Part 03 - Setup OpnSense

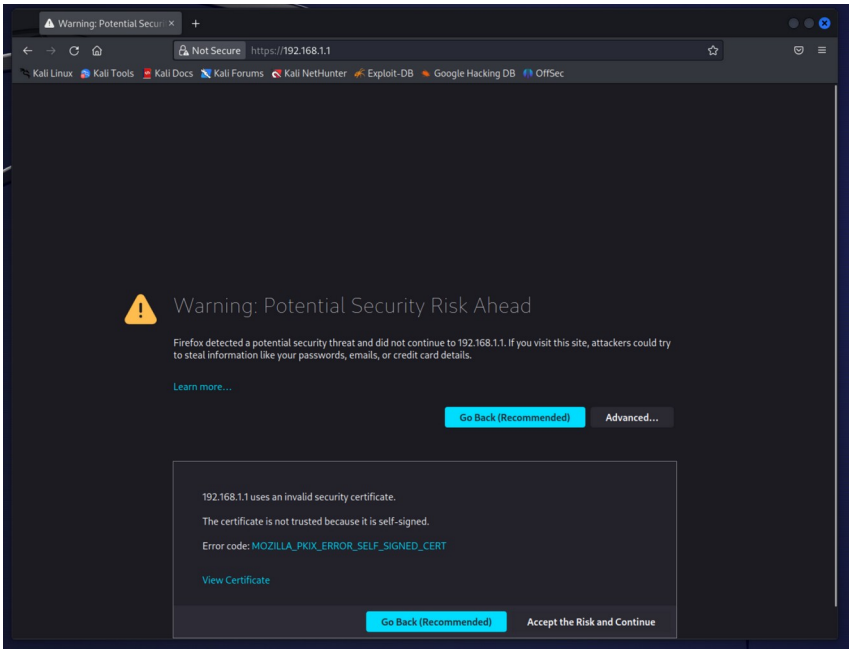
This tutorial covers setting up OpnSense and configuring the firewall, DHCP and IPS.

It is assumed that you have Virtual-Box installed. It is also assumed that Part 1 and Part 2 are completed.

1) Make sure that your OpnSense VM and your Kali Linux VM are running.

2) Log into your Kali Linux VM and open a web browser.

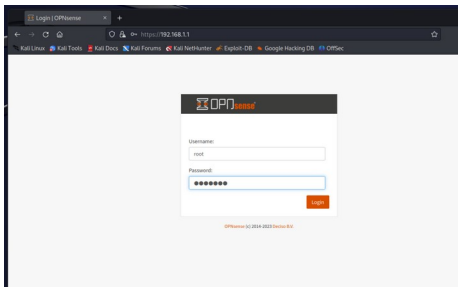
3) In the web browser, go to the IP address on the Firewall @ https://192.168.1.1



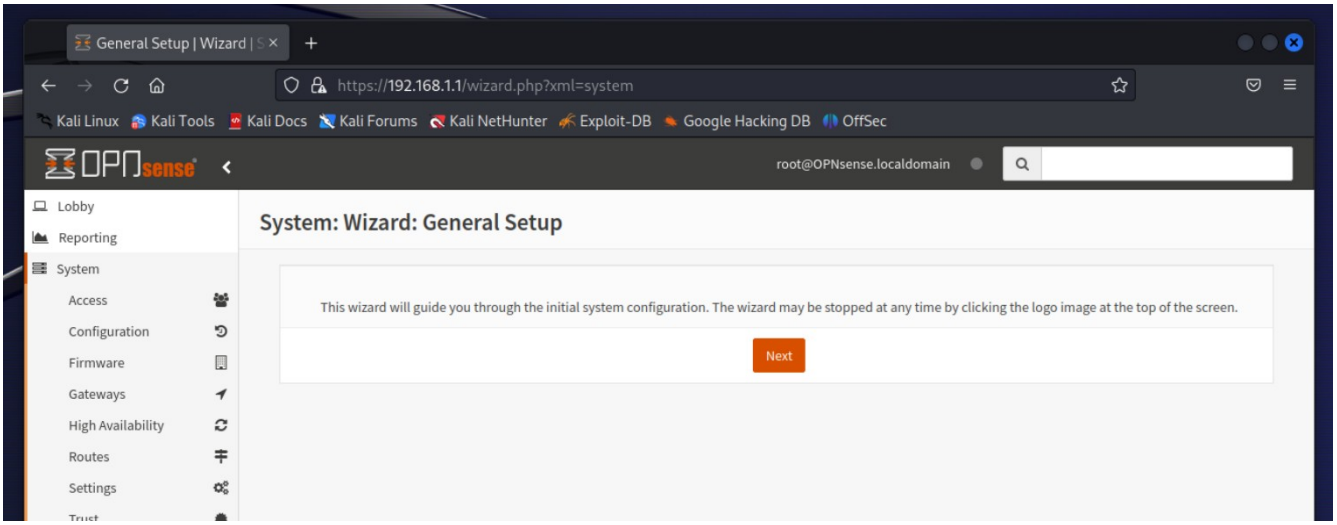
Since the connection is a self-signed certificate, you will need to select “Advanced…” and select “Accept Risk and Continue”.

