Neptunus: Jurnal Ilmu Komputer Dan Teknologi Informasi
Volume.3, Nomor.1 Tahun 2025
e-ISSN: 3031-898X; p-ISSN: 3031-8998, Hal 31-40
DOI: https://doi.org/10.61132/neptunus.v2i4.590
Available online at: https://journal.arteii.or.id/index.php/Neptunus

Evaluasi Keamanan Autentikasi Pengguna pada Sistem Operasi Windows dan Linux

Galva Al Godzali[1*], Rafif Isdarufa Athallah[2], Elkin Rivalni[3]
[1,2,3] Universitas Pelita Bangsa, Indonesia

Jl. Inspeksi Kalimalang Tegal Danas Arah Deltamas, Cibatu, Cikarang
Korespondensi penulis: galvaalghazali@gmail.com

Abstract. *Authentication security is an important aspect of the operating system. This research evaluates the security of user authentication on Windows and Linux operating systems by analyzing various methods such as the use of passwords and two-factor authentication. This study compares effectiveness, flexibility, and stability to provide insight into their advantages and vulnerabilities. The literature review method is used by utilizing secondary data from relevant sources. The research results show that Linux offers superior security due to its open-source nature and strong permission-based model, while Windows excels in ease of use and integrated features such as Active Directory. These results aim to provide information to users and organizations in choosing an operating system that suits their needs*.

Keywords: *Authentication, Linux, Windows, Security, Operating Systems*

Abstrak. Keamanan autentikasi merupakan salah satu aspek penting dalam sistem operasi. Penelitian ini mengevaluasi keamanan autentikasi pengguna pada sistem operasi Windows dan Linux dengan menganalisis berbagai metode seperti penggunaan kata sandi dan autentikasi dua faktor. Studi ini membandingkan efektivitas, fleksibilitas, dan stabilitas untuk memberikan wawasan tentang keunggulan dan kerentanannya. Metode tinjauan pustaka digunakan dengan memanfaatkan data sekunder dari sumber relevan. Hasil penelitian menunjukkan bahwa Linux menawarkan keamanan lebih unggul karena sifat *open-source* dan model berbasis izin yang kuat, sementara Windows unggul dalam kemudahan penggunaan dan fitur terintegrasi seperti *Active Directory*. Hasil ini bertujuan untuk memberikan informasi kepada pengguna dan organisasi dalam memilih sistem operasi yang sesuai dengan kebutuhan.

Kata kunci: Autentikasi, Linux, Windows, Keamanan, Sistem Operasi

1. LATAR BELAKANG

Sistem operasi adalah perangkat lunak utama dalam komputer dengan fungsi sebagai pengelola sumber daya perangkat keras dan perangkat lunak lainnya. Dalam sistem operasi terdapat komponen-komponen untuk menjalankan tugas yang penting seperti manajemen proses, file, memori utama, I/O, penyimpanan sekunder, sistem jaringan, sistem command interpreter, dan sistem proteksi. Sistem operasi yang populer saat ini adalah Windows dan Linux. Keduanya adalah sistem operasi dengan pendekatan yang berbeda, masing-masing menawarkan keunggulan dalam aspek-aspek seperti autentikasi pengguna. Windows mengadopsi pendekatan terpusat dengan menggunakan *Active Directory*, sedangkan Linux lebih modular dan desentralistik dengan sistem izin berbasisfile dan kemampuan kustomisasi yang tinggi (Imam, Krisna, 2020). Perbedaan ini pengaruhi cara kedua sistem dalam mengimplementasikan autentikasi dan merespons ancaman keamanan.

