



ESISS

Education Shared Information Security Service

ESISS Security Scanner

How to use the ESISS Automated Security Scanner

January 2013

v1.1

Education Shared Information Security Service

C/O Information Systems, The Nottingham Trent University
Burton Street, Nottingham, NG1 4BU

Email: info@esiss.ac.uk

Web: <https://www.esiss.ac.uk>

Table of Contents

The ESISS Automated Security Scanner.....	3
Using The ESISS Security Scanner.....	4
1. Logging On.....	4
2. The Dashboard Screen	5
3. Scans	8
4. My Account	11
5. Manage Users.....	12

The ESISS Automated Security Scanner

The ESISS automated security scanner is provided in conjunction with Sec-1¹. It allows institutions to externally scan servers, web services, IP address ranges or individual IP addresses from their institution for potential security problems.

The scanner features the following:

- **Administration**
 - Single platform to manage application and infrastructure security risks;
 - Flexible scheduling of scans including the ability to pause and resume scans;
 - Provides flexible filtering on either end systems or vulnerability title;
 - Download custom filtered reports in HTML, Docx or CSV format.
- **Infrastructure tests**, which consist of:
 - Port scan against the host to check open ports/service types;
 - AMAP probe of open ports found by the port scan;
 - DNS digging for information about the host/netblock;
 - Vulnerability tests against the open ports discovered. These are aimed at finding common security problems and are “safe” checks so as to not cause undue problems with the hosts being checked.
- **Web Application tests**, which consist of:
 - Each defined website is crawled to map site/application content;
 - A forced browsing scan is performed to test for common issues found in the OWASP top 10 (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project), eg email address harvesting, browsable dirs, writeable dirs through to SQL injection, XSS, etc;
 - Checks to identify weak administration interfaces.

These webform submission checks which are part of the web application testing may cause a significant amount of form email to be generated depending on the configuration of the web applications being tested.

Note: All scans will originate from the IP address 62.69.82.10. Janet CSIRT is aware of this IP address being used by ESISS and should not contact you about any potential threat.

¹ <http://www.sec-1.com>

Using The ESISS Security Scanner

1. Logging On

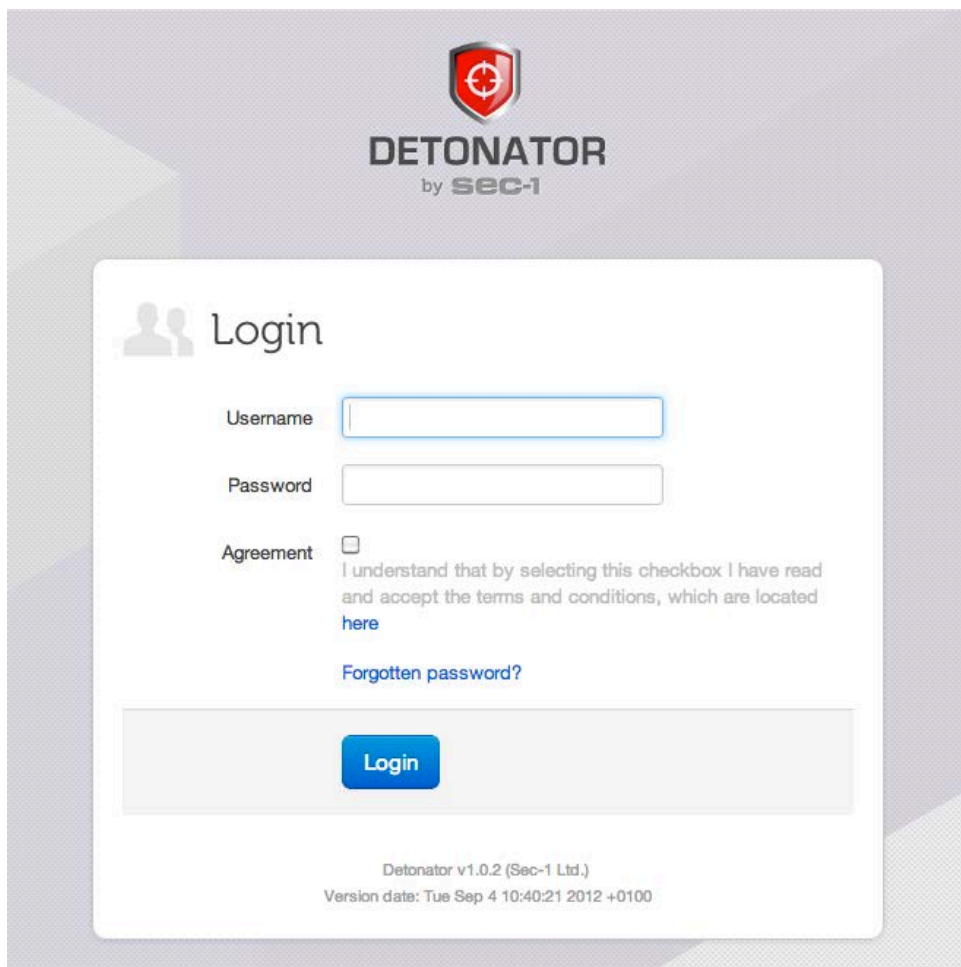
The scanner can be accessed at the following URL:

<https://scanner.sec-1.com/>


You will need to have had a company definition and user account created by a member of the ESISS team (email info@esiss.ac.uk with any ammendments to your initial connection or if you have any problems with this).

Note: Your logon username is your email address.

The Logon screen:



DETONATOR
by SEC-1

 Login

Username

Password

Agreement
I understand that by selecting this checkbox I have read and accept the terms and conditions, which are located [here](#)

[Forgotten password?](#)

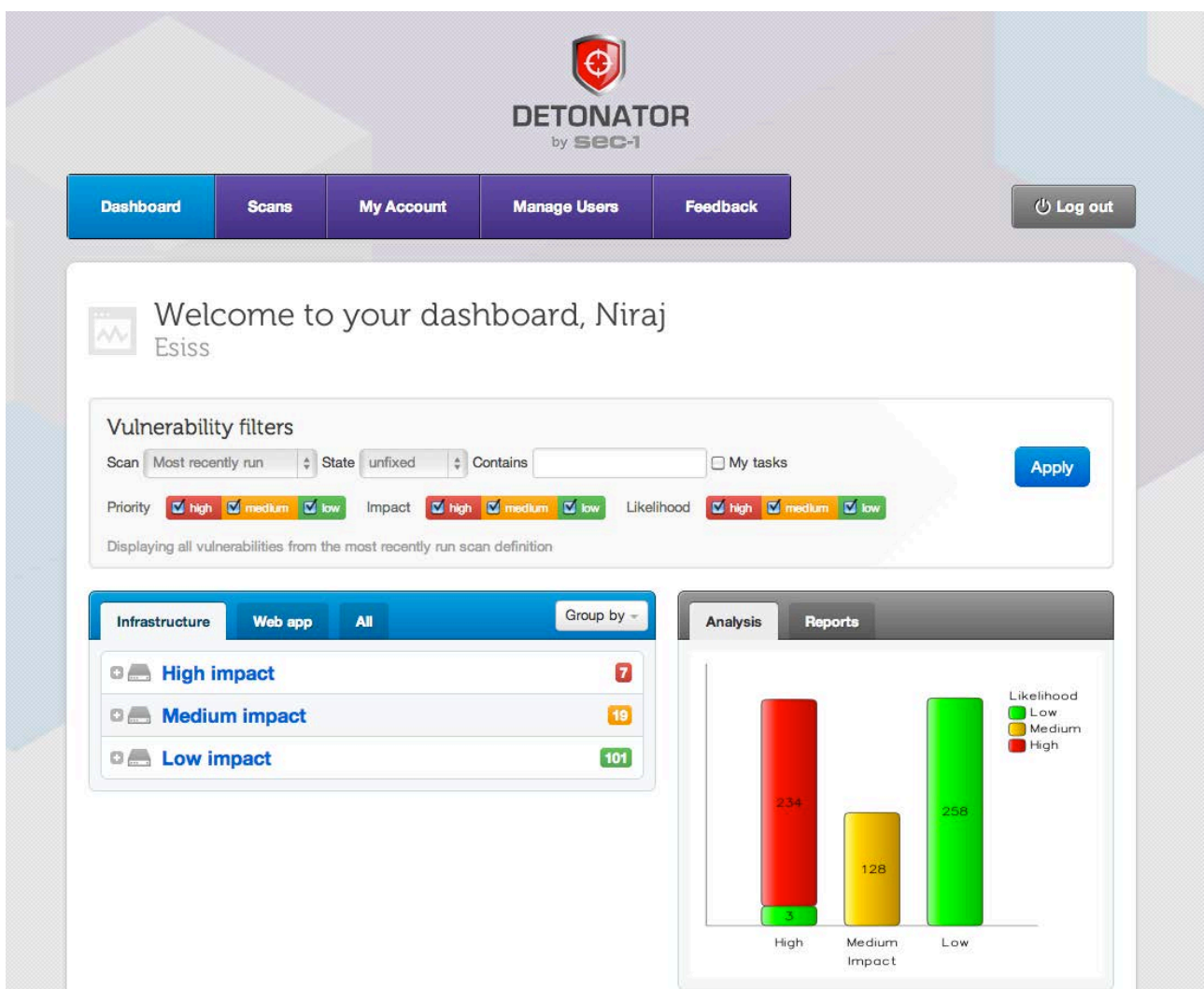
Login

Detonator v1.0.2 (Sec-1 Ltd.)
Version date: Tue Sep 4 10:40:21 2012 +0100

2. The Dashboard Screen

After logging on, you will be presented with the **dashboard** screen, as shown below. This provides you with a summary of the results for the last completed scan, split by the type of scan (infrastructure or web app). Filters can also be applied based on keywords and/or priority, impact or likelihood of the discovered vulnerabilities. You have the ability to download a report of the completed scan in both Word (docx) or csv format and the ability to review old scans.

Dashboard Screen:



Accessing Reports:

In order to download the report for the last completed scan, you need to click on the **Reports** tab in the right hand frame. This then shows a Word (docx) and a csv of the results.

Note: these are subject to any filters you may have applied to the results.

Report Screen:

The screenshot displays the DETONATOR by SEC-1 dashboard. At the top, there is a navigation menu with buttons for Dashboard, Scans, My Account, Manage Users, and Feedback, along with a Log out button. The main content area shows a welcome message for Niraj Esiss. Below this, there are vulnerability filters for Scan, State, Contains, My tasks, Priority, Impact, and Likelihood. The dashboard is divided into two main sections: Infrastructure and Reports. The Reports section is highlighted with a red circle and contains a message: "Click the appropriate icon to download these FILTERED results as a report. Note, it may take a short while after you click for the document to be generated before download begins." Below the message are icons for a Word document and a CSV file.

