Easy root with metasploit and MS17-010 (Eternal Blue).

Without metasploit:

Using enum4linux, we can check that username ‘’ with password ‘’ permits a login. This is the credentials for the guest login. Using 42315.py from exploitdb, we can get a shell. We have to make a few quick modifications to the 42315 script in order for the exploit to work. We replace user with ‘//’ or ‘guest’. We also have to use msfvenom to craft a reverse shell. Finally, we edit the smb_send line so that we are actually sending the crafted payload instead of pwn.txt. This means changing the path to the path of our executable, and changing the service_exec line to the command to execute our payload.