# AutoNessus

Geautomatiseerde Nessus scans met delta rapportage

**Frank Breedijk**

15 mei 2008

# Even voorstellen…

Frank Breedijk

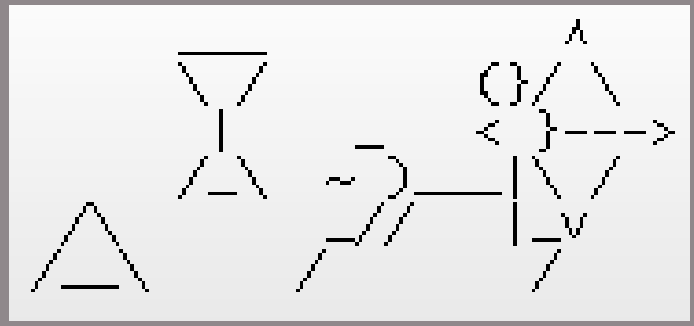
Sinds 2 jaar Security Engineer bij Schuberg Philis

- Daarvoor:
  - Security Consultant INS (BT Professional services)
  - Manager EMEA Security Operations Center (SOC) Unisys
  - ICT Security Officer Interxion

# AutoNessus

- Geautomatiseerd uitvoeren van Nessus scans met delta rapportage
- Open Source (GPLv3)
- Released: 15 mei 2008

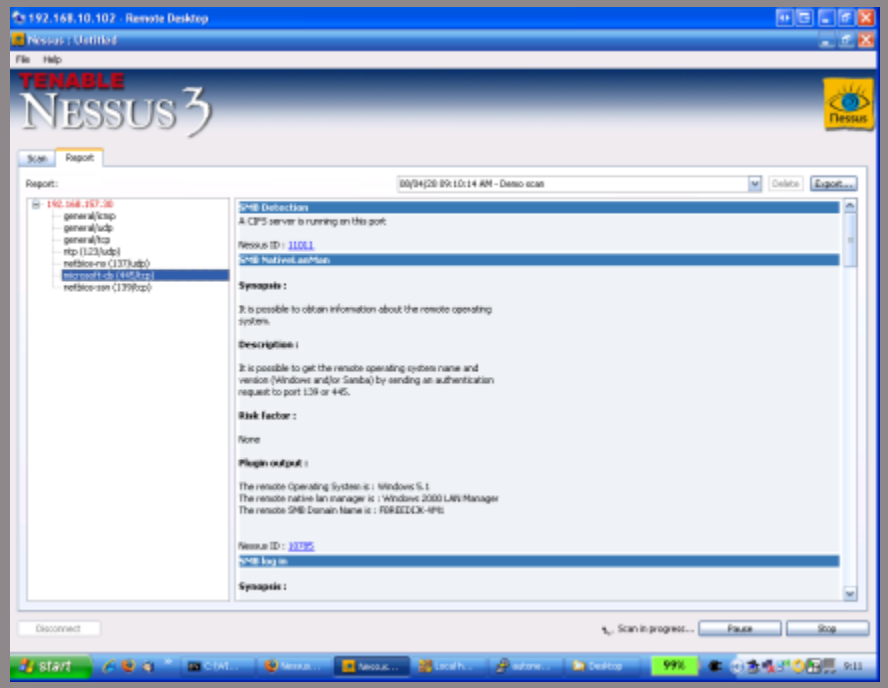
- Daarvoor…
  - Interne tool van Schuberg Philis
  - Geschreven door Frank Breedijk



# Nessus

- “Free” TCP/IP security scanner
- Meest gebruikte security scanner (Volgens sectools.org survey van 2000, 2003 en 2006)

