

# Açık Kod Dünyasında Ağ ve Sistem Güvenliği

**Afşin Taşkiran**

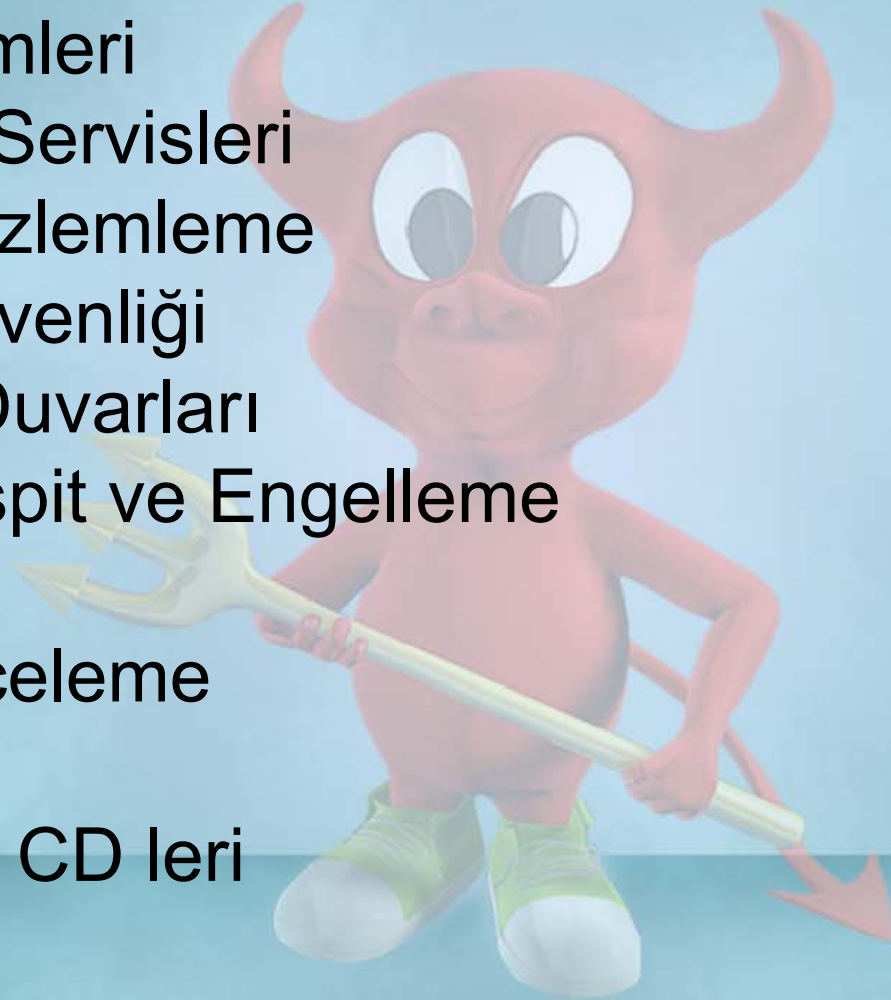
EnderUnix Çekirdek Takımı Üyesi

afsin ~ enderunix.org

[www.enderunix.org/afsin](http://www.enderunix.org/afsin)

