



Linux'da Özgür Güvenlik Yazılımları

Korhan GÜRLER
kg@dikey8.com

- Amaç
- Neden Özgür Yazılımlar?
- Şifreleme
- E-posta güvenliği
- Güvenlik Duvarı
- Saldırı tespiti
- Port tarayıcılar
- Zayıflık tarayıcılar
- Bütünlük denetleyiciler
- Anti-virüs
- Log analizi
- Delil toplama ve inceleme

- Özgür güvenlik yazılım portfoynün genişliğı
- Yazılımların tanıtımı
- Teknolojileri
- Sunum neleri hedeflemiyor:
 - Araçların kullanımını detaylı öğretmek
 - Kurulumlarını göstermek



Neden Özgür Yazılım?

- Açık kod
 - Hataları insanlar tarafından kısa sürede farkedilip giderilebilir
 - Özelleştirilebilir
- Güvenilirlik
 - Her türlü arka kapı veya art niyetli kodlar farkedilebilir
- Güvenlik
- Uzun vadeli kullanım



Şifreleme Kitaplığı - OpenSSL

- Ticari rakipleri ile yarışabilecek kalitede bir Güvenli Soket Katmanı (SSL) protokolüdür
- OpenSSL'in barındırdığı protokoller:
 - Transport Layer Security (TLS v1)
 - Secure Sockets Layer (SSL v2/v3)
- Proje dünya çapındaki gönüllülerin desteği ile yürüyor
- <http://www.openssl.org/>



E-posta Güvenliği - GnuPG

- GnuPG = The GNU Privacy Guard
- PGP yerine kullanılabilen GPL bir araç
- RFC2440 uyumlu (OpenPGP)
- Patentli IDEA algoritmasını kullanmadığı için kısıtlamalara gerek kalmadan kullanılabilir
- PGP'den daha çok fonksiyonelliğe sahip
- PGP 5, 6 ve 7 ile şifrelenmiş dosyaları çözebiliyor
- Desteklediği algoritmalar:
 - El Gamal
 - DSA
 - RSA
 - AES
 - 3DES
 - vb...
- Desteklediği e-posta programları:
 - Pine, mutt
 - Kmail, sylpheed, evolution



E-posta Güvenliği - GnuPG

- Aralarında Türkçe'nin de bulunduğu çoklu dil seçeneği
- Online yardım sistemi
- HKP keyserver'ları için bütünsel destek (wwwkeys.pgp.net)
- En son sürümü 1.0.7
- <http://www.gnupg.org/>

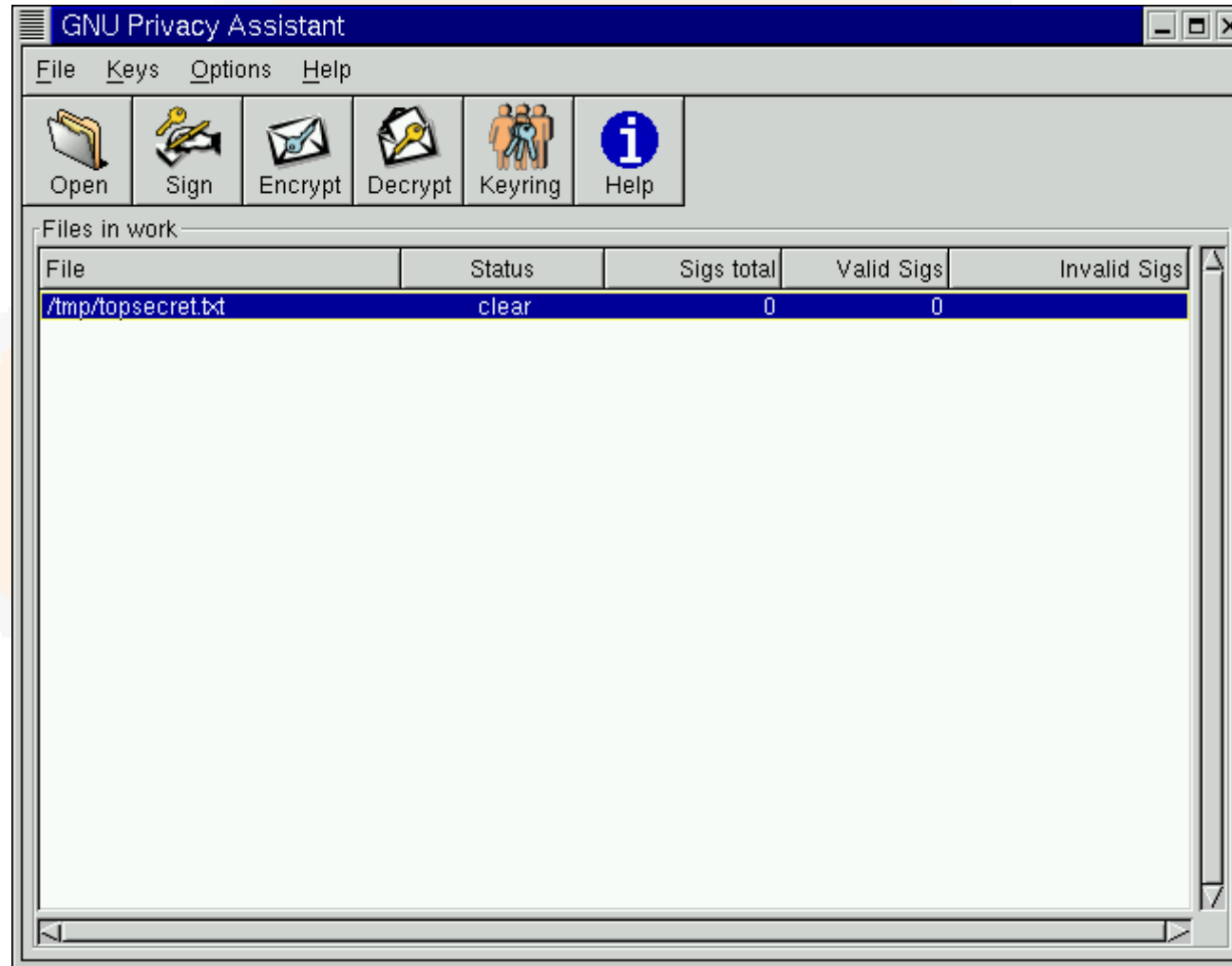
- GPGME = GnuPG Made Easy
- Üçüncü parti programların GnuPG'ye ulaşmasını kolaylaştıran bir kütüphanedir
- Yüksek seviye programlama API'si sunuyor
- Şu anda GnuPG'yi kullanıyor ama sadece bununla sınırlı değil

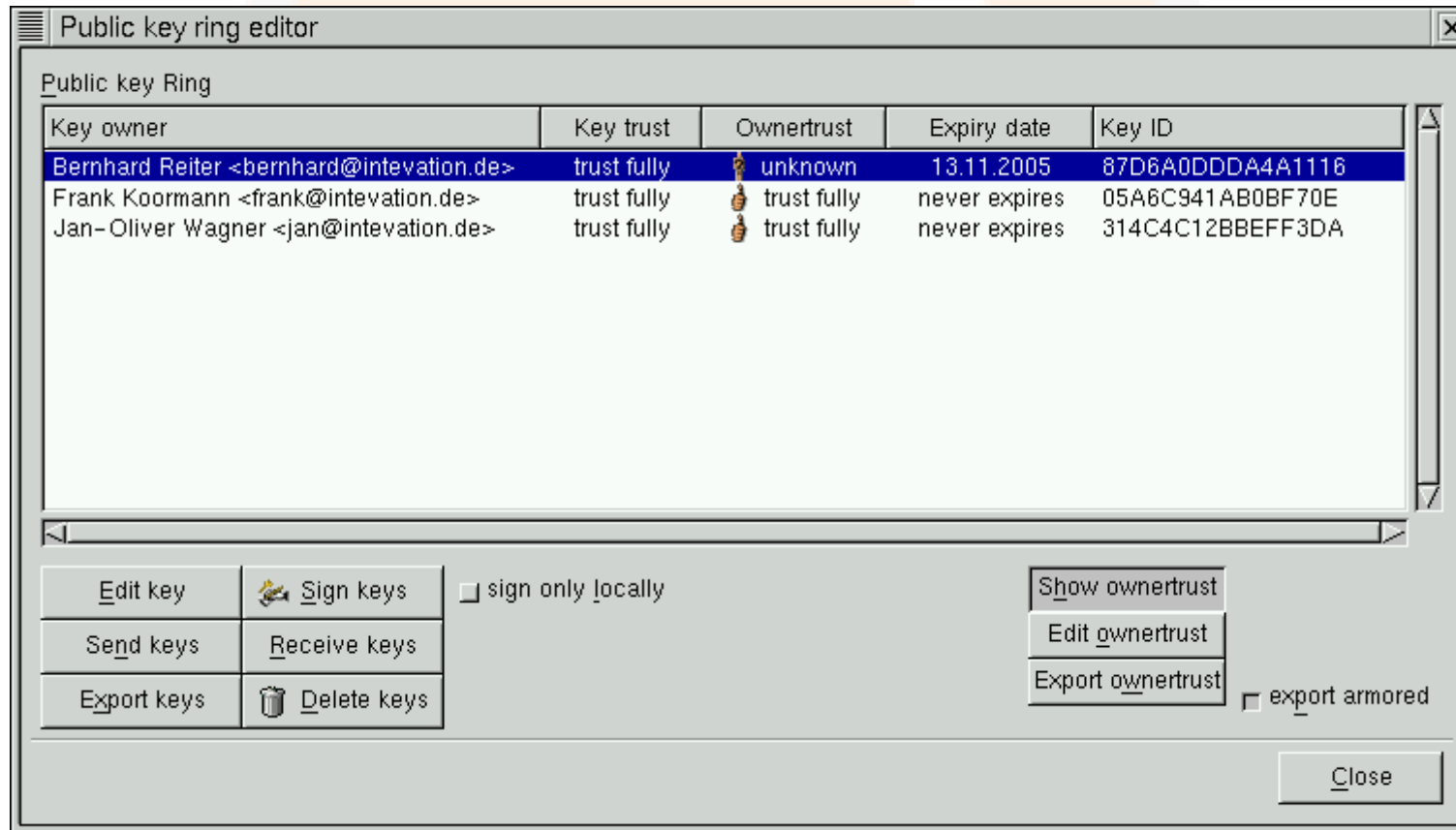
- GPA = The GNU Privacy Assistant
- GnuPG için grafik arabirimidir

