Vulnerability scanner

Kali Linux comes with OpenVAS as the vulnerability scanner by default. As a penetration tester, we can't rely only on one tool; we have to use several tools to give us a more thorough and complete picture of the target environment.

As an additional vulnerability scanner, we will briefly describe the NeXpose Vulnerability Scanner Community Edition from Rapid7.

NeXpose Community Edition

NeXpose Vulnerability Scanner Community Edition (**NeXpose CE**) is a free vulnerability scanner from Rapid7 that scans devices for vulnerabilities. It can also be integrated with the Metasploit exploit framework.

Following are several of the NeXpose Community Edition features:

- Vulnerability scanning for up to 32 IP addresses
- Regular vulnerability database updates
- Ability to prioritize the risk assessment
- Guide to remediation process
- Integration with Metasploit
- Community support at http://community.rapid7.com
- Simple deployment
- No cost start-up security solution

The commercial edition of NeXpose include additional features, such as no limitation of the IP addresses that can be scanned, distributed scanning, more flexible reporting, web and database server scanning, and technical support.

NeXpose consists of the following two main parts:

- **NeXpose scan engine**: This performs asset discovery and vulnerability detection operations. In the community edition, there is only one local scan engine.
- **NeXpose security console**: This console will communicate with NeXpose scan engines to start scans and retrieve scan information. The console also includes a web-based interface to configure and operate the NeXpose scan engine.

Now that we have looked at the features of NeXpose Community Edition, let's try to install it.

