

OPERATION TIZIMLAR • 5-MA'RUZA

Operation tizimlarda xavfsizlik

Xavfsizlikni ta'minlash usullari.

Hisob qaydnomalari. Kirish huquqlari

1. OT xavfsizligi tushunchasi
2. Tahdidlar va buzg'unchi modeli
3. Himoyalangan tizim tamoyillari
4. Xavfsizlikni ta'minlash usullari
5. Kirishni boshqarish modellari
6. Xavfsizlikning formal modellari
7. Identifikatsiya, autentifikatsiya, avtorizatsiya
8. Linuxda hisob qaydnomalari
9. Windowsda hisob qaydnomalari
10. Linuxda kirish huquqlari
11. Windowsda kirish huquqlari
12. sudo va UAC
13. SELinux, AppArmor, MIC
14. Amaliyot, xulosalar, savollar

1. OT xavfsizligi tushunchasi

Ta'rif

OT xavfsizligi — OTning ma'lumotlarni va o'z resurslarini (protssessor, xotira, fayllar, qurilmalar, tarmoq) ruxsatsiz kirish, o'zgartirish, yo'q qilish va ishlashning buzilishidan himoya qilish xususiyati.

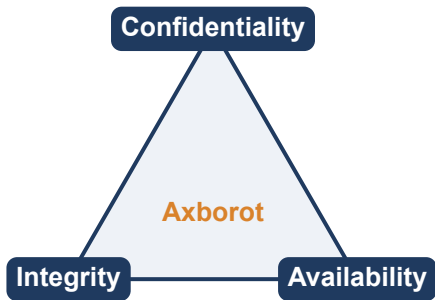
Nima uchun OT alohida o'rin tutadi?

- barcha dasturlar OT **ustida** ishlaydi va uning mexanizmlaridan foydalanadi;
- OT buzilsa — antivirus, shifrlash, MB paroli ham himoya qilmaydi;
- aynan OT **qaysi subyekt qaysi obyektga** kira olishini hal qiladi.

Tushuncha	Ta'rif	Misollar
Subyekt	Harakatni boshlaydigan faol mohiyat	Foydalanuvchi, jarayon, oqim, xizmat
Obyekt	Murojaat qilinadigan passiv mohiyat	Fayl, katalog, qurilma, xotira, soket, reyestr kaliti
Amal (huquq)	Subyektning obyekt ustidagi harakati	O'qish, yozish, bajarish, o'chirish, egani o'zgartirish

Muhim

Amalda OTdagi subyekt — bu **hisob qaydnomasi nomidan bajarilayotgan jarayon**. Foydalanuvchi fayllarga o'zi emas, u ishga tushirgan dastur orqali murojaat qiladi.

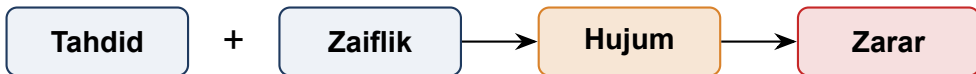


- **Konfidensiallik** — faqat ruxsat berilganlar uchun ochiq.
boshqa foydalanuvchi /home/ali/diplom.docx ni o'qiy olmaydi
- **Yaxlitlik** — ruxsatsiz o'zgartirib bo'lmaydi.
oddiy foydalanuvchi /etc/passwd ni o'zgartira olmaydi
- **Foydalanish imkoniyati** — kerakli paytda ochiq.
bitta jarayon butun xotirani egallay olmaydi

Qo'shimcha: hisobdorlik, rad etib bo'lmaslik, haqiqiylik.

2. Tahdidlar va buzg'unchi modeli

- **Tahdid** — xavfsizlikni buzishi mumkin bo'lgan potentsial hodisa.
- **Zaiflik** — tizimning zaif joyi (koddagi xato, noto'g'ri sozlama, zaif parol).
- **Hujum** — zaiflikdan foydalanishga qaratilgan urinish.
- **Xavf (risk)** — ehtimollik $\times$ oqibatlar og'irligi.



Toifa	Misollar
Ruxsatsiz kirish	Parolni tanlash, sessiyani o'g'irlash, birovning hisobidan foydalanish
Imtiyozlarni oshirish	Yadro yoki setuid-dasturdagi xato orqali root olish
Zararli dasturlar	Virus, chuvalchang, troyan, rutkit, to'lov talab qiluvchi dastur
Xizmatni rad etish (DoS)	Fork-bomba, diskni to'ldirish, xotirani tugatish
Axborot sizib chiqishi	Birovning xotirasini o'qish, qoldiq ma'lumotlar, yon kanallar
Yaxlitlikni buzish	Tizim fayllarini almashtirish, jurnallarni o'zgartirish
Ijtimoiy muhandislik	Fishing, foydalanuvchini aldab dastur ishga tushirtirish

Misol: fork-bomba va resurslarni cheklash

```
:(){ :|:& };;:
```

- : funksiyasi fonda o'zining 2 nusxasini ishga tushiradi;
- jarayonlar soni eksponensial o'sadi;
- jarayonlar jadvali to'ladi — tizim qotadi.

OT vositalari bilan himoya

Resurslarni cheklash: `ulimit -u`,
`/etc/security/limits.conf`, `cgroups`

```
ulimit -u 200    # 200 tadan ortiq jarayon  
emas
```

Buzg'unchi modeli: kimdan himoyalanamiz?

- **Tashqi** — hisobi yo'q, tarmoq orqali hujum qiladi
- **Ichki imtiyozsiz** — oddiy hisob (sinfdagi talaba)
- **Ichki imtiyozli** — huquqlarini suiiste'mol qiluvchi admin
- **Zararli dastur** — qonuniy foydalanuvchi nomidan ishga tushgan

Asosiy xulosa

Foydalanuvchi ishga tushirgan dastur uning **barcha** huquqlarini oladi.

