

41. İpucu: Uzak İşletim Sistemi Saptama Yazılımlarını Yanıltın

Uzak işletim saptama saldırılarını TCP/IP yığınızı değiştirerek yanıltın.

İşletim sistemi saptama saldırılarını engellemenin bir yolu da TCP/IP yığınızı değiştirerek başka bir işletim sisteminin yığınının taklit etmesini sağlamaktır. Zor gibi görünse de Linux tarafından çekirdeğinin IP Personality projesi (<http://ippersonality.sourceforge.net>) kodu ile birlikte tekrar derlenmesi ile mümkün olmaktadır. Bu kod kullanıcı seviyesindeki iptables komutunu ve çekirdeğin içindeki Netfilter güvenlik duvarını genişletmektedir.

IP Personality kodunu yapılandırabilmek için ilk olarak çekirdeğinize uygun olan paketi indirmeniz gerekmektedir. Eğer çekirdeğinize uygun sürüm için yama bulamazsanız daha yeni çekirdekler için yama içeren SourceForge sayfasını (http://sourceforge.net/tracker/?group_id=7557&atid=307557) ziyaret edebilirsiniz.

Çekirdeğinizi yalamamak için IP Personality kaynak kodunu açıp, çekirdek kaynağını barındıran dizine geçip patch komutunu çalıştırın:

```
# cd /usr/src/linux
# patch -p1 < \
../ippersonality-20020819-2.4.19/patches/ippersonality-20020819-linux-
2.4.19.diff
```

patch komutunun uygulandığından emin olmak için aşağıdaki komutu çalıştırın:

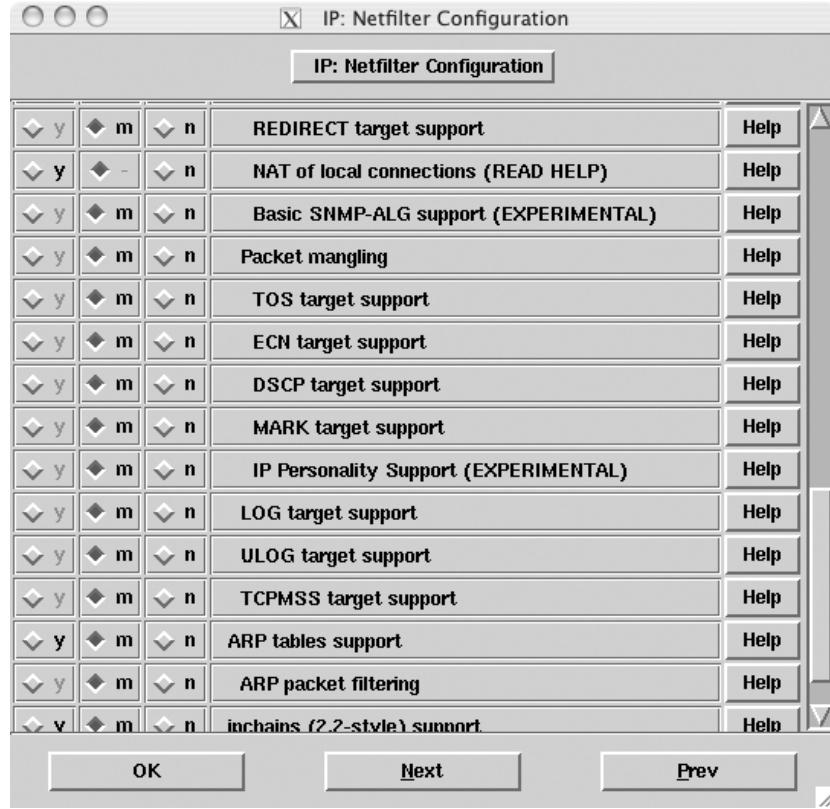
```
# find ./ -name \*.rej
```

Eğer yama düzgün şekilde uygulandı ise bu komut hiçbir dosya bulamayacaktır.

Çekirdeğimizi yamaladığımıza göre artık IP Personality desteği için çekirdeğimizi hazırlamaya başlayabiliriz. Daha önce bahsedildiği gibi [13. İpucu], çekirdek dizininde iken `make xconfig`, `make menuconfig` veya `make config` komutlarının çalıştırılması çekirdeğinin yapılandırılması için gerekli olan menüyü önünüze getirecektir.

İlk olarak "Kod Gelişmişlik Düzeyi Seçenekleri" (Code maturity level options) altında "Geliştirilmekte olan ve/veya tamamlanmamış kod/sürücü durumunda haber ver" (Prompt for development and/or incomplete code/drivers) seçeneğinin seçili olduğundan emin olun. Ağ seçenekleri altında ise Netfilter Yapılandırmasını etkinleştirin.

`make xconfig` tarafından önünüze çıkarılan liste [Şekil 3-7](#)'de görülebilir. IP "Personality Support" adındaki seçeneği bulun. Çekirdeğinizi statik olarak derlemek için `y` veya dinamik olarak eklenen modül olarak eklemek için `m` seçeneğini seçin.