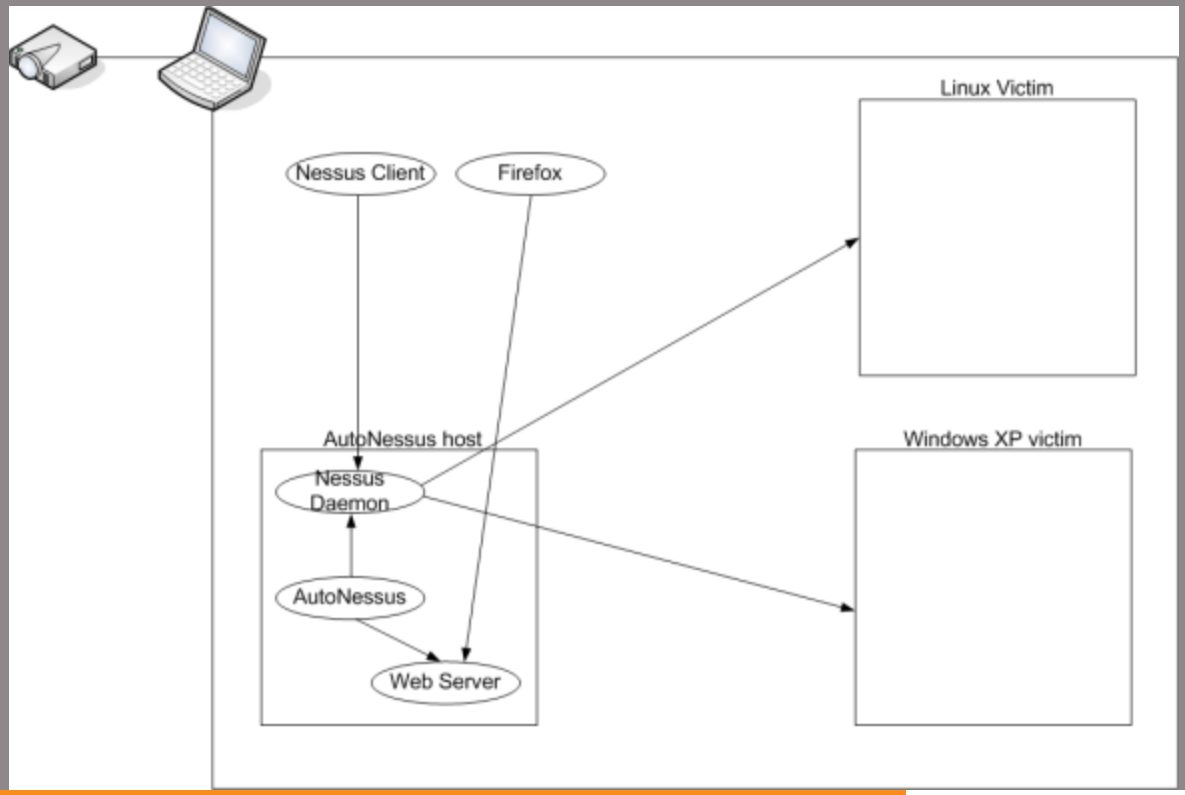
- Daarvoor…
  - Open Source software



# Wat is het probleem?

- Ik zal het laten zien…

# Demo netwerk

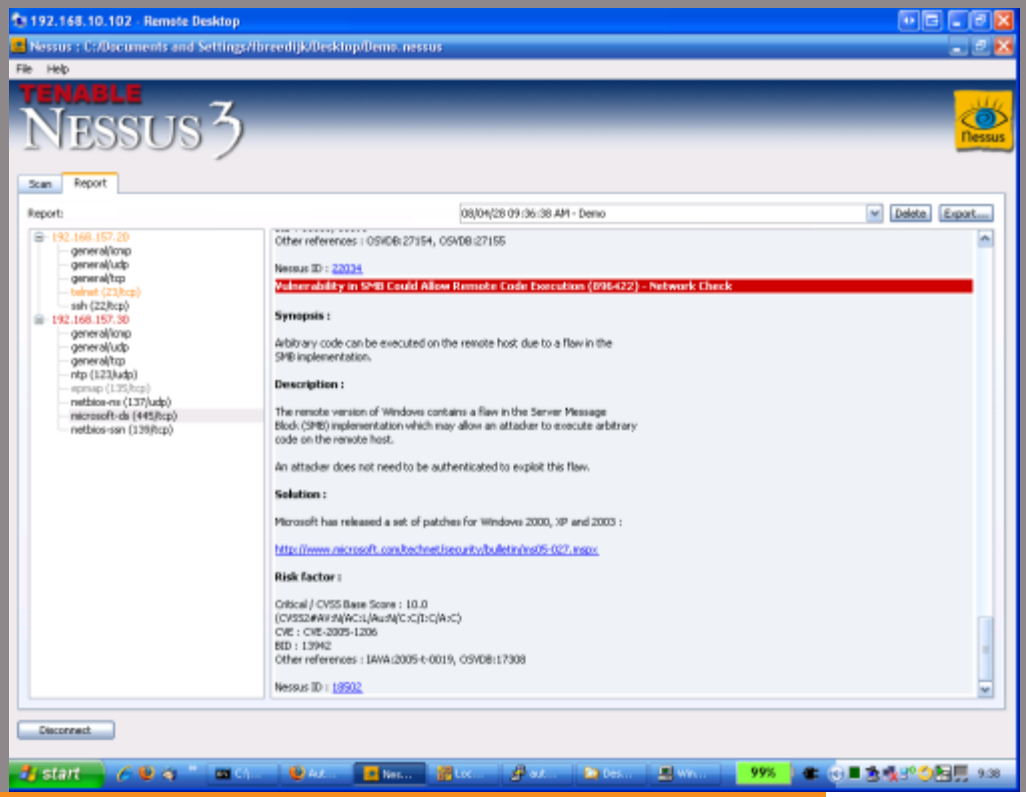


# Probleemstelling

- Nessus is een goede tool
- Veel output. Te veel?
- Scannen kan lang duren
- Analyse kost veel tijd

- **Vaak scannen, is vaak dezelfde findings zien. Dit stompt af en kost tijd.**

# Demo


192.168.10.102 - Remote Desktop
Nessus : C:\Documents and Settings\rbreedijk\Desktop\Demo.nessus
File Help
TENABLE
NESSUS 3
Scan Report
Report:
08/04/28 09:36:38 AM - Demo
Delete Export...
192.168.157.20
general/icmp
general/udp
general/tcp
telnet (23/tcp)
ssh (22/tcp)
192.168.157.30
general/icmp
general/udp
general/tcp
ntp (123/udp)
epmap (135/tcp)
netbios-ns (137/udp)
microsoft-ds (445/tcp)
netbios-ssn (139/tcp)
Other references : OSVDB:27154, OSVDB:27155
Nessus ID : 22034
Vulnerability in SMB Could Allow Remote Code Execution (896422) - Network Check
Synopsis :
Arbitrary code can be executed on the remote host due to a flaw in the SMB implementation.
Description :
The remote version of Windows contains a flaw in the Server Message Block (SMB) implementation which may allow an attacker to execute arbitrary code on the remote host.
An attacker does not need to be authenticated to exploit this flaw.
Solution :
Microsoft has released a set of patches for Windows 2000, XP and 2003 :
http://www.microsoft.com/technet/security/bulletin/ms05-027.mspx
Risk factor :
Critical / CVSS Base Score : 10.0
(CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)
CVE : CVE-2005-1206
BID : 13942
Other references : IAVA:2005-t-0019, OSVDB:17308
