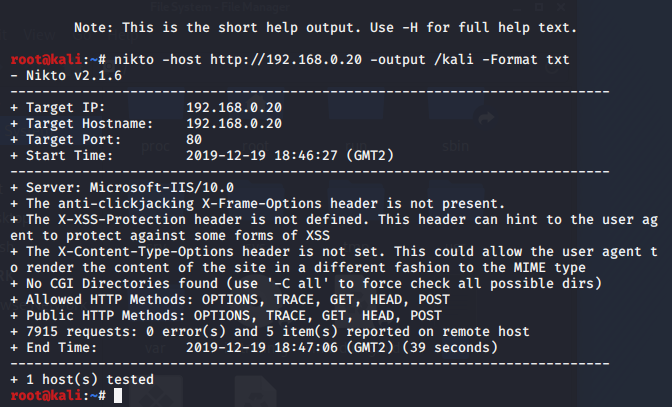
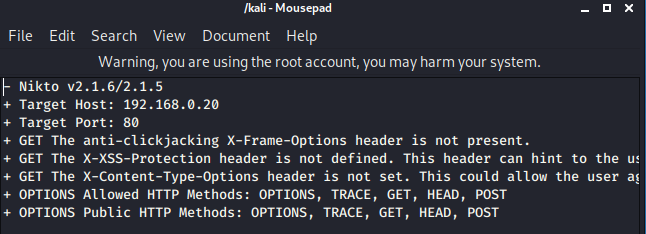
# Nikto

Nikto on ohjelma, jolla voi skannata webbi palvelimen heikkouksia.

Tässä skannataan kohteessa 192.168.0.20 olevaan www-palvelinta. Sivustoa ei ole salattu. Tulokset tulostuvat aina komentoriville, mutta -output ja -Format parametreilla voimme tallentaa tiedot tiedostoon halutussa muodossa. Tässä tiedot tallenetaan kali nimiseen tiedostoon jonka pääte on txt.

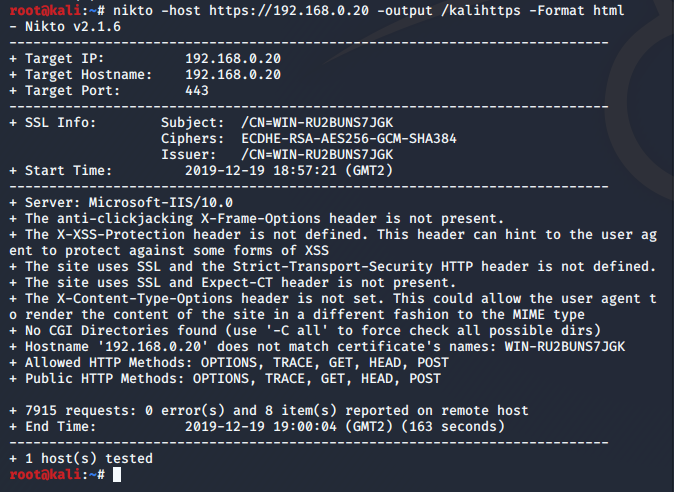


Nähdään mm. että sivusto on toteutettu IIS 10.0 versiolla.



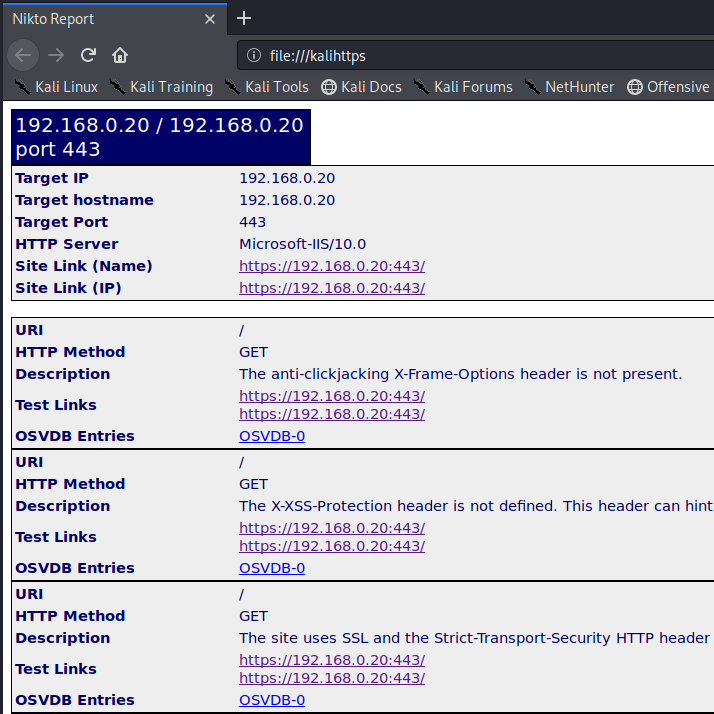
Tässä skannataa sama kohde, mutta sen salattu versio ja tiedot tallennetaan hiukan eri muodossa.

