Temat: Zarządzanie użytkownikami i logowaniem w systemach Linux

1. Zakres laboratorium:

Celem laboratorium jest zapoznanie studenta z podstawami zarządzania użytkownikami w systemach rodziny Linux, takimi jak: tworzenie użytkowników, automatyczne generowanie losowych haseł, przypisywanie użytkownika do grupy, umożliwienie zdalnego logowania.

W trakcie zajęć student zapozna się z podstawowymi poleceniami umożliwiającymi konfigurację systemu, a także dobrymi praktykami związanymi z pracą administratora.

Umiejętności nabyte przez studenta należą do zestawu elementarnych umiejętności, które powinni posiadać zarówno administratorzy IT (ang. DevOps), ale również programiści pracujący w środowisku Linux. Zdobyta wiedza może być wykorzystana zarówno w konfiguracji nowego jak i utrzymaniu istniejącego serwera firmowego, który jest używany przez wielu użytkowników o różnych uprawnianiach.

2. Wymagane oprogramowanie:

- program VirtualBox
- maszyna wirtualna z systemem CentOS 8 w wersji Minimal
- program putty
- program puttygen

3. Instalacja dodatkowego oprogramowania

Domyślnie systemy operacyjne nie mają zainstalowanego żadnego edytora tekstu, więc w celu instalacji swojego ulubionego edytora należy wykorzystać menadżer pakietów yum:

- VIM: `yum install vim`
- NANO: `yum install nano`

Jeśli będziesz potrzebował dodatkowego oprogramowania możesz

4. Przebieg laboratorium:

1. Uruchom maszynę wirtualną przy pomocy programu VirtualBox
2. Zaloguj się jako root (pass: root)
3. [root] utwórz dwóch użytkowników. Nazwy użytkowników powinny być kombinacją Twojego imienia i nazwiska. Przykłady dla Jana Kowalskiego: jankowalski, jkowalski, jank, jako. Dla obydwóch użytkowników ustal komentarz.

   ```
   adduser -c komentarz nazwa_uzytkownika
   ```

4. [root] wygeneruj silne losowe hasła (co najmniej 16 znaków) dla obydwóch użytkowników przy pomocy jednej z wybranych metod:
   - `date +%s | md5sum | head -c` *`liczba_znakow`*

- `date +%s | sha256 | base64 | head -c liczba_znakow`
- `< /dev/urandom tr -dc _A-Z-a-z-0-9 | head –c liczba_znakow`
- `tr -cd '[:alnum:]' < /dev/urandom | fold -w liczba_znakow | head -n1`
- `openssl rand -base64 liczba_znakow`

5. [root] zapisz wygenerowane hasła a następnie przypisz je użytkownikom

   ```
   passwd nazwa_uzytkownika
   ```

6. [root] wyświetl i zapisz wpisy w plikach **`/etc/passwd`** oraz **`/etc/shadow`** związane ze stworzonymi użytkownikami

   ```
   grep nazwa_uzytkownika /etc/passwd
   ```

   ```
   grep nazwa_uzytkownika /etc/shadow
   ```

7. [root] sprawdź status usługi sshd:

   ```
   systemctl status sshd
   ```

8. Jeśli usługa sshd jest nieaktywna, uruchom ją poleceniem:

   ```
   systemctl start sshd
   ```

9. Sprawdź stan interfejsu ethernetowego (enp0s…) oraz zapisz IP interfejsu (w CentOS `ifconfig` jest deprecated, zamiast tego używa się polecenia `ip`)

   ```
   ip addr
   ```

10. Jeśli interfejs nie ma przypisanego adresu IP, należy uruchomić klient DHCP

    ```
    dhclient nazwa_interfejsu
    ```

11. [user] wykorzystując putty zaloguj się jako jeden ze stworzonych użytkowników (wykonaj zrzut przedstawiający pomyślne zalogowanie)
12. [user] wykorzystując puttygen wygeneruj parę kluczy (typ: SSH-2 RSA, liczba bitów: >1024, powinna to być potęga 2)
13. Zapisz liczbę bitów wykorzystaną do stworzenia klucza
14. Po wygenerowaniu kluczy, skopiuj klucz publiczny do notatnika, natomiast prywatny zapisz na dysku
15. [putty user] stwórz w katalogu domowym plik .ssh/authorized_keys
16. Wklej do pliku wcześniej zapisany klucz publiczny (zapisz zrzut przedstawiający zawartość pliku authorized_keys)
17. [putty user] sprawdź i ewentualnie ustal uprawnienia dla katalogu .ssh i pliku authorized_keys
    - dla .ssh: `-rwx------`
    - dla .ssh/authorized_keys: `-rw-r-r-`
18. Wykonaj zrzut ekranu przedstawiający prawa dostępu do .ssh i authorized_keys
19. [root] zmień konfigurację usługi sshd tak, aby niemożliwe było logowanie się jako root. W tym celu należy otworzyć plik `/etc/ssh/sshd_config`, a następnie ustawić opcję `PermitRootLogin no`). Wykonaj zrzut ekranu przedstawiający zmienione fragmenty konfiguracji. Zrestartuj usługę sshd.

