**Kali Linux Tutorial Final mission**

이번 강의의 마지막 mission이다. 주어진 VM은 mailer라는 이름을 가지고 있었다. 처음에는 무슨 의미일까 싶었는데 nmap을 통해 scan을 해본 결과 21, 22, 25번 port가 열려있는 것을 확인할 수 있었다. 각각 ftp, ssh, smtp port에 해당된다. 또한 VM의 이름이 mailer인 것을 보아 mail과 관련된 문제라고 생각했다.

처음에 nmap scan을 할 때 scan 방식을 잘못 잡아서 꽤 먼 길을 돌아갔다. ftp의 경우vsftpd가 동작 중이었는데 버전이 3.0.2로 exploit 가능한 부분은 없는 것을 확인하였다. 다음으로는 smtp와 관련하여 시도하였는데 smtp의 경우 exim4를 사용하여 동작 중이었다. 물론 여러 exploit code를 찾아서 실행해보았지만 이렇다 할 결과는 얻을 수 없었다.

그래서 다시 nmap scan을 시도하였는데 이 때 ftp에서 anonymous login이 enable 되어 있는 것을 확인할 수 있었으며 어떤 파일이 존재하는 것을 확인할 수 있었다. 해당 파일에는 3개의 username과 password가 적혀 있었으며 ssh 접속에 사용할 수 있는 계정이라고 설명되어 있었다. 3개의 게정 중 하나의 경우 VM의 네트워크 주소 확인을 위한 계정이라고 하였기에 나머지 두 개의 계정에 대해 접속하여 힌트를 얻기로 하였다.

먼저 patty 계정으로 접속하였는데 확인할 수 있는 파일들을 찾아본 결과 Maildir/new 경로에 mail이 하나 존재하는 것을 확인할 수 있었다. 해당 메일은 administrator로부터 온 auto reply로 자신이 부재 중이기에 긴급한 메일의 경우 paul에게 보내라고 적혀 있었다. 그렇기에 paul 계정으로 접속하여 다시 파일을 확인해보았다. 그러나 paul 계정에는 administrator로부터 자신이 자리를 비우기에 대신 맡아달라는 내용의 메일만 있었다. 사실 여기서 가장 중요한 단서를 놓치게 되어 헤매게 되었는데, 메일에 my password is : 하고 문장이 있었는데 이 부분을 제대로 읽지 못해서 뻘짓을 하였다.

어찌되었든 paul 계정에서 administrator의 password를 알 수 있게 되었으므로 해당 정보로 ssh 로그인을 하면 메일에 취약점이 존재한다는 제보의 내용이 있다. 원래라면 해당 링크에 접속하여 exploit code를 획득할 수 있는 것으로 보이는데 code의 download link가 먹통이 되었다!.. 그래서 keyword를 통해 다른 epxloit code를 찾아냈다.

https://www.exploit-db.com/exploits/11651

결과적으로 root 권한을 획득할 수 있었고 목적을 달성할 수 있었다.