Linux IPCHAINS NASIL

Yazan:
Halis Osman Erkan
<hoerkan (at) bornova.ege.edu.tr>

23 Ocak 2007

Özet

Linux'un geliştirilmiş güvenlik duvarı yazılımı Ipchains'in NASIL sağlanacağı, kurulacağı ve yapılandırılacağı anlatılıyor, ayrıca kullanımı hakkında biraz fikir verilmeye çalışılıyor.

ipchains, 2.6.x çekirdekler tarafından desteklenmemektedir. Onun yerine **iptables** kullanılmaktadır. 2.4.x çekirdeklerde ise ikisinden birini kullanmak mümkündür. — Ocak 2007, belgeler.org

Konu Başlıkları

1. Giriş . . . 4
1.1. Telif Hakkı ve Lisans . . . 4
1.2. Feragatname . . . 4
2. Nedir? . . . 4
2.1. Ipchains Nedir? . . . 4
2.2. Hangi Sürüm? . . . 4
2.3. Neler Lazım? . . . 4
2.4. Hedef? . . . 4
3. Genel . . . 5
3.1. Genel Olarak Ipchains . . . 5
3.2. Kural Koşul Tanımlamaları . . . 5
3.3. Yaptırımlar . . . 6
3.3.1. Port Numaraları . . . 7
3.4. Firewall Kurarken . . . 7
3.4.1. Daha Neler Yapılabilir? . . . 7
3.4.2. Hangi Portlar? . . . 8
3.4.3. Betik Üzerinden Çalıştırma . . . 9
3.4.4. Güvenlik Duvarı Çatısını Kurmak . . . 10
4. Uzman . . . 10
4.1. Taklit Etme (spoofing) . . . 10
4.2. Paketlerin Bölünmesi . . . 11
4.3. Paket Sayımı . . . 11
4.4. Gelen Paketlerin Yapısına Müdahale . . . 11
4.5. Paketin TOS (Types Of Services) Kısmının Kontrolü . . . 11

4.6. TCP Bağlantı İsteklerinin Engellenmesi 12
5. Kümeler 13
5.1. Küme işlemleri 13
5.2. Kümeler üzerinde işlem yapan komutlar 14
6. Kaynakça 14
GNU Free Documentation License 15

Geçmiş

0.3	26 Eylül 1999	Halis Osman ERKAN hoerkan@bornova.ege.edu.tr

1. Giriş

1.1. Telif Hakkı ve Lisans

1.2. Feragatname

2. Nedir?

2.1. Ipchains Nedir?

Ipchains Linux çekirdeğinin 2.1.102 ve yukarı sürümlerinde desteği bulunan, çekirdek üzerinde bir güvenlik duvarı yönetim programıdır. Daha eski çekirdeklerde bulunan `ipfwadm`'nin yerini almasına karşın kullanımı ve özellikleri `ipfwadm`'den çok farklıdır. `ipfwadm`'nin yapamadığı defragment özelliği ve !(NOT–tersi) işlemimi gibi gelişmiş özellikleri bulunmaktadır.

2.2. Hangi Sürüm?

Ipchains'in 1.3.8 sürümü mevcuttur (şu gün için) ama 1.3.4 sürümünün daha güvenilir ve kalıcı olduğunu belirtmekte yarar görüyorum. Kullandığınız ipchains sürümünü öğrenmek için

```
# ipchains --version
```

komutunu kullanabilirsiniz.

2.3. Neler Lazım?

Çekirdek 2.1.102 üzeri veya 2.0.x + yama gereklidir.Bu belgede 2.0.x türü çekirdekler için ayarlamalardan bahsedilmeyecektir. Bununla beraber çalıştıracağınız makina bir sunucu olacaksa son çıkan kararlı çekirdeği indirip kurmanız mantıklıdır. Bu belgede anlatılacak örnekler de 2.2.10 (şu anda bulunan son kararlı çekirdek) çekirdeği üzerinde örneklenecektir.

Çekirdeğiniz şu destekler sağlanmış olarak derlenmiş olmalıdır. Çekirdek derlenmesi icin Çekirdek–NASIL belgesine başvurabilirsiniz.

Cekirdek 2.1.x | 2.2.x icin

```
  CONFIG_FIREWALL = y
  CONFIG_IP_FIREWALL = y
```

2.4. Hedef?

Güvenlik duvarı mantığında hedeflenen makinanızın veri iletişiminde kullandığı portların ve bu portlar üzerinden yapılan veri alışverişinin kontrolüdür. Bu kontrolü sağlamak için bazı portların kapatılması; bazı portların sadece bir tür veri alışverişine izin vermesi; sadece yönlendirme yapması gibi metodlar gereklidir.

