



# Sicherheits-Schulung

## Netzwerkaudit

# Sicherheits-Schulung

## Gesamtüberblick

### *Aktive Sicherheit für Ihr Netzwerk*

- Sicherheitsaudit
  - Vorbereitung
  - Durchführung
  - Ergebnispräsentation
- Port-Scanner
  - nmap
- Schwachstellen-Scanner
  - Nessus

*Nmap & Nessus braucht jeder*

# Sicherheits-Schulung

## Sicherheitsaudit I

- Vorbereitung
  - Erlaubnis des Rechnerbesitzers einholen
  - Erlaubnis des Netzwerkbesitzers einholen
  - Scan niemals unbeaufsichtigt durchführen
  - Administratoren in Bereitschaft während des Scans
- Durchführung
- Auswertung
  - Falsche Positive eliminieren
  - Statistische Darstellung
    - Anzahl der Rechner
    - Anzahl der Sicherheitslöcher
    - Risiko

nessus

# Sicherheits-Schulung

Sicherheitsaudit Ergebnispräsentation

## *Sicherheit ist ein Prozess*

Vorschläge für Prozessverbesserung

Dauerüberwachung



messus

# Sicherheits-Schulung

## Sicherheitsaudit Portscanner

Nmap Author Fyodor

- Flexible: viele Scan-Techniken (tcp/udp/ping)
- Schnell
- Portable
- Einfach: `nmap -O -sS targethost`
- Umsonst
- Ausgabe in Text, Maschinenlesbar, xml, ...
- Betriebssystemerkennung

nessus

# Sicherheits-Schulung

## Sicherheitsaudit nmap

- Tcp connect scan
- Tcp SYN scan (half open scan)
- FIN scan
  - Funktioniert nicht bei windows, da nicht tcp konform
- Fragmentation scan / SYN | FIN
- Ident scan
- ftp bounce scan
- Udp port unreachable scan
- Ping

lessus

# Sicherheits-Schulung

## Sicherheitsaudit Schwachstellen-Scanner

### Nessus Author Renaud Deraison

- Client – Server
  - Windows Client, Java Client, X Client
- Server
  - Linux, Solaris, ...
- Verschlüsselte Verbindung zwischen Client und Server
- Authentisierung durch Passwort und/oder Zertifikate
- Zentrale Regelvorgabe
  - „Dieser Nutzer darf diese Rechner nicht scannen“
- Plug-In basiert
  - Über 8000 Sicherheitschecks in NASL
- Dauerscan, Differenz-Ergebnis per Email

