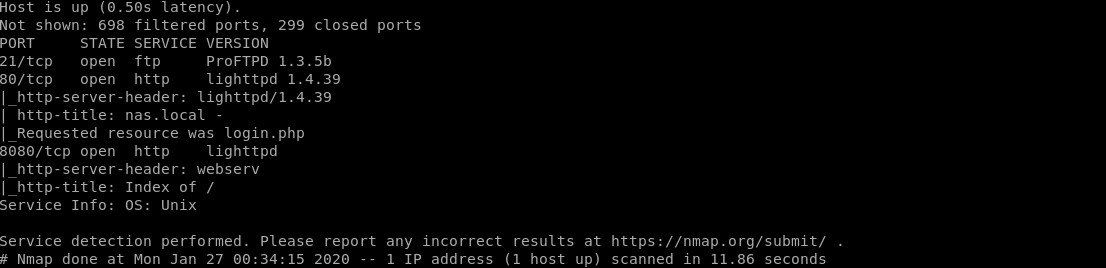
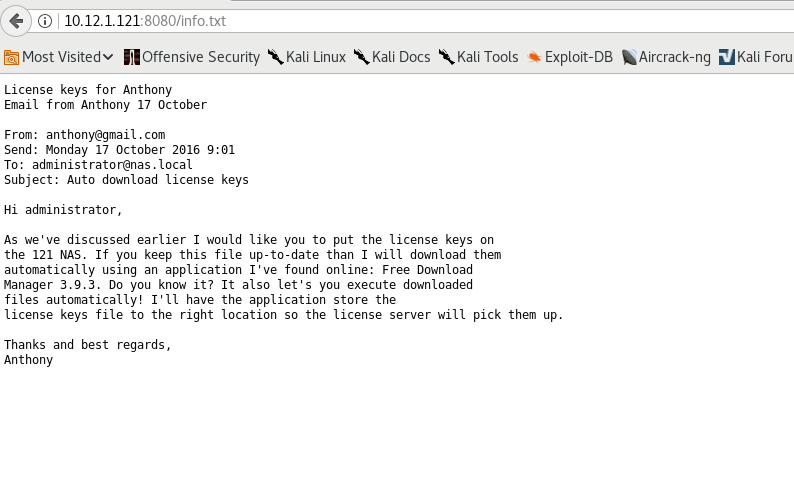
NAS(10.13.1.121)-GhostIA

Sarah Ferenczi

Enumeration

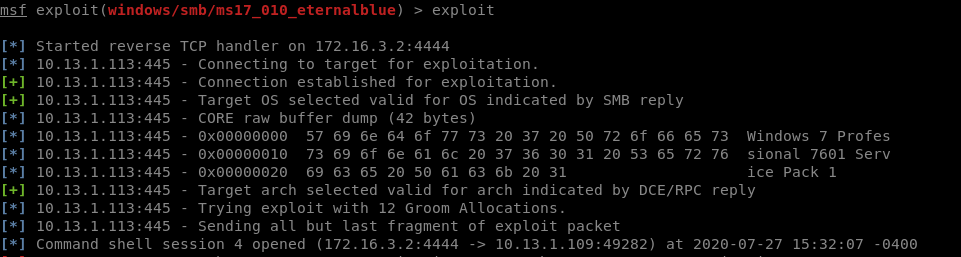


First let’s run an nmap scan. There is nothing currently useful on port 21, but port 80 and 8080 might have some interesting stuff.



