A ***Linux szerveren*** állítsa be az alábbi paramétereket, illetve vegyen fel egy felhasználót!

* A root jelszava jelenleg ***root***, változtassa meg erre: ***qwe123***

*passwd root* *[Enter]*

jelszó: *qwe123 [Enter]*

* gépnév: ***linuxSrv***

*nano /etc/hostname [Enter]*

tartalma:

*linuxSrv*

Mentsük el: *Ctrl + o* aztán lépjünk ki szerkesztőből: *Ctrl + x*

* IP cím: ***192.168.10.4/24***, átjáró: ***192.168.0.254***, DNS kiszolgáló: ***192.168.10.1***

*ip a [Enter] aktív-e az Ethernet kártya? a neve enp0s3?*

*nano /etc/network/interfaces [Enter]*

tartalmazza:

*auto enp0s3*

*iface enp0s3 inet static*

*address 192.168.10.4*

*netmask 255.255.255.0*

*broadcast 192.168.10.255*

Mentsük el: *Ctrl + o* aztán lépjünk ki szerkesztőből: *Ctrl + x*

*ifdown enp0s3 [Enter]*

*ifup enp0s3 [Enter] vagy: systemctl restart networking*

* felhasználónév: ***diak*** jelszó: ***diak***

*adduser diak [Enter]*

jelszava: *diak [Enter]*

* DNS kiszolgáló megadásához:

*nano /etc/resolv.conf*

*tartalmazza:*

*domain teszt.local*

*search teszt.local*

*nameserver 192.168.10.1*

***DHCP:***

A letöltött, de nem telepített és nem konfigurált DHCP szerver felhasználásával, konfiguráljuk a kiszolgálót:

*A címkiosztás paraméterei:*

*Címtartomány:* ***192.168.10.0 /24***

*Kizárt címek:* ***192.168.10.1 – 192.168.10.50***

*Alapértelmezett átjáró:* ***192.168.10.254***

*DNS kiszolgáló:* ***192.168.10.1***

*Tartománynév:* ***teszt.local***

*Fenntartás a kliens gépnek:* ***192.168.10.25***

Telepítsük: *apt-get install isc-dhcp-server [Enter]*

*Hálózat legyen konfigurálva, ellenőrizzük:*

*ip a*

*nano /etc/network/interfaces*

*ifdown enp0s3*

*ifup enp0s3*

*ping 192.168.10.4*

*Konfiguráljuk a DHCP kiszolgálót hogy figyeljen az enp0s3 interfészen:*

*nano /etc/default/isc-dhcp-server*

*…*

*INTERFACESv4= ”enp0s3”*

*# INTERFACESv6= ”” # ezt kitiltottuk!*

mentés, kilép: *Ctrl + o >> Ctrl + x*

*mv /etc/dhcp/dhcpd.conf /etc/dhcp/dhcpd.conf.orig #mentjük az eredeti konfig-ot*

Nyissuk meg (hozzuk létre) a konfigurációs állományt:

*nano /etc/dhcp/dhcpd.conf [Enter]*

***tartalma****:*

*authoritative;*

*default-lease-time 600;*

*max-lease-time 7200;*

*subnet 192.168.10.****0*** *netmask 255.255.255.****0 {***

*range 192.168.10.****51*** *192.168.10.****253****;*

*option domain-name-servers 192.168.10.****1****;*

*option domain-name "****teszt.local****";*

*option subnet-mask 255.255.255.****0****;*

*option broadcast-address 192.168.10.****255****;*

*option routers 192.168.10.****254****;*

***}***

*host win10* ***{***

*hardware ethernet 08:00:27:92:A7:79;*

*fixed-address 192.168.10****.25****;*

***}***

*mentés, kilép: Ctrl + o >> Ctrl + x*

Indítsuk újra a DHCP kiszolgálót: *systemctl restart isc-dhcp-server [Enter]*

*vagy*

*service isc-dhcp-server restart [Enter]*

***Hálózati fájlmegosztás:***

A Linux kiszolgálón ***az előre letöltött, de nem telepített SAMBA szervert*** konfiguráljuk az alábbiak szerint:

Telepítsük a SAMBA kiszolgálót:

apt-get install samba

**Hozzuk** **létre** a felhasználói **fiókokat**:

adduser diak1 *# jelszó: diak1*

adduser tanar1 *# jelszó: tanar1*

**Hozzunk** **létre** egy **csoportot** és adjuk hozzá a **csoporttagokat**: (feltételezve AD/OU: iskola/ Gp: iskola létezik)

addgroup iskola

adduser diak1 iskola # adduser tanar1 iskola

A létrehozott "diak1" és a "tanar1" **felhasználók engedélyezése a Samba felé**. A debian felhasználói közül választhatunk. Jelszót viszont külön be kell gépelni, ami eltérhetne a rendszerjelszótól.

