Ex0f0 Report

Benjamin Ruddy

2022-11-22

Contents

Goal

The goal in this exercise is to exploit a Linux machine using a recent vulnerability.

Technical Report

Finding: *Vulnerable version of sudo in combination with illegitimate system binary allows for regular user privilege escalation*

Severity Rating: 8.0

CVSS Base Severity Rating: 8.0 AV:A AC:L PR:L UI:N S:C C:H I:H A:L

Vulnerability Description

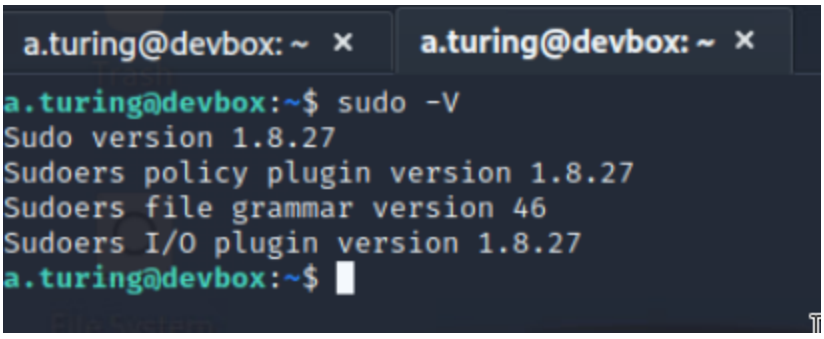
This vulnerability consists of two elements coming together to provide a user a pathway to privilege escalation:

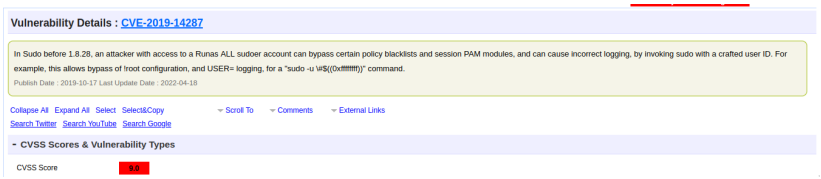
1) The /bin/ps binary on devbox.artstailor.com is edited to execute log the usages of the command, outputting them to a.turing's home directory, upon which the real /bin/ps is then executed (renamed to "realps")

2) With the outdated version of sudo on this machine (see screenshots below) a user may input the `-u#-1` argument to execute the specified command they are allowed to execute as per `/etc/sudoers` as root, even if the command in the sudoers file does not specify root as a user they may run the command as.

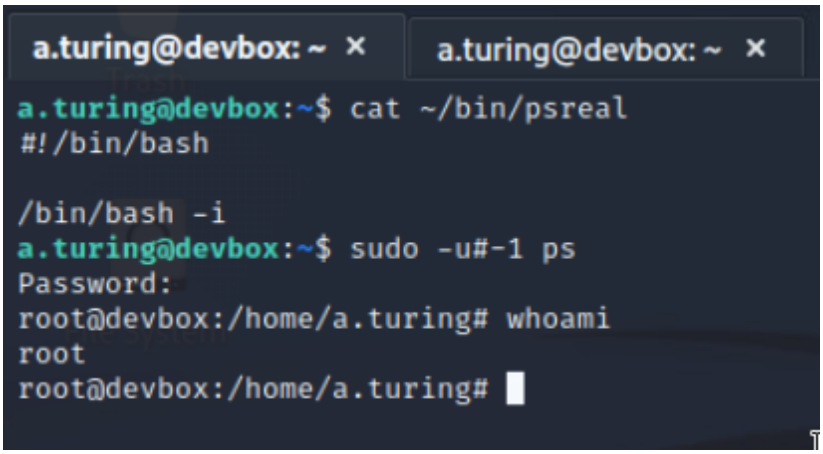
As a result, a malicious low-permissions user can make a script in a directory they have control over, name it psreal, and change their environment variable to that directory so that when they run "ps", their malicious program gets executed.