4) You will be brought to the login screen. The username as password are as follows:

- username: root
- password: *whatever you set in part 1, when you installed OpnSense.*
  - If you left the password default, the password is: opnsense

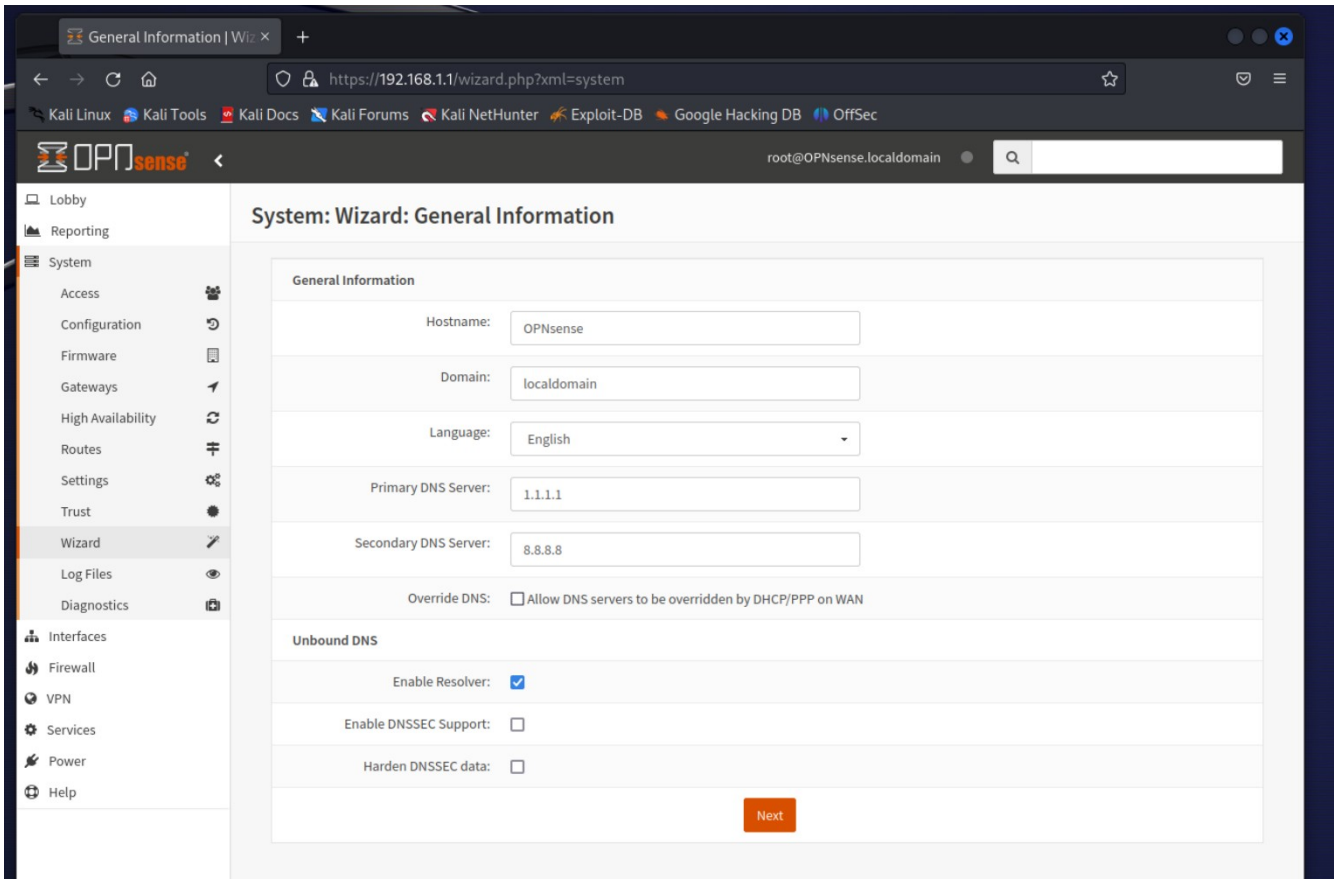


