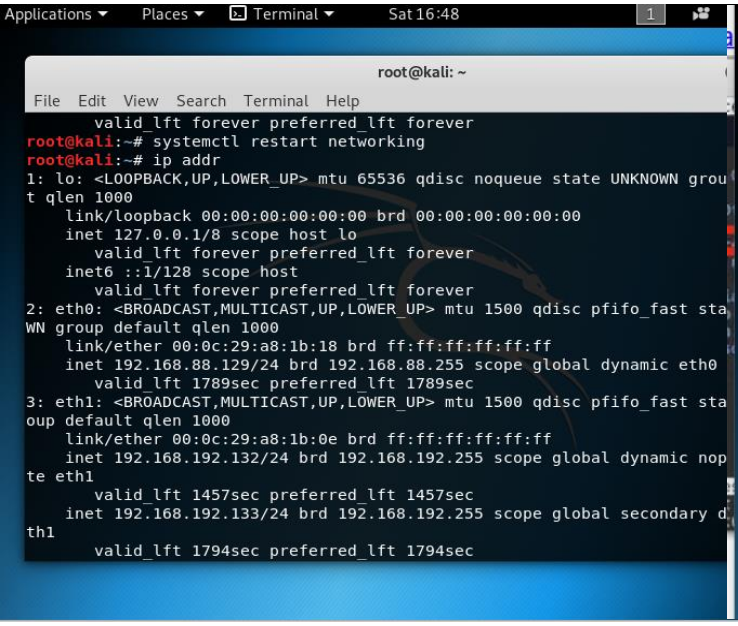
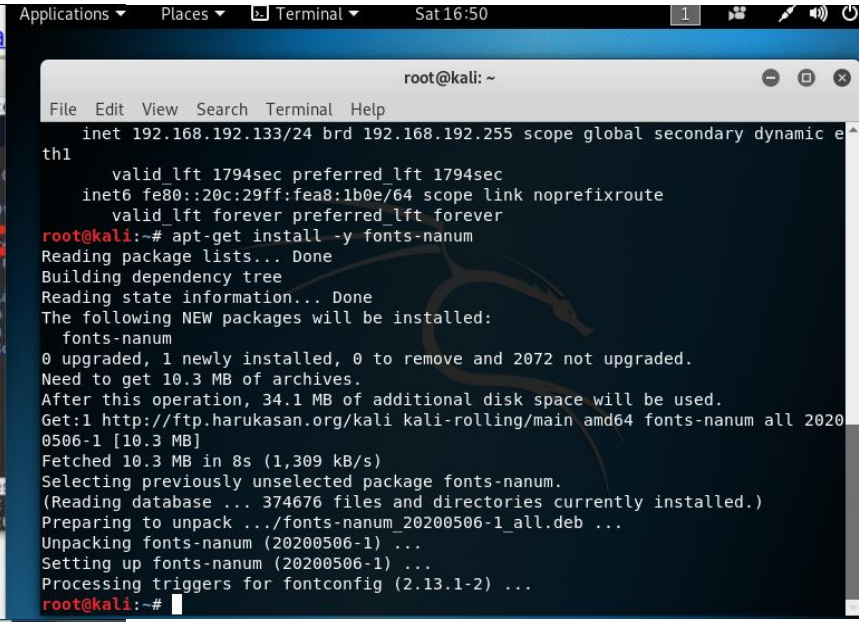
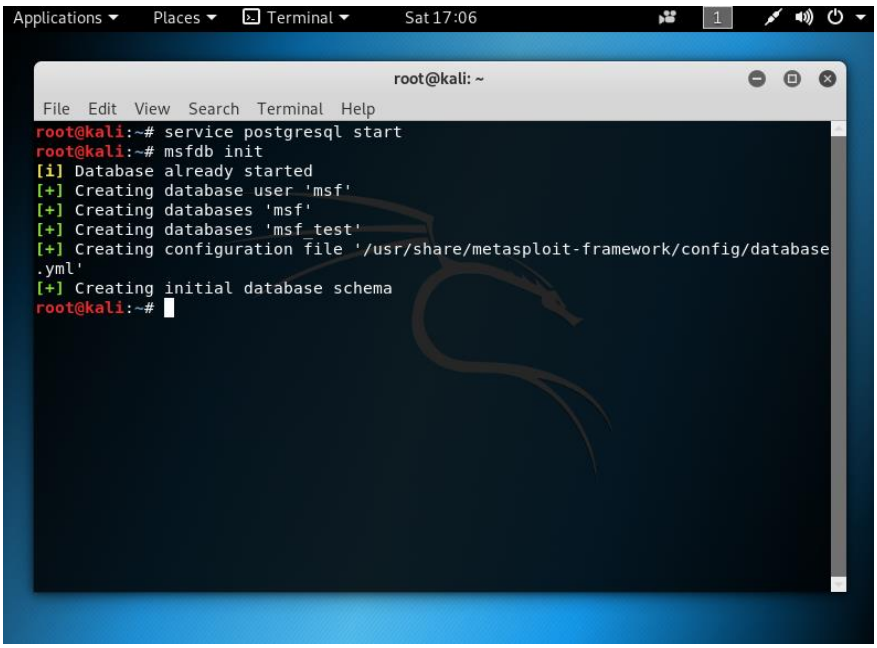
[7주차 웹해킹 과제] 2020111318 김수현

