Lab 14: XLM macros

Table of Contents

Lab 14: XLM macros	
Goals	1
Requirements	1
1. Create an XLM macro to execute a Windows command	1
2. Making the macro automatically execute when the document is opened	8
3. Observing the payload's process tree	

Goals

- Create an Excel spreadsheet that uses an XLM macro to execute a command when opened.
- Create an Excel spreadsheet that uses an XLM macro to execute shellcode when opened.

Requirements

- Windows 10 VM with Microsoft Office installed.
- Kali Linux Student VM.

1. Create an XLM macro to execute a Windows command

1. In this stage of the exercise, you will create a simple XLM macro that executes a command. First, open Microsoft Excel and create a new spreadsheet document.

Excel	Good morning	
斺 Home	∽ New	
🖹 New	A B C	
🗁 Open	1 2 3 4 4 5 5 6 7 Blank workbook	Take a tour
		More templates $ ightarrow$

Creating a New Excel Spreadsheet

2. Next, right-click on the "Sheet1" tab at the bottom of the spreadsheet and then click "Insert..." in the menu that appears.

2		Insert		_		
	Ш,	<u>D</u> elete		-		
	Ð	<u>R</u> ename				
 		Move or Copy		-		
	Q	<u>V</u> iew Code				
	4	Protect Sheet		-		
		<u>T</u> ab Color	2	>		
		<u>H</u> ide				
		<u>U</u> nhide		-		
	. .	Select All Sheets	-			
Sheet1		Select All Sheet	2			
Ч	5					



3. In the "Insert" window that appears, choose "MS Excel 4.0 Macro", and then click OK.

Insert	×
General Spreadsheet Solutions	
Worksheet Chart MS Excel 4.0 Macro MS Excel 5.0 Dialog	Preview not available.
Templates on Office.com	OK Cancel

Selecting "MS Excel 4.0 Macro"

4. A new tab named "Macro1" should appear at the bottom of the spreadsheet.

AutoSave 💽 🗄 り~	(2. ▲	Book1 - Exce	a 🗘 🗚	lice 🔺	F	- 0	×
File Home Insert	Page Layout	Formulas Data	Review Vi	ew He	elp	🖻 Share	1
Paste V Font Alignm	nent Number	Conditional Format	ting ~ III Cells ~	C Editing	Analyze Data	Sensitivity	
Clipboard 191	I	Styles	I	1	Analysis	Sensitivity	^
A1 🔻 : 🗙 🗸	f_x						~
A	В	с	D		Е		F 🔺
1							
2							
3							
4							
5							-
 → Macro1 Sh 	ieet1 🕴 🕂)	÷ •				F
Ready					_	+	100%

Macro1 Tab Appears

5. In the top-left cell (A1) of the Macro1 worksheet, enter the text shown below. This is a simple XLM macro that will execute the Windows Command Prompt when executed.





6. To test that the macro executes successfully, right-click on the cell and, then click on "Run..." in the menu.

A1 · Calib	ori - 11 - A^ A` \$ - % 🤊 🖻	
AB	I ≡ ॒ ~ <u>A</u> ~ <u>H</u> ~ 58 - % ≪	D
1 =EXEC("cmd.exe")		
2	Cut	
3 🕛 🗋	<u>С</u> ору	
4	Paste Ontions:	
5		
6		
7		
8	Paste <u>S</u> pecial	
9))	Smart Lookup	
10		
11	Insert	
12	Delete	
13		
14	Clear Co <u>n</u> tents	
15	New Comment	
16 +		
17	New Note	
18	Eormat Cells	
19	Pure C	
20	<u>Kun</u>	
21		
< → Macro1	Sheet1 (+)	: •

Testing Macro Execution

7. Then click on the "Run" button in the window that appears.

		А	В	С		D		E	
1	=EXEC("cmd.exe")							
2									
3		Macro			?	×			
4		Macro name:							
5		Al		± 1	Run				
6					<u></u>				
7					<u>S</u> tep Int	to			
8					Edit				
9									
10					Create	:			
11					Delete				
12									
13				~	Options				
14									
15		Macros in: All	Open Workbooks	\sim					
16		Description							
17									
18									
19					Cance	I			
20									
21									
	<	Macro	Sheet1 🕂)		: · · ·	(

Clicking "Run"

8. Clicking the Run button should execute the "cmd.exe" command contained in your macro, which will open the Windows Command Prompt. If you don't see the command prompt window appear, check the taskbar - it may run in a minimized window.

