



# Özgür Güvenlik Yazılımları

**Fatih Özavcı - Security Analyst**

**holden@siyahsapka.com**

**<http://www.siyahsapka.com>**





## Sunum İçeriği

- **Bilgi Güvenliği Kavramı**
- **Hareket Planı Bileşenleri**
- **Güvenlik Uygulamaları**
- **Özgür Güvenlik Yazılımları**
  - **Tanıtımları**
  - **Mimarileri**
  - **Kullanım Amaçları**





## Bilgi Güvenliği Kavramı

**Bilişim ürünleri ve cihazları ile bu cihazlarda işlenmekte olan verilerin bütünlüğü ve sürekliliğini korumayı amaçlayan çalışma alanıdır.**



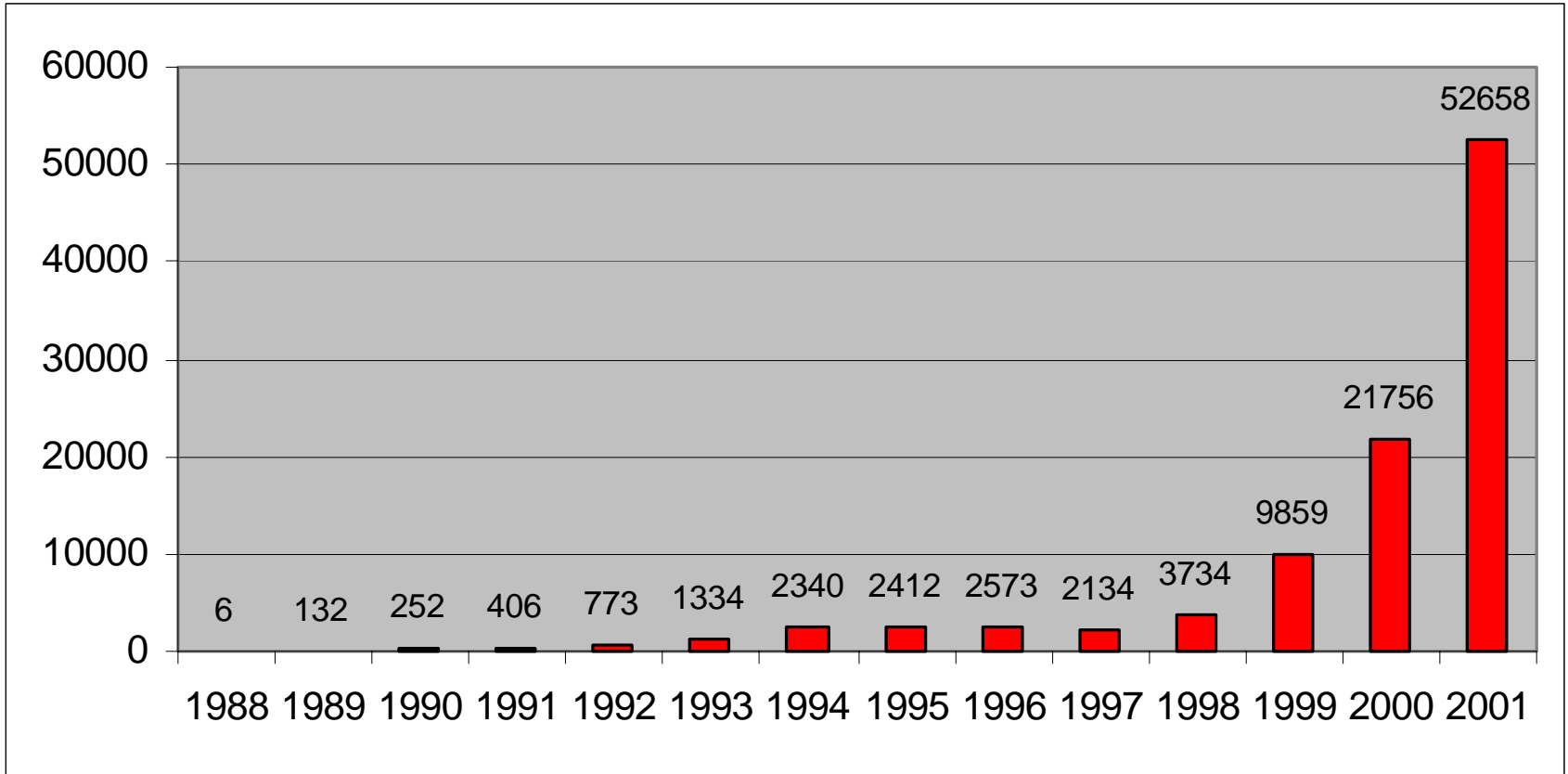


## Bilgi Güvenliğinin Amacı

- **Veri Bütünlüğünün Korunması**
- **Erişim Denetlemesi**
- **Mahremiyet ve Gizliliğin Korunması**
- **Sistem Devamlılığının Sağlanması**



## Cert CC – Yıllara Göre Rapor Edilen Olay Sayısı



## Risk ve Tehditler

- **Dahili Risk Unsurları**
  - Bilgisiz ve Bilinçsiz Kullanım
  - Kötü Niyet  
(Bilgi Sızdırma, İntikam İsteği)
- **Harici Risk Unsurları**
  - Hedefe Yönelmiş Saldırıları  
(Hacker, Cracker)
  - Hedef Gözetmeyen Saldırıları  
(Virüs, Worm)





## Saldırıya Uğrayabilecek Değerler

- Kurum İsmi, Güvenilirliği ve Markaları
- Özel / Mahrem / Gizli Bilgiler
- İşin Devamlılığını Sağlayan Bilgi ve Süreçler
- Üçüncü Şahıslarca Emanet Edilen Bilgiler
- Kuruma Ait Adli, Ticari Teknolojik Bilgiler





## Görülebilecek Zararın Boyutu

- **Müşteri Mağduriyeti**
- **Kaynakların Tüketimi**
- **İş Yavaşlaması veya Durdurulması**
- **Kurumsal İmaj Kaybı**
- **Üçüncü Şahıslara Yapılacak Saldırı Mesuliyeti**





## Güvenlik İhtiyacının Sınırları

**Saldırıya Uğrayabilecek Değerlerin,  
Kurum İçin Arzettiği Önem Seviyesi  
Güvenlik İhtiyacının Sınırlarını  
Belirlemektedir.**



## Hareket Planı Bileşenleri

### ● **Güvenlik Politikası Oluşturulması**

- Sunulacak Hizmet Planının Oluşturulması
- Erişim Seviyelerinin Belirlenmesi
- Bilgilendirme ve Eğitim Planı
- Savunma Bileşenlerini Belirleme
- Yedekleme ve Kurtarma Stratejisi Belirleme

### ● **Güvenlik Politikasının Uygulaması**

- Kullanılacak Bileşenlerin Belirlenmesi
- Bileşenlerin Uygun Biçimde Yapılandırılması
- Bilgilendirme ve Eğitim Seminerleri

### ● **Denetleme ve İzleme**

- Ağın Politikaya Uygunluğunun Denetlenmesi
- Oturumların ve Hareketlerin İzlenmesi
- Ağa Sızma Testleri



## Güvenlik Uygulamaları

- **Güvenlik Duvarı** iptables, fwbuilder
- **Saldırı Tespit Sistemi** snort, lids
- **Zayıflık Tarama Sistemi** nessus, nmap
- **Şifreleme Yazılımları** gpg, gpa, gpgp
- **Sistem Güçlendirme** bastille-linux
- **Anti-Virüs Sistemi** amavis (e-posta geçidi)
- **Sanal Özel Ağ Sistemi** frees/wan
- **Tümleşik Sistem** trinix

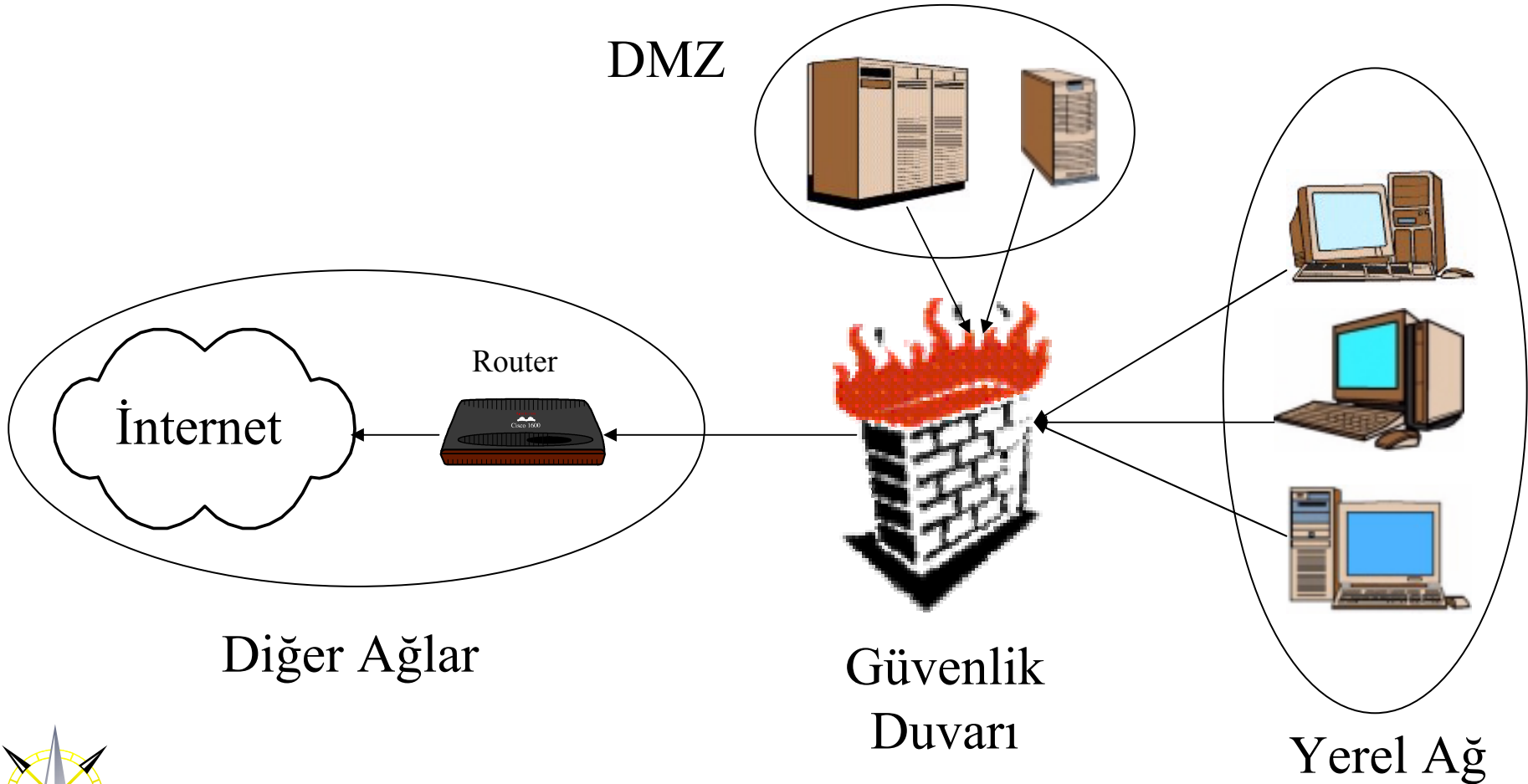


## Güvenlik Duvarı

- Ağlar arası erişimleri düzenlerler
- Mimarileri
  - Statik Paket Filtreleme
  - Dinamik Paket Filtreleme (Stateful Inspection)
  - Uygulama Seviyesinde Koruma (Proxy)
- Erişimleri kural tabanlı belirlerler
- Donanım ve Yazılım olarak sunulabilirler
- Amaca özel işletim sisteminde bulunmalıdırlar
- Her türlü formatta kayıt ve uyarı sunabilirler



