HACKING A WEBSITE AND GAINING ROOT ACCESS USING DIRTY COW EXPLOIT

Ameer Pornillos   October 23, 2016

This is a demo on hacking a vulnerable website and gaining root privilege access using Dirty COW (CVE-2016-5195) exploit.

Dirty COW (CVE-2016-5195) is a kernel local privilege escalation vulnerability in the Linux kernel.

As described on Red Hat Customer Portal:

LOOKING FOR SOMETHING?

Search the site

PAST ARTICLES

HackInOS Level 1 (VulnHub): Complete Walkthrough and …

W34kn3ss Level 1 (VulnHub): Complete Walkthrough and …

Metasploit Community CTF 2018: 2 of Diamonds …

ROOTCON 12 CTF Cryforbin 7 and Cryforbin …

Timisoara CTF 2018 Quals Write-Up

@AMEERPORNILLOS TWEETS

CVE-2016-5195

*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.*

This could be abused by an attacker to modify existing setuid files with instructions to elevate privileges. An exploit using this technique has been found in the wild.

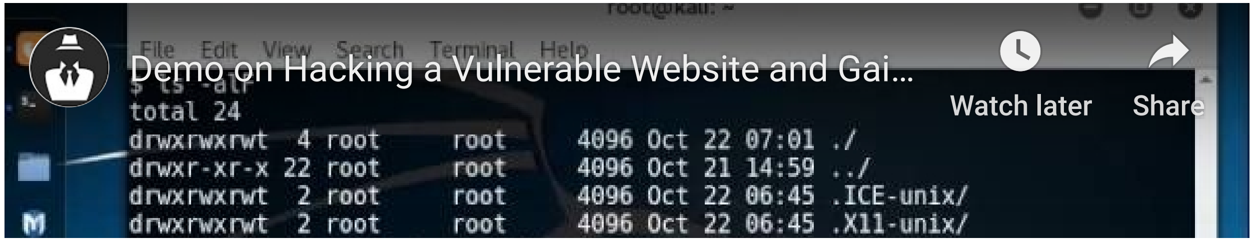
In the demo, the DirtyCOW exploit PoC will be used to escalate privileges of a local user (in this case www-data) thus gaining root or administrator privileges in the vulnerable web server.

- RT @metasploit: Heap overflow exploitation on Windows 10: primer and examples from @_sinn3r https://t.co/cmyyQ7HJGN
  2 days ago
- RT @4nqr34z: pwned Sputnik from @VulnHub by @ameerpornillos nice work! 👍🤓 #CTF https://t.co/ZCLQBWCXDT
  3 days ago
- RT @securityidiots: CollabOzark is a simple tool which helps the researchers track SSRF, Blind XSS, XXE, SQLi, External Resource Access pay…
  17 days ago
- RT @ush1c: https://t.co/uYzRhahssU
  17 days ago
- RT @FlatL1ne: Python3 Burp History parsing tool to discover potential SQL injection points. To be used in tandem with SQLmap. #BurpSuite…
  20 days ago

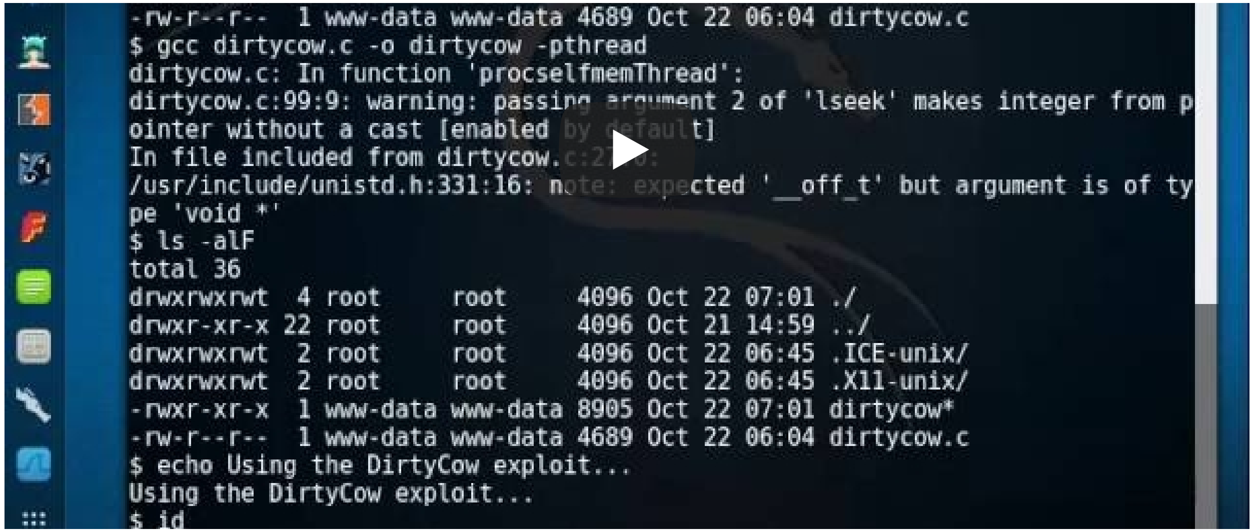
DIRTY COW
Dirty COW (CVE-2016-5195) is a privilege escalation vulnerability in the Linux Kernel

