SCHUBERG PHILIS

Seccubus Workshop

Exercises and guidelines

for:	SigInt 2010
date:	22 May 2010
version:	0.1
author:	Frank Breedijk
status:	Public

Schuberg Philis BV
Star Parc,Boeing Avenue 271
1119 PD Schiphol-Rijk
T +31 20 750 65 00
F +31 20 750 65 50
The Netherlands
www.schubergphilis.com

MISSION CRITICAL OUTSOURCING

Table of contents

1 Workshop Setup

This workshops makes heavy use of VMWare virtual machines to do the scanning. On the USB stick you will find:

- This document
- 3 virtual machines
    - Seccubus host
    - Webserver
    - Windows XP SP2 Unpatched
- Several version of VMWare player

If you do not have VMWare player installed, install it now. To install the Linux versions type the one of the following command as root:
VMware-Player-3.0.1-227600.i386.bundle # for 32 bit
VMware-Player-3.0.1-227600.x86_64.bundle # for 64 bit

Start all the virtual machines, the following network setup is assumed:

- All virtual machines are connected to the NAT network
- The IP addresses of the NAT network are: 192.168.237.0/24
- The IP address of your local machine is 192.168.237.2
- The VM use the following IP addresses:
    - Seccubus host: 192.168.237.10
    - Webserver: 192.168.237.20
    - XP: 192.168.237.30

Log into both linux boxes (root/toor)

2 Doing a Nessus scan the conventional way

This exercise requires Flash!
From you local machine open the following URL: https://192.168.237.10:8834, this will take you to the Nessus GUI.
In the Nessus GUI click on Scans, then launch the demo scan.

When the scan is finished, go to reports to see the results. Would you want to read through this every month?

3 Your First Seccubus scan

3.1 Starting the scan

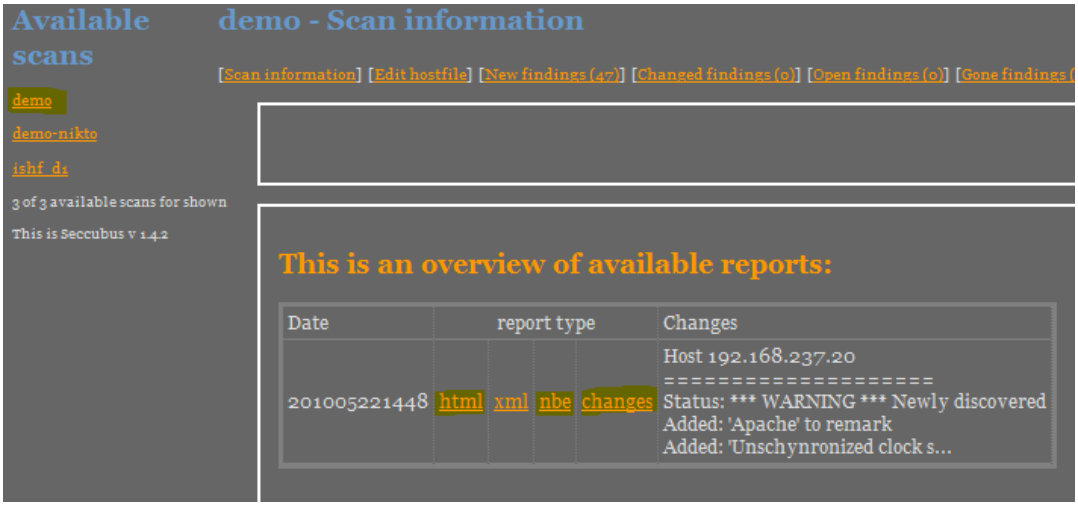
Now we are going to start and analyse our first Seccubus scan.

- Log into the Seccubus box as root
- Become user seccubus (su – seccubus)
- Start the demo scan by running: ~/bin/do-scan demo

3.2 Analysing the scan

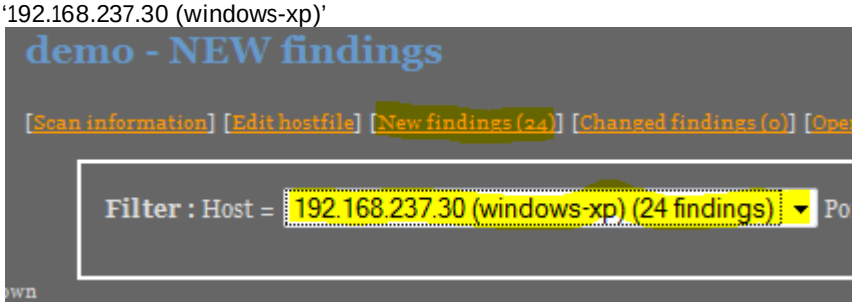
When the scan is finished we are going to look at the results:

- Point your browser at: http://192.168.237.10/
- Click on the scan labelled “demo”

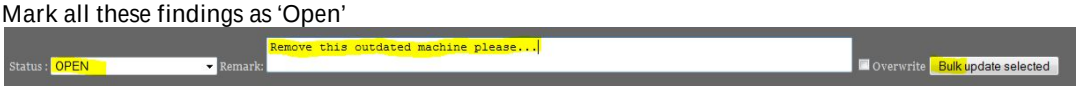


In this screen you can download the html or nbe version on the scan report and look at the changes detected by Seccubus.