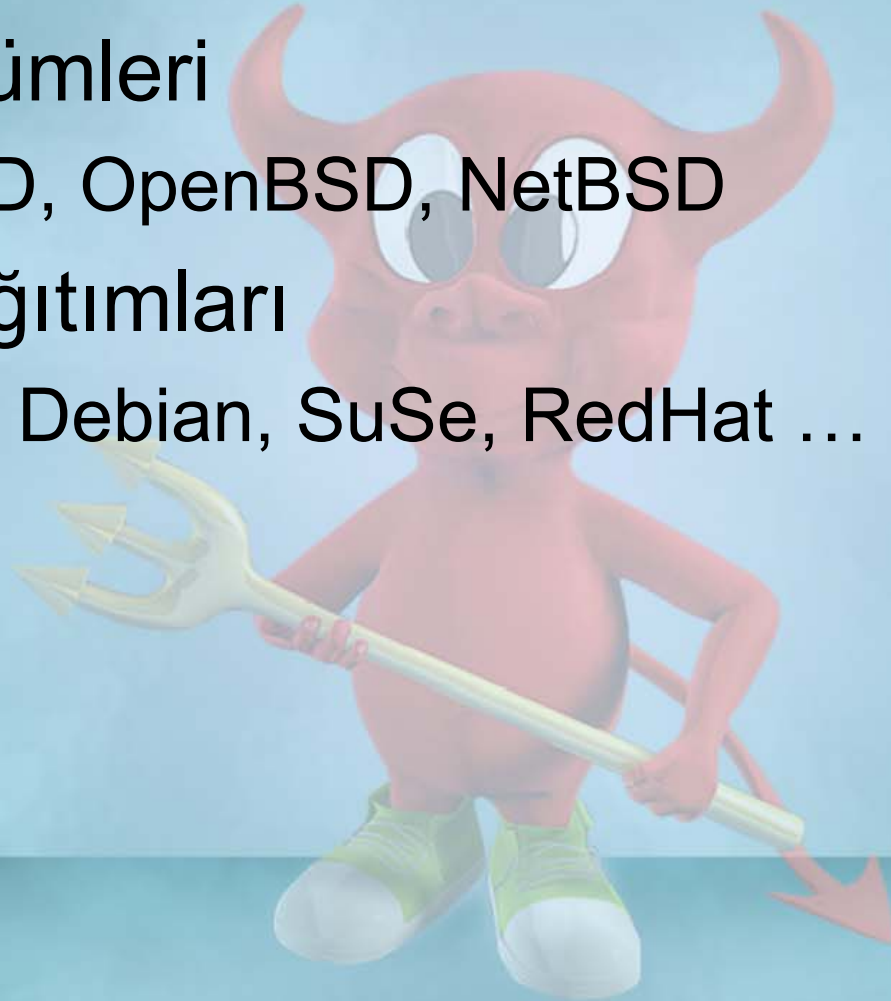
# Sunum Planı

- Unix Sürümleri
- Temel Ağ Servisleri
- Sistem Gözlemeleme
- Sistem Güvenliđi
- Güvenlik Duvarları
- Saldırı Tespit ve Engelleme
- VPN
- Zayıflık İnceleme
- Proxy
- Hazır Unix CD leri



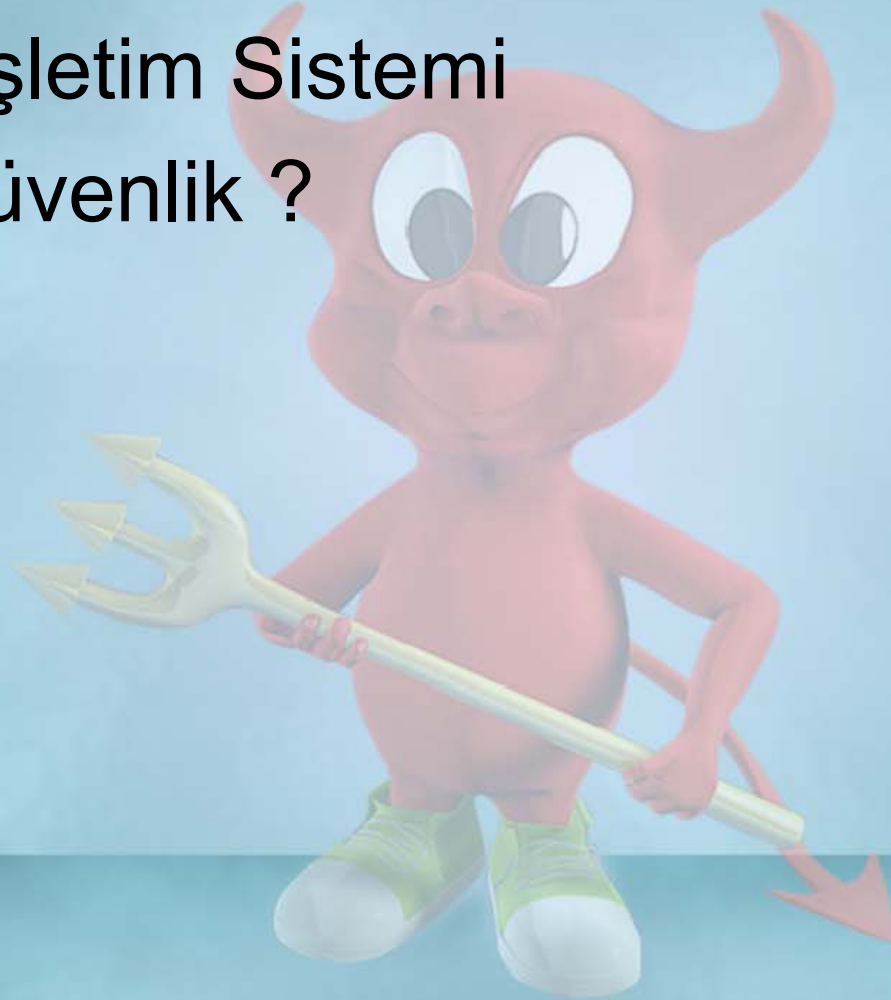
# Unix Sürümleri

- BSD Sürümleri
  - FreeBSD, OpenBSD, NetBSD
- Linux Dağıtımları
  - Gentoo, Debian, SuSe, RedHat ...



# Unix Sürümleri

- Güvenli İşletim Sistemi
- Ne için güvenlik ?



