



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.

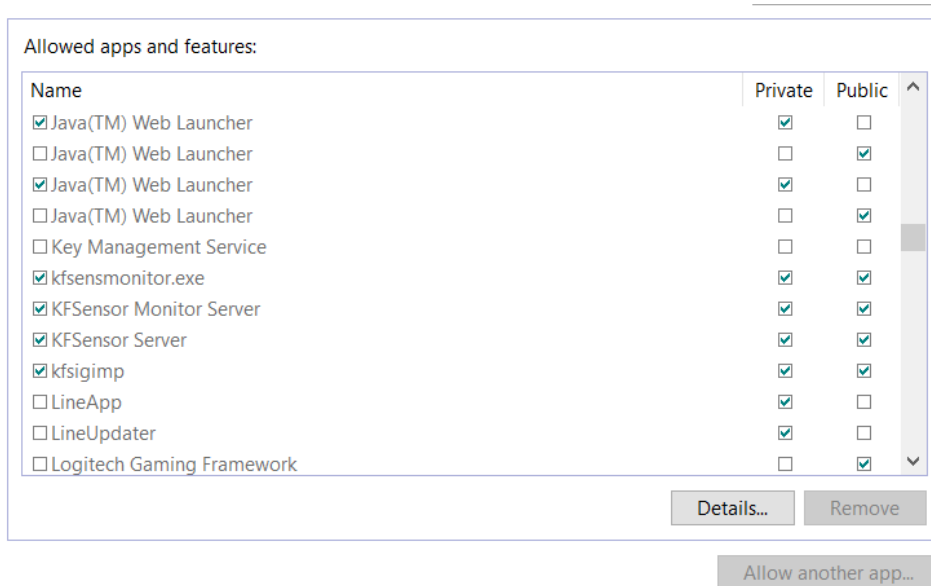
c. HoneyBot

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.

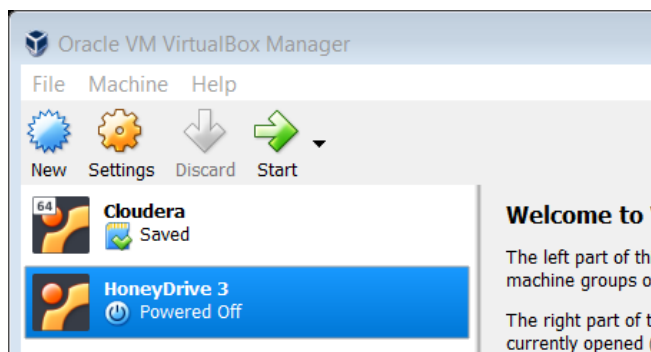
2. Cara menggunakan KFSensor

a. Install KFSensor

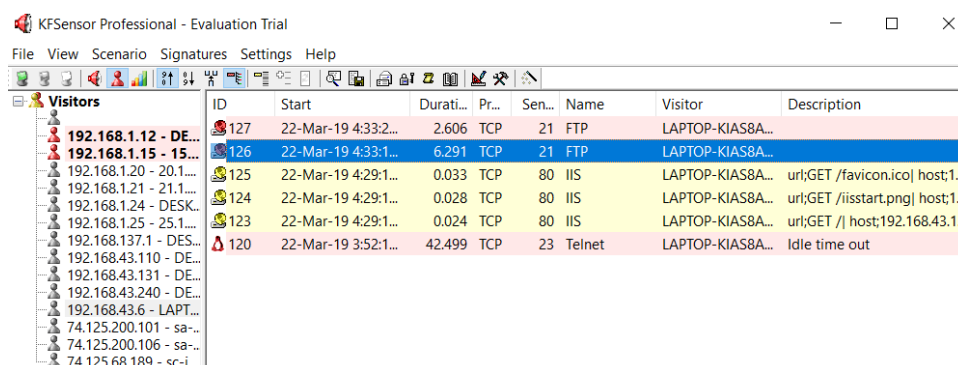
b. Ubah settingan pada firewall



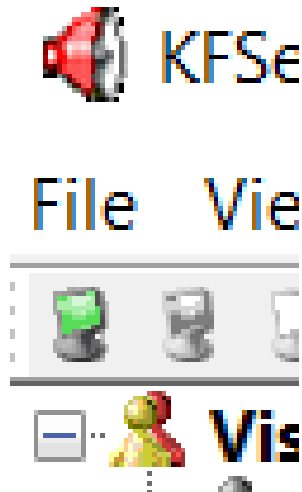
c. Buka HoneyDrive dengan menggunakan virtual machine



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

120 22-Mar-19 3:52:1... 42.499 TCP 23 Telnet LAPTOP-KIAS8A... Idle time out

Event - 120

Summary	Details	Signature	Data
Event			
Sensor ID:	server-irsyad	Event ID:	120
Start	22-Mar-19 3:52:17 PM.580	Severity:	High
Description:	Idle time out		
Visitor			
IP:	192.168.43.6	Port:	50156
Domain:	LAPTOP-KIAS8AF5		
Sensor			
Name:	Telnet		
Protocol:	TCP	Port:	23
Signature			
Message:			
Request Data - 92 Bytes			
{[AC DO SuppressGoAhead}{[AC WILL TerminalType}{[AC WILL Nego ^			

- h. Penyerang melakukan HTTP request ke IP praktikan dengan honeydrive



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

125	22-Mar-19 4:29:1...	0.033	TCP	80	IIS	LAPTOP-KIAS8A...	url;GET /favicon.ico host;1...
124	22-Mar-19 4:29:1...	0.028	TCP	80	IIS	LAPTOP-KIAS8A...	url;GET /iisstart.png host;1...
123	22-Mar-19 4:29:1...	0.024	TCP	80	IIS	LAPTOP-KIAS8A...	url;GET / host;192.168.43.1...

Event - 123



SummaryDetailsSignatureData

Event

Sensor ID: server-irsyadEvent ID: 123

Start: 22-Mar-19 4:29:18 PM.362Severity: Medium

Description: url;GET /| host;192.168.43.131| agent;Mozilla/5.0 (X11; Ubuntu

Visitor

IP: 192.168.43.6Port: 50433

Domain: LAPTOP-KIAS8AF5

Sensor

Name: IIS

Protocol: TCPPort: 80

Signature

Message:

Request Data - 290 Bytes

GET / HTTP/1.1
Host: 192.168.43.131
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:31.0) Gecko/2011
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.5
Accept-Language: en-gb,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive

- j. Penyerang melakukan FTP request dengan hydra pada honeydrive

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

127	22-Mar-19 4:33:2...	2.606	TCP	21	FTP	LAPTOP-KIAS8A...
126	22-Mar-19 4:33:1...	6.291	TCP	21	FTP	LAPTOP-KIAS8A...



Event - 126 ✕

Summary Details Signature Data

Event

Sensor ID: Event ID:

Start: Severity:

Description:

Visitor

IP: Port:

Domain:

Sensor

Name:

Protocol: Port:

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