Salah satu aspek krusial dalam keamanan sistem operasi adalah autentikasi

Received: November 30, 2024; Revised: Desember 10, 2024; Accepted: Desember 22, 2024; Published: Desember 24, 2024

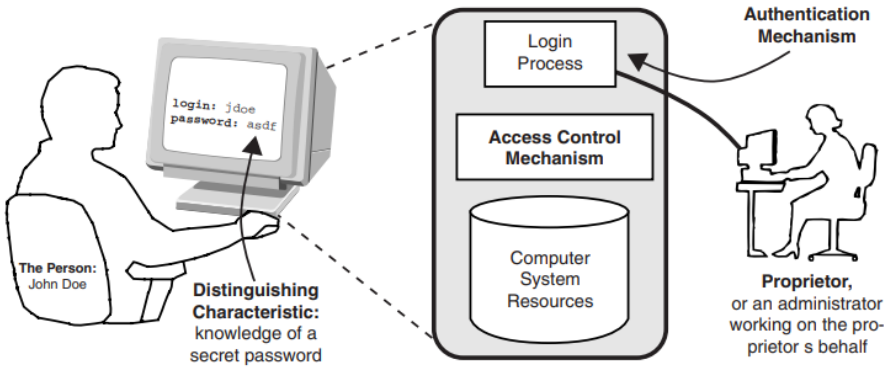
pengguna (Miclea, 2012). Meskipun kadang disepelekan, proses autentikasi memainkan peran penting dalam memastikan bahwa hanya pengguna yang sah yang dapat mengakses sistem dan datanya. Autentikasi juga penting karena pada prakteknya autentikasi memiliki backup dengan fungsi untuk menjaga kemungkinan jika server ada masalah serta mengenali pengguna yang berintegerasi ke dalam jaringan dan memuat semua informasi dari sang pengguna (Armin, Ali, Erick, 2017). Pada Windows, tidak memiliki modularitas yang berati jika salah satu sitem komponen gagal maka keseluruhan OS bisa gagal, sebaliknya pada Linux memberi pengguna akses terbatas karena tidak memberikan root secera *default* (Albatli, 2023). Batasan penelitian ini difokuskan pada dua sistem operasi, yaitu Windows 10 dan Windows 11 untuk sistem Windows, serta distribusi Linux berbasis Ubuntu LTS (*Long Term Support*). Maka dari itu timbulah pertanyaan penelitian untuk memyelesaikan masalah diatas bagaimana metode keamanan autentikasi pengguna dimasing-masing sistem operasi?

Penelitian ini bertujuan untuk mengevaluasi efektifitas kedua sistem degan mengkaji berbagai metode autentikasi, Seperti penggunaan kata sandi, autentikasi 2 faktor, serta melihat tinjauan evaluasi autentikasi kedua OS. Manfaat dari penelitian ini adalah untuk mengevaluasi keamanan sistem pengguna dalam memahami potensi kerentanan mekanisme autentikasi pada Windows dan Linux. Penelitian serupa mengungkapkan bahwa kedua sistem operasi menggunakan algoritma proteksi yang berbeda untuk meningkatkan keamanan data dan akses pengguna, meskipun masing-masing memiliki kelebihan dan kekurangan yang signifikan (Josephine, Sayidina, & Siahaan, 2023).

2. METODE PENELITIAN

Pendekatan Penelitian

Pendekatan penelitian yang digunakan adalah studi literatur dengan mengumpulkan berbagai informasi dari berbagai sumber yang relevan. Penelitian ini menganalisis sistem keamanan autentikasi operating system melalui pengumpulan dan analisis data dari sumber sekunder seperti buku yang ditulis oleh Smith, R. E. (2019). Authentication: From Passwords to Public Keys. O'Reilly Media.



