# Openvas

Opanvas on paketti jolla voidaan skannata laitteen haavoittuvuuksia.

Asenna openvas Kali linuxiin.

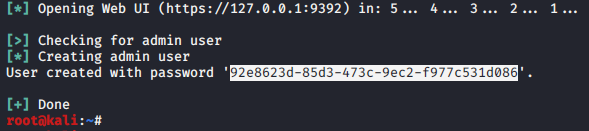
**apt install openvas**

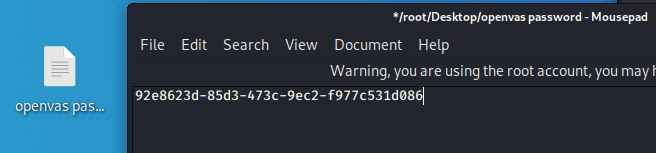
Aja openvas paketin setuppi

**openvas-setup**

Tämä prosessi vie melko kauan. Noin 15min. Älä lopeta prosessia.

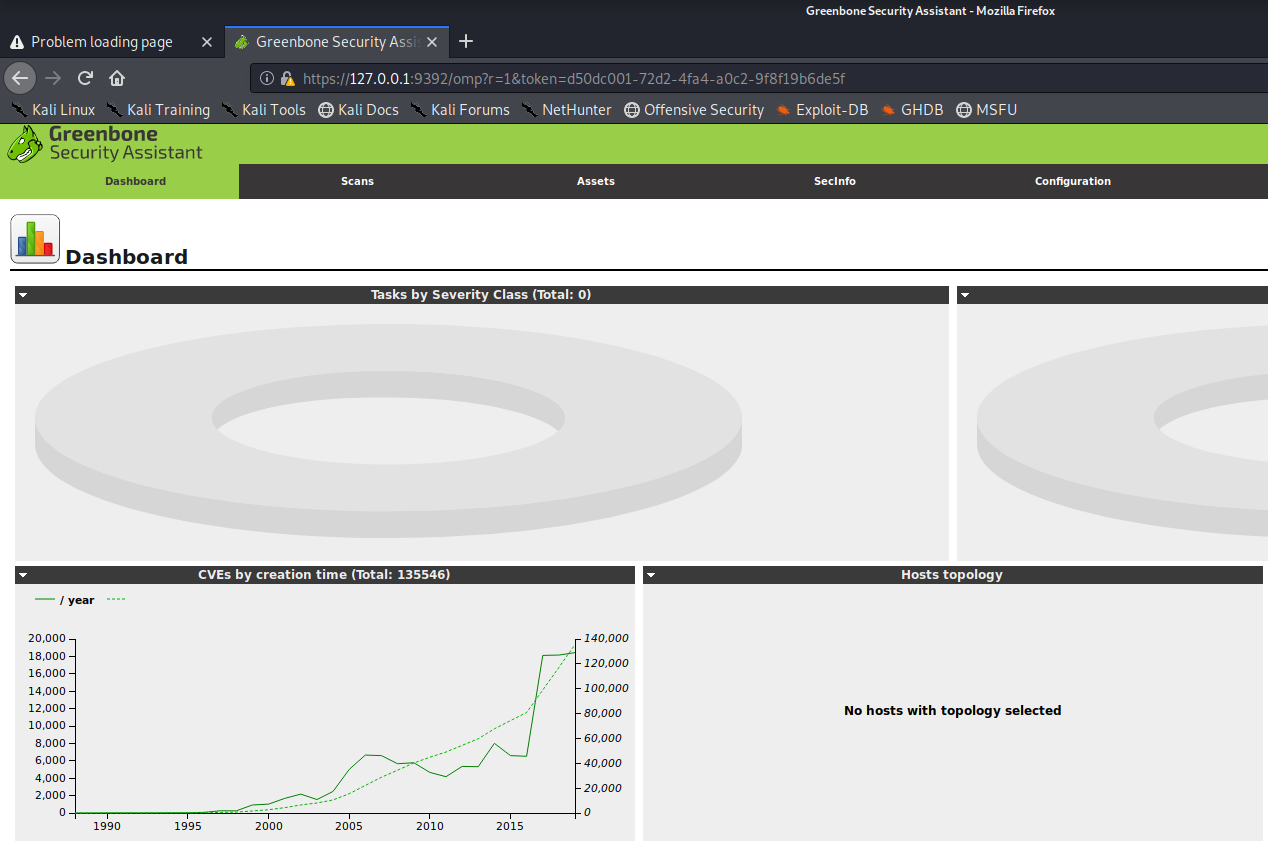
Asetuksen lopussa openvas luo admin nimisen käyttäjän ja sille salasanan. Kopioi salasana talteen johonkin! Esimerkiksi kalin työpöydälle tekstitiedostoon.