Portları dinleyip gelen paketleri sorgulamak ve istenilen türdeki veri paketlerini `yakalayıp` bu paketler için tanımlayacağınız `yaptırım`ları uygulamak da Ipchains yardımıyla mümkündür. Bu iş için daha önceden `ipfwadm` kullanılıyordu.

3. Genel

3.1. Genel Olarak Ipchains

Ipchains'de öntanımlı gelen veya kullanıcının tanımlayabileceği kural kümeleri (`chain` – burada küme diye bahsedilecek) sorgulamaları yürütür. Bu kümeler gelen paketleri sorgular ve tanımlara uyan paketleri yakalarlar. Öntanımlı olarak gelen 3 adet küme vardır:

input
: Makinanıza gelen paketler için geçerlidir. Bunun içine makinanın kendi haberleşmesi de dahildir.

output
: Makinanızdan çıkan paketler için.

forward
: Makinanız maskeleme yapıyorsa.

Bunlar haricinde kullanıcılar kendi kümelerini tanımlayabilirler veya öntanımlı kümeleri kullanabilirler. Bu komut `eth0-in` adlı bir küme oluşturur:

```
# ipchains -N eth0-in
```

`ipchains` komutuyla kullanılabilecek parametreleri 3 kısma ayırabiliriz:

- `[-p|-s|-d ...]` gibi sorguları düzenleyen parametreler.
- `[-N|-D|-X ...]` gibi kümeler zerinde işlem yapan parametreler.
- `[--version] [-help] ...` genel işlemler yapan parametreler.

3.2. Kural Koşul Tanımlamaları

Gelen / gönderilen / yönlendirilen her paket için kümeler ve kümeler altında gruplanmış kurallar olduğunu belirtmiştik. Her paket durumuna göre bu kurallarla karşılaştırılıyor ve yakalanırsa (kurallara uyarsa) belirtilen yaptırımlar paket üzerinde uygulanıyordu. Yani ben istersem `155.223.3.202` adresinin 21. portundan benim Linux makinemdeki 1025. geçici (ephemeral karşılığı olarak) porta gelen ftp isteğini reddedebilirim / kabul edebilirim / yerel herhangi başka bir porta yönlendirebilirim.

Şimdi paketi kabul etmeyen bir ipchains satırını inceleyelim:

```
# ipchains -A input -p tcp -s 155.223.3.202/32 -d 155.223.64.10/32 -j REJECT
            |        |      |                |   |               |   | |
            +---+    +--+   +------------+   |   +-----------+   |   | +-----+
            |   |    |  |   |            |   |   |           |   |   | |     |
              1        2          3         4          5       6   7    8
```

1. Burada `input` kümesi içinde (bu küme öntanımlı bir kümedir kullanıcının herhangi bir küme tanımı yapmasına gerek yoktur) kuralın nereye yerleştirileceği belirtilir.

   `-A`, kural kümenin sonuna eklenecek demektir. Çoğu durumda kuralların diziliş sırası önemlidir.

2. Hangi protokol için bu testin yapılacağı belirlenir. Burada protokol `tcp` seçilmiştir.

3. Kaynak makinanın adresidir. Bu adres bir ip olacağı gibi bir alan adı da olabilir.

4. Adresin ağ maskesidir. Buradaki sayı `255.255.255.255` olan maskeyi ifade eder. `255.255.255.255` için soldan itibaren aralıksız bit sayısı= 32.

5. Paket için hedef makina tanımı; 3'deki gibidir.

6. Hedef makinanın ağ maskesi.

7. Şu ana kadar olan kısımlar paketin test edileceği şartlardı. Eğer paket bu koşullara uyan paketse yani aranılan paketse bu pakete ne gibi bir yaptırım (policy) uygulanacağı burada belirtilir.

8. Yakalanan paket kabul edilmeyecektir (ayrıntılı açıklama *Yaptırımlar* (sayfa: 6) bölümünde bulunabilir).

3.3. Yaptırımlar

Yukarıdaki örnekte yakalanan paket reddedildi. Yani paketi gönderen makinaya (155.223.3.202) gelen `tcp` paketinin reddedildiğini belirten bir `ICMP` paketi geri gönderildi; başka neler yapılabilirdi?

DENY
: Paket öldürülebilir. Yani paketin çıktığı makinaya hiçbir geri bildirim yapılmaz. Bu biraz kabaca görünse de portlarınızı tarayan bir *portscan* esnasında bu işlemi karşıdaki için daha uzun bir hale getirir. Portlarınızı tarayan bu *meraklı* her seferinde `timeout` beklemek zorunda kalır.

REJECT
: Paket reddedilir ve geriye bilgisi döner.

ACCEPT
: Paket bir işleme tabi tutulmadan yoluna devam eder. Kabul edilir.

