Seccubus

Analyzing vulnerability assessment data the easy way…

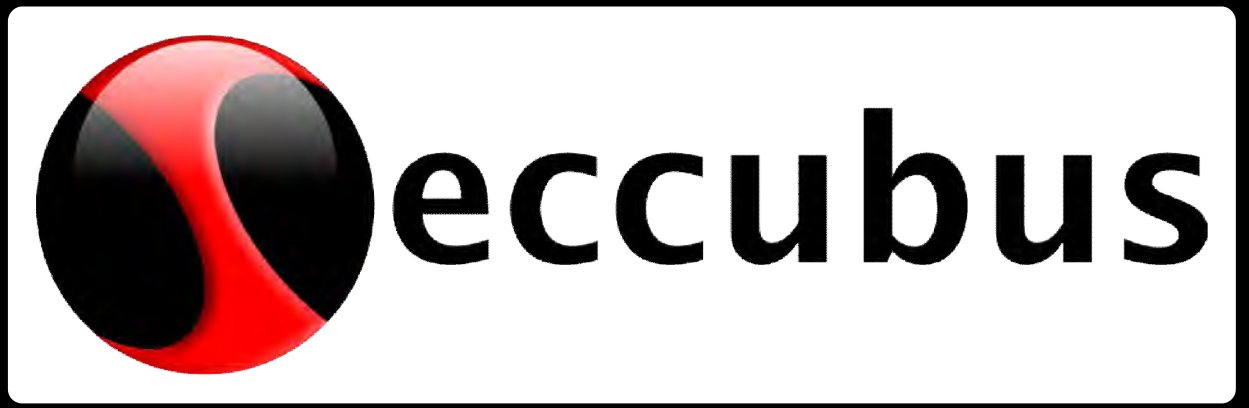


Photo taken by Arthur van Schendel

Who am I?

Frank Breedijk

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

Email: fbreedijk@schubergphilis.com
Twitter: @Seccubus
Blog: http://cupfighter.net
Project: http://www.seccubus.com
Company: http://www.schubergphilis.com

These and all non-attributed photos of Frank Breedijk are taken by Jan Jacob Bos

A story about two guys…

C. Lueless

Mission: Perform a weekly vulnerability scan of all our public IP addresses

B. Rightlad

C. Lueless…

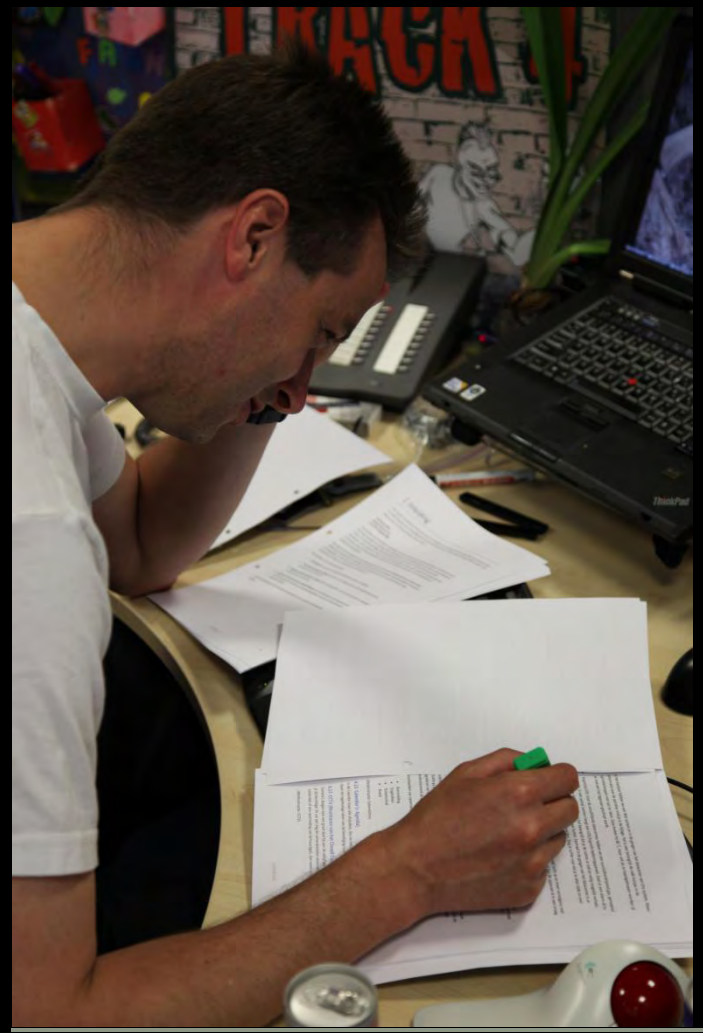
Decides to use a regular vulnerability scanner…