Gambar 1. Elemen-elemen dalam sistem autentikasi

Didalam gambar 1 dari elemen sebuah sistem autentikasi yang mencakup:

1. *The person* (Subjek Autentikasi): Seseorang yang mencoba mengakses suatu sistem. John Doe adalah pengguna yang mencoba memasuki sistem dengan memberikan informasi autentikasi, seperti yang ditunjukkan pada gambar.
2. *Distinguishing Charateristic*, juga dikenal sebagai "Karakteristik Pembeda": merujuk pada sesuatu yang diketahui, dimiliki, atau ditanamkan pada pengguna untuk membuatnya berbeda dari orang lain. Gambar menunjukkan bahwa pengguna mengetahui password rahasia sebagai komponen autentikasi.
3. *Authentication Mecanism* adalah proses atau alat yang digunakan untuk memastikan bahwa pengguna adalah pihak yang sah. Dalam hal ini, mekanisme autentikasi melibatkan proses login untuk memvalidasi kredensial pengguna.
4. *Acces Control Mecanism* (Mekanisme Kontrol Akses): mekanisme ini mengidentifikasi identitas pengguna dan menentukan sumber daya sistem mana yang dapat diakses oleh pengguna berdasarkan hak atau izin yang dimiliki.
5. *Proprietor:* Pemilik sistem atau administrator yang bertanggung jawab untuk mengatur akses dan melindungi sumber daya sistem.

Data Penelitian

Data sekunder merupakan data yang telah dikumpulkan atau telah dipublikasikan oleh pihak lain (Sugiono 2018). Data yang diambil dalam oleh penulis adalah jenis data yang telah terkumpul dianalisis secara deskriptif untuk mengevaluiasi perbandingan keamanan Autentikasi antara sistem operasi Windows dan Linux.

Data sekunder diperoleh melalui penelitian literatur, yaitu buku yang mencari teori yang relevan dan jurnal ilmiah yang mempelajari penelitian tentang Sistem keamanan autentikasi Windows dan Linux. Sumber data sekunder lainnya untuk penelitian ini adalah majalah dan internet, yaitu jurnal online dan berita tentang perbadingan keamanan antar sistem operasi Windows dan Linux

3. HASIL DAN PEMBAHASAN

Penelitian yang dilakukan ini menggunkan data sekunder yang relevan untuk mendukung hasil analisa yang dilakukan mengenai autentiaksi pada Windows dan Linux serta melihat keunggulan dan kelemahan kedua OS tersebut. Sebelum membahas lebih jauh, metode autentikasi dibagi menjadi 4 kategori (Pramartha, 2013):

1. *Something you know*

Ini adalah metode autentikasi yang paling umum, yang mengandalkan kerahasiaan informasi seperti password dan PIN. Ini berasumsi bahwa hanya Anda yang mengetahui rahasia itu.

2. *Something you have*

Metode ini biasanya merupakan komponen tambahan yang membuat autentikasi lebih aman. Metode ini bergantung pada produk yang unik, seperti token hardware, token USB, kartu magnetic, dan smartcard. Metode ini menganggap bahwa Anda adalah satu-satunya orang yang memiliki barang tersebut.

3. *Something you are*

Pendekatan yang paling jarang digunakan karena faktor manusia dan teknologi. Metode ini menganggap bahwa bagian tubuh anda seperti sidik jari dan sidik retina tidak mungkin sama dengan orang lain karena tidak mungkin ada pada orang lain.

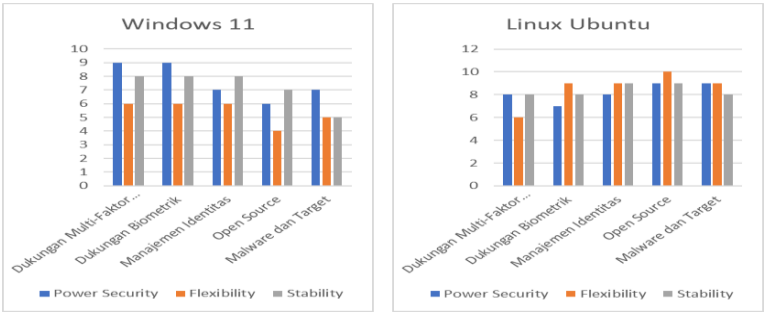
4. *Something you do*

Bahwa setiap pengguna melakukan sesuatu dengan cara yang berbeda. Contohnya adalah penggunaan analisis tulisan tangan dan analisis suara. Password adalah cara yang paling umum untuk melakukan autentikasi.

