# Testaaminen

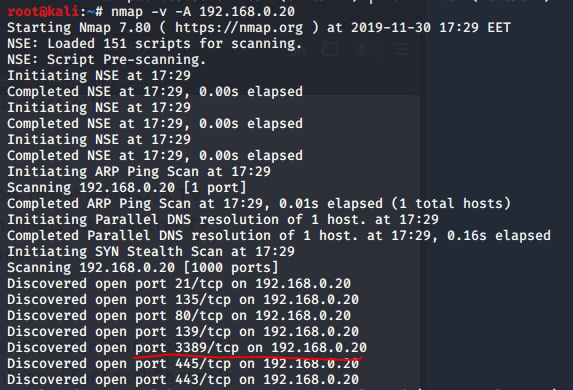
## Windows Remote Desktop

Palvelimella tulee olla päällä RDP etäyhteys. Tässä yritetään murtautua Administrator käyttäjälle käyttämällä Hydra nimisen paketin sanalistahyökkäystä eli Brute Forcea.

Voit käyttää jotakin netistä ladattavaa sanalistaa, luoda oman sanalistan tai käyttää Kalissa mukana tulevaa rockyou sanalistaa. Kalin oma sanalista löytyy polusta /usr/share/wordlists/rockyou.txt.gz. Pura se komennolla gunzip.

Voit varmistaa, että palvelimen Remote Desktop portti on päällä käyttämällä Kalin nmap pakettia.

**nmap -v -A palvelimenIP-osoite**



Jos portti on päällä voidaan aloittaa Brute Force Hydra paketilla.

**hydra -t 1 -V -f -l Administrator -P /usr/share/wordlists/rockyou.txt rdp://192.168.0.20**

-t voit määrittää useamman ytimen suorittamaan brute forcea.

-V antaa terminaalin palautetta miten homma etenee

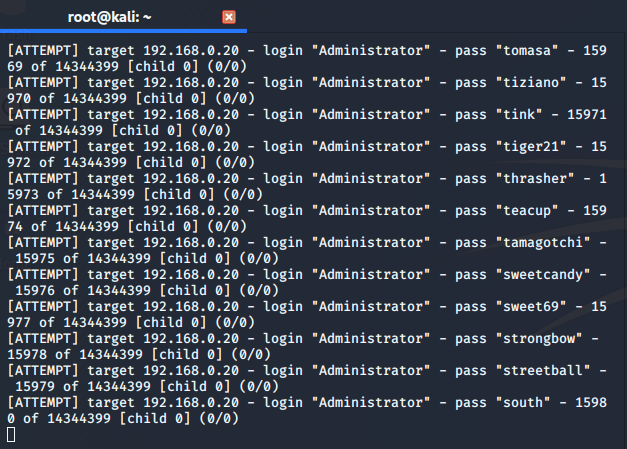
-f lopettaa Brute Forcen jos oikea salasana löydetään

-l käyttäjän nimi jonka salasana halutaan murtaa

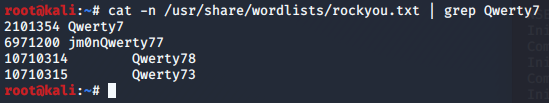
-P sanalista jota käytetään

rdp://192.168.0.20 hyökättävän kohteen IP-osoite

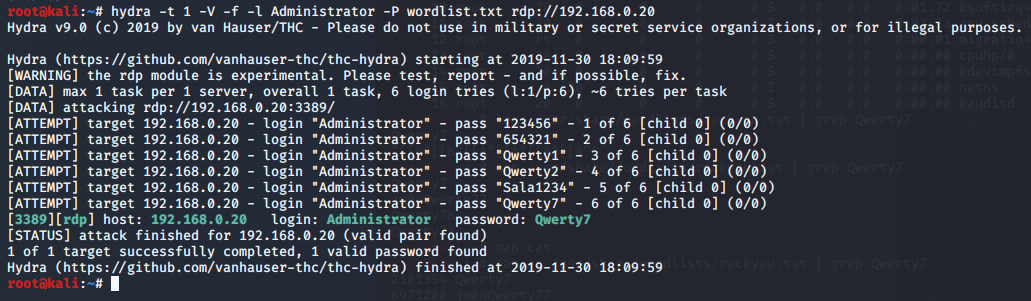
Hydran toiminta näyttäisi tältä. Kuten kuvastakin näkyy, näet mitä salasanaa Hydra on kullakin kerralla kokeillut ja nyt on menossa jo yritys 15979 / 14344399. Eli testattavia salasanoja on valtava määrä. Tämän takia tilien lukitseminen väärien yritysten jälkeen on tehokasta.



