IT Security ZH-hoz

1. **Videó**

A képen szöveg látható

Automatikusan generált leírás



Keressem meg azt a katalógust a /root/39834/ katalóguson belül, amelynek nem a root felhasználó a tulajdonosa. A katalógus teljes elérési útját írja a /root/39834.ans fájlba.

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

A képen szöveg látható

Automatikusan generált leírás



Készítsen egy user39825 felhasználói fiókot, majd zárolja annak jelszavát!

useradd user86315

passwd -l user86315

A képen szöveg látható

Automatikusan generált leírás



Döntse el, hogy a /root/contract-39796.txt állományt Anne, Bob, Carol, Daniel vagy Eve írta-e alá!

Az aláírás SHA 256 hash algoritmussal készült és a /root/contract-39796.sha256.signature állományban található.

Anne nyilvános kulcsa /root/Anne-39796.pub.pem

Bob nyilvános kulcsa /root/Bob-39796.pub.pem

Carol nyilvános kulcsa /root/Carol-39796.pub.pem

Daniel nyilvános kulcsa /root/Daniel-39796.pub.pem

Eve nyilvános kulcsa /root/Eve-39796.pub.pem

Az aláíró nevét írja a /root/39796.ans fájlba.

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

A képen szöveg látható

Automatikusan generált leírás



Az alábbi parancs segítségével töltse le a db2b5fdd állományt, amely egy titkosított fájlrendszert tartalmaz.

curl -o /db2b5fdd https://progcont.hu/docs/IT-Security/loop/db2b5fdd

Masolja a fájlrendszer tartalmát a /root katalógusba. A fájlrendszer eléréshez szükséges jelszó: db2b5fdd

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

A képen szöveg látható

Automatikusan generált leírás



Fejtse vissza az 13970 kulccsal és 0 inicializáló vektorral aes-128-cbc algoritmus segítségével titkosított /root/13970.enc állományt. Az eredményt /root/13970.txt állományban tárolja.

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

A képen szöveg látható

Automatikusan generált leírás



Fejtse vissza az 39721 jelszóval des-ede algoritmus segítségével titkosított /root/39721.enc állományt. Az eredményt /root/39721.txt állományban tárolja.

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

A képen szöveg, levél látható

Automatikusan generált leírás



Írja alá a /root/13940.txt állományt a következő privát kulccsal. Használjon SHA 256 hash függvényt. Az aláírás a /root/13940.sign állományba kerüljön!

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

A képen szöveg látható

Automatikusan generált leírás



Állítsa át a /root/39704.txt állomány jogosultságait úgy, hogy csak olvasható legyen.

chmod 444 /root/86237.txt

A képen szöveg látható

Automatikusan generált leírás



Állítsa át a /root/39691.txt állomány jogosultságait egy új USER ACL bejegyzés segítségével úgy, hogy az operator felhasználó olvashassa. (Mást ne változtasson az állományon, több jogot ne adjon.)

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

A képen szöveg látható

Automatikusan generált leírás



Állítsa át a /root/13908.txt állomány attribútumait úgy, hogy tulajdonosa az operator felhasználó legyen. (Mást ne változtasson az állományon.)

chown operator /root/86211.txt

A képen szöveg látható

Automatikusan generált leírás



Készítsen egy 138990 bájt méretű /root/13899.dat nevű állományt.

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

**vagy**

fallocate –l 138990 pelda.dat





Generáljon egy 2048 bites RSA kulcsot és mentse el a /root/13887.pem állományba PKCS8 szerinti privát kulcsként

c

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

A képen szöveg látható

Automatikusan generált leírás



Készítsen az /dev/sdc meghajtóra egy /dev/sdc1 partíciót. Formázza ext2 fájlrendszerrel, majd csatolja fel a /mnt katalógusba, csak olvashatóként.

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/

A képen szöveg, képernyőkép, hírlap látható

Automatikusan generált leírás



Érjük el, hogy az alábbi privát kulcs tulajdonosa a root felhasználó nevében bejelentkezhessen.

cat > kk egesz kulcs

mkdir .ssh

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

stat .ssh

stat .ssh/authorized\_keys

**2. Videó**

A képen szöveg látható

Automatikusan generált leírás



useradd user160184

su user160184

ssh-keygen

sok enter

ssh-copy-id root@localhost

yes

exit

A képen szöveg látható

Automatikusan generált leírás



Keressem meg azt a katalógust a /root/13856/ katalóguson belül, amelyen a sticky bit használatban van. A katalógus teljes elérési útját írja a /root/13856.ans fájlba.

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

A képen szöveg látható

Automatikusan generált leírás



change operator -M 100

change operator -d 2021-04-15

A képen szöveg látható

Automatikusan generált leírás



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

A képen szöveg látható

Automatikusan generált leírás



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

A képen szöveg látható

Automatikusan generált leírás



chmod 3470 /root/160101.txt





setfacl -b /root/160093.txt

A képen szöveg látható

Automatikusan generált leírás



chown operator:users /root/160076.txt

A képen szöveg látható

Automatikusan generált leírás



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

A képen szöveg látható

Automatikusan generált leírás



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

A képen szöveg látható

Automatikusan generált leírás



cryptsetup luksFormat /dev/sdc

Jelszó megadása

cryptsetup luksopen /dev/sdc x

mkfs.xfs /dev/mapper/x

unmount /mnt/

mount /dev/mapper/x /mnt

**Random Feladatok**

Készítsen egy user13944 felhasználót és állítsa be úgy, hogy minimum 10 de maximum 20 naponta jelszót kelljen váltania.

useradd userXXXX

chage –m 10 –M 20 userXXXX

Állítsa át a /root/13930.txt állomány jogosultságait úgy, hogy csak olvasható legyen.

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

Állítsa át a /root/13921.txt állomány jogosultságait egy új USER ACL bejegyzés segítségével úgy, hogy az operator felhasználó olvashassa. (Mást ne változtasson az állományon, több jogot ne adjon.)

chmod …..+r pelda.txt

Titkosítsa a /root/13832.txt állomány tartalmát a /root/13832.key.pub nyilvános kulcs segítségével. Az eredmény a /root/13832.enc állományba kerüljön!

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

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

Állítsuk be az user-70096 felhasználó home-mappájának a következőt: /home/u-70096. Hozzuk létre a mappát ha nem létezik.