Mengacu pada teori yang diberikan oleh Albatli (2023) yang mengungkapkan bahwa Pengoperasian OS Windows dan Linux menunjukkan bahwa sistem keamanan Linux lebih aman jika dibandingkan dengan sistem keamanan Windows karena fitur keamanan canggihnya karena, fakta bahwa sistem Linux adalah sistem *Open Source* dengan indikasi jangkauan yang lebih luas memungkinkan penggunakanya mengakses kode sumber selain itu juga windows merupakan OS yang mendominasi pasar dunia yang menjadikanya target menarik bagi para *hacker*.

Tabel 1 Analisis Aspek Keamanan Autentikasi

No.	Aspek keamanan autentikasi	Windows	Linux	Keterangan
1.	Dukungan Multi-Faktor Autentikasi (MFA)	Mendukung secara bawaan melalui Windows Hello dan integrasi Active Directory.	Tergantung pada distribusi; biasanya memerlukan konfigurasi tambahan atau alat pihak ketiga	Windows menawarkan solusi bawaan untuk MFA, sementara Linux lebih fleksibel tetapi membutuhkan usaha lebih
2.	Dukungan Biometrik	Mendukung biometrik bawaan melalui Windows Hello (sidik jari, pengenalan wajah).	Dukungan biometrik memerlukan pengaturan dan perangkat lunak pihak ketiga.	Windows memiliki dukungan biometrik bawaan, menjadikannya lebih mudah digunakan.
3.	Manajemen Identitas	Active Directory menawarkan manajemen pengguna terpusat dengan autentikasi terintegrasi.	LDAP digunakan untuk manajemen identitas, tetapi konfigurasi manual sering diperlukan.	Windows memiliki pendekatan terpusat dan lebih mudah digunakan untuk organisasi besar.
4.	Open Source	*Proprietary*, hanya Microsoft yang dapat memeriksa dan memperbaiki kode sumbernya.	Kode sumber terbuka, memungkinkan audit keamanan oleh komunitas global.	Linux memiliki sifat yang terbuka dan transparan sedangkan windows lebih tertutup
5.	Malware dan Target	Pangsa pasar besar Windows membuatnya menjadi target utama malware, sering kali melalui perangkat lunak dari sumber tak terpercaya.	arena pangsa pasar desktop kecil dan repositori aplikasi yang diverifikasi, Linux jarang menjadi target malware.	Jangkauan pasar yang luas menjadikan windows target utama serangan malware dibanding linux yang memiliki jangkuan lebih kecil



Gambar 2. Grafik perbandingan nilai keamanan autentikasi.

Perbedaan nilai autentikasi dalam konteks dengan dukungan multi-faktor (MFA) pada Windows 11 dan Linux Ubuntu bedasarkan aspek *Power Security*, *Flexibility* dan *Stability*.

- Linux membutuhkan alat pihak ketiga yang aman, tetapi memerlukan konfigurasi. Windows memiliki solusi multi-factor authentication (MFA) bawaan yang aman, seperti Windows Hello dan Active Directory, dan dukungan perangkat keras seperti TPM.
- Sementara Windows hanya mendukung metode tertentu secara bawaan, Linux lebih fleksibel karena dapat menggunakan berbagai metode MFA sesuai kebutuhan.
- Meskipun keduanya stabil, Windows bekerja lebih baik dengan beberapa perangkat keras, sementara Linux stabil di banyak platform setelah dikonfigurasi dengan benar.

Meskipun Linux Ubuntu lebih mudah untuk menerapkan MFA, Windows 11 unggul dalam keamanan daya karena solusi MFA bawaan yang lebih mudah digunakan.

Perbedaan nilai autentikasi dalam konteks dukungan biometrik pada Windows 11 dan Linux ubuntu bedasarkan aspek *Power Security*, *Flexibility* dan *Stability*.