Avaa selaimessa osoite <https://127.0.0.1:9392>. Ja syötä admin käyttäjätunnus ja sen salasana.

Pääset selaimessa toimivaan openvas päänäkymään.



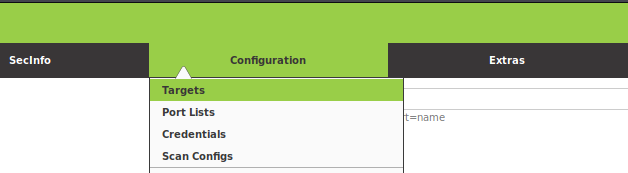
Openvas palvelun voit tarvittaessa lopettaa ja käynnistää uudelleen, jos et sitä enää tarvitse.

**openvas-stop**

**openvas-start**

## Kohteiden ja skannausten lisääminen

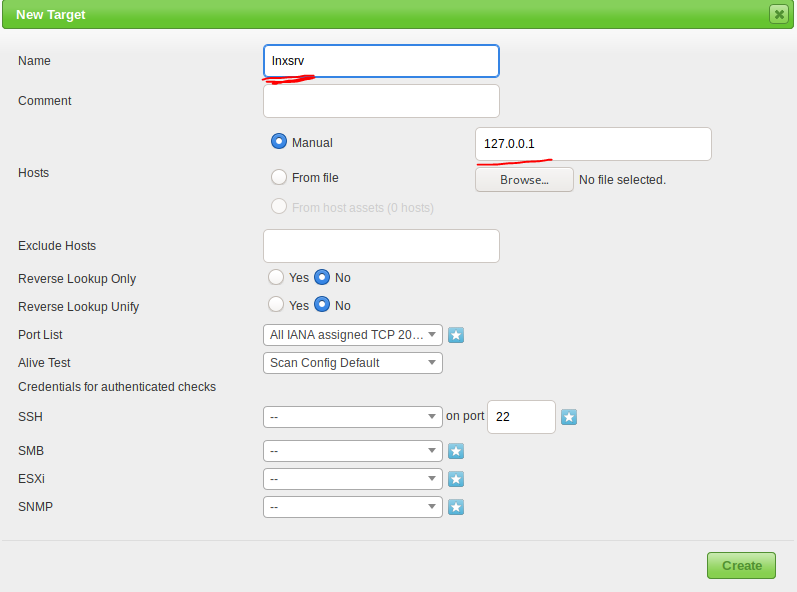
Lisätään kohde jota halutaan skannata. Configuration > Targets

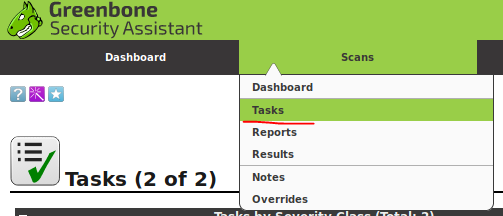


Tähti painikkeesta voit luoda uuden kohteen.

