BEZIT – 7. cvičení

Radek Janoštík

Univerzita Palackého v Olomouci

28. 3. 2024

Zapomenuté/ztracené heslo

- Přijde za vámi *kamarád*, že zapomněl heslo do svého Linuxu a nemůže na něj přijít
  - Na disku má ale jedinou kopii svojí bakalářské práce těsně před odevzdáním
  - Potřebuje to rychle a nemáte po ruce šroubovák na vytažení pevného disku

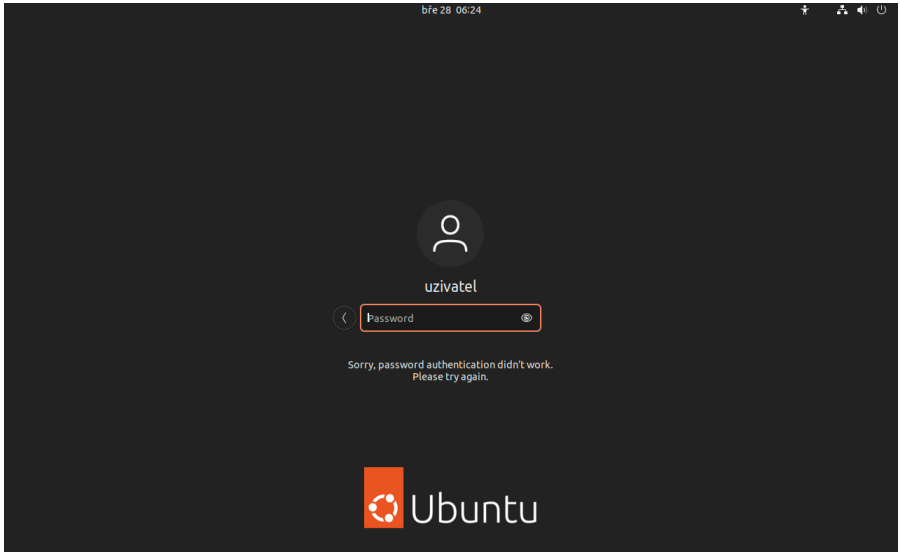
Zapomenuté/ztracené heslo

- Přijde za vámi *kamarád*, že zapomněl heslo do svého Linuxu a nemůže na něj přijít
  - Na disku má ale jedinou kopii svojí bakalářské práce těsně před odevzdáním
  - Potřebuje to rychle a nemáte po ruce šroubovák na vytažení pevného disku
- Je možné se k datům dostat?
- Je možné mu změnit heslo?

Zapomenuté/ztracené heslo

- Přijde za vámi *kamarád*, že zapomněl heslo do svého Linuxu a nemůže na něj přijít
  - Na disku má ale jedinou kopii svojí bakalářské práce těsně před odevzdáním
  - Potřebuje to rychle a nemáte po ruce šroubovák na vytažení pevného disku
- Je možné se k datům dostat?
- Je možné mu změnit heslo?
- Co vše by nám v tom mohlo zabránit?

Zapomenuté/ztracené heslo – ilustrační obrázek

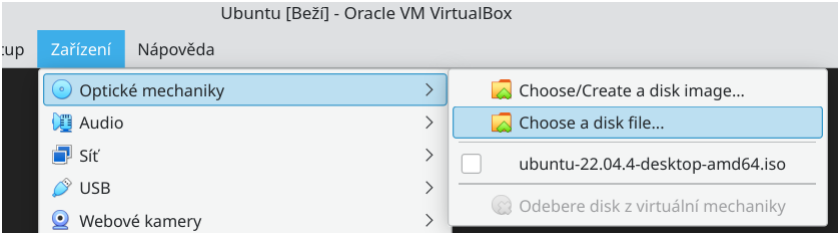


Fyzický přístup

- S fyzickým přístupem ke stroji toho zmůžeme opravdu hodně
- Můžeme nabootovat *live* distribuci (nějakého) Linuxu a k datům se dostat
  - Např. samotné instalační médium Ubuntu umí *live*
  - Specializované live distribuce Slax, SystemRescue
  - Doporučuji použít „co nejpodobnější“ systém
- Distribuce musí umět použitý souborový systém
- Podobný postup lze použít i pro záchranu „smazaných dat“ a částečnou obnovu
  - Případně úpravy bootladeru

