IP Karalistesi NASIL

Bir RBL Denemesi

Yazan:
Deniz Akkuş

Ocak 2005

Özet

Bu belge, kendi yerelinizde bir karaliste oluşturma yöntemlerini açıklar. Karaliste yazılımının kurulması (*rbldnsd*), normal DNS ile bütünleştirilmesi (*bind9*), Internet'te mevcut olan çeşitli karalistelerin sizin yerelinizde, sizin kullanımınız için yansılanması, kendi oluşturduğunuz bir karalistenin sizin yerelinizde kullanıma açılması ve otomatik karaliste oluşumlarına örnek olarak benim yerel ağıma izinsiz portlardan ulaşmaya çalışan Türk dinamik IP kullanıcılarının karalistesinin hazırlanmasını ele alır. Eğer herhangi bir sebepten dolayı bu karalisteyi elde etmek ister iseniz, güncel sürümünü

```
$ rsync -az --delete rsync.belgeler.org::rblzzz/rbl.zzz.gz ./rbl/
```

komutu ile alabilirsiniz.

Karaliste kullanıp kullanmamanın doğru olup olmadığı, sansüre girip girmediği bu yazının kapsamı dışındadır. Bu yazıyı okumak sizi karaliste kullanmaya zorlamaz.

Konu Başlıkları

Geçmiş

2.0	26 Ocak 2005	DA <>
Belge elden geçirilerek düzenlendi.		
1.0	8 Ocak 2005	DA <>
İlk sürüm.		

Sürüm Bilgileri

v2.0

Yasal Uyarı

1. Giriş

1.1. Karalisteler nerede kullanılıyor? Nasıl oluşturuluyor?

Internet üzerinde çeşitli karalisteler gönüllüler ve ticari kurumlar tarafından, spam engelleme ve diğer çeşitli güvenlik amaçları ile oluşturulmuştur. Oldukça kapsamlı bir karaliste sayfasını http://moensted.dk/spam adresinden bulabilirsiniz.

Bu karalisteler, spam engellemek ve hatta almayı reddetmek için *Postfix* gibi posta sunucu yazılımlarında veya *spamassassin* gibi spam filtreleme yazılımlarında kullanılabilirler.

Her karalistenin oluşturulma felsefesi farklıdır. Örneğin http://countries.nerd.dk listesi, bir IP numarasının hangi ülkeden geldiğini gösterir. Kimi karalisteler Internet üzerinde spam yaptığı tespit edilmiş IP numaralarını, kimileri ise çeşitli güvenlik açıkları barındırdığı tespit edilmiş IP numaralarını toplar. Hangi karalistenin sizin için faydalı olduğunun ve sağladıkları verinin sizin işinize yarayıp yaramadığının tespiti size aittir.

1.2. Neden Internet üzerindeki karalisteler yerine kendi karaliste yansımı çalıştırayım?

Kullanım sıklığınıza bağlı olarak yerel ağınızda karaliste yansıları bulundurmak faydalı olabilir. Çok posta trafiği olan bir ağınız var ise ve bu ağı spamden korumak için yoğun bir karaliste kullanımınız var ise, karaliste kontrolleri için her seferinde ağdan dışarı sorgu yapmak yerine kendi karaliste yansınızı tutabilirsiniz.

Her karalistenin yansısını alamayabilirsiniz. Yerelinizde yansısını tutmak istediğiniz karalistenin yansı dağıtımı yapıp yapmadığını kontrol etmelisiniz. Bizim örnek olarak kullandığımız http://countries.nerd.dk ve http://www.sorbs.net/ listeleri, bütün verilerini *rsync* üzerinden dağıtıyorlar.

Kendi karaliste yazılımınızı çalıştırmanızın bir faydası da, eğer ister iseniz, sadece kendinize özel bir karaliste oluşturup kullanma imkanınızın olmasıdır. Buna girişmeden önce, ciddi bir karaliste oluşturmanın ve güncel tutulmasının ağır bir iş olduğunu aklınızdan çıkarmayın.

1.3. Dağıttığınız karaliste nedir, kullanılabilir mi?

Dağıttığım karaliste, kendi ağıma, kullanıma açık olmayan portlardan girmeye çalışan Türk kökenli ve dinamik IP'ye sahip IP'lerin listesidir. Kullanılıp kullanılmayacağı *tamamen* size kalmış. Liste otomatik olarak güncellenmektedir.