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

Állítsuk be, hogy a /root/70299.txt fájlt csak a group tudjon vele bármit csinálni (senki más ne tudjon semmi mást csinálni vele) és kapcsoljuk be rajta a sticky bitet.

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

Állítsuk be, hogy a user-70259 felhasználót a jelszava lejárta előtt 10 nappal figyelmeztesse.

chage -W 10 user-70259

Adjuk hozzá az user-70228 felhasználót a group-70228 csoporthoz.

useradd user-70228

groupadd group-70228

usermod -aG group-70228 user-70228

Változtassuk meg az UID azonosítóját az user-70215 felhasználónak 1234-re.

usermod -u 1234 user-70215

Készítsen egy privát-publikus RSA kulcspárt az alapbeállításokkal /root/70199.pem és /root/70199.pub neveken, majd titkosítsa a /root/70199.txt fájlt a publikus kulcs felhasználásával. Mentse el a titkosított fájlt /root/70199.enc néven.

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

Állítsuk be, hogy a user-70192 felhasználónak csak írási joga legyen a /root/70192.txt fájlon. Ne változtassuk a többi felhasználó jogosultságait.

touch /root/70192.txt

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

Dekódoljuk a /root/70167.enc fájlt a 70167 kulcs és 0-s inicializációs vektor segítségével. A fájl az aes-128-cbc algoritmussal lett titkosítva. Mentsük el az eredményt /root/70167.txt néven.

Megoldás

openssl aes-128-cbc -d -K 70167 -iv 0 -in /root/70167.enc -out /root/70167.txt

Készítsen egy mappát /root/70144 néven és állítsuk be az ACL-jét úgy, hogy a user-70144 felhasználó automatikusan megkap minden jogot (olvasás-írás-futtatás) ennek a mappának az almappáira és fájljaira. Ne változtassuk a többi felhasználó jogosultságait.

Megoldás

mkdir 70144

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

Maszkolás segítségével állítsuk be, hogy minden újonnan létrejövő fájl és mappa 0640-es jogosultságokkal rendelkezzen.

umask 137

Dekódoljuk a /root/70109.enc állományt a 70109 jelszó és az des-ede algoritmus segítségével. Mentsük el a végeredményt /root/70109.txt néven.

cat /root/70109.txt

openssl des-ede -d -in /root/70109.enc -k 70109

openssl des-ede -d -in /root/70109.enc -k 70109 > /root/70109.txt

**Pentek 08:00**

2020-05-08 08:00 – 2020-05-08 08:41

**Feladatok**

FeladatElérhető: 1Elért: 1

Állítsuk be, hogy a /root/34484.txt fájlt csak a tulajdonos tudja olvasni (senki más ne tudjon semmi mást csinálni vele) és kapcsoljuk be rajta a sticky bitet.

chmod 400 34484.txt

chmod o+t 34484.txt

FeladatElérhető: 1Elért: 1

Állítsuk be, hogy a user-34465 felhasználónak 2020.05.18-ától ne legyen hozzáférhető (lejárjon) az accountja.

chage -E 2020-05-18 user-34465

FeladatElérhető: 1Elért: 1

Adjuk hozzá az user-34425 felhasználót a group-34425 csoporthoz.

FeladatElérhető: 1Elért: 1

usermod -a -G group-34425 user-34425

Változtassuk meg az UID azonosítóját az user-34421 felhasználónak 1237-re.

usermod -u 1237 user-34421

FeladatElérhető: 1Elért: 1

Állítsuk be, hogy a user-34374 felhasználónak olvasási és írási joga legyen a /root/34374.txt fájlon. Ne változtassuk a többi felhasználó jogosultságait.

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

FeladatElérhető: 2Elért: 2

Készítsük elő titkosított fájlrendszer tárolására a /dev/sdb meghajtót úgy, hogy egy új partíciót LUKS rendszerűre formázunk rajta.

fdisk /dev/sdb

cryptsetup luksFormat /dev/sdb1

FeladatElérhető: 1Elért: 1

Készítsen egy mappát /root/34341 néven és állítsuk be az ACL-jét úgy, hogy a user-34341 felhasználó automatikusan megkap minden jogot (olvasás-írás-futtatás) ennek a mappának az almappáira és fájljaira. Ne változtassuk a többi felhasználó jogosultságait.

mkdir 34341

setfacl -dm u:user-34341:rwx 34341

FeladatElérhető: 2Elért: 2

Készítsen egy RSA privát-publikus kulcspárt /root/34328.pem és /root/34328.pub nevekkel és írja alá a /root/34328.txt fájlt a segítségükkel. Az aláírásnak adja a /root/34328.sign nevet.

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

FeladatElérhető: 2Elért: 2

Titkosítsuk a /root/34306.txt fájlt DES CBC-vel az it34306 jelszóval. A titkosított fájl neve legyen /root/34306.enc.

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

FeladatElérhető: 1Elért: 1

Állítsuk be az user-34296 felhasználó home-mappájának a következőt: /home/u34296. Hozzuk létre a mappát ha nem létezik.

mkdir

usermod -d /home/u34296/ user-34296

FeladatElérhető: 1Elért: 1

Állítsuk be a /root/34289.txt fájl tulajdonosának az user-34289 felhasználót.

chown 34289.txt user…

FeladatElérhető: 1Elért: 1

Készítsünk egy felhasználót user-34273 néven.

useradd

FeladatElérhető: 1Elért: 1

Maszkolás segítségével állítsuk be, hogy minden újonnan létrejövő fájl és mappa 0464-es jogosultságokkal rendelkezzen.

umask 313

**Feladatok**

Fejtse vissza az 13970 kulccsal és 0 inicializáló vektorral aes-128-cbc algoritmus segítségével titkosított /root/13970.enc állományt. Az eredményt /root/13970.txt állományban tárolja.

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

Fejtse vissza az 13957 jelszóval des-ede algoritmus segítségével titkosított /root/13957.enc állományt. Az eredményt /root/13957.txt állományban tárolja.

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

Készítsen egy user13944 felhasználót és állítsa be úgy, hogy minimum 10 de maximum 20 naponta jelszót kelljen váltania.

