



Açık Kod yazılımlar ile Ağ ve Güvenlik Çözümleri

Huzeyfe ÖNAL
huzeyfe@EnderUNIX.org



Sunum Planı

- Linux, *BSD, Açık Kod, Özgür yazılım Terimleri
- Linux/UNIX zor mu?
- İhtiyaca yönelik seçim..
- Temel Ağ servisleri
 - DHCP, DNS, Monitoring, mail, web, ftp, file server
- Güvenlik Servisleri
 - Firewall, VPN, IDS/IPS, Proxy, CF, Security Scanner

Tanımlar..

- Linux, Linux dağıtımları.
- BSD
 - FreeBSD, NetBSD, OpenBSD
- Linux mu UNIX mi?
- Linux/UNIX gerçekten zor mu?
 - Kolaylık mı, basitlik(anlaşılabilirlik)mi ?
- Bilişimci ne iş yapar, ne bilmelidir?
- Bilişim meslek mi hobi mi?





Temel Ağ Servisleri

- DNS Sunucu
 - Internetin temel yapı taşlarından
 - Mail, web ..trafiğini etkiler
 - Yanlış yönetim kurbanı
 - ISC BIND, DJBDNS ...
- WEB, FTP, Mail, File server, DHCP...
 - Apache, PureFTPD, ProFTPD, Samba, ISC DHCP



BIND DNS Sunucu

- Açık kaynak kodlu
- Standartlara uygun
- Ek güvenlik özellikleri sağlar
 - Chroot, dnssec.
- View, blacklist vb ile özelleştirilmiş yönetim
- Kolay, anlaşılır yapılandırma dosyası
- GUI, WEB üzerinden yönetim için onlarca araç..
 - Freshmeat.net, sf.net, Webmin...
- Her eve lazım..☺

DHCP Hizmeti

- DHCP(Dynamic Host Conf. Protocol) ?
- ISC tarafından yönetiliyor
- Geniş kapsamlı bir proje
- Web ve konsol aracılığı ile kolay yönetim
 - Webmin, Freshmeat ,Sf.net
- Standartlara Uygun
- HA yapısında çalışabilirlik
- Birçok ticari sürümü var





Sistem Gözleme

- Orta ölçekli bir ağ için gerekli
- Nagios, BigBrother ...
- Nagios:
- Her tür servis kontrolü
 - Ssh, ftp, dns, telnet,
 - Ajan programlar uzak sistemlere ait disk, cpu, bellek gözleme
 - Gelişmiş uyarı mekanizması
 - Ses, mail, web, sms, Messenger

Nagios servis durumu..

Nagios - Netscape
File Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security Shop Stop

Bookmarks Go to: What's Related

Nagios

General

- Home
- Documentation

Monitoring

- Tactical Overview
- Status Detail
- Status Overview
- Status Summary
- Status Grid
- Status Map
- 3-D Status Map

Service Problems

- Network Outages

Trends

- Availability
- Alert History
- Notifications
- Log File

Comments

- Downtime

Process Info

- Performance Info

Configuration

- View Config

Current Network Status
Last Updated: Sun Jul 15 14:06:09 CDT 2001
Updated every 75 seconds
Nagios™ - www.nagios.org
Logged in as guest
- Monitoring process is running
- **Notifications cannot be sent out!**
- Service checks are being executed

[View History For all hosts](#)
[View Notifications For All Hosts](#)