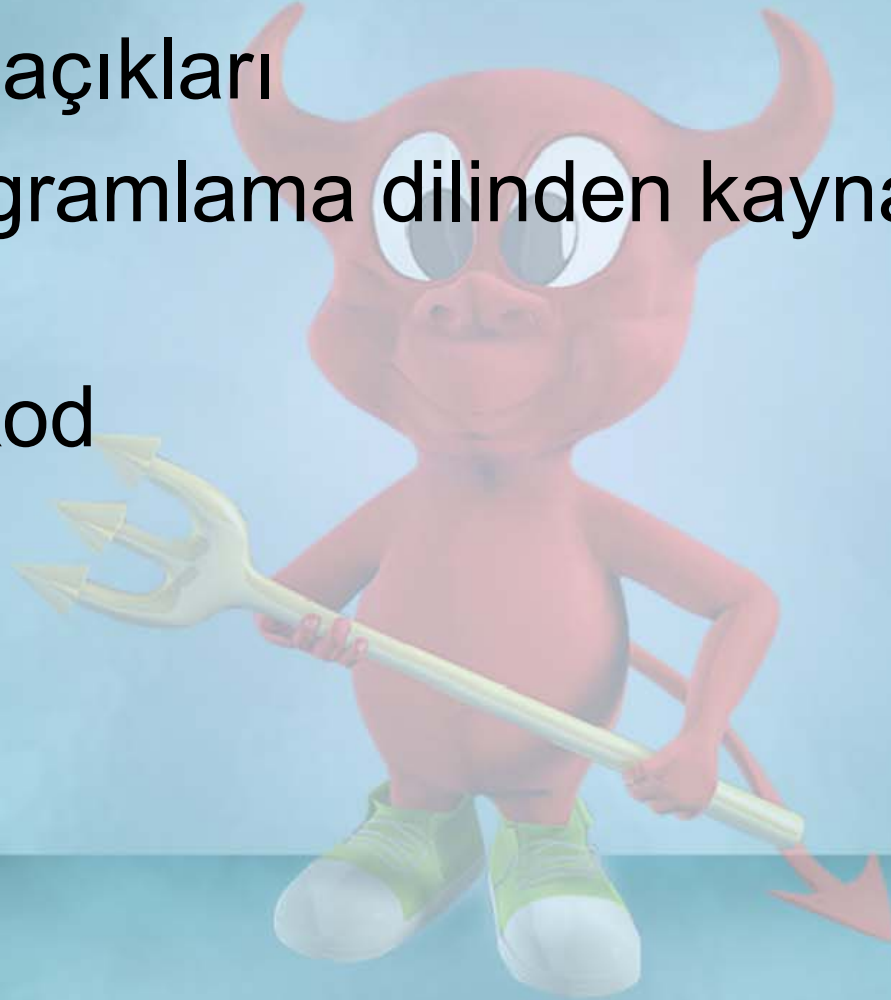
# Temel Ağ Servisleri

- Web Sunucusu
  - Apache
- DNS Sunucusu
  - Bind, TinyDNS, DjbdNS
- Mail Sunucusu
  - Qmail, Sendmail, Postfix, Exim ...
- FTP Sunucusu
  - ProFTP, vsFTP
- DHCP Sunucusu
  - ISC DHCP

# Temel Ağ Servisleri

## Web Sunucusu

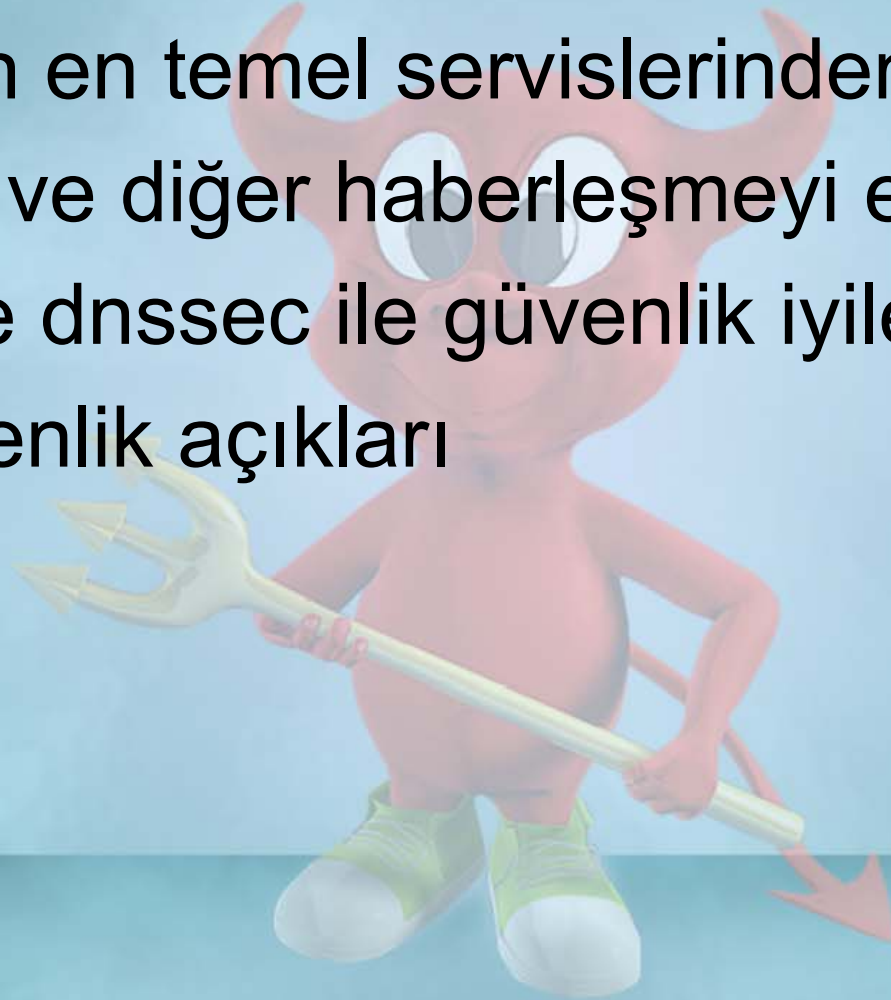
- Güvenlik açıkları
- Web Programlama dilinden kaynaklanan açıklar.
- Güvenli kod



# Temel Ağ Servisleri

## DNS Sunucusu

- Internet'in en temel servislerinden
- Mail,web ve diğer haberleşmeyi etkiliyor.
- Chroot ve dnssec ile güvenlik iyileştirme
- Bind güvenlik açıkları