…needs to get up very early

…manually starts his scan and waits…

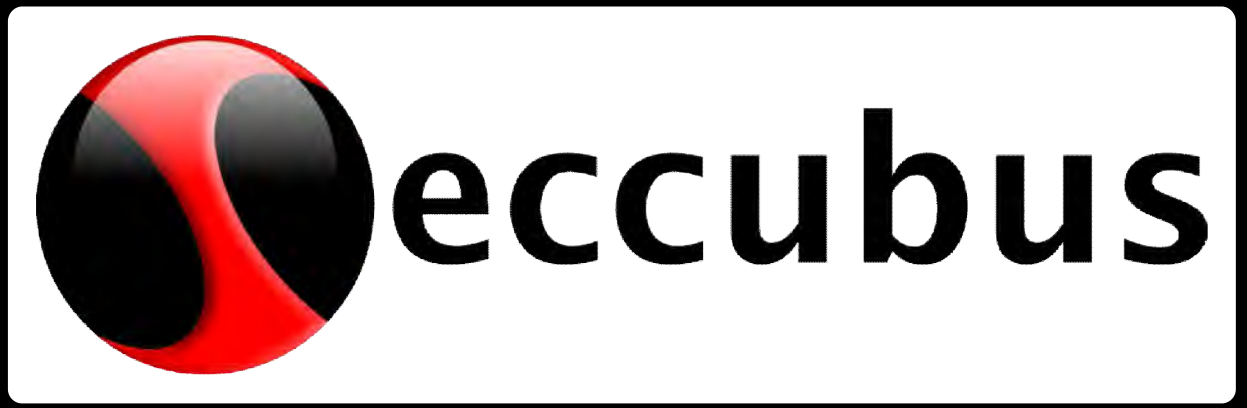
…finishes the scan and goes back to sleep…

… and analyzes the report in the morning



B. Rightlad

Uses Seccubus…



… he spends the morning configuring Seccubus…

… goes home …

... Relaxes ...

Image: Orion's Umbra, a Creative Commons Attribution Non-Commercial (2.0) image from jahdakinebrah's photostream

