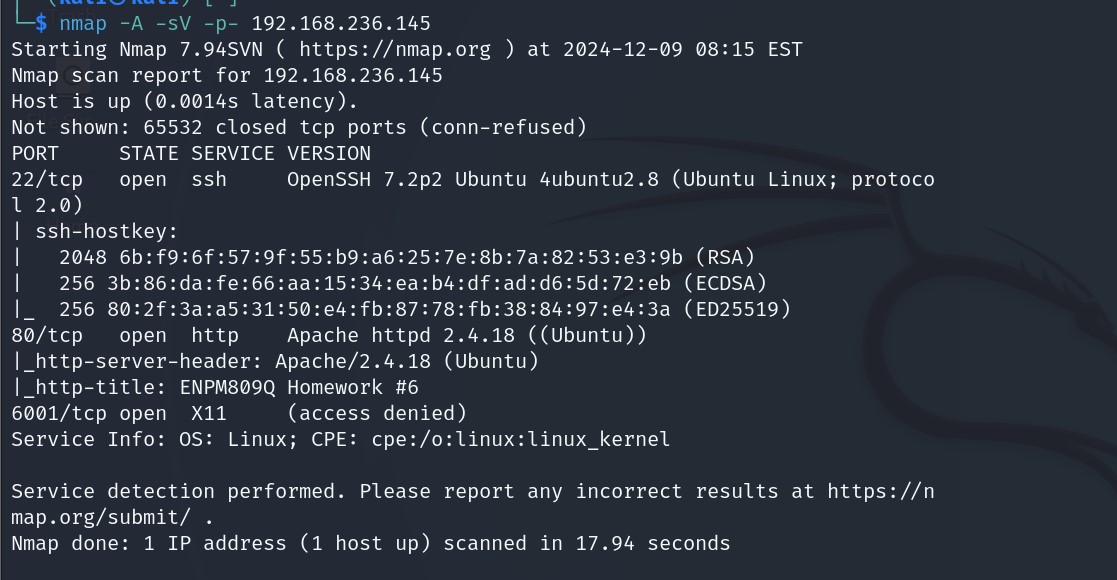
Name: Rithik Sarvesh Bharathiraja

UID: 120395246 (gbr2001)

