LOG FAYL TUSHUNCHASI, TURLARI VA ULARNING AXBOROT XAVFSIZLIGIDAGI AHAMIYATI

Abdullayev Xushnud Raxmatulla o‘g‘li
Axmatov Bekzod Nurali o‘g‘li
Normatov Husan Baxodir o‘g‘li
Qo‘ldosheva Dilnavoz Baxodir qizi
Muhammad al-Xorazmiy nomidagi TATU talabalari

Annotation: Mazkur maqolada log fayllarning axborot tizimlari va kompyuter tarmoqlaridagi o‘rni, ularning tuzilishi, asosiy turlari hamda axborot xavfsizligini ta’minlashdagi ahamiyati yoritilgan. Tadqiqot davomida log fayllarning Application Log, Security Log va Event Log kabi asosiy turlari tahlil qilinib, ularning tizim monitoringi, nosozliklarni aniqlash, foydalanuvchilar faoliyatini nazorat qilish va kiberhujumlarni aniqlashdagi vazifalari o‘rganilgan. Shuningdek, Microsoft Windows operatsion tizimidagi Event Viewer vositasi yordamida loglarni boshqarish imkoniyatlari ko‘rib chiqilgan. Ishda log ma’lumotlarining audit, forensika va insidentlarni tekshirish jarayonlaridagi amaliy ahamiyati ham tahlil qilingan.

Keywords: Log fayllar, jurnal yozuvlari, axborot xavfsizligi, Application Log, Security Log, Event Log, Event Viewer, monitoring, audit, forensika, autentifikatsiya, kiberhujum, insidentlarni tahlil qilish, tizim administratori, Windows loglari.

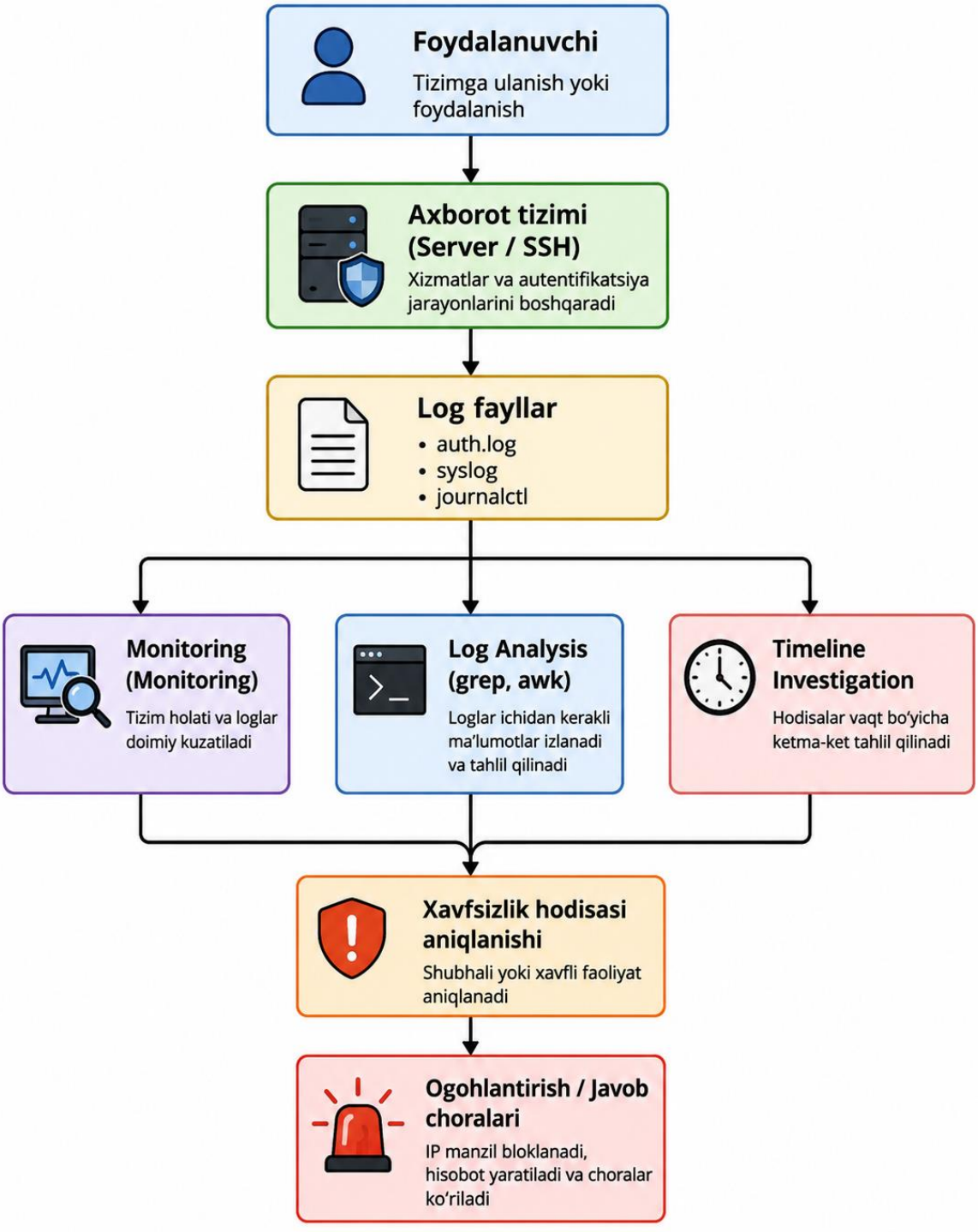
Zamonaviy axborot tizimlari va kompyuter tarmoqlarining uzluksiz ishlashini ta’minlashda log fayllar muhim ahamiyat kasb etadi. Har qanday operatsion tizim, dasturiy ta’minot yoki tarmoq qurilmasi o‘z faoliyati davomida sodir bo‘layotgan hodisalarni maxsus jurnal ko‘rinishida qayd etadi. Ushbu jurnal yozuvlari log fayllar deb ataladi. Log fayllar tizim administratorlari, axborot xavfsizligi mutaxassislari va forensika ekspertlari uchun tizim holatini kuzatish, nosozliklarni aniqlash va kiberhujumlarni tahlil qilishda muhim manba hisoblanadi.