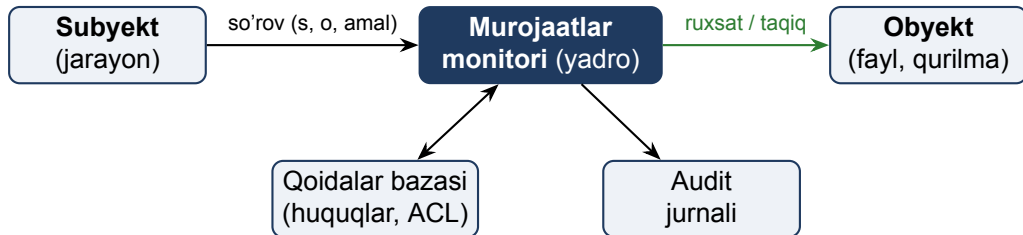
Hisob qaydnomasi huquqlarini cheklash — zararli dastur zararini bevosita cheklaydi.

3. Himoyalangan tizimlarni qurish tamoyillari

Saltzer va Schroeder tamoyillari (1975)

	Tamoyil	Mazmuni	OTdagi misol
1	Mexanizm tejamkorligi	Himoya mexanizmi oddiy va kichik	Mikroyadro
2	Standart bo'yicha xavfsizlik	Ruxsat bo'lmasa — taqiq	Bo'sh DACL = hammaga taqiq
3	To'liq vositachilik	Har bir murojaat tekshiriladi	Har open () da tekshirish
4	Ochiq dizayn	Xavfsizlik algoritmi sirligiga bog'liq emas	Ochiq xesh algoritmlari
5	Imtiyozlarni ajratish	Bir nechta shart talab qilinadi	Parol + ikkinchi omil
6	Minimal imtiyozlar	Faqat zarur huquqlar	Veb-server www-data nomi-dan
7	Umumiy mexanizmlar minimumi	Umumiy resurslarni kamaytirish	Alohida /tmp
8	Psixologik maqbullik	Himoya qulay bo'lishi kerak	Biometriya, SSO

Murojaatlar monitori (Reference Monitor)



Talablar:

1. **Muqarrarlik** — chetlab o'tib bo'lmaydi
2. **Himoyalanganlik** — foydalanuvchi rejimidan o'zgartirib bo'lmaydi
3. **Tekshiriluvchanlik** — tekshirish uchun yetarlicha kichik

Linux: VFS tekshiruvlari + LSM

Windows: Security Reference Monitor (SRM)

TCB — xavfsizlik bog'liq bo'lgan barcha komponentlar (yadro, yuklovchi, login, root dasturlari). Qanchalik kichik — shunchalik ishonchli.

4. Xavfsizlikni ta'minlash usullari

Apparat

- Himoya halqalari (0 va 3)
- MMU, virtual xotira
- NX/XD biti
- SMEP/SMAP
- TPM
- Secure Boot

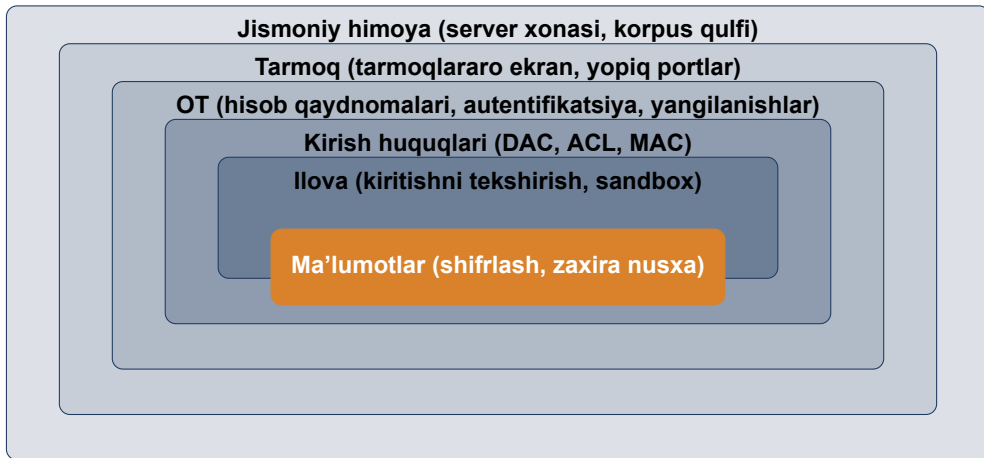
Dasturiy (tizimli)

- Identifikatsiya, autentifikatsiya
- Kirishni chegaralash
- Jarayonlar izolyatsiyasi
- Audit va jurnallash
- Shifrlash (LUKS, BitLocker)
- ASLR, DEP, CFG
- Yangilanishlar

Ma'muriy

- Parollar siyosati
- Minimal imtiyozlar
- Hisoblar auditi
- Zaxira nusxa (3-2-1)
- Foydalanuvchilarni o'qitish

Eshelonlangan himoya (Defense in Depth)



Hech bir usul o'zi yetarli emas — himoya qatlamlari bir-birini to'ldiradi.