- Windows 11 menyertakan keamanan perangkat keras seperti TPM dan dukungan biometrik melalui Windows Hello (sidik jari dan pengenalan wajah), tetapi Linux membutuhkan perangkat lunak tambahan yang dapat menimbilkan potensi masalah.
- Linux lebih fleksibel karena memungkinkan integrasi berbagai perangkat dan protokol biometrik, tetapi Windows memiliki pilihan sistem bawaan yang terbatas.
- Kedua sistem mendukung biometrik dengan baik, tetapi Linux sangat bergantung pada kompatibilitas driver, sementara Windows lebih mudah diintegrasikan.

Karena sifat *open source*-nya, Linux Ubuntu menawarkan fleksibilitas lebih yang memungkinkan integrasi dengan berbagai perangkat biometrik. Di sisi lain, Windows 11 memiliki keunggulan dalam keamanan berkat solusi biometrik bawaan yang aman dan mudah digunakan.

Perbedaan nilai autentikasi dalam konteks manajemen identitas pada Windows 11 dan Linux ubuntu bedasarkan aspek *Power Security*, *Flexibility* dan *Stability*.

- Windows 11 menggunakan *Active Directory* (AD) yang sangat kuat untuk manajemen identitas dan mendukung integrasi dengan berbagai protokol keamanan kontemporer. Linux menggunakan LDAP, yang juga aman tetapi membutuhkan konfigurasi manual yang sulit.
- Windows memiliki pendekatan yang lebih terpusat tetapi kurang fleksibel, sehingga Linux lebih fleksibel untuk manajemen identitas karena mendukung berbagai solusi *open source* dan kustomisasi.

- Kedua sistem manajemen identitas stabil. Sementara *Active Directory* Windows sangat andal, Linux dikenal sangat stabil dalam lingkungan server dan jaringan.

Linux Ubuntu lebih stabil dan fleksibel daripada Linux lainnya karena sifat open sourcenya dan kemampuan untuk disesuaikan dengan berbagai jenis organisasi. Tetapi Windows 11 memiliki pertahanan daya yang lebih baik berkat pendekatan terpusat dan fitur bawaan seperti *Active Directory*.

Perbedaan nilai autentikasi dalam konteks Open Source pada Windows 11 dan Linux ubuntu bedasarkan aspek *Power Security*, *Flexibility* dan *Stability*.

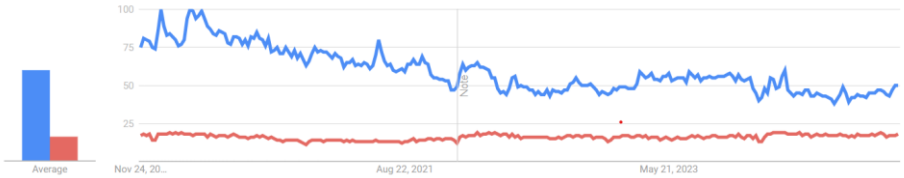
- Sebagai *open source*, Linux memungkinkan audit keamanan oleh komunitas global, meningkatkan transparansi, dan deteksi kerentanan. Sebaliknya, Windows bersifat *proprietary*, sehingga hanya Microsoft yang dapat memeriksa dan memperbaiki kode sumbernya.
- Linux sangat mudah beradaptasi karena bersifat *open source*, memungkinkan pengguna untuk mengubah dan mempersonalisasi sistem sesuai kebutuhan. Namun, Windows tidak memiliki kebebasan ini karena kode sumbernya yang terbatas.
- Linux stabil dalam banyak implementasi *open source*, baik server maupun desktop. Windows juga stabil, tetapi perbaikannya bergantung pada siklus pembaruan Microsoft.

Karena transparansinya, fleksibilitasnya, dan stabilitasnya yang tinggi, Linux Ubuntu unggul secara signifikan dalam hal open source. Sebaliknya, Windows 11, sebagai perangkat lunak proprietary, memiliki keterbatasan dalam fleksibilitas dan transparansi dibandingkan dengan Linux.