smbpasswd -a diak1 *# jelszó: diak1*

smbpasswd -a tanar1 *# jelszó: tanar1*

**Hozzuk létre** a megosztott könyvtárat: (***-p*** a még nem létező köztes könyvtárakat is létrehozza)

mkdir –p /srv/samba/megosztott # szabvány szerint itt a helye a megosztott könyvtáraknak

Tegyük elérhetővé **mindenkinek**:

chmod 777 /srv/samba/megosztott

Szerkesztés előtt **nevezzük át** az **eredeti** konfigurációs **fájlt**:

mv /etc/samba/smb.conf /etc/samba/smb.conf.orig

**Módosítsuk** a */etc/samba/****smb.conf*** tartalmát:

[global]

workgroup = teszt.local # munkacsoport (WORKGROUP) vagy tartomány neve (pl. teszt.local)

netbios name = samba # hálózat tallózáskor ezen a néven jelenik meg a kliensen

[megosztott] # A megosztás neve. Ezen a mappanéven láthatjuk majd a fájlkezelőben.

path = /srv/samba/***megosztott*** # a megosztott nevű mappa elérési útvonala

browsable = yes # engedélyezi a Windows Explorerből való tallózást

writable = yes # írható is a megosztott mappa

create mask = 0755 # az újonnan létrejövő fájlok a tulajdonos számára teljes jogkörrel,

# a többiek számára pedig futtatási és olvasási jogkörrel elérhetően jönnek létre

valid users = diak1 tanar1 # a "valid users" opcióval megadhatjuk azokat a felhasználókat -szóközökkel elválasztva-,

valid users = @iskola # akik elérhetik a könyvtárat. # csoport aminek a tagjai elérhetik

Indítsuk újra a SAMBA kiszolgálót:

systemctl restart smbd

A kliensen kitallózhatjuk fájlkezelőben a megosztásunkat (pl. a fájlkezelő címsorába beírva):

[\\192.168.10.4\megosztott](about:blank) *[Enter]*

A megosztott könyvtárat csatlakoztathatjuk a kliensen:

parancssorból (vagy bejelentkezési parancsfájlon, csoportházirenden keresztül):

net use S: [\\192.168.10.4\megosztott](about:blank) *[Enter]*

*A rendszer rákérdez a felhasználó/jelszó párosra!*

*net use* S: [\\192.168.10.4\megosztott](about:blank) /user: diak1 diak1 *[Enter]*

*A rendszer NEM kérdez már rá a felhasználó/jelszó párosra!*

a létrehozott meghajtó betűjellel való csatlakoztatás ellenőrizhető parancssorból is:

net use *[Enter]*

*a megjelenő listában szerepelni fog: s: \\192.168.10.4\megosztott*

*To set permissions using numbers, instead of letters. The numbers are represented like this in binary:*

*Base10 Number Binary Resulting permission*

*0 000 ---*

*1 001 --x*

*2 010 -w-*

*3 011 -wx*

*4 100 r--*

*5 101 r-x*

*6 110 rw-*

*7 111 rwx*

***Webkiszolgáló:*** A webes tartalom elérését ***csak HTTPS kapcsolaton keresztül*** biztosítsuk.

A Linux kiszolgálón **az előre letöltött, de még nem telepített** **Apache2** illetve **OpenSSL** szerverek felhasználásával, konfigurálja a kiszolgálót:

Telepítsük az Apache2 és az OpenSSL kiszolgálókat:

*apt-get install apache2*

*apt-get install openssl # már telepítve van*

Engedélyezzük az SSL használatát:

*a2enmod ssl*

Engedélyezzük az alapértelmezett webhelyhez az SSL-en keresztüli elérést:

*a2ensite default-ssl*

A felhasználandó tanúsítványaink tárolásához hozzunk létre egy mappát:

*mkdir /etc/apache2/ssl*

Generáljunk saját tanúsítványt, melynek nevében szerepeljen a ***teszt*** kifejezés! *(egyetlen utasítás, egy sorban!)*

*openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/apache2/ssl/****teszt****.key -out /etc/apache2/ssl/****teszt****.crt*

A tanúsítványokat tároló mappához szabályozzuk a hozzáférést:

*chmod 600 /etc/apache2/ssl/\** # chmod 600 [filename] rw------- private non-executable file

Az SSL kulcsokat beállítjuk egy virtuális hostra, itt az alapértelmezett webhelyhez:

*nano /etc/apache2/sites-available/default-ssl.conf*

*tartalmában javítjuk:*

*<Virtualhost \_default\_:443>*

*[…]*

*SSLCertificateFile* ***/etc/apache2/ssl/teszt.crt***

*SSLCertificateKeyFile* ***/etc/apache2/ssl/teszt.key***

*[…]*

Újraindítjuk az Apache kiszolgálót:

*systemctl reload apache2*

A kliensen ellenőrizze a web szerver működését!