5) On your first login, you will be prompted to begin a setup wizard.

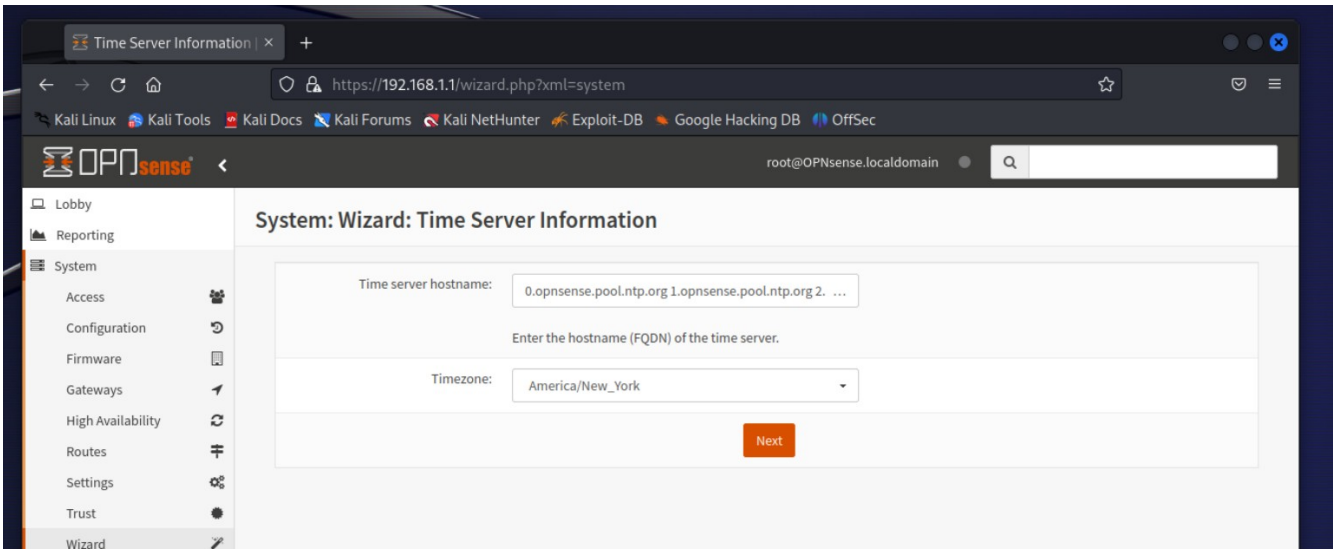


6) You can leave most of these default. For the Primary/Secondary DNS servers, you can set these to 1.1.1.1 and 8.8.8.8 (or a different dns server if you so choose for your application).