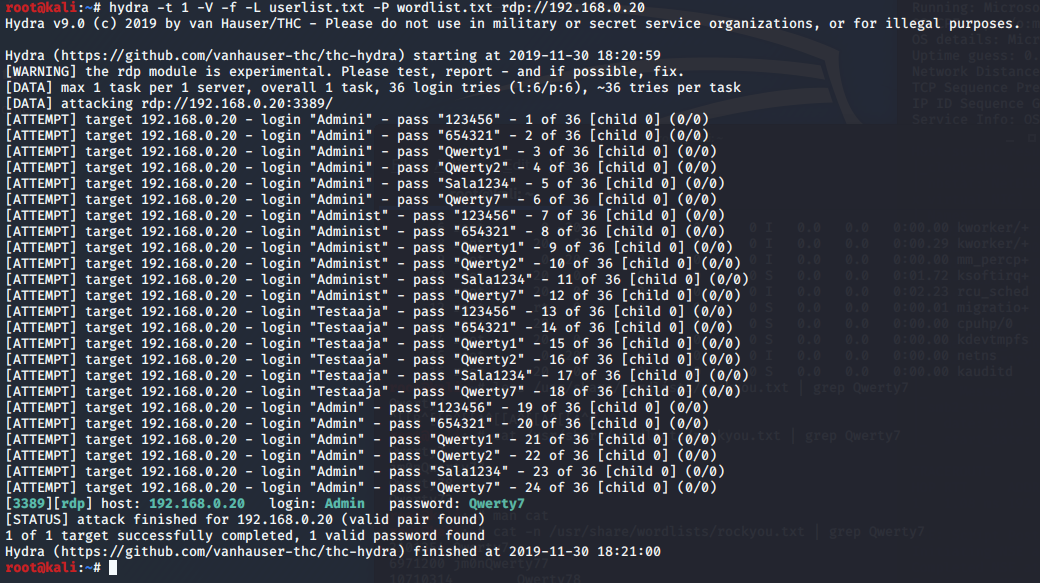
Tästä sanalistasta oikea salasana Qwerty7 löytyisi lopulta, mutta demoamisen vuoksi käytän seuraavassa kohdassa itse tehtyä sanalistaa, joka demoaa oikean salasanan löytymistä.



Tässä salasana saatiin selville omalla wordlist.txt nimisellä sanalistalla.

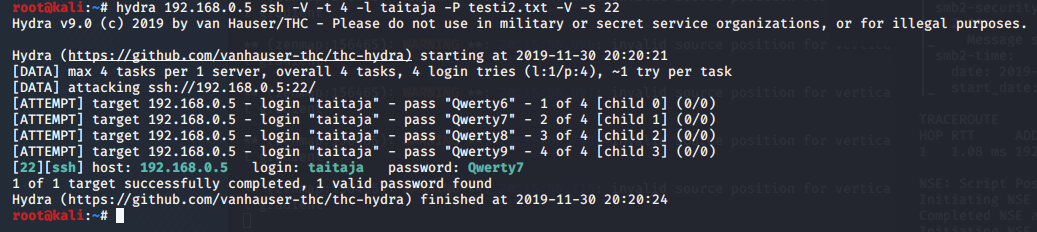


Jos et tiedä käyttäjänimeä voit käyttää myös käyttäjänimi listaa Hydran -L valitsimella. Näin tehtäessä Hydra kokeilee kaikki salasanat kaikille eri käyttäjille.



