Journal of Internet and Software Engineering Vol: 1, No 3, 2024, Page: 1-9

Kontrol Lalu Lintas Jaringan *Wi-Fi* menggunakan *Evil Limiter* pada *Kali Linux*

Nabil Arif A'isy*, David Zico Rafael Sitorus, Mohammad Hafiz Fachrezi Lubis, Shelvie Nidya Neyman

Teknologi Rekayasa Komputer, Sekolah Vokasi, IPB University

Abstrak: Kontrol lalu lintas jaringan *Wi-Fi* semakin kompleks dengan bertambahnya perangkat yang terhubung. Penelitian ini mengevaluasi penggunaan *Evil Limiter* di *Kali Linux* untuk mengendalikan dan membatasi lalu lintas jaringan *Wi-Fi*. Evil Limiter adalah perangkat lunak yang menggunakan teknik *spoofing* ARP untuk mengatur *bandwidth* perangkat dalam jaringan lokal. Tujuan utama penelitian ini adalah mengevaluasi efektivitas *Evil Limiter* dalam mengontrol lalu lintas data dan mengurangi penggunaan *bandwidth* yang berlebihan, sehingga meningkatkan kinerja jaringan. Metodologi penelitian mencakup pengujian di berbagai lingkungan jaringan dan analisis kinerja sebelum dan sesudah penerapan *Evil Limiter*. Hasil penelitian menunjukkan bahwa *Evil Limiter* dapat secara signifikan mengurangi konsumsi *bandwidth* dan meningkatkan stabilitas jaringan. Selain itu, penelitian ini mengidentifikasi potensi risiko dan dampak keamanan dari penggunaan alat ini. Kesimpulan penelitian ini menyatakan bahwa *Evil Limiter* di *Kali Linux* adalah solusi efektif dan efisien untuk manajemen lalu lintas jaringan *Wi-Fi*, meskipun penggunaannya harus mempertimbangkan aspek keamanan. Penelitian ini memberikan kontribusi penting bagi pengelolaan jaringan *Wi-Fi* di berbagai lingkungan seperti rumah, kantor, dan ruang publik.

Kata kunci: *Bandwidth*, *Evil Limiter*, Jaringan, *Kali Linux*, *Wi-Fi*

DOI: https://doi.org/10.47134/pjise.v1i3.2650
*Correspondence: Nabil Arif A'isy
Email: nabilarifaisy@apps.ipb,ac.id

Received: 15-05-2024
Accepted: 30-06-2024
Published: 31-07-2024

Abstract: *Wi-Fi network traffic control has become increasingly complex with the growing number of connected devices. This study evaluates the use of Evil Limiter on Kali Linux to control and limit Wi-Fi network traffic. Evil Limiter is software that uses ARP spoofing techniques to regulate the bandwidth of devices within a local network. The main objective of this research is to evaluate the effectiveness of Evil Limiter in controlling data traffic and reducing excessive bandwidth usage, thereby improving network performance. The research methodology includes testing in various network environments and analyzing performance before and after implementing Evil Limiter. The results show that Evil Limiter can significantly reduce bandwidth consumption and enhance network stability. Additionally, this study identifies potential risks and security impacts of using this tool. The conclusion of this research indicates that Evil Limiter on Kali Linux is an effective and efficient solution for managing Wi-Fi network traffic, although its use must consider security aspects. This study makes an important contribution to Wi-Fi network management in various environments such as homes, offices, and public spaces.*

Keywords: *Bandwidth, Evil Limiter, Kali Linux, Network, Wi-Fi*

Pendahuluan

Di era *digital* ini, internet dan jaringan *Wi-Fi* telah menjadi kebutuhan dasar dalam kehidupan sehari-hari. Penggunaan internet mencakup berbagai aspek kehidupan seperti komunikasi, pendidikan, bisnis, kesehatan, dan hiburan. Dengan perkembangan teknologi, permintaan untuk akses internet yang cepat, stabil, dan andal semakin meningkat.