Bu listedeki veri kümesini, bu şekilde oluşturmamın sebebi, dinamik IP bloklarından gelip olmadık portlardan benim ağımı ziyaret etmeye çalışan makinaların büyük ihtimal ile ya virüslü ya da kötü niyetli olduğunu düşünmemden kaynaklanıyor. Her iki ihtimalde de, bu makinaların spam yollama ihtimali başkalarına göre daha yüksek. Ayrıca, bu yazı için bir örneğe ihtiyacım vardı.

Karalisteyi:

```
$ rsync -az --delete rsync.belgeler.org::rblzzz/rbl.zzz.gz ./rbl/
```

komutu ile alabilirsiniz.

2. Karaliste yansısının kurulması ve çalıştırılması

2.1. Karaliste yazılımının kurulması

Teorik olarak favori DNS yazılımınızı karaliste amaçları için kullanabilirsiniz. Pratikte, çok uzun alan dosyalarından oluşan karalisteleri yüklemek DNS yazılımınızı yoracaktır. Dolayısıyla en uygun çözüm, karaliste kullanımı için hazırlanmış özel ve hafif bir DNS yazılımı olan *rbldnsd* yazılımını kullanmaktır. Tabii aynı makinada iki DNS sunucusu birden çalıştığı zaman port çakışması olacaktır. Bunu engellemek için rbldnsd yazılımını başka bir port üzerinden çalıştıracağız.

Eğer Debian kullanıyor iseniz,

```
$apt-get install rbldnsd
```

komutu ile *rbldnsd* yazılımını kurabilirsiniz. Bu kurulum bir Debian makinası üzerinde yapıldığından dolayı çeşitli ayar dosyalarının yerleri başka bir dağıtımda farklı olabilir. Red Hat RPM ve tar.gz paketleri http://www.corpit.ru/mjt/rbldnsd.html adresinden alınabilir.

/etc/default/rbldnsd dosyası içerisinde RBLDNSD tanımını aşağıdaki şekilde değiştirelim:

```
RBLDNSD="- -r/var/lib/rbldns -b127.0.0.1/530 \
-l requestlog -s statlog  \
"
```

Bu tanım, *rbldns* yazılımının 127.0.0.1 adresine bağlanacağını (yani makina dışından sorgulanamayacağını), 530 no'lu port üzerinde çalışacağını, dosyalarını /var/lib/rbldns dizininde tutacağını, istekleri ve istatistikleri günlük dosyasına kaydedeceğini belirtir.

Henüz elimizde bir karaliste dosyası olmadığından dolayı şu aşamada *rbldnsd*'yi çalıştırmak manasız. Bir kaç adet karaliste yansısı elde ettikten sonra yazılımı çalıştıracağız.

2.2. Yansıları indirmek

Yansılayacağımız ilk liste, Türk IP bloklarının listesi. Herhangi bir IP adresinin Türkiye'de olup olmadığını, şu şekilde sorgulayabilirsiniz:

Sorgulanacak IP no'su: 127.0.0.1

```
$ dig +short 1.0.0.127.tr.countries.nerd.dk
```

IP numarasının sorgu için tersten yazıldığına dikkat edin.

Bu listeyi http://countries.nerd.dk adresinden ilgili bağları takip ederek, veya

```
# cd /var/lib/rbldns
# rsync rsync://nubian.blitzed.org/countries/tr.countries.nerd.dk.rbldnsd .
```

komutu ile alabilirsiniz.

İkinci listemiz de, SORBS[B10] tarafından oluşturulmuş olan dinamik IP kullanıcıları listesi. Herhangi bir IP adresinin, ISS'lerin telefonla veya ADSL/Kablo ile bağlanan ev kullanıcılarına ait olup olmadığını gösteren bu listeyi şu şekilde sorgulayabilirsiniz:

Sorgulanacak IP no'su: 127.0.0.2

```
$ dig +short 2.0.0.127.dul.dnsbl.sorbs.net
127.0.0.10
```

IP numarasının sorgu için tersten yazıldığına dikkat edin.

Bu listeyi de, SORBS[B11]'daki linkleri takip ederek veya

```
# cd /var/lib/rbldns
# rsync rsync://rsync.bliab.com/sorbs/dul.dnsbl.sorbs.net .
```

komutu ile alabilirsiniz.