# Sicherheits-Schulung

## Nessus Knowledge Base

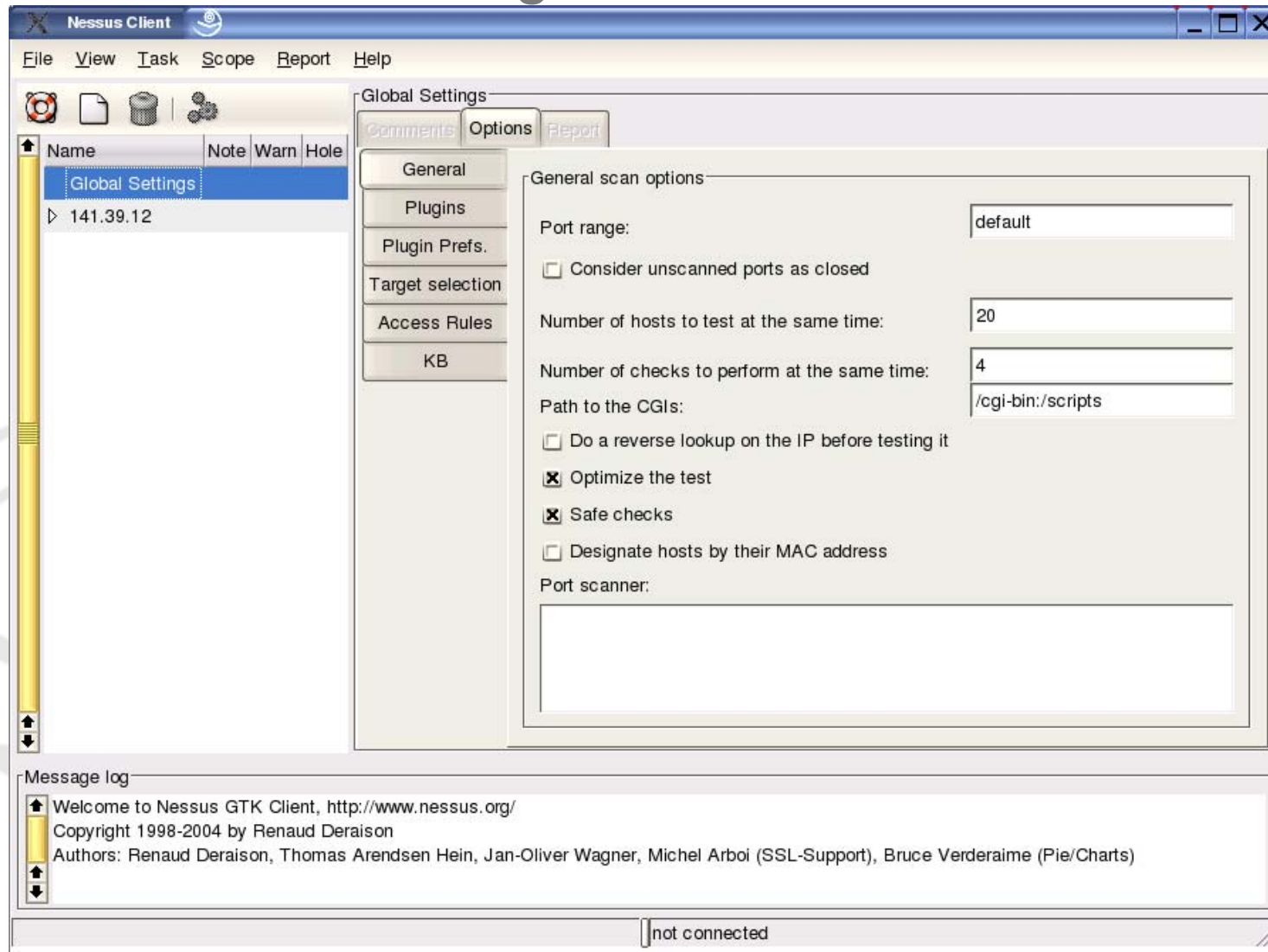
- Plugins speichern Ergebnisse in Knowledge Base
- Andere Plugins bauen darauf auf
- Die Abhängigkeiten zwischen den Plugins sind in der Skriptdefinition beschrieben -> nessusd ruft Plugins in der „richtigen“ Reihenfolge auf

The Nessus logo watermark is visible in the background, featuring a stylized eye with a blue spiral and the word 'nessus' in a light grey font.