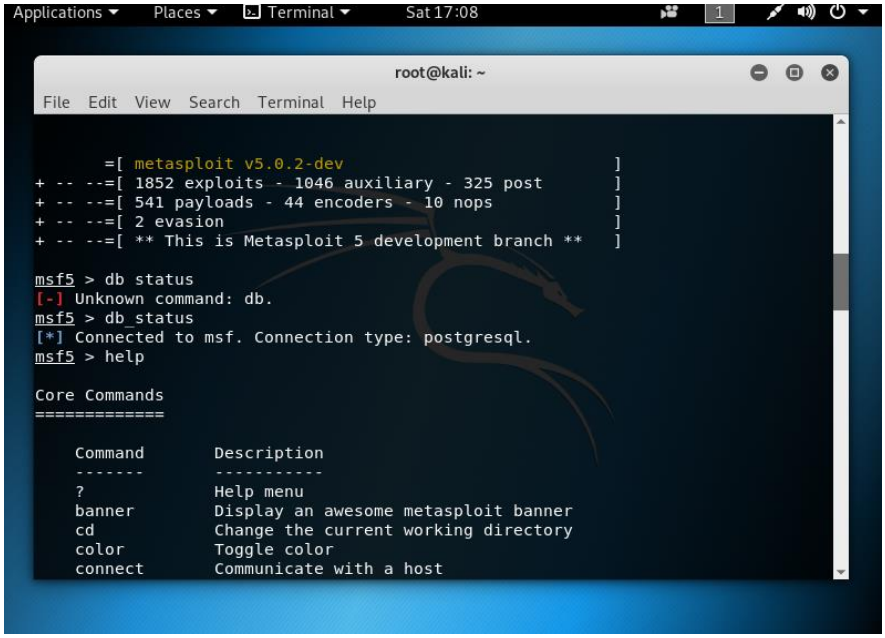




여러가지의 환경설정을 해준다-> systemctl restart networking -> ip addr -> apt-get install -y fonts-nanum

