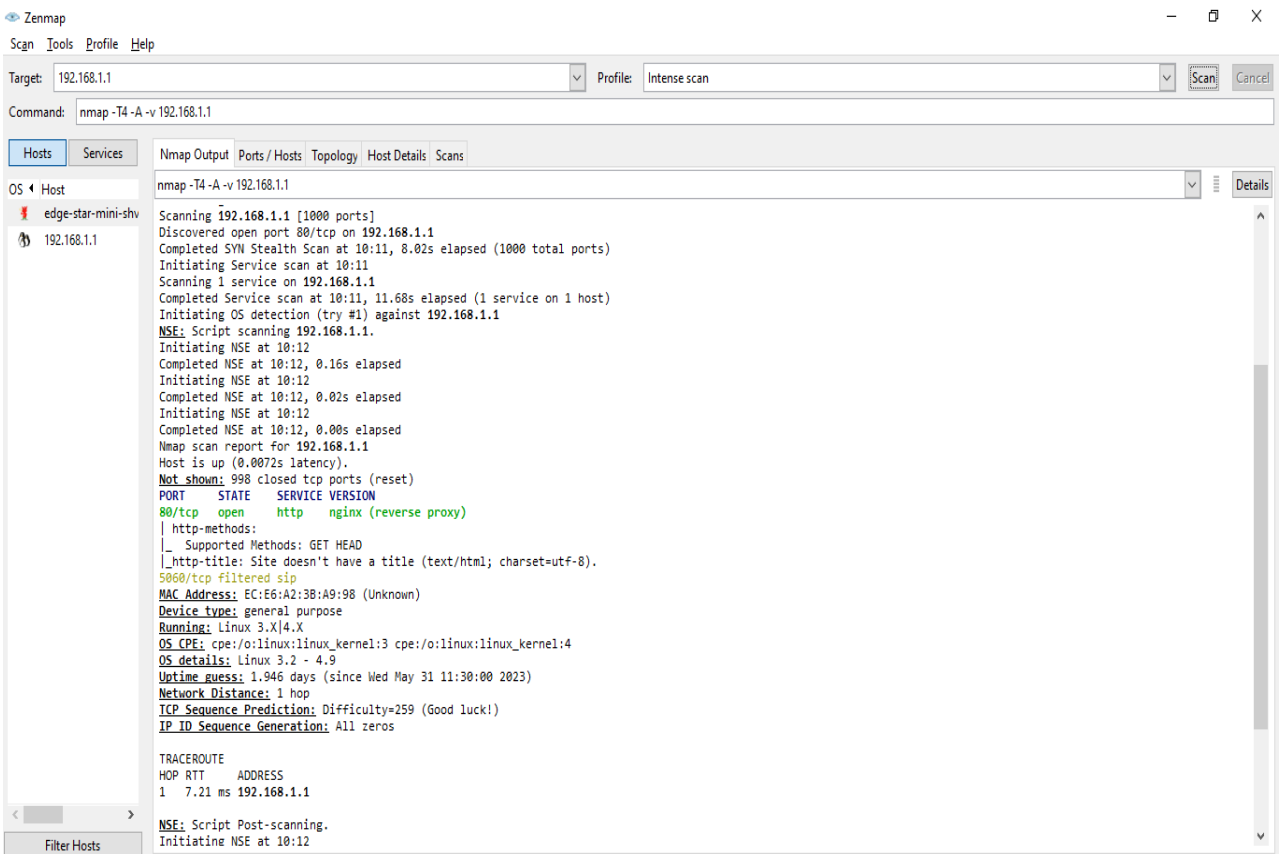
Pengumpulan data berupa informasi tentang kondisi target, karena sesuai kebutuhan sebagai akan keamanan jaringan mikrotik pada Kedai Tapangpass.