Keamanan jaringan nirkabel (*Wi-Fi*) merupakan aspek penting yang perlu diperhatikan oleh individu dan organisasi di era *digital* saat ini. Meskipun *Wi-Fi* memudahkan akses internet, jaringan ini rentan terhadap berbagai ancaman keamanan, termasuk pembobolan. Salah satu alat yang sering digunakan untuk menguji keamanan jaringan *Wi-Fi* adalah Kali *Linux*, sebuah distribusi *Linux* yang dirancang khusus untuk pengujian penetrasi dan audit keamanan.

Kali *Linux* sangat dikenal di kalangan profesional keamanan siber dan *hacker* etis karena menyediakan berbagai alat yang kuat untuk pengujian penetrasi. Beberapa alat yang sering digunakan untuk membobol *Wi-Fi* di Kali *Linux* antara lain *Aircrack-ng*, *Reaver*, dan *Wifite*. Alat-alat ini memungkinkan pengguna untuk menemukan kerentanan dalam jaringan *Wi-Fi* dan mengeksploitasi kelemahan tersebut untuk mengakses jaringan tanpa izin.

Internet dan jaringan *Wi-Fi* telah menjadi bagian penting dalam kehidupan sehari-hari di era *digital*. Kecepatan dan stabilitas koneksi internet menjadi faktor kunci yang mempengaruhi produktivitas dan kenyamanan pengguna. Namun, semakin banyak perangkat yang terhubung ke jaringan *Wi-Fi* sering kali menyebabkan penurunan kecepatan internet dan penggunaan *bandwidth* yang tidak terkendali. Untuk mengatasi masalah ini, diperlukan alat yang dapat mengelola dan membatasi penggunaan jaringan *Wi-Fi* secara efektif. Salah satu alat yang dapat digunakan untuk tujuan ini adalah *Evil Limiter*, sebuah perangkat lunak *open-source* yang berjalan di *Kali Linux*.

Evil Limiter adalah alat yang dirancang untuk memantau dan mengontrol perangkat yang terhubung ke jaringan lokal. Dengan *Evil Limiter*, pengguna dapat membatasi atau memblokir koneksi internet dari perangkat tertentu yang terhubung ke jaringan *Wi-Fi*. Alat ini bekerja dengan memanfaatkan teknik ARP *spoofing* dan *traffic shaping* untuk mengontrol aliran data di jaringan. *Evil Limiter* sangat berguna dalam situasi di mana pengguna ingin mengendalikan penggunaan bandwidth dan memastikan jaringan tidak terbebani oleh perangkat tertentu.

Metode

Penelitian ini menggunakan metode penelitian pengumpulan data. Data yang dibutuhkan untuk penelitian ini akan dikumpulkan melalui beberapa langkah berikut:

1. Studi Literatur: Mengumpulkan informasi dari jurnal, buku, dan sumber online yang berkaitan dengan kontrol lalu lintas jaringan dan penggunaan *Evil Limiter*.
2. Observasi: Melakukan pengamatan langsung terhadap jaringan *Wi-Fi* untuk memahami pola lalu lintas data serta mengidentifikasi masalah yang sering terjadi.
3. Eksperimen: Menerapkan *Evil Limiter* dalam lingkungan jaringan yang terkendali untuk mengumpulkan data mengenai efektivitasnya untuk mengendalikan lalu lintas jaringan.

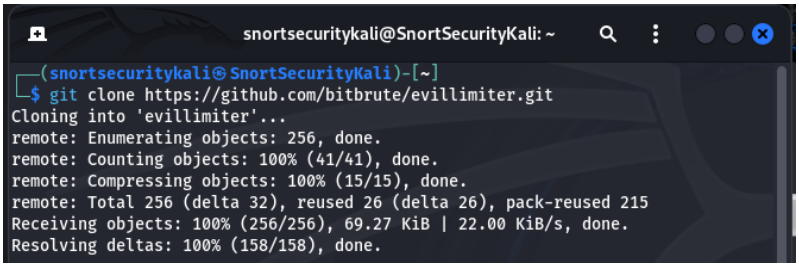
Hasil dan Pembahasan

Langkah-langkah instalasi Evil Limiter di Kali Linux:

1. Pertama, buka VM Kali Linux di *VirtualBox*.

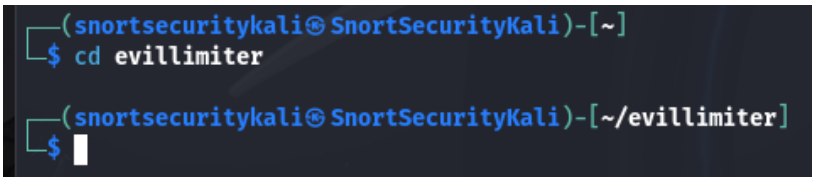
Gambar 1. Virtual Mesin *Kali Linux*

2. Selanjutnya buka terminal dan ketikkan "*git clone* https://github.com/bitbrute/evillimiter.git" untuk mendowload file installasi *Evil Limiter* dari *github*.