5. Kirishni boshqarish modellari

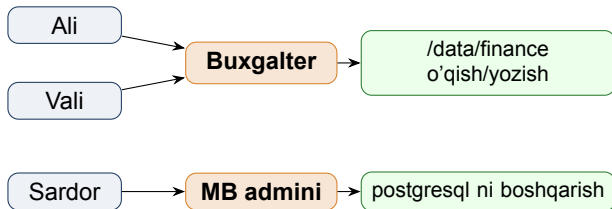
DAC — Discretionary Access Control

- Huquqlarni obyekt **egasi** o'z ixtiyoriga ko'ra belgilaydi
- Unix/Linux (rwx, ACL), Windows (NTFS DACL)
- **Kamchilik:** troyan foydalanuvchi nomidan huquqlarni tarqata oladi; nusxa ko'chirishni nazorat qilmaydi

MAC — Mandatory Access Control

- Huquqlarni **tizim siyosati** belgilaydi
- Subyekt va obyektlarda **xavfsizlik belgilari**
- Ega ham siyosatni o'zgartira olmaydi
- SELinux, AppArmor, Windows MIC, Astra Linux

RBAC — huquqlar **rollarga**, rollar foydalanuvchilarga



OTdagi analogi — **guruhlar** (Linux, Windows, AD)

ABAC — qaror **atributlar** bo'yicha

Qoida misoli

Kadrlar bo'limi xodimi shaxsiy hujjatlarni **faqat ish vaqtida** va **faqat korporativ tarmoqdan** o'qiy oladi.

AWS IAM, Azure, Windows Dynamic Access Control

	DAC	MAC	RBAC	ABAC
Huquqni kim belgilaydi	Obyekt egasi	Xavfsizlik siyosati	Admin, rollar orqali	Atributlar siyosati
Moslashuvchanlik	Yuqori	Past	O'rta	Juda yuqori
Troyanlarga chidamlilik	Past	Yuqori	O'rta	Siyosatga bog'liq
Ma'murlash murakkablighi	Past	Yuqori	O'rta	Yuqori
Misol	chmod, NTFS	SELinux	Guruhlar, AD	AWS IAM

6. Xavfsizlikning formal modellari

Kirish matritsasi (Lampson, 1971)

Subyekt \ Obyekt	report.txt	/usr/bin/gcc	printer	P2 jarayoni
ali	own, r, w	r, x	write	—
vali	r	r, x	—	—
root	r, w	r, w, x	write	kill

Ustunlar bo'yicha → ACL

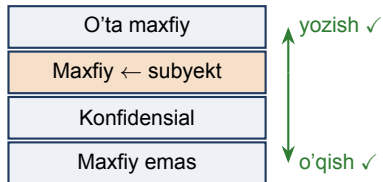
Har bir **obyekt** bilan: kim va nima qila oladi.
Linux, Windows.
"Faylga kim kira oladi?" — oson. Huquqni
qaytarib olish — oson.

Satrlar bo'yicha → Capabilities

Har bir **subyekt** bilan: nimaga kira oladi. Fayl
deskriptorlari, Capsicum, seL4.
Huquqni boshqa jarayonga uzatish — oson.

Bell–LaPadula (1973) — konfidensiallik

- **No Read Up** — yuqori darajani o'qib bo'lmaydi
- **No Write Down** — past darajaga yozib bo'lmaydi



Troyan maxfiy ma'lumotni pastga "oqiza" olmaydi.

Biba (1977) — yaxlitlik

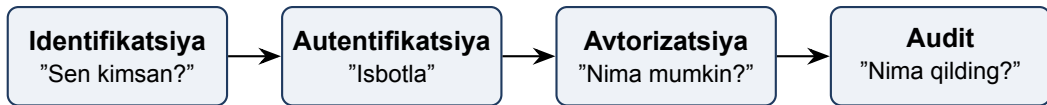
- **No Read Down** — "iflos" ma'lumotni o'qimaslik
- **No Write Up** — yuqori darajani o'zgartirib bo'lmaydi

Windows MIC

Brauzer **Low** darajada ishlaydi. Zararli kod uni egallasa ham, foydalanuvchi fayllariga (**Medium**) yoza olmaydi.

Clark–Wilson: ma'lumotlar faqat tekshirilgan tranzaksiyalar orqali; vazifalar taqsimlangan.

7. Identifikatsiya, autentifikatsiya, avtorizatsiya



Bosqich	Linux	Windows
Identifikatsiya	Foydalanuvchi nomi → UID	Foydalanuvchi nomi → SID
Autentifikatsiya	PAM, /etc/shadow, SSH kalitlari	LSASS, SAM, Kerberos, Windows Hello
Avtorizatsiya	UID/GID, huquqlar, ACL, capabilities, SELinux	Kirish markeri, DACL, imtiyozlar
Audit	journald, auditd, /var/log/auth.log	"Xavfsizlik" jurnali (Event Viewer)

Autentifikatsiya omillari va MFA

Omil	Tavsif	Misollar
Bilim	Foydalanuvchi biladigan narsa	Parol, PIN-kod, maxfiy savol
Egalik	Foydalanuvchida bor narsa	Smart-karta, token, TOTP telefon, FIDO2 kalit
Xususiyat	Biometriya	Barmoq izi, yuz, ko'z qorachig'i

MFA emas

Parol + PIN-kod — ikkalasi ham "bilim"

MFA

Parol + telefondagi ilova kodi — "bilim" + "egalik"

Qoida

OT parolni **hech qachon** ochiq ko'rinishda saqlamaydi:

$$\text{saqlanadigan_qiymat} = \text{Hash}(\text{tuz} + \text{parol})$$

- **Tuz (salt)** — har bir foydalanuvchi uchun noyob tasodifiy satr:
 - bir xil parollar — turli xeshlar;
 - "kamalak jadvallari" foydasiz.
- **Sekin** funksiyalar: SHA-512-crypt, bcrypt, yescrypt, Argon2 — brute force qimmat.
- Kirishda: kiritilgan parol + o'sha tuz → xesh → saqlangan qiymat bilan solishtirish.

8. Linuxda hisob qaydnomalari

Yadro **nomlarni bilmaydi** — faqat sonlar:

- **UID** — foydalanuvchi identifikatori
- **GID** — guruh identifikatori

UID	Vazifasi
0	root — superfoydalanuvchi
1–999	Tizim (xizmat) hisoblari
1000+	Oddiy foydalanuvchilar
65534	nobody

Muhim

root huquqlari **nom** bilan emas, **UID = 0** bilan belgilanadi. UID 0 bo'lgan admin ham superfoydalanuvchi!

