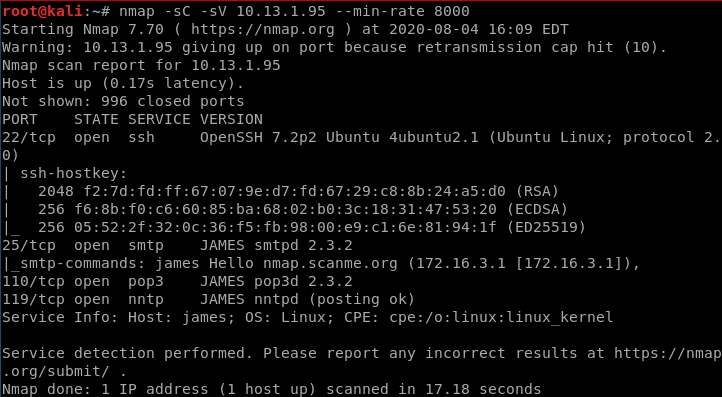
James(10.13.1.95)-GhostIA

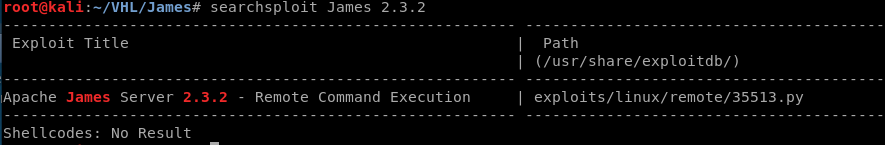
Sarah Ferenczi

Enumeration

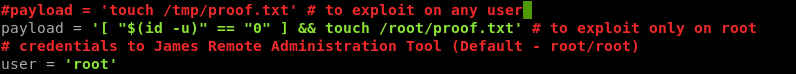


First run an nmap scan. Nothing seems too out of place except for port 25

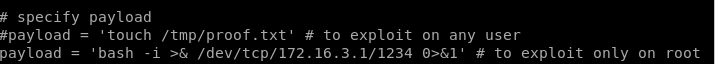
Exploitation



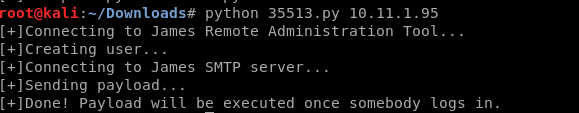
This is the main exploit we can find. With this we can check out this exploit.



One thing we can notice throughout the code is that the payload will not give us what we want. Let’s change this to a reverse shell payload.

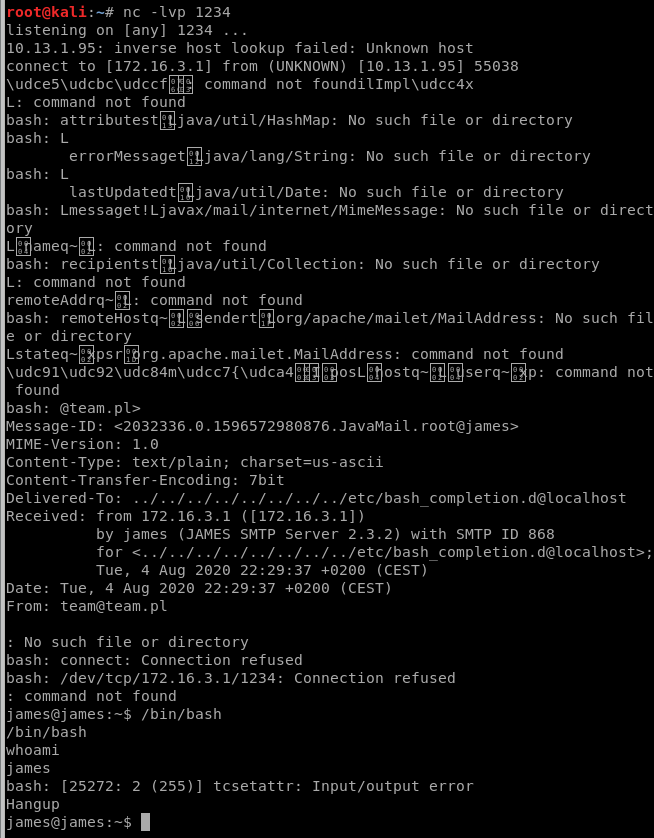


I will use a bash reverse shell because the box may not have Python installed.

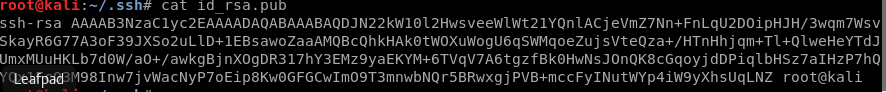


Let’s run the program now and set up our listener on 4444

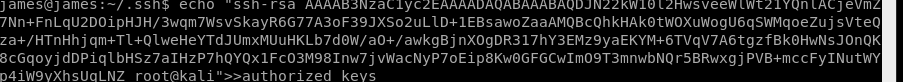




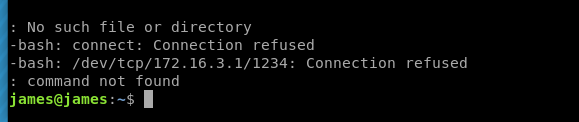
Make sure to run /bin/bash to maintain consistency



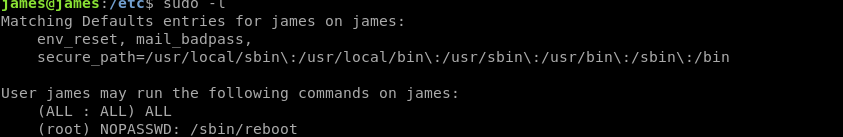
We want to try and maintain consistency on the box because there are several hangups. For this reason, let’s edit an ssh key.



This way, we can ssh into the box without a passcode



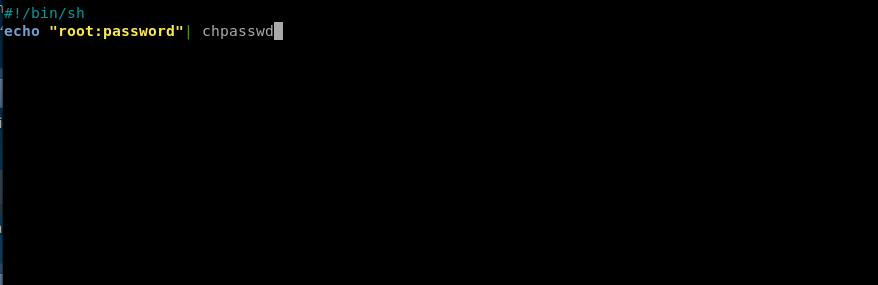
Now we have a fully upgraded shell



Privilege Escalation

Let’s check our permissions. In this instance, we can run any command as long as we have a password, but only be able to reboot without a password



When searching around, if we look in the etc file and check for writable files, we find an init.d file named james. Init.d files are run upon starting up, shutdown and reboot.

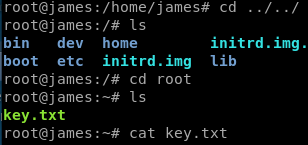
Since we can reboot this box without a password, let’s edit this file.



Now let’s reboot this machine



Give it a minute and then ssh back in. Run the command su and put in the password given before



Navigate to the directory where the key is and get it: yj351o4zt2wgplr4kafu