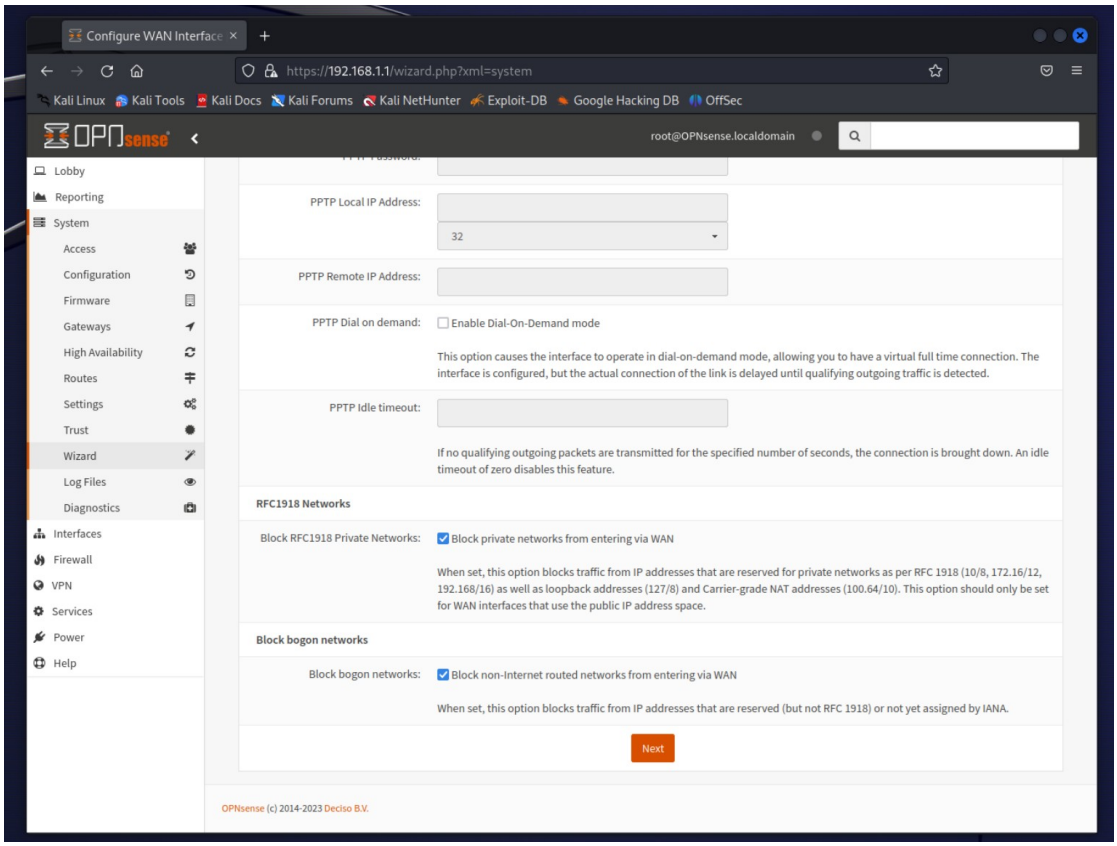
Additionally, select the check box to enable Unbound DNS resolver. You can optionally create static DNS entries at a later date.



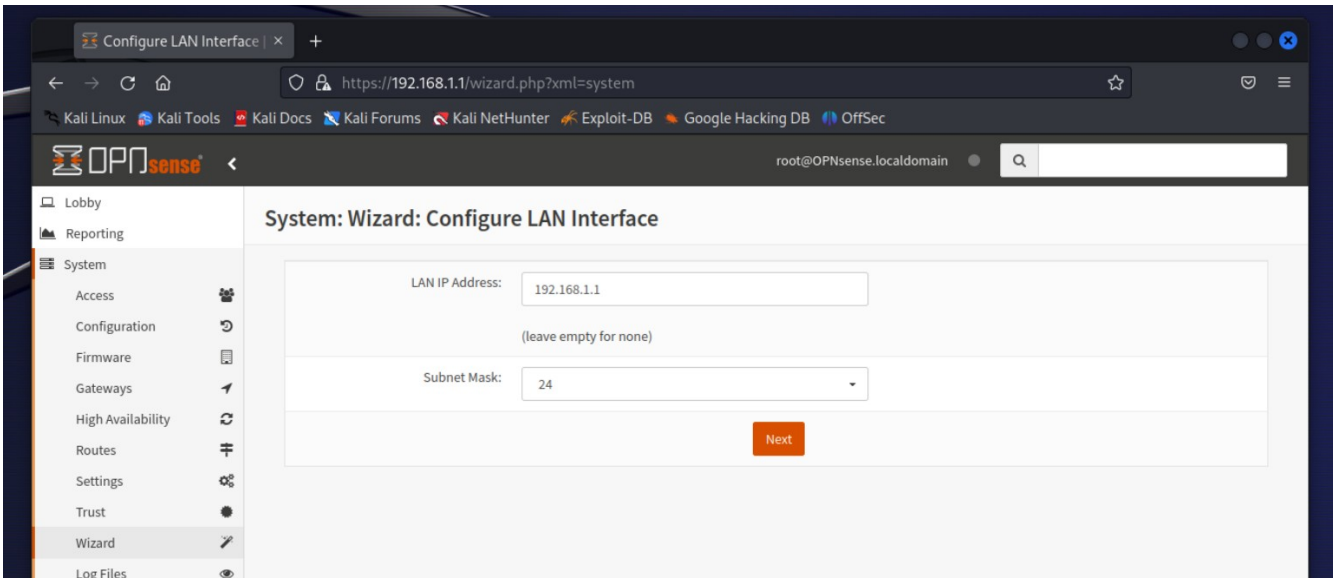
7) On the next screen, set you time server pool and your time zone.