nessus

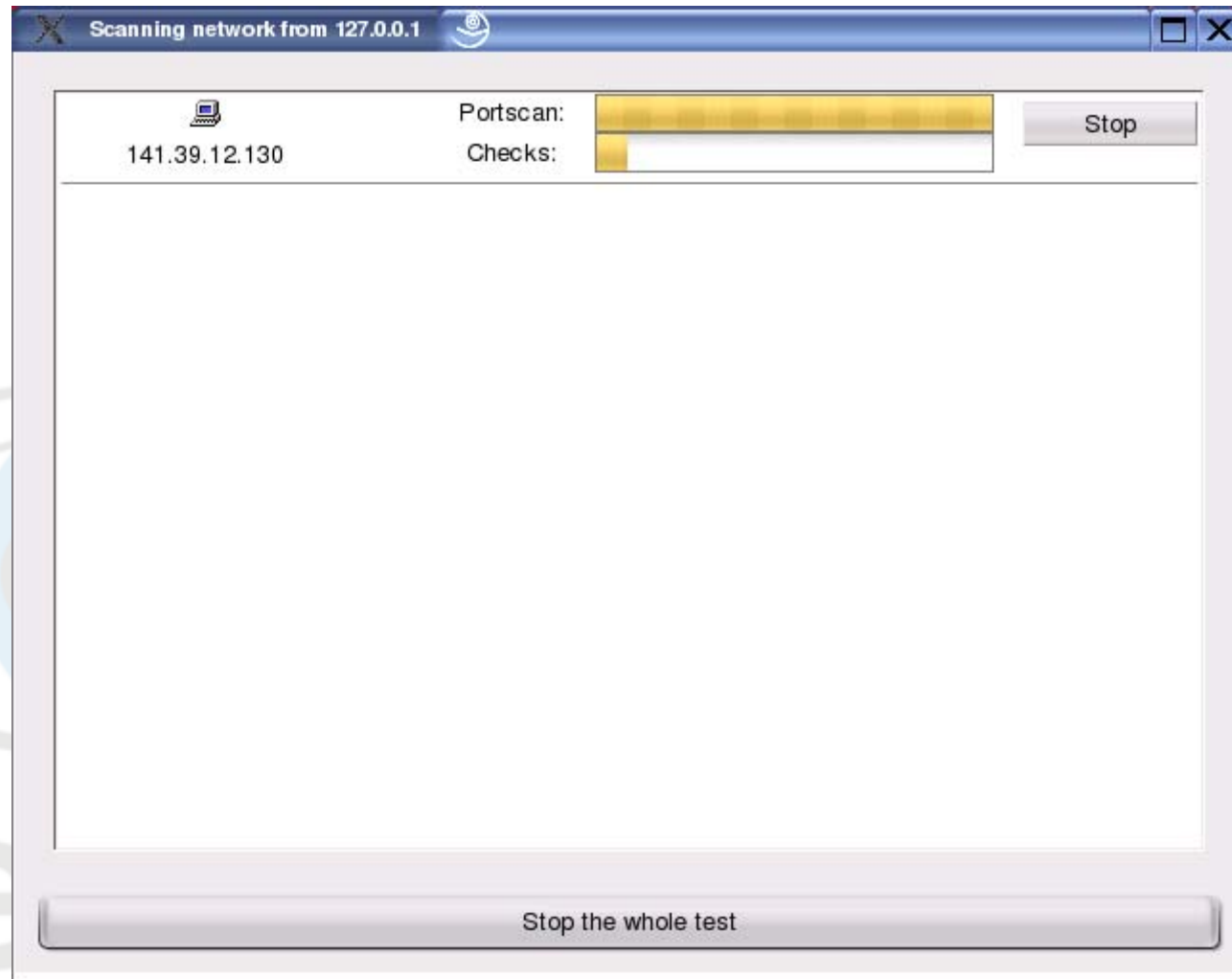
# Sicherheits-Schulung

## Nessus Einstellungenfenster



# Sicherheits-Schulung

## Nessus scannt



# Sicherheits-Schulung

## Nessus NASL

- C ähnliche Skriptsprache
- Kein Dateizugriff auf nessusd-Host
- Netzwerkzugriff nur auf den Zielhost
- -> Dadurch werden „trojanische“ Plugins verhindert
- „nützliche“ Routinen helfen Plugins zu schreiben
  - ftp\_log\_i(), http\_get()

nessus

# Sicherheits-Schulung

## Nessus Reportarten

- Ergebnisse können in den folgenden Formaten gespeichert werden:
  - .nsr oder .nbe
  - .LaTeX
  - .html (mit oder ohne Graphiken)
  - .xml
  - .txt

The image shows a large, faint watermark of the Nessus logo in the background. The logo consists of a stylized eye with a blue spiral in the center, and the word 'nessus' written in a lowercase, sans-serif font below it.

nessus

# Sicherheits-Schulung

## Nessus Reportfenster

The screenshot displays the Nessus Client interface. The main window title is "Nessus Client". The menu bar includes "File", "View", "Task", "Scope", "Report", and "Help". The left sidebar shows a tree view of the scan structure, with the selected report "Report 20050608-160036" highlighted. The main pane shows the report details for the scope "unnamed scope" (Task: mailer.berkom.de). The report is categorized as a "Security Hole" with a severity of "High". The affected host is "141.39.12". The report text includes the following information:

Report for scope: unnamed scope (Task: mailer.berkom.de)

Subnet: 141.39.12

Port: general/tcp  
bb (1984/tcp)  
compaq-scp (2766/tcp)

Severity: Security Hole

You should install this patch for your system to be up-to-date.