Host Status Totals

Up	Down	Unreachable	Pending
28	3	4	0

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
103	2	0	14	18

Service Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Service Information
app98	PING	OK	07-15-2001 14:04:09	4d 4h 7m 13s	1/3	PING ok - Packet loss = 0%, RTA = 0.60 ms
bogus-router	PING	CRITICAL	07-15-2001 14:04:39	4d 3h 46m 13s	1/3	CRITICAL - Plugin timed out after 10 seconds
bogus1	Something...	CRITICAL	07-15-2001 14:00:38	4d 4h 1m 45s	1/3	(Service Check Timed Out)
	PING	CRITICAL	07-15-2001 14:02:36	4d 4h 1m 45s	1/3	CRITICAL - Plugin timed out after 10 seconds
bogus2	PING	CRITICAL	07-15-2001 14:04:09	4d 3h 47m 23s	1/3	CRITICAL - Plugin timed out after 10 seconds
	Something...	CRITICAL	07-15-2001 14:04:39	4d 3h 45m 22s	1/3	(Service Check Timed Out)
bogus3	PING	CRITICAL	07-15-2001 14:05:38	4d 3h 45m 3s	1/3	CRITICAL - Plugin timed out after 10 seconds
	Something...	CRITICAL	07-15-2001 14:02:36	4d 3h 33m 31s	1/3	(Service Check Timed Out)
bogus4	PING	CRITICAL	07-15-2001 14:04:09	4d 3h 46m 31s	1/3	CRITICAL - Plugin timed out after 10 seconds
	Something...	CRITICAL	07-15-2001 14:04:39	4d 3h 45m 22s	1/3	(Service Check Timed Out)
bogus5	PING	CRITICAL	07-15-2001 14:05:43	4d 3h 44m 3s	1/3	CRITICAL - Plugin timed out after 10 seconds
	Something...	CRITICAL	07-15-2001 14:02:36	4d 3h 33m 21s	1/3	(Service Check Timed Out)
linux1	Log Anomalies	PENDING	N/A	4d 3h 38m 2s+	0/1	Service check is not scheduled for execution...
	TCP Wrappers	PENDING	N/A	4d 3h 38m 2s+	0/1	Service check is not scheduled for execution...
	Security Alerts	PENDING	N/A	4d 3h 38m 2s+	0/1	Service check is not scheduled for execution...
	PING	OK	07-15-2001 14:02:35	4d 4h 6m 14s	1/3	PING ok - Packet loss = 0%, RTA = 0.50 ms
linux2	PING	OK	07-15-2001 14:04:01	4d 3h 47m 34s	1/3	PING ok - Packet loss = 0%, RTA = 0.00 ms
	Security Alerts	PENDING	N/A	4d 3h 38m 2s+	0/1	Service check is not scheduled for execution...
	TCP Wrappers	PENDING	N/A	4d 3h 38m 2s+	0/1	Service check is not scheduled for execution...
	Log Anomalies	PENDING	N/A	4d 3h 38m 2s+	0/1	Service check is not scheduled for execution...

Güvenlik Hizmetleri

- Kime ? Ne derece güvenlik?
- Güvenlik Maliyet ilişkisi
- Güvenlik mi? Paranoya mı?
- Açık sistemler ne kadar güvenli?
 - Kodların açık olması ..
 - Protokollerin açık olması
- Zincirdeki en zayıf halka; insan...





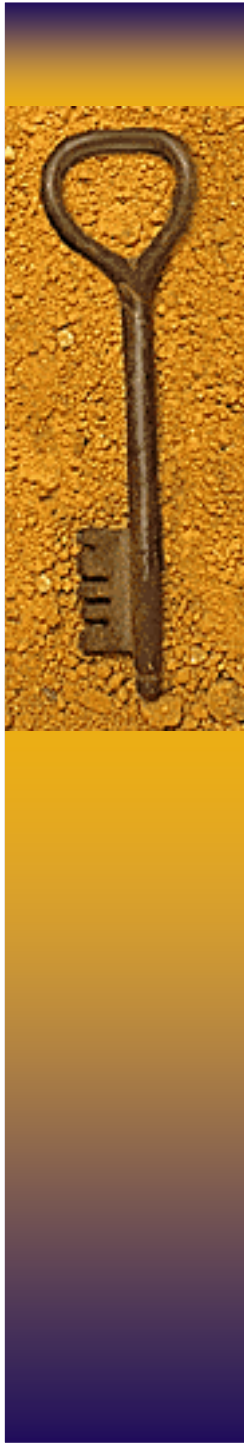
Güvenlik Hizmetleri-II

- Firewall(Güvenlik Duvarı)
 - En temel bileşen, olmazsa olmazlardan
 - Firewall ne işe yarar? Firewall != oyuncak
 - Güvenlik tasarımı.
 - Zone kavramı
 - DMZ, iç ağ, internet
- Özgür Firewall yazılımları
 - Linux Iptables, FreeBSD IPF, IPFW, OpenBSD Packet Filter(PF)