Perbedaan nilai autentikasi dalam konteks serangan malware pada Windows 11 dan Linux ubuntu bedasarkan aspek *Power Security*, *Flexibility* dan *Stability*.

- Karena pangsa pasarnya yang besar, Windows 11 memiliki fitur keamanan bawaan seperti Windows Defender dan sandboxing, tetapi lebih sering menjadi target malware. Dengan repositori aplikasi terpercaya dan kontrol akses yang ketat, Linux secara default lebih aman.
- Sementara Windows memiliki keterbatasan dalam hal ini, Linux memungkinkan pengguna untuk memodifikasi sistem untuk meningkatkan keamanan terhadap malware.
- Karena arsitektur berbasis izinnya yang ketat, Linux lebih tahan terhadap serangan malware, sementara Windows lebih rentan terhadap crash atau penurunan kinerja saat menghadapi serangan malware yang signifikan.

Karena sistemnya yang lebih fleksibel, transparan, dan memiliki arsitektur keamanan yang kuat, Linux Ubuntu unggul dalam hal perlindungan malware. Karena pangsa pasar yang besar dan pendekatan yang kurang fleksibel, Windows 11 lebih sering menjadi sasaran serangan meskipun memiliki perlindungan bawaan yang baik.



Gambar 3. Grafik data pengguna Windows (biru) dan Linux (merah)

Teori yang dibuat oleh Albatli (2023) tentang OS linux lebih baik dibanding dengan Windows memang benar adanya, karena analisis menujukan bahwa OS Linux lebih unggul dalam bidang *password*, *effectiveness*, *flexibility* dan *stability* meski begitu data yang ditunjukan pada *wolrdwide* menunjukan bawasanya sistem operasi Windows masih sangat unggul dalam 5 tahun terakhir yang menjadi alasan utamanya karena OS Windows sangat mudah digunakan.

4. KESIMPULAN DAN SARAN

Sistem operasi Windows dan Linux memiliki pendekatan yang berbeda dalam implementasi keamanan autentikasi pengguna. Evaluasi menunjukkan bahwa Linux lebih unggul dalam hal transparansi kode sumber dan fleksibilitas konfigurasi, yang memungkinkan penyesuaian keamanan secara lebih mendalam. Sebaliknya, Windows menawarkan solusi bawaan yang lebih mudah digunakan, seperti autentikasi biometrik dan manajemen identitas terpusat melalui *Active Directory*, yang cocok untuk kebutuhan organisasi besar. Namun, karena dominasi pasar, Windows lebih rentan terhadap serangan malware dibandingkan Linux. Keamanan Linux cenderung lebih stabil dan andal untuk server, terutama dengan dukungan metode 2FA berbasis alat pihak ketiga.

Keterbatasan penelitian ini terletak pada pendekatan studi literatur yang bergantung pada data sekunder, sehingga pengujian langsung terhadap kedua sistem operasi tidak dilakukan. Untuk penelitian mendatang, disarankan agar dilakukan uji coba dengan pengukuran kinerja dan analisis risiko lebih mendalam guna memperkuat hasil yang ada. Selain itu, penelitian lanjutan dapat mengeksplorasi dampak pengembangan teknologi baru terhadap keamanan kedua sistem operasi ini.

5. DAFTAR REFERENSI

Alassaf, A. S. (2023). Linux OS versus Windows OS security. *International Journal of Multidisciplinary Innovation and Research Methodology, 2*(3), 1–7.

Armin, A., Abrar, A., & Sorongan, E. (2017). Sentralisasi otentikasi pengguna dan pengelolaan sumber daya jaringan komputer Politeknik Negeri Balikpapan dengan menggunakan Active Directory Domain Services Windows Server 2012 R2. *Prosiding SNITT Poltekba, 2*(1), 326–332.

