Доповідь

на тему:

Безпека UNIX

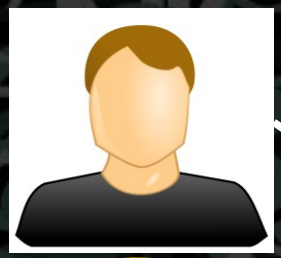
Студента групи СН-41
Рогожинського Тараса Олеговича

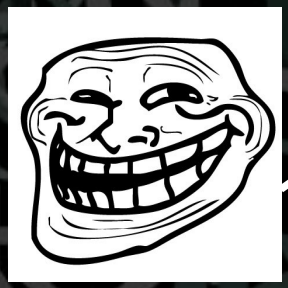
Історія UNIX

1969 р. - Випуск співробітниками Bell Labs першої версії UNICS
1977 р. - лабораторія Білла Джоя в університеті Берклі створила власну версію UNIX названу BSD (Berkley Software Distribution)
1982 р. - Випуск AT&T комерційної UNIX System III (пізніше від System V пішли AIX, HP-UX, IRIX, Solaris)
1983 р. - Створення Річардом Столлменом проекту GNU
1991 р. - Висуск першого ядра Linux

Управління доступом

Субєкти безпеки (користувачі):



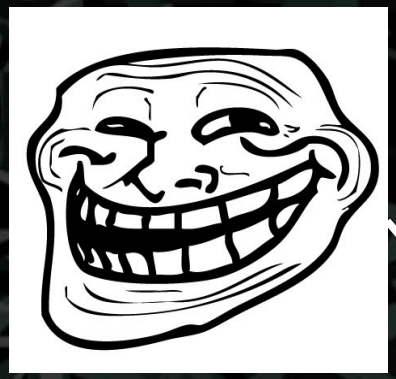


Правила безпеки

Обєкти безпеки:

Файли, пристрої..

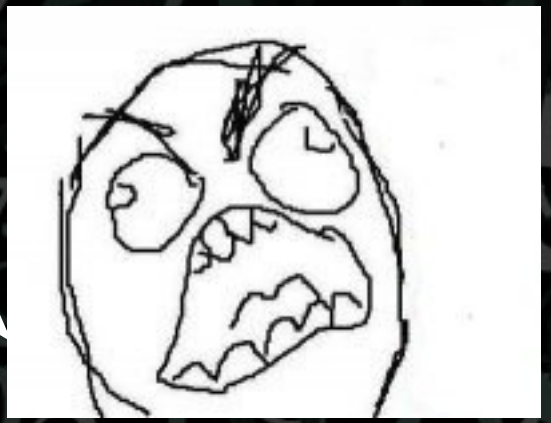
Управління доступом



Виконання дії в системі

Перевірка прав користувача

Заборона системою виконання дії



Користувач в UNIX

Login name (унікальне імя для входу)

User IDentifier, UID (унікальне для кожного користувача число)

Group IDentifier, GID (список груп в які входить даний користувач)

Взаємодія із системою

Користувач

Процеси користувача (із його UID):

Інформація:

Права доступу файлів

Субєкти доступу:
- Власник файлу (співпадіння UID власника файлу і процесу)
- Група власника (співпадіння GID власника файлу і процесу)
- Інші (якшо співпадінь UID і GID немає)

Права доступу:
- w. Запис
- r. Читання
- x. Виконання

- rw- r- - - - - taras users

- Доступ на читання, запис і виконання файлу(перший біт -) власнику(taras)
- Доступ на читання групі власника(users)
- Відсутній доступ всім іншим

Зміна прав доступу

- chmod xyz file

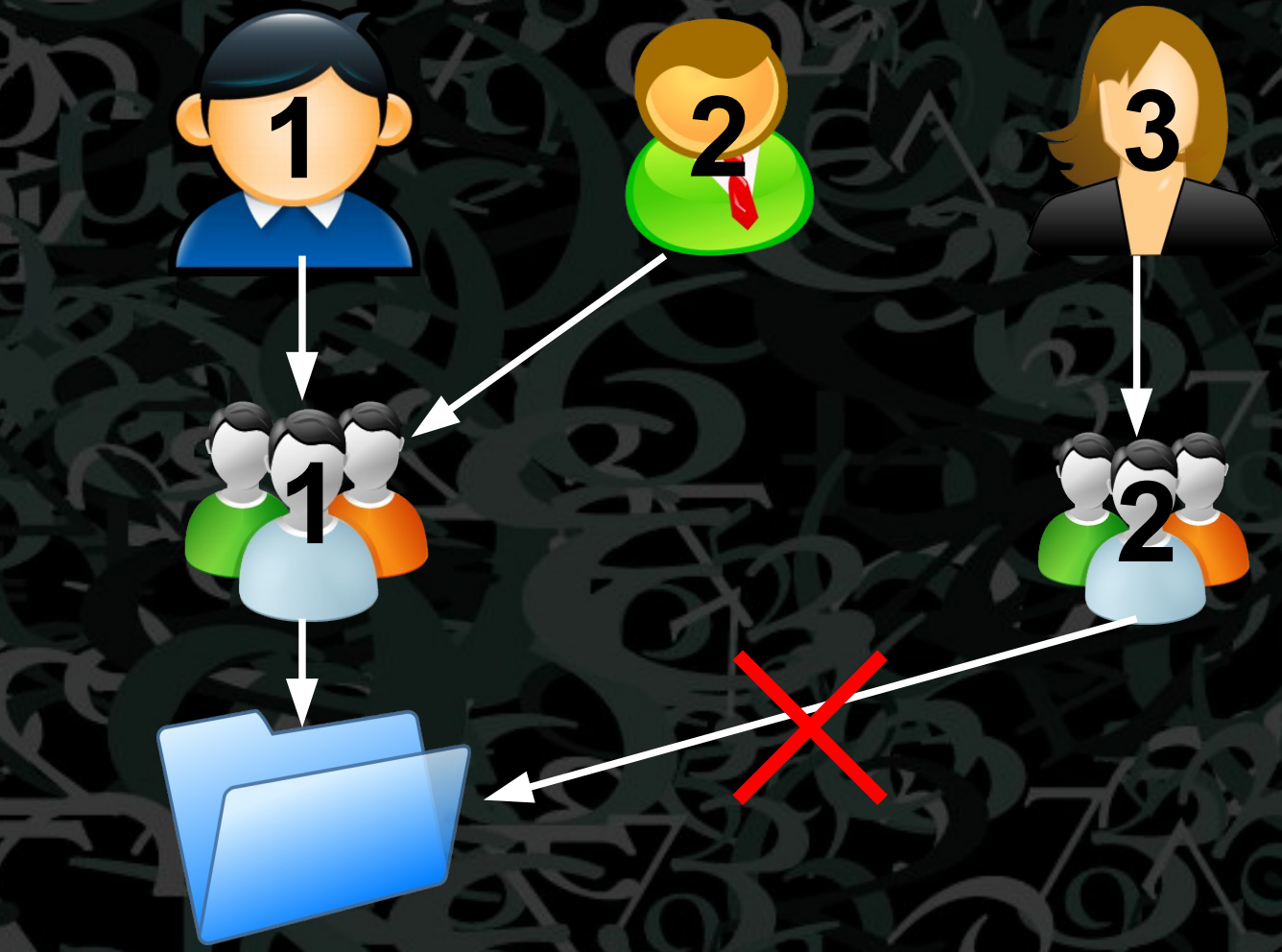
x, y, z – сума бітів доступу користувача, групи та інших
4 – читання
2- запис
1 – виконання
0 – немає доступу
Напр. Chmod 777 file надає **ПОВНИЙ** доступ **ВСІМ** до файлу