Melakukan *port scanning detection* dengan melakukan pengujian dengan *tool* NMAP menggunakan Kali Linux dengan memasukan perintah:

Scanning Tool Nmap

(kali㉿kali)-[~]

└─$ sudo nmap -v 192.168.1.1 -O



Gambar 2. Melakukan pengujian terhadap *IP* Tangpas Café menggunakan *tool* Nmap

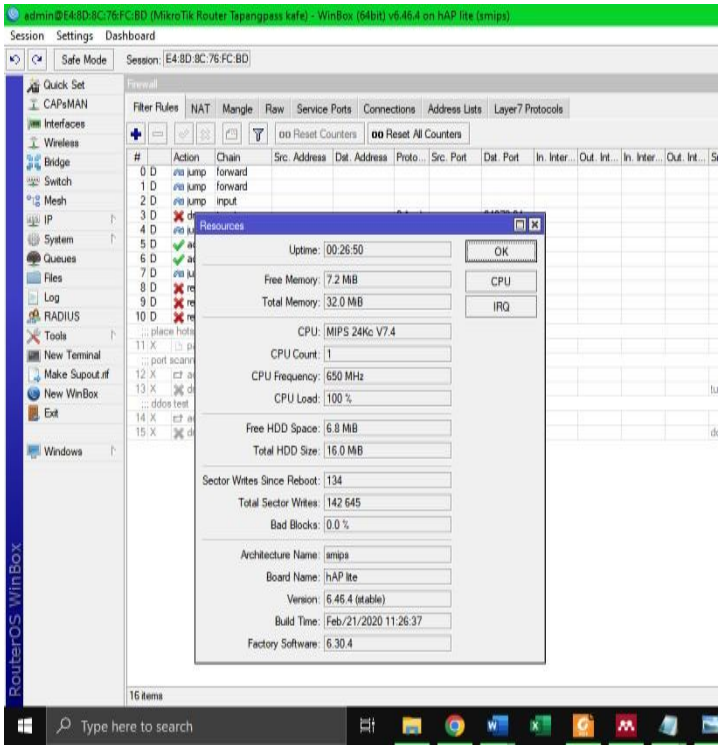
Pada gambar 2. dibawah merupakan perintah *port scanning* menggunakan *tool NMAP* pada kali linux, dan terlihat ternyata masih bisa ter*scanning* berhasil mendapatkan informasi *router mikrotik*, Tampilan aplikasi *advanced port scanning*. Tampilan aplikasi *advanced port scanning*.

3.2 *Design*

Gambar 3. Asal internet menggunakan provider Indihome Telkom

Di ketahui bahwa sumber internet dari modem diteruskan ke suatu *server* yang sudah dikonfigurasi *Webserver* dan *DNS*. Apabila terjadi serangan pada kondisi ini maka *server* dan administrator tidak dapat mengidentifikasi serangan yang terjadi pada *server* itu sendiri. Perlu adanya skenario *firewall* tambahan, seperti *IDS* dan pemblokiran *ICMP* untuk mendeteksi skenario serangan yang bila terjadi pada suatu *server*[11].

Resource dan mikrotik di Winbox:



Gambar 4. Serangan *DDos* yang berhasil masuk.

Seranga *DDos* yang berhasil menerobos blokir pada settingan winbox. Serangan *Distributed Denial of Service* (DDoS) adalah jenis serangan dunia maya yang bertujuan untuk mengganggu lalu lintas normal dari *server*, layanan, atau jaringan yang ditargetkan dengan membanjiri lalu lintas internet dari berbagai sumber. Pada tahun 2018, ditemukan kerentanan di Winbox yang memungkinkan penyerang melakukan serangan *DDoS* pada *router MikroTik*[12].