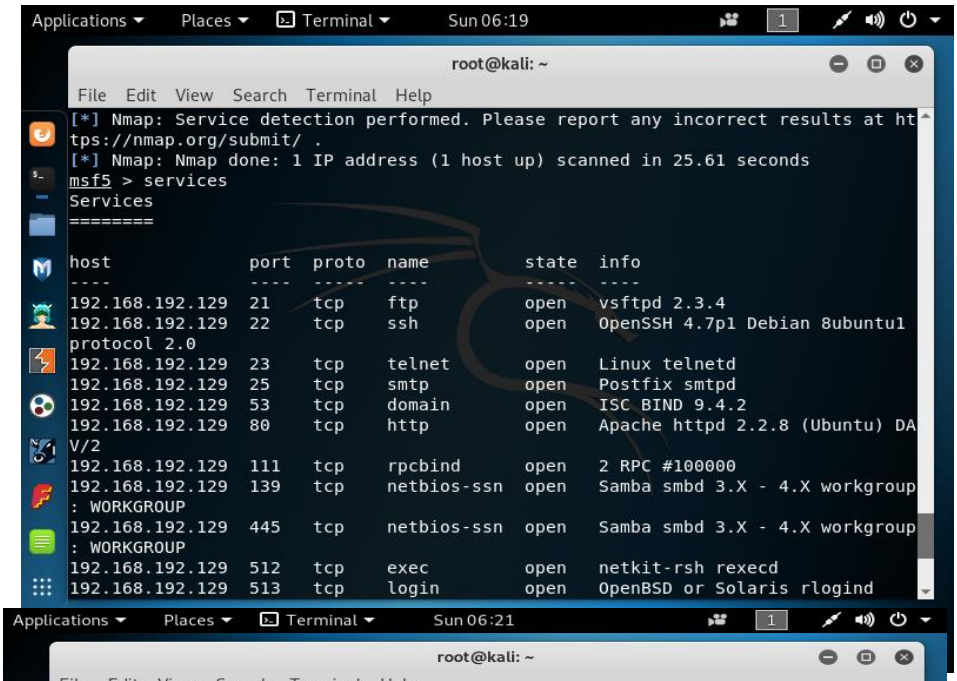


Db 에 연결하기 위해서 service postgresql start 를 입력한 후 msfdb init으로 Db 를 초기화해준다.



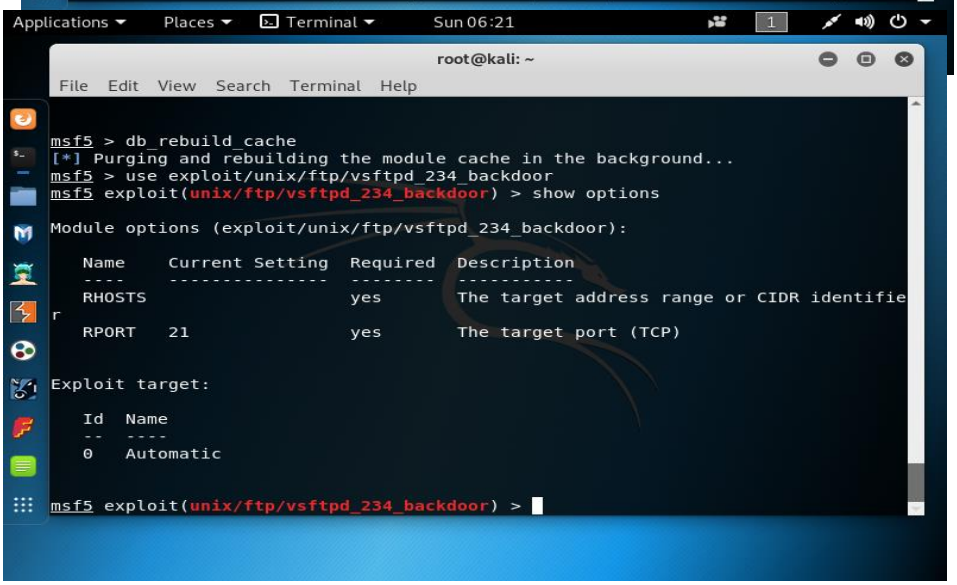
메타스플로잇을 실행시켜준 후 Db가 잘 연결되었는 지 확인하기 위해서 db status 명령어를 입력.

Help는 각 종 명령어들에 대한 설명을 자세히 볼 수 있도록 하는 명령어이다.

