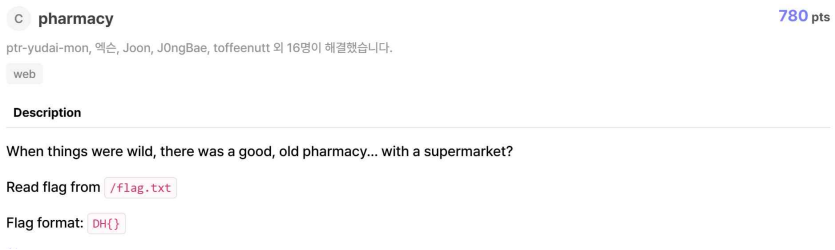
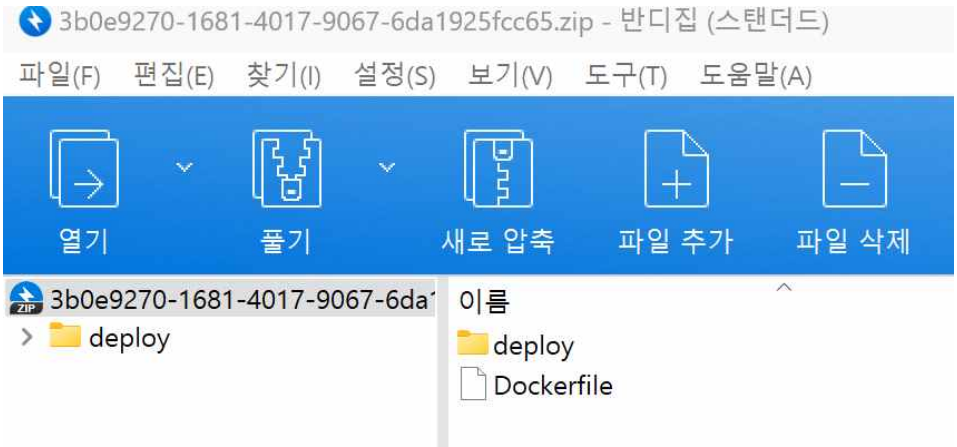
<Dreamhack CTF Season 5 Round #10>

Season 5 #Round 10 중 pharamacy를 선택했다. 선택에 별다른 이유는 없었고 그냥 '약학'이라길래 선택했다. 그리고 뒤늦게 알았지만 레벨3이라고 해서 후회했다.



설명을 보니 /flag.txt 파일을 열면 그 안에 flag가 있는 형식인 것 같다.

파일을 다운 받으니 여느 때와 같이 압축을 푸는 단계가 필요했다.



압축을 풀고 나니 파일이 생각보다 많았는데 그 중 Dockerfile을 메모장을 사용해 열었다.

```
FROM php:7.4-apache

COPY ./deploy/run.sh /usr/sbin/
RUN chmod +x /usr/sbin/run.sh

COPY ./deploy/src /var/www/html
RUN chmod 777 /var/www/html/uploads

COPY ./deploy/flag.txt /

EXPOSE 80
CMD ["/usr/sbin/run.sh"]
```

뭐 하라는건지 모르겠어서 일단 최대한 해석해보았다.