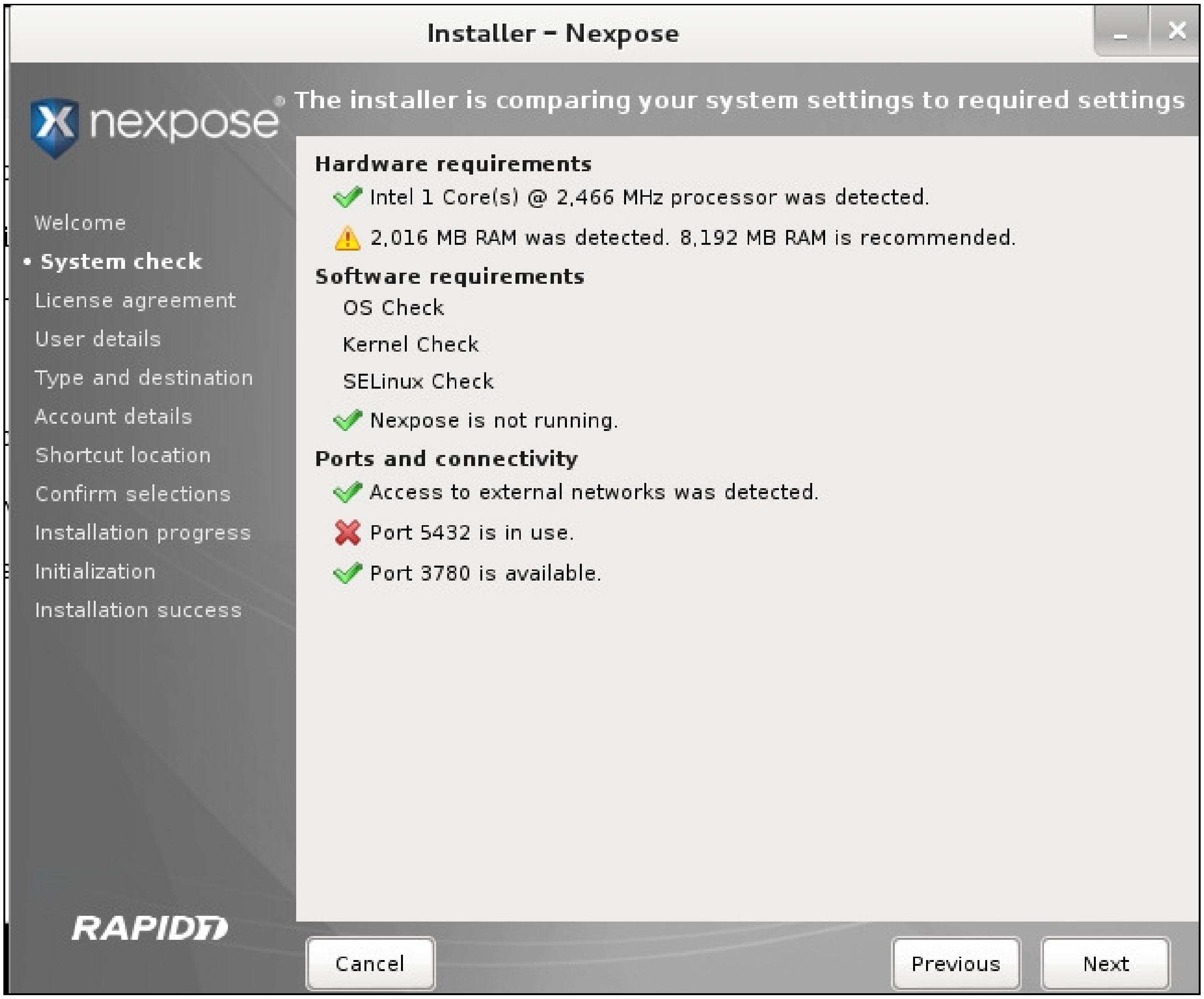
Installing NeXpose

Following are the steps that can be used to install NeXpose Community Edition in Kali Linux:

1. Complete the download form at http://www.rapid7.com/products/nexpose/nexpose-community.jsp. You need to provide your official e-mail address to register. After that, you will be sent an e-mail containing the license key and download instructions to get NeXpose CE.
2. Download the NeXpose CE installer from the location mentioned in the e-mail. As an example, I am downloading the `NeXposeSetup-Linux64.bin` file for the 64-bit Linux operating system.
3. Open a terminal, then go to the directory that contains the downloaded NeXpose installer.
4. Start the NeXpose installer by giving the following command:

   ```
   # ./NeXposeSetup-Linux64.bin
   ```

   The following screenshot shows us the NeXpose installer window:



The installer is comparing your system settings to required settings

Hardware requirements

✓ Intel 1 Core(s) @ 2,466 MHz processor was detected.

⚠ 2,016 MB RAM was detected. 8,192 MB RAM is recommended.

Software requirements

OS Check

Kernel Check

SELinux Check

✓ Nexpose is not running.

Ports and connectivity

✓ Access to external networks was detected.

✗ Port 5432 is in use.

✓ Port 3780 is available.

5. Follow the instructions displayed on the screen to continue the installation. Make sure you remember the username and password you had set during the configuration process. If you forget your username or password, you may need to reinstall NeXpose.

Starting the NeXpose community

After the installation process is complete, you can start NeXpose by going to the directory containing the script that starts NeXpose. The default installation directory is `/opt/rapid7/nexpose` . The command for starting NeXpose community is as follows:

```
# cd /opt/rapid7/nexpose/nsc
```

Run the following script to start NeXpose:

```
# ./nsc.sh
```

The startup process will take several minutes because NeXpose is initializing its vulnerabilities' database. After this process is finished, you can log on to the NeXpose security console web interface.

