***OpenVas***

*OpenVas* je jedan od široko rasprostranjenih skenera za testiranje ranjivosti distribuiran od strane *Greenbook Networks-a.* Uključuje razne ugrađene web testove i web sučelje. Testiranje je poprilično jednostavno nakon instalacije. *Openvas* je open source rješenje, kada prikaže *false positive* korisnik dodatno može provjeriti koji je stvarni uzorak pogrešno identificirane ranjivosti. Kada se označi opcija za false positive na *OpenVas* listi za slanje e-pošte ne mora se čekati dugo na povratnu informaciju. Tako se *false positive* može ispraviti u roku od nekoliko sati.

Skeniranjem ranjivosti omogućeno je praćenje mreže, sustava i aplikacija u potrazi za sigurnosnim ranjivostima. Skeneri poput OpenVas-a identificiraju i klasificiraju potencijalne točke slabosti u vašoj infrastrukturi, kvantificiraju mogući rizik i preporučuju mjere za rješavanjem istih. Cilj je spriječiti i minimizirati napade ciljanjem identificiranih eksploatacija prisutnih unutar mreže. OpenVas to postiže detaljnim pregledavanjem vatrozida, aplikacija i usluga kako bi se dobio neovlašteni pristup organizacijskim mrežama i imovini. Te se potencijalne slabosti zatim uspoređuju s poznatim ranjivostima iz baze podataka kako bi se brzo ispravile ako postoje.

Podržava autentificirano i neautentificarno skeniranje. Neautentificirano skeniranje pomaže pokazati slabosti u perimetru, primjerice pogrešna kongifuracija vatrozida ili izloženih web poslužitelja u DMZ-u. Autentificirano skeniranje s druge strane omogućuje izravan pristup mreži korištenjem protokola kao što su protocol udaljene površine(RDP) i SSH. Izravnim pristupom je skenerima omogućeno bolje otkirvanje prijetnji I bliža simulacija aktivnosti korisnika.

OpenVas skener koristi ažurirane izvorem feedovi mogu uključivati GSF(Greenbone Security Feed) ili besplatni Greenbone Community Feed(GCF). GSF je plaćena usluga koja koristi ažuriranja stručnjaka iz cijelog svijeta. Ažuriranja se isporučuju automatski putem *GSM(Greenbone Security Manager-a) i Greenbone Cloud Service(GCS).* Navedene feedove skener koristi za provjeru svih uređaja u mreži radi poznatih I potencijalnih sigurnosnih problema. Podržava oko 26,000 ranjivosti(*CVE).* Koristi wizarda koji pomaže postaviti skeniranja za ciljana računala. Kako bi se izvršilo skeniranje mora se postaviti ciljana adresa internetskog protokola(IP). Nakon unosa IP adrese započinje skeniranje i rezultati su prikazani na dnu stranice. Skeniranjem će također pokazati sažete podatke o trenutnom napretku i svim rezultatima skeniranja. Tijekom skeniranja na statusnoj traci će naveden ranjivosti biti prikazane, klikom na navedenu ranjivost može se dobiti detaljniji prikaz o njoj i kako ju ispraviti.

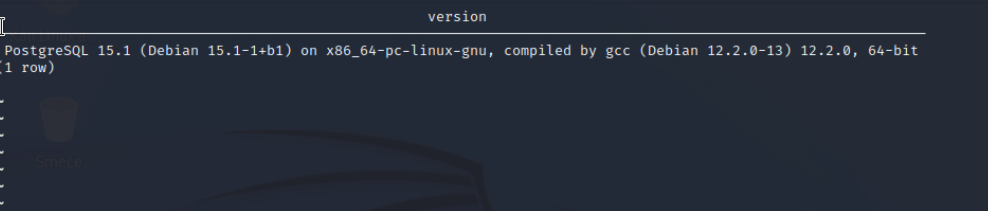
OpenVas također uključuje napredne*wizarde* za zadatke koji uključuju:

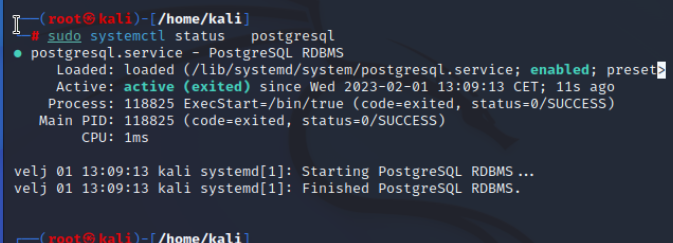
1. Imenovanje zadataka
2. Skeniranja
3. Ciljane IP adrese
4. Zakazivanje skeniranja
5. Ovlaštena skeniranja (s vjerodajnicama)

OpenVas pruža standardna zadana testiranja, omogućuje stvaranje korisničkih skeniranja i  stvaranje prilagođenih konfiguracija.

