Výskum Linux rootkitov - report

Vladyslav Havriuk

7. júna 2025

1 Letný semester

Počas letného semestra som sa zameral na analýzu detekčných mechanizmov a implementáciu vlastného riešenia. Hlavné aktivity zahŕňali:

- Detailnú analýzu projektu LKRG (Linux Kernel Runtime Guard)
- Štúdium techník detekcie rootkitov v jadre
- Implementáciu vlastného detekčného modulu minidetect
- Testovanie detekčných mechanizmov proti moderným rootkitom

2 Analýza LKRG

LKRG sa ukázal ako efektívny nástroj proti moderným rootkitom. Kľúčové zistenia:

- Úspešne deteguje pokusy o eskaláciu privilégií
- Blokuje pokusy o spustenie reverse shell
- Monitoruje integritu kredenciálov procesov
- Deteguje neautorizované modifikácie jadra

3 Implementácia minidetect

Na základe analýzy LKRG som implementoval vlastný detekčný modul minidetect:

- Sleduje kredenciály procesov pomocou kprobes
- Udržiava hash tabuľku s baseline informáciami
- Používa validačné príznaky na detekciu manipulácie
- Monitoruje kľúčové funkcie pre modifikáciu kredenciálov

4 Výsledky a zistenia

Hlavné výsledky výskumu:

- Tradičné detekčné nástroje (chkrootkit, rkhunter) nie sú efektívne proti moderným rootkitom
- LKRG predstavuje robustné riešenie pre detekciu rootkitov
- Monitorovanie kredenciálov je kľúčové pre detekciu pokusov o eskaláciu privilégií
- Moderné rootkity sa zameriavajú na obchádzanie detekčných mechanizmov pomocou ftrace

5 Záver

Výskum ukázal, že moderné rootkity vyžadujú sofistikované detekčné mechanizmy. Implementácia minidetect demonštruje možnosti detekcie manipulácie s kredenciálmi procesov, čo je častá technika používaná rootkitmi. Projekt LKRG predstavuje komplexné riešenie, ktoré efektívne deteguje a blokuje pokusy o kompromitáciu jadra.