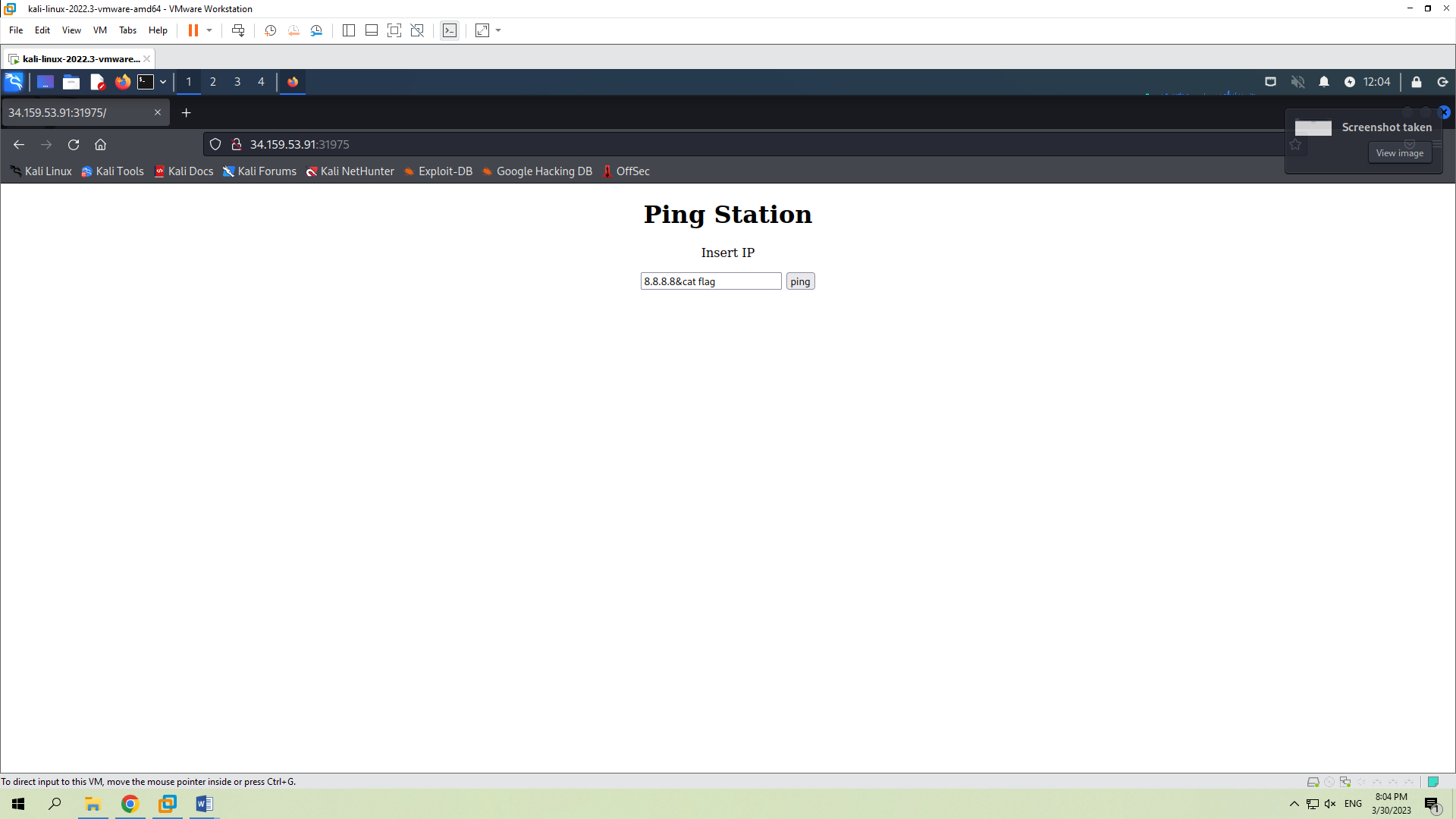
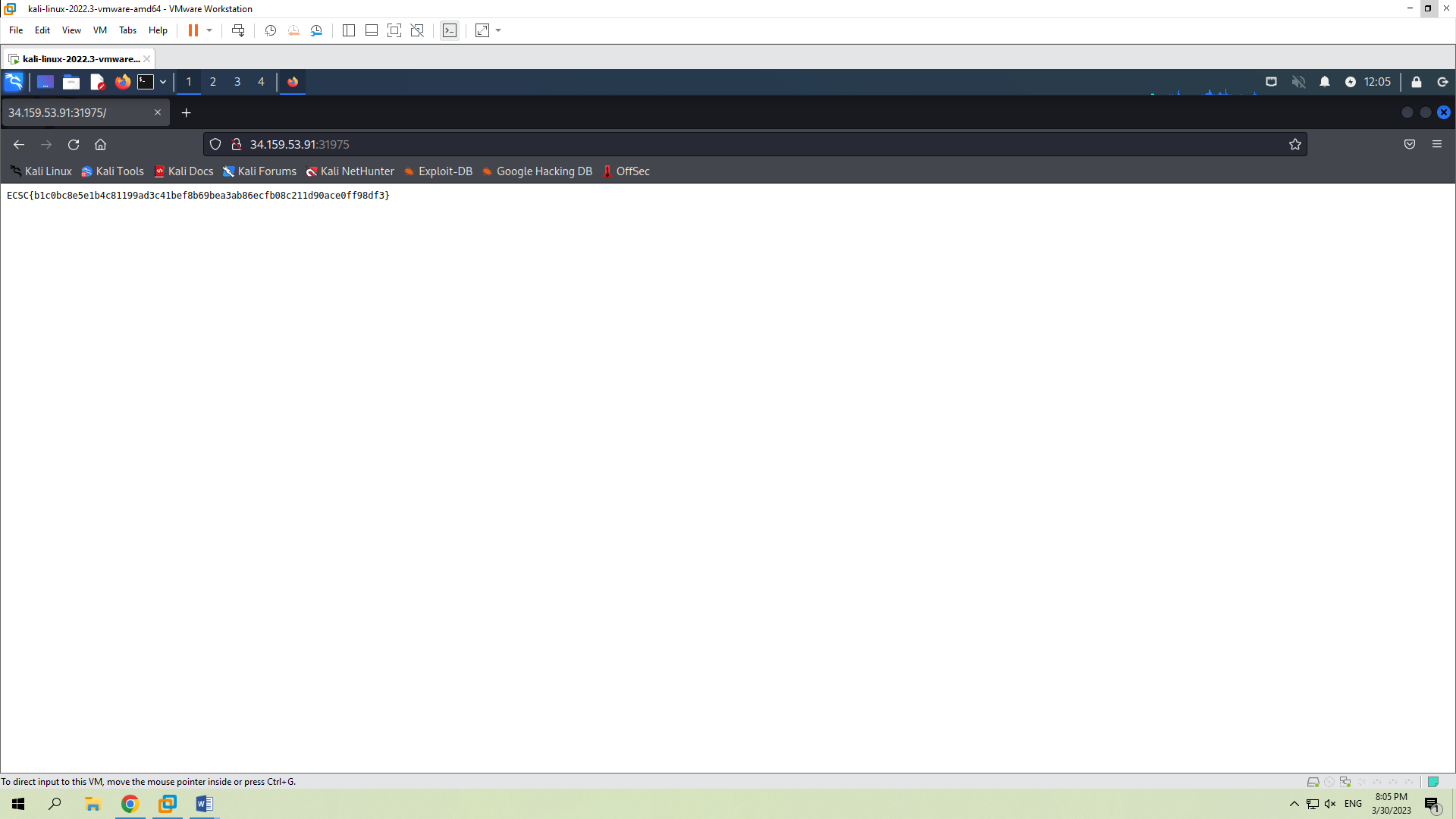
