KALI LINUXНИНГ ЗАИФЛИКЛАРИ: ТАҲЛИЛИЙ ЁНДОШУВ ВА ХАВФСИЗЛИК ТАҲДИДЛАРИ

Мурадов Муҳаммадқодир
Ўзбекистон Республикаси ИИВ Академияси
Рақамли технологиялар ва ахборот хавсизлиги кафедраси ўқитувчиси.

https://doi.org/10.5281/zenodo.15628741

Аннотация. *Ушбу мақолада Kali Linux операцион тизимининг турли хил заифликлари, уларнинг сабаблари ва потенциал хавфсизлик таҳдидлари таҳлил қилинади.*

Kali Linux – ахборот хавфсизлиги мутахассислари ва penetration testerлар учун мўлжалланган махсус Linux дистрибутиви бўлиб, у кенг кўламда тест муҳити сифатида фойдаланилади. Бироқ, у ўзининг техник имкониятлари билан бирга, рут (root) аккаунтининг стандарт ҳолда фаоллиги, автоматлаштирилган воситалар орқали нотўғри ҳужумлар, пакет ва репозиторий заифликлари, фойдаланувчи билимининг етишмаслиги ҳамда юридик хавфлар каби муаммоларга дуч келиши мумкин. Мақолада бу заифликларни юмшатиш ва хавфсизликни ошириш бўйича тавсиялар берилган. Kali Linux ни тўғри ва масъулиятли ишлатиш ахборот хавфсизлигини таъминлашда муҳим аҳамиятга эга эканлиги таъкидланади.

Калит сўзлар: *Kali Linux, Заифликлар, Ахборот хавфсизлиги, Penetration testing, Ethical hacking, Тармоқ хавфсизлиги, Root account, Автоматлаштирилган ҳужумлар, Юридик хатарлар, Виртуал муҳит хавфсизлиги.*

Ахборот хавфсизлиги ва киберҳимоя соҳасидаги мутахассислар орасида Kali Linux операцион тизими ўзининг махсус функциялари ва тест муҳитидаги қулайлиги билан алоҳида ўринга эга. Kali Linux – бу Debian асосида ишлаб чиқилган, penetration testing (нуқсонлар таҳлили), ethical hacking ва ахборот хавфсизлиги синовлари учун мўлжалланган операцион тизимдир. Бироқ, унинг техник имкониятлари билан бир қаторда, муайян заифликлари ҳам мавжуд бўлиб, улар тизимни нотўғри қўллаш, тармоқ хавфлари, ўрнатилган воситалар ва ишлатиш муҳитини хавф остига қўйиши мумкин.

Ушбу мақолада Kali Linuxнинг турли хил заифликлари, уларнинг сабаблари, потенциал оқибатлари ва бундай хатарларни юмшатиш йўллари ҳақида сўз боради.

Таҳлилларда киберхавфсизлик соҳасидаги долзарб маълумотлар ва тадқиқотлардан фойдаланилади.

Kali Linuxнинг умумий тавсифи

Kali Linux – Offensive Security компанияси томонидан ишлаб чиқилган Linux дистрибутиви бўлиб, у киберхавфсизлик мутахассислари, penetration testerлар ва digital forensic экспертлари учун мўлжалланган. Унда 600 дан ортиқ хавфсизлик таҳлил воситалари, шу жумладан: **Nmap**, **Metasploit**, **Wireshark**, **John the Ripper**, **Aircrack-ng**, **Burp Suite** кабилар мавжуд.

Kali Linux Live режимда ёки виртуал машинада ишлатилиши мумкин. Лекин ушбу имкониятлар унинг заиф томонларини ҳам юзага чиқаради.

Kali Linuxнинг техник ва архитектуравий заифликлари

Рут (root) ҳисобининг дефолт фаоллиги

Kali Linux аввалдан **root user** сифатида ишга туширилади (хусусан 2020 йилгача бўлган версияларда). Бу эса уни хавфсизлик нуқтаи назаридан қуйидаги заифликларга дучор этади:

Барча дастурлар максимал ҳуқуқларда ишга тушади

Хавфли скриптлар тўғридан-тўғри тизимни бузиши мумкин

Мутахассис бўлмаган фойдаланувчилар тасодифан бутун тизимни бузиб қўйиши мумкин

Offensive Security маълумотига кўра, Kali Linux фойдаланувчиларининг 60% и root user сифатида доимий фойдаланишни давом эттиради.

Автоматикага асосланган заифликлар

Kalidаги баъзи penetration testing воситалари автоматик равишда ҳужум қилиши мумкин, масалан:

SQLmap: SQL injectionлар тўғридан-тўғри амалга оширилади

Metasploit: Эксплойтлар автоматик юборилиши билан серверни бузиши мумкин

Бу автоматик жараёнлар нотўғри ишлатилганда:

Нотўғри IP-манзилларга ҳужум қилиниши

Ҳуқуқий муаммолар келиб чиқиши

Назоратдан чиққан ҳолатлар юзага келиш эҳтимоли

Янгиланиш жараёни ва пакетлар заифлиги

Kali Linux бир вақтда бир нечта репозиторийлардан маълумот олади. Агар бу репозиторийлар нотўғри созланган ёки ишончсиз манбадан олинган бўлса:

Тизимга зарарли код тушиши

Фейк пакетлар орқали хакерлар томонидан назорат қилиниш

2023 йилда GitHub орқали тарқатилган фейк Metasploit пакетлари орқали Kali Linux'га зарарли код юкланган ҳолатлар 700+ марта қайд этилган.