Güncel olmayan bir karaliste, hiç karaliste kullanmamaktan çok daha kötüdür. Dolayısıyla bu karalisteleri yansılama işlemini bir defaya mahsus olarak yapmanın bir manası yok. Cron kullanarak karalistelerin düzenli aralıklarla güncellenmesini sağlamalıyız.

Günde bir defa güncelleme işlemini yapan cron satırı:

```
$ crontab -l
37 1 * * * cd /var/lib/rbldns; \
rsync rsync://nubian.blitzed.org/countries/tr.countries.nerd.dk.rbldnsd .
¬ 2>&1 /dev/null;\
rsync rsync://rsync.bliab.com/sorbs/dul.dnsbl.sorbs.net . 2>&1 /dev/null
```

rbldnsd dosyaların güncellendiğini otomatik olarak farkedip yeniden yüklediği için onu yeniden başlatmaya gerek yok.

2.3. Karaliste yazılımını başlatmak

`/etc/default/rbldnsd` dosyası içerisinde `RBLDNSD` tanımını aşağıdaki şekilde değiştirelim:

```
RBLDNSD="- -r/var/lib/rbldns -b127.0.0.1/530 \
-l requestlog -s statlog -f \
tr.countries.nerd.dk:ip4set:tr.countries.nerd.dk.rbldnsd \
dul.dnsbl.sorbs.net:ip4set:dul.dnsbl.sorbs.net \
"
```

Eklediğimiz satırlar, `tr.countries.nerd.dk` ve `dul.dnsbl.sorbs.net` alanlarının IP numarası olarak ilgili dosyalarda tanımlandığını belirtiyor.

Şimdi *rbldnsd*'yi başlatalım:

```
# /etc/init.d/rbldnsd start
Starting rbldnsd: rbldnsd
rbldnsd: listening on 127.0.0.1/530
rbldnsd: ip4set:tr.countries.nerd.dk.rbldnsd: 20050126 233703:
¬ e32/24/16/8=2061/3910/46/0
rbldnsd: file dul.dnsbl.sorbs.net(3): compatibility mode: specify all NS
¬ records in ONE line
rbldnsd: ip4set:dul.dnsbl.sorbs.net: 20050126 233733:
¬ e32/24/16/8=704801/271341/1628/0
rbldnsd: zones reloaded, time 0.36e/0.22u sec, mem arena=408 free=60
¬ mmap=7628 Kb
rbldnsd: rbldnsd version 0.994 (18 Dec 2004) started (1 socket(s), 2 zone(s))
```

Karalisteyi sorgulayalım. Bu sorguların, daha önce Internet'ten yaptığımız sorgulara nazaran çok daha hızlı olduğunu farkedeceksiniz.

```
$ dig +short @127.0.0.1 -p 530 2.0.0.127.dul.dnsbl.sorbs.net
127.0.0.10
$ dig +short @127.0.0.1 -p 530 1.0.0.127.tr.countries.nerd.dk
```

2.4. Normal DNS'e karalisteyi entegre etmek

Az önce kullandığımız sorgularda, `dig` komutuna hangi sunucu (127.0.0.1) ve hangi port (530) kullanması gerektiğini belirttik. Şu anda bu tanım yapılmaksızın yapılacak olan sorgular gene Internet'e yönlenir. Bu karalisteleri posta yazılımınızda veya spamassassin içerisinde kullanıyorsanız, bunlar halen daha Internet'ten çözüm-

leniyor. Bunu değiştirmenin yolu, DNS sunucunuzda bu alanları yerel karaliste yansısından sorgulamasını belirtmektir.

Örneklerin hazırlandığı sistemde Debian üzerinde Bind9 çalıştırılmaktadır. Kendi dağıtım ve DNS yazılımınıza göre yapılacak ayarlar bir nebze farklı olabilir.

`/etc/bind/named.conf` dosyası içerisinde iki yeni alan tanımı yapalım:

```
zone "tr.countries.nerd.dk" IN {
        type forward;
        forward first;
        forwarders {
        127.0.0.1 port 530;
        };
};

zone "dul.dnsbl.sorbs.net" IN {
        type forward;
        forward first;
        forwarders {
        127.0.0.1 port 530;
        };
};
```

Özellikle `forward first;` komutuna dikkat edin. Eğer DNS sunucusu bir şekilde *rbldnsd* ile iletişim kuramaz ise, eskiden yaptığı gibi Internet üzerinden çözümlemeye gidecektir.