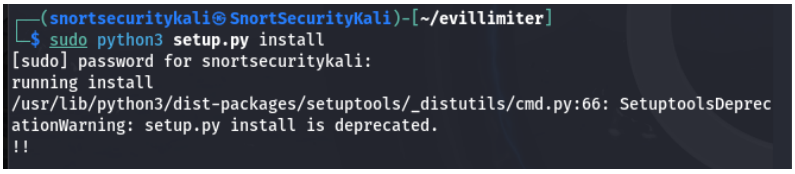
Gambar 2. Download File *Evil Limiter*

3. Ketikkan "*cd evillimiter*" untuk masuk ke *directory evillimiter*.



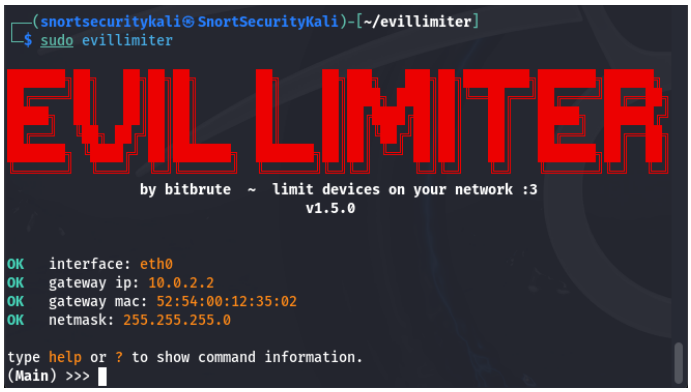
Gambar 3. *Directory Evil Limiter*

4. Ketikkan "*sudo python3 setup.py install*" untuk menginstall *python3*.



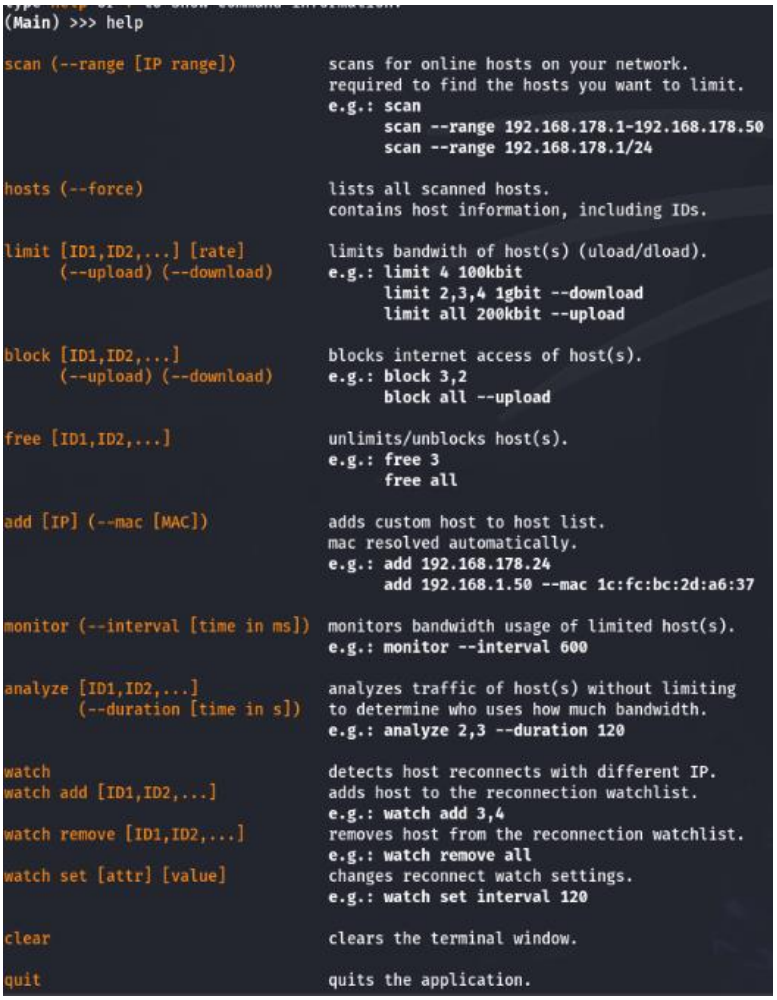
Gambar 4. Setup Python

5. Selanjutnya ketikkan "*sudo evillimiter*" untuk masuk ke *Evil Limiter* yang sudah di install.



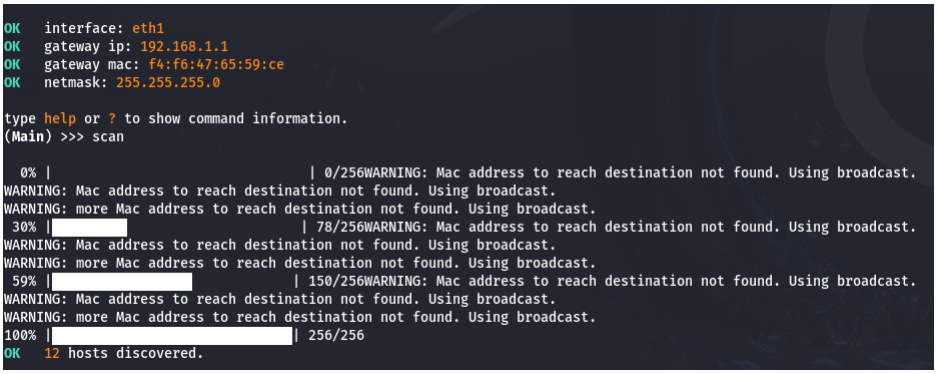
Gambar 5. Jalankan *Evil Limiter*

6. Ketikkan "*help*" untuk melihat command yang bisa digunakan pada *Evil Limiter*.



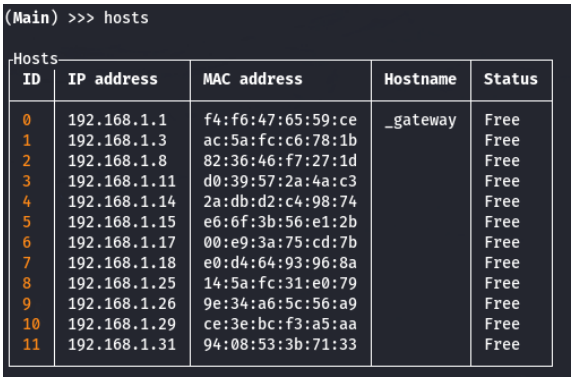
