

Analisis Kerentanan dan Eksploitasi Sistem Operasi Windows 11 Family Menggunakan Information System Security Assessment Framework (ISSAF) = Vulnerability and Exploitation Analysis of Windows 11 Family Operating Systems Using the Information System Security Assessment Framework (ISSAF)

Amanda Fairuz Syifa, author

Deskripsi Lengkap: <https://lib.ui.ac.id/detail?id=9999920544072&lokasi=lokal>

Abstrak

Pertumbuhan penggunaan Windows 11 mendorong perlunya evaluasi terhadap sistem operasi ini. Meski merupakan pembaruan dari Windows 10, fokus utama tetap pada risiko keamanan karena meningkatnya serangan siber. Banyak serangan terjadi di tingkat endpoint, sehingga perlindungan pengguna dan data sangat penting. Penelitian ini mengevaluasi kerentanan keamanan dan potensi serangan pada Windows 11 Home dan Enterprise menggunakan metode Information System Security Assessment Framework (ISSAF). Hasilnya menunjukkan adanya kerentanan signifikan pada protokol SMB dan RDP, dengan Windows 11 Enterprise lebih rentan terhadap serangan tertentu seperti SMB Relay Attack. Risiko lain termasuk potensi instalasi backdoor. Rekomendasi mitigasi meliputi pengaktifan SMB Signing, kebijakan kata sandi kompleks, menonaktifkan RDP jika tidak digunakan, dan pengaktifan antivirus. Penelitian ini memberikan wawasan berharga untuk meningkatkan keamanan Windows 11.

The growth in Windows 11 usage necessitates an evaluation of this operating system. Despite being an update from Windows 10, the main focus remains on security risks due to the increasing complexity of cyber attacks. Many attacks occur at the endpoint level, making user and data protection crucial. This study evaluates security vulnerabilities and potential attacks on Windows 11 Home and Enterprise using the Information System Security Assessment Framework (ISSAF) method. The results show significant vulnerabilities in the SMB and RDP protocols, with Windows 11 Enterprise being more susceptible to certain attacks such as SMB Relay Attack. Other risks include potential backdoor installations. Recommended mitigations include enabling SMB Signing, implementing complex password policies, disabling RDP if not in use, and activating antivirus software. This research provides valuable insights for enhancing the security of Windows 11.