AutoNessus

Analyzing vulnerability assessment data the easy way…

Who am I?

Frank Breedijk

- Security Engineer at Schuberg Philis
- Author of AutoNessus
- Blogger for CupFigther.net

Email: fbreedijk@schubergphilis.com
Twitter: @autonessus
Blog: http://cupfighter.net
Project: http://autonessus.com

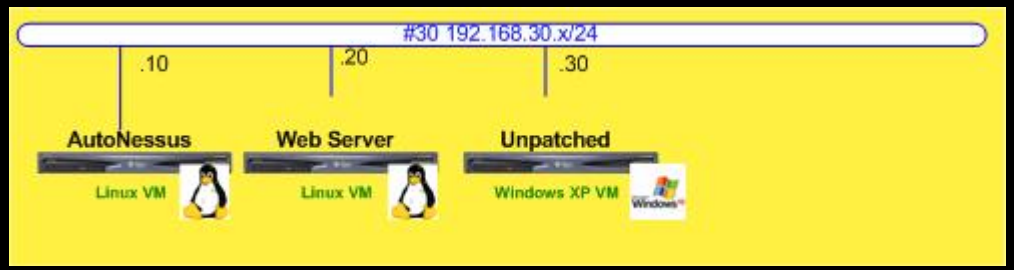
Why AutoNessus?

Let me show why...

On my laptop

- Nessus 4.0 client
- VMWare server

- AutoNessus host
- Linux web server
- Windows Victim



Problem description

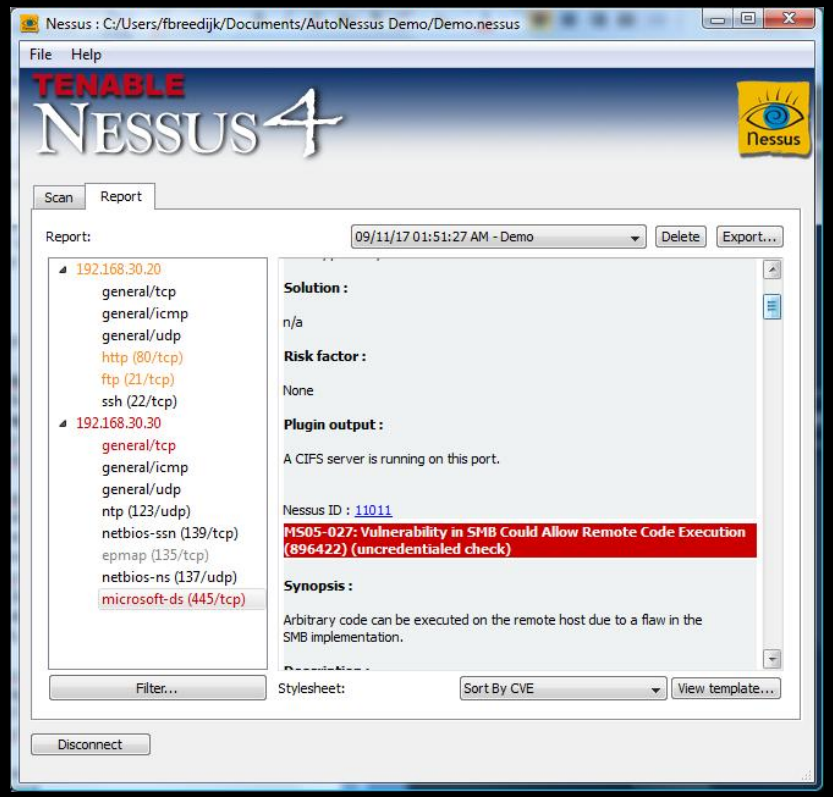
- Nessus is a very powerful vulnerability scanner
- ‘Free’ (As in beer) TCP/IP security scanner
- Best valued security scanner (sectools.org survey of 2000, 2003 and 2006)