## Güvenlik Duvarı Örnek Yerleşimi





## Iptables

- **GPL lisansı altında serbestçe dağıtılabilir/kullanılabilir**
- **Linux 2.3.x ve 2.4.x serisi kernel ile çalışabilmektedir**
- **Dinamik paket filtreleme yapabilmektedir**
- **Çeşitli IP seçeneklerine göre filtreleme yapılabilir**
  - **Paketlerin Bölünmüş Olma Özelliğine Göre**
  - **Taşıma Protokolü Türüne Göre (IPSec, TCP, UDP, ICMP v.s.)**
  - **TCP Bayraklarına ve Portuna Göre**
  - **UDP Portuna Göre**
  - **ICMP Türüne Göre**
- **MAC adresine göre filtrelemede yapılabilir**
- **Statik ve Dinamik NAT yapabilmektedir**
- **<http://www.samba.org/netfilter> adresinden temin edilebilir**



## Iptables – Kural Yapısı

- Üç ayrı tabloda bulunan zincirle ile kurallar belirlenir
  - filter
    - INPUT
    - OUTPUT
    - FORWARD
  - nat
    - PREROUTING
    - OUTPUT
    - POSTROUTING
  - mangle
    - PREROUTING
    - OUTPUT





## Örnek Kurallar

### Spooftng Engelleme

```
iptables -t nat -A PREROUTING -i $internet_arayüzü -s 192.168.0.0/16 -j DROP
```

### Statik Bir IP Adresi ile NAT

```
iptables -t nat -A POSTROUTING -o $internet_arayüzü -j SNAT --to-source $statik_ip
```

### SYN Bayrağı Taşımayan TCP Paketlerini Gözardı Etme

```
iptables -A FORWARD -p tcp ! --syn -m state --state NEW -j DROP
```

### Zincir İçin Varsayılan Politikayı Değıştirme

```
iptables -P INPUT DROP
```

### Yeni Bir Zincir Oluşturma

```
iptables -N Yeni_Zincir
```



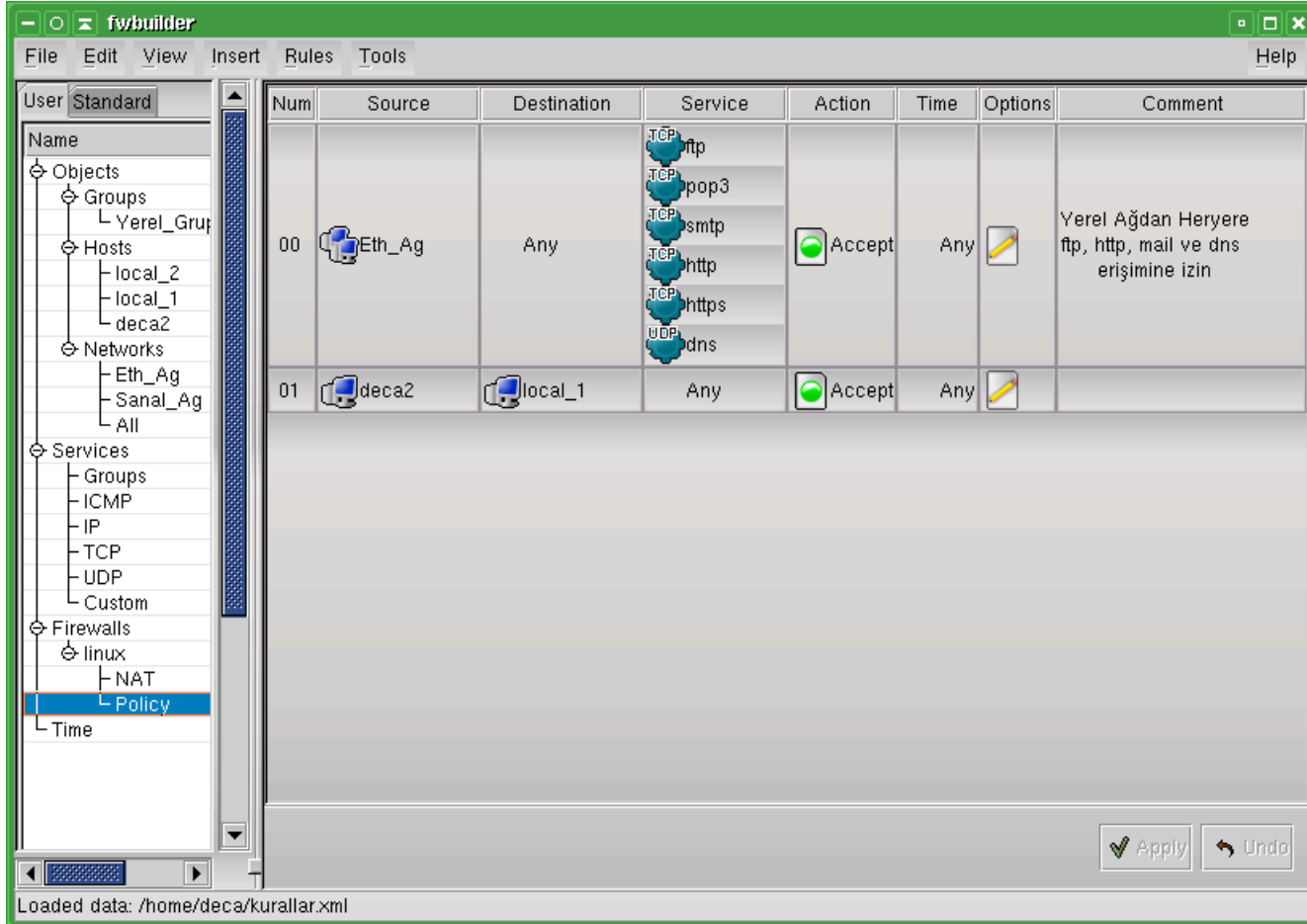


## Fwbuilder

- GPL lisansı altında serbestçe dağıtılabilir/kullanılabilir
- GTK arabirimi ile kolayca kural setleri oluşturulabilir
- 3 ayrı güvenlik duvarının kurallarını destekler
  - Iptables
  - Ipchains
  - Ipfiler
- Standart kural belirleme sihirbazı vardır
- Verileri XML formatında kayıt eder, böylece değişkenler belirlendikten sonra istenildiğinde tekrar kullanılabilir
- Sunucu ile aynı sistemde olması gerekmez
- <http://www.fwbuilder.org> adresinden temin edilebilir



## Fwbuilder – Ekran Görüntüleri – 1



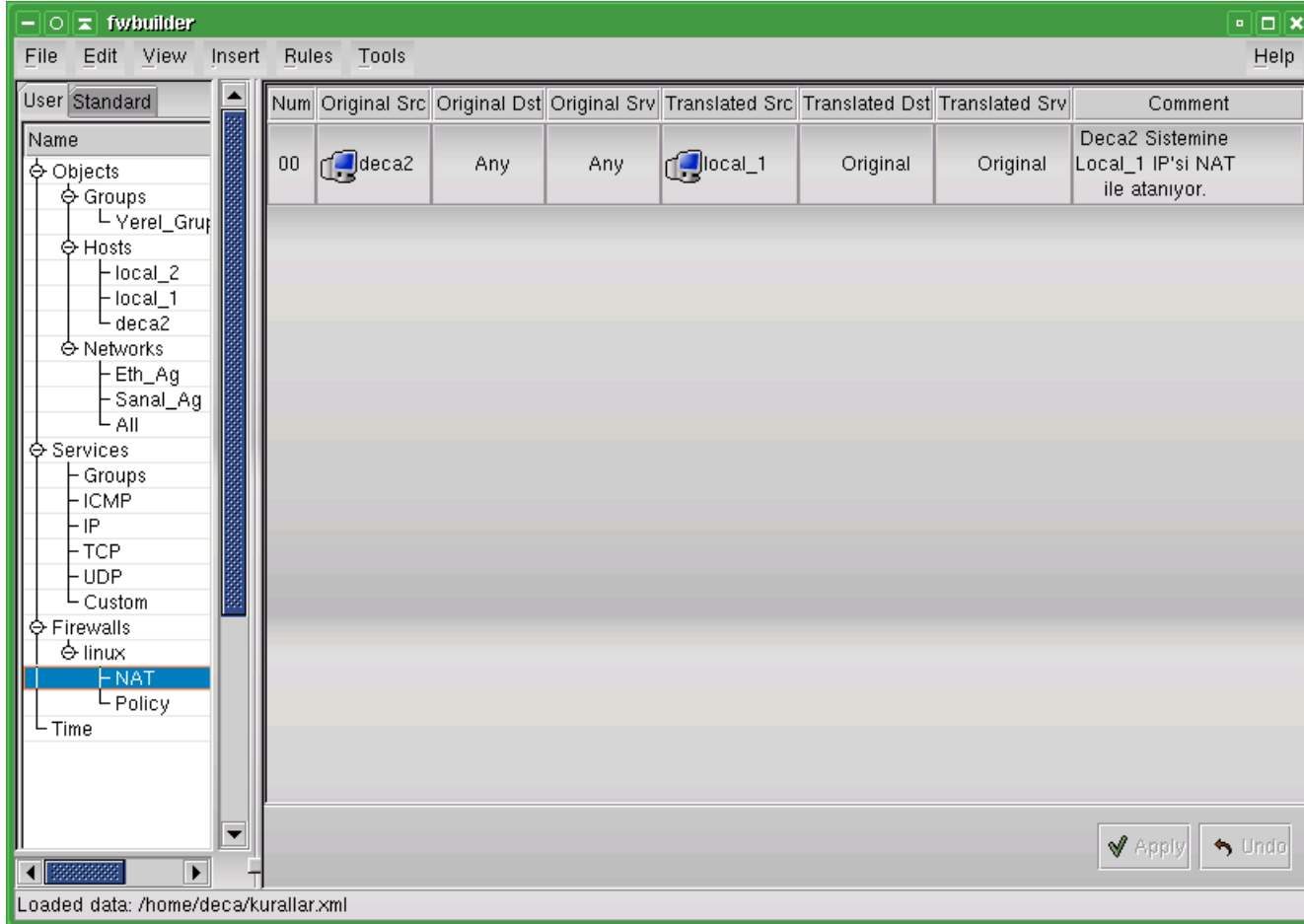
The screenshot displays the Fwbuilder application window. The interface includes a menu bar (File, Edit, View, Insert, Rules, Tools, Help) and a sidebar with a tree view of objects and services. The main area shows a table of firewall rules.

