Lab 11: Payload testing - Mark of the Web

Table of Contents

Goals

- Observe the effect of the Mark of the Web on a CHM payload file.
- Explore the use of container files to prevent the Mark of the Web being applied to the CHM payload.

Requirements

- Windows 10 VM

Introduction

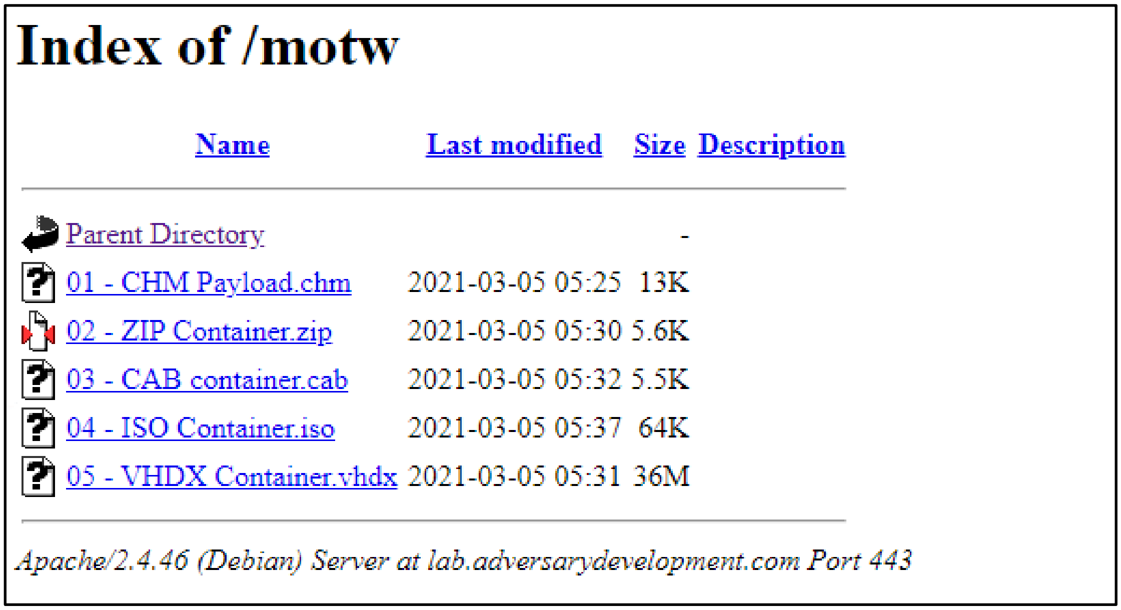
In this exercise, you'll observe the effects of the "Mark of the Web" (MOTW) on a payload file downloaded from the Internet. You'll also explore the use of container files as a means of preventing MOTW from being applied to the CHM payload.

A Compiled HTML Help (CHM) payload file that opens the Windows Calculator is used as the example for this exercise. A CHM file is used for the example because MOTW disables a CHM file's ability to execute commands. Unforeseen characteristics like this make it is very important to test payload files both with and without MOTW before delivering them to a target. (Similar CHM payload files can be created with the PowerShell script listed in the "Additional Resources" section at the end of this document.)

1. CHM files:

1. First, visit the URL below where the files used in this exercise are hosted. It's important that the files are hosted on an actual webserver during testing since downloading the files from the Internet is what causes the MOTW to be applied.

```
https://lab.adversarydevelopment.com/motw/
```



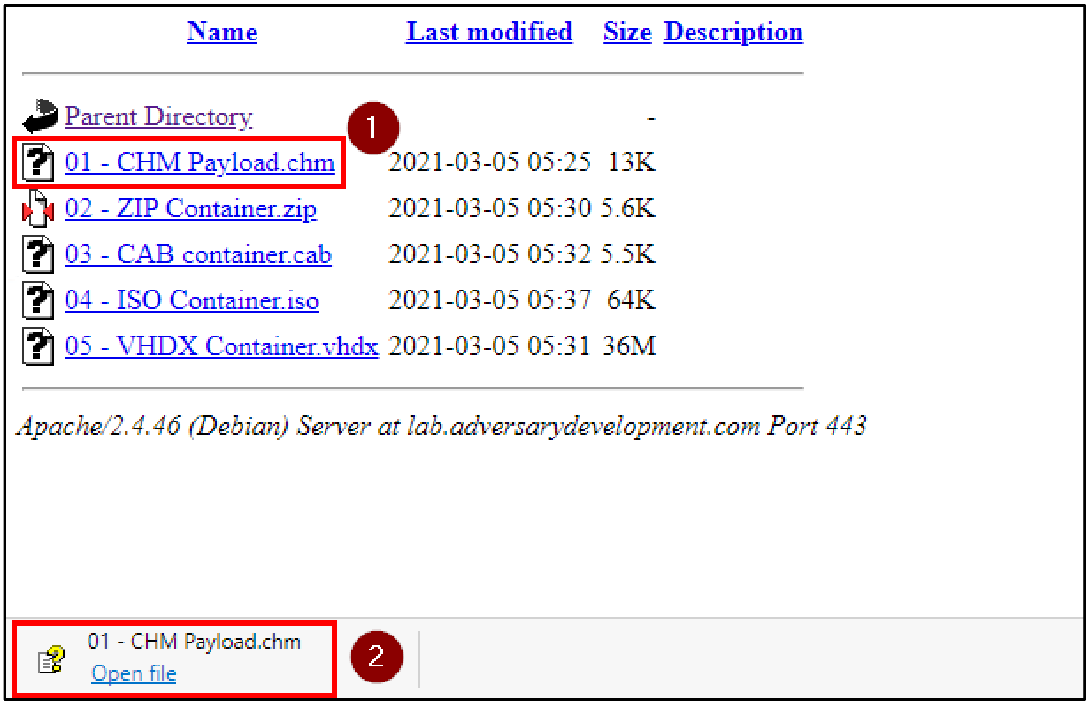
Index of /motw

Name	Last modified	Size	Description
Parent Directory		-	
01 - CHM Payload.chm	2021-03-05 05:25	13K	
02 - ZIP Container.zip	2021-03-05 05:30	5.6K	
03 - CAB container.cab	2021-03-05 05:32	5.5K	
04 - ISO Container.iso	2021-03-05 05:37	64K	
05 - VHDX Container.vhdx	2021-03-05 05:31	36M	

Apache/2.4.46 (Debian) Server at lab.adversarydevelopment.com Port 443

Lab Exercise Files

2. Click on the first file in the list, "01 - CHM Payload.chm", to download it to your Windows 10 VM. Then open the file after the download is complete.

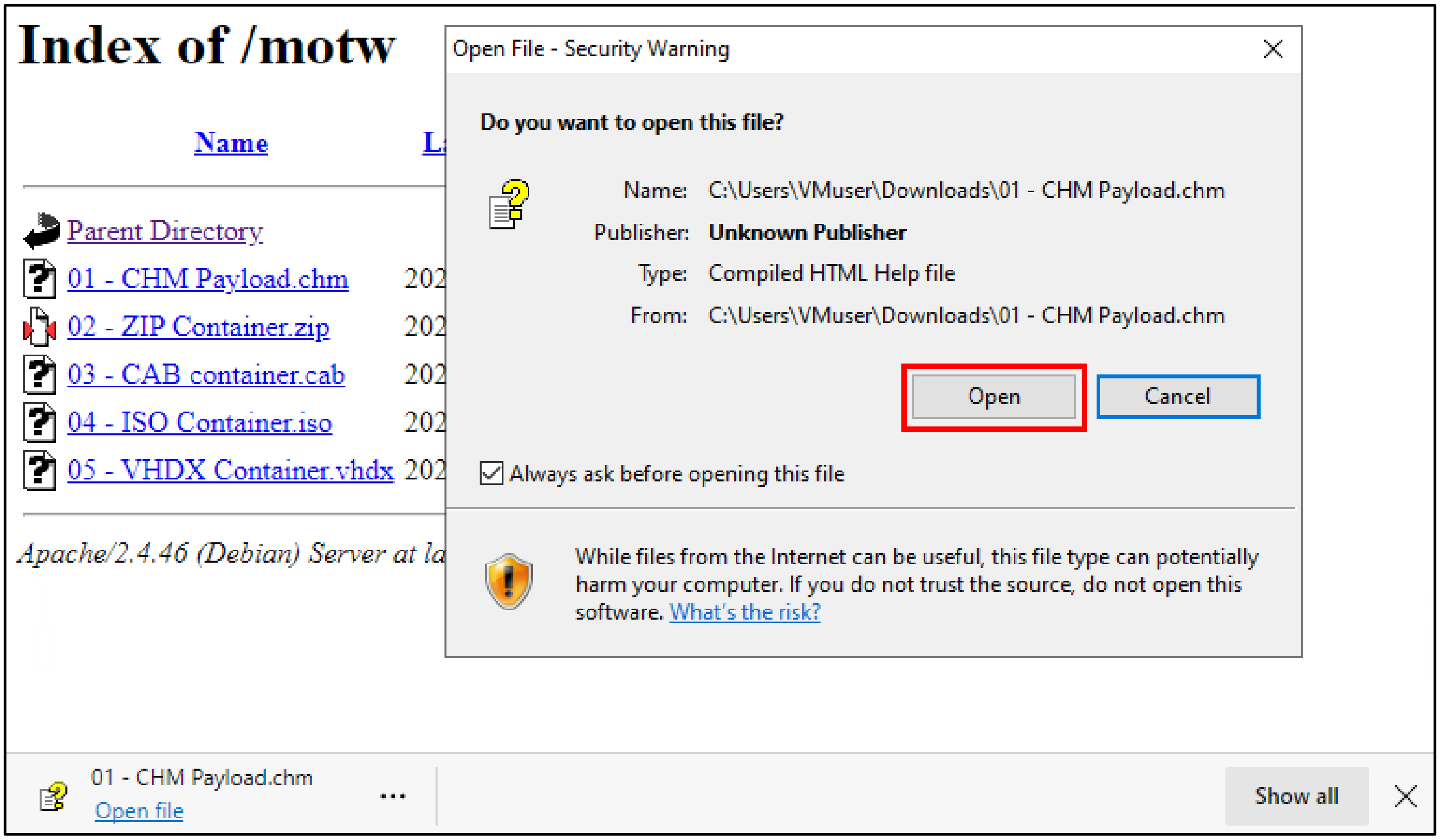


Name	Last modified	Size	Description
Parent Directory		-	
01 - CHM Payload.chm	2021-03-05 05:25	13K	
02 - ZIP Container.zip	2021-03-05 05:30	5.6K	
03 - CAB container.cab	2021-03-05 05:32	5.5K	
04 - ISO Container.iso	2021-03-05 05:37	64K	
05 - VHDX Container.vhdx	2021-03-05 05:31	36M	

Apache/2.4.46 (Debian) Server at lab.adversarydevelopment.com Port 443

Download and Open CHM File

3. Note that opening a downloaded CHM file from the web browser causes a Security Warning to appear. This message could increase recipients' suspicions. It also adds extra complexity and another point of failure to the attack since we rely on the end user to click "Open" and not "Cancel". Click "Open" in the warning message to continue opening the file.



Index of /motw

Name
L
Parent Directory
01 - CHM Payload.chm 202
02 - ZIP Container.zip 202
03 - CAB container.cab 202
04 - ISO Container.iso 202
05 - VHDX Container.vhdx 202
Apache/2.4.46 (Debian) Server at la

Open File - Security Warning

Do you want to open this file?

