Раздел: Жизненный цикл ИБ
Модуль 3.1: Целенаправленные атаки. Практическое задание. HIDS OSSEC.
Выполнил: Александр Ганицев

Условия задания:

Научиться использовать хостовую систему обнаружения вторжений.

Шаги реализации:

1. Установите OSSEC-сервер:
//
https://cdimage.debian.org/cdimage/archive/8.11.1/amd64/iso-cd/debian-8.11.1-amd64-netinst.iso
wget https://ossec.wazuh.com/repos/apt/debian/pool/main/o/ossec-hids/ossec-hids_2.8.3-4jessie_amd64.deb dpkg -i ossec-hids_2.8.3-4jessie_amd64.deb
sudo dpkg -i ossec-hids_2.8.3-4jessie_amd64.deb
sudo apt-get install ossec-hids sudo
apt-get -f install /var/ossec/bin/ossec-control start

Установка на Debian 10
#
https://gemmei.ftp.acc.umu.se/cdimage/archive/10.11.0/amd64/iso-cd/debian-10.11.0- amd64-netinst.iso
su root
apt update
apt install inotify-tools gcc zlib1g-dev
wget https://github.com/ossec/ossec-hids/archive/3.3.0.tar.gz
tar xzf 3.3.0.tar.gz -C /tmp/

скачиваем https://disk.yandex.ru/d/29ALvYefQ8nniw pcre2-10.32.tar.gz
tar zxf pcre2-10.32.tar.gz -C /tmp/ossec-hids-3.3.0/src/external/
sudo apt-get install build-essential
cd /tmp/ossec-hids-3.3.0/
./install.sh

2. Установите агента OSSEC на MS Windows.

Добавьте OSSEC-агенты:
/var/ossec/bin/ossec-control restart
/var/ossec/bin/manage_agents
- Adding a new agent (use '\q' to return to the main menu).
Please provide the following:
* A name for the new agent: ИМЯ_АГЕНТА
* The IP Address of the new agent: ИП_АГЕНТА
* An ID for the new agent[001]:

3. Установите WEB-интерфейс OSSEC:

```
# wget http://www.ossec.net/files/ui/ossec-wui-0.3.tar.gz
# tar -zxvf ossec-wui-0.3.tar.gz
# cd /var/www/ossec-wui/
# ./setup.sh
```

Проверьте работу настроенной системы, зафиксировав буртфорс-атаку на сервер.

Условия реализации.

В форму для отправки задания приложите скриншоты с зафиксированной брутфорс-атакой.

Выполнение.

1. Установка OSSEC server.

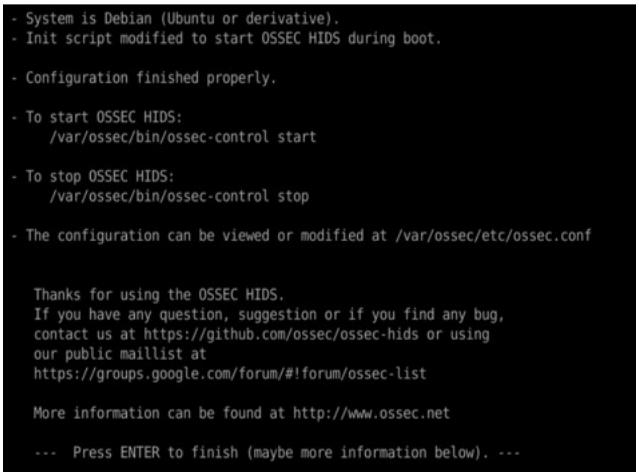
1.1. Настроил новый Ubuntu 20.04.6 (Focal Fossa).

1.2. Обновил VirtualBox до версии 7.0.10, установил VboxGuestAdditions.

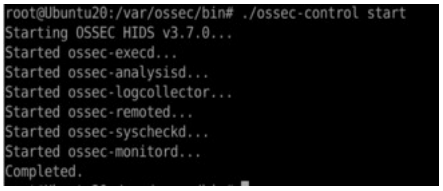
1.3. Установил необходимые зависимости:

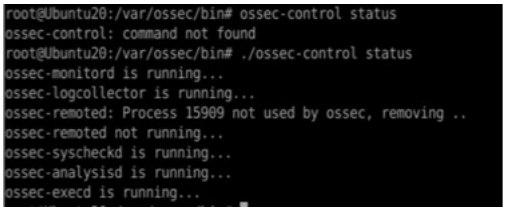
sudo apt install -y php php-cli php-common libapache2-mod-php apache2-utils inotify-tools apache2 build-essential gcc make git wget tar libz-dev libssl-dev libpcre2-dev libevent-dev libsystemd-dev

