



Nessus Güvenlik Denetim Sistemi

Fatih Özavcı
IT Security Consultant

fatih.ozavci@infosecurenet.com

holden@siyahsapka.com

<http://www.siyahsapka.com>

Sunum İeriđi

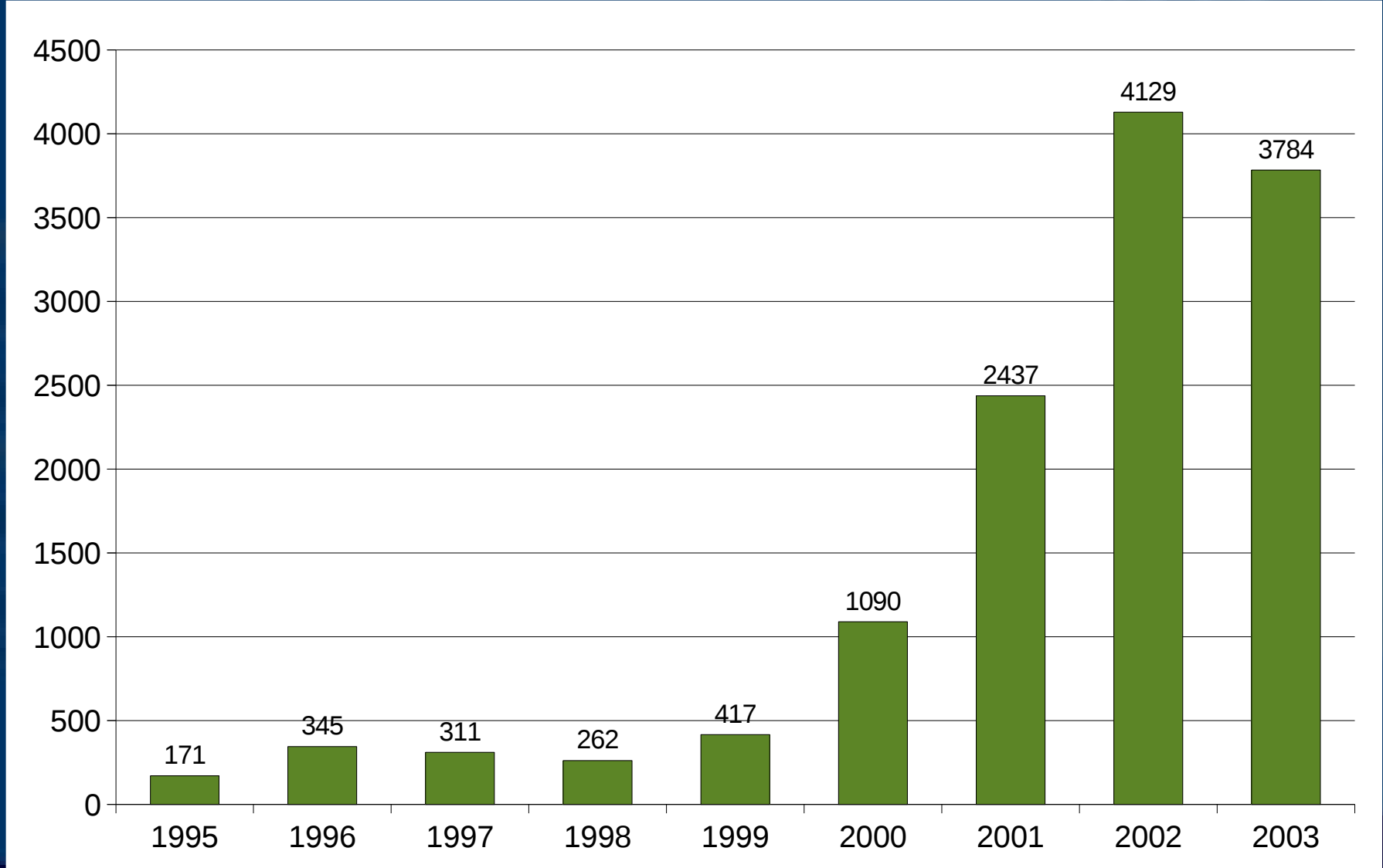
- Saldırı ve Zayıflıkların Gelişimi
- Güvenlik Denetim Sistemi Tanımı ve Gerekliliđi
- Nessus Zayıflık Tarama Sistemi
 - Tanıtım
 - Kurulum
 - Ayarlar ve Örnek Taramalar
 - Rapor İncelemeleri



Güvenlik Açığı Kavramı

- Kötü Programlama veya Tasarımdan kaynaklanabilir
- Bir donanım, uygulama, işletim sistemi, ağ tasarımı veya iletişim protokolünde bulunabilir
- Düzenlenen erişim yetkilerinin aşılmasına, gözardı edilmesine veya kötüye kullanılabilmesine sebep olur
- Bulunduğu sistemin işleyiş sürecini aksatabilir

Yayınlanan Güvenlik Açıklarının Yıllara Dağılımı – CERT/CC



Güvenlik Denetim Sistemleri

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

Ağ Temelli Güvenlik Denetim Sistemi Çalışma Yöntemi



Nessus Güvenlik Denetim Sistemi

- GPL lisansı altında serbestçe dağıtılabilir/kullanılabilir
- “<http://www.nessus.org>” adresinden temin edilebilir
- İstemci – Sunucu iletişimini SSL ile şifreleyebilmektedir
- İstemci/Sunucu mimarisinde ve çok kullanıcıdır
- Sunucu Unix, Linux türevlerinde, istemci ise her platformda çalışabilmektedir
- Güvenlik açığı veritabanı İnternet’ten kolayca güncellenebilir
- Güvenlik denetimi tanımlama dili NASL veya C dili sayesinde özgün güvenlik açıkları ve eklentilerin yazılması mümkündür.
- Birçok sisteme aynı anda güvenlik denetimi yapabilir

Nessus Güvenlik Denetim Sistemi

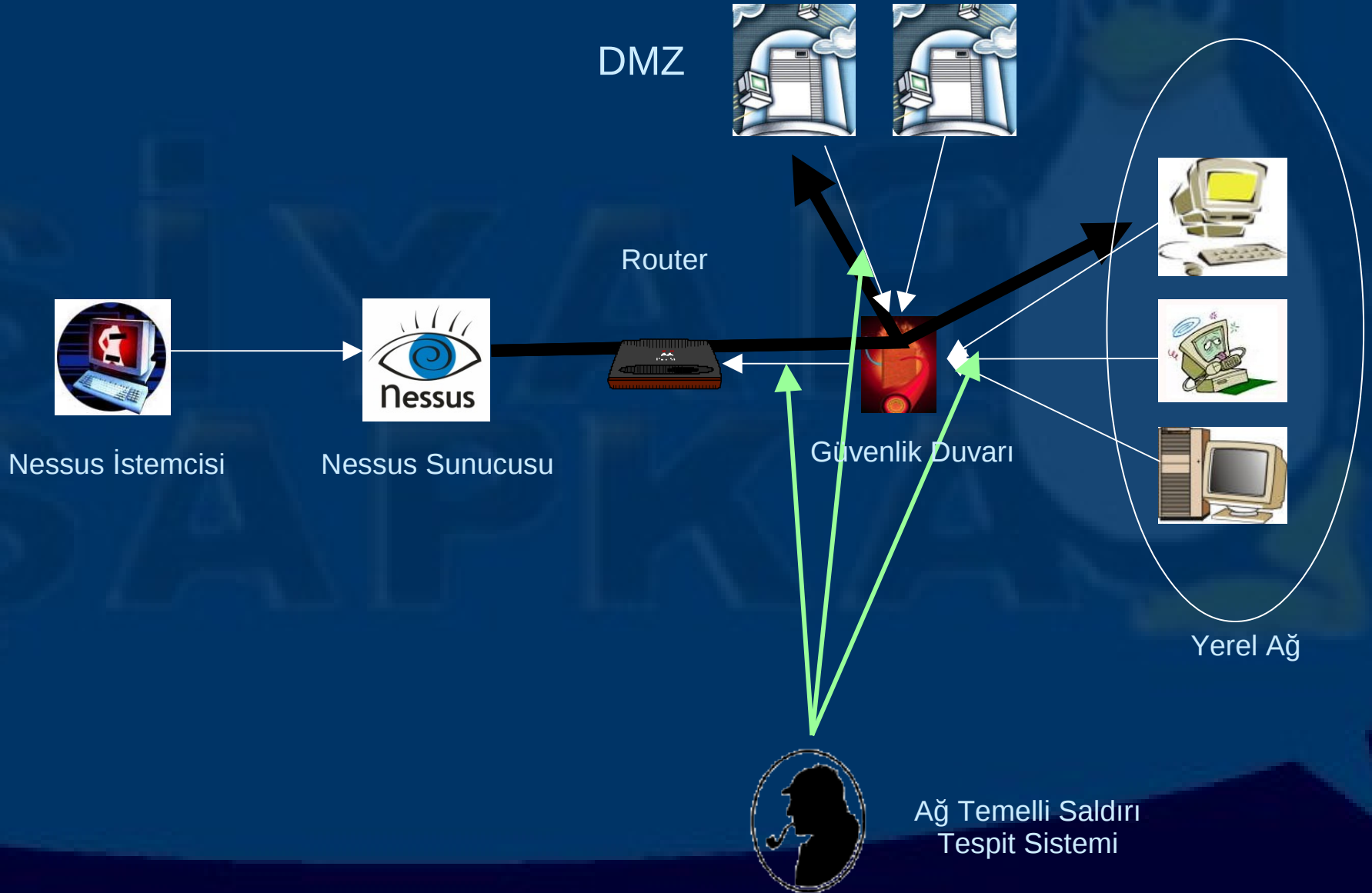
- Güvenlik açığı veritabanı sürekli güncellenmektedir
- XML, HTML, NSR, PDF formatında rapor sunmakta, raporlarda açığın nasıl kapatılabileceği ve referansları bulunmaktadır
- Denetimler arasında karşılaştırma yapabilmektedir
- Denetim sonuçlarını SQL veritabanlarına kayıt edebilir
- NASL (Nessus Attack Scripting Language) dili ile özel güvenlik denetimleri tanımlanabilmektedir
- Snort saldırı tespit sistemi ile beraber saldırı tespit kalitesini arttırabilir
- Nmap, Queso, WPoison ve Nikto gibi programları kullanabilmek için eklentileri mevcuttur
- “Ağ Temelli Saldırı Tespit Sistemleri”ni analiz edebilmektedir