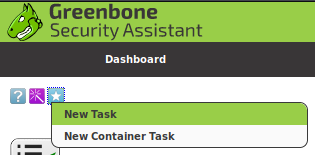


Anna kohteelle nimi joka kuvaa sitä, sekä kohteen IP-osoite. Kohde voisi olla esim. skannatun linux palvelimen IP-osoite.

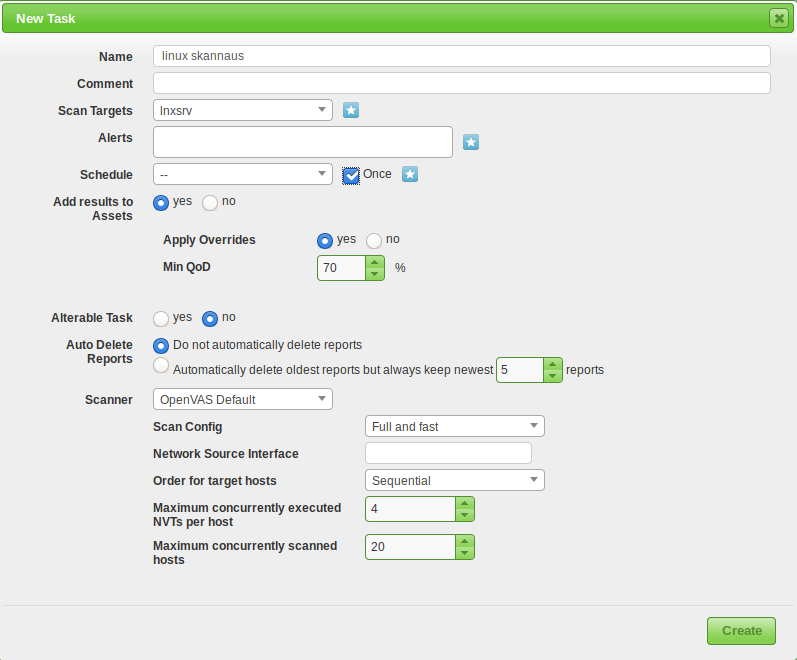


Kohteen lisäämisen jälkeen lisätään uusi skannaus. Scans > Tasks.

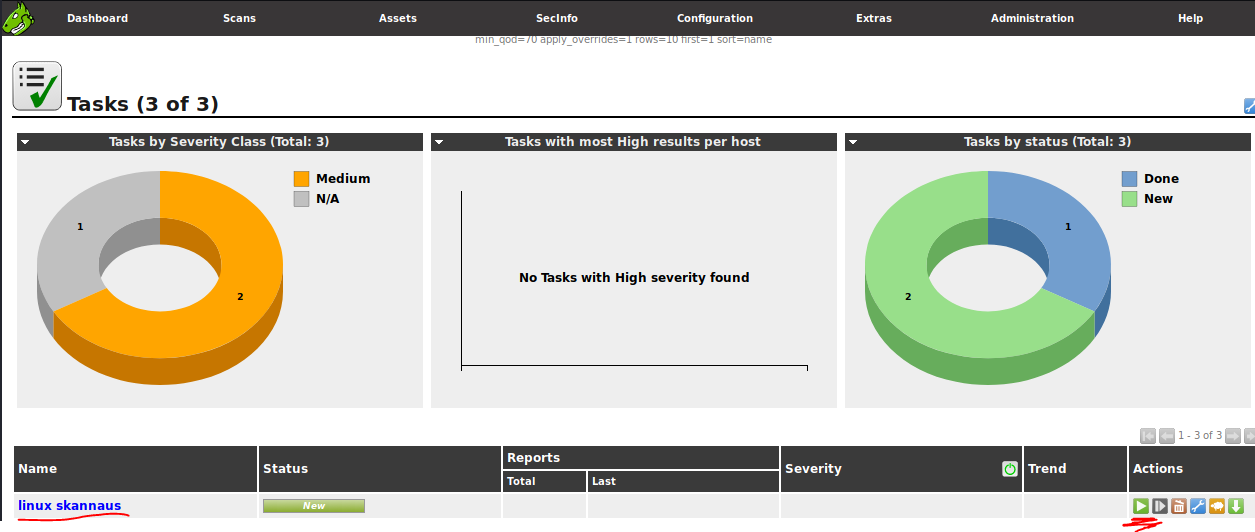
Tähti merkistä voit luoda uuden tehtävän.



