

**KATA PENGANTAR**

Puji syukur kami panjatkan kehadirat Allah SWT yang telah memberikan rahmat dan karunia kepada kami sehinnga dapat menyelesaikan makalah yang berjudul “Keamanan Sistem Operasi”. Kami menyadari bahwa masih banyak kekurangan dalam makalah ini, baik dari segi isi maupun penulisan. Oleh karena itu, kami mengharapkan kritik dan saran yang membangun dari pembaca demi penyempurnaan makalah ini.

Pada kesempatan ini kami mengucapkan terima kasih kepada dosen pengampu mata kuliah keamanan komputer Bapak Muhammad Jefri, S.Pd., M.Pd. Para pembaca, dan pihak-pihak lain yang membantu demi selesainya makalah ini.

Demikian makalah ini kami buat, semoga dapat bermanfaat bagi pembaca.

Selayar, 17 November 2024

Kelompok 6

**DAFTAR ISI**

[KATA PENGANTAR ii](file:///C:\Users\LENOVO\Documents\LAPORAN%20jaringan%20komputer.docx#_Toc180347483)

[DAFTAR ISI iii](file:///C:\Users\LENOVO\Documents\LAPORAN%20jaringan%20komputer.docx#_Toc180347484)

[BAB I PENDAHULUAN 1](file:///C:\Users\LENOVO\Documents\LAPORAN%20jaringan%20komputer.docx#_Toc180347485)

[A. Latar Belakang](file:///C:\Users\LENOVO\Documents\LAPORAN%20jaringan%20komputer.docx#_Toc180347486) 1

[B. Rumusan Masalah](file:///C:\Users\LENOVO\Documents\LAPORAN%20jaringan%20komputer.docx#_Toc180347487) 1

[C. Tujuan](file:///C:\Users\LENOVO\Documents\LAPORAN%20jaringan%20komputer.docx#_Toc180347488) 2

[BAB II PEMBAHASAN](file:///C:\Users\LENOVO\Documents\LAPORAN%20jaringan%20komputer.docx#_Toc180347489) 3

[A. Pengertian Sistem Operasi](file:///C:\Users\LENOVO\Documents\LAPORAN%20jaringan%20komputer.docx#_Toc180347490) 3

[B. Fitur-Fitur Keamanan Sistem Operasi](file:///C:\Users\LENOVO\Documents\LAPORAN%20jaringan%20komputer.docx#_Toc180347491) 4

[C. Jenis-Jenis Ancaman terhadap Keamanan Sistem Operasi](file:///C:\Users\LENOVO\Documents\LAPORAN%20jaringan%20komputer.docx#_Toc180347492) 7

[D. Manfaat Keamanan Sistem Operasi bagi Pengguna dan Organisasi](file:///C:\Users\LENOVO\Documents\LAPORAN%20jaringan%20komputer.docx#_Toc180347493) 8

[BAB III PENUTUP](file:///C:\Users\LENOVO\Documents\LAPORAN%20jaringan%20komputer.docx#_Toc180347501) 10

[A. Kesimpulan](file:///C:\Users\LENOVO\Documents\LAPORAN%20jaringan%20komputer.docx#_Toc180347502) 10

[B. Saran](file:///C:\Users\LENOVO\Documents\LAPORAN%20jaringan%20komputer.docx#_Toc180347503) 10

[DAFTAR PUSTAKA 11](file:///C:\Users\LENOVO\Documents\LAPORAN%20jaringan%20komputer.docx#_Toc180347504)

**BAB 1**

**PENDAHULUAN**

1. **LATAR BELAKANG**

Peningkatan globalisasi pada masa kini telah mendorong perkembangan teknologi menjadi semakin canggih pula. Dengan pesatnya perkembangan teknologi, keamanan sistem menjadi isu yang sangat penting, termasuk informasi keamanan fisik, keamanan data, dan keamanan aplikasi. Mencapai keamanan yang sempurna dianggap sulit, oleh karena itu, langkah yang dapat diambil adalah dengan meningkatkan sistem keamanan untuk mengurangi gangguan.

Salah satu sistem keamanan yang umum diketahui adalah pemberian kata sandi (password). Penggunaan password dapat menyediakan perlindungan bagi data-data yang bersifat pribadi (rahasia). Namun, banyak pengguna membuat kata sandi dengan sembrono tanpa memahami kebijakan keamanan kata sandi dan petunjuk untuk membuat kata sandi yang kuat. Mereka belum menyadari bahwa password yang mereka buat bisa diambil oleh orang-orang yang tidak bertanggungjawab. Maka penting untuk mengetahui tentang kebijakan keamanan sistem operasi di perangkat komputer.