… the scanning happens at night …

… and when he wakes up …

… he can analyze the findings and remediate

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

What is Seccubus…

» Seccubus is a wrapper around vulnerability scanners

» GUI is geared towards analyzing and “ticking-off” findings that have been seen

» Compares consecutive scans

» Supports multiple scanners:
- Nessus
- OpenVAS
- Nikto
- More to follow

What does Seccubus 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

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

A Seccubus scan…

DEMO

Let us commence to week two

C. Lueless…

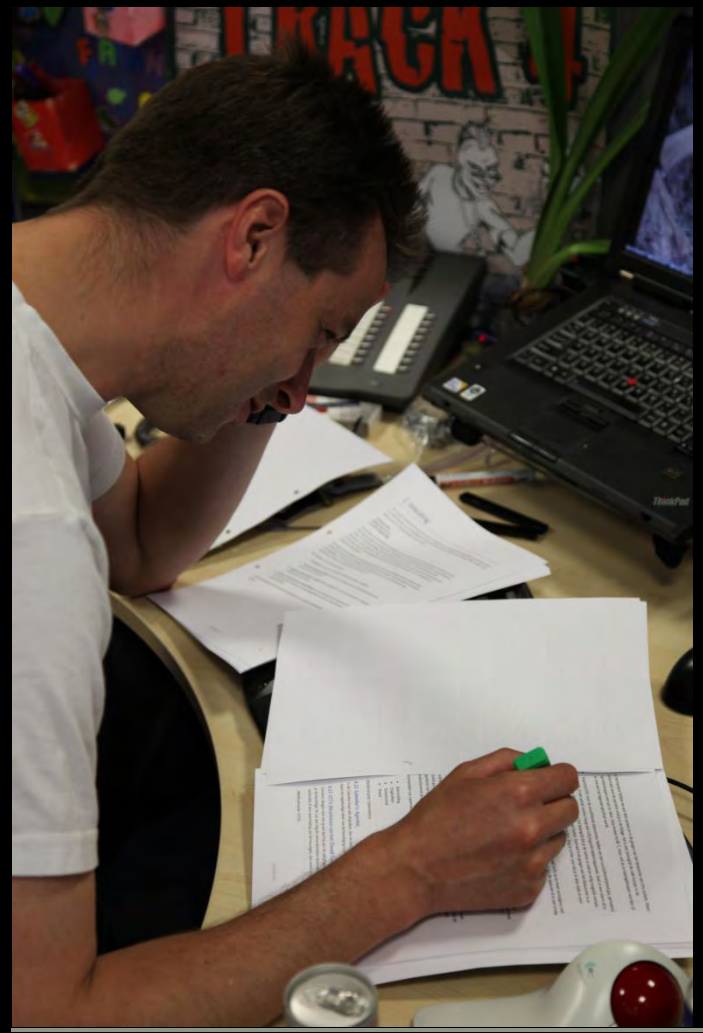
Decides to use a regular vulnerability scanner…

…needs to get up very early

…manually starts his scan and waits…

…finishes the scan and goes back to sleep…

… and analyzes the report in the morning

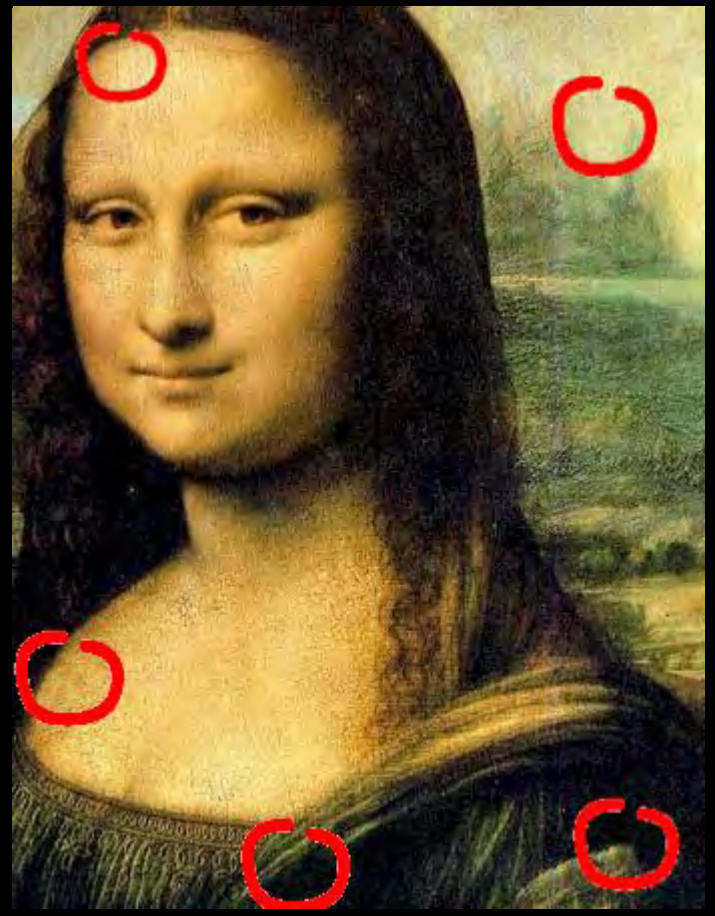


Images taken from http://www.art-games.co.uk

Would the effort be worth it?

