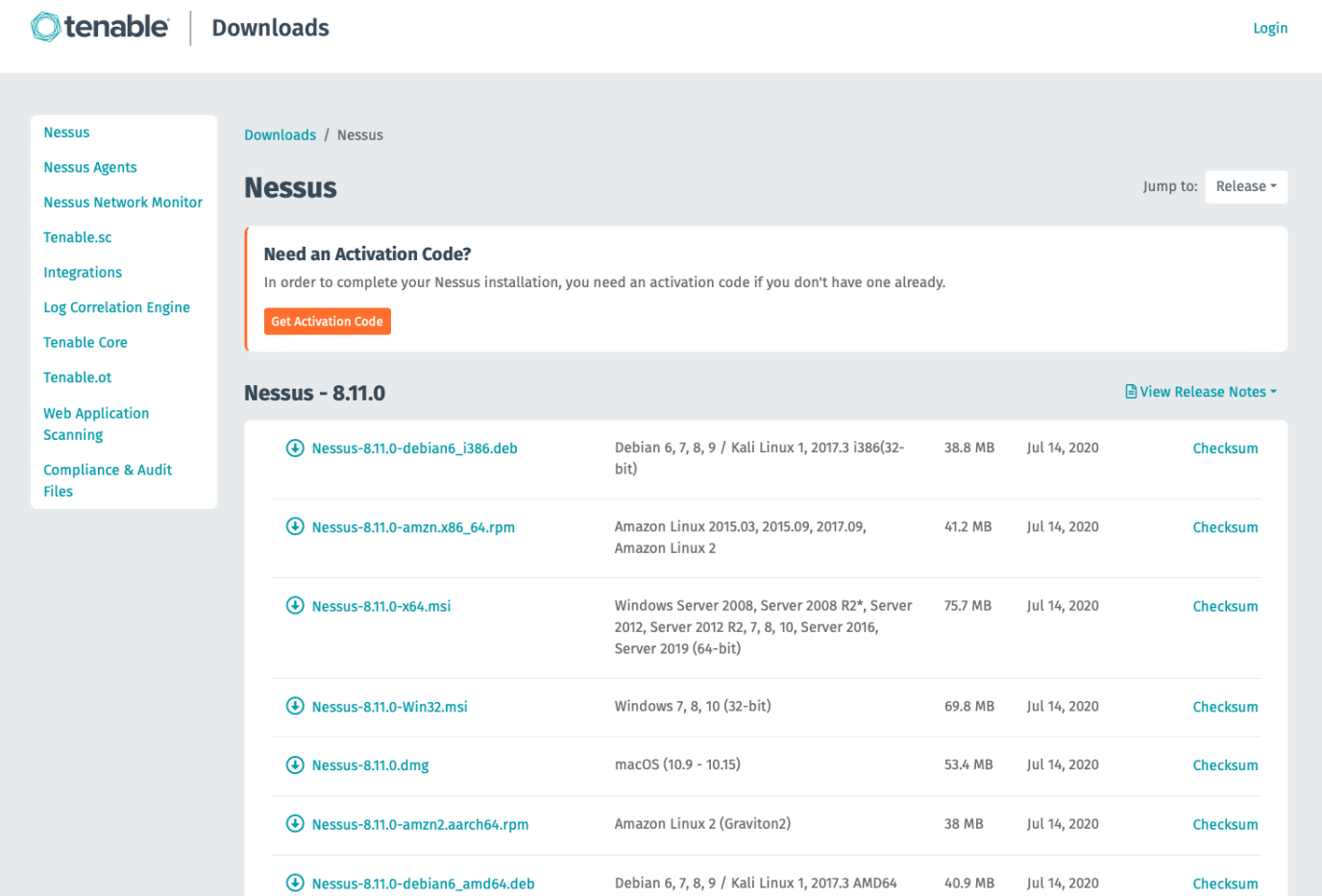
Scanning with Nessus

Part 1

Nessus is a vulnerability scanner. It is usually used as on external pentesting. We can download Nessus by doing a simple google search and going to the following link: https://www.tenable.com/downloads/nessus?loginAttempted=true and choosing the desired file type based on your OS as shown below:



Once we download the file, open a Terminal session and go to the `Downloads` directory uwhere the file is stored using the `cd ~ && cd Downloads` command. Next, use the `dpkg -i <Nessus_Package_File_Name>` command to unpack/depackage the .deb file as shown below:

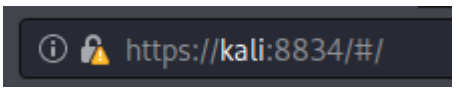
```
root@kali:~# cd ~ && cd Downloads
root@kali:~/Downloads# dpkg -i Nessus-8.11.0-ubuntu1110_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 343734 files and directories currently installed.)
Preparing to unpack Nessus-8.11.0-ubuntu1110_amd64.deb ...
Unpacking nessus (8.11.0) ...
Setting up nessus (8.11.0) ...
Unpacking Nessus Scanner Core Components...

 - You can start Nessus Scanner by typing /etc/init.d/nessusd start
 - Then go to https://kali:8834/ to configure your scanner

Processing triggers for systemd (245.6-2) ...
root@kali:~/Downloads#
```

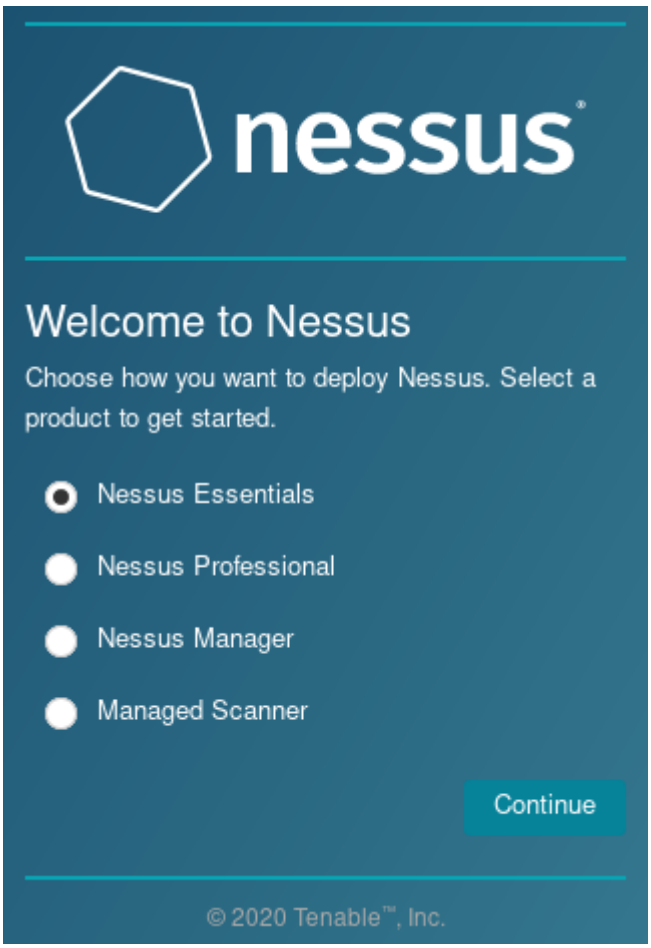
The package installed automatically.

As we can see, we have to use the `/etc/init.d/nessusd start` command to start the Nessus service as shown below:

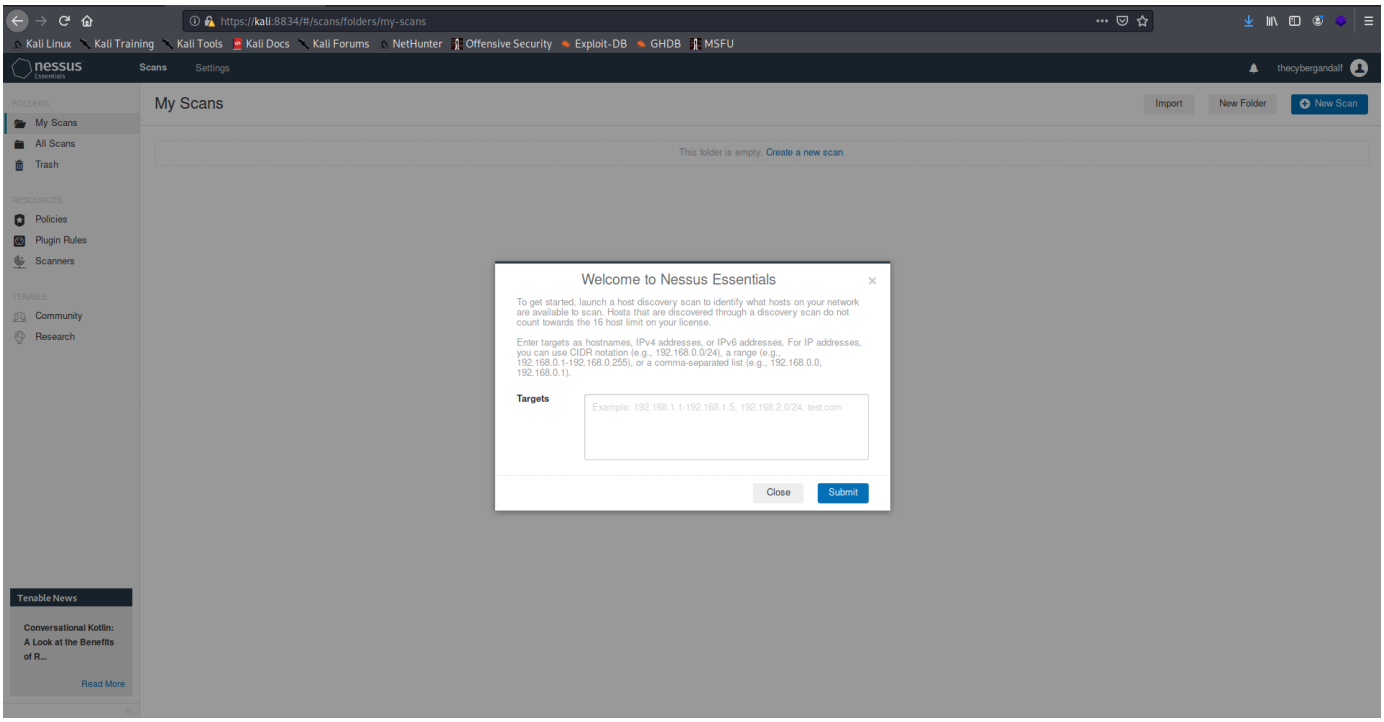
```
root@kali:~/Downloads# /etc/init.d/nessusd start
Starting Nessus : .
```

We can also see from the original `dpkg...` command that there is a URL that we can use to access the Nessus GUI, `https://kali:8834/` as shown below. It will give a warning (You can ignore this warning):

