Linux'da Özgür Güvenlik Yazılımları

Korhan GÜRLER
kg@dikey8.com

Konular

- 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

Amaç

- Özgür güvenlik yazılım portfoyünün genişliği
- 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 cok 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 bütünleşik destek (wwwkeys.pgp.net)
- En son sürümü 1.0.7
- http://www.gnupg.org/

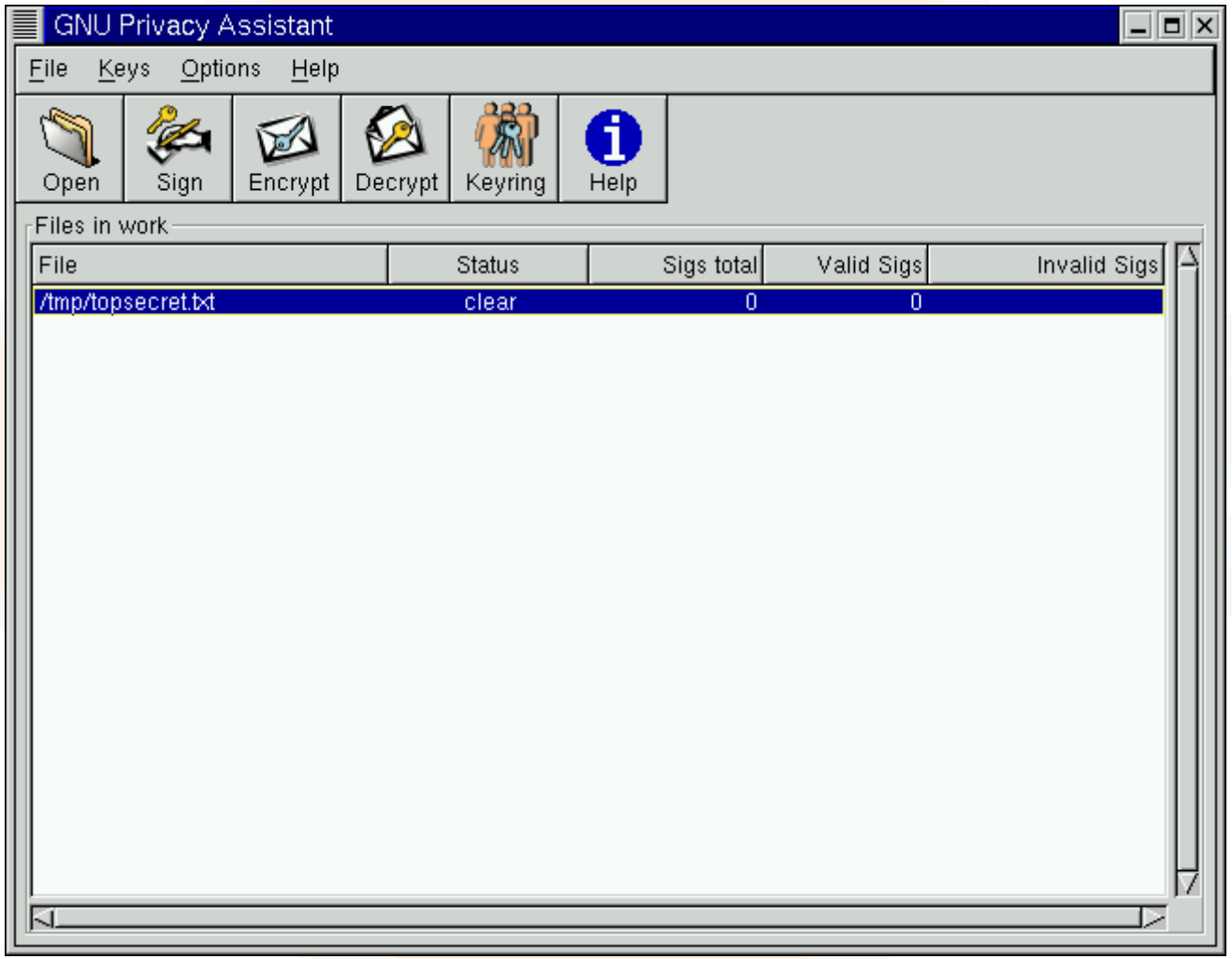
GPGME

- 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

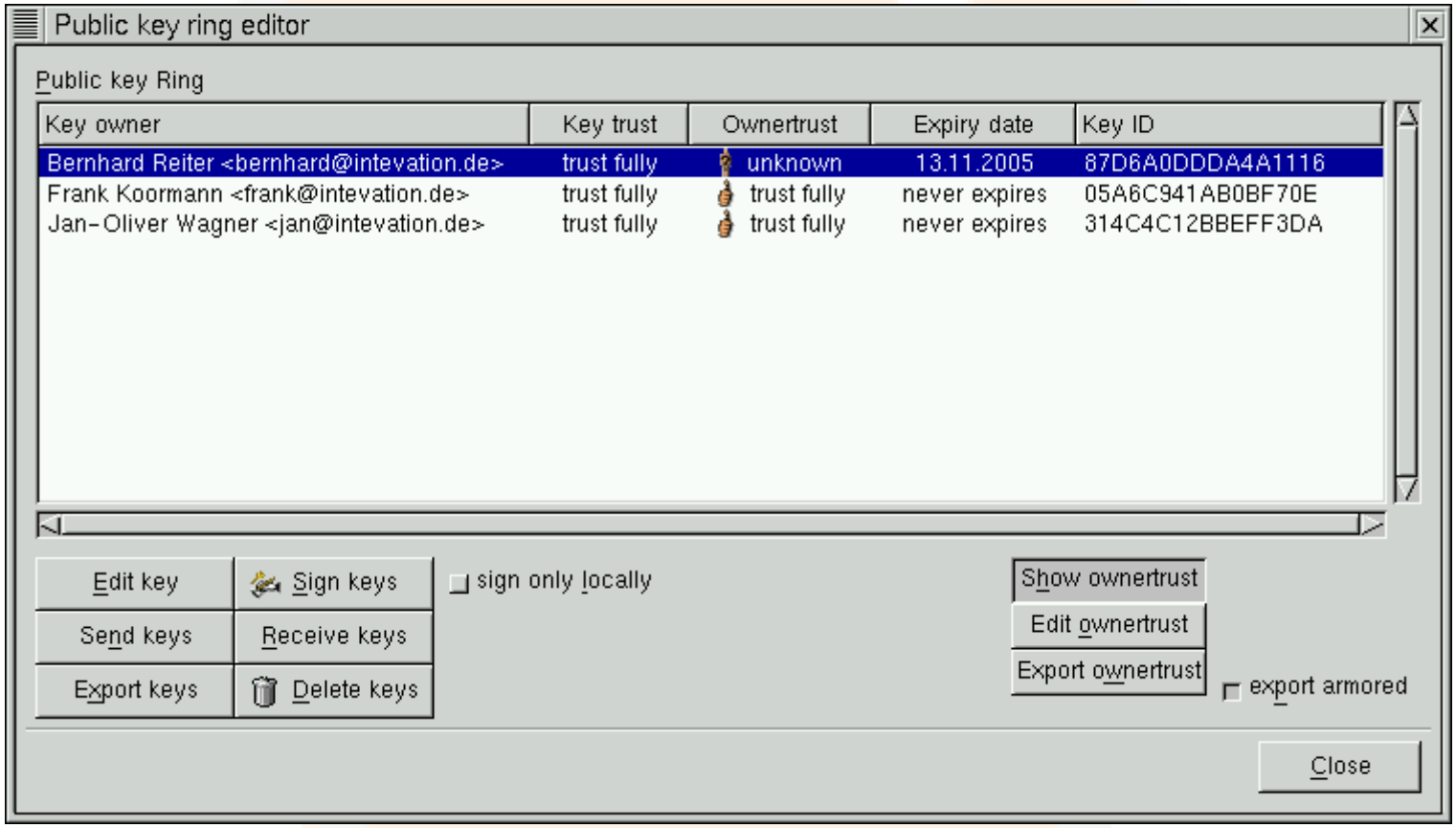
GPA

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

GPA



GPA



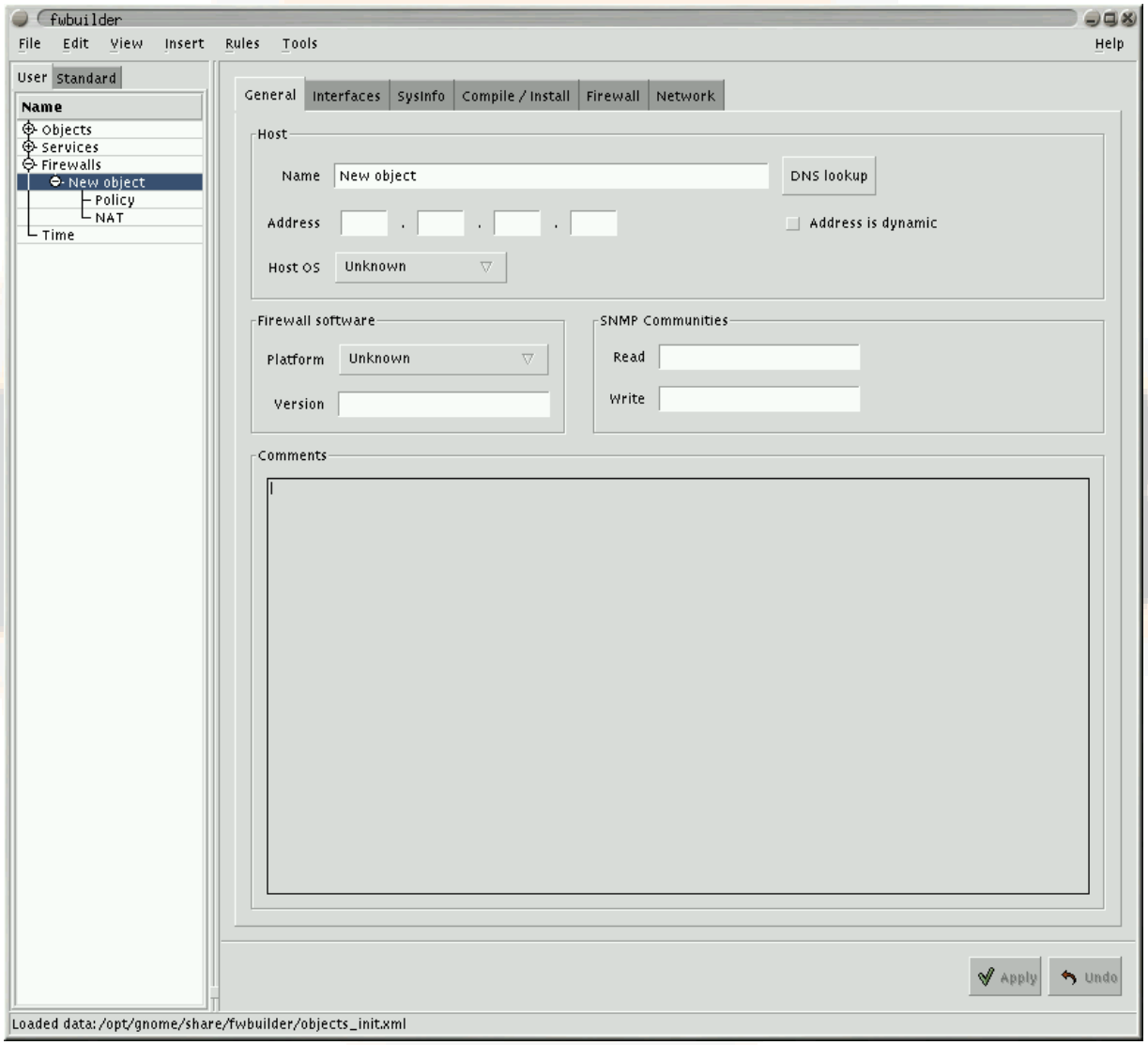
Güvenlik Duvarı - iptables