OpenBSD PF_(Packet filter)

- En gelişmiş açık kod Firewall çözümü
- Aktif gelişim süreci
- Kolay ve anlaşılır yapı
- HA ve Load Balancing
- İleri düzey trafik kontrolü
- Bandwidth Shaping
- Bridge mode çalışma yeteneği
- Üstün performans
 - Gerçek hayattan örnekler



OpenBSD PF -II

- GUI aracılığı ile yönetim
 - Fwbuilder
 - PFW
- Örnek kural söz dizimi

Filtreleme;

Pass in log on \$ext_if proto tcp from 1.2.3.4 to 4.5.6.7

Block in log on \$ext_if proto tcp from any to 172.16.10.1 port 23

Nat

Nat on \$ext_if from \$ic_ag to any -> 11.22.33.44

- Basit, performanslı, anlaşılır log yapısı
- Tcpdump kullanılarak izlenebilir.

Dec 02 17:20:31.046452 rule 15/(match) pass out on fxp0: 15.1.5.74.52741 > 83.41.39.166.4672: tcp

- Web arabiriminden rapor alınabilir



User

Object Tree:

- Firewalls
 - Metro Ethernet
 - dmz (ext)
 - inside
 - loopback
 - New Interface (ext)
 - outside (ext)
- Objects
- Services
- Tr...

Interface

Name:

Library:

Label:

☒ Regular interface
☐ Address is assigned dynamically
☐ Unnumbered interface
☐ Management interface
☒ This interface is external (insecure)

Comment:

Object Type:
Object Name:
Platform:
Version:
Host OS:

This firewall has three interfaces. Eth0 faces outside and has a static routable address; eth1 faces inside; eth2 is connected to DMZ subnet. Policy includes basic rules to permit unrestricted outbound access and anti-spoofing rules. Access to the firewall is permitted only from internal network and only using SSH. The firewall uses one of the machines on internal network for DNS. Internal network is configured with address 192.168.1.0/255.255.255.0, DMZ is 192.168.2.0/255.255.255.0. Since DMZ used private IP address, it needs

Metro Ethernet

Firewalls:

Policy	outside	inside	loopback	dmz	New Interface	NAT
Source	Destination	Service	Action	Options	Comment	
0	net-192.168.1.0	Metro Ethernet	TCP ssh	Accept	SSH Access to firewall is permitted only from internal network	
1	Metro Ethernet	internal server	DNS	Accept	Firewall uses one of the machines on internal network for DNS	
2	Any	Metro Ethernet	Any	Deny	All other attempts to connect to the firewall are denied and logged	
3	Any	Any	TCP auth	Reject	Quickly reject attempts to connect to ident server to avoid SMTP delays	
4	Any	server on dmz	TCP smtp	Accept	Mail relay on DMZ can accept connections from hosts on the Internet	
5	server on dmz	internal server	TCP smtp	Accept	this rule permits a mail relay located on DMZ to connect to internal mail server	
6	server on dmz	net-192.168.1.0	DNS, TCP smtp	Accept	Mail relay needs DNS and can connect to mail servers on the Internet	
7	net-192.168.2.0	net-192.168.1.0	Any	Deny	All other access from DMZ to internal net is denied	
8	net-192.168.1.0	Any	Any	Accept	This permits access from internal net to the Internet and DMZ	
9	Any	Any	Any	Deny		

Saldırı Tespit/Engelleme

- Normal trafik -saldırgan trafiği ?
- Anormal trafiği izlemek işe yarar mı?
- Snort, Snortsam, snort-inline en bilinen çözümler
- En bilinen özgür (N)IDS Snort
 - Kurucu firma Checkpoint tarafından 85k\$ alındı
 - SourceFire firması *OpenBSD+Snort+..* BOX ürünü
- Snortsam ve snort-inline Snort için engelleme eklentisi olarak kullanılabilir.