Confirmation method




Vulnerability Details : CVE-2019-14287
In Sudo before 1.8.28, an attacker with access to a Runas ALL sudoer account can bypass certain policy blacklists and session PAM modules, and can cause incorrect logging, by invoking sudo with a crafted user ID. For example, this allows bypass of !root configuration, and USER= logging, for a "sudo -u \#$((0xffffffff))" command.
Publish Date : 2019-10-17 Last Update Date : 2022-04-18
Collapse All Expand All Select Select&Copy Scroll To Comments External Links
Search Twitter Search YouTube Search Google
- CVSS Scores & Vulnerability Types
CVSS Score
9.0

6_ps_sus.png



Mitigation or Resolution Strategy

It is urgent that the correct version of the ps binary gets restored, and that sudo gets updated immediately on devbox.artstailor.com

User a.turing should be inspected for questioning.

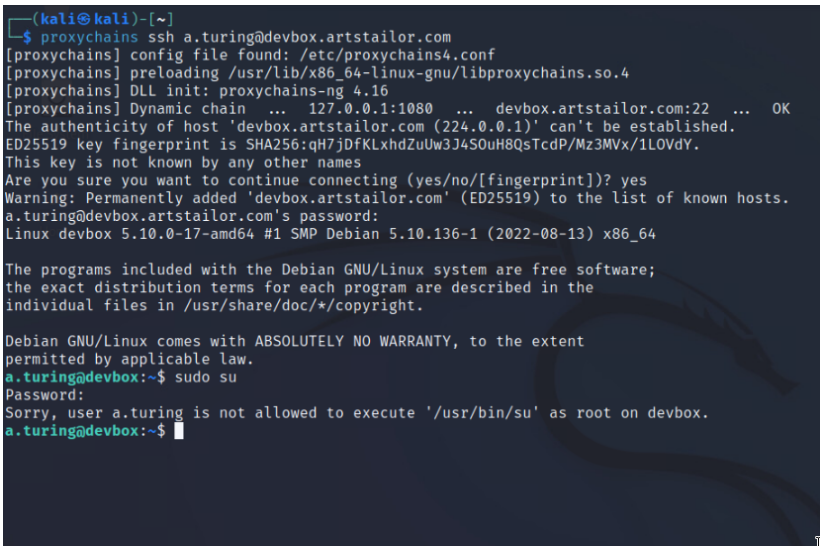
Attack Narrative

Pivoting with a SOCKS proxy through costumes machine

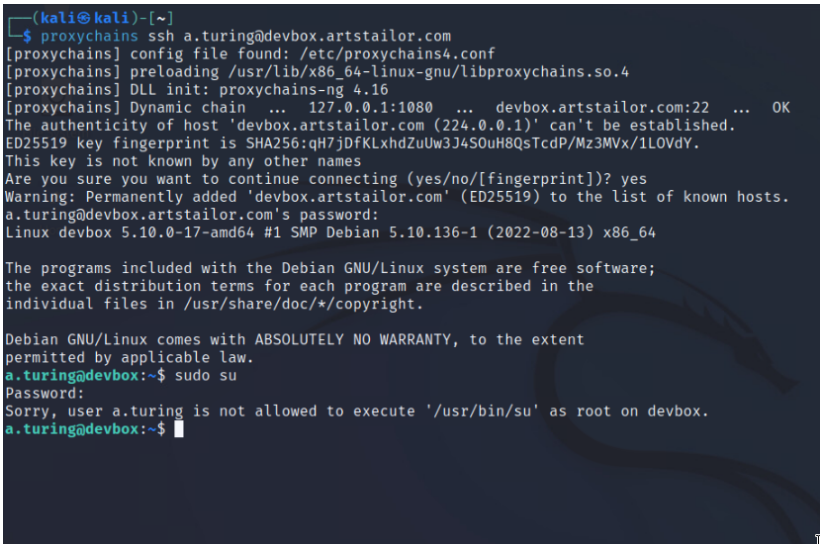
We do the same procedure as in Ex0e0 and Ex0d0 to get access to devbox, by first using our Administrator account on `costumes.artstailor.com` to copy our Chisel executable, and then using proxychains to SSH into `devbox.artstailor.com`.

