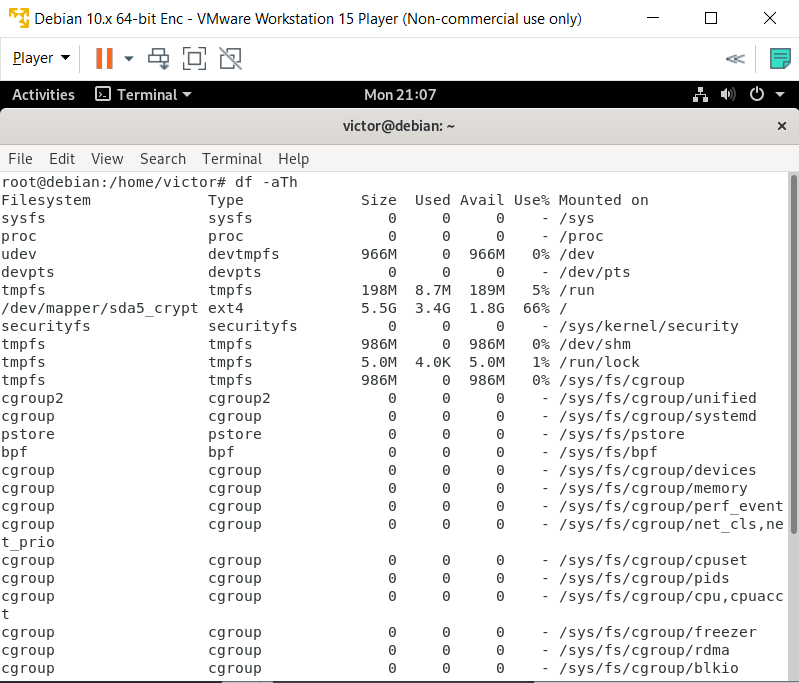
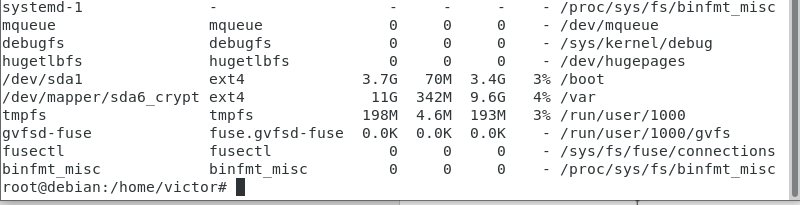
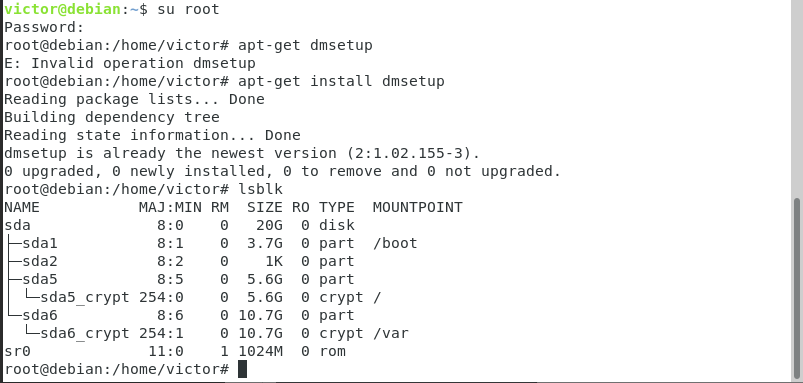
Roteiro 1.4

1.4.a)