Nessus Güvenlik Denetim Sistemi

Eksiklikler

- Kritik sunuculara yüklenebilecek yardımcı ajanlar ile sunucuda yerel zayıflık taramalarında yapabilmek
- Yardımcı ajanlar ile sunucuda bulunan zayıflıkları otomatik olarak düzeltebilmek
- Yapay zekaya sahip değildir, bu sebeple sadece tanımlanmış zayıflıkları bulabilmektedir
- Denetimi yapılacak ağda değişiklikler gerektirmemektedir; ancak verimli kullanım için değişiklikler gerekebilir
- Ağdaki paket kayıpları ve yanlış sunucu mesajları hatalı raporlar üretilmesine sebebiyet vermektedir

Nessus Zayıflık Tarama Sistemi Çalışma Yöntemi



Nessus ve Diğer Güvenlik Denetim Sistemleri Karşılaştırması – Network Computing

Vulnerability Scanner Features

	Axent Technologies NetRecon 3.0 + SU7	BindView HackerShield	eEye Digital Security Retina	Internet Security Systems Internet Scanner	Nessus Security Scanner	Network Associates CyberCop Scanner	SARA	World Wide Digital Security SAINT
Price	Starts at \$1,995	\$19.95 per IP scanned	Starts at \$1,145	Starts at \$2,795	Free	\$32 per node, \$2,252 server	Free	Free (report generator starts at \$100)
Platform	Windows NT	Windows NT	Windows NT	Windows NT Workstation	Unix	Windows NT	Unix	Unix
Built-in automatic signature update feature	● (download from Web)	●	●	●	● (download from Web)	●	○	○
Scans for host vulnerabilities	○	●	●	●	○	●	○	○
CVE cross-references	○	●	○	●	●	○	●	●
Automatic fixing of select vulnerabilities	○	●	●	○	○	●	○	○
Open source	○	○	○	○	●	○	●	●
Command-line automation	○	○	○	●	●	●	●	●
Integrates with a data- management suite	● (Enterprise Security Manager)	○	○	● (ISS SafeSuite)	○	● (Security Management Interface)	○	○
Capable of custom security checks	○	○	○	○	● (NASL)	● (CASL)	●	●

● Yes ○ No

Nessus Zayıflık Tarama Sistemi – Sürümler

- Güncel Sürüm : 2.0.10a
- Kurulum dosyaları
 - [nessus-libraries-2.0.10a.tar.gz](#)
 - [libnasl-2.0.10a.tar.gz](#)
 - [nessus-core-2.0.10a.tar.gz](#)
 - [nessus-plugins-2.0.10a.tar.gz](#)



Nessus Zayıflık Tarama Sistemi Kurulum

- Nessus Libraries
 - tar zvxvf nessus-libraries-2.0.10a.tar.gz
 - configure --enable-cipher --with-ssl=/usr/lib/
 - make ; make install
- NASL
 - tar zvxvf libnasl-2.0.10a.tar.gz
 - configure ; make ; make install
- Nessus Core
 - tar zxfv nessus-core-2.0.10a.tar.gz
 - ./configure --enable-save-kb --enable-gtk --enable-save-sessions
 - make ; make install
- Nessus Plugins
 - tar zxfv nessus-plugins-2.0.10a.tar.gz
 - configure --with-fetchcmd=wget ; make ; make install

Nessus Zayıflık Tarama Sistemi Alternatif Kurulum

Debian

- `apt-get install nessus*`

Otomatize Kurulum

- `nessus-installer.sh`

Dağıtıma Özel Kurulum

- web sitesinde rpm paketleri veya diğer paketler bulunabilir



Nessus Zayıflık Tarama Sistemi Programlar

\$prefix/bin/nessus

Nessus istemcisini çalıştırır.

\$prefix/bin/nessus-build

C kaynak kodlarından NASL script'leri oluşturur.

\$prefix/bin/nessus-config

Derleme sırasında belirlenen linkleri ve seçenekleri gösterir.

\$prefix/bin/nessus-mkrand
kullanılabilecek

Sertifika üretimi veya zayıflık denetimi sırasında rastgele byte'lar üretir.

\$prefix/bin/nasl

NASL yorumlayıcısıdır, scriptlerinin çalıştırılmasını sağlar.

\$prefix/bin/nasl-config

Derleme sırasında belirlenen linkleri ve seçenekleri gösterir.

\$prefix/sbin/nessus-adduser

Nessus sunucusuna kullanıcı tanımlamak için kullanılır.

\$prefix/sbin/nessus-mkcert

Nessus sunucusu için SSL sertifikası üretir.

\$prefix/sbin/nessus-mkcert-client

Nessus istemcisi için SSL sertifikası üretir.

\$prefix/sbin/nessus-nessusd

Nessus sunucusunu başlatmak için kullanılır.

\$prefix/sbin/nessus-rmuser

Nessus sunucusundan kullanıcı silmek için kullanılır.

\$prefix/sbin/uninstall-nessus

Nessus yazılımını kaldırmak için kullanılır.

\$prefix/sbin/nessus-update-plugins

Zayıflık tanımlamalarını ve diğer eklentileri internet üzerinden güncellemek için kullanılır.

Nessus Zayıflık Tarama Sistemi

Kullanıcı Ekleme #1

```
# nessus-adduser
```

Please see the `nessus-adduser(8)` man page for the rules syntax

```
Using /var/tmp as a temporary file holder
```

Enter the rules for this user, and hit ctrl-D once you are done :
(the user can have an empty rules set)

```
Add a new nessusd user
```

```
Login      : holden  
Password   : deneme  
DN         :  
Rules      :  
Is that ok ? (y/n) [y] y
```

```
Login : holden
```

```
Authentication (pass/cert) [pass] : pass
```

```
Login password : deneme
```

```
User rules
```

```
user added.
```

nessusd has a rules system which allows you to restrict the hosts

that holden has the right to test. For instance, you may want him to be able to scan his own host only.

Nessus Zayıflık Tarama Sistemi

Kullanıcı Ekleme #2

```
# nessus-adduser
Using /var/tmp as a temporary file holder
```

```
Add a new nessusd user
```

```
-----
Login : holden2
Authentication (pass/cert) [pass] : cert
Please enter User Distinguished Name:
Country: Turkey
STate:
Location: Istanbul
Organization: Siyah Sapka Security Solutions
Organizational Unit: Security
Common Name: Fatih Ozavci
e-Mail: holden@siyahsapka.com
```

```
User rules
```

```
-----
nessusd has a rules system which allows you to restrict the
hosts
that holden2 has the right to test. For instance, you may want
him to be able to scan his own host only.
Please see the nessus-adduser(8) man page for the rules
syntax
Enter the rules for this user, and hit ctrl-D once you are done :
(the user can have an empty rules set)
```

```
Login      : holden2
DN         : /C=Turkey/ST=Istanbul/O=Siyah
           Sapka Security Solutions/
           OU=Security/CN=Fatih Ozavci/
           M=holden@siyahsapka.com
Rules      :
Is that ok ? (y/n) [y] y
user added.
```

/usr/local/var/nessus/users/holden2/auth/password dosyasına kullanıcı şifresini girmelisiniz

Nessus Zayıflık Tarama Sistemi Sunucu Sertifikası #1

```
# nessus-mkcert
```

Creation of the Nessus SSL Certificate

This script will now ask you the relevant information to create the SSL certificate of Nessus. Note that this information will **NOT** be sent to anybody (everything stays local), but anyone with the ability to connect to your Nessus daemon will be able to retrieve this information.