DiKEY8



GPA







Güvenlik Duvarı - iptables

- 2.3.x, 2.4.x ve 2.5.x serisi çekirdeklerde çalışıyor
- Dinamik paket filitreleme yapabilir
- Çeşitli IP seçeneklerine göre filitreleme yapabilir
 - Paketlerin bölünmüş olma özelliğine göre
 - Taşıma protokolüne göre (TCP, UDP, ICMP, vs...)
 - TCP bayraklarına ve portuna göre
 - UDP portuna göre
 - ICMP türüne göre
- MAC adresine göre de filitreleme yapabilir
- Statik ve Dinamik NAT yapabilir
- Son versiyonu 1.2.6a
- <http://www.netfilter.org/> ya da <http://www.iptables.org/>

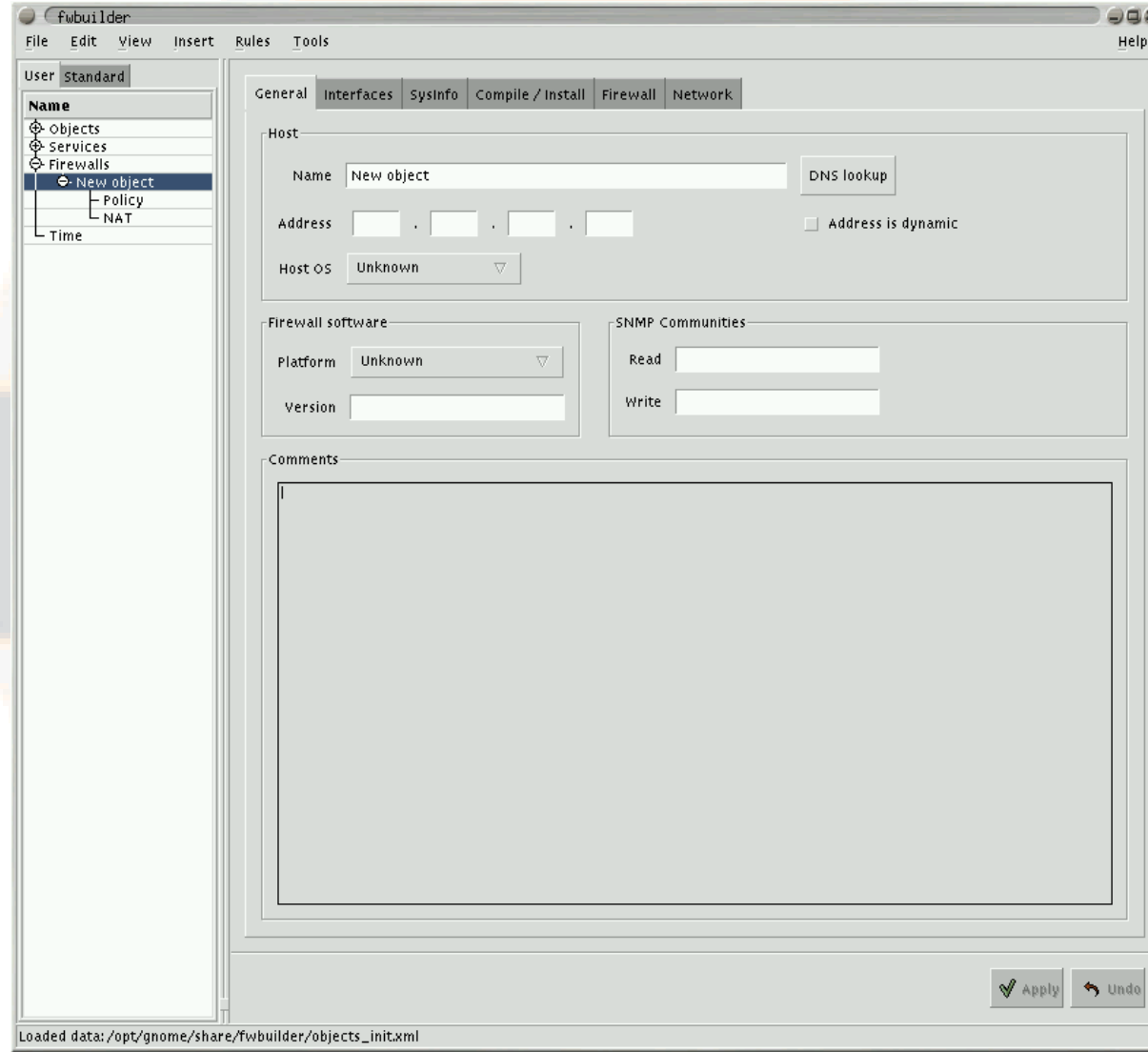


Güvenlik Duvarı - fwbuilder

- İki ayrı paket halinde geliyor
 - libfwbuilder
 - fwbuilder
- Nesne yönelimli grafik arabirim
 - GTK- kullanılarak yazılmış
 - Gnome ve KDE'nin ikisinde birden kullanılabilir
- Sürükle bırak politika oluşturma
- iptables, ipfilter, OpenBSD PF
- 0.9.3 versiyonundan sonra ipchains desteği kaldırıldı
- Özellikler kısmı ve nesne veritabanı XML biçiminde tutuluyor
- Mandrake ve Debian'la beraber geliyor
- Win32 desteği ekleniyor, yapım aşamasında
- Son versiyonu 1.0.2
- <http://www.fwbuilder.org>