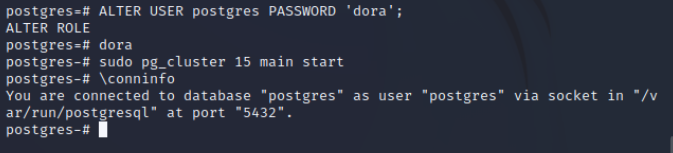
Instalacija ***OpenVas-a***:

Prvi korak je instalacija **Postgresql-a:**





Provjera konekcije sa serverom :

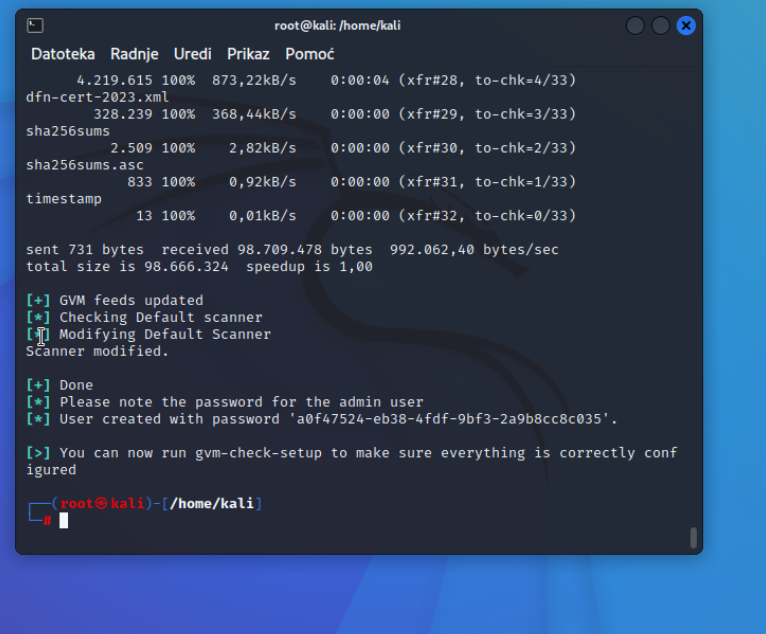


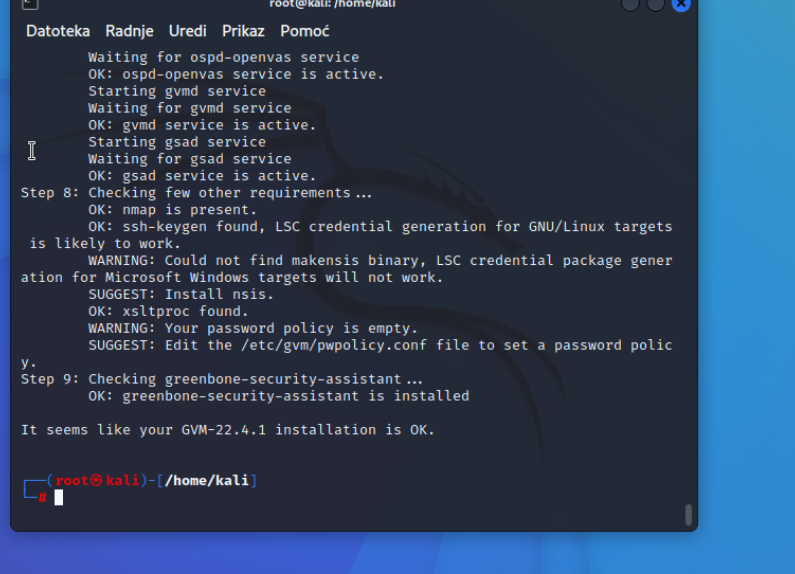
Provjera postojeće baze:

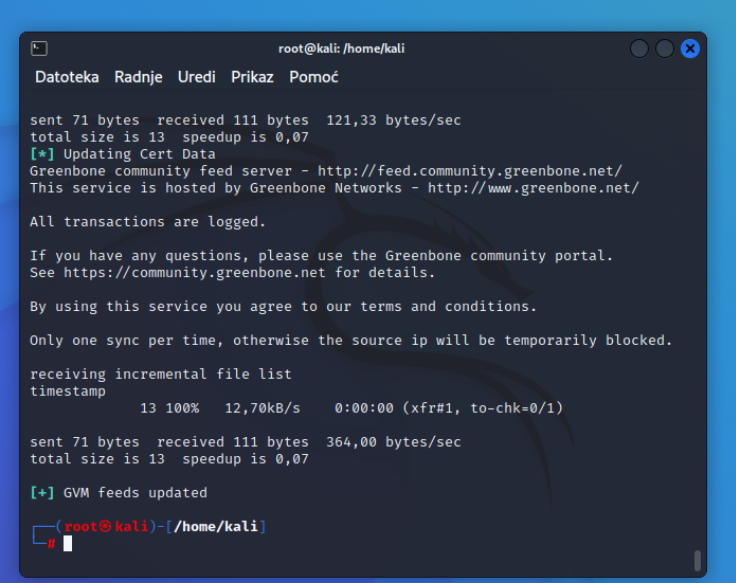
Graphical user interface

Description automatically generated

Nakon instalacije*Postgresqla* i navedenih provjera, može se započeti sa instalacijom *OpenVas-a(GVM-a):*