Week 1

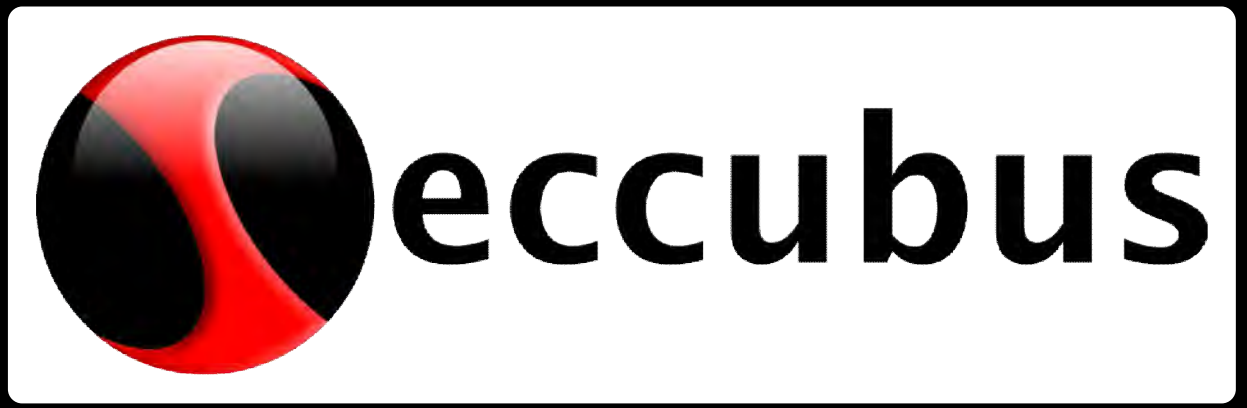
Spot the differences…



Week 2

B. Rightlad

Uses Seccubus…



… the scan is scheduled, he can simply go home …

... relax ...

Image: Half Moon, a Creative Commons Attribution Non-Commercial No-Derivative-Works (2.0) image from za3tooor's photostream

… the scanning happens at night …

… and when he wakes up …

… he can analyze the findings and remediate

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

It’s all about status...

Assigned by Seccubus	
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

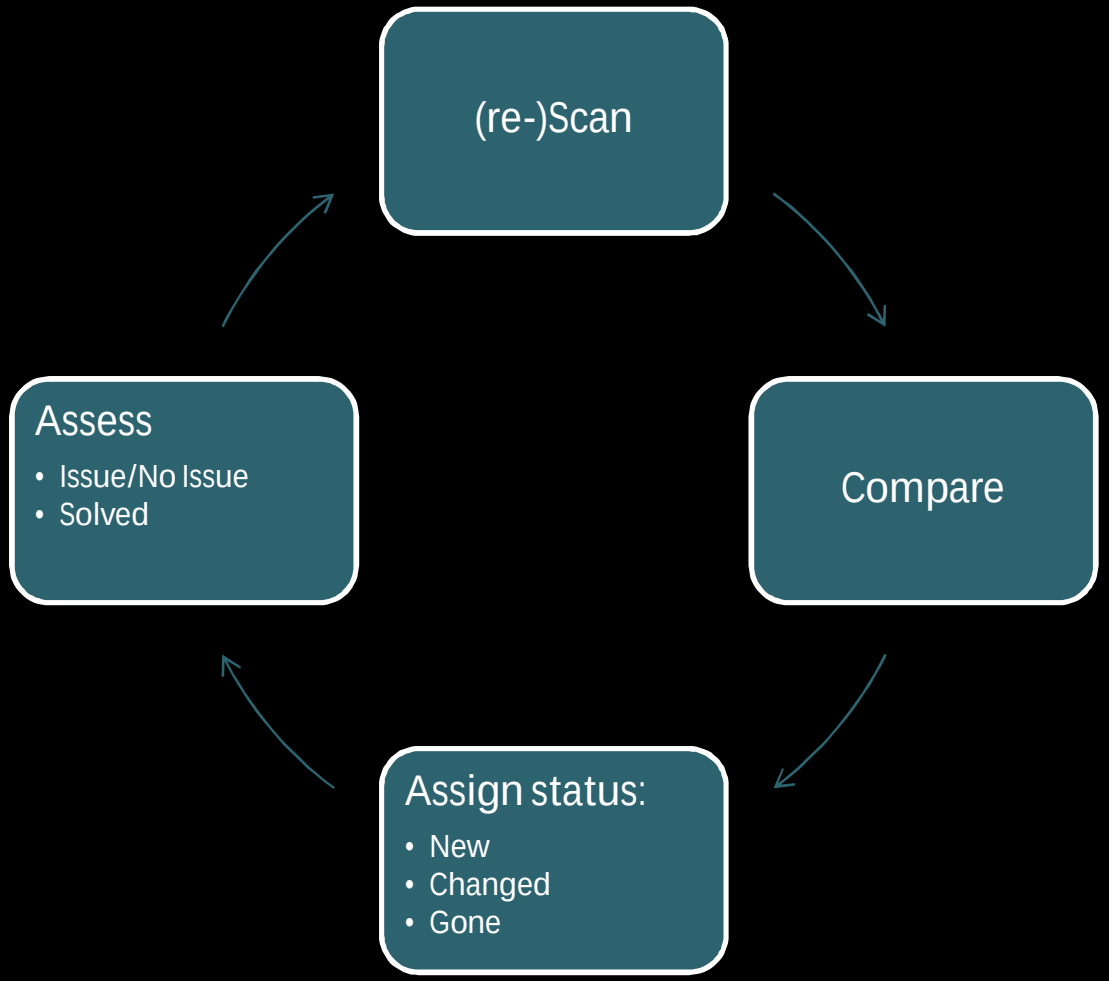
Hard masked, Gone, Fixed, etc...