If you want to install NeXpose as a daemon, you can start it automatically when the machine starts; it will continue running even if the current process user logs off. You can do this with the following steps:

1. Go to the directory containing the `nexposeconsole.rc` file using the following command:

   ```
   # cd [installation_directory]/nsc
   ```

2. Open that file and make sure that the line containing `NXP_ROOT` is set to the NeXpose installation directory.

3. Copy that file to the `/etc/init.d` directory and give it the desired script name, such as `nexpose` using the following command:

   ```
   # cp [installation_directory]/nsc/nexposeconsole.rc /etc/init.d
   ```

```
/nexpose
```

4. Set the executable permission for the startup script file using the following command:

```
# chmod +x /etc/init.d/nexpose
```

5. Make NeXpose start when the operating system starts using the following command:

```
# update-rc.d nexpose defaults
```

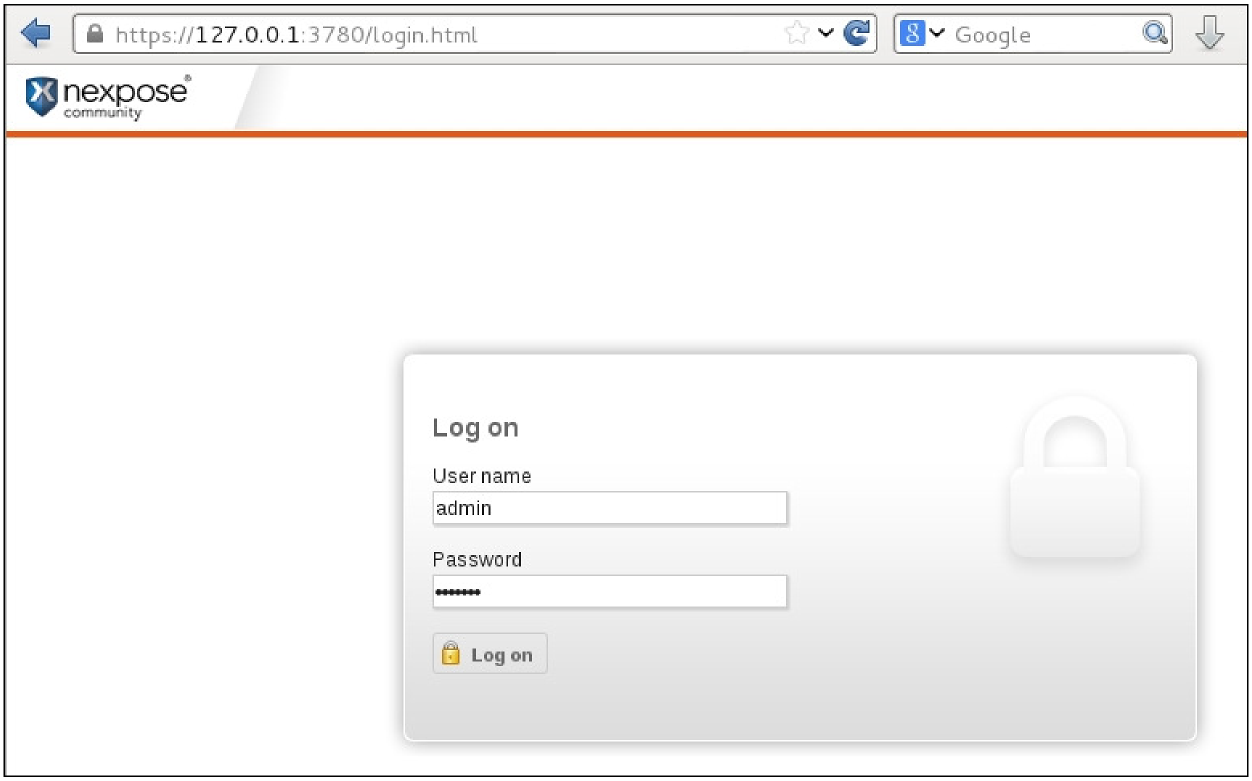
6. You can manage NeXpose to start, stop, or restart the daemon using the following command:

```
# /etc/init.d/nexpose <start|stop|restart>
```

Logging in to the NeXpose community

Following are the several steps that you must perform to log in to NeXpose community console's web interface:

1. Open your web browser. Then, go to this URL: `https://127.0.0.1:3780` . If there are no errors, you will be greeted with the login screen. You will see the **Untrusted Connection** message. After verifying the certificate, you can confirm whether or not to store the exception permanently, so you will not see the error message in the future.
2. After the first login, the security console will initialize; it will also download updates from the Rapid7 server. This process will take some time.
3. After the initialization has finished, you can log in using the username and password that you specified during the installation process, then click on the **Log on** button as shown in the following screenshot:



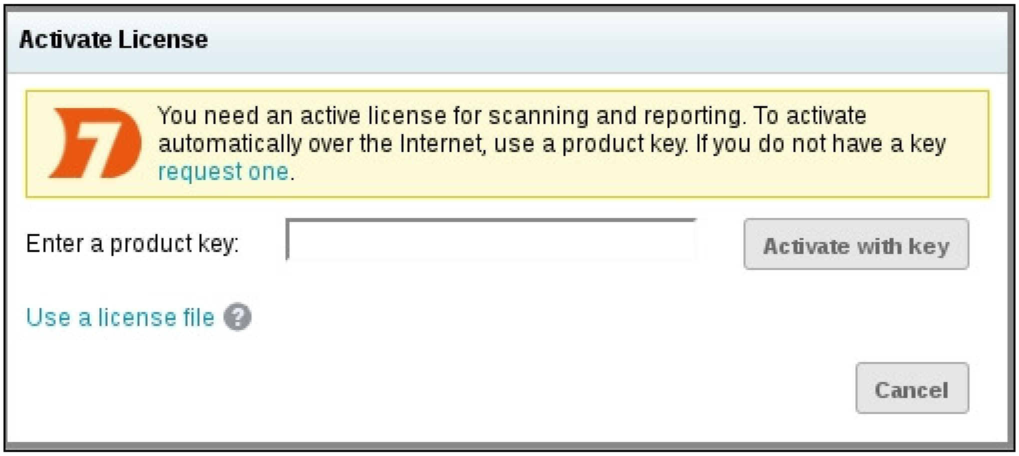
https://127.0.0.1:3780/login.html

Log on

User name: admin

Password: •••••••

4. The console will display an activation license dialog box. Enter the product key in the textbox and then click on **Activate with key** to complete this step, as shown in the following screenshot:



Activate License

You need an active license for scanning and reporting. To activate automatically over the Internet, use a product key. If you do not have a key request one.

Enter a product key:

The first time you log in to the console, you will see the NeXpose news page, which lists all of the updates and improvements in the installed NeXpose system. If you can see this page, it means that you have successfully installed the NeXpose Community Edition to your Kali Linux system.