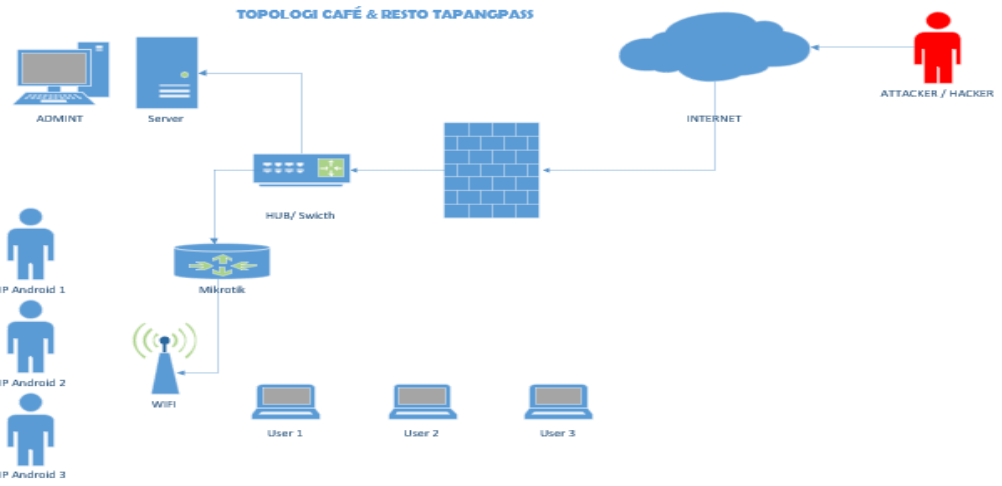
Kerentanan, yang dikenal sebagai *CVE*-2018-14847, memungkinkan penyerang melewati otentikasi dan mengeksekusi kode jarak jauh pada router yang ditargetkan. Penyerang kemudian dapat menggunakan router untuk meluncurkan serangan *DDoS* pada target lain atau menggunakannya sebagai *proxy* untuk menyembunyikan identitas mereka saat melakukan aktivitas berbahaya lainnya[13].

Gambar 5. Pengujian ke 2 menggunakan Nmap

Kemudian coba Kembali lagi melakukan scanning menggunakan *tools* NMAP pada kali linux dengan perintah dibawah ini: "> sudo nmap -v 192.168.0.1 -O" Gambar 4. 21 Tampilan perintah NMAP pada Kali Linux[14]. Pada gambar 5. Merupakan perintah serangan menggunakan *tools* NMAP pada kali linux, tapi serangannya gagal mendapatkan informasi dari *IP Routerboard Mikrotik*.

3.3 Impelementasi

Desain Topologi Resto & Café Tapangpass

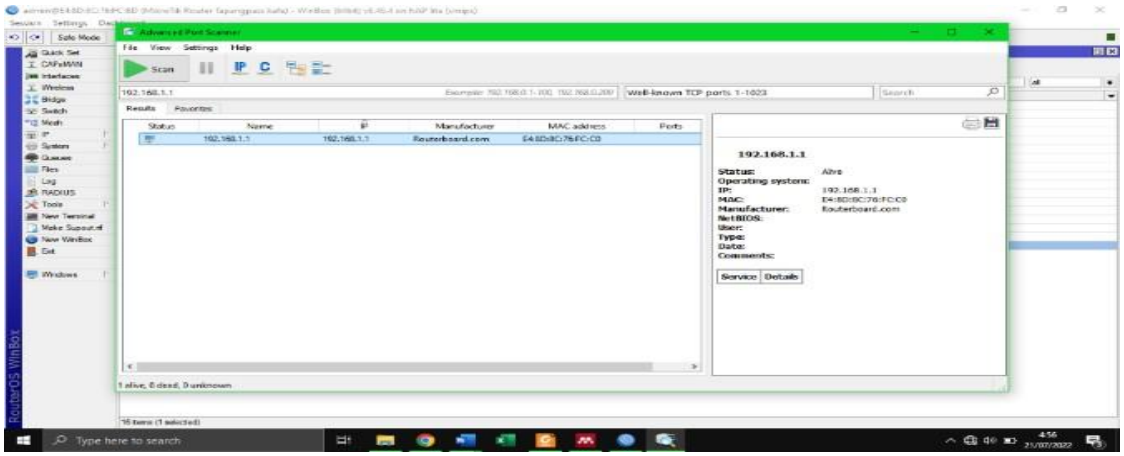


Gambar 6. Topologi café Tapangpass café & Resto

Café dan resto Tapangpass memeliki fasilitas wifi, baik digunakan dengan hp *android*, maupun dapat diakses dengan laptop. Dimana sekenario serangan oleh *attacker* di lakukan di luar jaringan LAN (*Local Area Network*). Dan gambaran infrastuktur jaringan pada Tapangpas resto sebagaimana pada gambar 6.