Name: C:\Users\VMuser\Downloads\01 - CHM Payload.chm

Publisher: **Unknown Publisher**

Type: Compiled HTML Help file

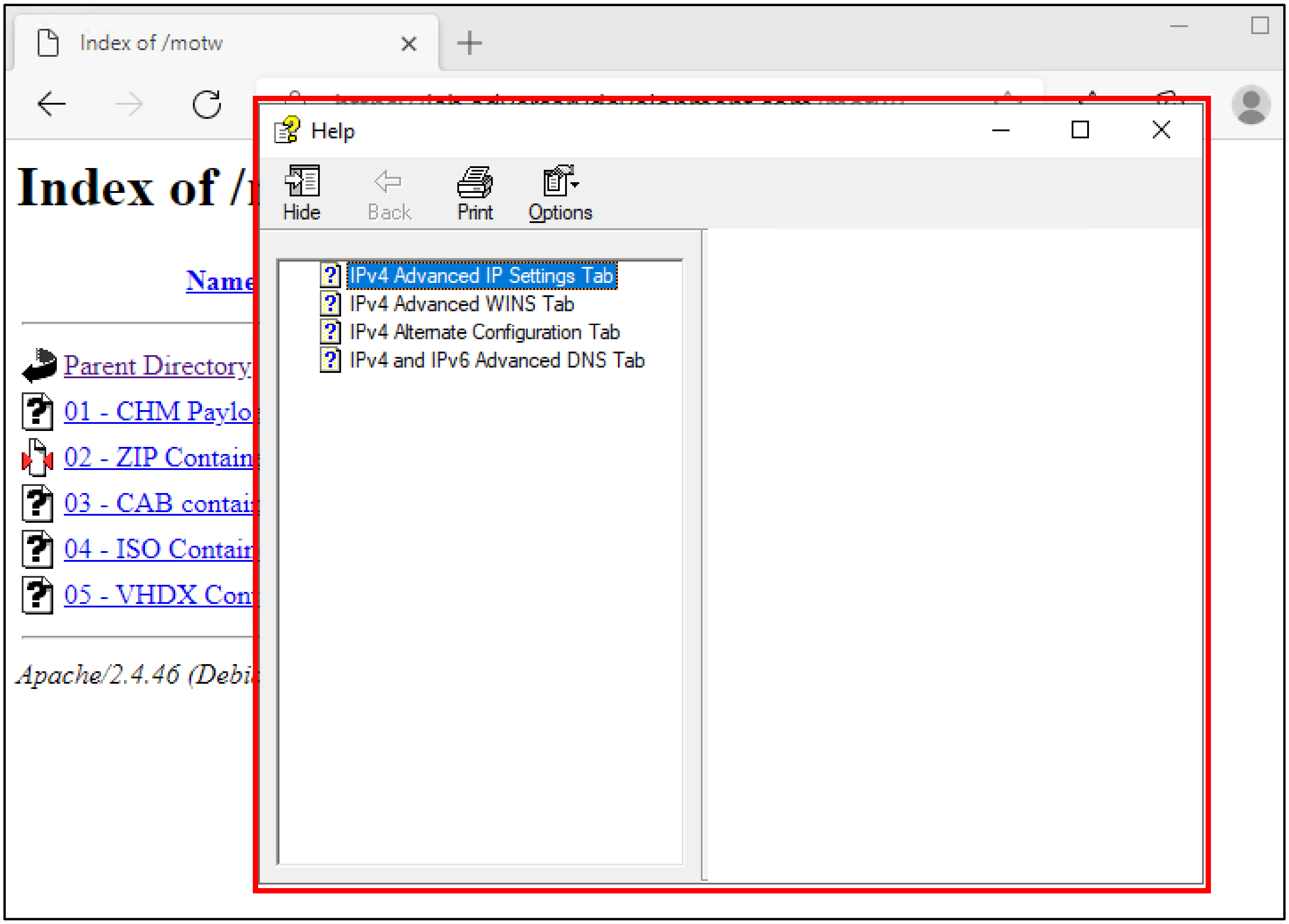
From: C:\Users\VMuser\Downloads\01 - CHM Payload.chm

☑ Always ask before opening this file

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open this software. What's the risk?

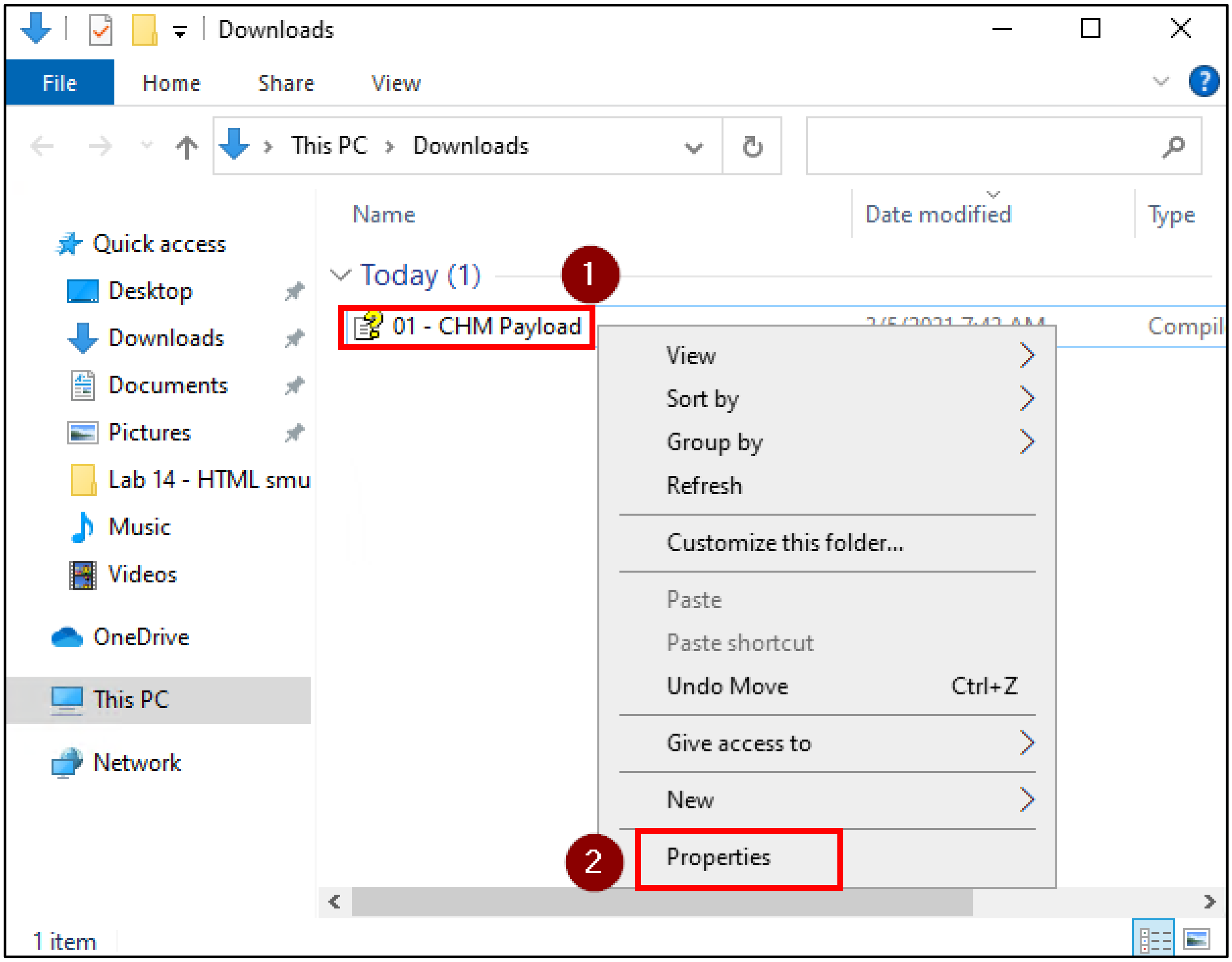
Click "Open" in Security Warning Window

4. When the CHM file opens, you'll see a Help window with no content appear. You might also notice that no Calculator window appears, which is not ideal since the payload file was supposed to open the Windows Calculator. So for some reason, the payload did not execute successfully.



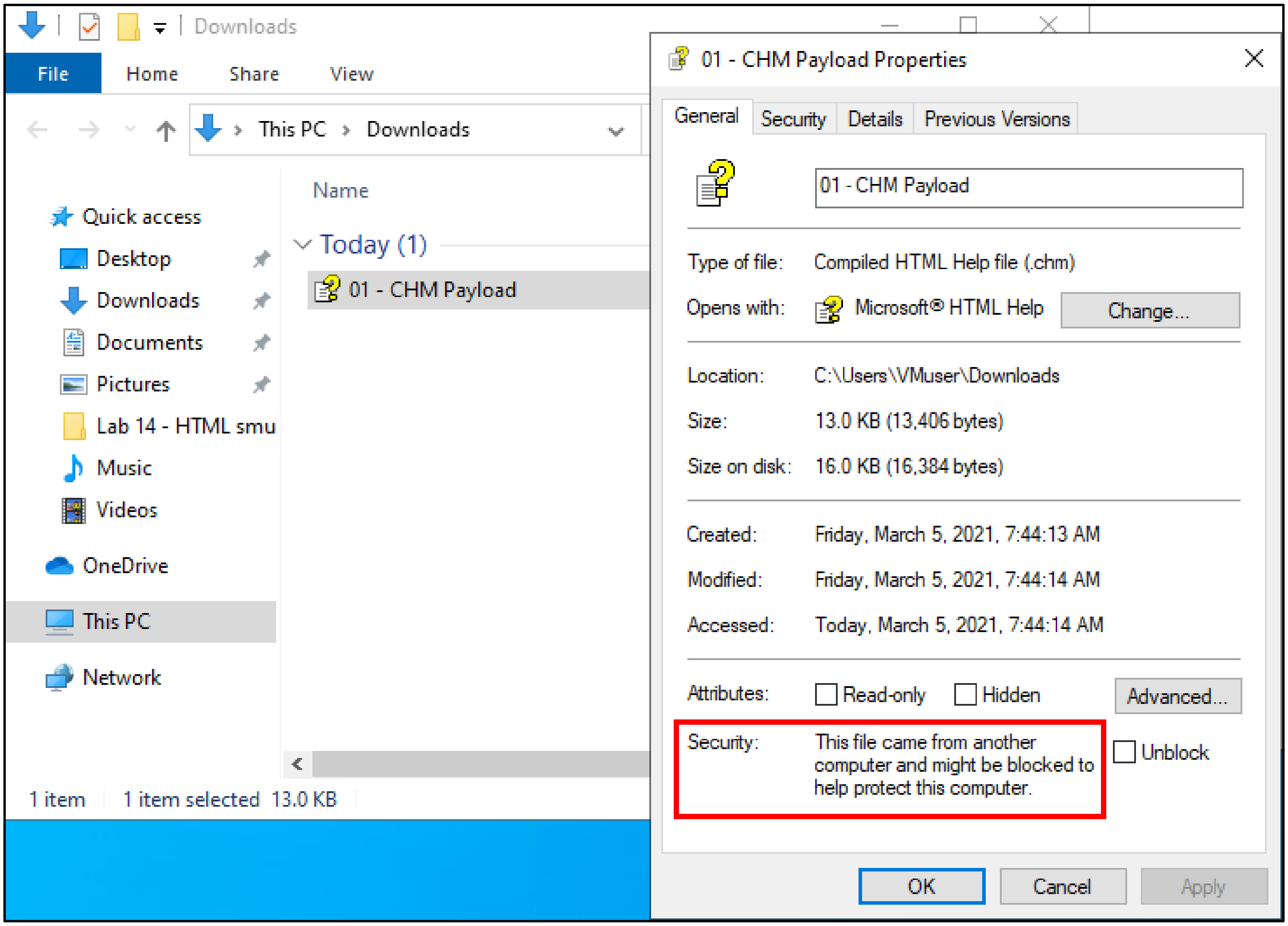
CHM Opened Without Payload Execution

5. Open the folder where the CHM file was downloaded (the "Downloads" folder by default). Then right-click on the CHM payload file and choose "Properties" from the menu.



Opening CHM File Properties

6. On the "General" tab in the Properties window, note the text near the bottom of the window that reads, "This file came from another computer and might be blocked to help protect this computer." This text indicates that the Mark of the Web is currently present on the downloaded CHM payload file.



