SECCUBUS WORKSHOP

For	Seccubus Workshop
Date	August 2017
Version	2.2
Author	Frank Breedijk
Status	Draft

Table of contents

1 INTRODUCTION

Welcome to this Seccubus workshop. This document contains the exercises for this workshop. For this workshop, we have set up a number of machines in the Schuberg Philis Mission Critical Cloud. All these machines are publicly accessible and use the same credentials for login. From your Seccubus host you will be performing real network scans across the Internet to your own victim machine. We ask you to play nicely. Do not log into the machines of you co-students (even though you can, in fact it is easy and does not require any 37331 skills). Do not to scan any systems you do not have explicit authorization to scan[1].

[1] I mean it…

2 SETUP

2.1 MAKE SURE YOUR KIT IS COMPLETE

At the start of this workshop you should have received a card with your lab number and credentials on it.

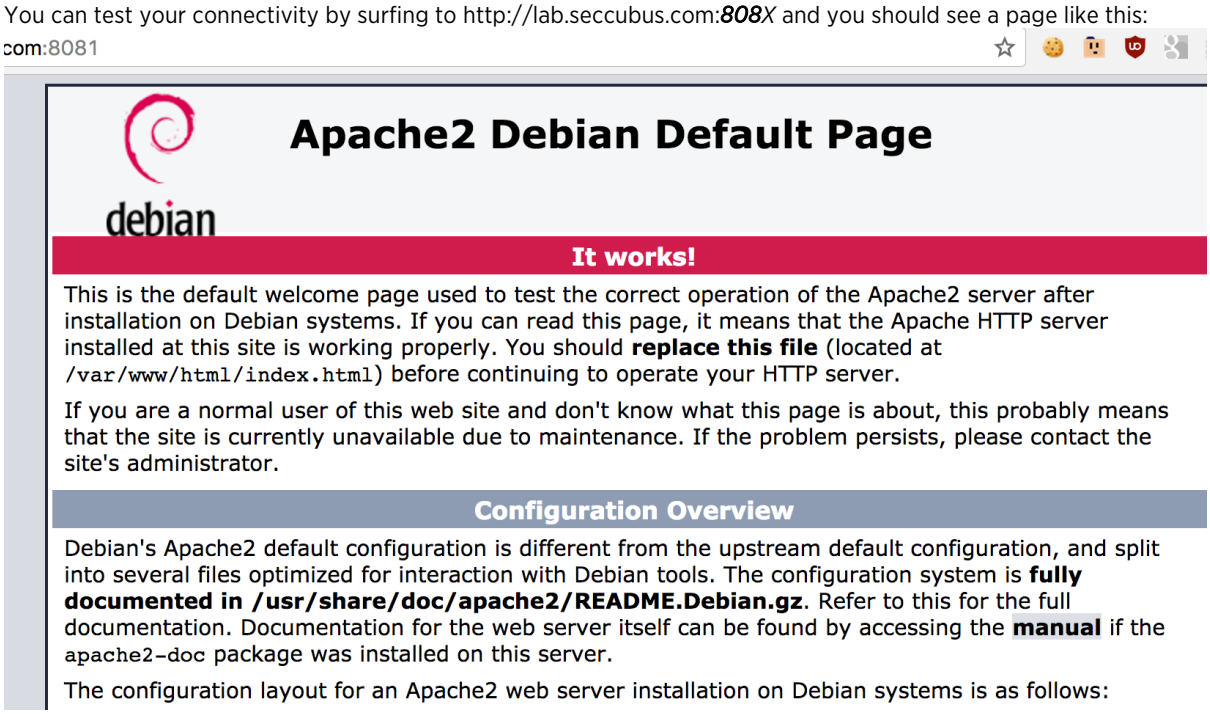
Generally speaking, the setup should look like this.