1. **RUMUSAN MASALAH**
2. Apa yang dimaksud keamanan sistem operasi?
3. Apa saja fitur-fitur pada keamanan sistem operasi?
4. Apa saja ancaman terhadap keamanan sistem operasi?
5. Apa manfaat keamanan sistem operasi bagi pengguna dan organisasi?
6. **TUJUAN**
7. Mengetahui apa itu keamanan sistem operasi
8. Mengetahui apa saja fitur-fitur pada kemananan sistem operasi
9. Mengetahui jenis ancaman terhadap keamanan sistem operasi
10. Mengetahui manfaat dari keamanan sistem operasi

**BAB II**

**PEMBAHASAN**

1. **Pengertian Sistem Operasi**

Sistem operasi adalah perangkat lunak yang menghubungkan pengguna dan kompuer ke perangkat keras komputer. Sistem operasi merupakan program yang megelola perangkat keras komputer, memberikan landasan bagi aplikasi yang berjalan di dalamnya, dan bertindak sebagai perantara antara pengguna perangkat keras tersebut. Menurut fery Indayudha, sistem operasi merupakan sistem penting yang diperlukan untuk menjalankan program dan perangkat lunak pada komputer.

Sistem operasi bertanggungjawab untuk mengendalikan dan mengelola penggunaan perangkat keras dari berbagai program aplikasi yang digunakan oleh pengguna berbeda. Komponen utama suatu sistem komputer pada dasarnya meliputi perangkat keras, program aplikasi, sistem operasi, dan pengguna. Sisstem operasi mengelola dan memonitor semua perintah pengguna.

Tujuan dari sistem operasi adalah untuk mengatur keadaan komputer agar dapat diterapkan secara tepat sesuai keinginan pengguna. Saat menggunakan komputer, masalah perbedaan sumber daya yang sama biasanya muncul. Kehadiran sistem operasi memungkinkan pengguna dapat mengatur akses antar pengguna. Sistem operasi juga bertindak sebagai sistem kontrol yang bertujuan untuk memperbaiki kesalahan, agar program dapat berjalan dengan baik. Untuk menghindari konflik ketika pengguna menggunakan sumber daya yang sama, sistem operasi mengatur akses pengguna yang mempunyai hak untuk menggunakan sumber daya tersebut. Sistem operasi sering disebut sebagai manajer sumber daya. Fitur lain yang sangat penting dari sistem operasi adalah kemampuan program kontrol yang bertujuan mencegah kesalahan. Sehinnga dapat disimpulkan bahwa sistem opersi merupakan bagian yang sangat penting pada komputer yang mengontrol akses kerja antara pengguna dan perangkat keras komputer. Sistem operasi menjalankan perintah sesuai dengan perintah pengguna. Hal ini memungkinkan pengguna untuk dengan mudah mengakses perangkat komputasi mereka.

1. **Fitur-Fitur Keamanan Sistem Operasi**

Fitur keamanan pada sistem operasi komputer memiliki peran yang vital dalam melindungi data, aplikasi, serta sumber daya dari ancaman yang dapat datang dari dalam maupun dari luar. Beberapa fitur pada keamanan system operasi:

1. Autentikasi

Autentikasi merupakan proses pemeriksaan identitas pengguna sebelum memberikan akses ke system. (Stalling, W. 2017). Beberapa jenis autentikasi:

* Kata sandi (password), pengguna memasukkan kata sandi yang benar agar bisa mndapatkan akses.
* Biometrik merupakan analisis atau idntifikasi karakteristik pngguna misalnya fitur sidik jari, deteksi wajah, dan iris mata.
* Token dan kartu pintar, menggunakan suatu pernagkat yang disebut token atau smartcard untuk memperoleh kode autentikasi.

1. **Kontrol akses**

**Kontrol akses yaitu mengatur pengguna yang dapat melakukan akses terhadap sumer daya dari sistem seperti file dan perangkat keras serta penggunaan dari sember daya tersebut** (Aderson, R. 2020). Jenis-jenis akses kontrol:

* **Discretionary Access Control (DAC),**  pengguna dapat melakukan akses file.
* **Mandatory Access Control (MAC), akses ditentukan oleh kebijakan sistem bukan pengguna**.
* **Role-Based Access Control (RBAC), pengguna diberikan akses sesuai perannya masing-masing dalam suatu organisasi.**

1. **Enkripsi**

Enkripsi yaitu memberikan pengamanan dengan mengubah informasi menjadi format yang tidak bisa dibaca kecuali menggunakan kode enkripsi (Schnier, B. 2015). Ada 2 jenis enkripsi:

* **Enkripsi Data (File dan Disk), memberikan pengamanan file atau seluruh disk, misalnya BitLocker (windows) atau file Vault (MacOs)**.
* **Enkripsi Transmisi, emberikan pengamanan pada komunikasi data di jaringan seperti HTTPS untuk website, atau VPN untuk koneksi jarak jauh.**

1. **Firewall**

Firewall dapat berupa perangkat keras (hardware) atau perangkat lunak (software). Firewall merupakan sistem yang memantau dan mengontrol lalu lintas data yang masuk dan keluar dari perangkat atau jaringan agar terhindar dari akses yang tidak sah (software) (Northcutt, S., & Novak, J. 2001). Firewall terdiri dari:

* **Firewall Berbasis Host, menyaring lalu lintas berdasarkan aturan yang ditetapkan pada perangkat lokal.**
* **Firewall Jaringan, berfungsi untuk memfilter lalu lintas antara jargan internal dan eksternal.**

1. Antivirus dan Antimalware

Program ini dapat digunakan untuk mendeteksi, menghapus, dan mencegah perangkat lunak yang berbahaya (malware) contohnya virus, trojan, ransomwarre, dan spyware. Biasanya sistem operasi yang modern telah dilengkapi dengan perangkat lunak antimalware bawaan atau sistem yang mendukung pihak ketiga (Gupta, B. B., & Jain, A. 2018).

1. **Pemantauan dan Logging**

Sistem pemantauan dan logging mencatat aktivitas sistem dan pengguna, serta memberikan wawasan tentang potensi ancaman atau penyalahgunaan. Log ini digunakan untuk analisis forensik dan pemecahan masalah. (Viega, J., & McGraw, G. 2001)

1. **Sandboxing**

Sandboxing merupakan teknik isolasi yang menyediakan ruang untuk menjalankan aplikasi dengan tujuan membatasi adanya potensi kerusakan yang mungkin dapat ditimbulkan. Aplikasi yang ada di dalam sanboxing tidak dapat mengakses data atau proses lain yang ada di sistem (Simmonds, P., & Salas, R. 2014).

1. **Pembaruan Keamanan**

**Pembaruan otomatis memungkinkan sistem operasi untuk mengunduh dan menginstal pebaruan keamanan trbaru tanpa campur tangan pengguna** (Kaspersky Lab. 2020).

1. Virtualisasi dan Isolasi

Virtualisasi dan isolasi memungkinkan pengguna untuk menjalankan beberapa mesin virtual dengan terpisah di satu perangkat fisik dan aplikasi atau sistem operasi yang berbeda, sehingga jika salah satu bagian diserang atau gagal, maka bagian lain tetap aman (Barham, P., & Dragovic, B. 2003).

1. Backup dan Pemulihan Data

Fitur backup memmunkinkan pengguna untuk menyimpan salinan data penting secara teratur. Pemuliah data memungkinkan sistem untuk kembali ke keadaan sebelumnya setelah terjadi kerusakan atau kehilangan data (Greene, S., & Shirley, C. 2014)

1. Proteksi terhadap Serangan Brute Force

Sistem operasi modern melindungi terhadap serangan brute force dengan memperkenalkan pembatasan seperti mengunci akun setelah beberapa kali upaya login gagal dan menggunakan CAPTCHA untuk mencegah upaya login bot (Jackson, C., & Wurster, S. 2014)

1. Keamanan Jaringan

Sistem operasi memiliki berbagai alat untuk melindungi data yang dikirim melalui jaringan, antara lain menggunakan VPN, protokol Enskripsi SSL?TLS, dan firefall untuk melindungi perangkat dan jaringan dari ancaman eksternal (Kaufman, C., Perlman, R., & Speciner, M. 2002).

1. Keamanan Sistem File

Sistem operasi menggunakan izin untuk mengontrol akses file unruk melindungi data. Pengguna atau aplikasi hanya memiliki izin untuk membaca, menulis atau mengeksekusi file berdasarkan izi yang diberikan. (McGilton, D. (2002).

1. Keamanan proses

Sistem operasi mengelola proses dengan memisahkan ruang memori setiap proses sehingga satu aplikasi dapat mengakses atau mengubah aplikasi lain. Teknik yang digunakan meliputi proteksi memori dan pengacakan letak ruang alamat (ASLR) (Silberschatz, A., Galvin, P. B., & Gagne, G. 2018).

1. Mode Aman (Safe Mode)

Mode aman memungkinkan penggguna menjalankan sistem operasi dengan jumlalh aplikasi dan driver minimal untuk memecahkan masalah dan menyelesaikan masalah yang disebabkan oleh malware (Windows IT Pro. 2020).

