Network Laboratory
Electrical Engineering Department, 2nd floor
Universitas Indonesia
Depok, 16424

Nama : Muhammad Irsyad Thoyib
NPM : 1606905891

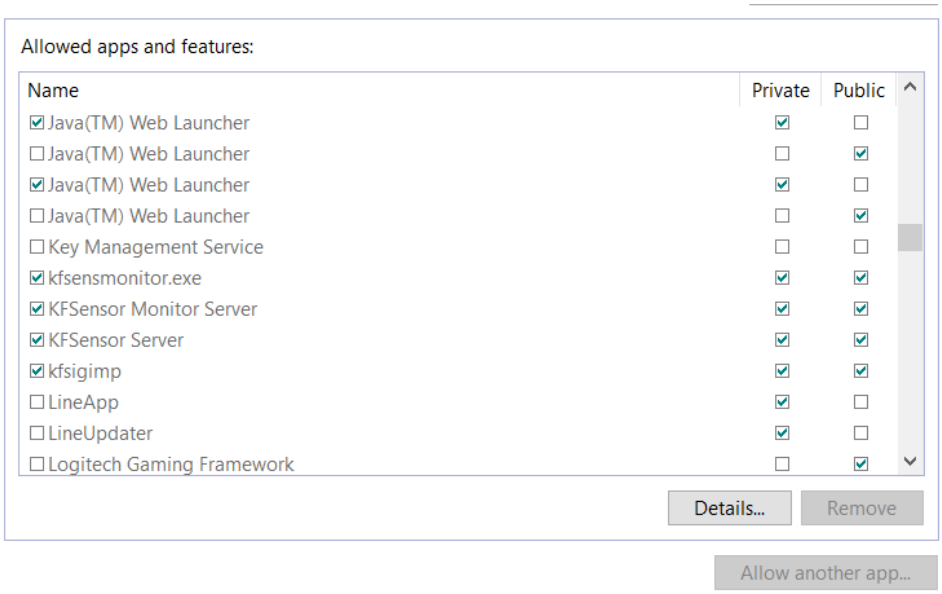
PRAKTIKUM KEAMANAN JARINGAN
Modul ke-6
AT

1. Perbedaan HoneyDrive dan KFSensor
    a. HoneyDrive

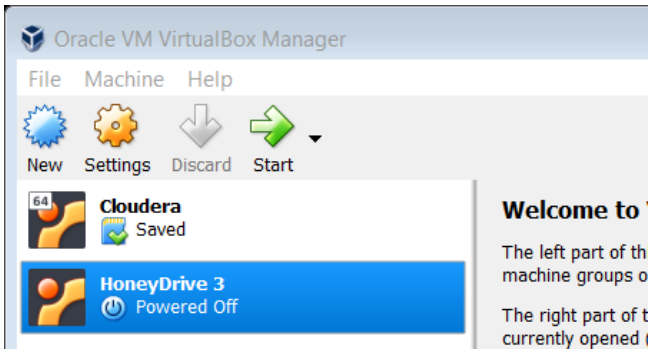
       HoneyDrive merupakan distro linux pertama yang dibuat untuk honeypot. Ia berbasis Xubuntu Desktop seri 12.04 LTS. HoneyDrive juga memiliki 10 aplikasi yang telah diinstal dan dikonfigurasi sebelumnya oleh pembuat distro. HoneyDrive dibuat untuk mempermudah implementasi dari honeypot yang dapat digunakan untuk simulasi atau percobaan.
    b. KFSensor

       KFSensor adalah honeypot yang berbasis Windows. Ia memiliki fungsi untuk menarik dan mendeteksi peretas dan worm dengan membuat suatu sistem yang lemah agar menarik untuk diserang.
    c. HoneyBot