Solution : <http://sunsolve.sun.com/search/document.do?assetkey=1-21>  
Risk factor : High

-----

The remote host is missing Sun Security Patch number 105210-52 (libaio, libc & watchmalloc patch).

You should install this patch for your system to be up-to-date.

Solution : <http://sunsolve.sun.com/search/document.do?assetkey=1-21>  
Risk factor : High  
BID : 7991

Scan took place from Wed Jun 8 15:53:51 2005 to Wed Jun 8 16:00:36 2005

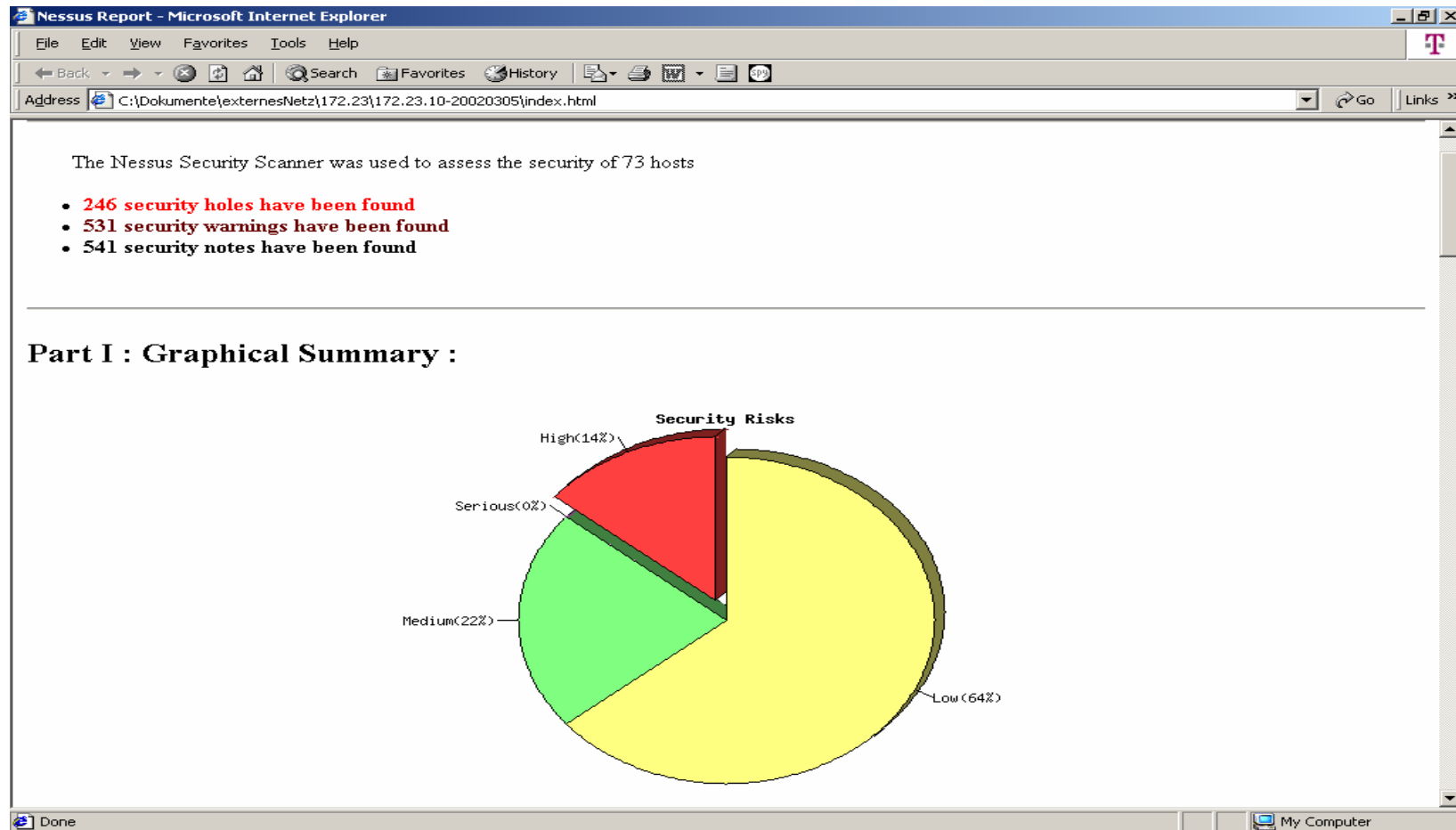
Message log

- Welcome to Nessus GTK Client, <http://www.nessus.org/>
- Copyright 1998-2004 by Renaud Deraison
- Authors: Renaud Deraison, Thomas Arendsen Hein, Jan-Oliver Wagner, Michel Arboi (SSL-Support), Bruce Verderaime (Pie/Charts)