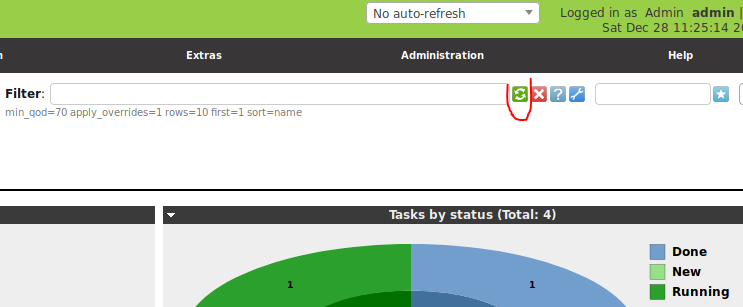
Anna uudelle tehtävälle hyvä nimi, määritä skannattava kohde listalta ja määritä että skannaus suoritetaan vain kerran.

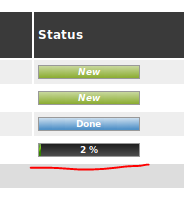
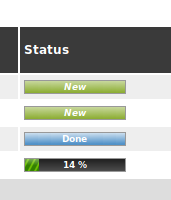


Aloita skannaus Play napista, joka löytyy oikeasta alalaidasta.



Skannaus voi viedä pitkänkin aikaa. Skannaus välilehdeltä löytyy Refresh painike joka päivittää Progress Barin.



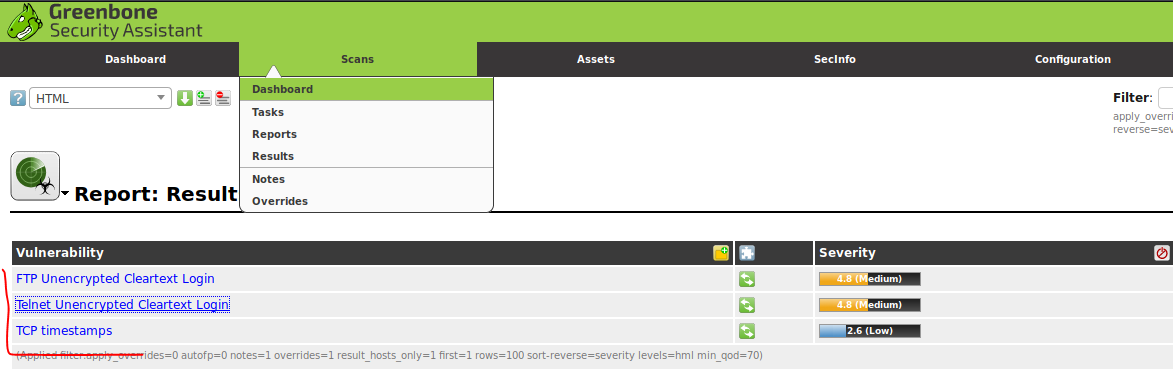
 

Kun skannaus on valmistunut löydät sen tulokset Reports kohdasta. Scans > Reports.

