

KIBERXAVFSIZLIKDA LINUX OPERATSION TIZIMINING O'RNI

Xolmatov Murodil Zoxid o'g'li*Farg'ona davlat texnika universiteti talabasi*

Annotatsiya: Ushbu maqolada Linux operatsion tizimining kiberxavfsizlik sohasidagi o'rni, afzalliklari hamda xavfsizlikni ta'minlashdagi imkoniyatlari yoritilgan. Linux tizimining ochiq kodli arxitekturasini, foydalanuvchi huquqlarini boshqarish mexanizmi va xavfsizlik vositalari tahlil qilingan. Shuningdek, Kali Linux distributivining penetratsion test va axborot xavfsizligidagi ahamiyati ko'rib chiqilgan.

Kalit so'zlar: Linux, kiberxavfsizlik, operatsion tizim, Kali Linux, penetratsion test, server xavfsizligi, terminal, ochiq kod.

Аннотация: В данной статье рассматривается роль операционной системы Linux в сфере кибербезопасности, её преимущества и возможности обеспечения безопасности. Проанализированы архитектура открытого исходного кода Linux, система управления пользовательскими правами и инструменты безопасности. Также рассмотрено значение дистрибутива Kali Linux в области тестирования на проникновение и информационной безопасности.

Ключевые слова: Linux, кибербезопасность, операционная система, Kali Linux, тестирование на проникновение, безопасность сервера, терминал, открытый исходный код.

Abstract: This article discusses the role of the Linux operating system in cybersecurity, its advantages, and its capabilities in ensuring security. The open-source architecture of Linux, user permission management system, and security tools are analyzed. In addition, the importance of the Kali Linux distribution in penetration testing and information security is examined.

Keywords: Linux, cybersecurity, operating system, Kali Linux, penetration testing, server security, terminal, open source.

Kirish: Bugungi kunda axborot texnologiyalarining jadal rivojlanishi bilan bir qatorda kiberxavfsizlik masalalari ham dolzarb ahamiyat kasb etmoqda. Internet tarmoqlarining kengayishi, bulutli texnologiyalar va onlayn xizmatlarning ko'payishi natijasida turli xil kiberhujumlar soni ortib bormoqda. Shu sababli xavfsiz, ishonchli va barqaror operatsion tizimlardan foydalanish zarurati paydo bo'lmoqda. Linux operatsion tizimi aynan

shunday tizimlardan biri hisoblanadi. Linux ochiq kodli bo'lib, xavfsizlik jihatidan kuchli himoya vositalariga ega. Hozirgi kunda ko'plab serverlar, superkompyuterlar hamda xavfsizlik markazlari Linux asosida ishlaydi. Mazkur maqolada Linux operatsion tizimining kiberxavfsizlikdagi o'rni va imkoniyatlari tahlil qilinadi.

Methods: Mazkur tadqiqot davomida ilmiy tahlil, taqqoslash va kuzatish metodlaridan foydalanildi. Linux operatsion tizimining xavfsizlik imkoniyatlari boshqa operatsion tizimlar bilan qiyosiy tahlil qilindi. Shuningdek, axborot xavfsizligi sohasida qo'llanilayotgan zamonaviy Linux distributivlari o'rganildi.

Asosiy qism: Linux — Unix oilasiga mansub ochiq kodli operatsion tizim bo'lib, 1991-yilda Linus Torvalds tomonidan yaratilgan. Linuxning asosiy afzalliklaridan biri uning bepul va ochiq kodli ekanligidir. Bu esa foydalanuvchilarga tizimni erkin o'zgartirish va takomillashtirish imkonini beradi.

Linuxning mashhur distributivlari quyidagilar:

- Ubuntu
- Debian
- Fedora
- CentOS
- Kali Linux

Linuxning kiberxavfsizlikdagi o'rni

Linux operatsion tizimi kiberxavfsizlik sohasida muhim o'rin egallaydi. Bunga bir nechta sabablar mavjud:

1. Ochiq kodli xavfsizlik

Linuxning ochiq kodli bo'lishi mutaxassislarga tizimni tekshirish, zaifliklarni aniqlash va tezkor ravishda yangilash imkonini beradi. Bu esa xavfsizlik darajasini oshiradi.

2. Foydalanuvchi huquqlarining boshqarilishi

Linuxda foydalanuvchilar uchun maxsus ruxsat tizimi mavjud. Har bir fayl va katalog uchun:

- 1.o'qish (read),
- 2.yozish (write),
- 3.bajarish (execute)

huquqlari belgilanadi. Bu zararli dasturlarning tizimga to'liq kirib kelishini cheklaydi.

3. Server xavfsizligi

Dunyo serverlarining katta qismi Linux asosida ishlaydi. Linux serverlari:

- 1.yuqori barqarorlik,
 - 2.kuchli himoya,
 - 3.kam resurs talab qilishi
- bilan ajralib turadi.

4. Terminal boshqaruvi

Linux terminal orqali boshqarilishi sababli administrator tizim ustidan to'liq nazoratga ega bo'ladi. Terminal buyruqlari yordamida:

Sudo

Chmod

Ssh

iptables

kabi vositalar orqali xavfsizlikni boshqarish mumkin.

Kali Linux va penetratsion test

Kali Linux kiberxavfsizlik mutaxassislari uchun maxsus yaratilgan Linux distributividir. Ushbu tizim tarkibida yuzlab xavfsizlik vositalari mavjud.

Kali Linux quyidagi maqsadlarda ishlatiladi:

- 1.tarmoq xavfsizligini tekshirish,
- 2.zaifliklarni aniqlash,
- 3.penetratsion test o'tkazish,
- 4.etik xakerlik faoliyati.

Mashhur vositalar:

1.Nmap

2.Wireshark

3.Metasploit

4.Aircrack-ng

Ushbu vositalar yordamida tizimdagi xavfsizlik muammolari aniqlanadi va bartaraf etiladi.

Natijalar: Tahlillar shuni ko'rsatadiki, Linux operatsion tizimi yuqori xavfsizlik darajasiga ega bo'lib, kiberxavfsizlik sohasida keng qo'llaniladi. Ayniqsa, server boshqaruvi, tarmoq monitoringi va penetratsion test jarayonlarida Linuxning ahamiyati juda katta. Linuxning ochiq kodli bo'lishi uning doimiy rivojlanishiga va zaifliklarning tezkor bartaraf etilishiga yordam beradi. Shu bilan birga, Linux asosidagi xavfsizlik vositalari axborot tizimlarini himoya qilishda samarali natija beradi.

Xulosa: Xulosa qilib aytganda, Linux operatsion tizimi kiberxavfsizlik sohasida muhim o'rin tutadi. Uning xavfsizlikka yo'naltirilgan arxitekturasini, kuchli boshqaruv tizimi va ochiq kodli imkoniyatlari sababli ko'plab

tashkilotlar aynan Linuxdan foydalanmoqda. Ayniqsa, Kali Linux kabi distributivlar axborot xavfsizligini ta'minlashda samarali vosita hisoblanadi.

FOYDALANILGAN ADABIYOTLAR:

1. Linux Basics for Hackers
2. The Linux Command Line
3. Kali Linux rasmiy hujjatlari
4. Linux Security Documentation
5. Axborot xavfsizligi bo'yicha ilmiy maqolalar va internet manbalari