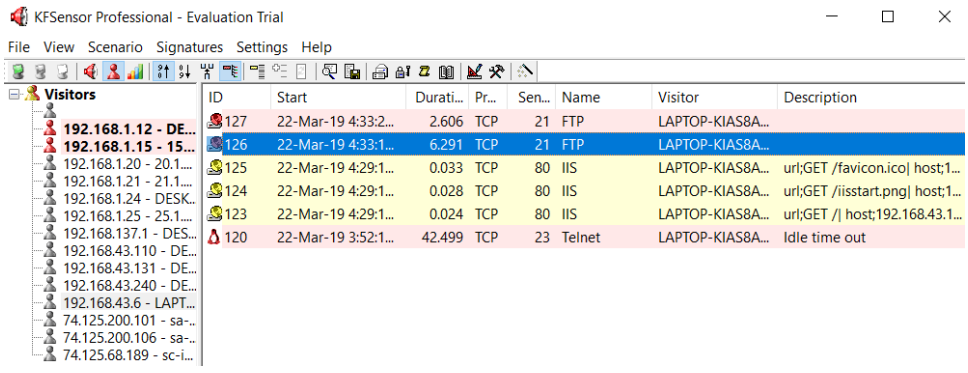
       HoneyBot adalah suatu honeypot yang berbasis Windows. Ia memiliki kemampuan untuk membuat lingkungan yang aman untuk menangkap dan melihat aktivitas pada suatu traffic atau jaringan. HoneyBot akan membaca log yang terjadi pada suatu network sehingga user dapat mengetahui sedang terjadi apa pada network tersebut terutama pada alamat IP miliknya.
2. Cara menggunakan KFSensor
    a. Install KFSensor
    b. Ubah settingan pada firewall