A Dirty COW vulnerable web server was setup in order to show the exploit in action. To better understand how serious the security problem can potentially be, a vulnerable website was also built – designed to be exploited to gain unprivileged local user access.

HACKING A VULNERABLE WEBSITE AND ESCALATING PRIVILEGE USING DIRTY COW (CVE-2016-5195) EXPLOIT DEMO VIDEO


root@kali: ~
File Edit View Search Terminal Help
Demo on Hacking a Vulnerable Website and Gai...
Watch later
Share

```
$ ls -alt
total 24
drwxrwxrwt  4 root     root     4096 Oct 22 07:01 ./
drwxr-xr-x 22 root     root     4096 Oct 21 14:59 ../
drwxrwxrwt  2 root     root     4096 Oct 22 06:45 .ICE-unix/
drwxrwxrwt  2 root     root     4096 Oct 22 06:45 .X11-unix/
```



```
-rw-r--r--  1 www-data www-data 4689 Oct 22 06:04 dirtycow.c
$ gcc dirtycow.c -o dirtycow -pthread
dirtycow.c: In function 'procselfmemThread':
dirtycow.c:99:9: warning: passing argument 2 of 'lseek' makes integer from p
ointer without a cast [enabled by default]
In file included from dirtycow.c:27:0:
/usr/include/unistd.h:331:16: note: expected '__off_t' but argument is of ty
pe 'void *'
$ ls -alF
total 36
drwxrwxrwt  4 root     root     4096 Oct 22 07:01 ./
drwxr-xr-x 22 root     root     4096 Oct 21 14:59 ../
drwxrwxrwt  2 root     root     4096 Oct 22 06:45 .ICE-unix/
drwxrwxrwt  2 root     root     4096 Oct 22 06:45 .X11-unix/
-rwxr-xr-x  1 www-data www-data 8905 Oct 22 07:01 dirtycow*
-rw-r--r--  1 www-data www-data 4689 Oct 22 06:04 dirtycow.c
$ echo Using the DirtyCow exploit...
Using the DirtyCow exploit...
$ id
```

As you can see from the video, the www-data local user has been quickly escalated with root privileges.

You can determine if your system is vulnerable by using this bash script from Red Hat.

List of affected Linux distributions includes: (Note that you can verify or test if your system is vulnerable by using the script above.)

- CentOS Linux 7.x
- CentOS Linux 6.x
- CentOS Linux 5.x
- Debian Linux wheezy
- Debian Linux jessie
- Debian Linux stretch
- Debian Linux sid
- Ubuntu Linux precise (LTS 12.04)
- Ubuntu Linux trusty

- Ubuntu Linux xenial (LTS 16.04)
- Ubuntu Linux yakkety
- Ubuntu Linux vivid/ubuntu-core
- Red Hat Enterprise Linux 7.x
- Red Hat Enterprise Linux 6.x
- Red Hat Enterprise Linux 5.x
- SUSE Linux Enterprise 11
- SUSE Linux Enterprise 12

HOW TO FIX DIRTY COW (CVE-2016-5195) ON LINUX

```
For Debian or Ubuntu Linux:
$ sudo apt-get update && sudo apt-get upgrade && sudo apt-get
```

```
For RHEL / CentOS Linux 5.x/6.x/7.x:
$ sudo yum update
```

```
For RHEL / CentOS Linux 4.x:
$ sudo up2date -u
```

```
For Suse Enterprise Linux or Opensuse Linux:
# zypper patch
```

Reboot your system afterwards, then verify by running the **Dirty COW (CVE-2016-5195) vulnerability checker script** again.

Share 0 Like 0 Tweet Save Share

ABOUT THE AUTHOR

Ameer Pornillos

Ameer is an OSCE, OSCP, I.T. security enthusiast from Philippines. You can find Ameer at LinkedIn and Twitter.

LEAVE A REPLY

Comment Text*

Name*

Email*

Website

□ Save my name, email, and website in this browser for the next time I comment.

□ I'm not a robot

reCAPTCHA
Privacy - Terms

POST COMMENT