Nessus ID : 18502
Disconnect
start
99%

# Scannen met AutoNessus

- AutoNessus scant hosts via een command line. (crontab)
- Findings in een flatfile database (=directory structuur).
- Presentatie via web GUI.

# Demo

- Scan wordt gestart via do-scan <scannaam> (demo in dit geval)

- ~/etc/config wordt gelezen
- ~/var/<scannaam>/config wordt gelezen
- PRESCAN commando wordt uitgevoerd
- Adressen uit hosts worden gescand met cofing ~/etc/<MODE>-nessusrc
- Status rapport wordt gemail aan <EMAIL>
- POSTSCAN commando wordt uitgevoerd

# Status rapport email

```
To: frank@localhost.localdomain
Subject: Autonessus output for demo

Host 192.168.157.20
====================
Status: *** WARNING *** Newly discovered
Added: 'Unschynronized clock suspected' to remark
NEW Open port 2
NEW Security Note 9
NEW Security Warning 1

Host 192.168.157.30
====================
Status: *** WARNING *** Newly discovered
Added: 'Unschynronized clock suspected' to remark
NEW Open port 4
NEW Security Hole 3
NEW Security Note 18
NEW Security Warning 1
```

# Web GUI

- 4 findings automatisch gemarkeerd als HARD MASKED
- Andere findings te filteren per host, port of plugin
- Status toekennen aan findings :
  - Wel relevant -> OPEN
  - Niet relevant -> NO ISSUE

# Onder de motorkap

- Nessus client wordt via de command line gestart

- Resultaten beschikbaar als:
  - HTML
  - XML
  - NBE

# NBE formaat

Simpel formaat

- <type> | <netwerk> | <ip> | <port> | <plugin ID> | <prio> | <plugin output>

Finding:

- results|192.168.157|192.168.157.30|ntp (123/udp)|10884|Security Note|\nSynopsis :\n\nAn NTP server is listening...