Gambar 6. Command Evil Limiter

7. Ketikkan "*scan*" untuk melakukan *scanning* berapa banyak *host* yang ada di dalam jaringan *Wi-Fi* yang sama dengan *device Evil Limiter*.



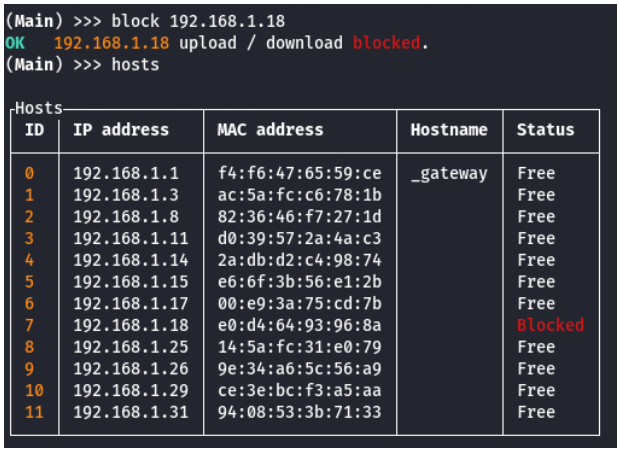
Gambar 7. *Command Scan*

8. Ketikkan "*hosts*" untuk melihat semua *host* beserta IPnya.



Gambar 8. Command Hosts

9. Gunakan *command "block* (IP)" seperti gambar di bawah untuk memblok jaringan *host* dengan IP tersebut.



Gambar 9. *Command Block*

10. Gunakan *command "limit* (IP) *...bit*" untuk membatasi penggunaan *bandwidth* kepada *host* yang dituju.

```
(Main) >>> limit 192.168.1.17 1gbit
OK   192.168.1.17 upload / download limited to 1gbit.
(Main) >>> hosts

Hosts
```

