

Backdoor | Difficulty : Easy |

Synopsis :

Backdoor is a low-level Linux machine hosting a Wordpress blog with an installed plugin vulnerable to a directory traversal exploit. This enables us to read the files in the /proc directory and identify the gdbserver that is running on one of the server's ports. To gain access, an RCE exploit for gdbserver can be used.

Furthermore, it is discovered that a screen session is running on the system after analysing the processes running on it.

root privileges are being used. Connecting to this screen session grants root access.

Enumeration :

1. Nmap Scan

We will start with nmap tool and scan the open ports and services running on the server.



```
nmap -sV -sC 10.10.11.125 --min-rate 1000 -p- -vv
```

```

PORT      STATE SERVICE REASON  VERSION
22/tcp    open  ssh      syn-ack OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_ssh-hostkey:
|_  3072 b4:de:43:38:46:57:db:4c:21:3b:69:f3:db:3c:62:88 (RSA)
|_ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQDqz2EAb2SBSzEIXcu+9dzgUZzDJGdCFWjwuxjhwtppq3sGiUQ1jgwf7h5BE+ALYhSX0oqo
OLPKA/QHLxvJ9sYz0iJBL7aEJU8tYHchYMCMu0e8a71p3UGiRtjn2tBVe3RSCo/XRQOM/ztrBzLqLKHCqMpttqJHphVA0/1dP7uoLCJLA00Wn
W0K311DXkxf0iKRc2izbgfgimMDR4T1C17/oh9355TBgGGg2F7AooUpdtsahsiFiTcRkvVB1G7DQiGqRTWsFaKBkHPVMQFaLEm5DK9H7PRwE+
UYCah/Wp95NkwWj3u3H93p4V2y0Y6kdjF/L+BRmB44XZxm2Vu7BN0ouuT1SP3zu8YUe3FHshFImL7Ac/8zL1twLpnQ9Hv8KXnNKPoHgrU+sh3
5cd0JbCqyPFG5yziL8smr7Q4z9/XeATKzL4bcjG87sGtZMtB8aLQS7yFA6wmqyWqLFQ4rpi2S0CoslyQnighQSwNaWuBYXvOLi6AsgckJLS44
L8LxU4J8=
|_  256 aa:c9:fc:21:0f:3e:f4:ec:6b:35:70:26:22:53:ef:66 (ECDSA)
|_ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBiUoNkiwo7nM8ZE767bKSHJh+RbMsbItjT
bVvKK4xKMfZFHZroaLEe9a2/P1D9h2M6khvPI74azqcqni8SUJAK=
|_  256 d2:8b:e4:ec:07:61:aa:ca:f8:ec:1c:f8:8c:c1:f6:e1 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIB7eoJSCw4DyNNaFftGoFcX4Ttpwf+RPo0ydNk7yfqca
80/tcp    open  http      syn-ack Apache httpd 2.4.41 ((Ubuntu))
|_http-generator: WordPress 5.8.1
|_http-methods:

```

Based on the nmap scan, we can see that the SSH service is running on port 22 and the apache web server is running a wordpress site on port 80.

Furthermore, a port 1337 is open, but nmap is unable to verify the service is operational. It appears to be intriguing.

Using the whatweb tool, we confirm that the wordpress website is running on port 80.

```

(shiv@kali)-[~]
└─$ whatweb backdoor.htb
http://backdoor.htb [200 OK] Apache[2.4.41], Country[RESERVED][ZZ], Email[wordpress@example.com], HTML5, HTTP
Server[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], IP[10.10.11.125], JQuery[3.6.0], MetaGenerator[WordPress 5.8.1]
, PoweredBy[WordPress], Script, Title[Backdoor 8#8211; Real-Life], UncommonHeaders[link], WordPress[5.8.1]

```

the wordpress 5.8.1 version is detected.

Website Enumeration :

The website home page looks like a wordpress blog.