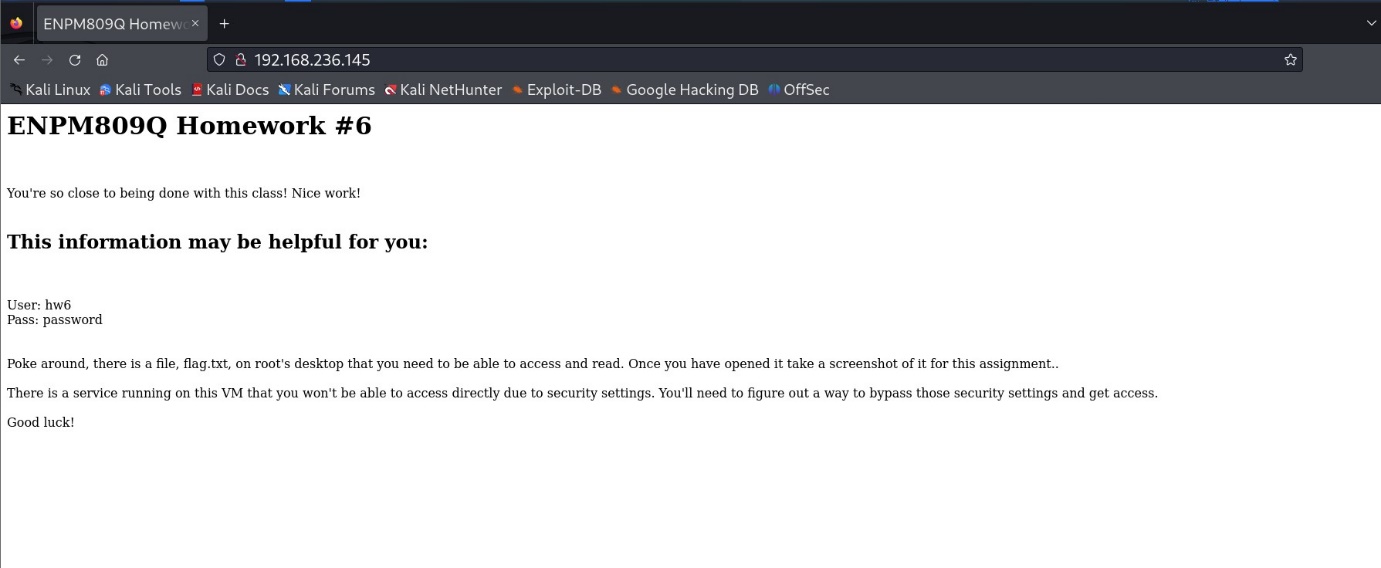
Task: Homework 6

Course: ENPM634

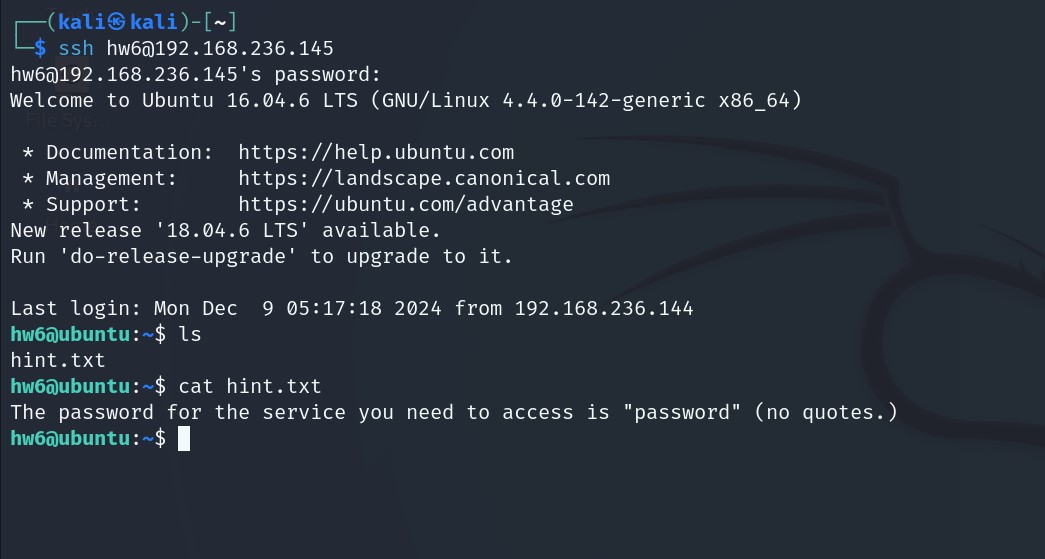
1. Once we boot up the VM, it showed us the IP address to work on. To do active recon, nmap was used in our kali machine. The scan showed that there were three services running, SSH, HTTP and X11.



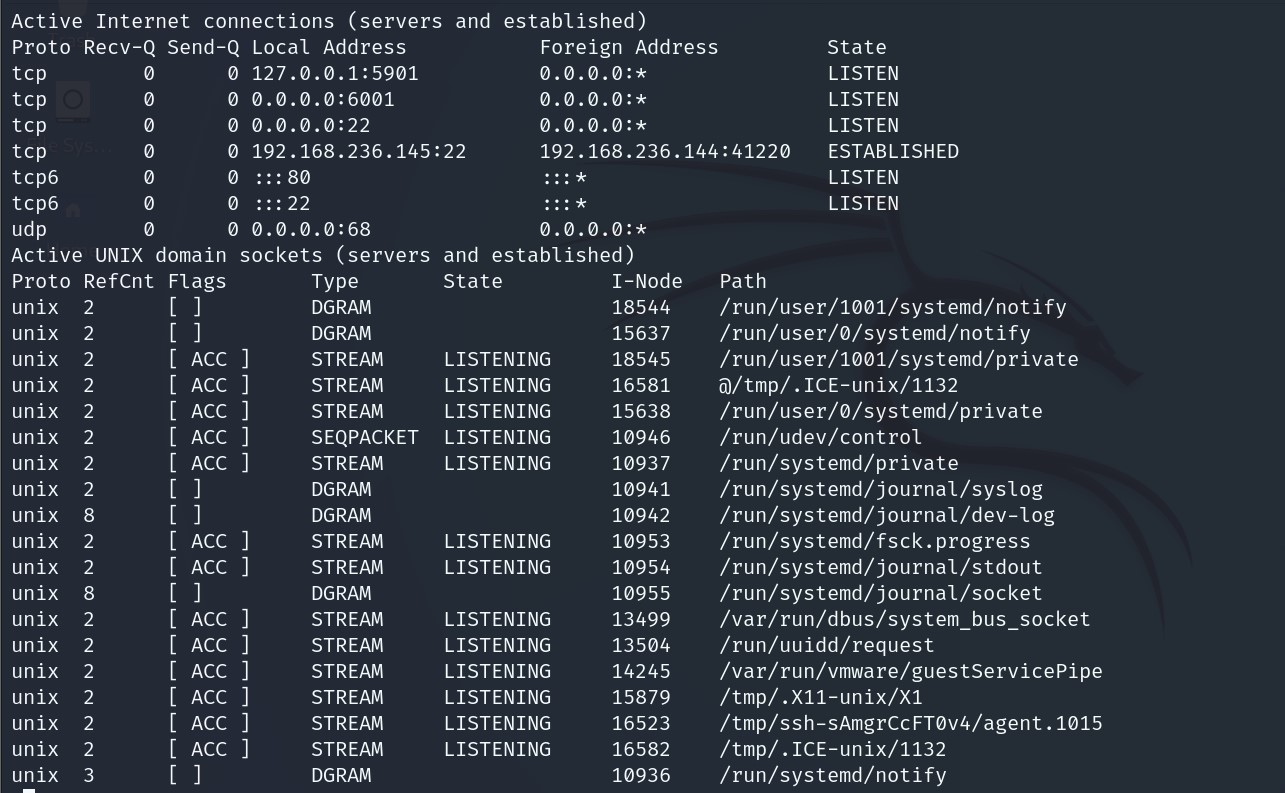
1. The HTTP service was accessed by the browser. It had the credentials for the SSH connection to the VM. It also stated that there was a service running on the system which couldn’t be accessed directly due to security settings.



