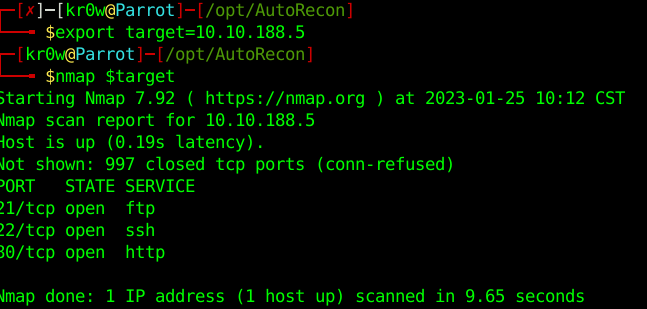
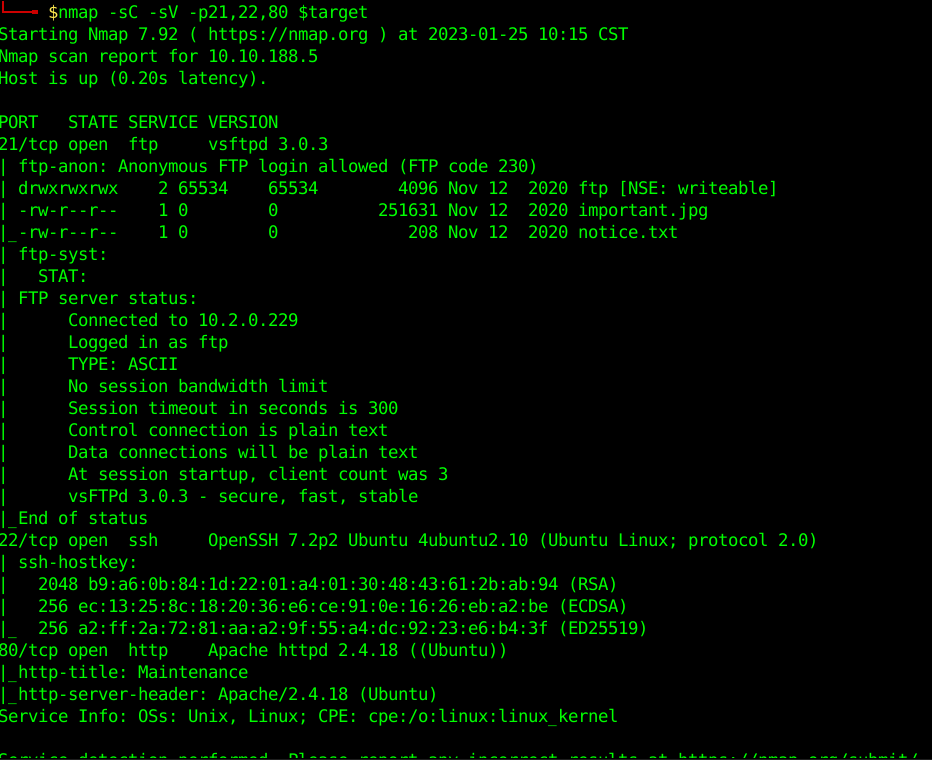


This is my first attempt at a writeup so bear with me if it sucks lol. The first thing I will say is after solving this in my own way I went back and looked at the writeups. Im not sure if something changed since those were posted or if they just liked doing things the hard way but my method is way faster and much much easier.

I started with a simple command to make things quicker then did a basic nmap scan

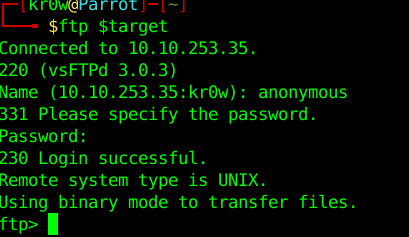


Scan a little deeper with nmap

Browse the website, and look at source code. Nothing really stands out so lets move on.

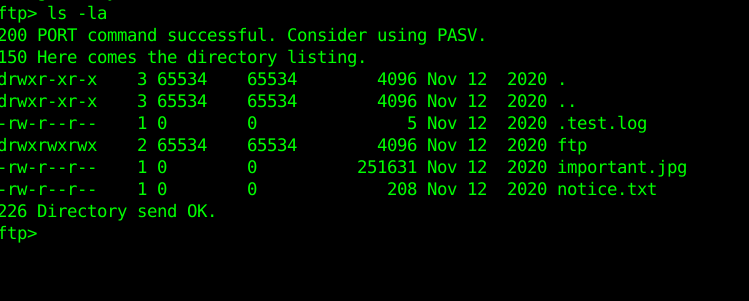
SSH but bruteforcing that could take forever so lets look at the low hanging fruit FTP

Anonymous ftp is working.

