



Açık Kod Dünyasında Ağ ve Sistem Güvenliği

Afşin Taşkiran

EnderUnix Çekirdek Takımı Üyesi

afsin ~ enderunix.org

www.enderunix.org/afsin

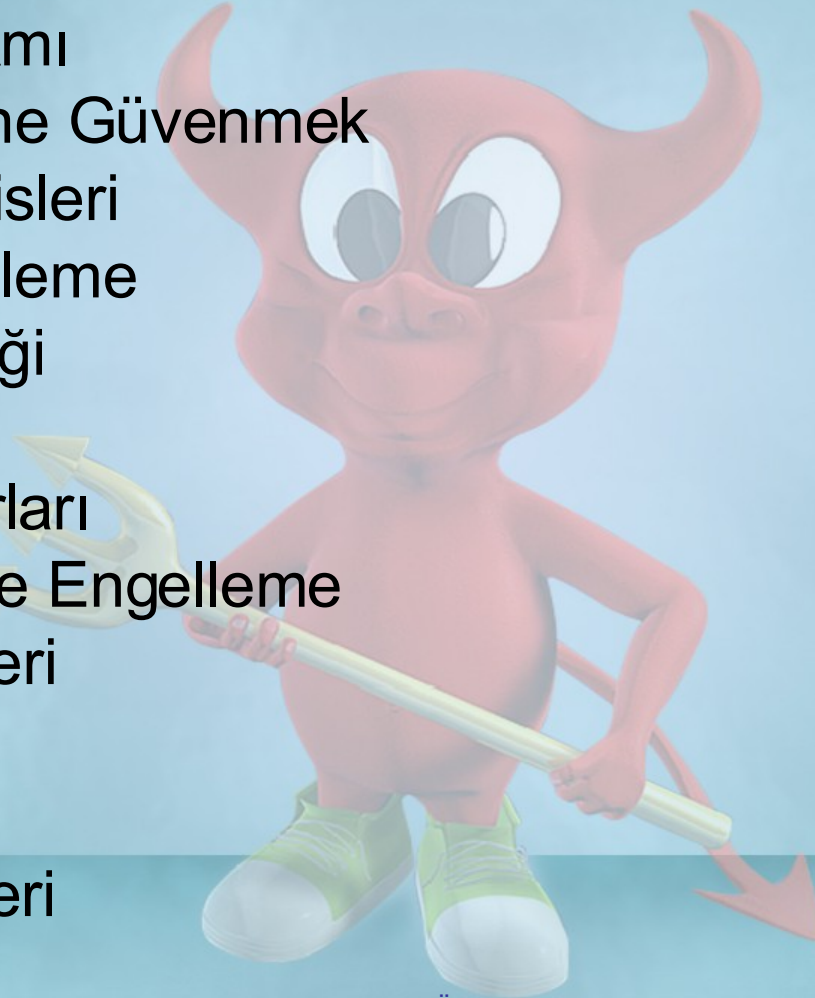


Samsun Ondokuz Mayıs Üniversitesi
Nisan 2007

Açık Kod Dünyasında
Ağ ve Sistem Güvenliği

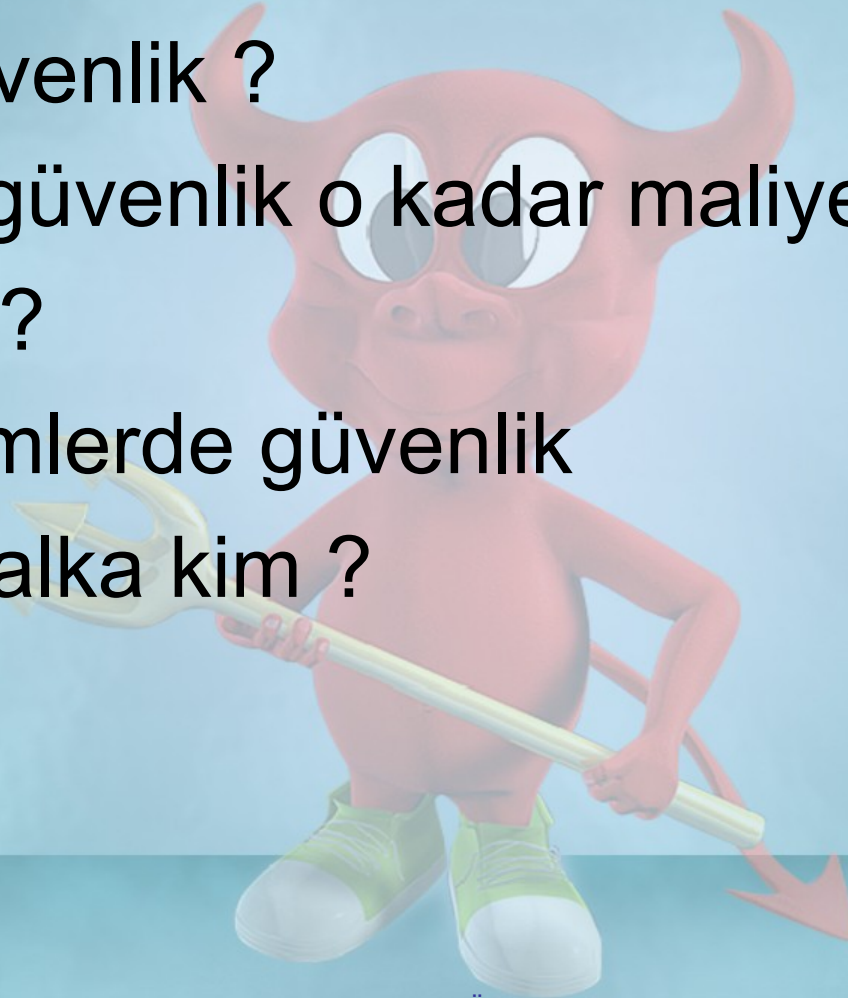
Sunum Planı

- Güvenlik Kavramı
- İşletim Sistemine Güvenmek
- Temel Ağ Servisleri
- Sistem Gözlemleme
- Sistem Güvenliği
- Ağ Güvenliği
- Güvenlik Duvarları
- Saldırı Tespit ve Engelleme
- VPN Teknolojileri
- Zayıflık
- Proxy
- Hazır *nix CD leri



Güvenlik Kavramı

- Ne için güvenlik ?
- Ne kadar güvenlik o kadar maliyet
- Paranoya ?
- Açık sistemlerde güvenlik
- En zayıf halka kim ?