1. **Jenis-Jenis Ancaman terhadap Keamanan Sistem Operasi**

Keamanan sistem operasi merupakan aspek penting dalam melindungi integritas, kerahasiaan, dan ketersediaan data dalam sistem komputer. Berikut adalah beberapa jenis ancaman yang dapat mengganggu keamanan sistem operasi dan perlu diwaspadai:

1. Malware  
   Malware adalah perangkat lunak berbahaya yang dimaksudkan untuk merusak atau mendapatkan akses tidak sah ke system. Jenis malware antara lain virus, worm , Trojan horse, dan spyware. Malware ini dapat mencuri data, merusak file, dan mengambil kendali system operasi.
2. Serangan Phishing

Phishing adalah teknik penipuan yang digunakan untuk menyamar sebagai organisasi terpercaya dalam komunikasi elektronik untuk mendapatkan informasi sensitif seperti nama pengguna, kata sandi, dan kartu kredit. Serangan ini sering dilakukan melalui email dan pesan teks yang tmapak asli.

1. Serangan DDoS (Distributed Denial of Service)

Tujuan dari serangan DDoS adlah membanjiri system dengan lalu lintas yang berlebihan, sehingga layanan tidak tersedia. Serangan-serangan ini dapat mempengaruhi ketersediaan system operasi dan apliksai yang berjalan di dalamnya, sehingga menyebabkan downtime yang merugikan.

1. Eksploitasi Kerentanan (Vulnerbility Exploits)

Dengan mengekploitasi kerentanan dalam sistem operasi atau aplikasi yang berjalan di dalamnya, penyerang dapat memperoleh akses tidak sah atau mengeksekusi kode berbahaya. Untuk menutup celah keamanan ini, harus menginstal pembaruan keamanan (patch keamanan) secara rutin.

1. Serangan Brute Force

Serangan brute force adalah metode dimana penyerang mencoba semua kemungkinan kombinasi kata sandi hingga mereka menemukan kata sandi yang benar. Serangan ini dapat digunakan untuk mendapatkan akses tidak sah ke akun pengguna atau sistem operasi.

1. Man in the Middle (MitM)

Serangan MitM terjadi ketika penyerang menyadap komunikasi antara dua pihak untuk mencuri informasi atau mengubah data yang dikirim. Serangan ini dapat membahayakan integritas dan kerahasiaan data yang dikirim melalui jaringan.

1. **Manfaat Keamanan Sistem Operasi bagi Pengguna dan Organisasi**

Keamanan sistem operasi (OS) memainkan peran penting dalam melindungi data, perangkat lunak, infrastruktur berbagai ancaman dunia nyata. Manfaatnya tidak hanya dirasakan oleh pengguna perorangan namun juga organisasi. Beberapa manfaat keamanan sistem operasi meliputi:

1. Perlindungan privasi, keamanan system operasi yang kuat mencegah informasi sensitif seperti informasi keunagn, informasi pribadi, dan kata sandi diekspos ke pihak yang tidak berwenang.
2. Keamanan online yang ditingkatkan, keamanan sisitem operasi yang baik melindungi pengguna dari malware, phishing, dan serangan siber lainnya saat berselancar di internet, berbelanja online atau menggunakan online lainnya.
3. Melindungi data bisnis, terdapat organisasi yang dapat menyimpan data berharga seperti informasi keuangan, data pelanggan, dan data rahasia dagang. Keaamanan data yang kuat membantu melindungi data ini dari kebocoran dan akses tidak sah.

**BAB III**

**PENUTUP**

1. **Kesimpulan**

Keamanan system operasi komputer merupakan aspek yang sangat penting untuk menjaga kerahasiaan dan ketersediaan data serta mencegah akses tidak sah dan serangan yang dapat merusak system. System operasi modern dilengkapi dengan berbagai fitur keamanan yang dirancang untuk melindungi system dari berbagai ancaman internal dan ekstenal.

1. **Saran**

Tingkatkan sistem keamanan opersi dengan menerapkan kebijakan keamaan yang ketat, memperbarui perangkat lunak secara berkala, melibatatkan pengguna dalam pelatihan keamanan, dan menggunakan teknologi seperti enkripsi, autentikasi dua folder dan virtualisasi.

**DAFTAR PUSTAKA**

Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems (3rd ed.). Wiley.

Barham, P., & Dragovic, B. (2003). Xen and the Art of Virtualization. ACM SIGOPS Operating Systems Review.

Gupta, B. B., & Jain, A. (2018). Handbook of Research on Secure Multimedia Distribution. IGI Global.