MASQ
: Eğer makinanız arkada bir kaç sisteme maskeleme hizmeti veriyorsa (masquerade–howto incelenebilir) makinanız ve dolayısıyla ethernet kartlarınız üzerinden o sistemlere ait paketler taşınmalıdır. Bu yaptırım kullanıcı tanımlı kümelerde veya öntanımlı `forward` kümesinde kullanılabilir. Çekirdekte ise `CONFIG_IP_MASQUERADE` tanımlanmalıdır.

  `155.223.3.0/255.255.255.0` ağını elimizdeki bir makina ile maskelediğimizi farzedersek maskeleme ayarları şu şekilde yapılabilirdi:

```
# ipchains -A forward -p all -s 155.223.3.0/24 -d 0/0 -j MASQ
                          |                            |
                    tcp/udp/icmp                   yaptırım
```

REDIRECT
: Eğer çekirdeğe `CONFIG_IP_TRANSPARENT_PROXY` desteği verilmiş ise yakalanan paket bir başka YEREL porta yönlendirilebir. Proxy kullanmak için web isteklerini proxy'ye yöneltmek gerekir. Bu durumda yapılmasi gereken ise 80. port isteklerini 8080 porta ve/veya 8081'i 8080'e yönlendirmektir.

```
# ipchains -A input -p tcp -s 0/0 -d 155.223.3.202 80 -j REDIRECT 8080
```

3.3.1. Port Numaraları

Bu arada port numaralarına da değinmek gerek; port numarası için iki tam sayı ayrılmıştır `port_a:port_b` biçeminde. Alabileceği değerler –doğal olarak– 0 ile 65536 arasındadır. Belirtilmeyen port max veya min değer alır. Yani:

```
 1023:          -->   1023 - 65535
:1023           -->   0    - 1023   portları belirtir.
```

`!` parametresi de geçerlidir:

```
! 6000:6010    -->   1..5999 ve 6011..65536 portlar,
! 22           -->   22. port hariç tümü manasına gelir.
```

değer girilmezse tüm portlar ele alınır.

3.4. Firewall Kurarken

3.4.1. Daha Neler Yapılabilir?

Güvenlik duvarı kurarken genel olarak izlenen yol belirli bir sınırın altındaki portların tamamını kapatmak ve makinada verilecek servisler gözönüne alınarak sadece gerekli portları açmaktır. Bu şekilde bir ölçüde korunma sağlanır.

Örnek:

```
# ipchains -F input
# ipchains -F forward
# ipchains -F output
```

veya

```
# ipchains -F
```

ve

```
# ipchains -P input ACCEPT
# ipchains -P forward ACCEPT
# ipchains -P output ACCEPT
```

Bu şekilde daha önceden tanımlı olması muhtemel ipchains tanımlarını silmiş olduk. Mutlaka güvenlik duvarı betiğinizin başında bulunması gereklidir. Daha önceden kazara eklenen bir komut veya deneme amaçlı açılan bir port güvenlik duvarı üzerinde önemli delik oluşturabilir. Veya o an sizin dışarıyla olan bağlantınız kesebilir. (`output DENY` gibi)

Böyle bir yapıyı oluştururken temel olarak tamamen birbirinin tümleyeni olan iki yöntemden biri kullanılabilir:

```
# ipchains -P input DENY
# ipchains -P forward DENY
# ipchains -P output ACCEPT
```

Bütün öntanımlı kümeler için ana yaptırımları tanımladık. Burası paket kurallardan geçip yakalanmadığında uygulanır. Yani şu anda elimizdeki giriş portları kapalı durumda.Kullanacağımız her portu açmamız gerekli.

VEYA

```
# ipchains -P input ACCEPT
# ipchains -P forward ACCEPT
# ipchains -P output ACCEPT
```

Şeklinde tanımlar yapıp belli portları kapatmak ve istemediğimiz bağlantıları yakalamak gereklidir. Kolayca anlaşılacağı gibi ikinci yol yakalanmayan paketleri kabul eder yani gözümüzden kaçan bir durum olduğunda port açık kalır. Özellikle `ipfwadm`'den kalma bir alışkanlıkla tanımlayacağınız tablolar bu şekilde olabilir. AMA birinci yöntem her durumda ikinciden daha emindir.

Eğer gözümüzden kaçan bir durum varsa; hiç önemli değil; kabul edilmeyecektir. Tabii ki bu bahisler çıkış kümesi olan output için geçerli değildir.Yapının bu şekilde kurulması daha zor görünse de güvenlik duvarı bir defa ayağa kalktıktan sonra da bir zorluk çıkmaz.

Şu durumda bütün öntanımlı yaptırımları DENY kabul ediyoruz. Daha önce bahsettiğimiz üzere REJECT kullanmadık. Elimizde dışarıdan hiçbir bağlantı kabul etmeyen ve hiçbir bağlantı yönlendirmeyen (`forward`) bir güvenlik duvarı var. `Output` için de özel ve çok geçerli bir sebep olmadıkça `ACCEPT` kullanmak mantıklı olacaktır. Aksi takdirde çoğu durumda kendimizi hapsetmiş oluruz.