01 - CHM Payload Properties

01 - CHM Payload

Type of file: Compiled HTML Help file (.chm)

Opens with: Microsoft® HTML Help

Location: C:\Users\VMuser\Downloads

Size: 13.0 KB (13,406 bytes)

Size on disk: 16.0 KB (16,384 bytes)

Created: Friday, March 5, 2021, 7:44:13 AM

Modified: Friday, March 5, 2021, 7:44:14 AM

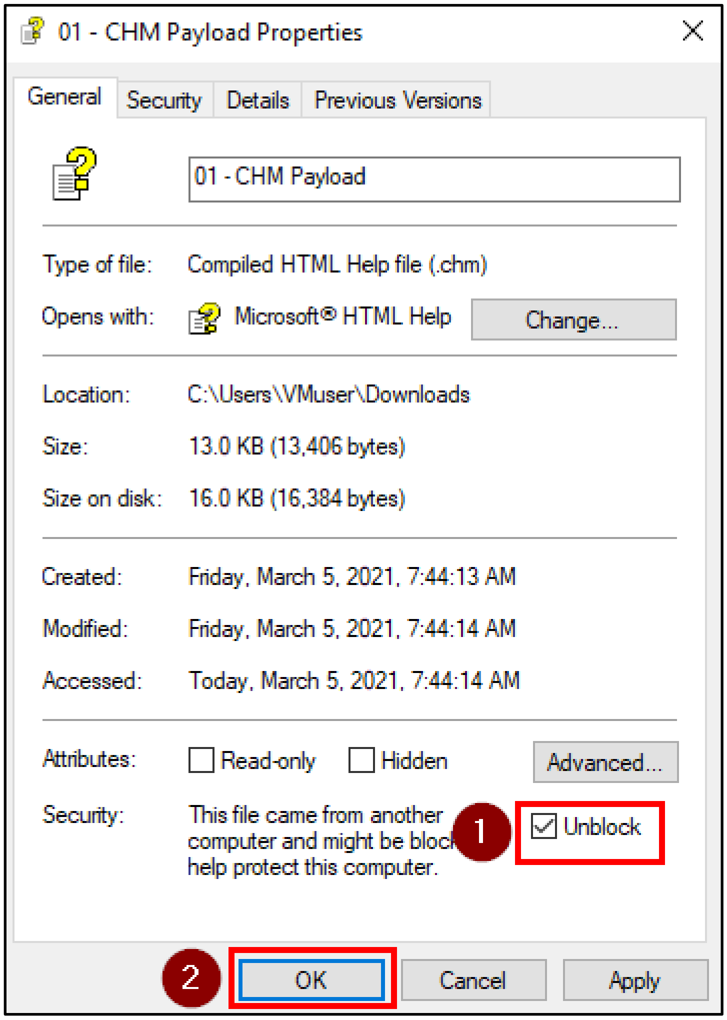
Accessed: Today, March 5, 2021, 7:44:14 AM

Attributes: □ Read-only □ Hidden

Security: This file came from another computer and might be blocked to help protect this computer. □ Unblock

Mark of the Web Present on CHM File

7. Check the box labeled "Unblock" beside the security text in the properties window, and then click OK to remove the MOTW from the CHM payload file.



01 - CHM Payload Properties

01 - CHM Payload

Type of file: Compiled HTML Help file (.chm)

Opens with: Microsoft® HTML Help

Location: C:\Users\VMuser\Downloads

Size: 13.0 KB (13,406 bytes)

Size on disk: 16.0 KB (16,384 bytes)

Created: Friday, March 5, 2021, 7:44:13 AM

Modified: Friday, March 5, 2021, 7:44:14 AM

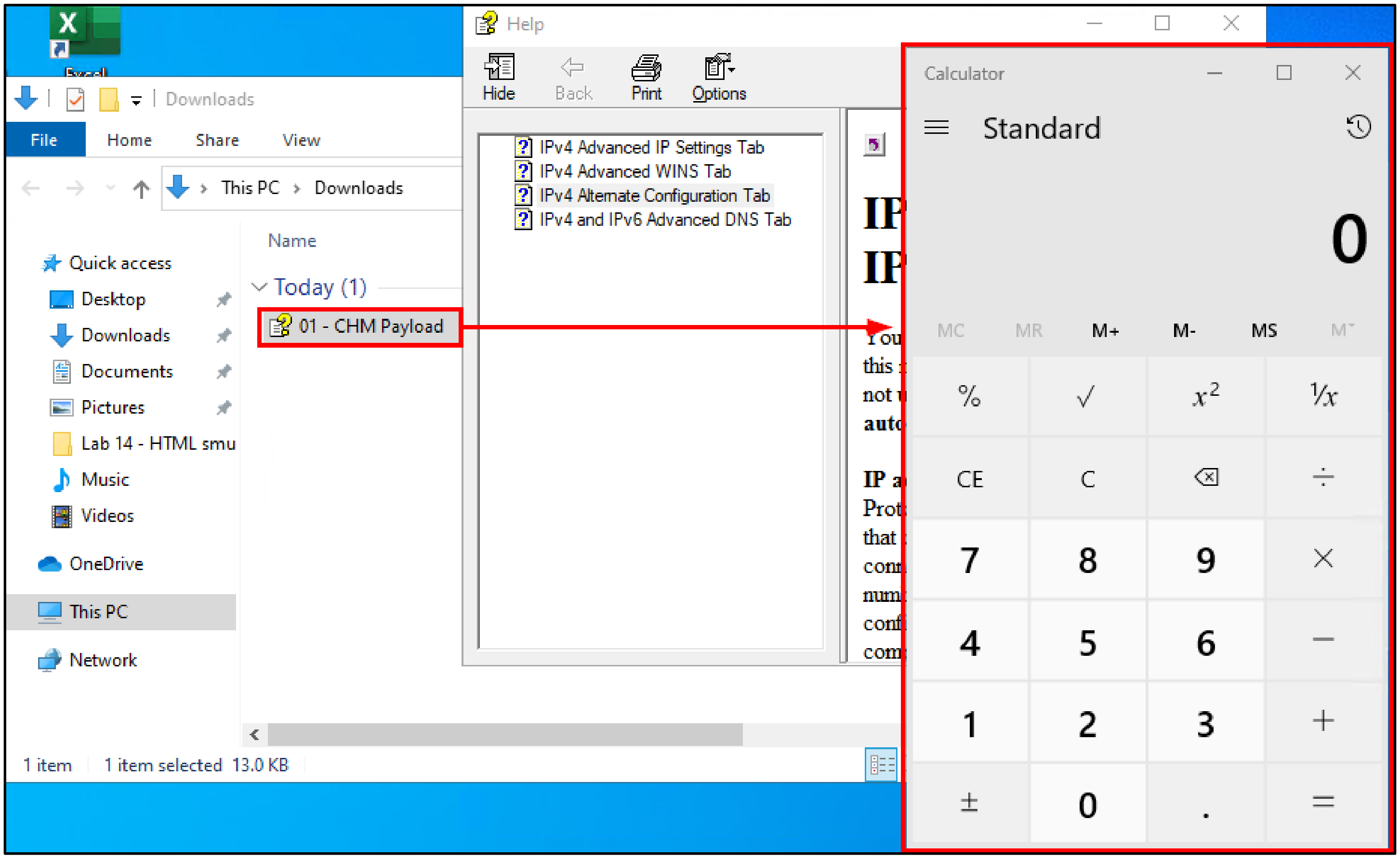
Accessed: Today, March 5, 2021, 7:44:14 AM

Attributes: □ Read-only □ Hidden

Security: This file came from another computer and might be bloc[k]ed to help protect this computer. ☑ Unblock

Removing MOTW

8. Now try opening the CHM file in your Downloads folder again. This time you should see Windows Calculator appear, indicating that the command embedded in the CHM file executed successfully.

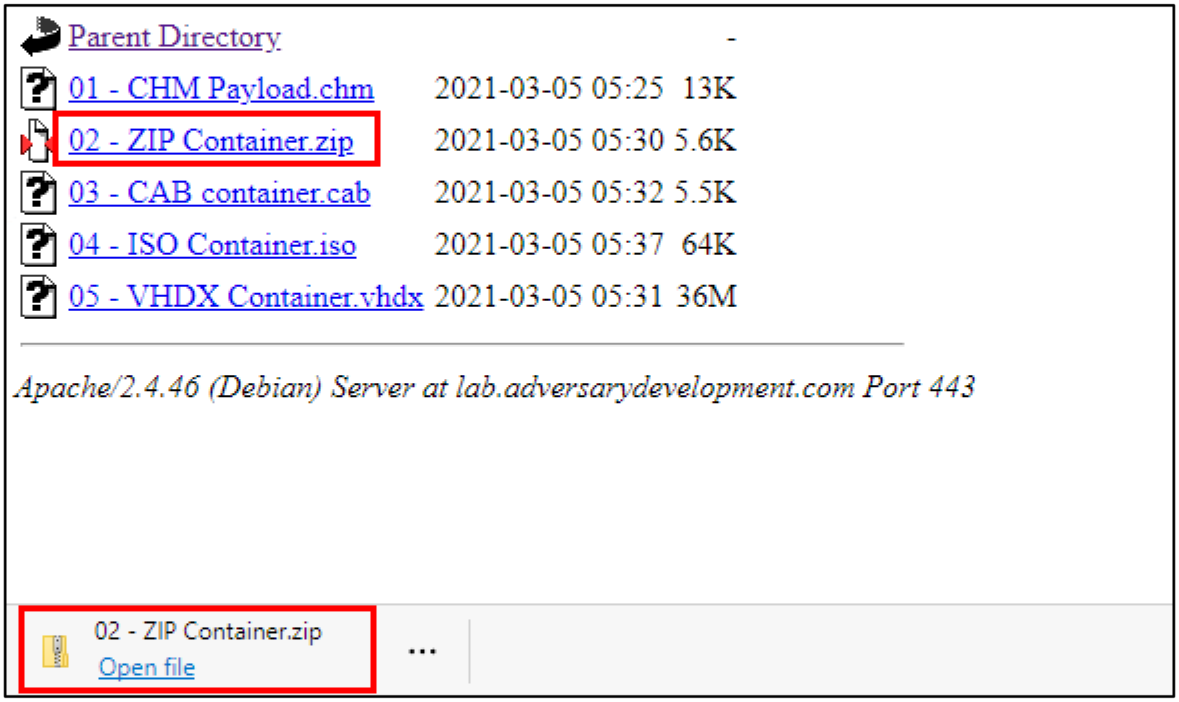


Payload Execution Successful

9. In the sections that follow, you'll observe whether the effects of the MOTW on the CHM file can be prevented by embedding the CHM file inside various container file formats.

2. CHM payload delivered inside a ZIP file

1. Download the ZIP container file from the web server, and then open the downloaded file. When you open the file, you might notice that, unlike the CHM file, the ZIP file does not generate a Security Warning message.



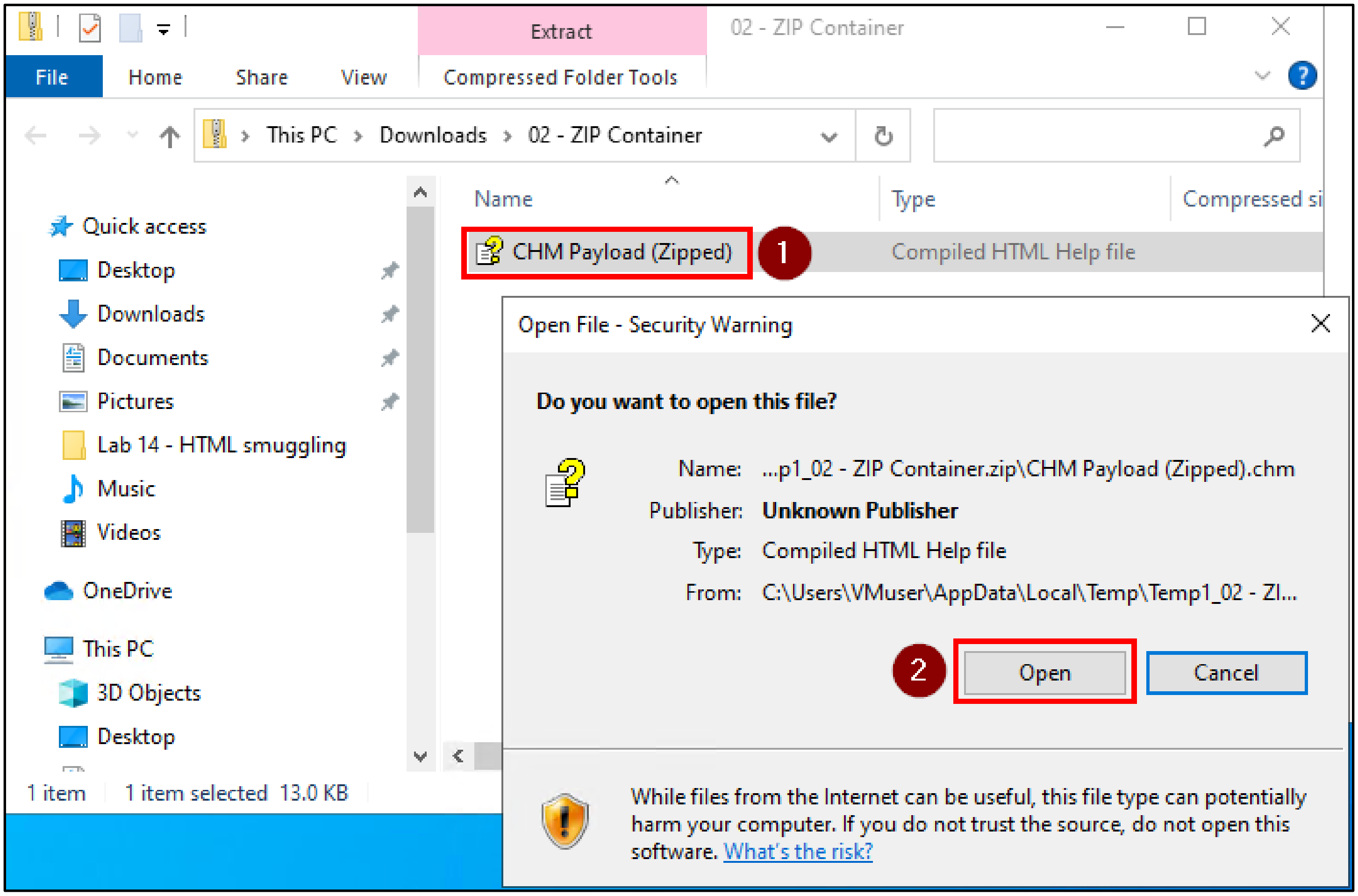
```
Parent Directory                              -
01 - CHM Payload.chm      2021-03-05 05:25  13K
02 - ZIP Container.zip    2021-03-05 05:30 5.6K
03 - CAB container.cab    2021-03-05 05:32 5.5K
04 - ISO Container.iso    2021-03-05 05:37  64K
05 - VHDX Container.vhdx 2021-03-05 05:31  36M

Apache/2.4.46 (Debian) Server at lab.adversarydevelopment.com Port 443
```