Recent Events:

The Recent Events box in the bottom right of the dashboard screen shows a list of recent scans carried out. Clicking on the bar graph icon shows the results for that scan in the dashboard and the bin icon will delete the scan results.

Recent Events:

Recent events

The screenshot shows a dashboard titled "Recent events" with two tabs: "Scans" and "User workflow". The "Scans" tab is active, displaying a list of five completed scan events. Each event entry includes a date and time, a name, a "COMPLETED" status, a bar graph icon, and a trash bin icon.

Date	Time	Name	Status
Fri 06 Jul 2012	11:26AM	Sample	COMPLETED
Wed 23 May 2012	09:15AM	westmin	COMPLETED
Thu 17 May 2012	03:41PM	whitsend	COMPLETED
Thu 17 May 2012	03:40PM	ccalmb	COMPLETED
Thu 17 May 2012	10:04AM	test reputation	COMPLETED

3. Scans

Clicking the **Scans** tab along the top menu shows all currently defined scans that have been setup, and allows you to create new scans. You are also able to view scans carried out by other members of your organisation by clicking the **All** tab next to the **Mine** tab.

Scans screen:

Scan Definitions

+ Define new scan

Description	Next run	Repeat interval	Actions	Scan activity
whitsend Paul Whitton	Not scheduled	Never		COMPLETED Thu 17 May 2012 10:59PM
Sample Paul Whitton	Not scheduled	Never		COMPLETED Tue 10 Jul 2012 02:27AM
westmin Paul Whitton	Not scheduled	Never		COMPLETED Wed 23 May 2012 10:25AM
ccalmb Paul Whitton	Not scheduled	Never		COMPLETED Thu 17 May 2012 03:43PM
test reputation Paul Whitton	Not scheduled	Never		COMPLETED Thu 17 May 2012 11:18AM
ccspa Paul Whitton	Not scheduled	Never		COMPLETED Wed 02 May 2012 06:42PM
fileport Paul Whitton	Not scheduled	Never		COMPLETED Fri 27 Apr 2012 03:00PM

Detonator v1.0.2 (Sec-1 Ltd.)
Version date: Tue Sep 4 10:40:21 2012 +0100

Scans can be controlled by the following actions:



This button starts the scan immediately;



This button shows the latest results for the scan;



This button edits the scan settings;



This button deletes the scan.