3.4.2. Hangi Portlar?

Makinanın (sunucu) ne tür hizmetler vereceğini saptamamız ve bu hizmetler için hangi portlara ihtiyaç duyacağımızı belirlememiz gerekir. Bunun için elimizde hazır olan kaynakları kullanabiliriz. `/etc/services` dosyası bize yeterli bilgiyi verecektir. Örnek olarak `ftp` hizmeti verebilmek için hangi portlara ihtiyacımız olduğunu saptayalım:

```
# cat /etc/services | grep ftp

  ftp-data    20 tcp
  ftp         21 tcp
```

Anlaşıldığı üzere `ftp` için 20. port ve 21. portların açılması gerekli. Bu portları sadece `tcp` protokolü için açmamız yeterli olacaktır.

Böylece kullanılmayan `udp` protokolü için bir boş port bırakmamış oluruz.

```
# ipchains -A input -p tcp -s 0/0 -d 155.223.3.202/32  20 -j ACCEPT
# ipchains -A input -p tcp -s 0/0 -d 155.223.3.202/32  21 -j ACCEPT
```

ya da

```
# ipchains -A input -p tcp -s 0/0 -d 155.223.3.202/32  20:21 -j ACCEPT
```

komutları `input` kümemize *herhangi bir yerden* `tcp` *ile (doğal olarak) 20 ve 21. portlara istek gelirse bu isteği yakala ve kabul et* manasına gelen satırı ekler .(–A= küme sonuna ekle; append; bkz. *Kümeler* (sayfa: 13))

Eğer e–posta alışverişini sağlamak istersek:

```
# ipchains -A input -p tcp -s 0/0 -d 155.223.3.202/32 25 -j ACCEPT
```

`ssh` için:

```
# ipchains -A input -p tcp -s 0/0 -d 155.223.3.202/32 22 -j ACCEPT
# ipchains -A input -p udp -s 0/0 -d 155.223.3.202/32 22 -j ACCEPT
```

Dikkat edilirse `ssh` icin 22. port hem `tcp` hem de `udp` olarak açıldı.

Özel olarak bildiğimiz bir makinadan telnet kabul edelim:

```
# ipchains -A input -p udp -s 10.1.10.3/32 23 -d 155.223.3.202/32 23 -j ACCEPT
```

Bizim de aynı şekilde çıkmamız gerekirse (şu durumda gerekmiyor çünkü `output` yaptırımı `accept`) şu satırı da eklememiz gerekir.

```
# ipchains -A input -p udp -d 155.223.3.202/32 23 -d 10.1.10.3/32 23 -j ACCEPT
```

Bunun kısa yolu ise yukarıdaki komutlardan birini –b parametresiyle kullanmaktır. (–b: [b]idirectional – iki yönlü kip).

Benzer şekilde `web`, `domain`, vb. portlar da ihtiyaca göre açıldıktan sonra rahatlayabiliriz. Tabii ki bu onlarca komutu her sistem açılışında da yazmak işkence olur kaldı ki çoğu zaman acil olarak güvenlik duvarının devreden çıkması gerekebilir. Bir –F komutu sonrası kuralların tamamı (genel yaptırımlar hariç) iptal edilir. Bu sebeple yaptığımız bu ayarları yani oluşturduğumuz kural kümelerini saklamalıyız. Bunu bir betik yardımıyla da yapabiliriz. Ama ipchains komutunun bu işi görebilecek işlevleri olduğunu bilmek de yararlı olur.

3.4.3. Betik Üzerinden Çalıştırma

Burada vereceğim basit bir betik size bu konuda yardımcı olabilir. Bu betik `/etc/firewall.conf/` adlı tanım dosyanızdaki komutları işletir.

Gerekirse de –F (`flush`) ile iptal eder istenirse yeniden çalıştırır:

```
#!/bin/bash
#ipchains yükleme betiğidir
#/etc/firewall.conf dosyasını okur

set -e

case "$1" in

        start)
        echo "Güvenlik Duvarı çalıştırılıyor..."
        /etc/firewall.conf
        echo "TAMAM"
        ;;
        stop)
        echo "Güvenlik Duvarı durduruluyor..."
        /sbin/ipchains -F
        /sbin/ipchains -P input ACCEPT
        /sbin/ipchains -P forward ACCEPT
        /sbin/ipchains -P output ACCEPT
        echo "TAMAM"
        ;;
        restart)
        echo "Güvenlik Duvarı yeniden çalıştırılıyor..."
        /sbin/ipchains -F
        /sbin/ipchains -P input ACCEPT
        /sbin/ipchains -P forward ACCEPT
        /sbin/ipchains -P output ACCEPT
        /bin/sleep 1
        /etc/firewall.conf
        echo "TAMAM"
        ;;
        * )
        echo "Kullanımı : $N {start|stop|restart}" >&2
        exit 1
        ;;
esac
```

```
exit 0
```

