IT ZH-biro zsofia

Katologus kereses, kataloguson belul, nem root a felhasznalo

find /root/86344/ -not -user root > /root/86344.ans

Felhasználói fiók keszites, jelszo zarolasa

useradd user86315

passwd -l user86315

Alairas eldontes

openssl dgst -verify /root/(név)-(szám).pub.pem -signature /root/contract-(szám).sha256.signature /root/contract-(szám).txt

Ahol Verified OK: echo (név) > /root/(szám).ans

**openssl dgst -verify csanatpub -sha256 -signature document.sign document.txt** – authenticate

állomány letoltes, titkosított fájlrendszer, katalogusba masolas, jelszo

letöltés a megadott paranccsal

losetup -f /5d3a8e1b

cryptsetup luksOpen /dev/loop0 loop

-Enter passphrase for /5d3a8e1b: 5d3a8e1b

mnt /dev/mapper/loop /mnt

ls /mnt

cp /mnt/070f /root

cp -r /mnt/lost+found/ /root

kulccsal valo visszfejtes, inicializáló vektorral, aes-128-cbc algoritmus

openssl aes-128-cbc -d -in /root/86261.enc -K 86261 -iv 0 > /root/86261.txt

**vagy**

openssl aes-128-cbc –K pelda –iv 0 –d –in pelda.enc –out pelda.txt

openssl [algoritmus] -d -iv [inicializáló vektor szám] -K [kulcs] -in [filename.enc] -out [filename.txt]

openssl aes-128-cbc -d -iv 0 -K 262826 -in 262826.enc -out 262826.txt

jelszóval visszafejtes, des-ede algoritmus

openssl des-ede -d -i /root/86257.enc -k 86257 > /root/86257.txt

**vagy**

openssl des-ede –d –in pelda.enc –K –iv –out pelda.txt

alairas privát kulccsal, SHA 256 hash függvény

ctrl+c feladat kulcs

nano kulcs <- ctrl+v

openssl dgst -sign [kulcs] -sha256 -out [filename.sign] [filename.txt]

openssl dgst -sign kulcs -sha256 -out /root/262826.sign /root/262826.txt

openssl dgst -sign pelda.txt -sha256 -out pelda.sign pelda.txt

openssl dgst -verify key.pem.pub -sha256 -signature pelda.sign pelda.txt

jogosultságait csak olvasható

chmod 444 /root/86237.txt

jogosultság atallitas, USER ACL, operator felhasználó olvashatja csak

setfacl -m u:operator:r /root/86224.txt

txt állomány tulajdonosa  operator felhasználó

chown operator /root/86211.txt

bajt méretű  állomány

dd if=/dev/zero of=/root/86198.dat bs=861980 count=1

bites RSA kulcs generalas,pem allomanyba mentes, privat kulcskent

openssl genpkey -algorithm RSA -out pelda.pem -pkeyopt rsa\_keygen\_bits:2048

openssl genpkey -algorithm RSA -pkeyopt rsa\_keygen\_bits:1024 -out /root/86191.pem

**vagy**

openssl genpkey -algorithm RSA -out pelda.pem -pkeyopt rsa\_keygen\_bits:2048

openssl rsa -in pelda.pem -pubout -out key.pem.pub

ssh-keygen -f key.pem.pub -e -m pkcs8

meghajtora,sdc1 partíció, formazas ext2 fájlrendszerrel, katalogusba csatolas, olvashatokent