Num	Source	Destination	Service	Action	Time	Options	Comment
00	Eth_Ag	Any	TCP ftp TCP pop3 TCP smtp TCP http TCP https UDP dns	Accept	Any		Yerel Ağdan Heryere ftp, http, mail ve dns erişimine izin
01	deca2	local_1	Any	Accept	Any		

Loaded data: /home/deca/kurallar.xml



## Fwbuilder – Ekran Görüntüleri – 2



The screenshot shows the Fwbuilder application window. The left sidebar displays a tree view of the configuration hierarchy, with 'NAT' selected under the 'linux' firewall. The main area shows a table of NAT rules. The first rule is selected, with the following details:

Num	Original Src	Original Dst	Original Srv	Translated Src	Translated Dst	Translated Srv	Comment
00	deca2	Any	Any	local_1	Original	Original	Deca2 Sistemine Local_1 IP'si NAT ile ataniyor.

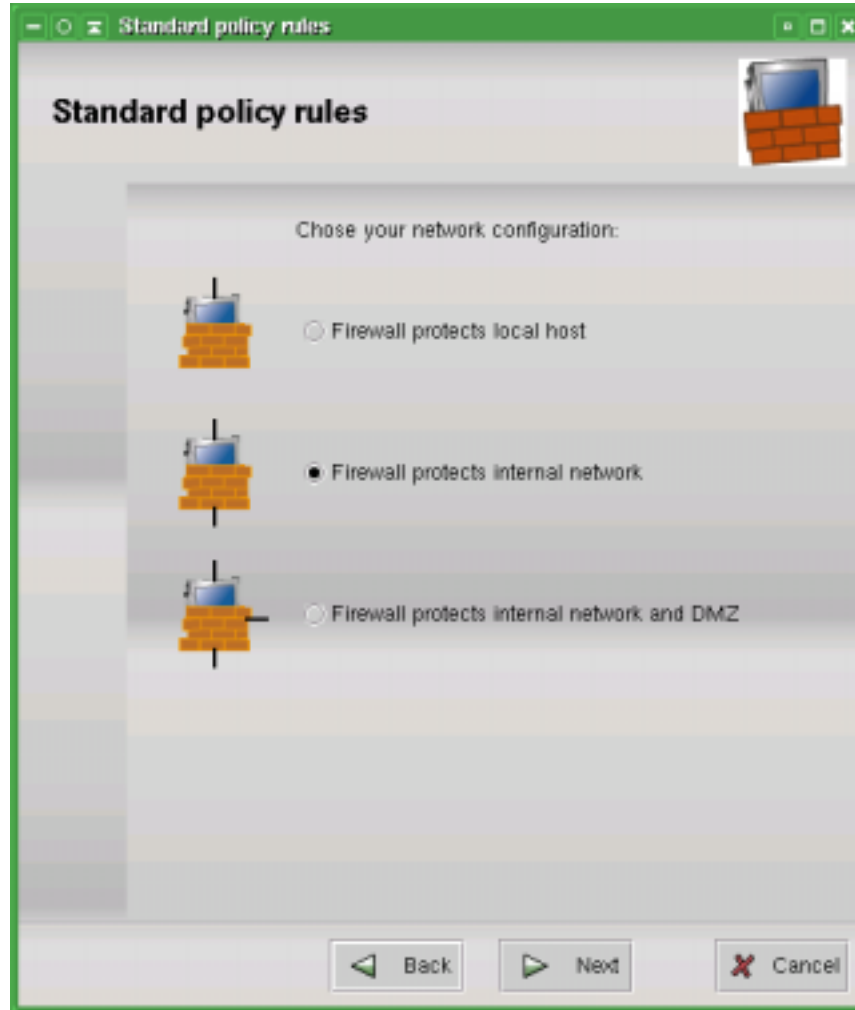
At the bottom right of the window, there are 'Apply' and 'Undo' buttons. The status bar at the bottom indicates 'Loaded data: /home/deca/kurallar.xml'.



## Fwbuilder – Ekran Görüntüleri – 3



## Fwbuilder – Ekran Görüntüleri – 4



## Saldırı Tespit Sistemleri

- **Amaçlarına Göre 3'e Ayrılırlar**
  - Ağ Temelli Saldırı Tespiti
  - Sunucu Temelli Saldırı Tespiti
  - Uygulama Temelli Saldırı Tespiti
- **Mimarilerine Göre 2'ye Ayrılırlar**
  - Anormallik Saptama Temelli
  - Saldırı İmzası Arama Temelli



## Ağ Temelli / Saldırı İmzası Arama

- Belirli bir ağ parçasını dinleyerek saldırıları tespit etmeye çalışırlar
- Tanımlı olan imzalar ile saldırıları belirler ve engelleyebilirler
- Birden fazla yardımcı ile çalışarak, merkezi yönetim ve raporlama sağlayabilirler
- Güvenlik Duvarı ve Router üzerine, saldırı sonucu dinamik kurallar koyabilirler
- Köprü (Bridge) modunda çalışarak kendilerini gizleyebilirler
- SMS, Pager, WinPopup, Sistem Kaydı, XML ve Veritabanı gibi uyarı ve kayıt çıktıları sağlayabilirler



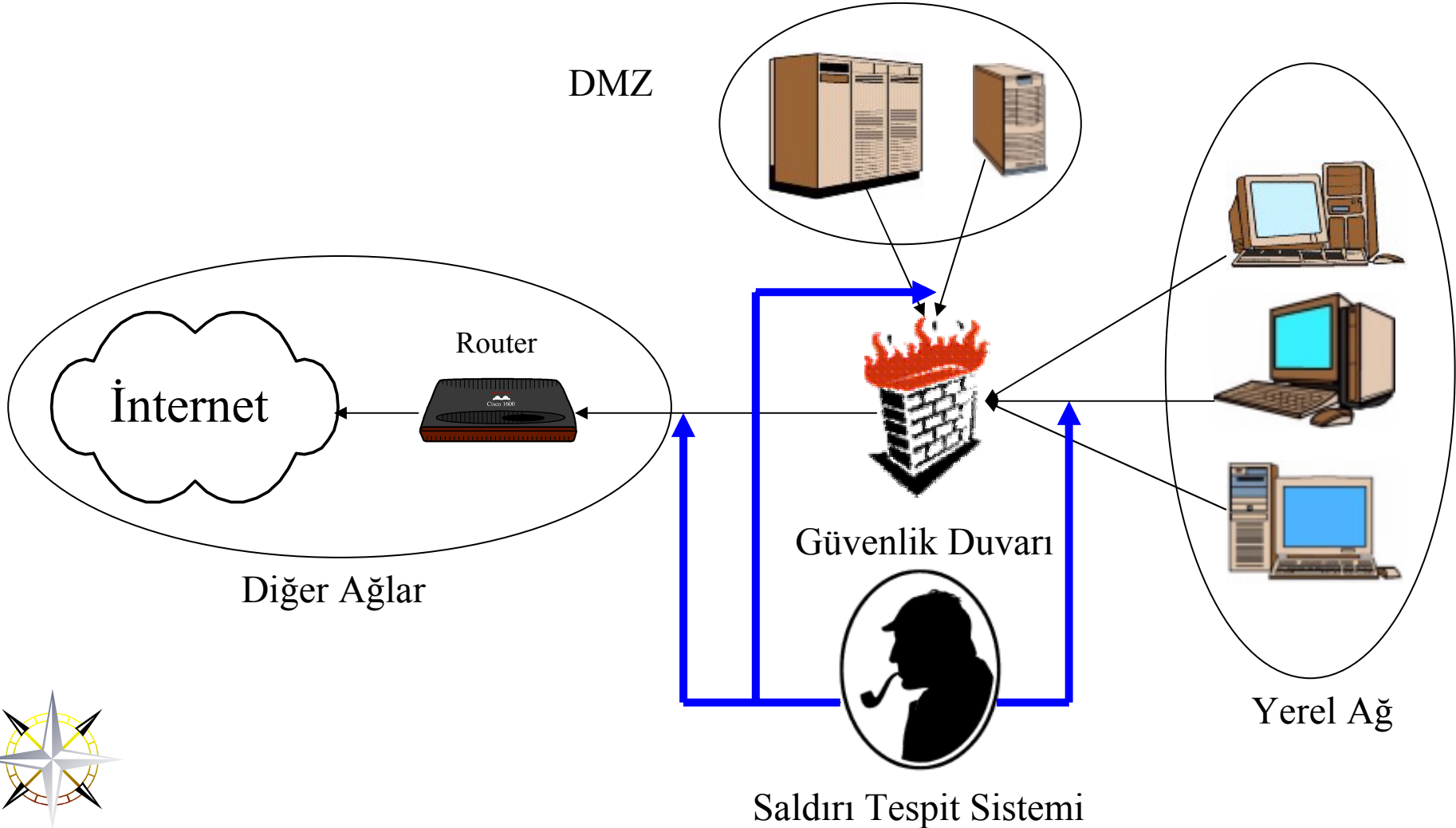


## Sunucu Temelli / Saldırı İmzası Arama

- Özel dosyaları, sistem kayıtlarını ve sürücülerini izleyerek, değişiklikleri rapor edebilirler
- Tanımlı olan imzalar ile saldırıları belirlerler
- Sistemde aktif bulunan işlemleri takip edebilirler
- Gerekli görüldüğü durumlarda, servis durdurabilir ve başlatabilirler
- SMS, Pager, WinPopup, Sistem Kaydı, XML ve Veritabanı gibi uyarı ve kayıt çıktıları sağlayabilirler



## Ağ Temelli Saldırı Tespit Sistemi Örnek Yerleşimi





# Özgür Güvenlik Yazılımları

## Snort

- GPL lisansı altında serbestçe dağıtılabilir/kullanılabilir
- Farklı platformlarda çalışabilir (Unix, Linux, Windows)
- Ağ Temelli / Saldırı İmzası Arama mimarisi ile çalışır
- Saldırı imzası veritabanı İnternet'ten kolayca güncellenebilir
- Birden fazla snort tek merkezden yönetilebilir, merkezi raporlama oluşturulabilir
- Birçok sistem ve ağ segmenti bir tek snort ile izlenebilir
- Özgün kurallar, saldırı önem dereceleri ve tepkiler belirlenebilir
- Eklenti sistemi ile çalışabilir, özgün eklentiler hazırlanabilir
- <http://www.snort.org> adresinden temin edilebilir



## Snort Eklentileri

- **Ön-İşlem Eklentileri** : Özel paketleri saldırı için incelenebilecek hale getirmek için kullanılırlar

http-decode , stream4, portscan

- **İşlem Eklentileri** : Kural diline yeni özellikler ekleyerek zenginleştirmek için kullanılırlar

content, ttl, flags

- **Çıktı Eklentileri** : Saldırı belirlendikten sonra yapılabilecek işlemleri arttırmak için kullanılırlar.

xml, alert\_smb, database



## Snort Kural Yapısı

alert	tcp	any	any	->	x.x.x.x	139	(content:"deneme"; msg:"deneme saldırısı");
Eylem	Protokol	IP Adresi 1	Port Adresi 1	Yön	IP Adresi 2	Port Adresi 2	Seçenek Adı
							Seçenek Parametreleri

Kural Seçenekleri  
İşlem Eklentileri  
İle Vardır





## Snort Arabirimleri - Demarc



**demarc**  
-network security monitor-

summary events monitor integrity search configure

122162 events currently in database, 83 unique. joeuser - logout - 6

6:08:38 AM, Tue Sep 25 2001  
Last login from 192.168.41.35 on Tuesday September 25, 2001 at 06:07:42 AM.