not connected

# Sicherheits-Schulung

## Nessus Beispielbericht html



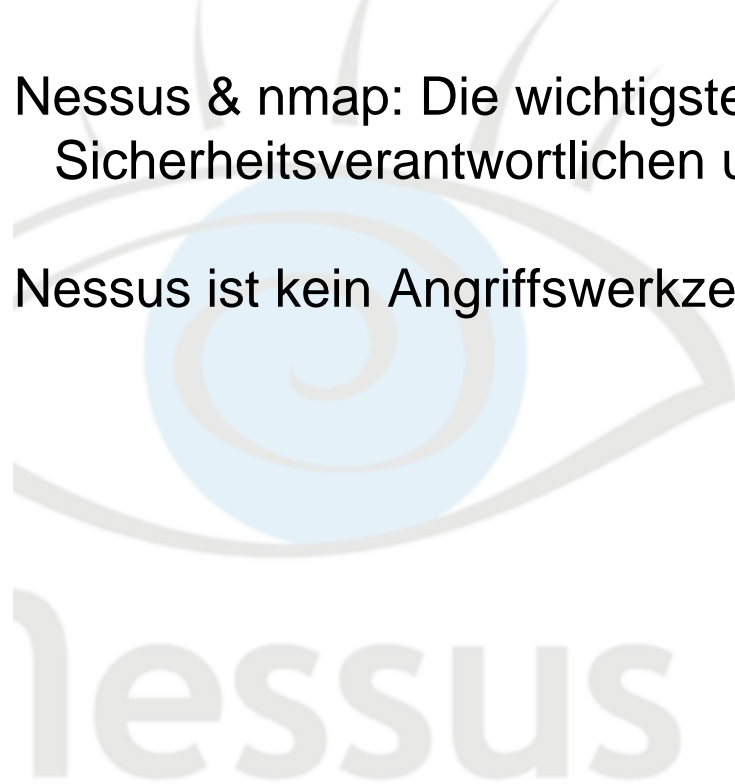
# Sicherheitsschulung

## Resources / Zusammenfassung

- <http://www.insecure.org>
- <http://www.nessus.org>

Nessus & nmap: Die wichtigsten Werkzeuge für alle Sicherheitsverantwortlichen und Auditoren

Nessus ist kein Angriffswerkzeug (zu laut)



# Netzwerksicherheitsaudit

## Ansprechpartner

Axel Nennker

T-Systems International GmbH

SSC ENPS / Technologiezentrum

Tel: 030 / 34 97 - 3256

Fax: 030 / 34 97 - 3257

email: [axel.nennker@t-systems.com](mailto:axel.nennker@t-systems.com)

lessus

# Netzwerksicherheitsaudit

## Fragen



Zusammenfassung

Fragen???

nessus