

Amaliy topshiriq: Tizimdagi foydalanuvchilar faoliyatini kuzatish (Monitoring)

Ushbu topshiriq orqali siz Linux tizimiga kimlar kirganligini, qachon chiqqanligini va qanday harakatlar (buyruqlar) amalga oshirganligini kuzatishni o'rganasiz.

1-Qism: Amaliy vazifalar

1-Vazifa: Joriy foydalanuvchilarni aniqlash

Hozirgi vaqtda tizimga qaysi foydalanuvchilar ulanib turganligini va ular ayni paytda qanday jarayonlar (buyruqlar) bilan band ekanligini ko'rsatadigan buyruqlarni yozing.

2-Vazifa: Kirish (login) tarixini tahlil qilish

Foydalanuvchilarning tizimga qachon kirgani va qachon chiqqanligi (login/logout) tarixini, shuningdek, tizimga kirish uchun qilingan muvaffaqiyatsiz urinishlarni (failed logins) qanday ko'rish mumkinligini yozing.

3-Vazifa: Kiritilgan buyruqlarni kuzatish

Foydalanuvchi terminalda qanday buyruqlarni kiritganini (buyruqlar tarixi) qaysi buyruq yordamida va qaysi fayldan ko'rish mumkinligini tushuntiring.

4-Vazifa: Xavfsizlik jurnallarini (Security logs) tekshirish

Tizimda foydalanuvchilarning autentifikatsiyasi (parol terishlari, sudo ishlatishlari, SSH ulanishlari) haqidagi ma'lumotlar saqlanadigan tizim jurnalini (log faylini) o'qish buyrug'ini yozing.

2-Qism: Javoblar (Solutions)

1-Vazifa javobi:

Tizimdagi joriy foydalanuvchilarni ko'rish uchun quyidagi buyruqlar ishlatiladi:

- `who` — Tizimga kirgan foydalanuvchilar ro'yxatini, ular qayerdan va qachon ulanganligini ko'rsatadi.
- `w` — Tizimga ulanib turgan foydalanuvchilar kimligi va ayni vaqtda nima ish qilayotganligi (qaysi jarayonlarni ishga tushirgani), shuningdek tizimning umumiy yuklanishi (load average) haqida batafsilroq ma'lumot beradi.
- `users` — Tizimga kirgan foydalanuvchilarning faqat nomlarini qisqacha qatorda chiqaradi.

2-Vazifa javobi:

Login va logout tarixini tahlil qilish uchun quyidagi buyruqlar mavjud:

- `last` — Foydalanuvchilarning tizimga kirish va chiqish (login/logout) hamda tizimning qayta yuklanishi (reboot) tarixini ko'rsatadi (ma'lumotlar `/var/log/wtmp` faylidan o'qiladi).
- `lastb` — Tizimga kirish uchun qilingan muvaffaqiyatsiz urinishlarni ko'rsatadi (`/var/log/btmp` faylidan o'qiydi). Bu tizimga ruxsatsiz kirishga harakat qilganlarni (parolni noto'g'ri kiritganlarni) aniqlashda juda muhim (odatda `sudo` talab qilinadi: `sudo lastb`).
- `lastlog` — Barcha foydalanuvchilarning tizimga oxirgi marta qachon kirganligini ro'yxat qilib beradi.

3-Vazifa javobi:

Buyruqlar tarixini kuzatish:

- `history` — Joriy terminal seansida va oldin kiritilgan buyruqlar tarixini raqamlangan ro'yxat

ko'rinishida chiqaradi.

- Aslida, foydalanuvchi kiritgan buyruqlar uning uy katalogidagi yashirin faylda saqlanadi. Masalan, Bash qobig'i (shell) uchun ushbu faylni quyidagicha o'qish mumkin:
cat ~/.bash_history
(Agar siz administrator root bo'lsangiz, boshqa foydalanuvchilarning tarixini ularning uy katalogidan, masalan cat /home/ali/.bash_history orqali ko'rishingiz mumkin).

4-Vazifa javobi:

Foydalanuvchi faoliyati va autentifikatsiya yozuvlari maxsus tizim log fayllarida saqlanadi. Distributivga qarab ushbu faylni quyidagicha o'qish mumkin:

- **Debian/Ubuntu** tizimlarida (eskiroq yoki rsyslog o'rnatilgan versiyalarda):
sudo cat /var/log/auth.log
(Real vaqtda jurnalga tushayotgan yangi yozuvlarni kuzatib turish uchun: sudo tail -f /var/log/auth.log)
- **Debian 12** (va undan yangi, rsyslog o'rnatilmagan tizimlarda) loglar systemd-journald orqali boshqariladi. Ularni ko'rish uchun:
sudo journalctl -u ssh (SSH ulanishlarini ko'rish) yoki
sudo journalctl (barcha tizim jurnallarini ko'rish).
- **Red Hat/CentOS/Fedora** tizimlarida:
sudo cat /var/log/secure