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?

The scanning cycle...



DEMO

Image: Cosas hechas, a Creative Commons Attribution Non-Commercial (2.0) image from srgblog's photostream

Let us commence to week three

C. Lueless…

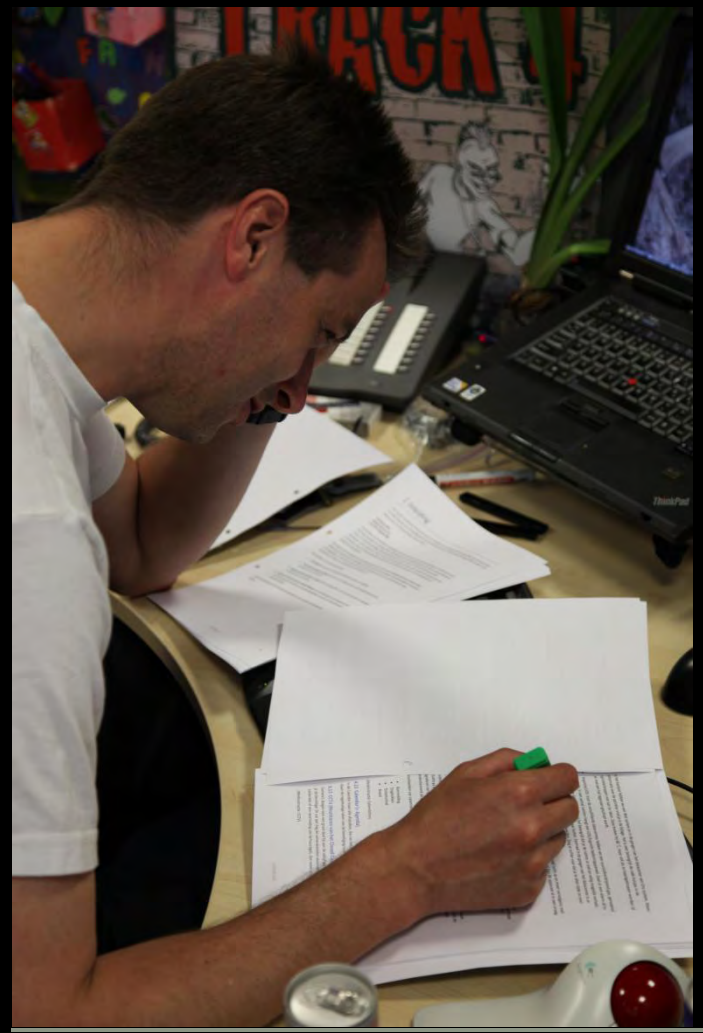
Decides to use a regular vulnerability scanner…

