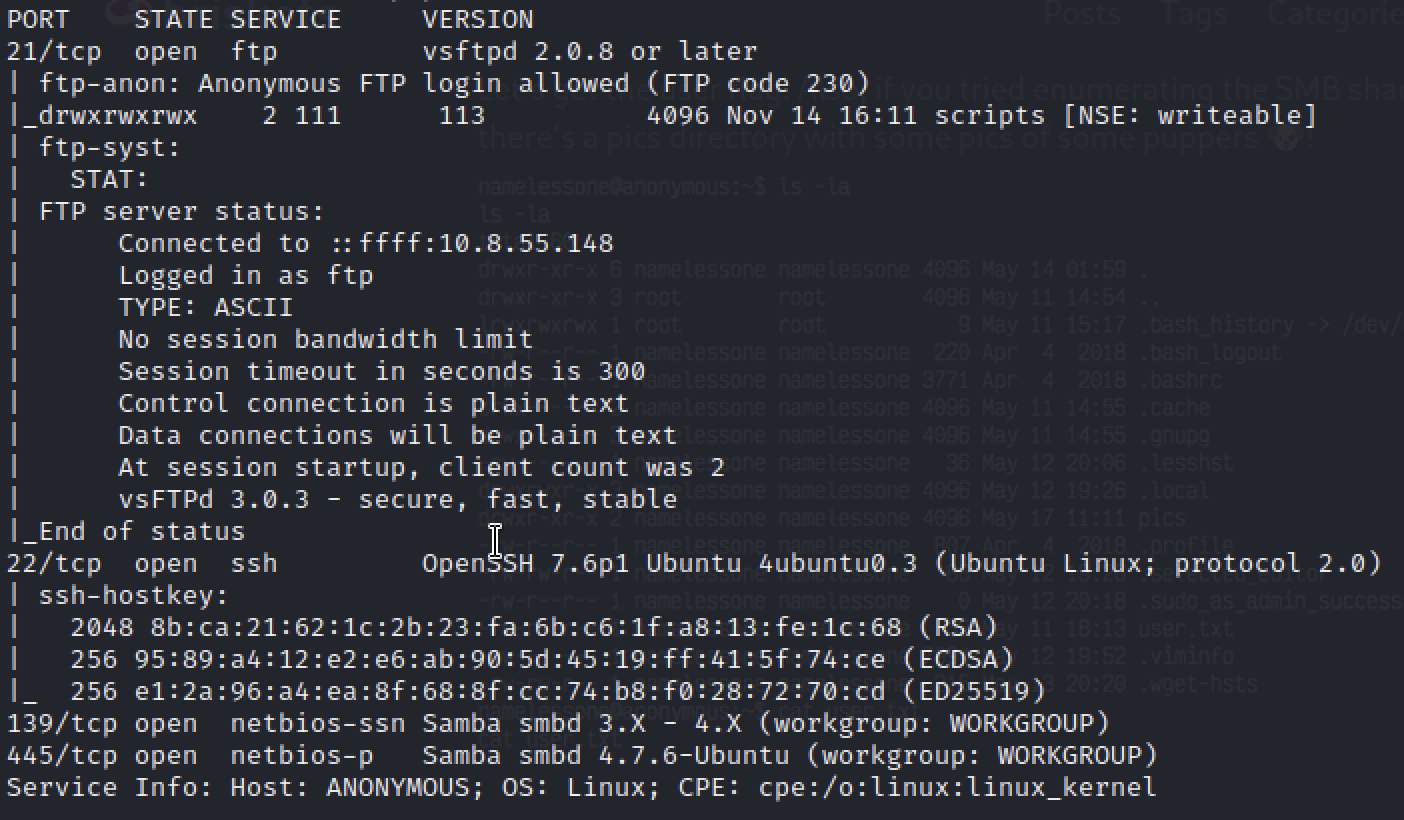
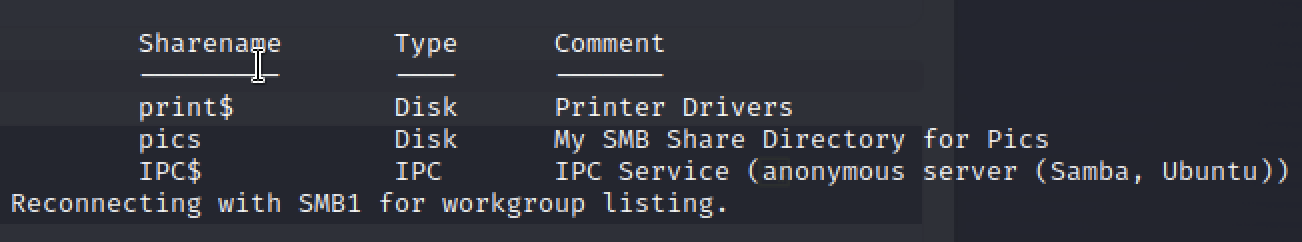
