**Лекція № 12**

**4.1. Ідентифікація користувачів у системах UNIX**

Операційні системи, які дотримуються традицій UNIX, істотно відрізняються від систем, які наслідують традиції MS-DOS. Різниця між ними полягає у тому, що крім їх багатозадачності, вони ще й багатокористувацькі. Це означає, що комп’ютером можуть одночасно користуватись декілька користувачів. Попри те, що зазвичай комп’ютер має всього одну клавіатуру і монітор, це не заважає спільному користуванню. Наприклад, якщо комп’ютер підключений до локальної мережі або до Інтернету, віддалені користувачі можуть зайти на нього через протокол SSH і виконувати операції. Також вони мають можливість запуску застосунків з графічним інтерфейсом і отримувати зображення на віддаленому дисплеї, оскільки таку можливість підтримує X Window System.

У моделі безпеки UNIX користувач може бути власником файлів або каталогів. У цьому випадку можна керувати доступом до них. За замовчуванням будь-який користувач є власником свого домашнього каталогу. Користувач стає власником файлів та каталогів, які він створив, і може бути примусово призначений адміністратором системи у якості власника інших файлів та каталогів.

Користувачі можуть також належати до певної групи, до якої входять декілька користувачів, і отримати права доступу до файлів і каталогів для членів групи, які визначаються власниками. Крім прав доступу для групи, власник може визначити деякі права доступу для всіх інших користувачів. Для отримання інформації щодо облікового запису певного користувача використовується команда ***id***. Застосування команди без аргументу в результаті виведе інформацію про обліковий запис поточного користувача.

Розглянемо результат команди ***id*** детально. Під час створення облікового запису користувача, йому присвоюється число, яке називається **ідентифікатором користувача (User ID)**, або **UID**. Це число, яке відображується як ім’я користувача (логін) виключно заради зручності самого користувача. У наведеному прикладі його іменем є **debianuser**, а UID – **1000**.

Користувачеві призначається **ідентифікатор основної групи (primary Group ID)**, або **GID**, і він додатково може включатися до складу інших груп. У наведеному прикладі основна група називається **debianuser**. Це поведінка системи за замовчуванням, якщо при створенні користувачем у якості основної групи не було вказано жодної іншої групи. GID має значення **1000**. Значення UID та GID для певного користувача можуть співпадати, однак вони ніяк не пов’язані один з одним. В інших дистрибутивах виведення команди ***id*** може трохи відрізнятися.

У якості аргументу команді ***id*** можна задати ім’я користувача, відмінного від поточного. У такому випадку буде виведена інформація щодо облікового запису користувача. Це демонструє наступний приклад.



У наведеному прикладі виводиться інформація про користувача **1710101** (подібні назви мають облікові записи користувачів студентів ЧНУ ім. Петра Могили де перші 2 цифри означають рік вступу, наступні 3 – номер групи на першому році навчання, останні 2 – порядковий номер студента у списку групи). Таким чином, ми дізналися, що користувач має UID зі значенням **1001** та входить до 2 груп (**gr201** та **students**), основною з яких є група **gr201**, оскільки її ідентифікатор (**1010**) вказаний у якості GID для облікового запису користувача.

Додатково можна скористатися командою ***groups***, яка виводить інформацію, до яких груп входить певний користувач. Застосуємо таку команду для поточного користувача (***debianuser***).



А тепер застосуємо команду ***groups*** і для користувача **1710101**:



Може виникнути слушне питання, де у системи зберігається інформація щодо облікових записів користувачів. Як і багато іншої системної інформації у Linux, вона зберігається у конфігураційних файлах: інформація щодо облікових записів користувачів у файлі **/etc/passwd**, а про групи – у файлі **/etc/group**. Обидва файли мають жорстку структуру, отже розглянемо їх.

Для того, щоб переглянути файл з інформацією щодо облікових записів користувачів, необхідно виконати команду ***less /etc/passwd***:



Це тільки початок файлу **/etc/passwd**. Тут ми можемо бачити спеціальні облікові записи, які насправді не належать кінцевим користувачам. Облікові записи можуть належати спеціальним програмам, що працюють у системі. Це, наприклад, записи **daemon**, **bin**, **sys**, **sync** та інші. Перейшовши файлом далі, ми побачимо облікові записи звичайних користувачів, більшістю з яких є студенти ЧНУ ім. Петра Могили.



Першим у файлі ***/etc/passwd*** знаходиться рядок, що відповідає обліковому запису користувача **root**, який є адміністратором системи. Цей обліковий запис завжди має значення ідентифікатора користувача, яке дорівнює **0**. Наступними у файлі будуть системні облікові записи, які є спеціальними записами, що використовують певні існуючі служби для того, щоб отримати доступ до ресурсів системи.

Усі служби, які працюють у фоновому режимі, мають бути зареєстровані в системі Linux, під певним обліковим записом користувача системи. На початкових етапах розвитку Linux, коли ще не приділялося значної уваги безпеці даних, ці служби часто реєструвалися завдяки застосуванню облікового запису користувача **root**. Однак у випадку зламу зловмисником захисту однієї зі служб він отримав би доступ до всієї системи. Тому в сучасних версіях Linux практично всі служби, що працюють у фоновому режимі, мають свій власний обліковий запис користувача і реєструються за його допомогою.

У системі Linux ідентифікатори користувачів з числовими значеннями менше 1000 зарезервовані для системних облікових записів (принаймні у системі Debian, яка розглядається у посібнику, в інших дистрибутивах можливі інші принципи).