- Nessus generates a lot of output. Maybe too much?
- Scanning takes a lot of time and is not automated
- A lot of time is spent on analysis
- Nessus GUI is not great for analyzing scans

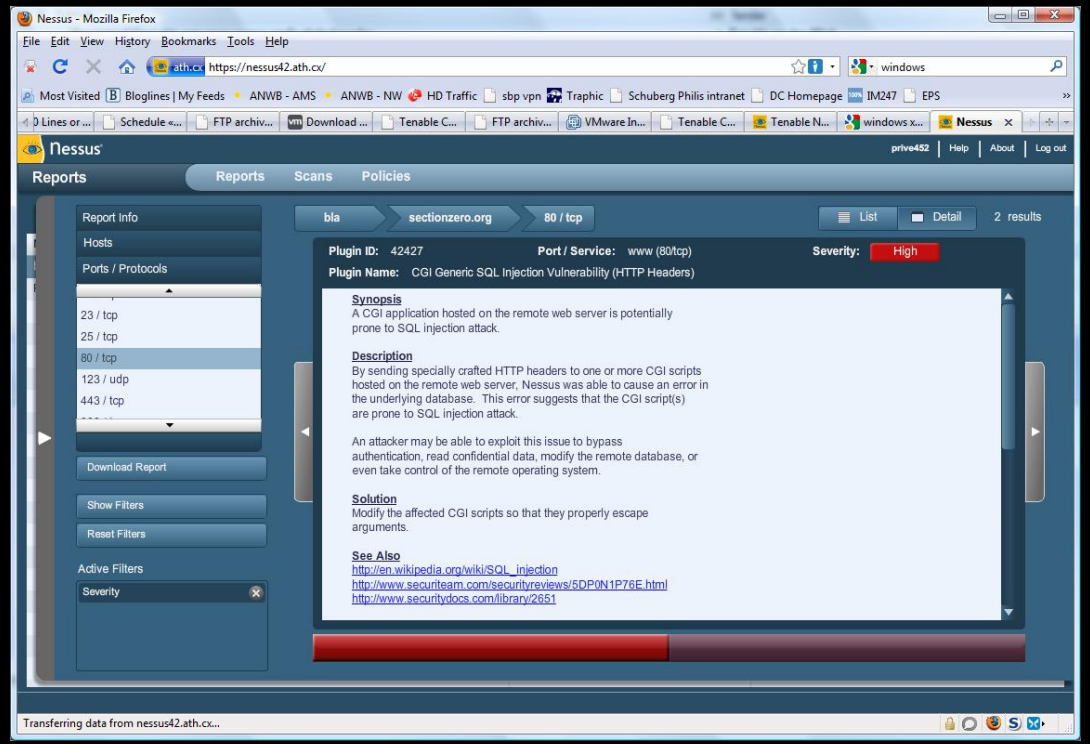
- Work risk ratio

Nessus GUI

Nessus 3/4.0 GUI



Nessus 4.2



What does AutoNessus do differently?

Scanning is started from the command line

» This means it can be started from cron

The findings are stored in a “database”

» Currently the database is a directory structure

Presentation via a WebGUI

» Easy triage via filtering

» Status allows you to “tick-off” findings

Demo

Scan is started via do-scan <scanname> (demo)

- ~/etc/config
- ~/var/<scannaam>/config
- PRESCAN command
- Adresses in hosts file are scanned using config
- /etc/<MODE>-nessusrc
- Status repor via mail to <EMAIL>
- POSTSCAN command