Asti, R. M., Laila, E., & Firdaus, A. (2021). Manajemen dan autentikasi hotspot menggunakan Remote Access Dial-In User Service (RADIUS) Server pada Jurusan Teknik Komputer. *Jurnal Laporan Akhir Teknik Komputer, 1*(2), 52–59.

Awan, M. T., & Khan, K. (2022). Linux vs. Windows: A comparison of two widely used platforms. *Journal of Computer Science and Technology Studies, 4*(1), 41–53.

Bassil, Y. (2012). Windows and Linux operating systems from a security perspective. *arXiv preprint arXiv:1204.0197*.

Bator, R. J., Bryan, A. D., & Schultz, P. W. (2011). Who gives a hoot?: Intercept surveys of litterers and disposers. *Environment and Behavior, 43*(3), 295–315. https://doi.org/10.1177/0013916509356884

Darmadi, E. A. (2018). Perancangan sistem otentikasi radius pada pengguna jaringan wireless untuk meningkatkan keamanan jaringan komputer. *IKRA-ITH Informatika: Jurnal Komputer dan Informatika, 2*(3), 9–16.

Duncan, R., & Schreuders, Z. C. (2019). Security implications of running Windows software on a Linux system using Wine: A malware analysis study. *Journal of Computer Virology and Hacking Techniques, 15*, 39–60.

Hidayati, S. N. (2016). Pengaruh pendekatan keras dan lunak pemimpin organisasi terhadap kepuasan kerja dan potensi mogok kerja karyawan. *Jurnal Maksipreneur: Manajemen, Koperasi, dan Entrepreneurship, 5*(2), 57–66. http://dx.doi.org/10.30588/SOSHUMDIK.v5i2.164

Josephine, T. S. S., & Siahaan, P. (2023). Analisis sistem keamanan dan proteksi pada sistem operasi Windows, Linux, dan MacOS. *Sistem Dan Teknologi Informasi Indonesia (SINTESIA), 2*(2), 64–70. Retrieved from https://journal.unj.ac.id/unj/index.php/SINTESIA/article/view/44081

Kemas, K. O. K. S., Supriyatna, A. R., & Putra, S. D. (2024). Autentikasi user dengan metode single sign-on berbasis Windows Active Directory pada PT. XYZ. *ROUTERS: Jurnal Sistem dan Teknologi Informasi*, 70–78.

Miclea, S. (2012). Windows and Linux security audit. *Journal of Applied Business Information Systems, 3*(4). Retrieved from http://www.jabis.ro/2012/4/0304012012.pdf

Motero, C. D., Higuera, J. R. B., Higuera, J. B., Montalvo, J. A. S., & Gómez, N. G. (2021). On attacking Kerberos authentication protocol in Windows Active Directory Services: A practical survey. *IEEE Access, 9*, 109289–109319.

Nelfira, N. (2017). Rancang bangun aplikasi pembelajaran sistem operasi Windows pada matakuliah sistem operasi di STMIK Indonesia Padang berbasis multimedia interaktif. *Jurnal Edik Informatika Penelitian Bidang Komputer Sains dan Pendidikan Informatika*, *2*(2), 182–189.

Risdwiyanto, A., & Kurniyati, Y. (2015). Strategi pemasaran perguruan tinggi swasta di Kabupaten Sleman Yogyakarta berbasis rangsangan pemasaran. *Jurnal Maksipreneur: Manajemen, Koperasi, dan Entrepreneurship, 5*(1), 1–23. http://dx.doi.org/10.30588/SOSHUMDIK.v5i1.142

Smith, R. E. (2002). *Authentication: From passwords to public keys*. Addison-Wesley Professional.

Yudhana, A., & Riadi, I. (2022). Analisis kinerja perangkat lunak forensic imaging pada sistem operasi Linux menggunakan metode static forensic. *Insect (Informatics and Security): Jurnal Teknik Informatika, 8*(1), 38–47.

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.