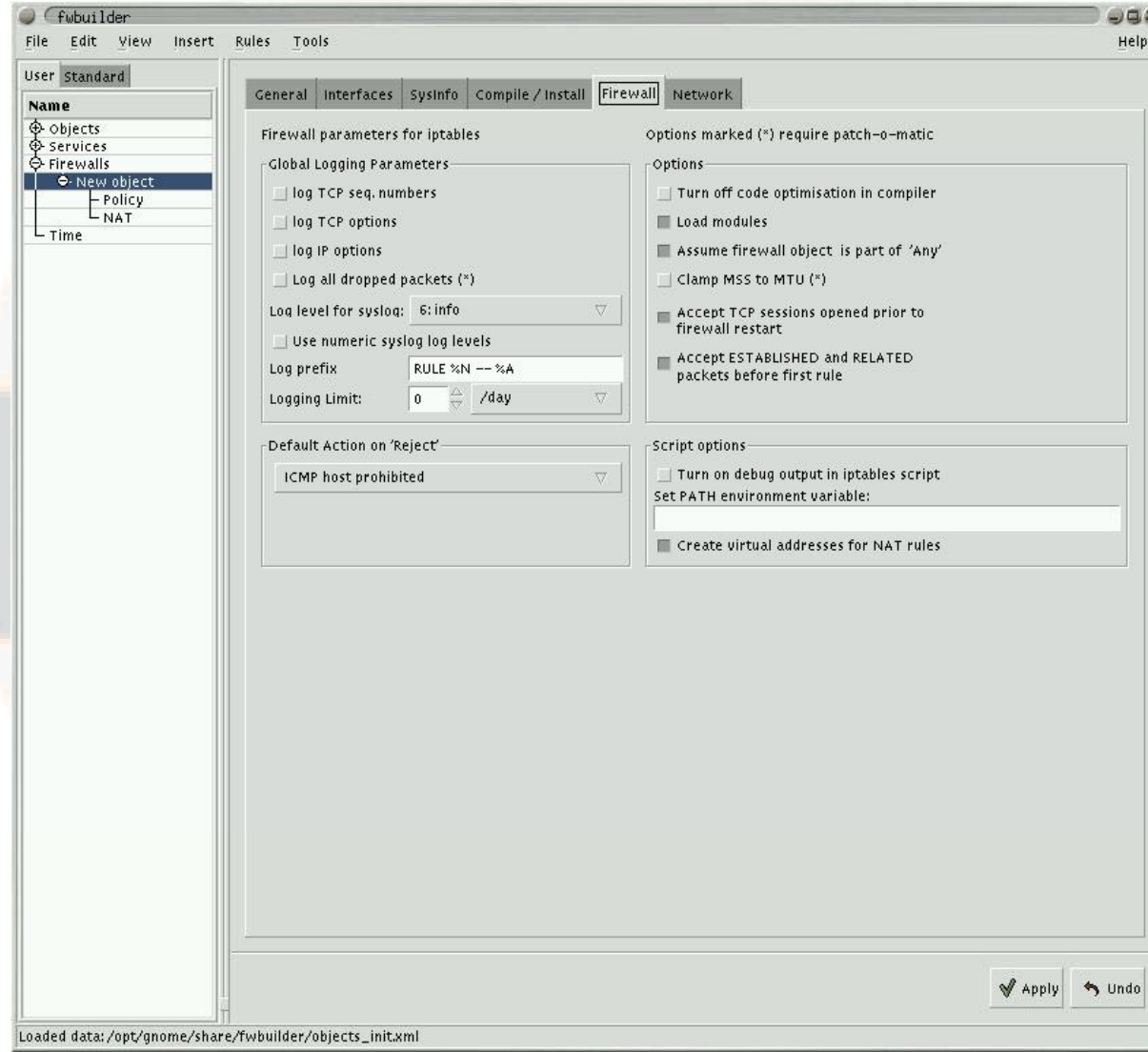


Güvenlik Duvarı - fwbuilder



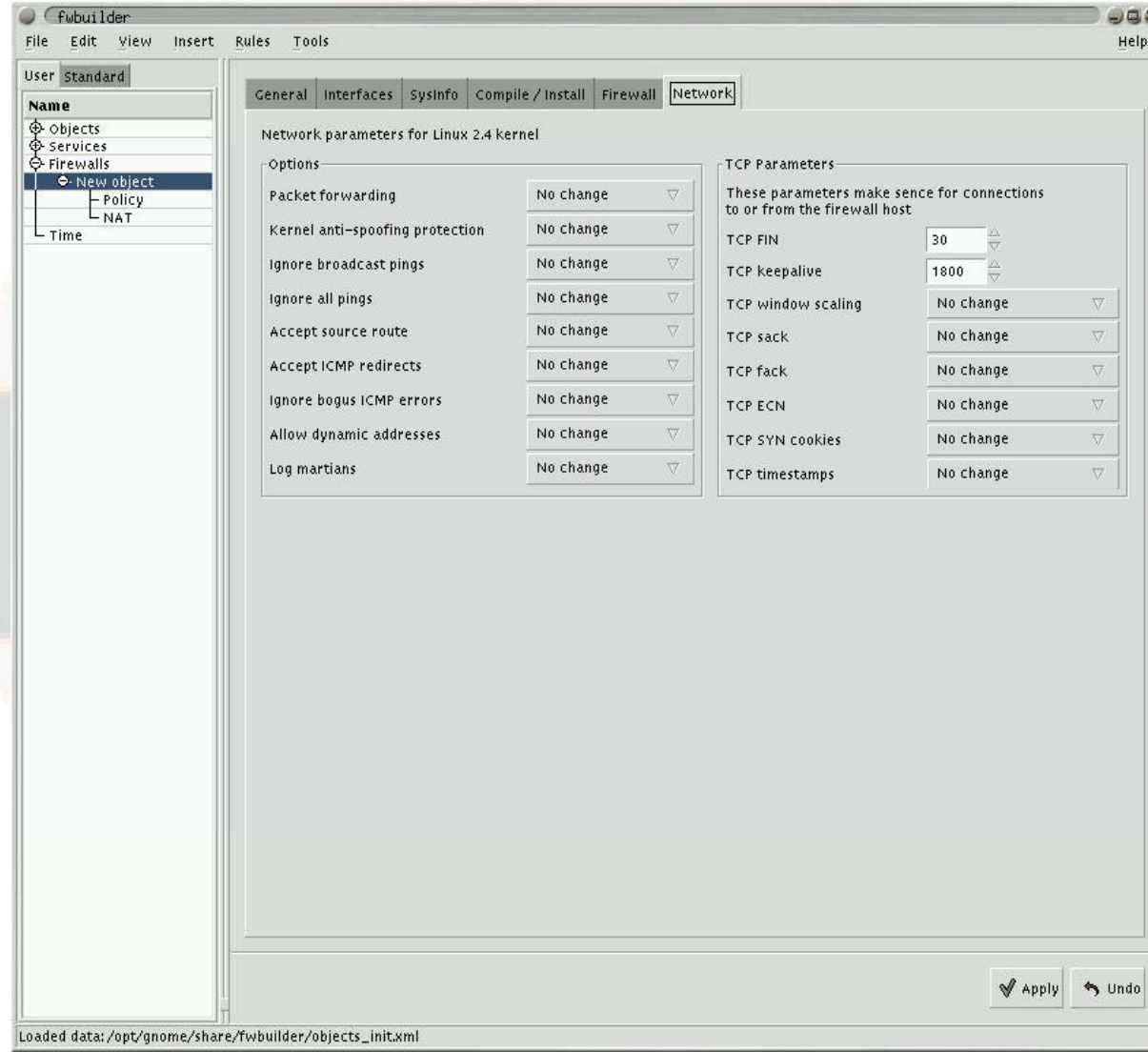


Güvenlik Duvarı - fwbuilder



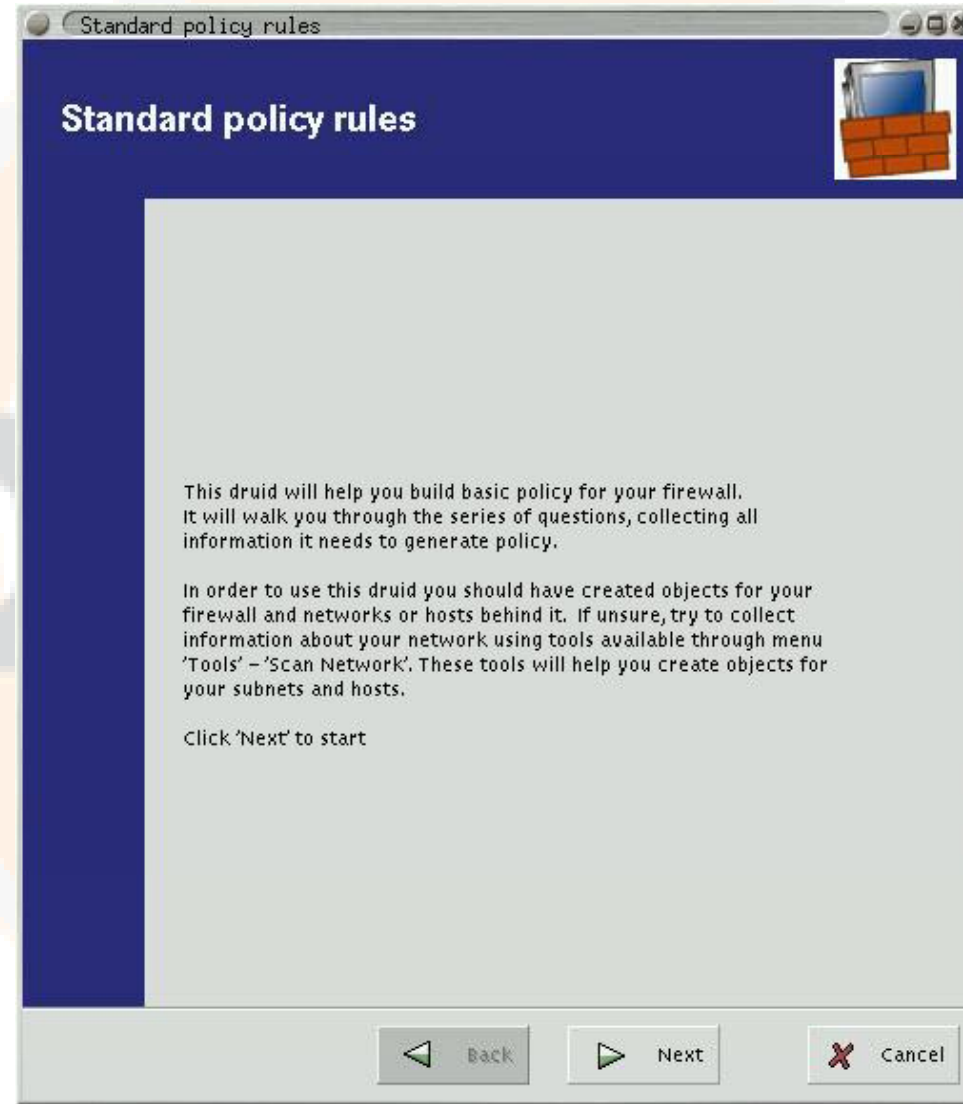


Güvenlik Duvarı - fwbuilder



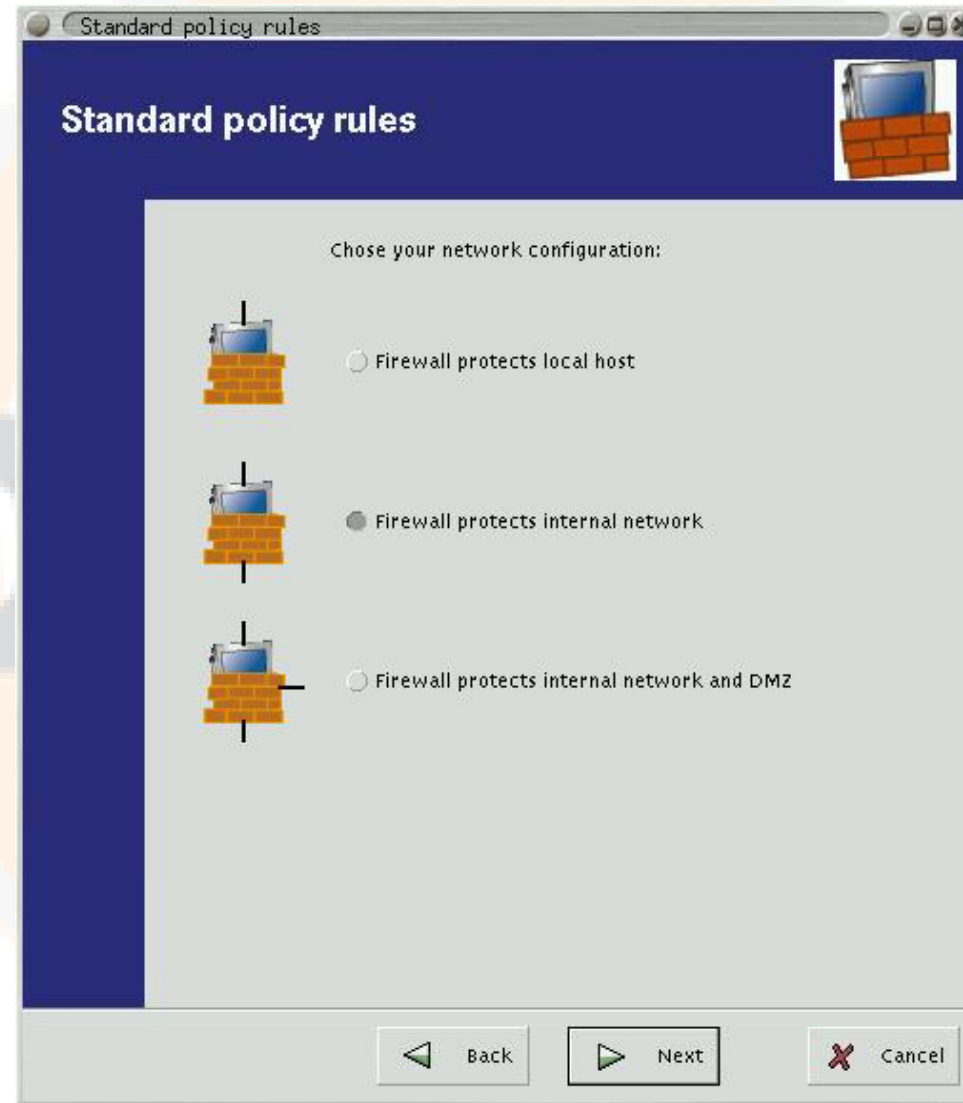


Güvenlik Duvarı - fwbuilder