CA certificate life time in days [1460]:

Server certificate life time in days [365]:

Your country (two letter code) [FR]: TR

Your state or province name [none]:

Your location (e.g. town) [Paris]: Istanbul

Your organization [Nessus Users United]: Siyah Sapka Security Solutions

Nessus Zayıflık Tarama Sistemi

Sunucu Sertifikası #2

Congratulations. Your server certificate was properly created.

/usr/local/etc/nessus/nessusd.conf updated

The following files were created :

. Certification authority :

 Certificate = /usr/local/com/nessus/CA/cacert.pem

 Private key = /usr/local/var/nessus/CA/cakey.pem

. Nessus Server :

 Certificate = /usr/local/com/nessus/CA/servercert.pem

 Private key = /usr/local/var/nessus/CA/serverkey.pem

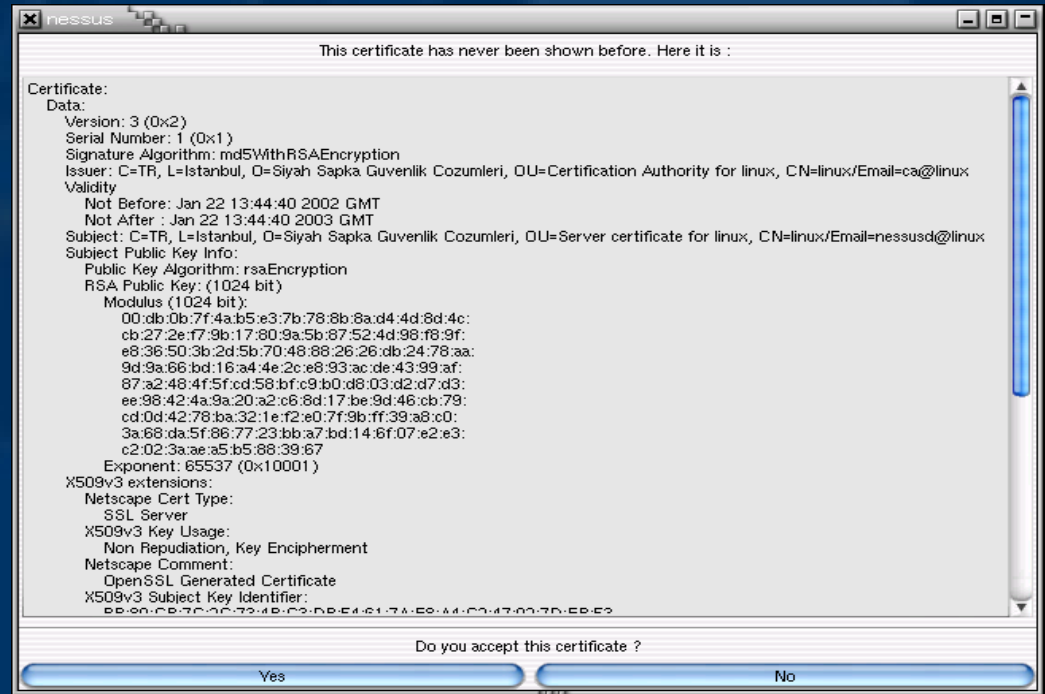
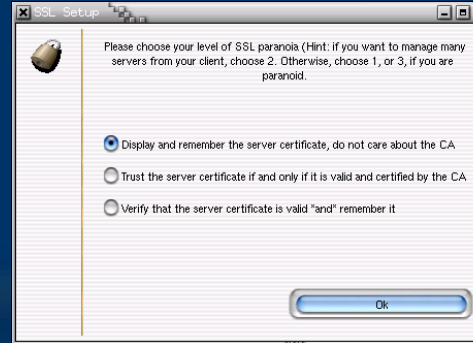
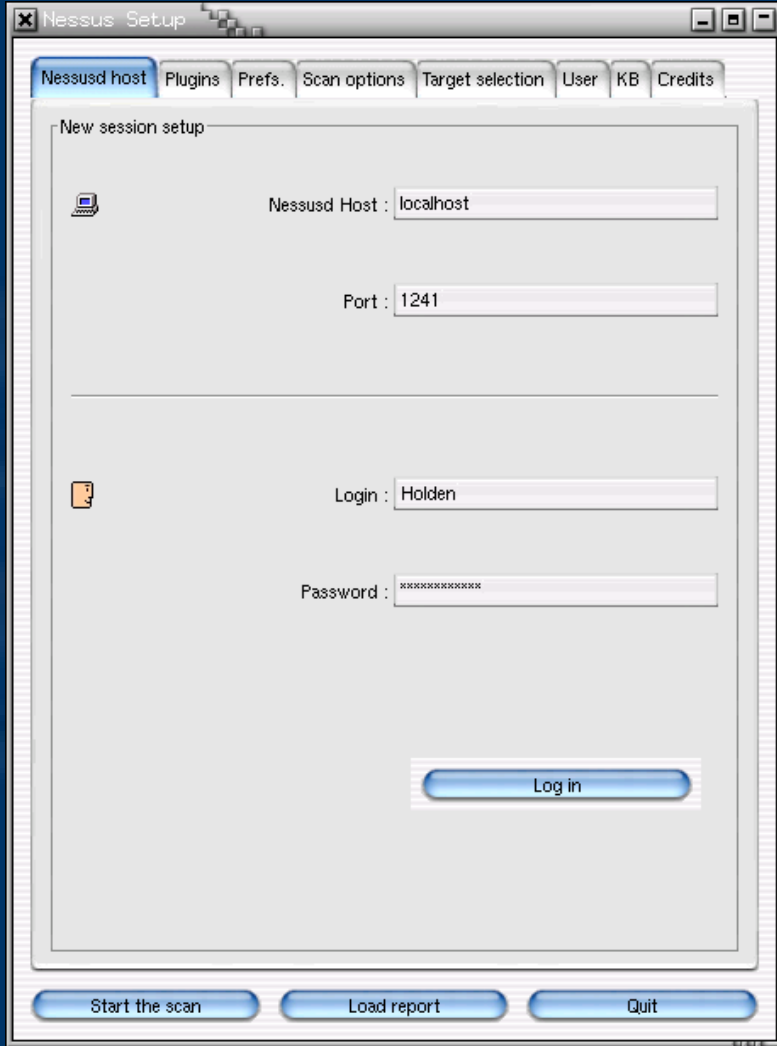
Press [ENTER] to exit