Snort ..



- 7 yıl öncesinde basit bir sniffer projesi..
- Günümüzde: Ağ temelli , imza tabanlı saldırı tespit sistemi
- Açık kaynak kodlu, Aktif geliştirici topluluğu
- Bol ve açık dökümantasyon
Belgeler, kitaplar, e-posta listeleri...
- Snortsam ile Firewall'a kural gönderme
- Onlarca yönetim arabirimi
 - En bilinenleri: Acid-Base, Squil, Ids center.

IDS Policy Manager

Policy Editor - Full Policy

File View Options Help

bad-traffic

Signatures Settings

Folder Items

- ☒ bad-traffic
- ☐ exploit
- ☒ scan
- ☒ finger
- ☒ ftp
- ☒ telnet
- ☒ smtp
- ☒ rpc
- ☒ rservices
- ☒ dos
- ☒ ddos
- ☒ dns
- ☒ tftp
- ☒ web-cgi
- ☒ web-coldfusion
- ☒ web-frontpage
- ☒ web-iis
- ☒ web-misc
- ☒ web-attacks
- ☒ sql
- ☒ x11
- ☒ icmp
- ☒ netbios
- ☒ misc
- ☒ attack-responses
- ☐ backdoor

Name: bad-traffic

Last Updated:

Last Modified Date: 1/13/2002 8:26:31 AM

of Rules: 8

of Active Rules: 8

Base Directory: Set All Groups

Description:

These signatures are representative of traffic that should never be seen on any network. None of these signatures include datagram content checking and are extremely quick signatures

Signature Name	Action	Protocol	Source IP/Port	Direction	Destination IP/Port
☒ BAD TRAFFIC tcp port 0 traffic	alert	tcp	\$EXTERNAL_NET/any	<>	\$HOME_NET/0
☒ BAD TRAFFIC udp port 0 traffic	alert	udp	\$EXTERNAL_NET/any	<>	\$HOME_NET/0
☒ BAD TRAFFIC data in TCP SYN pac...	alert	tcp	\$EXTERNAL_NET/any	->	\$HOME_NET/any
☒ BAD TRAFFIC loopback traffic	alert	ip	any/any	<>	127.0.0.0/8/any
☒ BAD TRAFFIC same SRC/DST	alert	ip	any/any	->	any/any
☒ BAD TRAFFIC ip reserved bit set	alert	ip	\$EXTERNAL_NET/any	->	\$HOME_NET/any
☒ BAD TRAFFIC 0 ttl	alert	ip	\$EXTERNAL_NET/any	->	\$HOME_NET/any
☒ BAD TRAFFIC bad frag bits	alert	ip	\$EXTERNAL_NET/any	->	\$HOME_NET/any

Total Rules: 1495 Rules Enabled: 1006 Rules File: E:\code\IDS2.0\FullPolicy\snort.conf

VPN hizmetleri

- VPN(Virtual Private Network) ?
- VPN Çeşitleri
 - Ipsec VPN, L2TP, PPTP, SSL VPN
- İhtiyaca göre seçim...