1.4. “Собрал” OSSEC сервер:



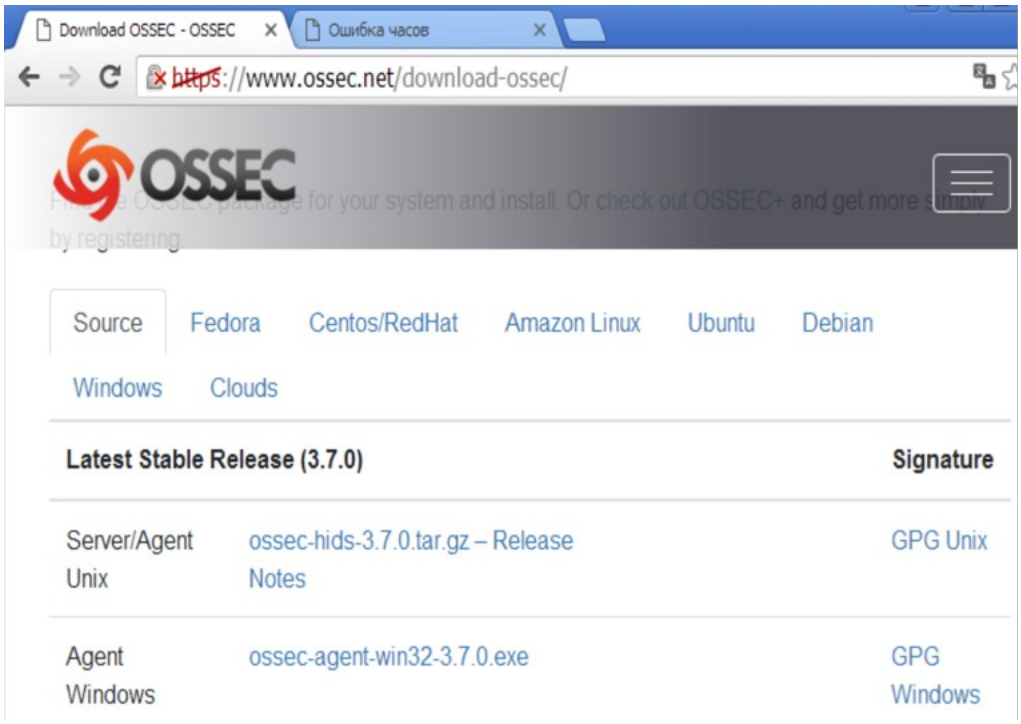
1.5. Запустил OSSEC сервер:

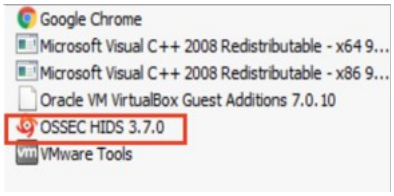




2. Установка агента на Windows Server 2008.

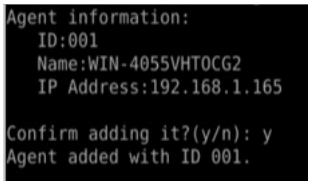
2.1. Скачал и установил OSSEC агент на Windows Server 2008:



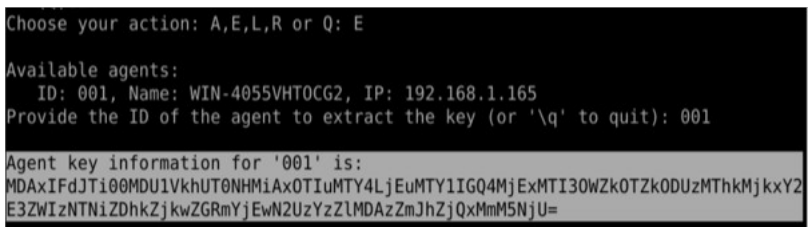


2.2. Настроил агент на OSSEC сервере:

Windows Server 2008 host name: WIN-4055VHTOCG2, IP: 192.168.1.165.