## Linux SSH

Tässä Brute Forcetaan linux palvelimella sijaitsevan openssh-serverin käyttäjätunnuksen salasana.



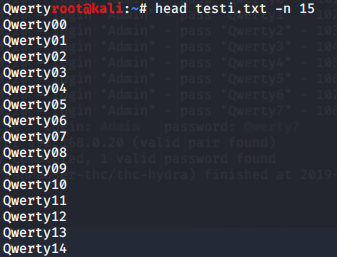
## Muut

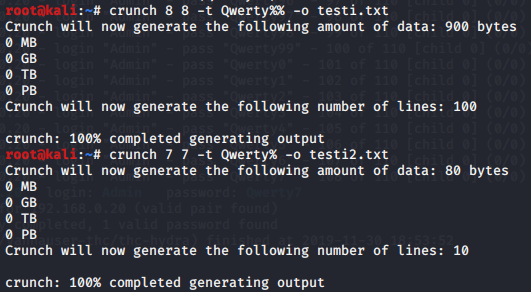
Samoilla metodeilla voisit myös murtautua FTP/http tai Telnet kohteisiin. Vaihtaisit vain kohdetta hydran komennossa.

# Crunch

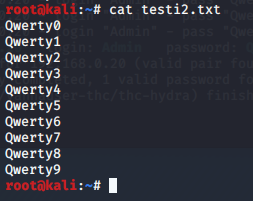
Crunch on työkalu, jolla voit tehdä omia sanalistoja. Tässä muutama esimerkki.

Ensimmäisessä kohdassa tehdään sanoja joiden pituus on 8 merkkiä. Ne alkavat merkeillä Qwerty jonka jälkeen tulee kaksi numeroa. Lista luodaan tiedoston testi.txt. Listassa olisi tälläisia sanoja:

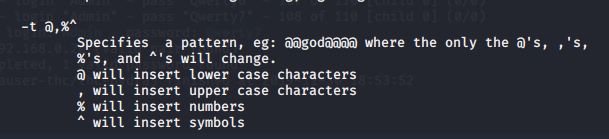




Toisessa kohdassa tehdään sanoja joiden pituus on 7 merkkiä. Ne alkavat merkeillä Qwerty jonka jälkeen tulee yksi numero. Lista luodaan tiedoston testi2.txt. Listassa olisi tälläisia sanoja:



Alla olevassa kuvassa näkyy esimerkkejä, miten -t valitsinta voisi käyttää.



Näitä sanalistoja voisi sitten käytä Brute Force hyökkäyksissä.

# Suojautuminen

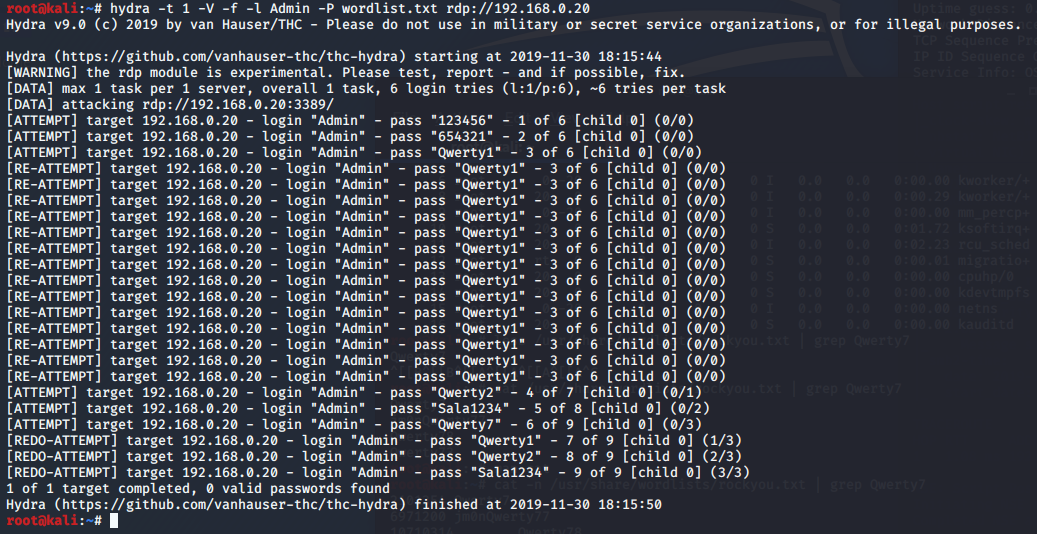
Tällaiselta Brute Force hyökkäykseltä voi suojautua mm. asettamalla käyttäjätilit menemään lukkoon jos tietyn ajan aikana tapahtuu liian monta epäonnistunutta kirjautumista. Tämän saa tehtyä esim. ryhmäkäytäntöjen avulla toimialueen käyttäjille.