Nessus Zayıflık Tarama Sistemi Yardımcı Komutlar

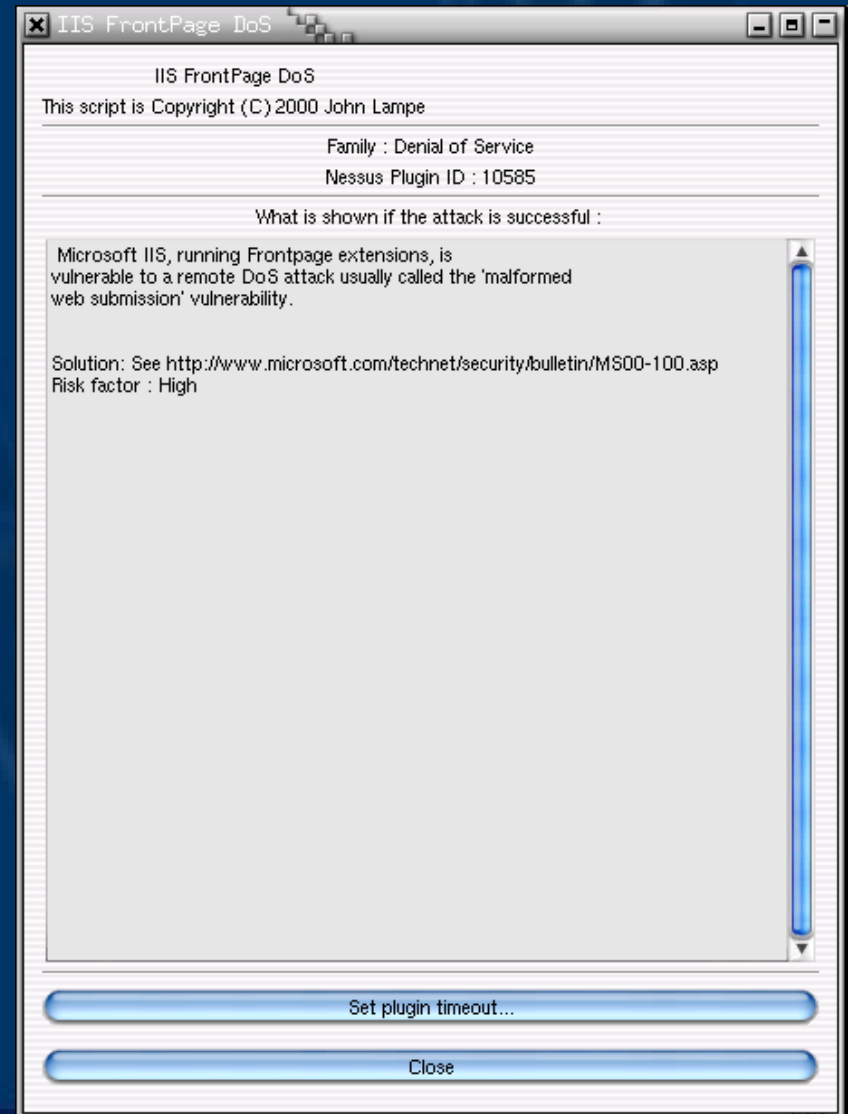
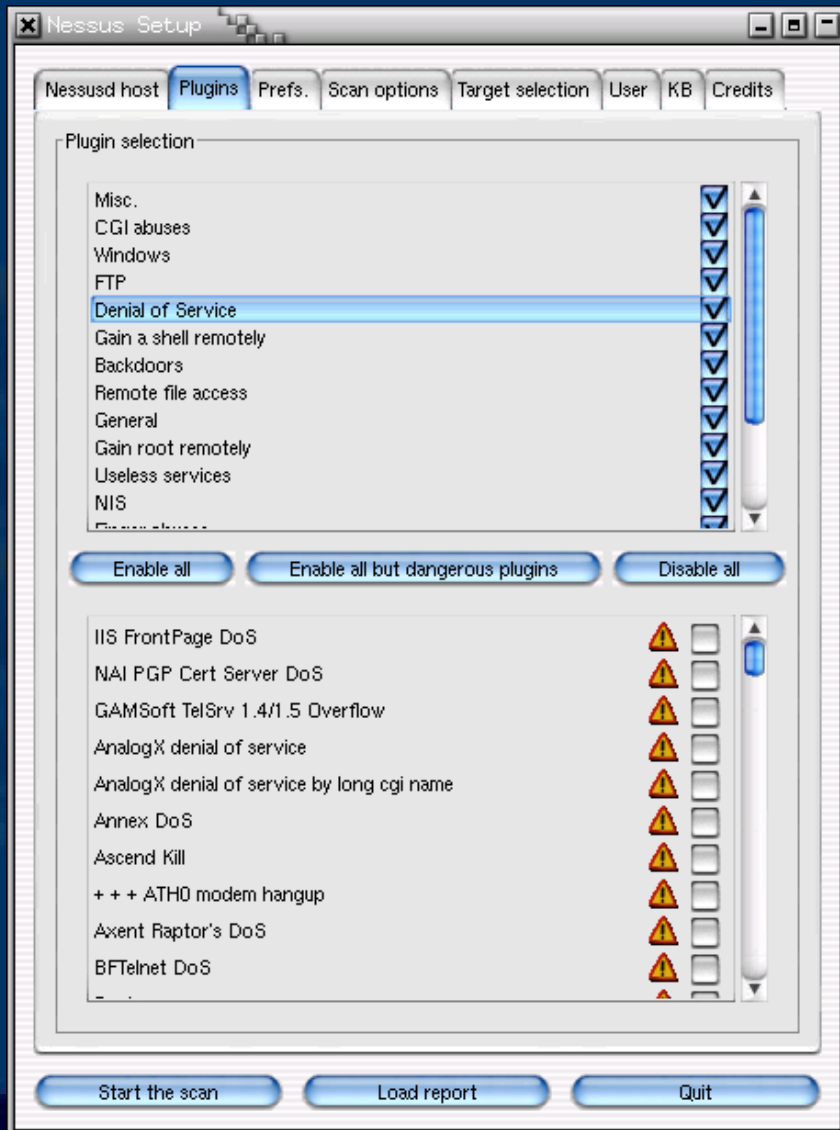
- Nessus Sunucusunu Başlatmak İçin
 - `nessusd -D`
- Sunucu ve İstemci Sertifikası Üretmek İçin
 - `nessus-mkcert`
 - `nessus-mkcert-client`
- Denetim Veritabanı Güncellemesi İçin
 - `nessus-update-plugins -v`
- İstemciyi çalıştırmak için
 - `nessus`
- Sistemden Kaldırmak İçin
 - `/nessus-libraries/uninstall-nessus`
- NASL İle İlgili Dökümantasyon için
 - `cd libnasl/doc ; make`

Nessus Ekran Görüntüleri

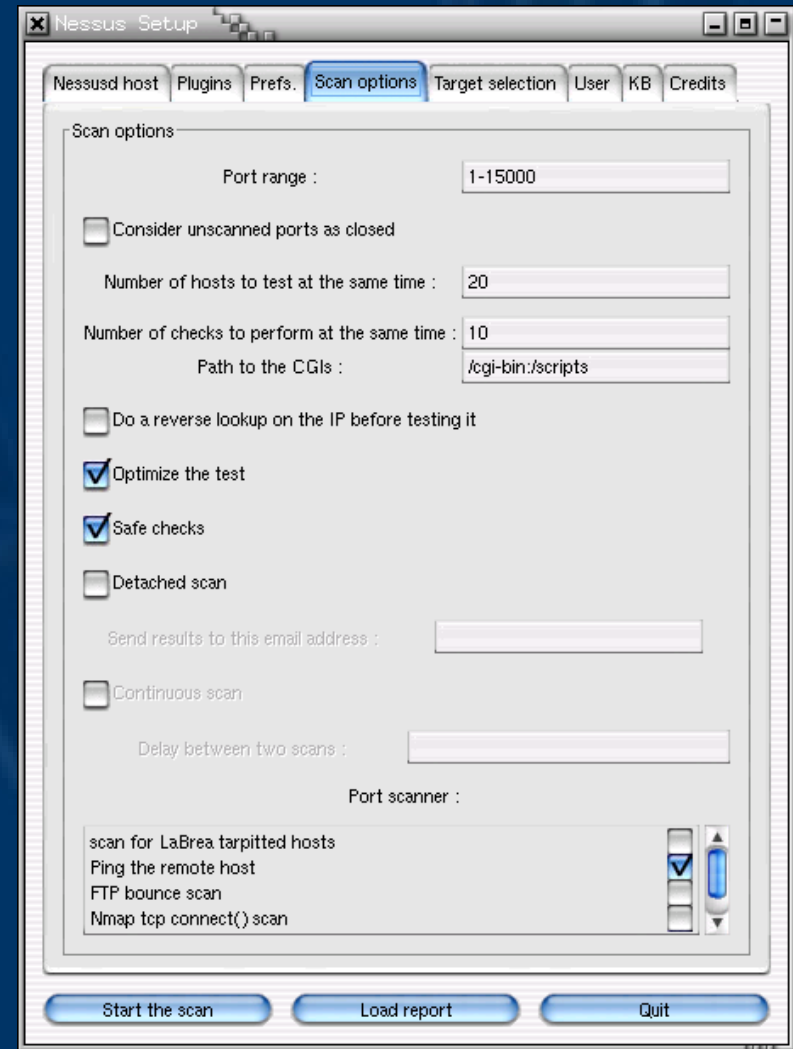
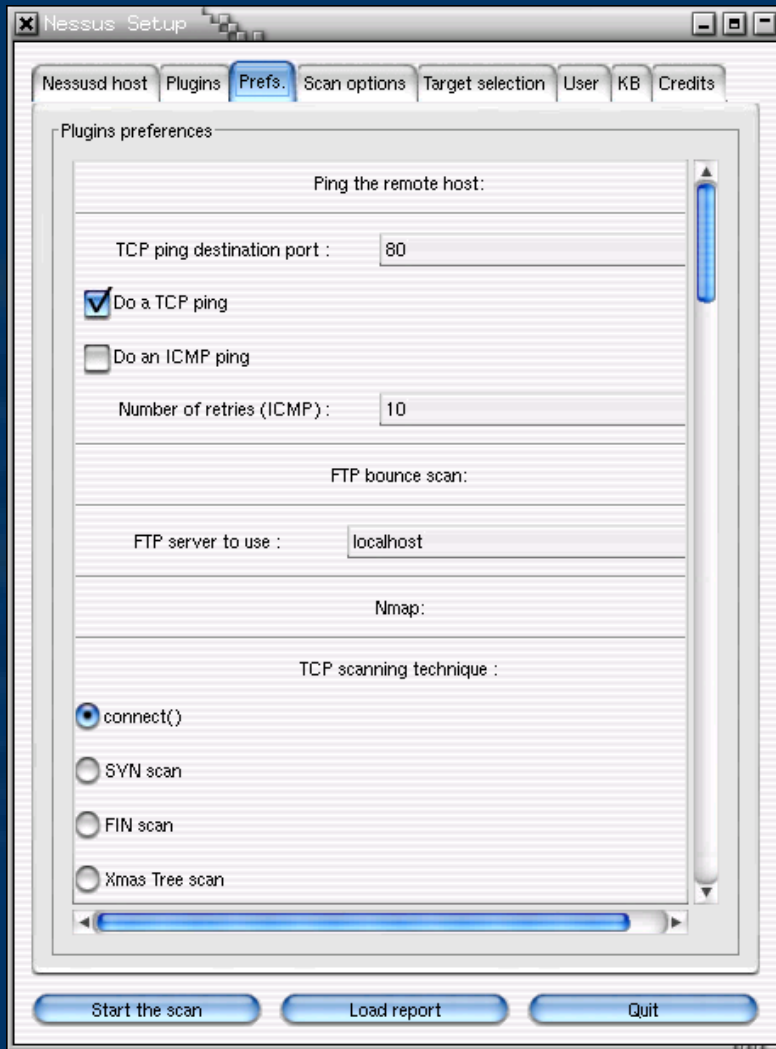
İstemci Doğrulama



