SISTEM PAKAR DIAGNOSA *PRIVILEGE ESCALATION* DI LINUX MENGGUNAKAN *FORWARD CHAINING* BERDASARKAN MITRE ATT&CK

Dimas Fajar Kurniawan
Program Studi Teknik Informatika
Jurusan Teknologi Informasi

ABSTRACT

Cybersecurity on the Linux operating system is crucial due to its dominance in global server infrastructure. One major threat is privilege escalation, where attackers elevate standard user privileges to administrator through misconfiguration exploitation. This research aims to build an expert system for diagnosing privilege escalation using the Forward Chaining method based on the MITRE ATT&CK framework. The system is designed to mimic the reasoning of a cybersecurity professional in analyzing technical facts on a target system. The system's knowledge base is developed from 7 MITRE ATT&CK sub-techniques decomposed into 9 Linux-specific vulnerabilities. The results show that the system is capable of automatic fact acquisition, logic pattern matching through 9 rule bases, and providing appropriate mitigation recommendations. Testing was conducted through attack scenarios on Debian 12, where the system successfully diagnosed security gaps transparently or declared the system secure if no rules were met.

Keywords : Linux, Privilege Escalation, MITRE ATT&CK, Security.