



Linux Çekirdeđi 2.6 ve Güvenlik

Fatih Özavcı
IT Security Consultant

holden@siyahsapka.com
<http://www.siyahsapka.com>

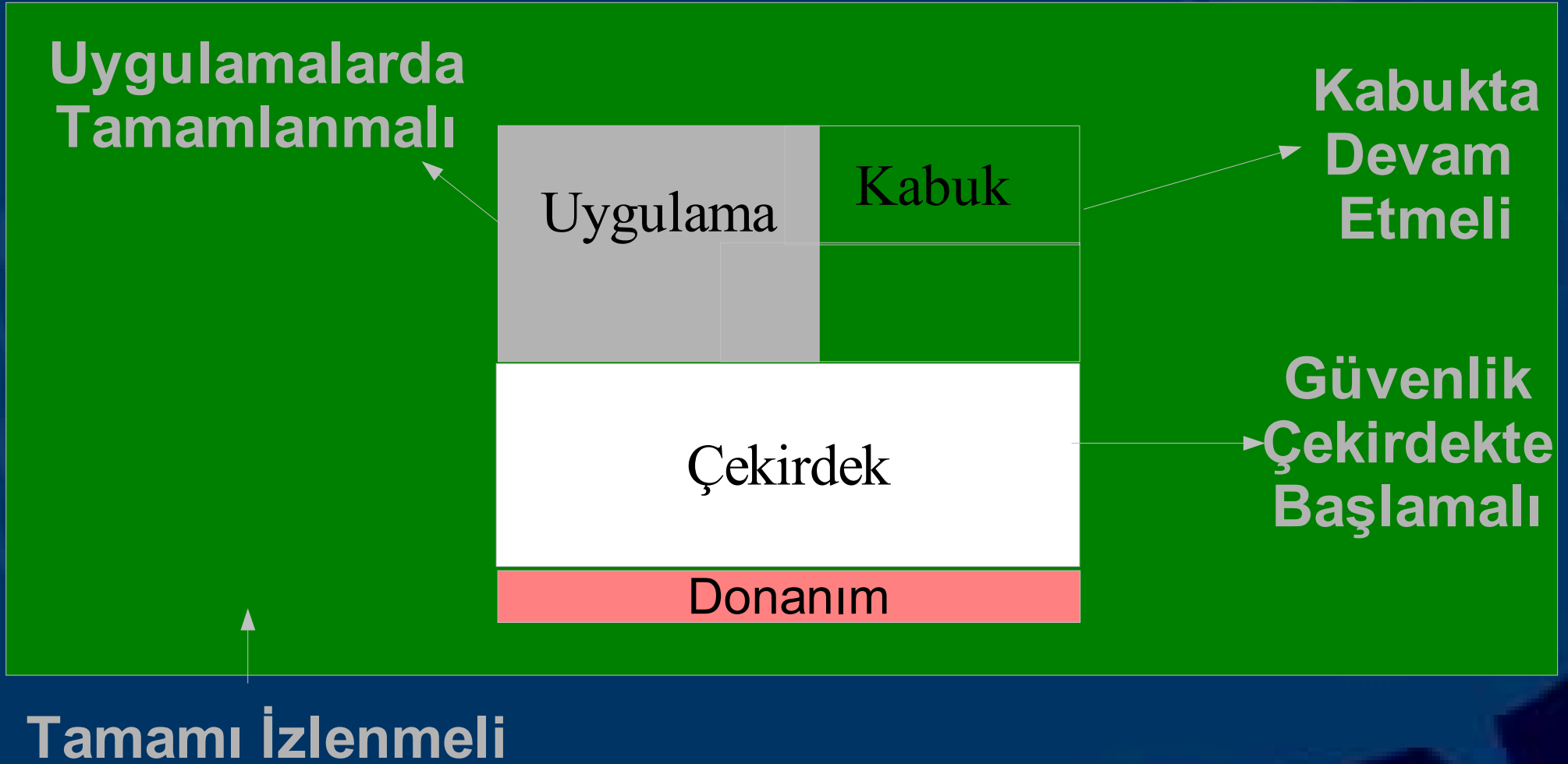
GNU/Linux

- Linux Çekirdeđi Linus Torvalds Tarafından Geliştirilmiş ve İlk Sürüm 25 Ağustos 1991'de Duyurulmuştur
- Free Software Foundation'ın Hamiliđini Yaptıđı GNU Projesi ile Birleştirelerek GNU/Linux İşletim Sistemi Oluşturulmuştur
- GPL Lisansı ile Dađıtılmaktadır
- Açık Kaynak Kodludur ve Gelişimi Gönüllü Kişilerce Yürütölmektedir
- Çok Kullanıcılı ve Çok Görevlidir
- Ölçeklenebilir, Farklı Mimariler ve Donanımlarda Çalışabilmektedir
- Açık Kaynaklı Olduđu İçin Güvenilirdir
- Linux Çekirdeđi, Gnu Araçları ve Çeşitli Uygulamaları İçeren Birçok Linux Dađıtımı Bulunmaktadır

