**Kali Linux Tutorial Mission 2**

두 번째 미션이다. Target 시스템을 VMWare에 load하고 가장 기본적인 주소와 open port에 대해 검색을 하였다. Ping scan(-sn)을 통하여 VM 이름과 일치하는 주소를 가진 host를 찾을 수 있었으며 주소의 경우 192.168.219.67의 주소를 가지고 있었다.

다음으로는 nmap을 사용하여 port scan을 진행하였다. Port scan의 범위는 기본값으로 진행하였으며 tcp 8080 port만 열려있었다. 처음에는 열려있는 port가 너무 적길래 범위를 1부터 65535까지 지정하고 다시 하였음에도 결과에 변화는 없었다.

우선 http://192.168.219.67:8080으로 접속하였을 경우 간단한 웹 페이지를 만날 수 있었다. 기본 화면의 경우 간단한 화면 문구가 있었고 페이지 중앙 부분에 Powered by Struts라고 흔히 볼 수 있는 웹 제공자 문구가 있었는데 해당 문구에 마우스를 올릴 경우 하이퍼링크로 연결된 다른 페이지를 볼 수 있었다.

nessus를 사용해서 취약점을 확인한 결과 apache tomcat이 동작 중이었으며 tomcat의 기본 파일(eg. Manager) 등이 존재한다고 하였다.

Nmap Script Engine : 스크립트를 통해 취약점이 exploit 가능한지 파악

기본적으로 /*usr/share/nmap/scripts* 경로에 있음.

Powered by struts라는 문구를 아까 볼 수 있었는데 이를 토대로 apache struts의 취약점을 이용한 공격을 하는 것으로 보임. 취약점이 꽤 있는 것으로 보이는데 이 중 CVE-2017-5638을 이용하여 진행하였다.

Nmap script engine을 사용할 때 사용할 스크립트의 경우 --script=[file name]을 통해서 지정할 수 있고 스크립트 실행 시 사용할 arguments의 경우 --script-args [argument name]=[value]를 통해서 지정할 수 있다. script의 argument 목록의 경우 <https://nmap.org/nsedoc/>페이지에서 확인하고자 하는 스크립트 명에 해당하는 항목을 클릭하면 관련된 자세한 내용과 사용 가능한 arguments를 확인할 수 있다.

Metasploit에서 해당 CVE에 해당하는 exploit module을 찾을 수 있었다. 찾는 방법의 경우 search cve:[CVE 뒤 4자리] 를 통해서 쉽게 검색할 수 있다.