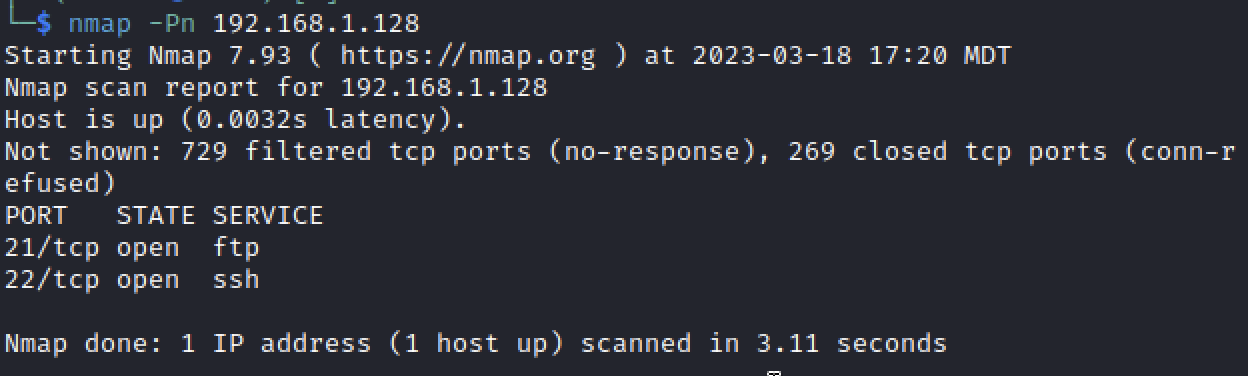
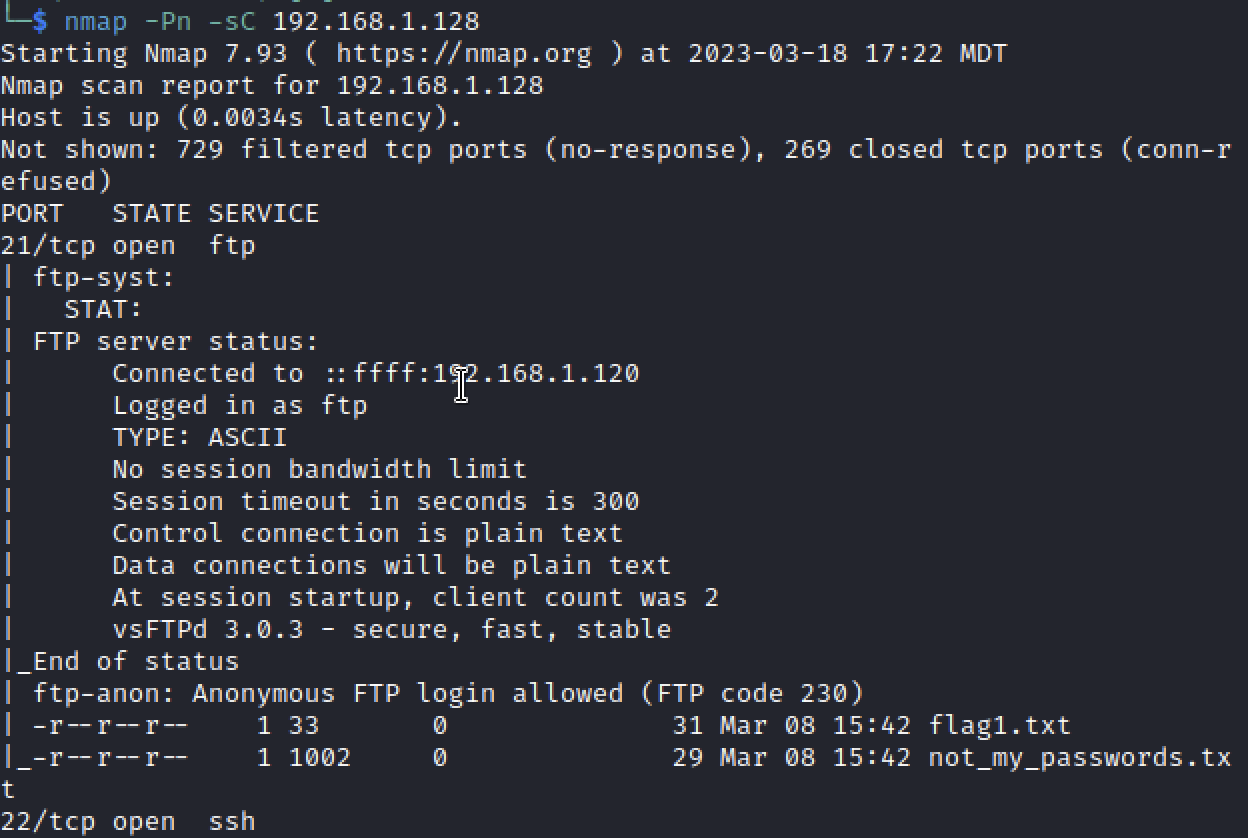
Name: **MI6configuration**