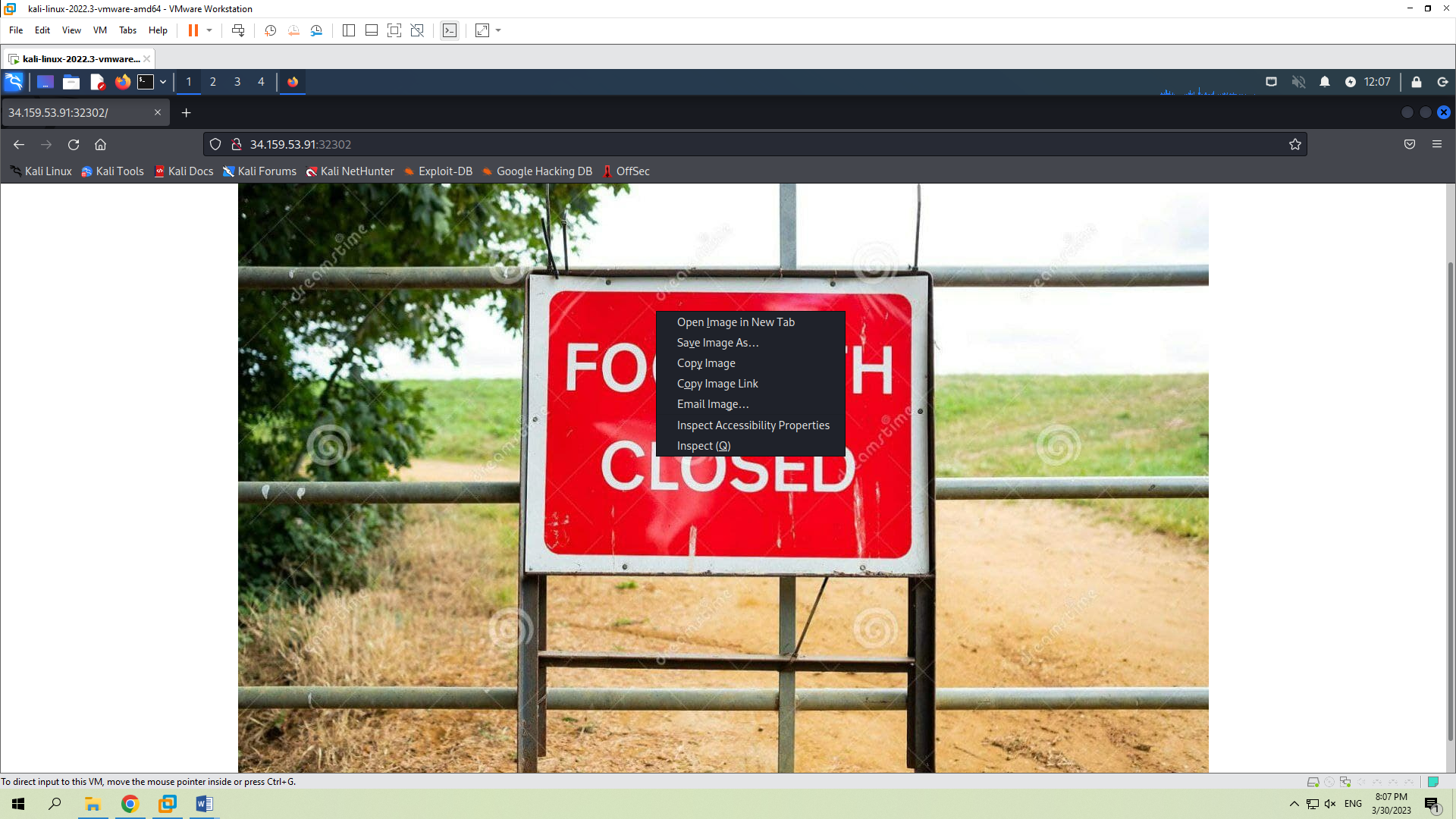
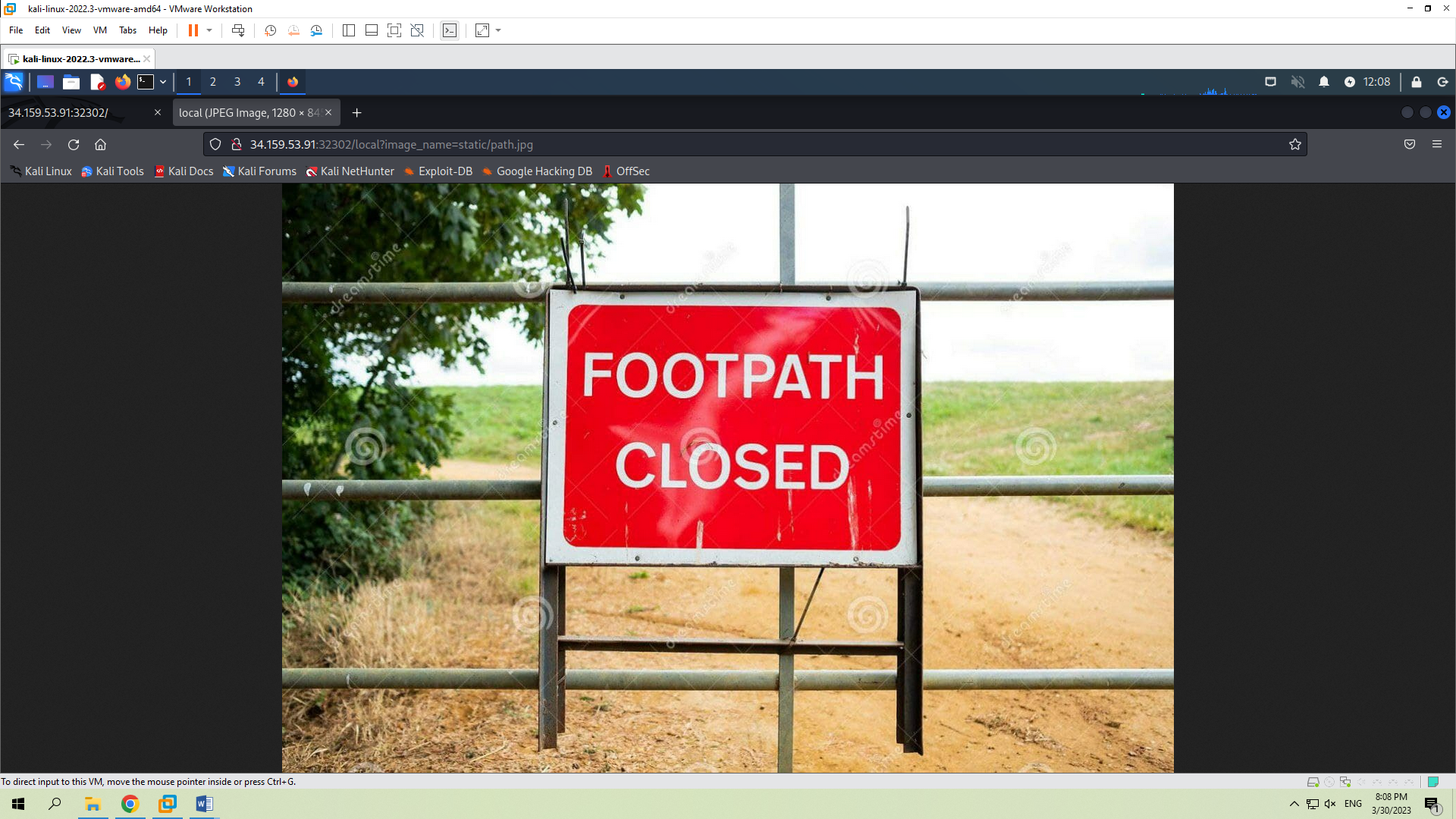
1. I tried to run a command that could bring flag. Is command didn’t work, that’s why I used cat command for bringing out content, what was written in flag and it worked, which was a vulnerability.