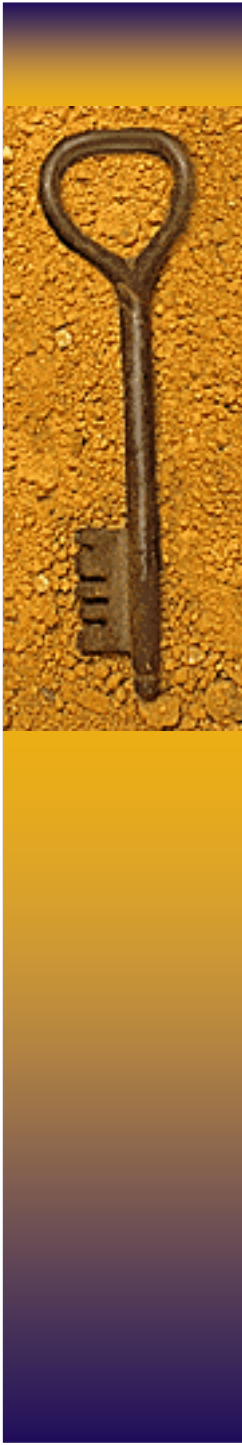
IPsec VPN Çözümleri

- Standart bir Çözüm
- Tam güvenlik
- Kompleks yapı, kurulum kullanım zor(?)
- Linux FreeSWAN/OpenSWAN
- OpenBSD Ipsec altyapısı



PPTP Çözümü

- Uçtan uca tünelleme/şifreleme sağlar
- Microsoft destekli...
- Hızlı, kolay yapılandırma kullanım tercih sebebi
- Windows işletim sistemi ile birlikte istemcisi gelir.
- Linux'lar için pptpclient.sf.net
- Şifreli kullanımı yeter seviyede güvenli



PopToP

- PopTop (The PPTP server for Linux) BSD, Solaris
- GPL Lisanslı
- Kolay kurulum ve yönetim
- Microsoft uyumlu kimlik denetimi ve şifreleme(MSCHAPv2, MPPE 40 - 128 bit RC4)
- Eşzamanlı birden fazla kullanıcı desteği
- Radius eklentisi ile samba ve ldap üzerinden onaylama yapabilir.
- www.poptop.org



OpenVPN

- MultiPlatform SSL VPN Çözümü
 - Linux,*BSD, Solaris, Windows...
- Geniş, anlaşılır dökümantasyon
- TCP/UDP tek port üzerinden çalışır, NAT sorunsuz
- OpenSSL kütüphanesinin sunduğu herşey..
- Kolay kurulum ve yönetim
 - GUI, konsol, Web
 - IPsec kompleksliği yok
- www.openvpn.net



OpenVPNAdmin GUI

Connection

Type: client
Nickname:
Description:

General Certificate Proxy Networking Security

Protocol: tcp Vebosity level: 1
Device: tap Device node:
Remote: Port: 1194
User: Group:
Local IP: Remote IP:
Ping: Ping restart:

Options

☐ Pull ☐ Persist Key ☐ Mute Replay Warnings
☐ No Bind ☐ Persist Tun ☐ LZO Compression