Status 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
```

Presentation in the Web GUI

Automatic status assignmet:

» 4 findings automatically marked as HARD MASKED

Easy triage

» Findings can be filtered by:
  - Host
  - Port
  - Plugin
  - Status

Tick off you findings by assiging them a status

» Relevant/risk OPEN

» Not relevant/no risk NO ISSUE

What happened under the hood?

The Nessus client was started via the command line.

Results where saved as:

» HTML

» XML (No longer supported as of Nessus 4.x)

» NBE

Nessus backend (.NBE) format

Simpel format

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

Findings have all fields populated, e.g.:

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

For open ports, only the first four fields are populated, e.g.:

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

Findings are converted to a directory structure

Findings

- Host
  - Port
    - Pluginid (Portscanner voor open port)
      - Remark – Text entered via web GUI
      - Status - The status given in the web GUI
      - YYYYMMDDhhmmss

This tree structure can be easily used to compare consecutive scans

Its all about status...

Assigned by AutoNessus	
NEW	Found for the first time
CHANGED	Output has changed
GONE	Not found anymore
Assigned by the User	
OPEN	Risk
NO ISSUE	No risk
FIXED	Should not trigger again
HARD MASKED	Ignore this

Hard masked, Gone, Fixed, etc...

HARD MASKED	Will be ignored
GONE / FIXED	Keeps its status untill found again
OPEN / NO ISSUE	Keeps its status untill output changes
CHANGED	Was NO ISSUE or OPEN, but output changed
NEW	Was GONE or FIXED, but reappeared

IF IT IS OK, IT IS OK

...WHY MAKE A FUZZ?

AutoNessus at Schuberg Philis

Schuberg Philis is a high end provider of managed services for Mission Critical applicaiton infrastructure

Security is a key

Customer profile:

» Bla, bla, bla

Schuberg Philis some scan statistics

Scans all external IP addresses of all customers it manages monthly

First scan: 28 August 2007

Infrastructures converge to 0 findings

IP addresses on 4 February 2009: 4038

Nessus findings January 2009: 8777

Mission Impossible without AutoNessus

Other references

Soleus
- Community provider of virtual private servers

Molecular Science Computing Facility in Richland, Washington
- 4800+ nodes

Global provider of air defense, air traffic control, airline and airport operations management, and data integration and distribution
- Approx 450 hosts

Others:
- Dutch ISP
- Treasury Software as a Service provider
- Dutch and US IT service providers
- Large Caribbean distillery
- Bink.nu – Windows technology blog
- 2 Dutch IT security firms
- Dutch multimedia company

Recap…

Monthly scanning with Nessus would mean:

» Getting up a night to start the scans

» Looking at non-informative findings (e.g. traceroute) every month

» A lot of boring repetative work, high change of errors

» A lot of work even if there are no changes to the infrastructure

So…

Monthly AutoNessus runs means:

- Scans are scheduled via crontab
- Only the findings that need attention get it
- Less errors due to less repetative work.
- The amount of effort is proportional to the amount of changes
- Risk is proportional to the amount of changes

Why did we develop and release an open source tool?

We needed it!

We decided to give something back because we use a lot of open source tools:

- Nagios
- CFEngine
- Rancid
- MRTG
- RRD tool
- Cacti
- “LAMP”
- CVS /
- Etc, etc, etc

Roadmap…

The next version of AutoNessus will…

Have a database backend
- » Better performance
- » Easier to link multiple findings to a single issue
- » Easier to link a single finding to multiple issues

Support more scanners
- » Nessus
- » OpenVAS
- » NMAP
- » Nikto
- » Others

Open architecture:
- » More scanners can be added
- » Pluggable authentication?
- » Trouble ticket integration?

More “manager” information:
- » Graphs
- » Dashboards

Who am I?

Frank Breedijk

- Security Engineer at Schuberg Philis
- Author of A[redacted]
- Blogger for CupFigther.net

Email: fbreedijk@schubergphilis.com
Twitter: @a[redacted]
Blog: http://cupfighter.net
Project: http://a[redacted].com

Seccubus

The prize goes to…

Jason Mansfield

http://clinicallyawesome.com

Who am I?

Frank Breedijk

- Security Engineer at Schuberg Philis
- Author of ~~Se[illegible]~~
- Blogger for CupFigther.net

Email: fbreedijk@schubergphilis.com
Twitter: ~~@se[illegible]~~
Blog: http://cupfighter.net
Project: ~~http://se[illegible]~~