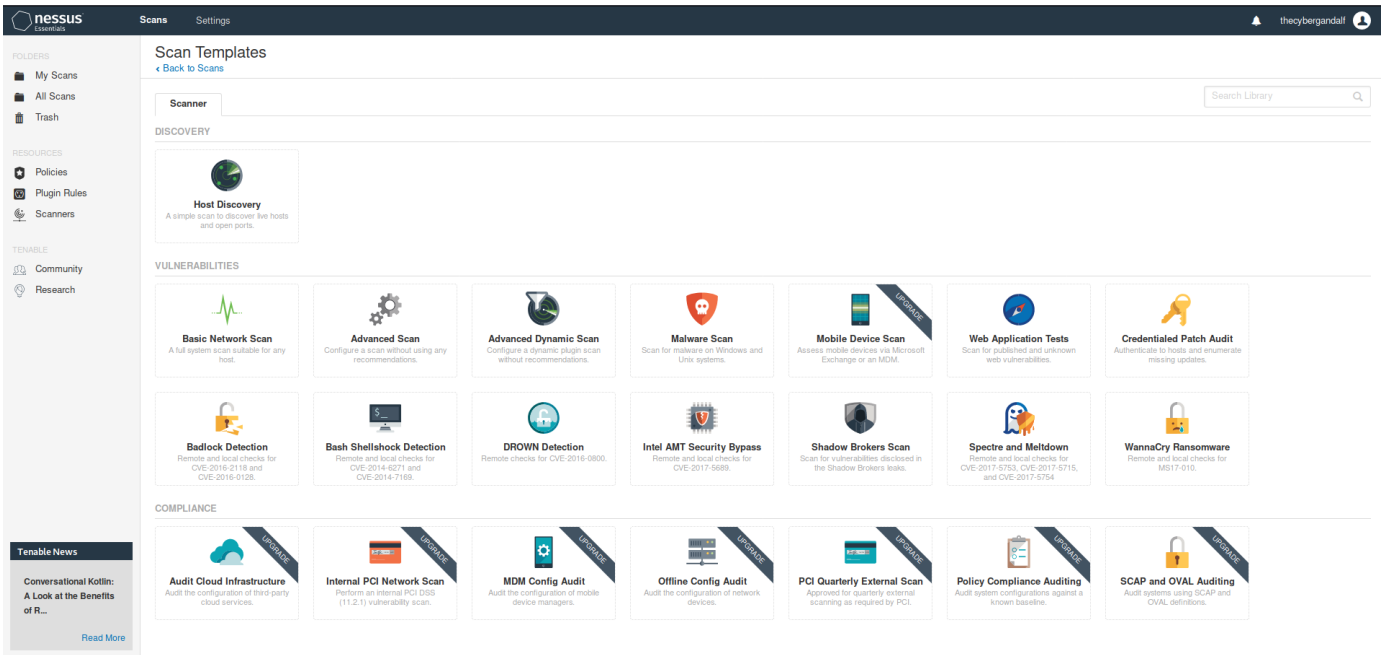




We will be using `Nessus Essentials`. You will also need a valid email for an activation code. Go through the process and complete the account creation process. Once the account setup process is done, the system will take some time to download required plugins for full functionality. Once you are done with the process and login, you will be met with this page:



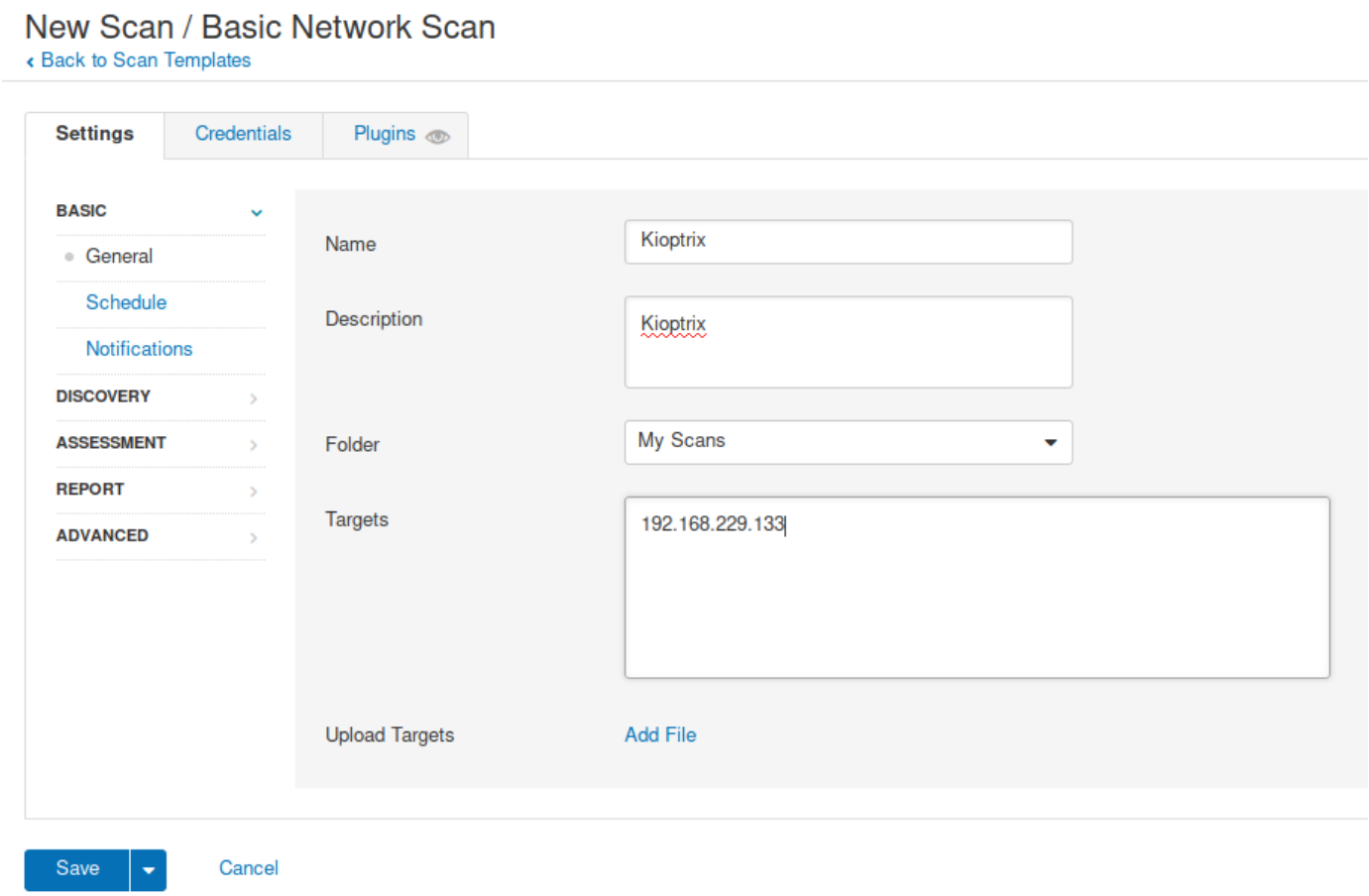
In the `Targets` box, you can enter the IP address of a target or IP adress range of targets. We will click on `Close` as we are not ready to start scanning. On the top-right corner, click on `New Scan` and we will get this page:



Since we are using the free edition of Nessus, we are allowed to perform scans on any Private IP (network address) and we can scan up to 16 IP addresses at a time.