If you are using machine pair ***X***, you can use the following hostnames and port to connect:

What	External	Internal
Generig lab DNS name	lab.seccubus.com	
Lab website with ssh keys	https://seccubus.com/lab	
SSH to scanner	ssh://lab.seccubus.com:***5X22***	ssh://scanner***X***:22
Seccubus gui on scanner	https://lab.seccubus.com:***X443***	https://scanner***X***:8443
Nessus gui on scanner	https://lab.seccubus.com:***800X***	https://scanner***X***:8834
SSH to victim	ssh://lab.seccubus.com:***6X22***	ssh://victim***X***:22
Website on victim	http://lab.seccubus.com:***808X***	http://victim***X***

Default username is 'pantone' you need the ssh key from https://seccubus.com/lab to log in.

You can test your connectivity by surfing to http://lab.seccubus.com:***808X*** and you should see a page like this:



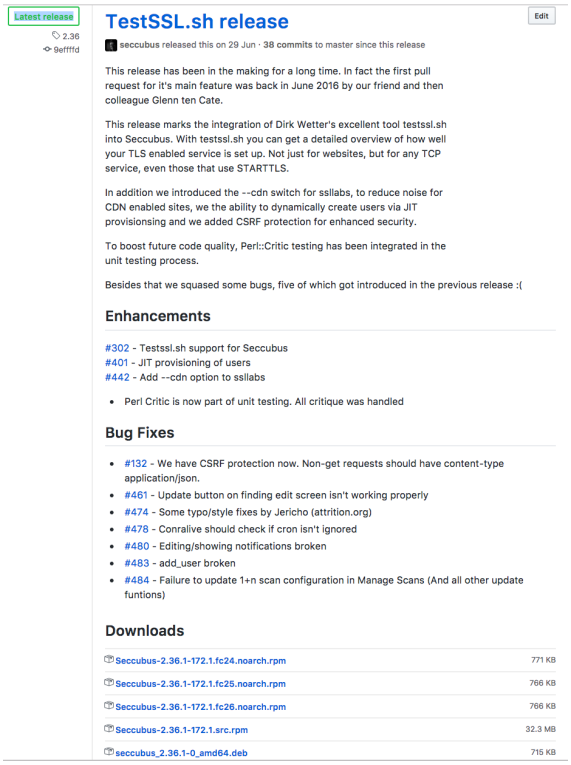
Additionally, if you surf to https://lab.seccubus.com:800***X*** you should see a login screen like this:

Please also test if you can SSH to both your victim and scanner machine.

2.2 INSTALLING SECCUBUS

Your scanner machines comes preinstalled with Nessus, Nikto, Nmap and Testssl.sh. You need to install Seccubus yourself.

Find the latest version of the Seccubus package for Debian by surfing to https://github.com/schubergphilis/Seccubus/releases/latest, you will see a page like this.



Latest release

2.36

9effffd

TestSSL.sh release

Edit

seccubus released this on 29 Jun · **38 commits** to master since this release

This release has been in the making for a long time. In fact the first pull request for it's main feature was back in June 2016 by our friend and then colleague Glenn ten Cate.

This release marks the integration of Dirk Wetter's excellent tool testssl.sh into Seccubus. With testssl.sh you can get a detailed overview of how well your TLS enabled service is set up. Not just for websites, but for any TCP service, even those that use STARTTLS.

In addition we introduced the --cdn switch for ssllabs, to reduce noise for CDN enabled sites, we the ability to dynamically create users via JIT provisionsing and we added CSRF protection for enhanced security.

To boost future code quality, Perl::Critic testing has been integrated in the unit testing process.

Besides that we squased some bugs, five of which got introduced in the previous release :(

Enhancements

#302 - Testssl.sh support for Seccubus
#401 - JIT provisioning of users
#442 - Add --cdn option to ssllabs