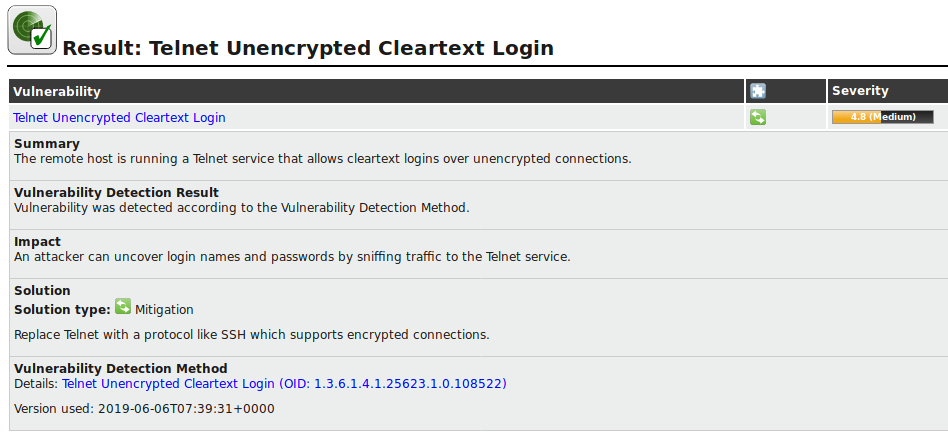
## Raportit



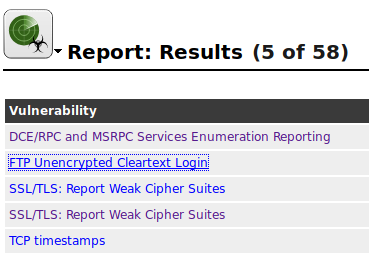
Raportista näet mitä haavoittuvuuksia skannatusta kohteesta löytyi. Linux palvelimelta löytyi, että se käyttää ei-suojattua telnet ja ftp yhteyttä.



Klikkaamalla haavoittuvuutta saat lisää tietoa siitä ja ehdotuksia mitä kannattaa tehdä haavoittuvuuden korjaamiseksi.



Windows palvelimen skannaus tuotti tällaisia tuloksia.

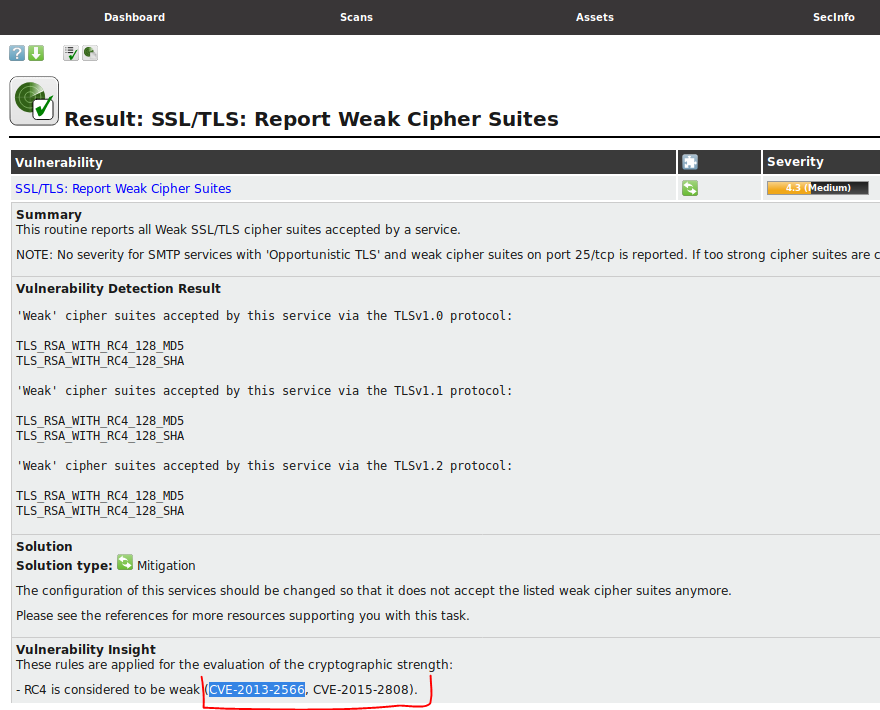


Openvas löysi saman haavoittuvuuden, koska ftp ei ole suojattu.

