# Metasploit

Kun kohteesta löydetään jokin haavoittuvuus, voidaan sitä yrittää hyödyntää. Tätä varten kalista löytyy metasploit niminen paketti.

Metasploittia on helpointa testata lataamalla Metasploitable niminen virtuaalikone joka on tarkoitettu testausta ja harjoittelua varten, eli se on täynnä erilaisia haavoittuvuuksia. Lataa se osoitteesta: <https://sourceforge.net/projects/metasploitable/>

*Metaploitable koneesta löytyy tekemistä vaikka vuoden päiviksi jos haluaa tutustua kaikkeen mitä sillä voi harjoitella. Halutessaan se kannattaa asentaa omalle kotikoneella virtuaaliympäristöön kalin kanssa!*

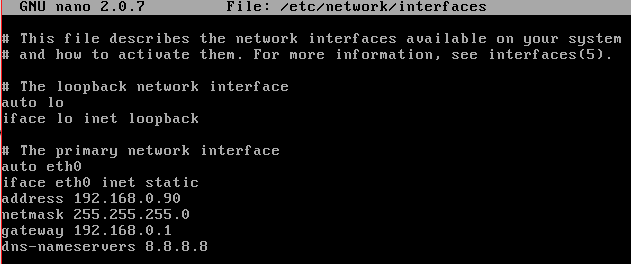
Aluksi pura ladattu pakattu kansio.

Luo virtualboxiin uusi virtuaalikone ja käytä sen virtuaalikiintolevynä lataamaasi metaploitable levyä.

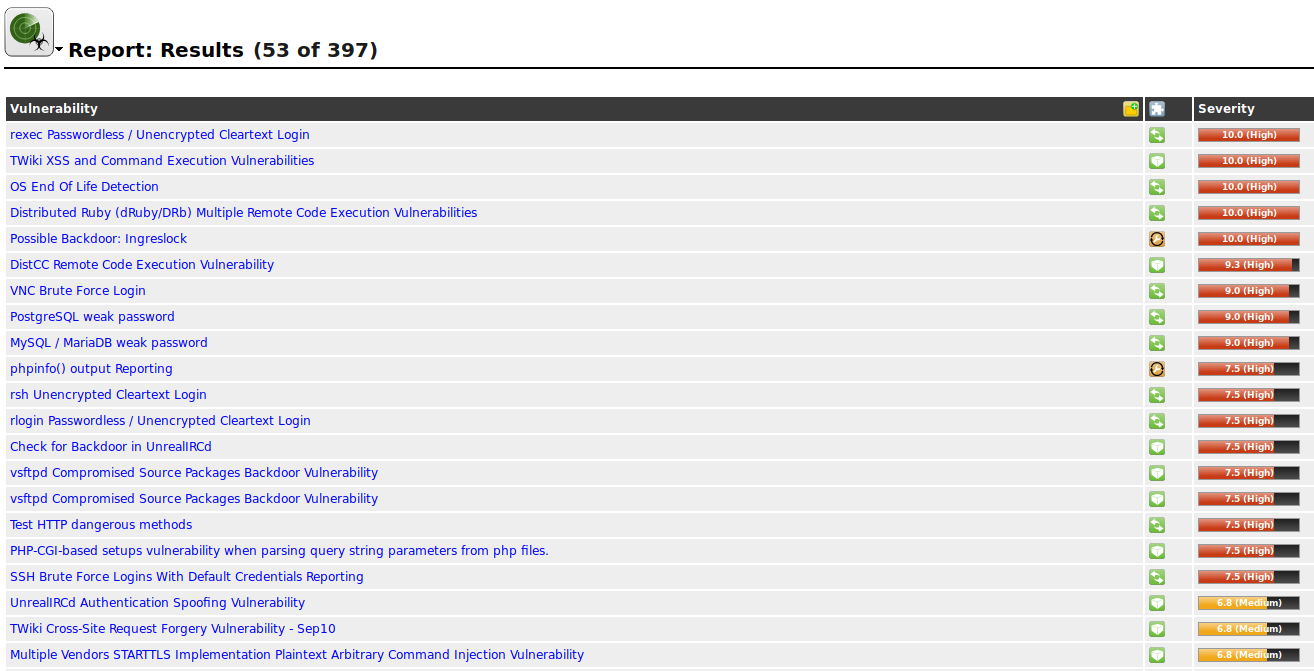
**Metasploitin käyttö Hyper-V:llä on hankalampaa sillä ladattu virtuaalikiintolevy tulisi muuttaa .vhd tai .vhdx muotoon joka ei aina toimi niin kuin pitäisi.**

Metasploitable koneen käyttäjätunnus ja salasana on: **msfadmin**

Metasploitable on ubuntu eli perustuu debianiin. Vaihda sille kiinteä IP-osoite, käynnistä kone uudestaan jotta asetukset tulevat voimaan. Tässä laitetaan koneelle seuraavat IP-asetukset.

