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
Blog: http://cupfighter.net
Project: http://www.seccubus.com
Company: http://www.schubergphilis.com
A story about two guys...

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

» 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 were saved as:
» HTML
» XML (No longer supported as of Nessus 4.x)
» NBE
A Seccubus scan...
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
Would the effort be worth it?

Spot the differences...

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

Week 1

Week 2
B. Rightlad

Uses Seccubus...
... the scan is scheduled, he can simply go home ...
... relax ...
... the scanning happens at night ...
... and when he wakes up ...
... he can analyze the findings and remediate
Nessus backend (.NBE) format

Simpel format

\(<type>\) | \(<\text{netwerk}>\) | \(<ip>\) | \(<port>\) | \(<\text{plugin ID}>\) | \(<\text{prio}>\) | \(<\text{plugin output}>\)

Findings have all fields populated, e.g.:

- results\|192.168.157\|192.168.157.30\|ntp (123/udp)\|10884\|Security Note\nSynopsis:

An 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...

<table>
<thead>
<tr>
<th>Assigned by Seccubus</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>NEW</td>
<td>Found for the first time</td>
</tr>
<tr>
<td>CHANGED</td>
<td>Output has changed</td>
</tr>
<tr>
<td>GONE</td>
<td>Not found anymore</td>
</tr>
<tr>
<td>Assigned by the User</td>
<td></td>
</tr>
<tr>
<td>OPEN</td>
<td>Risk</td>
</tr>
<tr>
<td>NO ISSUE</td>
<td>No risk</td>
</tr>
<tr>
<td>FIXED</td>
<td>Should not trigger again</td>
</tr>
<tr>
<td>HARD MASKED</td>
<td>Ignore this</td>
</tr>
</tbody>
</table>
Hard masked, Gone, Fixed, etc...

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HARD MASKED</td>
<td>Will be ignored</td>
</tr>
<tr>
<td>GONE / FIXED</td>
<td>Keeps its status until found again</td>
</tr>
<tr>
<td>OPEN / NO ISSUE</td>
<td>Keeps its status until output changes</td>
</tr>
<tr>
<td>CHANGED</td>
<td>Was NO ISSUE or OPEN, but output changed</td>
</tr>
<tr>
<td>NEW</td>
<td>Was GONE or FIXED, but reappeared</td>
</tr>
</tbody>
</table>
WHY MAKE A FUZZ?

IF IT IS OK, IT IS OK

...WHY MAKE A FUZZ?
The scanning cycle...

(re-)Scan

Assess
- Issue/No Issue
- Solved

Compare

Assign status:
- New
- Changed
- Gone
The delta engine at work
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 ...
... 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

SCHUEBERG PHILIS
Just to show you...
Seccubus at Schuberg Philis

Schuberg Philis is a high end provider of managed services for Mission Critical application 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 repetitive work.

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

» Risk is proportional to the amount of changes
Compare
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...
We need your help…

» Coding

» Requirements

» User interface design

» Report design

» Testers

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

Seccubus v1.5 can handle Nessus compliance jobs.

<table>
<thead>
<tr>
<th>Compliance Checks Tools</th>
<th>CIS Compliance Audit Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Download compliance check policy tools and documentation.</td>
<td>CIS certified configuration audit policies for Windows, Solaris, Red Hat, FreeBSD and many other operating systems.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sensitive Content Audit Policies</th>
<th>Configuration Audit Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit policies that look for Credit Cards, Social Security numbers and many other types of sensitive data.</td>
<td>Audit policies based on CERT, DISA STIG, GLBA and HIPAA standards.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Windows Audit Policies</th>
<th>Cisco Audit Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit policies based upon standard Microsoft security templates.</td>
<td>Audit policies that perform configuration audits for IOS-based Cisco devices.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Antivirus Audit Policies</th>
<th>Virus Detection Audit Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit policies designed to allow users to determine if an antivirus package is installed and set to a working state.</td>
<td>Audit policies that Tenable’s Research group has produced that scan for known trojans and rootkits.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PCI Audit Policies</th>
<th>Tenable Application Audit Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit policies developed by Tenable to test AV, HP-UX, Linux, Solaris and Windows systems for minimum required PCI configuration settings.</td>
<td>Audit policies that examine hosts to determine if Tenable software applications exist and notify of the presence and estate of those packages.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Database Audit Policies</th>
<th>Control System Audits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit policies designed to allow users to audit their database configuration using the Nessus Database Compliance Check plugin.</td>
<td>Nessus audit policies are available for a wide variety of Control Systems and SCADA applications from Digital Bond.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Nessus NIST and FDDC Compliance Audit Policies</th>
<th>SecurityCenter NIST and FDDC Compliance Audit Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit policies that perform FDDC and NIST SCAP configuration audits. These audit files test for the required settings specified by the NIST SCAP and FDDC programs.</td>
<td>Audit policies that perform FDDC and NIST SCAP configuration audits. These audit files were generated directly from the XCCDF SCAP content and are suitable for reporting to OMB.</td>
</tr>
</tbody>
</table>
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
Questions?
Who am I?

Frank Breedijk

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

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