Adminisztratív protokollok ellenőrzési lehetőségei

Höltzl Péter CISA
holtzl.peter@balabit.hu
http://www.balabit.hu/

Miről lesz szó?

Hozzáférés szintek

Mi látszik és mi nem?

Megoldási módok

Elérhető technológiák

Példák

A hozzáférés szintjei

OS

Alkalmazás

Adatbázis

Jogosultsági szintek a-tól z-ig

Példa

Webes alkalmazás:

- Szerver admin
- Webmester
- DB admin
- DB user
- Iktató admin
- Iktató felhasználó

Admin mindig van!

Kérdés, tudjuk-e mit csinál?

Példa – Linux

groupadd[4609]: group added to /etc/group: name=proba, GID=1003

groupadd[4609]: group added to /etc/gshadow: name=proba

groupadd[4609]: new group: name=proba, GID=1003

useradd[4613]: new user: name=proba, UID=1003, GID=1003, home=/home/proba, shell=/bin/bash

passwd[4620]: pam_unix(passwd:chauthtok): password changed for proba

chfn[4621]: changed user 'proba' information

Példa

Nem mindig van napló:

- Vi /etc/passwd
- Vi /etc/group
- visudo

Egy hack

File változás figyelése:

- Csak napló
- Tartalom nem

Példa

type=SYSCALL msg=audit(1320920870.653:34): arch=c000003e syscall=2
success=yes exit=3 a0=c3f3a0 a1=241 a2=120 a3=0 items=1 ppid=998 pid=1037
auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0
tty=pts1 ses=4294967295 comm="vi" exe="/usr/bin/vim.tiny" key=(null)

type=CWD msg=audit(1320920870.653:34): cwd="/root"

type=PATH msg=audit(1320920870.653:34): item=0 name="/etc/sudoers"
inode=262413 dev=08:01 mode=0100440 ouid=0 ogid=0 rdev=00:00

type=SYSCALL msg=audit(1320920870.663:35): arch=c000003e syscall=90
success=yes exit=0 a0=c3f3a0 a1=8120 a2=48fbf7 a3=7fffaf097ca0 items=1
ppid=998 pid=1037 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0
sgid=0 fsgid=0 tty=pts1 ses=4294967295 comm="vi" exe="/usr/bin/vim.tiny"
key=(null)

type=CWD msg=audit(1320920870.663:35): cwd="/root"

type=PATH msg=audit(1320920870.663:35): item=0 name="/etc/sudoers"
inode=262413 dev=08:01 mode=0100440 ouid=0 ogid=0 rdev=00:00

Hátrányok

Értelmezhető?

Bonyolult

Csak a kiemelt események láthatóak!

Eltüntethető

Leállítható

Megoldás

Távoli elérés rögzítése

Példa

SSH video

RDP video

Piaci megoldások

Agentek

Snifferek

Jumphostok

Proxyk

Agentek

Telepítés

Rendszer módosítás

Passzív

Natív kliens

Minden protokoll funkció

Megkerülhető

Snifferek

Port tükrözés

~~Rendszer módosítás~~

Passzív

~~Csatorna ellenőrzés~~

Natív kliens

Megkerülhetetlen

~~Minden protokoll funkció~~

Jumphostok

Kapcsolat a bastion-ról

~~Rendszer módosítás~~

~~Natív kliens~~

~~Teljes funkcionalitás~~

„Bármilyen” protokoll

~~Minden protokoll funkció~~

Proxyk

Teljes protokoll értelmezés

Aktív

Natív kliens

~~Rendszer módosítás~~

Csatorna és paraméter kontroll

Csatorna kontroll

Csatorna → Funkcionalitás

- Fájl átvitel
- TCP port átvitele
- X11
- Eszköz átvitel

Példa

Csatorna engedélyezés

Csatorna paraméter kontroll

Fájl transzfer visszajátszás

Köszönöm a figyelmet!

Höltzl Péter CISA
holtzl.peter@balabit.hu
http://www.balabit.hu/