3.4 *Enforment*

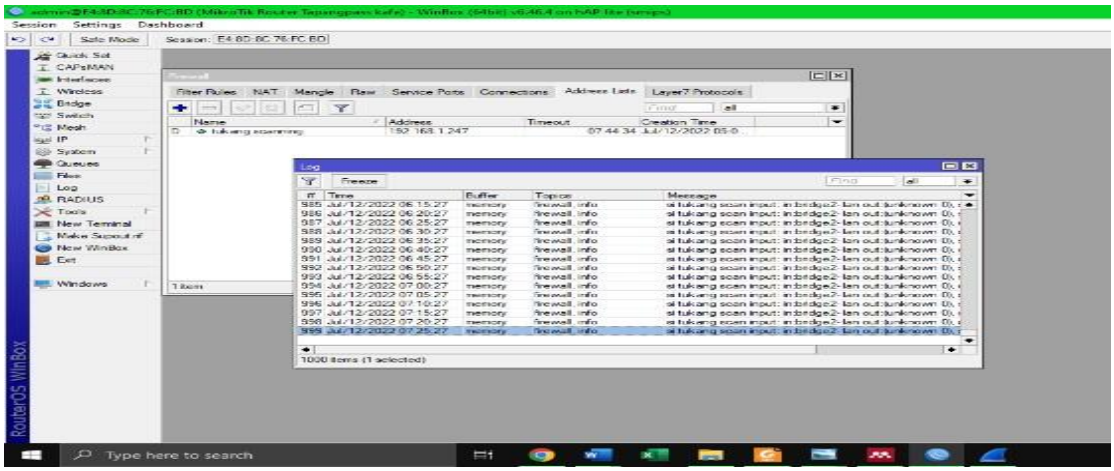
a. **Pengujian** bersifat menyerang atau Attacker :



Gambar 7. Serangan Pada Winbox

Merupakan pengujian serangan *port scanning* menggunakan aplikasi *advanced port scanner* pada *IP router* 192.168.1.1. dinyatakan gagal mendapatkan informasi *router mikrotik*[15].

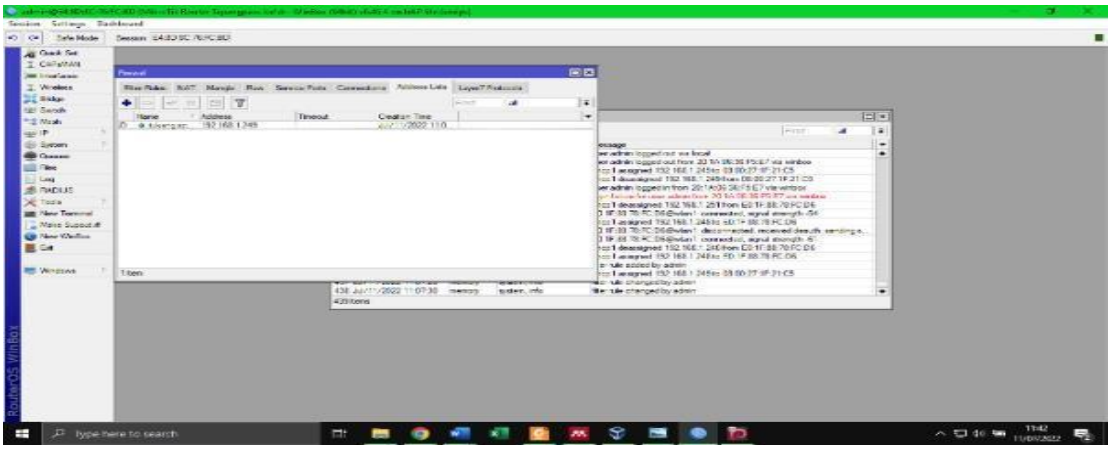
b. **Monitoring** *log message* di winbox *port scanning*:



Gambar 8. Mematau Log yang masuk pada winbox

Pada gambar 8. merupakan hasil *log* pesan dari informasi *port scanning* yang masuk, berarti serangan *port scanning* berhasil di blok.