Log fayl — bu operatsion tizim, dasturiy ta’minot, server, tarmoq qurilmasi yoki boshqa axborot tizimi komponentlari tomonidan avtomatik ravishda yaratiladigan va tizimda sodir bo‘lgan hodisalar haqidagi ma’lumotlarni saqlovchi elektron jurnal hisoblanadi. Log fayllar tizim faoliyatining tarixini aks ettiradi hamda ma’lum bir vaqt oralig‘ida bajarilgan amallarni ketma-ket qayd etib boradi. Har bir log yozuvi odatda hodisaning sodir bo‘lgan vaqti (timestamp), hodisani amalga oshirgan foydalanuvchi yoki xizmat nomi, manba IP manzili, bajarilgan amal turi, hodisaning holati (muvaffaqiyatli yoki muvaffaqiyatsiz) va qo‘shimcha texnik ma’lumotlarni o‘z ichiga oladi.

Log fayllar tizim administratorlari va axborot xavfsizligi mutaxassislari uchun muhim axborot manbasi hisoblanadi. Ular yordamida tizimning normal ishlash holatini kuzatish, yuzaga kelgan nosozliklarning sabablarini aniqlash, foydalanuvchilar faoliyatini nazorat qilish hamda xavfsizlik bilan bog‘liq hodisalarni tahlil qilish mumkin. Masalan, foydalanuvchining tizimga kirishi, fayllarni o‘zgartirishi, dastur ishga tushirishi yoki

tarmoq orqali ulanishlarni amalga oshirishi kabi barcha muhim harakatlar loglarda qayd etilishi mumkin.

Log yozuvlari axborot xavfsizligi sohasida ayniqsa katta ahamiyatga ega, chunki ular kiberhujumlarni aniqlash va tekshirish jarayonida asosiy dalil manbasi vazifasini bajaradi. Hujum sodir bo‘lgan taqdirda mutaxassislar log fayllarni tahlil qilish orqali hujumning qachon boshlanganini, qaysi manbadan amalga oshirilganini, qanday usullar qo‘llanilganini va tizimga qanday zarar yetkazilganini aniqlashlari mumkin. Shu sababli loglarni to‘g‘ri yig‘ish, saqlash va tahlil qilish zamonaviy axborot xavfsizligi tizimlarining ajralmas qismi hisoblanadi.