fdisk /dev/sdc

sok enter

mkfs.ext2 /dev/sdc1

mount -o ro /dev/sdc1

**vagy**

fdisk /dev/sdb

cryptsetup luksFormat /dev/sdb1

**és/vagy**

cryptsetup luksOpen /dev/sdb1 enc-home

mkfs.ext2 /dev/mapper/enc-home

mount /dev/mapper/enc-home /mnt/

privát kulcs tulajdonosa a root felhasználó nevében bejelentkezhet

cat > kk egesz kulcs

mkdir .ssh

ssh-keygen -y -f kk >.ssh/authorized\_keys

stat .ssh

stat .ssh/authorized\_keys

katalógust root katalóguson belül, amelyen a sticky bit használatban van

find /root/168171/ -perm /1000 > /root/160171.ans

operator felhasznalo, jelszo lejar, jelszo valtas

change operator -M 100

change operator -d 2021-04-15

curl paranccsal fajl letoltes, titkositott fajlrenszer, mappaba masolas

letöltés a megadott paranccsal

losetup -f /5d3a8e1b

cryptsetup luksOpen /dev/loop0 loop

-Enter passphrase for /5d3a8e1b: 5d3a8e1b

monut /dev/mapper/loop0 /mnt

ls /mnt

cp /mnt/\* /root

cp -r /mnt/lost+found/ /root

jogosultsag valtoztatas a rooton -r--rw-- T

chmod 3470 /root/160101.txt

ACL bejegyzesek torlese

setfacl -b /root/160093.txt

tulajdonjog valtoztatas, user – operator, group - users

chown operator:users /root/160076.txt

70 bajt masolas

dd if=/root/160067.dat of=/root/160067.part bs=70 count=1

1024 bit RSA kulcs, PKCS8 privat kulcs

openssl genpkey -algorithm RSA -pkeyopt rsa\_keygen\_bits:1024 -out /root/86191.pem

titkositott xfs filerenszer keszitese , mount directory

cryptsetup luksFormat /dev/sdc

Jelszó megadása

cryptsetup luksopen /dev/sdc x

mkfs.xfs /dev/mapper/x

unmount /mnt/

mount /dev/mapper/x /mnt

user falhasznalo keszites, minimum es maximum naponta jelszo valtas

useradd userXXXX

chage –m 10 –M 20 userXXXX

txt állomány jogosultsaga csak olvashato

chmod a+r pelda.txt vagy chmod ugo+r pelda.txt

txt állomány titkositas, nyilvános kulccsal

openssl des-ecb -in pelda.txt -K pelda.key.pub -out pelda.enc

openssl des-ecb -d -in pelda.enc -K pelda.key.pub

home mappaba beallitas

usermod -d /home/u-70096 user-70096

txt fájlt, group, sticky bit

chmod u=,g=rwx,o=,o+t 70299.txt

Megjegyzés (t:stickybit s:setuidbit)

jelszo lejarta előtt valamennyi nappal figyelmeztetes

chage -W 10 user-70259

user felhasználó hozzaadas group csoporthoz

useradd user-70228

groupadd group-70228

usermod -aG group-70228 user-70228

UID azonosító megvaltoztatasa felhasználónak

usermod -u 1234 user-70215

RSA kulcspár keszites , publikus kulccsal titkositas

openssl genrsa -out /root/70199.pem

openssl rsa -in 70199.pem -out 70199.pub–pubout

openssl rsautl -encrypt -inkey 70199.pem -in 70199.txt -out 70199.enc

felhasználónak írási jog txt fájlon

touch /root/70192.txt

setfacl -m user:user-70192:w /root/70192.txt

root mappa keszites, user ACL bellitasa minden jogra

mkdir 70144

setfacl -dm user:user-70144:rwx /root/70144

maszkolas, , minden újonnan létrejövő fájl és mappa 0640-es jogosultság

umask 137

txt fájlt csak a tulajdonos tud olvasni, sticky bit

chmod 400 34484.txt

chmod o+t 34484.txt

, felhasznalo fiok lejar Account lejar

chage -E 2021-06-13 user-34465

user felhasználónak olvasasi és irasi joga egy txt fajlon.

setfacl -m u:user-34374:rw 34374.txt

titkosított fájlrendszer tárolására meghajtó, új partíció LUKS

fdisk /dev/sdb

cryptsetup luksFormat /dev/sdb1

RSA privát-publikus kulcspár, alairas

openssl genpkey -algorithm RSA -out key.pem -pkeyopt rsa\_keygen\_bits:2048

openssl rsa -in key.pem -pubout -out key.pem.pub

openssl dgst -sign key.pem -sha256 -out document.sign document

txt fájlt titkosita, DES CBC-vel, jelszóval

openssl des-cbc -k it34306 -in 34306.txt -out 34306.enc

txt fájl tulajdonosa user

chown user 34289.txt

felhasznalo keszites xy neven

useradd xy

txt állomány alairasa privát kulccsal, SHA 256 hash függvény.