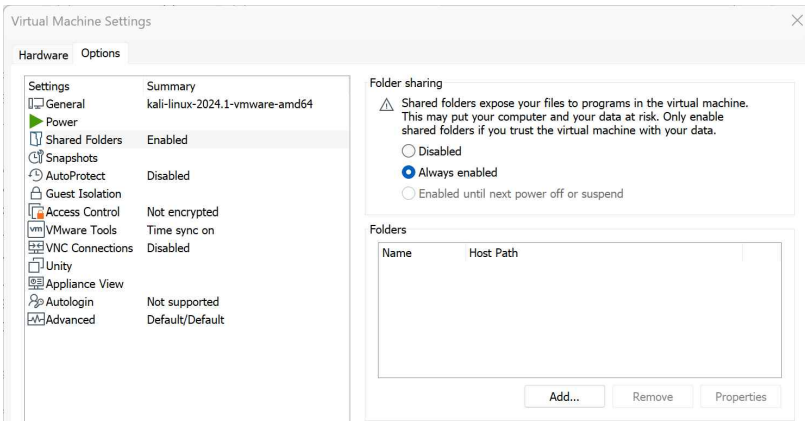
1. /usr/sbin/run.sh 파일을 복사하고 실행 권한을 부여한다
2. ./deploy/src 디렉토리의 파일들을 /var/www/html에 복사한다
3. /var/www/html/uploads 디렉토리의 권한을 777(읽기, 쓰기, 실행)로 설정한다
4. /flag.txt 파일을 복사한다
5. 80번 포트를 노출한다
6. run.sh 스크립트를 실행한다

앞서 말한 것과 같이 “Read flag from /flag.txt” 라고 안내 되어 있으니까 해당 텍스트 파일에 들어가면 Flag 값이 있을 것 같다. 칼리 리눅스를 사용하려고 하는데 문제는 칼리에서 윈도우로 다운 받은 Dockerfile을 여는 방법을 모르겠다.

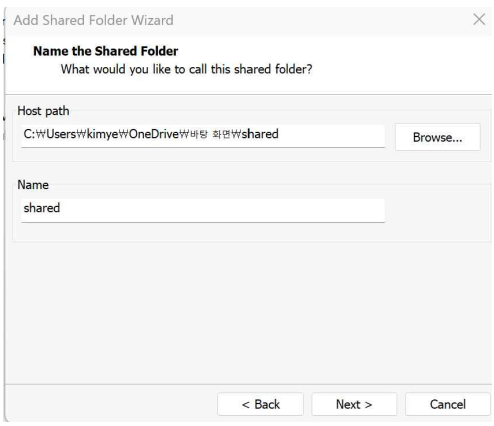
구글링을 해 본 결과 공유 기능을 사용하면 윈도우의 파일을 리눅스에서도 열 수 있다고 하여 Window에서 다운 받은 파일을 Linux로 전송 및 공유하는 방법을 찾아보았다.

알게 된 방식대로 다음과 같이 실제로 시도해보았다.

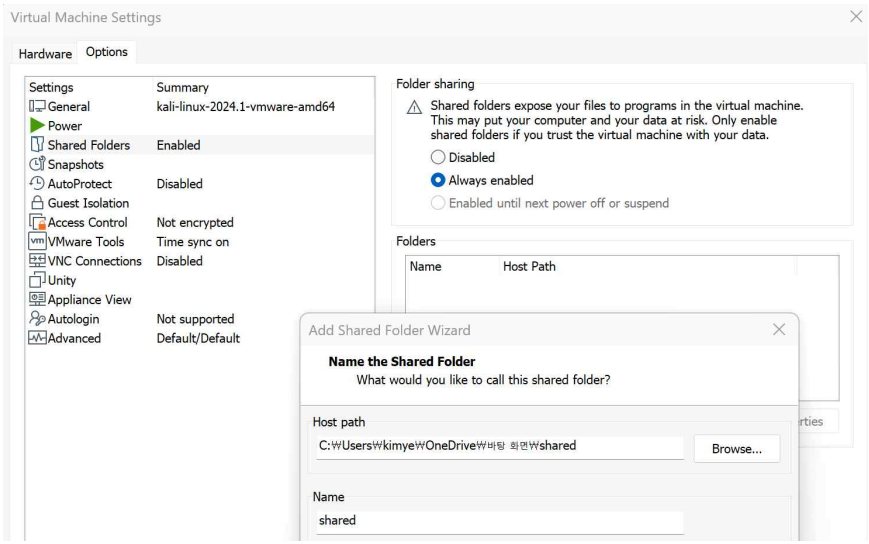
1. Edit 창을 열고 Option을 열어서 Shared Folders로 들어가 공유 기능을 활성화한다.