# Temel Ağ Servisleri

## Mail Sunucusu

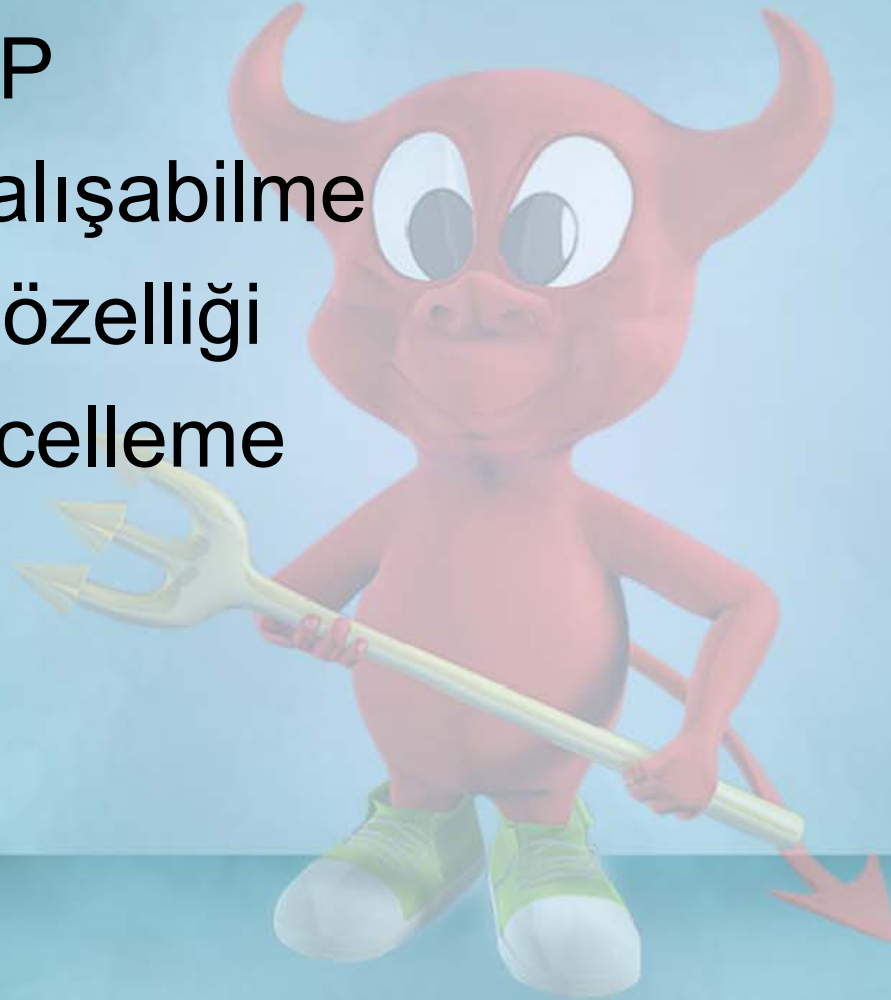
- Sendmail
- Postfix
- Qmail



# Temel Ağ Servisleri

## DHCP Sunucusu

- ISC DHCP
- Cluster çalışabilme
- Karaliste özelliği
- DNS güncelleme



# Sistem Gözleme

- Sunucu ve ađ ekipmanının gözlememesi



# Sistem Gözleme

## Nagios

- Ağ için komple bir gözleme aracı
- Sistemin ayakta olduğunun ve servislerinin gözlemlenmesi
  - Ssh, dns, dhcp, ldap, \*sql
  - Ping, tcp
- Dışarıdan kontrol edilemeyen fonksiyonların yerel makineye yüklenen yazılımlar yardımıyla kontrol edilmesi (Agent yapısı)
- Mail, sms, telefon ile gelişmiş uyarı mekanizması
- Detaylı ayakta bulunurluk raporu çıkarabilme

# Sistem Gözlemeleme

## Nagios

**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](http://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
22	3	4	0
<b>All Problems</b>		<b>All Types</b>	
7		35	

**Service Status Totals**

Ok	Warning	Unknown	Critical	Pending
103	2	0	14	18
<b>All Problems</b>		<b>All Types</b>		
16		137		

**Service Details For All Hosts**

Host	Service	Status	Last Check	Duration	Attempt	Service Information
app08	PING	OK	07-15-2001 14:04:09	4d 4h 7m 13s	1/3	PING ok - Packet loss = 0%, RTA = 0.60 ms
logrouter	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 Wrapper	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 Wrapper	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...