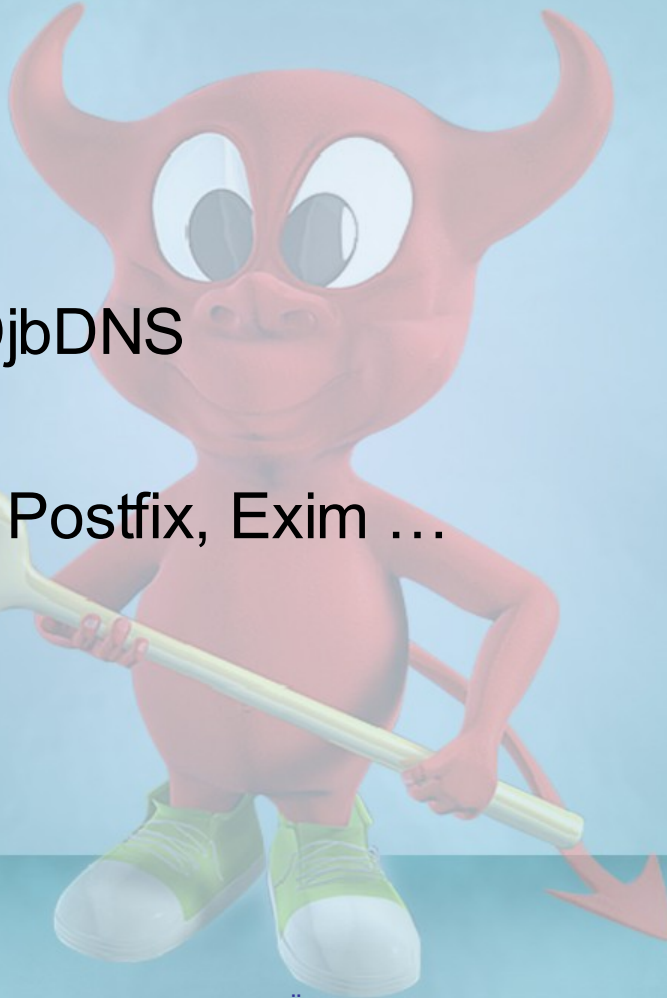
İşletim Sistemine Güvenmek

- Güvenilir işletim sistemi
- İşletim sisteminin güvenliği neden önemlidir ?
- BSD Sürümleri
 - FreeBSD, OpenBSD, NetBSD
- Linux Dağıtımları
 - Gentoo, Debian, SuSe, RedHat ...



Temel Ağ Servisleri

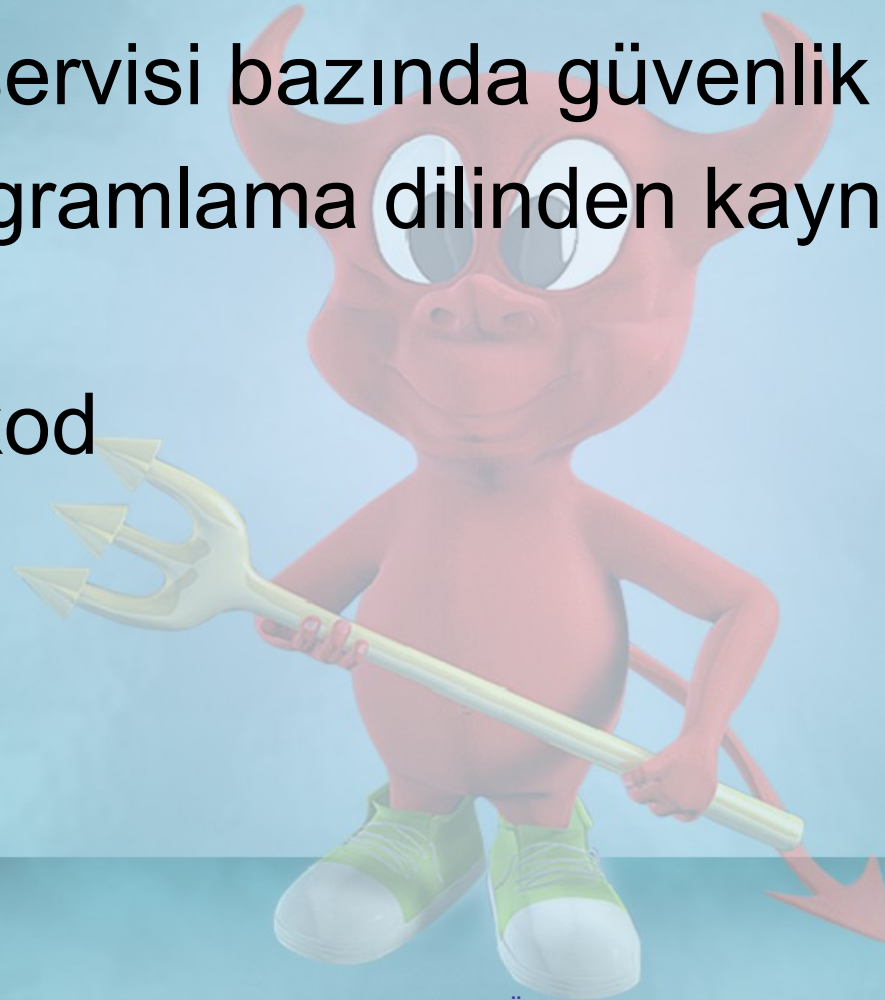
- Web Sunucusu
 - Apache
- DNS Sunucusu
 - Bind, TinyDNS, DjbdNS
- Mail Sunucusu
 - Qmail, Sendmail, Postfix, Exim ...
- FTP Sunucusu
 - ProFTP, vsFTP
- DHCP Sunucusu
 - ISC DHCP



Temel Ağ Servisleri

Web Sunucusu

- Sunucu servisi bazında 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, dnssec ve TSIGS (Transaction Signatures) ile güvenlik iyileştirme
- Bind güvenlik açıkları
- Zone transfer

