How to set up scans

This document explains how to setup and execute scans in Seccubus V2

- Nessus scan via XML rpc
- Nessus scan via legacy port 1241
- Nikto
- OpenVAS
- Nmap
- Skipfish Web-application scanner

1.1 Nessus scan via XML rpc

Configuring a Nessus scan consist of the following steps:

- Creating a policy in Nessus
- Creating a scan in Seccubus

First we need to create a scan policy on the Nessus scanner. So if your Nessus scanner is located at 10.6.6.6 you need to log into http://10.6.6.6:8834

In the Nessus GUI you need to create one or more policies. This example assumes you have created a policy with the default options named 'default'.

Now we need to set up a scan in Seccubus.

If you have not yet created a workspace, go to the 'Manage Workspaces' tab and click the 'New workspace' button.

Go to the 'Manage scans' tab and select the workspace you want to create the scan in. Then click on the 'New scan' button.

Next we need to fill out a name for the scan, select the 'Nessus' scanner provide the scanner parameters and the scan targets.

The scanner parameters determine which command line parameters are sent to the scanners/<scannername>/scan script. In the case of the Nessus scanner they should be:

```
--user <Nessus username> --password '<Nessus password>' --sever <Nessus IP address> --policy
<Nessus policy name> --hosts '$HOSTS'
```

If you use '$HOSTS' in a scan parameters, if will be replaced by the text typed in the 'Scan targets' field. If you use @HOSTS it will be replaced with the path to a file containing the information provided in the 'Scan targets fields'

You can test if your scan works by running the following command:

```
> bin/do-scan --workspace <Seccubus workspace name> --scan <Seccubus scan name> -v
```

1.2 Nessus via legacy port 1241

Setting up a Nessus Legacy scan (a scan via the port 1241 interface) can be done via the Seccubus GUI. In order for this type of scan to work you need to have the Nessus command line client installed on the server running Seccubus.

If you have not yet created a workspace, go to the 'Manage Workspaces' tab and click the 'New workspace' button.

Go to the 'Manage scans' tab and select the workspace you want to create the scan in. Then click on the 'New scan' button.

Next we need to fill out a name for the scan, select the 'Nessus' scanner provide the scanner parameters and the scan targets.

Next we need to fill out a name for the scan, select the 'NessusLegacy – Nessus(tm) vulnerability scanner via legacy port 1241 interface' scanner and provide the scanner parameters and the scan targets.

The scanner parameters determine which command line parameters are sent to the scanners/<scannername>/scan script. In the case of the NessusLegacy scanner they should be:

```
--nessus_path <path to the Nessus client> --user <Nessus username> --password '<Nessus
password>' --sever <Nessus IP address> --rc <path to the .nessusrc file> --hosts @HOSTS
```

If you use '$HOSTS' in a scan parameters, if will be replaced by the text typed in the 'Scan targets' field. If you use @HOSTS it will be replaced with the path to a file containing the information provided in the 'Scan targets fields'

The 'nessus_path' parameter is optional. Seccubus will look for the Nessus client binary in the usual places, however if Seccubus cannot find the binary you will need to specify the full path to it.

You can test if your scan works by running the following command:

```
> bin/do-scan --workspace <Seccubus workspace name> --scan <Seccubus scan name> -v
```

Example nessusrc files can be found in the Seccubus etc directory.

1.3 Nikto

Setting up a Nikto scan can also be done via the Seccubus GUI. In order to this type of scan to work you need to have Nikto installed on the server running Seccubus.

If you have not yet created a workspace, go to the 'Manage Workspaces' tab and click the 'New workspace' button.

Go to the 'Manage scans' tab and select the workspace you want to create the scan in. Then click on the 'New scan' button.

Next we need to fill out a name for the scan, select the 'Nikto' scanner and provide the scanner parameters and the scan targets.

The scanner parameters determine which command line parameters are sent to the scanners/<scannername>/scan script. In the case of the Nikto scanner they should be:

```
--nikto_path <path to nikto or nikto.pl> --nikto_options <additional options pass to Nikto> --
hosts @HOSTS --workspace <Seccubus workspace name> --scan <Seccubus scan name>
```

If you use '$HOSTS' in a scan parameters, if will be replaced by the text typed in the 'Scan targets' field. If you use @HOSTS it will be replaced with the path to a file containing the information provided in the 'Scan targets fields'

The 'nikto_path' parameter is optional. Seccubus will look for nikto or nikto.pl in the usual places, however if Seccubus cannot find these files you will need to specify the full path to it.

The string specified by nikto_options will be passed as command line options to Nikto. See http://cirt.net/nikto2-docs/options.html for a full explanation of these options. Do not specify the –Format and –output options as these options will be set by Seccubus

You can test if your scan works by running the following command:

```
> bin/do-scan --workspace <Seccubus workspace name> --scan <Seccubus scan name> -v
```

1.4 OpenVAS

Setting up a OpenVAS scan can be done via the Seccubus GUI. In order to this type of scan to work you need to have the OpenVas command line client (usually called OpenVAS-Client) installed on the server running Seccubus.

If you have not yet created a workspace, go to the 'Manage Workspaces' tab and click the 'New workspace' button.

Go to the 'Manage scans' tab and select the workspace you want to create the scan in. Then click on the 'New scan' button.

Next we need to fill out a name for the scan, select the 'Nessus' scanner provide the scanner parameters and the scan targets.

Next we need to fill out a name for the scan, select the 'OpenVAS' scanner and provide the scanner parameters and the scan targets.

The scanner parameters determine which command line parameters are sent to the scanners/<scannername>/scan script. In the case of the NessusLegacy scanner they should be:

```
--openvas_path <path to the OpenVAS client> --user <OpenVAS username> --password '<OpenVAS
password>' --sever <OpenVAS IP address> --rc <path to the .openvasrc file> --hosts @HOSTS
```

If you use '$HOSTS' in a scan parameters, if will be replaced by the text typed in the 'Scan targets' field. If you use @HOSTS it will be replaced with the path to a file containing the information provided in the 'Scan targets fields'

The 'openvas_path' parameter is optional. Seccubus will look for the OpenVAS client binary in the usual places, however if Seccubus cannot find the binary you will need

to specify the full path to it.

You can test if your scan works by running the following command:

```
> bin/do-scan --workspace <Seccubus workspace name> --scan <Seccubus scan name> -v
```

Example openvasrc files can be found in the Seccubus etc directory.

1.5 Nmap

Setting up an Nmap scan can also be done via the Seccubus GUI. In order to this type of scan to work you need to have Nmap installed on the server running Seccubus.

If you have not yet created a workspace, go to the 'Manage Workspaces' tab and click the 'New workspace' button.

Go to the 'Manage scans' tab and select the workspace you want to create the scan in. Then click on the 'New scan' button.

Next we need to fill out a name for the scan, select the 'Nmap' scanner and provide the scanner parameters and the scan targets.

The scanner parameters determine which command line parameters are sent to the scanners/<scannername>/scan script. In the case of the Nmap scanner they should be:

```
--nmap_path <path to nmap> --nmap_options <additional options passed to Nmap> --hosts @HOSTS
```

If you use '$HOSTS' in a scan parameters, if will be replaced by the text typed in the 'Scan targets' field. If you use @HOSTS it will be replaced with the path to a file containing the information provided in the 'Scan targets fields'

The 'nmap_path' parameter is optional. Seccubus will look for nmap in the usual places, however if Seccubus cannot find the Nmap executable you will need to specify the full path to it.

The string specified by nmap_options will be passed as command line options to Nmap. See 'nmap –help' or http://nmap.org/book/man.html for a full explanation of these options. Do not specify the –o option as this option will be set by Seccubus

You can test if your scan works by running the following command:

```
> bin/do-scan --workspace <Seccubus workspace name> --scan <Seccubus scan name> -v
```

1.6 Skipfish

Setting up a Skipfish scan can also be done via the Seccubus GUI. In order for this type of scan to work you need to have Skipfish installed on the server running Seccubus.

If you have not yet created a workspace, go to the 'Manage Workspaces' tab and click the 'New workspace' button.

Go to the ‘Manage scans’ tab and select the workspace you want to create the scan in. Then click on the ‘New scan’ button.

Next we need to fill out a name for the scan, select the ‘Skipfish’ scanner and provide the scanner parameters and the scan targets.

The scanner parameters determine which command line parameters are sent to the scanners/<scannername>/scan script. In the case of the Skipfish scanner they should be:

```
-o "<additional options passed to Skipfish>" --hosts $HOSTS
```

With Skipfish you **only** can use the ‘$HOSTS’ option in and specify the host in the ‘Scan targets fields’. Currently Skipfish **doesn't support multiple scan targets**.

The string specified by -o options will be passed as command line options to Skipfish. See ‘skipfish –help’ or https://code.google.com/p/skipfish/wiki/SkipfishDoc for a full explanation of these options.

You can test if your scan works by running the following command:

```
> bin/do-scan --workspace <Seccubus workspace name> --scan <Seccubus scan name> -v
```