Під час детального розгляду файлу ***/etc/passwd***, можна помітити, що в ньому наведено не тільки реєстраційне ім’я та ідентифікатор користувача. Кожен рядок файлу має жорстку структуру, представлену у вигляді полів, що розділяються символом ‘***:***’. Інформація про обліковий запис певного користувача має 7 полів, що містять наступну інформацію:

1. реєстраційне ім’я користувача;
2. пароль користувача;
3. унікальний ідентифікатор користувача (UID);
4. унікальний ідентифікатор основної групи користувача (GID);
5. необов’язковий коментар, що може бути опущений (зазвичай у ньому міститься певна довідкова інформація про користувача: повне ім’я, номер телефону);
6. абсолютний шлях до домашнього каталогу користувача;
7. командна оболонка, яка застосовується для користувача за замовчуванням при вході у систему.

Звернемо увагу на друге поле, де знаходиться пароль користувача. У вищенаведеному прикладі в кожному рядку задане значення ‘**x**’. Однак це зовсім не означає, що всі облікові записи користувачів мають однаковий пароль. У більш ранніх версіях у файлі ***/etc/passwd*** дійсно містилися зашифровані версії паролів користувачів. Однак з часом це стало небезпечно, оскільки почало з’являтися програмне забезпечення, яке дозволяло відносно легко розшифровувати засекречені паролі. Тому сьогодні у більшості дистрибутивів Linux, паролі користувачів зберігаються в окремому файлі, що має назву ***/etc/shadow*** та доступ до якого дозволений тільки спеціальним програмам. Однак порожнім залишати поле, яке призначалося для пароля, у файлі ***/etc/passwd*** також не можна, оскільки у цьому випадку система дійде висновку, що користувачу взагалі дозволений вхід без пароля. У другому полі файлу ***/etc/passwd*** можна побачити символ ‘***x***’ або ‘***\****’, хоча може знаходитися практично будь-який символ.

Є очевидним і те, що файл ***/etc/passwd*** є звичайним текстовим файлом, який можна відредагувати будь-яким текстовим редактором. Редагуючи цей файл можна управляти користувачами (додавати, змінювати та видаляти), однак це є доволі небезпечним, оскільки при порушенні структури файлу система не зможе його прочитати, і у цьому випадку всі користувачі включаючи і користувача **root** не зможуть увійти в систему. Тому існує більш безпечний шлях, що полягає у використанні спеціальних команд роботи з користувачами, які доступні до виконання тільки адміністратору. Ці команди розглянемо далі у розділі.

Розглянемо файл ***/etc/shadow***, про який вже було зазначено вище та який має набагато більший контроль над управлінням паролів у системі Linux. Порівняно з файлом ***/etc/passwd*** файл ***/etc/shadow*** захищений набагато краще, оскільки до нього має доступ тільки користувач **root**. Введення в дію системи тіньових паролів дозволило забезпечити більш деталізований контроль над паролями користувачів. Зокрема можливе управління того, як часто користувач має змінювати свій пароль і коли повинен відключитися його обліковий запис, якщо зміна пароля не відбулася.

Зареєструвавшись у системі як адміністратор, переглянемо вміст файлу ***/etc/shadow***.



У прикладі була представлена тільки певна частина файлу ***/etc/shadow***, однак уже можна зрозуміти його структуру. Подібно до файлу ***/etc/passwd*** кожен рядок файлу ***/etc/shadow*** складається з полів, що розділяються символом ‘***:***’. Таких полів дев’ять:

1. реєстраційна назва, відповідна реєстраційній назві у файлі

***/etc/passwd***;

1. зашифрований пароль;
2. кількість днів, що відраховується з 1 січня 1970 р., що дозволяє визначити дату останньої зміни пароля;
3. мінімальна кількість днів, після закінчення якої може бути змінений пароль;
4. кількість днів до того, як може змінитися пароль;
5. кількість днів до закінчення терміну дії пароля, після чого користувач отримає попередження в зв’язку з необхідністю його змінити;
6. кількість днів після закінчення терміну дії пароля, після чого його обліковий запис буде відключено;
7. дата (збережена як кількість днів з 1 січня 1970 р.), після якої обліковий запис користувача було відключено;
8. поле, зарезервоване для подальшого використання.

Відомості про групи зберігаються у файлі ***/etc/group***, кожен рядок якого також жорстко структурований. Аналогічно до двох інших файлів, розглянутих вище, рядок розділяється на поля за допомогою символу ‘***:***’. Переглянемо зазначений файл:



Пояснимо структуру файлу ***/etc/group*** більш детально. Подібно до ідентифікаторів користувачів, ідентифікатори груп присвоюються за допомогою спеціального формату. У цьому файлі використовуються наступні чотири поля:

1. назва групи;
2. пароль групи;
3. унікальний ідентифікатор групи (GID);
4. список облікових записів користувача, які належать до групи, якщо вона для них не є основною.

Групам, які призначені для системних облікових записів, присвоюються ідентифікатори груп з числовим значенням менше **1000** (принаймні у дистрибутиві Debian), а групам для користувачів – ідентифікатори груп, що починаються з **1000**.

Під час створення певної групи їй можна задати пароль, який дозволить користувачу, що не є членом групи стати ним на певний час. Хоча схожа можливість застосовується не дуже часто, але все ж вона існує.

Аналогічно, як і у випадку з файлом ***/etc/passwd***, не рекомендується створювати, змінювати та видаляти групи шляхом редагування файлу ***/etc/group***. Краще для цього застосувати спеціальні команди, що будуть розглянуті далі.