UNIVERSITAS AMIKOM YOGYAKARTA

LAPORAN 11

SISTEM ADMINISTRATOR & LAYANAN JARINGAN

IDS PADA CENTOS 7

Dibuat oleh :

Nama : Nurhalis Jusman

NIM : 17.83.0079

Kelas : 17-S1TK-02

A. TUJUAN

1. Mahasiswa dapat mengetahui dan dapat membuat sebuah IDS memakai OSSEC
2. Mahasiswa paham cara kerja IDS OSSEC

3. PERALATAN

1. Laptop atau PC
2. Virtual Machine dengan VMware atau Virtual Box
3. VM ber-Sistem Operasi Linux CentOS

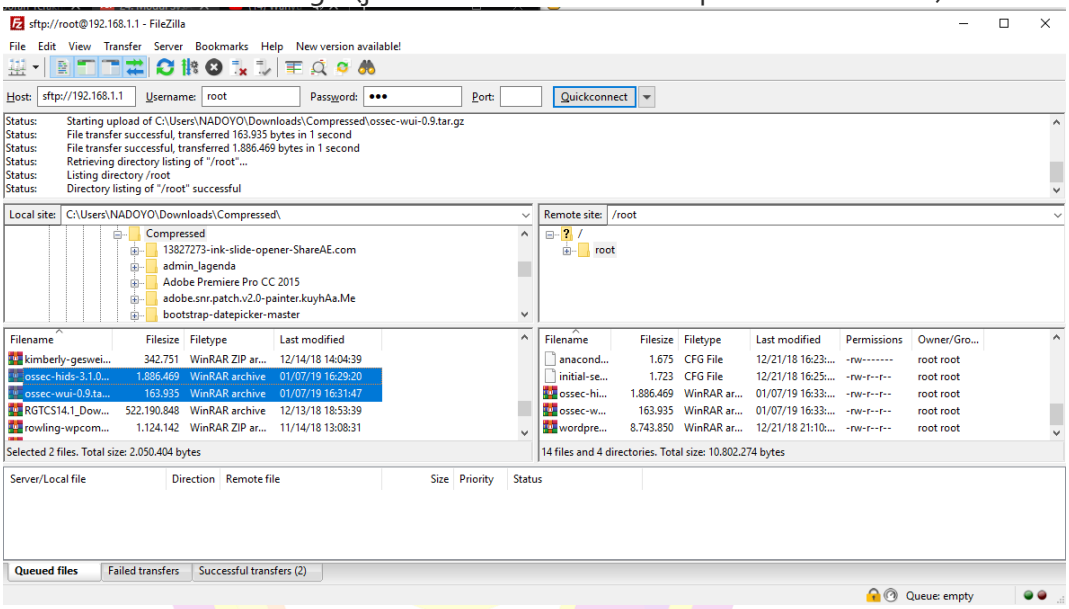
4. TEORI SINGKAT

IDS (Intrusion Detection System) adalah sebuah sistem yang melakukan pengawasan terhadap traffic jaringan dan pengawasan terhadap kegiatan-kegiatan yang mencurigakan didalam sebuah sistem jaringan. Jika ditemukan kegiatankegiatan yang mencurigakan berhubungan dengan traffic jaringan maka IDS akan memberikan peringatan kepada sistem atau administrator jaringan. Dalam banyak kasus IDS juga merespon terhadap traffic yang tidak normal/ anomaly melalui aksi pemblokiran seorang user atau alamat IP (Internet Protocol) sumber dari usaha pengaksesan jaringan.

1. Sebelum install ossec, pertama install gcc

```
[root@nadoyo ~]# yum install gcc_
```

2. Setelah itu download 2 file yang bernama ossec-hids.. yang digunakan untuk instalasi ossecnya dan ossec-wui yang digunakan untuk membuka ossec via web. Disini saya memakai client untuk mendownload file tersebut setelah itu kirim ke centosnya. Atau anda juga bisa mendownload langsung dari server centos memakai tool wget(jika di server centos terdapat akses internet)



3. 2 file tersebut saya kirim ke directory home user root. Dan saya cek di directorynya ada. Setelah itu saya extract file ossec-hids di folder yang sama. Untuk file ini bebas mau diextract dimana. Karena file ini nanti hanya digunakan untuk instalasi package ossec.

```
[root@nadoyo ~]# ls
anaconda-ks.cfg       ossec-hids-3.1.0.tar.gz  wordpress
initial-setup-ks.cfg  ossec-wui-0.9.tar.gz     wordpress-4.9.8.tar.gz
[root@nadoyo ~]# tar xvf ossec-hids-3.1.0.tar.gz _
```

4. Setelah itu masuk ke directory dan install ossec. Kemudian isi semua sesuai perintah

```
[root@nadoyo ~]# cd ossec-hids-3.1.0/
[root@nadoyo ossec-hids-3.1.0]# ls
active-response  CHANGELOG  contrib       doc  INSTALL     LICENSE     src
BUGS             CONFIG     CONTRIBUTORS  etc  install.sh  README.md   SUPPORT.md
[root@nadoyo ossec-hids-3.1.0]# ./install.sh
```