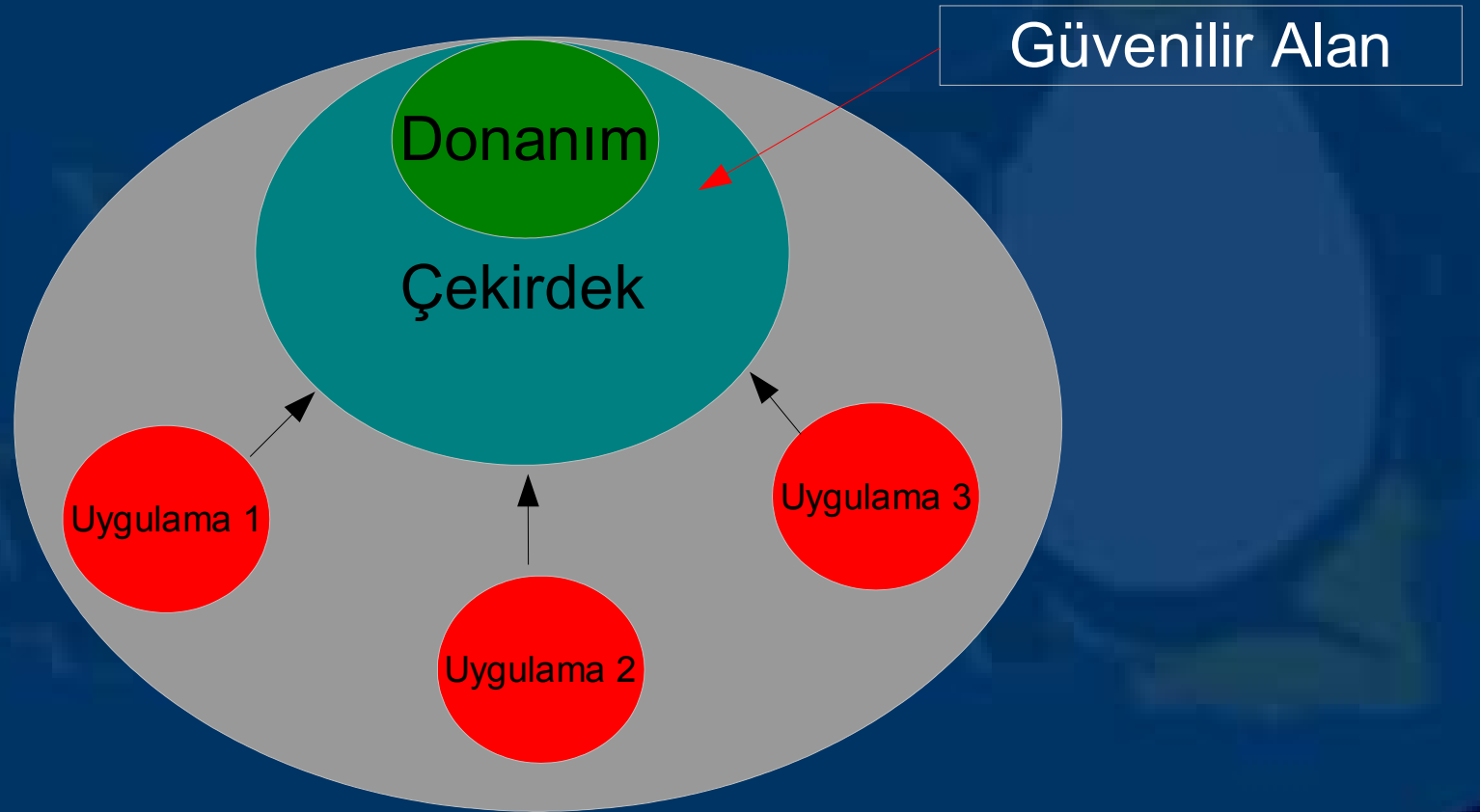
Çekirdek

- Donanım ile Yazılım haberleşmesini sağlar
- Süreklilik, Kararlılık ve Güvenliğin temelidir
- Sistemin çalışmasından, kaynakların etkin kullanımından ve kaynak erişimlerinin düzenlenmesinden sorumludur
 - Bellek Yönetimi
 - İşlemci Yönetimi
 - Donanım Erişim Yönetimi
 - Süreçlerin Yönetimi
 - Girdi/Çıktı İşlemlerinin Yönetimi

Çekirdek ve İşletim Sistemi Yapısı



Çekirdek'te Güvenliđi Sađlamak



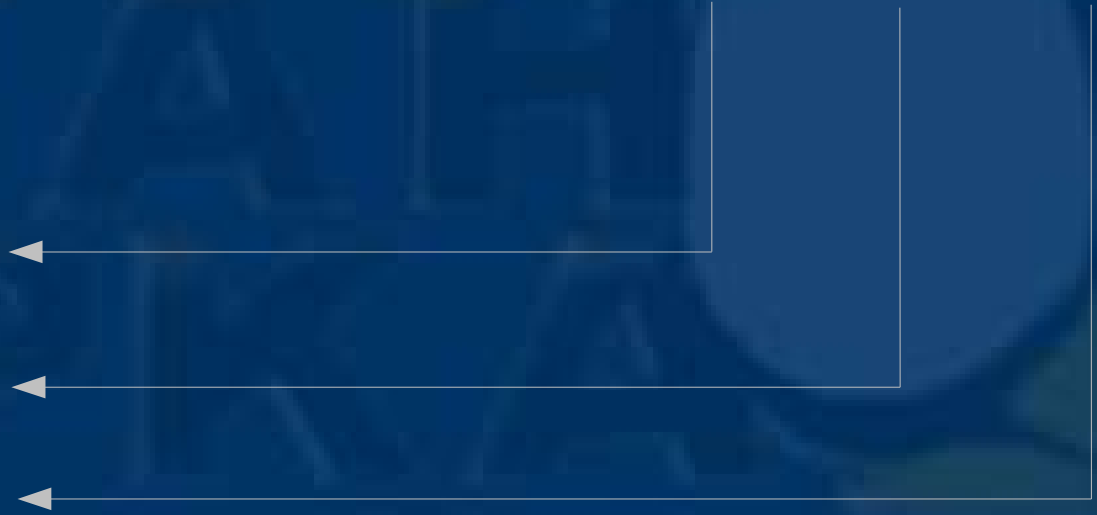
Linux Çekirdek Sürümleri

İlk Linux çekirdeği 9/1991 'de 0.01 ile duyuruldu

Güncel Sürümü : 2.6.Test11 ve 2.4.23

2.6.0

- Birincil Sürüm Numarası
- İkincil Sürüm Numarası
- Alt Sürüm Numarası



Yama Kavramı

- Linux çekirdeğine ek özellikler katmak, varolan özellikleri değiştirmek veya sürüm yükseltmek/düşürmek için yama yapılmaktadır
- Varolan kaynak kodun üstüne yapılmakta ve yamada bulunan değişiklikler uygulanmaktadır
- Bazı durumlarda yamalar çakışabilmektedir
 - Aynı dosyaların değiştirilmesi gereken durumlarda
 - Farklı dosyalarda aynı fonksiyonları uygulamaları gereken durumlarda
- Güvenlik için birçok yama yayınlanmıştır (Kriptolama, Sanal özel ağ, Özel dosya sistemleri, Güvenlik duvarı, Erişim denetim özellikler vb.)