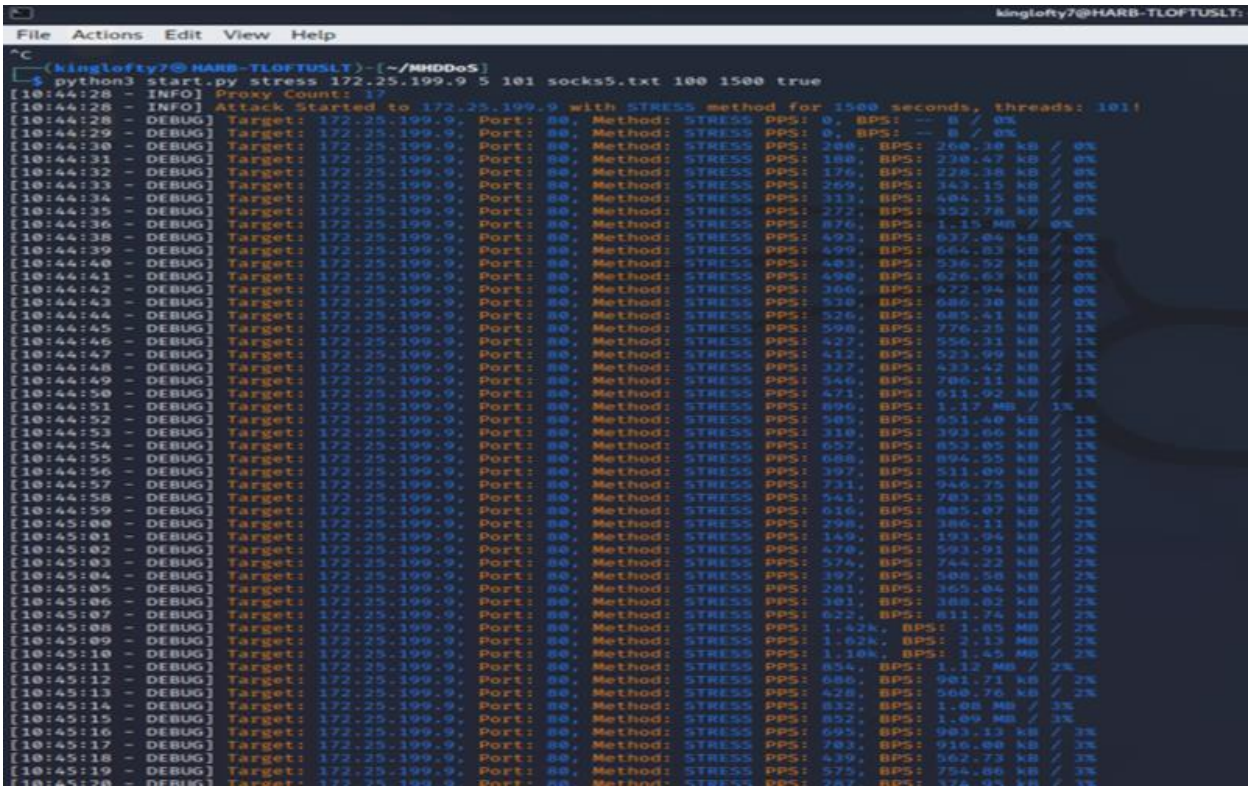
c. **Scanning** Tool Router Mikrotik.