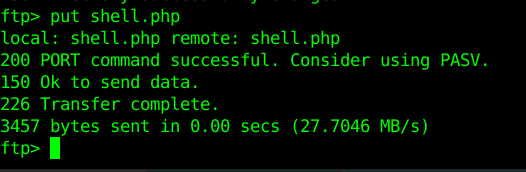


Listing the contents gives us a directory and a couple of files

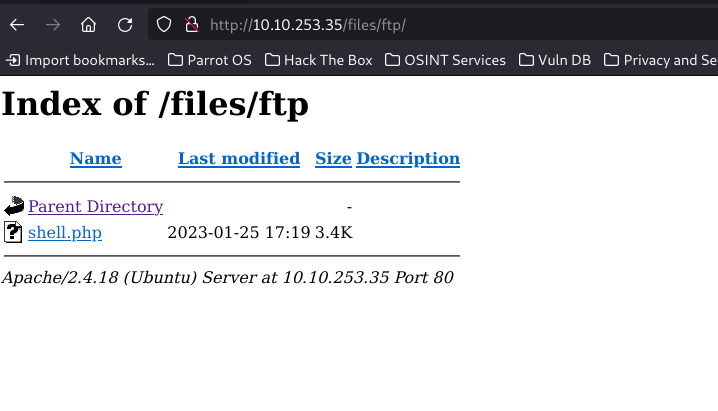
ftp is writeable



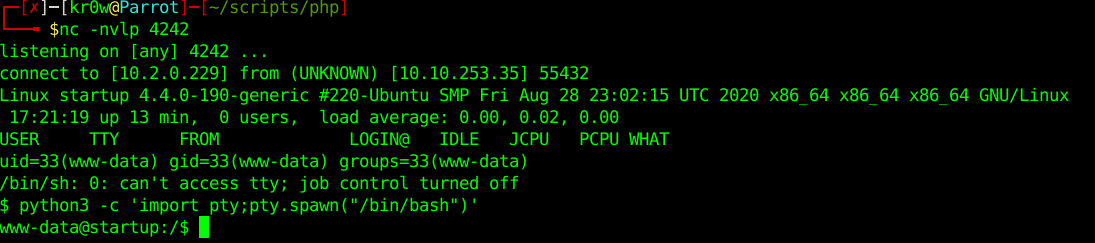
Lets try uploading files. Using a php reverse shell



Start a listener using nc -nvlp 4242 and browsed to the file I just uploaded.



Got a shell, lets upgrade that shell.



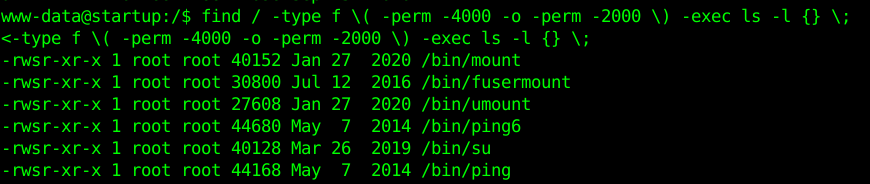
Listing the directory and we see the recipe.txt file.

Cat recipe.txt

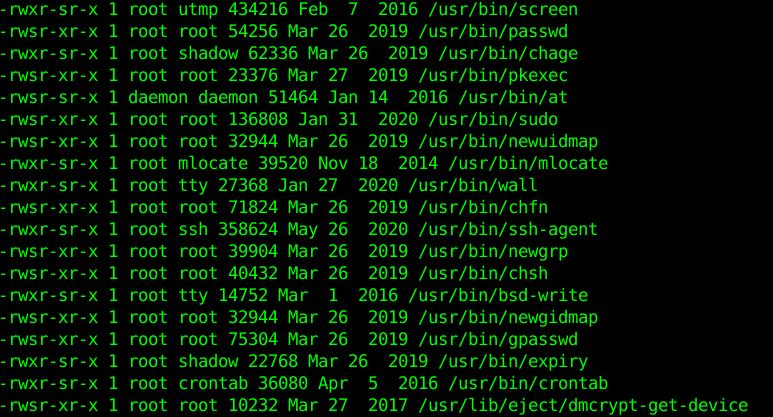


Home directory has Lennie but we cannot access it.

Escalate privileges. I always go straight to suid/guid bits if sudo doesn’t work which is the case here.



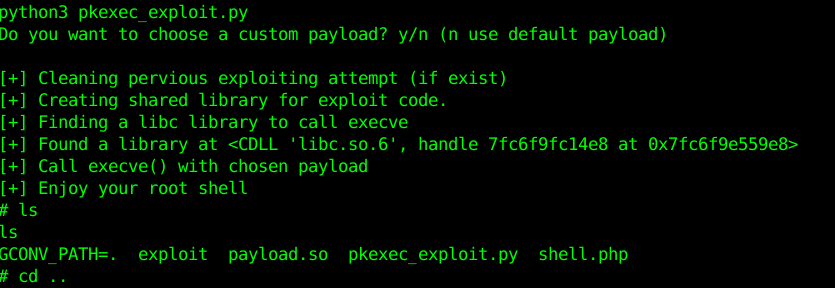




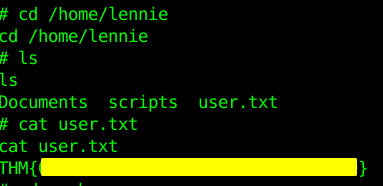
Out of all those the one that I saw that stood out the most is pkexec. I have used this binary many times to get root as its an old one. CVE-2021-4034

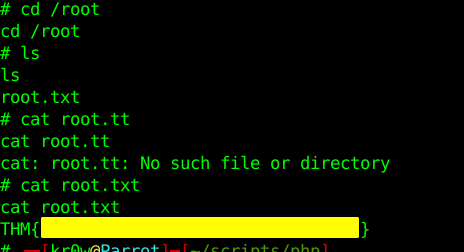
[pkexec-exploit/CVE-2021-4034.py at main · Almorabea/pkexec-exploit · GitHub](https://github.com/Almorabea/pkexec-exploit/blob/main/CVE-2021-4034.py)

Created pkexec\_exploit.py and moved it to the target. FYI you either have to use vim (which I suck at) or use ftp or wget to move the file. Now run the exploit



From here you can finish all the questions.





That’s it! I hope this helps you later on as you will now know to look for that exploit.

Best wishes,

sk4r3kr0w