**Last NIDS Alert**  
24 sec ago  
P-1-WEB-IS cmd.exe access

**Monitored Hosts**  
host3.your\_domain.com - HTTPS

**Monitored Files**  
192.168.112.69 (3)

**Alerts (Last 6 Hrs)**

Time	Count
6 AM	12
5 AM	572
4 AM	238
3 AM	303
2 AM	180
1 AM	309

**% Alerts/Sensor**

Sensor	% Alerts
192.168.112.69	91%
192.168.112.10	9%
slugger	<1%

**Host Monitoring Alerts**  
your\_domain Main Routers  
host3.your\_domain.com 192.168.112.1

**Last 6 Events**

Signature	Source	Destination
P-1-WEB-IS cmd.exe access	192.168.41.35	192.168.112.60
P-1-WEB-IS cmd.exe access	192.168.41.35	192.168.112.60
P-1-WEB-IS cmd.exe access	192.168.41.35	192.168.112.60
P-1-WEB-IS cmd.exe access	192.168.41.35	192.168.112.60
P-1-WEB-IS cmd.exe access	192.168.41.35	192.168.112.60
P-1-WEB-IS cmd.exe access	192.168.41.35	192.168.112.60

Events in the past: 1 Days #/Page: 60 TCP:  UDP:  ICMP:  Go

**Unique Events in the past 1 day**

Freq	Signature	Graph	Sensor
1939	WEB-IS cmd.exe access	1d · 1w · 4w	192.168.112.69
1502	spp_unicode: Invalid Unicode String detected	1d · 1w · 4w	192.168.112.69
1296	P-1-WEB-IS cmd.exe access	1d · 1w · 4w	192.168.112.69
1001	spp_unicode: Unicode Directory Traversal attack detected	1d · 1w · 4w	192.168.112.69

**Protocol Breakdown**





## LIDS (Linux Intrusion Detection System)

- GPL lisansı altında serbestçe dağıtılabilir/kullanılabilir
- Yalnızca Linux platformunda çalışmaktadır
- Sunucu Temelli / Saldırı İmzası Arama mimarisi ile çalışır
- Çeşitli kernel modülleri ve programlardan oluşur
- Kernel'a özeldir, her kernel için ayrı sürümü bulunmaktadır
- Sistem kaynaklarına erişimleri izleyebilir, engelleyebilir
- <http://www.lids.org> adresinden temin edilebilir



## LIDS Ayarları

**2** program ve **4** yapılandırma dosyası aracılığıyla yönetilir

### ● Yönetim Programları

- **lidsadm**
- **lidsconf**

**Yönetim Programı**

**Yapılandırma Programı**

### ● Yapılandırma Dosyaları

- **/etc/lids/lids.conf**
- **/etc/lids/lids.cap**
- **/etc/lids/lids.pw**
- **/etc/lids/lids.net**

**LIDS ACL yapılandırma dosyası**

**LIDS özellikleri dosyası**

**LIDS şifre dosyası**

**LIDS mail uyarı yapılandırma dosyası**

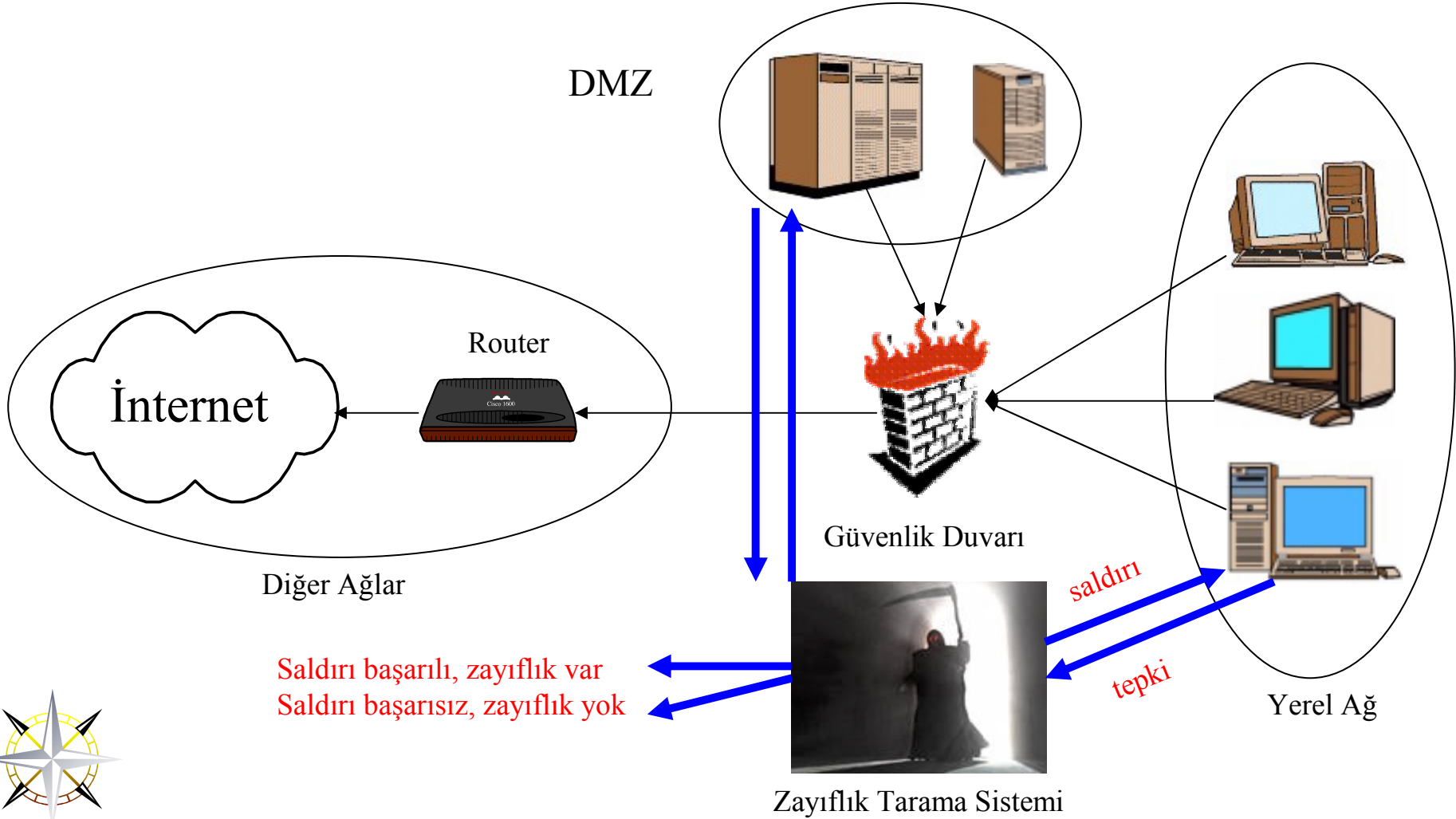


## Zayıflık Tarama Sistemleri

- **Yayınlanmış, bilinen uygulama ve sistem zayıflıklarını test eden araçlardır**
- **Veritabanlarında bulunan zayıflıkları hiçbir özel yöntem uygulamadan test etmektedirler**
- **Zaman içerisinde oluşabilecek zayıflıkları düzenli takip etmeyi sağlarlar**
- **Script dilleri sayesinde yeni zayıflıklar kolayca tanımlanabilir**
- **3 farklı mimaride çalışabilirler : Ağ Temelli, Uygulamaya özel ve Sunucu Temelli**



## Ağ Temelli Zayıflık Tarama Sistemi - Çalışma Yöntemi





## Nessus

- GPL lisansı altında serbestçe dağıtılabilir/kullanılabilir
- İstemci/Sunucu mimarisinde ve çok kullanıcıdır
- Sunucu Unix, Linux türevlerinde, İstemci ise her platformda çalışabilmektedir
- Zayıflık veritabanı İnternet'ten kolayca güncellenebilir
- Zayıflık tanımlama dili NASL veya C dili sayesinde özgün zayıflıkların ve eklentilerin yazılmasında mümkündür.
- Birçok sistemin zayıflığı aynı anda taranabilir
- <http://www.nessus.org> adresinden temin edilebilir

