
Seccubus

Analyzing vulnerability assessment data the easy way...

Who am I?

Frank Breedijk

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

Email: fbreedijk@schubergphilis.com

Twitter: [@Seccubus](https://twitter.com/Seccubus)

Blog: <http://cupfighter.net>

Project: <http://www.seccubus.com>

Company: <http://www.schubergphilis.com>



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



SCHUBERG PHILIS

...manually starts his scan and waits...



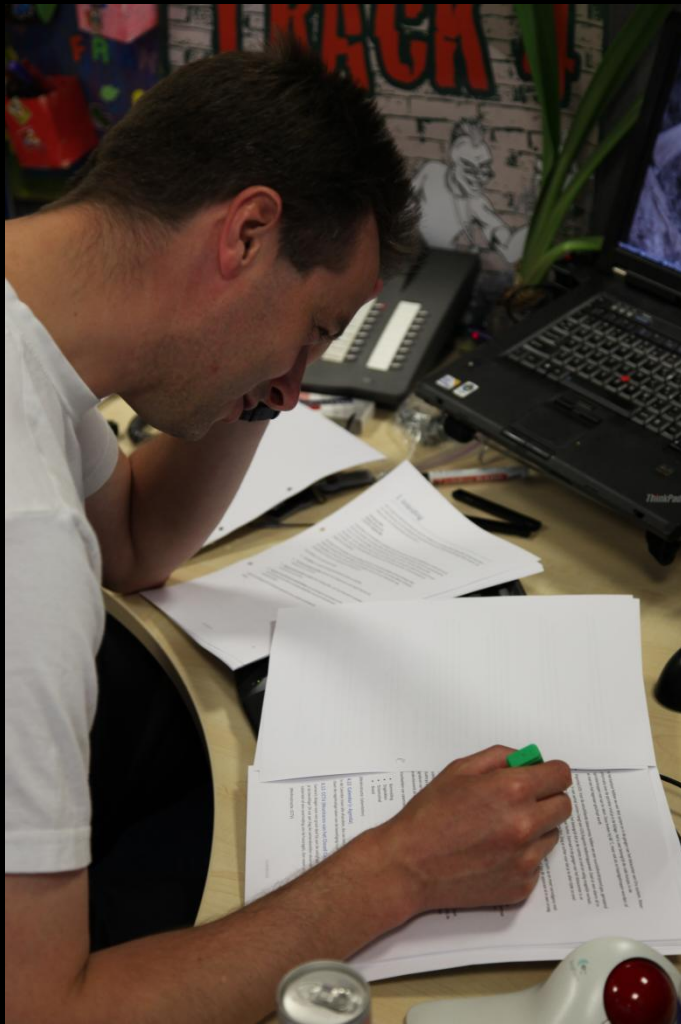
SCHUBERG PHILIS

...finishes the scan and goes back to sleep...



SCHUBERG PHILIS

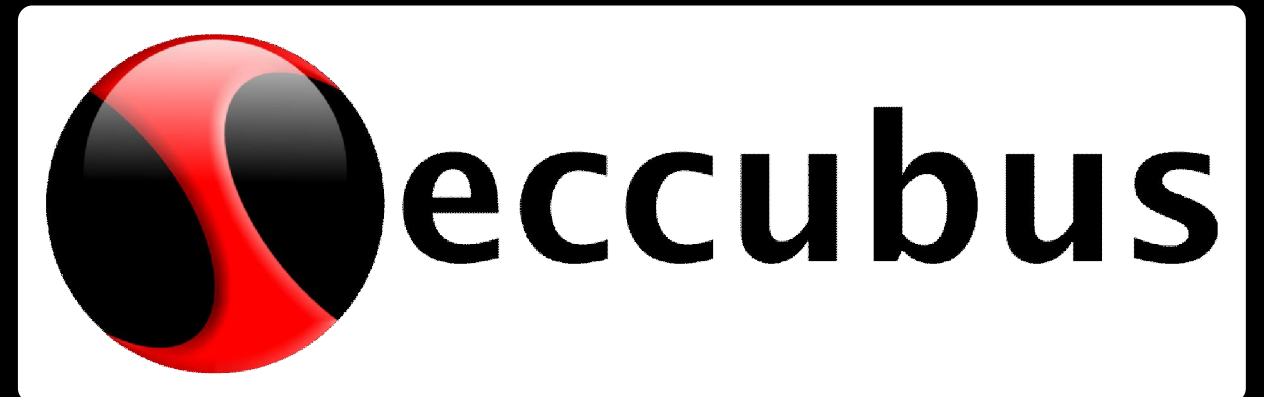
... and analyzes the report in the morning



SCHUBERG PHILIS

B. Rightlad

Uses Seccubus...