ZIP File Download and Open

2. By default, Windows 10 opens ZIP files in Windows Explorer. You should see the opened ZIP file appear in an Explorer window like the one shown below, with the CHM payload stored inside. Double-click on the CHM payload inside the ZIP file to open it. When you open the file, you should also see the Security Warning message that seemed to be missing in the previous step. (As you will see, this message is a common indicator that the

MOTW is being applied to the file you're opening.) Click "Open" in the Security Warning window to continue opening the file.



Open File - Security Warning

Do you want to open this file?

Name: ...p1_02 - ZIP Container.zip\CHM Payload (Zipped).chm

Publisher: **Unknown Publisher**

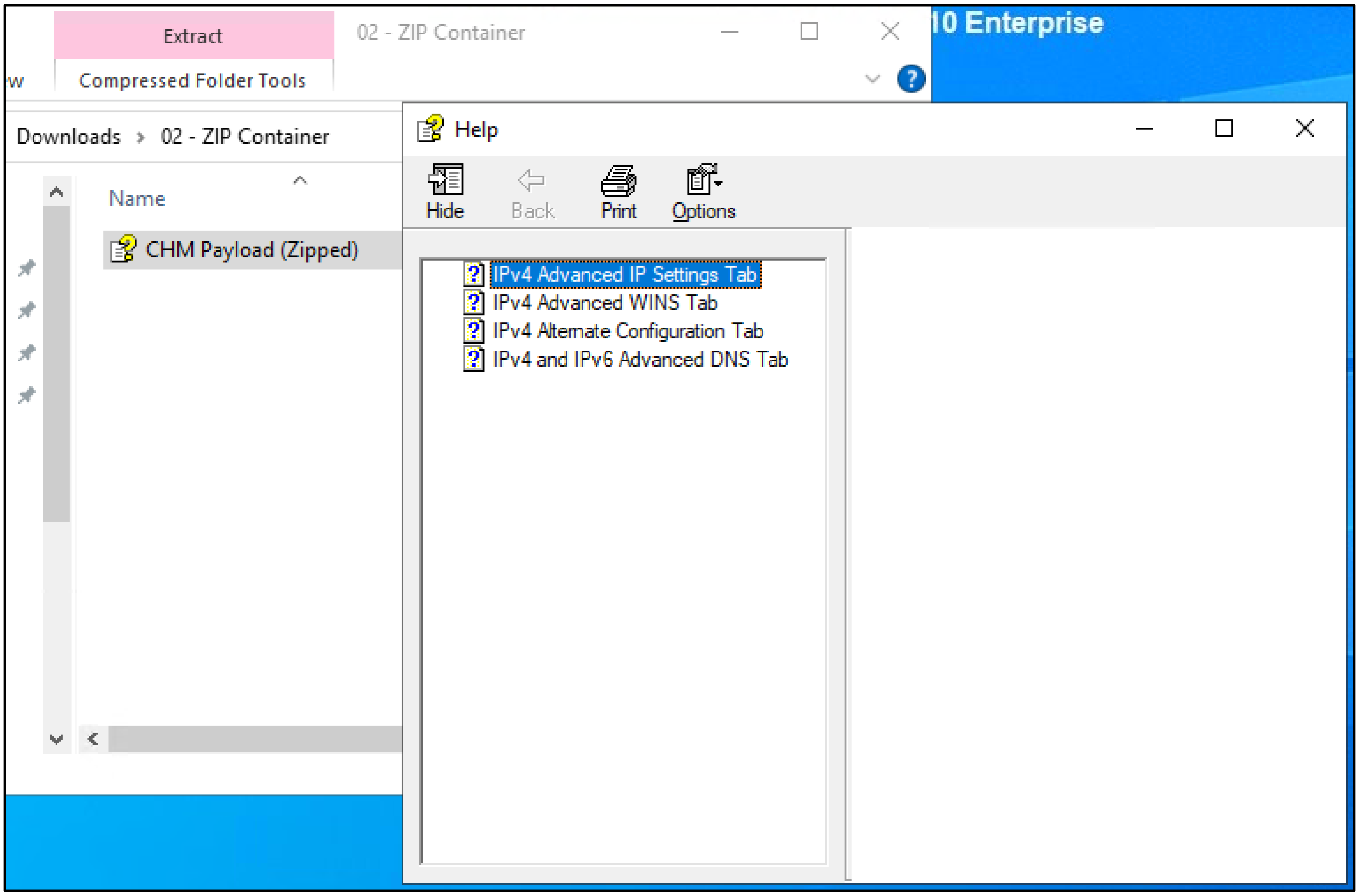
Type: Compiled HTML Help file

From: C:\Users\VMuser\AppData\Local\Temp\Temp1_02 - ZI...

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open this software. What's the risk?

Security Warning Displayed

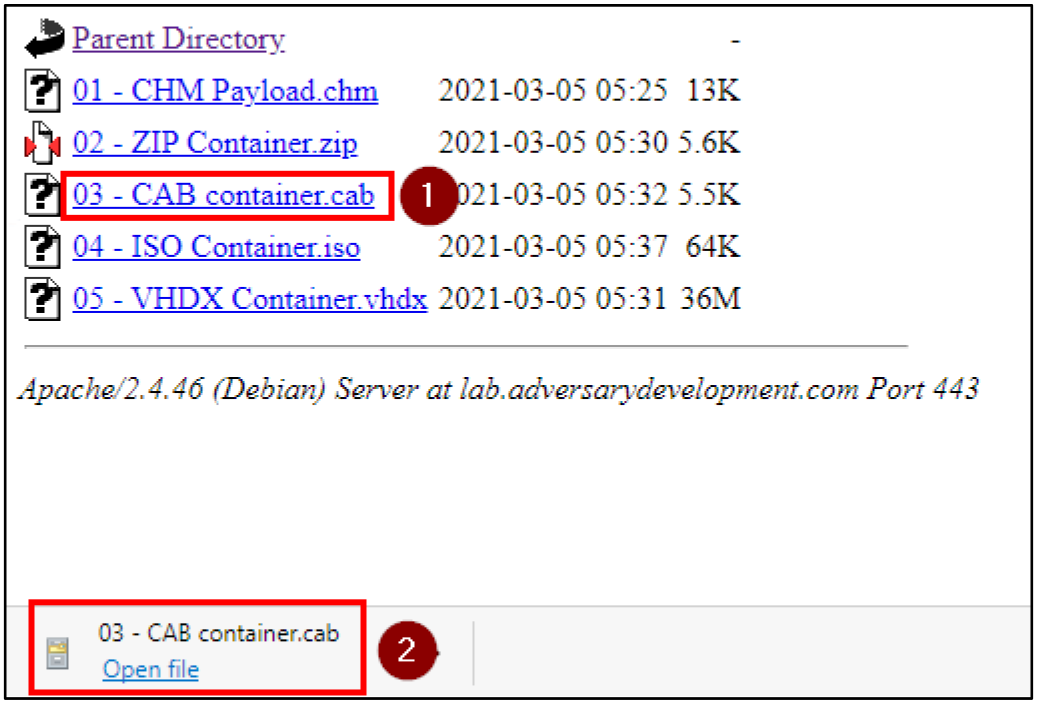
3. When the CHM file opens, you should see something like the screenshot below - a Help window with no text, and no Calculator in sight. This indicates that the ZIP file container is not successful at preventing the MOTW from being applied to our CHM payload file, and as a result, the payload command did not execute.



CHM Opened Without Payload Execution

3. CHM payload delivered inside a CAB file

1. Next, download the CAB container file from the web server, and open the downloaded file. Like with the ZIP file, opening the CAB file does not generate a Security Warning message.

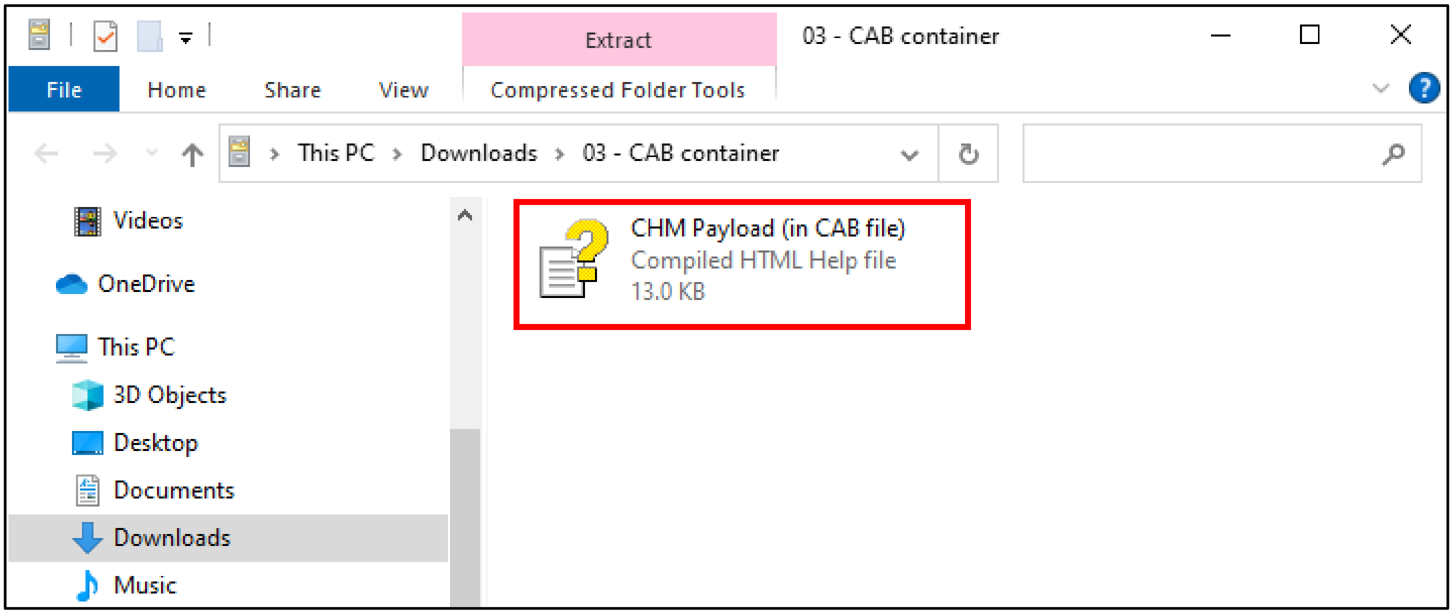


Parent Directory		-
01 - CHM Payload.chm	2021-03-05 05:25	13K
02 - ZIP Container.zip	2021-03-05 05:30	5.6K
03 - CAB container.cab	2021-03-05 05:32	5.5K
04 - ISO Container.iso	2021-03-05 05:37	64K
05 - VHDX Container.vhdx	2021-03-05 05:31	36M

Apache/2.4.46 (Debian) Server at lab.adversarydevelopment.com Port 443

CAB File Downloaded and Opened

2. You'll see that Windows also opens CAB files in Windows Explorer by default - just like ZIP files. Double-click on the CHM payload inside the CAB container to continue.