If we head over to port 8080 and click on info.txt, we can notice that there is some information that may be useful in getting past the login page. Since it is referred to by Anthony, we can safely assume that exploiting the box Anthony might get us some information

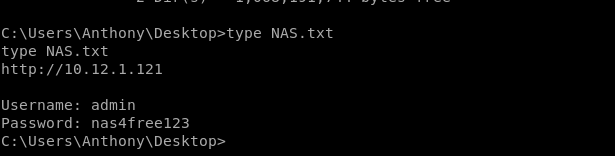
Exploitation



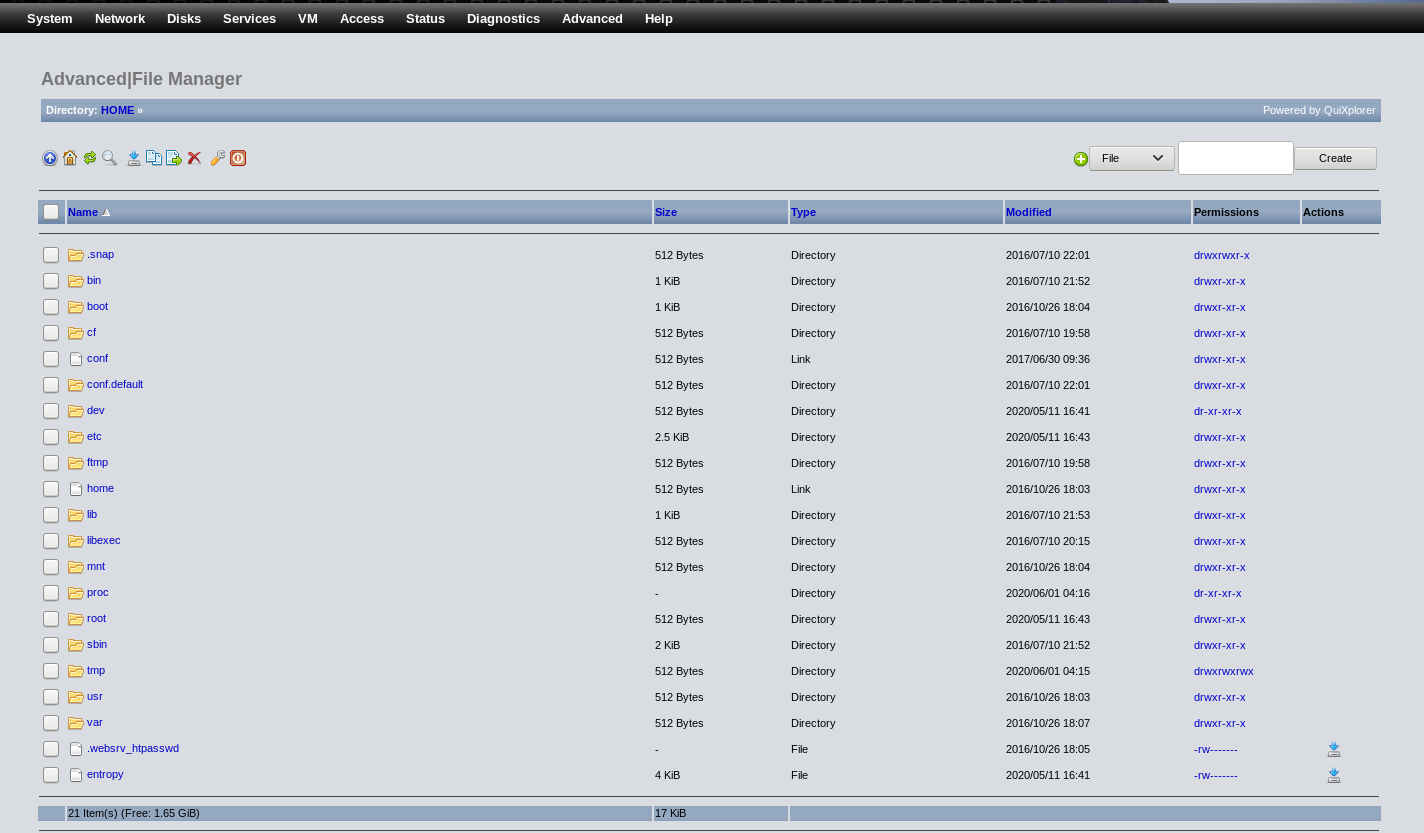
From doing Anthony, there is an SMB vulnerability on this box, so let’s run eternalblue to get root.