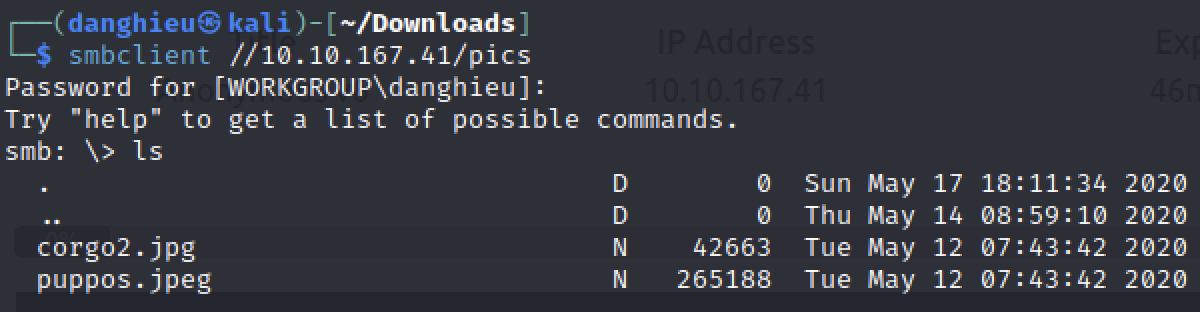
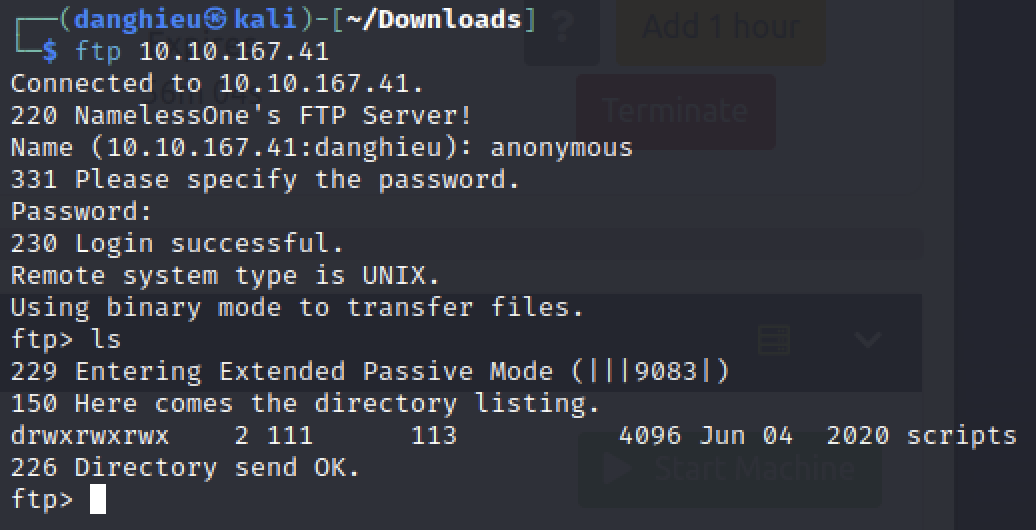
nmap -sC -sV -A 10.10.34.245

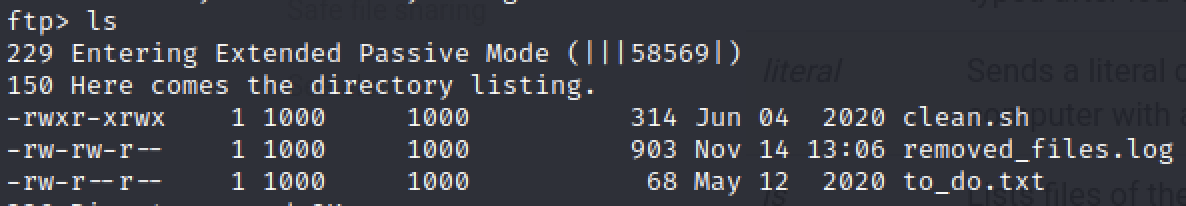


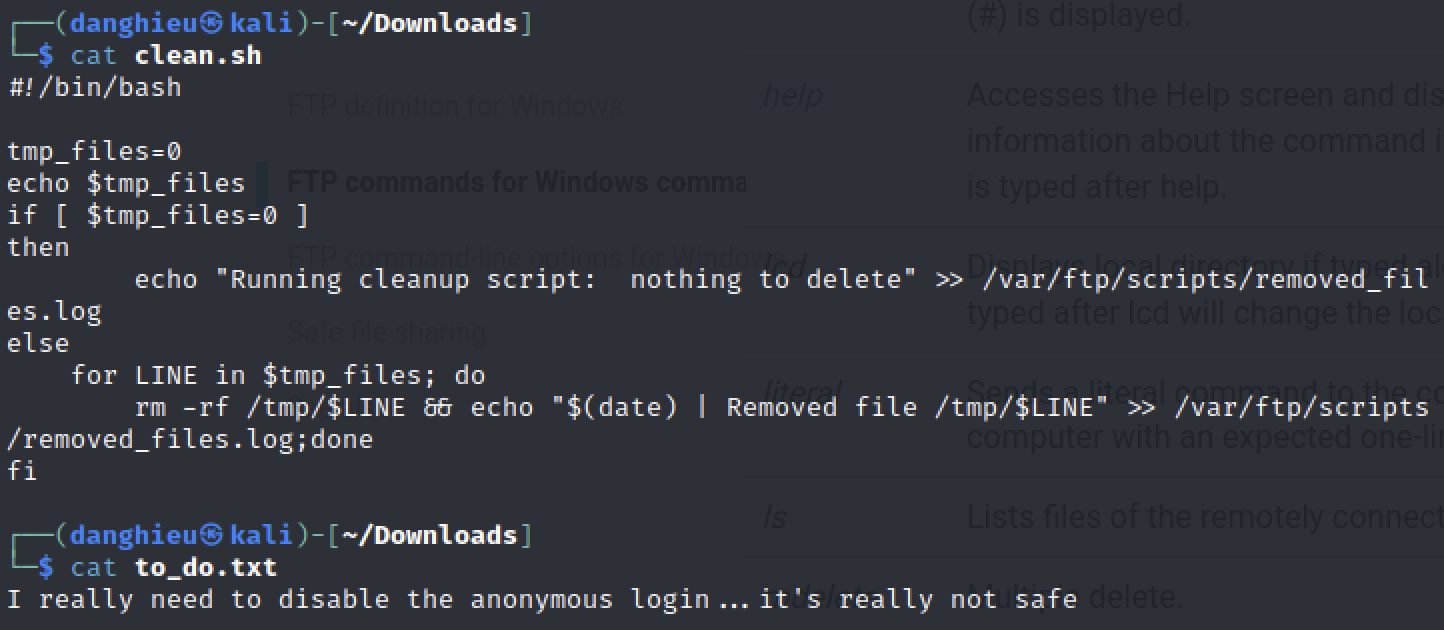
Liệt kê dịch vụ SMB: enum4linux -a 10.10.167.41

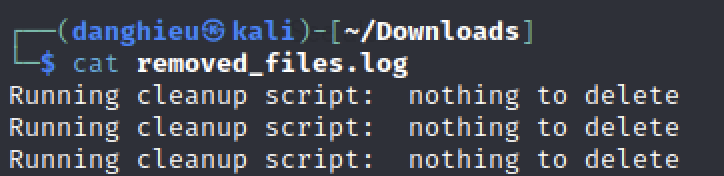












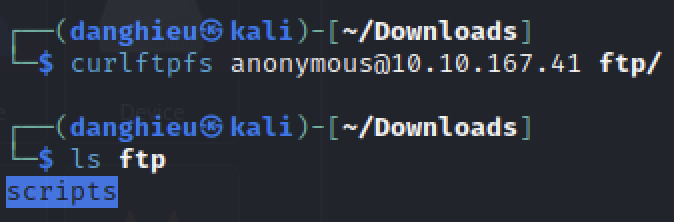
File cleanup.sh cho ta manh mối về cron tab. Bài này sẽ dạy cho ta cách ghi file trong ftp.

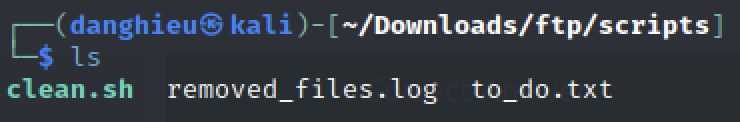
**Mounting**

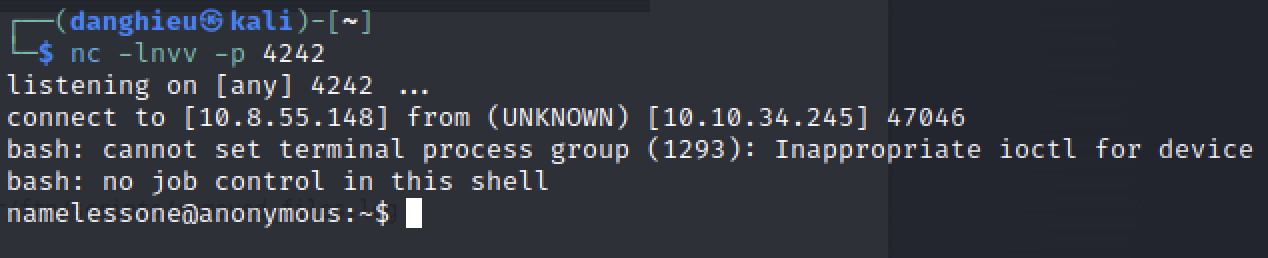
Bạn có thể làm bằng nhiều cách khác nhau. Tôi sẽ mount share bằng curlftpfs và điều chỉnh clean.sh với vim

mkdir ftp

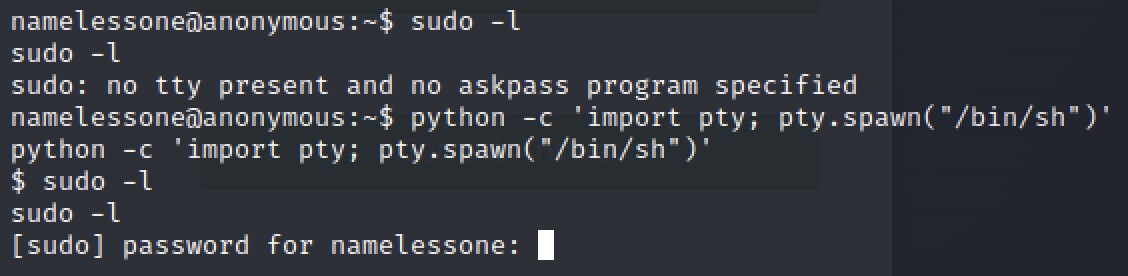
curlftpfs anonymous@10.10.167.41 ftp/







Nếu bạn reverse shell thì không chạy được lệnh sudo -l (nó yêu cầu mật khẩu)



Kiểm tra SUID:

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