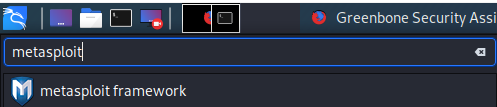


Kun metasploitable kone toimii sen haavoittuvuudet voi skannata openvas ohjelmalla. Kuten näkyy siitä löytyy iso kasa haavoittuvuuksia.

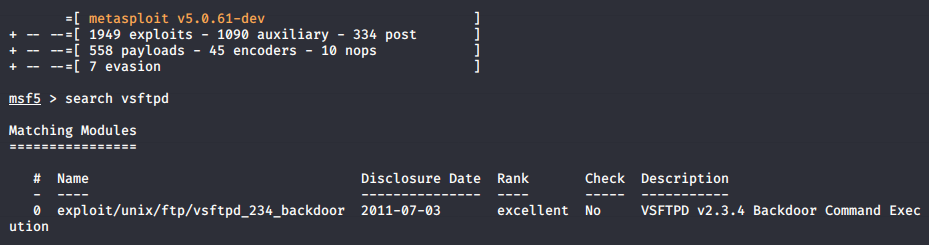


Metasploitable koneesta löydettiin mm vsftpd backdoor, käytetään sitä.

Avaa metasploit ohjelma



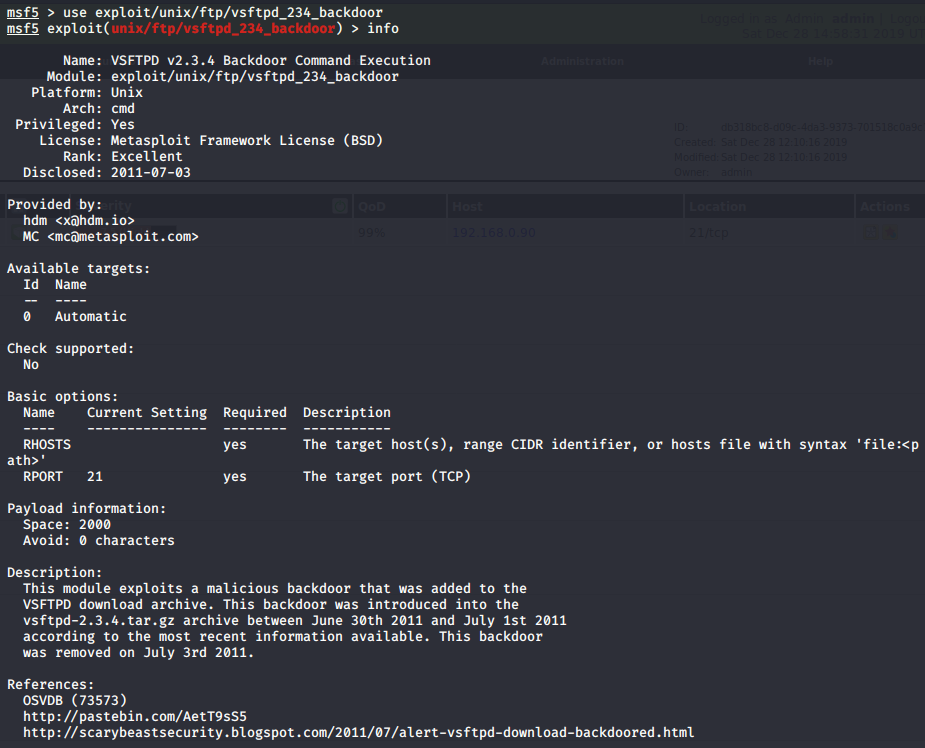
Etsi löytyykö vsftpd ohjelmaan exploitteja.



Metasploit löysi exploitin joka mahdollistaisi backdoorin vsftpdn kautta linux palvelimelle.

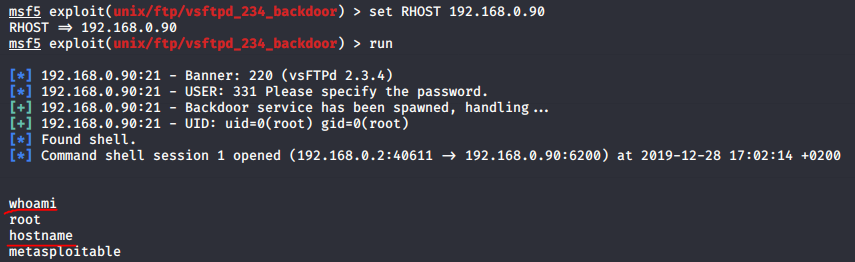
Käytä kyseistä exploittia use komennolla.

Info komennolla saat lisää tietoa exploitista.



RPORT on jo valmiiksi 21, eli exploitti käyttää sitä porttina. Sillä ei kuitenkaan ole vielä RHOST eli kohdetta. Set Rhost komennolla asetetaan kohteeksi linux palvelimen IP-osoite.

Hetken odottelun jälkeen pääset sisälle ja vähän erilainen terminaali aukeaa. Tässä whoami komennolla testataan kenellä ollaan kirjautuneena sisään ja hostname komennolla mikä on koneen nimi.



Kun olet koneella kirjautuneena root käyttäjälle olet periaatteessa murtautunat siihen ja voit tehdä sillä mitä tahansa.