***useradd userXXXX***

***chage –m 10 –M 20 userXXXX***

Írja alá a /root/13940.txt állományt a következő privát kulccsal. Használjon SHA 256 hash függvényt. Az aláírás a /root/13940.sign állományba kerüljön!

-----BEGIN PRIVATE KEY-----

MIICdgIBADANBgkqhkiG9w0BAQEFAASCAmAwggJcAgEAAoGBALGxXdQslY2y33Hr

6JBmdQL4fJmDZolEKJIojg9IapEI95SV5gsZb9+K6J+1sJAeq0k4wzm6LNWdMT3n

xDaWM0rN/wvM+MzMDoz2IOep6I/VQMFvq9/kL0iwhM5w6NJtkIfwNJhimw5KsEF7

iAtr9xl+3Gx6VIZ5ZgzpSHOeFspTAgMBAAECgYBpfApgX0s0wCAHZ+06c6g46DxH

gYrIJ+8RvQOALRQeHz2iNk5G/oW8JaEs1lYHaD10jT7PsSbWdKd7wW9onEe7vcfx

miJbcZaXON6pY11BZOVaGgSMWR2/frQVVPH9pdVk5L+UyJfE/kNGgdgAnKU8+jRT

yeMUer8bh5/GSJL8YQJBAONwyYVuOQo2dkVZTtGormh28NDt3o8NK9NaKUlzjS3E

YvzPdABDhjY+kjeA0LhT1xVwFr7MgekGks/EgbKlbbECQQDIAWifEguMgV0fCYB/

gXJTNNqbNgLf3+tQBNru8HCo1Ed4HPscx5tpfZHieXUW63PYbZC/kofMmoZ1e+Dc

mKVDAkBiEuyTIOhvwvRVCyG1vqsWWNOXBDuILAHN7X8IMU+bgKe+pCY9RuDE205p

qJ5YHa8Ni3wDYmRSe4crGG1k/3jBAkEAss3/mGZriLuGYt790AAMEzMnVKdevoLT

PoB4sjCmp2jQVCOko8AXwqGOMKhg85KfyJd7VqlLWrGzD4kmKFEXPQJAEj/QSzkJ

Dmqu2Q+KrIyYSDfWwdFDda6qkH9QHoTQ2aE6RtkShhAShA6EsJdOX2d3tCuSdZ2B

2o0qC6Dvgv2y/A==

-----END PRIVATE KEY-----

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

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

Állítsa át a /root/13930.txt állomány jogosultságait úgy, hogy csak olvasható legyen.

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

Állítsa át a /root/13921.txt állomány jogosultságait egy új USER ACL bejegyzés segítségével úgy, hogy az operator felhasználó olvashassa. (Mást ne változtasson az állományon, több jogot ne adjon.)

***chmod …..+r pelda.txt***

Állítsa át a /root/13908.txt állomány attribútumait úgy, hogy tulajdonosa az operator felhasználó legyen. (Mást ne változtasson az állományon.)

***chown operator pelda.txt***

Készítsen egy 138990 bájt méretű /root/13899.dat nevű állományt.

***fallocate –l 138990 pelda.dat***

Generáljon egy 2048 bites RSA kulcsot és mentse el a /root/13887.pem állományba PKCS8 szerinti privát kulcsként

***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***

Készítsen az /dev/sdc meghajtóra egy /dev/sdc1 partíciót. Formázza ext2 fájlrendszerrel, majd csatolja fel a /mnt katalógusba, csak olvashatóként.

***fdisk /dev/sdb***

***cryptsetup luksFormat /dev/sdb1***

***cryptsetup luksOpen /dev/sdb1 enc-home***

***mkfs.ext2 /dev/mapper/enc-home***

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

Érjük el, hogy az alábbi privát kulcs tulajdonosa a root felhasználó nevében bejelentkezhessen.

-----BEGIN PRIVATE KEY-----

MIICdwIBADANBgkqhkiG9w0BAQEFAASCAmEwggJdAgEAAoGBANCjZa5k9CCKIN0w

eOSzHrJt6OpltytqGozrKij+emNV4988yFo64QpdSVBXGUZN34aYo0mvnMo4B6M3

IQjMQ9NFeVvboTUugzgCL0or0+9GHelK4LaSC0xgMpGO+jvb5dxiqDEE2KVhejau

8HYiAr98VLNQgCHx16ZLvNfgy2rdAgMBAAECgYA523YRHJHOjD981zpPQZTbqjsS

9U4MTgo61eQFJjzOWz0r5PEyhG1vsFrqWpz5sBKygpWVk4uJUGxdyKXyiKKt7VNy

Lxv1HTHgxSTrdu1Gwk7ZSO9eX+AAHNkCU3PMhBdHEy8viaJmt1Dfw31zNePDeUKZ

2GU54Wd3jtYb96IagQJBAPrnXhOA3JvpX4kV3vWCUEYp4ek0wJPjsHjm5VYFHSyv

tzuUmnrYRkJidOVy9FUxrv8zJVfPRfSEZA0l99RMDI0CQQDU4EKnnR38kgrbymMv

bzTL+zC2i4tmcU6zMIbGdtpXJfxv+3ZpS2OTnlHpFRApviRHhLunD6eUnmFXnGK2

90uRAkEAtEferwDegyCyxptyctHJwECD1L9UyG7H9HdjveU6y0sOy77BKReRlE2O

VPe+XCCw7yne4TNLvqAKC/CGHILwWQJAeJ4xZmPCL/BYMr10gdYTJllH+scKz5r4

KtQeKaoCgUrGxHTJXVQYMfaNFvKWW/CfAd8VrM1T+QPcyBWWYXGx4QJBAIxAJocH

OScnZl2qb2ZPHh0C1F+L2PhhymLwJGW9DE7UmNB6xlOpdqLsNE3pfoh23P+zahXu

oNNgdlnYLBmGRiA=

-----END PRIVATE KEY-----

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

Keressem meg azt a katalógust a /root/13864/ katalóguson belül, amelyen a sticky bit használatban van. A katalógus teljes elérési útját írja a /root/13864.ans fájlba.

find /root/13864/ -perm -o=t > /root/13864.ans

find /root/13864/ |wc -l – állományok megszámolása

find /root/13864/ -perm -1000

Készítsen az /dev/sdb meghajtóra egy /dev/sdb1 partíciót, majd készítse elő a partíciót titkosított fájlrendszer fogadására. Ehhez használja a cryptsetup programot és a LUKS formátumot.

