Skillbox

Linux как домашняя ОС для специалиста ИБ

Анастасия Полякова

Старший инженер безопасности в «Alibaba cloud»

Цель урока

Цель: познакомиться с Linux-системой как с объектом защиты и платформой для запуска рабочих утилит специалиста ИБ и с основными механизмами безопасности Linux.

Linux как домашняя ОС для специалиста ИБ

- Гибкие настройки секьюрити-механизмов ОС
- Возможность запускать рабочие программы для тестирования безопасности
- Разнообразие специализированных дистрибутивов
- Возможность установки практически на любую платформу

Механизмы безопасности в Linux

- DAC
- ACLs
- Capabilities
- Namespaces
- Network Security
- Cryptography
- Linux Security Modules (MAC)
  - SELinux, Smack, AppArmor, etc
- Audit
- Seccomp
- Integrity Management

Программы для тестирования безопасности на Linux

- Metasploit
- Wireshark
- NMap
- SQLmap
- ZAP
- Edb-debugger
- Cutter
- Many more

Linux-дистрибутивы для специалиста ИБ

- Kali Linux
- BackBox
- Parrot Security OS
- BlackArch
- Bugtraq
- Samurai Web Testing Framework

Платформы для запуска Linux

- Ноутбуки
- Смартфоны
- Планшеты
- Cloud
- Кастомные решения

Вывод

Познакомились с Linux-системой как с объектом защиты и платформой для запуска рабочих утилит специалиста ИБ и с основными механизмами безопасности Linux.

Спасибо за внимание!