We will use the `Basic Network Scan` first as shown below:

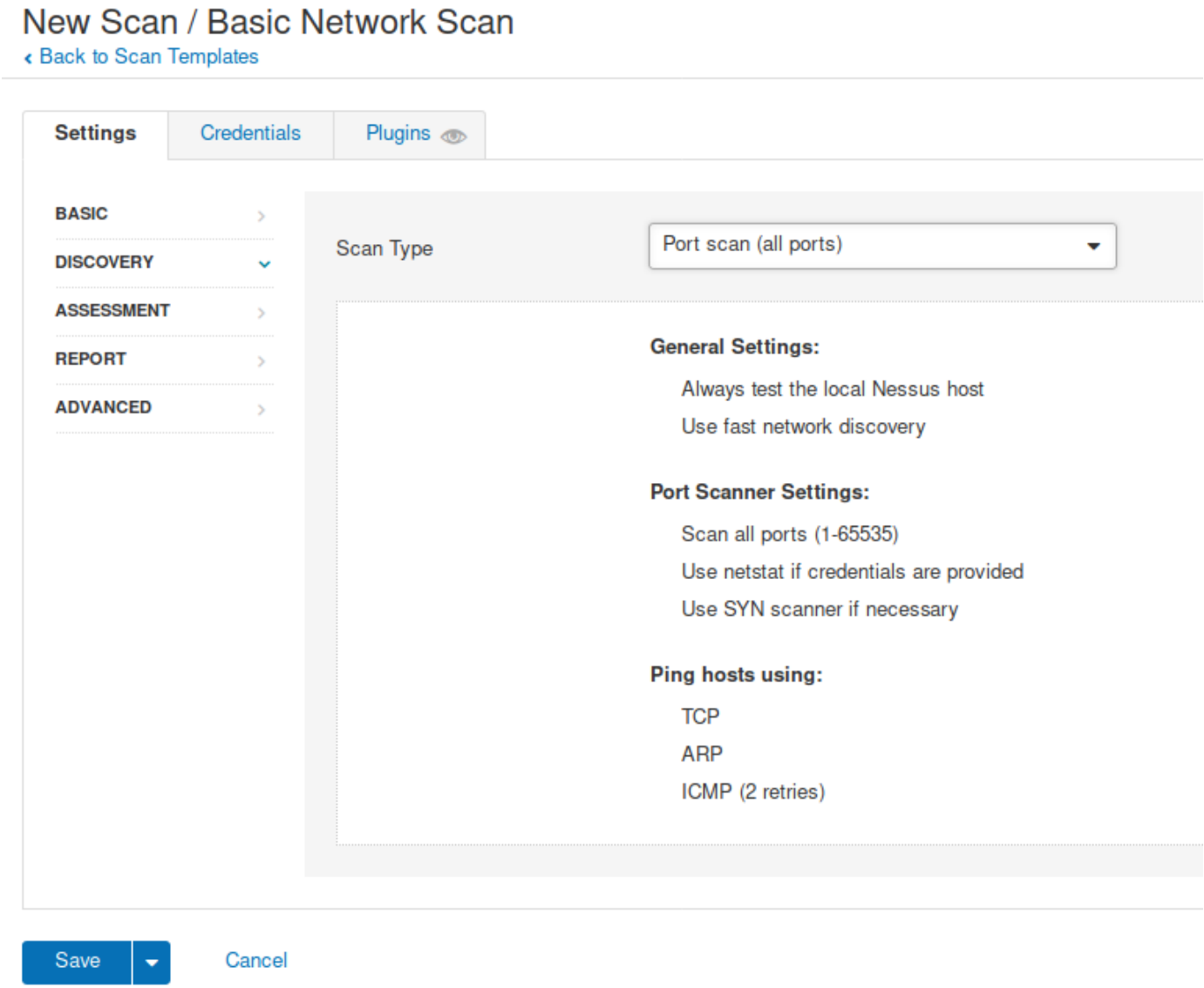
In the `Settings` tab, select `Basic`. Under `Basic`, select `General`. Since our target is the Kioptrix VM, we did the following:



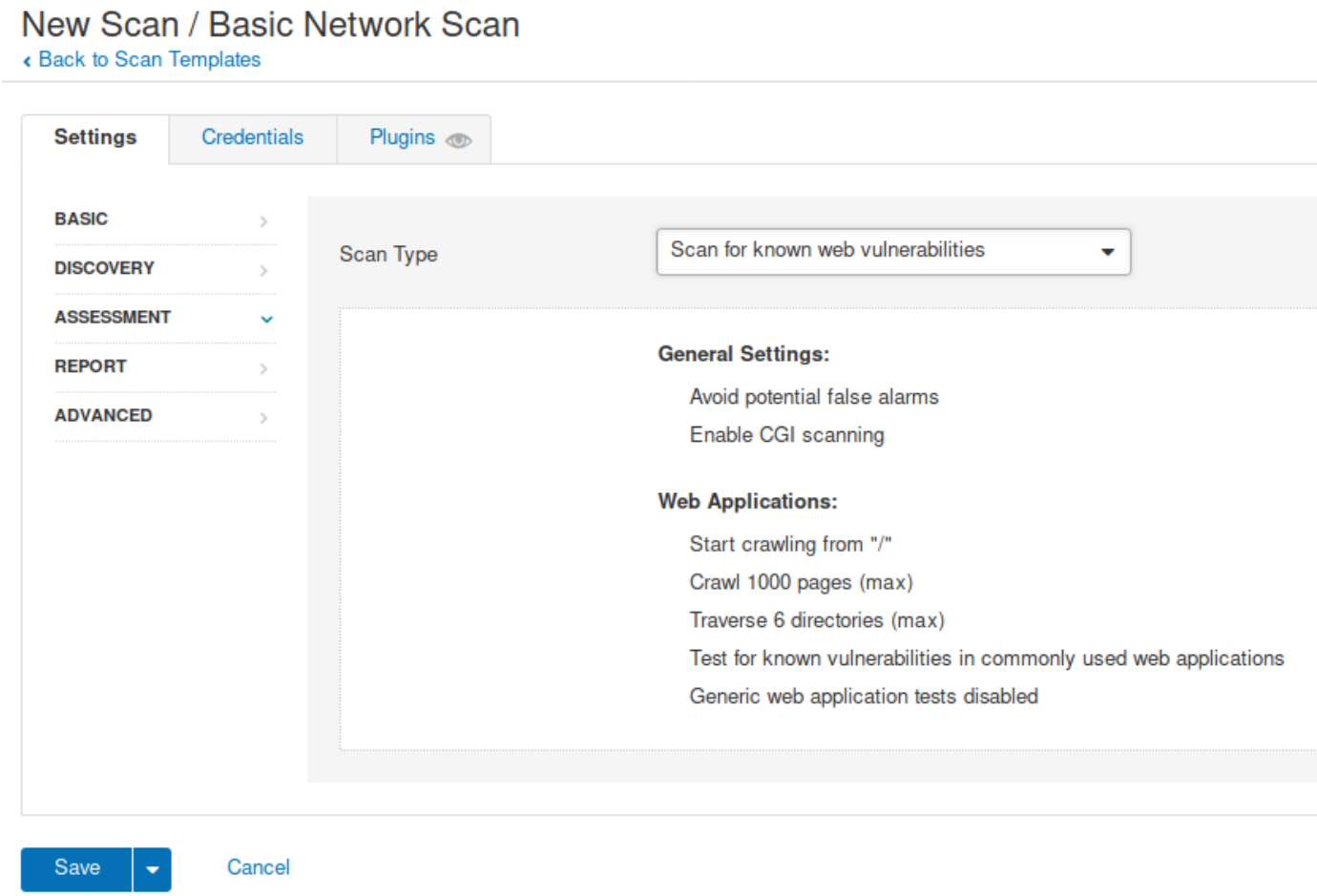
Next, go to the `Schedule` option. This option allows you to automate the scans.

The `Notifications` option allows you to send email notifications about scan progress if you have an SMTP server.

Next, go to the `Discovery` menu. Change the `Scan Type` to `Port scan (all ports)` is similar to `-p-` in Nmap as shown below:



Next, go to the `Assessment` option and change the `Scan Type` to `Scan for known web vulnerabilities` as shown below. The other options such as, `Scan for all web vulnerabilities (complex)` might take a longer time:



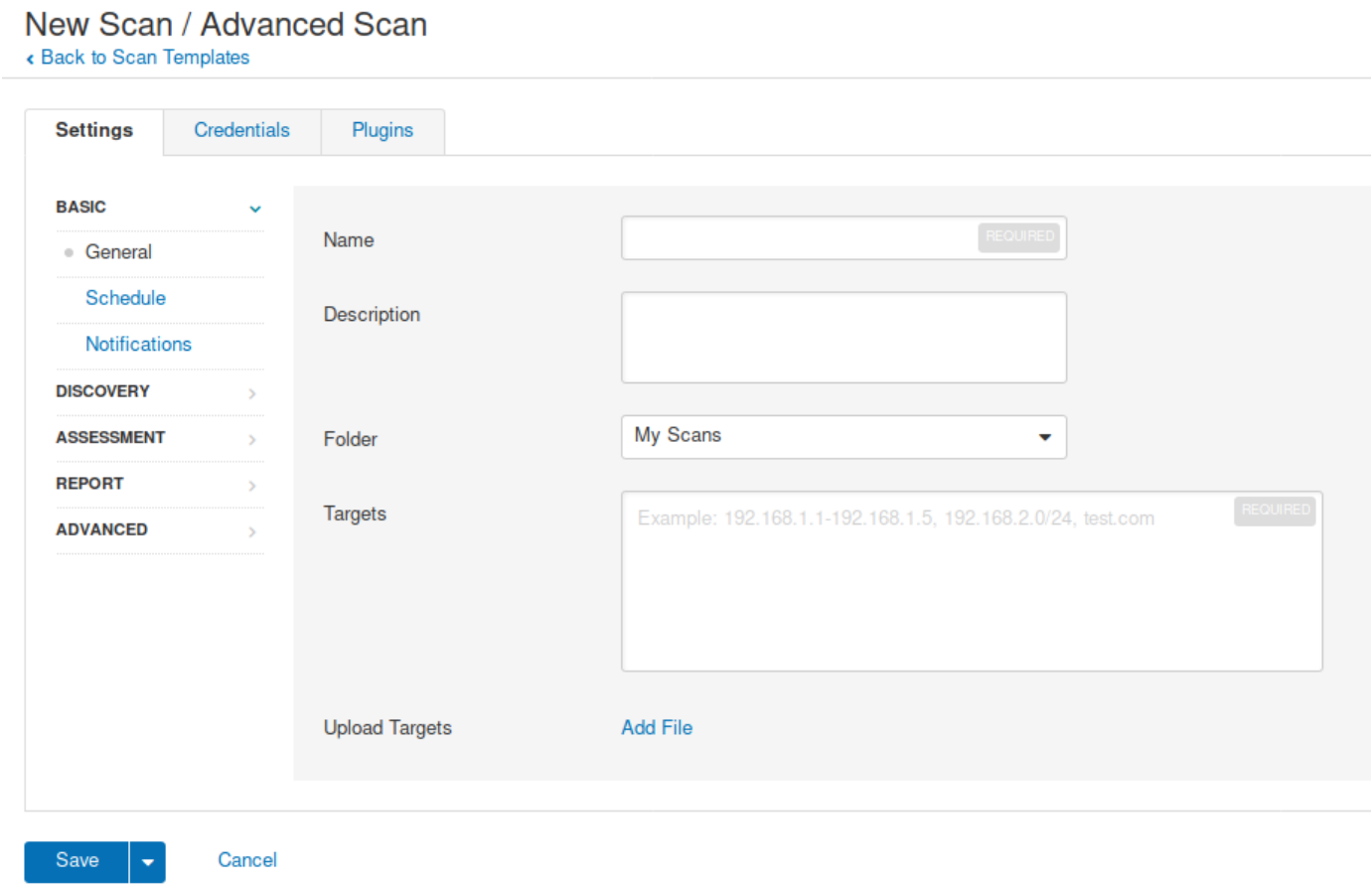
Next, go to the `Report` option, under `Output` leave the default settings.