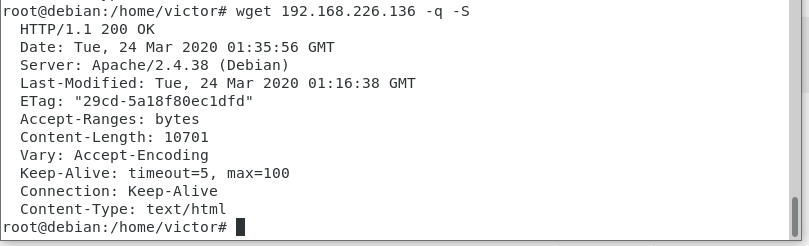


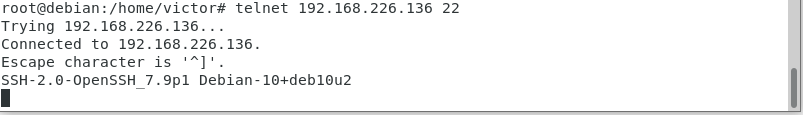
1.4.b)

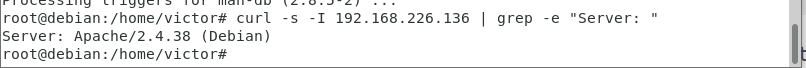


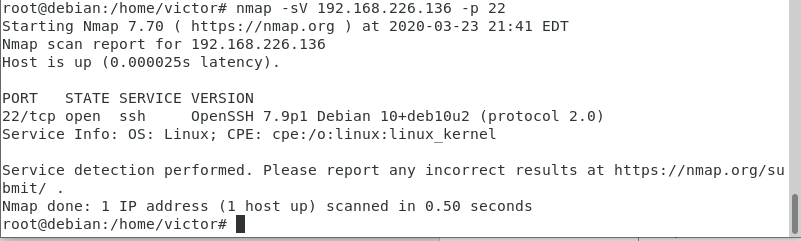
1.4.d)

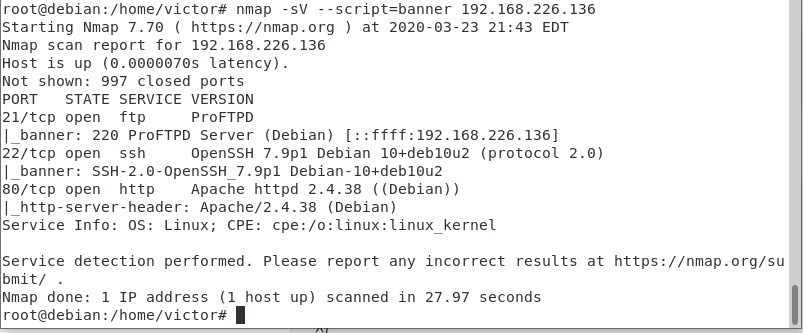
Testando os serviços que exploram o acesso à versões de software da máquina, encontrei algumas vulnerabilidades:



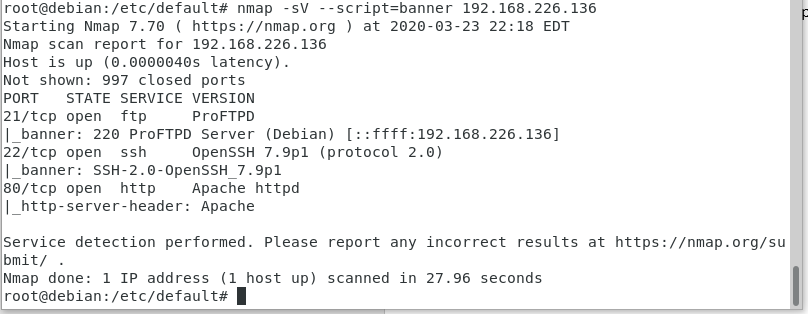








De forma a esconder esses banners foi preciso entrar nos arquivos de configuração de cada um destes serviços (ssh, apache) para desabilitar o print das versões. Para isso, foram realizadas alterações nos arquivos ssh\_config, sshd\_config, apache2.conf. A versão do openssh não foi possível retirar, porque ao realizar uma pesquisa na internet cheguei à conclusão de que ela é necessária para o estabelecimento da compatibilidade na comunicação. Depois das alterações, o resultado foi o seguinte:



1.4.e)

O diretório /boot é o único que não deveria ser criptografado numa instalação de sistema operacional porque ele é necessário para realizar o boot da máquina.