Fail2ban

Fail2ban adalah sebuah aplikasi untuk melindungi akses server dari serangan brute force pada user maupun root password. Fail2ban akan melakukan ban ip yang gagal melakukan login sebanyak yang telah diatur. Defaultnya, fail2ban akan memblokir ip yang gagal melakukan login sebanyak 5 kali dengan waktu 60 menit.

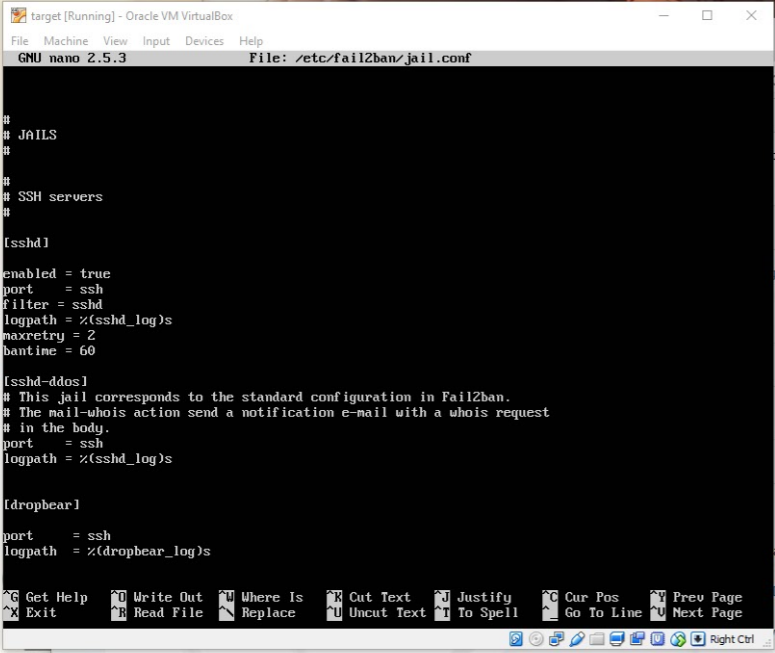
Konfigurasi Fail2ban

Pertama kita install fail2ban terlebih dahulu

apt-get install fail2ban

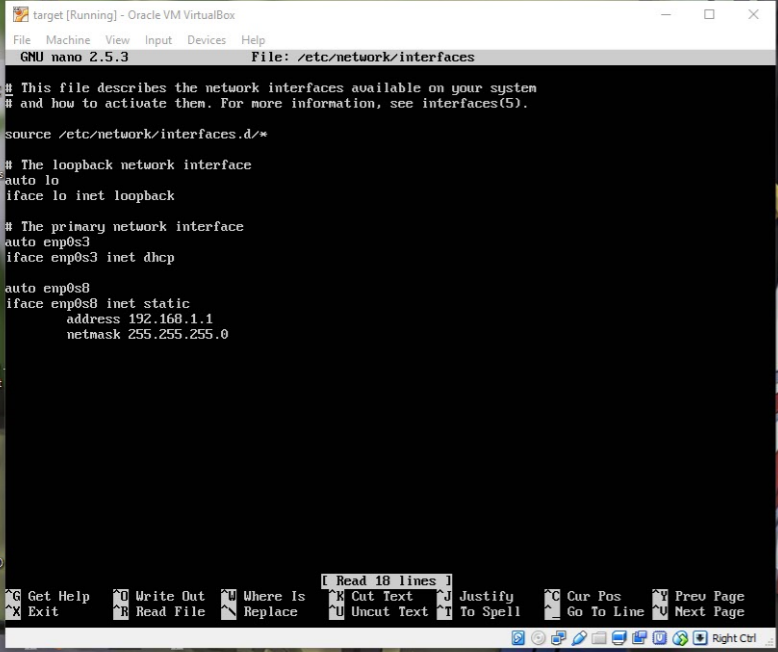
lalu edit file /etc/fail2ban/jail.conf

Pada konfigurasi fail2ban, kita mengubah setingan pada **max retry** / maksimal gagal login dari 5 menjadi 2, dan **bantime** dari 60 menit menjadi 1 menit.