Güvenlik Duvarı - fwbuilder



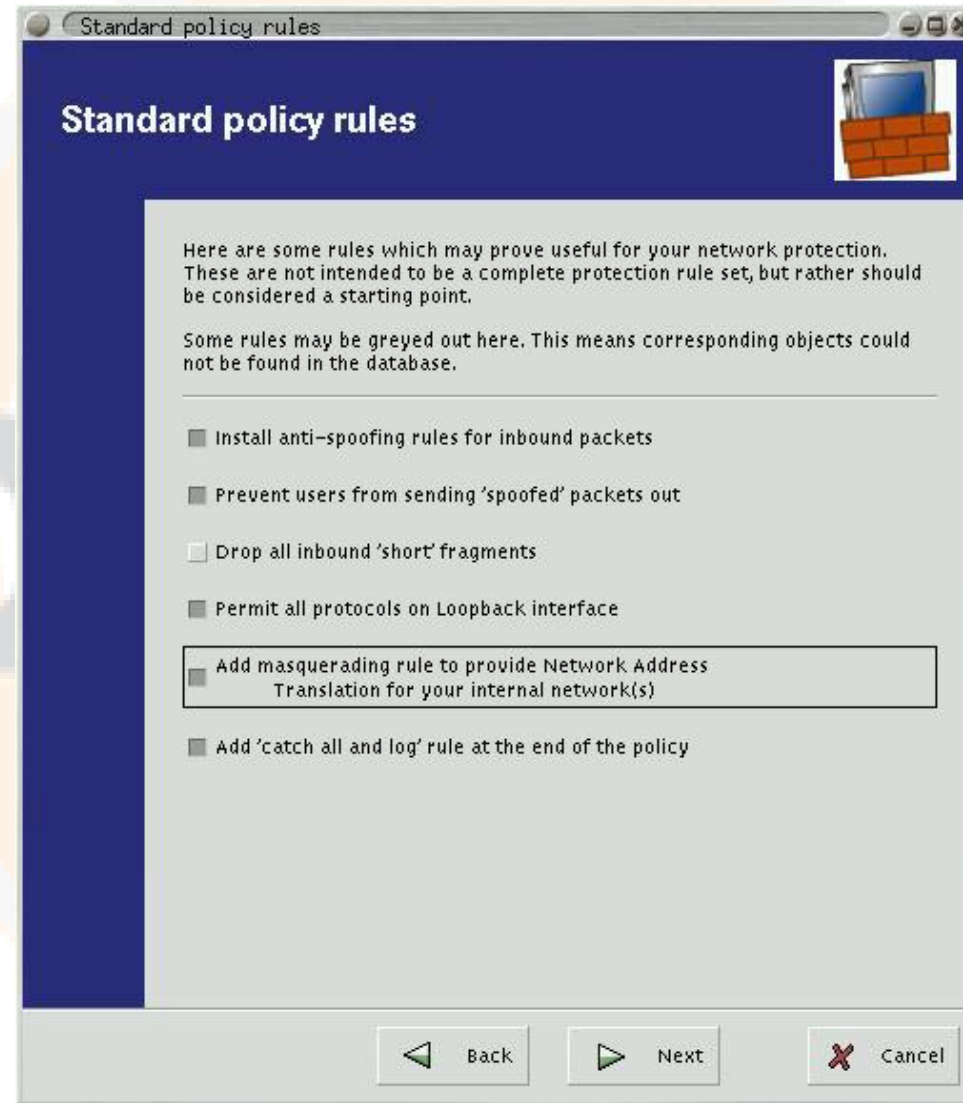


Güvenlik Duvarı - fwbuilder





Güvenlik Duvarı - fwbuilder





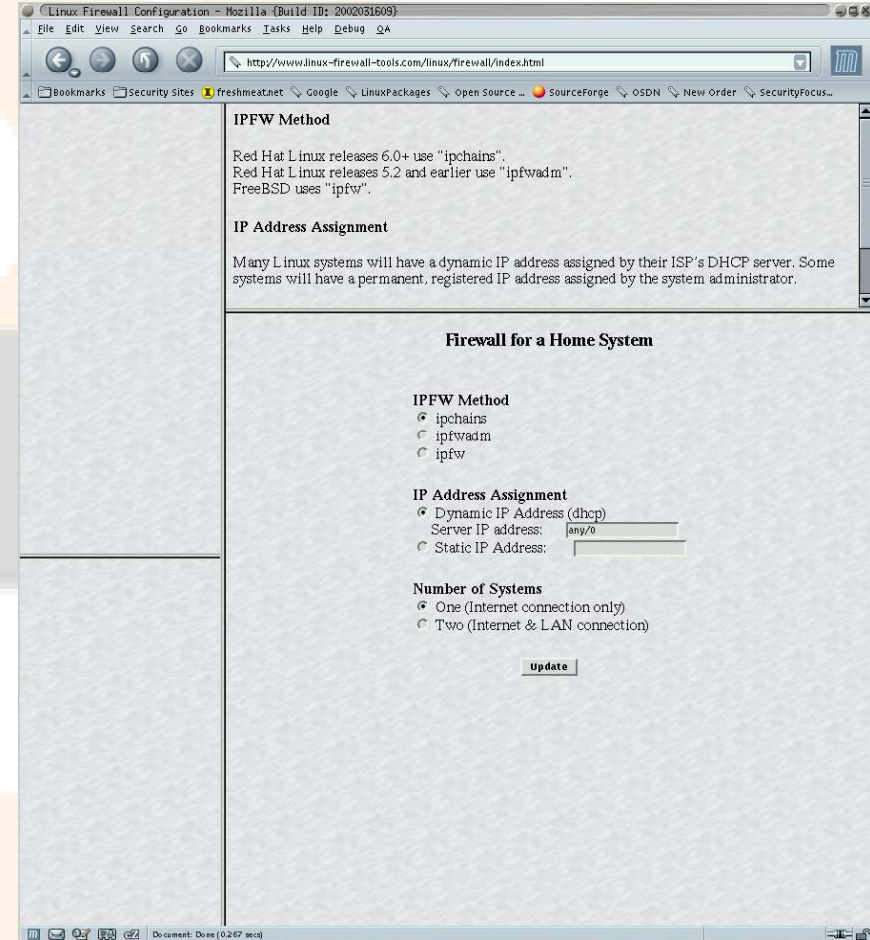
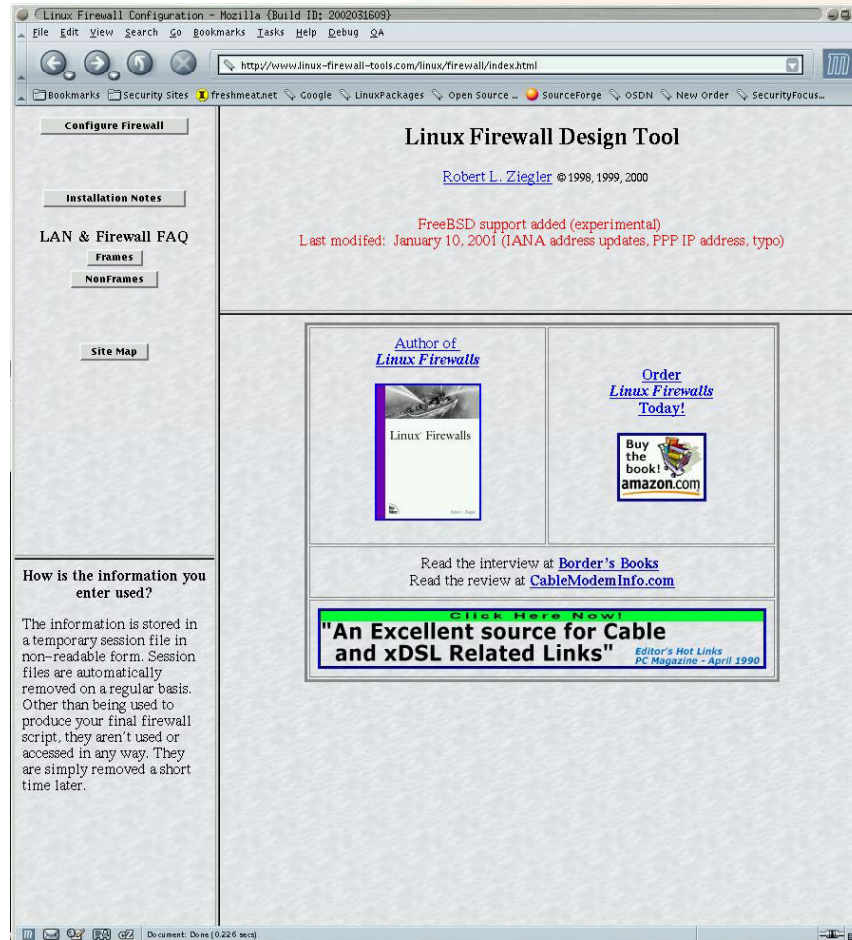
Güvenlik Duvarı – Linux Firewall Design Tool

