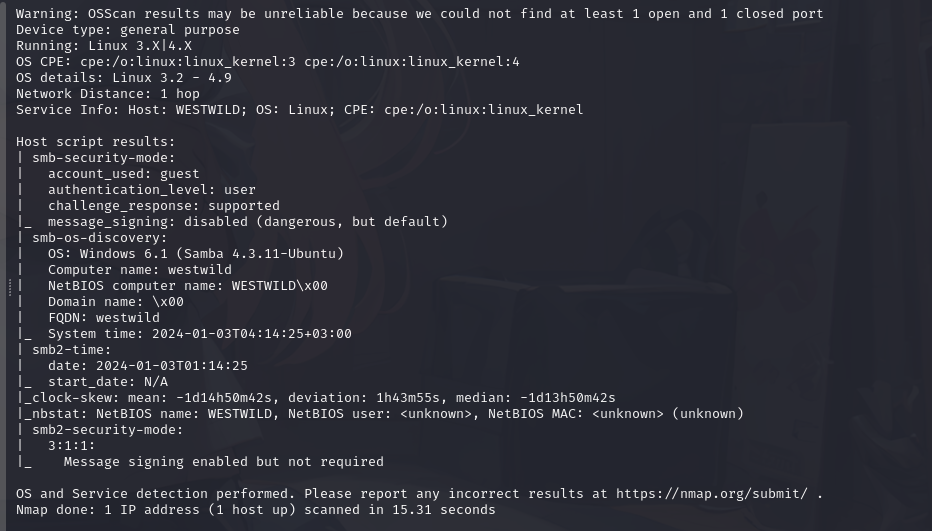
# 信息收集

Nmap详细信息收集发现samba的匿名登录



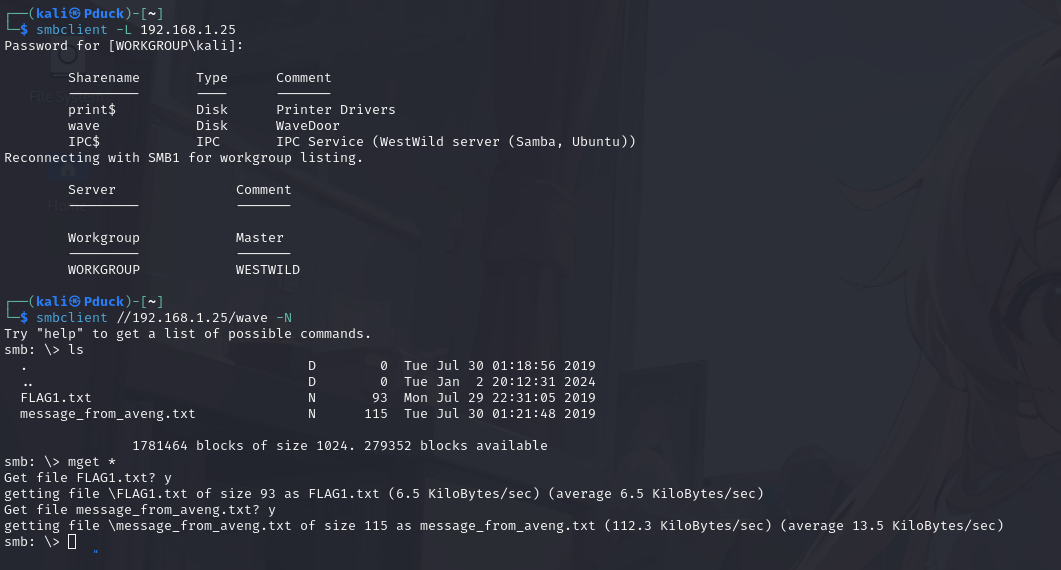
# Samba信息收集

Smbclient -L 192.168.1.25列出samba下有哪些共享目录发现wave

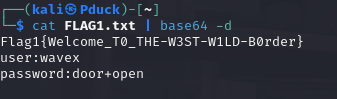
Smbclient //192.168.1.25/wave -N 登录下载

-N不进行密码验证

-L列出samba下的信息



阅读发现是base64编码，解码阅读



# Web信息收集

目录爆破,dirsearch 和gobuster没有爆出任何信息，nikto也没有发现有用信息，主页源码也没有有用信息

# 提权

将刚刚的用户密码ssh登录尝试

Find / -writable -type f ! -path “/proc/\*” 2>/dev/null

寻找可执行文件发现有一个/usr/share下的，查看文件发现新的用户密码登录