Next, go to the `Advanced` option and leave the default settings.

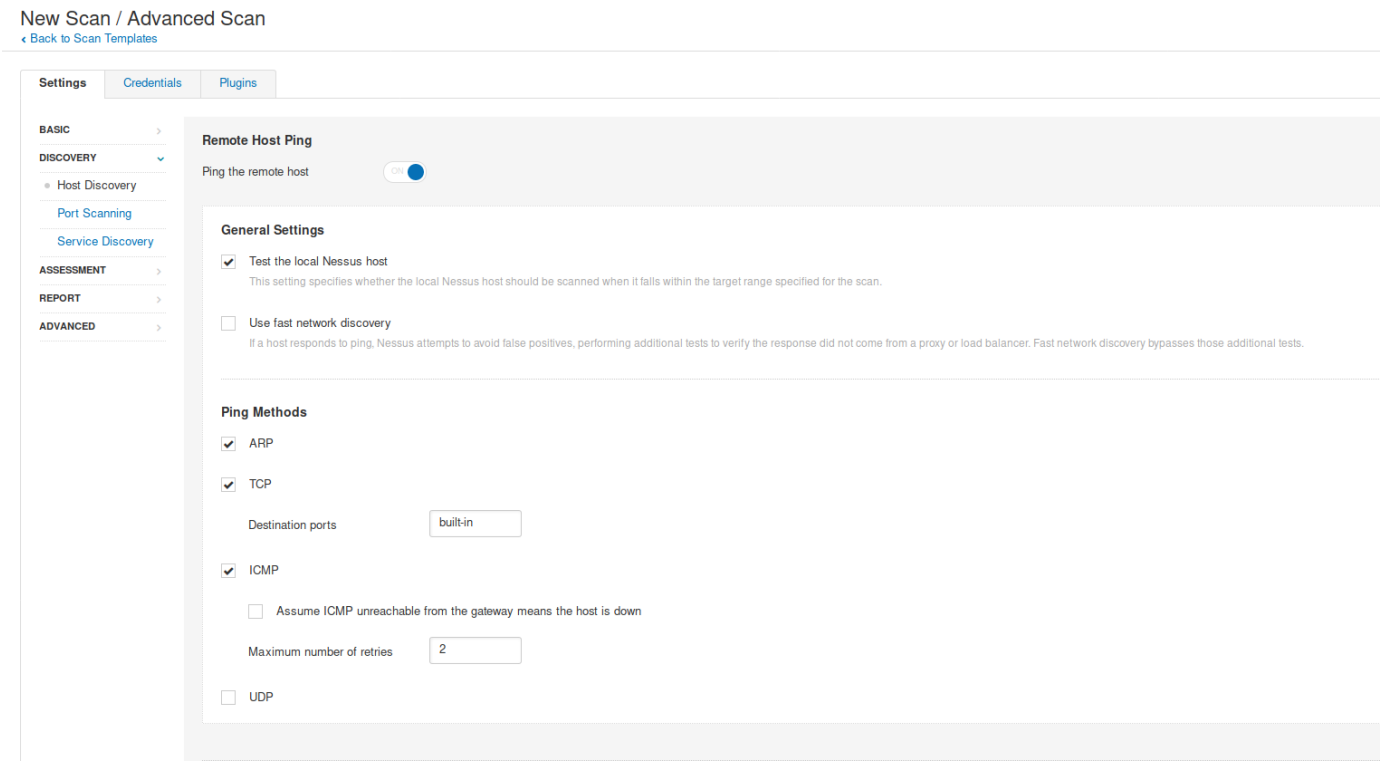
Finally, click on `Save`.