Hisob turlari:

1. root — cheklanmagan huquqlar
2. Tizim hisoblari — no login, parolsiz
3. Oddiy foydalanuvchilar

```
ali:x:1001:1001:Ali Valiyev,,,:/home/ali:/bin/bash
```

No	Qiymat	Tavsif
1	ali	Foydalanuvchi nomi (login)
2	x	Parol /etc/shadow da saqlanadi
3	1001	UID
4	1001	Asosiy guruh GID si
5	Ali Valiyev,,,	GECOS — izoh
6	/home/ali	Uy katalogi
7	/bin/bash	Buyruq qobig'i

Hammaga o'qish uchun ochiq — dasturlarga UID ↔ nom o'girish kerak.

```
ali:$y$j9T$Fh3k...$Qx9...:20001:0:90:7:14::
```

No	Tavsif
----	--------

1	Foydalanuvchi nomi
2	Parol xeshi: \$id\$tuz\$xesh
3	Oxirgi o'zgartirish (1970 dan kunlar)
4	Minimal muddat (kun)
5	Maksimal muddat
6	Ogohlantirish (kun)
7	Muddat tugagach bloklash
8	Hisobni bloklash sanasi

\$1\$	MD5 (eskirgan)
-------	----------------

\$5\$	SHA-256-crypt
-------	---------------

\$6\$	SHA-512-crypt
-------	---------------

\$2b\$	bcrypt
--------	--------

\$y\$	yescrypt (standart)
-------	---------------------

! / * — parol bilan kirish yo'q

!\$6\$... — bloklangan

bo'sh — parolsiz kirish!

Faqat root o'qiy oladi.

```
# /etc/group  
developers:x:1050:ali,vali,sardor
```

- **Asosiy guruh** — bitta, /etc/passwd da; yangi fayllarga beriladi
- **Qo'shimcha guruhlar** — bir nechta, /etc/group da

```
$ id ali  
uid=1001(ali) gid=1001(ali) groups=1001(ali),27(sudo),1050(developers)
```

Muhim guruhlar: sudo/wheel (sudo), adm (jurnallar), dialout, video, audio, **docker** — **amalda root ga teng!**

RUID	Haqiqatda kim ishga tushirgan
EUID	Huquqlar kim nomidan tekshiriladi
SUID	Saqlangan UID (imtiyozni qaytarish)
FSUID	Fayl tizimi tekshiruvlari uchun
R/E/S GID	Guruh analoglari

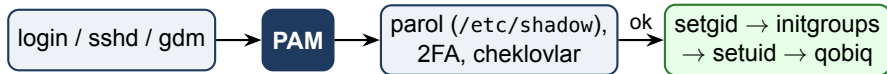
Odatda RUID = EUID.

setuid dasturda farq qiladi:

passwd: RUID = 1001, **EUID = 0**

```
$ grep -E 'Uid|Gid|Groups' \
    /proc/self/status
Uid:  1001 1001 1001 1001
Gid:  1001 1001 1001 1001
Groups: 27 1001 1050
# real effective saved fs
```

Tizimga kirish va PAM



```
# /etc/pam.d/common-auth (parcha)
auth required pam_faillock.so preauth deny=5 unlock_time=900
auth [success=1 default=ignore] pam_unix.so nullok
auth requisite pam_deny.so
```

Modul turlari: auth, account, password, session

Modullar: pam_unix, pam_pwquality,
pam_faillock, pam_limits, TOTP

Hisob qaydnomalarini boshqarish

Harakat	Buyruq
Foydalanuvchi yaratish	<code>sudo useradd -m -s /bin/bash -c "Ali Valiyev" ali</code>
Parol o'rnatish	<code>sudo passwd ali</code>
Qo'shimcha guruhga qo'shish	<code>sudo usermod -aG developers ali</code>
Bloklash / ochish	<code>sudo usermod -L ali / -U ali</code>
Hisob muddati	<code>sudo usermod -e 2026-12-31 ali</code>
Parol siyosati / ko'rish	<code>sudo chage -M 90 -m 1 -W 7 ali / chage -l ali</code>
O'chirish (uy katalogi bilan)	<code>sudo userdel -r ali</code>
Guruh yaratish / guruhdan chiqarish	<code>groupadd developers / gpasswd -d ali developers</code>
Men kimman / kim tizimda	<code>whoami, id / who, w</code>
Kirishlar tarixi / xatolar	<code>last, lastb, faillock --user ali</code>

Ko'p uchraydigan xato

`usermod -G developers ali` (-a siz) qo'shimcha guruhlar ro'yxatini **almashtiradi** — sudo yo'qolishi mumkin. Guruh o'zgarishlari faqat **yangi seansda** kuchga kiradi.

9. Windowsda hisob qaydnomalari

Xavfsizlik identifikatori (SID)



S-1-5-18	SYSTEM
S-1-5-19 / -20	LocalService / NetworkService
...-500	Administrator
...-501	Guest
...-1000+	Oddiy foydalanuvchilar

S-1-5-32-544	Administrators
S-1-5-32-545	Users
S-1-1-0	Everyone
S-1-5-11	Authenticated Users

Foydalanuvchi qayta yaratilsa — **yangi SID**, eski fayllarga kirish yo'q.

Qayerda saqlanadi

- **SAM** — mahalliy hisoblar, NT-xeshlar (System32\config\SAM)
- **Active Directory** — domen hisoblari, Kerberos
- **Microsoft Entra ID** — bulut

LSASS

lsass.exe parolni tekshiradi va marker yaratadi. Uning xotirasi — hujumchilar nishoni (Mimikatz). Himoya: Credential Guard.