Temel Ağ Servisleri

Mail Sunucusu

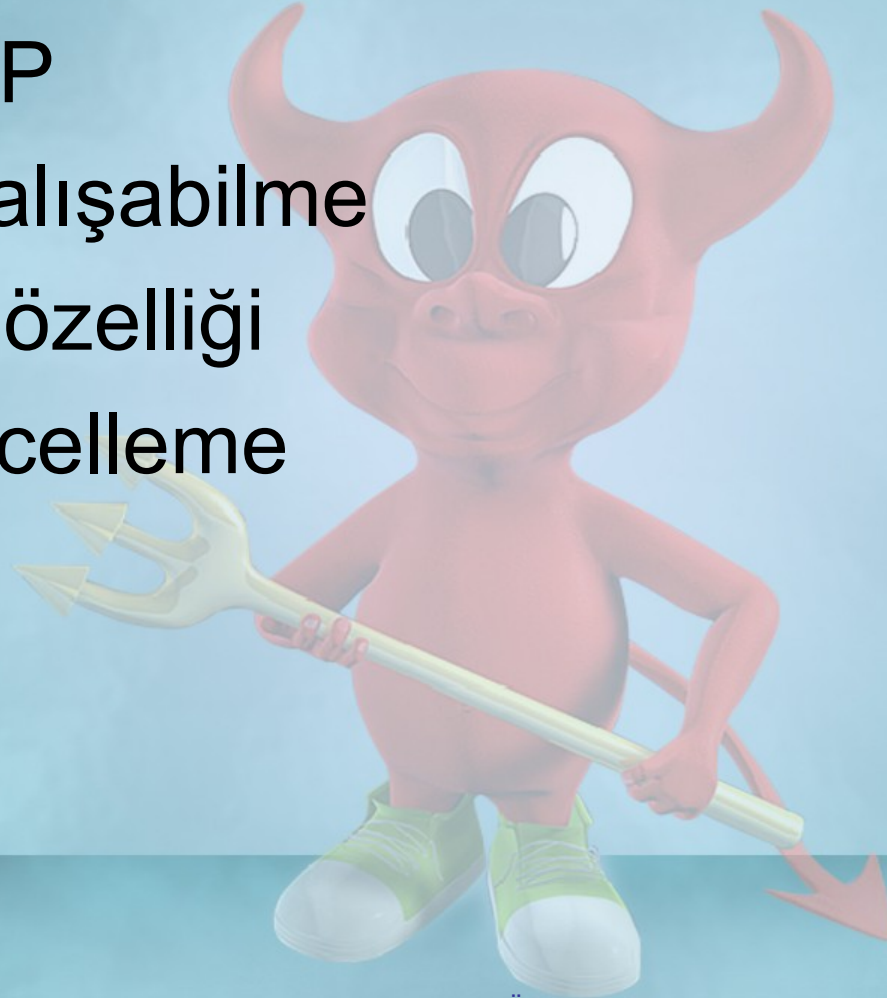
- Sendmail
- Postfix
- Qmail



Temel Ağ Servisleri

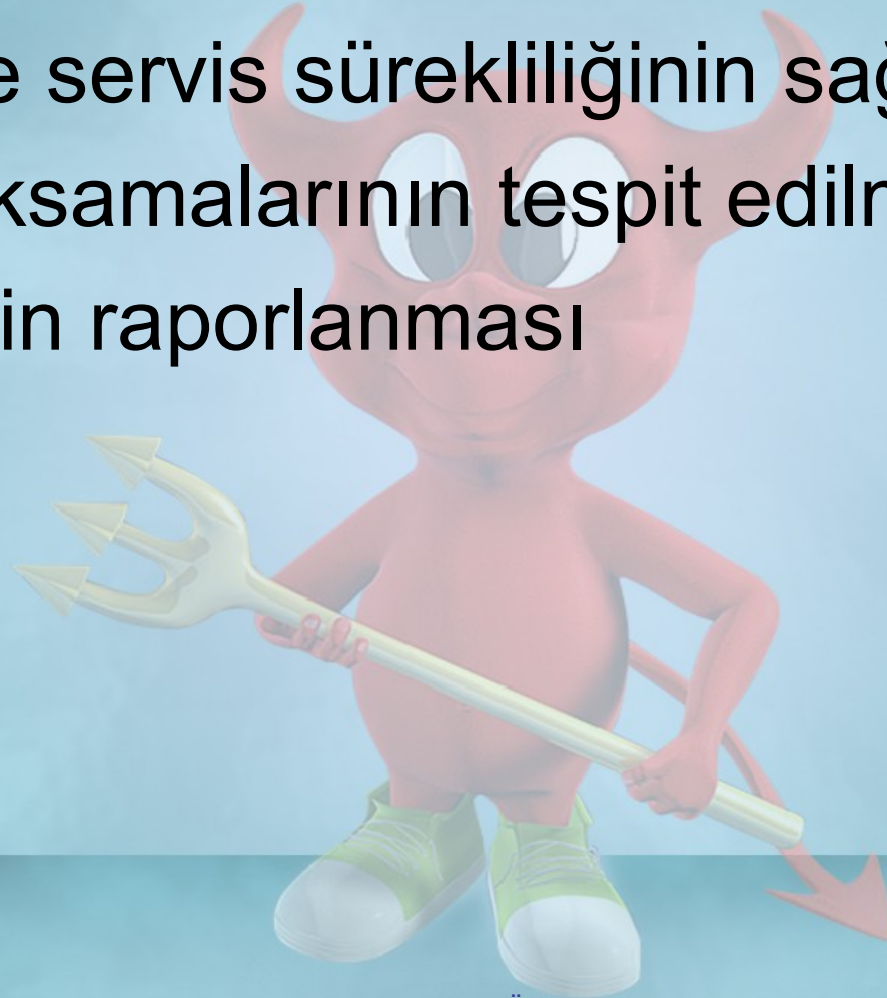
DHCP Sunucusu

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



Sistem Gözlemleme

- Sistem ve servis sürekliliğinin sağlanması
- Hizmet aksamalarının tespit edilmesi
- Kesintilerin raporlanması



