ÖN BİLGİ

Bu belge

- https://www.syslogs.org/docs/Ag_Ayarlari.doc

resmi adresindeki veya linkin kırık olması ihtimaline karşın alternatif olarak

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/Syslogs.org_9_Ag_Ayarlari.pdf

adresindeki makaleye çalışılarak elde edilen notlarımı kapsamaktadır. Bu çıkarılan notlar belgemde alıntılar ve/veya kişisel ilavelerim mevcuttur.

1)

Sisteminizin kullandığı port numaralarını ve o portu kullanan uygulama adını /etc/services dosyasından görebilirsin.

> cat /etc/services

(Page 2)

2)

Linux işletim sisteminde tüm ayarlar metin dosyalarında saklanmaktadır. Bu sayede yapılması gereken ayarlar belirli dosyaların düzenlenmesi ile kolayca yapılmaktadır. Linux işletim sisteminde ağ ayarları da dosyalarda tutulmaktadır. İstenildiği takdirde bu dosyalar düzenlenerek, istenildiği takdirde ise grafik arayüzlü programlar kullanılarak ağ ayarlarının yapılması mümkündür. Linux'ta ağ ayarları ile ilgili dosyalar ve dizinler aşağıdaki gibidir:

- /etc/hosts
- /etc/resolv.conf
- /etc/nsswitch.conf
- /etc/services
- /etc/sysconfig/network (dosya)
- /etc/sysconfig/network-scripts (dizin)

/etc/hosts Dosyası

/etc/hosts dosyası DNS servisi kullanılmadan önce geçerli olan methottur. Bu dosya içinde makineler ile ilgili olarak makine ismi , makinenin IP adresi ve makine için kısaltma bulunmaktadır. Her makine için ayrı bir kayıt olmak zorundadır. Ağ üzerindeki bilgisayarların artmasıyla birlikte bu dosyanın kullanılması imkansız hale gelmiş ve DNS servisi geliştirilmiştir.

/etc/hosts dosyasındaki satırlar aşağıdaki formata sahiptir :

127.0.0.1 localhost.localdomain localhost
10.0.0.2 laptop.linuxegitim.com laptop

İlk satırda loopback IP numarası ve buna karşılık gelen makina ismi ve ardından kısaltma ismi vardır. Bu satırı silmemelisiniz. İkinci satırda ise laptop.linuxegitim.com makinasının IP numarası 10.0.0.2 olarak belirtilmiş ve bu bilgisayara laptop ismi ile de ulaşılabilmesi sağlanmıştır.

/etc/resolv.conf Dosyası (DNS Sunucu Ayarları)

Linux işletim sisteminde diğer Unix türevi işletim sistemlerinde olduğu gibi DNS ayarları için kullanılan dosya **/etc/resolv.conf** dosyasıdır. En basit şekilde DNS ayarlarının yapılması için **/etc/resolv.conf** dosyası aşağıdaki şekilde düzenlenmelidir.

Syntax:

nameserver DNSSunucusununIPAdresi

Example:

nameserver 160.75.2.20

/etc/nsswitch.conf Dosyası (İsim Çözümleme Sırasını Belirleme)

Linux işletim sisteminde makine ismi - IP adresi , IP adresi - makine ismi dönüşümleri için birden fazla metot kullanılmaktadır. Bu metotlar aşağıdaki gibidir :

- /etc/hosts dosyasının kullanımı
- DNS sunucu kullanımı
- NIS sunucu kullanımı

Yukardaki metotlardan hagilerinin, hangi sırada kullanılması gerektiği /etc/nsswitch.conf dosyasında tanımlanmaktadır. Bu dosyada hosts ile başlayan satırda bulunan bilgiler kullanılacak metotları ve sırasını belirler.

hosts: files nis dns

Yukarıdaki satırda belirtilen 3 methodun da kullanılabileceği belirtilmiştir. Ilk olarak /etc/hosts dosyası, eğer bulunamaz ise NIS sunucusu, yine bulunamaz ise DNS sunucusunun kullanılacağı belirtilmiştir.