- 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/

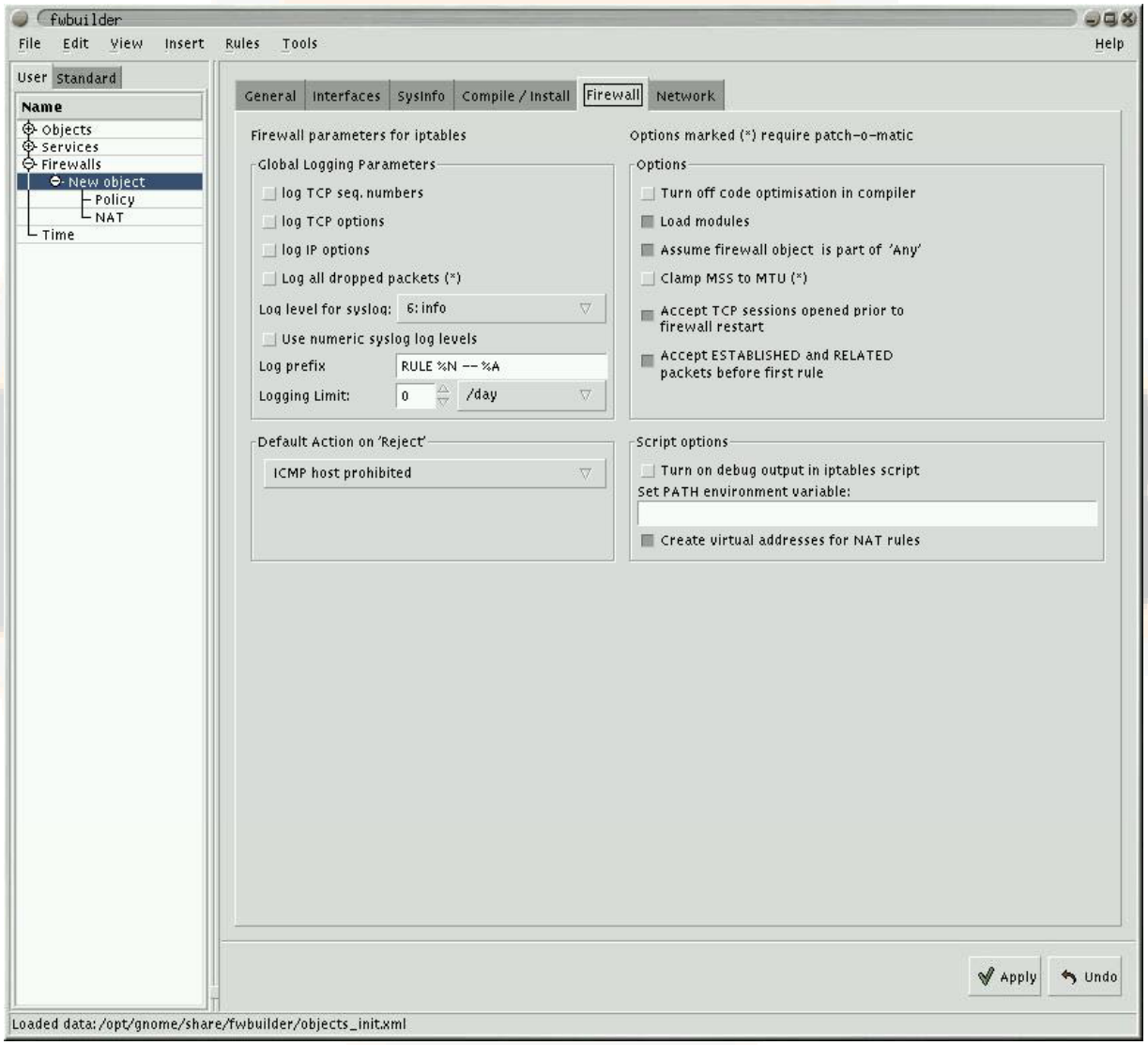
Güvenlik Duvarı - fwbuilder

- 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

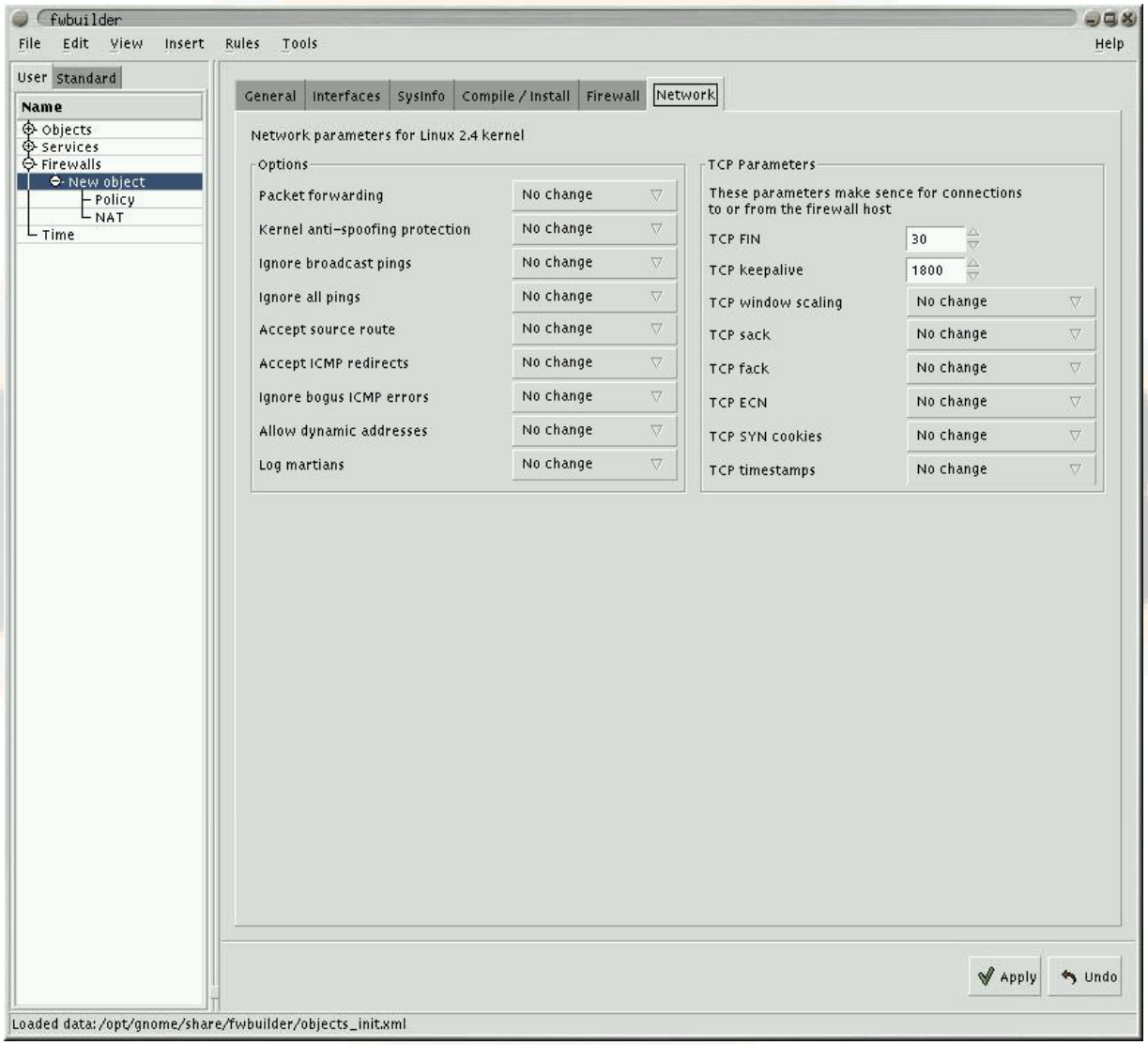
Güvenlik Duvarı - fwbuilder



Güvenlik Duvarı - fwbuilder

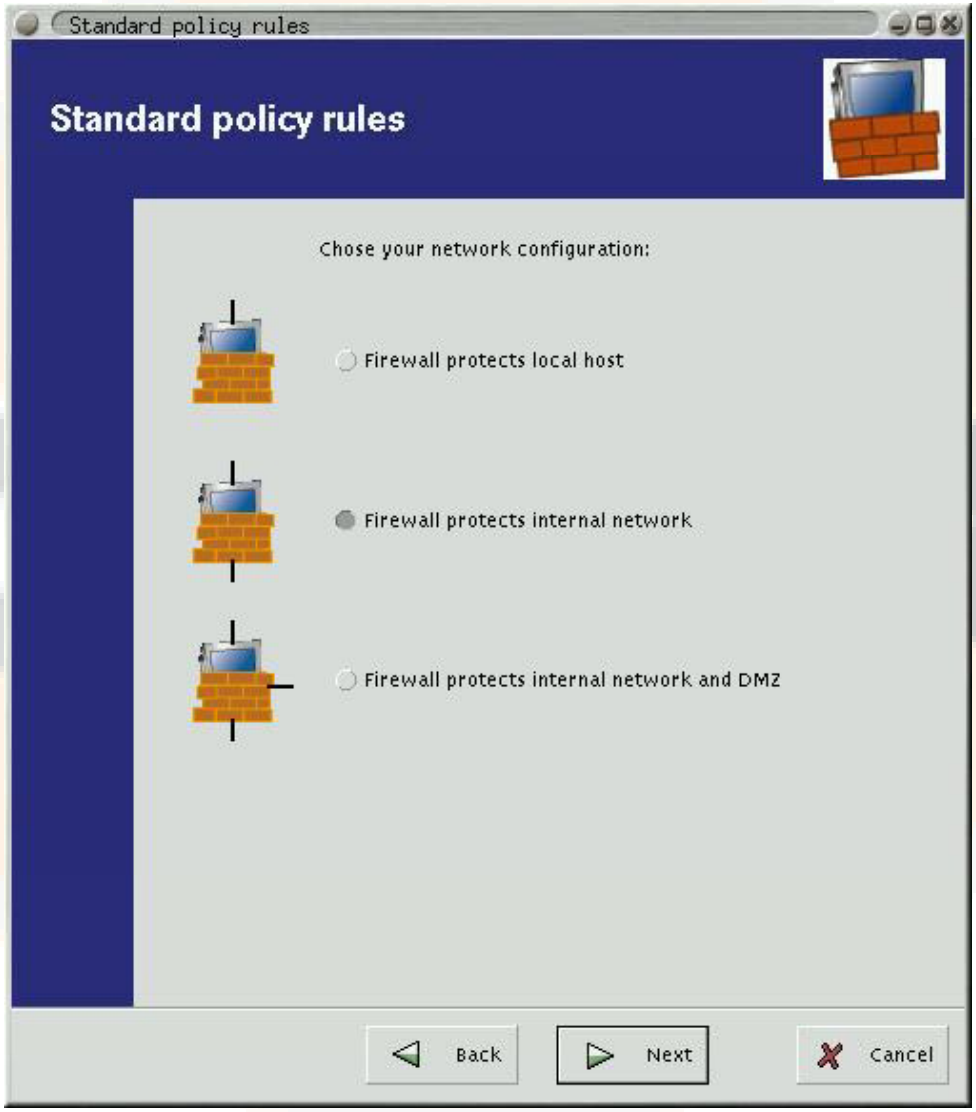