THE NEW UMOMA OPENS ITS DOORS

The premier destination for modern art in Northern Sweden. Open from 10 AM to 6 PM every day during the summer months.



Works and Days

August 1 – December 1

[Read More](#)

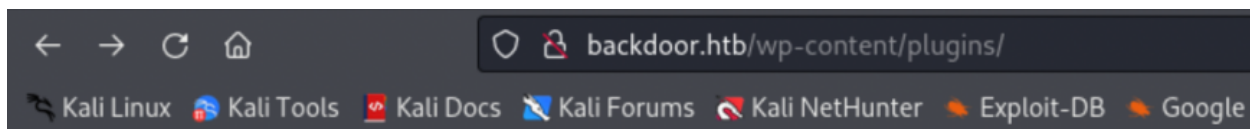
The Life I Deserve

August 1 – December 1




[Read More](#)

After browsing through , we did not get a useful information. We further move the manually looking a standard wordpress directory.

We found a `"/web-content/plugins"` directory. In which `ebook-download` plugin is install.

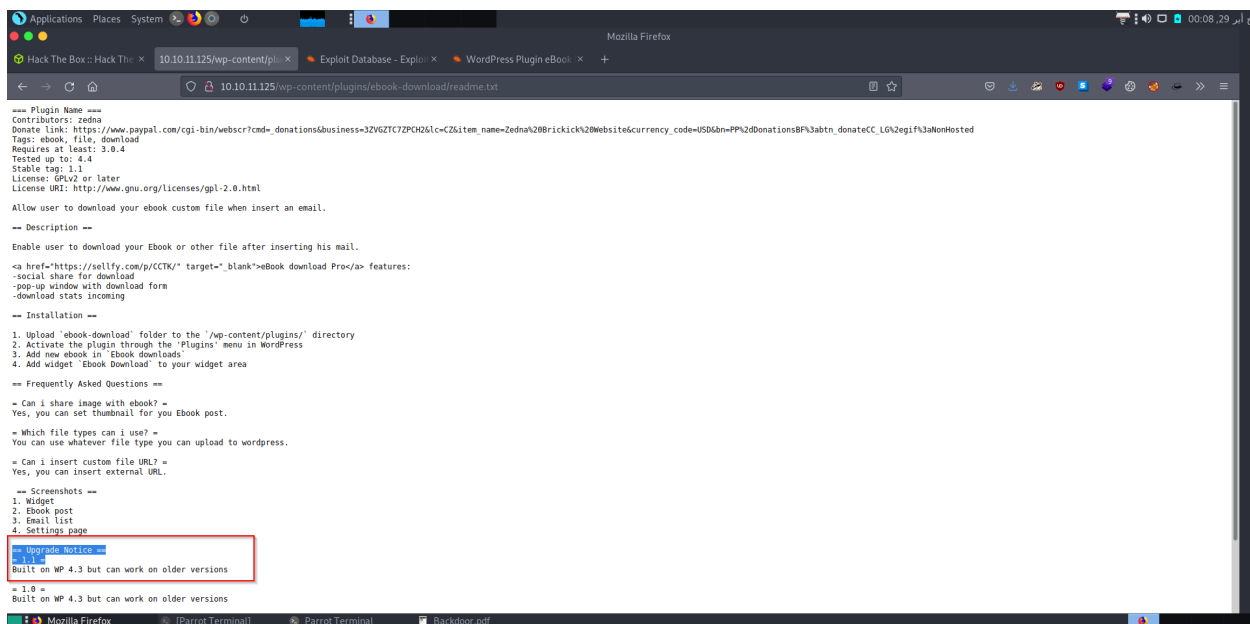


Index of /wp-content/plugins

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 ebook-download/	2021-11-10 14:18	-	
 hello.php	2019-03-18 17:19	2.5K	