c. Buka HoneyDrive dengan menggunakan virtual machine



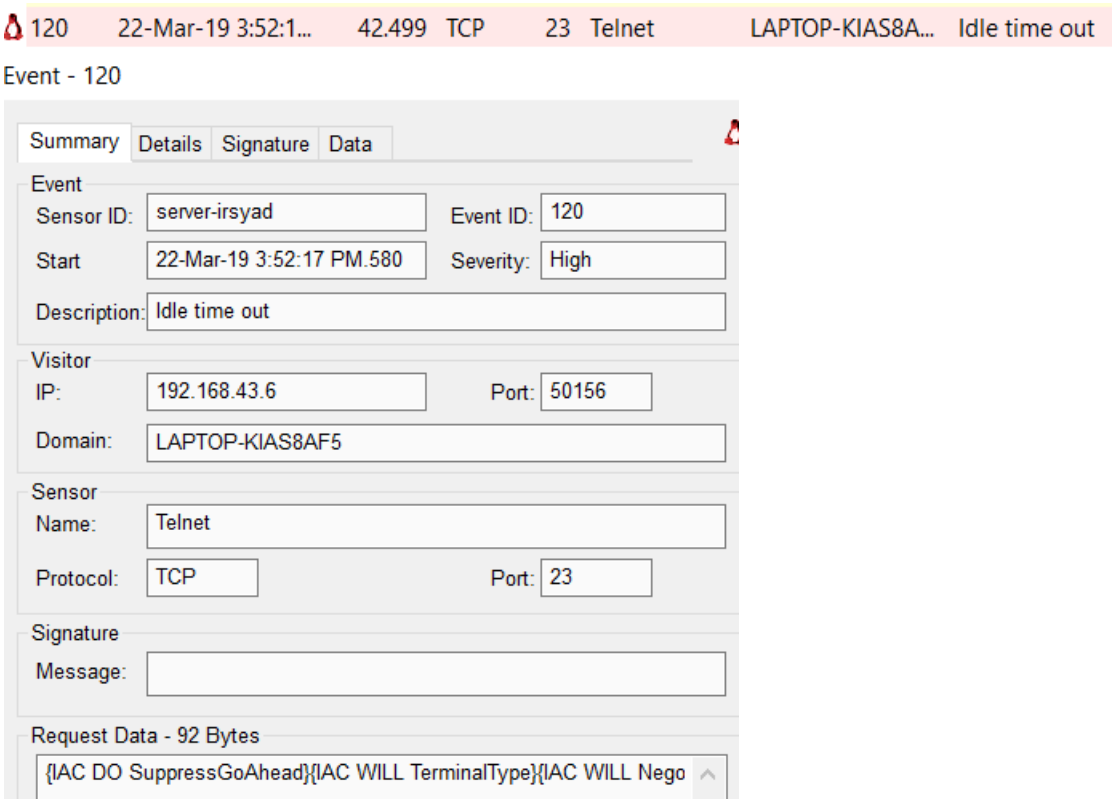
d. Buka KFSensor pada Windows



e. Jalankan service pada KFSensor

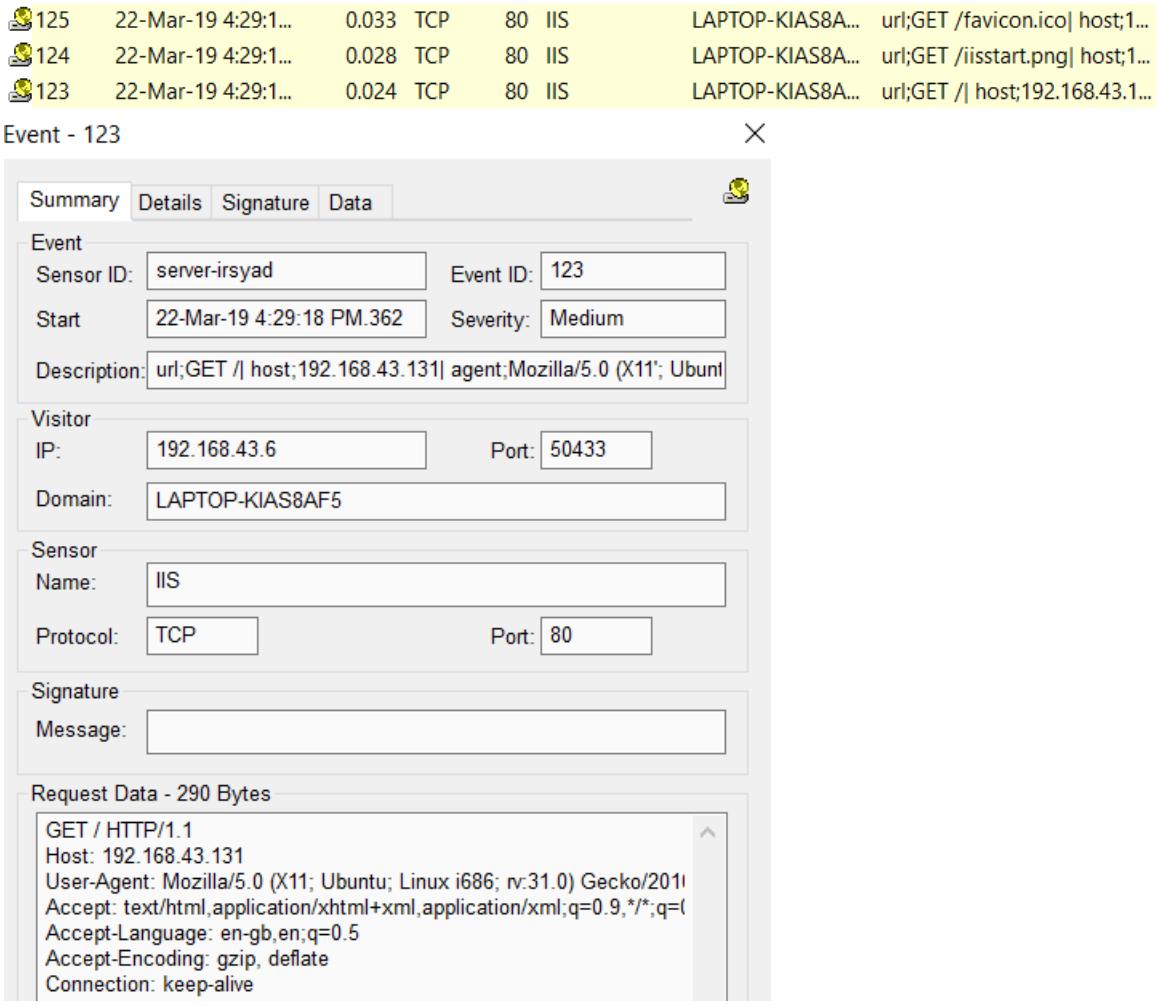
f. Minta teman untuk berperan sebagai penyerang. Penyerang melakukan telnet ke PC praktikan dengan honeydrive

g. Cek KFSensor dan lihat pada IP penyerang, maka akan didapat hasil sebagai berikut



