ABSTRACT

Tails is a Debian-based operating system within the Linux family, designed to provide anonymity and privacy for users through the Tor network. This research aims to evaluate and analyze the capabilities of Tails OS in maintaining anonymity and privacy through profiling applications, networking, and system storage. The study involves identifying software features that support anonymity and privacy, as well as measuring relevant metrics to evaluate their functionality. The results of this research show that Tails has features supporting the implementation of anonymity and privacy, illustrated through data flow diagrams and metrics based on profiling results. Applications that fully meet the profiling criteria for anonymity and privacy include Onion Share, Pidgin OTR, KeePassXC, Thunderbird, and Tor Browser, all scoring "Yes" on 5 out of 5 metrics. Social media accessed through Tor Browser achieved a "Yes" on 3 out of 5 metrics, indicating partial anonymity and privacy. Unsafe Browser did not meet the criteria, scoring "Yes" on 2 out of 5 metrics. In networking, Tor and Dnsleaktest fully met the anonymity and privacy criteria, scoring "Yes" on 4 out of 4 metrics, while VPN did not meet any criteria, scoring "Yes" on 0 out of 4 metrics. For system storage, Persistent Storage met the criteria with "Yes" on 4 out of 4 metrics, whereas LUKS only scored "Yes" on 2 out of 4 metrics, indicating it does not fully support anonymity and privacy.In conclusion, the metrics used in profiling applications, networking, and system storage in Tails OS comprehensively show that this operating system provides a service environment that supports anonymity and privacy.

Keywords - anonymity, privacy, profiling, Tor, metrics