3.4.4. Güvenlik Duvarı Çatısını Kurmak

`firewall.conf` dosyasını oluşturmak içinse 2 yolunuz var:

1. Yazdığınız komutları bir metin düzenleyici (pico, emacs) ile `/etc/firewall.conf` dosyasına ekleyebilirsiniz.
2. Tüm komutlar bellekteyken

   ```
   # ipchains-save > firewall.conf
   ```

   komutu ile dosyaya eklenir. Parametresiz girilen komut bütün kümeleri ekler; istenirse

   ```
   # ipchains [küme ismi] > firewall.conf
   ```

   ile istenilen küme yazılabilir.

   Sonra

   ```
   # ipchains-restore < firewall.conf
   ```

   ile yeniden yüklenebilir. Burada bellekte halihazırda kullanımda olan `ipchains` kümeleri varsa bunları silmek için sizden onay bekler. Eğer `-f` parametresini de eklerseniz bu uyarıyı almazsınız.

4. Uzman

Buraya kadar `ipchains` ile basitce bir güvenlik duvarı nasıl kurulur anlatıldı. Bu aşamadan sonra ise duyarlı ve daha güvenilir güvenlik duvarı kurulumu ve `ipchains` komutunun daha ayrıntılı kullanımı anlatılacaktır.

4.1. Taklit Etme (spoofing)

`ipchains -i [arabirim]` Bu parametre ile paketin makinaya hangi arabirim aracılığıyla geldiğini kontrol edebiliriz. `lo` ,`eth*`, `ppp*` bu arabirimlerden biri olabilir. Bu şekilde beklemediğimiz yerden gelen paketleri de kontrol edebiliriz. İki ethernet kartı aracılığıyla arkada bir ağı maskeleme ile internete çıkarıyor olabiliriz. Ve sadece arkadaki ağ üzerinden gelen paketleri maskelemek için sadece IP kontrolu yetmeyebilir. Arabirim kontrolü ile ip–taklidini önüne bir ölçüde geçilebilir. Örneklersek:

`10.1.10.x` ağına `eth1` aracılığıyla maskeleme yaptığımızı düşünürsek maskeleme tanımında arabirim belirtmek; kendini bu adrestenmiş gibi gösteren birinin; bu ağa tanıdığımız haklardan yararlanmasını engelleyecektir.

```
# ipchains -A forward -s 10.1.10.0/24 -d 0/0 -i eth1 -j MA
                                             ^^^^^^^
# ipchains -A forward -s 10.1.10.0/24 -d 0/0 -i eth+ -j MASQ
                                                ^
```

```
eth+ = eth1 eth2 .....
ppp+ = ppp1 ppp2 .....
```

şeklinde de olabilir.

IP taklidinin engellenmesi için daha başka yollar da vardır. Güvenlik duvarı genelde bu işi tam karşılamaz. Mesela çekirdek 2.1 den sonrası ip'si `127.x.x.x` gibi davranan paketleri kabul etmez. Benzer şekilde çekirdekten kaynak adres kontrolü (Source Adres Verification) özelliği kullanılabilir.

`/proc/sys/net/ipv4/conf/all/rp-filter`'a değer yüklenebilir.

```
# echo "1" > /proc/sys/net/ipv4/conf/all/rp-filter
```

Daha geniş bilgi için Çekirdek–NASIL[B5] incelenebilir.

4.2. Paketlerin Bölünmesi

Paketler, kullanılan araçların bir defada açabileceği boyutlarda taşınırlar. `MTU` ile belirtilen (**M**aximum **T**ransmission **U**nit) belli boyutlara uyulmak zorunludur. Mesala `FDDI` bir ağ 4000 baytlık paketler gönderebilirken buraya bağlı olan bir ethernet ağ ise ancak 1518 bayt olarak bu paketleri alabilir. Bu durumda büyük gelen paket bölünür (*fragmentation*). Bölünen paketler `Fragment Header` denilen bir başlık ile tanınırlar. Böyle bir paketin sadece ilk parçası `ipchains` tarafından kontrole tabi tutulabilir. Diğer paketler kontrole tabi tutulamazlar. Pek önemli görülmese de bu durumun da gözönünde tutulması kimseye bir şey kaybettirmez.

`ipchains` içinde bu durumu engellemek için `-f` parametresi kullanılabilir. Yalnız bu durumda bölünmüş olan paketin iki ve daha sonraki alt paketleri anlaşılabilir. Port adresi ise okunamaz. Bu sebeple de bu parametre ile port numarası kullanılmaz.