ID	IP address	MAC address	Hostname	Status
0	192.168.1.1	f4:f6:47:65:59:ce	_gateway	Free
1	192.168.1.3	ac:5a:fc:c6:78:1b		Free
2	192.168.1.8	82:36:46:f7:27:1d		Free
3	192.168.1.11	d0:39:57:2a:4a:c3		Free
4	192.168.1.14	2a:db:d2:c4:98:74		Free
5	192.168.1.15	e6:6f:3b:56:e1:2b		Free
6	192.168.1.17	00:e9:3a:75:cd:7b		Limited
7	192.168.1.18	e0:d4:64:93:96:8a		Blocked
8	192.168.1.25	14:5a:fc:31:e0:79		Free
9	192.168.1.26	9e:34:a6:5c:56:a9		Free
10	192.168.1.29	ce:3e:bc:f3:a5:aa		Free
11	192.168.1.31	94:08:53:3b:71:33		Free

Gambar 10. *Command Limit*

11. Gunakan *command "free"* untuk melepaskan blok dan *limit bandwidth* kepada *host*.

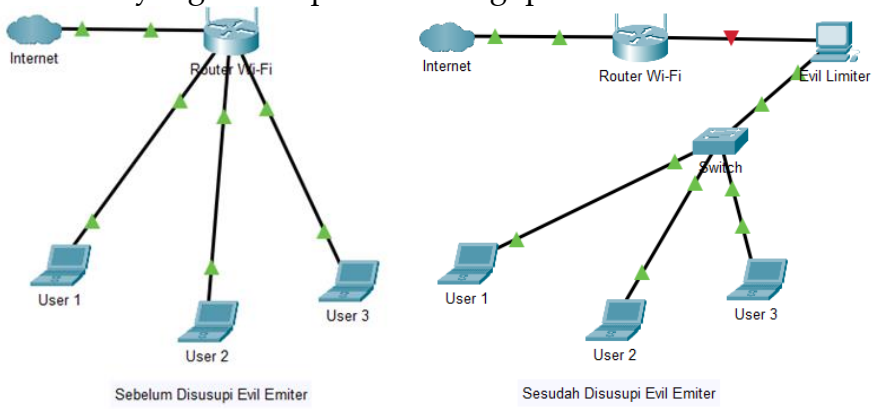
```
(Main) >>> free 192.168.1.17
(Main) >>> free 192.168.1.18
(Main) >>> hosts

Hosts
```

ID	IP address	MAC address	Hostname	Status
0	192.168.1.1	f4:f6:47:65:59:ce	_gateway	Free
1	192.168.1.3	ac:5a:fc:c6:78:1b		Free
2	192.168.1.8	82:36:46:f7:27:1d		Free
3	192.168.1.11	d0:39:57:2a:4a:c3		Free
4	192.168.1.14	2a:db:d2:c4:98:74		Free
5	192.168.1.15	e6:6f:3b:56:e1:2b		Free
6	192.168.1.17	00:e9:3a:75:cd:7b		Free
7	192.168.1.18	e0:d4:64:93:96:8a		Free
8	192.168.1.25	14:5a:fc:31:e0:79		Free
9	192.168.1.26	9e:34:a6:5c:56:a9		Free
10	192.168.1.29	ce:3e:bc:f3:a5:aa		Free
11	192.168.1.31	94:08:53:3b:71:33		Free

Gambar 11. *Command Free*

Di atas sudah dipraktekkan beberapa contoh command yang bisa digunakan pada *Evil Limiter*. Untuk *command* yang lain dapat dilihat lagi pada Gambar 7 *Command Evil Limiter*.



