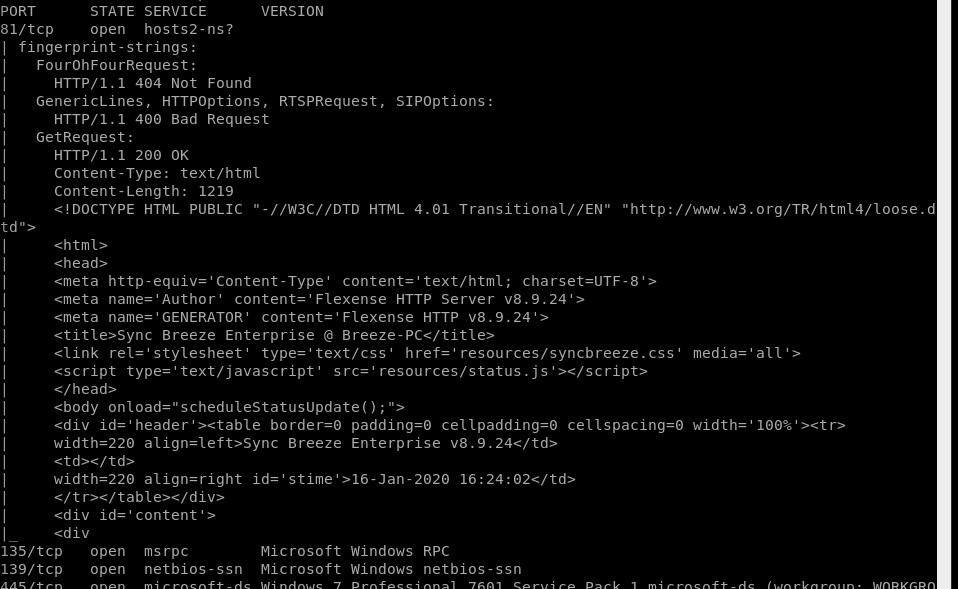
Breeze(10.13.1.124)-GhostIA

Sarah Ferenczi

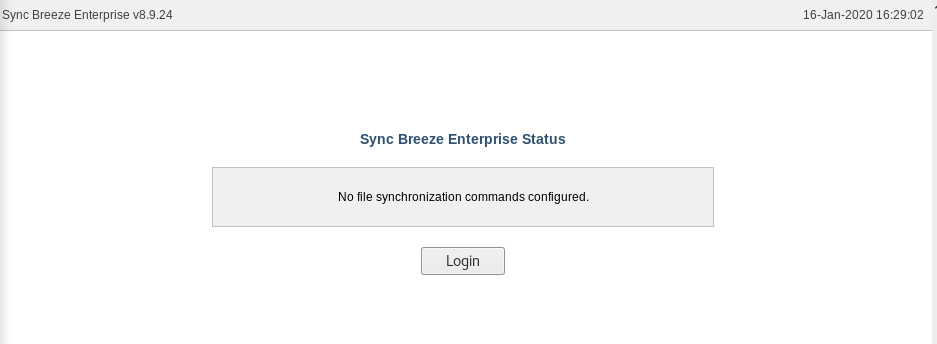
Enumeration



First, let’s run an nmap scan.

