Güvenlik Duvarı Test Aşamaları

Semen Cirit

29 Haziran 2009

1. Menü → Sistem Ayarları yolunu izleyerek Güvenlik Duvarı Yöneticisi'ni açmayı deneyin.
   Sorunsuz bir şekilde açılabildiğini gözlemleyin.
2. Menü → Uygulamalar → Sistem yolunu izleyerek Güvenlik Duvarı Yöneticisi'ni açmayı deneyin.
   Sorunsuz bir şekilde açılabildiğini gözlemleyin.
3. Güvenlik Duvarı servisini başlat/durdur butonunu kullanarak durdurun.
   Şu komutu çalıştırın:

   ```
   # service list
   ```

   iptables servisinin kapalı olduğunu gözlemleyin.
4. Güvenlik Duvarı servisini başlat/durdur butonunu kullanarak başlatın.
   Şu komutu çalıştırın:

   ```
   # service list
   ```

   iptables servisinin başlatılmış olduğunu gözlemleyin.
5. Gelen Bağlantıları Engelle ve Giden bağlantıları engelle seçenekleri için, bu seçeneklerin sağ tarafında bulunan yapılandırma butonuna basın ve aşağıdaki işlemleri gerçekleştirin:

   5.1. Port eklemeye çalışın.
   5.2. Port silmeye çalışın.
   5.3. Bir portu yukarı çekmeye çalışın.
   5.4. Bir portu aşağı çekmeye çalışın.

   Bu işlemlerin sorunsuz bir şekilde gerçekleştiğini gözlemleyin.
   Not: Bu komutun aşağıda gerçekleşen her durum için çıktısını gözlemleyin.

   ```
   # iptables --list-rules
   ```

6. Gelen Bağlantıları Engelle seçeneği:
   Güvenlik duvarı Yöneticisinden port ekledikten sonra.

   6.1. Gelen Bağlantıları Engelle seçeneğini aktifleştirin.
   İlgili komutun çıktısının şunları içerdiğini gözlemleyin:

   ```
   -A PARDUS-IN-MOD-SERVING -p tcp -m multiport --dports <EklenenPort> \
   -j ACCEPT
   -A PARDUS-IN-MOD-SERVING -p tcp -m multiport --dports 0:1024 \
   -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -j REJECT --reject-with \
   icmp-port-unreachable
   -A PARDUS-IN-MOD-SERVING -p udp -m multiport --dports 0:1024 \
   -j REJECT --reject-with icmp-port-unreachable
   ```

   6.2. Gelen bağlantıları engelle şeçeneğini iptal edin:
   Yukarıdaki satırların ilgili komutun çıktısından silindiğini doğrulayın.

7. Internet paylaşımı seçeneği:

   Internet paylaşımını aktifleştirin Internet paylaşımını aktifleştirin (Dahili iki ethernet kartınız veya fazladan harici bir ethernet kartınız varsa bu bölümü test edebilirsiniz, yoksa bu adımı geçin.)

   7.1. İnternet ve ev ağınız için farklı köprüler seçin.
   İlgili komutun çıktısının aşağıdakileri içerdiğini gözlemleyin:

```
-A PARDUS-FW-MOD-SHARING -i <input> -o <output> -m state \
--state ESTABLISHED,RELATED -j ACCEPT
-A PARDUS-FW-MOD-SHARING -i <output> -o <input> -j ACCEPT
-t nat -A PARDUS-POST-MOD-SHARING -o <input> -j MASQUERADE
```

   7.2. Aynı değerleri verin
   Yukarıdaki satırların ilgili komutun çıktısından silindiğini gözlemleyin.

8. Giden bağlantılar engelle seçeneği:

   Yapılandırma kısmına bir port ekledikten sonra.

   8.1. Giden bağlantıları engellemeyi aktifleştirin
   Bu portun eklendiğini ilgili komutu çalıştırarak gözlemleyin.

```
-A PARDUS-FW-MOD-BLOCK -p tcp -m multiport --dports <EklenenPort> \
-j DROP
-A PARDUS-OUT-MOD-BLOCK -p tcp -m multiport --dports <EklenenPort> \
-j DROP
```

   8.2. Giden bağlantıları engellemeyi iptal edin
   Yukarıdaki satırların ilgili komutun çıktısından silindiğini doğrulayın.

9. Testlerin pratik bölümü:

   Her iki bilgisayarda güvenlik duvarını aktileştirin.

   Openssh servisi kapalı ise, servis yöneticisinden başlatın.

   9.1. Gelen Bağlantıları Engelle seçeneği:
   (Sabit ip'niz var ise veya aynı ağda iki adet makineniz var ise, bu adımı test edebilirsiniz, diğer durumda bu adımı geçin.)

      9.1.1. Gelen Bağlantıları Engelleme seçeneğini pasifleştirin.
      Başka bir bilgisayardan kendi bilgisayırınıza bağlanmayı deneyin.
      Bu işlem için aşağıdaki komutu çalıştırın:
      `# ssh <sizin_bilgisayarınızın_adı>@<sabit_ip>`
      Bağlantının kabul edildiğini gözlemleyin.

      9.1.2. Gelen Bağlantıları Engelle seçeneğini aktifleştirin.
      Bilinen bir portu bu işlem için port olarak ekleyin.
      Bu port için ilgili bir servis var ise, bu servisi servis yöneticisinden açın.

         9.1.2.1. Başka bir bilgisyardan kendi bilgisayarınıza uzaktan bağlanmayı deneyin.
         Bu işlem için aşağıdaki komutu çalıştırın:
         `# ssh <sizin_bilgisayarınızın_adı>@<sabit_ip>`
         Bağlantıya izin verilmediğini gözlemleyin.

         9.1.2.2. Engellenecek olan port dışında bir port kullanarak kendi bilgisyarınıza uzaktan bağlanmayı deneyin.
         Bu işlem için aşağıdaki komutu çalıştırın:
         `# ssh -p <port> <sizin_bilgisayarınızın_adı>@<sabit_ip>`
         Bağlantının kabul edildiğini gözlemleyin.

   9.2. İnternet paylaşımı seçeneği:
   (Dahili iki ethernet kartınız veya fazladan harici bir ethernet kartınız varsa bu bölümü test edebilirsiniz, yoksa bu adımı geçin.)

      9.2.1. Harici veya dahili ethernet kartınızı kullanarak, kendi bilgisayarınız ile diğer bilgisayarı ethernet kablosu ile birbirine bağlayın. Eğer diğer bilgisayarın internet erişimi varsa durdurun.)

      9.2.2. Güvenlik Duvarı Yöneticisinden internet paylaşımını aktifleştirin.

      9.2.3. Birinci ethernet kartınızı internete köprü için, ikincisini ev ağınıza köprü için seçin.
      Diğer makinanın sizin makinanız üzerinden internete bağlanabildiğini gözlemleyin. (Diğer makina üzerinden ağ yöneticisi ile bunu gerçekleştirebilirsiniz.)

9.3. Giden Bağlantıları Engelleme seçeneği:

(Sabit ip'niz varsa ya da aynı ağda iki makine varsa, bu adımı test edebilirsiniz, diğer durumda bu adımı atlayın.)

9.3.1. Giden bağlantı engelle seçeneğini pasifleştirin.

9.3.1.1. Kendi bilgisayarınızdan, bilinen bir portu kullanarak, diğer bilgisayara bağlantı oluşturmayı deneyin.
(Uzaktaki bilgisayar statik ip'ye sahipse uzaktan bağlantı için onu kullanabilirsiniz.)
Bu işlemi gerçekleştirebilmek için aşağıdaki komutu çalıştırın:

```
# ssh -p <port> <diğer_bilgisayarın_adı>@<sabit_ip>
```

Bağlantının kabul edildiğini gözlemleyin.

9.3.1.2. Bilinen bir portu ekleyin ve giden bağlantıları engellemeyi aktifleştirin.
Kendi bilgisayarınızdan eklediğiniz portu kullanarak diğer bilgisayara uazaktan bağlantı oluşturmayı deneyin.

```
# ssh -p <port> <diğer_bilgisayarın_adı>@<sabit_ip>
```

Bağlantıya izin verilmediğini gözlemleyin.