***fdisk /dev/sdb***

***cryptsetup luksFormat /dev/sdb1***

Titkosítsa a /root/13832.txt állomány tartalmát a /root/13832.key.pub nyilvános kulcs segítségével. Az eredmény a /root/13832.enc állományba kerüljön!

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

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

IT-Security (minta ZH)

**Állítsuk be, hogy a user-70177 felhasználónak olvasási és írási joga legyen a /root/70177.txt fájlon. Ne változtassuk a felhasználó jogosultságait.**

setfacl –m user:user-70177:rw /root/70177.txt

**Állítsuk be, hogy a /root/70287.txt fájlt csak a tulajdonos tudja olvasni (senki más ne tudjon semmi mást csinálni vele) és kapcsoljuk be rajta a sticky bitet.**

chmod 400 /root/70287.txt

chmod o+t /root/70287.txt

**Állítsuk be, hogy a user-70256 felhasználó két jelszóváltoztatás között legalább 10 napnak kelljen eltenie.**

chage –m 10 user user-70256

**Adjuk hozzá a user 70237 felhasználót a group-70237 csoporthoz.**

usermod –a -G group-70237 user-70237

**Változtassuk meg az UID azonosítóját user-70215 felhasználónak 1234-re**

usermod –u 1234 user-70215

**Dekódoljuk a /root/70170.enc fájlt a 70170 kulcs és 0-s inicializációs vektor segítségével. A fájl az aes-128cbc algoritmussal lett titkosítva. Mentsük el az eredményt /root/70170.txt néven.**

openssl aes-128-cbc –d –K 70170 –iv 0 –in /root/70170.enc –out /root/70170.txt

**Készítsen egy mappát /root/70147 néven és állítsuk be az ACL-jét úgy, hogy a user-70147 felhasználó automatikusan megkap minden jogot (olvasás-írás-futtatás) ennek a mappának az almappáira és fájljaira. Ne változtassuk a többi felhasználó jogosultságait.**

setfacl –dm user:user-70147:rwx /root/70147

**Dekódoljuk a /root/70106 jelszó és a des-ede algoritmus segítségével. Mentsük el a végeredményt /root/70106.txt néven.**

openssl des-ede –d –k 70106 –in /root/70106.enc –out /root/70106.txt

**Állítsuk be a user-70093 felhasználó home-mappájának a következőt: /home/u70093. Hozzuk létre a mappát ha nem létezik.**

mkdir /home/u70093 (ha nem létezik)

usermod –d /home/u70093 user-70093

chown user-70093:user-70093 /home/u70093

**Állítsuk be a /root/70083.txt fájl tulajdonosának az user-70083 felhasználót**

chown user-70083 /root/70083.txt

**Készítsünk egy felhasználót user-70067 néven.**

useradd user-70067

**Maszkolás segítségével állítsuk be, hogy minden újonnan létrejövő fájl és mappa 0462-es jogosultságokkal rendelkezzen.**

umask 0315

**Érje el, hogy a root felhasználó be tudjon lépni user-70163 nevében SSH segítségével (ténylegesen nem kell belépni) a felhasználó jelszavának megadása nélkül. A kulcsgenerálás során ne változtasson semmit az alapbeállítások.**

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

(talán még kell egy chown a végére, ha nem kapsz pontot (3ik sor megismétlése))

**Készítsen egy privát-publikus RSA kulcspárt az alapbeállításokkal /root/70202.pem és /root/70202.pub neveken, majd titkosítsa a /root/70202.txt fájlt a privát kulcs felhasználásával. Mentse el titkosított fájlt /root/70202.enc néven.**

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

(ha publikus kulccsal titkosítunk egy fájlt ez kell))

**Készítse fel a /root/70137.img fájlt titkosításra úgy, hogy felcsatolja loop device-ként, majd LUKS formátumra formázza. A titkosítás további lépéseit nem kell végrehajtania.**

losetup –f /root/70137.img

cryptsetup luksFormat /dev/loop0

1) Állítsuk be, hogy a /root/35003.txt fájlt csak a tulajdonos tudja írni (senki más ne tudjon semmi mást csinálni vele) és kapcsoljuk be rajta a setuid bitet.

chmod 4200 /root/35003.txt

2) Állítsuk be, hogy a user-34969 felhasználó két jelszóváltoztatása között legalább 10 napnak kelljen eltelnie.

chage -m 10 user-34969

3) Adjuk hozzá az user-34941 felhasználót a group-34941 csoporthoz.

usermod -g group-34941 user-34941

4) Változtassuk meg az UID azonosítóját az user-34928 felhasználónak 1234-re.

usermod -u 1234 user-34928

5) Készítsen egy privát-publikus RSA kulcspárt az alapbeállításokkal /root/34921.pem és /root/34921.pub neveken, majd titkosítsa a /root/34921.txt fájlt a privát kulcs felhasználásával. Mentse el a titkosított fájlt /root/34921.enc néven.

openssl genrsa -out /root/34921.pem

openssl rsa -in /root/34921.pem -pubout -out /root/34921.pub

openssl rsautl -sign -inkey /root/34921.pem -in /root/34921.txt -out /root/34921.enc

5/b

Készítsen egy privát-publikus RSA kulcspárt az alapbeállításokkal /root/70211.pem és /root/70211.pub neveken, majd titkosítsa a /root/70211.txt fájlt a publikus kulcs felhasználásával. Mentse el a titkosított fájlt /root/70211.enc néven.

openssl genrsa -out /root/70211.pem

openssl rsa -in /root/70211.pem -pubout -out /root/70211.pub

openssl rsautl -encrypt -pubin -inkey 70211.pub -in 70211.txt -out 70211.enc

6) Állítsuk be, hogy a user-34893 felhasználónak csak futtatási joga legyen a /root/34893.txt fájlon. Ne változtassuk a többi felhasználó jogosultságait.