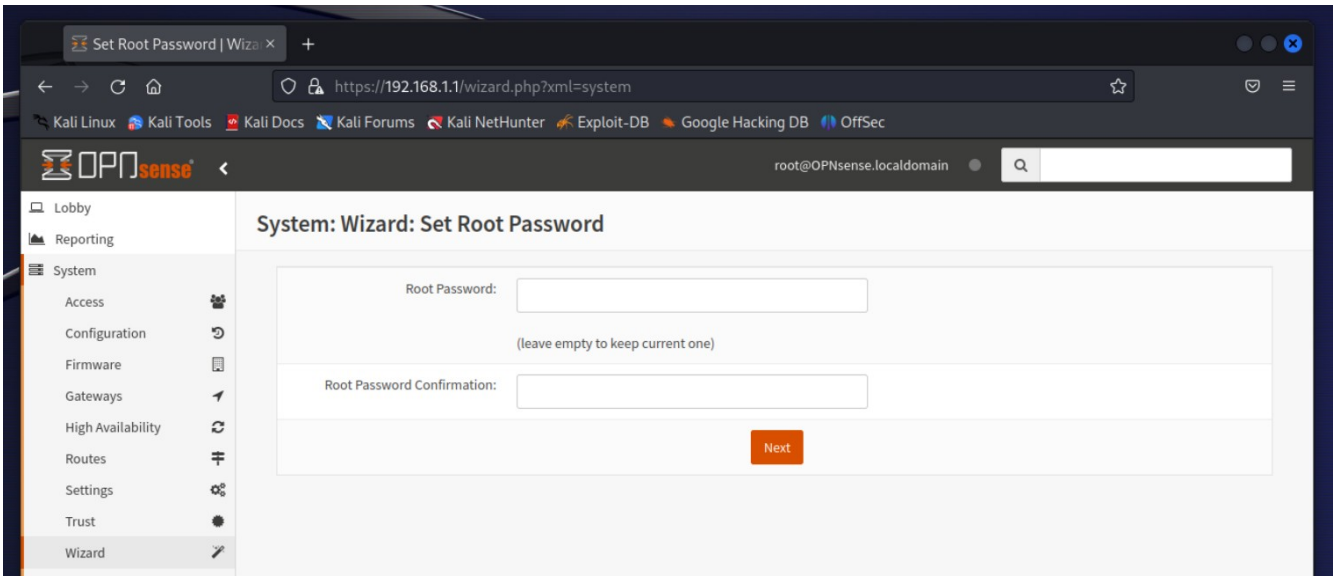
8) On the next screen, you can leave most options blank. Make sure you set the RFC 1918 block and Bogon network block at the bottom of the screen to on.



9) On the next screen you can change the network. Leave this as default and select next.