***openssl dgst -sign pelda.txt -sha256 -out pelda.sign pelda***

***openssl dgst -verify key.pem.pub -sha256 -signature pelda.sign pelda***

privát kulcs tulajdonosa a root felhasználó nevében bejelentkezhet

cat >ppkey beleirányítás

ssh-keygen -e -m pem -f ppkey

chmod 400 ppkey

ssh-keygen -e -m pem -f ppkey > pubkey

ssh-keygen -i -m pem -f pubkey > sshkey

mkdir /root/.ssh/

cat sshkey >> /root/.ssh/authorized\_keys

chmod 700 .ssh/

chmod 600 .ssh/authorized\_keys

**két jelszóváltoztatás között legalább x napnak kelljen eltenie**

chage –m 10 user user-70256

**belepes SSH segítségével, jelszo nelkul**

ssh-keygen (lot of enters)

mkdir /home/user-70163/.ssh

chown user-70163:user-70163 /home/user-70163/.ssh

cat /root/.ssh/id\_rsa.pub >> /home/user-70163/.ssh/authorized\_keys

chown user-70163:user-70163 /home/user-70163/.ssh

**RSA kulcspárt, titkositas privát kulcs felhasználásával**

openssl genrsa –out /root/70202.pem

openssl rsa –in /root/70202.pem –out /root/70202.pub-pubout

openssl rsautl –sign –inkey /root/70202.pem –in /root/70202.txt –out /root/70202.enc

(openssl rsautl –encrypt –inkey /root/70202.pub –in /root/70202.txt –out /root/70202.enc –pubin

**.img fájlt titkosítása, loop device-ként, LUKS formatumban**

losetup –f /root/70137.img

cryptsetup luksFormat /dev/loop0

txt fájlt csak a tulajdonos tudja írni, setuid bitet.

chmod 4200 /root/35003.txt

felhasználónak csak futtatási joga legyen egy fajlon

setfacl -m user-34893:x /root/34893.txt

DES CBC segítségével titkositas, inicializációs vektorral

openssl des-cbc -K 0123456789ABCDEF -iv 0 -in /root/34831.txt -out /root/34831.enc

img fájlt titkosítása, LUKS formátum, majd megnyitja titkos néven, ext4 fájlrendszert, loop device-ként

lsblk -f --> Megnézni, hogy melyik szaron kell csinálni

losetup -f /[amitmegad, valamelyik loop]

cryptsetup luksFormat /dev/[amelyiken\_loopon\_lesz] -> Ahol nincs crypto\_LUKS szöveg (vagy bármilyen más szöveg)

cryptsetup luksOpen /dev/[amelyiken\_loopon\_lesz] [amilyen nevet megad]

mkfs.ext4 /dev/mapper/[amilyen nevet megad] --> Lehet ext4 is akár, vagy bármi

mkdir /root/189522

mount /dev/mapper/[amitmegad] [és amelyik mappába] --> Ez a titkosított

fajl dekodolasa jelszó használatával és a des-ede algoritmussal, pbkdf1-t 1000 iterációval

openssl des-ede -k 189342 -iv 0 -iter 1000, -pbkdf2 -in /root/189342.txt -out /root/189342.enc

Dekodolas privát kulcs segítségével

**nano fajl.txt -belemasolni a kodot**

**openssl pkeyutl –decrypt –inkey fajl.txt –in** /root/13848.enc  **-out** /root/13848.txt

**tulajdonos tudjon a fajllal bármit csinálni ,setuid bitet.**

* + • chmod u=rwx,g=,o=,u+s /root/70302.txt

**felhasználónak csak írási joga legyen**

setfacl -m user:user-70192:w /root/70192.txt

**uj csoportot letrehozasa**

groupadd newgroup-70073

**onalairt tanusitvany**

**openssl req -x509 -nodes -days 365 -newkey rsa:3072 -keyout /etc/ssl/my-company.eu -out /root/my-comapny.crt**