DNS'i yeniden başlatın:

```
# /etc/init.d/bind9 restart
Stopping domain name service: named.
Starting domain name service: named.
```

Şu anda `tr.countries.nerd.dk` ve `dul.dnsbl.sorbs.net` alanlarına sistemden gelen herhangi bir sorgu, *rbldnsd*'ye yönlenecektir. Eğer bu sorguları posta sunucunuzda veya spamassassin içerisinde kullanıyor idiyseniz, bu sorguların hızlandığını göreceksiniz.

2.5. Yapmak istedikleriniz bitmiş olabilir

Eğer sisteminizde yaptığınız çeşitli karaliste sorgularını hızlandırmak amacında iseniz, buraya kadar uyguladıklarımızla bunu gerçekleştirebilirsiniz. Sıklıkla kullandığınız karalistelerin yansısını elde edip, kendi sisteminizde *rbldnsd* içerisinde çalıştıracaksınız.

Bu yazının geri kalan kısmı, benim hazırladığım bir karalisteyi örnek olarak kullanarak, kendinize ait bir karalisteyi nasıl sisteminize entegre edeceğinizi konu almaktadır.

3. Kendi karalistenizi kullanmak

3.1. Karaliste dosyasının oluşumu

Internet'te olan herhangi bir alan adı ile karışmaması için karalistemizi `rbl.zzz` alanı olarak tanımlayacağız. Herhangi bir metin düzenleyici içerisinde `/var/lib/rbldns/rbl.zzz` dosyasını oluşturalım.

Bütün DNS listeleri bir `SOA` "Start of Authority" – otorite başlangıcı – satırı ile başlar.

`/var/lib/rbldns/rbl.zzz` ilk satır:

```
$SOA 172800 bizimfirma.com.tr. root.bizimfirma.com.tr. 0 7200 7200 604800 3600
```

Dikkatinizi, `bizimfirma.com.tr. root.bizimfirma.com.tr.` ibaresine çekmek istiyorum. Alan adının Internet'te bulunan herhangi bir şeyle çakışmaması için `rbl.zzz` kullandık. Ama burada kendi gerçek alan adımızı ve ulaşılabilir bir posta adresimizi kullanıyoruz. Bundan sonra gelen tanım ise `0`. Bu da önemli. Bu, dosyanın seri numarası ve DNS'in, alan dosyasında değişiklik olduğunu farketmesinin yöntemi. `rbldns`'e özgü bir kolaylık ile, bu tanım 0 ise, dosyanın değişme tarihini seri numarası olarak alıyor.

Bundan sonra karalisteye alacağımız numaraları tanımlayacağız. Biçem,

karalisteli no : *kısa cevap* : *açıklama*

şeklinde olacak.

`/var/lib/rbldns/rbl.zzz` örnek:

```
$SOA 172800 bizimfirma.com.tr. root.bizimfirma.com.tr. 0 7200 7200 604800 3600
195.174.102.72 :127.0.0.2: Izinsiz erisim yapan TR dinamik IP -- 2005-01-08
```

3.2. Karaliste dosyasını rbldns'e entegre etmek

`/etc/default/rbldnsd` dosyası içerisinde `RBLDNSD` tanımını aşağıdaki şekilde değiştirelim:

```
RBLDNSD="- -r/var/lib/rbldns -b127.0.0.1/530 \
-l requestlog -s statlog -f \
tr.countries.nerd.dk:ip4set:tr.countries.nerd.dk.rbldnsd \
dul.dnsbl.sorbs.net:ip4set:dul.dnsbl.sorbs.net \
rbl.zzz:ip4set:rbl.zzz \
"
```

rbldnsd'yi başlatalım:

```
# /etc/init.d/rbldnsd restart
Restarting rbldnsd: rbldnsd
rbldnsd: listening on 127.0.0.1/530
rbldnsd: ip4set:tr.countries.nerd.dk.rbldnsd: 20050126 233703:
¬ e32/24/16/8=2061/3910/46/0
rbldnsd: file dul.dnsbl.sorbs.net(3): compatibility mode: specify all NS
¬ records in ONE line
rbldnsd: ip4set:dul.dnsbl.sorbs.net: 20050126 233733:
¬ e32/24/16/8=704801/271341/1628/0
rbldnsd: ip4set:rbl.zzz: 20050129 061909: e32/24/16/8=4763/0/0/0
rbldnsd: zones reloaded, time 0.36e/0.22u sec, mem arena=408 free=60 mmap=7628 Kb
rbldnsd: rbldnsd version 0.994 (18 Dec 2004) started (1 socket(s), 3 zone(s))
```