1. After trying different techniques on the port 6001, we couldn’t able to exploit it successfully. So, with the given credentials, SSH connection was established to the VM. The hint stated that the password for the service we need to access is “password”.



1. To know about the service running on the system, “netstat -an ” was used. It showed that the port 5901 was running a service and it was listening for the client. As stated by the hint, we weren’t able to access the service directly. Actually, port 5901 was used by the VNC server. VNC stands for Virtual Network Computing. It is a cross-platform screen sharing system that was created to remotely control another computer.



1. Thus, port forwarding using SSH protocol was used to access the service. The port 5901 in the VM was accessed using the port 4444 of our machine usign the SSH. “-N -f -l ” arguments were used.

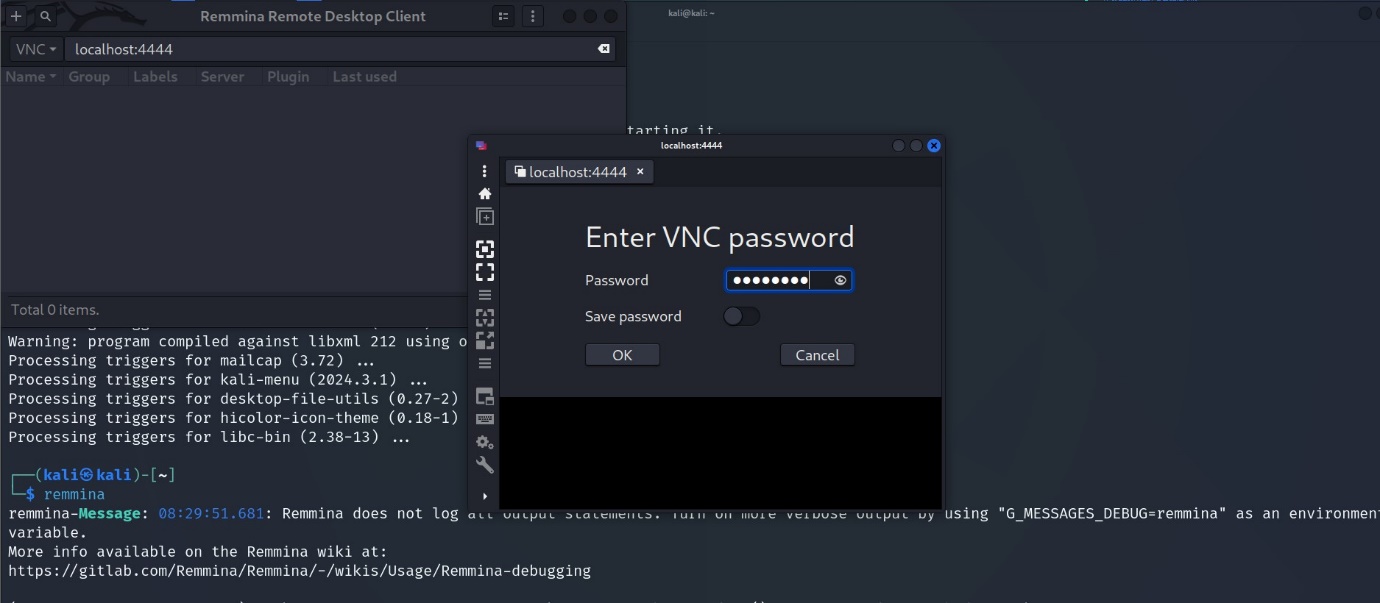
-N – to not execute any remote command

-f – after connection establishment, terminal can be used for other commands as this task will be running in the background

-l - to specify the username



1. Once it was done, remmina was installed and executed to access the VNC server. After connection establishment, we can access the service in our localhost and in the port 4444, with the password (‘password’) we found in the home directory of the user ‘hw6’.



1. Once given the password, we got access to the root user of the same VM. The flag was found in the root directory of the VM. The flag contains some bitter and harsh truth. (I feel sorry for him.)