/etc/services Dosyası (Servis Portları)

Bu dosya her bir servis için port eşleştirmeleri bilgisini tutar. Bu dosyanın ilk birkaç satırı aşağıda görülmektedir, bu dosya yüzlerce satır içerebilir.

```
#
# This file contains port numbers for well-known services defined by IANA
#
# Format:
#
# <service name> <port number>/<protocol> [aliases...] [#<comment>]
#
echo            7/tcp
```

```
echo            7/udp
discard         9/tcp           sink null
discard         9/udp           sink null
systat          11/tcp          users                   #Active users
systat          11/tcp          users                   #Active users
daytime         13/tcp
daytime         13/udp
qotd            17/tcp          quote                   #Quote of the day
qotd            17/udp          quote                   #Quote of the day
chargen         19/tcp          ttytst source           #Character generator
chargen         19/udp          ttytst source           #Character generator
ftp-data        20/tcp                                  #FTP, data
ftp             21/tcp                                  #FTP. control
telnet          23/tcp
smtp            25/tcp          mail                    #Simple Mail Transfer Protocol
time            37/tcp          timserver
time            37/udp          timserver
```

/etc/sysconfig/network Dosyası

Bu dosya genel ağ ayarları için kullanılan dosyadır. Bu dosya içinde sistemin ağ desteği olup olmadığı, gateway tanımı, makine ismi gibi bilgiler bulunur. Bu dosyada çoğunlukla kullanılan terimler aşağıdaki gibidir :

- NETWORKING **:** Sistemin ağ desteği olup olmadığını belirtir. Bu parametre "yes" olarak tanımlanmamış ise sistemde ağ ayarları yapılmaz.
- HOSTNAME **:** Sistemin ismini belirtir.
- GATEWAY **:** Sistemin gateway'ini belirtir

/etc/sysconfig/network-scripts Dizini

Bu dizin sistemde bulunan ağ arayüzleri için gerekli tanımların bulunduğu dizindir. Her arayüz için bir adet konfigürasyon dosyası bulunmaktadır. Konfigürasyon dosyalarının dışında arayüzlerin aktif ve pasif hale getirilmeleri için gerekli program parçalarını da içeren dosyalar bu dizin içinde bulunmaktadır.

(Page 3-6)

3)

ifconfig komutunun syntax'ı şudur:

ifconfig arayuzIsmi IPadresi [netmask AgMaskesi broadcast yayinAdresi]

Bir linux makinasına ifconfig komutu ile IP adresi verme:

ifconfig eth0 192.168.2.33 netmask 255.255.255.0 up

(!) ifconfig komutu ile verilen IP adresi bir yere kaydedilmez. Sistem restart edince kaybolur.

Bir linux makinasındaki Ethernet kartını disable konuma getirme:

ifconfig eth0 down

Bir linux makinasındaki Ethernet kartını aktif hale getirme:

ifconfig eth0 up

(Page 7)

4)

route komutu makinenin yönlendirme ile ilgili ayarlarını yapmak için kullanılan komuttur. Bu komut sayesinde makinenin yönlendirme tablosu oluşturulur. Makinenin ağ üzerinde tam anlamıyla çalışabilmesi için yönlendirme tablosunun doğru olarak yapılandırılması şarttır. Yönlendirme tablosu giden paketlerin hangi arayüz üzerinden, hangi makineye gideceği bilgilerini içerir. route komutuna hiç bir parametre gönderilmez ise mevcut olan yönlendirme tablosu gösterilir.

> route

Output:

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
160.75.100.0	*	255.255.255.0	U	0	0	0	eth0
127.0.0.0	*	255.0.0.0	U	0	0	0	lo
default	160.75.100.254	0.0.0.0		UG	0	0	0
eth0							

Bir linux makinasına default gateway adresi verme:

> route add default gw 192.168.2.1

(Page 8)

5)

Temel Ağ Komutları

- netstat
- ping
- traceroute

Netstat Komutu

netstat komutu ağ bağlantıları , yönlendirme tablosu , arayüz istatistikleri gibi ağ ile ilgili temel bilgileri göstermeye yarayan bir programdır. Hiçbir seçenek verilmediği takdirde netstat programı sistemde kullanımda olan soketler hakkında bilgi verecektir. Bu durumda yapılmış ağ bağlantıları ile ilgili olan bilgiler gözükecektir.