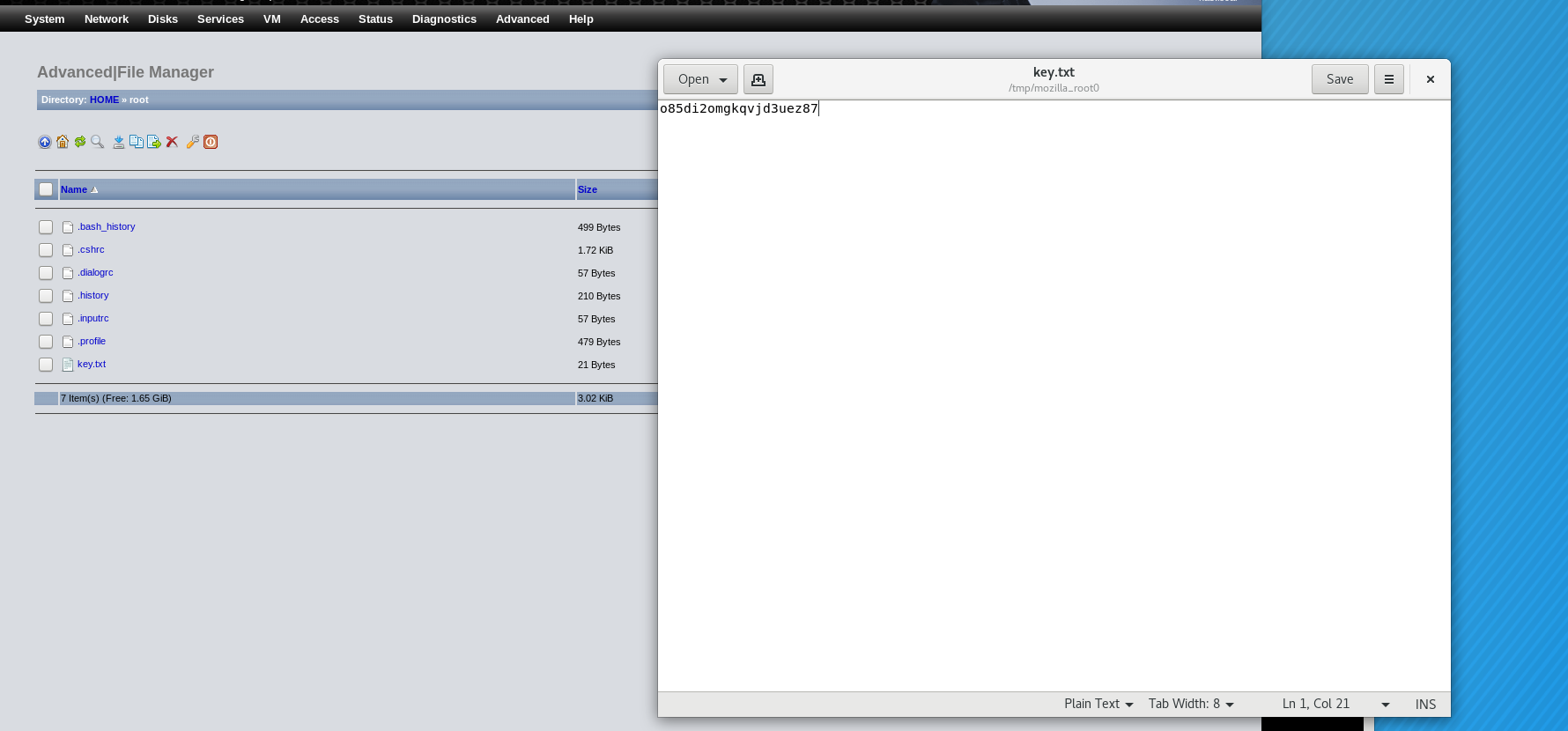
Once we navigate to C:\Users\Anthony\Desktop, we can notice that there is a file for Anthony.



Now, we have credentials to log into the NAS admin panel.



Once we are in the system, we can navigate over to Advanced>File Manager



Then we can head over to /root and open the file that has the key inside.