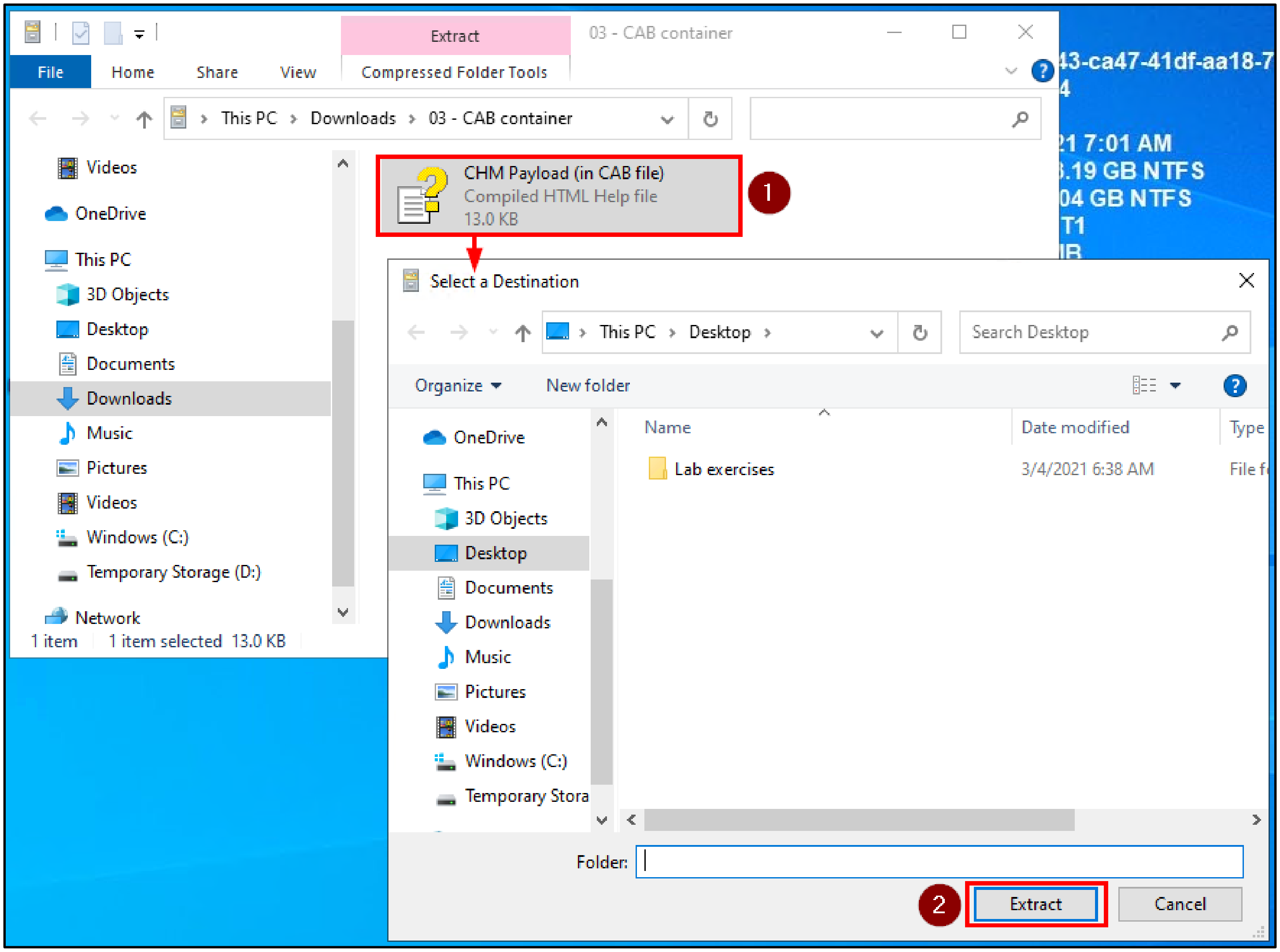


CHM Payload (in CAB file)
Compiled HTML Help file
13.0 KB

Opening CHM File Inside CAB Container

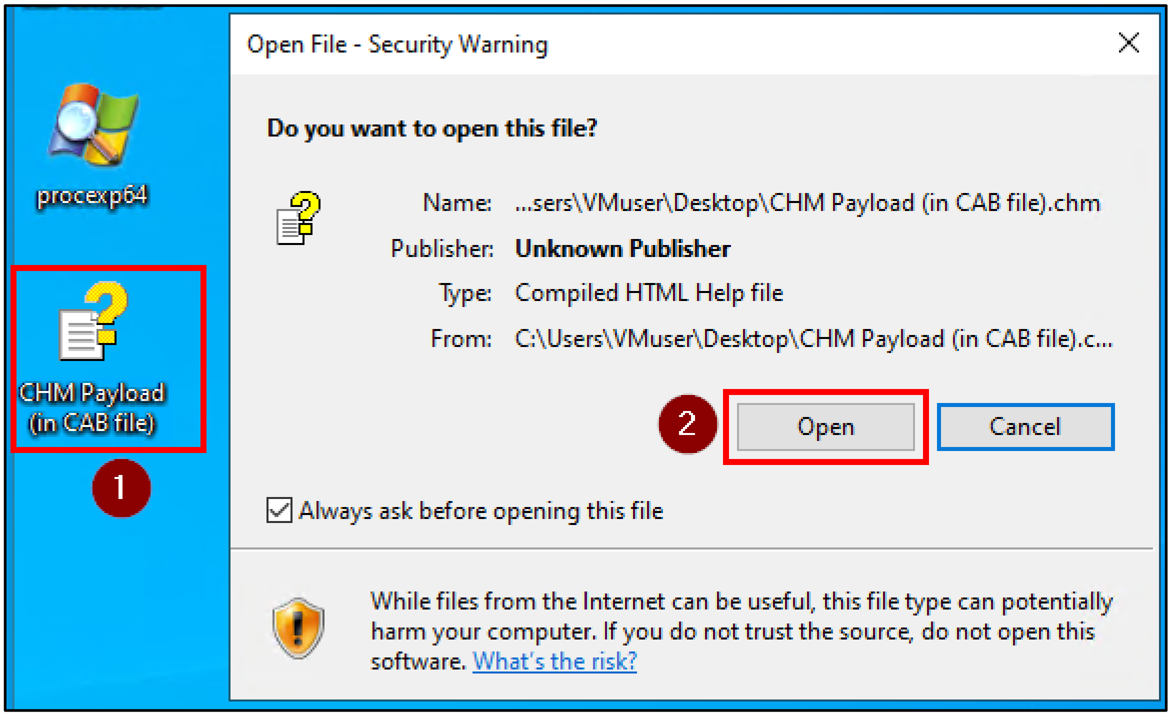
3. After double-clicking the CHM file, you'll notice that CAB files behave differently than other container files. Instead of automatically opening the CHM file, a window appears that prompts the user to select a destination

where the CHM file should be extracted. Make sure the Windows Desktop is selected as your destination, and then click "Extract" to extract the CHM file.



Extracting CHM File to Desktop

4. After extracting the file, double-click the CHM payload that is on your desktop. You'll see the familiar Security Warning appear again - meaning that things aren't looking good for this payload. Click the "Open" button in the Security Warning window to give it a try anyway.



Open File - Security Warning

Do you want to open this file?

Name: ...sers\VMuser\Desktop\CHM Payload (in CAB file).chm

Publisher: **Unknown Publisher**

Type: Compiled HTML Help file

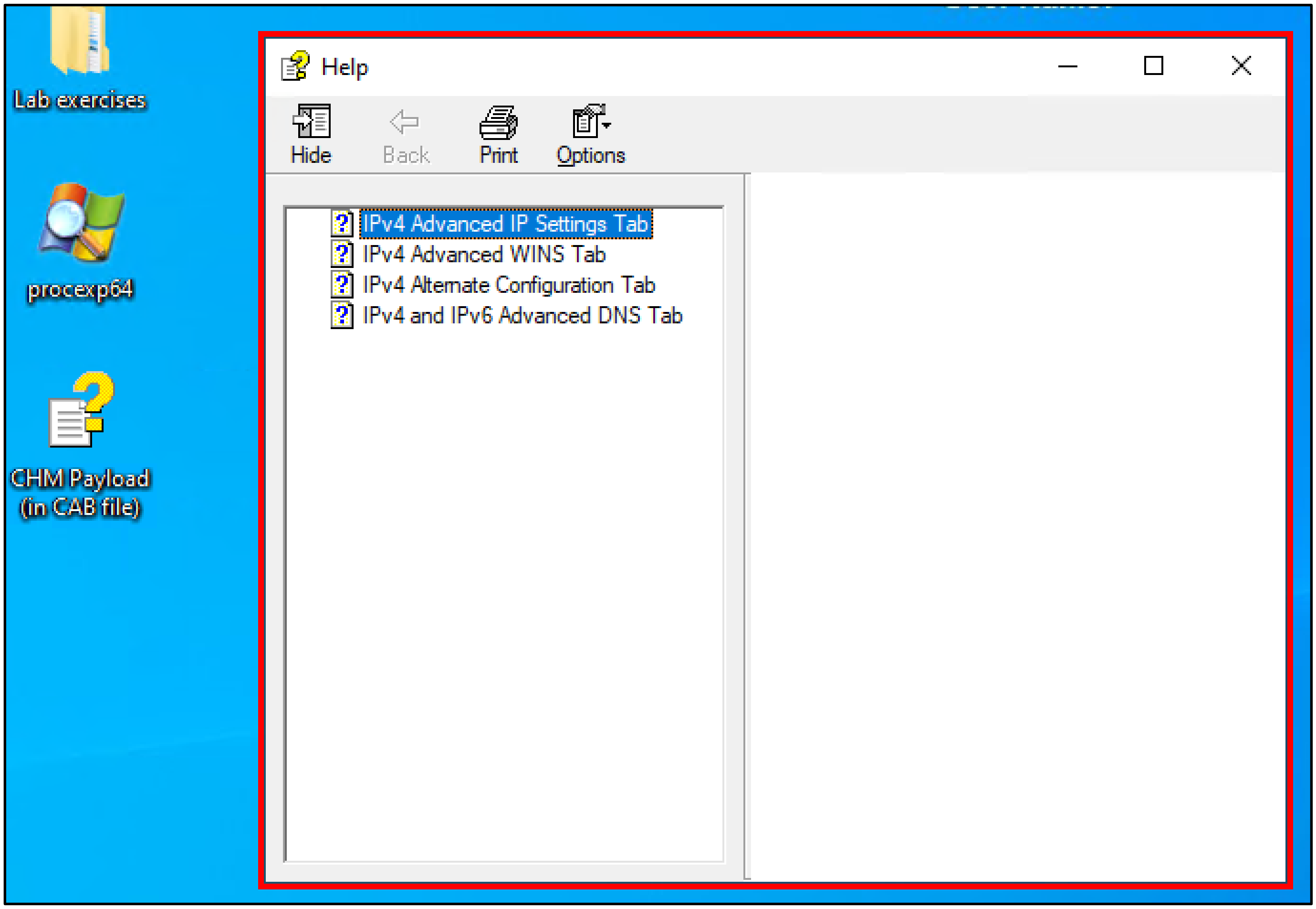
From: C:\Users\VMuser\Desktop\CHM Payload (in CAB file).c...

☑ Always ask before opening this file

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open this software. What's the risk?