> netstat

Active Internet connections (w/o servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	atlas.cc.itu.edu.t:2012	mail.cc.itu.edu.tr:auth	ESTABLISHED
tcp	0	0	atlas.cc.itu.edu.t:smtp	mail.cc.itu.edu.tr:4021	ESTABLISHED
tcp	0	1	atlas.cc.itu.edu:telnet	160.75.59.68:1292	ESTABLISHED
tcp	0	0	atlas.cc.itu.edu.tr:www	212.29.64.132:6309	ESTABLISHED
tcp	0	0	atlas.cc.itu.edu.t:pop3	bio3.bio.itu.edu.t:1523	TIME_WAIT
tcp	0	0	atlas.cc.itu.edu.t:smtp	160.75.59.205:1252	TIME_WAIT
tcp	0	0	atlas.cc.itu.edu.tr:www	gw-ehv01.pnl.phil:47459	TIME_WAIT
tcp	0	0	atlas.cc.itu.edu.t:pop3	cascade.geop.itu.e:1243	TIME_WAIT

Netstat komutu çıktısının “Active Internet Connections” bölümünde bulunan sutünlar ve anlamları aşağıdaki gibidir :

- **Proto** **:** Soket tarafından kullanılan protokolü belirtir. Tcp veya udp değerlerini içerebilir.
- **Recv-Q** **:** Bu soketi kullanan programa gönderilen verinin büyüklüğünü byte olarak belirtir.
- **Send-Q** : Karşıdaki sistem tarafından alındığı onaylanmayan verinin büyüklüğünü byte olarak belirtir.
- **Local Adress:** Soketin yerel uçtaki IP adresi ve port numarasını belirtir. Eğer netstat programı -n seçeneği ile çalıştırılmamış ise IP adresi ve port numarası için çözümleme yapılır.
- **Foreign Adress:** Soketin uzak uçtaki IP adresi ve port numarasını belirtir. Eğer netstat programı -n seçeneği ile çalıştırılmamış ise IP adresi ve port numarası için çözümleme yapılır.
- **State** **:** Soketin durumunu belirtir. Soketler aşağıdaki durumlarda olabilirler:
  - **ESTABLISHED :** Soket bağlantı gerçekleştirmiş durumdadır.
  - **CLOSED :** Soket kullanılmamaktadır.
  - **LISTEN :** Soket gelebilecek bağlantılar için dinleme konumundadır.

Ping Komutu

Ping komutu çoğunlukla karşıdaki makinenin ayakta olup olmadığını kontrol etmek için kullanılır. Eğer ping isteğine cevap gelmiyor ise uzaktaki makine çalışmıyor olabilir. Aynı zamanda ping komutunun çıktısından iki makine arasındaki transferin ne kadar hızlı olabileceği hakkında tahmin yürütülebilir. Daha kısa sürede cevap veren bir makine ile yapılan haberleşme , daha uzun sürede cevap veren makine ile yapılan haberleşmeden coğu zaman daha hızlıdır.

- **-c sayı :** Sayı ile belirtilen kadar ping paketi gönderdikten sonra programdan çıkılmasını sağlar. Bu seçenek kullanılmadığı takdirde ping programı kullanıcıdan kapatma isteği gelene kadar çalışacaktır. En basit kapatma isteği CTRL-C tuşları verilir.

- **-i süre :** Her bir ping paketinin gönderilmesi arasında geçmesi gereken sürenin ayarlanması için kullanılır. Belirtilen süre saniye cinsindendir. Bu seçenek kullanılmadığı takdirde her bir saniyede bir ping paketi gönderilir.