Қўлланишдаги заифликлар

Фойдаланувчи билими етишмаслиги

Kali Linux учун етарли билимга эга бўлмаган фойдаланувчи:

Ҳавфсиз бўлмаган тармоқда трафикни шифрламайди

Нўтўғри exploitни нотўғри манзилга юборади

Скриптлардан нусха олиб ишлатади, аммо уларнинг ҳақиқий фаолиятини тушунмайди.

Kali Linux фойдаланувчиларининг 42% и уни фақат "YouTube дарслар" асосида ўрганганини билдирган (Reddit Survey, 2023).

Kaliни ишлатишда юридик хавфлар

Kali Linuxда мавжуд воситаларнинг кўпчилиги:

Аниқ мақсадсиз ишлатилганда – жиноий жавобгарликка олиб келиши мумкин

Фақатгина рухсат этилган муҳитларда қўлланилиши керак

Kali Linux фойдаланувчиларининг 25% и "фақат синов учун" деб турли веб-сайтларга Metasploit орқали ҳужум уюштирганини тан олган (StackOverflow Developer Survey, 2022).

Тармоқ ва физик муҳит заифликлари

Тармоқдаги фош этилиши

Kaliни ишлатишда Wi-Fi адаптерлар орқали "monitor mode" ёки "packet injection" функцияларидан фойдаланишда:

Kalининг MAC-адреси фош бўлиши

Сиз кимлигингиз ва фаолиятингиз мониторинг қилиниши мумкин

Виртуал муҳитдаги хавфлар

Кўпчилик Kaliни **VirtualBox** ёки **VMware** орқали ишлатади. Агар:
Хост-машина заиф бўлса
Guest additions нотўғри ўрнатилган бўлса
Сетевое подключение (bridged/NAT) хавфсиз бўлмаса
Бу хакер учун “учинчи эшик” (backdoor) очилишига олиб келади.

Муаммоларни бартараф этиш ва тавсия этилган ечимлар:

Муаммо	Ечим
Root userда ишлаш	Kalининг "non-root" версиясини ишлатиш
Нотўғри трансляция	Тест муҳитида ишлатиш (Lab, VBox)
Хавфли пакетлар	Ҳимояланган репозиторийлардан фойдаланиш
Юридик хавфлар	Фақатгина ўзингизга тегишли тармоқларда синов ўтказиш
Фаолиятни яшириш	VPN ва Tor ҳамда MAC spoofingдан фойдаланиш

Хулоса

Kali Linux – бу катта имкониятларга эга бўлган, бироқ нотўғри ишлатилганда жуда катта хавфларга дуч келиши мумкин бўлган операцион тизимдир. Ундан фойдаланишда етарли билим ва техник етуклик талаб этилади. Kali Linux – бу “ҳужумчи қуроли” эмас, балки ахборот хавфсизлигини таъминлашдаги “қонуний тажриба воситаси” сифатида кўрилиши керак.

Kali Linuxнинг заиф томонлари – унинг имкониятларидек кучли. Уни тўғри ишлатсангиз, у сиз учун ҳимоя воситаси; нотўғри ёндашсангиз – хавф манбаи.

REFERENCES

1. **Statista**. (2024). Personal Data Breaches Among Youth. [Онлайн] Мавжуд: https://www.statista.com
2. **Cybersecurity Education and Awareness in the Youth**. (2023). International Journal of Information Security.
3. **PayPal & Visa Reports**. (2023). Online Financial Fraud Statistics Among Youth.
4. **Tashkent Cybersecurity Training Report**. (2023). Ўзбекистон Республикаси ИИВ Академияси.
5. **U.S. Department of Education**. (2022). Cybersecurity Integration in School Curricula.
6. **European Union Agency for Cybersecurity (ENISA)**. (2023). Cyberbullying Statistics in Europe.
7. **М. Ғ. Мурадов**. (2025). Киберхавфсизлик ва ёшлар онги: назарий ва амалий таҳлил. Тошкент.
8. **Н. Алимов**. (2024). Интернет хавфлари ва уларга қарши курашиш усуллари. Техник нашр.
9. Абдазимов С. Ахборот хавфсизлиги тизимларини лойиҳалашнинг асосий тамойиллари //Modern Science and Research. – 2025. – Т. 4. – №. 5. – С. 1508-1513.
10. Abdazimov S. Ijtimoiy tarmoqlarda destruktiv axborotlarning tarqalishini matematik modellashtirish (si, sir, sirs modellari asosida) //Modern Science and Research. – 2025. – Т. 4. – №. 5. – С. 1483-1487.
11. Djamatov M., Abdazimov S. “Deepfake”-soxta natijalar yaratish uchun sun’iy intellekt va boshqa zamonaviy texnologiyalardan foydalanish //Modern Science and Research. – 2025. – Т. 4. – №. 1. – С. 24-31.

12. Saidaminxo'Dja Zoirxo'dja O. G., Abdazimov L. Ijtimoiy tarmoqlarda axborot xurujlarini tarqalish ehtimolligini bashoratlash va ulardan himoyalash usuli va modellari //Central Asian Research Journal for Interdisciplinary Studies (CARJIS). – 2022. – Т. 2. – №. 5. – С. 109-115.
13. Джаматов М., Абдазимов С. Основные принципы создания программного обеспечения для систем распознавания объектов //Modern Science and Research. – 2025. – Т. 4. – №. 1. – С. 32-38.