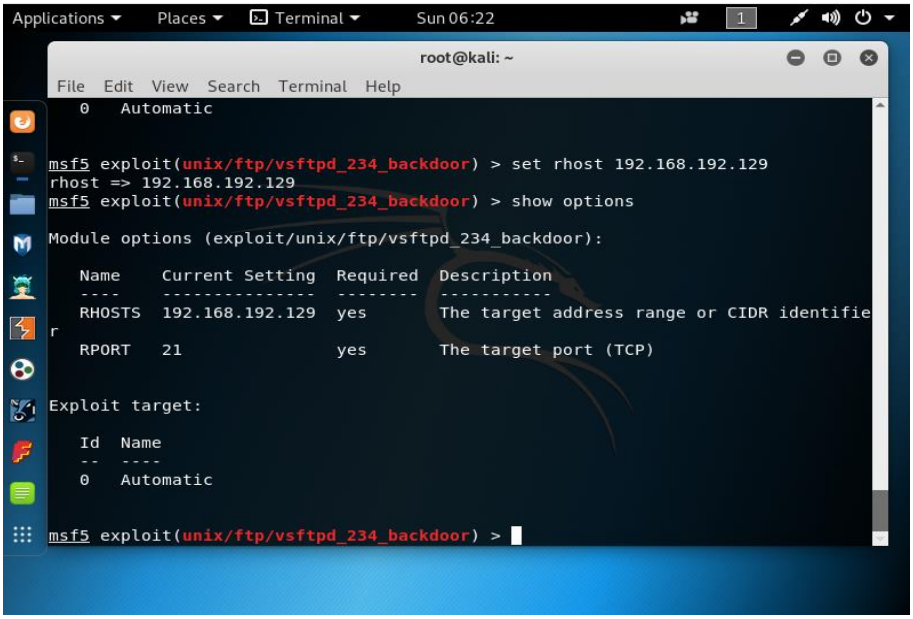


Db nmap (내 메타스플로잇 ip) -sV 를 입력하면, 버전 정보까지 알려준다. (사진 상에는 입력한 창을 캡쳐 하지 못했는데 Nmap이 있는 것으로 보아 위의 과정을 했다는 것을 증명한다.)

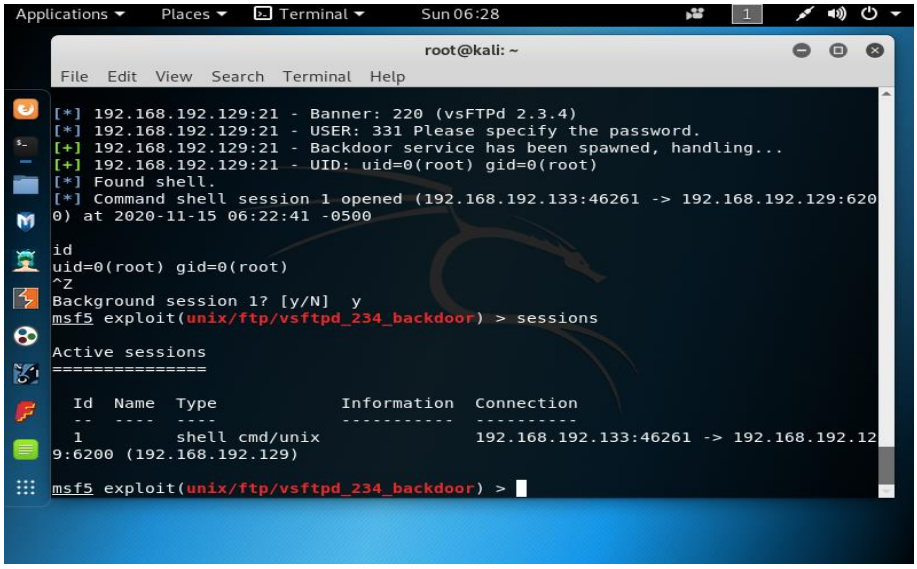
그리고 services는 nmap결과를 바로 확인할 수 있는 명령어이다.



Db_rebuild_cache 는 백그라운드로 캐시를 생성해서 모듈의 검색 속도를 높여주는 명령어이다. Use 는 search vsftpd해서 나온 name, show option은 설정해야 할 옵션을 확인할 수 있다.

