Výskum Linux rootkitov - report

Vladyslav Havriuk

21. januára 2025

1 Zimný semester

Počas zimného semestra som sa zameral na výskum moderných rootkitov pre Linuxové systémy. Hlavné aktivity zahŕňali:

- Vytvorenie testovacieho prostredia pomocou nástroja Vagrant s Debian Bookworm
- Analýzu existujúcich rootkitov a ich kompatibility s jadrami Linux 5.x a 6.x
- Testovanie detekčných nástrojov ako chkrootkit a rkhunter
- Štúdium rozdielov medzi tradičnými a modernými technikami rootkitov
- Identifikáciu kompatibilných rootkitov (Diamorphine, BDS LKM Ftrace)

Kľúčovým výsledkom bolo zistenie, že väčšina existujúcich rootkitov nefunguje na moderných jadrách, čo vytvára priestor pre nový výskum.

2 Plány na letný semester

V budúcom semestri sa zameriam na:

- Vývoj vlastných detekčných metód pre moderné rootkity
- Hlbšiu analýzu ftrace mechanizmov v jadre Linux
- Testovanie na rôznych distribúciách Linuxu

Cieľom letného semestra je vytvoriť komplexnú štúdiu o moderných rootkitoch a navrhnúť efektívne spôsoby ich detekcie.