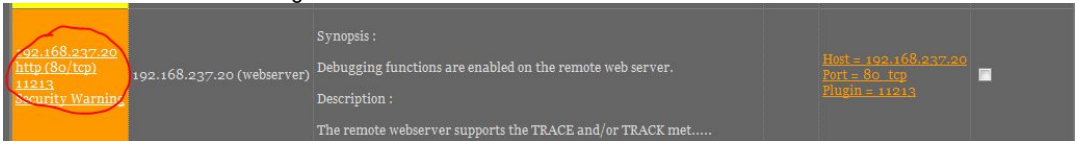
Next we are going to set statuses for findings. Click on ‘New Findings’ and filter for host ‘192.168.237.30 (windows-xp)’



Mark all these findings as ‘Open’



- Clear the host filter
- Filter for port 21 and mark all findings as ‘OPEN’, becaus having FTP open is a policy violation.
- Filter for port 22 and mark all findings as ‘NO ISSUE’
- Do the same of general_icmp and general_tcp
- Clear all filters
- Click on the finding about “TRACE”



- Mark this finding as open
- Refresh the list
- Mark all other findings as no issue

3.3 Cleaning up

Webserver

- Log into the webserver and stop the ftp daemon by running service vsftpd stop
- Copy /root/http.conf-second to the apache configuration (cp /root/http.conf-second /etc/httpd/conf/httpd.conf)
- Restart the webserver (service httpd restart)

Windows XP host

- Stop the virtual machine

4 Seccubus scan #2

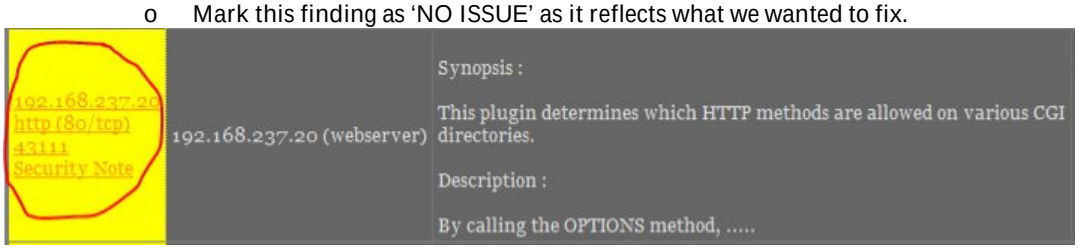
4.1 Running the scan

Starting the scan has not changed:

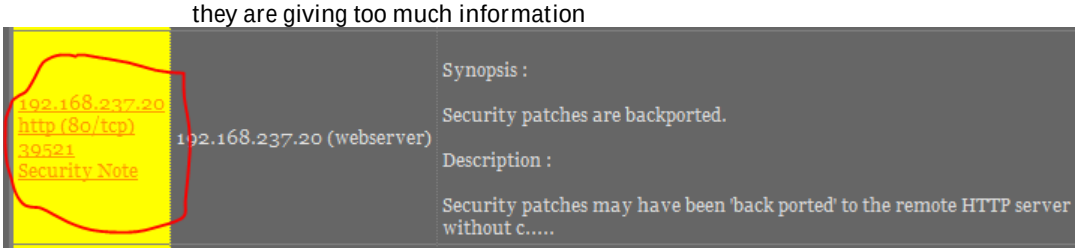
- As seccubus user run ~/bin/do-scan demo

4.2 Analysing the results

- Click the demo link again to refresh the findings list
- Start with the 'GONE' findings
  - These findings can all be marked a 'FIXED' because we do not want them to reappear
- Now go the change findings.
  - Mark this finding as 'NO ISSUE' as it reflects what we wanted to fix.



  - Mark the other findings as 'OPEN' because they are giving too much information
- Now go to the 'NEW' findings.
  - Mark the finding below as 'NO ISSUE' and the other findings as 'OPEN' because they are giving too much information



4.3 Cleaning up

Webserver

- Copy /root/http.conf-third to the apache configuration (cp /root/http.conf-third /etc/httpd/conf/httpd.conf)
- Restart the webserver (service httpd restart)

5 Running a third scan

5.1 Running the scan

Starting the scan has not changed:

- As seccubus user run ~/bin/do-scan demo

5.2 Analysing the results

By now you should get it...

6 Running a Nikto scan

Running Nikto scan will be supported from Seccubus v1.5.0 and requires a specific Nikto version (currently in development). The Nikto version on the VMs is patched to produce .nbe output.

By editing the configuration and setting MODE=nikto you can start Nikto straight from Seccubus.

6.1 Running the scan

Starting the scan demo-nikto:

- As seccubus user run ~/bin/do-scan demo-nikto

6.2 Analysing the scan

While normally these findings would not be o.k. we are going to mark all findings as no issue

6.3 Breaking the machine

We will now introduce a vulnerability on the webserver:

- Copy /root/http.conf-first to the apache configuration (cp /root/http.conf-first /etc/httpd/conf/httpd.conf)
- Restart the webserver (service httpd restart)

7 Second Nikto scan

Starting the scan demo-nikto:

- As seccubus user run ~/bin/do-scan demo-nikto

7.1 Analysing the scan

You will notice that there is one changed and one new finding.