Getting on devbox again

Once we are back on devbox, we see, as described by our exercise briefing, that we don't have the same `sudo` root permissions as we did before:

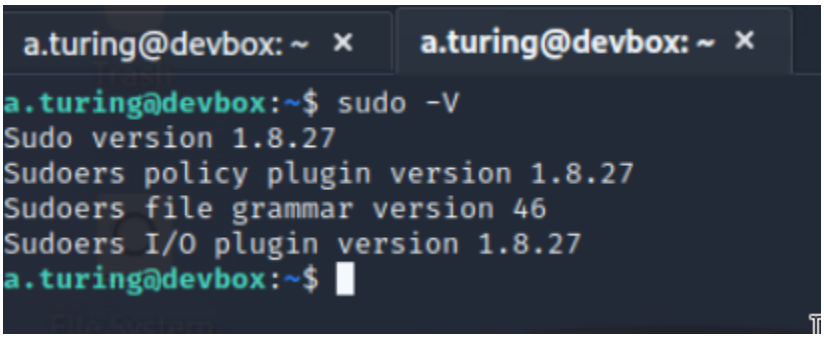


Looking at the `/etc/suoders` file, we can see the reason why – we don't have permissions to run any command as root anymore. Furthermore, the file says that the one command we can run as other users than a.turing, we can't even run as root:

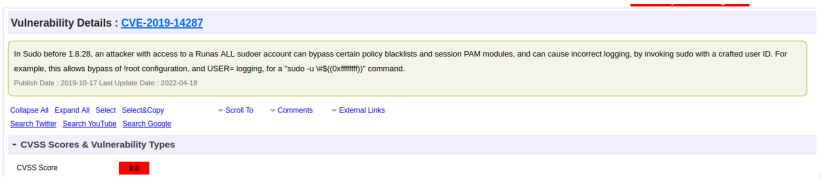


Privilege escalation

With the peculiar sudo changes that were made, we check the version of sudo with `sudo -V` to try and get some ideas for pvrivilege escalation:



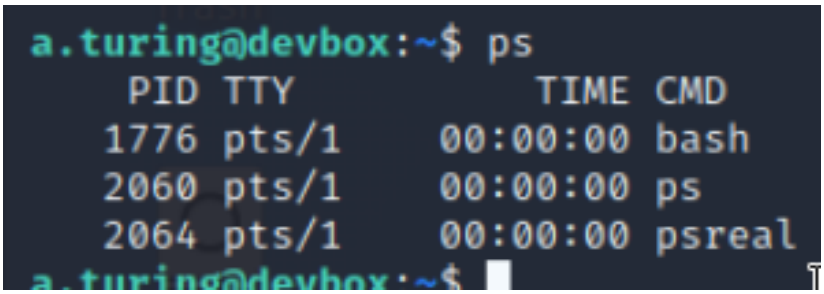
From our previous class knowledge, we know that this version of sudo is in fact vulnerable to CVE-2019-14287:



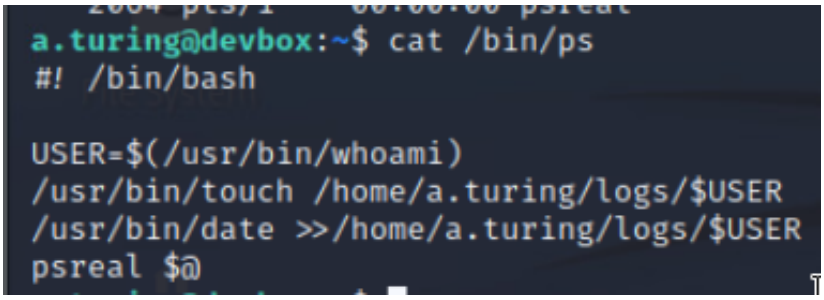
With this, we know that we can abuse the parsing of this particular version of sudo to run the `ps` command as root with the following command:

```
sudo -u#-1 ps
```

Normally, running the ps command as root wouldn't give us much to do, but when running the command, we see something suspicious about this ps binary:



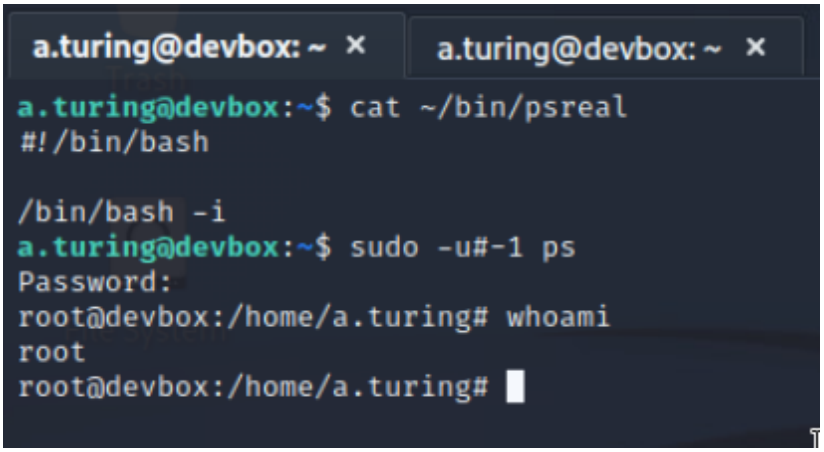
Opening the ps binary, we see it is actually a bash script that a.turing seems to have replaced the original ps with:



Here we seem to have gotten lucky, because this script executes another command, which we can redirect to our own custom command by using the Linux PATH environment variable. Since we can run this 'ps' script as root with the sudo vulnerability, we can effective run any command as root.

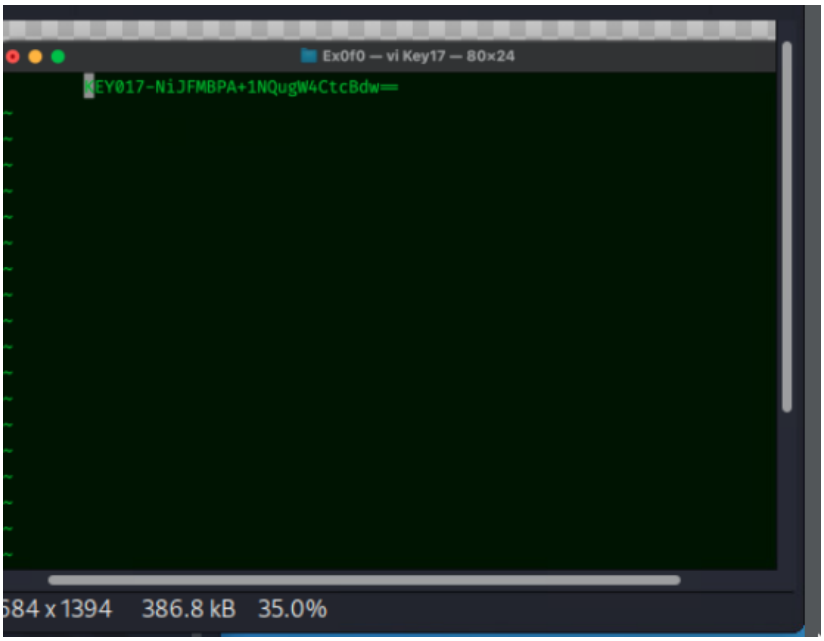
The following is our `$PATH$`:

With the way that this was set up by a.turing, commands inputted in the terminal without specifying a directory will first be searched for in `/home/a.turing/bin/` Thus, we simply make a script titled "psreal" that switches us to the root user:



KEY017

In the `/root` directory, a file named "MyDream.png" exists. By hosting an HTTP server with `python -m SimpleHTTPServer` on devbox, the image can be downloaded on the Kali host and viewed to reveal KEY017:



MITRE ATT&CK Framework TTPs

TA0011: Command and Control
- **T1090:** Proxy
  - **.001:** Internal Proxy

TA004: Privilege Escalation
- **T1548:** Sudo and Sudo Caching
  - **.003:** NA