Note

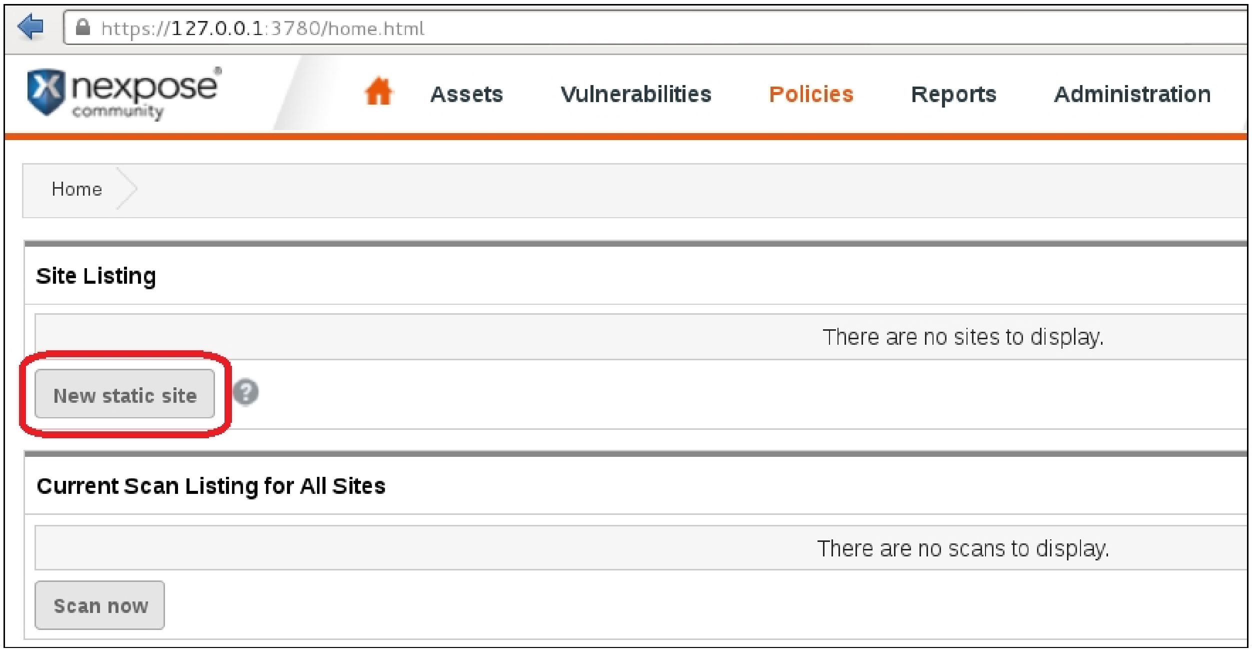
I found out that you may need to use the Firefox web browser instead of the Iceweasel web browser to successfully log in to the NeXpose security console. You can find references on how to install Firefox in Kali at:

http://kali4hackers.blogspot.com/2013/05/install-firefox-on-kali-linux.html

Using the NeXpose community

In our exercise, we will do a simple scan against our local network:

1. In the NeXpose dashboard, click on **Home**; to scan a site, click on **New static site** in **Site Listing**, as shown in the following screenshot:



https://127.0.0.1:3780/home.html

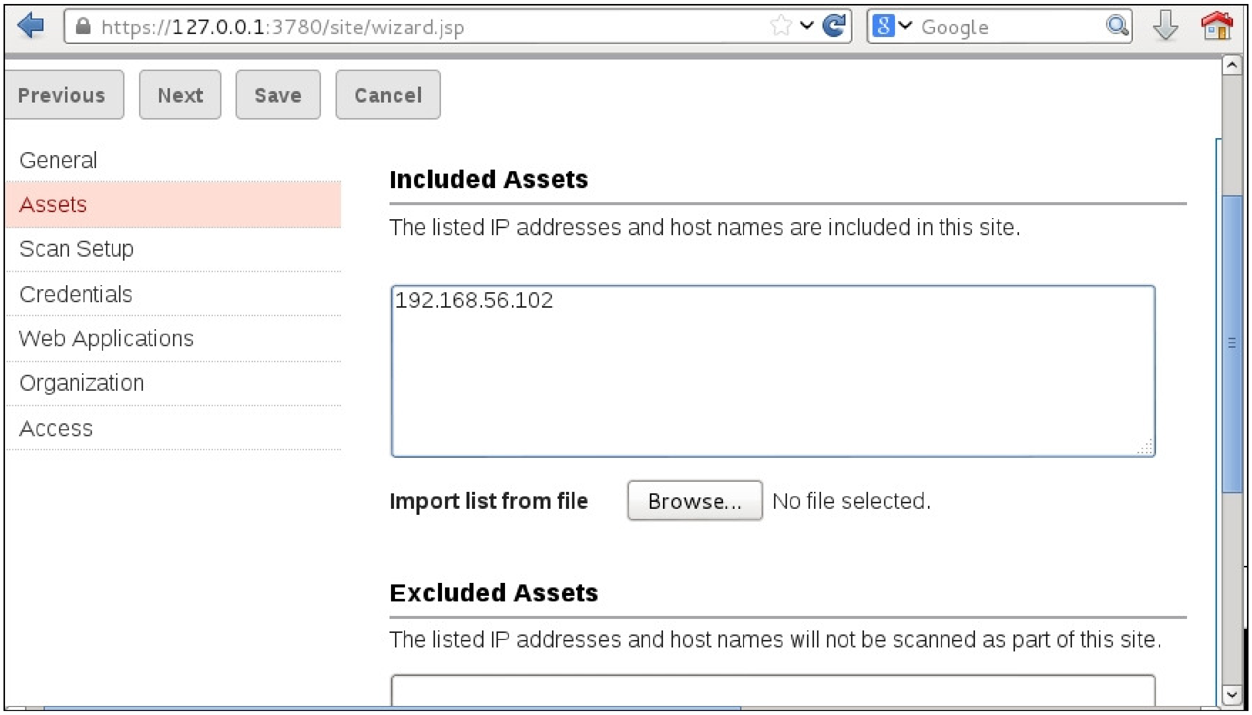
Site Listing

There are no sites to display.

Current Scan Listing for All Sites

There are no scans to display.

2. Next, you will be guided by the wizard to configure the site. First, navigate to the **Site Configuration** | **General** tab. In this tab, you give the site a name, importance, and description. Click on **Next** to continue to the next tab.
3. In the **Assets** tab, you define the IP addresses that you want to scan. Bear in mind that in the NeXpose Community Edition, you are limited to scan only 32 IP addresses. Click on **Next** to continue to the next tab. In this example, we are going to scan the IP address of the **Metasploitable 2** machine that has the IP address of `192.168.56.102`, as shown in the following screenshot:



Included Assets

The listed IP addresses and host names are included in this site.

192.168.56.102

Import list from file No file selected.

Excluded Assets

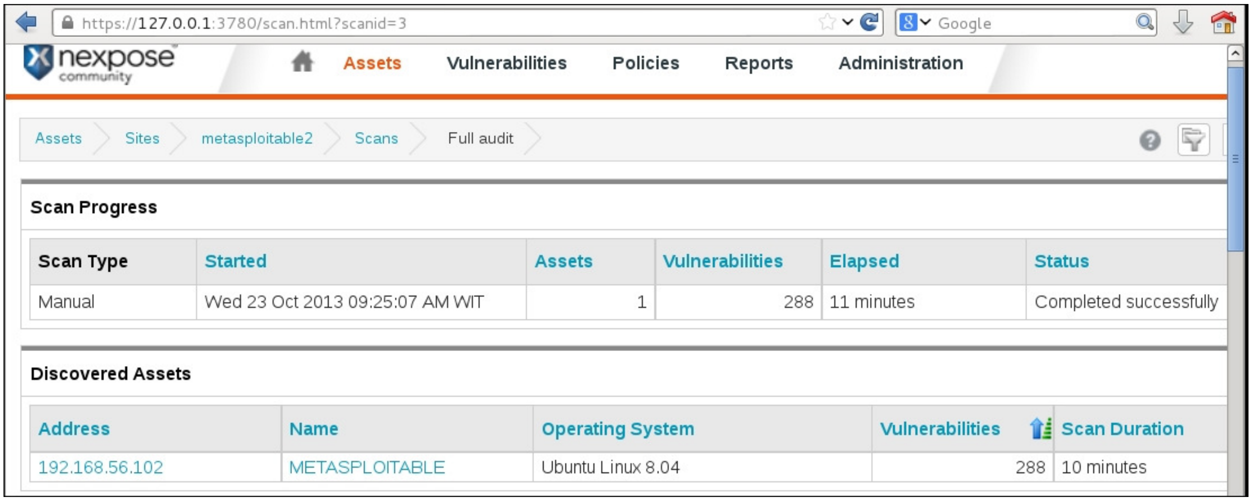
The listed IP addresses and host names will not be scanned as part of this site.

