

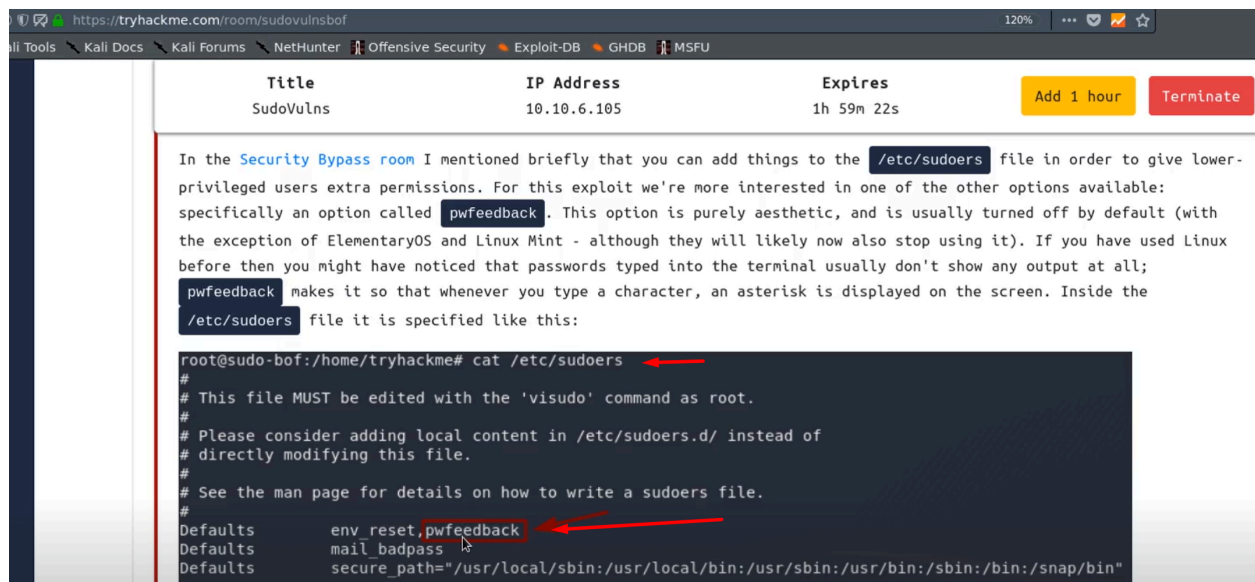


# Sudo Buffer Overflow - THM (Done)

<https://tryhackme.com/r/room/sudovulnsbof>

Resources for this video:

Exploit for CVE-2019-18634 - <https://github.com/saleemrashid/sudo-cve-2019-18634>



https://nvd.nist.gov/vuln/detail/CVE-2019-18634

Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

VULNERABILITIES

## CVE-2019-18634 Detail

**MODIFIED**

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

**QUICK INFO**

**CVE Dictionary Entry:**  
CVE-2019-18634

**NVD Published Date:**  
01/29/2020

**NVD Last Modified:**  
02/07/2020

### Current Description


In Sudo before 1.8.26, if pwfeedback is enabled in /etc/sudoers, users can trigger a stack-based buffer overflow in the privileged sudo process. (pwfeedback is a default setting in Linux Mint and elementary OS; however, it is NOT the default for upstream and many other packages, and would exist only if enabled by an administrator.) The attacker needs to deliver a long string to the stdin of getln() in tgetpass.c.

**Source:** MITRE  
[View Analysis Description](#)

**Severity**

CVSS Version 3.x CVSS Version 2.0

**CVSS 3.x Severity and Metrics:**

 **NIST: NVD** **Base Score: 7.8 HIGH** **Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H**

### References to Advisories, Solutions, and Tools

```
File Edit View Search Terminal Help
tryhackme@sudo-bof:~$ sudo -l
[sudo] password for tryhackme:
Sorry, user tryhackme may not run sudo on sudo-bof.
tryhackme@sudo-bof:~$ cat /etc/sudoers
cat: /etc/sudoers: Permission denied
tryhackme@sudo-bof:~$ sudo -V
Sudo version 1.8.21p2
Sudoers policy plugin version 1.8.21p2
Sudoers file grammar version 46
Sudoers I/O plugin version 1.8.21p2
tryhackme@sudo-bof:~$ ls
exploit
tryhackme@sudo-bof:~$ ./exploit
[sudo] password for tryhackme:
Sorry, try again.
# id
uid=0(root) gid=0(root) groups=0(root),1000(tryhackme)
#
```

sudo -V #always check sudo version and see if we can exploit

When you see "pwfeedback" in "cat /etc/sudoers", we can bufferflow this vuln (CVE-2019-18634). "pwfeedback" is OFF by default but if it is turned on we

can attack this.

What is "pwfeedback"?

If you have used Linux before then you might have noticed that passwords typed into the terminal usually don't show any output at all; "pwfeedback" makes it so that whenever you type a character, an asterisk is displayed on the screen.

This attack can be successful only when the machine has

- Sudo versions 1.7.1 to 1.8.30 inclusive are affected.
- "pwfeedback" must be ON.