- chmod x[+-=]y file

x – користувач (u), його група (g), інші (o), всі (a)
+ додавання права доступу
- забирання права доступу
= встановлення саме такого права доступу
r – читання
w - запис
x – виконання
Наприклад chmod o+r file надасть дозвіл всім іншим на читання файлу

- chown user file. Зміна власника файлу

Недоліки системи прав UNIX



Збереження паролів

В UNIX необхідна інформація щодо користувачів зберігається в **/etc/passwd**

Формат стрічки файлу:

nickname:password_hash:UserID:GroupID:Complete_Name:home_dir:shell_bin

Для того щоб користувачі не мали доступу до хешу паролей інших в багатьох системах він зберігається в іншому файлі - **/etc/shadow**, котрий доступний лише користувачеві root.

xfze:1zuW2nX3sslp3qJm9MYDdglEApAc36r/:::::

На місце хешу в /etc/passwd при цьому вставляється символ x.

Антивірусне забезпечення

Файрволи

Список найбільш поширених UNIX файрволів:
- iptables/netfilter. Платформа: Linux
- IPFilter. Платформа: FreeBSD, NetBSD, OpenBSD, Solaris, Linux, HP-UX...
- Pf. Платформа: OpenBSD, FreeBSD, NetBSD, DragonFlyBSD, MasOS X
- ipfirewall. Платформа: MacOS X, DragonFlyBSD, FreeBSD

На прикладі iptables керування файрволом здійснюється на основі правил. Правила будуються для вхідного трафіку(**INPUT**), вихідного (**OUTPUT**) та прохідного (**FORWARD**). Якщо пакет підходить під якесь із правил то файрвол щодо нього може здійснити такі задані дії як: **ACCEPT**, **DROP**, **REJECT** або **RETURN**.

iptables -P INPUT DROP

iptables -A INPUT -p tcp --dport 46272 -j ACCEPT

Поради щодо безпеки UNIX

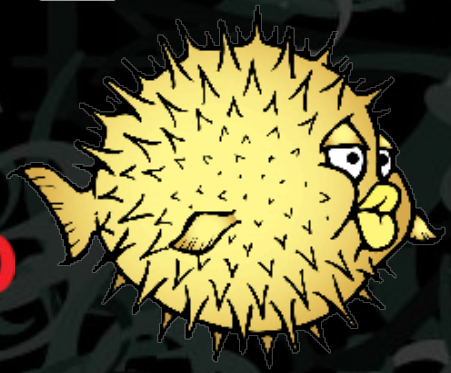
- Встановлення як найбільш надійного пароля для облікового запису root.
- Зведення до мінімуму використання користувача root. При необхідності використовувати команду sudo(підміна suid процесу).
- Контроль над групами користувачів. Максимально обмежити доступ до wheel (дозволяє виконувати sudo і в деяких системах su).
- Контроль користувачів. Видалення старих та неактивних юзерів.
- Заборона віддаленого входу адміністратора.
- Не використовувати telnet котрий не забезпечує шифрування. Натомість ssh.
- Видалити непотрібне програмне забезпечення, виключити непотрібні демони.
- Використовувати лише довірені репозиторії програмного забезпечення від розробників дистрибутиву системи.

Використання UNIX

Нижче подані деякі із компаній котрі використовують Linux та інші Unix системи:

- Департамент захисту США (Red Hat)
- Підводний флот США
- Поштова служба США
- Novell
- Google (Goobuntu)
- IBM
- Panasonic
- Cisco
- Amazon
- Wikipedia
- Біржа Ню-Йорку та Лондона
- Європе́йська організа́ція з я́дерних дослі́джень (Linux використовується на андронному коллайдері)
- NASA (Solaris, Red Hat, OS X)
- Oracle (Solaris, Linux)

Дякую за увагу!



Be UNIX ;-)