Open port

- results|192.168.157|192.168.157.20|ssh (22/tcp)

# Conversie naar directory structuur

- Findings
  - Host
    - Port
      - Pluginid (Portscanner voor open port)
        - » Remark – Tekst ingevuld in web GUI
        - » Status - De status in de GUI
        - » YYYYMMDDhhmmss

- Op basis van deze boomstructuur zijn scans gemakkelijk te vergelijken.

# Status, status, status…

| | |
|---|---|
| NEW | Voor het eerst aangetroffen |
| OPEN | Eerder aangetroffen |
| CHANGED | Output is gewijzigd |
| NO ISSUE | Geen risico |
| GONE | Niet meer aangetroffen |
| FIXED | Komt niet meer voor |
| HARD MASKED | Negeer dit |

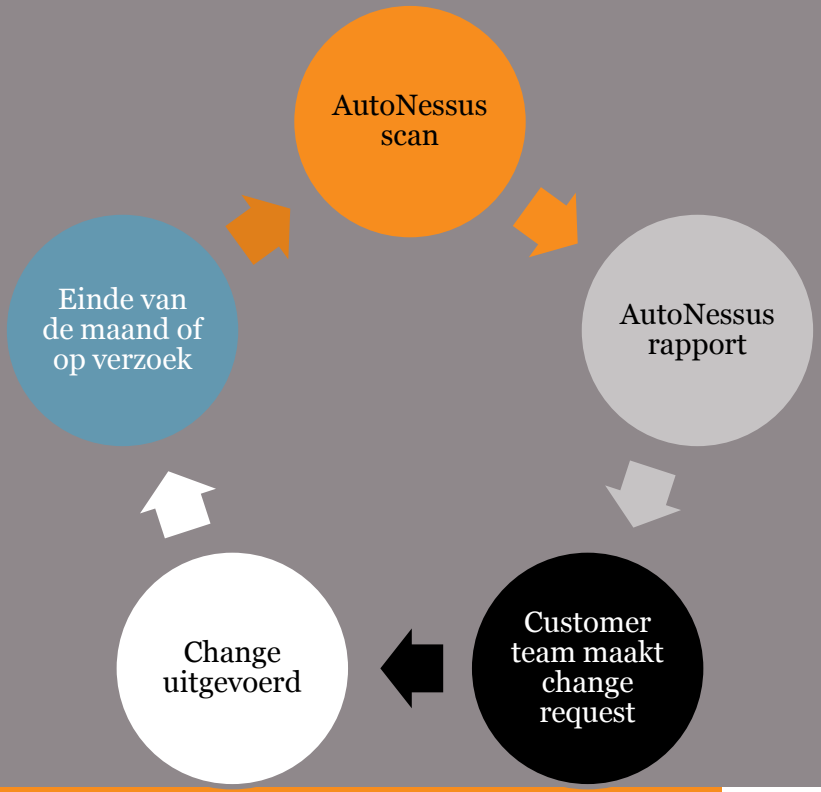
# Open, No issue, fixed, hard masked

| | |
|---|---|
| HARD MASKED | Wordt genegeerd |
| GONE / FIXED | Behoudt status tot weer aangetroffen |
| NO ISSUE | Behoudt status tot output wijzigt |
| | |
| CHANGED | Was ooit GONE, FIXED, NO ISSUE of OPEN<br>Behoud van status tot gebruiker deze wijzigt |

# Als het goed is, is het goed...

...daar hoef je je dus niet meer druk over te maken

# AutoNessus proces



# DUS…

- Maandelijks handmatig scannen met Nessus betekent:
  - ‘s nachts je bed uit om de scan te starten.
  - Onzinnige findings (à la traceroute) iedere maand weer bekijken.
  - Grote kans of fouten door grote herhaling in het werk.
  - Een werkdruk die ook hoog is als er geen veranderingen zijn.

# DUS…

- Maandelijks automatisch scannen met AutoNessus betekent:
  - Scans vooruit via crontab schedulen.
  - Onzinnige findings niet zichtbaar als ze niet moeten worden bekeken.
  - Kleinere kans op fouten door minder herhaling in het werk.
  - Veel verandering is meer werk, maar ook meer risico.

# Waarom Open Source?

- Wij geloven in Open Source
  - Nagios
  - CFEngine
  - Rancid
  - MRTG
  - RRD tool
  - Cacti
  - “LAMP”
  - CVS
  - Etc

- Dank!

# Puzzelen

# Verder vragen…

Email
Fbreedijk <at> schubergphilis <dot> com

Website
www.AutoNessus.com  en www.sourceforge.net