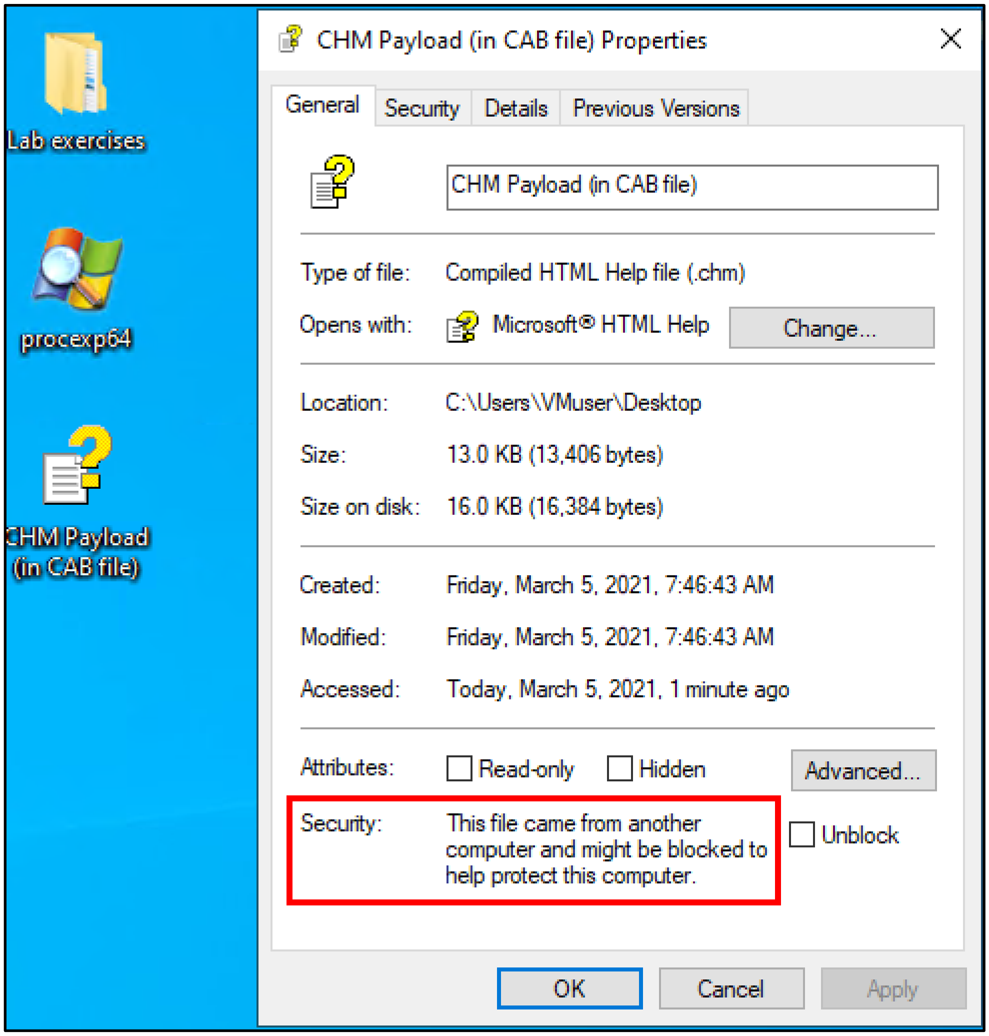
Opening the Extracted CHM File

5. As before, an empty Help window is displayed and the Windows Calculator is not. Payload execution was unsuccessful.


Lab exercises
procexp64
CHM Payload (in CAB file)
Help
Hide
Back
Print
Options
IPv4 Advanced IP Settings Tab
IPv4 Advanced WINS Tab
IPv4 Alternate Configuration Tab
IPv4 and IPv6 Advanced DNS Tab

CHM Opened Without Payload Execution

6. If you're interested, you can right-click on the CHM file on your desktop, and view its properties to confirm that the MOTW is present. Therefore, CAB files are also not suitable for bypassing MOTW.



CHM Payload (in CAB file)

Type of file: Compiled HTML Help file (.chm)

Opens with: Microsoft® HTML Help

Location: C:\Users\VMuser\Desktop

Size: 13.0 KB (13,406 bytes)

Size on disk: 16.0 KB (16,384 bytes)

Created: Friday, March 5, 2021, 7:46:43 AM

Modified: Friday, March 5, 2021, 7:46:43 AM

Accessed: Today, March 5, 2021, 1 minute ago

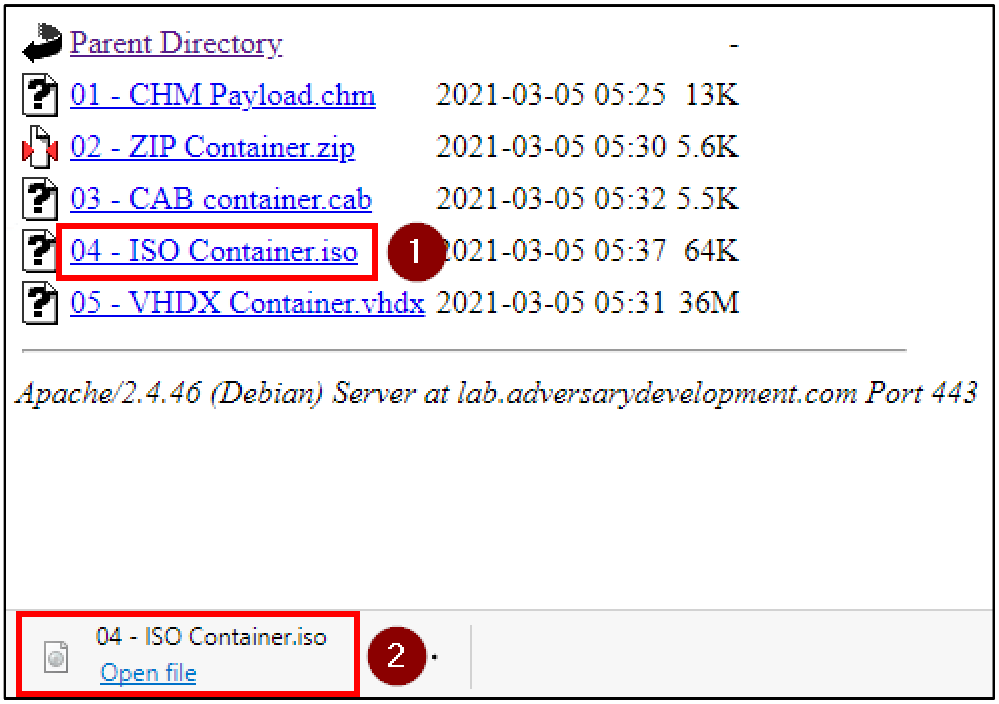
Attributes: □ Read-only □ Hidden

Security: This file came from another computer and might be blocked to help protect this computer. □ Unblock

Mark of the Web Present on Extracted CHM File

4. CHM payload delivered inside an ISO file

1. Download the ISO container file from the web server, and open the downloaded file. Like with the two previous container files, opening the ISO file does not generate a Security Warning message.



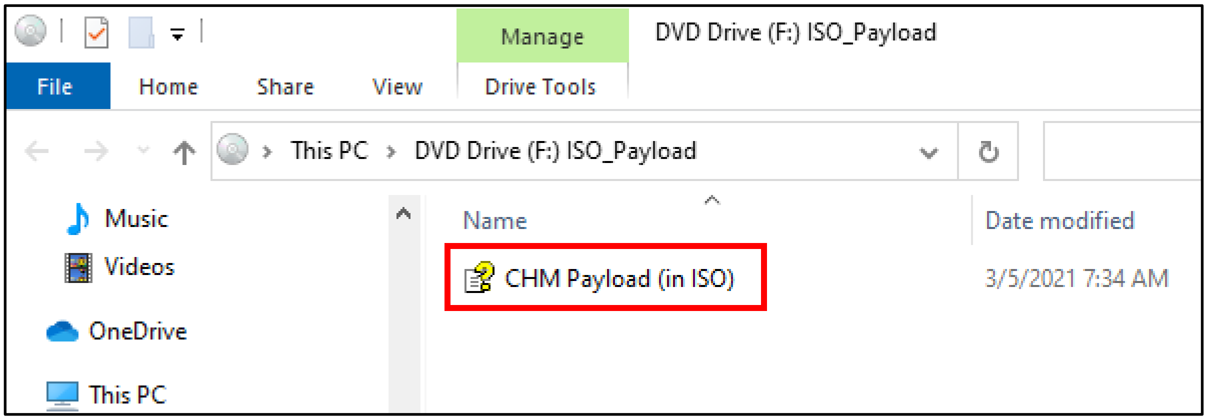
```
Parent Directory                                    -
01 - CHM Payload.chm        2021-03-05 05:25  13K
02 - ZIP Container.zip      2021-03-05 05:30 5.6K
03 - CAB container.cab      2021-03-05 05:32 5.5K
04 - ISO Container.iso      2021-03-05 05:37  64K
05 - VHDX Container.vhdx    2021-03-05 05:31  36M

Apache/2.4.46 (Debian) Server at lab.adversarydevelopment.com Port 443
```

04 - ISO Container.iso
Open file

ISO File Downloaded and Opened

2. You should see the ISO file opened in Windows Explorer. Double-click on the CHM payload inside the ISO container to continue.

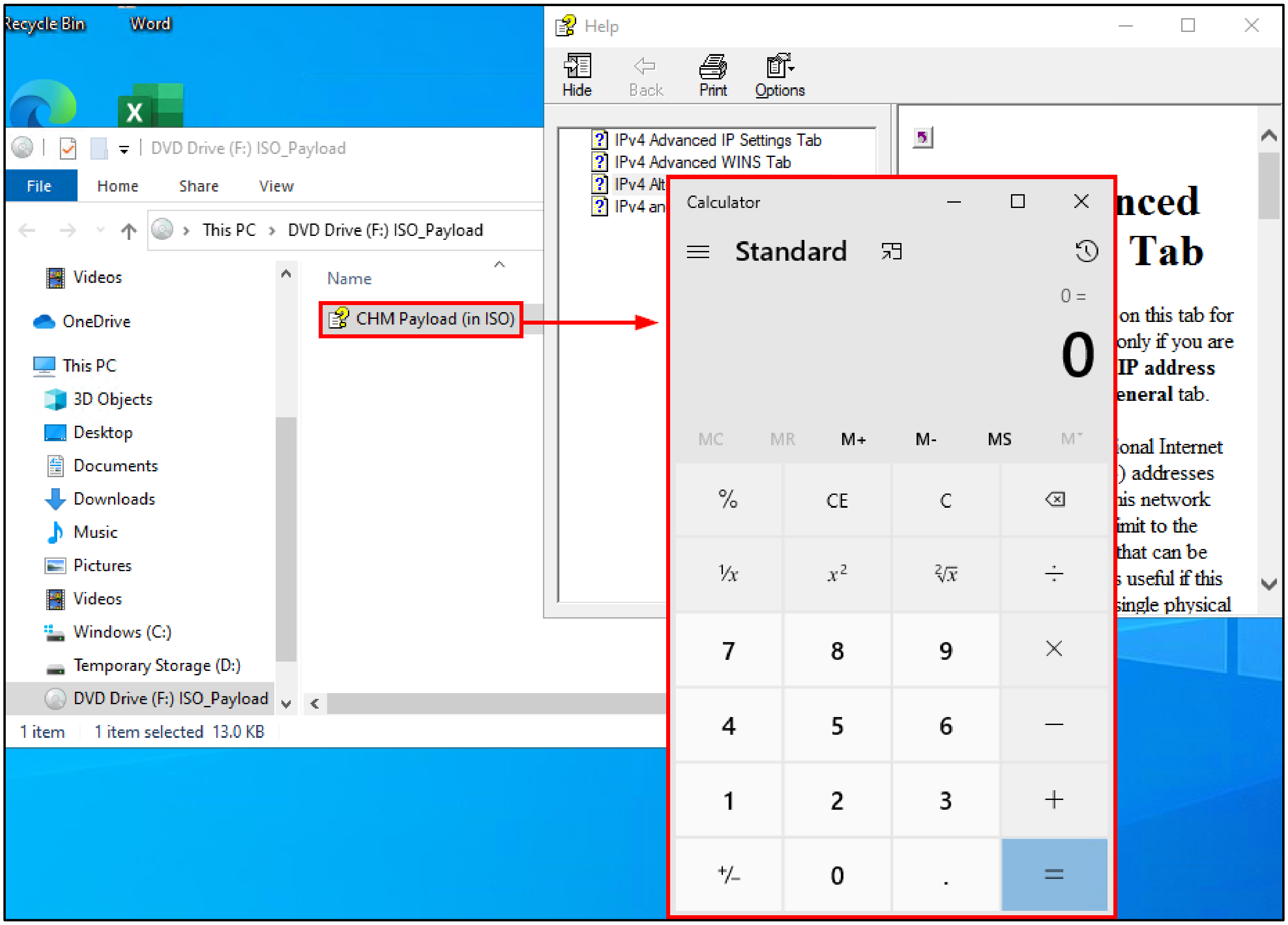


Manage
DVD Drive (F:) ISO_Payload
File
Home
Share
View
Drive Tools
This PC › DVD Drive (F:) ISO_Payload
Music
Videos
OneDrive
This PC