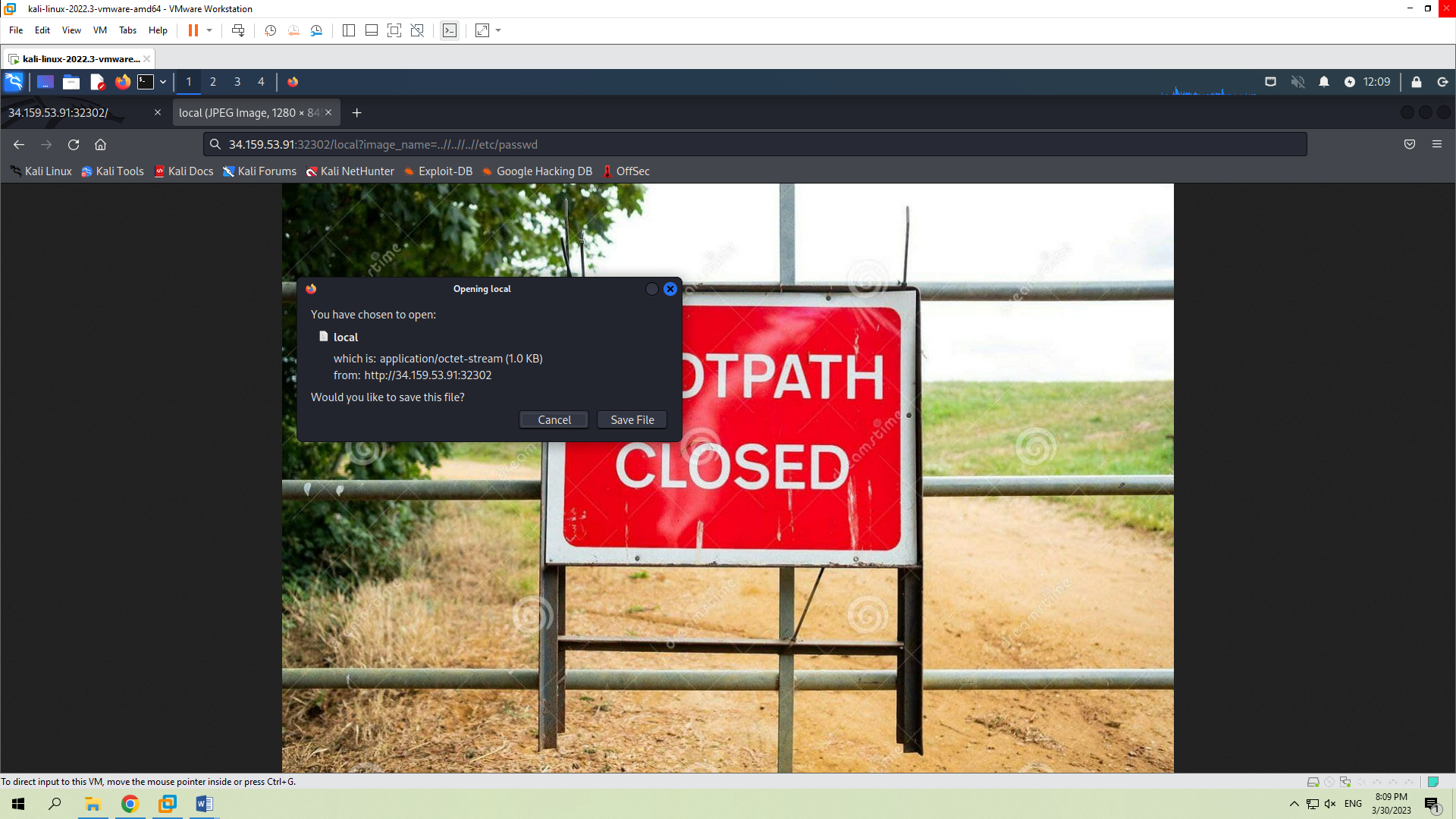


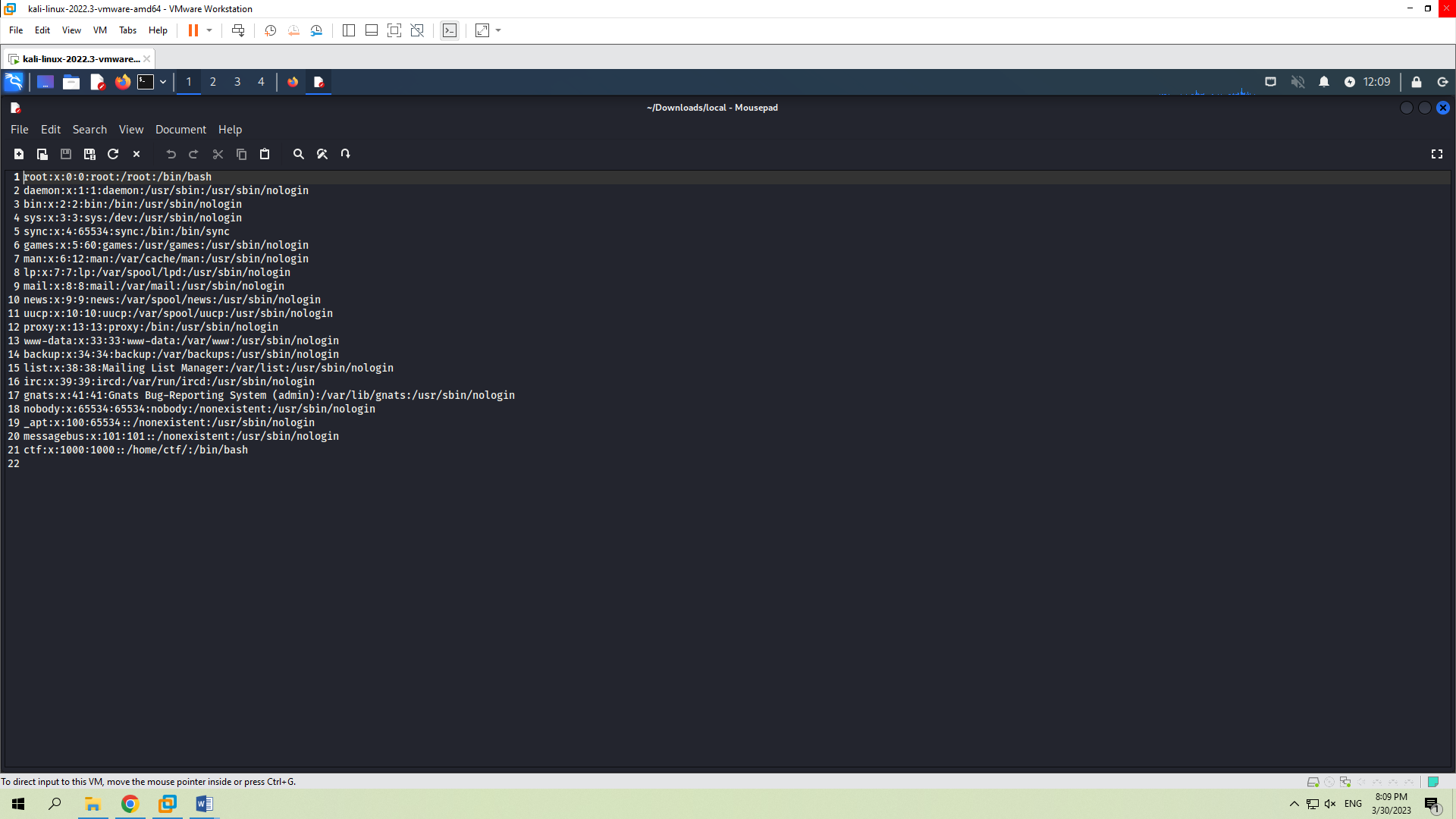


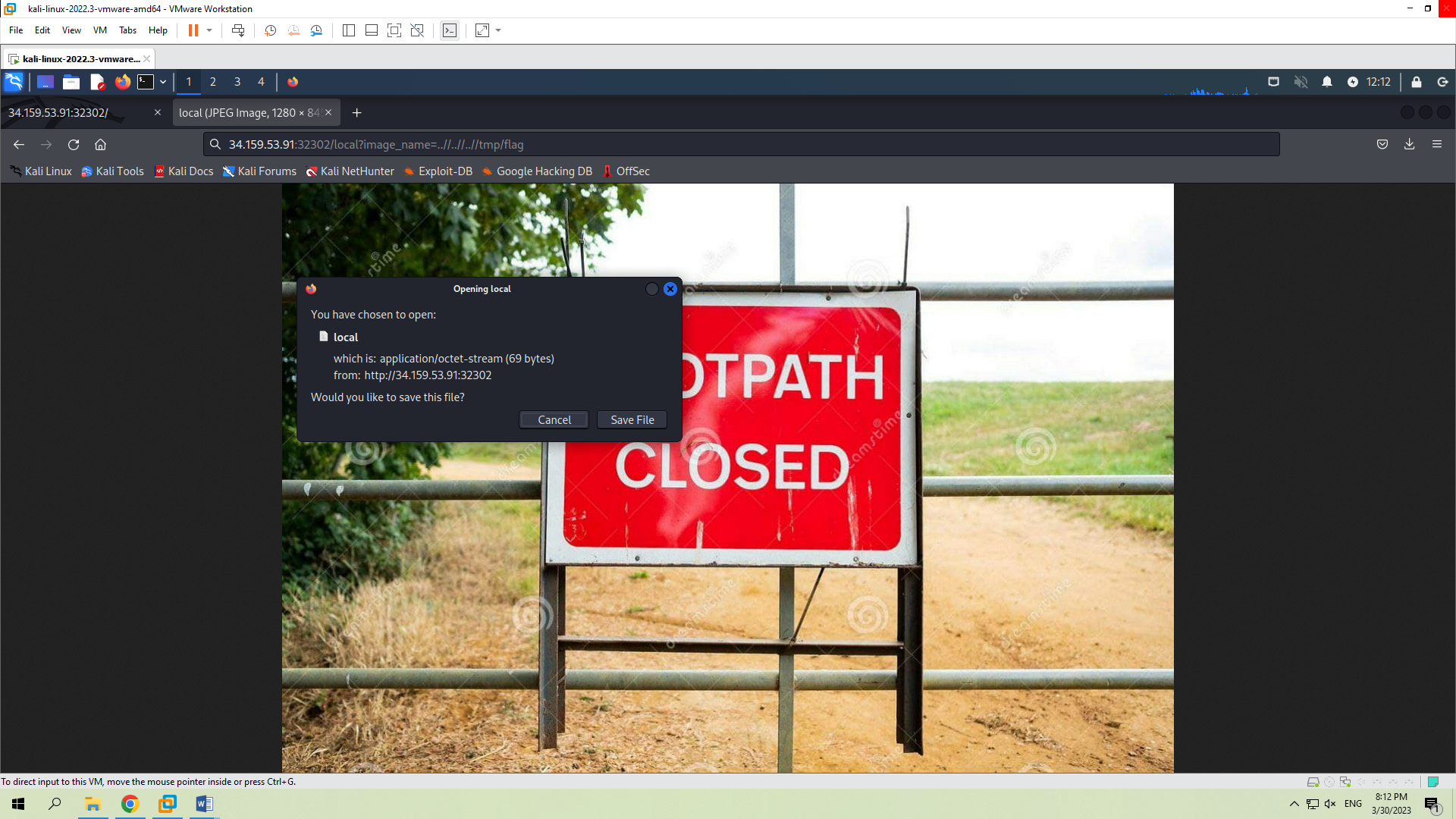
1. In the first screenshot I right clicked the photo and pressed copy image link to open it in new tab. Afterwards I tried a simple payload, where we got the result as a simple file. After that I used different directory, which gave me the satisfactory result and we see a file where flag is written in the last screenshot.

