**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.

**Text

Description automatically generated**

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

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

Press enter.

Find the IP address for your eth0 adapter.

Text

Description automatically generated

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>.

Text

Description automatically generated

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.

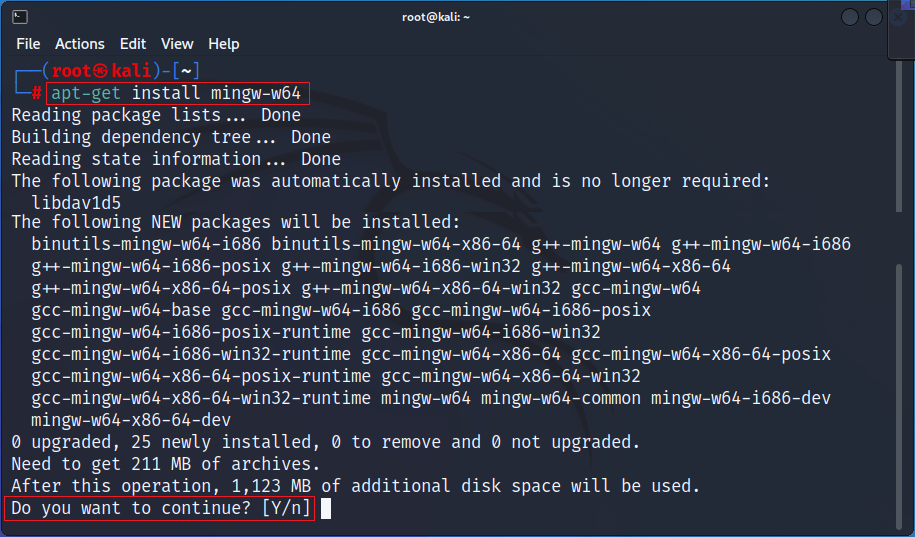
**Begin the lab**

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.

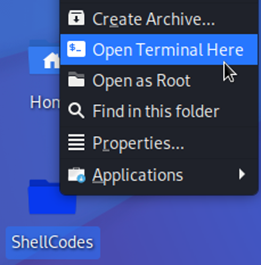
We will first need to install Mingw-w64 first before we can compile any exploit for Windows on our Kali Linux.

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

apt-get install mingw-w64



Once the installation has completed, Right-click on your working folder from your Kali desktop, and from the context menu, select, **Open terminal here**.



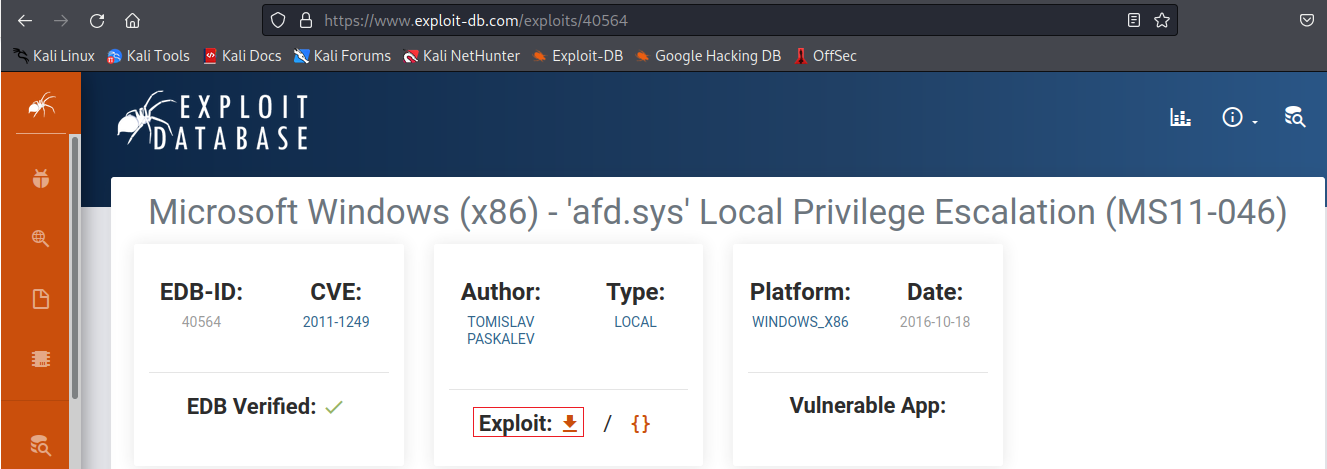
Now that we have Mingw-w64 installed, we can compile our Window exploit. For this lab, we will be compiling a Windows exploit written in c to exploit the CVE-2011-1249 (MS11-046) vulnerability in Windows 7.