Tur

Tavsif

Administrator

To'liq huquq; standart bo'yicha o'chirilgan

Administrators a'zosi

Admin huquqlari + UAC

Standart foydalanuvchi

Tizim sozlamalarini o'zgartira olmaydi

Guest

Minimal, o'chirilgan

SYSTEM, Local/NetworkService

Xizmatlar uchun

NT SERVICE\x, gMSA

Har xizmatga alohida hisob

Kirish markeri (Access Token)

Muvaffaqiyatli kirishda LSASS yaratadi;
har bir jarayon nusxasini oladi.

Tarkibi:

- foydalanuvchi SID i
- barcha guruhlar SID lari
- **imtiyozlar** (SeShutdownPrivilege, SeBackupPrivilege, SeDebugPrivilege)
- **yaxlitlik darajasi**
- seans SID i, marker turi

```
PS> whoami /all  
PS> whoami /priv
```

Ruxsat $\neq$ imtiyoz

Ruxsatlar — **obyektga** tegishli, uning ACL ida.

Imtiyozlar — **hisobga** tegishli, tizim miqyosidagi harakatlar: o'chirish, vaqtni o'zgartirish, debug.

secpol.msc → Foydalanuvchi huquqlarini tayinlash

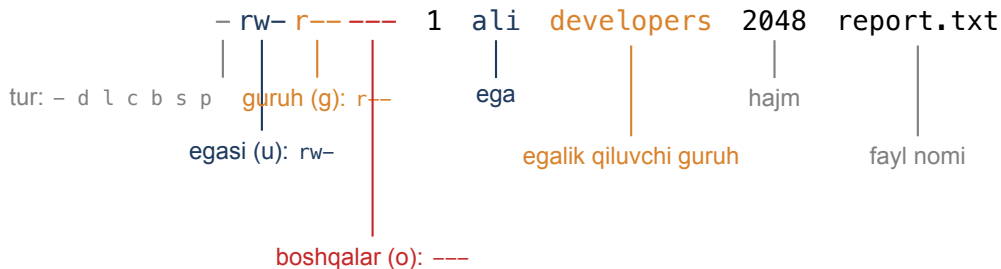
Windows buyruqlari va Linux bilan taqqoslash

Harakat	cmd / PowerShell
Ro'yxat	net user, Get-LocalUser
Yaratish	net user ali P@ss /add
Guruhga qo'shish	net localgroup Users ali /add
O'chirib qo'yish	net user ali /active:no
O'chirish	net user ali /delete
Parol siyosati	net accounts /minpwlen:12
GUI	lusrmgr.msc, secpol.msc

	Linux	Windows
Identifikator	UID/GID	SID
Superuser	root (UID 0)	SYSTEM, Administrators
Saqlash	passwd, shadow	SAM, AD
Autentifikatsiya	PAM	LSASS, NTLM, Kerberos
Jarayon	struct cred	Kirish markeri
Oshirish	sudo, setuid	UAC, runas
root ni bo'lish	capabilities	imtiyozlar

10. Linuxda kirish huquqlari

Klassik model: ega, guruh, boshqalar



Har bir inode saqlaydi: **ega UID i, guruh GID i, 12 bitli rejim** (9 bit huquq + 3 maxsus bit).

Huquq	Fayl	Katalog
r (4)	Tarkibni o'qish	Nomlar ro'yxati (ls)
w (2)	Tarkibni o'zgartirish	Fayl yaratish, o'chirish, nomini o'zgartirish
x (1)	Dastur sifatida bajarish	"O'tish": cd, nom bo'yicha murojaat

- **Faylni o'chirish — katalog huquqlariga bog'liq!** $w+x$ bo'lsa, begona faylni ham o'chirish mumkin (himoya — sticky bit).
- $--x$ katalog — "ko'r": tarkib ko'rinmaydi, ma'lum nomli fayl ochiladi.
- $r--$ katalog — nomlar ko'rinadi, lekin birorta fayl ochilmaydi.
- `/home/ali/docs/a.txt` uchun yo'ldagi **har bir** katalogga x kerak.

Rejim	Belgili	Qo'llanilishi
600	rw-----	Shaxsiy, SSH kalit
644	rw-r--r--	Oddiy fayl
640	rw-r-----	Sirli konfiguratsiya
700	rwX-----	~/ .ssh
755	rwXr-xr-x	Dasturlar
750	rwXr-x---	Loyiha katalogi
777	rwXrwxrwx	Xavfli!

$r = 4, w = 2, x = 1; \quad 6 = 4 + 2 = rw-$

```
chmod 640 report.txt
chmod u+x script.sh
chmod g-w,o= report.txt
chmod -R u=rwX,g=rX,o= project/
```

```
chown ali report.txt # faqat root
chown ali:developers report.txt
chgrp developers report.txt
```

Nega egani faqat root o'zgartiradi?

Aks holda faylni boshqaga "sovg'a qilib" kvotalarni chetlab o'tish mumkin edi.

Maxsus bitlar: setuid, setgid, sticky

Bit	Son	Faylda	Katalogda	ls
setuid	4000	Fayl egasining EUID i bilan bajariladi	—	rws-----
setgid	2000	Fayl guruhining EGID i bilan	Yangi fayllar katalog guruhini oladi	---rws---
sticky	1000	—	Faylni faqat egasi / katalog egasi / root o'chiradi	-----rwt

Katta harf (S, T) — maxsus bit bor, x yo'q.

setuid: passwd

```
-rwsr-xr-x root /usr/bin/passwd  
-rw-r----- root /etc/shadow  
EUID = 0 bilan shadow ga yozadi.
```

sticky: /tmp

```
drwxrwxrwt root /tmp  
Hamma yaratadi, begona faylni hech kim o'chira olmaydi.
```

setgid: umumiy papka

```
chgrp developers /srv/project  
chmod 2770 /srv/project  
Fayllar developers guruhini oladi.
```

root ga tegishli setuid-dastur — imtiyozni oshirish nishoni: `find / -perm -4000 -type f`

