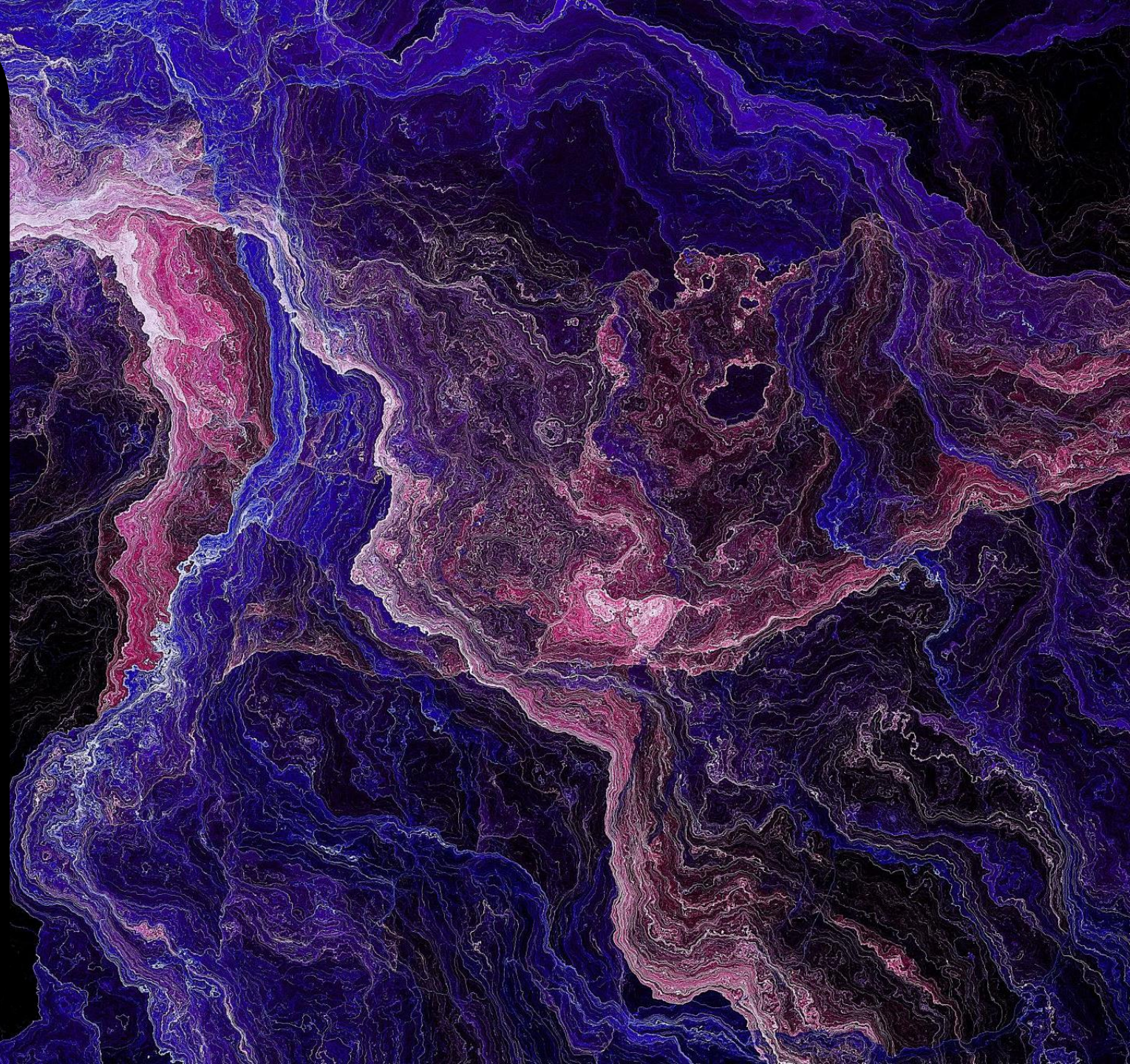
SELinux



Norbert Matuška

Princípy bezpečnosti informačných technológií

Pondelok 15:00

Úvod

- SELinux (Security-Enhanced Linux) ako bezpečnostné vylepšenie jadra Linuxu
- Mandatory Access Control (MAC)
- Ciele projektu:
  + Analýza a implementácia na Ubuntu 22.04
  + Testovanie a hodnotenie schopností

Hlavné funkcionality

- Povinné riadenie prístupu (MAC)
- Typová politika (Type Enforcement)
- Sandboxovanie a izolácia procesov
- Význam v zabezpečení dát

Implementácia na Ubuntu

- Postup inštalácie:
  + Deaktivácia AppArmor
  + Inštalácia SELinux balíčkov
    - policycoreutils a selinux-basics
  + Konfigurácia režimov (permissive a enforcing)
- Význam ladenia politík

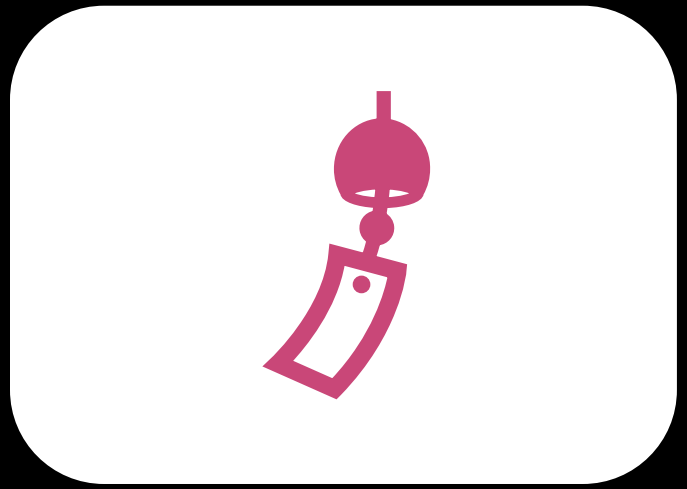
Testovanie

- Testované oblasti:
  + Izolácia procesov a sandboxovanie
  + Obmedzenie prístupu sieťových služieb
    - ftpd_full_access
  + Simulácia útokov (buffer overflow)
  + Prispôsobenie bezpečnostných politík
    - audit2allow
- Výsledky:
  + Zlepšená kontrola prístupu
  + Efektívna ochrana pred neoprávnenými akciami
  + Flexibilita pri tvorbe vlastných politík

Hodnotenie

- Prínosy:
  + Detailná kontrola prístupu
  + Flexibilita politík
- Nevýhody:
  + Zložitosť konfigurácie
  + Možné narušenie funkcionality
- Odporúčanie: postupná implementácia a ladenie politík

Ďakujem za pozornosť



Zdroje

- https://github.com/SELinuxProject/
- https://www.linode.com/docs/guides/how-to-install-selinux-on-ubuntu-22-04/