Özellikle `ICMP` paketleri kullanan exploitler için iyi bir savunma mekanizması oluşturulabilir. `ICMP` paketleri bölünmeyecek kadar küçük paketlerdir. (ayrıca bölünmeyi üzerlerindeki `don't fragment` biti de engeller). Yani bölünmüş bu tür paketleri reddetmek yararınızadır.

```
# ipchains -A -t icmp input -s x.x.x.x/x -d y.y.y.y/y -f -j DENY
                 ^^^^                                  ^^^
```

4.3. Paket Sayımı

Her bir paket yakalandığında; paketle alakalı çekirdek tarafından kontrol edilen iki sayaca işlenir. Birinci sayaç her yakalanan pakette 1 diğeri ise paket boyutu kadar artar. Paketin sayaçlarının artışı için ille de pakete bir yaptırım uygulanmış olması gerekmez. Yakalanması yeter şarttır.

```
# ipchains -A output -p tcp -s 155.223.3.202/32 6667 -d 0/0
```

komutu ile makinanızdan genelde `irc` için kullanılan `6667`. port üzerinden kaç defa paket yollanmış ve toplam ne kadar veri akmış öğrenebilirsiniz.

Sayım sonuçlarını `-L [küme] -v` ile görebilirsiniz.

```
# ipchains -L output -v
```

Eğer istenirse yakalanan paketlerin bir disk sahasına depolanması da mümkündür. `-o [max boyut]` parametresi ile kullanılır.

4.4. Gelen Paketlerin Yapısına Müdahale

Ipchains yakalanan paketlerin üzerinde belirli işlemler yapabilmenizi sağlar. Paketi işaretleyebilir; TOS (*types of service*) bilgisini değiştirebilir; hangi tür paketin ne kadar yakalandığını ve ne kadarlık bilgi aktığını anlayabilirsiniz.

Eğer isterseniz de gelen paketleri işaretleyebilirsiniz. Gelen paketler 32bit işaretsiz bir sayı ile işaretlenebilir. Hatta birden çok defa işaretlenebilir. Hiç işaretlenmemiş bir paketin işaret değeri 0 dır. Paket her işaretlendiğinde tanımlanan 32 bit sayı kadar artırılır ve azaltılır.

Eğer *kernel hacking* konusunda meraklı iseniz başka NASILlar öneririm.

`-m +-[32 bit sayı]` biçemindedir.

4.5. Paketin TOS (*Types Of Services*) Kısmının Kontrolü

Gelen paket içinde bulunan TOS istenirse iki onaltılık 8 bit sayı ile AND'lenip sonuç ikinci değer ile XOR'lanır.

Örnek olarak ftp'de *minimum delay* ve *maximum throughput* sağlanmalıdır.

Çünkü karşıdaki kullanıcı komutları girecek (*minimum delay* burada) ve dosya aktarımı yapacaktır (dosya aktarımı için ise *maximum throughput*).

Bunları sağlamak için de TCP paketlerinin başında bulunan 4 bit ile oynanabilir. Ve bir defada sadece biri 1 konumuna getirilebilir.

Bazı servisler için tavsiye edilen TOS değerleri:

Servis	Minimize delay	Maximize throughput	Maximize reliability	Minimize cost	Hex Value
Telnet/Rlogin	1	0	0	0	0x10
FTP					
control	1	0	0	0	0x10
data	0	1	0	0	0x08
any bulk data	0	1	0	0	0x08
TFTP	1	0	0	0	0x10
SMTP					
command phrase	1	0	0	0	0x10
data phrase	0	1	0	0	0x18
DNS					
UDP Query	1	0	0	0	0x10
TCP Query	0	0	0	0	0x00
zone transfer	0	1	0	0	0x08
ICMP					
error	0	0	0	0	0x00
query	0	0	0	0	0x00
any IGP	0	0	1	0	0x04
SNMP	0	0	1	0	0x04
BOOTP	0	0	0	0	0x00
NNTP	0	0	0	1	0x02

Bu değerler tavsiye edilen değerlerdir. (R.Stevens,TCP/IP,1998)

4.6. TCP Bağlantı İsteklerinin Engellenmesi

Bilindiği üzere TCP protokol olarak çok kullanılmaktadır. ftp, telnet vs. TCP paketleri ile yapılacak olan veri aktarımlarında ise TCP'nin üç–koşullu–onaylama (*three way hanshaking*) olarak adlandırılan yöntemi kullanılır.

Yöntem bir bağlantı isteği (*active open* olarak geçer) ile işlemeye başlar.

İstemci makina sunucuya SYN (*syncronise*) sayısı içeren bir paket gönderdiğinde sunucu buna SYN ve ACK (*acknowledgement*) ile cevap verir.

Üçüncü adım olarak da istemciden sadece bir ACK geri döner (*passive open*).