Извлечённый ключ:



Перезагрузил сервер:

```
manage_agents: Exiting.
manage_agents: Exiting.
root@Ubuntu20:/var/ossec/bin# ./ossec-control restart
Killing ossec-monitord ..
Killing ossec-logcollector ..
ossec-remoted not running ..
Killing ossec-syscheckd ..
Killing ossec-analysisd ..
ossec-maild not running ..
Killing ossec-execd ..
OSSEC HIDS v3.7.0 Stopped
Starting OSSEC HIDS v3.7.0...
Started ossec-execd...
Started ossec-analysisd...
Started ossec-logcollector...
Started ossec-remoted...
Started ossec-syscheckd...
Started ossec-monitord...
Completed.
root@Ubuntu20:/var/ossec/bin# ./ossec-control status
ossec-monitord is running...
ossec-logcollector is running...
ossec-remoted is running...
ossec-syscheckd is running...
ossec-analysisd is running...
ossec-execd is running...
```

3. Установил WEB-интерфейс OSSEC.

3.1. Клонировал ossec-wui с github.com, удалил index.html и запустил скрипт настройки:

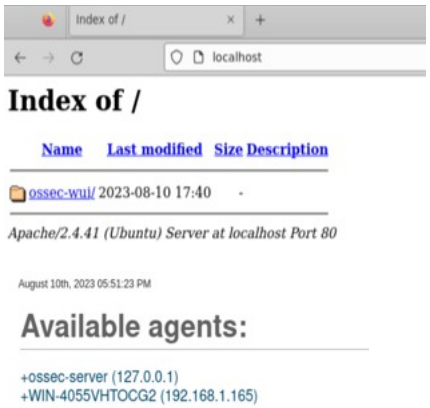
```
root@Ubuntu20:/tmp# git clone https://github.com/ossec/ossec-wui.git
Cloning into 'ossec-wui'...
remote: Enumerating objects: 205, done.
remote: Total 205 (delta 0), reused 0 (delta 0), pack-reused 205
Receiving objects: 100% (205/205), 217.04 KiB | 32.00 KiB/s, done.
Resolving deltas: 100% (69/69), done.
root@Ubuntu20:/tmp# mv ossec-wui/ /var/www/html/
root@Ubuntu20:/tmp# cd /var/www/html/
root@Ubuntu20:/var/www/html# ls
index.html  ossec-wui
root@Ubuntu20:/var/www/html# rm index.html
root@Ubuntu20:/var/www/html# ls
ossec-wui
```

```
root@Ubuntu20:/var/www/html/ossec-wui# ls
CONTRIB  htaccess_def.txt  index.php  lib      ossec_conf.php  README.search  site
css      img               js         LICENSE  README          setup.sh
root@Ubuntu20:/var/www/html/ossec-wui# ./setup.sh
trap: SIGHUP: bad trap
Setting up ossec ui...

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

Setup completed successfully.
```

3.2. Установил права для www-data и перезагрузил apache2:

```
root@Ubuntu20:/var/www/html/ossec-wui# chown -R www-data:www-data /var/www/html/ossec-wui
/
root@Ubuntu20:/var/www/html/ossec-wui# chmod -R 755 /var/www/html/ossec-wui/
root@Ubuntu20:/var/www/html/ossec-wui# systemctl restart apache2
root@Ubuntu20:/var/www/html/ossec-wui# systemctl status  apache2
* apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enable>
     Active: active (running) since Thu 2023-08-10 17:49:52 MSK; 5s ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 19326 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 19331 (apache2)
      Tasks: 6 (limit: 9430)
     Memory: 9.5M
     CGroup: /system.slice/apache2.service
             |-19331 /usr/sbin/apache2 -k start
             |-19332 /usr/sbin/apache2 -k start
             |-19333 /usr/sbin/apache2 -k start
             |-19334 /usr/sbin/apache2 -k start
             |-19335 /usr/sbin/apache2 -k start
             `-19336 /usr/sbin/apache2 -k start

авг 10 17:49:52 Ubuntu20 systemd[1]: Starting The Apache HTTP Server...
авг 10 17:49:52 Ubuntu20 systemd[1]: Started The Apache HTTP Server.
```

3.3. Подключился к веб-серверу в браузере, проверил доступные агенты:



4. Запустил eternalblue эксплойт в Kali:

```
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

После долгих экпериментов с этой системой, и предоставления нового образа Александром Сергеевичем Цукановым, попытки эксплойта данной Windows Server 2008 не увенчались успехом, то есть **Kali/msfconsole** так и не доходит до стадии взлома, до вызова meterpreter.

Соответственно, я не могу показать следы взлома ни в Kali, ни в OSSEC wui...