Güvenlik Duvarı - fwbuilder



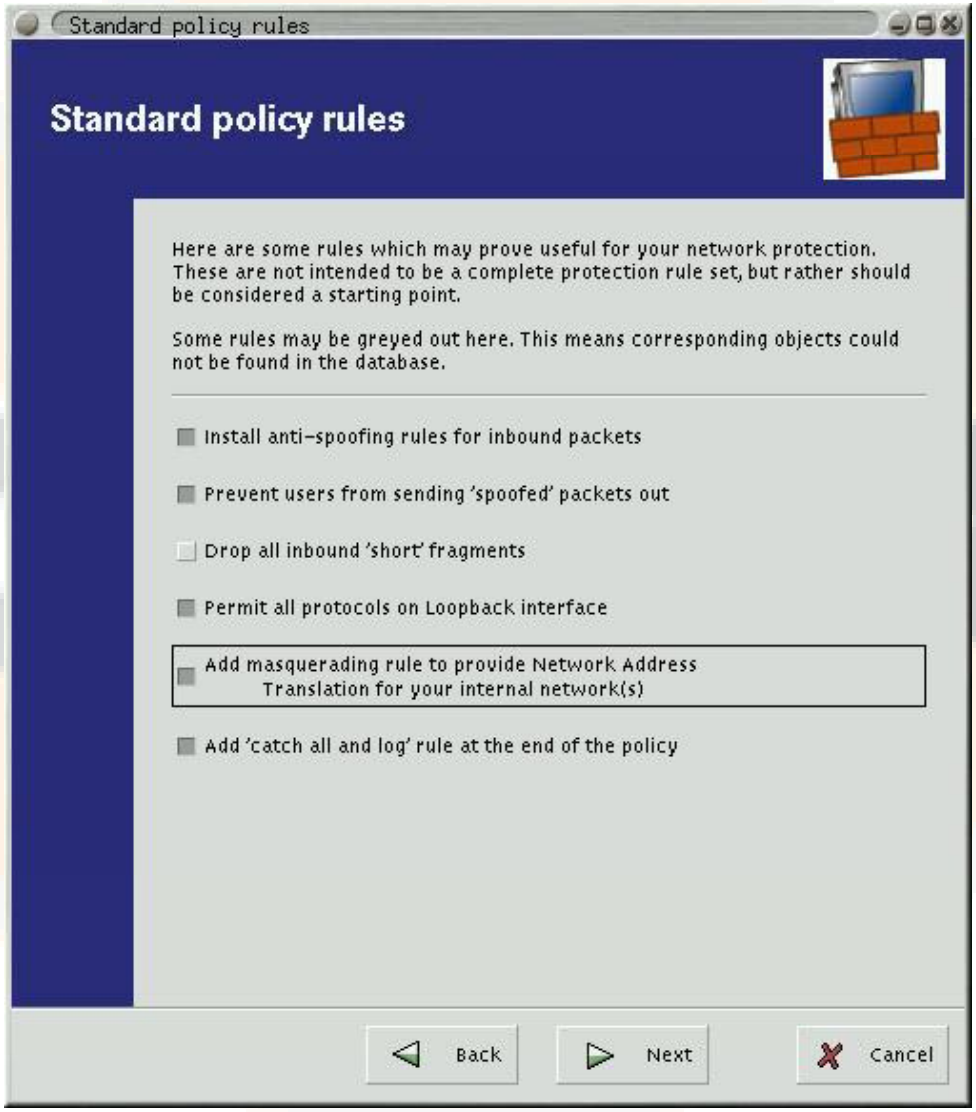
Güvenlik Duvarı - fwbuilder

Güvenlik Duvarı - fwbuilder



Güvenlik Duvarı - fwbuilder

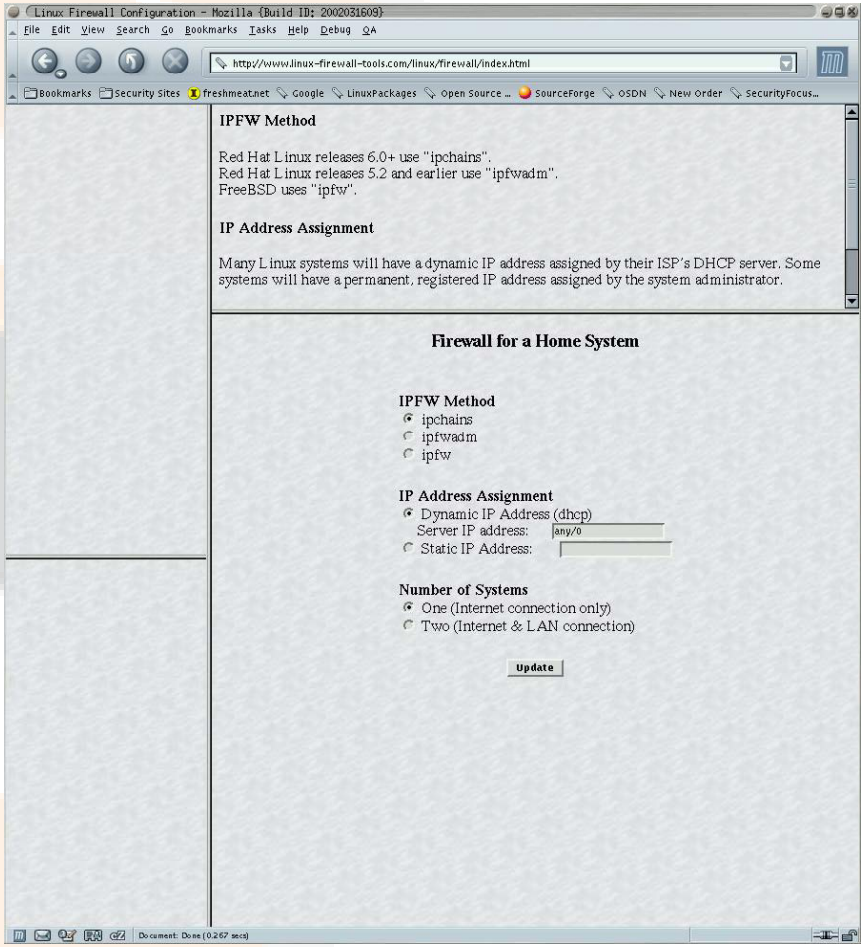
Güvenlik Duvarı - fwbuilder



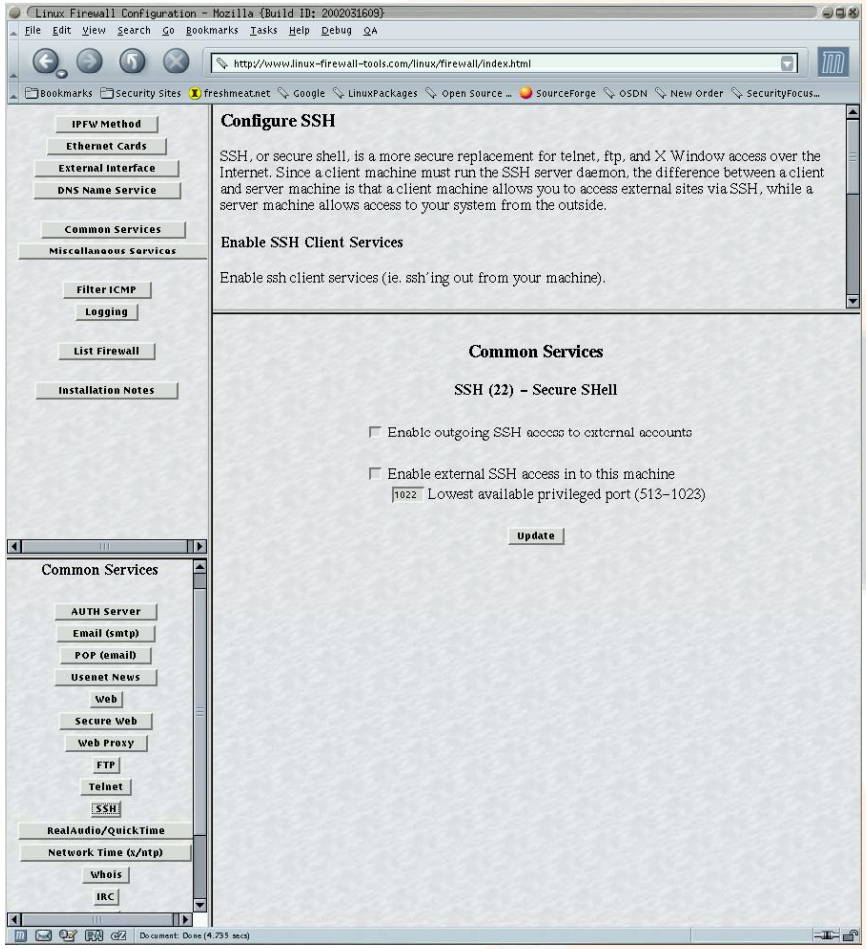
Güvenlik Duvarı – Linux Firewall Design Tool