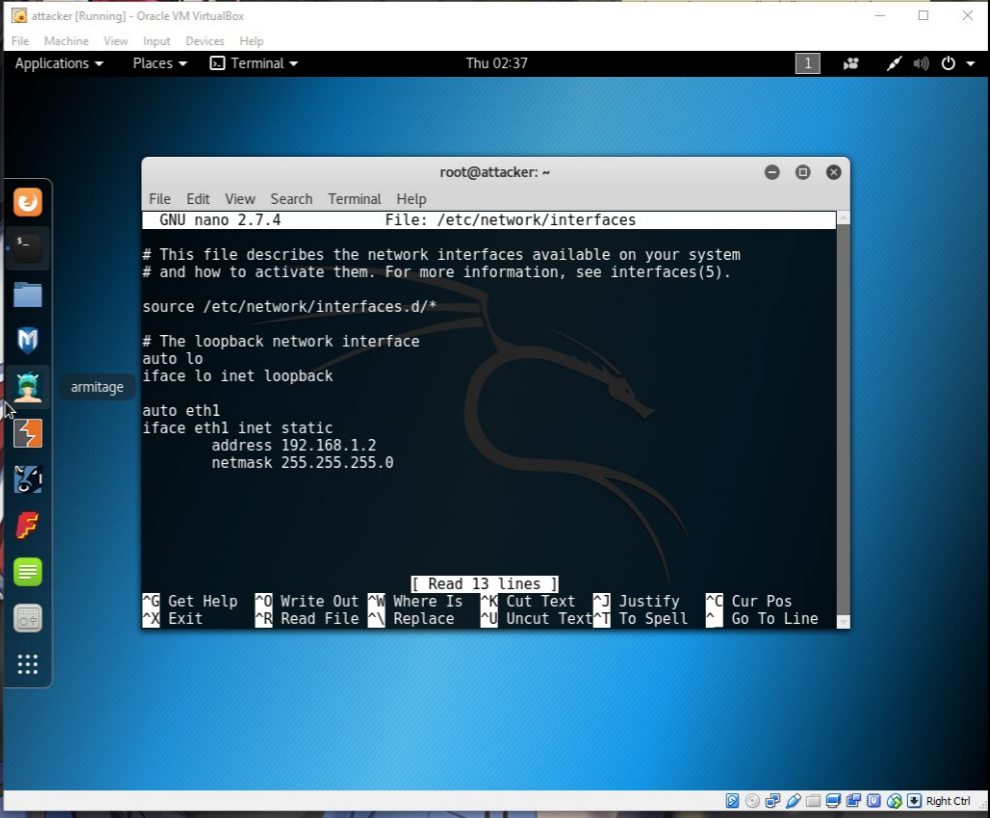


Setting pada maxretry dan bantime (windows sebelah kiri)

Setelah itu atur ip dari masing – masing virtual machine pada file /etc/network/interfaces