Formula

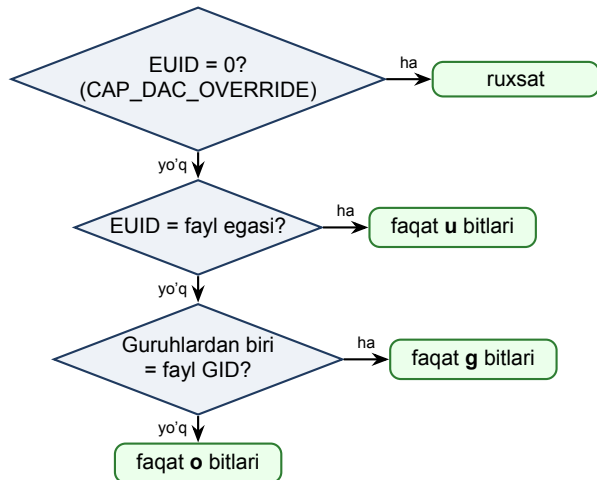
$$\text{yakuniy_huquqlar} = \text{so'ralgan_huquqlar} \text{ AND } (\text{NOT umask})$$

so'ralgan: fayl — 666, katalog — 777

umask	Fayl	Katalog	Qo'llanilishi
022	644	755	Ko'pchilik tizimlarda standart
002	664	775	Guruhda birgalikda ishlash
027	640	750	Serverlar
077	600	700	Maksimal maxfiylik

Doimiy sozlash: `~/.bashrc` yoki `/etc/login.defs`

Linuxda huquqlarni tekshirish algoritmi



Huquqlar qo'shilmaydi!

Birinchi mos toifa tanlanadi. So'ng LSM (SELinux/AppArmor) taqiqlashi mumkin.

Tuzoqli masala

```
----r--r-- ali ali secret.txt
```

```
ali$ cat secret.txt
```

```
Permission denied
```

ali — ega, faqat --- tekshiriladi. Lekin ega
chmod u+r qila oladi.

```
setfacl -m u:vali:rw report.txt
setfacl -m g:teachers:r report.txt
# meros: yangi fayllar uchun
setfacl -d -m g:developers:rwX /srv/project
getfacl report.txt
setfacl -x u:vali report.txt      # yozuvni
setfacl -b report.txt            # barchasini
```

- `ls -l` da +: -rw-rw----+
- **mask** — nomlangan yozuvlar uchun maksimum
- samarali = yozuv **AND** mask
- `chmod g=...` mask ni o'zgartiradi

```
# file: report.txt
# owner: ali
# group: developers
user::rw-
user:vali:rw-
group::r--
group:teachers:r--
mask::rw-
other::---
```

Tartib: ega → nomlangan foydalanuvchi →
guruhlar → boshqalar

root vakolatlari ~40 qismga bo'lingan

CAP_NET_BIND_SERVICE	< 1024 portlar
CAP_NET_RAW	xom soketlar
CAP_DAC_OVERRIDE	rwX ni chetlab o'tish
CAP_CHOWN	egani o'zgartirish
CAP_KILL	begona jarayonga signal
CAP_SYS_PTRACE	begona jarayonni debug
CAP_SYS_ADMIN	"yangi root"

```
sudo setcap 'cap_net_bind_service=+ep' \  
    /usr/local/bin/myserver  
getcap /usr/local/bin/myserver
```

Minimal imtiyozlar

To'liq root o'rniga — aynan bitta kerakli vakolat. Windows analogi — **imtiyozlar**.

ext4 atributlari (root uchun ham!)

```
chattr +i /etc/resolv.conf # o'zgarmas  
chattr +a /var/log/app.log # faqat qo'  
    shish  
lsattr /etc/resolv.conf
```

+a — buzg'unchi jurnalidagi izlarni o'chira olmaydi.

11. Windowsda kirish huquqlari

Xavfsizlik deskriptori	
Owner SID — obyekt egasi	
Group SID — POSIX mosligi uchun	
DACL — KIM va NIMA qila oladi	
	Allow ali Modify
	Deny Guest Read
	Allow Administrators Full
SACL — nimani audit qilish	
	Audit Failure Everyone Write
	Mandatory Label: Medium

Himoyalananadigan obyektlar: fayl, katalog, reyestr kaliti, xizmat, jarayon, printer, umumiy papka.

ACE (Access Control Entry):

- tur: Allow / Deny / Audit
- SID
- huquqlar maskasi
- meros bayroqlari

Ruxsat	Fayl	Katalog
Full Control	Hammasi huquq/ega	+ Hammasi
Modify	O'qish, yozish, o'chirish	+ yaratish/o'chirish
Read & Execute	O'qish, ishga tushirish	Ko'rish, o'tish
List folder contents	—	Ro'yxat
Read	Tarkib, atributlar	Ro'yxat, atributlar
Write	Tarkibni o'zgartirish	Fayl/papka yaratish
Maxsus	14 ta batafsil huquq	

Meros bayroqlari (icac'ls)

(OI) fayllar meros oladi
(CI) ichki kataloglar
(IO) faqat avlodlarga
(NP) faqat bir daraja
(I) otadan meros

Merosni obyekt uchun o'chirish mumkin.

Windowsda kirishni tekshirish algoritmi

1. **MIC**: jarayon darajasi past → yozish yo'q
2. **NULL DACL** → **hammaga to'liq kirish!**
3. **Bo'sh DACL** → hammaga taqiq
4. Ega bilvosita READ_CONTROL, WRITE_DAC oladi
5. ACE lar **tartib bilan**:
 - mos Deny → **rad**
 - mos Allow → huquqlarni qo'shish
 - hammasi to'plandi → **ruxsat**
6. Ro'yxat tugadi, yetarli emas → **rad**

Kanonik ACE tartibi

1. aniq Deny
2. aniq Allow
3. meros Deny
4. meros Allow

Linuxdan farqi

Huquqlar barcha guruhlar bo'yicha **qo'shiladi**: Users=Read + Developers=Modify ⇒ Modify.