…needs to get up very early

…manually starts his scan and waits…

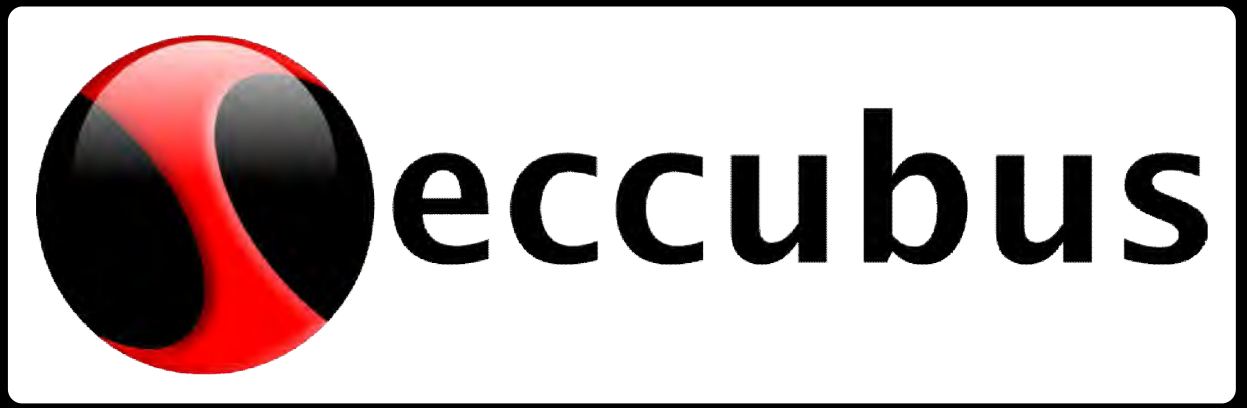
…finishes the scan and goes back to sleep…

… and analyzes the report in the morning



B. Rightlad

Uses Seccubus…



… the scan is scheduled, he can simply go home …

... relax ...

Image: Himalayan Moonrise, a Creative Commons Attribution Non-Commercial No-Derivative-Works (2.0) image from swamysk's photostream

… the scanning happens at night …

… and when he wakes up …

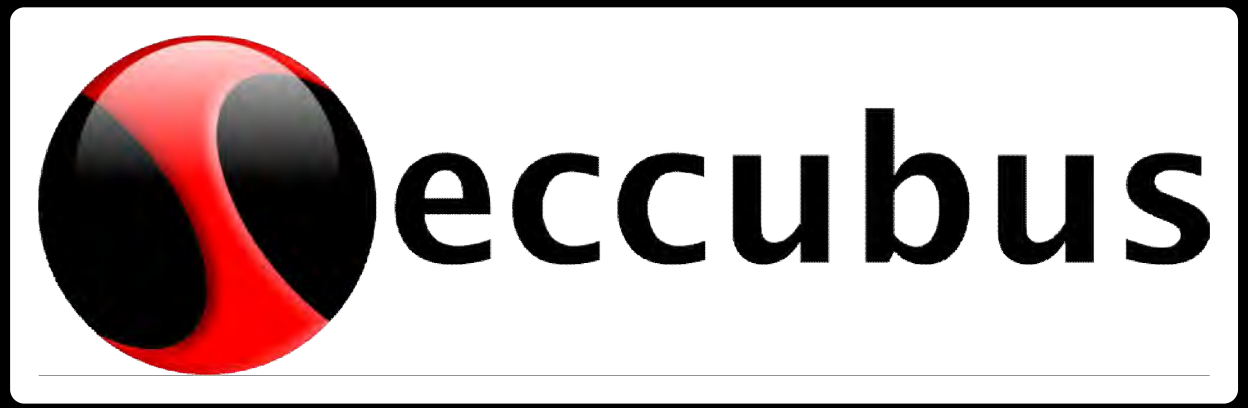
… he can analyze the findings and remediate

That’s in a name?