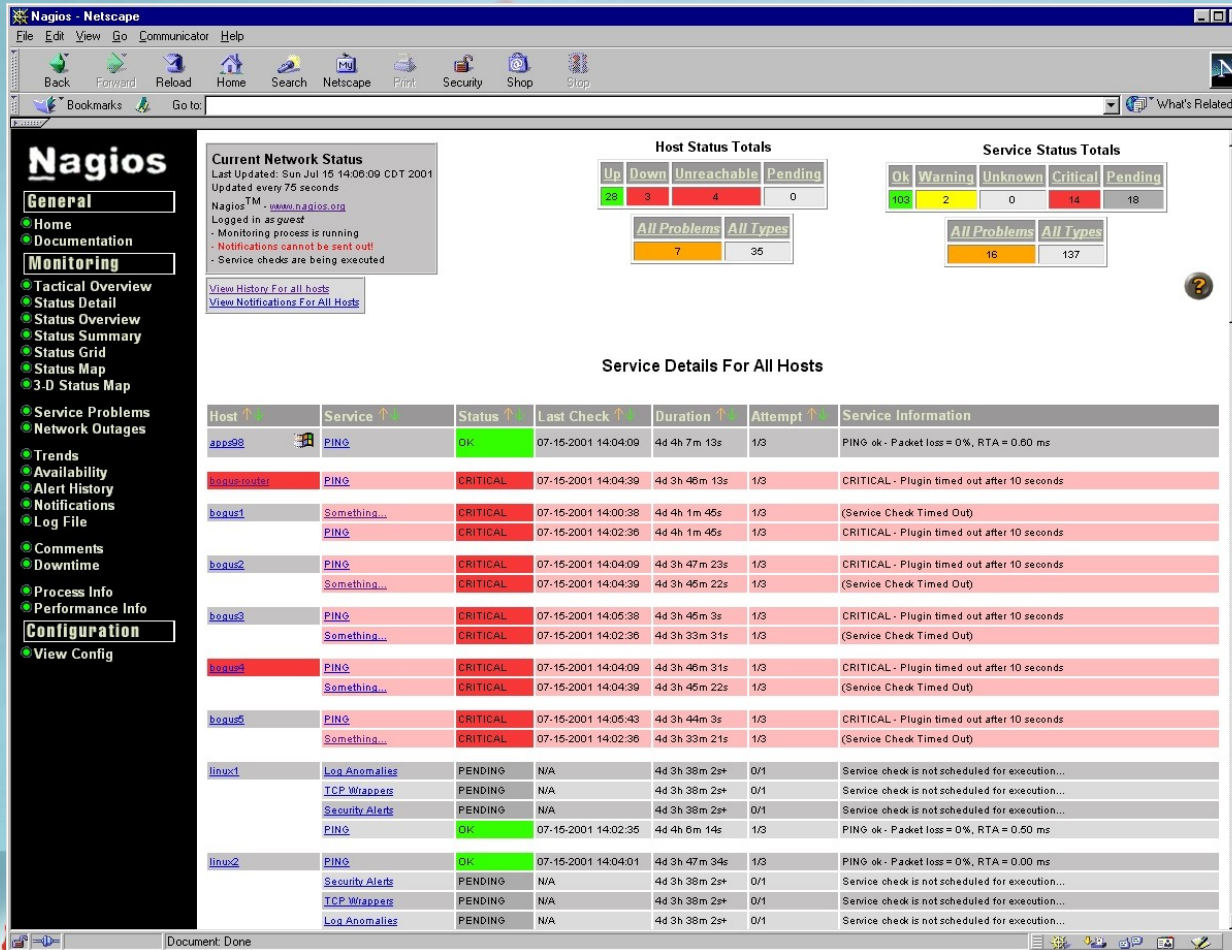
Sistem Gözlemeleme

Nagios

- Ağ için komple bir gözlemeleme 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 bulunulurluk raporu çıkarabilme

Sistem Gözlemleme

Nagios



Sistem Gözlemleme Cacti



Sistem Güvenliği

- Güvensiz kodlar
 - Binary dağıtımlar, RPM, DEB, tbz
 - HASH kontrolü
- Güncel paketler
 - Güvenlik açıkları ve duyurulan yamalar
- Rootkit tehlikeleri
 - chkrootkit, rootkit hunter
- Yerel erişim taşmaları
- Bütünlük Kontrolü
 - Tripwire



Ağ Güvenliği

- Güvenlik duvarları
 - Packet Filter, IpFW, IpFilter, Iptables
- Proxy ve İçerik Kontrol Sistemleri
 - Squid, DansGuardian, SquidGuard
- Saldırı tespit ve engelleme sistemleri (IDS / IPS)
 - Snort
- Honeypot

Güvenlik Duvarları

- Ağdaki en temel ve gerekli ekipman
- Güvenlik tasarımı
- DMZ, Yerel ağ, Internet kavramları
- Durum koruması (Stateful Inspection)
- Filtreleme, NAT
- Temelde L4'e kadar güvenlik sağlayabilme

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
- Round Robin ile arkadaki sunucularda yük paylaşımı
- 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