Share + NTFS — eng qat'iysi

Share	NTFS	Natija
Full	Read	Read
Read	Modify	Read
Change	Modify	Modify

F to'liq, M o'zgartirish, RX
o'qish+bajarish, R o'qish, W yozish, D
o'chirish

PowerShell: Get-Acl, Set-Acl

```
icacs C:\Data\report.docx
icacs C:\Data /grant ali:(OI)(CI)M
icacs C:\Data /grant "Students":(OI)(CI)RX
icacs C:\Data\exam /deny Students:(W)
icacs C:\Data /remove ali
icacs C:\Data /inheritance:d
icacs C:\Data /setowner Administrators /T
icacs C:\Data /reset /T
```

Kirish huquqlari: Linux va Windows

Jihat	Linux	Windows
Asosiy model	9 bit rwx + POSIX ACL	Istalgan sondagi ACE dan iborat DACL
Aniq taqiq	Yo'q	Bor (Deny ACE)
Guruh huquqlari	Birinchi mos toifa	Barcha guruhlar bo'yicha qo'shish
Meros	default ACL, setgid katalog	O'rnatilgan, OI/CI/IO/NP
Faylni o'chirish	Katalog huquqlari	Delete yoki Delete Child huquqi
Audit	auditd	SACL
Superuser tekshiruvni chetlab o'tadi	Ha (root CAP_DAC_OVERRIDE)	/ Qisman: egaga aylanib DACL ni o'zgartiradi; Se-BackupPrivilege

12. Imtiyozlarni oshirish: sudo va UAC

su dan afzalliklari:

- root paroli shart emas
- buyruqlarni cheklash mumkin
- hammasi jurnallanadi

Faqat visudo orqali tahrirlang!

Qo'shimcha qoidalar: /etc/sudoers.d/

```
sudo -l      # ruxsatlarim
sudo -i      # root qobig'i
sudo -u postgres psql
```

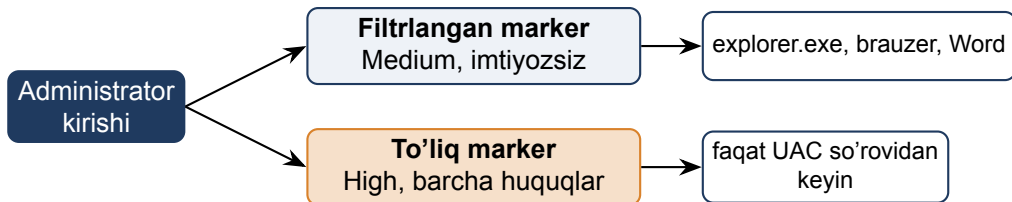
```
# kim  xostlar=(kim_nomidan:guruh)  buyruqlar
root   ALL=(ALL:ALL) ALL
%sudo  ALL=(ALL:ALL) ALL

operator ALL=(root) NOPASSWD: \
    /usr/bin/systemctl restart nginx

%teachers ALL=(root) /usr/sbin/useradd, \
    /usr/sbin/usermod, /usr/bin/passwd [a-z]*
```

Xavf

sudo orqali vim, less, python, find -exec, awk — amalda to'liq root (GTFOBins).



- So'rov **himoyalangan ish stolida** (Secure Desktop) — zararli dastur "Ha" ni bosa olmaydi.
- Standart foydalanuvchi uchun — administrator login va paroli so'raladi.
- UAC qat'iy **xavfsizlik chegarasi emas**; standart foydalanuvchi sifatida ishlash ishonchliroq.

13. Mandatli mexanizmlar

NSA ishlab chiqqan MAC, LSM orqali. RHEL, Fedora, Android.

Xavfsizlik konteksti: user:role:type:level

```
system_u:system_r:httpd_t:s0      #  
    jarayon  
system_u:object_r:httpd_sys_content_t:s0  #  
    fayllar
```

Type Enforcement: httpd_t faqat httpd_sys_content_t ni o'qiydi. Veb-server buzilsa ham /etc/shadow (shadow_t) yopiq.

```
getenforce  
ls -Z /var/www/html  
ps -eZ | grep httpd  
sudo restorecon -Rv /var/www/html  
sudo ausearch -m avc -ts recent
```

Tartib

Avval **DAC**, keyin **MAC**. Ikkalasi ham ruxsat bersagina — kirish.

AppArmor — yo'llarga asoslangan profillar

```
/usr/sbin/nginx {  
  /var/www/** r,  
  /var/log/nginx/** w,  
  network inet tcp,  
  deny /etc/shadow r,  
}
```

`aa-status, aa-enforce, aa-complain`

	SELinux	AppArmor
Asos	belgilar	yo'llar
Murakkablik	yuqori	o'rta
Distributiv	RHEL	Ubuntu

Windows MIC

Untrusted	Anonim jarayonlar
Low	Brauzer sandbox, AppContainer
Medium	Oddiy dasturlar
High	"Administrator sifatida"
System	OT xizmatlari

Qoida — **No Write Up** (Biba)

```
whoami /groups | find "Mandatory Label"  
icacls file.txt /setintegritylevel low
```

14. Amaliyot va xulosalar

1. **Hisobni o'rganish:** `id`, `/etc/passwd`, `/etc/shadow`, `chage -l`; UID 0 li hisoblarni toping.
2. **Loyiha guruhi:** `project` guruhi, 3 talaba, `/srv/project 2770`; sticky bit bilan `3770` ni tekshiring.
3. **umask:** `022` va `077` da fayl/katalog huquqlarini hisoblang.
4. **ACL:** `setfacl -m u:student3:r`, `chmod g-r` dan keyin mask ni tahlil qiling.
5. **Xavfli sozlamalar:** `setuid/setgid` fayllar, hammaga yoziladigan fayllar, sticky siz kataloglar, egasiz fayllar, bo'sh parollar.
6. **Capabilities:** `python3` nusxasiga `cap_net_bind_service` berib, 80-portda root siz ishga tushiring.
7. **Windows:** `whoami /all`, `C:\Lab` uchun `icacls` bilan meros va huquqlarni sozlang; yaxlitlik darajalarini solishtiring.

