**Mission 1**

mission의 내용은 간단하게 target system을 하나 제공해주고 해킹하는 것이었다. 제공받은 target VM에 직접적으로 로그인 할 수 없었기에 DHCP service가 동작중인 네트워크 대역에 할당하여 사용하였다.

target에 대한 정보가 하나도 없기에 우선 IP address를 특정하기로 했다. Nmap -sn [network range]를 통해 ping scan 방식으로 찾아냈다. hostname이 VM의 이름과 같아서 쉽게 찾을 수 있었으며 IP 주소는 192.168.219.89였다.

그 후 target system을 대상으로 port scan을 진행하였을 때 open 되어 있는 port는 tcp 22, 80번 port였다. 80번 port에서 Apache2 service가 동작하고 있었기에 browser에서 http://192.168.219.89 주소로 접속하였다. 접속을 하면 고양이 두 마리가 같이 있는 메인 페이지가 있고 하단에 두 개의 메뉴는 각각 고양이에 대한 설명글로 보였다. 메인 페이지의 경우 별다른 특이점이 안보였기에 우선 smooch라는 고양이 페이지에 접속하였다.

페이지에는 고양이 사진과 짧은 설명글이 있었다. 처음에는 설명글의 경우 별로 중요한 내용이 없는 줄 알고 넘겼었으나 이후 다시 확인해보니 다음과 같은 메시지를 발견할 수 있었다.

*“그녀는 무언가 숨기는 것을 매우 좋아한다. 어쩌면 당신에게도 그녀가 무엇인가를 숨기고 있을 수 있다.”*

해당 메시지를 기반으로 하여 우선 개발자 도구를 사용해 웹 페이지의 source code를 확인해 보았다. 놀랍게도 source code에 다음과 같은 내용을 찾을 수 있었다.

*<!-- Y2hlY2sgb3V0IHNtb29jaF9zZWNyZXQudHh0 -->*

html code 내에 주석문을 통해 위와 같은 내용이 있었고 이와 같은 구성은 Base64의 Encoding 중 하나기에 Base64 decoding을 하여 얻은 결과는 다음과 같다.

*check out smooch\_secret.txt*

smooch\_secret.txt 파일을 확인하라는 내용을 확인하고 http://192.168.219.89/smooch\_secret.txt 로 접속하였다. 해당 경로에도 Base64로 Encoding 되어있는 아주 긴 내용이 있었는데 Decoding한 결과 x509 형식으로 작성된 RSA Private Key였다.

RSA Private Key가 SSH 통신할 때 사용이 가능한 것 까지는 추측하였으나 어떤 계정으로 접근해야 하는지 몰라서 접속에는 실패하였다. 기존에는 root user로 시도하였으나 솔루션을 찾아본 결과 sm00ch user로 로그인이 가능했다. 참고로 sm00ch의 경우 웹 사이트의 하단에 written by sm00ch라고 적혀있다.

그 다음 root의 권한을 얻어야 하는데 여기서 문제는 현재 로그인한 sm00ch 계정도 SSH 개인키 인증을 통해 로그인한 것이기에 비밀번호를 모른다는 점이다. 그래서 솔루션을 슬쩍 봤는데 커널의 버전을 확인하더니 exploit code를 찾아서 root 권한을 얻었다. 강의 내용만으로 과연 kernel exploit에 접근할 수 있었을까 싶다. 우선 전체 솔루션 링크를 첨부하였다.

https://medium.com/infosec-adventures/zhr01-walkthrough-576277966225

위 kernel exploit은 처음 본 것이기에 공부를 더 해야하지만 여기서 알 수 있는 점은 /etc/issue 파일에 OS version이 명시되어 있고 uname -a 명령어를 통해서 kernel의 version을 확인할 수 있다는 것이다.