Daha fazla ayrıntısına girmeyeceğim bu iletişim bir TCP bağlantısı başlatır. Biz eğer makinamıza giren TCP isteklerini kontrol etmek istersek (bu sekilde TCP kullanan tüm servisler kontrol edilir; ftp, telnet, ssh, finger www vs.) ipchains'in -y parametresi yardımımıza koşar.

Bu parametre ile içinde SYN biti 1 olan ve aynı zamanda ACK ve FIN bitleri 1'e eşit olan (SYN=1 && ACK=0 && FIN=0 durumu) paketler yakalanabilir.

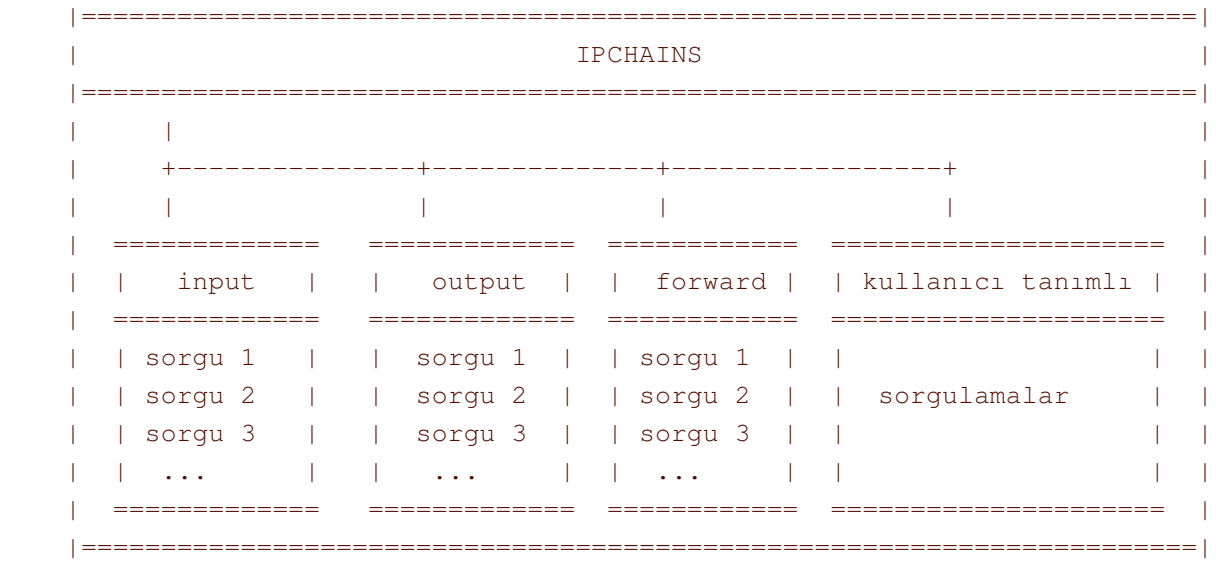
Parametrenin ! (tersi) seçeneği de vardır. (bit durumlarının tersi değil koşul sağlanmasının tersi). Ve de doğal olarak sadece TCP protokolü için kullanılır.

```
# ipchains -A input -p tcp -s 0/0 -d 155.223.3.202/32 -y -j DENY
```

Komutu ile makinaya gelen tüm SYN_REQ'ler kabul edilmemiş olur. Böylece dışardan hiçbir şekilde makinaya TCP bağlantısı yapılamaz.

Ve de bizim dışarıya TCP bağlantısı isteklerimiz de bundan etkilenmez. (çünkü bizim başlattığımız TCP'lerde de bu bitler kullanılır ne kadar sadece output kümesini ilgilendiriyor görünse de TCP'nin çift taraflı özelliğinden ötürü input kümesi de olaya girer. Ama belirttiğimiz gibi -y parametresi bizim başlattığımız TCP bağlantılarını görmez).

5. Kümeler



Ipchains ile sorgulanacak kurallar birbirinden farklı 4 tip küme içinde bulunabilirler. Kullanıcı tanımlı bir küme olması zorunlu değildir ama kullanıldığında hiyerarşik bir yapı oluşturulup daha sonraki incelemelerde kolaylık sağlanabilir.

5.1. Küme işlemleri

Şimdi ağ üzerinden ethernet kartı ile gelen bir paket için olası bir senaryo düzenleyelim:

Ulaşan paket önce input kümesi tarafından sorgulanacaktır. Sorgulamalar içinde kullanıcı tanımlı bir kümeye bağ varsa; bağ üzerinden kullanıcı tanımlı küme de işlenir, bu küme sonlandığında (RETURN veya kural sonu) kümeyi çağıran sorguya geri dönüp bir sonraki input kümesi sorgusuyla devam edecektir (bir program kodunda alt yordam çağrılması gibi). Eğer paket hiçbir sorguyla uyuşmadı ise o zaman input kümesinin genel yaptırımıyla işlenecektir (*input chain policy*). Paket ise iki türlü yakalanabilir:

1. Küme sorgusu ile

2. Kullanıcı tanımlı bir küme sorgusuna bağ ile

1. durumda koşulun içeriğinde belirtilen, paketin yakalanması sonucu uygulanacak yaptırım işlenir. (paketi kabulet, redddet, yönlendir gibi). 2. durumda ise koşulun bulunduğu kümeyi çağıran 1. türde bir yakalama söz konusu olur ve çağıran koşulun yaptırımı uygulanır.