Nessus Ekran Görüntüleri Güvenlik Denetim Seçimleri



Nessus Ekran Görüntüleri Eklenti Ayarları ve Denetim Seçenekleri



Nessus Ekran Görüntüleri

Saldırı Tespit Sistemi Denetim Seçenekleri

Nessus Setup

Nessusd host Plugins Prefs. Scan options Target selection User KB Credits

Plugins preferences

NIDS evasion:

TCP evasion technique

none

split

injection

short ttl

Send fake RST when establishing a TCP connection

SMB use host SID to enumerate local users:

Start UID : 1000

End UID : 1200

SMB use domain SID to enumerate users:

Start UID : 1000

Start the scan Load report Quit

Nessus Setup

Nessusd host Plugins Prefs. Scan options Target selection User KB Credits

Plugins preferences

HTTP NIDS evasion:

Use HTTP HEAD instead of GET

URL encoding

none

Hex

UTF-16 (double byte)

UTF-16 (MS %u)

Incorrect UTF-8

Absolute URI type

none

file

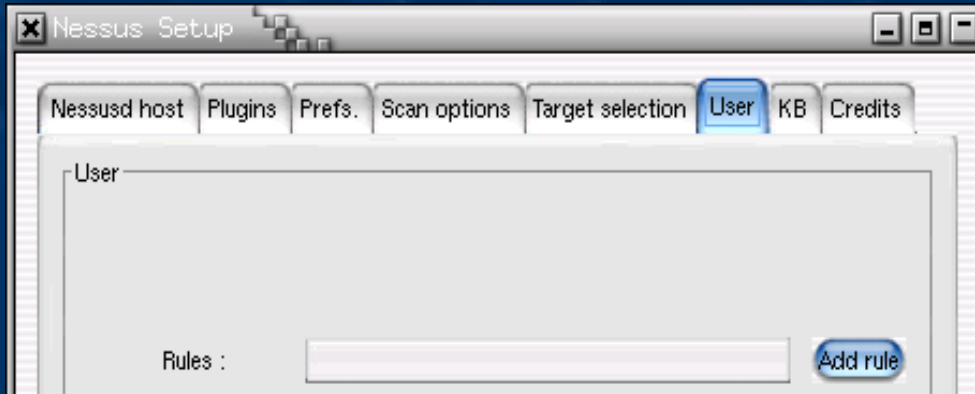
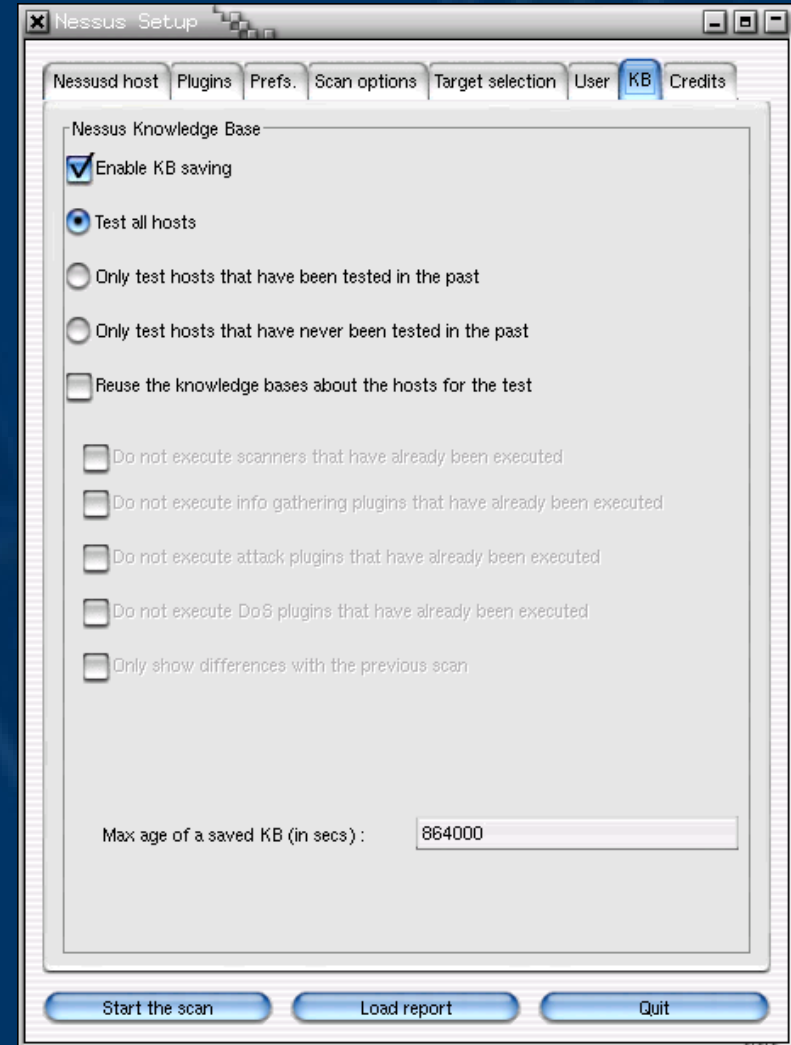
gopher

http

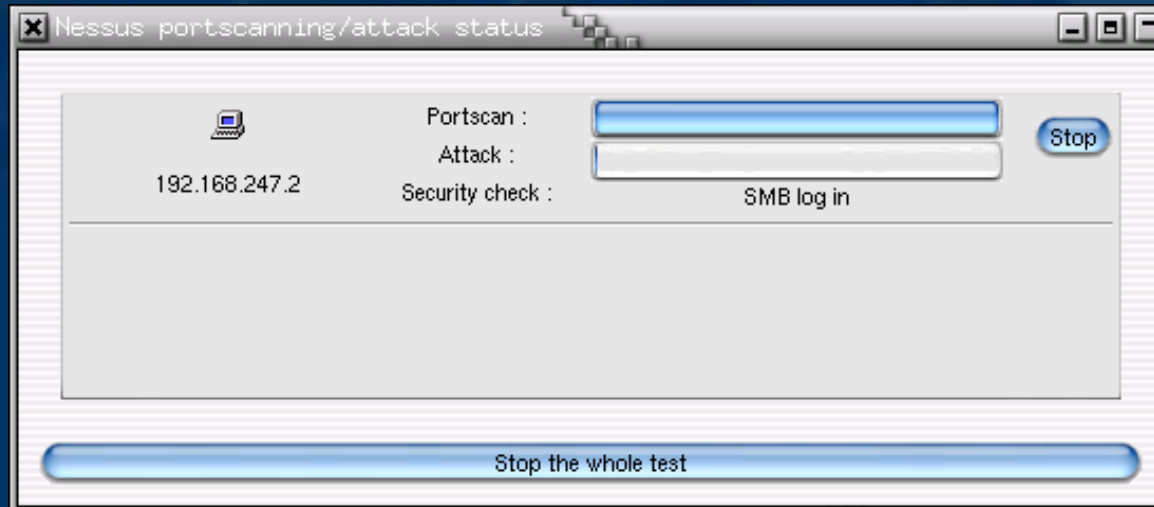
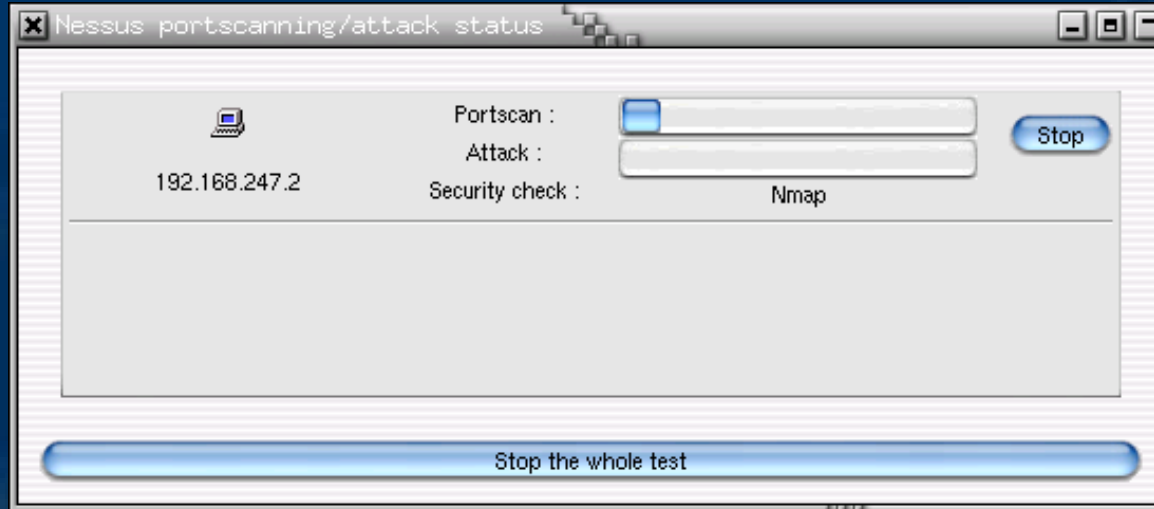
Start the scan Load report Quit