... he spends the morning configuring Seccubus...



... goes home ...



SCHUBERG PHILIS

... Relaxes ...



SCHUBERG PHILIS

... the scanning happens at night ...



... and when he wakes up ...



SCHUBERG PHILIS

... he can analyze the findings and remediate



A Seccubus scan...

DEMO

SCHUBERG PHILIS

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

Let us commence to week two



C. Lueless...

Decides to use a regular vulnerability scanner...



...needs to get up very early



SCHUBERG PHILIS

...manually starts his scan and waits...



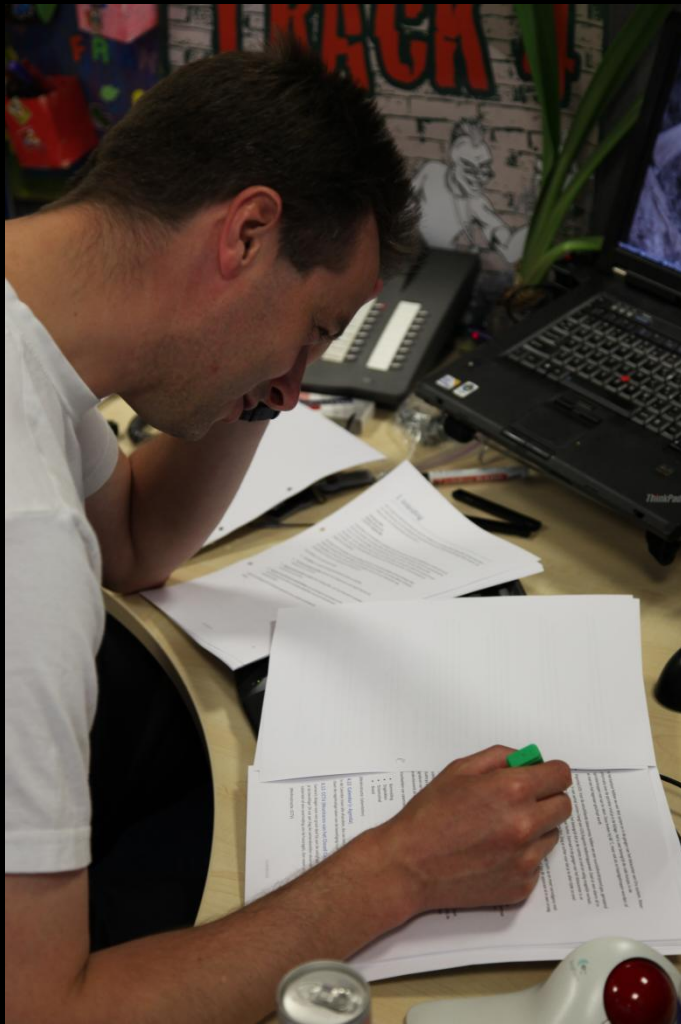
SCHUBERG PHILIS

...finishes the scan and goes back to sleep...