## Windows

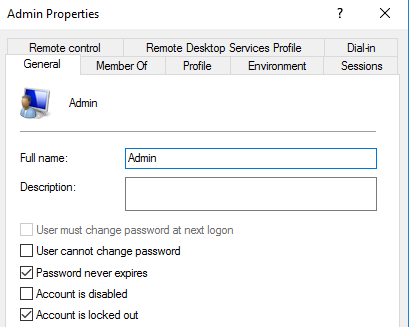
Etätyöpöytäyhteyden käyttöä voi rajoittaa vain sitä tarvitseville henkilöille, esim. tietohallinnolle.

On mahdollista myös käyttää RDP Gatewayta, jolloin RDP etäyhteydet menevät ikään kuin RDP palvelun kautta ennen kuin saapuvat kohteeseen.

Tässä on tehty salasanasääntö, joka määrittää, että kahden epäonnistuneen yrityksen jälkeen tili lukitaan. Hydran Brute Force ei siis onnistunut.



Tili on lukittu.

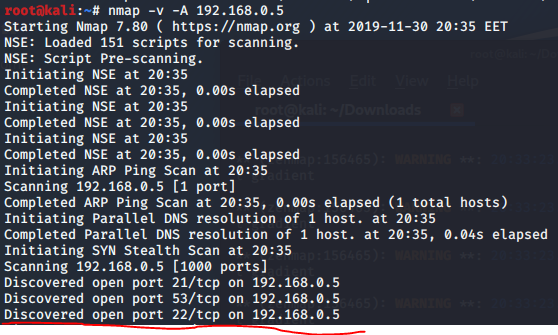


## Linux

Linuxissa Brute Forcet saa estettyä fail2ban paketilla. Paketti toimii heti asennuksen jälkeen (apt install fail2ban). Oletuksena se bännää hyökkääjän IP-osoitteen 10 minuutiksi jos siitä tulee 5 väärää kirjautumisyritystä.

Voit varmistaa, että palvelimen SSH portti on päällä käyttämällä Kalin nmap pakettia.

**nmap -v -A palvelimenIP-osoite**



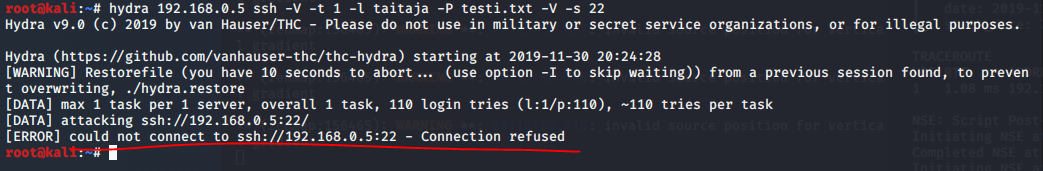
Fail2ban asennettu, ei vielä bänneja.



Tässä kuva kun bännit tulivat:



Jos bännien aikaan yrittäisi Brute Forcea, se ei onnistuisi koska palvelin hylkää kaikki ssh yhteydet kyseisestä IP-osoitteesta.



Bännätyn IPn voi unbännätä alla olevalla tavalla.