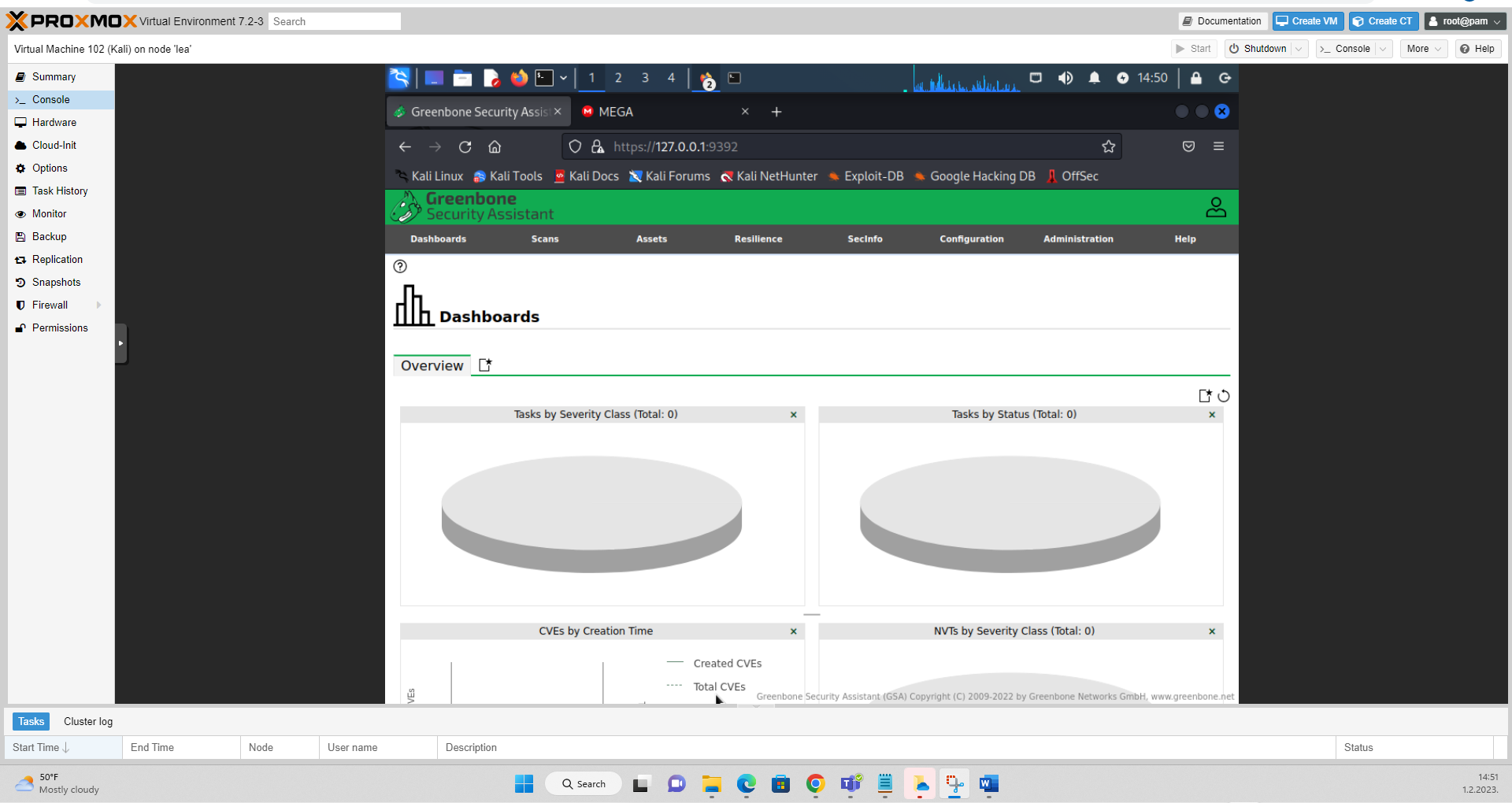
Text

Description automatically generated

Nakon uspješne instalacije prikaže se navedeno sučelje:

Graphical user interface, application, website

Description automatically generated



Skeniranje meta redom:  
1. <https://fieldservice-api-stage.apps.thingstalk.eu/api/tms/resources/event-log/123/images?tbsession=123>

2. <https://brodplin-poc.apps.thingstalk.eu/>

3. <https://fieldservice-api.apps.thingstalk.eu/>

4. <https://cp521-frontend-cp521.apps.ocp4.heptk.hr/>

  5. . <https://hposta.apps.thingstalk.eu/>