Greene, S., & Shirley, C. (2014). Disaster Recovery and Backup Essentials. Wiley.

Idayudha, Fery. (2020). Sistem Operasi: Konsep dan Implementasi. Jakarta: Informatika.

*I*TBOX. (2024). Keamanan Siber: Mengenal Sistem Keamanan Sistem Operasi untuk Keamanan Komputer.

Jackson, C., & Wurster, S. (2014). The Risks of Brute Force Attacks and How to Mitigate Them. Springer.

Kaspersky Lab. (2020). Cybersecurity for Everyone: Guide to Keeping Safe in the Digital Age. Kaspersky.

Kaufman, C., Perlman, R., & Speciner, M. (2002). Network Security: Private Communication in a Public World (2nd ed.). Prentice Hall.

McGilton, D. (2002). File Systems and their Security. Wiley.

Northcutt, S., & Novak, J. (2001). Network Intrusion Detection: An Analyst's Handbook. New Riders.

Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms, and Source Code in C (2nd ed.). Wiley.

Silberschatz, A., Galvin, P. B., & Gagne, G. (2018). Operating System Concepts (9th ed.). Wiley.

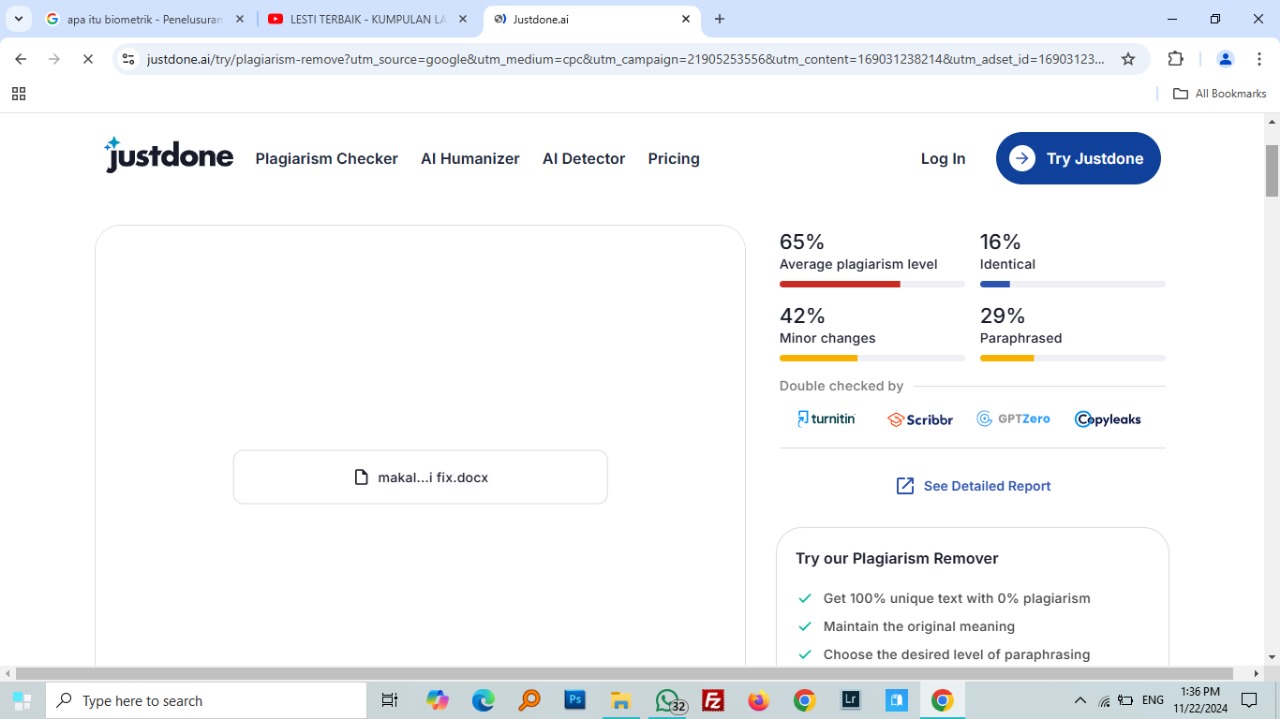
Simmonds, P., & Salas, R. (2014). Cyber Security: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare. Springer.

Stallings, W. (2017). Computer Security: Principles and Practice (4th ed.). Pearson.

Viega, J., & McGraw, G. (2001). Building Secure Software: How to Avoid Security Problems the Right Way. Addison-Wesley.

Windows IT Pro. (2020). Windows Safe Mode: What It Is and How to Use It. Windows IT Pro.

**Bukti Cek Plagiasi**

****