1.1-rasm. Log fayllarning axborot xavfsizligidagi o‘rni

Axborot xavfsizligini ta’minlash jarayonida loglar bir qator muhim vazifalarni bajaradi. Ular tizimda sodir bo‘layotgan barcha muhim hodisalarni qayd etib borish orqali xavfsizlik holatini nazorat qilish imkonini beradi. Loglar yordamida foydalanuvchilarning harakatlari kuzatiladi, ruxsatsiz kirish urinishlari aniqlanadi, zararli faoliyat belgilari topiladi hamda yuzaga kelgan insidentlar bo‘yicha batafsil tahlil o‘tkaziladi. Bundan tashqari, log ma’lumotlari audit jarayonlarida, qonunchilik talablariga muvofiqlikni tekshirishda va raqamli forensika tadqiqotlarida keng qo‘llaniladi. Axborot xavfsizligini ta’minlash jarayonida loglar quyidagi vazifalarni bajaradi:

- tizim faoliyatini monitoring qilish;
- foydalanuvchilar harakatlarini kuzatish;
- ruxsatsiz kirish urinishlarini aniqlash;
- kiberhujumlarni tahlil qilish;
- insidentlarni tekshirish;
- audit va hisobotlarni shakllantirish;
- tizimdagi nosozliklarni aniqlash.

Masalan, SSH xizmatiga bir necha marotaba noto‘g‘ri parol bilan kirishga urinishlar loglarda qayd etiladi. Ushbu yozuvlarni tahlil qilish orqali brute-force hujumlari aniqlanishi mumkin.

Log fayllarning asosiy turlari. Log fayllar axborot tizimlarida bajaradigan vazifasiga, saqlanadigan ma’lumot turiga va qo‘llanilish sohasiga qarab turli kategoriyalarga ajratiladi. Loglarni to‘g‘ri tasniflash va tahlil qilish tizim administratorlari hamda axborot xavfsizligi mutaxassislariga tizim holatini chuqurroq tushunish imkonini beradi. Amaliyotda loglar ko‘pincha Application Log, Security Log va Event Log kabi asosiy turlarga bo‘linadi. Har bir log turi ma’lum bir vazifani bajaradi va tizim faoliyatining muayyan jihatlarini aks ettiradi.

Application Log. Application Log (dastur jurnali) dasturiy ta’minot tomonidan yaratiladigan jurnal yozuvlari hisoblanadi. Ushbu loglarda dastur ishga tushirilishi, foydalanuvchi harakatlari, ma’lumotlar bazasi bilan bog‘lanishlar, xatoliklar va boshqa dasturiy hodisalar qayd etiladi. Application loglar dastur ishlashidagi muammolarni aniqlash, nosozliklarni bartaraf etish va foydalanuvchi faoliyatini kuzatishda muhim ahamiyatga ega. Masalan, veb-ilova foydalanuvchining tizimga kirishi, ma’lumotlarni o‘zgartirishi yoki server bilan bog‘lanishida yuzaga kelgan xatoliklarni Application Log orqali qayd etadi. Dasturchilar va tizim administratorlari ushbu ma’lumotlardan foydalanib dastur samaradorligini oshirishlari mumkin. Masalan:

2025-09-18 10:15:32 User admin logged in

2025-09-18 10:18:21 Database connection established

Yuqoridagi yozuvlardan birinchisi administrator foydalanuvchisining tizimga muvaffaqiyatli kirganligini, ikkinchisi esa ma’lumotlar bazasi bilan aloqa muvaffaqiyatli o‘rnatilganligini bildiradi.

Security Log. Security Log (xavfsizlik jurnali) axborot xavfsizligi bilan bog‘liq hodisalarni qayd etuvchi eng muhim log turlaridan biri hisoblanadi. Ushbu loglar tizimga kirish va chiqishlar, autentifikatsiya jarayonlari, foydalanuvchi huquqlarining o‘zgarishi

hamda xavfsizlik siyosatiga taalluqli boshqa hodisalarni saqlaydi. Security Log quyidagi ma’lumotlarni o‘z ichiga oladi:

- muvaffaqiyatli kirishlar;
- muvaffaqiyatsiz kirishlar;
- foydalanuvchi huquqlarining o‘zgarishi;
- autentifikatsiya hodisalari;
- hisob yozuvlarining yaratilishi yoki o‘chirilishi;
- xavfsizlik siyosatidagi o‘zgarishlar.

Mazkur loglar kiberhujumlarni aniqlashda alohida ahamiyatga ega. Masalan, bir IP manzildan qisqa vaqt ichida ko‘plab muvaffaqiyatsiz kirish urinishlari qayd etilsa, bu brute-force hujumining belgisi bo‘lishi mumkin. Shuningdek, administrator huquqlarining kutilmagan tarzda o‘zgarishi ham xavfsizlik insidenti sifatida baholanadi.