AutoSave 💽 🔐	୬• ୯ · •	Book1 - Exc	cel 🔎 🖌	Alice 🔺	• –		×
File Home Ins	ert Page Layout	Formulas Data	Review Vi	iew He	lp	ය Share	P
Paste V Font	Alignment Number	E Conditional Forma Format as Table ~	atting ~ Cells	C Editing	Analyze Se Data	nsitivity	
Clipboard 😼		Styles			Analysis Se	nsitivity	^
A1 🔻 :	× √ <i>f</i> _x =EX	(EC("cmd.exe")					~
A 1 =EXEC("cmd.exe") 2 3	В	С	D		E		F 🔺
4 5 6 7							
A Macro	1 Sheet1 🕂)	: 4				Þ
Ready				3 🗉		+	100%
H $ \mathcal{P} $ Type here	to search	0	Hi 💽	-	🗄 🖻	×	D'N-

Command Prompt Appears in the Task Bar

9. Click on the command prompt icon that appeared in your task bar, and close the command prompt window before continuing with the instructions in the next section.



Closing the Command Prompt

2. Making the macro automatically execute when the document is opened

1. Now you'll configure the macro to execute automatically whenever the spreadsheet is opened. Make sure that the cell where your macro is stored is selected, and then click in the Name Box in the toolbar above the cell.

AutoSave 💽 Off 🛛	¶ 9·~	Book1 - Exc	el 🔎 Alice	• A 🖻
File Home In	sert Page Layout	Formulas Data	Review View	Help
Paste Clipboard	Image: Alignment % Number *	E Conditional Forma Format as Table ~ Cell Styles ~ Styles	atting ~ E	diting Analyze Data Analysis
A1] 🔹 :	$\times \checkmark f_x = EX$	(EC("cmd.exe")		
Name Box A	В	с	D	E
1 =EXEC("cmd.exe")				
2				
3				
4				
5				
6				
7				
< → Macr	ol Sheet1 (+)		

Changing the Cell Name

2. After you click inside the Name Box, change the name of the cell from "A1" to "Auto_open", and press Enter to confirm the change.

AutoSave 💽 🕅	୬• ୯· ₹	Book1 - Excel	Alice	A 🗹	- 0	×
File Home Ins	ert Page Layout	Formulas Data	Review View	Help	🖻 Share	P
Paste V V Clipboard V	Alignment Vumber	Conditional Formatti	ng ~ 🗐 Cells E	Analyze Data	Sensitivity Sensitivity	~
Auto_open 🔻 🗄	\times \checkmark f_x =E)	(EC("cmd.exe")				~
A	В	с	D	E		F 🔺
1 =EXEC("cmd.exe")						
2						
2						
						_
4						
4 5						
4 5 6 7						

Name Changed to "Auto_open"

3. Now save the document by clicking the floppy disk icon at the top of the Excel window. Then save the file to your desktop as either an "Excel Macro-Enabled Workbook" (file extension .XLSM), or "Excel 97-2003 Workbook" (file extension .XLS). This process is illustrated in the four screenshots below.

AutoSave 💽 😗 📙	५२८२ र	Book1 - Exe	cel O	Alice	A
File Home Inse	ert Page Layout Alignment Number	Formulas Data	Review atting ~	View	Help
Clipboard 5	 ✓ ✓ f_x =EX 	EC("cmd.exe")		*	~ [An
A	В	с	D		
2					

Clicking the Save Icon

Save	this file	
File Nan	ne	
Book1	.xlsm	
Choose	a Location OneDrive - Roll Communication Services	
	alice@rollcomsvs.onmicrosoft.com » OneDrive - Roll Communication Services	
More of	otions Save Cancel	

Clicking "More options..."

e	Save As	
斺 Home		_
🗅 New	C Recent	Pinned Pin folders you want to easily find later. Click the pin icon t hover over a folder.
🗁 Open	Roll Communication Services	X I
Info	OneDrive - Roll Communicatio alice@rollcomsvs.onmicrosoft.com	Vesterday Desktop Desktop
Save	Sites - Roll Communication Ser alice@rollcomsys.onmicrosoft.com	
Save As	Other locations	
Print	This PC	
Share	Add a Place	
Export		
Publish	Browse	
Close		