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.

Form 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 web page. The exploit will be saved to your download folder.

Graphical user interface, text

Description automatically generated

From the right of your browser’s taskbar, Open your downloads folder.

Graphical user interface, text, application

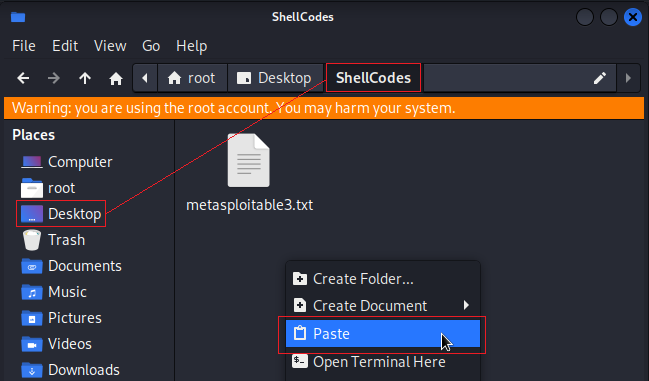
Description automatically generated

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

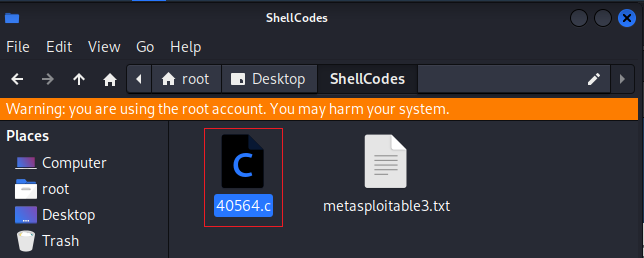
Graphical user interface, application

Description automatically generated

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.



Closeout your working folder and return to your terminal prompt.

Graphical user interface, application, website

Description automatically generated

At your kali prompt, type of copy and paste the following at the prompt.

**x86\_64-w64-mingw32-gcc 40564.c -o exploit.exe -lws2\_32**

Graphical user interface, text, application

Description automatically generated

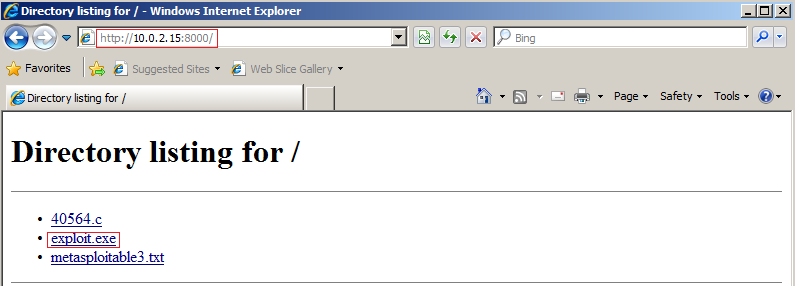
From the Desktop of your Kali machine, right-click on your working folder, and from the context menu, select, **Open terminal here**.

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.



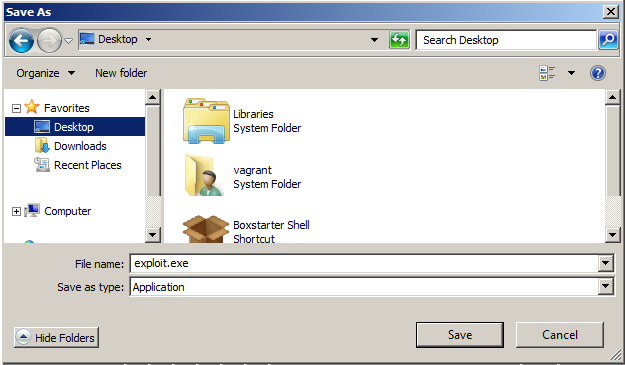
Find the compiled exploit from the directory listing inside your Python3 Simple HTTP Server.

Right-click and from the context menu, select Save target as.

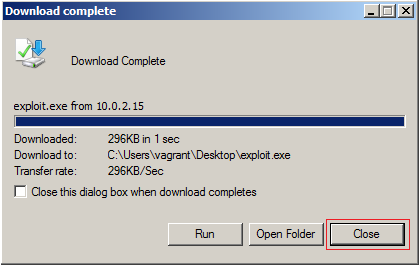
Graphical user interface, text, application

Description automatically generated

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**

A black screen with white text

Description automatically generated with low confidence

Press enter. The script completes successfully.

The prompt, type, **whoami**.

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

Text

Description automatically generated

**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’ll 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.