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

Állítsuk be, hogy a user-70177 felhasználónak olvasási és írási joga legyen a /root/70177.txt fájlon. Ne változtassuk a többi felhasználó jogosultságait.

setfacl -m user-70177:rw /root/70177.txt

Dekódoljuk a /root/70173.enc fájlt a 70173 kulcs és 0-s inicializációs vektor segítségével. A fájl az aes-128-cbc algoritmussal lett titkosítva. Mentsük el az eredményt /root/70173.txt néven.

openssl aes-128-cbc -d -in /root/70173.enc -K 70173 -iv 0 >> /root/70173.txt

7) Készítse fel a /root/34880.img fájlt titkosításra úgy, hogy felcsatolja loop device-ként, majd LUKS formátumra formázza. A titkosítás további lépéseit nem kell végrehajtania.

fdisk 34880.img

n p w

cryptsetup luksFormat 34880.img

YES jelszó, jelszó megint

cryptsetup luksOpen 34880.img 34880

8) Érje el, hogy a root felhasználó be tudjon lépni user-34864 nevében SSH segítségével (ténylegesen nem kell belépni) a felhasználó jelszavának megadása nélkül. A kulcsgenerálás során ne változtasson semmit az alapbeállításokon.

ssh-keygen

cd .ssh

mkdir /home/user-34864/.ssh

chmod 700 /home/user-34864/.ssh

chown user-34864 /home/user-34864/.ssh

cat id\_rsa.pub >> /home/user-34864/.ssh/authorized\_keys

chmod 400 /home/user-34864/.ssh/authorized\_keys

chown user-34864 /home/user-34864/.ssh/authorized\_keys

9) Készítsen egy mappát /root/34854 néven és állítsuk be az ACL-jét úgy, hogy a user-34854 felhasználó automatikusan megkap minden jogot (olvasás-írás-futtatás) ennek a mappának az almappáira és fájljaira. Ne változtassuk a többi felhasználó jogosultságait.

mkdir /root/34854

setfacl -dm user-60569:rwx /root/34854

10) Készítsen egy RSA privát-publikus kulcspárt /root/34847.pem és /root/34847.pub nevekkel és írja alá a /root/34847.txt fájlt a segítségükkel. Az aláírásnak adja a /root/34847.sign nevet.

openssl -genrsa -out /root/34847.pem

openssl rsa -in /root/34847.pem -pubout -out /root/34847.pub

openssl dgst -sign /root/34847.pem -out /root/34847.sign /root/34847.txt

11) Titkosítsuk a /root/34831.txt állományt DES CBC segítségével a 0123456789ABCDEF kulcs felhasználásával és 0-s inicializációs vektorral. A titkosított fájl neve legyen /root/34831.enc.

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

12) Állítsuk be az user-34818 felhasználó home-mappájának a következőt: /home/U34818. Hozzuk létre a mappát ha nem létezik.

mkdir /home/U34818

usermod -d /home/U34818 user-34818

13) Állítsuk be a /root/34802.txt fájl tulajdonosának az user-34802 felhasználót.

chown user-34802 /root/34802.txt

14) Készítsünk egy felhasználót user-34789 néven.

useradd user-34789

15) Maszkolás segítségével állítsuk be, hogy minden újonnan létrejövő fájl és mappa 0446-es jogosultságokkal rendelkezzen.

umask 331

Készítse fel a /root/189522.img fájlt titkosításra úgy, hogy LUKS formátumra formázza, majd megnyitja titkos néven, létrehoz egy ext4 fájlrendszert, majd felcsatolja loop device-ként az Ön által létrehozott /root/185922 mappába

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

Dekódoljuk a /root/189342.enc fájlt a 189342 jelszó használatával és a des-ede algoritmussal. Mentsük el a kimenetet a /root/189324.txt néven. Használjunk pbkdf1-t 1000 iterációval

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

Fejtse vissza az 13970 kulccsal és 0 inicializáló vektorral aes-128-cbc algoritmus segítségével titkosított /root/13970.enc állományt. Az eredményt /root/13970.txt állományban tárolja.

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

Fejtse vissza az 13957 jelszóval des-ede algoritmus segítségével titkosított /root/13957.enc állományt. Az eredményt /root/13957.txt állományban tárolja.

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

Készítsen egy user13944 felhasználót és állítsa be úgy, hogy minimum 10 de maximum 20 naponta jelszót kelljen váltania.

***useradd userXXXX***

***chage –m 10 –M 20 userXXXX***

Írja alá a /root/13940.txt állományt a következő privát kulccsal. Használjon SHA 256 hash függvényt. Az aláírás a /root/13940.sign állományba kerüljön!

-----BEGIN PRIVATE KEY-----

MIICdgIBADANBgkqhkiG9w0BAQEFAASCAmAwggJcAgEAAoGBALGxXdQslY2y33Hr

6JBmdQL4fJmDZolEKJIojg9IapEI95SV5gsZb9+K6J+1sJAeq0k4wzm6LNWdMT3n

xDaWM0rN/wvM+MzMDoz2IOep6I/VQMFvq9/kL0iwhM5w6NJtkIfwNJhimw5KsEF7

iAtr9xl+3Gx6VIZ5ZgzpSHOeFspTAgMBAAECgYBpfApgX0s0wCAHZ+06c6g46DxH

gYrIJ+8RvQOALRQeHz2iNk5G/oW8JaEs1lYHaD10jT7PsSbWdKd7wW9onEe7vcfx

miJbcZaXON6pY11BZOVaGgSMWR2/frQVVPH9pdVk5L+UyJfE/kNGgdgAnKU8+jRT

yeMUer8bh5/GSJL8YQJBAONwyYVuOQo2dkVZTtGormh28NDt3o8NK9NaKUlzjS3E

YvzPdABDhjY+kjeA0LhT1xVwFr7MgekGks/EgbKlbbECQQDIAWifEguMgV0fCYB/

gXJTNNqbNgLf3+tQBNru8HCo1Ed4HPscx5tpfZHieXUW63PYbZC/kofMmoZ1e+Dc

mKVDAkBiEuyTIOhvwvRVCyG1vqsWWNOXBDuILAHN7X8IMU+bgKe+pCY9RuDE205p

qJ5YHa8Ni3wDYmRSe4crGG1k/3jBAkEAss3/mGZriLuGYt790AAMEzMnVKdevoLT

PoB4sjCmp2jQVCOko8AXwqGOMKhg85KfyJd7VqlLWrGzD4kmKFEXPQJAEj/QSzkJ

Dmqu2Q+KrIyYSDfWwdFDda6qkH9QHoTQ2aE6RtkShhAShA6EsJdOX2d3tCuSdZ2B

2o0qC6Dvgv2y/A==

-----END PRIVATE KEY-----

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

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

Állítsa át a /root/13930.txt állomány jogosultságait úgy, hogy csak olvasható legyen.