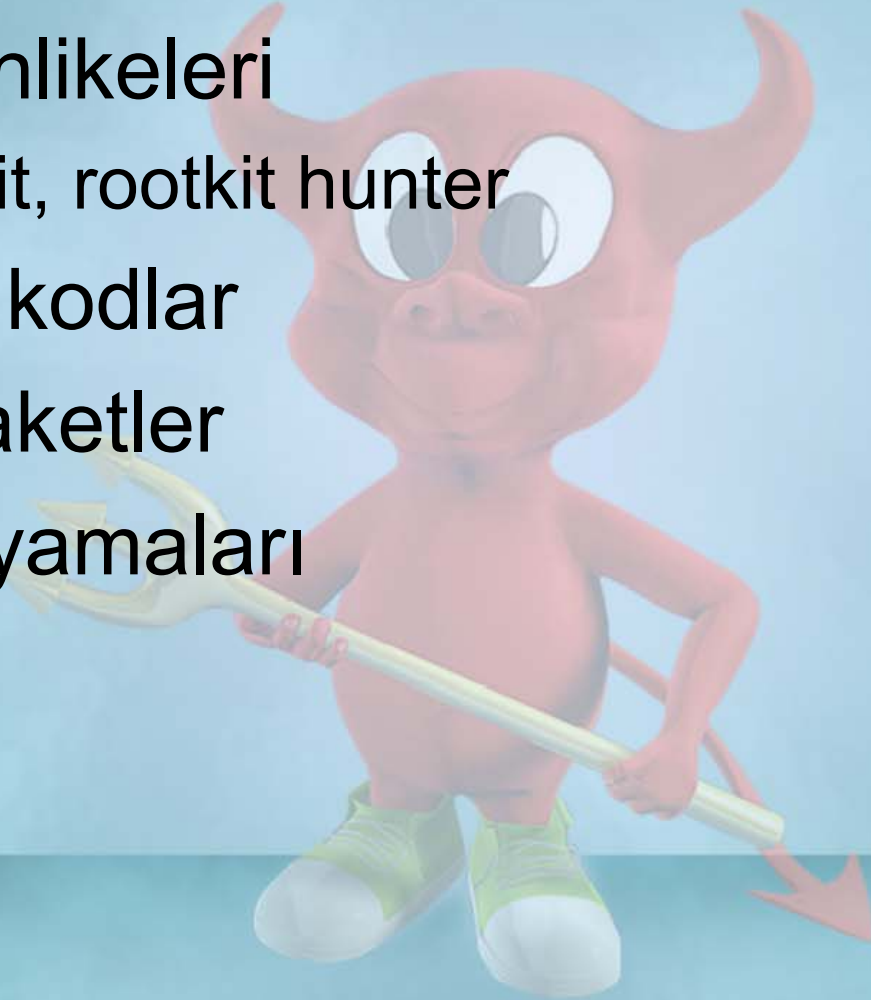
Document: Done

# Güvenlik Kavramı

- Ne kadar güvenlik ?
- Güvenlik / Maliyet ikilemi
- Paranoya ?
- Açık sistemlerde güvenlik
- En zayıf halka kim ?

# Sistem Güvenliđi

- Rootkit tehlikeleri
  - chkrootkit, rootkit hunter
- Güvensiz kodlar
- Güncel paketler
- Güvenlik yamaları



# Güvenlik Duvarları

- Ağdaki en temel ve gerekli ekipman
- Güvenlik tasarımı
- DMZ, Yerel ağ, İnternet kavramları
- Durum koruması (Stateful Inspection)
- Filtreleme, NAT

# Açık Kodlu Güvenlik Duvarları

- Iptables
- Packet Filter
- IPF
- IPFW



# Açık Kodlu Güvenlik Duvarları Iptables

- Linux 2.4 çekirdeği ile birlikte geldi.
- Ipchains'e göre en önemli özelliği durum korumalı olması (Stateful Inspection)
- Netfilter modülleri
- Zincir yapısı
- Patch-o-Matic ile üst düzey paket filtreleme işlemleri
- GUI aracılığı ile yönetilebilir
  - fwbuilder

# Açık Kodlu Güvenlik Duvarları

## Iptables

- Temel paket filtreleme işlemleri
  - iptables –A INPUT –i eth1 –p tcp –d 10.0.0.1 –dport 22 –m state –state NEW –j ACCEPT
- NAT İşlemleri
  - iptables –t nat –A POSTROUTING –o eth1 –j SNAT --to-source 10.0.0.1
  - iptables –t nat –A PREROUTING –i eth0 –j DNAT --to-destination 10.0.0.1

# Açık Kodlu Güvenlik Duvarları

## Packet Filter (PF)

- OpenBSD Projesi
- Kolay ve anlaşılır yapı
- İleri düzey trafik kontrolü
- HA ve Load balance olarak cluster çalışma
- Band genişliği yönetimi
- Yüksek performans
- GUI aracılığı ile yönetilebilir
  - Fwbuilder, pfw

# Açık Kodlu Güvenlik Duvarları

## Packet Filter (PF)

- Paket Filtremele

- 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 10.1.1.5 port 23

- NAT

- nat on \$ext\_if from \$ic\_ag to any -> 172.16.1.1

- Anlaşılır kayıt yapısı

- Dec 09 12:26:71.042152 rule 11/(match) **pass out on fxp0: 10.1.6.74.42841 > 12.13.14.15.4652: tcp**

# Açık Kodlu Güvenlik Duvarları FWBUILDER

Firewall Builder: PF.fwb, rev 1.1

File Edit Object Rules Help

Firewalls: Metro Ethernet

Policy outside inside loopback dmz New Interface NAT

Policy	Source	Destination	Service	Action	Options	Comment
0	net-192.168.1.0	Metro Ethernet	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	auth	Reject		Quickly reject attempts to connect to ident server to avoid SMTP delays
4	Any	server on dmz	smtp	Accept		Mail relay on DMZ can accept connections from hosts on the Internet
5	server on dmz	internal server	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 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		