Şimdi *rbldns*'i sorgulayalım:

```
$ dig +short @127.0.0.1 -p 530 72.102.174.195.rbl.zzz
127.0.0.2
$ dig +short -t txt @127.0.0.1 -p 530 72.102.174.195.rbl.zzz
"Izinsiz erisim yapan TR dinamik IP -- 2005-01-08"
```

3.3. DNS içinden erişim

`/etc/bind/named.conf` dosyası içerisinde yeni bir alan tanımı yapalım:

```
zone "rbl.zzz" IN {
        type forward;
        forward only;
```

```
        forwarders {
        127.0.0.1 port 530;
        };
};
```

Özellikle `forward only;` komutuna dikkat edin. Eğer DNS sunucusu bir şekilde *rbldnsd* ile iletişim kuramaz ise, Internet üzerinden çözümlemeye gitmeyecek. Bu alan yalnızca bize mahsus olduğundan dolayı bu şekilde çalışıyor.

DNS'i yeniden başlatın:

```
# /etc/init.d/bind9 restart
Stopping domain name service: named.
Starting domain name service: named.
```

Artık bu alan için rutin DNS sorgusu yapabiliriz:

```
$ dig +short 72.102.174.195.rbl.zzz
127.0.0.2
$ dig +short -t txt 72.102.174.195.rbl.zzz
"Izinsiz erisim yapan TR dinamik IP -- 2005-01-08"
```

3.4. Posta Sunucusunda Karalistenin Kullanılması

Bu örnek `postfix` posta sunucusunu ele almaktadır. Kendi posta sunucunuz için farklı ayarlar olacaktır.

Postfix 1.x sürümlerinde kendi karalistemizi kullanmak istersek; `main.cf` içerisinde,

```
maps_rbl_domains = rbl.zzz
smtpd_client_restrictions = reject_maps_rbl
```

değişikliğini yapın.

Postfix 2.x sürümlerinde ise biçim biraz farklı, yine `main.cf` içerisinde,

```
smtpd_client_restrictions = reject_rbl_client rbl.zzz
```

`maps_rbl_domains` ve `smtpd_client_restrictions` değerleri için bunların bir ekleme olduğunu unutmayın. Başka değerlerin yerine değil, ek olarak koyun. Daha fazla bilgi için Postfix Anti–UCE Cheat–Sheet[B12] adresine bakabilirsiniz.

Bu değişiklik ile birlikte, `postfix` posta sunucusu `rbl.zzz` karalistesinde bulunan IP numaralarından posta almayı reddedecektir.

3.5. SpamAssassin'e kendi karalistenizi tanımlamak

Karalisteyi, posta sunucusunda kullanıp karalisteden gelen postaları reddetmek yerine, `spamassassin` içerisinde, karalisteden gelen postalara not vermek şeklinde kullanmayı tercih edebilirsiniz.

Bunu yapmak için, `spamassassin` için kendi kuralımızı yazacağız. `/etc/mail/spamassassin/local.cf` içerisine şunları ekliyoruz:

```
header RCVD_IN_RBL_ZZZ  eval:check_rbl('rbl-notfirsthop', 'zzz.',
'127.0.0.2')
describe RCVD_IN_RBL_ZZZ        RBL_ZZZ: Yerel karaliste
tflags RCVD_IN_RBL_ZZZ  net
score RCVD_IN_RBL_ZZZ 10
```

Bu ayarlarla, spamassassin içinde, RCVD_IN_RBL_ZZZ adında kendi kuralımızı tanımlıyor ve bu kurala uyan durumlarda spamassassin'in 10 puan vermesini sağlıyoruz.

3.6. Yapmak istedikleriniz bitmiş olabilir

Eğer karalistenizin içeriğini nasıl oluşturacağınızı biliyor iseniz, buraya kadar işlediklerimizle bu karalisteyi sisteminizle nasıl bütünleştireceğinizi gördük. Bundan sonra, karalistelerin otomatik olarak nasıl oluşturulabileceğine bir örnek teşkil etmesi amacı ile rbl.zzz dosyasının içerisini nasıl dolduracağımızı ele alacağız.