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

Állítsa át a /root/13921.txt állomány jogosultságait egy új USER ACL bejegyzés segítségével úgy, hogy az operator felhasználó olvashassa. (Mást ne változtasson az állományon, több jogot ne adjon.)

***chmod …..+r pelda.txt***

Állítsa át a /root/13908.txt állomány attribútumait úgy, hogy tulajdonosa az operator felhasználó legyen. (Mást ne változtasson az állományon.)

***chown operator pelda.txt***

Készítsen egy 138990 bájt méretű /root/13899.dat nevű állományt.

***fallocate –l 138990 pelda.dat***

Generáljon egy 2048 bites RSA kulcsot és mentse el a /root/13887.pem állományba PKCS8 szerinti privát kulcsként

***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***

Készítsen az /dev/sdc meghajtóra egy /dev/sdc1 partíciót. Formázza ext2 fájlrendszerrel, majd csatolja fel a /mnt katalógusba, csak olvashatóként.

***fdisk /dev/sdb***

***cryptsetup luksFormat /dev/sdb1***

***cryptsetup luksOpen /dev/sdb1 enc-home***

***mkfs.ext2 /dev/mapper/enc-home***

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

Érjük el, hogy az alábbi privát kulcs tulajdonosa a root felhasználó nevében bejelentkezhessen.

-----BEGIN PRIVATE KEY-----

MIICdwIBADANBgkqhkiG9w0BAQEFAASCAmEwggJdAgEAAoGBANCjZa5k9CCKIN0w

eOSzHrJt6OpltytqGozrKij+emNV4988yFo64QpdSVBXGUZN34aYo0mvnMo4B6M3

IQjMQ9NFeVvboTUugzgCL0or0+9GHelK4LaSC0xgMpGO+jvb5dxiqDEE2KVhejau

8HYiAr98VLNQgCHx16ZLvNfgy2rdAgMBAAECgYA523YRHJHOjD981zpPQZTbqjsS

9U4MTgo61eQFJjzOWz0r5PEyhG1vsFrqWpz5sBKygpWVk4uJUGxdyKXyiKKt7VNy

Lxv1HTHgxSTrdu1Gwk7ZSO9eX+AAHNkCU3PMhBdHEy8viaJmt1Dfw31zNePDeUKZ

2GU54Wd3jtYb96IagQJBAPrnXhOA3JvpX4kV3vWCUEYp4ek0wJPjsHjm5VYFHSyv

tzuUmnrYRkJidOVy9FUxrv8zJVfPRfSEZA0l99RMDI0CQQDU4EKnnR38kgrbymMv

bzTL+zC2i4tmcU6zMIbGdtpXJfxv+3ZpS2OTnlHpFRApviRHhLunD6eUnmFXnGK2

90uRAkEAtEferwDegyCyxptyctHJwECD1L9UyG7H9HdjveU6y0sOy77BKReRlE2O

VPe+XCCw7yne4TNLvqAKC/CGHILwWQJAeJ4xZmPCL/BYMr10gdYTJllH+scKz5r4

KtQeKaoCgUrGxHTJXVQYMfaNFvKWW/CfAd8VrM1T+QPcyBWWYXGx4QJBAIxAJocH

OScnZl2qb2ZPHh0C1F+L2PhhymLwJGW9DE7UmNB6xlOpdqLsNE3pfoh23P+zahXu

oNNgdlnYLBmGRiA=

-----END PRIVATE KEY-----

Keressem meg azt a katalógust a /root/13856/ katalóguson belül, amelyen a sticky bit használatban van. A katalógus teljes elérési útját írja a /root/13856.ans fájlba.

Készítsen az /dev/sdb meghajtóra egy /dev/sdb1 partíciót, majd készítse elő a partíciót titkosított fájlrendszer fogadására. Ehhez használja a cryptsetup programot és a LUKS formátumot.

***fdisk /dev/sdb***

***cryptsetup luksFormat /dev/sdb1***

Dekódolja az alábbi privát kulcs segítségével kódolt /root/13848.enc állományt. Az eredmény a /root/13848.txt állományba kerüljön!