Gambar 12. Skema Jaringan

Gambar di atas merupakan skema jaringan *Wi-Fi* saat sebelum ada *Evil Limiter* dan saat sesudah adanya *Evil Limiter*. Sebelum adanya *Evil Limiter*, jaringan *user* langsung terkoneksi ke *Router Wi-Fi*. Setelah adanya Evil Limiter, jaringan tersebut di manipulasi oleh

Evil Limiter menggunakan teknik ARP *spoofing*, sehingga mengakibatkan koneksi jaringan dari *user* tersebut harus melewati *Evil Limiter* dulu sebelum sampai ke *Router Wi-Fi*. Disinilah *Evil Limiter* bekerja untuk memblok atau melimitasi penggunaan internet dari user lain di satu jaringan *Wi-Fi* yang sama. Dengan menggunakan *command-command* yang ada pada Gambar 7 *Command Evil Limiter*, *user* bisa memanfaatkan semua fitur yang disediakan oleh *Evil Limiter*.

Simpulan

Evil Limiter terbukti efektif dalam mengontrol dan membatasi lalu lintas jaringan *Wi-Fi*. Alat ini dapat memblokir atau membatasi akses internet pada perangkat yang tidak diinginkan, sehingga meningkatkan kontrol terhadap penggunaan jaringan. Penggunaan *Evil Limiter* dapat mempengaruhi kinerja jaringan, terutama dalam hal kecepatan dan latensi. Perangkat yang dibatasi menunjukkan penurunan signifikan dalam kecepatan akses internet.

Meskipun efektif dalam mengontrol lalu lintas, dapat menimbulkan potensi risiko keamanan. Teknik ARP *spoofing* yang digunakan oleh alat ini dapat dimanfaatkan oleh pihak tidak bertanggung jawab untuk melakukan serangan terhadap jaringan. Meskipun demikian, *Evil Limiter* memiliki keterbatasan, termasuk potensi untuk terdeteksi oleh alat deteksi intrusi jaringan (IDS) dan *firewall* yang canggih.

Daftar Pustaka

Andria, A. (2020). Audit Keamanan Website Menggunakan Uniscan di Kali Linux. *Prosiding SEMNAS INOTEK (Seminar …*, 323–328. https://proceeding.unpkediri.ac.id/index.php/inotek/article/view/107

Arief, M. F., Santoso, N. A., & Kurniawan, R. D. (2022). Systematic Literatur Review: Keamanan Komputer Pada Jaringan Nirkabel. *Indonesia Journal of Internasional Relations (IJIR)*, *3*(2), 1–8.

Ariyadi, T., Irham, & Cahyadi, E. F. (2024). Evaluation of Wireless Network Security with Penetration Testing Method at PT PLN UP2D S2JB. *Jurnal Infotel*, *16*(1), 120–135. https://doi.org/10.20895/infotel.v16i1.1057

Asaad, R. R. (2021). *Penetration Testing : Wireless Network Attacks Methods on Kali Linux OS*. *10*(1), 1–6.

Budi, E., Wira, D., & Infantono, A. (2021). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0. *Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia (SENASTINDO)*, *3*(November), 223–234. https://doi.org/10.54706/senastindo.v3.2021.141

Faishol, D. E., Cahyanto, T. A., & Rahman, M. (2024). Analisis Dan Evaluasi Protokol Keamanan Jaringan Nirkabel Wi-Fi Protected Access 3 dengan Metode Penetration Testing. *Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)*, *9*(1), 420–432. https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

Hermawan, R. (2021). Teknik Uji Penetrasi Web Server Menggunakan SQL Injection dengan SQLmap di Kalilinux. *STRING (Satuan Tulisan Riset Dan Inovasi Teknologi)*, *6*(2), 210.

https://doi.org/10.30998/string.v6i2.11477

Hidayah, A. K., Fernandez, S., Prihantoro, C., Marhalim, & Khairullah. (2021). Pelatihan Instalasi Sistem Operasi Linux Deepin di SMKS 9 Muhammadiyah Bengkulu. *Jurnal Pengabdian Masyarakat Teknologi Terbarukan*, *1*(2), 49–54.