- Online bir araç
- ipchains, ipfwadm, ipfw destekliyor
- <http://www.linux-firewall-tools.com/linux/firewall/index.html>

DiKEY8

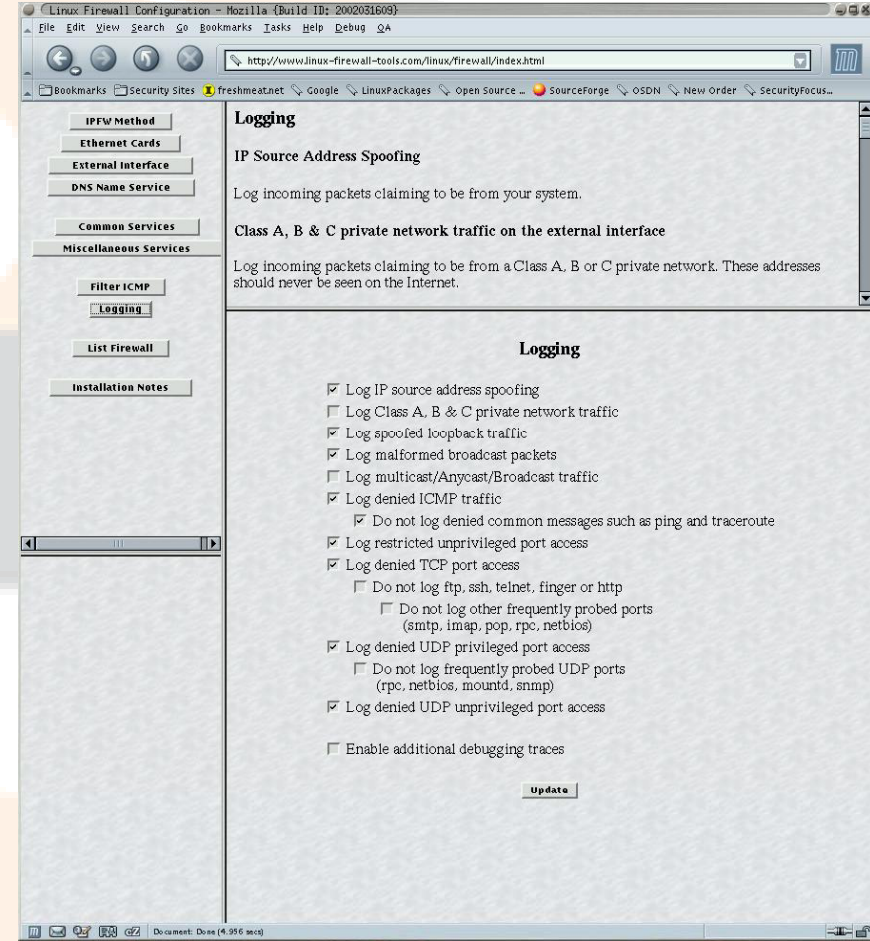
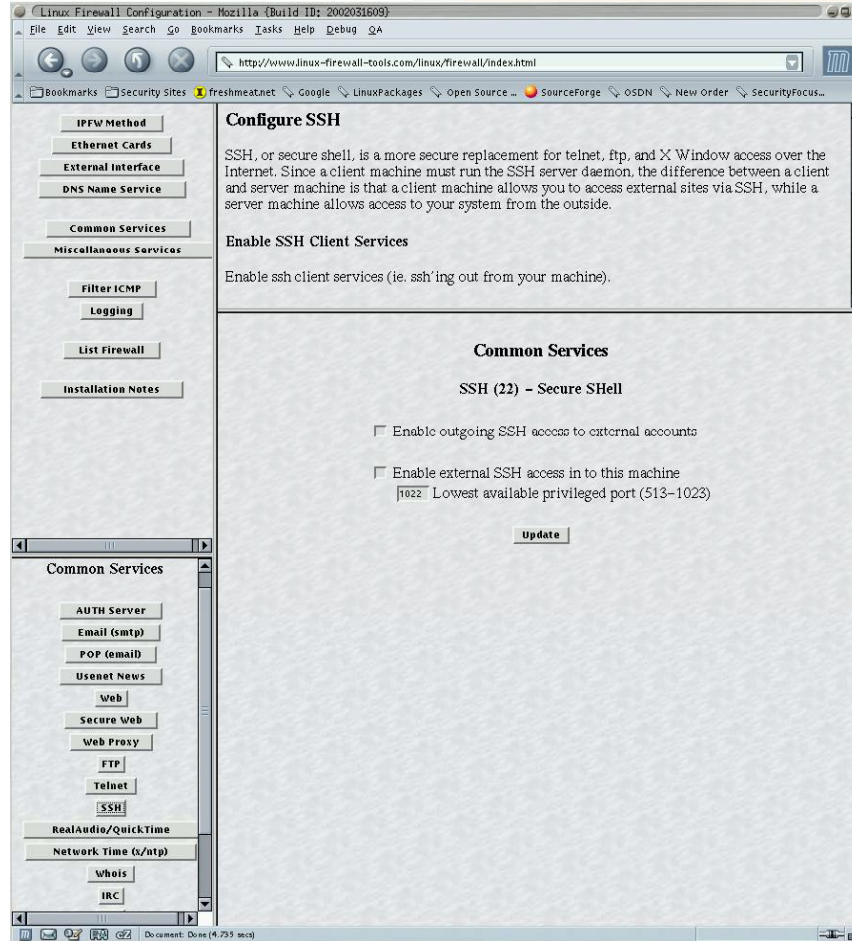