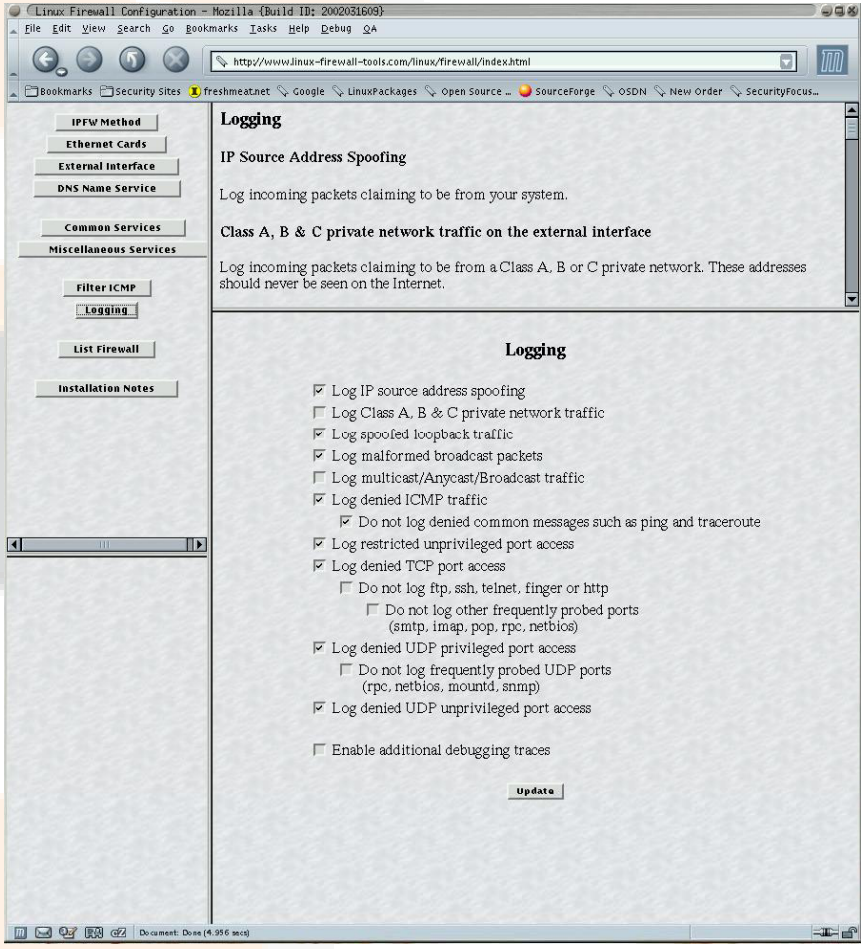
- Online bir araç
- ipchains, ipfwadm, ipfw destekliyor
- http://www.linux-firewall-tools.com/linux/firewall/index.html