-----BEGIN RSA PRIVATE KEY-----

MIIEpAIBAAKCAQEAuI4w+hLD5XXDfdWhStYJMxWn13QNgbf9nSy8P5Tl8aEp7RA4

9FANsyT6E1yFyxcYh0DLvgx47dNp+xHHD7h3a7Gv+hG+ipPbem6+3WoBOsWg+Zz9

0D5Jeu7TVMZqYdmH6ngdaG5qj4R4XZ6UpjhH34TXlyE1n0XlZB/27qDgEDkwT8wd

FNI2a//SvyLviqrGQ3vZB+1TsCMIJSsc9UFHtbl3O008pVqsEPMgTgT1cW++GS6n

zKR5p2mnR9D9mpKimy2uWXjvmWUWamqXanw2rF5ghlwxgnsR8zjQyuuo3S5KLBU9

ZTjJVDNrEwJtYaHIyTOjESgp6ptZ4zUIQ8r/UwIDAQABAoIBAQC0J2k707GSfiB0

52LpUIHucgdDVDATHm3dTdv9HPZRpobsuNc/9h1JcKEE4V5hX4w8C05XmIk7bxKX

WUU93U4FvJARxdyAHdEzdIOwU1gb7Os0fsFs1ECaViPJL16NYfFBOjtKw+4VZrSw

fqqQj4Ppdx2Uk4Bql6pS0LkVO8k9S0qmM0MfT7LWigd0uc25eppXAFNkB1TWwW28

rGDxaZndFkO4RvfLL9VXA2uYM3ObgyaPrtaYfhCJ30lHtK3HVn6B6/QWu/djxEXl

dhosc7tygnmCinsa23Mc6xiqC4PXs/0soKBv7gSginLzBnvIg6tFYhzXNwdhJ/KY

zlQoE+1BAoGBAPUa5HHxZ5QSm9ajf8zyAembby99D8z5oli2evtHuhV5IqZPSPE0

evLD5r/fTEdeL42vJH5CLfxKn93djyIvNQ9kPa4/2jlzMesAkyMuu2RcljAfn1J9

b34LuZZfgGdE0/GKi6No0UUMlD8tKcSUqdL4+iJdyIlZSLtUGyLw4VNxAoGBAMDC

Sm5sYwvnMltNuXyGEyNJZn08Kp454gr5ILb+zpSDi6HgbOGCXtp2issqVmKDPLkx

x3xu5679qYuJt9vueURVOE9KHIe3JerkbWugsMqagjdwq3tFE7eY6YdwNlK7tDYS

DEpTzlkn8Mppjt/JeS567a3VbYrgzDa4x0QxWtUDAoGAenbyV4AfmZtmo+rTSypM

DFWuSxL4lxjPpfWfIvgmoN4CkwggUOxA1hVNsOa4LRyBNBCjcjZM1bbPg8JU5uah

Y0xZiTu8JGJLObjyy2xpEu8z112ldEjaMSdYliqndHGuWAw6Uu5nSVHMrHg7W05Q

P+pIyG0FaqLitT6DxISIgPECgYBqb95hsv/OJs+rkvOFSxNuPK2XIY326Mdkf8QM

yA6R+0EzFZWJwE9YGnTxUmN46jaxnEcm8qaD/hWMs3MOwlO748LAJZAzcHJDjfbN

o2F7vm2A53oJC0+j5Y+t9cxJStRrtvOKZ1Rd7qwLWNZHxBxiCgcMIfnm4dJhtQ5z

HT2muQKBgQDL+ygG9RdHKYGXaFNENOr+oC8TU+8GDjYKzu8ZNbFTENq74DUOwP+n

3rfFKMuJHHxrrx/T5K3jDQKqYmxP4S7lqOV/pI8Y9MO++u1fIlQwoljoA62+K6Dl

XgvGBPWpfZM6jA8vrrPh1D8DHrPbCGQbIRJ3GdOJUvXR51L86pSw8A==

-----END RSA PRIVATE KEY-----

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

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

openssl rsa -in 188.pem -pubout > 188.pub

openssl rsautl -inkey 188.pub -pubin -in /root/18821.enc > /root/18821.txt

Titkosítsa a /root/13832.txt állomány tartalmát a /root/13832.key.pub nyilvános kulcs segítségével. Az eredmény a /root/13832.enc állományba kerüljön!

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

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

Állítsuk be, hogy a /root/70299.txt fájlt csak a group tudjon vele bármit csinálni (senki más ne tudjon semmi mást csinálni vele) és kapcsoljuk be rajta a sticky bitet.

Megoldás

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

Megjegyzés (t:stickybit s:setuidbit)

Állítsuk be, hogy a user-70259 felhasználót a jelszava lejárta előtt 10 nappal figyelmeztesse.

Megoldás

chage -W 10 user-70259

Adjuk hozzá az user-70228 felhasználót a group-70228 csoporthoz.

Megoldás

usermod -aG group-70228 user-70228

Változtassuk meg az UID azonosítóját az user-70215 felhasználónak 1234-re.

Megoldás

usermod -u 1234 user-70215

Készítsen egy privát-publikus RSA kulcspárt az alapbeállításokkal /root/70199.pem és /root/70199.pub neveken, majd titkosítsa a /root/70199.txt fájlt a publikus kulcs felhasználásával. Mentse el a titkosított fájlt /root/70199.enc néven.

Megoldás

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

Megjegyzés (-encrypt kell ha publikus kulcs felhasználást kér,

-sign kell ha privát kulcs felhasználást kér)

Állítsuk be, hogy a user-70192 felhasználónak csak írási joga legyen a /root/70192.txt fájlon. Ne változtassuk a többi felhasználó jogosultságait.

Megoldás

touch /root/70192.txt

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

Dekódoljuk a /root/70167.enc fájlt a 70167 kulcs és 0-s inicializációs vektor segítségével. A fájl az aes-128-cbc algoritmussal lett titkosítva. Mentsük el az eredményt /root/70167.txt néven.

Megoldás

openssl aes-128-cbc -d -K 70167 -iv 0 -in /root/70167.enc -out /root/70167.txt

Érje el, hogy a root felhasználó be tudjon lépni user-70160 nevében SSH segítségével (ténylegesen nem kell belépni) a felhasználó jelszavának megadása nélkül. A kulcsgenerálás során ne változtasson semmit az alapbeállításokon. (még nem jó)

Megoldás

ssh-keygen

mkdir /home/user-70160/.ssh

chown user-70160:user-70160 /home/user-70160/.ssh

cat .ssh/id\_rsa.pub >> /home/user-70160/.ssh/authorized.key

chown user-70160:user-70160 /home/user-70160/.ssh

Készítsen egy mappát /root/70144 néven és állítsuk be az ACL-jét úgy, hogy a user-70144 felhasználó automatikusan megkap minden jogot (olvasás-írás-futtatás) ennek a mappának az almappáira és fájljaira. Ne változtassuk a többi felhasználó jogosultságait.

Megoldás

mkdir 70144

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

Készítsünk egy felhasználót user-70070 néven.

Megoldás

useradd user-70070

Maszkolás segítségével állítsuk be, hogy minden újonnan létrejövő fájl és mappa 0640-es jogosultságokkal rendelkezzen.

Megoldás

umask 137

Megjegyzés mask törlése umask 002

Dekódoljuk a /root/70109.enc állományt a 70109 jelszó és az des-ede algoritmus segítségével. Mentsük el a végeredményt /root/70109.txt néven.

Megoldás

cat /root/70109.txt

openssl des-ede -d -in /root/70109.enc -k 70109

openssl des-ede -d -in /root/70109.enc -k 70109 > /root/70109.txt

Állítsuk be az user-70096 felhasználó home-mappájának a következőt: /home/u-70096. Hozzuk létre a mappát ha nem létezik.

Megoldás

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

Állítsuk be a /root/70086.txt fájl tulajdonosának az user-70086 felhasználót.