Güvenlik Duvarı – Linux Firewall Design Tool





Güvenlik Duvarı – Linux Firewall Design Tool





Güvenlik Duvarı – Linux Firewall Design Tool

```
rc.firewall - Mozilla {Build ID: 2002031609}
File Edit View Search Go Bookmarks Tasks Help Debug QA
http://www.linux-firewall-tools.com/cgi-bin/firewall.cgi
Bookmarks Security Sites freshmeat.net Google LinuxPackages Open Source ... SourceForge OSDN New Order SecurityFocus...

#!/bin/sh

# Script generated Fri May 10 17:28:40 2002

#
# Copyright (C) 1997, 1998, 1999, 2000 Robert L. Ziegler
#
# Permission to use, copy, modify, and distribute this software and its
# documentation for educational, research, private and non-profit purposes,
# without fee, and without a written agreement is hereby granted.
# This software is provided as an example and basis for individual firewall
# development. This software is provided without warranty.
#
# Any material furnished by Robert L. Ziegler is furnished on an
# "as is" basis. He makes no warranties of any kind, either expressed
# or implied as to any matter including, but not limited to, warranty
# of fitness for a particular purpose, exclusivity or results obtained
# from use of the material.
#
# /etc/rc.d/rc.firewall
# Invoked from /etc/sysconfig/network-scripts/pump-done, or
# from /etc/dhcpd/dhcpd-eth0.exe, or
# from /etc/sysconfig/network-scripts/ifdhcpd-done.

echo "Starting firewalling..."

#
# Some definitions for easy maintenance.
# EDIT THESE TO SUIT YOUR SYSTEM AND ISP.

EXTERNAL_INTERFACE="eth0"          # Internet connected interface
LOOPBACK_INTERFACE="lo"           # or your local naming convention

IPADDR="my ip address"            # your IP address

ANYWHERE="any/0"                  # match any IP address

DHCP_SERVER="any/0"
NAMESERVER_1="any/0"              # everyone must have at least one

LOOPBACK="127.0.0.0/8"            # reserved loopback address range
CLASS_A="10.0.0.0/8"              # class A private networks
CLASS_B="172.16.0.0/12"           # class B private networks
CLASS_C="192.168.0.0/16"          # class C private networks
CLASS_D_MULTICAST="224.0.0.0/4"   # class D multicast addresses
CLASS_E_RESERVED_NET="240.0.0.0/5" # class E reserved addresses
BROADCAST_SRC="0.0.0.0"           # broadcast source address
BROADCAST_DEST="255.255.255.255"  # broadcast destination address
PRIVPORTS="0:1023"                # well known, privileged port range
UNPRIVPORTS="1024:65535"          # unprivileged port range

#
# nameservers are originally from /etc/dhcpd/resolv.conf.
# The example ifdhcpd-done script updates these automatically and
# appends them to /etc/dhcpd/hostinfo-EXTERNAL_INTERFACE or
# /etc/dhcpd/dhcpd-EXTERNAL_INTERFACE.info.

# The IP address, $IPADDR, is defined by dhcpd

if [ -f /etc/dhcpd/hostinfo-EXTERNAL_INTERFACE ]; then
    . /etc/dhcpd/hostinfo-EXTERNAL_INTERFACE
elif [ -f /etc/dhcpd/dhcpd-EXTERNAL_INTERFACE.info ]; then
```




Güvenlik Duvarı

- Diğer yardımcı araçlar:
 - knetfilter - <http://expansa.sns.it:8080/knetfilter>
 - GIPTables Firewall - <http://www.giptables.org>
 - Juniper Firewall Toolkit - <http://www.obtuse.com/juniper/>



Saldırı Tespiti - snort

- Ağ Temelli / Saldırı İmzası Arama mimarisi ile çalışır
- Çok sayıda sistem tek bir snort ile izlenebilir
- Birden fazla snort tek bir merkezden yönetilebilir
- Merkezi raporlama oluşturulabilir
- Saldırı önem dereceleri ve tepkiler belirtilebilir
- Modüler bir yapıya sahip
- Kuralları kolayca yazılıp eklenebiliyor
- Web'den snort veritabanı 30 dakikada bir güncellenebilir
- Üretilen alarmlar çeşitli şekillerde tutulabilir (XML, mySQL vb...)
- Ek modüller ile güvenlik duvarına talimat vererek uygun kuralların eklenmesini sağlayabilir
- Son versiyonu 1.8.6
- <http://www.snort.org/>



Saldırı Tespiti - firestorm

- Küçük ve esnek
- Hızlı
- Linux'e özel paket yakalama modülü
- Kolay konfigürasyon (firestorm.conf dosyasında vim benzeri syntax)
- Snort kuralları desteği
- Veritabanı en az snort kadar geniş
- <http://www.scaramanga.co.uk/firestorm/>



Port Tarayıcı

- nmap = Network Mapper
- Büyük ağları çabuk bir şekilde tarayabilmek için dizayn edilmiş
- GTK grafik arabirimi var
- Kısaca neler yapabiliyor?
 - Ağ'da hangi makineler var
 - Ne tür servisler sunuyorlar
 - Üzerlerinde hangi işletim sistemi çalışıyor
 - Ne tür paket filtreleme/güvenlik duvarı kullanılıyor
 - Tarama sonuçlarını XML olarak kaydedebilir
 - vs...
- Bir çok port tarama mekanizmasını kullanabilir:
 - Vanilla TCP connect() tarama
 - TCP SYN (yarı açık) tarama
 - TCP FIN tarama
 - UDP rcvfrom() tarama
 - ICMP tarama
 - vs...
- En son versiyonu 2.54BETA34
- <http://www.insecure.org/nmap/>



Port Tarayıcı (devam)

```
Nmap V. 2.54BETA34 Usage: nmap [Scan Type(s)] [Options] <host or net list>
Some Common Scan Types ('*' options require root privileges)
  -sT TCP connect() port scan (default)
* -sS TCP SYN stealth port scan (best all-around TCP scan)
* -sU UDP port scan
  -sP ping scan (Find any reachable machines)
* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)
  -sR/-I RPC/Identd scan (use with other scan types)
Some Common Options (none are required, most can be combined):
* -O Use TCP/IP fingerprinting to guess remote operating system
  -p <range> ports to scan. Example range: '1-1024,1080,6666,31337'
  -F Only scans ports listed in nmap-services
  -v Verbose. Its use is recommended. Use twice for greater effect.
  -P0 Don't ping hosts (needed to scan www.microsoft.com and others)
* -Ddecoy_host1,decoy2[,...] Hide scan using many decoys
  -T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy
  -n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]
  -oN/-oX/-oG <logfile> Output normal/XML/grepable scan logs to <logfile>
  -iL <inputfile> Get targets from file; Use '-' for stdin
* -S <your_IP>/-e <devicename> Specify source address or network interface
  --interactive Go into interactive mode (then press h for help)
Example: nmap -v -sS -O www.my.com 192.168.0.0/16 '192.88-90.*.*'
SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES
root@darkstar:~#
```



Port Tarayıcı (devam)



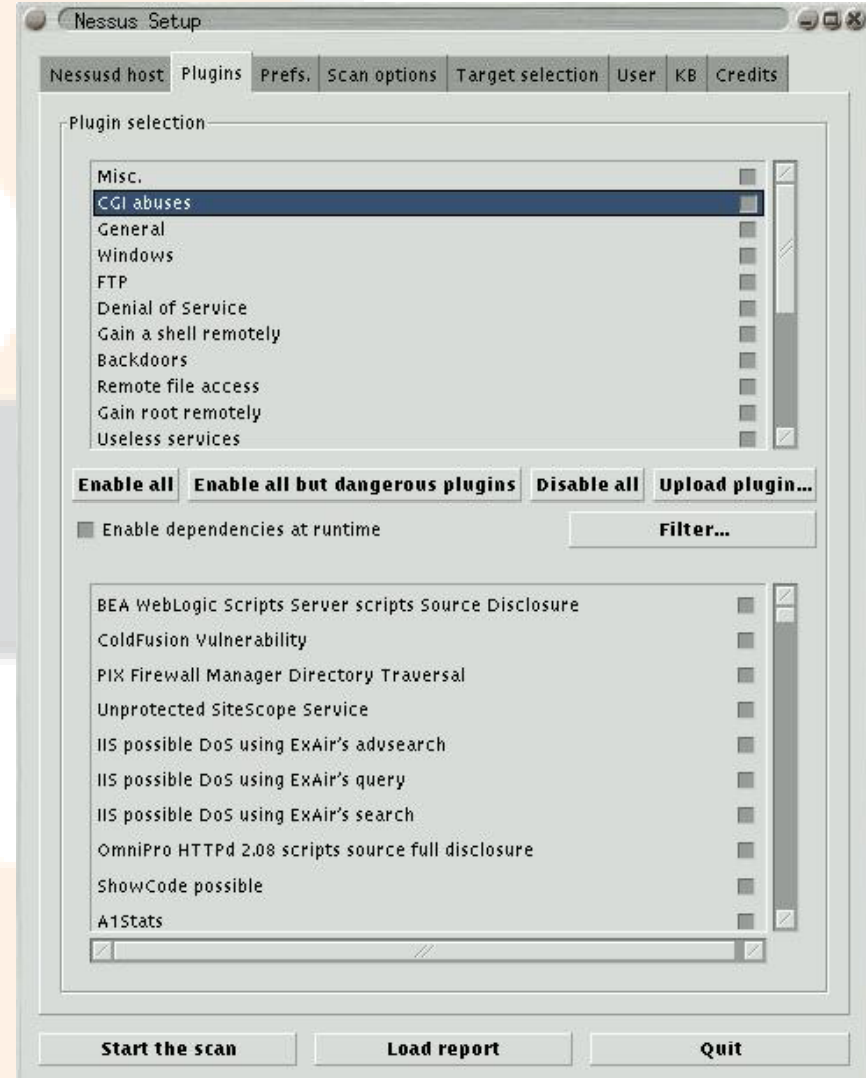


Zayıflık Tarayıcı - nessus

- İstemci/sunucu teknolojisi ile çalışır
- İstemci ve sunucu arasındaki trafiği SSL ile şifreleyebilir
- XML, HTML, NSR gibi formatlarda rapor sunabilir
- Raporlarında zayıflığın nasıl giderilebileceği hakkında bilgi bulundurur
- Raporlarında zayıflık hakkında referanslar verir
- Taramalar arasında karşılaştırma yapabilir
- NASL (Nessus Attack Scripting Language) dili ile özel saldırılar düzenlenebilir
- Nmap ve queso gibi araçlarla kullanabilmek için eklentileri mevcuttur
- En son sürümü 1.2.0
- <http://www.nessus.org/>