Connection

Type: client
Nickname: tls-home
Description: test für TLS

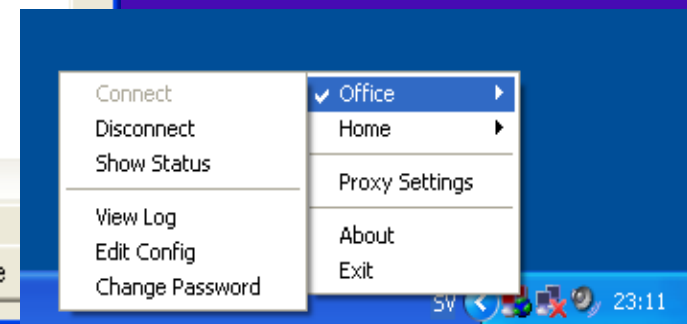
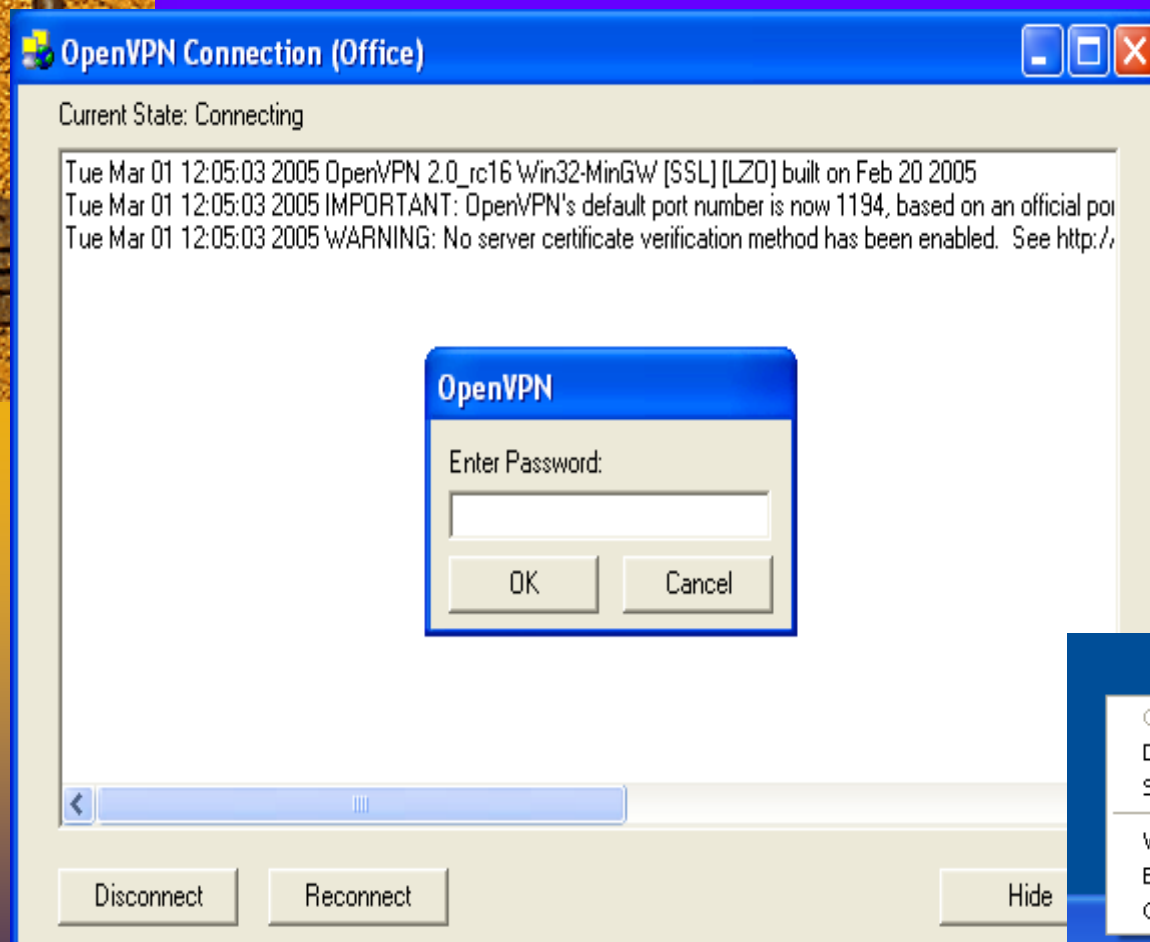
General Certificate Proxy

Protocol: tcp Vebosity level: 1
Device: tun Device node:
Remote: exploit.de Port: 1194
User: nobody Group: nobody
Local IP: Remote IP:
Ping: 15 Ping restart: 45

Options

☐ Pull ☒ Persist Key ☐ Mute Replay Warnings
☐ No Bind ☒ Persist Tun ☒ LZO Compression

OpenVPN GUI..



Zayıflık inceleme

- Açıklarınızı Hackerler keşfetmeden siz bulun..
- Ethical Hacking: Son yıllarda oldukça popüler
- Nessus, Nmap, nikto...