Clicking Browse

Save As				Х
	_			
$\leftarrow \rightarrow \land \uparrow$ $\square \rightarrow$ This PC \rightarrow Desktop \rightarrow	~ C) Search Deskto	p	م ر
Organize 🔻 New folder				?
^ Name ^	Date	modified	Туре	
Quick access Lab exercises	2/27/	/2021 7:48 PM	File folder	I
Downloads Documents				
Pictures *				
h Music				
Videos				
🔊 Microsoft Excel 🗸 🧹				>
File name: XLM sample 1				~
Save as type: Excel Macro-Enabled Workbook				~
Authors: Excel Workbook				
Excel Macro-Enabled Workbook				
Excel 97-2003 Workbook				
CSV UTF-8 (Comma delimited)				
Single File Web Page				
Hide Folders Web Page Excel Template				

Saving as an Appropriate Format

4. After saving the document, close Microsoft Excel. You should see the spreadsheet file you just created saved on your desktop.

Recycle Bin	W R Word		
Microsoft Edge	X Excel		
Lab exercises	X I		
procexp64			

Excel Spreadsheet Saved to Desktop

5. Double-click on the file to open it in Excel again. When the file opens, you should see a Security Warning displayed at the top of the Excel window that indicates that the file contains macros. Click on the "Enable Content" button to execute the macro you created.

AutoSave 💽 🕅 📙	9~~~ ₹	XLM sample 1 👻	♀ Search	
File Home Inse	ert Page Layout	Formulas Data	Review View	Help
Calibri	<u>→</u> 11 → =	≡ ≡ ce Gener	ral 🗸 🖾 Conditi	onal Formatting
Dacta B I	⊻ - A^ A Ξ -	≡≡⊠∽∣\$~	% 🤊 🛛 📆 Format	as Table ∽
× ダ	<u>⊘</u> ~ <u>A</u> ~ <u>∈</u>	→= ≫ ? ~ (0.1	Cell Sty	les ~
Clipboard 🗔	Font 🗔 Al	lignment 🗔 Num	nber 🖂	Styles
SECURITY WARNING	i Macros have been disa	abled. Enable Cont	tent	
Auto_open 🔻 🗄	$\times \sqrt{f_x} = E$	(EC("cmd.exe")		
A	В	с	D	E
1 =EXEC("cmd.exe")				
2				

Clicking "Enable Content"

6. After you click "Enable Content", Windows Command Prompt should appear again. Remember to check the taskbar if you don't see the window open. This time, don't close the command prompt window after it opens. Leave it running for the instructions in the next section.

Au	uto_open 🔻	: ×	< 🗸 -	f _x :	=EXEC("c	md.exe'	')								*
	А		E	3		С			D		E			F	
1	=EXEC("cmd.ex	(e")													
2															
3															
4															
5															-
-	< > N	lacro1	Sheet		÷			:	4					•	
]		1	+	100%	,
ӯре	here to search				0	∐i	0		•		x	PN -		,	^ '

Command Prompt Opened in Taskbar

3. Observing the payload's process tree

1. With the Excel and Command Prompt programs still running, double-click on the "procexp64" on your desktop. This will open the Sysinternals "Process Explorer" program and allow you to inspect the process tree created your payload.

procexp64	AutoSave Off 目 タッ C' マ	XLM • ,0	Alice 🛕 🖻	×
	FileHomeInsertPage LayouImage: ClipboardImage: Clipboard <th>t Formulas Data Conditional Formatting Format as Table ~ Cell Styles ~ Styles</th> <th>Review View</th> <th>Help</th>	t Formulas Data Conditional Formatting Format as Table ~ Cell Styles ~ Styles	Review View	Help
	Auto_open 🔻 : 🗙 🗸 f_x	=EXEC("cmd.exe")		v
	A B	с	D	E
	2 3			
	4 5			
	Macro1 Sheet1	÷ :		
				+ 100%

Opening Process Explorer

2. Within the Process Explorer window, scroll down until your find the Excel process, "EXCEL.EXE". It will probably be at or near the bottom of the list.