Şekil 3-7. IP Personality Support Seçeneğinin Açılması

IP Personality desteğini yapılandırdıktan sonra yapılandırmayı saklayın. Daha sonra çekirdek ve çekirdek modüllerini derleyip kurmak için şu komutları çalıştırın.

```
# make dep && make clean
# make bzImage && make modules
# cp arch/i386/boot/bzImage /boot/vmlinuz
# make modules_install
```

Sisteminizi yeni çekirdek ile yeniden başlatın. Çekirdeğinizi yamalamanın yanında Netfilter'ın kullanıcı seviyesinde çalışan iptables komutunu da yamalamanız gerekecektir. Bunun için Netfilter web sitesine (<http://www.netfilter.org>) gidip IP Personality paketinizle gelen yama ile uygun olan paketi indirin. Örneğin *ippersonality-20020819-2.4.19.tar.gz* ile uygun olan sürüm Netfilter Sürüm 1.2.2.'dir.

Uygun iptables sürümünü indirip açtıktan sonra iptables'ı IP Personality paketi içinde bulunan yama ile yamalamanız gerekecektir. Bundan sonra iptables'ı normal bir şekilde derleyip kurabilirsiniz.

```
# tar xvj iptables-1.2.2.tar.bz2
# cd iptables-1.2.2
# patch -p1 < \
```

```
../ippersonality-20020819-2.4.19/patches/ippersonality-20020427-iptables-1.2.2.diff
patching file pers/Makefile
patching file pers/example.conf
patching file pers/libipt_PERS.c
patching file pers/pers.h
patching file pers/pers.l
patching file pers/pers.y
patching file pers/pers_asm.c
patching file pers/perscc.c
# make KERNEL_DIR=/usr/src/linux && make install
```

Bu işlem yeni iptables komutunu, iptables'ın desteklediği kütüphaneleri ve yeni man sayfalarını (/usr/local altına) kuracaktır. Eğer ön tanımlı yükleme dizinlerini değiştirmek isterseniz Makefile dosyasına girip, BINDIR, LIBDIR, MANDIR, ve INCDIR makrolarının değerlerini değiştirebilirsiniz. KERNEL_DIR dizinini daha önce derlediğiniz çekirdek kaynak dosyalarının olduğu dizin olarak ayarladığınıza emin olun.

Eğer Red Hat Linux kullanıyorsanız, yeni yüklenecek iptables komutunu eskisi ile değiştirmek için ilgili değerleri aşağıdaki gibi değiştirebilirsiniz:

```
LIBDIR:=/lib
BINDIR:=/sbin
MANDIR:=/usr/share/man
INCDIR:=/usr/include
```

make install komutunu çalıştırmanın yanında işletim sistemi yapılandırma dosyaları için de bir dosya yaratmanız gerekecektir. Bu yapılandırma dosyaları IP Personality dağıtımı altında *samples/* dizininde bulunabilir. Örneğin, */etc/personalities* adında bir dizin oluşturup bu dosyaları buraya yerleştirebilirsiniz.

IP Personality yazılımını yapılandırmadan önce kendi sisteminizi Nmap ile tarayarak hangi işletim sistemi sonucu verdiğine bir göz atın.

```
# nmap -O colossus
Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2003-12-12
18:36 MST
Interesting ports on colossus (192.168.0.64):
(The 1651 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
505/tcp   open  mailbox-lm
631/tcp   open  ipp
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux Kernel 2.4.0 - 2.5.20
Uptime 3.095 days (since Tue Dec 9 16:19:55 2003)
Nmap run completed -- 1 IP address (1 host up) scanned in 7.375 seconds
```

Eğer 192.168.0.64 IP adresine sahip bir sisteminiz varsa ve işletim sisteminizin Mac OS 9 olduğunun düşünülmesini istiyorsanız iptables komutunu şu şekilde kullanabilirsiniz:

```
# iptables -t mangle -A PREROUTING -d 192.168.0.64 -j PERS \  
--tweak dst --local --conf /etc/personalities/macos9.conf  
# iptables -t mangle -A OUTPUT -s 192.168.0.64 -j PERS \  
--tweak src --local --conf /etc/personalities/macos9.conf
```

Şimdi tekrar Nmap yazılımı ile tarayalım:

```
# nmap -O colossus  
Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2003-12-12  
18:47 MST  
Interesting ports on colossus (192.168.0.64):  
(The 1651 ports scanned but not shown below are in state: closed)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
25/tcp    open  smtp  
111/tcp   open  rpcbind  
139/tcp   open  netbios-ssn  
505/tcp   open  mailbox-lm  
631/tcp   open  ipp  
Device type: general purpose  
Running: Apple Mac OS 9.X  
OS details: Apple Mac OS 9 - 9.1  
Uptime 3.095 days (since Tue Dec 9 16:19:55 2003)  
Nmap run completed -- 1 IP address (1 host up) scanned in 5.274 seconds
```

Tâbii ki IP Personality dağıtımı ile gelmemiş olan işletim sistemlerini de deneyebilirsiniz. Tek ihtiyacınız olan şey Nmap işletim sistemi parmak izi dosyalarıdır (*nmap-os-fingerprints*). Bundan sonra Nmap tarafından bilinen tüm işletim sistemleri için IP Personality yapılandırmanızı gerçekleştirebilirsiniz.