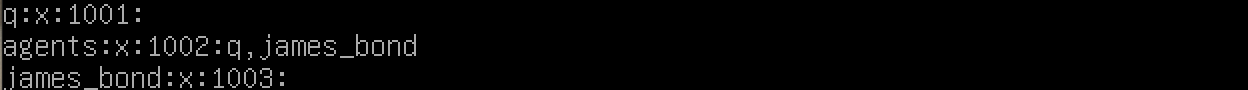
Flavor text:

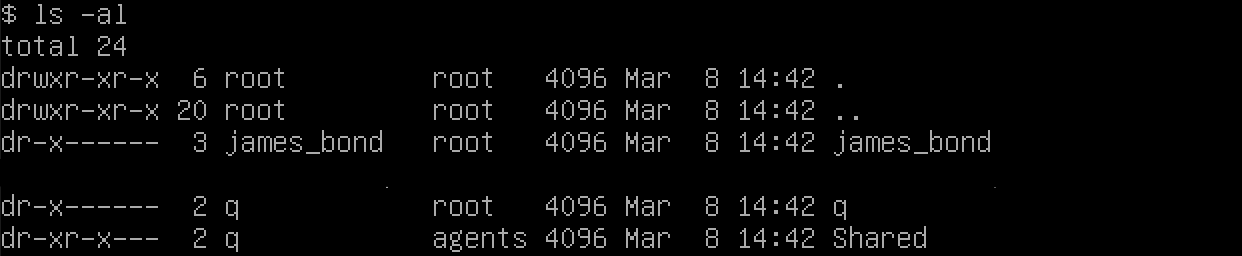
We recently acquired the ip address to a computer at MI6 and it seems like they might have made some mistakes. Can you hack it using their misconfigurations and get all their important data? (Download the vm file and power it on. Get the ip address and start hacking!)

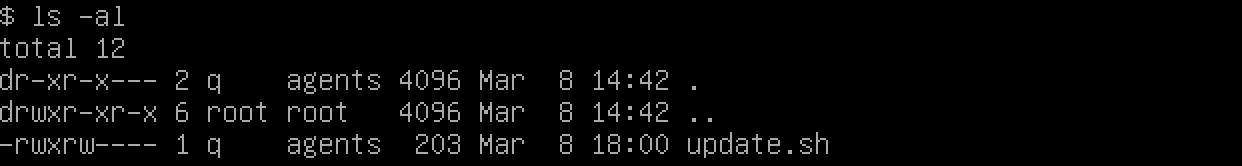
Writeup:

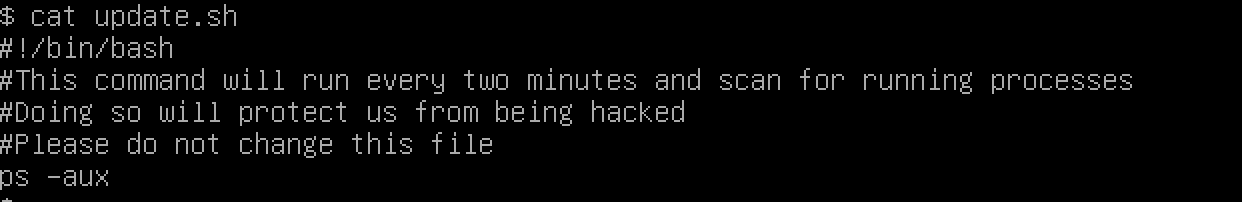
Upon spooling up the vm, we can begin to view the services that are running. After running an Nmap scan on the machine gives us this output:

We can then begin to enumerate, and see if there is anything further we can find out:

We can see that FTP can be logged in anonymously, and has two files that are readable by all. After we get the commands from the server, we see that the username and password are included in the **not\_my\_passwords.txt** file. So, we can log in through ssh or simply through the VM. Next, we want to find as much information about the system and the users to find a way to privilege escalate to **root**. Upon viewing **/etc/group** we can see that there is a group named **agents** with **james\_bond** and **q**:

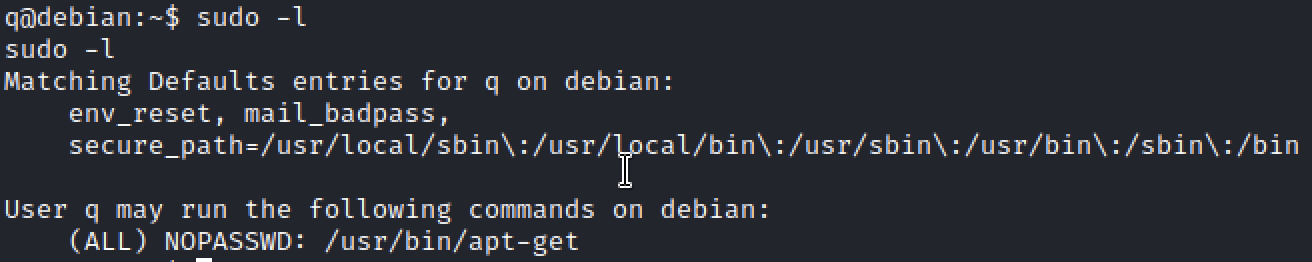
This means that if there are any files owned by **q**  and the **agents** group would share permission with **james\_bond**. Upon going to the **/home** directory, we can view the following files:

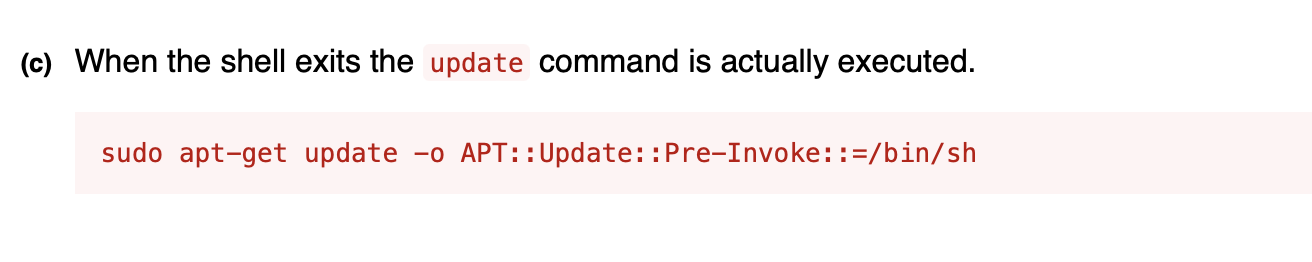
We can see that there is a directory called **Shared** that is owned by **q** and the **agents** group. Upon viewing the files with in that directory we find the following:

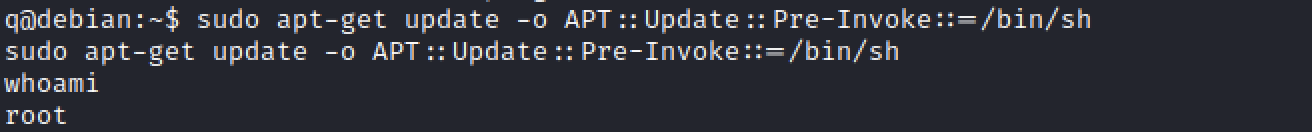
There is a file called **update.sh** and it is again owned by **q** and the **agents** group. Viewing the file, we find something interesting.

This seems like a cronjob, which is a task scheduler. We can see that **q** is running this script every 2 minutes. Upon searching the internet, we find this website: <https://stackoverflow.com/questions/55240626/bash-reverse-shell-command-cron-job-not-working-i-give-up>

Upon typing that in to the **update.sh** file and waiting for 2 minutes we see this:

We are now in as the user **q**! Now lets see if he has any **sudo** access.

Wow! **Q** can run the command **apt-get** without any password…. How can we use this? Navigating to <https://gtfobins.github.io/gtfobins/apt-get/#sudo> tells us that we can do the following:

Great! Let’s put that into our terminal! We get the following:

We now are in as **root**! Going to the **/root** directory will give us our flag!