Örnek Yamalama İşlemi

```
cd /usr/src/linux
```

```
patch -Np1 -i /yamaninyeri/yama.diff
```

Linux Çekirdeği 2.6 Güvenlik Yenilikleri

- 2.4'te harici yamalar ile sağlanan birçok özellik 2.6'da çekirdeğe dahil edilmiştir.
- LSM ile SELinux ve RSBAC gibi erişim denetim model örneklerinin yamaları uygulanmıştır. (LIDS bu yamalardan yararlanabilmektedir.)
- Netfilter yamaları arttırılmış özelliklere kavuşmuştur. (Bu yamalardan bazıları 2.4'e uygulanamamaktadır.)
- FreeSWAN tarafından kullanılan IPSEC özellikleri çekirdeğe dahil edilmiştir.
- Kriptolama yamaları çekirdeğe dahil edilmiş ve kriptolu disk kullanımı örnek uygulaması yapılmıştır.

Linux Çekirdeği 2.4 ve 2.6 Yama Karşılaştırması

- 2.6 ile gelen birçok modül 2.4'e yamalar ile eklenebilmektedir
 - Kriptolama
 - IPSEC
 - Netfilter
 - LIDS / LSM / SELinux
 - NFS için ACL Desteği
- Halen 2.6 ve 2.4 için harici yamalar devam etmektedir
 - LIDS
 - GRSecurity
 - SELinux
 - Uzatılmış ACL Desteği
 - StegFS Desteği

Kriptolama Modülleri

- Diğer modüllerin veya uygulamaların kriptolama amaçlı işlemleri çekirdek seviyesinde yapabilmesi için eklenmiştir.
 - VPN Desteği
 - Kriptolu Dosya Sistemi Desteği
- Yasal olarak kullanımı problem oluşturmayan algoritmalar kullanılmıştır
 - Simetrik Algoritmalar
 - Veri Özeti Algoritmaları

- Cryptographic API
 - HMAC support (NEW)
 - Null algorithms (NEW)
 - MD4 digest algorithm (NEW)
 - MD5 digest algorithm (NEW)
 - SHA1 digest algorithm (NEW)
 - SHA256 digest algorithm (NEW)
 - SHA384 and SHA512 digest algorithms (NEW)
 - DES and Triple DES EDE cipher algorithms (NEW)
 - Blowfish cipher algorithm (NEW)
 - Twofish cipher algorithm (NEW)
 - Serpent cipher algorithm (NEW)
 - AES cipher algorithms (NEW)
 - CAST5 (CAST-128) cipher algorithm (NEW)
 - CAST6 (CAST-256) cipher algorithm (NEW)
 - Deflate compression algorithm (NEW)
 - Testing module (NEW)

Netfilter Modülleri

- Güvenlik duvarı işlemlerinin uygulanabilmesi için eklenmiştir. (2.4 ile gelen Netfilter'ın devamı niteliğindedir.)
 - Bağlantı takibi
 - NAT
 - Trafik yönetimi
 - Önemli ağ protokollerinin tanımlanması
 - ARP desteği
 - Paket limitleri desteği
 - Zaman temelli kural desteği