5. Selanjutnya menyalakan ossec

```
[root@nadoyo ~]# /var/ossec/bin/ossec-control start
Starting OSSEC HIDS v3.1.0 (by Trend Micro Inc.)...
2019/01/07 16:38:38 ossec-maild: INFO: E-Mail notification disabled. Clean Exit.
Started ossec-maild...
Started ossec-execd...
Started ossec-analysisd...
Started ossec-logcollector...
2019/01/07 16:38:38 ossec-syscheckd(1702): INFO: No directory provided for syscheck
2019/01/07 16:38:38 ossec-syscheckd: WARN: Syscheck disabled.
2019/01/07 16:38:38 rootcheck: Rootcheck disabled. Exiting.
2019/01/07 16:38:38 ossec-syscheckd: WARN: Rootcheck module disabled.
Started ossec-syscheckd...
Started ossec-monitord...
Completed.
[root@nadoyo ~]#
```

6. Untuk melihat log dari ossec

```
[root@nadoyo ~]# tail -f /var/ossec/logs/ossec.log
```

7. Untuk melihat alert. Jika sudah masukkan email. Makan email anda akan mendapatkan pemberitahuan

```
[root@nadoyo ~]# tail -f /var/ossec/logs/alerts/alerts.log
```

8. Konfigurasi ossec.conf

```
[root@nadoyo ~]# vi /var/ossec/etc/ossec.conf
```

9. Jika tadi penulisan email salah/belum bisa menuliskan disini

```
<ossec_config>
  <global>
    <email_notification>yes</email_notification>
    <email_to>admin@nadoyo.com</email_to>
    <smtp_server>mail.nadoyo.com</smtp_server_from>
    <email_from>ossec@nadoyo.com</email_from>
  </global>
```

10. Menambahkan rules baru. Jika mempunyai rules baru/ingin merubah ruler yang sudah ada disarankan mengganti di file local_rules.xml

```
[root@nadoyo ~]# cd /var/ossec/rules/
[root@nadoyo rules]# vi local_rules.xml
```

```
<group name="local,syslog,">
        <rule id="554" level="7" overwrite="yes">
                <category>ossec</category>
                <decoded_as>syscheck_new_entry</decoded_as>
                <description>file added to the system.</description>
                <groyp>syscheck,</group>
        </rule>
```

11. Jika sudah selesai restart ossecnya

```
[root@nadoyo rules]# /var/ossec/bin/ossec-control restart
```

12. Disini saya akan mengakses via web memakai subdomain ossec.nadoyo.com, karena saya belum mendeklarasikan subdomain tersebut. Maka saya tambahkan di file forward dan file reverse

```
@       IN SOA  nadoyo.com. root.nadoyo.com. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
@       IN      NS      nadoyo.com.
@       IN      PTR     nadoyo.com.
1       IN      PTR     nadoyo.com.
1       IN      PTR     ossec.nadoyo.com._
2       IN      PTR     client.nadoyo.com.
```

13. Kemudian restart dan check

```
[root@nadoyo ~]# systemctl  restart named
[root@nadoyo ~]# dig ossec.nadoyo.com
```

14. Ekstrak file ossec-wui

```
[root@nadoyo ~]# tar xvf ossec-wui-0.9.tar.gz _
```

15. Pindah directory ke sekaligus ke mengganti Namanya. Disini nama directory nya sebelumnya adalah ossec-wui-0.9 kemudian dipindah ke /var/www/html dengan nama directory menjadi ossec.

```
[root@nadoyo ~]# mv ossec-wui-0.9 /var/www/html/ossec
[root@nadoyo ~]# chown -R apache:apache /var/www/html/ossec/
[root@nadoyo ~]# _
```

16. Masuk ke directory tadi kemudian jalankan setup.sh dengan perintah "./setup.sh" disini digunakan agar login terlebih dahulu sebelum bisa mengakses ossec web.

```
[root@nadoyo ~]# cd /var/www/html/ossec/
[root@nadoyo ossec]# ./setup.sh
Setting up ossec ui...

Username: nadoyo
New password:
Re-type new password:
Adding password for user nadoyo
Enter your web server user name (e.g. apache, www, nobody, www-data, ...)
apache
You must restart your web server after this setup is done.

Setup completed successfully.
[root@nadoyo ossec]# _
```

17. Setelah itu buat virtualhost. Disini sebelumnya saya sudah membuat virtualhost dengan nama php.conf jadi tinggal dicopy/salin kemudian diedit sedikit.

```
[root@nadoyo ossec]# cd /etc/httpd/conf.d/
[root@nadoyo conf.d]# ls
autoindex.conf  php.conf  ssl.conf          userdir.conf
non-ssl.conf    README    ssl.conf.rpmsave  welcome.conf
[root@nadoyo conf.d]# cp php.conf ossec.conf
[root@nadoyo conf.d]# vi ossec.conf
```

```
<VirtualHost *:80>
        DocumentRoot /var/www/html/ossec
        ServerName ossec.nadoyo.com
        ServerAdmin admin@nadoyo.com
        <Directory /var/www/html/ossec>
                AllowOverride All
        </Directory>
</VirtualHost>
~
```

18. Kemudian restart httpdnya dan login ossec di web browser dengan menggunakan ossec.nadoyo.com

```
[root@nadoyo conf.d]# systemctl restart httpd
```