Defining a new Scan.

Under the scan menu, clicking on **" + Define new scan "** takes you to the scan definition screen. This allows you to specify the type of test to carry out:

- Web Application Scanner;
- Network Infrastructure Scanner;
- Both.

For Web Application scanning, provide the URLs that you require to be scanned and choose whether to post forms during the web application testing.

For the Network Infrastructure Scanner, select an IP address or a range of IP addresses.

Finally, set the time and date for when you would like the scan to run and whether you wish the scan to repeat and at what intervals.

Scan definition:

Scan definition

Name
Enter a descriptive name for this scan definition (e.g. 'Full quarterly scan', 'Web application scan', etc.)

Web Application Scanner

Enabled
Allows the web application scanning component of the scan to be enabled/disabled.

Target Web Application(s)
One valid URL per line (e.g. http://www.sec-1.com, http://someapp.somewhere.com, https://app.mysite.co.uk, http://200.168.0.1:5657, https://mysite.com/my.logout.php?errorcode=20, http://user:pass@www.somewhere.com, etc.)

Post Forms
Warning: though effective for finding vulnerabilities, posting forms may cause disruption (e.g. generating contact email or application content).

Network Scanner

Enabled
Allows the network scanning component of the scan to be enabled/disabled.

Target Hosts
One valid host or host range per line (e.g. 200.168.0.7, 200.168.0.0/25, 200.168.1.5-15, 200.168.3.6, 200.168.6.50, ftp.site.com, www.sec-1.com, etc.)

Scan Scheduling

Next Scan
The date and time of the next scan. Leave empty to disable scheduling

Scan definitions

A scan definition is like a template that embodies one or more actual scans over time.

It is useful, therefore, to create scan definitions for distinct business tasks (e.g. web-application only scans, logical service groups, one-off scan, etc.), since:

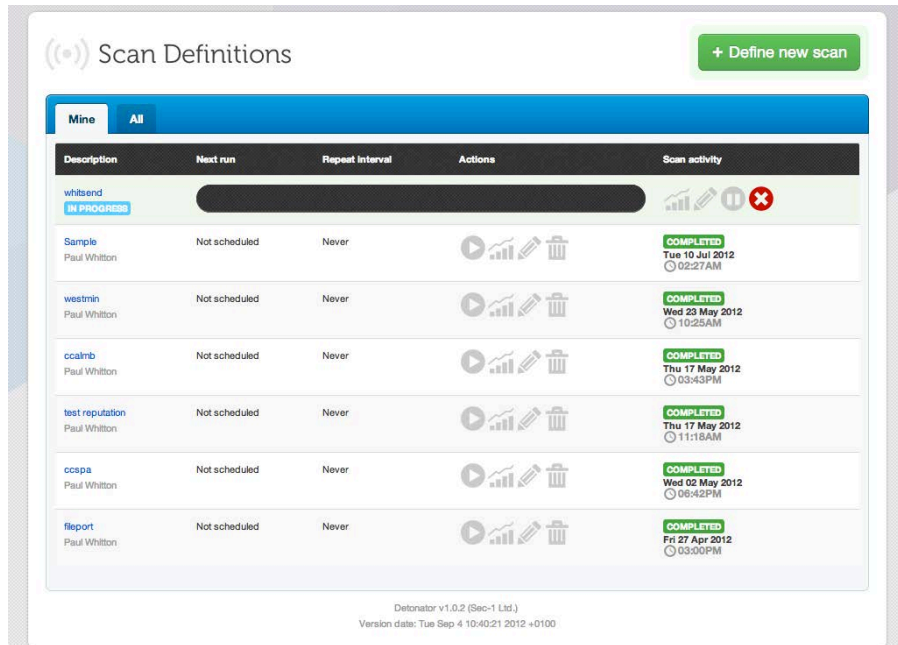
- this allows related scan results to be easily filtered for vulnerability resolution workflow;
- and each scan definition may be given its own periodic scheduling routine