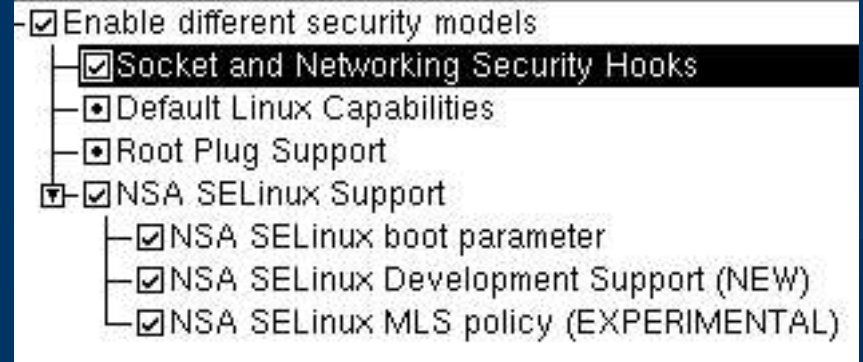
Netfilter Modülleri

- Connection tracking (required for masq/NAT)
 - FTP protocol support
 - IRC protocol support
 - TFTP protocol support
 - Amanda backup protocol support
- Userspace queueing via NETLINK
- IP tables support (required for filtering/masq/NAT)
 - limit match support
 - IP range match support
 - MAC address match support
 - Packet type match support
 - netfilter MARK match support
 - Multiple port match support
 - TOS match support
 - recent match support
 - ECN match support
 - DSCP match support
 - AH/ESP match support
 - LENGTH match support
 - TTL match support
 - tcpmss match support
 - Helper match support
 - Connection state match support
 - Connection tracking match support

- Connection state match support
- Connection tracking match support
- Owner match support
- Packet filtering
 - REJECT target support
 - Full NAT
- MASQUERADE target support
- REDIRECT target support
- NETMAP target support
- SAME target support
- NAT of local connections (READ HELP)
- Basic SNMP-ALG support (EXPERIMENTAL)
- Packet mangling
 - TOS target support
 - ECN target support
 - DSCP target support
 - MARK target support
 - CLASSIFY target support
- LOG target support
- ULOG target support
- TCPMSS target support
- ARP tables support
 - ARP packet filtering
 - ARP payload mangling
- ipchains (2.2-style) support
 - ipfwadm (2.0-style) support (NEW)

LSM Modülleri

- Erişim denetim modellerinin uygulanabilmesi için eklenmiştir. (MAC, RSBAC)
- Soket ve Ağ temelli erişim denetimi
- USB aygıtlardan “root” haklarına sahip programların çalışmasının engellenmesi
- SELinux desteği
 - MAC Desteği
 - RSBAC Desteği



IPSEC Modülleri

- Daha önceleri birçok modülden oluşan IPSEC artık kriptografi özelliklerine link vermektedir
- AH, ESP, IPComp ve IPSec modülleri bu amaçla kullanılabilir
- FreeSWAN bu modülleri kullanmaktadır

- IP: AH transformation
- IP: ESP transformation
- IP: IPComp transformation
- IP: Virtual Server Configuration
- The IPv6 protocol (EXPERIMENTAL)
- DECnet Support
- 802.1d Ethernet Bridging
- Network packet filtering (replaces ipchains)
- IPsec user configuration interface

Linux Çekirdeği 2.6 Güvenlik Yamaları

- Iptables/Netfilter ekibi halen deneme seviyesinde veya kararlı olarak birçok modülü yama olarak sunmaktadır.
- LIDS, LSM'i kullanabilse de diğer özellikleri için yama yayınlamaya devam etmektedir.
- GRSecurity, LSM ile çalışmadığından kendi yamalarını kullanmaktadır.
- RSBAC ve SELinux, LSM tarafından içerilmektedir; ancak halen geliştirmeler ile yama yayınlamaları devam etmektedir.
- Dosya sistemleri için daha fazla erişim denetim kuralı koyulabilmesini sağlayan uzatılmış ACL desteği yama olarak bulunabilmektedir
- FreeSWAN'nın bazı özelliklerinin geliştirilebilmesi için extra yamalar sunulmaktadır.

Çekirdek Seçim Tavsiyeleri

- Gerekli olmayan herhangi bir destek verilmemelidir, tüm modülleri ihtiyaçları doğrultusunda seçilmelidir.
- Kullanılmayacaksa takılabilir cihaz destekleri çıkarılmalıdır. (USB, Paralel vb.)
- Kullanılmayacaksa Bluetooth , IRDA ve Wireless destekleri çıkarılmalıdır.
- Bir erişim denetim modeli seçilmeli ve gerekli yamalar yüklenmelidir. (MAC, DAC, RSBAC vb.)
- Erişim denetimi modeli doğrultusunda ACL yapılandırılması kullanılmalıdır.
- Önemli veriler için kriptolu disk alanı yaratılmalı ve kullanılmalıdır.

