

Uživatelé a oprávnění

Datum zpracování: 17.10.2023

Zpracovali: Kevin Daněk

Zadání

Adresa stanice	kevin.danek@a0322.nti.tul.cz
Adresa virtuálního systému	student@192.168.56.2
Heslo k virtuálnímu systému	123456NTI

Ve **virtuálním systému** proveďte následující úkony.

1. Vytvořte uživatele pro jména Adam Bednář, Bohumil Coufal, Cyril Duda, David Egrt a Eva Filová. Zvolte vhodná uživatelská jména (login). Všichni budou ve skupině "uzivatele".
2. Nastavte všem hesla s instantní expirací (uživatel bude nucen si změnit heslo při prvním přihlášení).
3. Každému uživateli vytvořte v domovském adresáři adresář **groupshare**, kam budou mít přístup členové skupiny a jehož bude vlastníkem.
4. Každému uživateli vytvořte v domovském adresáři adresář **publicshare**, kam bude mít přístup jakýkoliv uživatel a který bude vlastněný správcem.
5. Vytvořte v každém domovském adresáři adresář **readonly**, ve kterém budou soubory uživatelům přístupné pouze pro čtení.

Všechna nastavení ověřte z vytvořených účtů. Postup dokumentujte screenshoty a kopiemi příkazů.

Úkol zpracujte individuálně!

Elaborát do e-learningu nahrávejte ve **formátu PDF**.

Příprava prostředí

Vzhledem k tomu, že cvičení probíhá ve sdíleném virtuálním stroji, bylo velké riziko, že již někdo cvičení vypracoval přede mnou. Proto jsem si pomocí souboru `/etc/passwd` zjistil, co za uživatele bylo na systému přítomno. A skutečně jsem dospěl k tomu, že přede mnou již tento úkol někdo vypracoval. Tyto uživatele jsem tedy důkladně smazal.

```
student@virta:~$ sudo userdel abednar
student@virta:~$ sudo userdel bcoufal
student@virta:~$ sudo userdel cduda
student@virta:~$ sudo userdel degrt
student@virta:~$ sudo userdel efilova
```

Smazání existujících uživatelů od předchozího uživatele

Vytvoření uživatelů

Jakožto první krok jsem vytvořil skupinu pomocí příkazu `groupadd`. Ten přijímá jediný parametr, a tím je název skupiny.

```
student@virta:~$ sudo groupadd uzivatele
```

Vytvoření skupiny "uzivatele"

Vytvořením skupiny ještě před vytvořením uživatelů mi dá tu výhodu, že mohu skupinu přiřadit uživatelům rovnou při jejich vytváření a nemusím tak po jejich vytvoření je explicitně definovat před `usermod`. Vytváření uživatelů pak již probíhá přes příkaz `useradd`, kterému jsem kromě názvu uživatele dodal také dva příznaky:

- `-m` pro okamžité vytvoření domovského adresáře
- `-g` pro přiřazení do skupiny `uzivatele`

```
student@virta:~$ sudo useradd -m -g uzivatele adam.bednar
student@virta:~$ sudo useradd -m -g uzivatele bohumil.coufal
student@virta:~$ sudo useradd -m -g uzivatele cyril.duda
student@virta:~$ sudo useradd -m -g uzivatele david.egrt
student@virta:~$ sudo useradd -m -g uzivatele eva.filova
```

Vytvoření uživatelů

Po vytvoření uživatelských účtů bylo potřeba jim přidat výchozí hesla. Pro každého uživatele jsem nastavil heslo `123456` pomocí příkazu `passwd` (password) a následně nastavil jejich expiraci na okamžitou pomocí příznaku `-e`.

```
student@virta:~$ sudo passwd -e adam.bednar
passwd: password expiry information changed.
student@virta:~$ sudo passwd -e bohumil.coufal
passwd: password expiry information changed.
student@virta:~$ sudo passwd -e cyril.duda
passwd: password expiry information changed.
student@virta:~$ sudo passwd -e david.egrt
passwd: password expiry information changed.
student@virta:~$ sudo passwd -e eva.filova
passwd: password expiry information changed.
```

Nastavení expirace hesel



Vytvoření adresářů

Vytváření adresářů probíhá pomocí příkazu `mkdir` (make directory), který při vytváření adresáře kromě cesty může také přijímat příznak `-m`, kterému lze předat numerickou reprezentaci masky oprávnění.

Pro jednotlivé adresáře jsem zvolil následující masky:

groupshare	0740
publicshare	0766
readonly	0444

Jednotlivé adresáře měly být dle zadání umístěny v domovských adresářích uživatelů, tudíž po vypsání jednotlivých příkazů vypadalo vytvoření adresářů takto:

```
student@virta:/home$ sudo mkdir -m 0740 /home/adam.bednar/groupshare
student@virta:/home$ sudo mkdir -m 0740 /home/bohumil.coufal/groupshare
student@virta:/home$ sudo mkdir -m 0740 /home/cyril.duda/groupshare
student@virta:/home$ sudo mkdir -m 0740 /home/david.egrt/groupshare
student@virta:/home$ sudo mkdir -m 0740 /home/eva.filova/groupshare
```

Vytvoření adresářů groupshare

```
student@virta:/home$ sudo mkdir -m 0766 /home/adam.bednar/publicshare
student@virta:/home$ sudo mkdir -m 0766 /home/bohumil.coufal/publicshare
student@virta:/home$ sudo mkdir -m 0766 /home/cyril.duda/publicshare
student@virta:/home$ sudo mkdir -m 0766 /home/david.egrt/publicshare
student@virta:/home$ sudo mkdir -m 0766 /home/eva.filova/publicshare
```

Vytvoření adresářů publicshare

```
student@virta:~$ sudo mkdir -m 0444 /home/adam.bednar/readonly
student@virta:~$ sudo mkdir -m 0444 /home/bohumil.coufal/readonly
student@virta:~$ sudo mkdir -m 0444 /home/cyril.duda/readonly
student@virta:~$ sudo mkdir -m 0444 /home/david.egrt/readonly
student@virta:~$ sudo mkdir -m 0444 /home/eva.filova/readonly
```

Vytvoření adresářů readonly





Tím, že jednotlivé adresáře byly vytvořeny v režimu sudo, stal se root jejich vlastníkem. To je pro případ složky groupshare nežádoucí a tudíž bylo zapotřebí změnit jejich vlastníka na daného uživatele, v jehož domovském adresáři se daná složka nacházela.

```
student@virta:/home$ sudo chown adam.bednar:uzivatele
/home/adam.bednar/groupshare
student@virta:/home$ sudo chown bohumil.coufal:uzivatele
/home/bohumil.coufal/groupshare
student@virta:/home$ sudo chown cyril.duda:uzivatele
/home/cyril.duda/groupshare
student@virta:/home$ sudo chown david.egrt:uzivatele
/home/david.egrt/groupshare
student@virta:/home$ sudo chown eva.filova:uzivatele
/home/eva.filova/groupshare
```

Změna vlastníka adresáře groupshare

Ověření nastavení

K ověření expirace hesla došlo hned při prvním přihlášení. Po přihlášení k uživateli cyril.duda jsem byl vyzván k zadání aktuálního hesla a k zadání nového hesla. Po změně bylo ssh spojení přerušeno, načež při dalším přihlášení s novým heslem vše fungovalo tak, jak se předpokládalo.

```
kevin.danek@a0322:~$ ssh cyril.duda@192.168.56.2
cyril.duda@192.168.56.2\'s password:
You are required to change your password immediately (administrator enforced).
You are required to change your password immediately (administrator enforced).
Last login: Tue Oct 17 15:07:56 2023 from 192.168.56.1
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for cyril.duda.
Current password:
New password:
Retype new password:
passwd: password updated successfully
Connection to 192.168.56.2 closed.
kevin.danek@a0322:~$ ssh cyril.duda@192.168.56.2
cyril.duda@192.168.56.2\'s password:
$ pwd
/home/cyril.duda
```

Změna hesla nově vytvořeného uživatele



Závěr

Tvorba uživatelských účtů s minimálními oprávněními a jednorázovými hesly při vytvoření jsou základem dobré praxe, která je dnes již prakticky všude napříč sysadmin světem. Pro usnadnění správy oprávnění jsou právě skupiny skvělým nástrojem, protože nám umožňují centralizovaně spravovat práva pro více uživatelů najednou a ušetřit si tak haldu práce. Celkově lze říci, že správa uživatelů a práv má klíčový význam pro zabezpečení informačních systémů a ochranu dat, což je v dnešní době nezbytné vzhledem k rostoucím kybernetickým hrozbám.

Nebudu lhát, když řeknu, že infrastruktura, na které cvičení probíhalo, mě více než trápila. Neustálé záseky shellu, k přihlášení bylo potřeba pomalu provádět obětní rituály a když už se člověku podařilo překonat tyto překážky, naházel mu klacky pod nohy linux samotný. Celkový dojem z toho cvičení bych hodnotil jako hořký.