Succubus

In seccubus

Seccubus



Just to show you…

DEMO

Seccubus at Schuberg Philis

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

Security is key...

We focus exclusively on the applications that businesses rely on 24 hours a day, guaranteeing 100% uptime; a focus that we feel is instrumental in providing
high-quality services

Our customer profile

- Large sized to medium enterprises
- Operating in regulated markets
- Strong focus on governance and change/risk management
- Balance between control, flexibility and innovation
- Augmenting corporate IT shared service centers or specific business unit as a specialist
- Application partnership with critical application vendors

- Rabobank, ING, ABN Amro, Energy Trading Floors, Deloitte, Bol.com…

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 Seccubus

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
- Bacardi
- 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 manually 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 Seccubus runs means:

» Scans are scheduled via crontab

» Only the findings that need attention get it

» Less errors due to less repetitave work.

» The amount of effort is proportional to the amount of changes

» Risk is proportional to the amount of changes

Image: Apples & Oranges - They Don't Compare, a Creative Commons Attribution (2.0) image from thebusybrain's photostream

Compare

Image: Slimmer, a Creative Commons Attribution Non-Commercial No-Derivative-Works (2.0) image from mkmabus's photostream

Dramatic reduction

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
- ……

Roadmap…

What is up for next versions of Seccubus?

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
- » Nikto (v1.5)
- » NMAP (v2.0)
- » Metasploit/Metasploit express (v2.1)
- » Others ?

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

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

The ultimate goal…

Image: Hang On, a Creative Commons Attribution Non-Commercial No-Derivative-Works (2.0) image from brraveheart's photostream

We need your help…

- Coding
- Requirements
- User interface design
- Report design
- Testers
- Users

Metasploit Express

METASPLOIT express

@Jabra if you contact somebody at @seccubus ya. I think I know a few ppl generating xml test data in the software

RT @Jabra: generating xml test data in

@seccubus change ur slides.... module

@Jabra thanks man, this really cool.

Metasploit Express module will be released during the @seccubus talk at #defcon #metasploit

about 1 hour ago via mobile web

Retweeted by 2 people

Reply Retweet

Jabra

Josh Abraham

Roadmap…

What is up for next versions of Seccubus?

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
- » Nikto (v1.5)
- » NMAP (v2.0)
- » Metasploit/Metasploit express (v2.1)
- » Others ?