    ```
    systemctl restart sshd
    ```

20. Przy użyciu putty sprawdź, czy jest możliwe zalogowanie się jako root. Wykonaj zrzut ekranu przedstawiający próbę zalogowania.
21. [root] zmień konfigurację usługi sshd tak, aby niemożliwe było logowanie przy pomocy hasła. W tym celu w pliku `/etc/ssh/sshd_config` ustaw opcja `PasswordAuthentication no`. Zrestartuj usługę sshd.
22. Przy użyciu putty spróbuj się zalogować jako użytkownik. Wykonaj zrzut ekranu przedstawiający próbę zalogowania.
23. Przy użyciu putty spróbuj zalogować się jako użytkownik wykorzystując wcześniej wygenerowany prywatny klucz. Aby dodać klucz wybierz Connection -> SSH -> Auth -> Private key file for authentication -> wskaż położenie klucza. Wykonaj zrzut ekranu przedstawiający próbę zalogowania.
24. Zablokuj jednego z utworzonych użytkowników wykorzystując polecenie chage. Ustaw datę na dzień przed terminem zajęć (format: YYYY-MM-DD):

    ```
    chage -E data nazwa_uzytkownika
    ```

25. Ustaw komentarz dla zablokowanego konta opisujący powód zablokowania konta.

    ```
    usermod -c komentarz nazwa_uzytkownika
    ```

26. Wykonaj zrzut ekranu przedstawiający zawartość pliku `/etc/passwd`
27. Spróbuj zalogować się jako użytkownik, którego konto zostało zablokowane. Wykonaj zrzut ekranu przedstawiający próbę zalogowania.
28. Wykonaj zrzut przedstawiający zawartość logów usługi ssh (`/var/log/secure`). Następnie wypisz godziny zalogowania i wylogowania poszczególnych użytkowników wraz z komentarzem jaka metoda autentykacji została wykorzystana (hasło, klucz).

5. Punktacja:

- stworzenie użytkowników + wygenerowanie haseł: **0,25pkt**
- jw. + wygenerowanie kluczy: **0,5pkt**
- jw. + pomyślne zalogowanie przy pomocy kluczy: **0,75pkt**
- jw. + zablokowanie dostępu dla użytkownika + logi z usługi ssh: **1pkt**

6. Notatki z ćwiczenia:

Data	*Grupa*
Imię i nazwisko	

1. Nazwy użytkowników:
    a. …
    b. …
2. Polecenie wykorzystane do wygenerowania hasła:

3. Wygenerowane hasła dla obydwóch użytkowników:

4. Wpisy w pliku /etc/passwd dla stworzonych użytkowników (zrzut ekranu):

5. Wpisy w pliku /etc/shadow dla stworzonych użytkowników (zrzut ekranu):

6. Status usługi sshd (zrzut ekranu):

7. Status interfejsów sieciowych (zrzut ekranu):

8. Pomyślne zalogowanie się do systemu przy pomocy putty (zrzut ekranu):

9. Wygenerowany klucz prywatny:

10. Wygenerowany klucz publiczny:

11. Uprawnienia katalogu .ssh i pliku authorized_keys (zrzut ekranu):

12. Zmieniona konfiguracja sshd_config (zrzut ekranu przedstawiający zmienione fragmenty):

13. Nieudana próba zalogowania się jako root przy pomocy putty (zrzut ekranu):

14. Nieudana próba zalogowania się jako użytkownik przy pomocy putty wykorzystując hasło (zrzut ekranu):

15. Próba zalogowania się jako użytkownik przez putty wykorzystując klucz (zrzut ekranu):

16. Zrzut ekranu przedstawiający plik /etc/passwd po zablokowaniu dostępu dla użytkownika (zrzut ekranu):

17. Logi usługi ssh wraz z komentarzem: