Bounty Hacker

TRYHACKME -: ROOM : BOUNTY HACKER

1) nmap --> http ,ftp and ssh open
2) nikto (no clue in this)
3) dirbuster (no clue in this)
4) ftp login , user anonymous
5) find the 2 txt file one containing the username , other password list
6) brute force ssh with the password list using hydra
7) login into ssh
8) find one text file which is password for superuser access (sudo -l)
9) use scp and get the export linpeas into the remote ssh machine (not nessassary)
10)sudo -l will reveal the /ect/tar file
11) using tar to escalate with the command sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh (found in the internet with bit of searching .

12) access root with it and there you go ! find the last txt file !