Lateral Movement and Pivoting | Linux

Pivoting via SSH Tunneling

- ssh *user*@*TARGETIP* -D 9050 (The socks4 proxychains port | /etc/proxychains.conf)
- The *TARGETIP* should be the IP of the pivot machine, not the final machine we want to reach

Pivoting with reGeorg

- reGeorg is to be able to pivot without high privileges on the pivot machine
- Location: /root/Desktop/tools/reGeorg/tunnel.php
- Upload tunnel.php to pivot machine
- On attacker machine: python reGeorgSocksProxy.py -p 9050 -u http://*TARGETIP*/*PATHTO_TUNNEL.PHP*
- proxychains *command FinalTargetIP*