Ağ İçin Çekirdek Düzenlemesi - 1

- Tüm Ping Paketlerinin Gözardı Edilmesi
echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_all
- Yayın Adresi Ping Paketlerinin Gözardı Edilmesi
echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
- Bozuk ICMP Hata Cevaplarını Gözardı Etmek
echo 1 > /proc/sys/net/ipv4/icmp_ignore_bogus_error_responses
- Hedefi İmkansız Olan Paketler için Kayıt Tutulması
echo 1 > /proc/sys/net/ipv4/conf/all/log_martians
- IP Yönlendirmenin Pasifleştirilmesi
echo 0 > /proc/sys/net/ipv4/ip_forward
- TCPSynCookies'in Aktif Hale Gelmesi
echo 1 > /proc/sys/net/ipv4/tcp_syncookies
- Bölünmüş Paketlerin Gözardı Edilmesi İçin
echo 1 > /proc/sys/net/ipv4/ip_always_defrag

Ağ İçin Çekirdek Düzenlemesi - 2

- IP Spoofing Koruması
for dosya in /proc/sys/net/ipv4/conf/*/rp_filter ; do
echo 1 > \$dosya ; done
- ICMP Redirect Paketlerinin Gözardı Edilmesi
for dosya in /proc/sys/net/ipv4/conf/*/accept_redirects ; do
echo 0 > \$dosya ; done
- ICMP Redirect Paketlerinin Gönderiminin Engellenmesi
for dosya in /proc/sys/net/ipv4/conf/*/send_redirects ; do
echo 0 > \$dosya ; done
- Kaynak Yönlendirmesi Yapılmış Paketlerin Gözardı Edilmesi
for dosya in /proc/sys/net/ipv4/conf/*/accept_source_route ; do
echo 0 > \$dosya ; done
- Son Üç Seçenekte Gözardı Edilen Tüm Paketlerin Loglanması
for dosya in /proc/sys/net/ipv4/conf/*/log_martians ; do
echo 0 > \$dosya ; done

Kaynak Kodda Gezinti



Yama Adresleri

- Kernel Homepage – <http://www.kernel.org>
- LSM Homepage – <http://lsm.immunix.org>
- Netfilter/Iptables – <http://www.netfilter.org>
- FreeSWAN – <http://www.freeswan.org>
- RSBAC - <http://www.rsbac.org>
- LIDS – <http://www.lids.org>
- GRSecurity – <http://www.grsecurity.org>
- Extended ACL Support – <http://acl.bestbits.at>
- LOMAC – <http://opensource.nailabs.com/lomac>

Diğer Güvenlik Yazılımları

- Güvenlik Duvarı
 - Iptables <http://www.netfilter.org>
- Saldırı Tespit Sistemi
 - Snort <http://www.snort.org>
 - LIDS <http://www.lids.org>
 - GRSecurity <http://www.grsecurity.org>
- Sanal Özel Ağ Sunucusu
 - FreeSWan <http://www.freeswan.org>
 - PoPToP <http://www.poptop.org>
- SSL Kütüphaneleri ve Araçları
 - OpenSSL <http://www.openssl.org>
- PGP Kriptolama
 - GnuPG <http://www.gnupg.org>
- Güvenlik Denetimi
 - Nessus <http://www.nessus.org>
 - Nmap <http://www.insecure.org/nmap>

Yararlı Kaynaklar

- Security Focus <http://online.securityfocus.com>
- Sans Reading Room <http://rr.sans.org>
- CERT <http://www.cert.org>
- LinuxDoc <http://www.linuxdoc.org>
- Linux Security <http://www.linuxsecurity.com>
- Redhat <http://www.redhat.com>
- Suse <http://www.suse.com>
- Linux.Org.TR <http://www.linux.org.tr>
- Belgeler.Org <http://www.belgeler.org>
- Siyah Şapka <http://www.siyahsapka.com>

Sorular



Teşekkürler.....