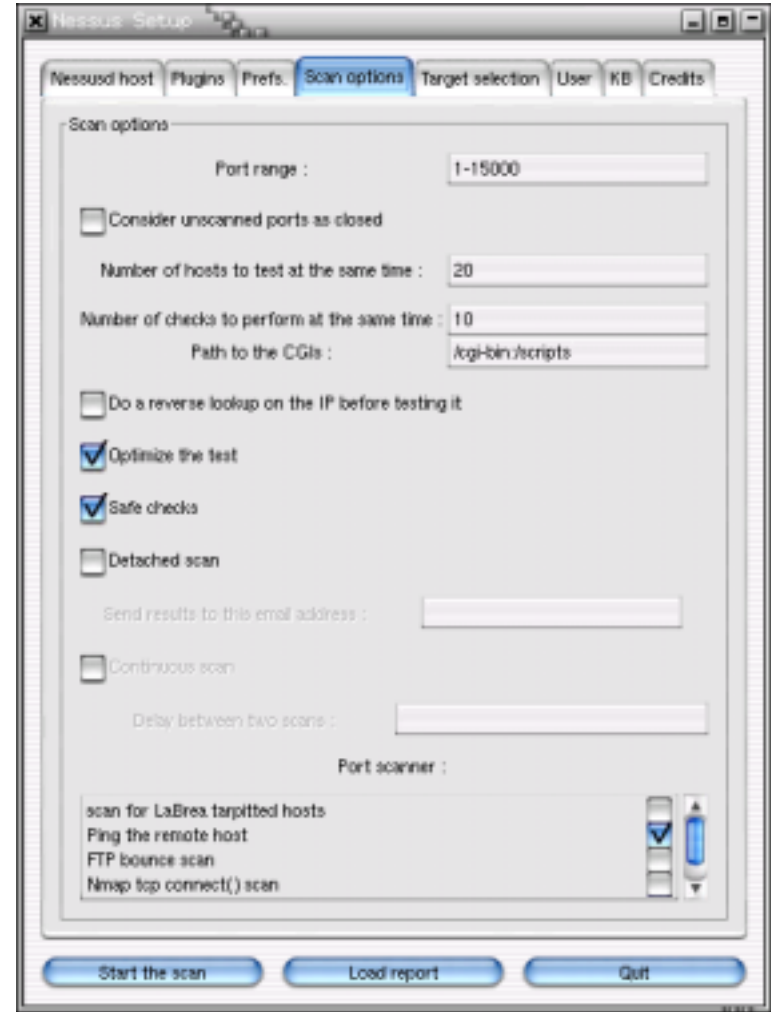
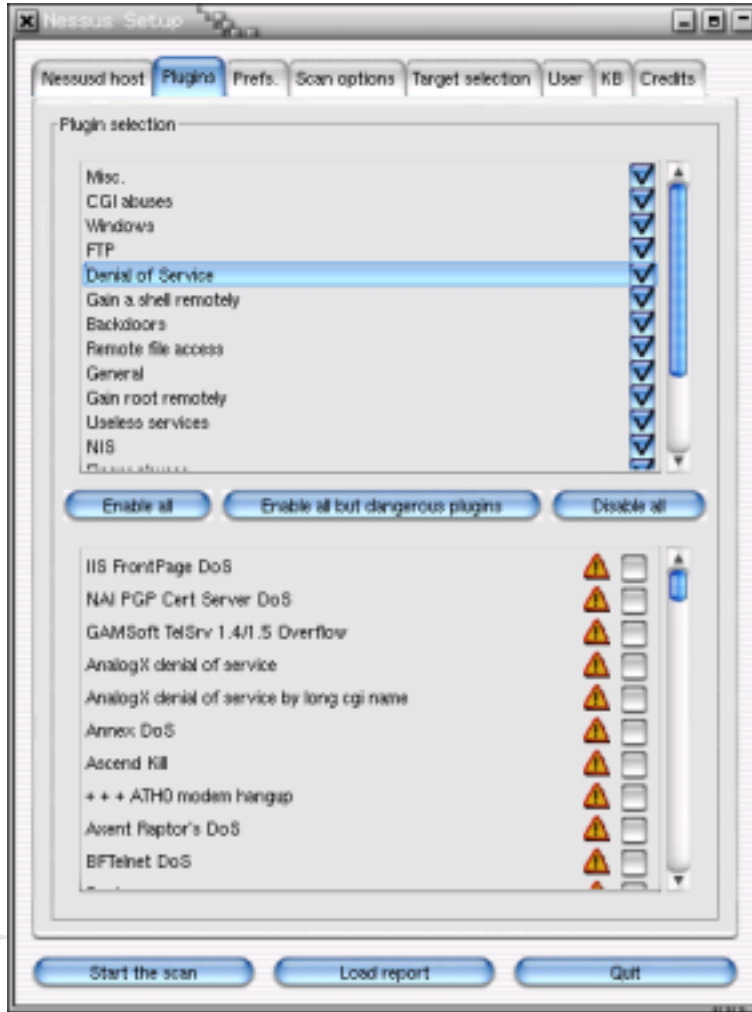


## Nessus - Özellikleri

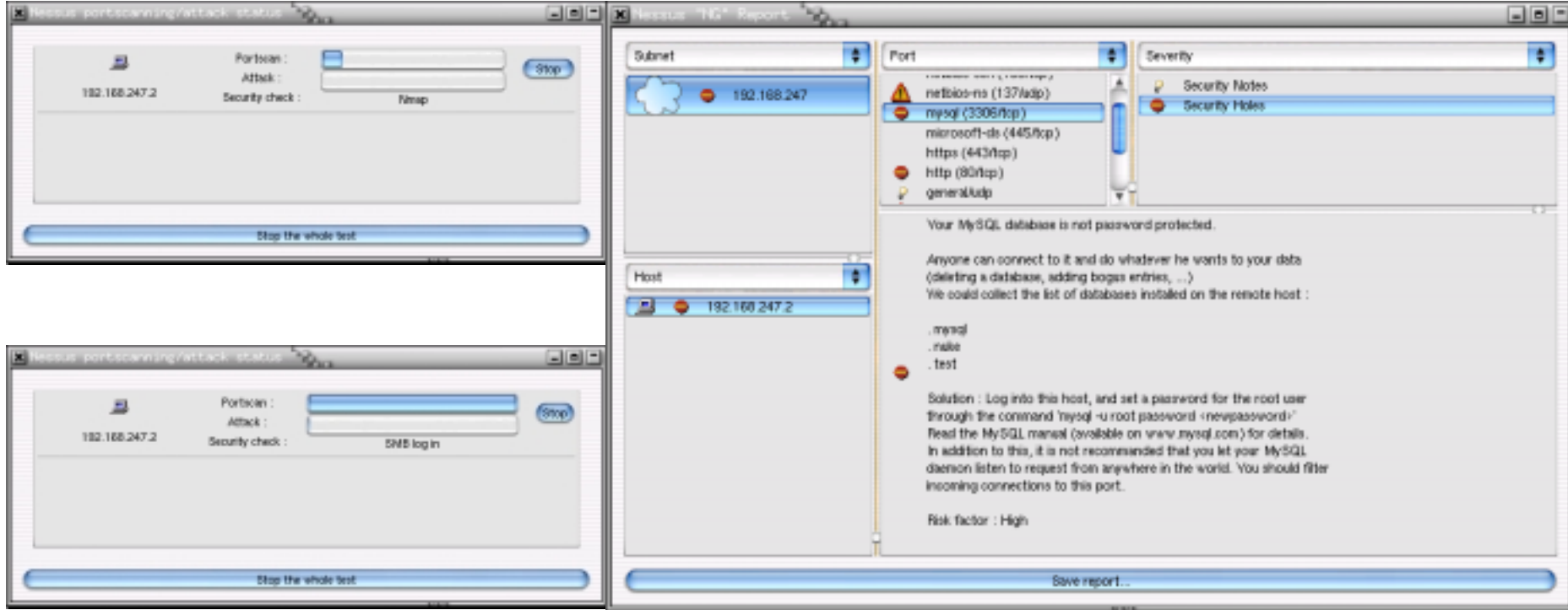
- Zayıflık veritabanı sürekli güncellenmektedir
- XML, HTML, NSR gibi formatlarda rapor sunmakta, raporlarda zayıflığın nasıl giderileceği ve referansları bulunmaktadır
- Taramalar arasında karşılaştırma yapabilmektedir
- NASL (Nessus Attack Scripting Language) dili ile özel saldırılar düzenlenebilmektedir
- İstemci – Sunucu iletişimini SSL ile şifreleyebilmektedir
- Nmap , Queso gibi programları kullanabilmek için eklentileri mevcuttur



## Nessus – Ekran Görüntüleri – 1



## Nessus – Ekran Görüntüleri – 2



The image displays two screenshots of the Nessus interface. The top-left screenshot shows the 'Nessus: portscanning/attack - status' window for host 192.168.247.2. It indicates that the 'Ports can' and 'Attack' fields are empty, and the 'Security check' is 'Nmap'. A 'Stop' button is visible. The bottom-left screenshot shows the same window, but the 'Security check' is now 'SMB log in'. The right-side screenshot shows the 'Nessus: "192" Report' window. It lists several ports with their severity levels: netbios-ns (137/tcp) is low, mysql (3306/tcp) is high, microsoft-ds (445/tcp) is medium, https (443/tcp) is medium, http (80/tcp) is medium, and general/tcp is low. A detailed security note for the MySQL database is highlighted, stating: 'Your MySQL database is not password protected. Anyone can connect to it and do whatever he wants to your data (deleting a database, adding bogus entries, ...). We could collect the list of databases installed on the remote host: .mysql, .nake, .test. Solution: Log into this host, and set a password for the root user through the command 'mysql -u root password <newpassword>'. Read the MySQL manual (available on www.mysql.com) for details. In addition to this, it is not recommended that you let your MySQL daemon listen to request from anywhere in the world. You should filter incoming connections to this port. Risk factor: High'. A 'Save report...' button is at the bottom.



## Nmap

- **GPL lisansı altında serbestçe dağıtılabilir/kullanılabilir**
- **Aktif olan Sistemleri ve Servisleri saptayabilir**
- **Gelişmiş işletim sistemi saptama özellikleri vardır**
- **Unix, Linux, Windows platformlarında çalışabilmektedir**
- **Identd, Rpc, ISN, Ftp Bounce ve DOS testleri ile çeşitli zayıflıkları saptayabilir**
- **Spoofing ve Decoy yapabilir**
- **Çeşitli zombi sistemleri kullanarak tarama yapabilir**
- **Bölünmüş paketler kullanabilir**
- **<http://www.nmap.org> adresinden temin edilebilir**

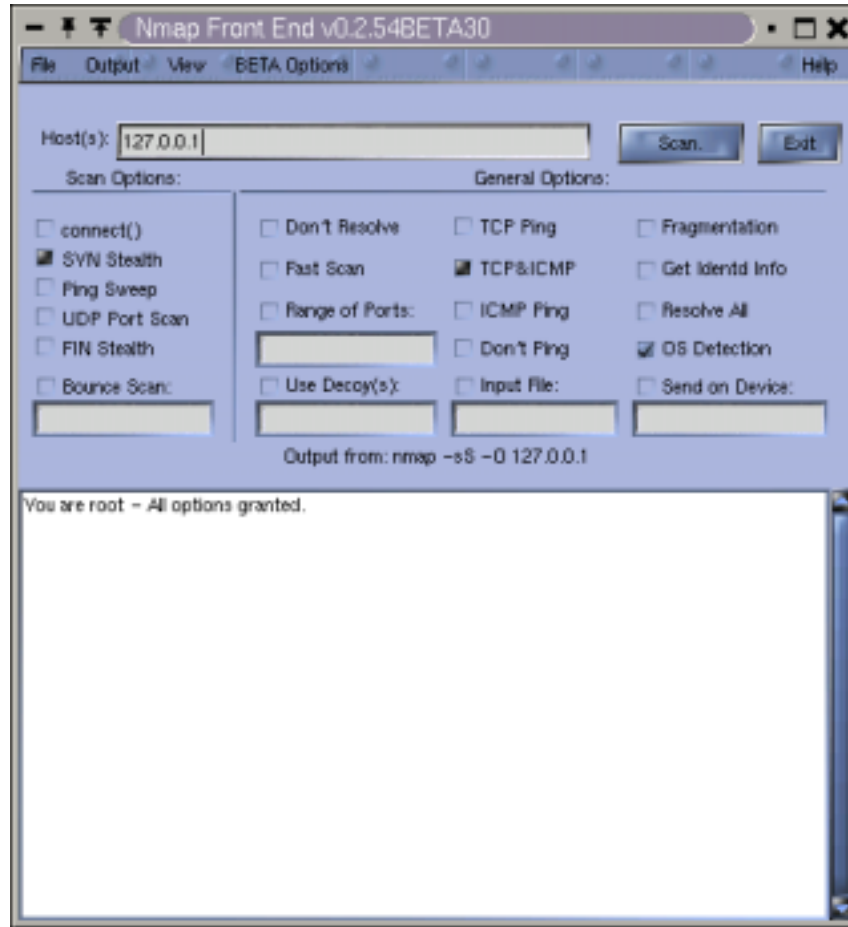


## Nmap – Tarama Seçenekleri

- -sT TCP Connect Scan
- -sS SYN Scan
- -sF FIN Scan
- -sU UDP Scan
- -sX Xmass Tree Scan
- -sN Null Scan
- -sP Ping Scan
- -sR RPC Scan
- -I Identd Scan
- -S Source IP
- -O Tcp/Ip Fingerprinting
- -b <ftp relay host> Bounce FTP Scan
- -Po/-PT/-PS/-PI/-PB Ping Seçenekleri



## Nmap Grafik Arayüzü



## Şifreleme

- İnternet ortamında verilerin güvenli şekilde aktarımını, bütünlüğünü ve gönderenin doğruluğunu sağlamaktadırlar
- Mail, Dosya, Disk ve Veri trafiğini şifreleyebilmektedirler
- Des, MD5, 3Des, Sha-1 gibi çeşitli algoritmalar kullanmaktadırlar





## Gnu Privacy Guard (GPG)

- GPL lisansı altında serbestçe dağıtılabilir/kullanılabilir
- PGP şifreleme ve doğrulama için kullanılmaktadır
- Dosya ve mail şifreleme için PGP'nin desteklediği standartları desteklemektedir
- Özel ve Genel anahtarların yönetilmesi, üretilmesi, şifreleme, doğrulama gibi işlemlerde kullanılmaktadır
- Pine, Mutt, Kmail, Sylpheed, Evolution, Outlook Express ve Eudora mail istemcileri ile kullanılabilir
- Gnu Privacy Assistant (GPA) , X Privacy Guard (XPG) ve Gnome PGP (GPGP) gibi arabirimleride bulunmaktadır
- <http://www.gnupg.org> adresinden temin edilebilir



## GPG – Desteklediği Algoritmalar

- **Cipher: 3DES, CAST5, BLOWFISH, RIJNDAEL, RIJNDAEL192, RIJNDAEL256, TWOFISH**
- **Public key: RSA, RSA-E, RSA-S, ELG-E, DSA, ELG**
- **Hash: MD5, SHA1, RIPEMD160**





## GPG – Şifrelenmiş Bir Metin

-----BEGIN PGP MESSAGE-----

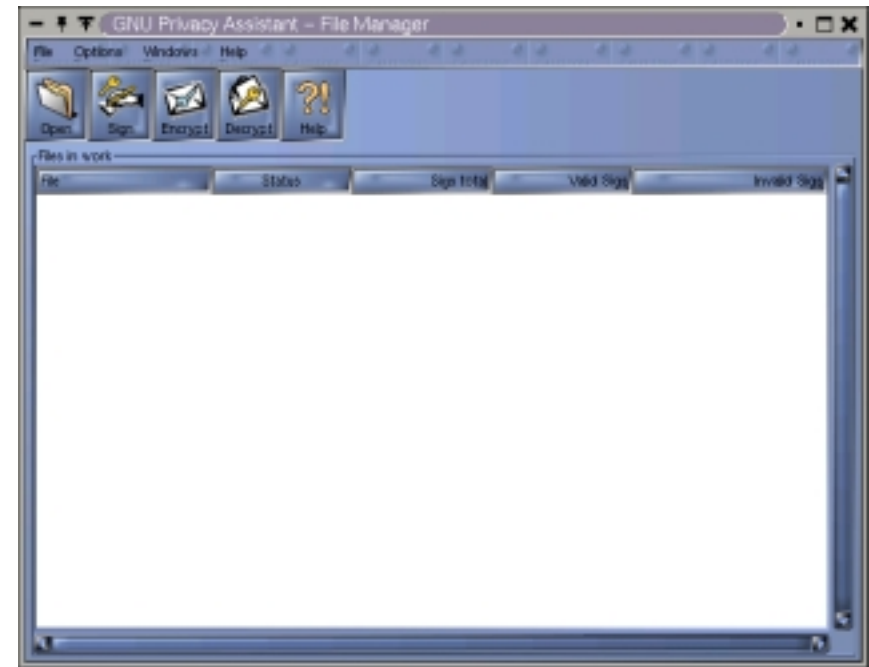
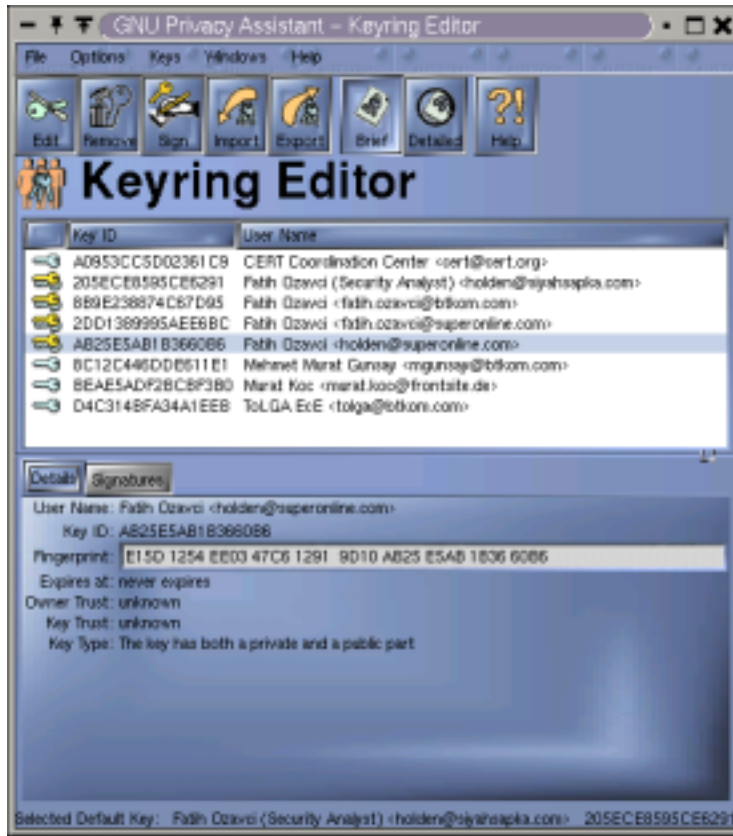
Version: GnuPG v1.0.4 (GNU/Linux)

Comment: Gnome PGP version 0.4

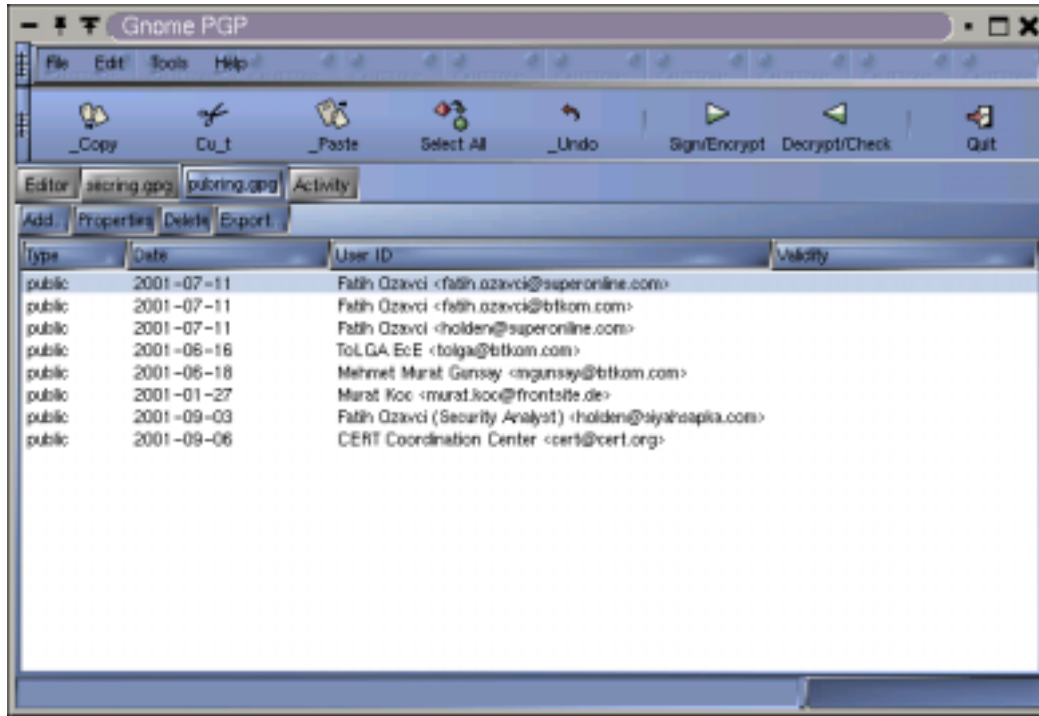
hQIOA7HMZGc8Py7SEAf/eWVrPAF/k75uWRthVdsQcy7e725F2cl5kQDlDl44/KdP  
vyaCEMd+4eVqEh3Ao3PmdGzAc31KGLA56sWPYySk4f7YlbyRF8bLL1odZNa3Mbwu  
BomH6vsUDmgMAoSSvTn3ckWNaDaVjXMn1RFD+1yzrs/hCoBzTMx12aH628JE+qeg  
KG9fRununsabmV3a29uaZKSaxkyXIBMVms7E377SEuiDj+Q4+xjqVL49v8u9nWci  
EaUovJEcrJVDBEfP/575jc6DJZZ9I448nK5IHHpV6808s+xwZ7GESGHfLUcoBPcn  
HOuUC7I9o2dry+zFDT9aIsWGtPL9nSMJ1fSGNbpkLQf9Hybi96v8QEp8F+8bomHs  
qEfsuMlxWRsMtNNj3gc3YAZquiUGDqcUD58uOssUqe/vdE6LaTV99rPThI2zf3ro  
sMe7U9CmvFa6hoYkkAt6hoLdkDkM+1XzVNuyibvsWSOez3fko9BJ+YUOLNvTgWwO  
rTIX6c+f2tObTk9P3jzzu9qy2GVgV8zajd23Bh12JTlygBhOa4WivYibVvCNHu3n  
DdpqO9WaSVWSsKyE9wLYxM90Wz3cVjFeNd2ZQsIxoxZv+1yTyyIR1nOpz5MjuGrZ  
WPLVThjfUUEAbOsqF2MhIEWoXH+j25DWgUrjnKoCxPKC1TR3hX8yHhGPglow+MFH  
LNKRADJ5uOqgd3ET6NfV5x2gFaW2Bn/fta024Z1P4IEQ/dis3M8QW/71Z5CZ7/8w  
MUREmJiEaWc6YOxahWO/2D3i5DflM2dArDRu4c9hXIA5+dwyxewEKerGUvb1X5Xo  
9ZFGULUtWKXC7ZzoODxvIQvCUBO+nMUD/lo4OAPDxWrHKHE7lDhpCBGxa/ja/9fD  
XtwrvA==  
=nDBS  
-----END PGP MESSAGE-----