4. Then, you need to configure the **Scan Setup**; just use **Full audit** as the template. For the other settings, just use the default settings. Click on **Next** to continue to the next tab.

5. After that, save the configuration by clicking on the **Save** button; you will see your newly created site in **Site Listing**. You can run the manual scan by clicking on the scan icon.

6. You will see the **Start New Scan** window. Verify that the information is correct. After that, you can start the scan by clicking on the **Start now** button.

7. The scan process runs. After several minutes, the scan is completed and shows the results that are shown in the following screenshot:



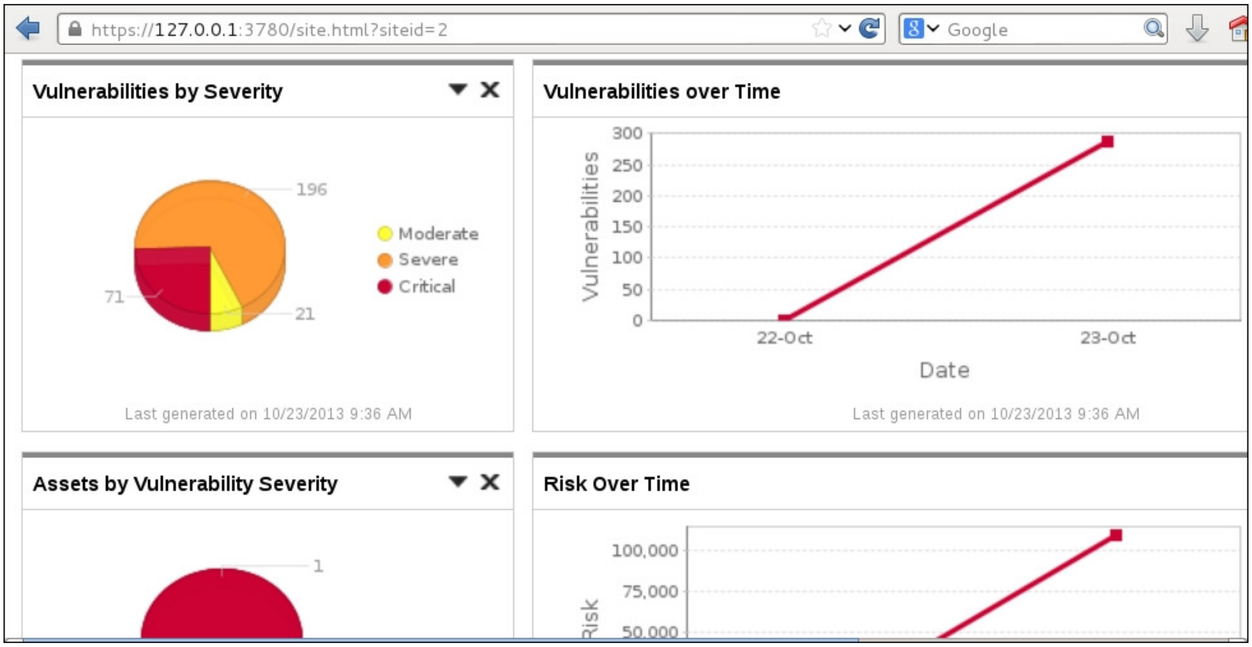
Scan Progress

Scan Type	Started	Assets	Vulnerabilities	Elapsed	Status
Manual	Wed 23 Oct 2013 09:25:07 AM WIT	1	288	11 minutes	Completed successfully

