Yabancı Bir Kurum'da AD veya SAMBA4 Domain'e alma

1. Gerekli Paketler Kurulur:

a) apt install **samba**

b) apt install **winbind krb5-user ntpdate libpam-krb5 libnss-winbind libpam-winbind**

2. Domain bilgileri öğrenilir:

a) samba-tool domain info **TEST.NET**

* Bu adımda domain adı sonucunda invalid IP address bilgisi dönüyorsa /etc/resolv.conf dosyası içerisine DNS sunucusunun adresi girilmelidir.
Çıkan sonuç aşağıdaki gibi olacaktır:

Forest	: test.net
Domain	: test.net
Netbios domain	: TEST
DC name	: TDC1.test.net
DC netbios name	: TDC1
Server site	: İçerik
Client site	: İçerik

Bilgisayarın hostname'i istenilen şekilde düzenlenir:
b) hostname **yenihostname**
c) echo "**yenihostname**" > /etc/hostname
d) ***/etc/hosts*** dosyasının içerisinde de gerekli hostname düzenlemesi yapılmalıdır.

3. Samba Ayarlarını düzenlemek:

a) Bu bilgiler ışığında ***vim /etc/samba/smb.conf*** dosyasının içi şu şekilde yapılmalıdır. Kalın karakterli bölümler değiştirilecek, diğer kısımlar domaine alma işlemi için değiştirilmeyecektir:

```
[global]
workgroup = TEST
domain logons = yes
netbios name = yenihostname
server string = yenihostname
realm = TEST.NET
idmap uid= 10000-20000
idmap gid= 10000-20000
template shell = /bin/bash
template homedir = /home/%D/%U
winbind enum groups = yes
winbind enum users = yes
winbind use default domain = yes
client use spnego = yes
client ntlmv2 auth = yes
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
usershare allow guests = yes
usershare owner only = false
hosts allow = all
```

security = ADS

Bu ayarları yaptıktan sonra workgroup bilgisinin doğruluğunu kontrol etmek için;
b) net ads workgroup
Workgroup: **TEST**

c) net ads info
LDAP server: **10.10.1.145**
LDAP server name: **TDC1.test.net**
Realm: **TEST.NET**
Bind Path: **dc=TEST,dc=NET**
LDAP port: 389
Server time: Pzt, 02 Eki 2017 08:48:12 +03
KDC server: **10.10.1.145**
Server time offset: 11
Last machine account password change: Prş, 01 Oca 1970 02:00:00 EET

d) ***/etc/hosts*** dosyasına LDAP IP'sini eklemeniz gerekmekte:
10.10.1.145 TDC1.test.net TDC1

4. Kerberos yükleme ve ayarları:

a) ***vim /etc/krb5.conf*** dosyası aşağıdaki gibi olmalıdır:

[logging]
default=FILE:/var/log/krb5.log
[libdefaults]
default_realm = **TEST.NET**
clock_skew = 300
ticket_lifetime = 24000

[realms]
TEST.NET = {
kdc = **TDC1.test.net**
admin_server = **TDC1.test.net**
default_domain = **test.net**
}

[domain_realm]
.kerberos.server = **TEST.NET**
.test.net = **TEST.NET**
test.net = **TEST.NET**

[login]
krb4_convert = true
krb4_get_tickets = false

[appdefaults]
pam = {
debug = false
ticket_lifetime = 36000
renew_lifetime = 36000
forwardable = true

krb4_convert = false
}

b) Kerberos ticket'ı almak için domain şifrenizle birlikte: (Yönetici yetkili olmasına gerek yok, yalnızca domainde ve aktif olması yeterli)

kinit **kullanıcıadı@TEST.NET**

c) kerberos ticket'ı alınıp alınmadığını kontrol etmek için:

klist

Ticket cache: FILE:/tmp/krb5cc_10537_BxPjmp
Default principal: **kullaniciadı@TEST.NET**

Valid starting Expires Service principal
25-09-2017 07:37:38 25-09-2017 17:37:37 krbtgt/**TEST.NET@TEST.NET**
renew until 25-09-2017 17:37:37

5. Bilgisayarı Domain'e alma işlemi

a) klist komutu ile kerberos ticket'ının olduğu kontrol edilir.

b) net ads info komutu ile samba ayarlarının doğruluğu kontrol edilir.

c) ntpdate **TEST.NET** komutu ile sunucu ile zaman senkronizasyonu sağlanır.

d) Aşağıdaki komut ile yönetici yetkisine sahip kullanıcıadı ile bilgisayar domaine alınır:
net ads join -U **domainyoneticikullaniciadı**
net ads join -k

6. Winbind ile giriş sağlama:

a) ***vim /nsswitch.conf*** dosyası içerisinde aşağıdakine benzer satırlarda compat'tan sonra winbind eklenir.

passwd: compat **winbind**
group: compat **winbind**
shadow: compat **winbind**

b) Giriş sorunlarını önlemek için aşağıdaki komut çalıştırılır:
session required pam_mkhomedir.so skel=/etc/skel umask=0022

c) Farklı Kerberos ve winbind sorunlarını önlemek için aşağıdaki dosyalarda ***pam_krb5.so minimum_uid=1000*** satırlarını 1000 yerine ***100000*** yapılması önerilir;

- ***vim /pam.d/common-password***
- ***vim /etc/pam.d/common-auth***
- ***vim /etc/pam.d/common-sessions***
- ***vim /etc/pam.d/common-account***

Renk	Anlamı
	Dosya üzerinde değişiklik veya ekleme yapılacak satırlar.
	Komut satırına yazılabilen komutlar.
	Komut satırı çıktıları.
	Başlık Madde Numarası.
* **Koyu** yazılan yazılar sisteme göre değiştirilecek bilgileri barındırmakta. * *eğik* yazılan yazılar dosya isimleri ve değişiklikleri belirtmektedir.	