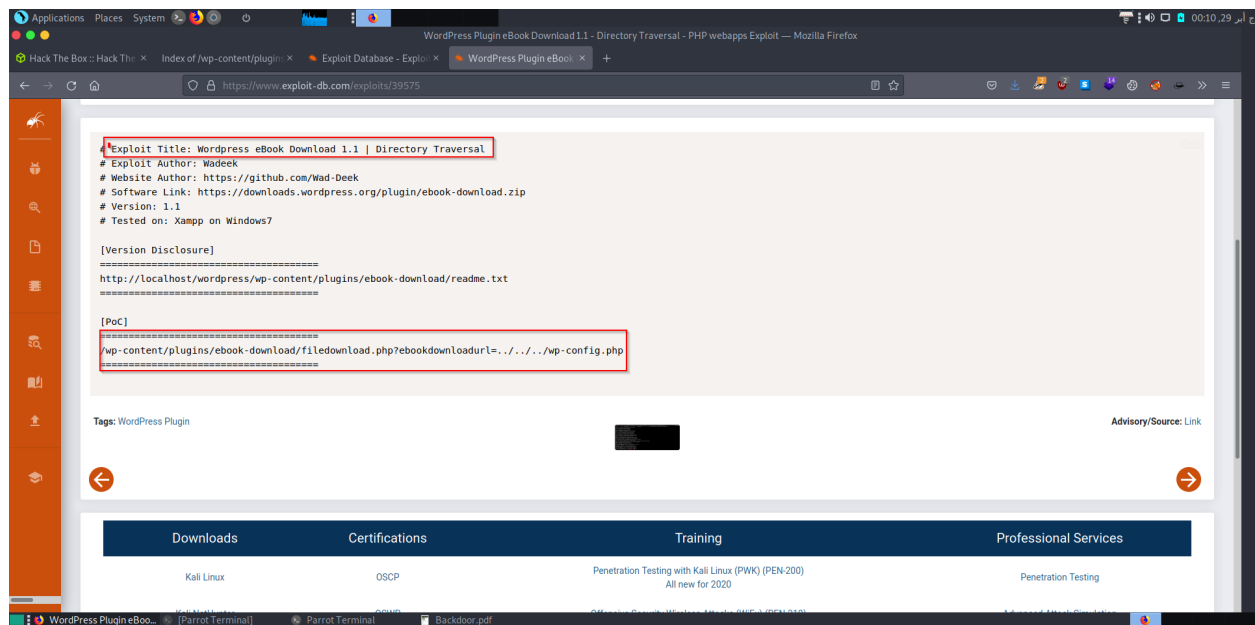
Apache/2.4.41 (Ubuntu) Server at backdoor.htb Port 80

Getting digger into directories, we get a readme.txt and it reveals the version 1.1



Exploitation :

As we have the plugin version info. We try to use some googling technique to find the available exploit of this particular version.



And We found a LFI(Local File Inclusion) vulnerability in this plugin version.

What is LFI ?



LFI is a web vulnerability caused by mistakes made by a programmer of a website or web application. If an LFI vulnerability exists in a website or web application, an attacker can include malicious files that are later run by this website or web application.

As the PoC suggests, we must navigate to the specified URL and specify the target file to be read using the ebookdownloadurl parameter.

When dealing with a Wordpress blog, one of the most important files is wp-config.php, which typically contains database credentials and other sensitive configuration information. Let's go to backdoor.htb/wp-content/plugins/ebook-download/filedownload.php?

ebookdownloadurl=../../wp-config.php

In the wp-config.php file, the following Database credentials were revealed.

```
DB_NAME = wordpress
DB_USER = wordpressuser
DB_PASSWORD = MQYBJSaD#DxG6qbm
```

We were able to read the specified target file after browsing to the target URL, indicating that the directory traversal exploit was successful. We found the user admin and password but login unsuccessful.

Coming back to the port 1337 which was found to be open by the Nmap scan, we notice that attempts to

access it with telnet and netcat are unsuccessful.

Since we have LFI and so we can read the files on the remote server there is one possible way to potentially

find some useful information about the service on port 1337. This can be done by brute forcing the

/proc/{PID}/cmdline file.