Zayıflık Tarayıcı – nessus





Zayıflık Tarayıcı – nessus

Nessus Setup

Nessus host Plugins Prefs Scan options Target selection User KB Credits

Plugins preferences

Ping the remote host:

TCP ping destination port: 80

☐ Do a TCP ping

☐ Do an ICMP ping

Number of retries (ICMP): 10

☐ Make the dead hosts appear in the report

FTP bounce scan:

FTP server to use: localhost

Nmap:

TCP scanning technique:

☐ connect()

☐ SYN scan

☐ FIN scan

☒ Xmas Tree scan

☐ Null scan

☐ UDP port scan

☐ RPC port scan

☐ Ping the remote host

☐ Identify the remote OS

☐ Use hidden option to identify the remote OS

☐ Fragment IP packets (bypasses firewalls)

☐ Get ident info

Port range

☒ User specified range

☐ Default range (nmap-services + privileged ports)

☐ Fast scan (nmap-services)

☐ Do not scan the ports in which ports are closed

Start the scan Load report Quit

Nessus Setup

Nessus host Plugins Prefs Scan options Target selection User KB Credits

Scan options

Port range: 1-35000

☐ Consider unscanned ports as closed

Number of hosts to test at the same time: 20

Number of checks to perform at the same time: 10

Path to the CGIs: /cgi-bin/scripts

☐ Do a reverse lookup on the IP before testing it

☐ Optimize the test

☐ Safe checks

☐ Designate hosts by their MAC address

☐ Detached scan

Send results to this email address:

☐ Continuous scan

Delay between two scans:

Port scanner:

scan for LaBrea tar-pitted hosts

Ping the remote host

FTP bounce scan

Nmap tcp connect() scan

Nmap

Start the scan Load report Quit



Zayıflık Tarayıcı - SARA

- SARA = Security Auditor's Research Assistant
- SANS/ISTS sertifikalı
- Üçüncü parti araçlar için eklentisi var
- CVE standartları desteği var
- SATAN (Security Administrator's Tool for Analyzing Networks) modeli üzerine geliştirilmiş
- İşletim sistemi tespiti için nmap ile entegre çalışabiliyor
- SMB güvenlik analizi için SAMBA ile çalışabilir
- Son versiyonu 3.5.6
- <http://www-arc.com/sara/sara.html>



Zayıflık Tarayıcı - SAINT

- SAINT = The Security Administrator's Integrated Network Tool
- SATAN'ın güncellenmiş ve geliştirilmiş hali
- Kullanımı kolay grafik arabirimi
- Son versiyonu 3.4.10
- <http://www.wwdsi.com/saint/>



Bütünlük Denetleyici - samhain

- Linux ve UNIX için bir bütünlük denetleyici ve saldırı tespit sistemi
- Komple bir bütünlük denetleyici
 - Dosyaların değişimlerini kontrol edebilmek için kriptografik imzalarını kullanır
 - Yüklenebilir çekirdek modülü rootkitleri bulabilir (sadece Linux'da)
- Veritabanı ve konfigürasyon dosyaları imzalanabilir
- Ürettiği log'lar ve gönderdiği e-postalar imzalanabilir
- Merkezi bir sistemden kontrol edilebilir
- Çok iyi dökümente edilmiş
- Desteklediği platformlar:
 - Linux, FreeBSD, AIX 4.x, HP-UX 10.20, Unixware 7.1.0
 - OpenBSD ve HP-UX 11 sistemlerinde de yüklenebilir
 - Mac OS X de derlenebiliyor ama samhain ekibi tarafından test edilmemiş
 - Windows 2000'de Cygwin ile derlenip çalıştırılabilir ama problemli
- <http://la-samhna.de/samhain/>



Anti-virüs - AMAVIS

- E-posta geçitidir
- Perl ile yazılmış betikler topluluğudur
- Sendmail, Qmail, Postfix ve Exim ile çalışır
- E-postaların eklerini inceleyerek geçici bir dizine kaydedip anti-virüs uygulamasına ulaştırmaktan sorumludur
- Çeşitli sıkıştırma formatlarını desteklemektedir
- <http://www.amavis.org/>
- <http://www.openantivirus.org/>



syslog Analizi - swatch

- swatch = The Simple WATCHer
- Kaliforniya Üniversitesinde Todd Atkins tarafından geliştiriliyor
- Perl betiklerinden oluşuyor
- Bütün ayarları tek bir konfigürasyon dosyasından yapılabiliyor
- Belirlenen şartlar gerçekleştiğinde istenilen kişiye e-posta gönderebiliyor



Log Analizi - logcheck

- Gauntlet Firewall tarafından kullanılan frequentcheck.sh'in bir uyarlaması
- Bazı kısımları tamamı ile yeniden yazılmış
- Doğal olmayan bazı eylemleri bildirebiliyor (bunlar için özel olarak bir tetikleme yazılmamış olsa bile)
- İki çalıştırılabilir dosya halinde geliyor
 - logtail
 - logcheck.sh
- logtail
 - En son ne kadar log dosyasının izlendiğini tutuyor
 - Performans göz önünde bulundurulduğundan C ile yazılmış
- logcheck.sh
 - Bütün süreçleri ve log dosyalarının içeriklerini kontrol ediyor
 - cron'dan çağırılmak üzere düşünülmüş
 - En azından saat başı çalıştırılmalı

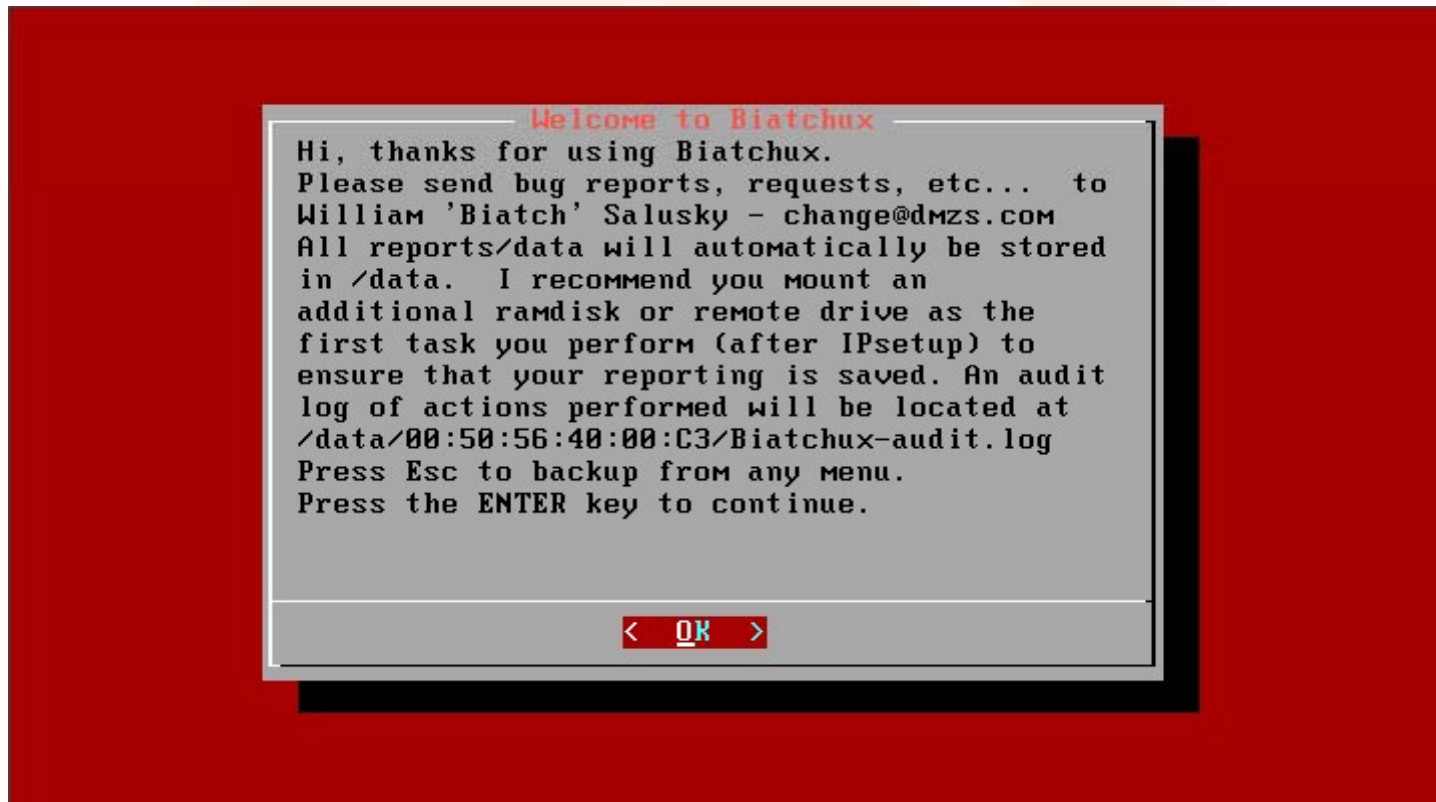


Delil Toplama ve İnceleme - biatchux

- Taşınabilir ve bootable bir CDRom dağıtımı
- Amacı:
 - Delil toplama ve inceleme
 - Olaylara müdahale
 - Veri kurtarma
 - Virüs tarama
 - Zayıflık bulma
- İçindeki araçlar statik derlendiğinden desteklediği platformlarda direkt CD'den de çalıştırılabilir
- Desteklediği platformlar:
 - Win32
 - Sparc Solaris
 - x86 linux
- Kapsadığı araçlardan bazıları:
 - burneye: ELF şifreleme programı
 - fdisk
 - gpg
 - wipe: Güvenli dosya silme programı
 - tcpdump
 - vb...
- Son versiyonu v.0.1.0.6b
- <http://biatchux.dmzs.com/>