Setting IP pada ubuntu server

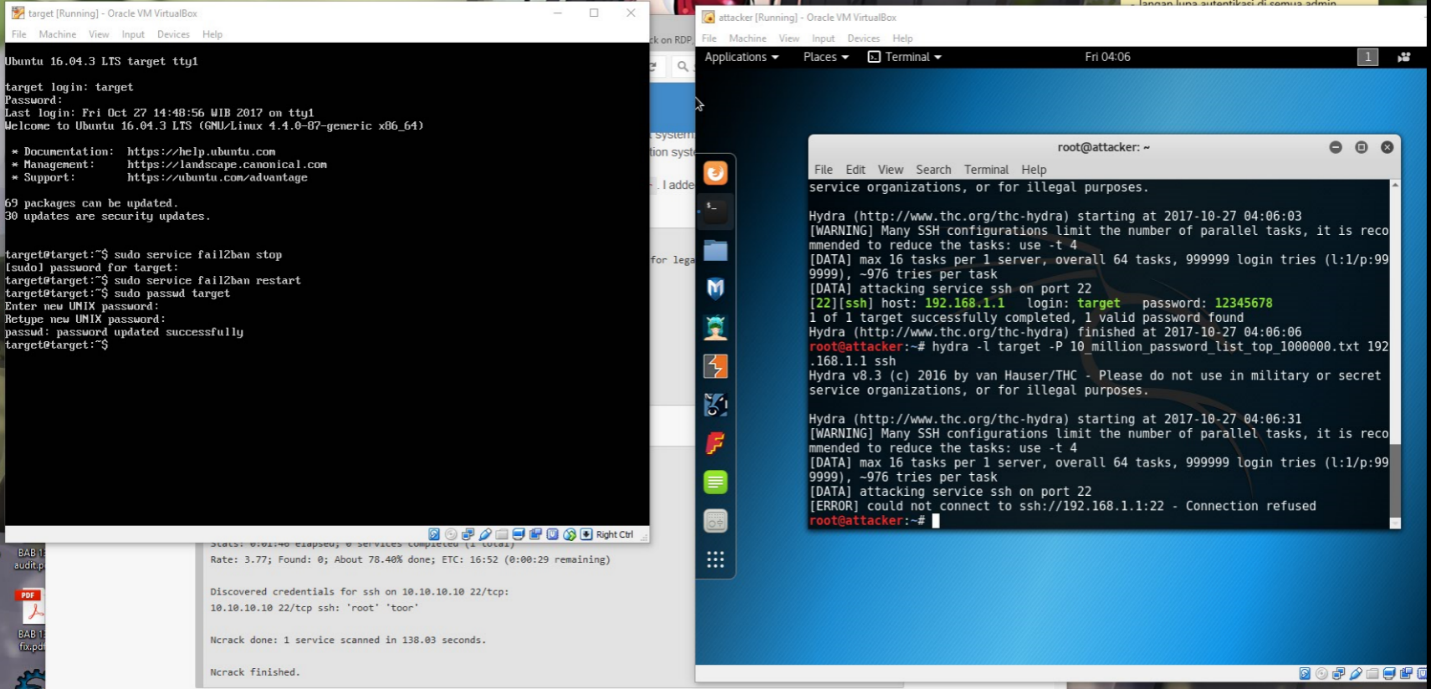


Setting ip pada kali linux

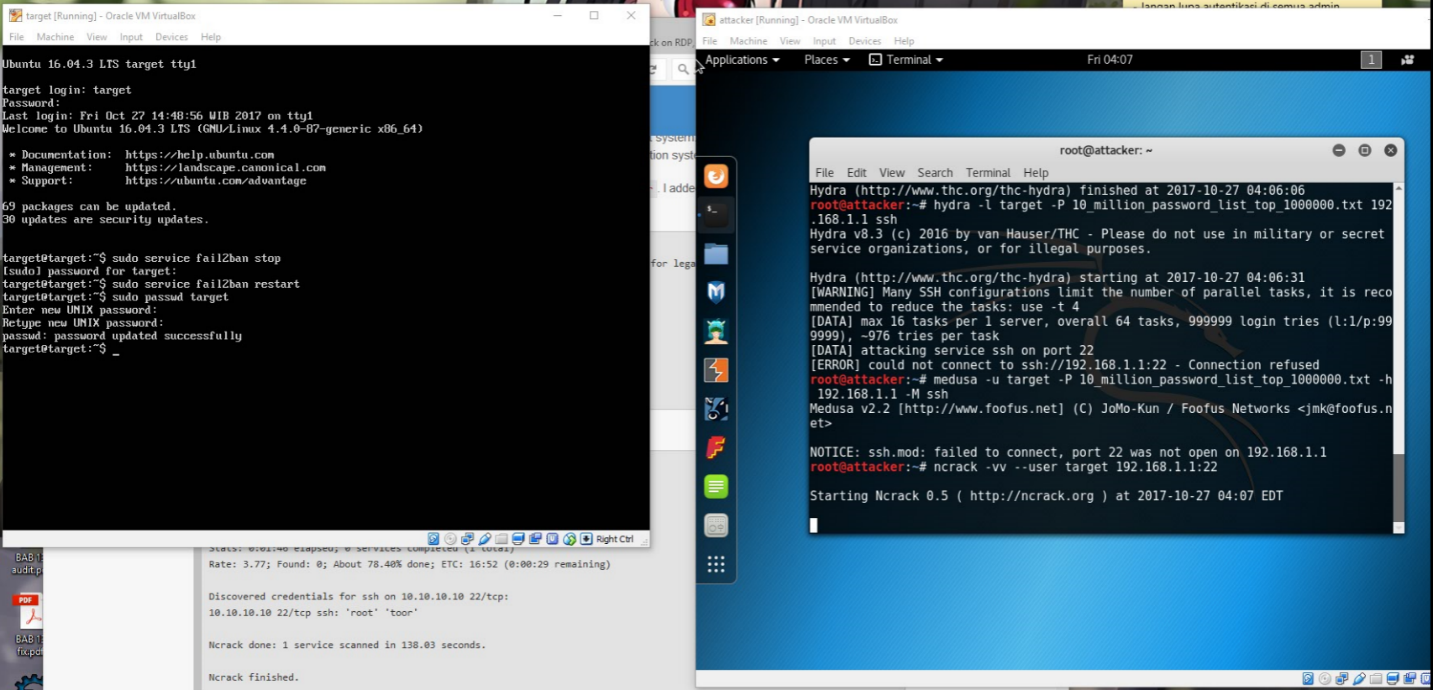
Jangan lupa lakukan restart

Service networking restart

Setelah disetting, ubuntu server siap untuk diserang. tools sama menggunakan nCrac, Medusa dan Hydra.



Penyerangan hydra dengan fail2ban terinstall



Penyerangan medusan dan ncrack dengan fail2ban terinstall

Bisa dilihat VM penyerang gagal mendapatkan password karena ip nya telah diblokir terlebih dahulu.

Kesimpulan

Serangan brute force walaupun membutuhkan waktu yang lama, password yang rumit sekalipun pasti akan didapatkan. Namun dengan menggunakan fail2ban, percobaan brute force akan gagal karena adanya pembatasan percobaan oleh fail2ban. Dengan fail2ban serangan brute force dapat terpenuhi.