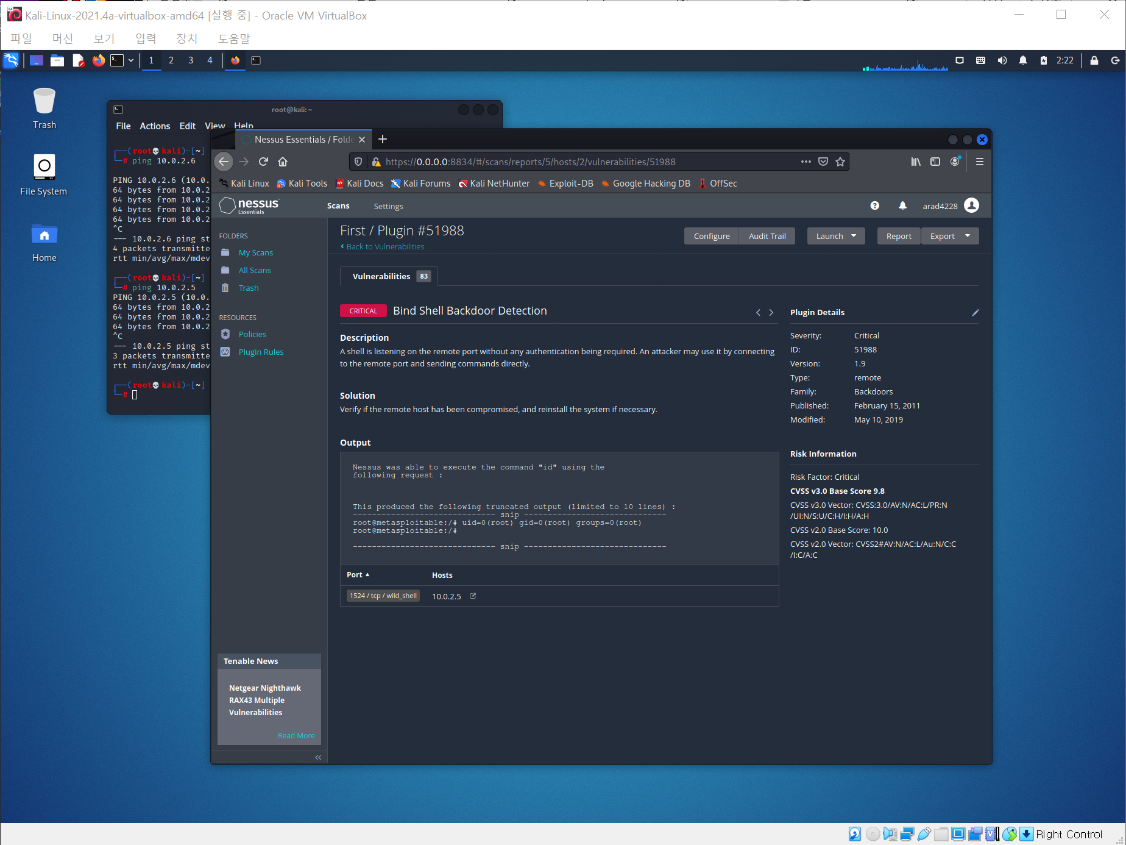
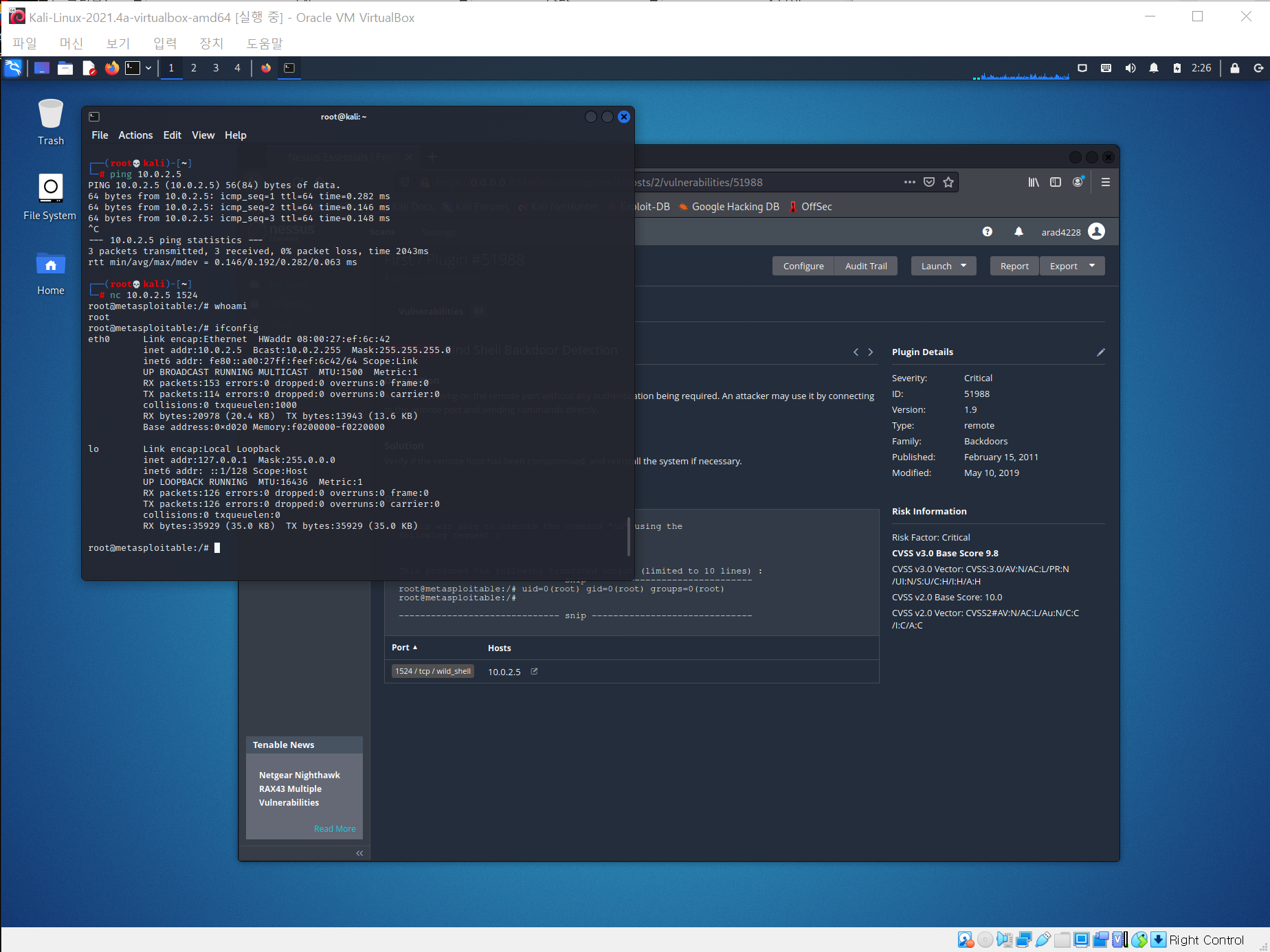
Attack을 할 취약점

  
이를 공격하는 방법은 아래의 포트번호를 통해 취약점을 공격할 것이다.  
아래의 명령어를 통해 타겟의 포트를 연결한다면 다음과 같은 결과를 얻을 수 있다.

1. nc [Metasploitable2의 주소] [공격 포트번호] ex) nc 10.0.2.5 1524  
   연결이 됬다면 whoami를 통해 누구로 접속했는지 알 수 있다.

  
현재 상황을 보면 다음과 같은 결과가 벌어진다.  
Bind Shell Backdoor Detection을 통해 해당 포트로 접속하여 Metasploitable2의 Shell을 얻게 되었다.

그후 whoami를 통해 root의 권한을 얻고 있음을 알게 되었다.

따라서 우리는 root의 권한을 얻었기에 많은 일들을 할 수 있다.

그중 우리는 사용자의 password의 hash 정보를 가지고 있는shadow 파일을 접근해 볼 것이다.