Gambar 9. Address list dan *log* pada menu *firewall*

Pada gambar 9. Diatas merupakan hasil *scanning* dari aplikasi *advanced port scanning*, dan terlihat bahwa berhasil mendapatkan informasi *router mikrotik* dari melakukan *scanning* pada *Ip Router Mikrotik* 192.168.1.1.

d. Tool MHDDOS



Gambar 10. Serangan DDos pada jaringan

Perintah serangan *Denial of Service* menggunakan *tools* MHDDOS di kali linux untuk melakukan pengujian serangan *DDOS* yang dimana meyerang *Ip Router Mikroik* 192.168.1.1[16][17]. Berikut perintah *CLI* dari serangan *Denial Of Service* menggunakan *tools MHDDOS* pada kali linux:

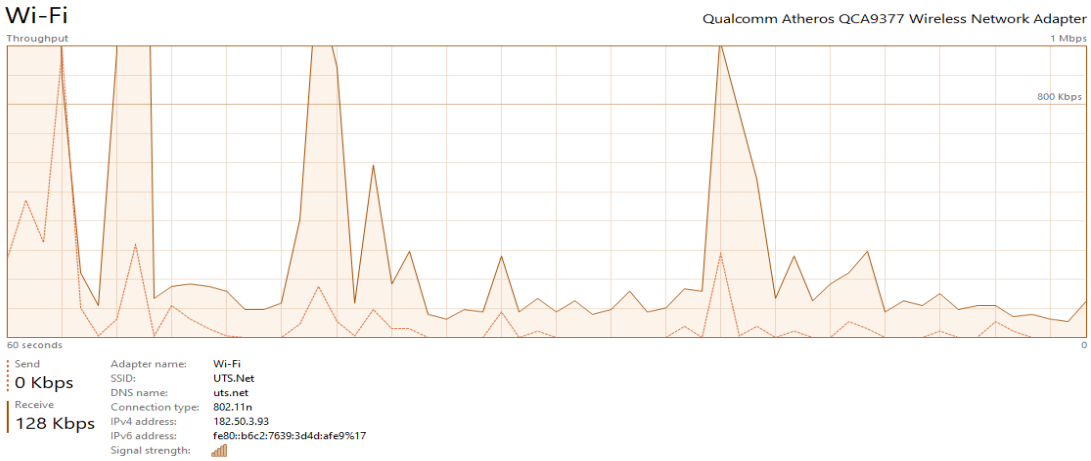
"*cd MHDDoS"*

"Python3 start.py dgb 192.168.1.1/HIT 1 100 *proxy.txt* 1000 8585".

Hasil yang dpat disajikan pada bagian 4 dapat berupa

1. Implementasi jaringan, *interface*, prototipe
2. Pengujian kinerja, quisoner pengujian
3. Hasil pengujian dalam bentuk *table* dan *graphic*

Berdasarkan serangan DDos dilakukan secara simultan oleh *Hacker* pada *server* utama.



Gambar 11. Grafik serangan DDOS pada jaringan utama.

Winbox yang dimana untuk melihat CPU *load* yang sebelunya mencapai 100% karena adanya serangan *denial of service* dan sekarang kembali normal dibawah 5 % karena sudah dicegah oleh drop *firewall rules*. Berikut adalah perbandingan dari jaringan sebelum dilakukan pengamanan dan setelah pengamanan dilakukan jaringan pada *firewall mikrotik*[18] [19].

3.5 *Enchment*

Perbaikan sistem keamanan yang telah dibangun karean sebelumnya masih ada celah untuk serangan. yaitu membuat keamanan dari serangan *port scanning* dan *denial of service* pada *firewall mikrotik* dan hasil perbandingan dari sistem jaringan sebelumnya[20].