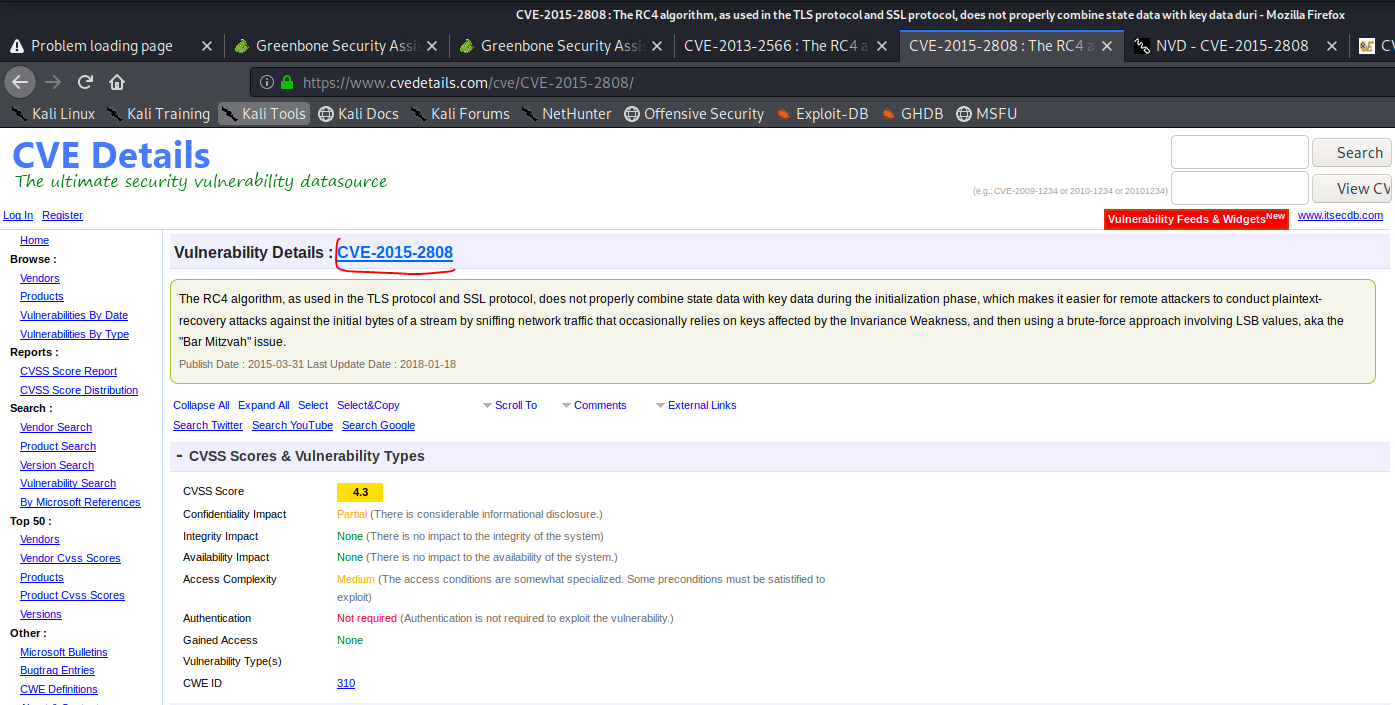
IIS käyttää myös itse luotua https sertifikaattia ja openvas havaitsi tämän (koska sertifikaatti on itse luotu, eli se on tarkoitettu vain testaamista varten, siitä ei siis salata tarpeeksi hyvin).

## Lisäinfoa

Löydetyissä haavoittuvuuksissa on yleensä maininta CVE ja sen perässä numerosarja. CVE on ohjelma jolla ylläpidetään listaa haavoittuvuuksista joita eri palveluista, laitteista ja ohjelmistoista löydetään.



Googlaimella CVE+numerosarja löytyy enemmän tietoa netistä.



## Tulosten vienti

Raportin tulokset saat vietyä helposti esim. html tiedostoksi alla olevan kuvan mukaisesta kohdasta. Valitse missä muodossa haluat tulokset ja paina sitten download painiketta.