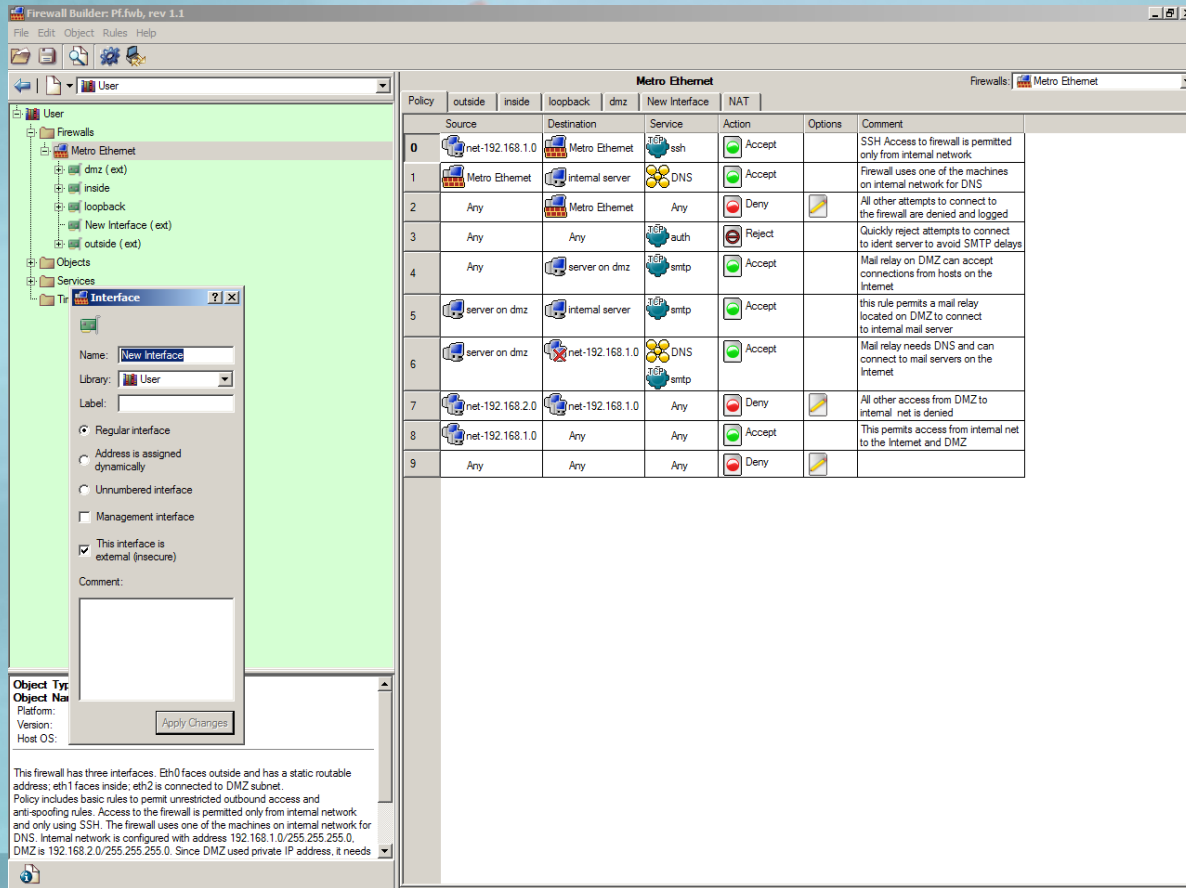
- NAT

- nat on \$ext_if from \$ic_ag to any -> 172.16.1.1

- Anlaşılır kayıt yapısı

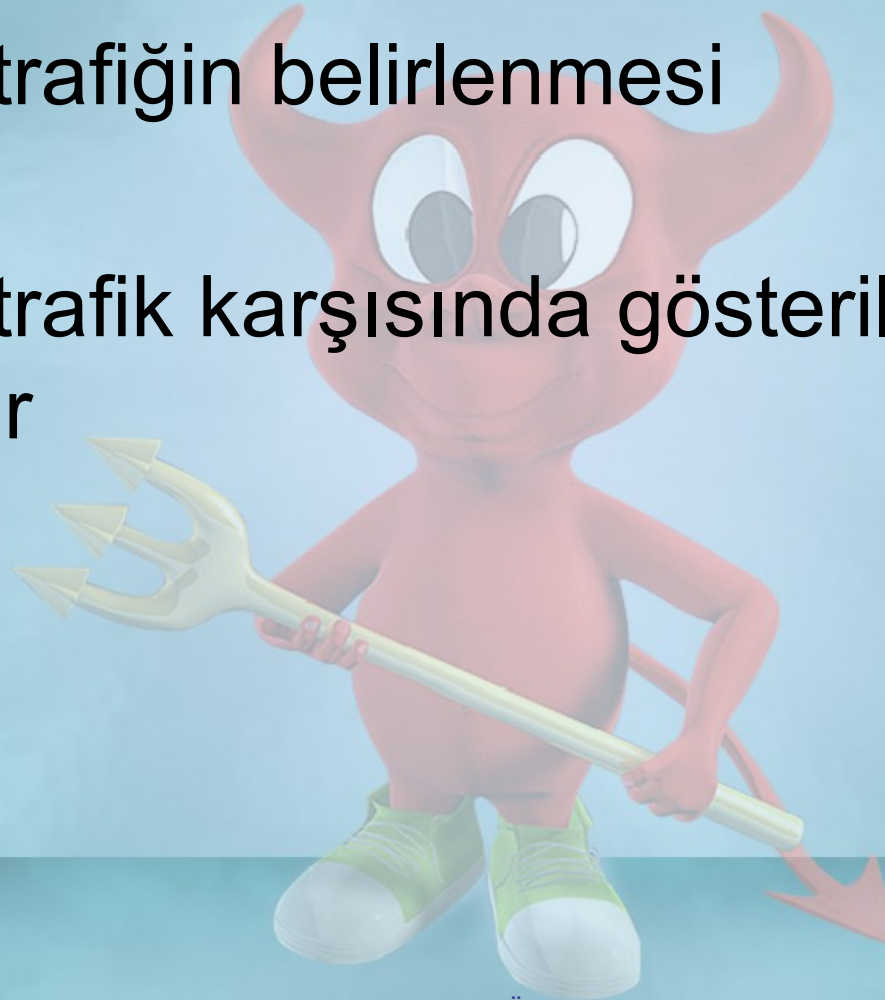
- Dec 09 12:26:71.042152 rule 11/(match) **pass out on**
fxp0: 10.1.6.74.42841 > 12.13.14.15.4652: tcp

Açık Kodlu Güvenlik Duvarları FWBUILDER



Saldırı Tespit ve Engelleme Sistemleri

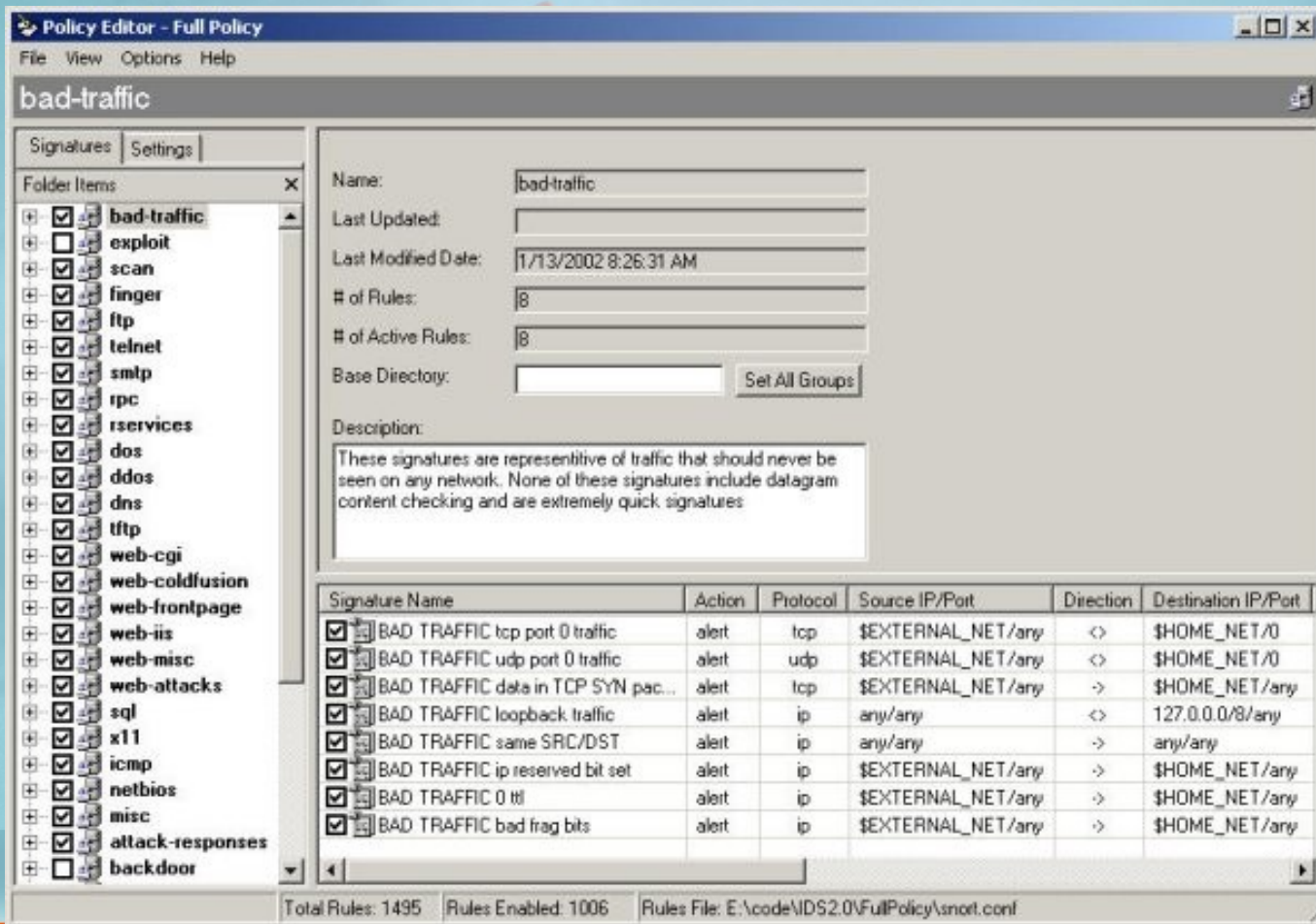
- Anormal trafiğin belirlenmesi
 - IDS
- Anormal trafik karşısında gösterilen aksiyonlar
 - IPS
- IDP