A böngésző címsorába írjuk be: [*https://www.teszt.local:*](about:blank)*443*

**LINUX SSH telepítése**

* A Linux szerverre telepítsük **az előre letöltött, de még nem telepített** **OpenSSH** **kiszolgáló alkalmazást**!
* A kiszolgáló legyen elérhető az ***ssh.teszt.local*** néven, a Windows szerverre telepített DNS kiszolgáló címkeresési zónájába vegye fel az ***ssh*** nevet!
* Állítsa be a konfigurációs állományában, hogy ne az alapértelmezett ***22***-es, hanem a ***2222***-es porton működjön a szolgáltatás!
* Engedélyezzük a rendszergazda SSH-n keresztüli kapcsolódását a kiszolgálóhoz!
* a telepített ***PuTTY*** nevű program segítségével kapcsolódjunk a kiszolgálóhoz és ***mentsük a beállítást***! (kiszolgáló: ***ssh.teszt.local*** port: ***2222*)**

Telepítsük az OpenSSH kiszolgáló alkalmazást

apt-get install openssh-server

Állítsuk át az alapértelmezett portot:

nano /etc/ssh/sshd\_config

keressük meg a # port 22 kifejezést tartalmazó sort és módosítsuk:

port 2222

Ha szeretnénk hogy a rendszergazda bejelentkezhessen SSH-n keresztül:

PermitRootLogin yes

A rendszergazda használhatja az SSH-t jelszó nélkül (pl. hogy a jelszava ne haladjon át a hálózaton):

PermitRootLogin without-password

Indítsuk újra az ssh kiszolgálót:

systemctl restart ssh

***FTP kiszolgáló:***

A Linux kiszolgálón ***az előre letöltött, de nem telepített ProFTPd szerver*** felhasználásával, konfigurálja a kiszolgálót:

* A tartományi felhasználók közül kettőt hozzon létre itt is egy ***ftpgroup*** nevű csoportban, hogy be tudjanak jelentkezni az FTP kiszolgálóra! (*példánkban* ***helga*** *és* ***ivan*** *a két felvett felhasználó)*
* Az ***ftpgroup*** nevű csoport tagjain kívül más ne használhassa az FTP kiszolgáló szolgáltatásait!
* A rendszergazda felhasználó ne használhassa az FTP szolgáltatást!

*Telepítsük a ProFtpd kiszolgálót:*

*apt-get install proftpd*

*Hozzuk létre a csoportot:*

*addgroup* ***ftpgroup***

*1. ha minden felhasználónak saját könyvtára lesz az* ***ftpRoot*** *mappán belül:*

*adduser* ***helga*** *-shell /bin/false -home /ftpRoot/****helga*** *# jelszó: helga*

*adduser* ***ivan*** *-shell /bin/false -home /ftpRoot/****ivan*** *# jelszó: ivan*

*adduser* ***helga******ftpgroup***

*adduser* ***ivan******ftpgroup***

*2. vagy ha közös könyvtárat hozunk létre a másik két felhasználónak (****anna, emma****):*

*adduser* ***anna*** *-shell /bin/false -home /ftpRoot # jelszó: anna*

*adduser* ***emma*** *-shell /bin/false -home /ftpRoot # jelszó: emma*

*adduser* ***anna******ftpgroup***

*adduser* ***emma******ftpgroup***

*chmod -R 1777 /ftpRoot/*

*nano /etc/proftpd/proftpd.conf tartalmazza:*

*DefaultRoot ~ a felhasználók nem tudnak kilépni a saját könyvtárukból!*

*<Global>*

*RequireValidShell off*

*</Global>*

*<Limit LOGIN>*

*AllowGroup* ***ftpgroup*** az ***ftpgroup*** csoport tagjai beléphetnek FTP-re,

*DenyAll de* mindenki másnak tiltjuk a belépést FTP-re

*</Limit>*

*Indítsuk újra a proftpd szolgáltatást:*

*systemctl restart proftpd*

*Ötletes megoldás lehet:* *(minden csoportnak tiltjuk a hozzáférést amelynek nem ftpgroup a neve)*

*<Limit LOGIN>*

*DenyGroup !****ftpgroup***

*</Limit>*