Name	Date modified
CHM Payload (in ISO)	3/5/2021 7:34 AM

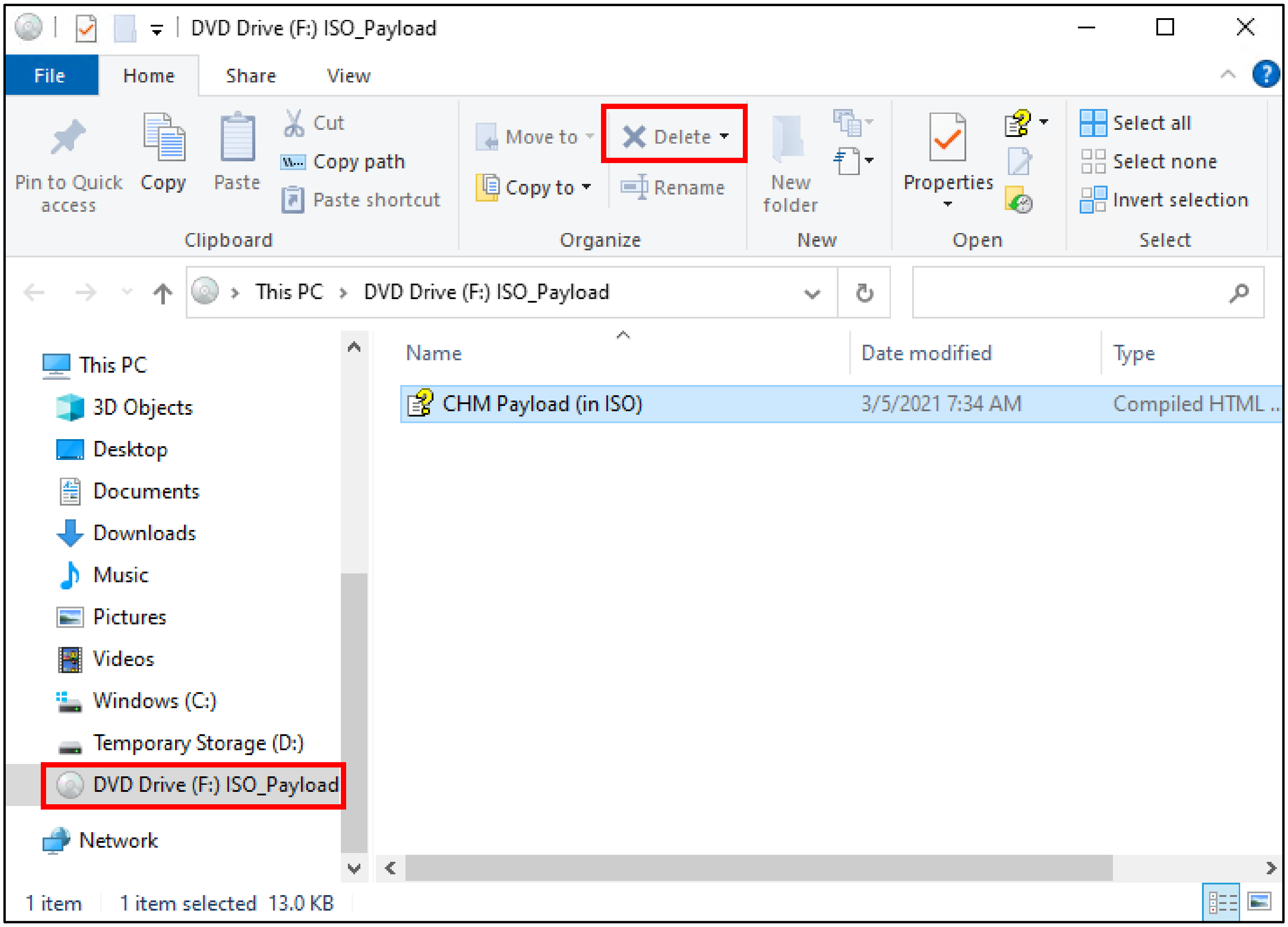
Opening CHM File Inside ISO Container

3. This time when you open the CHM file, you'll notice that no Security Warning appears. And once the file opens, the "calc.exe" command executes and a calculator window appears. Since execution was successful, you've confirmed that ISO files are a viable option for bypassing restrictions imposed by MOTW.



Successful Payload Execution

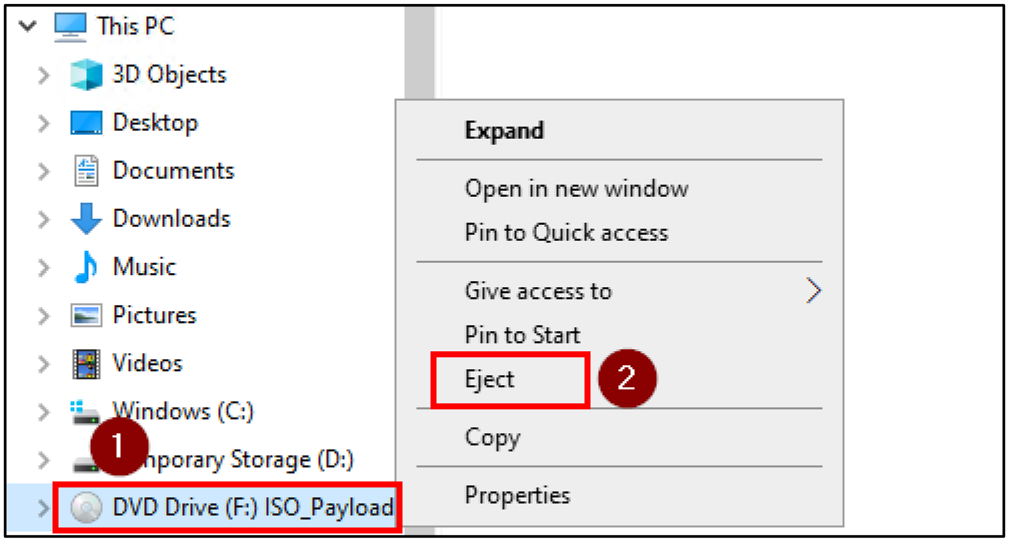
4. Another interesting feature of ISO files is that they are mounted by Windows and behave just like physical CD or DVD discs. And just like real CDs and DVDs, the contents inside mounted ISO images are read-only, as indicated by the disabled "Delete" button when viewing the ISO contents in Windows Explorer.



Name	Date modified	Type
CHM Payload (in ISO)	3/5/2021 7:34 AM	Compiled HTML ..

ISO Mounted Read-Only

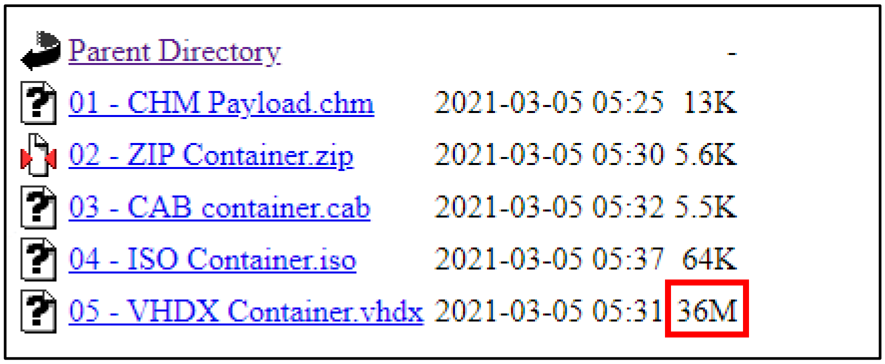
5. Also similar to physical discs, the ISO file cannot be closed until the user "Ejects" it from the computer. Until the image is ejected, the ISO file itself cannot be deleted from the hard drive.



Ejection of ISO File

5. CHM payload delivered inside a VHDX file

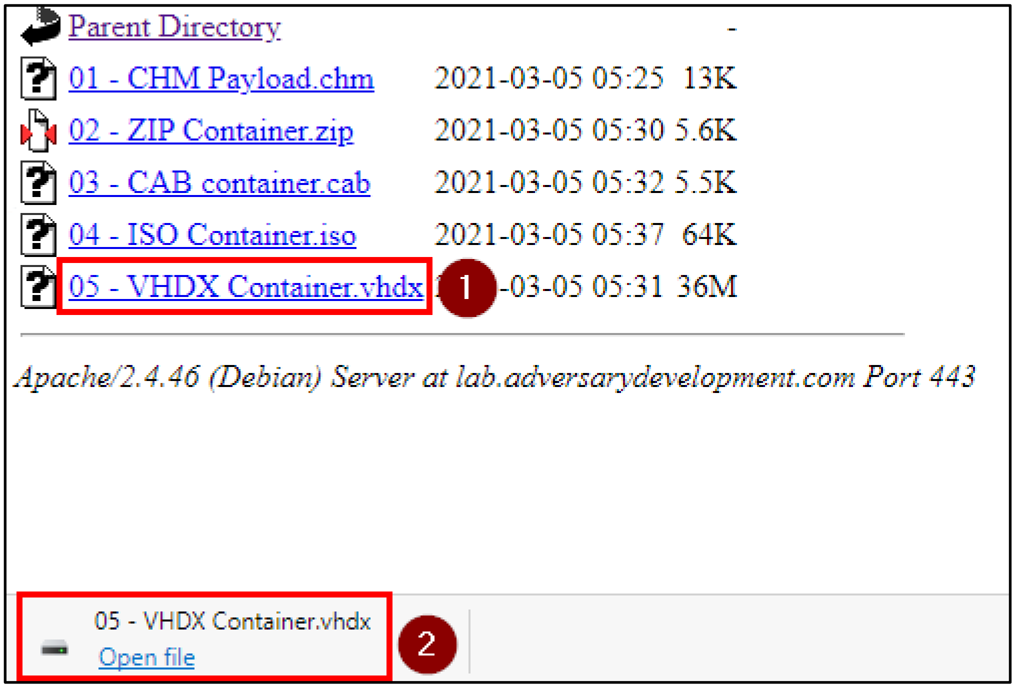
1. The ISO file had a lot of things going for it, so for no reason at all, we'll continue with another container file. Before downloading the VHDX file, you might notice that it is significantly larger than all the other files we've tested so far. Depending on your ruse and the speed of your target's Internet connection, this could be an advantage or a disadvantage.