Güvenlik Duvarı – Linux Firewall Design Tool

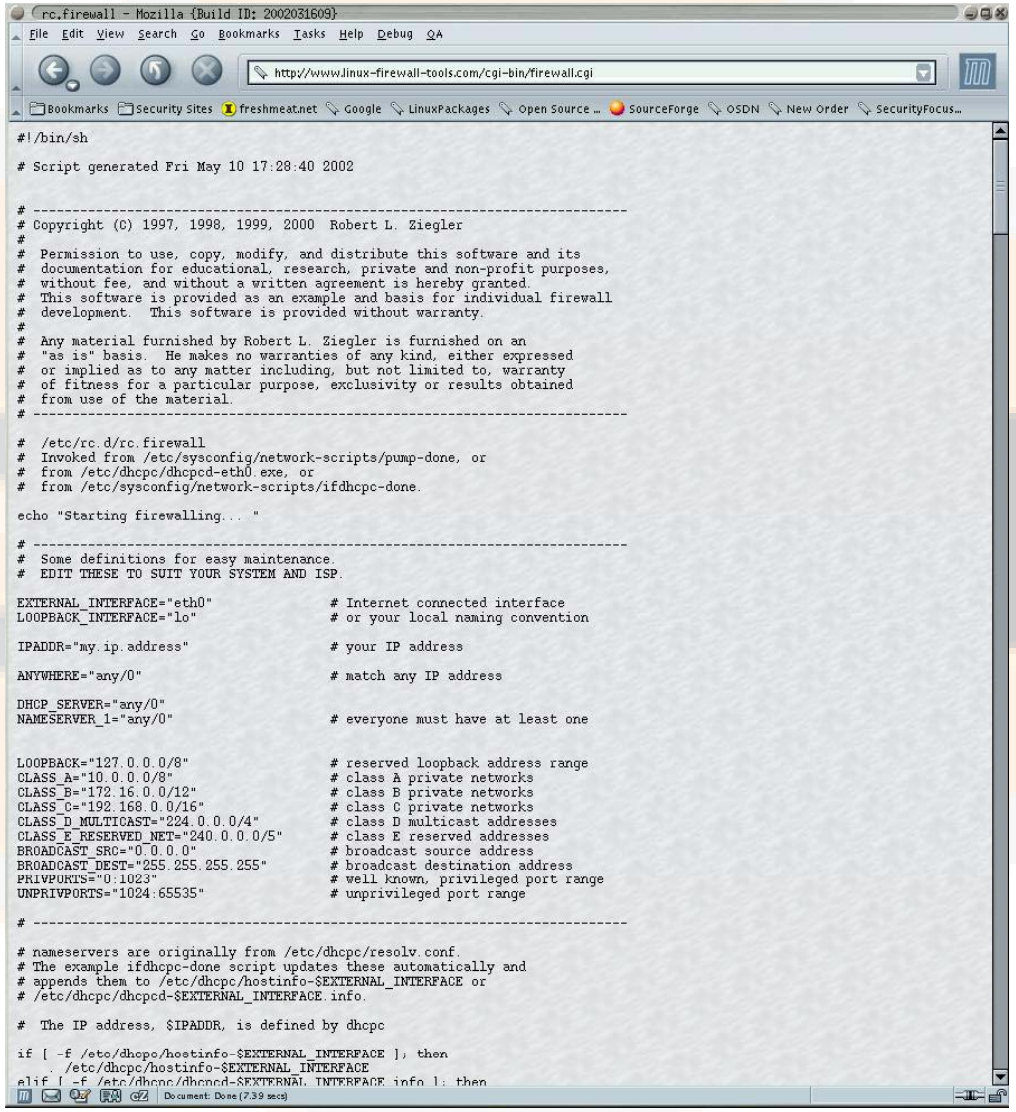


Güvenlik Duvarı – Linux Firewall Design Tool





Güvenlik Duvarı – Linux Firewall Design Tool



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/

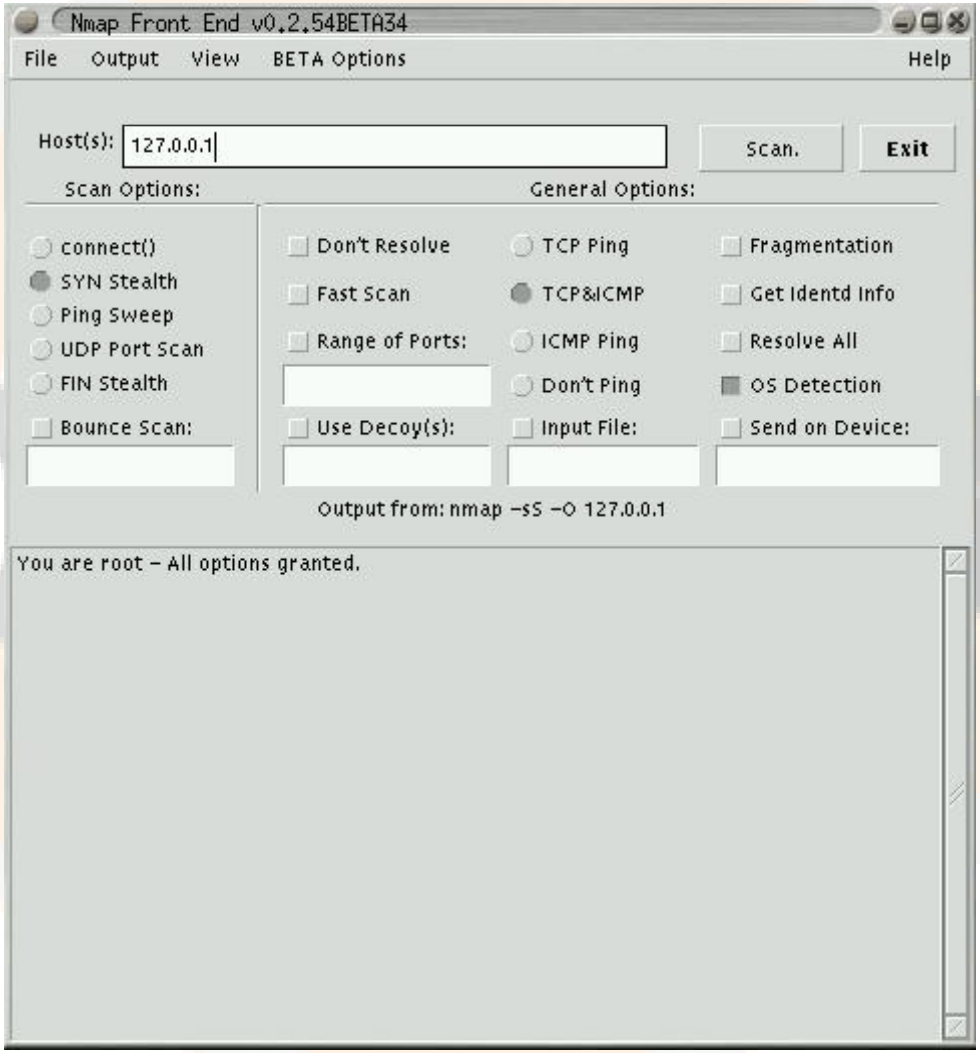
Port Tarayıcı

- nmap = Network Mapper
- Büyük ağları çabuk bir şekilde tarayabilmek için dizayn edilmiş
- GTK grafik arabirimi var
- Kısaca neler yapabiliyor?
  - Ağ'da hangi makinalar 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:~#
```

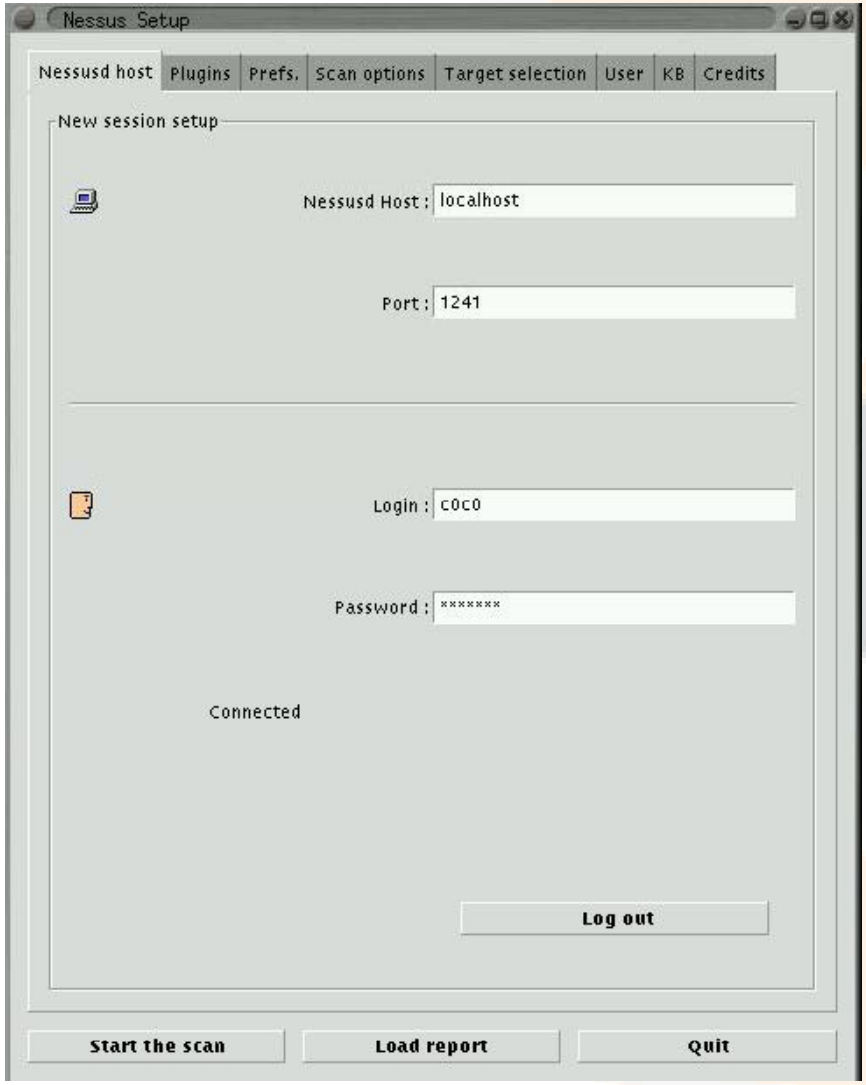
Port Tarayıcı (devam)

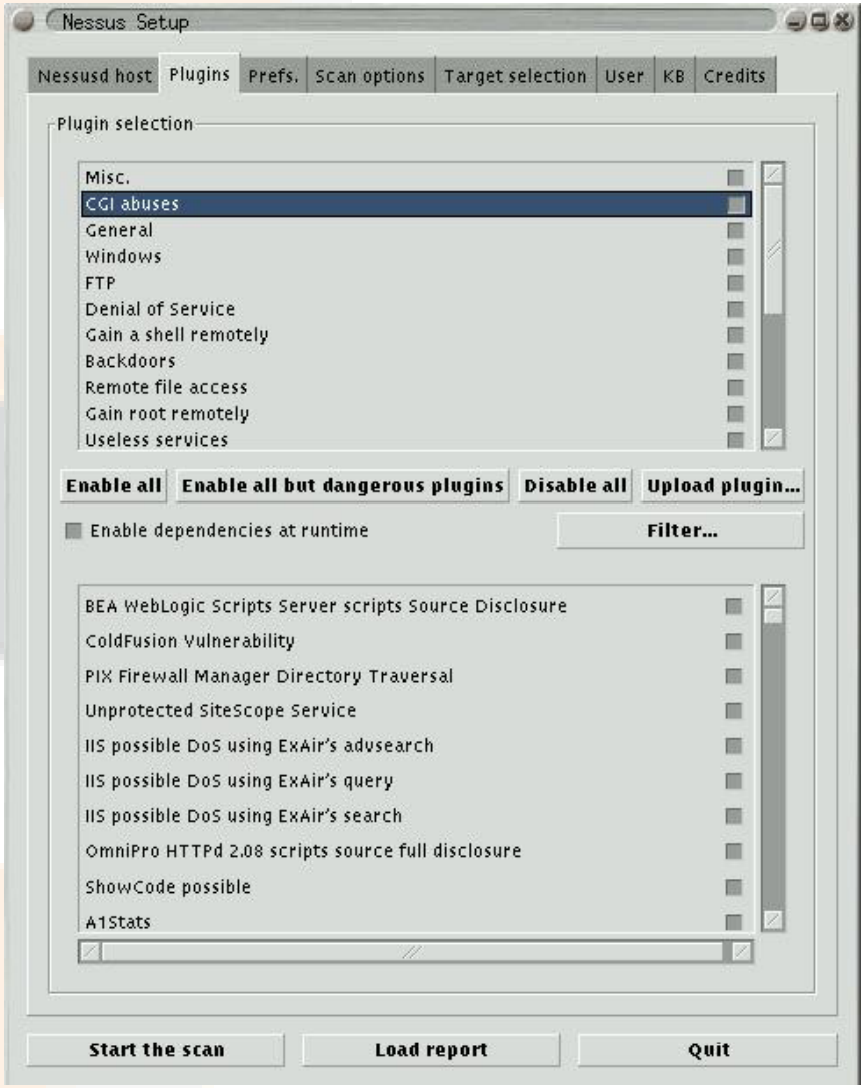