Name: New Interface  
Library: User  
Label:   
 Regular interface  
 Address is assigned dynamically  
 Unnumbered interface  
 Management interface  
 This interface is external (insecure)  
Comment:   
Apply Changes

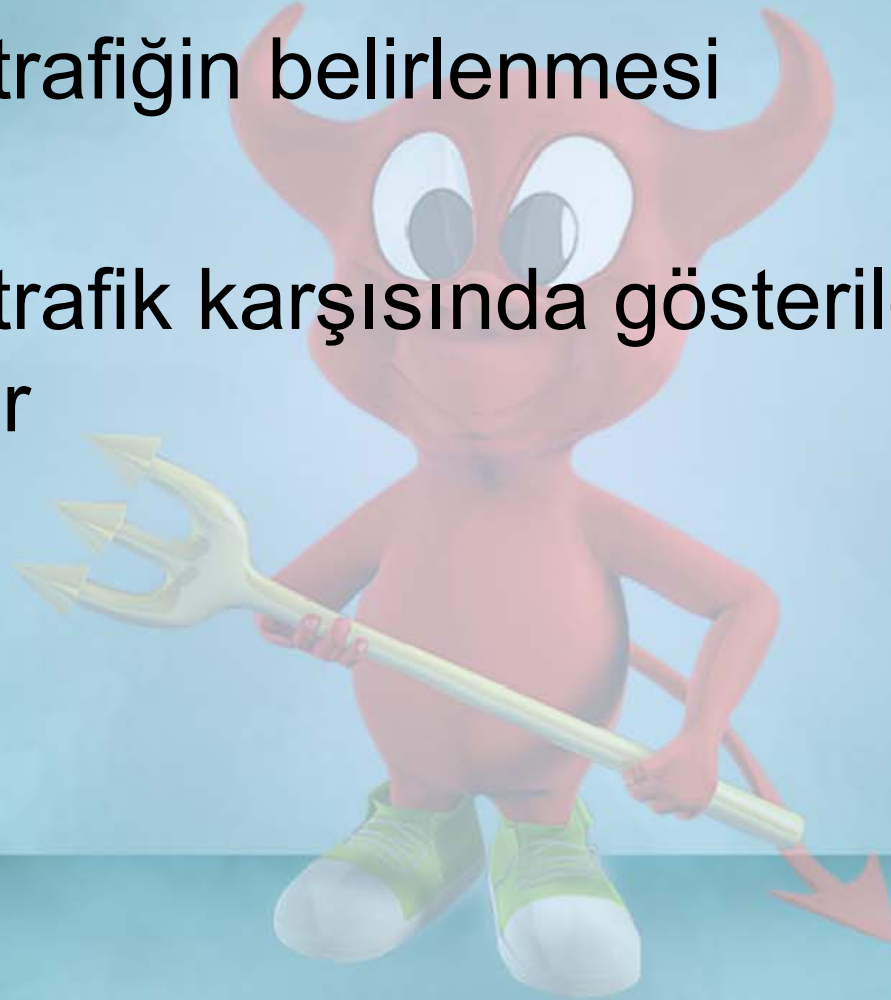
Object Type: Interface  
Object Name:   
Platform:   
Version:   
Host OS:   
Apply Changes

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

Start [Taskbar icons] 14:19 Cuma

# Saldırı Tespit ve Engelleme Sistemleri

- Anormal trafiğin belirlenmesi
  - IDS
- Anormal trafik karşısında gösterilen aksiyonlar
  - IPS
- IDP



# Saldırı Tespit ve Engelleme Sistemleri - SNORT

- 8 yıl önce başlayan sniffer projesi
  - snort
- Snort ile anormal trafik tespiti
- Ağ temelli ve imza tabanlı saldırı tespiti
- Snortsam ve snort-inline eklentileri
  - Snortsam ile güvenlik duvarına kural ekleme
- Açık kaynak kodlu
- Bir çok yönetim arayüzü
  - acid-base, squil, lds center

