Felhasználói parancs-naplózás és csoportuserek

Kadlecsik József
MTA Wigner FK
kadlecsik.jozsef@wigner.mta.hu

Tartalom

- Parancs-naplózás login szervereken
- Csoportuserek

Parancs-naplózás

- “Felhasználók” milyen parancsokat adnak ki… betörés esetén?
  - Grsec vs “valami más”
- Shell history
  - unset HISTFILE
  - Nem naplózható
- Syslog-ba terelt parancs-naplózás a cél:
  - Shell szinten: Köveshegyi László
  - Preexec vagy trap

bash

- “trap [[arg] sigspec] ….If sigspec is DEBUG, the command arg is executed before every simple command…”

```
trap 'TTY=`tty`;\
  logger -t “$HOSTNAME hist \
        $USER ${TTY##/dev/} $0” \
        “$BASH_COMMAND”' DEBUG
```

tcsh

- “precmd runs just before each prompt is printed….postcmd runs before each command executed”

```
alias postcmd \
  'logger -t “$HOST hist $user $tty $0” \
        ”\!#:q”'
```

zsh

- “preexec: Executed just after a command has been read and is about to be executed.”

```
preexec() {
    logger -t "\$HOST hist \
        $USER ${TTY##/dev/} zsh" "$1"
}
```

2013. szeptember 30.

- Betörés
  - Jelszóval, próbálgatás **nélkül**
    - /tmp/... fájl, zérus mérettel
    - User home dir módosítási dátuma változott
    - /usr/bin/crond processz fut
  - Nincs nyom
    - a history fájlban
    - a naplózó szerveren

Naplózás?

- Nem futtattak **login** shell-t
- Ssh flexibilitás:
  - ForceCommand
    - A specifikált programot hajtja végre a megadott helyett

ForceCommand

```
#!/bin/bash
if [ “$SSH_ORIGINAL_COMMAND” ]; then
  cmd=”$SSH_ORIGINAL_COMMAND”
  login_shell=no
else
  cmd=$SHELL
  login_shell=yes
fi
logger “ssh command: $cmd”
```

ForceCommand, folyt.

```
if [ $login_shell = “yes” ]; then
  shell=${cmd##*/}
  exec -l -a $shell $cmd
else
  exec $SHELL -c “$cmd”
fi
```

Ssh flexibilitás: connection sharing

- Háromféle parancs végrehajtási mód
  - Login shell
  - Parancs argumentum
  - Parancs connection-sharing-en keresztül

```
ssh victim -M -S /tmp/victim-socket
ssh victim -S /tmp/victim-socket cmd
….
ssh -S /tmp/victim-socket -O exit
```

Ssh naplózása: snoopy

- Snoopy, preloaded library az execve() hívások naplózására:
  - Login shell
  - Parancs argumentum
  - Parancs connection-sharing-en keresztül
- Shell-beni naplózás továbbra is szükséges

```
# /etc/default/ssh
export LD_PRELOAD=/lib/snoopy.so
```

Csoportuserek

- Csoportuser
  - account, amihez több személy fér hozzá a jelszó megosztásával
- Céljai
  - Fájl megosztás
  - Közös levélkezelés
  - Közös webfejlesztés

Személyhez kötés

- Csoportuser
  - account, amihez több személy fér hozzá, mindegyik a **saját** felhasználói jelszavával
- Dovecot master user
  - Speciális azonosító: `username*masteruser`
  - Minden accounthoz hozzáfér
- Általánosítsuk PAM modul segítségével

pam-groupuser

- Kétfázisú működés
  - Ha a username `groupuser*masteruser` alakú
    - És groupuser, masteruser létezik
    - És masteruser a groupuser csoport tagja, akkor
  - Hazudjuk be a master user-t autentikációhoz
  - Hazudjuk be a groupuser-t account, session kezeléshez

```
auth required pam_groupuser.so
@include common-auth
auth required pam_groupuser.so second-pass
```

Levelezés

- Dovecot
  - **Nincs** master user aktiválva
  - De * hozzáadva az `auth_username_chars`-hoz
  - És PAM a kétfázisú groupuser modullal
- Roundcubemail
  - Minimális patch, hogy a csoportuser nevével, email címével, stb. jöjjön létre a roundcubemail account.

Fájlműveletek

- Vsftpd
  - FTPS üzemmód
  - És PAM a kétfázisú groupuser modullal

PAM modul forrása

- http://git.wigner.mta.hu