Saldırı Tespit ve Engelleme Sistemleri - SNORT

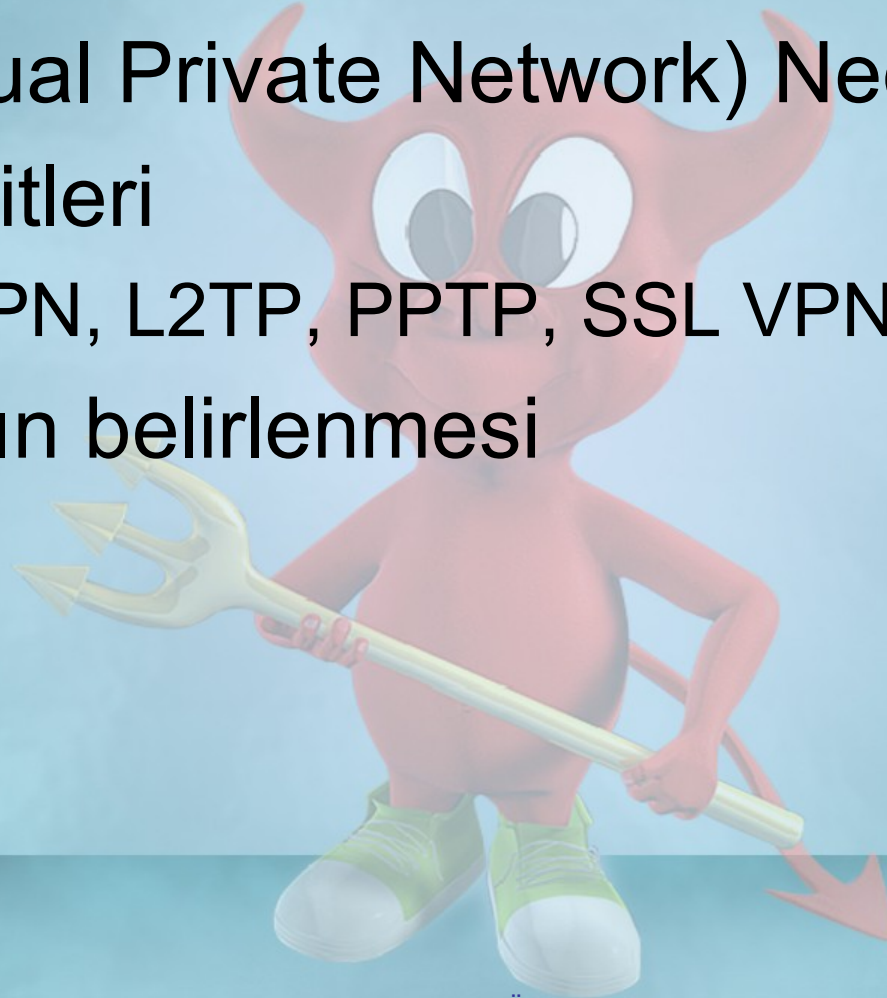
- 8 yıl önce başlayan sniffer projesi
 - snort
- Snort ile anormal trafik tespiti
- Ağ temelli ve imza tabanlı saldırı tesbiti
- Snortsam ve snort-inline eklentileri
 - Snortsam ile güvenlik duvarına kural ekleme
- Açık kaynak kodlu
- Bir çok yönetim arayüzü
 - acid-base, squil, lds center