Kurniawan, R. W. (2020). *Rancang Bangun Simulasi Data Center Dengan Kemampuan Disaster Recovery Menggunakan Virtual Machine*. 7–48. https://elibrary.unikom.ac.id/id/eprint/2709/%0Ahttps://elibrary.unikom.ac.id/id/eprint/2709/8/12.10115593_RAMA WAHYU KURNIAWAN_BAB 2.pdf.pdf

Lynn, T., Rosati, P., Conway, E., Curran, D., Fox, G., & O'Gorman, C. (2022). Infrastructure For Digital Connectivity. *Digital Towns*, *Chapter 6*(February), 109–132. https://doi.org/10.1007/978-3-030-91247-5

Morsy, S. M., & Nashat, D. (2022). D-ARP: An Efficient Scheme to Detect and Prevent ARP Spoofing. *IEEE Access*, *10*, 49142–49153. https://doi.org/10.1109/ACCESS.2022.3172329

Mumcu, F., Doshi, K., & Yilmaz, Y. (2022). Adversarial Machine Learning Attacks Against Video Anomaly Detection Systems. *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, *2022-June*, 206–213. https://doi.org/10.1109/CVPRW56347.2022.00034

Pradana, E. A., Putry, A. A., & Mursidayanti, S. (2023). Rancang Bangun Media Praktikum Mata Kuliah Sistem Operasi Dengan Kernel Virtual Machine Server Terintegrasi Dengan Sistem Akademik. *Indo-MathEdu Intellectuals Journal*, *4*(2), 1237–1248. https://doi.org/10.54373/imeij.v4i2.273

Prihantoro, C., Hidayah, A. K., & Fernandez, S. (2021). Analisis Manajemen Bandwidth Menggunakan Metode Queue Tree pada Jaringan Internet Universitas Muhammadiyah Bengkulu. *Just TI (Jurnal Sains Terapan Teknologi Informasi)*, *13*(2), 81–86. https://doi.org/10.46964/justti.v13i2.750

Raji, I. A., Bugaje, I. B., & Usman, S. (2022). The International Journal of Business and. *International Journal of Business and Management Research*, *13*(1).

Roberto, C., Muriani, & Kolyaan, Y. (2017). Interworking Wimax dan WIfi. *Jurnal Teknologi Informasi*, *5*(2), 38–50. http://ojs.ustj.ac.id/jti/article/view/231/162

Rustam, M. (2017). Internet dan Penggunaannya (Survei di kalangan masyarakat Kabupaten Takalar Provinsi Sulawesi Selatan). *Jurnal Studi Komunikasi Dan Media*, *21*(1), 13–24. https://doi.org/10.31445/jskm.2017.210102

Sandhiyadini Rosari, H., Syaibani Al Hakim, M., Sibagariang, E., Rosadi Kardian, A., & Siber dan Sandi Negara, P. (2022). Analisis Kecepatan MySQL dan PostgreSQL pada Windows 11 dan Kali Linux 2022. *Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)*, *8*(1), 213–222. https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

Santoso, N. A., Maulidin, Z., & Kurniawan, R. D. (2022). Analisis Jaringan Komputer Menggunakan Teknologi Virtualisasi. *Jurnal Minfo Polgan*, *11*(2), 52–60. https://doi.org/10.33395/jmp.v11i2.11652

Utami, P. R. (2020). *Analisis Perbandingan Quality Of Service Jaringan Internet Berbasis Wireless Pada Layanan Internet Service Provider (ISP) Indihome dan First Media*. *25*(2), 125–137.

Wahib, P., Narotama, A. T., Rijki, N. M., Sahrudin, Permana, F., Sagara, D., Azkhal, D. I.,

Anwar, M., & Juniawan, M. R. (2022). Sosialisasi Cyber Security Untuk Meningkatkan Literasi Digital. *Ajp-Abdi Jurnal Publikasi*, *1*(2), 64–68. https://jurnal.portalpublikasi.id/index.php/AJP/index

Yunianto, I., & Adhiyarta, K. (2020). Jurnal Review: Perbandingan Sistem Operasi Linux Dengan Sistem Operasi Windows. *JUPITER : Journal of Computer & Information Technology*, *1*(1), 1–7. https://doi.org/10.53990/jupiter.v1i1.3