Megoldás

chown user-70086 /root/70086.txt

* + **1. Állítsuk be, hogy a /root/70302.txt fájlt csak a tulajdonos tudjon vele bármit csinálni (senki más ne tudjon semmi mást csinálni vele) és kapcsoljuk be rajta a setuid bitet.**
  + • chmod u=rwx,g=,o=,u+s /root/70302.txt
  + **2. Állítsuk be, hogy a meglévő user-70274 felhasználónak 2020.05.22-étől ne legyen hozzáférhető ("lejárjon") az accountja.**
  + • chage -E 2020-05-22 user-70274
  + **3. Adjuk hozzá az user-70228 felhasználót a group-70228 csoporthoz.**
  + • usermod -aG group-70228 user-70228
  + **4. Változtassuk meg az UID azonosítóját az user-70224 felhasználónak 1237-re.**
  + • usermod -u 1237 user-70224
  + **5. Készítsen egy privát-publikus RSA kulcspárt az alapbeállításokkal /root/70211.pem és /root/70211.pub neveken, majd titkosítsa a /root/70211.txt fájlt a publikus kulcs felhasználásával. Mentse el a titkosított fájlt /root/70211.enc néven.**
  + • openssl genrsa -out /root/70211.pem
  + • openssl rsa -in /root/70211.pem -out /root/70211.pub -pubout
  + • openssl rsautl -encrypt -inkey /root/70211.pub -in /root/70211.txt -out /root/70211.enc -pubin
  + **6. Állítsuk be, hogy a user-70192 felhasználónak csak írási joga legyen a /root/70192.txt fájlon. Ne változtassuk a többi felhasználó jogosultságait.**
  + • setfacl -m user:user-70192:w /root/70192.txt
  + **7. Dekódoljuk a /root/70170.enc fájlt a 70170 kulcs és 0-s inicializációs vektor segítségével. A fájl az aes-128-cbc algoritmussal lett titkosítva. Mentsük el az eredményt /root/70170.txt néven.**
  + • openssl aes-128-cbc -d -K 70170 -iv 0 -in /root/70170.enc -out /root/70170.txt
  + **8. Érje el, hogy a root felhasználó be tudjon lépni user-70157 nevében SSH segítségével (ténylegesen nem kell belépni) a felhasználó jelszavának megadása nélkül. A kulcsgenerálás során ne változtasson semmit az alapbeállításokon.**
  + • ssh-keygen, majd millió enter
  + • mkdir /home/user-70157/.ssh
  + • chown user-70157:user-70157 /home/user-70157/.ssh
  + • cat /root/.ssh/id\_rsa.pub >> /home/user-70157/.ssh/authorized\_keys
  + **9. Készítsen egy mappát /root/70144 néven és állítsuk be az ACL-jét úgy, hogy a user-70144 felhasználó automatikusan megkap minden jogot (olvasás-írás-futtatás) ennek a mappának az almappáira és fájljaira. Ne változtassuk a többi felhasználó jogosultságait.**
  + • mkdir 70144
  + • setfacl -dm user:user-70144:rwx /root/70144

**10. Dekódoljuk a /root/70103.enc állományt a 70103 jelszó és az des-ede algoritmus segítségével. Mentsük el a végeredményt /root/70103.txt néven.**

* 1. openssl des-ede -d -k 70103 -in /root/70103.enc -out /root/70103.txt

**11. Állítsuk be az user-70096 felhasználó home-mappájának a következőt: /home/u-70096. Hozzuk létre a mappát ha nem létezik.**

* 1. • mkdir u-70096
  2. • usermod -d /home/u-70096 user-70096
  3. • chown user-70096 /home/u-70096

**12. Állítsuk be a /root/70089.txt fájl tulajdonosának az user-70089 felhasználót.**

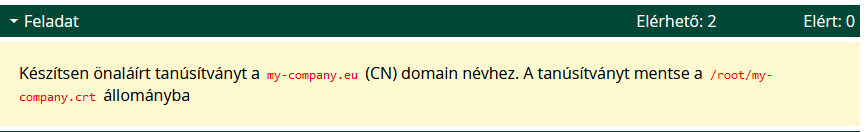
* 1. • chown user-70089 /root/70089.txt

**13. Hozzunk létre egy új csoportot newgroup-70073 néven!**

* 1. • groupadd newgroup-70073

**14. Maszkolás segítségével állítsuk be, hogy minden újonnan létrejövő fájl és mappa 0462-es jogosultságokkal rendelkezzen.**

* 1. umask -S u=r,g=rw,o=w



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

A képen szöveg, Betűtípus, képernyőkép látható

Automatikusan generált leírás

cryptsetup luksOpen /5d3a8e1b titkosmeghajtó

Jelszó

mkdir /root/titkosmeghajtó\_mappa

mount /dev/mapper/titkosmeghajtó /root/titkosmeghajtó\_mappa

A képen szöveg, levél, Betűtípus, képernyőkép látható

Automatikusan generált leírás

**/home/root/.ssh**

**chmod 700 /.ssh**

**nano authorized\_keys - ide bemasolni a kulcsot**

**chmod 400 authorized\_keys**

**A képen szöveg, levél, képernyőkép, dokumentum látható

Automatikusan generált leírás**

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

**openssl rsa -in fajl.txt -pubout > 13845.public**

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

nano 13845\_code.txt -belemasolni a kodot

openssl rsa -in 13845\_code.txt -pubout > 13845.public

openssl rsautl -inkey 13845.public -pubin -in /root/13845.enc > /root/13845.txt



**fdisk /dev/sdb -> n -> enterek -> vegen w**

**cryptsetup luksFormat /dev/sdb1 (YES) (jelszó megadása)**

**lsblk -f**

**cryptsetup luksOpen /dev/sdb1 titkosmeghajto**

**lsblk -f**

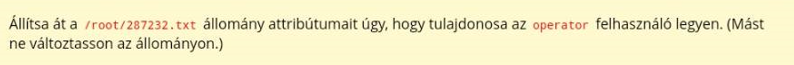
A képen szöveg, levél, Betűtípus, képernyőkép látható

Automatikusan generált leírás

**touch privkulcs**

**nano privkulcs – ide bemasolnia privatkulcsot**

**openssl dgst -sign privkulcs -sha256 -out /root/287252.sign /root/287252.txt**

****

chown operator /root/287232.txt