Scanner addresses

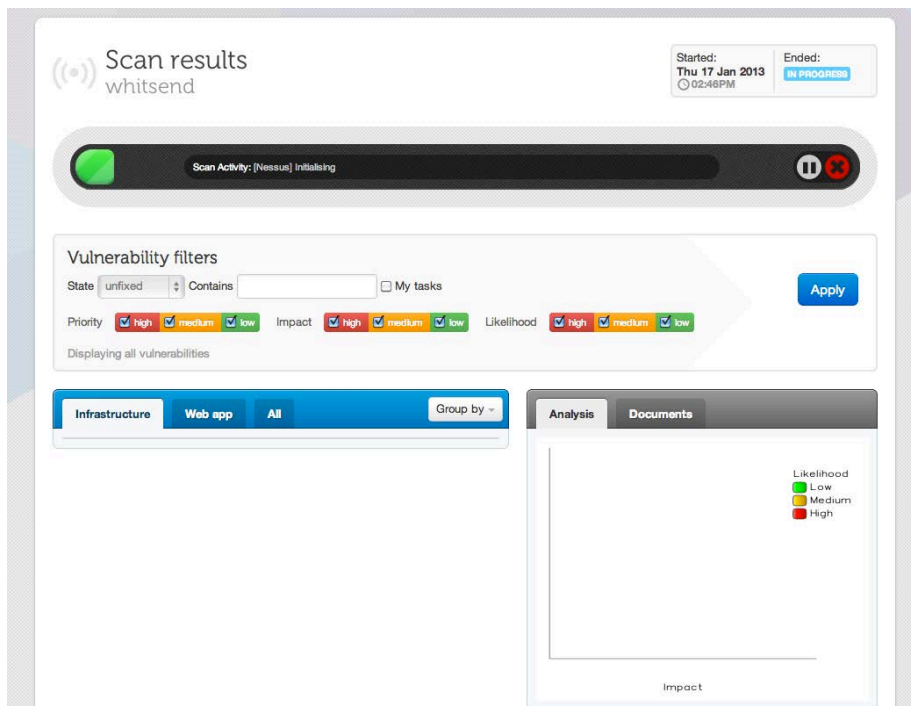
Scans of your services will originate from the following addresses:

Live scan results:

If a scan is in progress, on the scan screen you will see a black progress bar and icons to cancel and pause the scan as shown below:



Clicking on the black bar takes you to the scan results screen. This is the same as the dashboard screen, apart from having the live progress of the scan shown by the black bar as can be seen below:



4. My Account

Clicking the **My Account** tab along the top menu allows you to update your details and change the way you get alerted via email about scans. You can also see the licence applied to your account of what you are allowed to scan, as shown below:

The screenshot shows a web form titled "My details" for the user "Esiss". The form contains the following fields and options:

- Name:** Text input field containing "Niraj Kacha".
- Email address:** Text input field with a blacked-out email address. Below it is the text: "This is effectively a unique username."
- Email alerts:** A dropdown menu currently set to "Alerts of all completed scans". Below it is the text: "Select which email alerts you would like to receive. No sensitive data will be disclosed in any email."
- Password:** Text input field. Below it is the text: "Enter to change. Password must be at least 8 characters and contain at least one capital, digit and special character."
- Retype password:** Text input field.

At the bottom of the form are two buttons: "Save" (in blue) and "Cancel".

On the right side of the form, there is a "Tips" box with the text: "Ensure you choose a strong password, since the data held within this system is extremely sensitive to your organisation."

At the bottom center of the form, there is small text: "Detonator v1.0.2 (Sec-1 Ltd.)
Version date: Tue Sep 4 10:40:21 2012 +0100"

My details Loughborough University

The screenshot shows the "Licence details" tab selected in the "My Account" section. The content of the tab is as follows:

My details | **Licence details**

The details of your current licence are as follows:

Licence expires: 2013-04-13 00:00:00

Scanning scope:

- http://*.lboro.ac.uk
- https://*.lboro.ac.uk
- 131.231.0.0/16
- 158.125.0.0/16

5. Manage Users

Clicking the **Manage Users** tab along the top menu shows the current users within your organisation and allows you to add new users if you licence allows. This can be seen below:

