

SSH tippek és trükkök

1. ssh-desktopról

1. ssh adminla@firewall-1

1. ujjlenyomat ellenőrzése

1. ssh-firewall-on:

1. ssh-keygen -lvf /etc/ssh/ssh_host_ecdsa_key.pub

2. Mi ez a szép minta?

1. ssh -o VisualHostKey=yes adminla@firewall-1

2. A known_hosts

1. cat .ssh/known_hosts

3. És mi van ha megváltozik a kulcs?!

1. Teszt

1. firewall gépen

1. ls -lh /etc/ssh

2. sudo rm /etc/ssh/ssh_host_*

3. sudo dpkg-reconfigure openssh-server

4. ls -lh /etc/ssh

5. kilépés

2. desktopról

1. ssh -o VisualHostKey=yes adminla@firewall-1

2. nem megy be és hibát dob!

3. eltérnek a kulcsok!

4. tegyük fel, hogy ez jogos (pl. lecserélted mint most, újratelepítetted, stb.)

1. firewall-on ismét ellenőrizd a kulcsot!

1. ssh-keygen -lvf
/etc/ssh/ssh_host_ecdsa_key.pub

1. célszerű a telepítéskor megtenni és biztonságos hordozón magaddal vinni, mert amikor be akarsz lépni már nem fogod tudni ellenőrizni távolról...

2. Töröld a known_hosts-ból:

1. ssh-keygen -f .ssh/known_hosts -R firewall-1

3. Jöhet a belépés

1. ssh -o VisualHostKey=yes
adminla@firewall-1
2. az IP-re is dob egy figyelmeztetést
 1. igen, az IP címet is eltette...
 2. ezt is törölheted:
 1. ssh-keygen -f
.ssh/known_hosts -R
192.168.2.51

2. Folytatás a firewall-1 gépen

3. sshd

1. Port: kintről ne a 22...
 1. Port 2222
 2. sudo vi /etc/ssh/sshd_config
 1. ListenAddress 0.0.0.0:2222
 2. ListenAddress 192.168.1.1:22
 3. PermitRootLogin no
 3. sudo service ssh restart
 4. ssh adminla@firewall-1
 1. nem megy
 5. ssh -p 2222 adminla@firewall-1
 1. scp esetén -P

2. DenyHosts

1. sudo apt-get install denyhosts
2. sudo vi /etc/denyhosts.conf
 1. PURGE_DENY = 2w
 2. PURGE_THRESHOLD = 2
 3. BLOCK_SERVICE = ALL
 4. DENY_THRESHOLD_INVALID = 3
 5. DENY_THRESHOLD_VALID = 5
 6. DENY_THRESHOLD_ROOT = 1
 7. DENY_THRESHOLD_RESTRICTED = 1
 8. ADMIN_EMAIL =
 1. + SMTP beállítások
 9. SYSLOG_REPORT=YES
 - 10.AGE_RESET_VALID=5d
 1. hány napig számolja a hibás belépéseket
 2. az ennyinél régebbieket elfelejti
 - 11.AGE_RESET_ROOT=25d

1. ugyanaz, de root felhasználóra
- 12.AGE_RESET_RESTRICTED=25d
 1. és belépésre nem jogosult felhasználókra
- 13.AGE_RESET_INVALID=10d
 1. és a nem létező felhasználókra
- 14.RESET_ON_SUCCESS = yes
- 15.SYNC_SERVER = <http://xmlrpc.denyhosts.net:9911>
- 16.SYNC_INTERVAL = 1h
- 17.SYNC_UPLOAD = yes
 1. te is segíthetsz..
- 18.SYNC_DOWNLOAD = yes
- 19.SYNC_DOWNLOAD_THRESHOLD = 10
 1. hány szerver kell jelentse a támadást a letöltéshez
- 20.SYNC_DOWNLOAD_RESILIENCY = 2d
 1. mennyi idő telhet el max. a támadások között a letöltéshez

3. Egyéb

1. Ahonnan sose tiltson:
 1. sudo vi /var/lib/denyhosts/allowed-hosts
4. sudo service denyhosts restart
5. tail -f /var/log/denyhosts
6. desktop gépről:
 1. ssh -p 2222 root@firewall-1
 1. és még párszor....
 2. kis idő kell: a denyhosts 30 másodpercenként nézi át a logokat
 1. de ettől kezdve nem megy az ssh...
 3. engedjük magunkat vissza...
 1. sudo -s
 2. service denyhosts stop
 3. vi /etc/hosts.deny
 1. sort törölni
 4. grep 192.168.2.128 /var/lib/denyhosts/*
 1. mindenből töröld magad
 2. most egyszerű lesznek:
 1. rm /var/lib/denyhosts/*
 5. vi /var/lib/denyhosts/allowed-hosts
 1. 192.168.2.128

6. service denyhosts start

7. most megint megy az ssh... többet ne rontsd el a belépést! :-)

3. Kopogtatás

1. A Haladó Linux tűzfal készítés képzésen lépésről lépésre megtanulhatod

4. SSH kulcs

1. desктоpon csináljuk

2. ssh-keygen

1. Opcionális lehetőségek

1. -f: másik fájlba

1. konkrét kulcs használata: ssh -i kulcsfájl

2. -C: komment

3. cat .ssh/id_rsa.pub

4. ssh-copy-id adminla@firewall-1

1. jó lenne és egyszerű, de a portot ennek nem tudod megadni...

2. Ubuntu 13.10-től a -p opcióval már igen

5. akkor marad a másolás és beillesztés

1. cat .ssh/id_rsa.pub

1. másolás...

2. ssh -p 2222 adminla@firewall-1

1. mkdir .ssh

2. chmod 700 .ssh

3. vi .ssh/authorized_keys

1. beillesztés

4. kilépés

6. próbáld meg most

1. szövegesen is megy, ott a konzolon kéri

2. X11 rendszerben felugrik a grafikus jelszó kérő: az ssh kulcs jelszavát kérdezi

1. megjegyzi (hozzáadja az agenthez: legközelebb már nem kéri)

3. mi ez az agent és mire jó?

1. Linuxon és MacOS-en automatikusan megy

2. Windows: pagent (putty)

3. Milyen kulcsok vannak betöltve?

1. ssh-add -l

2. ssh-add -L

1. teljes kulcsot mutatja

3. kulcs betöltése: ssh-add

1. akár távolról is, ha van agent továbbítás (erről később)

4. kulcs törlése az agentből

1. ssh-add -d azonosító

2. ssh-add -D

1. mindet

4. Mi az az agent továbbítás és mire jó (és miért veszélyes)?

1. ssh -o ForwardAgent=yes -p 2222 adminla@firewall-1

1. ssh-add -l

1. és itt van, ha innen ssh-zol tovább használni fogja

2. a helyi rendszergazda (és bárki, aki a te nevedben be tud lépni) TOVÁBB TUDJA HASZNÁLNI ARRÓL A GÉPRŐL AMIRE BELÉPTÉL!!!

7. Az authorized_keys fájl

1. milyen opciók lehetnek benne?

1. az opciók a sor elejére kerülnek, vesszővel (majd szóköz és a többi)

2. arra azért figyelj, hogy ezt a user tudja szerkeszteni magának...

3. belépés korlátozása adott címekről

1. from="címlista"

4. pl. csak sftp hozzáférés

1. command="/usr/lib/sftp-server"

2. teszt: felveszem...

1. ssh -p 2222 adminla@firewall-1

1. nem sokra jutok... nincs prompt

2. sftp -P 2222 adminla@firewall-1

1. működik

5. no-agent-forwarding

6. no-port-forwarding

1. vagy:

1. permitopen="host:port"

1. -L engedélyek

7. no-X11-forwarding

8. Így, hogy van kulcsod, a jelszavas belépést tiltsd le!

1. sudo vi /etc/ssh/sshd_config

1. PasswordAuthentication no

2. `sudo service ssh restart`
3. kilép...
4. `ssh-add -D`
5. `ssh -p 2222 adminla@firewall-1`
 1. NE add meg a kulcs jelszavát!
 2. nem enged be (egyébként kérné a sima jelszavad)

5. vi `.ssh/config`

1. `HashKnownHosts yes`
2. `Compression yes`
3. Host hostnév hostnév ... (akár rövid név!)
 1. Host fw1 firewall-1 firewall-1.lan
 1. `HostName firewall-1`
 1. így minden fentnél ennek a kulcsát nézi
 2. Port 2222
 3. User adminla
 2. Host mail web
 1. `HostName %h.linuxakademia.hu`
4. Így már egyszerűbb a belépés:
 1. `ssh firewall-1`
5. Tipp változó gépek (telepítések, stb.)
 1. Nem fogja elmenteni és ellenőrizni a host kulcsát
 2. Host 192.168.* 172.16.* 10.*
 1. `UserKnownHostsFile /dev/null`
 2. `StrictHostKeyChecking no`
 3. User root

6. port forward

1. helyi->távoli (-L)
 1. `ssh -L 8888:192.168.200.2:80 firewall-1`
 1. majd a böngészőben a 127.0.0.1:8888
 2. majd kilépés: böngésző újratöltés és nem megy
 2. bárki kapcsolódhasson a helyi hálóból: -g
3. vi `.ssh/config`
 1. Host remotesshserver
 1. `LocalForward 8888 192.168.200.2:80`
 2. `ssh firewall-1`
 3. Majd böngésző teszt
 4. töröld a forwardot a configból ha nem kell!

4. kiváló intranetes webszerverhez, távoli gépen mysql szerverhez kapcsolódni, ha az csak alkalomszerűen kell

1. tipp: autossh

2. távoli->helyi (-R)

1. -R megnyitandóport:célszerver:célport

2. pl: ideglenesen egy belső webszerverhez hozzáférés kintieknek

3. dinamikus

1. -D [bind-address:]port

2. Socks proxy

1. állítsd be a portot a böngészőben, mint socks proxy!

2. mire jó? nem megbízható hálózathoz kell böngészni: a saját szerveredig biztonságos lesz (egyszerűbb, mint a VPN)

3. érdemes tömöríteni (-C)

3. Példa

1. ssh -ND 1080 firewall-1

1. -N: ne futtasson semmit a túloldalon

2. -D: dinamikus proxy a 1080 porton (socks)

2. Böngészőben:

1. TESZT: 192.168.200.2 NEM megy

2. beállítás > speciális > hálózat > proxy

1. socks proxy 127.0.0.1 1080

3. újra teszt: MEGY!

3. -f: a belépés után fusson a háttérben (nincs interaktív session, csak átirányítás)

1. távoli X11 program futtatásnál is ez az ideális mód

4. A végén kapcsold ki a proxyt a böngészőben!

7. VPN

1. HOGYAN?

1. csak rootként...

1. Tűzfalon:

1. sudo vi /etc/ssh/sshd_config

1. PermitRootLogin yes

2. PermitTunnel yes

2. sudo service ssh restart

2. Az ssh kulcs miatt a root-nak is kell a kulcs:

1. ssh firewall-1

1. sudo -s

2. cp -a /home/adminla/.ssh /root/

3. `chown -R root.root /root/.ssh`
3. `sudo ssh -i /home/slapi/.ssh/id_rsa -p 2222 -w 0:0 root@firewall-1`
 1. `ip link set tun0 up`
 2. `ip addr add 172.16.42.1/32 peer 172.16.42.2 dev tun0`
 3. `iptables -I INPUT -i tun0 -j ACCEPT`
 4. `iptables -I FORWARD -i tun0 -o eth1 -j ACCEPT`
4. Desktopon:
 1. `sudo ip link set tun0 up`
 2. `sudo ip addr add 172.16.42.2/32 peer 172.16.42.1 dev tun0`
 3. `sudo ip route add 192.168.200.0/24 via 172.16.42.1 dev tun0`
 4. `ping 172.16.42.1`
 5. `ping 192.168.200.2`
 6. böngésző: 192.168.200.2
5. Kilépés (ctrl-c kell) törli az egészet (kivéve a tűzfal szabályok!!!)
2. tipp: sshuttle
 1. Transzparens proxy port átirányításokkal
 2. `sudo apt-get install sshuttle`
 3. `sshuttle -vNhr root@firewall-1:2222 192.168.200.0/24`
 4. A héttérben:
 1. `sshuttle -Dhr root@firewall-1:2222 192.168.200.0/24`
 5. kell helyi sudo jog!
 1. tűzfalat állít!!!!
 6. ettől kezdve minden forgalom az ssh csatornán át megy
 7. -H: a helyi hosts fájlba betesz mindent, amit a túloldali szerver ismer, így névvel is megy a hivatkozás
8. SSH kapcsolódás másik gépen keresztül, mint proxy
 1. Másik ssh szerverről
 1. `ssh 192.168.200.2`
 1. nem megy...
 2. `vi .ssh/config`
 1. Host 192.168.200.2
 1. Port 22
 2. User adminla
 3. ProxyCommand ssh -q -W %h:%p firewall-1
 3. `ssh 192.168.200.2`
 2. Tipp: HTTP proxyn átjutás
 1. ProxyCommand corkscrew proxy.example.com 8080 %h %p

9. Típek és trükkök

1. Nagyobb fájlok másolása

1. scp mit user@hova:
2. scp user@honnan: hova
 1. -r: rekurzív
 2. -l: sávszélesség korlátozása
3. scp esetén a port -P (nagy), míg sima ssh-nál -p (kicsi)
4. rsync ssh-n keresztül

2. sshfs

1. sudo apt-get install sshfs
2. mkdir server
3. sshfs adminla@192.168.200.2:/ /home/slapić/server/ -o reconnect,follow_symlinks,large_read,kernel_cache,direct_io,auto_cache,big_writes,port=22
4. ls -lh server
5. date > server/date.txt
6. ssh 192.168.200.2
 1. ls -lh
 2. exit
7. fusermount -u server

3. Kapcsolat megosztása több ssh között

1. Egyszer belépsz, a többi belépés ugyan azon szerverre az első kapcsolatot újrahasználja:
2. mkdir .ssh/connections
3. chmod 700 .ssh/connections
4. vi .ssh/config
 1. ControlMaster auto
 2. ControlPath ~/.ssh/connections/ssh-%h_%p_%r
5. ssh 192.168.200.2
 1. jelszót kér, lassúcska
6. másik ablakból
 1. ssh 192.168.200.2
 1. azonnali és nem kér jelszót
7. Ha mindenhol kilépsz, újra kéri
8. Fenntartása a kilépés után 4 órán át (hogya újra gyorsan menjen pl. egy scp):
 1. vi .ssh/config
 1. ControlPersist 4h

2. ssh 192.168.200.2

1. elsőre kér jelszót

2. kilépsz....

3. és ki-be-ki-be és nem kér jelszót és azonnali...

4. Tipp: AutoSSH

1. sudo apt-get install autossh

2. Pl. socks tunnel vagy port forward újraépítése ha le bomlik

10.Windowson

1. PuTTY

1. pageant

2. WinSCP

3. Total Commander SSH plugin

4. ExpanDrive, WebDrive

11.Android

1. VX ConnectBot