- Perl Critic is now part of unit testing. All critique was handled

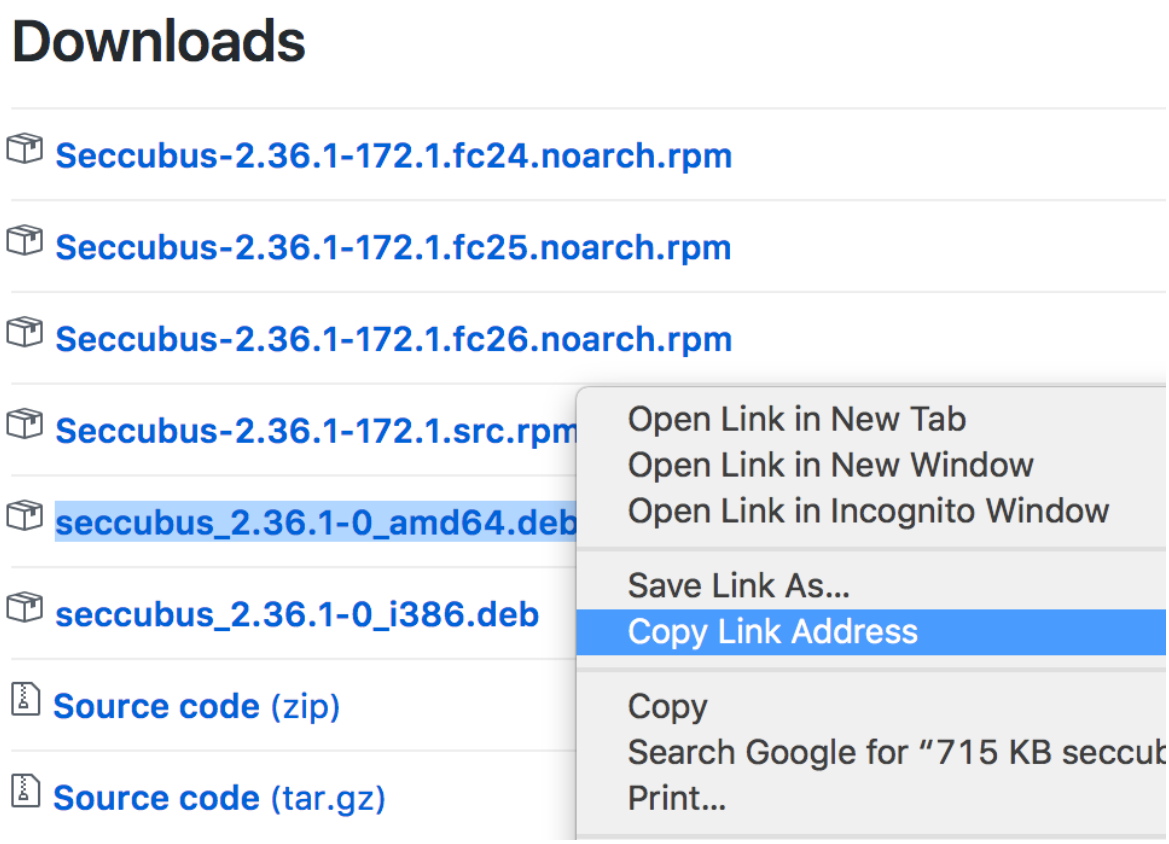
Bug Fixes

- #132 - We have CSRF protection now. Non-get requests should have content-type application/json.
- #461 - Update button on finding edit screen isn't working properly
- #474 - Some typo/style fixes by Jericho (attrition.org)
- #478 - Conralive should check if cron isn't ignored
- #480 - Editing/showing notifications broken
- #483 - add_user broken
- #484 - Failure to update 1+n scan configuration in Manage Scans (And all other update funtions)

Downloads

Seccubus-2.36.1-172.1.fc24.noarch.rpm	771 KB
Seccubus-2.36.1-172.1.fc25.noarch.rpm	766 KB
Seccubus-2.36.1-172.1.fc26.noarch.rpm	766 KB
Seccubus-2.36.1-172.1.src.rpm	32.3 MB
seccubus_2.36.1-0_amd64.deb	715 KB

Right click on the amd64.deb file and copy the URL.