4. Karaliste oluşturmak

Karalisteler herhangi bir şekilde oluşturulabilir. Sonuçta, karaliste, sizin iletişim kurmak istemediğiniz bir IP numaraları listesinden ibarettir. Tabii gereksiz yere iletişim kurmayı reddetmek sizin zararınızadır, dolayısıyla karalistelerinizi sizin için uygun bir veri kümesini içerecek şekilde hazırlamalısınız.

Bu karaliste için kullanılacak veri kümesinini, ağa gereksiz portlardan ulaşmaya çalışıp erişimi engellenen, Türk dinamik IP bloklarından gelen IP adreslerinden oluşturmayı düşünüyorum. Tabii ki, böyle bir veri kümesi oluşturmak istememin bazı sebepleri var:

1. Kolayca elde edebiliyorum, bir yerden başlamak lazım. Dolayısıyla karalisteye girmeye aday veri kümesini, ağa hizmet verilmeyen portlardan (örneğin Netbios portları) girmeye çalışan IP'lerden oluşturuyorum.
2. Bir kullanıcı statik IP'li olabilir. Fakat eğer Netbios v.b. portundan iletişim kurmaya çalışıyor ise ya bilgisayarında virüs vardır ve spam yollamaya (kendi farkında olmaksızın) başlama ihtimali yüksektir ya da kötü niyetlidir.
3. Bir kullanıcı tamamen dinamik IP'li olabilir. O zaman bir daha bağlandığı zaman o IP tamamen başka bir kullanıcıya verilecektir. Fakat ne ilk, ne de sonraki kullanıcının bu kadar dinamik bir düzende posta sunucusu çalıştırıp posta kabul etmesi mümkün değildir. Eğer posta sunucusu çalıştırmak istiyorlar ise, o zaman statik IP başvurusu yapmışlardır (ücretsiz). Eğer (çok uzak ihtimal), dinamik DNS metodları ile dinamik bloklar üzerinden bir posta sunucusu çalıştırıyorlar ise, çok daha az zahmet ile TTNET'e başvurup bir statik IP tahsis ettirebilirler. Dolayısıyla tamamen dinamik IP'lerden kaynaklanan posta, spam olacaktır.

4.1. Veri Kümesinin Oluşturulması

Bu örnek, birebir sizin için uygulanabilir olmayacaktır. Daha ziyade fikir vermesi amacı ile hazırlanmıştır. Donanım Zyxel ADSL router'dan oluşmaktadır. İlk önce bu donanımın günlüklerinin Linux makinası üzerinde tutulması için gereken ayarları yapacağız.

Ağa gereksiz portlardan erişmeye çalışıp erişimi engellenen IP adreslerini toplayacağım için güvenlik duvarı olarak kullandığım makinanın bana günlük kayıtlarını göndermesini sağlamalıyım. Günlük kayıtlarını Linux makinama local1 tanımı ile göndertiyorum. Bu durumda Linux makinamdaki /etc/syslog.conf dosyasına,

```
local1.*                        -/var/log/firewall.log
```

yazarak günlük kayıtlarının ayrı bir dosyada birikmesini sağlıyorum. Ayrıca, bu kayıtların bir de /var/log/messages dosyasına eklenmesini engellemek için,

```
*.=info;*.=notice;*.=warn;  -/var/log/messages
```

olan tanımı,

```
*.=info;*.=notice;*.=warn;local1.none  -/var/log/messages
```

haline getiriyorum.

Tabii bir de günlük dosyalarının sonsuz büyümesini engellemekte fayda var. `/etc/logrotate.d` dizinine `firewall` adında bir dosya koyarak `firewall.log`'un ne şekilde tutulacağını belirliyorum:

```
/var/log/firewall.log {
        weekly
        missingok
        rotate 52
        compress
        delaycompress
        notifempty
        create 640 root adm
}
```

Bu, haftada bir yeni bir günlük dosyası açıp 52 haftalık günlükleri diskte tutacaktır. Bu şekilde ham veri kümemizi firewall.log dosyalarından toplayabileceğiz.