# IDS Policy Manager

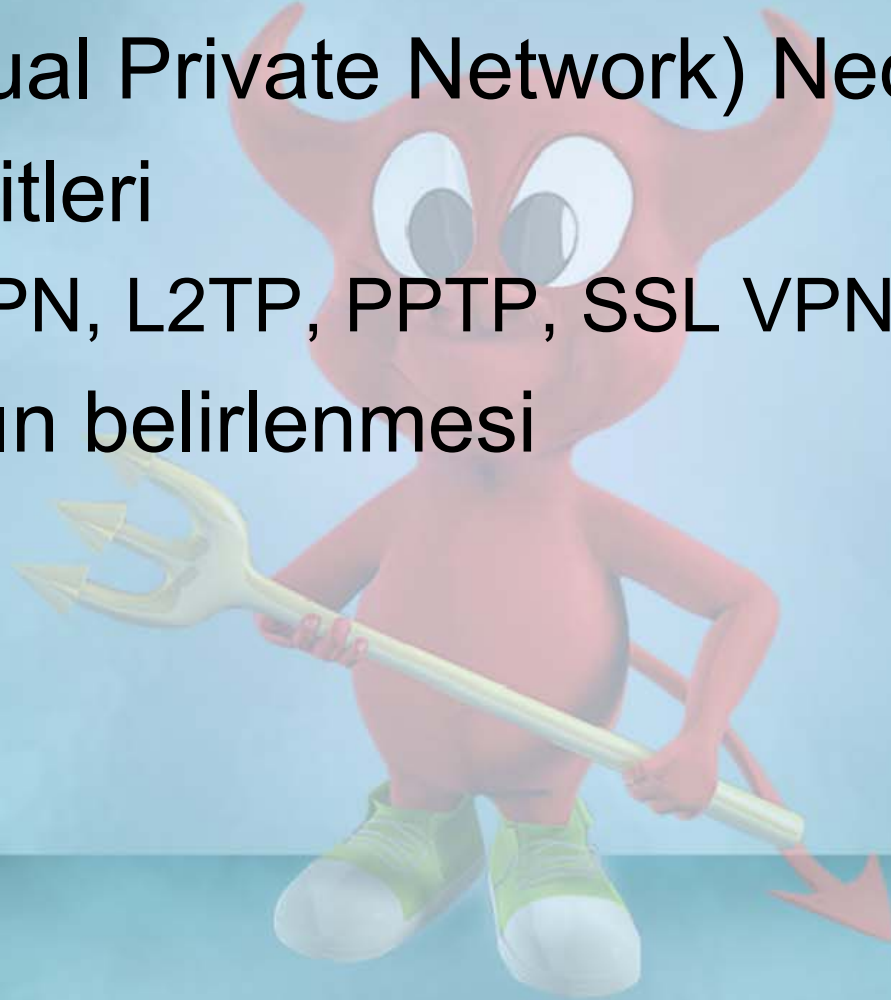
The screenshot shows the 'Policy Editor - Full Policy' window. The title bar includes 'File View Options Help'. The main window title is 'bad-traffic'. There are two tabs: 'Signatures' and 'Settings'. The 'Signatures' tab is active, showing a 'Folder Items' list on the left and a configuration panel on the right. The 'Folder Items' list includes: 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, and backdoor. The configuration panel for 'bad-traffic' shows: Name: bad-traffic, Last Updated: (empty), Last Modified Date: 1/13/2002 8:26:31 AM, # of Rules: 8, # of Active Rules: 8, Base Directory: (empty) with a 'Set All Groups' button. The Description field contains: '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'. Below the description is a table of signatures.

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

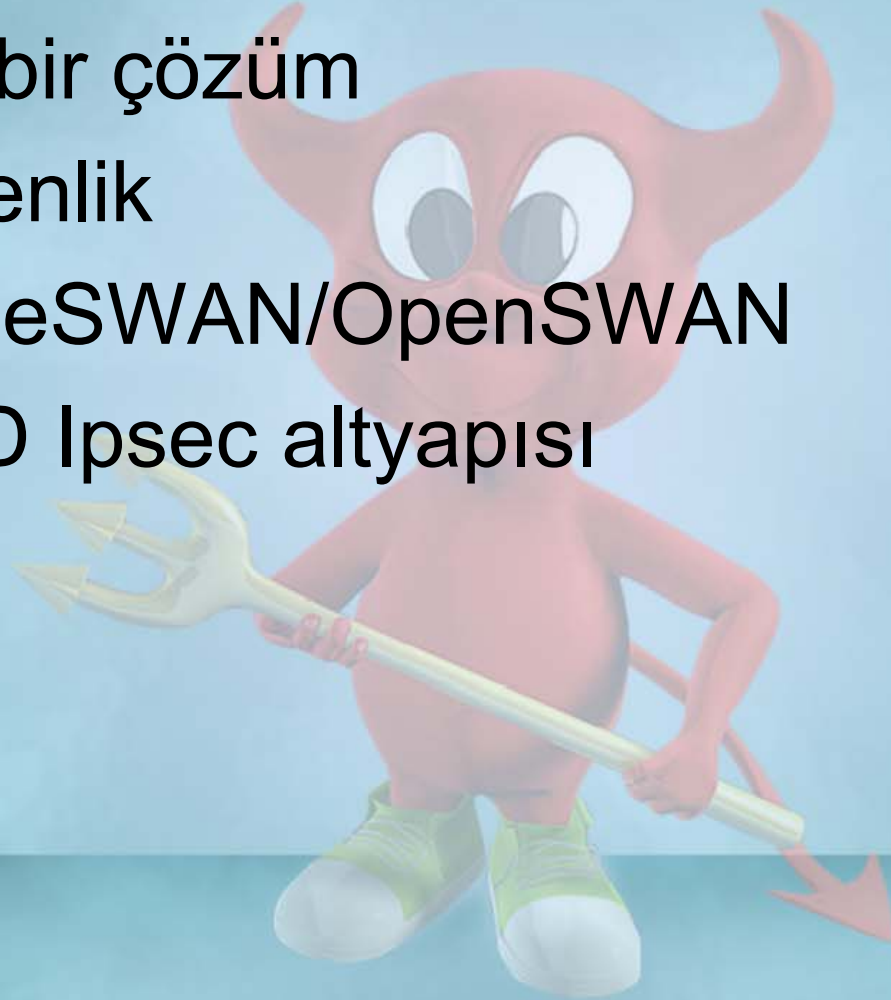
# VPN Hizmetleri

- VPN(Virtual Private Network) Nedir ?
- VPN Çeşitleri
  - Ipsec VPN, L2TP, PPTP, SSL VPN
- İhtiyaçların belirlenmesi