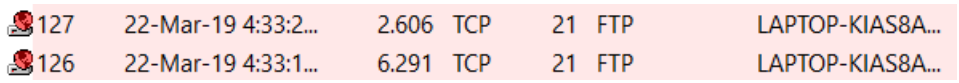
h. Penyerang melakukan HTTP request ke IP praktikan dengan honeydrive

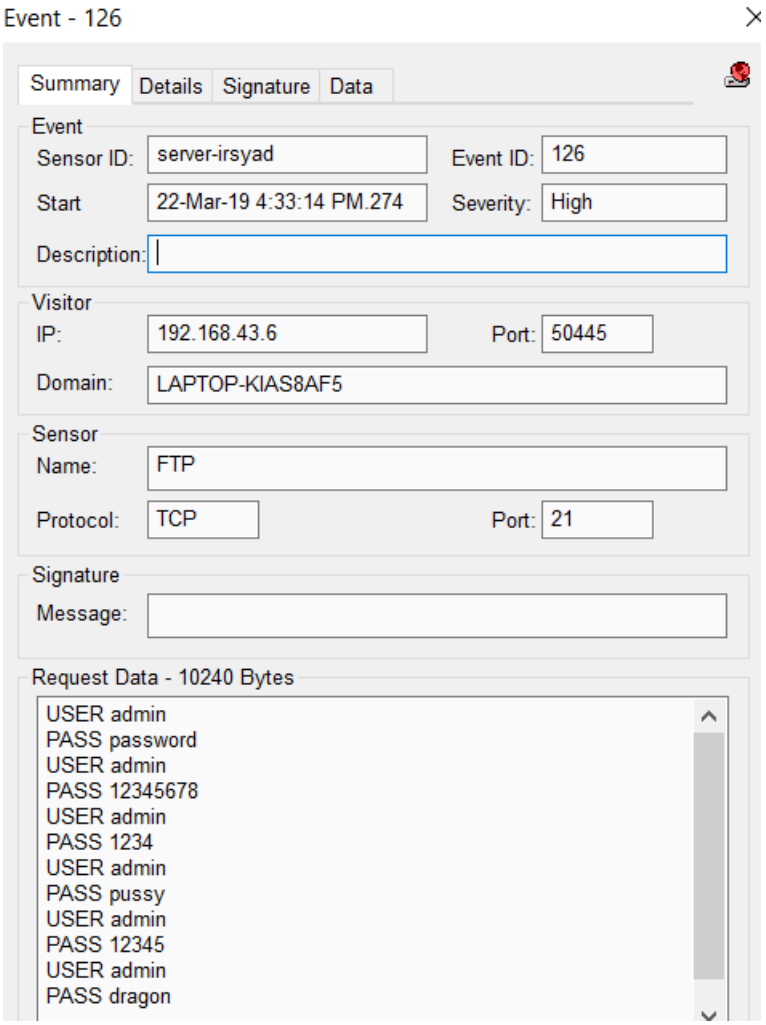
i. Cek KFSensor dan lihat pada IP penyerang, maka akan didapat hasil sebagai berikut



j. Penyerang melakukan FTP request dengan hydra pada honeydrive

k. Cek KFSensor dan lihat pada IP penyerang, maka akan didapat hasil sebagai berikut




Event - 126
Summary
Details
Signature
Data
Event
Sensor ID:
server-irsyad
Event ID:
126
Start
22-Mar-19 4:33:14 PM.274
Severity:
High
Description:
Visitor
IP:
192.168.43.6
Port:
50445
Domain:
LAPTOP-KIAS8AF5
Sensor
Name:
FTP
Protocol:
TCP
Port:
21
Signature
Message:
Request Data - 10240 Bytes
USER admin
PASS password
USER admin
PASS 12345678
USER admin
PASS 1234
USER admin
PASS pussy
USER admin
PASS 12345
USER admin
PASS dragon