Traceroute Komutu

traceroute komutu ile uzaktaki makineye giden yol hakkında bilgi alınır. Bu bilgilerden en temel olanı uzaktaki makineye giderken geçilen yönlendiricilerdir. Komutun temel kullanım şekli aşağıdaki gibidir :

traceroute [seçenekler] makineIsmi

Traceroute komutu varsayılan olarak UDP paketleri ile çalışır. UDP paketlerinde TTL (TimeToLive) değerlerini ayarlayarak geçilen geçitlerin ortaya çıkmasını sağlar. Bir yönlendirici üzerinden geçen paketi yönlendireceği zaman TTL değerini bir azaltır. Bu değer sıfır olduğu zaman paketi gönderen makineye ICMP “time exceeded” paketi gönderilir. Traceroute bu özelliği kullanarak yol bilgisini çıkarmaktadır. Örneğin ilk olarak TTL değeri 1 olan bir UDP paketi oluşturulur. Bu paket ilk yönlendiriciye geldiğinde yönlendirici kaynak makineye ICMP “time exceeded” paketi gönderir. Bu paket traceroute komutu tarafından işlenir. Daha sonra TTL değeri 2 olan bir paket gönderilir. Bu olay hedef makineye varana kadar devam eder.

Başlangıç TTL değeri istenildiği takdirde -f seçeneği ile ayarlanabilmektedir.

> traceroute -f 3 www.metu.edu.tr

(Page 14-16)

6)

Temel Ağ Programları

- Telnet Programı
- Ftp Programı

Telnet

Telnet programı uzaktaki sunucu ile TELNET protokolü ile haberleşmeyi sağlayan bir programdır. Bu program sayesinde uzaktaki makinede kullanıcıya bir çalışma alanı açılır. Kullanıcının gerçekleştirdiği her işlem uzaktaki sunucuda gerçekleşir.

Kullanıcı telnet programı ile uzaktaki bir sunucuya bağlandığı takdirde kendisinden kullanıcı ismi ve şifre isteyen bir ekranla karşılaşacaktır. Bu ekranda gerekli bilgileri girdikten sonra kullanıcı için sistemde tanımlı olan kabuk programı çalışmaya başlayacak ve kullanıcıdan komut bekleyecektir.

```
[tufan@aontws4044 tufan]$ telnet atlas.itu.edu.tr
Trying 160.75.2.22...
Connected to atlas.cc.itu.edu.tr (160.75.2.22).
Escape character is '^]'.
login: tufan
Password:
Last login: Mon Aug 27 17:42:13 from dnw2kpro104
You have new mail.
[tufan@atlas tufan]$
```

Ftp Programı

FTP protokolü uzaktaki sunucudan dosya transferi için kullanılan bir protokoldür. Bu protokol kullanılarak uzaktaki ftp sunucusu ile dosya transferi yapmayı sağlayan bir çok istemci bulunmaktadır. Bu istemcilerden en yaygın olanı *ftp* programıdır. Bir çok işletim sisteminde hemen hemen aynı komutlar ve aynı arayüze sahiptir. ftp programının temel kullanım şekli aşağıdaki gibidir :

> ftp ftp.itu.edu.tr

Output:

```
Connected to atlantis.cc.itu.edu.tr.
220 ProFTPD 1.2.1 Server (ITU FTP Server) [atlantis.cc.itu.edu.tr]
Name (ftp.itu.edu.tr:root): ftp
331 Anonymous login ok, send your complete email address as your password.
Password:
230 Anonymous access granted, restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp >
```

Kullanıcı ismi ve şifre doğrulatıldıktan sonra yukarıdaki en son satırda da görebileceğiniz gibi ftp programı komut beklemek için bilgi istemi durumuna dönecektir. Bu durumda iken birçok komut kullanılabilir. Bu komutlardan en çok kullanılanları aşağıdaki gibidir:

- **ls** **:** Uzaktaki sunucuda bulunulan dizinin içeriğinin görülmesini sağlar.
- **dir** **:** ls ile aynı görevi görür. İki komutun çıktısı ftp sunucusuna göre değişebilir.
- **cd** **:** Uzaktaki sunucuda bulunulan dizini değiştirmek için kullanılır.
- **get** **:** Uzaktaki sunucudan bir dosya almak için kullanılır.
- **mget** **:** Uzaktaki sunucudan birden fazla dosya almak için kullanılır.
- **put** **:** Uzaktaki sunucuya bir dosya koymak için kullanılır.
- **mput** **:** Uzaktaki sunucuya birden fazla dosya koymak için kullanılır.
- **bye** **:** Ftp bağlantısını kapatmak için kullanılır.

(Page 17-18)