Nessus Ekran Görüntüleri

Hedef Özellikleri



Nessus Ekran Görüntüleri Güvenlik Denetimi



Nessus Ekran Görüntüleri

Denetim Değerlendirme Ekranı

The screenshot displays the Nessus 'NG' Report interface. The window title is 'Nessus "NG" Report'. The interface is divided into several sections:

- Subnet:** A dropdown menu showing '192.168.247' with a cloud icon.
- Host:** A dropdown menu showing '192.168.247.2' with a laptop icon.
- Port:** A list of ports with a scrollbar. The selected port is 'mysql (3306/tcp)'. Other ports listed include 'netbios-ns (137/udp)', 'microsoft-ds (445/tcp)', 'https (443/tcp)', 'http (80/tcp)', and 'general/udp'.
- Severity:** A dropdown menu showing 'Security Holes'.

The main content area displays the following text:

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
- . nuke
- . 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

At the bottom of the window, there is a button labeled 'Save report...'.

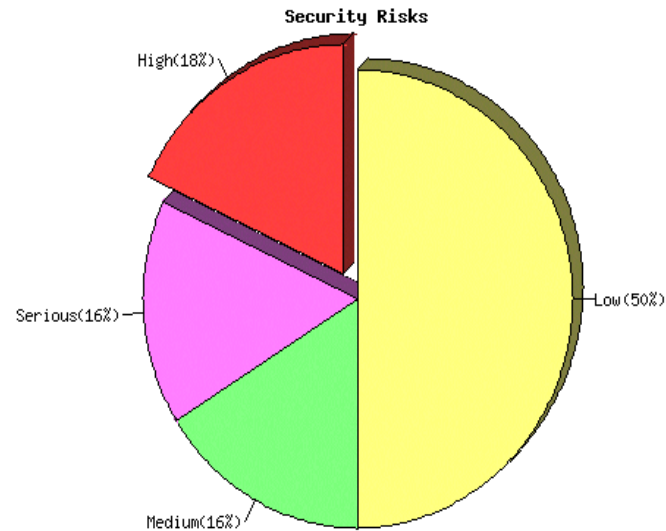
Nessus Ekran Görüntüleri – Html Rapor

Nessus Report

The Nessus Security Scanner was used to assess the security of 1 host

- 2 security holes have been found
- 4 security warnings have been found
- 12 security notes have been found

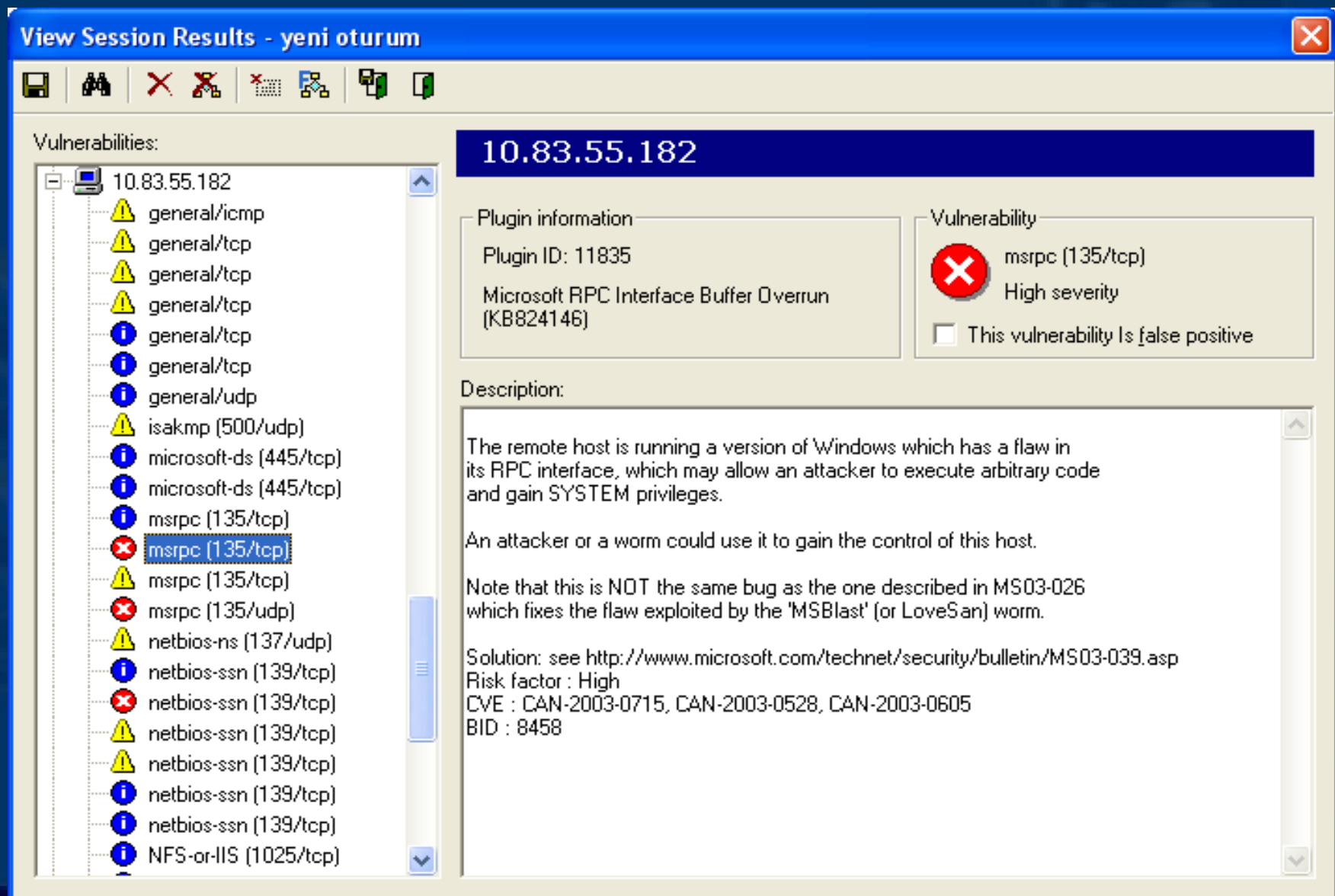
Part I : Graphical Summary :