Log into your scanner machine and download the package.

```
$ wget https://github.com/schubergphilis/Seccubus/releases/download/2.xx/seccubus_2.xx.x-0_amd64.deb
```

Update your apt repository

```
$ sudo apt-get update
Get:1 http://security.debian.org jessie/updates InRelease [63.1 kB]
Ign http://deb.debian.org jessie InRelease
Hit http://deb.debian.org jessie-updates InRelease
Hit http://deb.debian.org jessie Release.gpg
Hit http://deb.debian.org jessie Release
Get:2 http://security.debian.org jessie/updates/main amd64 Packages [548 kB]
Get:3 http://deb.debian.org jessie-updates/main amd64 Packages [17.8 kB]
Get:4 http://deb.debian.org jessie/main amd64 Packages [9063 kB]
Fetched 9692 kB in 6s (1386 kB/s)
Reading package lists... Done
```

Attempt to install the deb file, this should fail on dependency problems.

```
$ sudo dpkg -I seccubus_2.xx.x-0_amd64.deb
Reading package lists... Done
Building dependency tree
Reading state information... Done
<snip>
dpkg: dependency problems prevent configuration of seccubus:
 seccubus depends on perl; however:
  Package perl is not installed.
 seccubus depends on mysql-server; however:
  Package mysql-server is not installed.
 seccubus depends on libalgorithm-diff-perl; however:
  Package libalgorithm-diff-perl is not installed.
 seccubus depends on libdbi-perl; however:
  Package libdbi-perl is not installed.
 seccubus depends on libdbd-mysql-perl; however:
  Package libdbd-mysql-perl is not installed.
 seccubus depends on libjson-perl; however:
  Package libjson-perl is not installed.
 seccubus depends on libxml-simple-perl; however:
  Package libxml-simple-perl is not installed.
 seccubus depends on libwww-perl; however:
  Package libwww-perl is not installed.
 seccubus depends on liblwp-protocol-https-perl; however:
  Package liblwp-protocol-https-perl is not installed.
 seccubus depends on libnet-ip-perl; however:
  Package libnet-ip-perl is not installed.
 seccubus depends on libtimedate-perl; however:
  Package libtim
dpkg: error processing package seccubus (--install):
 dependency problems - leaving unconfigured
Errors were encountered while processing:
 seccubus
```

Next run apt-get to fix the dependency problems.

```
$ sudo apt-get -f install
Reading package lists... Done
Building dependency tree
Reading state information... Done
Correcting dependencies... Done
The following extra packages will be installed:
  javascript-common libaio1 libalgorithm-c3-perl libalgorithm-diff-perl libalgorithm-diff-xs-perl
<snip>
Suggested packages:
  apache2 lighttpd httpd libgssapi-perl libclone-perl libmldbm-perl libnet-daemon-perl libsql-
statement-perl
<snip>
```

```
Recommended packages:
  libarchive-tar-perl
The following NEW packages will be installed:
  javascript-common libaio1 libalgorithm-c3-perl libalgorithm-diff-perl libalgorithm-diff-xs-perl
<snip>
0 upgraded, 124 newly installed, 0 to remove and 0 not upgraded.
1 not fully installed or removed.
Need to get 20.6 MB of archives.
After this operation, 151 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

2.3 CREATING THE DATABASE

Create the seccubus database