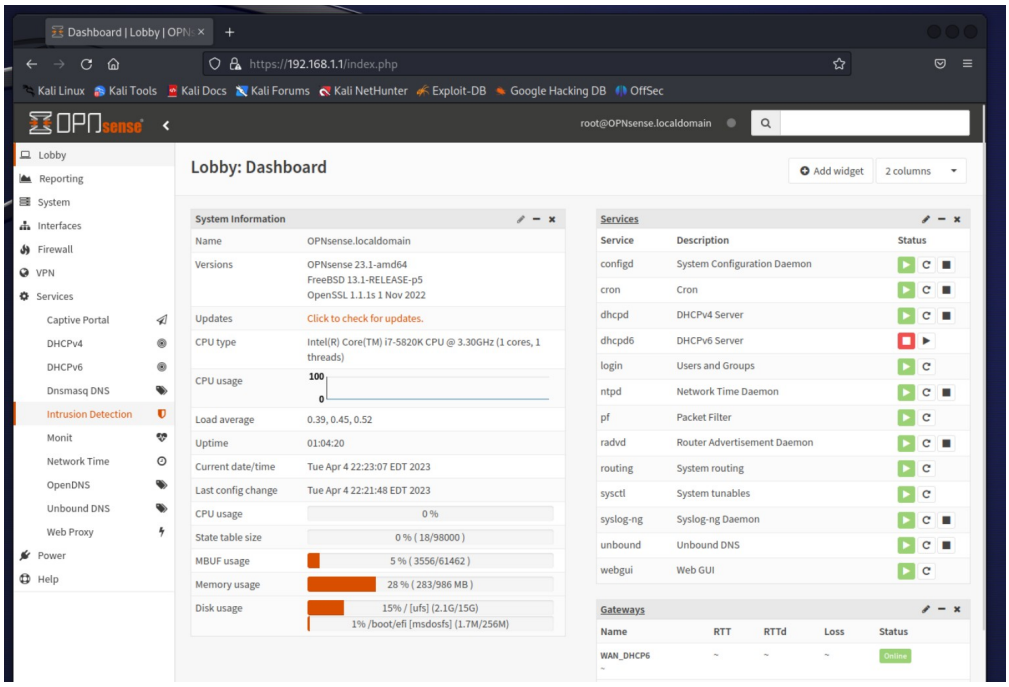
10) On the next screen, you can change the root password. Leaving this blank will keep the existing password set.



11) You will be now asked to reload the firewall to commit the setup.

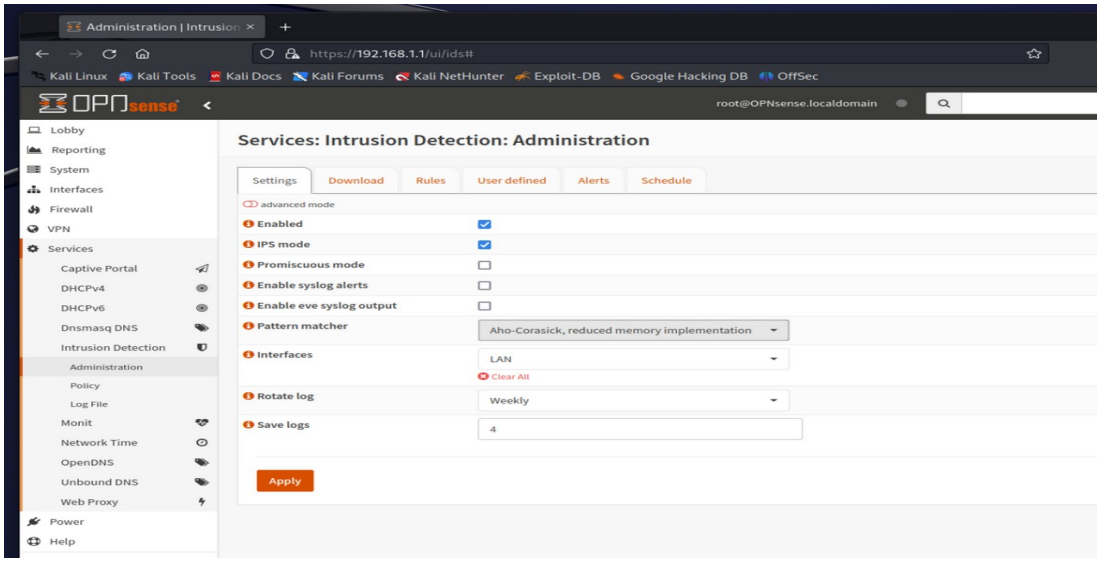
12) When your reload is complete, you should the landing page.

13) On the left hand side, under services, select Intrusion Detection. Since this virtual network will be running potentially malicious machines, we want to enable IPS filtering inside our virtual network, to protect our class/lab/home networks.



14) Under Intrusion Detection, turn on/set the following options:

- Enabled: Check
- IPS Mode: Check
- Pattern Matcher: Aho-Corasick, reduced memory implementation
- Interfaces: LAN (WAN optional)



15) Apply the changes.

16) Return to the Dashboard. You should see under running services, Intrusion Detection, listed as running. If it is not running, select the Play button, to start the service.