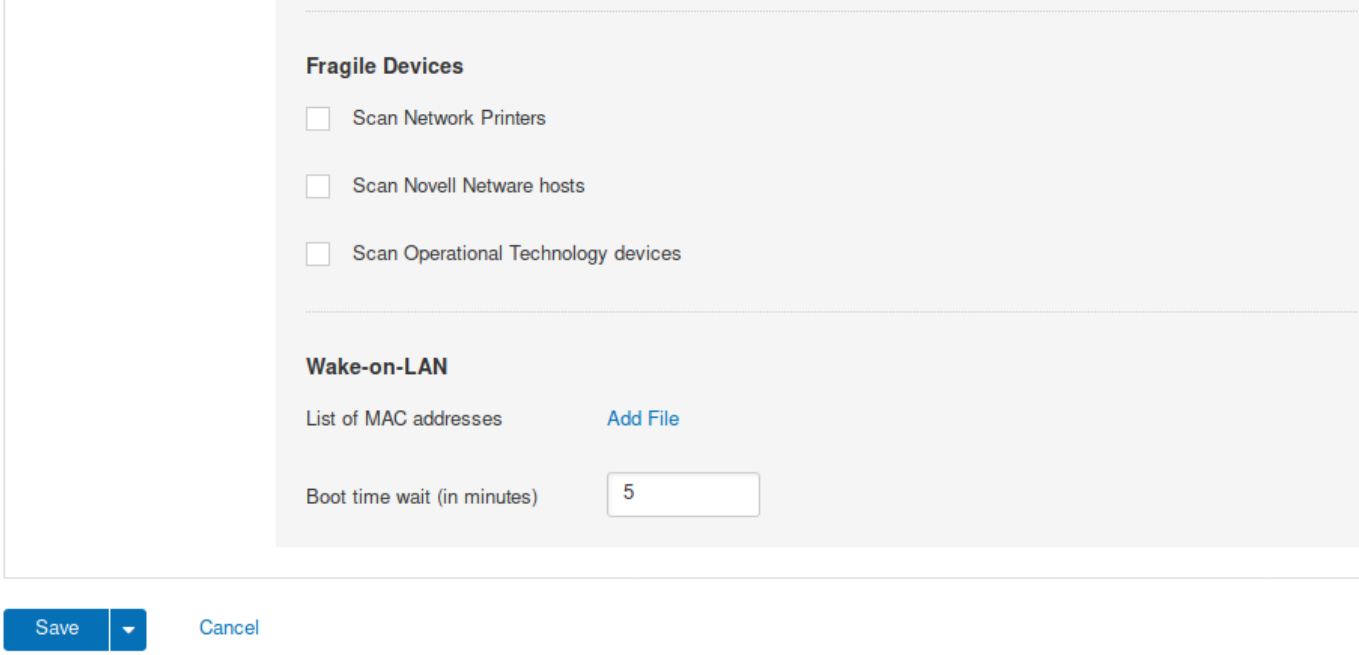
Back in the `My Scans` folder, click on the "Play" button to launch the scan as shown below:

While the scan is running, we'll go look at some of the other scan types by clicking on `New Scan`. We will look at `Advanced Scan` as shown below:



The `Basic` options are similar to the `Basic Scan` scan type. However, the `Discovery` option is different as shown below. The `Host Discovery` option gives us the option to ping or not ping the remote host (target) and few other options.



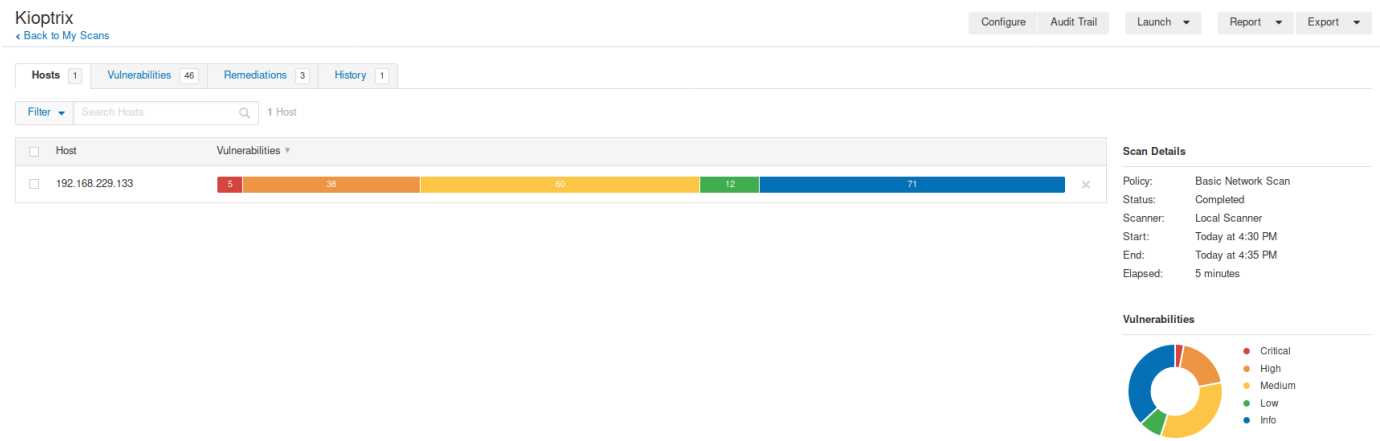


There are more tabs and options that will be discussed in the video (Youtube)

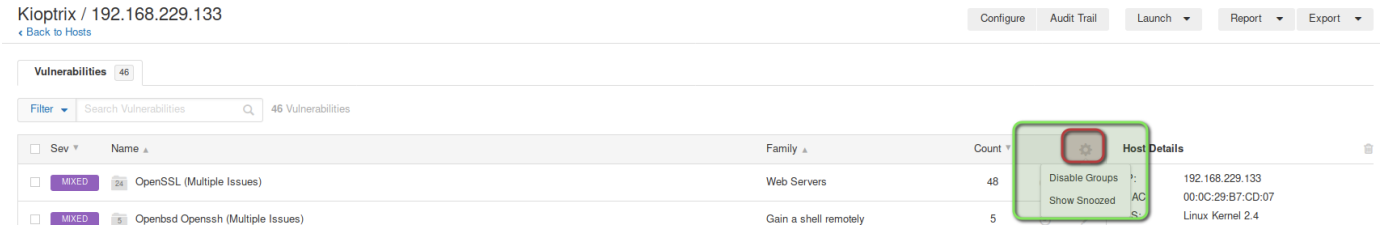
Part 2

Let's view the results of our Basic Scan. To do this, go to `My Scans`, click on the desired scan, then click on the IP address of the desired host, then click on the gear (Settings) button and select `Disable Groups` to help us view the individual vulnerabilities as shown below:

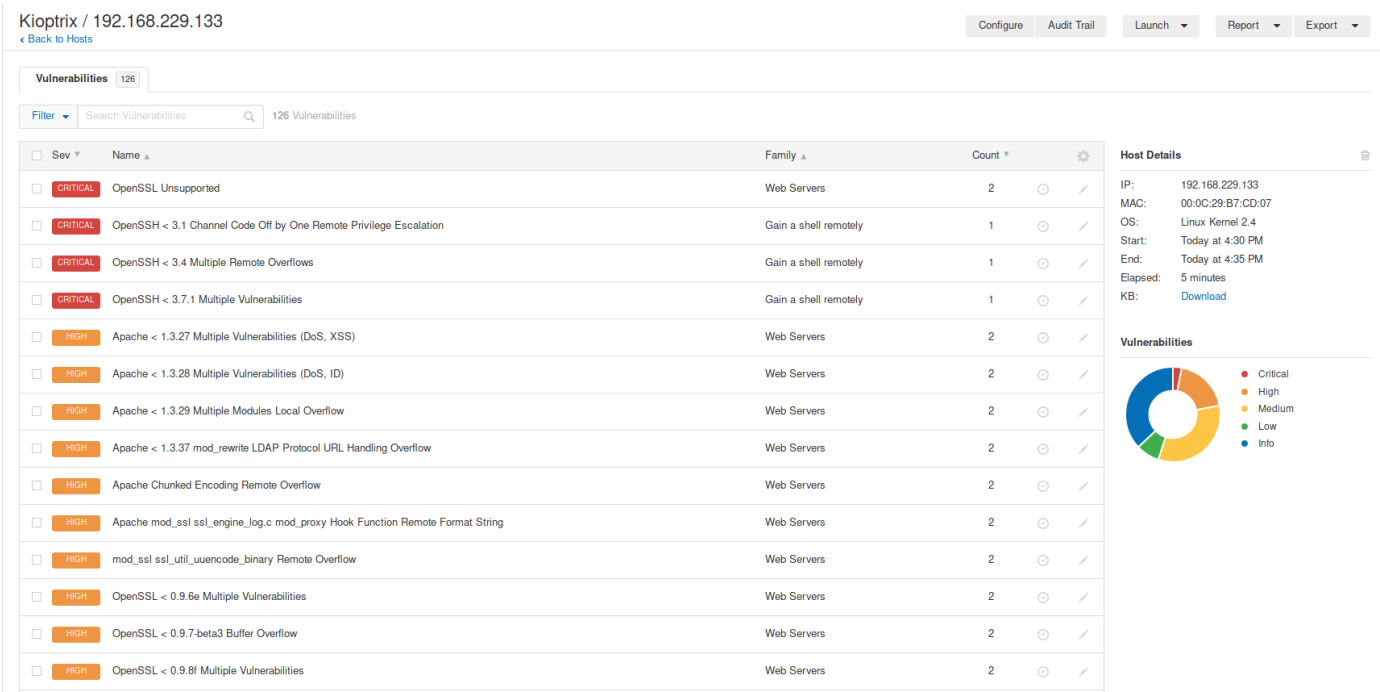
Next =>



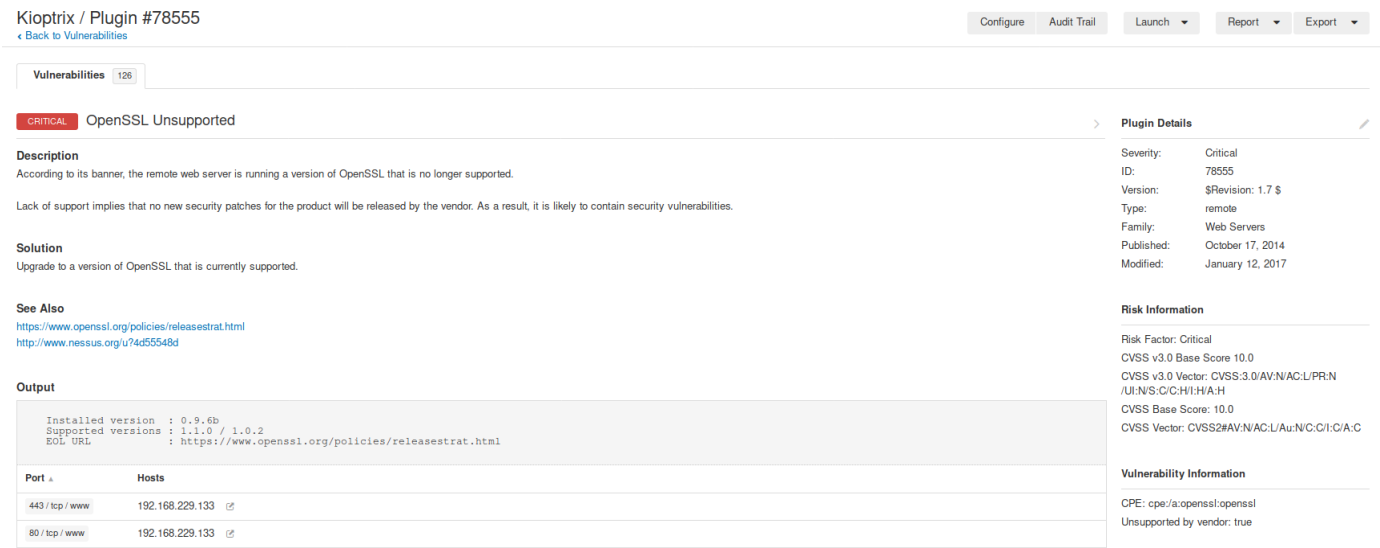
Next =>



Next =>



We can click on any vulnerability and examine the details as shown below:



We can do this for necessary vulnerabilities such as critical vulnerabilities and we can research and report these.

We can also try to export the vulnerabilities as shown in the video (Youtube).

Do not always trust vulnerability scanners. Always go out and use other tools to find these vulnerabilities.