Security-Enhanced Linux

Sasan Torabkheslat
inbox@torabkheslat.ir
www.torabkheslat.ir

SELinux

ساسان
تراب‌خصلت

۲۴ آذر ۱۳۹۲

مقدمه

تاریخچه

چکیده

مفاهیم

نقطه شروع

ساختار سنتی کنترل دسترسی

- همه چیز درلینوکس یک فایل است.
- روش کنترل دسترسی رایج
  - مالک، گروه، بقیه
  - rwx ،rwx ،rwx
  - 7 ،7 ،7

تاریخچه SELinux.

- توسعه‌دهنده اولیه: آژانس امنیت ملی ایالات متحده
- شروع: اول ژانویه ۱۹۹۸
- اولین نسخه: ۲۲ دسامبر ۲۰۰۰
- در ۸ آگوست ۲۰۰۳ در کرنل نسخه 2.6.0-test3 پیاده سازی شد.
- شرکت‌های همکار:
  - Network Associates
  - Red Hat
  - Secure Computing Corporation

مقدمه
تاریخچه
چکیده
مفاهیم
نقطه شروع

چکیده

- هدف: افزایش امنیت سرورها (و نهایتا سازمان‌ها)
- روشی برای پیاده کردن "کنترل دسترسی اجباری" (Mandatory Access Control)
- پیاده‌سازی در سطح هسته سیستم‌عامل
- هرچیزی یک context است.
- مدل‌های امنیتی گوناگون

مفهوم

- file labeling چیست؟!
  - SELinux User
  - SELinux Role
  - SELinux Type (SELinux Domain)
- مدل‌های امنیتی:
  - TE (Type Enforcement)
  - RBAC (Role-Based Access Control)
  - MLS (Multi-Level Security)

مثالی از روش Type Enforcement

- نقطه شروع!

۱. یافتن خطا
۲. بررسی و تحلیل
۳. استفاده از ابزار audit2why
۴. استفاده از ابزار audit2allow به صورت زیر:

```
cat error.log | audit2allow -m test > test.te
```

۵. و نهایتا:

```
semodule -i test.pp
```

پرسش و پاسخ

؟؟؟؟؟؟؟

مقدمه
تاریخچه
چکیده
مفاهیم
نقطه شروع