Xato	Oqibat	To'g'risi
chmod -R 777	Hamma hamma narsani o'zgartiradi	Minimal huquqni aniq subyektga
Doimo root / admin	Virus to'liq nazorat oladi	Oddiy hisob + sudo / UAC
Umumiy hisob	Kim nima qilgani noma'lum	Shaxsiy hisoblar
Ketganlar hisoblari qoladi	Sobiq xodim kira oladi	Muntazam audit, muddat
usermod -G (-a siz)	Guruhlar yo'qoladi	usermod -aG
Xizmat root nomidan	Xizmat buzilsa — tizim buziladi	Alohida foydalanuvchi, capabilities, MAC
docker guruhida	Parolsiz root	Rootless Docker yoki sudo
SELinux ni o'chirish	Himoya yo'qoladi	ausearch, kontekstlarni tuzatish
NULL DACL	Hammaga to'liq kirish	Minimal aniq DACL
Sirlar 644 faylda	Har kim parolni o'qiydi	600 / 640

1. Xavfsizlik = **konfidensiallik**, **yaxlitlik**, **foydalanish imkoniyati**.
2. Subyekt — **jarayon**, obyekt — fayl, qurilma, xotira.
3. Barcha murojaatlar — **murojaatlar monitori** orqali.
4. **DAC** — ega, **MAC** — siyosat, **RBAC** — rollar, **ABAC** — atributlar.
5. Bell–LaPadula — konfidensiallik; Biba — yaxlitlik.
6. Linux — **UID/GID**, Windows — **SID**; root = UID 0.
7. Parollar — faqat **tuzli xesh**.
8. Linux: bitta toifa; Windows: guruhlar qo'shiladi, **Deny** ustuvor.
9. Faylni o'chirish — **katalog** huquqi; sticky bit himoya qiladi.
10. **setuid** — kuchli va xavfli.
11. ACL kengaytiradi; capabilities va imtiyozlar root ni bo'ladi.
12. **Minimal imtiyozlar tamoyili!**

Nazorat savollari (1)

1. Tahdid zaiflikdan nimasi bilan farq qiladi?
2. Saltzer–Schroeder tamoyillaridan qaysilarini chmod 777 buzadi?
3. Murojaatlar monitori qaysi uchta talabga javob berishi kerak?
4. Nima uchun DAC troyan dasturlarga zaif?
5. Bell–LaPadula va Biba qoidalarini ifodalang.
6. ACL capability list dan nimasi bilan farq qiladi?
7. Nima uchun parol + PIN-kod MFA emas?
8. Parollarni xeshlashda tuz nima uchun kerak?
9. /etc/passwd va /etc/shadow maydonlarini tavsiflang.
10. Linuxda superfoydalanuvchi huquqini nima belgilaydi?
11. real UID va effective UID qachon farq qiladi?
12. Foydalanuvchi qayta yaratilganda Linux va Windows qanday farq qiladi?
13. Windows kirish markeri nimalarni o'z ichiga oladi?
14. Imtiyozlar ruxsatlardan nimasi bilan farq qiladi?
15. Katalog uchun r, w, x nimani anglatadi?

Nazorat savollari (2)

16. `umask 027` da yangi fayl va katalog huquqlarini hisoblang.
17. `setuid`, `setgid`, `sticky` bitlariga misol keltiring.
18. Ega `---`, boshqalar `r---`: ega faylni o'qiy oladimi?
19. POSIX ACL dagi `mask` nima uchun kerak?
20. Linux capabilities dan foydalanishga misol keltiring.
21. DACL SACL dan nimasi bilan farq qiladi?
22. NULL DACL va bo'sh DACL farqi nimada?
23. Kanonik ACE tartibi va Windows tekshirish algoritmi.
24. `Share = Read`, `NTFS = Modify`: yakuniy huquq qanday?
25. Nima uchun `sudo` orqali `vim` ga ruxsat berish xavfli?
26. UAC qanday ishlaydi? Filtrlangan marker nima?
27. SELinux va AppArmor farqi; DAC va MAC tartibi.
28. Windows yaxlitlik darajalari Biba ning qaysi qoidasini amalga oshiradi?
29. Universitet kompyuter sinfi uchun hisoblarni himoya qilish choralarini taklif qiling.

1. Tanenbaum A., Bos H. *Modern Operating Systems*. 4th ed. — Pearson, 2014. — 9-bob.
2. Silberschatz A., Galvin P., Gagne G. *Operating System Concepts*. 10th ed. — Wiley, 2018. — 16–17-boblar.
3. Stallings W. *Operating Systems: Internals and Design Principles*. 9th ed. — Pearson, 2017. — 15-bob.
4. Russinovich M. va boshq. *Windows Internals*. 7th ed., Part 1. — Microsoft Press, 2017. — 7-bob.
5. Kerrisk M. *The Linux Programming Interface*. — No Starch Press, 2010.
6. Saltzer J., Schroeder M. *The Protection of Information in Computer Systems*. Proc. IEEE, 1975.
7. man 5 passwd, man 5 shadow, man 5 acl, man 7 capabilities, man 5 sudoers, man 8 pam.
8. Microsoft Learn: *Access Control, Security Identifiers, How User Account Control works*.

E'tiboringiz uchun rahmat!

Savollar?