Zayıflık Tarayıcı - nessus

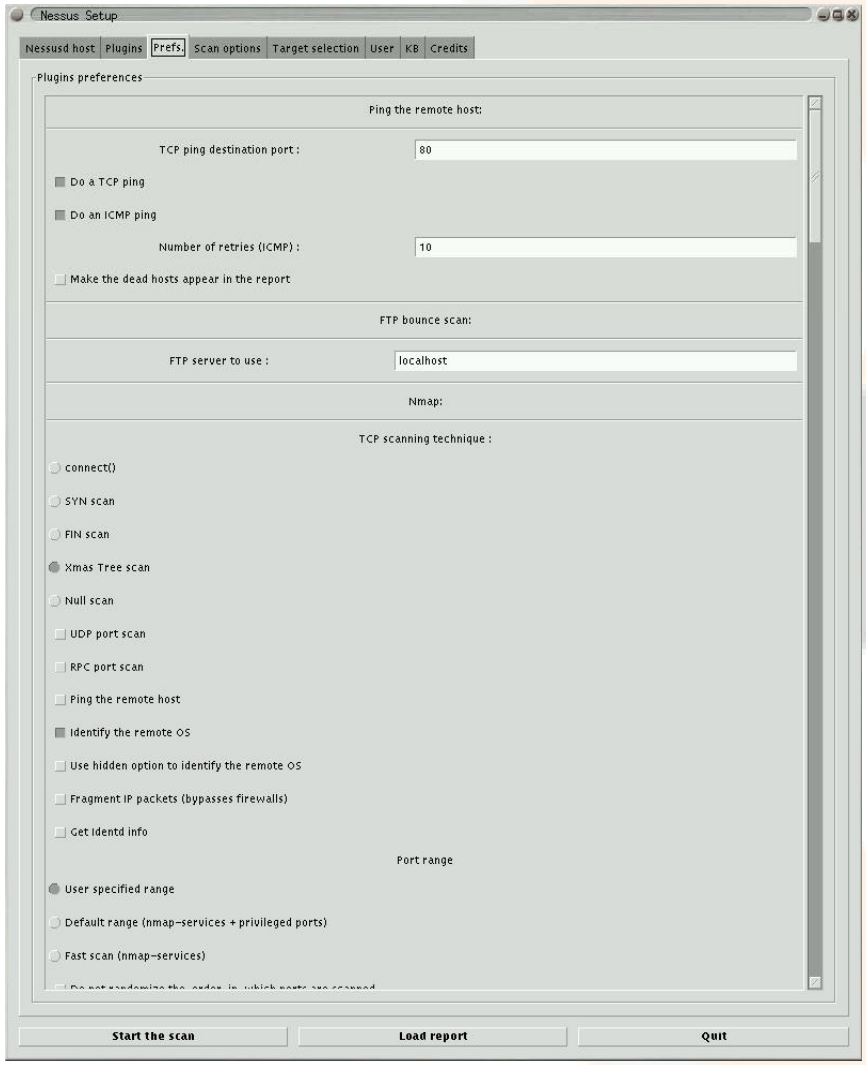
- İstemci/sunucu teknolojisi ile çalışır
- İstemci ve sunucu arasındaki trafiği SSL ile şifreleyebilir
- XML, HTML, NSR gibi formatlarda rapor sunabilir
- Raporlarında zayıflığın nasıl giderilebileceği hakkında bilgi bulundurur
- Raporlarında zayıflık hakkında referanslar verir
- Taramalar arasında karşılaştırma 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



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 deişimlerini 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 dökümante 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

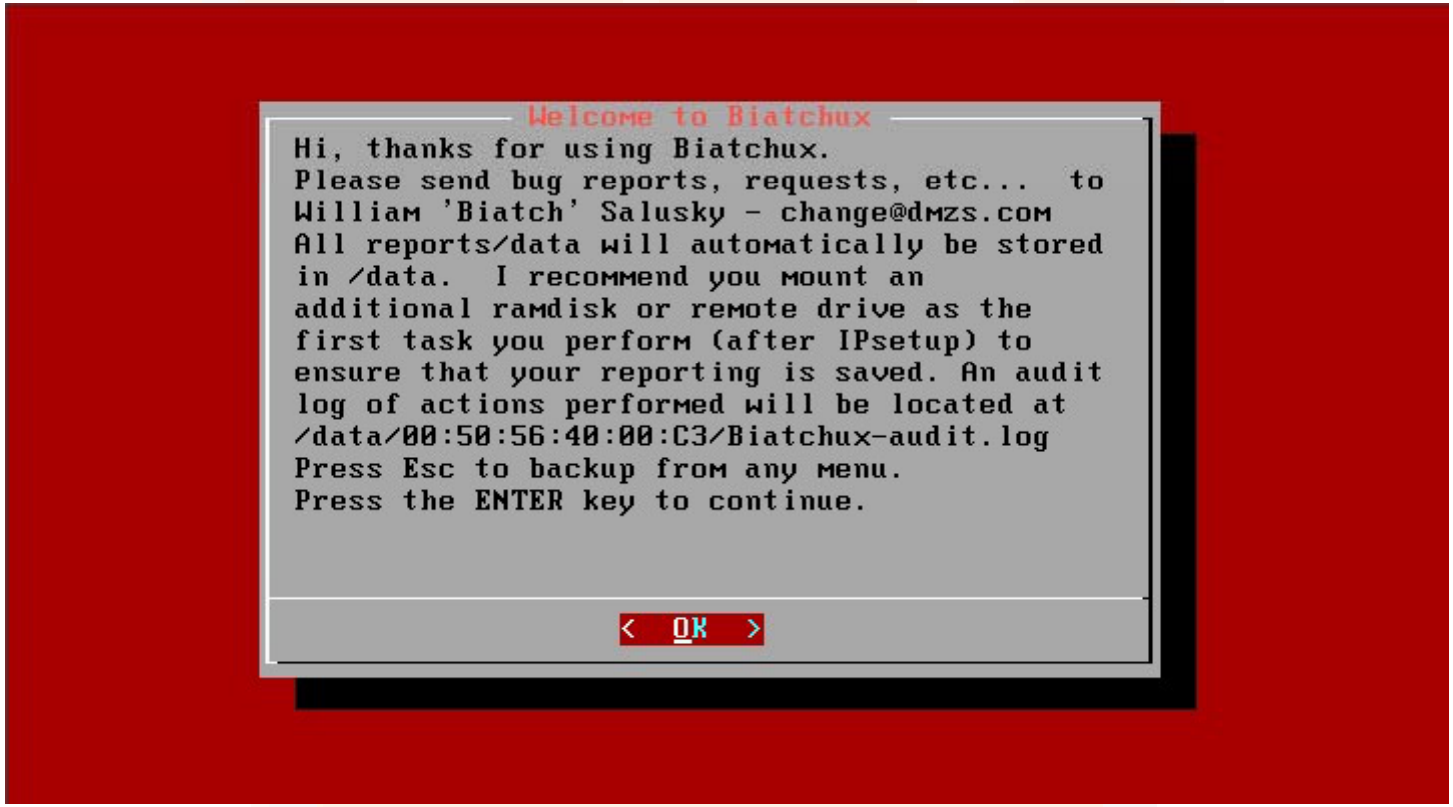
