Exercise 05: Drupal

Jan-Matthias Braun

06. of October, 2022

Penetration testing exercise using metasploit on Drupal. The exercise targets the Drupal web application framework running under Linux in the metasploitable 3 image.

In this lab we use the Kali machine (for penetration testing) and the vulnerable machine is the metasploitable Ubuntu Linux image. We'll

- target a specific service
- research a known vulnerability
- exploit it
- and look into metasploit tools for the post-exploitation phase

Please note that all questions (full lines/bullet points) marked with † should be answered in the report.

Background

Powerup Metasploitable3-Ubuntu and Kali. Using the browser in Kali, navigate to the webpage for that server, i.e., http://<Ubuntu's_IP>

What's behind "drupal/"? (Wikipedia on Drupal)

As a pentester, you want to find out if there are known security issues for Drupal. Searching with searchploit we see there are possible exploits.

```
kali@kali:~# searchsploit Drupal
```

But there are many and they are for specific versions. Seeing that we do not know the version for Drupal running on the server, going through each of them will take time.

As searchsploit returns many results (Figure 1), let's try metasploit, to find out which exploits will be readily available

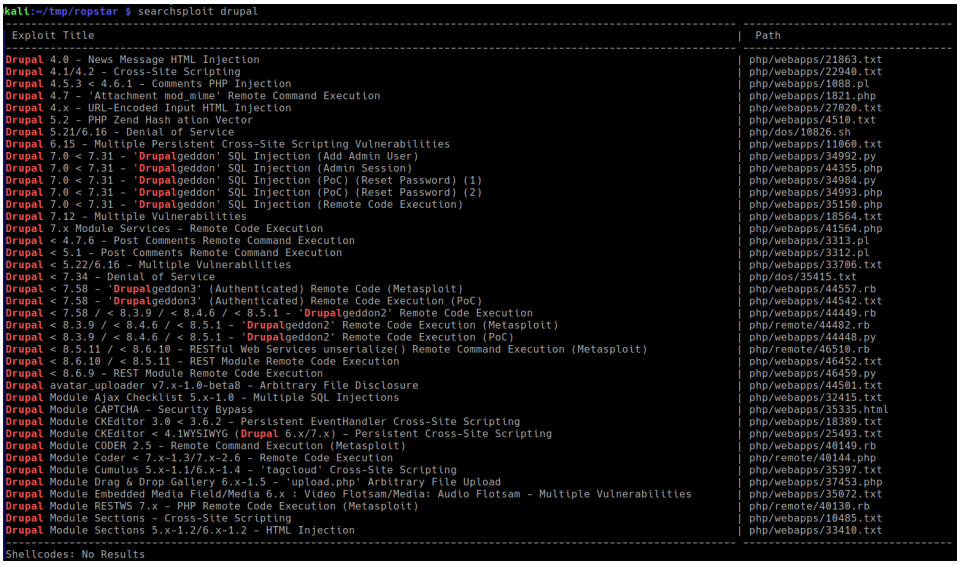

Figure 1: Searchsploit returns many issues with Drupal.

```
kali@kali:~# msfconsole
msf6 > search drupal
```

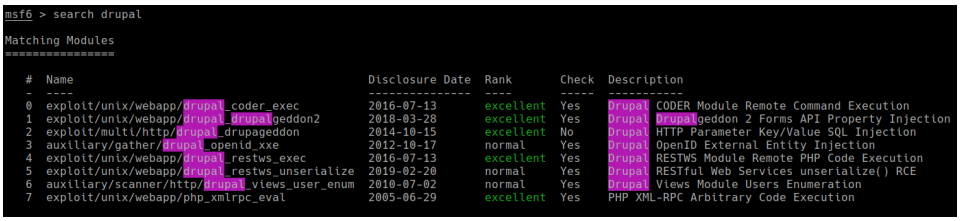

Figure 2: The number of available exploits for Drupal in metasploit is more accessible.

That's way less to go through (Figure 2). Let's start investigating exploits with an "excellent" rating which is not too far off, time wise, and see what its all about. I.e., using the list of exploits in metasploit, check dates which might be relevant for the drupal version, use the "info" command and read the "Description" about the relevant modules which have a good rating.

```
msf6 > info exploit/multi/http/<exploit-name>
```

Questions:

- †Which vulnerabilities do you think can be used? Pick two potential vulnerabilities and describe them in terms of why you picked them, i.e., date and exploit effect.
- †For the rest of the tutorial, we will use the vulnerability dubbed *drupageddon*. What is the underlying vulnerability?

- †What is so severe about the issue?

Description: We can even get a shell? Awesome. Lets use the module to pentest Drupal on Metasploitable3-Ubuntu.

Exploitation

Of course, as long as we do not know version numbers, we cannot say if the exploit will work without testing. But staying in the date regime we are confident that the issue was current at the time the image was built. Let's try it out.

```
msf > use exploit/multi/http/drupal_drupageddon
```

Now... you have used metasploit before. Complete the pentesting and run the module. Hint: Besides IPs and Port numbers, you also need the target URI (the relative URL). Figured out what it is?

When all works well, you will get a meterpreter session open. This will indicate that you have remote access to the server.

```
meterpreter >
```

Good luck!

Post-Exploitation

When you do have the meterpreter session, you can use the help command to see the commands that you can run. Alternatively, you can run metasploits "post" modules to execute additional functions. Post modules are used to execute further commands when you have gained access into the system (which you have done). To see post modules for linux you need to open a separate terminal and start metasploit again. At the "msf6 >" prompt, you can then just enter "search post/linux". For Windows you would search "post/windows/"

What I would like you do to is to run a module that will give you system and user information. Here it is.

```
meterpreter > run post/linux/gather/enum_system
```

As you can see all the data extracted from the Ubuntu machine is stored in your Kali machine in the folder "~/.msf4/loot". I.e., "~/" referes to your user's home directory. Don't ask me why msf6 still uses the "~/.msf4" directory. I assume there is no reason. Whatever the reasons, in your terminal, use can use the "cat" command to display plain text files and see all the data the post exploitation script extracted for you, which includes usernames.

Questions:
†What are possible activities/aims for the post-exploitation phase?
†Write out the list in the file that has the "User Accounts"?
†How does having a list of user names help?
†What do the excellent post exploitation scripts for linux offer?

Reflection

Questions:

- †What is the main issue with the web server? How did it help selecting potential exploits?
- †When opening the drupal web page, you are greeted by a warning. Do you think this is good practice? Why or why not?
- †Given a more restrictive web server configuration, finding the relevant information wouldn't have been that easy. Please check *dirbuster*, to be found in the "Web Application Analysis" menu. How could this tool help you finding information? Try it out on the Ubuntu metasploitable VM. Use */usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt* as dictionary.
- †How can effective spying with tools like *dirbuster* be prevented?
- †This attack didn't get us all the way to root. How would you continue the pentest? What would be your next actions?
- †Do you have any specific things in mind you would try to get root access?
- †What makes getting a remote shell so powerful?