IDS Policy Manager



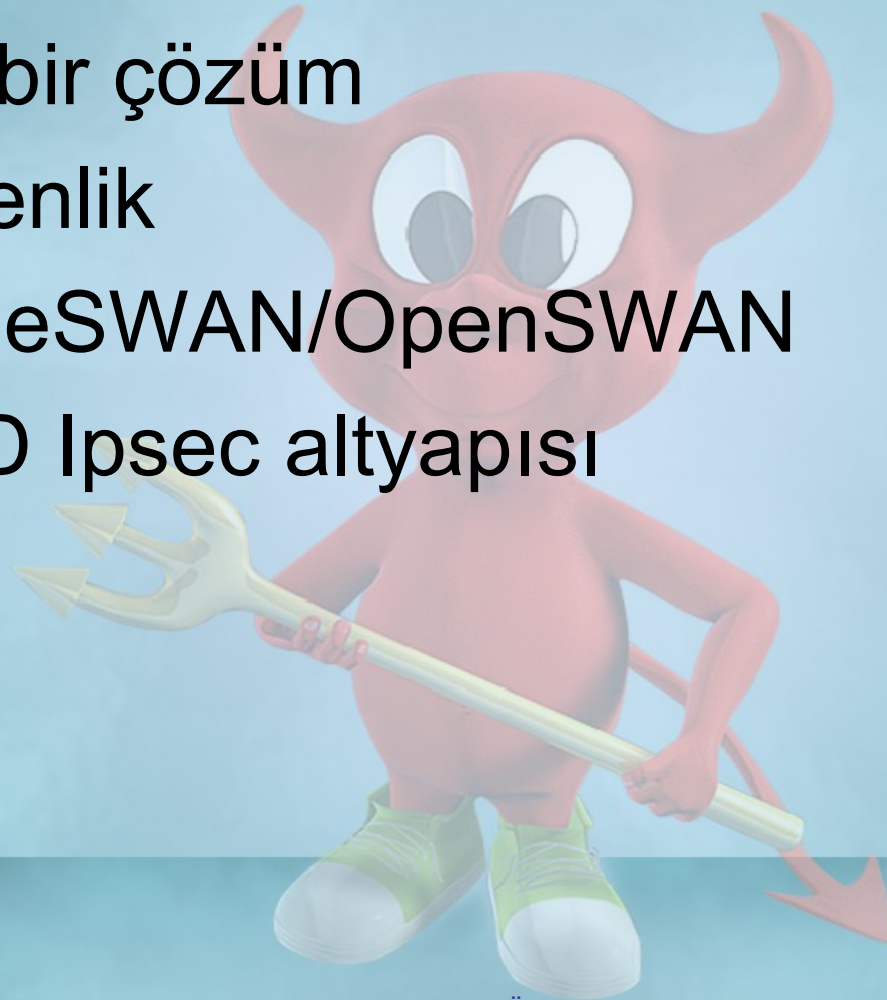
VPN Çözümleri

- 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
- 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



OpenVPN Admin GUI

Connection

Type: client

Nickname:

Description:

General Certificate Proxy Networking Security

Protocol: tcp ▾ Verbosity 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

 Cancel  OK

Connection

Type: client

Nickname: tls-home

Description: test für TLS

General Certificate Proxy

Protocol: tcp ▾ Verbosity level: 1 ▴ ▾

Device: tun ▾ Device node:

Remote: exploit.de Port: 1194

User: nobody Group: nobody

Local IP: Remote IP:

Ping: 15 Ping restart: 45

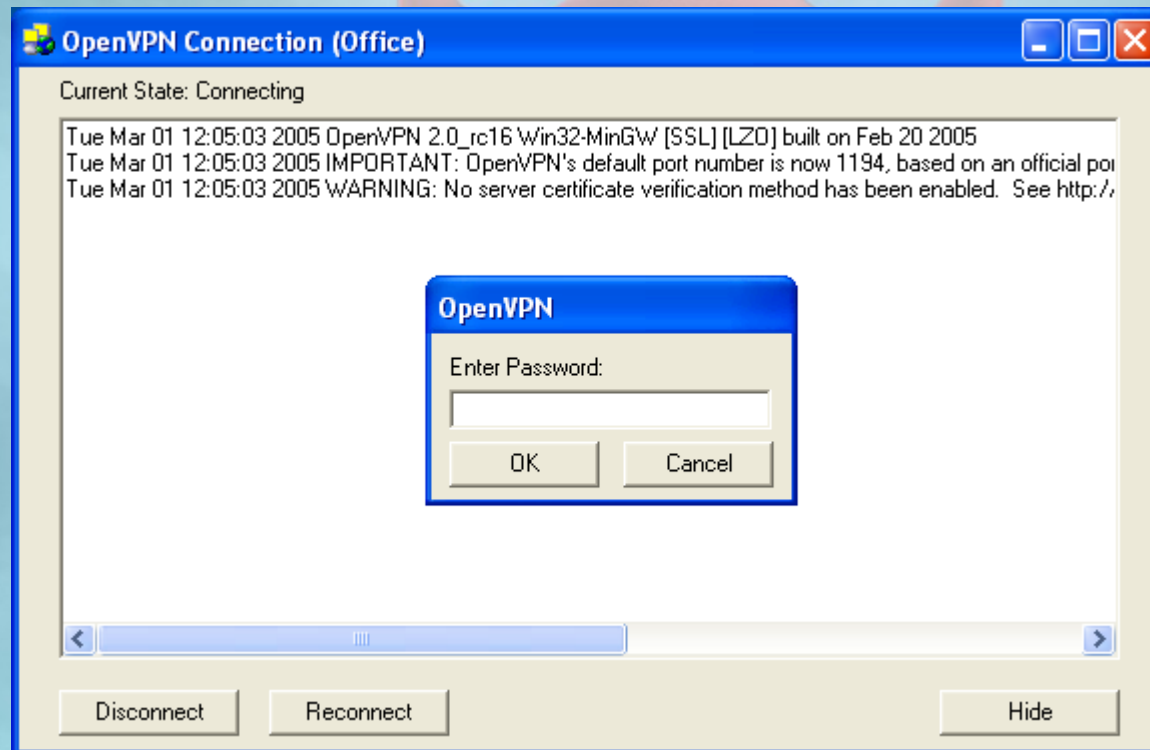
Options

☐ Pull ☒ Persist Key ☐ Mute Replay Warnings

☐ No Bind ☒ Persist Tun ☒ LZO Compression

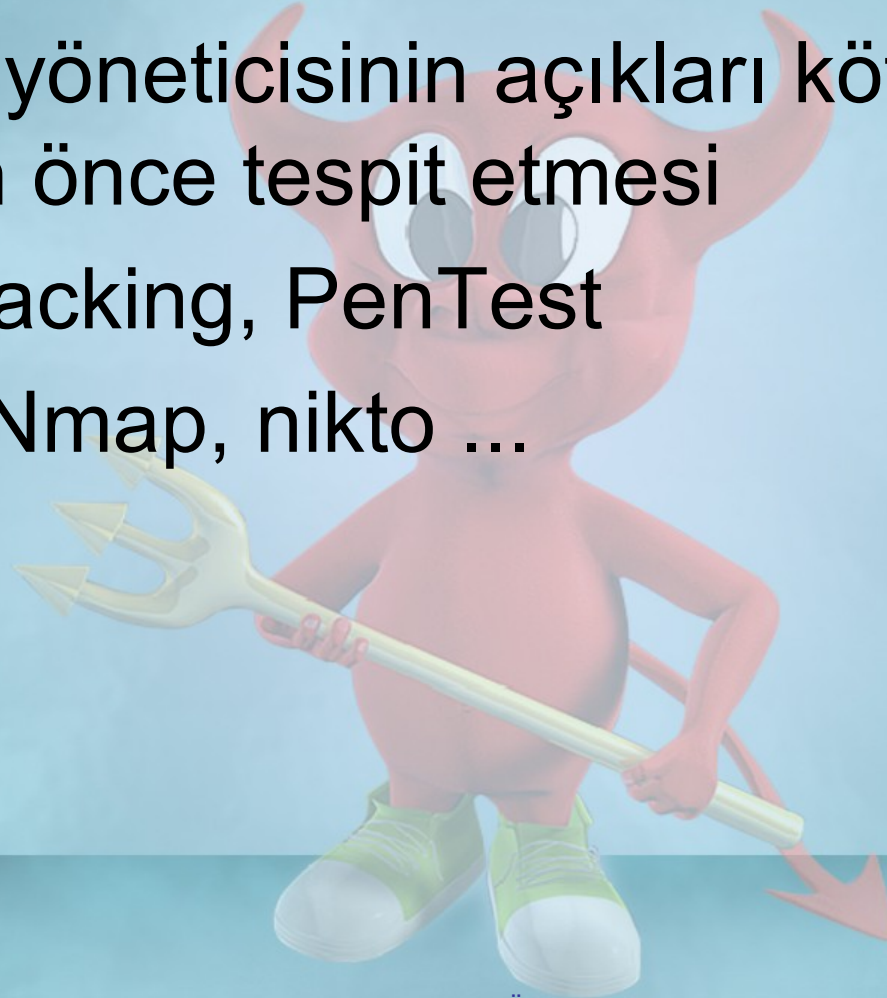
 Abbrechen  OK

OpenVPN GUI



Zayıflık İnceleme

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



Ethical Hacking ve Penetration Testler

- Ethical hacker: Terbiyeli hacker :)
 - Blackhat hacker lar bulmadan olası zayıflıkların tespiti
 - Kendi sistemlerine ya da haberli olarak yapılan testler
 - Kesinlikle izin ve bilgi dahilinde olmalı
 - Yan etkilere karşı ehil kişiler olmalılar
 - Güvenlik araçlarını kullanan, ancak gerektiğinde kendi araçlarını yazabilen
 - Pratik düşünüp sıradışı hareket edebilen
 - Ne yaptığını bilen !

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 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 özelliği
- Birçok ticari kopyası var

Nmap

- Gelişmiş protokol kullanımı ile port tarama sistemi
- TCP bayraklarını kullanabilme
- OS Tespiti
- Hedef sistemdeki servislerin tespiti
- Nmapfe ile grafik arayüzden kullanım imkanı

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, BackTrack, 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

Update

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

[CLEAR SETTINGS](#)

Currently displaying 10 LiveCD/DVDs

Key:

Primary Functions:



Samsun Ondokuz Mayıs Üniversitesi
Nisan 2007

Açık Kod Dünyasında
Ağ ve Sistem Güvenliği

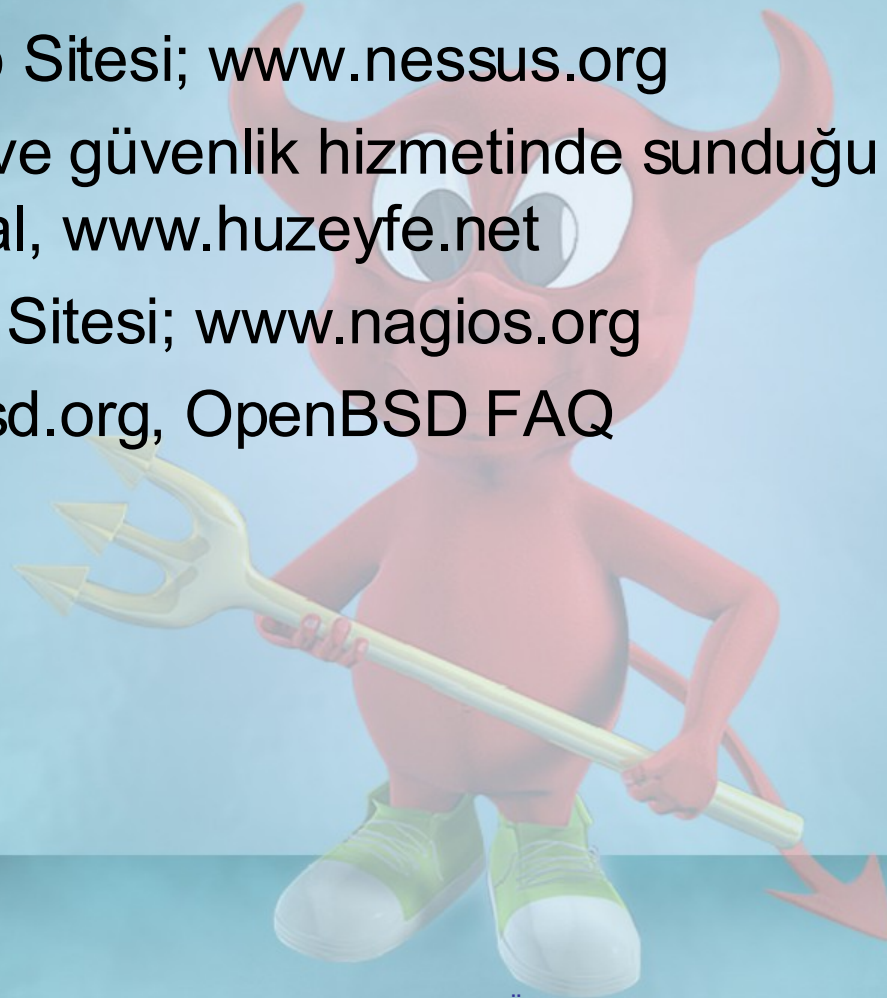
Adresler

- EnderUnix Güvenlik E-Posta Listesi
 - <http://lists.enderunix.org>
- EnderUnix Dökümanları
 - <http://www.enderunix.org/docs>
- Günlüğüm
 - <http://www.enderunix.org/afsin/blog>



Yararlanılan Kaynaklar

- Nessus Web Sitesi; www.nessus.org
- Linux'un ağ ve güvenlik hizmetinde sunduğu olanaklar, Huzeyfe Önal, www.huzeyfe.net
- Nagios Web Sitesi; www.nagios.org
- www.openbsd.org, OpenBSD FAQ



Teşekkürler

Açık Kod Dünyasında Ağ ve Sistem Güvenliği

Afşin Taşkiran

afsin ~ enderunix.org

www.enderunix.org/afsin



Samsun Ondokuz Mayıs Üniversitesi
Nisan 2007

Açık Kod Dünyasında
Ağ ve Sistem Güvenliği