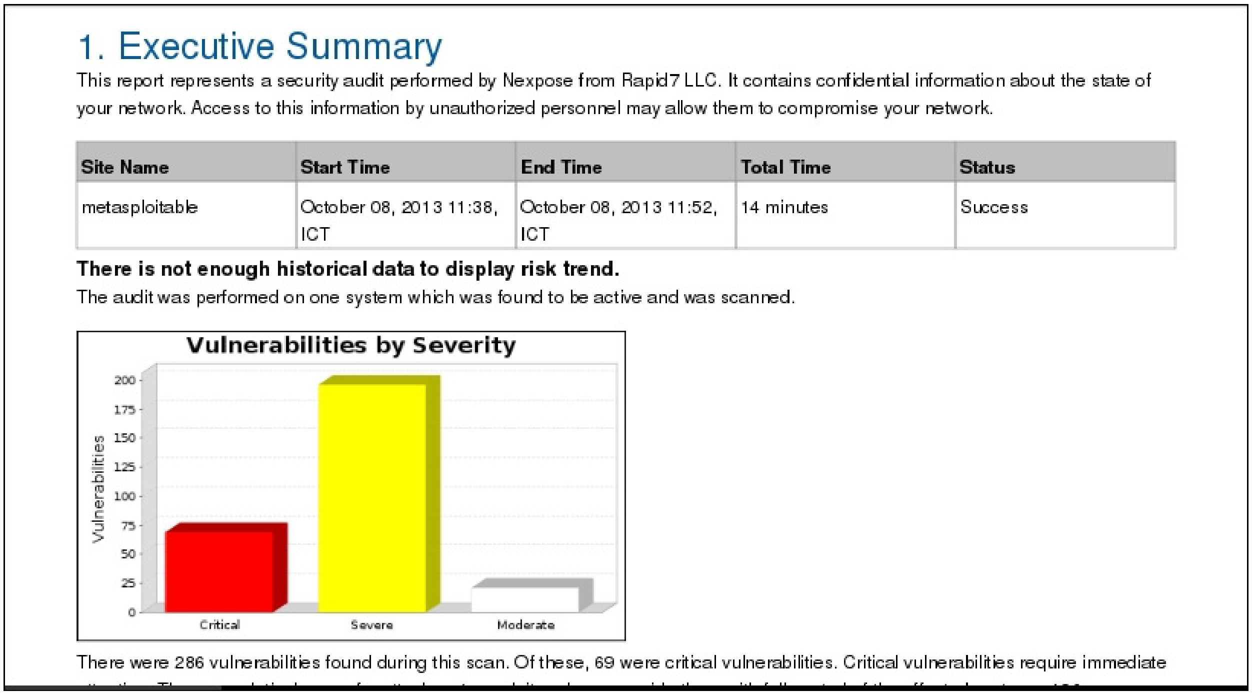
Discovered Assets

Address	Name	Operating System	Vulnerabilities	Scan Duration
192.168.56.102	METASPLOITABLE	Ubuntu Linux 8.04	288	10 minutes

8. Following screenshot is the vulnerabilities report for the target machine:


https://127.0.0.1:3780/site.html?siteid=2
Google
Vulnerabilities by Severity
196
71
21
Moderate
Severe
Critical
Last generated on 10/23/2013 9:36 AM
Vulnerabilities over Time
Vulnerabilities
300
250
200
150
100
50
0
22-Oct
23-Oct
Date
Last generated on 10/23/2013 9:36 AM
Assets by Vulnerability Severity
1
Risk Over Time
Risk
100,000
75,000
50,000

9. To see a detailed audit report, you need to run the **Report Generator** option, made accessible by clicking on **Reports** on the top menu. Following is the result of the report:



1. Executive Summary

This report represents a security audit performed by Nexpose from Rapid7 LLC. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

Site Name	Start Time	End Time	Total Time	Status
metasploitable	October 08, 2013 11:38, ICT	October 08, 2013 11:52, ICT	14 minutes	Success

There is not enough historical data to display risk trend.

The audit was performed on one system which was found to be active and was scanned.

There were 286 vulnerabilities found during this scan. Of these, 69 were critical vulnerabilities. Critical vulnerabilities require immediate

That's all for a very brief overview of NeXpose Community Edition; in the next section, we will describe several web application tools.