Nessus Ekran Görüntüleri – XML Rapor

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE scanreport SYSTEM "nsr.dtd">
<scanreport>
<summary>
  <alivehosts>1</alivehosts>
  <securityholes>2</securityholes>
  <securitywarnings>4</securitywarnings>
  <securitynotes>12</securitynotes>
</summary>
<testedhostsummary>
  <testedhost hostname="192.168.247.2">
    <result>Security holes found</result>
  </testedhost>
</testedhostsummary>
<details>
  <host hostname="192.168.247.2">
    <openports>
      <port service="http" protocol="tcp" portnum="80">
        <info>Security hole found</info>
      </port>
      <port service="epmap" protocol="tcp" portnum="135">
        <info>Security warning found</info>
      </port>
      <port service="netbios-ssn" protocol="tcp"
portnum="139">
        <info>Security notes found</info>
      </port>
      <port service="https" protocol="tcp" portnum="443">
```

NessusWX – Windows İçin Nessus İstemcisi



View Session Results - yeni oturum

Vulnerabilities:

- 10.83.55.182
 - general/icmp
 - general/tcp
 - general/tcp
 - general/tcp
 - general/tcp
 - general/tcp
 - general/tcp
 - general/udp
 - isakmp (500/udp)
 - microsoft-ds (445/tcp)
 - microsoft-ds (445/tcp)
 - msrpc (135/tcp)
 - msrpc (135/tcp)**
 - msrpc (135/tcp)
 - msrpc (135/udp)
 - netbios-ns (137/udp)
 - netbios-ssn (139/tcp)
 - netbios-ssn (139/tcp)
 - netbios-ssn (139/tcp)
 - netbios-ssn (139/tcp)
 - netbios-ssn (139/tcp)
 - netbios-ssn (139/tcp)
 - NFS-or-IIS (1025/tcp)


10.83.55.182

Plugin information

Plugin ID: 11835

Microsoft RPC Interface Buffer Overrun (KB824146)

Vulnerability

 msrpc (135/tcp)

High severity

This vulnerability is false positive

Description:

The remote host is running a version of Windows which has a flaw in its RPC interface, which may allow an attacker to execute arbitrary code and gain SYSTEM privileges.

An attacker or a worm could use it to gain the control of this host.

Note that this is NOT the same bug as the one described in MS03-026 which fixes the flaw exploited by the 'MSBlast' (or LoveSan) worm.

Solution: see <http://www.microsoft.com/technet/security/bulletin/MS03-039.asp>

Risk factor: High

CVE : CAN-2003-0715, CAN-2003-0528, CAN-2003-0605

BID : 8458

NessusWX – Windows İçin Nessus İstemcisi

The screenshot displays the Nessus Console interface. At the top, the window title is "Nessus Console" with standard Windows window controls. Below the title bar is a menu bar (File, Session, Communications, View, Help) and a toolbar with various icons. The main area shows a "Manage Session Results - yeni oturum" dialog box. Inside this dialog, there is a table with the following data:

ID	Date	Time	Source	Config	Owner
01C435CB6A3BBE70	09-May-2004	13:42:05	NBE	Present	<unknown>

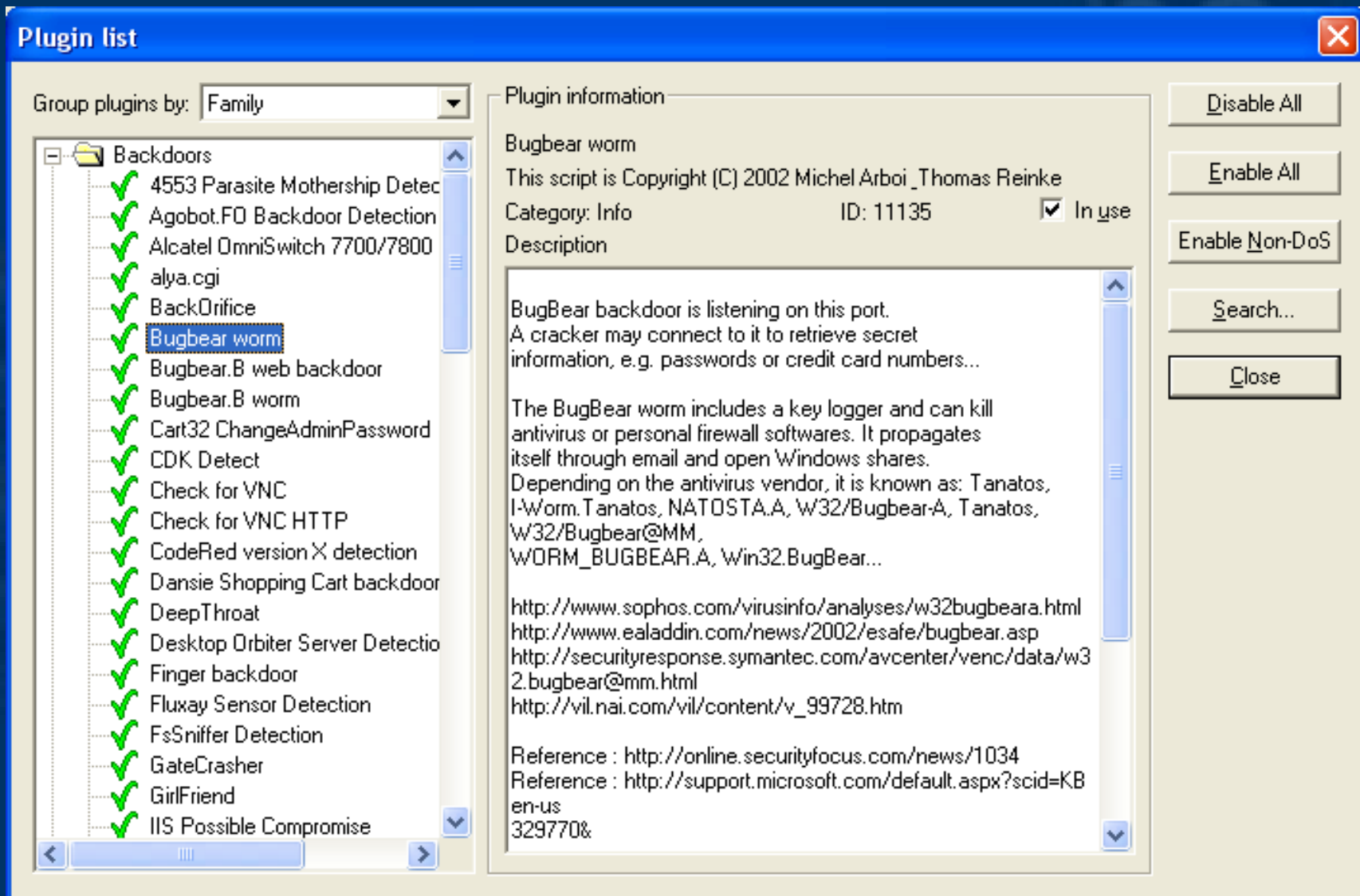
To the right of the table are buttons for "View...", "Report...", "Delete", "Export...", "Import...", "Diff...", and "Exit". Overlaid on top of the "Manage Session Results" dialog is a "Report Options" dialog box. This dialog has the following settings:

- Report type: Adobe Acrobat (.pdf)
- File name: G:\deneme_rapor.pdf
- Sort by: Host names, Vulnerabilities
- Options: Do not include vulnerabilities marked as "false", Include scan configuration
- Filter: Open ports, Low severity, Medium severity, High severity

At the bottom of the Nessus Console window, there is a status bar showing "Disconnected" on the left and "2248K" on the right. A terminal window at the bottom left shows the following text:

```
Nessus Console  
SSL library initialized  
New encryption key was generated  
Database directory "C:\Documents and Settings\user\My Recent Documents" was created successfully.  
New session named "yeni oturum" created
```

NessusWX – Windows İçin Nessus İstemcisi



Nessus Temelli Yazılımlar ve Yardımcılar

- NessusWeb
- NessusWI
- NessusPHP
- NessusWX
- **Sussen ***
- zNessus
- update-nessusrc
- update-nessus-plugins
- update-nessusrc.py
- nessQuick
- Webmin arayüzü
- nbe2sql

Nessus Temelli Ticari Ürünler (Tenable Security)

- **Lightning Console :**

Merkezi güvenlik yönetimi yazılımı ; Nessus temelli sistemlerin yönetimi ve saldırı tespit sistemleri ile eş zamanlı çalışabilme için kullanılmaktadır.



- **Nevo Passive Vulnerability Scanner :**

Pasif Güvenlik Tarama Yazılımı ; Nessus temelli, paket yakalama yoluyla güvenlik açıklarını saptama amaçlı kullanılmaktadır.



- **NEWT Vulnerability Scanner :**

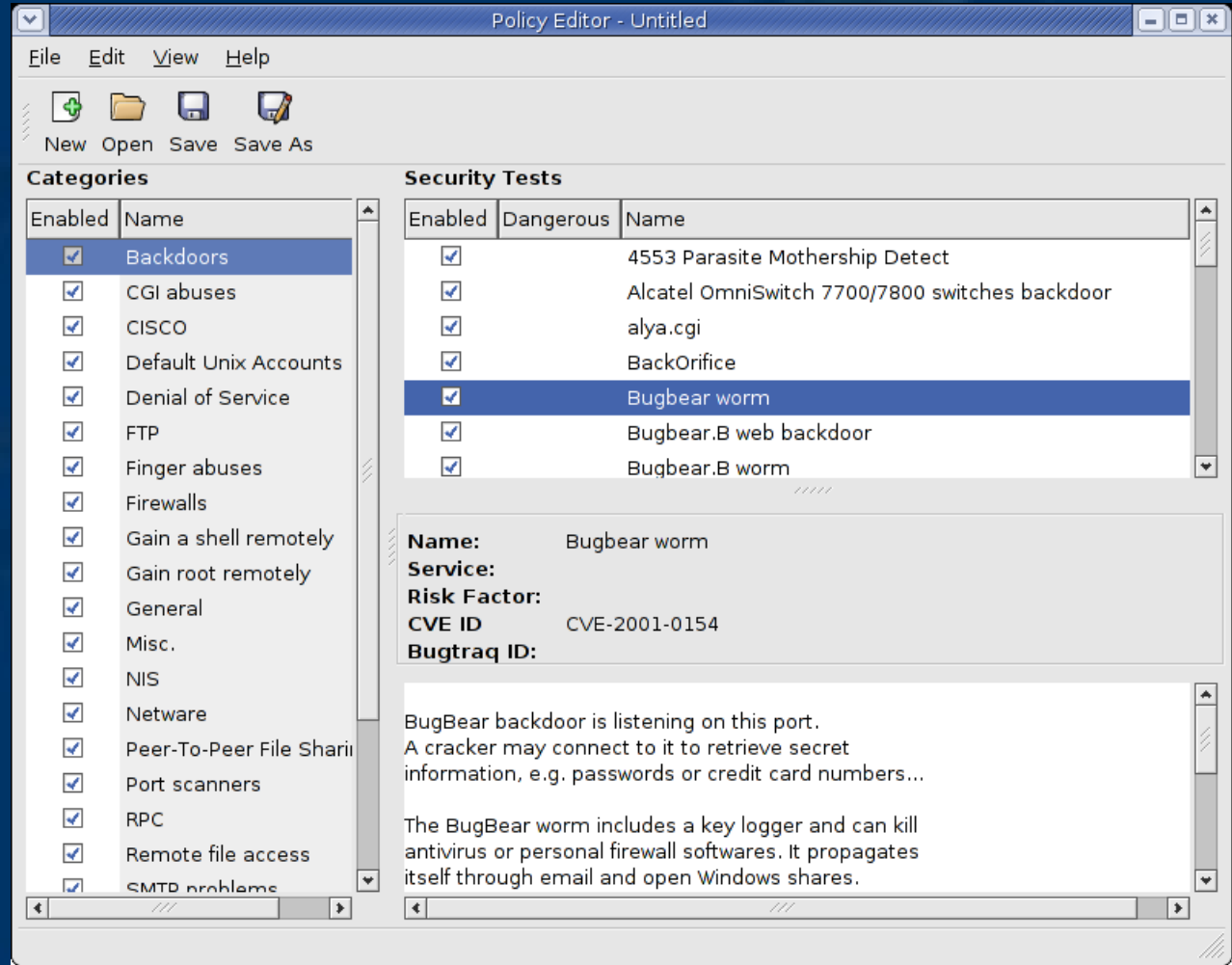
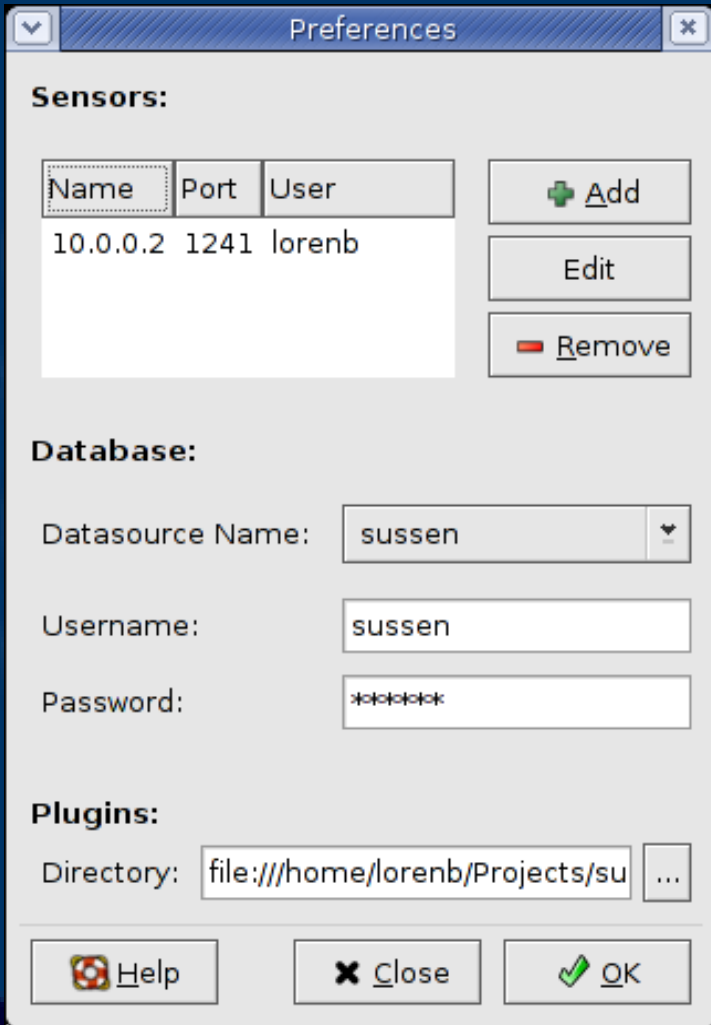
Nessus güvenlik denetim yazılımının Windows işletim sistemi sürümü, kendi istemcisi ve sunucusu bulunmaktadır.



Sussen Gvenlik Denetim Yazılımı

- Nessus iin istemci tarafındaki eksiklikleri giderebilmek iin yeni bir istemci yazılarak yola ıkılmıřtır.
- Zaman ierisinde istemciye ek olarak sunucu ve kendi modl altyapısı da geliřtirilmiřtir.
- Eklentileri Python temellidir ve Nessus eklentileri ile uyumludur.
- PDF raporlama, GnomeDB ile veritabanı entegrasyonu, harici denetim politikası dzenleme ekranı ve zel denetim hazırlama ekranı en ciddi artılarıdır.
- Henz kararlı olarak alıřmamaktadır, uygulama aılıř veya denetim esnasında sorun ıkarabilmektedir.
- <http://sussen.sf.net>

Sussen Güvenlik Denetim Yazılımı Ekran Görüntüleri



Neden Nessus Tercih Edilmeli ?

- Denetim veritabanı, alternatiflerinden çok daha hızlı güncellenir
- NASL dili ile özel denetimler tanımlanabilir
- Denetim sonuçları kayıt edilebilir, karşılaştırmalar, eklemeler ve analizler yapılabilir
- Artımlı taramalar yaparak zaman kazandırır
- Ücretsiz ve açık kodludur , ücretsiz işletim sistemlerine kurulabilmektedir (Linux, FreeBSD v.s.)
- Sınırsız sayıda sistemi aynı anda tarayabilir (Donanımsal Sınır)
- XML çıktılar üreterek farklı programların raporları yorumlaması sağlanabilir
- İstemci – Sunucu mimarisi sebebiyle taşınabilirliği ve güvenliği öne çıkarmıştır
- Snort saldırı tespit sistemi ile korelasyon yapılabilir, eş zamanlı çalışma ile daha etkin saldırı tespiti yapılabilir

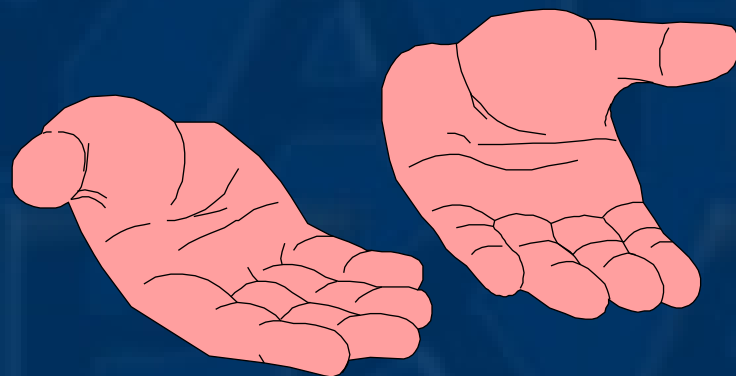
Neden Özgür Güvenlik Yazılımları Tercih Edilmeli ?

- 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 örnekleri 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

Daha Fazla Bilgi İçin Kaynaklar

- Nessus – <http://www.nessus.org>
- NessusWX – <http://nessuswx.nessus.org>
- Sussen – <http://sussen.sf.net>
- Tenable Security – <http://www.tenablesecurity.com>
- Nmap – <http://www.insecure.org/nmap>
- CERT – <http://www.cert.org>
- SANS – <http://www.sans.org>
- Security Focus – <http://www.securityfocus.com>

Sorular



Teşekkürler...



SSİNYARMA
SARKA

Dağıtım ve Kullanım Lisansı

Bu belgeyi, Free Software Foundation tarafından yayınlanmış bulunan GNU Özgür Belgeleme Lisansının 1.2 ya da daha sonraki sürümünün koşullarına bağlı kalarak kopyalayabilir, dağıtabilir ve/veya değiştirebilirsiniz. Lisans'ın bir kopyasını <http://www.gnu.org/copyleft/gfdl.html> adresinde bulabilirsiniz.

Bu belgedeki bilgilerin kullanılmımdan doğacak sorumluluklar ve olası zararlardan belge yazarı sorumlu tutulamaz. Bu belgedeki bilgileri uygulama sorumluluğu uygulayana aittir.

Tüm telif hakları aksi özellikle belirtilmediği sürece sahibine aittir. Belge içinde geçen herhangi bir terim, bir ticari isim ya da kuruma itibar kazandırma olarak algılanmamalıdır. Bir ürün ya da markanın kullanılmış olması ona onay verildiği anlamında görülmemelidir.