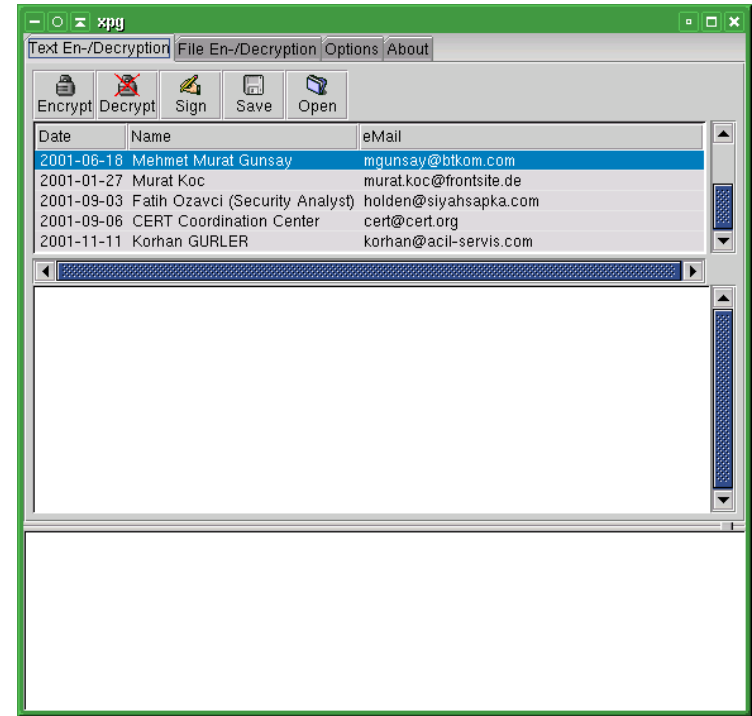
## Gnu Privacy Assistant



## Gnome PGP



## X Privacy Guard





## Hardening (Sistem Güçlendirme)

İşletim sistemi veya uygulamaların ayarlarının değiştirilmesi, bazı yamalarının uygulanması, potansiyel zayıflıklarının giderilmesi ve bir güvenlik politikası çerçevesinde yapılandırılması işlemlerinin tümüne “**hardening**” denilmektedir.





## Bastille-Linux (Hardening Scriptleri)

- GPL lisansı altında serbestçe dağıtılabilir/kullanılabilir
- Redhat ve Mandrake Linux sistemlerinin hardening işlemi için geliştirilmiştir
- Perl script'lerinden oluşur (Çeşitli özelleştirmeler ve diğer dağıtımlara uygulama imkanı bu sebeple bulunmaktadır)
- Yeni sürümünde TK Grafik arayüzde eklenmiştir
- <http://www.bastille-linux.org> adresinden temin edilebilir



## Bastille-Linux (Yapılandırma Seçenekleri)

- Güvenlik duvarı kurallarının oluşturulması
- Önemli dosyaların yetkilerinin kontrol edilmesi ve düzenlenmesi
- Hesap yönetiminde çeşitli politikalar uygulanmasının sağlanması
- Açılış ile ilgili güvenlik önlemlerinin sağlanması
- Çeşitli komutların pasif hale getirilmesi
- Bazı servislerin düzenlenmesi (DNS, Apache, Identd)
- TMP dizini ile ilgili yetki problemlerinin düzenlenmesi





## Bastille-Linux – Arayüz

**Modules**

- Title Screen
- Firewall
- FilePermissions
- AccountSecurity
- BootSecurity
- Securelnetd
- DisableUserTools
- ConfigureMiscPAM
- Logging
- MiscellaneousDaemons
- DNS
- Apache
- Printing
- FTP
- TMPDIR
- End Screen

**Question**

**Explanation**

(Tk User Interface)

v1.2.0.prerelease

Please answer all the questions to build a more secure system.

The Next and Back buttons navigate forward and backward in the questions database. Changes made in the Answer field are \*only\* saved when you push the Next button! The "modules" in the questions database are listed to the left. You can jump to the start of any module simply by clicking on its name.

Some questions have two levels of explanatory text, which you can adjust with the Explain Less/More button.

Please address bug reports and suggestions to [jay@bastille-linux.org](mailto:jay@bastille-linux.org)  
Bugs in the Tk user interface are the fault of [allenp@nwlinc.com](mailto:allenp@nwlinc.com).

**Answer**

**Back** **Next** **Explain Less**



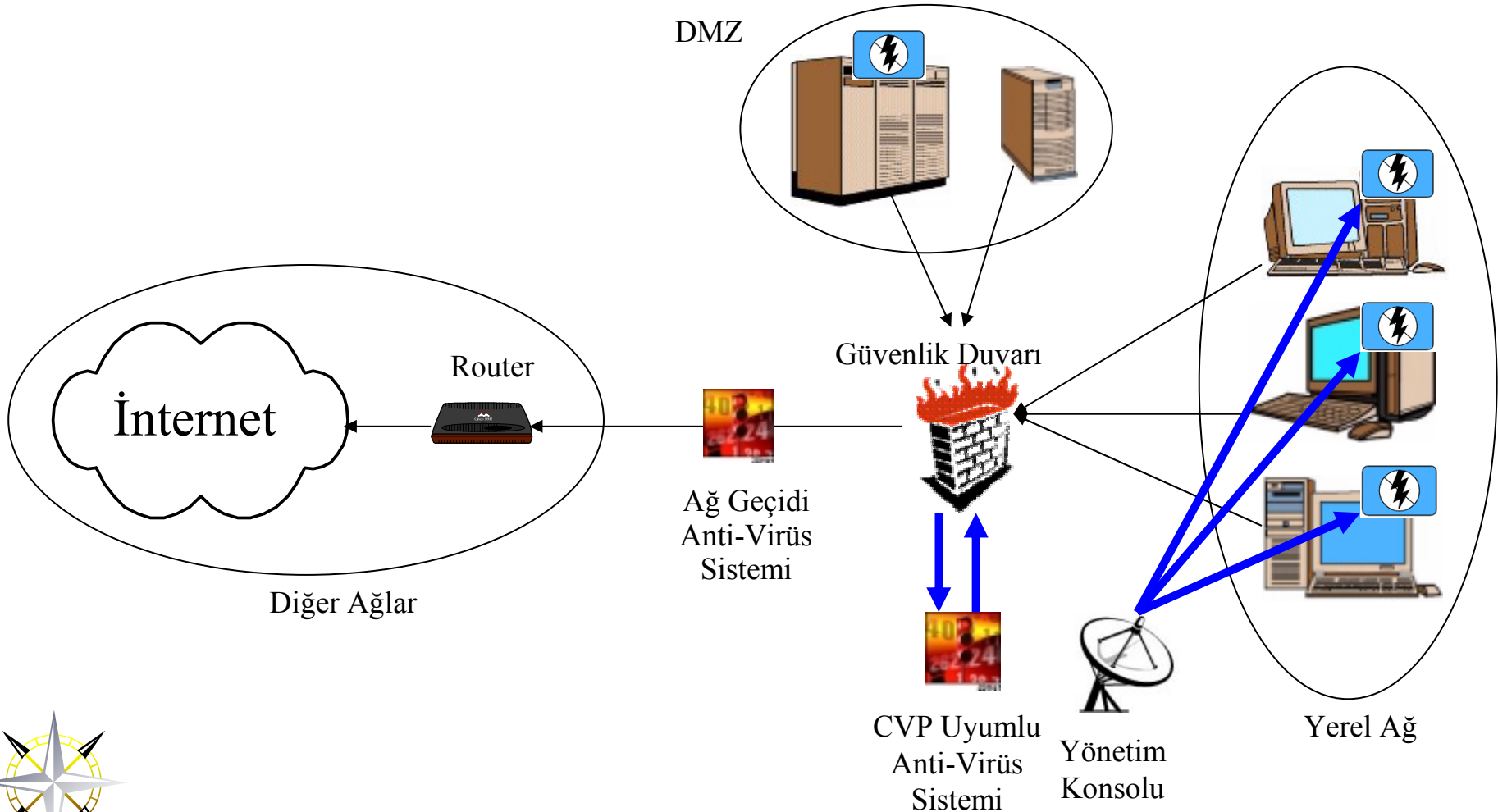


## Anti-Virüs Sistemleri

- **Virüs, Worm ve Truva Atlarını tanımlı imzaları ile saptarlar**
- **İmzaları tanımlanmamış virüsleride çeşitli yöntemler ile saptayabilen örnekleri mevcuttur**
- **Virüs imzaları bir veritabanında tutulur ve İnternet aracılığıyla düzenli olarak güncellenir**
- **Ağdaki tüm sistemleri korumadıkça anlamlı değildir**
- **Bir ağ parçasını, belirli bir trafiği, bir sunucu yada bir istemciyi koruyabilirler**



## Anti-Virüs Sistemleri Örnek Yerleşimi



## Amavis

- E-posta geçididir, Anti-Virüs değildir
- Perl ile yazılmış scriptler topluğudur
- Sendmail, Qmail, Exim ve Postfix ile çalışır
- E-postaların eklerini inceler ve geçici bir dizine kaydeder, daha sonra Anti-Virüs programına göndererek, virüs bulunmuyorsa hedefe ulaştırır
- Çeşitli sıkıştırma formatlarında desteklemektedir
- <http://www.openantivirus.org> adresinden Unix'ler için çeşitli Anti-Virüs yazılımları indirilebilir
- <http://www.amavis.org> adresinden temin edilebilir





# Özgür Güvenlik Yazılımları

## **Amavis – Desteklediği Anti-Virüs Sistemleri**

**Network Associates Virus Scan**

**DrSolomon (obsolete)**

**H+BEDV AntiVir/X**

**Sophos Sweep**

**Kaspersky Lab AntiViral Toolkit Pro (AVP)**

**CyberSoft VFind**

**Trend Micro FileScanner**

**CAI InoculateIT**

**F-Secure Inc. (former DataFellows) F-Secure AV**



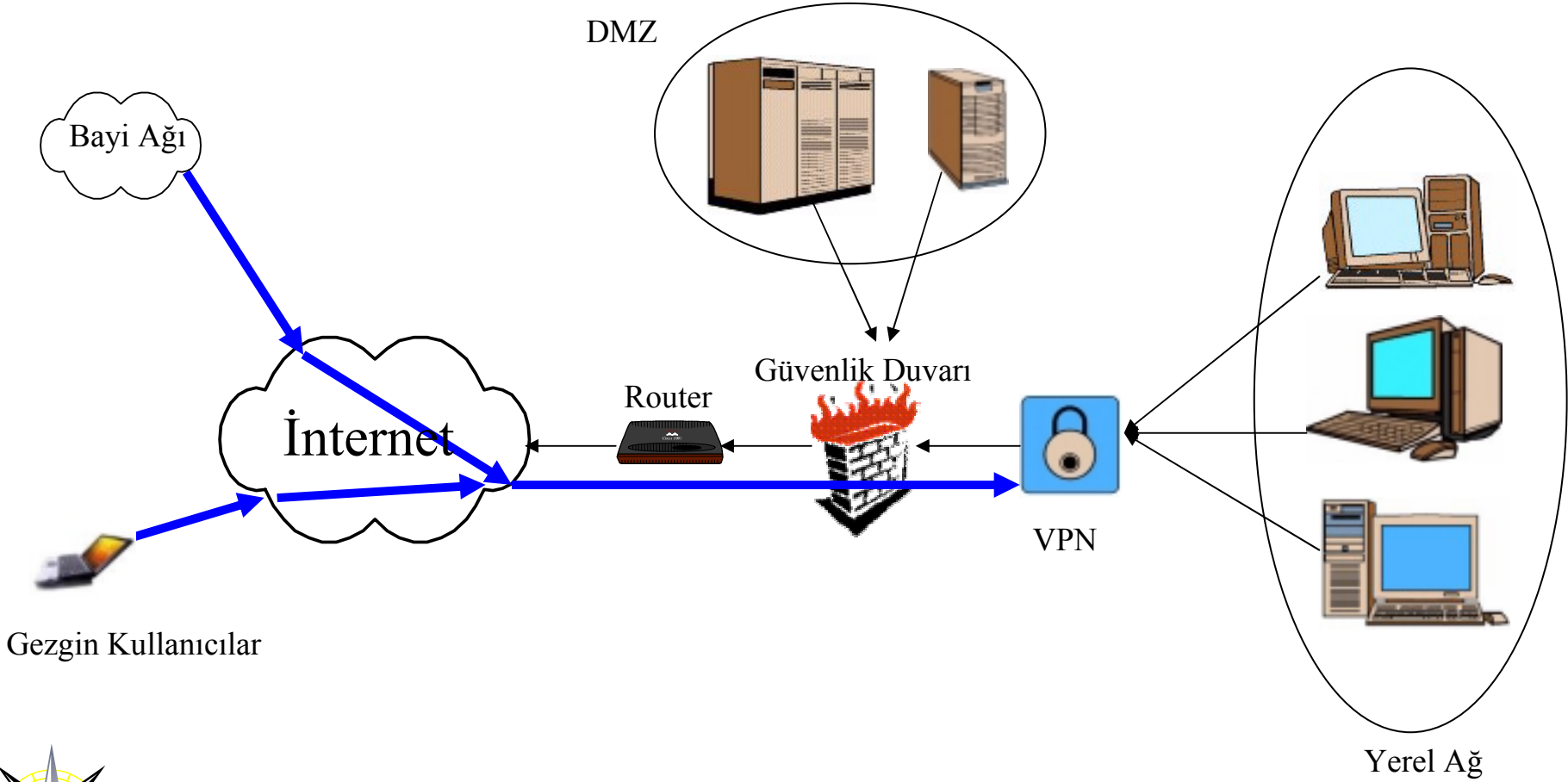


## Sanal Özel Ağ Sistemleri (VPN)

- **Birden fazla sistem veya ağın, güvensiz ağlar üzerinden, güvenli iletişimini sağlayan ağ bileşenleridir**
- **Donanım ve yazılım olarak bulunabilirler**
- **IPSec, PPTP, L2TP, SSH gibi protokolleri kullanarak iletişimin şifrelenmesini sağlarlar**
- **Harici onaylama sistemleri ile beraber kullanılmaları önerilmektedir**



## Sanal Özel Ağ Sistemleri Örnek Yerleşimi



## FreeS/Wan

- IPsec uyumlu sanal özel ağlar kurulması için oluşturulmuş bir yazılımdır
- Linux x.509 ve diğer PKI sertifikalarını destekler (Henüz Radius, SecureID gibi doğrulama sistemlerini desteklemiyor)
- Çeşitli yamalar ile ek desteklerde sağlanmaktadır (PGPnet ile kullanılabilirlik gibi...)
- Linux kernel modülleri ve yazılımlar olmak üzere 2 bölümden oluşur
- 3DES şifrelemeyi desteklemektedir (DES şifreleme algoritmasını desteklemiyor)
- <http://www.freeswan.org> adresinden temin edilebilir.





# Özgür Güvenlik Yazılımları

## FreeS/Wan – Desteklediği İstemciler

- **F-Secure VPN+**
- **Checkpoint SecureRemote VPN-1 4.1**
- **IRE SafeNet SoftPK**
- **Xedia's AccessPoint QVPN "Client" or "Builder"**
- **Lucent**
- **Ashleylaurent**
- **Diğer IPSec uyumlu VPN istemcileri**





## Tümleşik Sistemler

**Güvenliğe özel, çeşitli dağıtımlar oluşturulmaktadır, bu dağıtımlar hepsi birarada tarzında çözümler üretmeyi hedeflemektedirler. Bu tarz dağıtımlar ; Sanal özel ağ sistemi, Güvenlik duvarı, Saldırı tespit sistemi, Zayıflık tarama sistemi, zayıflık tarama ve ağ izleme için ek yazılımları birarada içermektedirler.**





# Özgür Güvenlik Yazılımları

## Trinux

- 1998 yılında geliştirilmeye başlamıştır
- Özel paket yapısı ile İnternette ve diğer disk bölümlerinden yazılım yüklenebilir
- 1 CD yada 3 disketten oluşmaktadır
- Çeşitli kategorilerde yazılımları barındırır
  - Ağ izleme ve Sniffer (Dsniff, p0f, Hunt, Fragrouter, Ettercap)
  - Ağ Haritalama ve Güvenlik İnceleme (Arping, Winscan)
  - Saldırı Tespiti (Snort, Pakemon, Despoof, Iplog)
  - Paket Üretme (Hping, NASL, Sing, Nemesis, Isic)
  - Proxy ve Tünelleme (Httpstunnel, Tunnel, Redir)
  - Şifreleme Yazılımları (FreeS/Wan, Openssl, Openssh, GPG)
  - İnternet Yardımcıları (Links, Curl, Webfsd(web sunucusu))
  - Script Dilleri (Perl, PHP)
- <http://trinux.sourceforge.net> adresinden temin edilebilir





# Özgür Güvenlik Yazılımları

## Neden Özgür Güvenlik Yazılımları Tercih Edilmeli ?

- Hataları herkes tarafından kısa sürede farkedilebilir ve giderilebilir
- Genelde ücretsizdirler ve bütçenin kısıtlı olduğu durumlar için idealdirler
- Kaynak kodlarında her türlü arka kapı ve art niyetli kod kolayca farkedilebilir
- İstenildiği oranda özelleştirilip, ekleme ve çıkarmalar yapılabilir
- Ticari ürünler kadar başarılı örnekler vardır
- Dünya çapında birçok kuruluş güvenlik çözümlerini açık kodlu ücretsiz ürünlerle sağlayarak %99 güvenlik sınırını yakalamakta ve maliyetlerini minimumda tutmaktadır
- Kişisel veya kurumsal, araştırma, geliştirme ve deneme ortamları için idealdirler





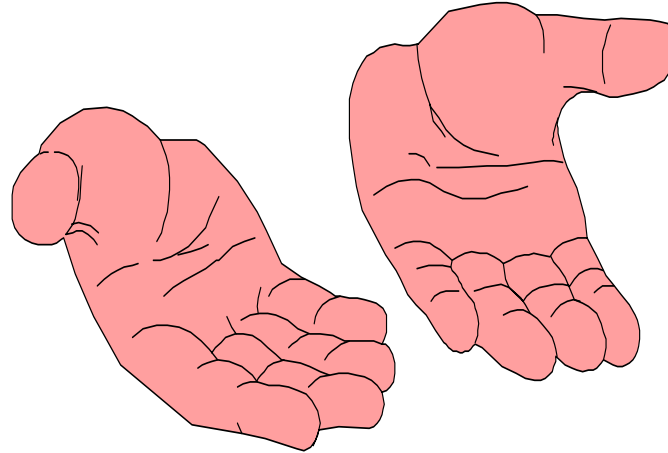
# Özgür Güvenlik Yazılımları

## Daha Fazla Bilgi İçin Kaynaklar

<b>CERT</b>	– <a href="http://www.cert.org">http://www.cert.org</a>
<b>SANS</b>	– <a href="http://www.sans.org">http://www.sans.org</a>
<b>Security Focus</b>	– <a href="http://www.securityfocus.com">http://www.securityfocus.com</a>
<b>Siyah Şapka</b>	– <a href="http://www.siyahsapka.com">http://www.siyahsapka.com</a>
<b>Nessus</b>	– <a href="http://www.nessus.org">http://www.nessus.org</a>
<b>Nmap</b>	– <a href="http://www.insecure.org/nmap">http://www.insecure.org/nmap</a>
<b>Snort</b>	– <a href="http://www.snort.org">http://www.snort.org</a>
<b>GPG</b>	– <a href="http://www.gnupg.org">http://www.gnupg.org</a>
<b>Iptables</b>	– <a href="http://netfilter.samba.org/">http://netfilter.samba.org/</a>
<b>GPA</b>	– <a href="http://www.gnupg.org/gpa.html">http://www.gnupg.org/gpa.html</a>
<b>Gnome PGP</b>	– <a href="http://www.geocities.com/SiliconValley/Chip/3708/gpgp/gpgp.html">http://www.geocities.com/SiliconValley/Chip/3708/gpgp/gpgp.html</a>
<b>ACID</b>	– <a href="http://www.cert.org/kb/acid">http://www.cert.org/kb/acid</a>
<b>Demarc</b>	– <a href="http://www.demarc.org">http://www.demarc.org</a>
<b>Fwbuilder</b>	– <a href="http://www.fwbuilder.org">http://www.fwbuilder.org</a>
<b>Bastille-Linux</b>	– <a href="http://www.bastille-linux.org">http://www.bastille-linux.org</a>
<b>FreeS/Wan</b>	– <a href="http://www.freeswan.org">http://www.freeswan.org</a>
<b>Amavis</b>	– <a href="http://www.amavis.org">http://www.amavis.org</a>
<b>LIDS</b>	– <a href="http://www.lids.org">http://www.lids.org</a>
<b>Trinix</b>	– <a href="http://trinix.sourceforge.net">http://trinix.sourceforge.net</a>



## Sorular ?





Özgür Güvenlik Yazılımları

Teşekkürler ....





# Özgür Güvenlik Yazılımları

**Fatih Özavcı - Security Analyst**

**holden@siyahsapka.com**

**<http://www.siyahsapka.com>**