Log Analizi - logcheck

- 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

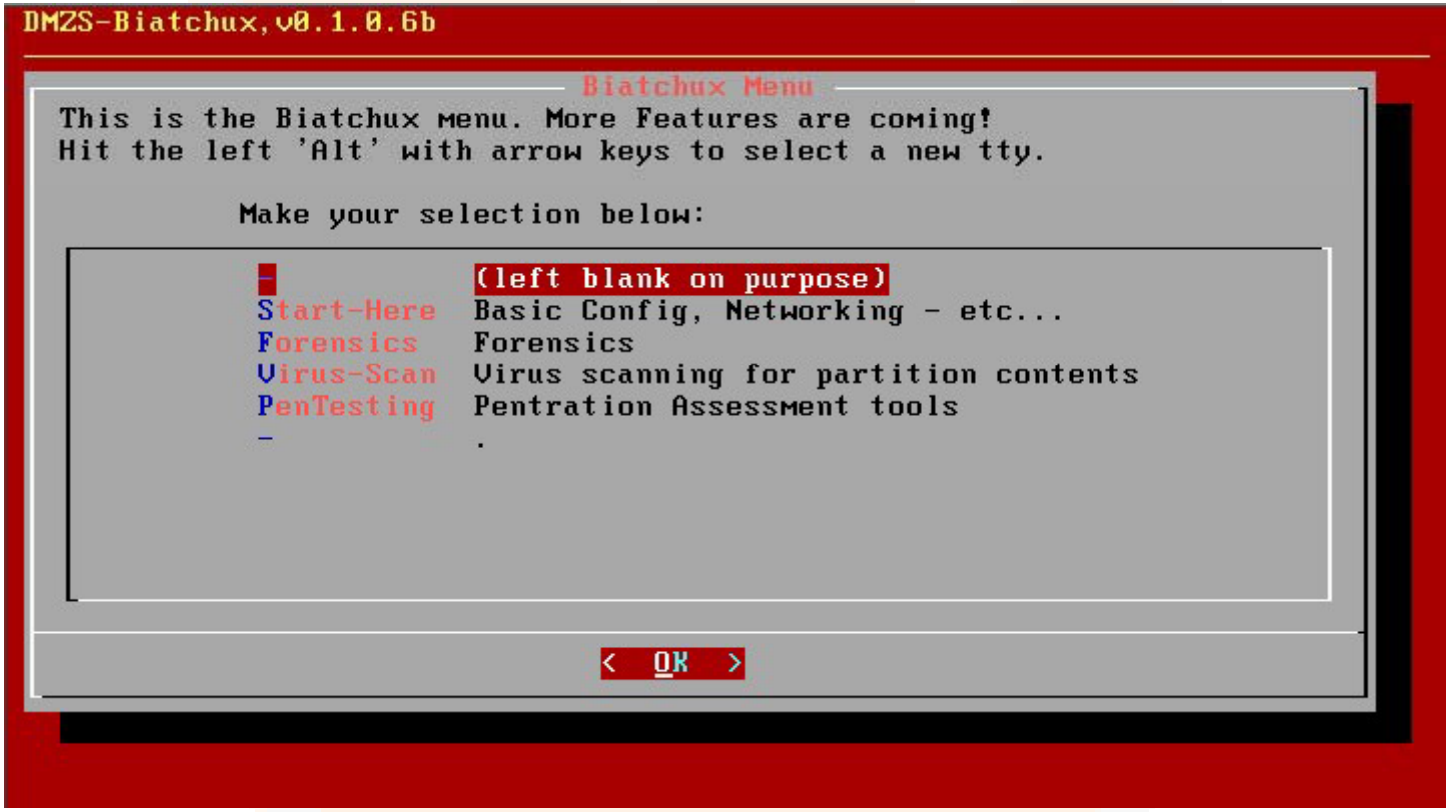
Delil Toplama ve İnceleme - biatchux

- Taşınabilir ve bootable bir CDROM dağıtımı
- Amacı:
  - Delil toplama ve inceleme
  - Olaylara müdahele
  - Veri kurtarma
  - Virüs tarama
  - Zayıflık bulma
- İçindeki araçlar statik derlendiğinden desteklediği platformlarda direkt CD'den de çalıştırılabiliyor
- 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/

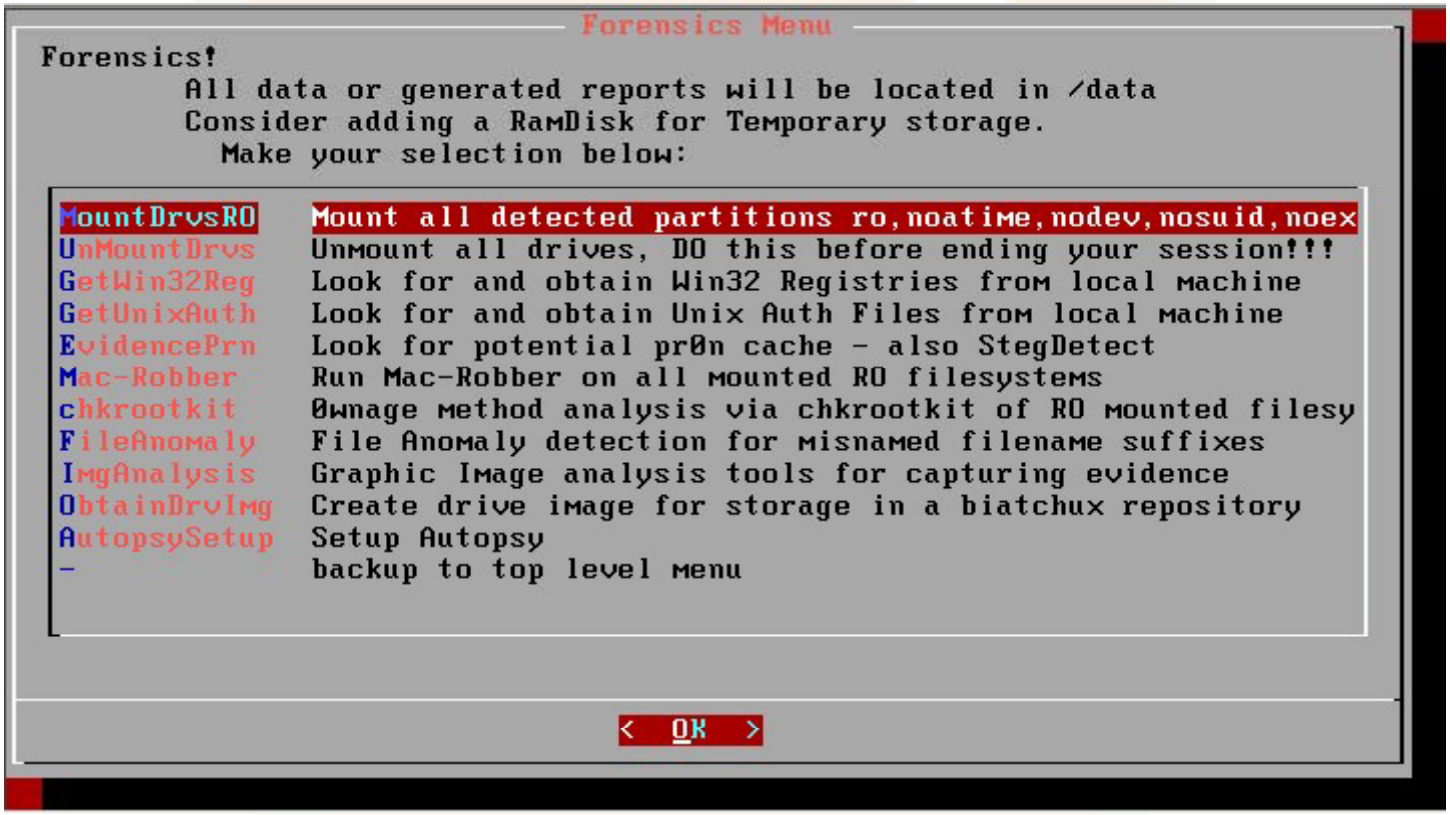
Delil Toplama ve İnceleme - biatchux



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

Teşekkürler

TEŞEKKÜRLER