```
$ sudo mysqladmin create seccubus
```

Next grant seccubus rights on the database

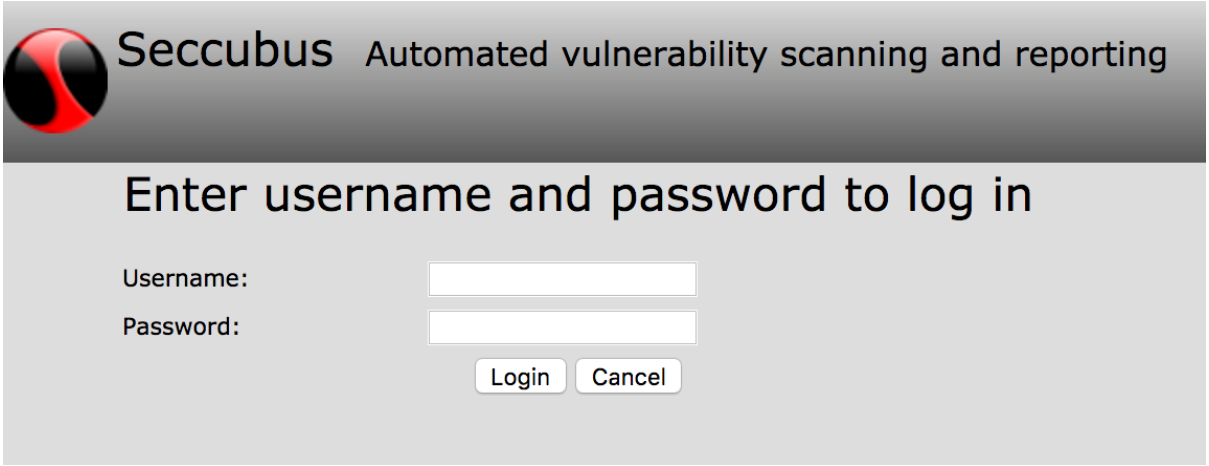
```
$ sudo mysql seccubus
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 11
Server version: 10.1.23-MariaDB-9+deb9u1 Debian 9.0

Copyright (c) 2000, 2017, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [seccubus]>grant all privileges on seccubus.* to seccubus identified by 'seccubus';
Query OK, 0 rows affected (0.00 sec)

MariaDB [seccubus]> flush privileges ;
Query OK, 0 rows affected (0.00 sec)
```

Load the structure and the contents of the database

```
$ sudo mysql seccubus < /var/lib/seccubus/structure_v10.mysql
$ sudo mysql seccubus < /var/lib/seccubus/data_v10.mysql
```

2.4 LOG INTO SECCUBUS

Surf to http://lab.seccubus.com:X443 see this screen.



Default username is ‘admin’ and password is ‘GiveMeVulns!’.

3 OUR FIRST SCAN

3.1 CONFIGURING A WORKSPACE

Seccubus works with the concept of workspaces. Scans that belong together (e.g. scans of the same infrastructure) can be kept together in a workspace.

- Click on the 'New Workspace' button on the 'Manage Workspaces' tab to create a workspace called 'Workshop'

3.2 CONFIGURING A NESSUS SCAN

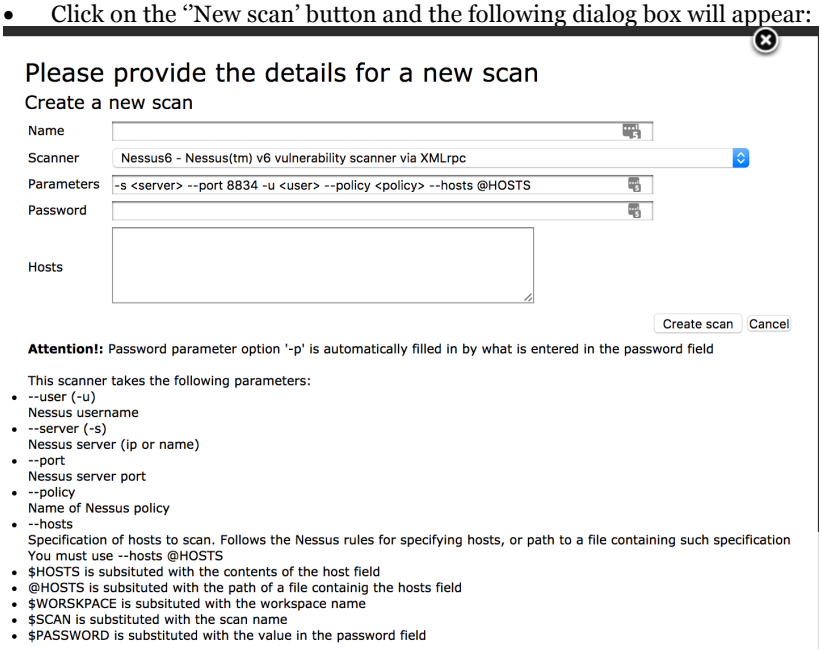
In this workshop we want to scan a web server for the presence of vulnerabilities on various ports.

3.2.1 Setting up Nessus

Login into Nessus make sure a scanning policy named 'workshop' exists and is valid.

3.2.2 Setting up Seccubus

- Go to the 'Manage Scans' tab
- Select the 'Workshop' workspace form the dropdown
- Click on the ''New scan' button and the following dialog box will appear:



- Fill out the following parameters:

  Scan name: **Nessus**

  Scanner: **Nessus6**

  Scan parameters: **-s localhost --port 8834 -u seccubus --policy workshop --hosts @HOSTS --export nessus**

  Password: **seccubus**

  Scan targets: **<ip address of your victim>**

- If you want to find out what these parameters mean run the following from command line:

```
$ cd /opt/seccubus/
$ scanners/Nessus/scan --help

Usage: scan       --user=<username> --password=<password> --server=<server>
<snip>
```

- Workspace and scan parameters are added automatically

3.3 RUNNING THE SCAN

- Start the scan from the command line. Go to /opt/seccubus and start the scan

```
$ cd /opt/seccubus
$ bin/do-scan --workspace Workshop --scan Nessus -v
```

- After about 5-10 minutes the scan should be finished

3.4 ANALYZING THE SCAN

When you analyze a scan, you determine which findings are relevant and which are not. You also assign a status to these findings accordingly.

» Reload the Seccubus GUI
» Select the workspace 'Workshop' in the workspaces tab
» Select the scan 'Nessus' in the scans tab
» Select the findings tab
» At the top of the page you see a number of statuses, there are approx 30 findings which have the NEW state.
» Mark the findings that you think pose a security risk as OPEN and those that don't as NO ISSUE.

3.5 FIXING THE FINDINGS

Now we log in as user workshop with the provided key on the victim machine and fix some of our findings.

- Log into the victim host and make yourself root.

```
$ sudo su -
```

- First we are going to disable xinetd which launches the chargen service

```
# service xinetd stop
```

- Now we are going to tackle the webserver configuration

```
# vi /etc/httpd/conf/httpd.conf
```

- We need to find and update the following lines

```
ServerTokens Full-> ServerTokens ProductOnly
```

- Now we need to restart the webserver to read in the new configuration

```
# service httpd reload
```

4 THE SECOND SCAN

Now that we fixed some findings it is time to scan the same target again.

4.1 INITIATING THE SECOND SCAN

- Start the scan from the command line.

```
$ cd /opt/seccubus
$ bin/do-scan --workspace Workshop --scan Nessus -v
```

- After about 5-10 minutes the scan should be finished

4.2 ANALYZING THE SCAN

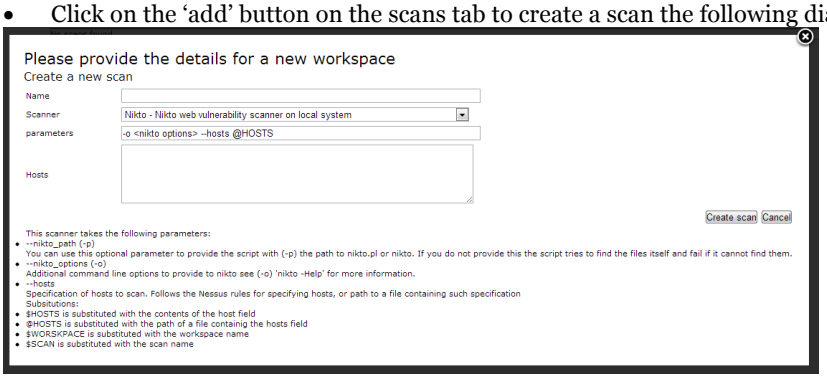
When you analyze a scan you determine which findings are relevant and which are not. Since this is the second scan we only need to focus on findings that are NEW, have CHANGED or have GONE. You also assign a status to these findings accordingly.

» Reload the Seccubus GUI
» Select the workspace 'Workshop' in the workspaces tab
» Select the scan 'Nessus' in the scans tab
» Select the findings tab
» First we will concentrate on the GONE findings. If we agree with the fact that these findings are indeed GONE, we should set the status to CLOSED.
» Then we need to check all CHANGED findings to see if any problems where corrected or reintroduced
» Finally we have a look at the NEW findings to see if any security issues have been introduced.

5 SCANNING WITH NIKTO

5.1 SETTING UP SECCUBUS

- Reload the Seccubus GUI
- Select the 'Workshop' scan and click on the scans tab
- Click on the 'add' button on the scans tab to create a scan the following dialog box will appear:



- Fill out the following parameters:
  Scan name: **Nikto**
  Scanner: **Nikto**
  Scan parameters: **--hosts @HOSTS**
  Scan targets: **<ip address of your victim>**

5.2 RUNNING THE SCAN

- Start the scan from the command line.