Event Log. Event Log operatsion tizim va xizmatlar tomonidan yaratiladigan umumiy jurnal hisoblanadi. Ushbu loglar tizimda sodir bo‘layotgan turli hodisalarni markazlashgan holda saqlaydi va tizim holatini monitoring qilish imkonini beradi. Event Log tarkibida quyidagi hodisalar qayd etilishi mumkin:

- tizim ishga tushishi;
- tizimning qayta yuklanishi;
- qurilmalar ulanishi yoki uzilishi;
- xizmatlarning ishga tushirilishi va to‘xtatilishi;
- dasturiy va apparat xatoliklari;
- tarmoq hodisalari.

Event Log tizimdagi nosozliklarni aniqlash va ularning sabablarini tahlil qilishda muhim manba hisoblanadi. Masalan, serverning kutilmaganda o‘chib qolishi yoki xizmatning ishlamay qolishi bilan bog‘liq ma’lumotlar aynan Event Log orqali aniqlanishi mumkin.

Jadval 1.1

Windows Event Log turlari

Log turi	**Tavsifi va vazifasi**
Application	Operatsion tizimda ishlayotgan dasturlar va xizmatlar tomonidan yaratiladigan hodisalarni qayd etadi. Dasturiy xatolar, ogohlantirishlar, nosozliklar va ilovalarning ishlash holati haqidagi ma’lumotlarni o‘z ichiga oladi.
Security	Autentifikatsiya, avtorizatsiya va boshqa xavfsizlik bilan bog‘liq hodisalarni qayd etadi. Muvaffaqiyatli va muvaffaqiyatsiz login urinishlari, foydalanuvchi huquqlarining o‘zgarishi, audit hodisalari va xavfsizlik siyosati buzilishlari ushbu logda saqlanadi.
System	Operatsion tizim yadrosi, drayverlar va tizim xizmatlari bilan bog‘liq hodisalarni qayd etadi. Qurilmalar nosozligi, xizmatlarning ishga tushishi yoki to‘xtashi hamda tizim xatolari haqidagi ma’lumotlarni o‘z ichiga oladi.

Setup	Windows operatsion tizimi va uning komponentlarini o‘rnatish, yangilash yoki konfiguratsiya qilish jarayonlariga oid hodisalarni saqlaydi. Tizim yangilanishlari va o‘rnatish jarayonidagi xatolarni tahlil qilishda foydalaniladi.
Forwarded Events	Boshqa kompyuterlar yoki serverlardan markazlashtirilgan tarzda yuborilgan log yozuvlarini saqlaydi. Korporativ tarmoqlarda markazlashgan monitoring va SIEM tizimlari bilan integratsiyada muhim ahamiyatga ega.

Windows operatsion tizimidagi loglar. Microsoft Windows operatsion tizimida loglar Event Viewer vositasi orqali boshqariladi.

Xulosa

Zamonaviy axborot tizimlari va kompyuter tarmoqlarida log fayllar tizim faoliyatini nazorat qilish, xavfsizlik hodisalarini aniqlash va tahlil qilishning asosiy vositalaridan biri hisoblanadi. Har qanday operatsion tizim, server, tarmoq qurilmasi yoki dasturiy ta’minot tomonidan yaratiladigan log yozuvlari tizimda sodir bo‘layotgan jarayonlar haqida muhim ma’lumotlarni taqdim etadi. Ushbu ma’lumotlar tizim administratorlari va axborot xavfsizligi mutaxassislariga tizimning joriy holatini baholash, yuzaga kelgan nosozliklarning sabablarini aniqlash hamda xavfsizlik insidentlarini tekshirish imkonini beradi.

FOYDALANILGAN ADABIYOTLAR:

1. Computer Security: Principles and Practice. Pearson Education, 5th Edition, 2023.
2. Network Security Essentials. Pearson Education, 7th Edition, 2023.
3. National Institute of Standards and Technology. Computer Security Log Management Guide (SP 800-92). Gaithersburg, USA.
4. National Institute of Standards and Technology. Cybersecurity Framework Documentation.
5. Microsoft Learn - Windows Event Logs Documentation
6. Microsoft Learn - Event Viewer Overview
7. Guide to Computer Forensics and Investigations. Cengage Learning, 7th Edition, 2022.
8. Digital Forensics and Incident Response. Packt Publishing, 2020.
9. Practical SIEM Implementation. Packt Publishing, 2018.
10. The Practice of Network Security Monitoring. No Starch Press, 2013.