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

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

New release

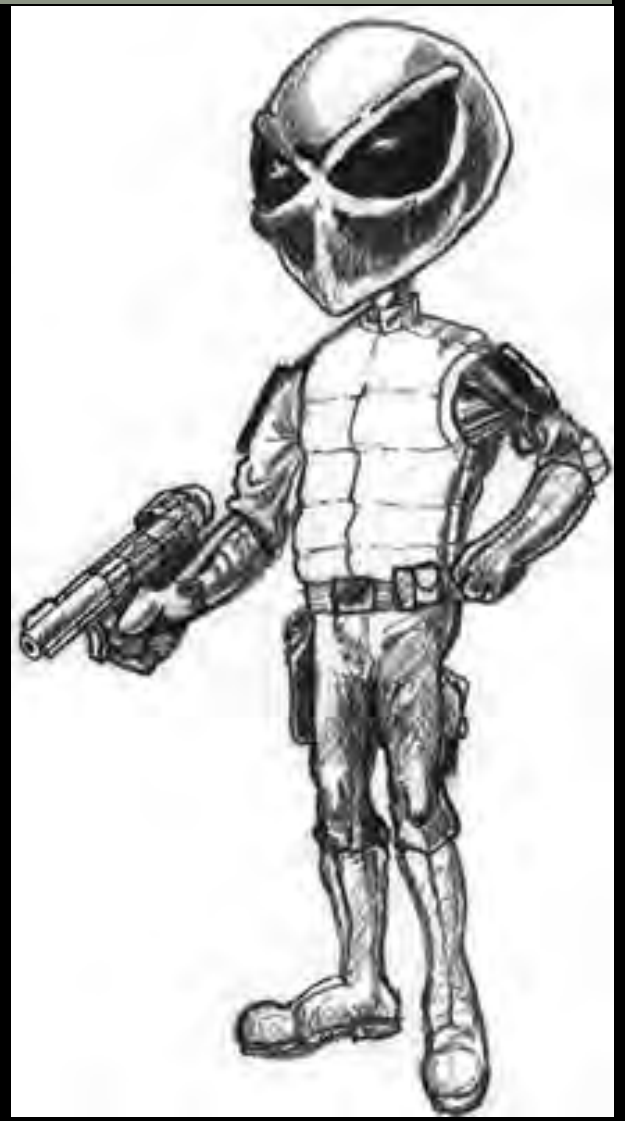
V1.5

The DefCon edition

SCHUBERG PHILIS

Nikto scanning

- Nikto version 2.1.3 supports .nbe output
- Nikto can be launched natively from the box running Seccubus
- Each line in the Nikto output becomes a finding in Seccubus



Installation package

Version 1.5 can be installed via an RPM package

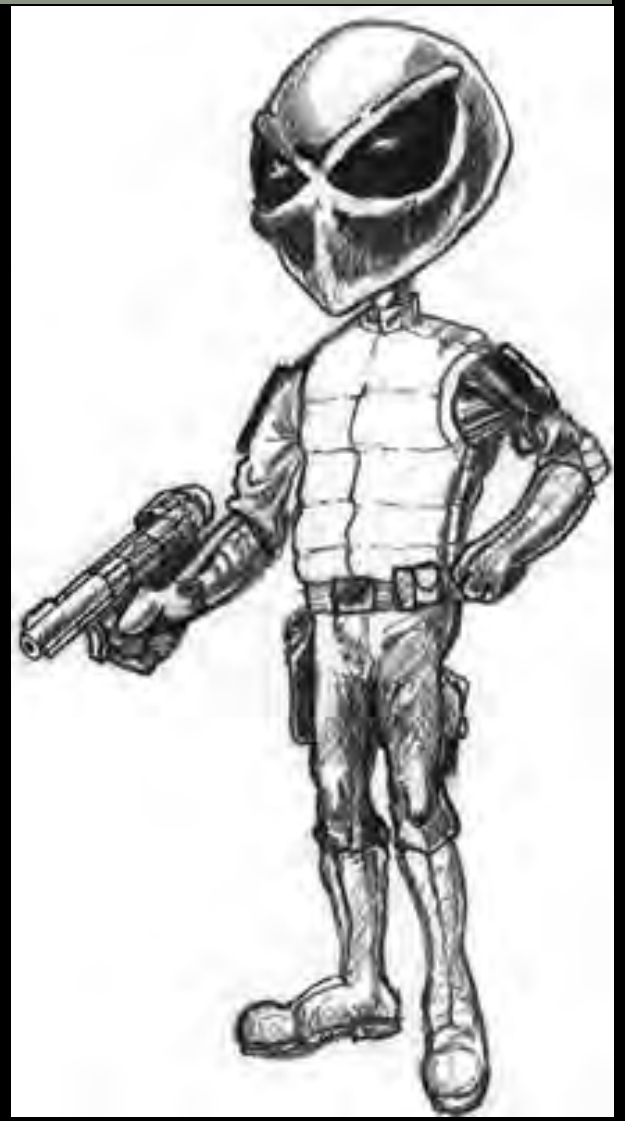
Image: Revs Per Minute, a Creative Commons Attribution (2.0) image from msvg's photostream

Compliance

Seccubus v1.5 can handle Nessus compliance jobs

Nikto scanning

- Nikto version 2.1.3 supports .nbe output
- Nikto can be launched natively from the box running Seccubus
- Each line in the Nikto output becomes a finding in Seccubus



Seccubus.com

Image: What now?, a Creative Commons Attribution No-Derivative-Works (2.0) image from laurenclose's photostream

Questions?

Photo taken by Arthur van Schendel

Who am I?

Frank Breedijk

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

Email: fbreedijk@schubergphilis.com
Twitter: @Seccubus
Blog: http://cupfighter.net
Project: http://www.seccubus.com
Company: http://www.schubergphilis.com