2. 공유하고자 하는 파일의 경로를 명시하고 이름을 설정한다.

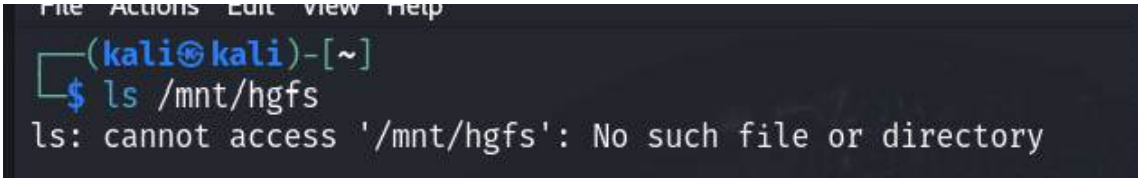


전체적인 화면으로 보면 다음과 같은 상태이다.



공유하라는 방법대로 공유하고 공유가 잘 되었는지 확인하기 위해서 ls /mnt/hgfs를 입력했는데 해당 디렉토리가 파일이 존재하지 않는다고 뜬다. 원래 공유가 성공적으로 이루어지면 해당 디렉토리에 마운팅이 된다는데 뭐가 잘못된 건지 전혀 모르겠다.

원래 해당 명령어를 입력하면 Shared Folder 목록이 떠야 하는 것 같은데 안 뜬다.

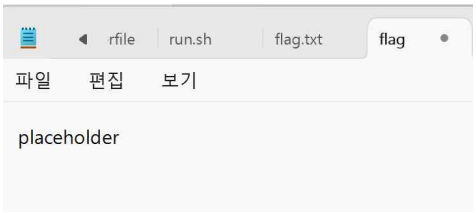


마운팅이 먼저 필요한가 해서 다른 명령어를 입력해봤는데 이 방법도 안 된다.

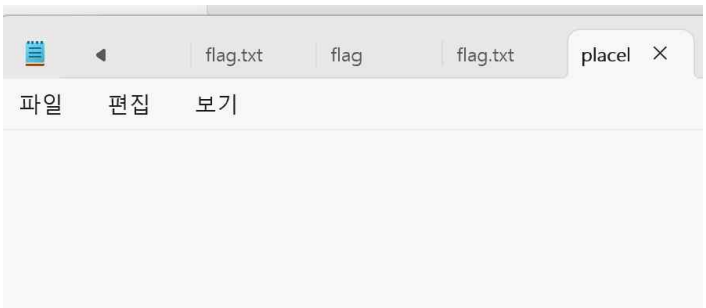
vmhgfs는 VMware Tools가 설치되면 자동으로 로드되는 거라는데 존재하지 않는다는 메시지가 뜬다. 가상머신에 VMware Tools가 설치가 안 되어 있는걸까?

여기서 어떻게 더 해야 할지 모르겠어서 일단 다른 파일들을 열어 보았다.

압축을 푼 파일에 있는 flag 텍스트 문서에 들어가보니 placeholder라고 적혀 있다.



scr 파일을 보니 placeholder 텍스트 문서가 또 존재해서 역시나 메모장으로 열어봤다.



아무것도 없는 빈 문서이다.

아.. 쉬운 레벨도 어려울 것 같아서 제일 쉬운 걸 하려고 했는데 아무 생각 없이 선택한 문제가 레벨3이었다. 어디서부터 공부를 해야 하는 건지 잘 모르겠다.

머릿속으로 구상한 방법은 Dockerfile을 칼리 리눅스로 열어서 flag.txt을 여는 것이었는데 칼리로 윈도우 파일을 여는 법을 모르겠어서 시도조차 못했다. 항상 시도 단계에서 뭔가 하나가 해결이 안 돼서 문제에 대한 접근도 못하게 되는 것 같다.