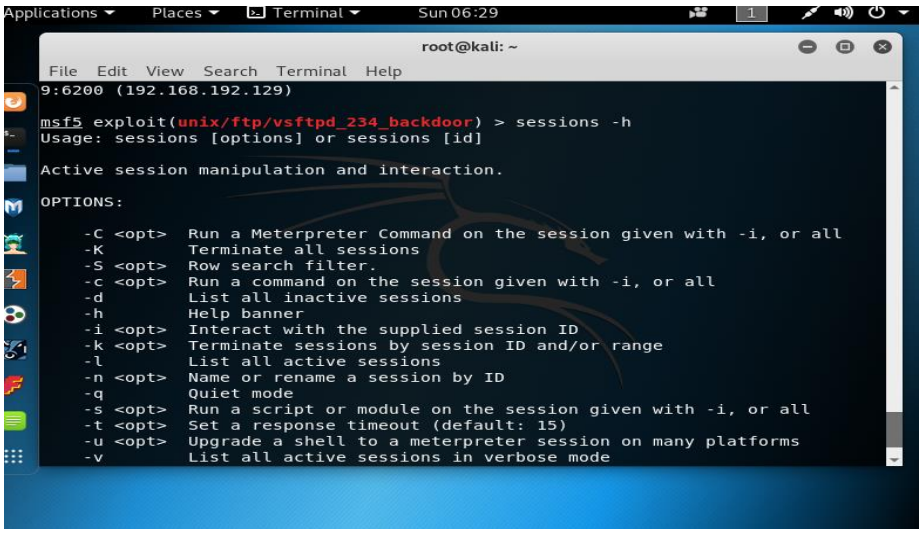


set rhost (내 메타스플로잇 ip 주소) 를 입력하면 rhost의 ip주소가 설정된다.

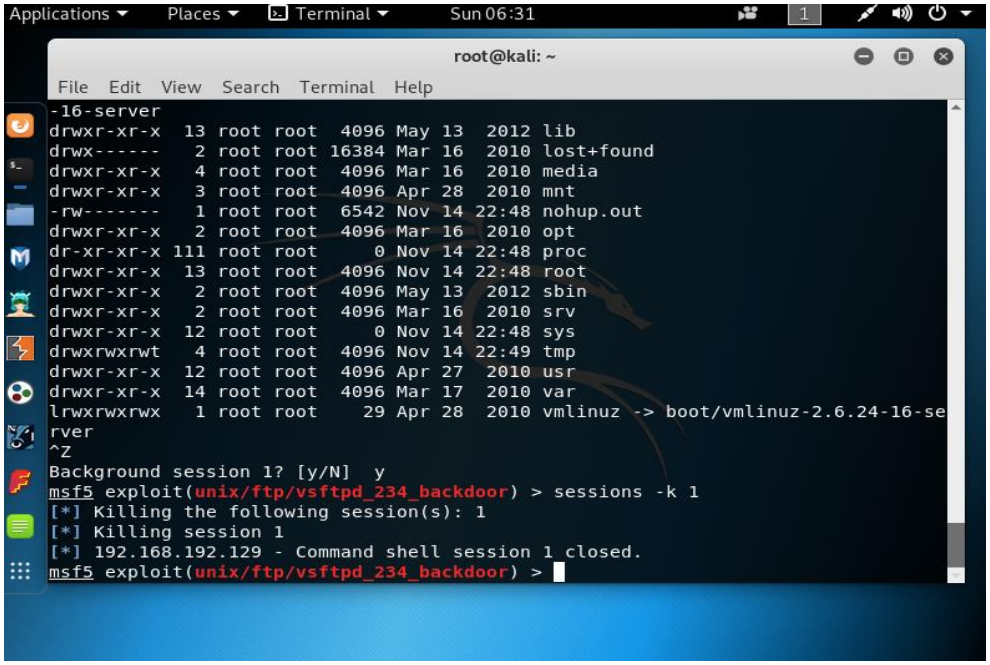


Run을 입력하면 모듈을 실행하므로, 공격에 성공했다는 출력이 뜬다. Id를 입력하면 uid와 gid가 모두 root인 것을 알 수 있다. Ctrl+z를 누르면 세션을 백그라운드로 만들 수 있다.

Sessions는 백그라운드에 열려있는 session의 정보를 간단하게 표시한다.



Session -h는 세부 옵션을 표시하는 명령어이다.



sessions -k의 명령어를 입력하면 세션이 종료된다.