SCHUBERG PHILIS

... and analyzes the report in the morning



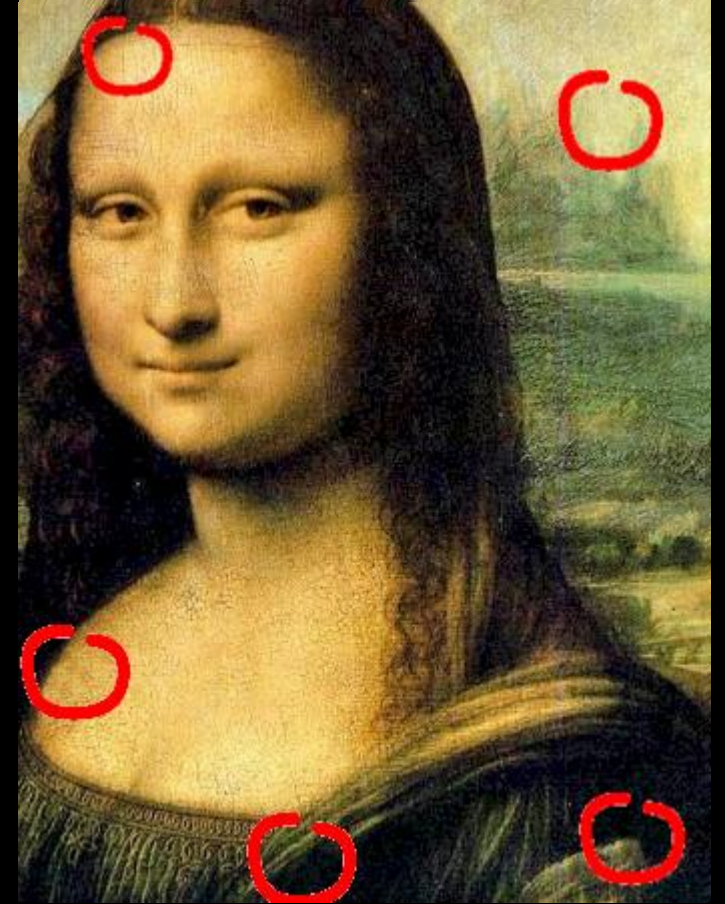
SCHUBERG PHILIS

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 ...



SCHUBERG PHILIS

... relax ...



SCHUBERG PHILIS

... the scanning happens at night ...



Za3t0o0r!!

... and when he wakes up ...



SCHUBERG PHILIS

... he can analyze the findings and remediate



The delta engine at work

DEMO

SCHUBERG PHILIS

Let us commence to week three



C. Lueless...

Decides to use a regular vulnerability scanner...

...needs to get up very early



SCHUBERG PHILIS

...manually starts his scan and waits...



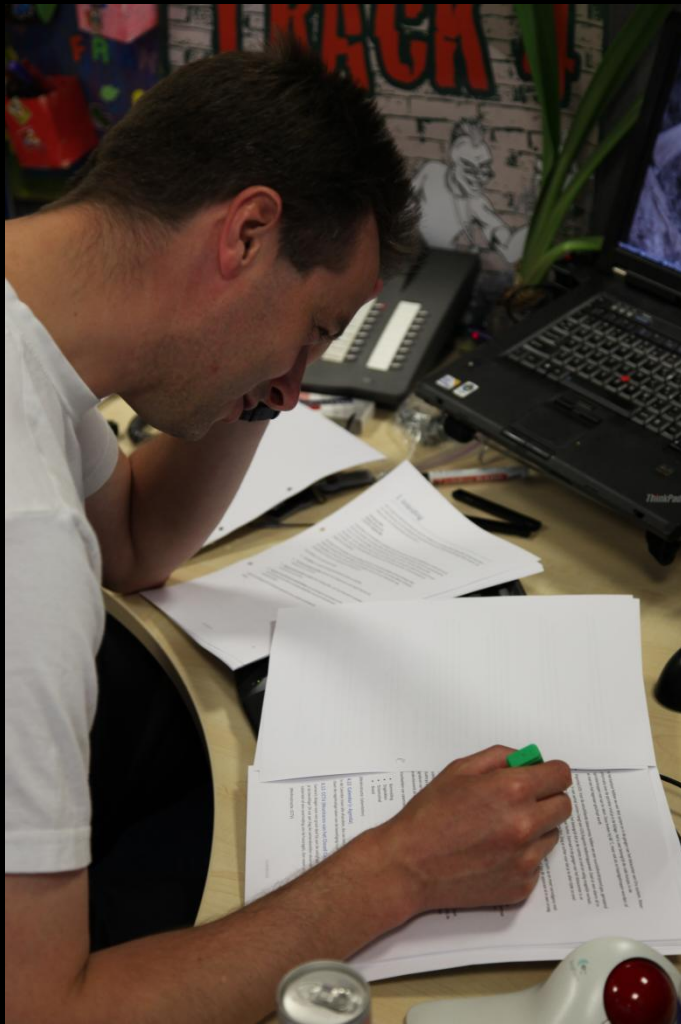
SCHUBERG PHILIS

...finishes the scan and goes back to sleep...



SCHUBERG PHILIS

... and analyzes the report in the morning



SCHUBERG PHILIS

B. Rightlad

Uses Seccubus...



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



SCHUBERG PHILIS

... relax ...



SCHUBERG PHILIS

... the scanning happens at night ...



... and when he wakes up ...



SCHUBERG PHILIS

... he can analyze the findings and remediate



Just to show you...

DEMO

SCHUBERG PHILIS

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 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

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?

How about a third scan (Chapter 5)

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 IDB, Eneco Energy Trading, Deloitte,...

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 start the scans
- » Looking at non-informative findings (e.g. traceroute) every month
- » A lot of boring repetitive 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 repetitive 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
- »

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

- » NMAP
- » Metasploit/Metasploit express?
- » Others ?

Open architecture:

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

More "manager" information:

- » Graphs
- » Dashboards

New release

V1.5

SCHUBERG PHILIS

Installation package

Version 1.5 can be installed via an RPM package



Compliance

Seccubus v1.5 can handle Nessus compliance jobs



Compliance Checks Tools
Download compliance check policy tools and documentation.