```
$ cd /opt/seccubus
$ bin/do-scan --workspace Workshop --scan Nikto -v
```

- After about 5-10 minutes the scan should be finished

5.3 ANALYZING THE SCAN

When you analyze a scan you determine which findings are relevant and which are not. You also assign a status to these findings accordingly.

» Reload the Seccubus GUI
» Select the workspace 'Workshop' in the workspaces tab
» Select the scan 'Nikto' in the scans tab
» Select the findings tab
» At the top of the page you see a number of statuses, there are approximately 7 findings which have the NEW state.
» Mark the findings that you think pose a security risk as OPEN and those that don't as NO ISSUE.

6 THE SECOND NIKTO SCAN

6.1 INTRODUCING AN ISSUE

- Log into the victim host and make yourself root.

```
$ sudo su -
```

- Let's edit the webserver configuration

```
# vi /etc/apache2/apache2.conf
```

- We need to find and update the following lines

```
ServerTokens ProductOnly -> ServerTokens Full
TraceEnable On -> TraceEnable Extended
```

- Now we need to restart the webserver to read in the new configuration

```
# service httpd reload
```

6.2 INITIATING THE SECOND NIKTO SCAN

- Start the scan from the command line.

```
$ cd /opt/seccubus
$ bin/do-scan --workspace Workshop --scan Nikto -v
```

- After about 5-10 minutes the scan should be finished

6.3 ANALYZING THE SCAN

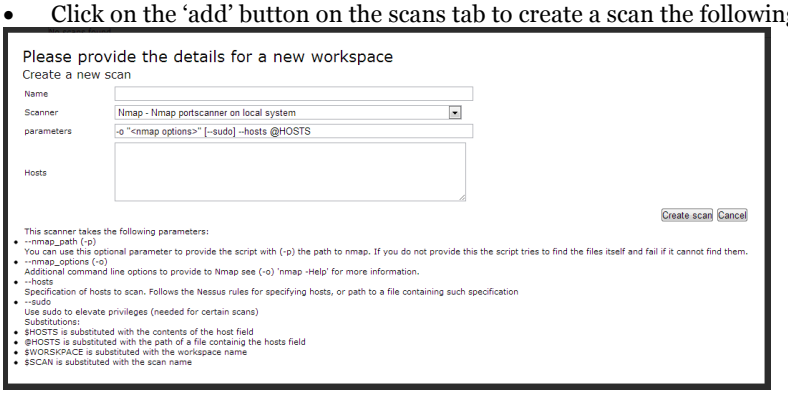
When you analyze a scan you determine which findings are relevant and which are not. Since this is the second scan we only need to focus on findings that are NEW, have CHANGED or have GONE. You also assign a status to these findings accordingly.

» Reload the Seccubus GUI
» Select the workspace 'Workshop' in the workspaces tab
» Select the scan 'Nikto' in the scans tab
» Select the findings tab
» First we will concentrate on the GONE findings. If we agree with the fact that these findings are indeed GONE, we should set the status to CLOSED.
» Then we need to check all CHANGED findings to see if any problems where corrected or reintroduced
» Finally we have a look at the NEW findings to see if any security issues have been introduced.

7 SCANNING WITH NMAP

7.1 SETTING UP SECCUBUS

- Reload the Seccubus GUI
- Select the 'Workshop' scan and click on the scans tab
- Click on the 'add' button on the scans tab to create a scan the following dialog box will appear:



- Fill out the following parameters:
  Scan name: **Nmap**
  Scanner: **Nmap**
  Scan parameters: **-o "-Pn" --hosts @HOSTS**
  Scan targets: **<ip address of your victim>**

7.2 RUNNING THE SCAN

- Start the scan from the command line.