5.2. Kümeler üzerinde işlem yapan komutlar

Görüldüğü gibi kullanıcı kendisi bir kural kümesi tanımlayabilir. Bu tanımlarda ise şu komutlar geçerlidir:

–N [*küme ismi*]

Yeni bir küme tanımlamak için kullanılır.Yalnız küme isminin 8 karakteri geçmemesi gerekir. Örneğin:

```
# ipchains -N input_eth0
# ipchains -N input_eth1
```

komutları `input_et` adlı **bir** tane küme açarlar.

–L [*küme ismi*]

Verilen kümenin içerdiği koşulları listeler. Eğer parametresiz kullanılırsa tüm tanımlı kümeleri gösterir.

```
# ipchains -L input
# ipchains -L eth0-in
```

–F [*küme ismi*]

Verilen kümenin kurallarını iptal eder. Tüm kümenin kurallarını tek tek silmek gibidir. Parametresiz kullanılırsa öntanımlı ve kullanıcı tanımlı tüm kümeleri / kuralları iptal eder. Eğer bir betik yazılacaksa en başta kuralları sıfırlamak için bulunması çok mantıklı olacaktır.

–Z [*küme ismi*]

Her koşulun çekirdekte tutulan iki adet sayacı vardır. Birisi koşulu tutan yani yakalanan paket sayısını, diğeri ise bu şekilde geçen bayt sayısını tutar. –Z (= zero) parametresi ise tutulan sayaçları sıfırlamaya yarar.

–X [*küme ismi*]

Bir kümenin tamamını silmeye yarar. Parametre girilmezse kullanıcı tanımlı bütün kümeleri siler. Yalnız bir kümenin silinebilmesi için içinin boş olması yani kural içermemesi gerekir (*rm komutuyla dizin silmek gibi*).

6. Kaynakça

1. man ipchains
2. man ipfw_adm
3. man ipfw_chains
4. ipchains–nasil (P. Russel)
5. firewall–howto
6. ip_masq howto
7. Stevens W . R , 1998, TCP/IP Vol 1 The Protocols
8. Arnett M. F. , 1995 Inside TCP/IP

GNU Free Documentation License

Version 1.2, November 2002

1. PREAMBLE

   The purpose of this License is to make a manual, textbook, or other functional and useful document *free* in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

   This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

   We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

2. APPLICABILITY AND DEFINITIONS

   This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world–wide, royalty–free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

   A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

   A "Secondary Section" is a named appendix or a front–matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

   The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

   The "Cover Texts" are certain short passages of text that are listed, as Front–Cover Texts or Back–Cover Texts, in the notice that says that the Document is released under this License. A Front–Cover Text may be at most 5 words, and a Back–Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine–readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ascii without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard–conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine–generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

3. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

4. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front–Cover Texts on the front cover, and Back–Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine–readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer–network location from which the general network–using public has access to download using public–standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

5. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a

work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front–matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties—-for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front–Cover Text, and a passage of up to 25 words as a Back–Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front–Cover Text and one of Back–Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

6. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements."

7. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

8. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

9. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

10. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

11. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version

number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

```
  Copyright (C)  year  your name.
  Permission is granted to copy, distribute and/or modify this document
  under the terms of the GNU Free Documentation License, Version 1.2
  or any later version published by the Free Software Foundation;
  with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
  A copy of the license is included in the section entitled "GNU
  Free Documentation License".
```

If you have Invariant Sections, Front–Cover Texts and Back–Cover Texts, replace the "with...Texts." line with this:

```
with the Invariant Sections being list their titles, with
the Front-Cover Texts being list, and with the Back-Cover Texts
being list.
```

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.

Notlar

Belge içinde dipnotlar ve dış bağlantılar varsa, bunlarla ilgili bilgiler bulundukları sayfanın sonunda dipnot olarak verilmeyip, hepsi toplu olarak burada listelenmiş olacaktır.

(B5) ../howto/kernel-«nasil.pdf

Bu dosya (ipchains–nasil.pdf), belgenin XML biçiminin TEXLive ve belgeler-xsl paketlerindeki araçlar kullanılarak PDF biçimine dönüştürülmesiyle elde edilmiştir.

23 Ocak 2007