Nessus



- '98 yılında Renaud Deraison tarafından GPL olarak başlatıldı
- 2005 Lisans değişikliği...☹
- İstemci sunucu mimarisine göre çalışır
- Uzak ve yerel sistem güvenliği kontrolü
- Uzak ve yerel sistem güvenlik tarama özelliği
 - Nessus yerel güvenlik taraması yapabilen ik ürün
 - Windows, UNIX ve Mac makinelerle login olarak gerekli taramaları, eksik yamaları belirleyebilir
- Web, GUI , konsol ile kolay yönetim
- Güncel zayıflık veritabanı(günlük)
- Bulunan açıklar için detaylı bilgi ve referans
- 8000~farklı zayıflık imzası
- NASL ile zayıflık tanımlama özelliği
- Birçok ticari kopyası var



Proxy Hizmeti

- Proxy (Vekil Sunucu) nedir?
- Kullanım amacı
 - internet kullanımını kısıtlama
 - Bandwidth ayarlama
 - Raporlama
 - Güvenlik
 - Virus tarama vs
 - Squid, oops



Squid...

- http, https, ftp... için Caching proxy
- Şeffaf proxy (transparent Proxy) özelliği
- ACL yapısı ile gelişmiş kural tanıma imkanı
- LDAP, AD, Mysql üzerinden kullanıcı onaylama
- ClamAv deteği ile birlikte WEB trafiğinde virüs kontrolü
- Redirector desteği ile ek özellikler..



İçerik Filtreleme

- İçerik kontrolü nedir?
- Özgür bir çözüm: DansGuardian
- DansGuardian
 - Herhangi bir Proxy ile çalışabilir
 - Siteleri PICS(<http://www.w3.org/PICS/>) etiketleme sistemine göre bloklayabilir
 - MIME tipine ve dosya uzantısına göre filtreleme yapabilir.
 - Düzenli ifadeler ile URL filtreleme yapabilir.
 - IP tabanlı URL filtreleme
 - Veritabanına uygun CSV formatında log üretir.
 - Belirli IP ve kullanıcı adına göre filtreleme



Hazır CD'ler

- İhtiyaca yönelik hazırlanmış dağıtımlar
- Disksiz çalışan sürümler oldukça popüler
- Knoppix ile başlayan Live CD serüveni..
- Hemen hemen her ihtiyaca yönelik Live CD
 - Oyun, Matematik, Firewall, Güvenlik, Kurtarma, Router vs vs.
- Knoppix STD, Phlax, Whoppix, MonoWall



Tux Says:
Get FrozenTech's Linux CDs and DVDs
Just 99¢ to \$1.99 per disc with 49¢ shipping

hide ads

FrozenTech's LiveCD List

[News](#) :: [Forums](#) :: [Create a LiveCD](#) :: [Books](#) :: [Store](#)

Display LiveCDs with a function of

Votes [go vote]	Name	ISO Size (megabytes)		Prin		Download	Links
		Min	Max				
4	m0n0wall	5	5				W DW
2	redWall Firewall	148	154				W DW
1	NetBoz	53	143				W DW
0	Devil-Linux	88	88				W DW
0	floppyfw	2	2				W DW
0	Linux Live-CD Router	83	83				W DW
0	Public IP ZoneCD	271	271				W DW
0	Sentry Firewall CD	288	288				W DW
0	Trx Live Firewall	653	653				W DW
0	XORP Live CD	132	132	Firewall			W DW

- All Functions
- Astronomy
- Bioinformatics
- Clustering
- Desktop
- Development
- Diagnostics
- Education
- Firewall/Router
- Forensics
- Gaming
- GIS
- Hobby
- Home Entertainment
- Media Production
- Medical
- OS Replacement
- Rescue
- Robotics
- Science

[CLEAR SETTINGS](#)

Currently displaying 10 LiveCD/DVDs

Key:

Primary Functions:



Türkiye'den..

- Linux Kullanıcıları Derneği
 - Linux.org.tr, www.lkd.org.tr
- EnderUNIX Yazılım geliştirme ekibi
 - EnderUNIX.org
- Mutasyon.net
- Belgeler.org
- Fazlamesai.net
- Ceviz.net Linux Forumu
- www.huzeyfe.net



Teşekkürler..

Sunum adresi

http://www.enderunix.org/slides/acikkod_sec.pdf



Eskiz.NET'e teşekkürler...