Table 1. Hasil pengujian yang telah dilakukan

No	Metode Pengujian	Hasil perbandingan
1	Sebelum melakukan konfigurasi pengamanan dengan menggunakan *firewall* dari Serangan *port Scanning* dan *Denial of service.*	Mudah untuk dilakukan penyerangan oleh port scanning dan *denial of service* sehingga menyebabkan jaringan menjadi *down* saat digunakan dan winbox nya langsung tidak bisa *login*.
2	Setealah melakukan konfigurasi pengamanan dengan menggunakan *firewall* dari Serangan *port Scanning* dan *Denial of service.*	Jaringan tidak dapat lagi diserang oleh *Port Scanning* dan *Denial of service* karena telah dilakukan pengamanan jaringan dengan menggunakan konfigurasi *firewall* dari *mikrotik*

4. KESIMPULAN

Berdasarkan dari hasil pengujian pada pembahasan diatas jaringan mikrotik kafe tapangpass rentan terhadap celah serangan jadi diperlukan nya keamanan pada *firewall* rulenya. Dari penelitian ini juga mendapatkan solusi bagaimana mengamankan jaringan sehingga menjadi evaluasi dalam meningkatkan keamanan nya. Pada penelitian ini pula sangatlah diperlukan bagi *administrator network,* tidaklah mudah diterapkan oleh seorang *attacker* apabila *bug* dari suatu *network* dan *website* tidak ditemukan dan adanya juga pengamanan enkripsi pada *page login password MD5* enkripsi, dikarenakan untuk mengetahui *bug* suatu jaringan dan *website* dibutuhkan kemampuan yang cukup mengenai structure dari *MYSql,* dalam artian *SQL injecton* akan terjadi jika memang ada kesalahan *setting port* yang terbuka atau *open* serta *script* pada *website*, *webserver* hasil deteksi yang dilakukan oleh *tool snort* yang ditemukan dari percobaan *attacker* menggunakan *software sqlmap* tapi hasil *scan*nya tidak menemukan *database* maka serangan terdeteksi oleh *snort* sebagai serangan *DDoS* dengan tingkat *priority 2* (medium), Pada pengujian teknik serangan *DDoS* yang dilakukan dengan berfokus pada *port 22 ssh,port 80 open* didapat teknik ini.

REFERENCES

[1] R. Umar and A. P. Marsaid, "Analisis Keamanan Jaringan LAN Terhadap Kerentanan Jaringan Ancaman DDoS Menggunakan Metode Penetration Testing," vol. 10, no. 1, pp. 317–329, 2023, doi: 10.30865/jurikom.v10i1.5835.

[2] C. D. Berliana, T. A. Saputra, and I. Gunawan, "Analisis Serangan dan Keamanan pada Denial of Service (DOS): Sebuah Review Sistematik," *JIIFKOM (Jurnal Ilm. Inform. Komputer) STTR Cepu*, vol. 1, no. 2, pp. 33–38, 2022, [Online]. Available: https://www.sttrcepu.ac.id/jurnal/index.php/jiifkom/article/view/229/140.

[3] M. A. Ridho and M. Arman, "Analisis Serangan DDoS Menggunakan Metode Jaringan Saraf Tiruan," *J. Sisfokom (Sistem Inf. dan Komputer)*, vol. 9, no. 3, pp. 373–379, 2020, doi: 10.32736/sisfokom.v9i3.945.