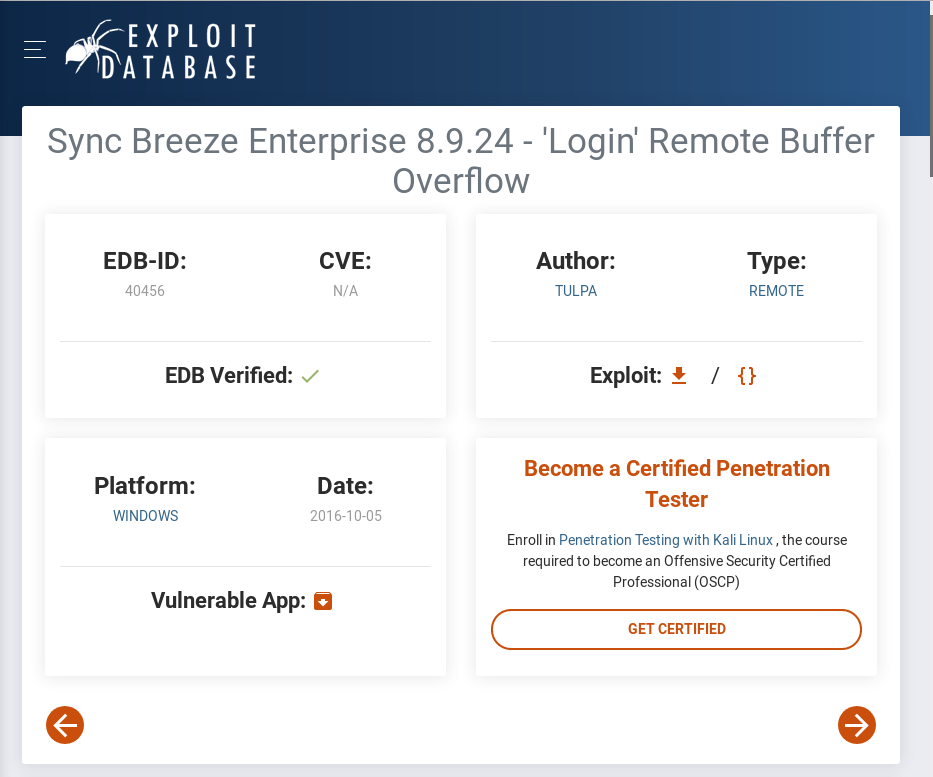


We know the operating system that’s currently running. Oddly enough, port 81 has a webpage.

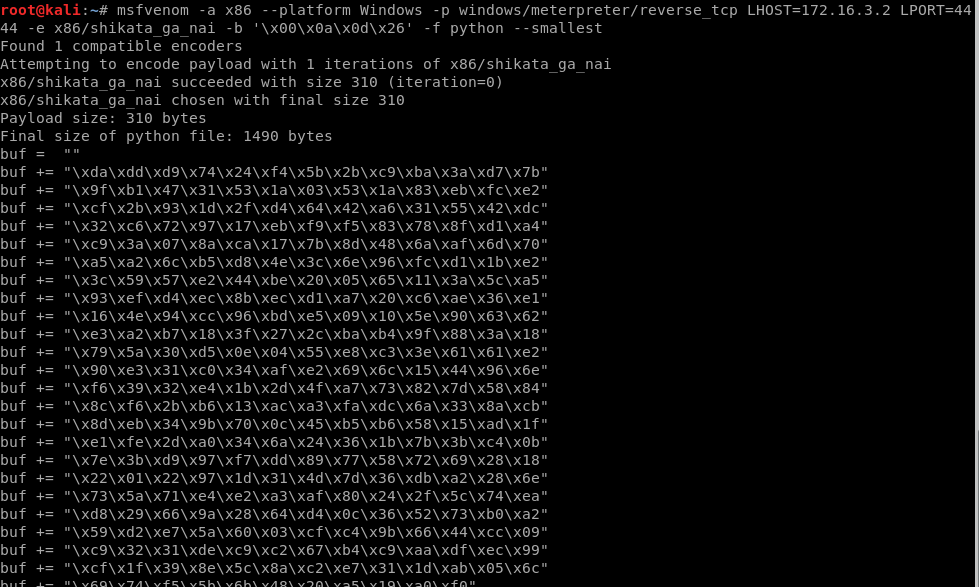


It is running Sync Breeze. There is nothing of interest on this for web exploitation.

Exploitation



We find a vulnerability that may work on our machine.

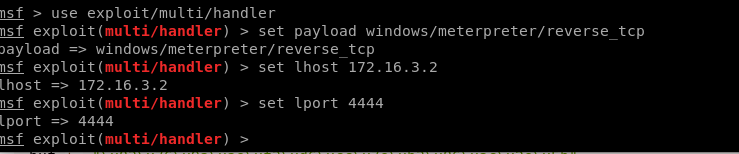


Let’s run the command to generate the shellcode.



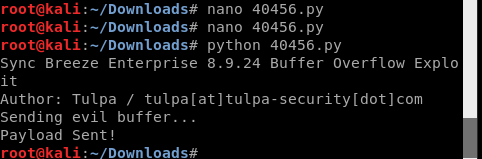


Make sure to change the IP address and port first. We need to paste the shellcode we generated in. The amount of bytes we got is 310, 2 more than the amount generated in the original code. For this reason, we need to subtract 2 from the \x41 line because our shellcode took up more space.





Now we open up metasploit and use the settings we set for this and run the exploit in the background



Now run the code



Now that we have root access, we can go ahead and navigate for the key: s3n12e9526irbwc641cx