Tulos on hiukan eri. Näet esimerkiksi että sivustossa käytetään itse tehtyä sertifikaattia ja että se käyttää porttia 443.

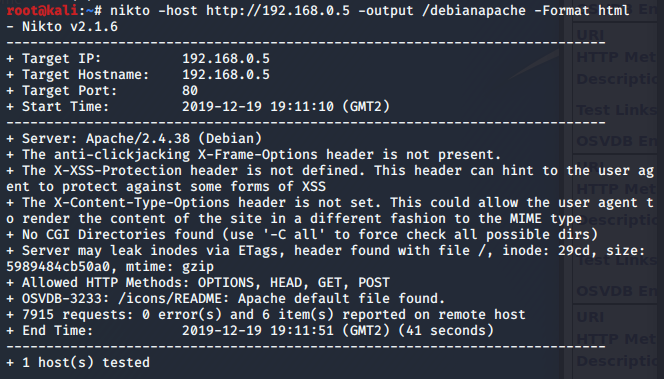


Tällä kertaa tiedot tallennettiin html tiedostoon josta tulokset näkee hiukan käyttäjäystävällisemmin.

Palvelimelta löytyy haavoittuvuuksia mm. x-xss protection ja x-frame-options liittyen. Näitä googlaimella löytäisi niistä lisää tietoa ja miten hyökkäyksiltä voi suojautua.



Seuraavaksi skannataan Debian koneessa sijaitseva apache2 palvelin.

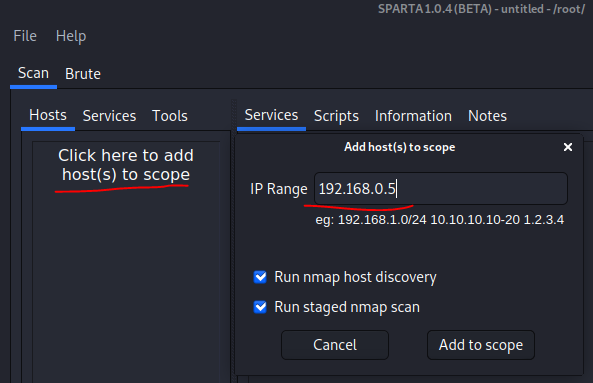


Nikto havaitsee heti alkuun että käytössä on Apache 2.4.38 versio.

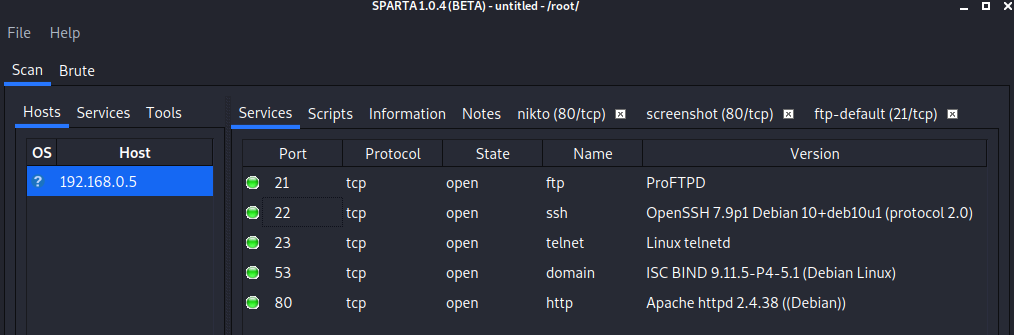
Palvelimesta löytyi haavoittuvuus OSVDB-3233. Googlaimella lisää esim. nikto apache default file found, voisi löytää listää tietoja ja miten suojautua mahdollisilta murtautujilta.

# Sparta

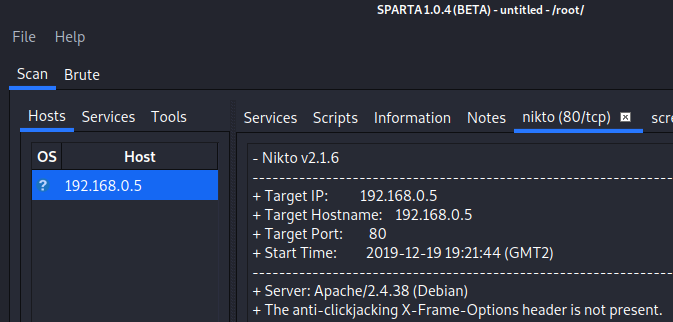
Sparta on työkalu joka yhdistää usean työkalun yhteen graafiseen käyttöliittymään. Lisää skannattava kohde ja paina Add to scope.