# IPSEC VPN

- Standart bir çözüm
- Tam güvenlik
- 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](http://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 Idap üzerinden onaylama yapabilir.
- [www.poptop.org](http://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](http://www.openvpn.net)

# OpenVPN Admin GUI

**Connection**

Type: client

Nickname: |

Description:

General Certificate Proxy Networking Security

Protocol: tcp Veboesity 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 Veboesity level: 1

Device: tun Device node:

Remote: exploit.de Port: 1194

User: nobody Group: nobody

Local IP: Remote IP:

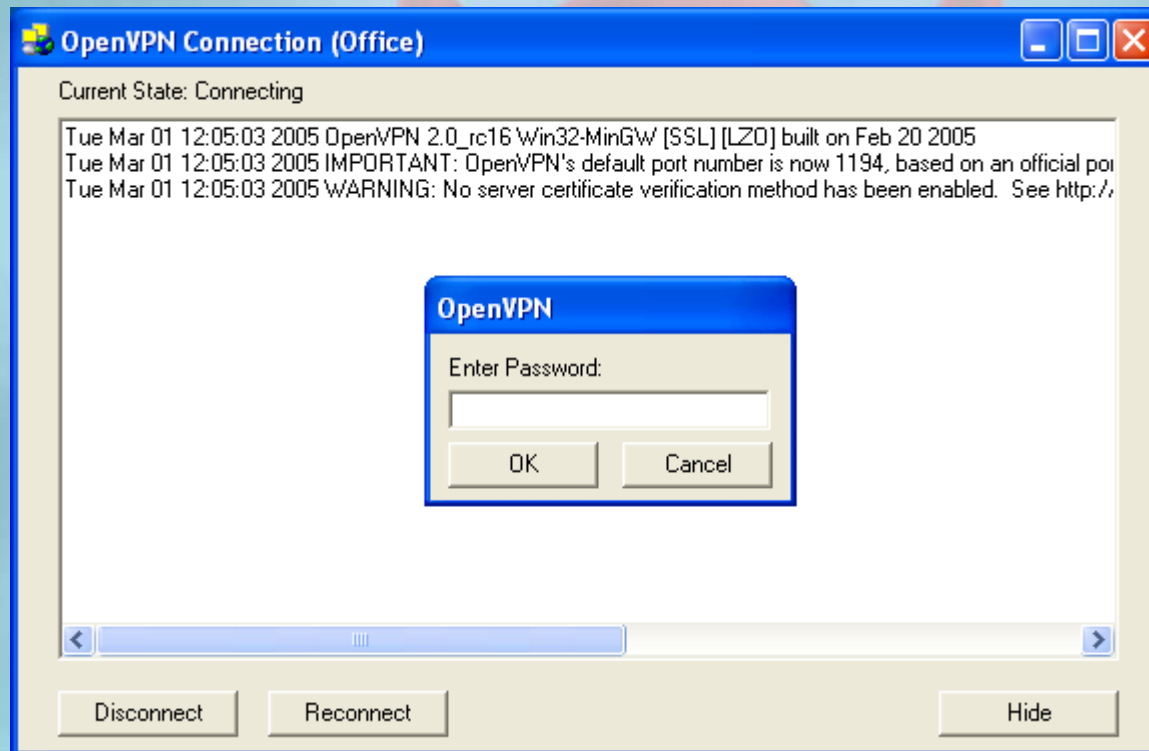
Ping: 15 Ping restart: 45

**Options**

Pull  Persist Key  Mute Replay Warnings

No Bind  Persist Tun  LZO Compression

# OpenVPN GUI



# Zayıflık İnceleme

- Güvenlik yöneticisinin açıkları kötü niyetli kişilerden önce tespit etmesi
- Ethical Hacking
- Nessus, Nmap, nikto...



# Nessus

- '98 yılında Renaud Deraison tarafından GPL olarak başlatıldı
- 2005 Lisans deęişikliği...
- İstemci sunucu mimarisine göre çalışır
- Uzak ve yerel sistem güvenliği kontrolü
- Uzak ve yerel sistem güvenlik tarama özellięi
  - Nessus yerel güvenlik taraması yapabilen ilk ürün
  - Windows, UNIX ve Mac makinelere 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 özellięi
- Birçok ticari kopyası var

# Proxy Hizmetleri

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

# Proxy Hizmetleri

## 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..

# Proxy Hizmetleri

## 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

# Hazır CD ler



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

- 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:



# Adresler

- EnderUnix Güvenlik E-Posta Listesi
  - <http://lists.enderunix.org>



# Yararlanılan Kaynaklar

- Nessus Web Sitesi; [www.nessus.org](http://www.nessus.org)
- Linux'un ağ ve güvenlik hizmetinde sunduğu olanaklar, Huzeyfe Önal, [www.enderunix.org/huzeyfe](http://www.enderunix.org/huzeyfe)
- Nagios Web Sitesi; [www.nagios.org](http://www.nagios.org)



# Sponsorlarımız / Teşekkürler

- Açık Akademi Kitabevi
  - <http://www.acikakademi.com>
- EnderSYS Yazılım Danışmanlık
  - <http://www.endersys.com>
- Sun Microsystems Türkiye
  - <http://tr.sun.com>

# Teşekkürler

## Açık Kod Dünyasında Ağ ve Sistem Güvenliği

**Afşin Taşkiran**

afsin ~ enderunix.org

[www.enderunix.org/afsin](http://www.enderunix.org/afsin)