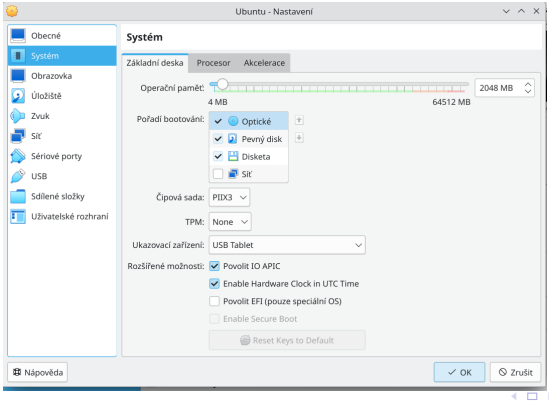
Přístup k datům – ukázka

- V reálném světě je dobré mít live linux neustále s sebou (flashdisk na klíčích)
- Většina management konzolí serverů umožňuje na dálku připojit `.iso` soubor
- Podobně je na tom i VirtulBox



Přístup k datům – pořadí bootování

- Většinou se ihned bootuje z pevného disku
- Je potřeba změnit pořadí/vynutit boot z iso souboru/flash disku
- Reálný stroj: BIOS
- VirtualBox



Přístup k datům – boot

- Po zavedení live distribuce se objeví její bootloader
  - Pro instalátor Ubuntu zvolíme Try/Install Ubuntu
  - Poté pouze Try ubuntu
- Naběhne nám live distribuce linuxu, která běží pouze v operační paměti RAM
- Avšak nic nám nebrání připojit pevný disk a bakalářskou práci získat
- Zjistíme si všechny pevné disky: `lsblk`

```
loop8     7:8    0  40.4M  1 loop /snap/snapd/20671
sda       8:0    0  38.7G  0 disk
├─sda1    8:1    0     1M  0 part
├─sda2    8:2    0   513M  0 part
└─sda3    8:3    0  38.2G  0 part
sr0      11:0    1   4.7G  0 rom  /cdrom
root@ubuntu:/home/ubuntu#
```

- A ten si připojíme příkazem `mount /dev/sda3 /mnt/disk`

Heslo

- Je možné zjistit aktuální znění hesla?

Heslo

- Je možné zjistit aktuální znění hesla?
- Ne, pouze jeho hash
  - Údaje o uživatelích najdeme v `/etc/passwd/`
  - Hashe jejich hesel v `/etc/shadow`

Heslo

- Je možné zjistit aktuální znění hesla?
- Ne, pouze jeho hash
  - Údaje o uživatelích najdeme v `/etc/passwd/`
  - Hashe jejich hesel v `/etc/shadow`
- Pro změnu hesla nestačí připojit jen datový disk potřebujeme mít funkční celý ekosystém (programy, zařízení, . . .)
- Můžeme „naroubovat“ zařízení,tmp,proc,sys z běžící live distribuce na cílovou a pak se do ní „vnořit“

Heslo

- Je možné zjistit aktuální znění hesla?
- Ne, pouze jeho hash
  - Údaje o uživatelích najdeme v `/etc/passwd/`
  - Hashe jejich hesel v `/etc/shadow`
- Pro změnu hesla nestačí připojit jen datový disk potřebujeme mít funkční celý ekosystém (programy, zařízení, . . .)
- Můžeme „naroubovat“ zařízení,tmp,proc,sys z běžící live distribuce na cílovou a pak se do ní „vnořit“
- K tomu nám poslouží `chroot`

Chroot

- Připojíme všechny potřebné adresáře

```
mount --rbind /dev /mnt/disk/dev
mount --make-rslave /mnt/disk/dev
mount -t proc /proc /mnt/disk/proc
mount --rbind /sys /mnt/disk/sys
mount --make-rslave /mnt/disk/sys
mount --rbind /tmp /mnt/disk/tmp
mount --bind /run /mnt/disk/run
```

- Poté se již můžeme „vnořit“ do cílového systému

```
chroot /mnt/disk /bin/bash
```

- A můžeme heslo změnit

Úkol – „Co vše by mohl udělat útočník“

- Importujte systém `https://apollo.inf.upol.cz/~janostik/data/Ubuntu.ova`
  - 6GB stažení
  - $\approx$ 16GB na disku

1. Zjistěte hash hesla "uzivatel"+ jakým algoritmem to bylo hashováno
2. Zjistěte alespoň 4 přístupové údaje, které uživatel "uzivatel"používá. Tzn. jakou službu uživatel využívá (server) a přístupové údaje k ní.
3. Jak se dá změnit heslo uživatele zpět (bez jeho znalosti) tak, aby to uživatel nepoznal?
4. Jak byste se podobně dostali do (nezašifraných) windows / MacOS? Popřípadě alespoň k nějakým datům?
5. Navrhněte obranu