Parent Directory		-
01 - CHM Payload.chm	2021-03-05 05:25	13K
02 - ZIP Container.zip	2021-03-05 05:30	5.6K
03 - CAB container.cab	2021-03-05 05:32	5.5K
04 - ISO Container.iso	2021-03-05 05:37	64K
05 - VHDX Container.vhdx	2021-03-05 05:31	36M

VHDX File Size

2. Download the ISO container file from the web server, and open the downloaded file.



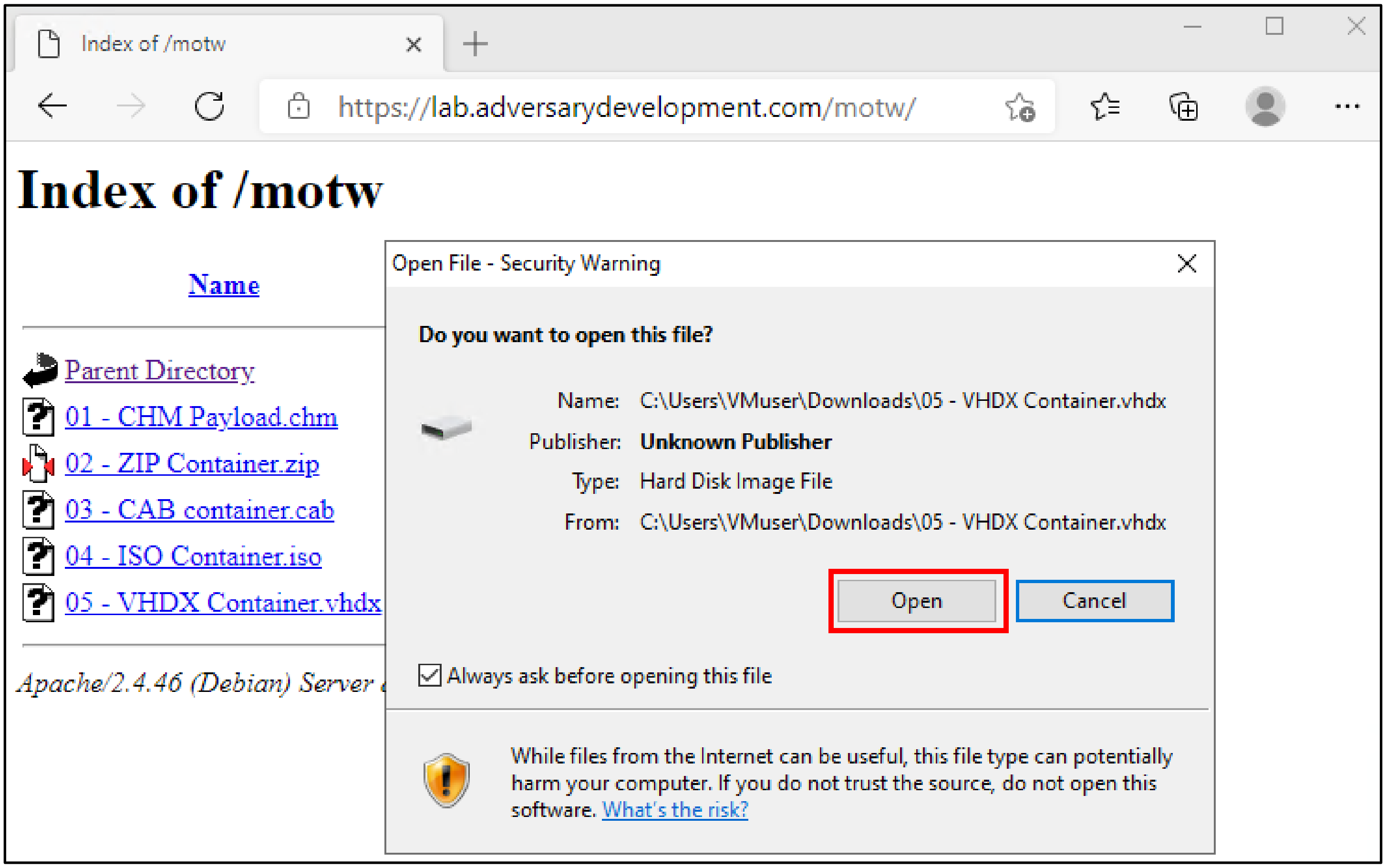
```
Parent Directory                              -
01 - CHM Payload.chm       2021-03-05 05:25  13K
02 - ZIP Container.zip     2021-03-05 05:30 5.6K
03 - CAB container.cab     2021-03-05 05:32 5.5K
04 - ISO Container.iso     2021-03-05 05:37  64K
05 - VHDX Container.vhdx     -03-05 05:31  36M
```

Apache/2.4.46 (Debian) Server at lab.adversarydevelopment.com Port 443

05 - VHDX Container.vhdx
Open file

VHDX File Downloaded and Opened

3. Unlike the previous container files, opening the VHDX file does generate a Security Warning message. However, that only indicates that the MOTW is being applied to the VHDX file itself - not necessarily the contents inside. Click "Open" to continue opening the VHDX file.



Index of /motw

Name

Parent Directory
01 - CHM Payload.chm
02 - ZIP Container.zip
03 - CAB container.cab
04 - ISO Container.iso
05 - VHDX Container.vhdx

Apache/2.4.46 (Debian) Server

Open File - Security Warning

Do you want to open this file?

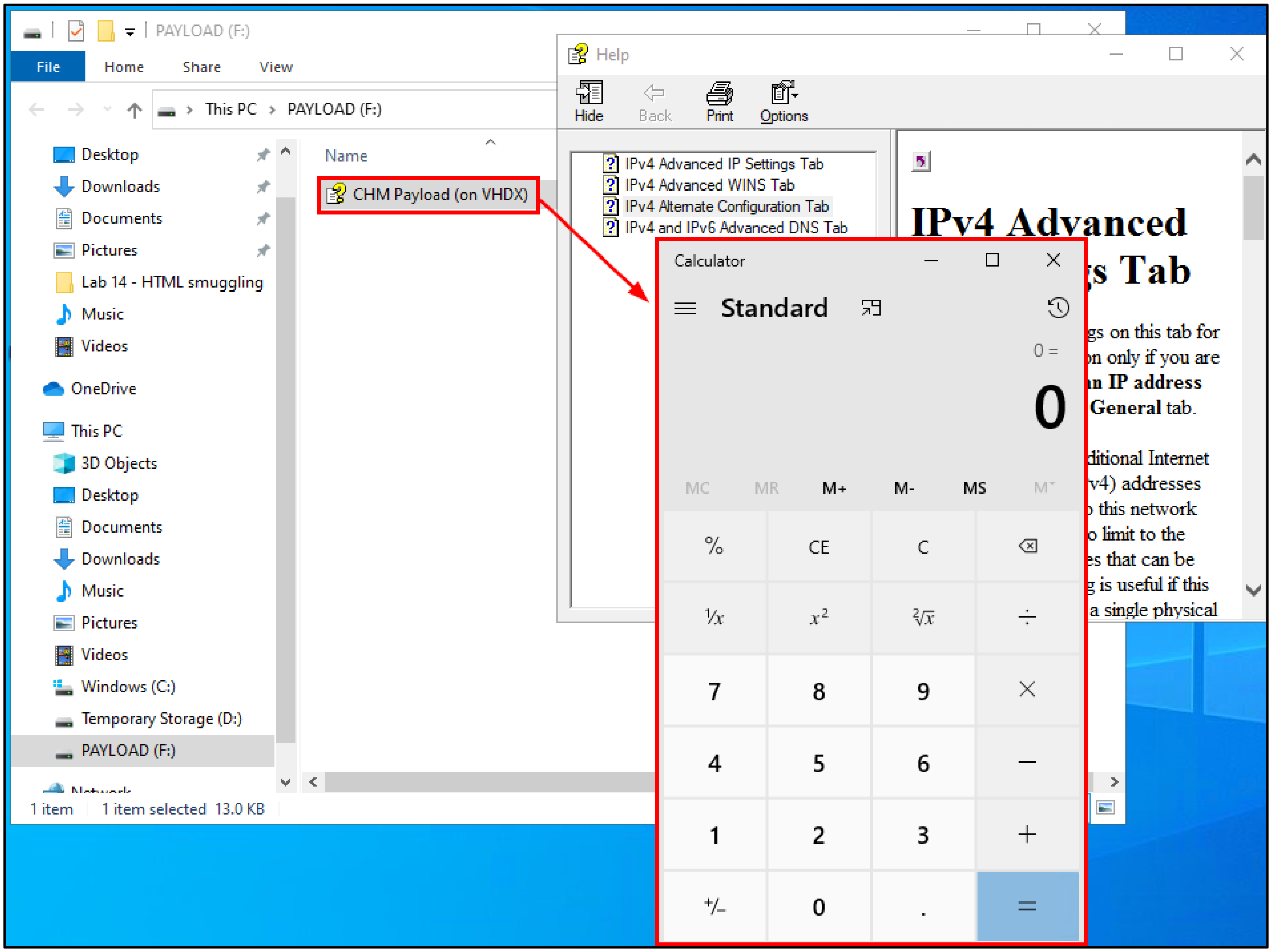
Name: C:\Users\VMuser\Downloads\05 - VHDX Container.vhdx
Publisher: **Unknown Publisher**
Type: Hard Disk Image File
From: C:\Users\VMuser\Downloads\05 - VHDX Container.vhdx

☑ Always ask before opening this file

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open this software. What's the risk?

Security Warning Generated by VHDX File

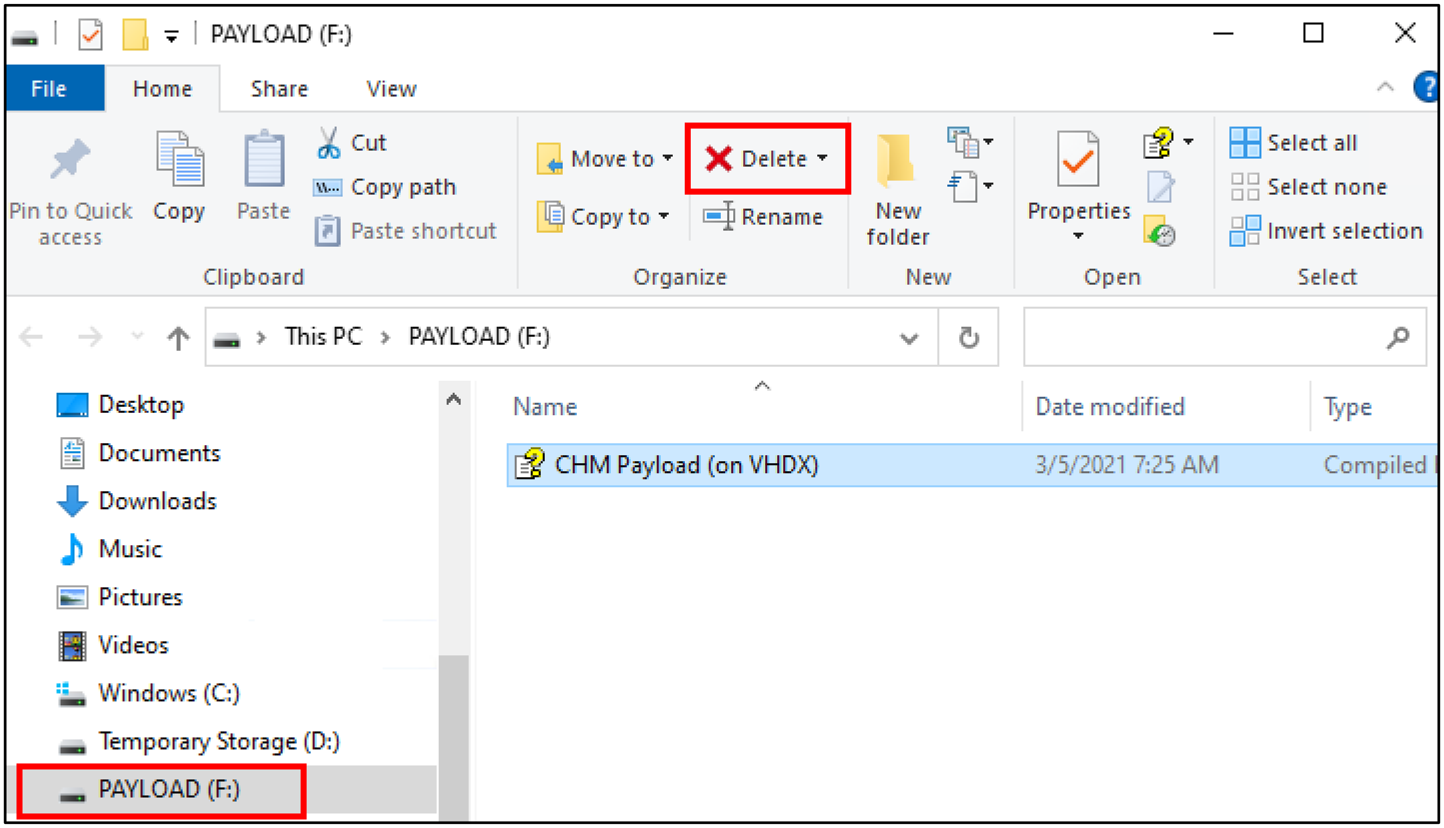
4. The VHDX file should open in Windows Explorer, and you should see the CHM payload file inside. Double-click on the CHM payload file, and when you do, you should see the Calculator program successfully executed by the Help document. It looks like VHDX files are also a viable option for bypassing MOTW.



Successful Payload Execution

5. Like ISO files, VHDX files are disk images. But instead of optical disc images, VHDX files are mounted as removeable hard disks. The VHDX file must be ejected before it can be deleted from disk, but it's contents can

be deleted or modified by the end user. Again, this can be advantageous or disadvantageous depending on the situation.



Name	Date modified	Type
CHM Payload (on VHDX)	3/5/2021 7:25 AM	Compiled

VHDX Mounted as a Read-Write Filesystem

Additional resources

- Nishang "Out-CHM.ps1" script