```
$ cd /opt/seccubus
$ bin/do-scan --workspace Workshop --scan Nmap -v
```

- After about 5-10 seconds the scan should be finished

7.3 ANALYZING THE SCAN

When you analyze a scan you determine which findings are relevant and which are not. You also assign a status to these findings accordingly.

» Reload the Seccubus GUI
» Select the workspace 'Workshop' in the workspaces tab
» Select the scan 'Nmap' in the scans tab
» Select the findings tab
» At the top of the page you see a number of statuses, there are approximately 30 findings which have the NEW state.
» Mark the findings that you think pose a security risk as OPEN and those that don't as NO ISSUE.

8 THE SECOND NMAP SCAN

8.1 REOPENING SOME PORTS

- Log into the victim host and make yourself root.

```
$ sudo su -
```

- Let's restart chargen and vsftpd

```
# service xinetd start
```

8.2 INITIATING THE SECOND NMAP SCAN

- Start the scan from the command line. Become the seccubus user

```
# su - seccubus
$
```

- Start the scan

```
$ bin/do-scan --workspace Workshop --scan Nmap -v
```

- After about 5-10 seconds the scan should be finished

8.3 ANALYZING THE SCAN

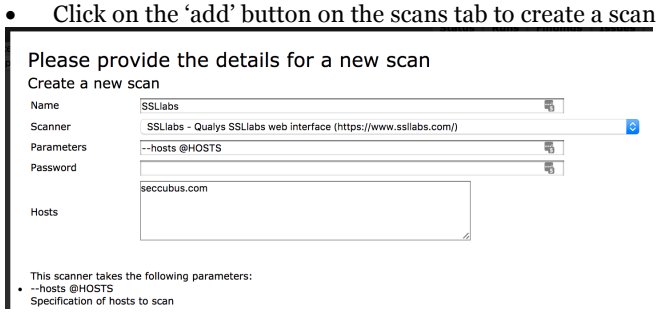
When you analyze a scan you determine which findings are relevant and which are not. Since this is the second scan we only need to focus on findings that are NEW, have CHANGED or have GONE. You also assign a status to these findings accordingly.

» Reload the Seccubus GUI
» Select the workspace 'Workshop' in the workspaces tab
» Select the scan 'Nmap' in the scans tab
» Select the findings tab
» First we will concentrate on the GONE findings. If we agree with the fact that these findings are indeed GONE, we should set the status to CLOSED.
» Then we need to check all CHANGED findings to see if any problems where corrected or reintroduced
» Finally we have a look at the NEW findings to see if any security issues have been introduced.

9 SSLLABS SCAN

9.1 SETTING UP SECCUBUS

- Reload the Seccubus GUI
- Select the 'Workshop' scan and click on the scans tab
- Click on the 'add' button on the scans tab to create a scan the following dialog box will appear:



- Fill out the following parameters:
  Scan name: **SSLlabs**
  Scanner: **SSLlabs**
  Scan parameters: **--hosts @HOSTS**
  Scan targets: **www.seccubus.com**

9.2 RUNNING THE SCAN

- Start the scan from the command line.

```
$ cd /opt/seccubus
$ bin/do-scan --workspace Workshop --scan SSLlabs -v
```

9.3 ANALYZING THE SCAN

When you analyze a scan you determine which findings are relevant and which are not. You also assign a status to these findings accordingly.

» Reload the Seccubus GUI
» Select the workspace 'Workshop' in the workspaces tab
» Select the scan 'Nmap' in the scans tab
» Select the findings tab
» At the top of the page you see a number of statuses, there are approximately 30 findings which have the NEW state.
» Mark the findings that you think pose a security risk as OPEN and those that don't as NO ISSUE.