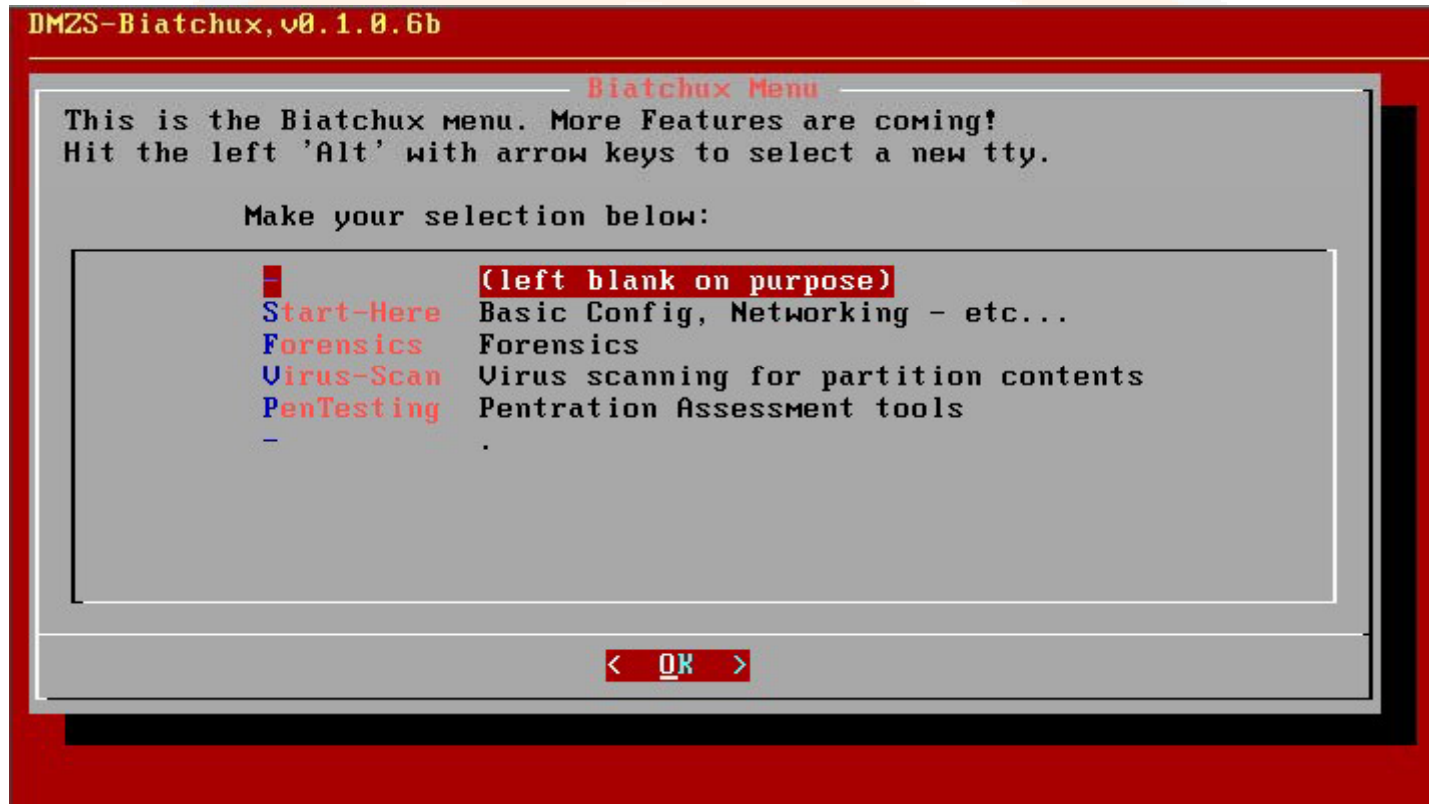


Delil Toplama ve İnceleme - biatchux



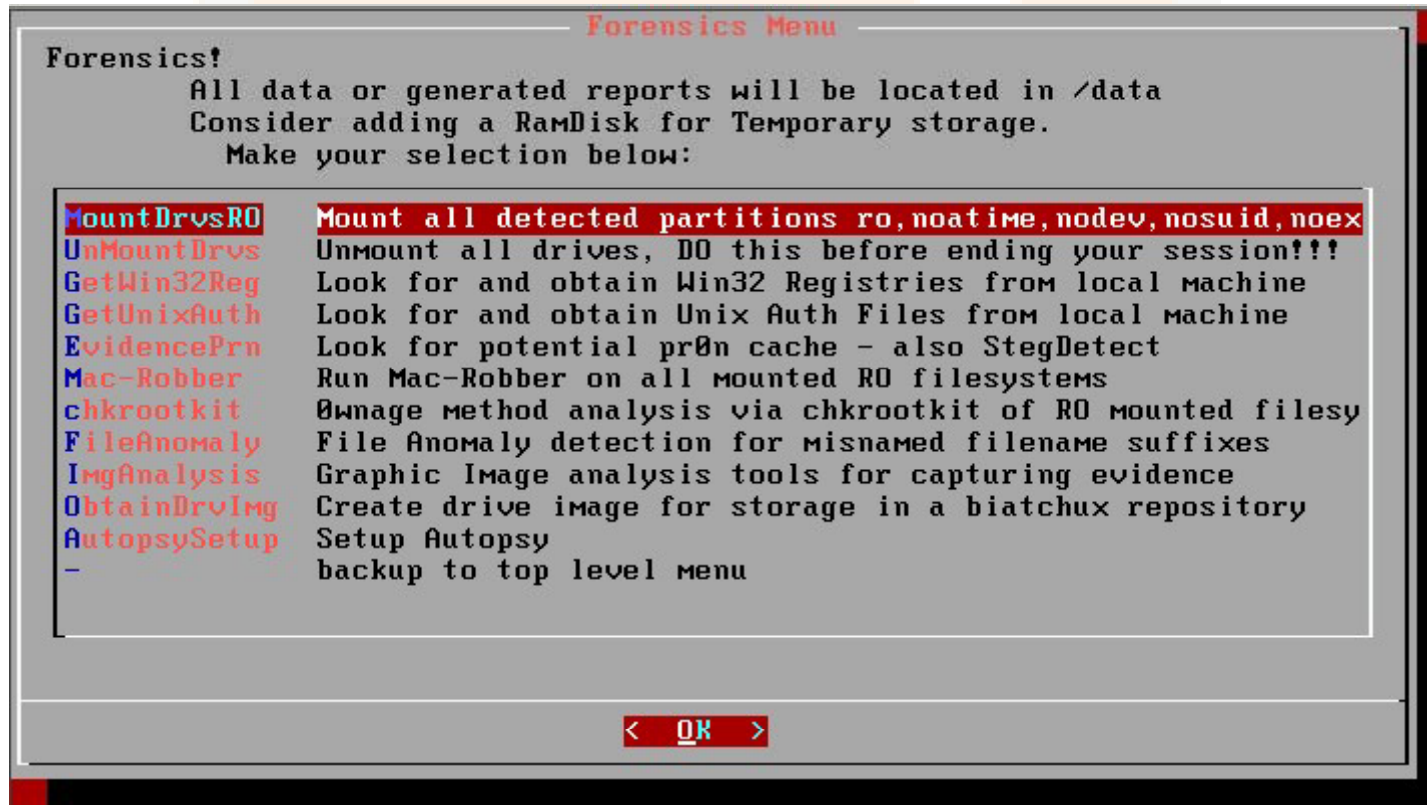


Delil Toplama ve İnceleme - biatchux





Delil Toplama ve İnceleme - biatchux





Delil Toplama ve İnceleme – TCT

- TCT = The Coroner's Toolkit
 - Dan Farmer ve Wietse Venema tarafından geliştirilen çeşitli programlar
 - Sistem kırıldıktan sonra incelemeye yarıyor
 - Test edilen sistemler:
 - Solaris 2.4, 2.5.1, 2.6, 7.0, 8
 - FreeBSD 2.2.1, 3.4, 4.0
 - RedHat 5.2, 6.1
 - BSD/OS 2.1, 4.1
 - OpenBSD 2.5
 - SunOS 4.1.3_U1, 4.1.4
 - <http://www.porcupine.org/forensics/tct.html>
-



Delil Toplama ve İnceleme - dd

- fileutils ile beraber geliyor
- Bir diskin bire bir imajını almak için kullanılıyor
- Basit kullanımı
 - `dd if=/dev/hdb1 of=hdb1.dd`

DiKEY8



Teşekkürler

DiKEY8
TEŞEKKÜRLER