CIS Compliance Audit Policies
CIS certified configuration audit policies for Windows, Solaris, Red Hat, FreeBSD and many other operating systems.



Sensitive Content Audit Policies
Audit policies that look for Credit Cards, Social Security numbers and many other types of sensitive data.



Configuration Audit Policies
Audit policies based on CERT, DISA STIG, GLBA and HIPAA standards.



Windows Audit Policies
Audit policies based upon standard Microsoft security templates.



Cisco Audit Policies
Audit policies that perform configuration audits for IOS-based Cisco devices.



Antivirus Audit Policies
Audit policies designed to allow users to determine if an antivirus package is installed and set to a working state.



Virus Detection Audit Policies
Audit policies that Tenable's Research group has produced that scan for known trojans and rootkits.



PCI Audit Policies
Audit policies developed by Tenable to test AIX, HP-UX, Linux, Solaris and Windows systems for minimum required PCI configuration settings.



Tenable Application Audit Policies
Audit policies that examine hosts to determine if Tenable software applications exist and notifies of the presence and state of these packages.



Database Audit Policies
Audit policies designed to allow users to audit their database configuration using the Nessus Database Compliance Check plugin.



Control System Audits
Nessus audit policies are available for a wide variety of Control Systems and SCADA applications from Digital Bond.



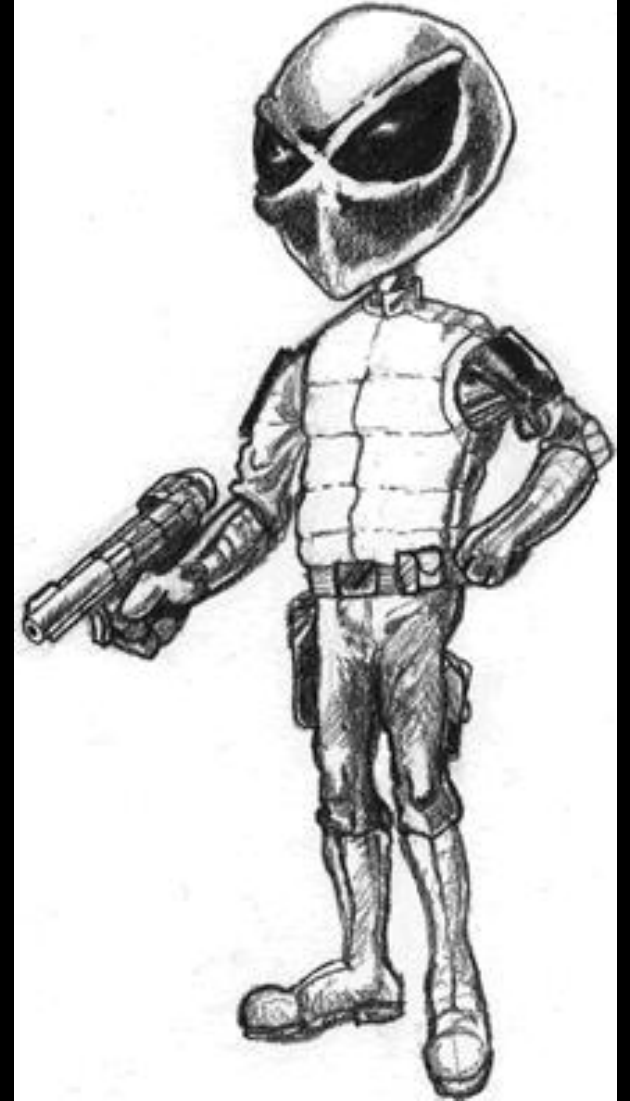
Nessus NIST and FDCC Compliance Audit Policies
Audit policies that perform FDCC and NIST SCAP configuration audits. These audit files test for the required settings specified by the NIST SCAP and FDCC programs.



SecurityCenter NIST and FDCC Compliance Audit Policies
Audit policies that perform FDCC and NIST SCAP configuration audits. These audit files were generated directly from the XCCDF SCAP content and are suitable for reporting to OMB.

Nikto scanning

- » Nikto version 2.1.2 supports .nbe output
- » Nikto can be launched natively from the box running Seccupus
- » Each line in the Nikto output becomes a finding in Seccupus



Questions?



Who am I?

Frank Breedijk

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

Email: fbreedijk@schubergphilis.com

Twitter: [@Seccubus](https://twitter.com/Seccubus)

Blog: <http://cupfighter.net>

Project: <http://www.seccubus.com>

Company: <http://www.schubergphilis.com>