Process Explorer - Sysinternals: www.sysinternals.com [CLIENT1\VMuser] (Administrator)								
File Options View Process Find Users Help								
😼 🖻 🚍 🗉 🦳 🚳 😁 メ 🗛 🐵					A Aux			
Process	CPU	Private Bytes	Working Set	PID	Description	Company	^	
🕞 dwm.exe	0.01	18,372 K	43,448 K	1032	Desktop Window Manager	Microsoft C	2	
csrss.exe	0.03	1,724 K	5,824 K	4276	Client Server Runtime Process	Microsoft C	2	
🖃 🔳 winlogon.exe		2,184 K	10,064 K	4660	Windows Logon Application	Microsoft C	2	
fontdrvhost.exe		4,016 K	9,048 K	4688	Usermode Font Driver Host	Microsoft C	2	
dwm.exe	0.15	27,452 K	62,344 K	1320	Desktop Window Manager	Microsoft C	2	
🖃 🐂 explorer.exe	0.08	29,072 K	99,380 K	5784	Windows Explorer	Microsoft C	1	
SecurityHealthSystray.exe		1,636 K	8,940 K	7736	Windows Security notificatio	Microsoft C	2	
OneDrive.exe		19,176 K	60,872 K	7976	Microsoft OneDrive	Microsoft C	2	
	0.10	80,148 K	124,600 K	5032	Microsoft Excel	Microsoft C	2	
😑 🚓 cmd.exe		2,048 K	3,800 K	3152	Windows Command Processor	Microsoft C	2	
conhost.exe		6,992 K	15,460 K	4856	Console Window Host	Microsoft C	2	
procexp64.exe	0.65	23,828 K	42,444 K	4324	Sysinternals Process Explorer	Sysinternal	k	
							~	
	<					>		
CPU Usage: 1.55% Commit Charge: 16.61%								

Finding EXCEL.exe

3. On the indented lines beneath Excel, you can see other programs that were started by Excel. This is known as the process tree - Excel is the parent process, and those processes branching down beneath it are its children. In this case, "cmd.exe" is shown beneath Excel. "conhost.exe" is also present, which was executed by "cmd.exe".

Process Explorer - Sysinternals: www.sysinternals.com [CLIENT1\VMuser] (Administrator)							
File Options View Process Find Users Help							
😼 🖉 📰 🗉 🧮 🚳 🚰 🤸 🏘 🌚				A Aux			
Process	CPU	Private Bytes	Working Set	PID Description		Company 🗠	
dwm.exe	0.01	18,372 K	43,448 K	1032 Desktop Window Mar	nager	Microsoft C	
CSrss.exe	0.03	1,724 K	5,824 K	4276 Client Server Runtime	Process	Microsoft C	
🖃 📰 winlogon.exe		2,184 K	10,064 K	4660 Windows Logon Appli	ication	Microsoft C	
fontdrvhost.exe		4,016 K	9,048 K	4688 Usermode Font Driver	r Host	Microsoft C	
dwm.exe	0.15	27,452 K	62,344 K	1320 Desktop Window Mar	nager	Microsoft C	
🖃 🐂 explorer.exe	0.08	29,072 K	99,380 K	5784 Windows Explorer		Microsoft C	
SecurityHealthSystray.exe		1,636 K	8,940 K	7736 Windows Security not	tificatio	Microsoft C	
CneDrive.exe		19,176 K	60,872 K	7976 Microsoft OneDrive		Microsoft C	
	0.10	80,148 K	124,600 K	5032 Microsoft Excel		Microsoft C	
🖃 🔜 cmd.exe		2,048 K	3,800 K	3152 Windows Command F	rocessor	Microsoft C	
conhost.exe		6,992 K	15,460 K	4856 Console Window Hos	t	Microsoft C	
🖉 procexp64.exe	0.65	23,828 K	42,444 K	4324 Sysinternals Process	Explorer	Sysintemal	
						~	

Excel's Process Tree

4. Since Excel doesn't execute "cmd.exe" or "conhost.exe" during normal use, this is suspicious behavior that may be detected by defenders. Furthermore, console programs like "cmd.exe", "powershell.exe", and "conhost.exe" (which gets spawned by both cmd.exe and powershell.exe) are **even more suspicious** because they are frequently executed by attackers but less frequently executed by the majority of end users.

In other words, "cmd.exe" being a child process of Excel (like it is here) would be a very strong indicator that an attack is taking place.