4.2. Veri Kümesinin İşlenmesi

`firewall.log` dosyasından örnek satır:

```
Jan  8 01:53:53 192.168.1.1 RAS: src="81.213.17.202:4747"
dst="XXX.XXX.XX.XXX:445"
msg="Firewall default policy: TCP (W to W/PRESTIGE)"  note="ACCESS BLOCK"
devID="EF63AF"
cat="Access Control"
```

Yapacağım işlem, bu satırlardan IP adreslerini çıkartarak bu adreslerin Türk kökenli ve dinamik olduğunu kontrol etmek ve daha önce karalisteye alınmamış ise karalisteye almak.

`/var/lib/rbldns/karaliste_ekle` diye bir betik oluşturalım:

```
#!/bin/bash

grep "ACCESS BLOCK" /var/log/firewall.log.0 | \
awk '{ if ($6 ~ /^src.*/ ) { \
  srcip=$6; gsub(/src\=\"/,"",srcip); \
  gsub(/\:.*/,"",srcip); \
  gsub(/\"/,"",srcip); \
  split(srcip,A,/\./); \
  printf( \
          "%s\t%s.%s.%s.%s.tr.countries.nerd.dk\
          \t%s.%s.%s.%s.dul.dnsbl.sorbs.net\
          \t%s.%s.%s.%s.rbl.zzz\n",\
          srcip, \
          A[4], A[3], A[2], A[1], \
          A[4], A[3], A[2], A[1], \
          A[4], A[3], A[2], A[1]) }  }'   \
   | sort | uniq > /tmp/tmp.rbl

tarih=`date +%F`

while read srcip tr_test dul_test rbl_test
do
rbl_result=`dig +short $rbl_test`
if [[ $rbl_result != '127.0.0.2' ]] ; then
   tr_result=`dig +short $tr_test`
```

```
   if [[ -n $tr_result ]] ; then
      dul_result=`dig -p 530 $dul_test`
      if [[ -n $dul_result ]] ; then
         printf "%s :127.0.0.2: Izinsiz erisim yapan TR dinamik IP -- %s\n" \
                $srcip $tarih >> /var/lib/rbldns/rbl.zzz
      fi
   fi
fi
done < /tmp/tmp.rbl
rm -f /tmp/tmp.rbl
```

Bu betik, yukarıda örneğini verdiğim günlük kaydından IP adresini alıyor. Yukarıdaki örneğe uygular isek, `srcip` değişkeni 81.213.17.202 olacak. Daha sonra, IP kontrolünü yapabilmek için bu adresi A dizisine alıyor ve ters çevirerek `/tmp/tmp.rbl` dosyasına şu satırı ekliyor:

```
81.213.17.202 202.17.213.81.tr.countries.nerd.dk
¬ 202.17.213.81.dul.dnsbl.sorbs.net 202.17.213.81.rbl.zzz
```

Daha sonra, betik, `/tmp/tmp.rbl` dosyasını işleyerek bu karalisteleri kontrol ediyor ve eğer Türk kökenli ise, dinamik IP ise ve mevcut karalistede yok ise, karaliste dosyasına ekliyor.

Her hafta `firewall.log` döndürülürken karalisteye ekleme yapılması makul olur. `/etc/logrotate.d/firewall` dosyasını aşağıdaki şekilde değiştirelim:

```
/var/log/firewall.log {
        weekly
        missingok
        rotate 52
        compress
        delaycompress
        notifempty
        create 640 root adm
        sharedscripts
        postrotate
                /var/lib/rbldns/karaliste_ekle
        endscript
}
```

4.3. Internet'ten rbl.zzz Dosyasının Temini

Eğer bu şekilde oluşturulan karalistenin sizin için faydalı olacağını düşünürseniz,

```
$ rsync -az --delete rsync.belgeler.org::rblzzz/rbl.zzz.gz .
```

komutu ile alabilirsiniz.

5. Sonuç

Çeşitli karalisteleri yerelinizde nasıl şeffaf olarak yansılayarak hız kazanabileceğinizi gösterdik. Kendi oluşturacağınız bir karalisteyi nasıl tanımlayacağınızı ve bu karalisteyi Postfix ve SpamAssassin içerisinde nasıl kullanabileceğinizi işledik. Güvenlik duvarı günlüklerinden faydalanarak otomatik bir karalistenin nasıl oluşturulabileceğini örnekledik.

Notlar

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

(*B10*) http://www.sorbs.net

(*B11*) http://www.sorbs.net

(*B12*) http://jimsun.linxnet.com/misc/postfix-«anti-«UCE.txt

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

1 Şubat 2007