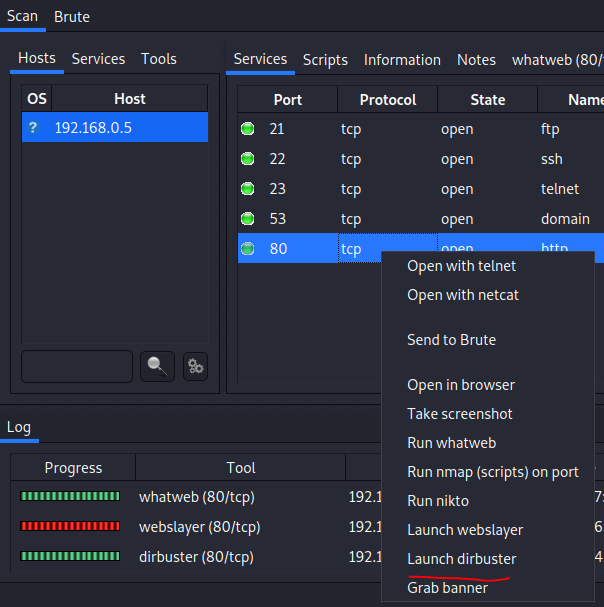
Yleisnäkymä tuloksista. Eli välilehdiltä näet enemmän tietoja.



Nikto välilehdeltä näet samat jutut kuin aikaisemmin käytetyssä nikto skannauksessa.



Päänäkymästä voit myös avata muita sovelluksia kuten dirbuster työkalun.

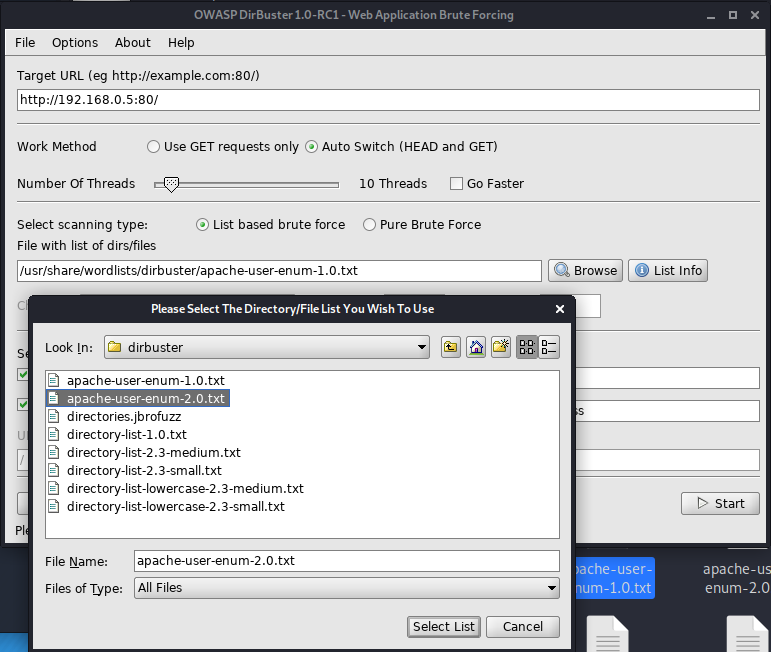


# Dirbuster

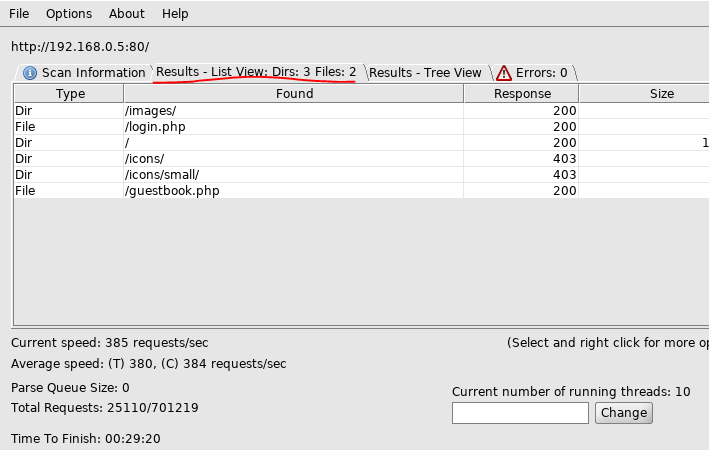
Dirbuster on työkalu jolla löydät mitä kansioita webbisivustolta löytyy. Yleensä nettisivustoilta löytyy kansiot esim. kuvia varten ja eri html tai php tiedostot eri asioita varten.

Valitse sanalista, jota dirbuster käyttää kun se lähettää kyselyitä webbi palvelimille. Sanalistan löytyy kuvassa olevasta polusta /usr/share/wordlists/dirbuster. Voit myös tehdä oman sanalistan.

**Directory-list 2.3.small vaikutti hyvältä listalta.**



Skannauksen aikana voit tarkastella löytyneitä tuloksia.



Kun skannaukset ovat valmiit, voit generoida raportin tuloksista. Tässä tulokset tallennetaan / juurihakemistoon.