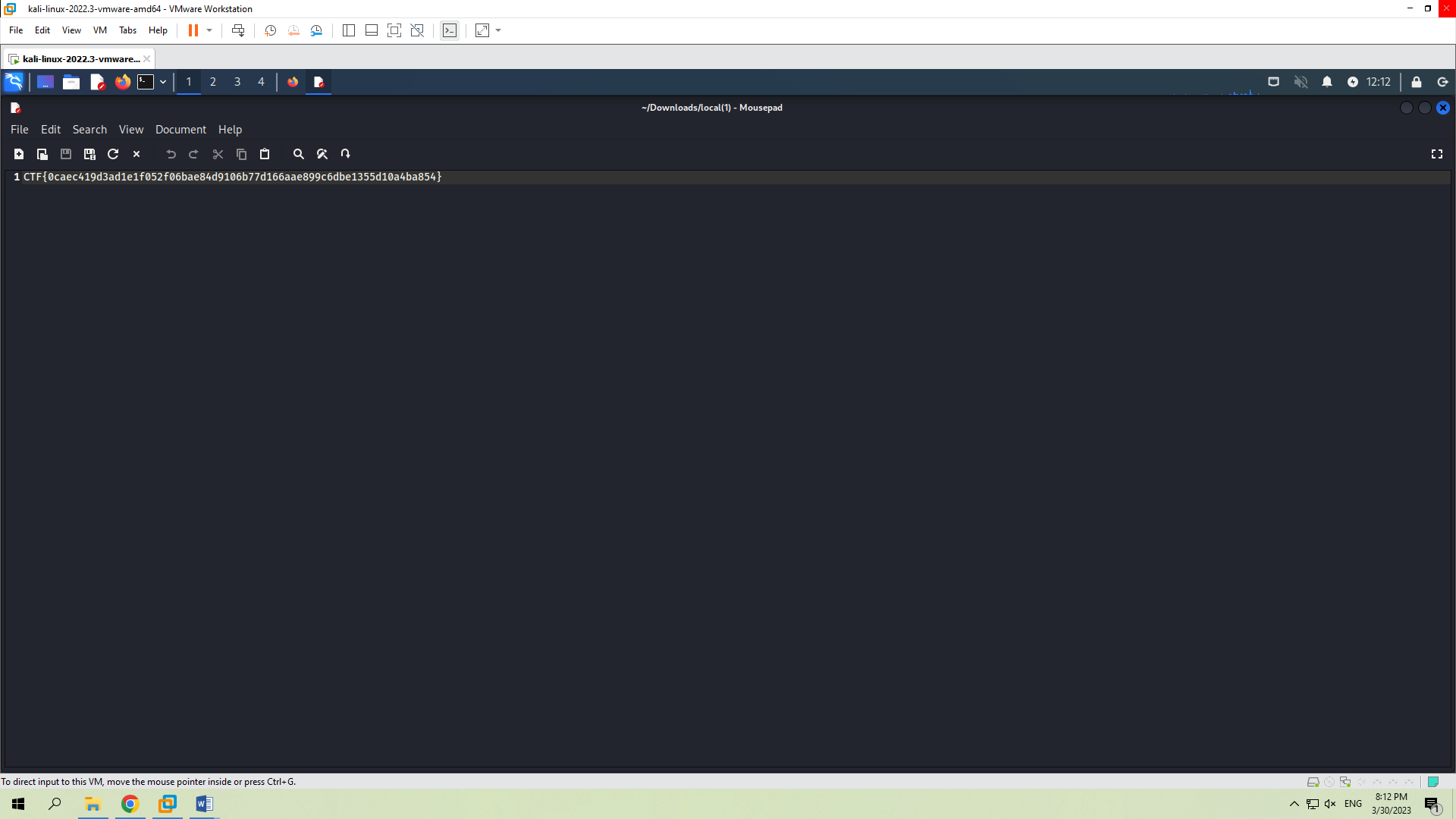












1. Gathered information from the site and built the following command given in the screenshot below, where –data attribute gives us info from a request and in start parameter we can use the name of flag file.