[4] I. Riadi, A. Yudhana, and Y. W, "Analisis Keamanan Website Open Journal System Menggunakan Metode Vulnerability Assessment," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 7, no. 4, p. 853, 2020, doi: 10.25126/jtiik.2020701928.
[5] Yunanri. W and Yasinta Bella Fitriana, "Analisis Network Security Komputer Tingkat Desa Menggunakan Metode Security Policy Development Life Cycle (SPDLC)," *J. Tek. Juara Aktif Glob. Optimis*, vol. 1, no. 2, pp. 11–21, 2021, doi: 10.53620/jtg.v1i2.28.
[6] M. Jufri and H. Heryanto, "Peningkatan Keamanan Jaringan Wireless Dengan Menerapkan Security Policy Pada Firewall," *JOISIE (Journal Inf. Syst. Informatics Eng.*, vol. 5, no. 2, pp. 98–108, 2021, doi: 10.35145/joisie.v5i2.1759.
[7] Y. W, R. Anto, D. Teguh Yuwono, and Y. Yuliadi, "Deteksi Serangan Vulnerability Pada Open Jurnal System Menggunakan Metode Black-Box," *J. Inform. dan Rekayasa Elektron.*, vol. 4, no. 1, pp. 68–77, 2021, doi: 10.36595/jire.v4i1.365.
[8] R. Yasuda and G. J. Augustine, "Teknologi informasi dan Komunikasi sebagai Media Pembelajaran," *Brain Cell Biol.*, vol. 36, no. 1–4, pp. 1–2, 2008, doi: 10.1007/s11068-008-9037-4.
[9] T. H. Damayanti and I. R. Hikmah, "Network Forensic Serangan DoS pada Jaringan Cloud berdasarkan Generic Framework for Network Forensics (GFNF)," *Edumatic J. Pendidik. Inform.*, vol. 6, no. 2, pp. 334–343, 2022, doi: 10.29408/edumatic.v6i2.6466.
[10] F. Antony and R. Gustriansyah, "Deteksi Serangan Denial of Service pada Internet of Things Menggunakan Finite-State Automata," *MATRIK J. Manajemen, Tek. Inform. dan Rekayasa Komput.*, vol. 21, no. 1, pp. 43–52, 2021, doi: 10.30812/matrik.v21i1.1078.
[11] J. Hu *et al.*, "A memory-related vulnerability detection approach based on vulnerability features," *Tsinghua Sci. Technol.*, vol. 25, no. 5, pp. 604–613, 2020, doi: 10.26599/TST.2019.9010068.
[12] D. Pasha, A. thyo Priandika, and Y. Indonesian, "Analisis Tata Kelola It Dengan Domain Dss Pada Instansi Xyz Menggunakan Cobit 5," *J. Ilm. Infrastruktur Teknol. Inf.*, vol. 1, no. 1, pp. 7–12, 2020, doi: 10.33365/jiiti.v1i1.268.
[13] A. Ranitania and A. Fahmi, "Analisis Tata Kelola Proses Layanan Keamanan Kegiatan E-Procurement Pada Lpse Provinsi Jawa Tengah Berdasarkan Kerangka Kerja COBIT 5," pp. 1–7, 2015.
[14] A. Schröter, N. Bettenburg, and R. Premraj, "Do stack traces help developers fix bugs?," *Proc. - Int. Conf. Softw. Eng.*, pp. 118–121, 2010, doi: 10.1109/MSR.2010.5463280.
[15] M. Alenezi, A. Agrawal, R. Kumar, and R. A. Khan, "Evaluating Performance of Web Application Security through a Fuzzy Based Hybrid Multi-Criteria Decision-Making Approach: Design Tactics Perspective," *IEEE Access*, vol. 8, pp. 25543–25556, 2020, doi: 10.1109/ACCESS.2020.2970784.
[16] R. Hermawan, "Analisis Konsep Dan Cara Kerja Serangan Komputer Distributed Denial of Service (Ddos)," *Anal. Konsep Dan Cara Kerja Serangan Komput. Distrib. Denial Serv.*, vol. 5, no. 1, pp. 1–14, 2013.
[17] M. A. Ridho and M. Arman, "Analisis Serangan DDoS Menggunakan Metode Jaringan Saraf Tiruan," *J. Sisfokom (Sistem Inf. dan Komputer)*, vol. 9, no. 3, pp. 373–379, 2020, doi: 10.32736/sisfokom.v9i3.945.
[18] J. D. Santoso, "Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System," *Infos*, vol. 1, no. 3, pp. 44–50, 2019.
[19] T. Mahjabin, Y. Xiao, T. Li, and C. L. P. Chen, "Load Distributed and Benign-Bot Mitigation Methods for IoT DNS Flood Attacks," *IEEE Internet Things J.*, vol. 7, no. 2, pp. 986–1000, 2020, doi: 10.1109/JIOT.2019.2947659.
[20] A. Alzahrani, A. Alqazzaz, N. Almashfi, H. Fu, and Y. Zhu, "Web Application Security Tools Analysis," *Stud. Media Commun.*, vol. 5, no. 2, p. 118, 2017, doi: 10.11114/smc.v5i2.2663.