Bezpečnosť Počítačových systémov a Dát

Cvičenie 02 - riadenie prístupu v prostredí Linux

Ústav informatiky, PF UPJŠ v Košiciach

EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja

OPERAČNÝ PROGRAM
ĽUDSKÉ ZDROJE

MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje

www.minedu.sk www.employment.gov.sk/sk/esf/ www.itakademia.sk

Virtualbox image Debian 9.5.0 – **`BPD02.ova`**

```
root:0bpd2
bpd01:bpd01
bpd02:bpd02
bpd03:bpd03
bpd04:bpd04
bpd05:bpd05
```

EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja
OPERAČNÝ PROGRAM ĽUDSKÉ ZDROJE
MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY
UNIVERZITA MATEJA BELA V BANSKEJ BYSTRICI

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje

www.minedu.sk www.employment.gov.sk/sk/esf/ www.itakademia.sk

Discretionary Access Control prístupové práva k súborom

- User, Group, Other
- Read, Write, eXecute

EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja
OPERAČNÝ PROGRAM ĽUDSKÉ ZDROJE
MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY
Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje
www.minedu.sk www.employment.gov.sk/sk/esf/ www.itakademia.sk

Discretionary Access Control prístupové práva k súborom

- User, Group, Other
- Read, Write, eXecute
- setuid, setgid, sticky bit (Special File Permissions)

chmod 1755 *priecinok*, **umask**

chmod u=rx,g+sx,o-w *priecinok*

chown *pouzivatel*:*skupina subor*

EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja
OPERAČNÝ PROGRAM ĽUDSKÉ ZDROJE
MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY
UNIVERZITA MATEJA BELA V BANSKEJ BYSTRICI

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje

www.minedu.sk www.employment.gov.sk/sk/esf/ www.itakademia.sk

Discretionary Access Control prístupové práva k súborom

- User, Group, Other
- Read, Write, eXecute
- setuid, setgid, sticky bit (Special File Permissions)

  chmod 1755 *priecinok*, **umask**

  chmod u=rx,g+sx,o-w *priecinok*

  chown *pouzivatel*:*skupina subor*

- attributes

  lsattr *subor*

  chattr +i *subor*, **chattr** -a *subor*

EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja
OPERAČNÝ PROGRAM ĽUDSKÉ ZDROJE
MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY
UNIVERZITA MATEJA BELA V BANSKEJ BYSTRICI

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje

www.minedu.sk www.employment.gov.sk/sk/esf/ www.itakademia.sk

Access Control Lists
`apt install acl`

- partícia musí byť pripojená s príznakom acl (`/etc/fstab`, dnes defaultné nastavenie)

  `mount` `-o acl` *`particia`*

  `tune2fs` `-l` *`/dev/sda1`* `|` **`grep`** `acl`

- zobrazenie práv

  `getfacl` *`subor`*

- nastavenie práv

  `setfacl` `-m g:`*`skupina`*`:r` *`subor`*

```
drwxr-xr-x+ 2 root root 4096 Oct  2 10:20 tst
```

EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja
OPERAČNÝ PROGRAM ĽUDSKÉ ZDROJE
MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY
UNIVERZITA MATEJA BELA V BANSKEJ BYSTRICI

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje

www.minedu.sk www.employment.gov.sk/sk/esf/ www.itakademia.sk

Access Control Lists

- nastavenie defaultných práv pre adresár

setfacl –d –m u:*pouzivatel*:rw,g:*skupina*:r *adresar*

- odstránenie všetkých ACL práv

  setfacl –b *subor*

- kopírovanie práv

  getfacl *original* | **setfacl** –M – *novy*

  setfacl –M <(**getfacl** *original*) *novy*

- zálohovanie

  tar -p --acls …

EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja
OPERAČNÝ PROGRAM ĽUDSKÉ ZDROJE
MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY
UNIVERZITA MATEJA BELA

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje

www.minedu.sk www.employment.gov.sk/sk/esf/ www.itakademia.sk

Mandatory Access Control Security Enhanced Linux

- inštalácia SELinuxu

```
apt install selinux-basics selinux-policy-default auditd
```

- aktivovanie SELinuxu

  selinux-activate && reboot

- zistenie a zmena aktuálneho stavu/režimu

  sestatus, getenforce

  setenforce [01], /etc/selinux/config

- audit

  audit2why -al, /var/log/audit/audit.log

  ausearch -m AVC,USER_AVC,SELINUX_ERR -ts today

EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja
OPERAČNÝ PROGRAM ĽUDSKÉ ZDROJE
MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY
UNIVERZITA MATEJA BELA

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje

www.minedu.sk www.employment.gov.sk/sk/esf/ www.itakademia.sk

SELinux Context user:role:type:level

- zobrazenie `unconfined_u:object_r:user_home_t:s0 selinux/`

  ls -Z *subor*

  ps -eZ

- zmena

  chcon -t *typ subor*

  semanage fcontext -a -t *typ subor*

- Obnova

  restorecon -v subor

EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja
OPERAČNÝ PROGRAM ĽUDSKÉ ZDROJE
MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY
UNIVERZITA MATEJA BELA

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje

www.minedu.sk www.employment.gov.sk/sk/esf/ www.itakademia.sk

SELinux Management

- používatelia SELinuxu

```
id -Z
seinfo -u
semanage login -l
```

- role, typy

```
seinfo -r, seinfo -t
```

- nastavenia

```
semanage boolean -l
getsebool -a
```

EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja
OPERAČNÝ PROGRAM ĽUDSKÉ ZDROJE
MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY
UNIVERZITA MATEJA BELA

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje

www.minedu.sk www.employment.gov.sk/sk/esf/ www.itakademia.sk

- kopírovanie

```
cp --preserve=context
```

- zálohovanie

```
tar -p –selinux
```

- štatistika

```
avcstat
```

kontrola označení

```
matchpathcon –V adresar
```

EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja
OPERAČNÝ PROGRAM ĽUDSKÉ ZDROJE
MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY
UNIVERZITA MATEJA BELA V BANSKEJ BYSTRICI

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje

www.minedu.sk www.employment.gov.sk/sk/esf/ www.itakademia.sk