REPORT

SW보안개론

(2번과제: pen test : 소프트웨어 취약점을 이용한 권한상승)



**과목명 :SW보안개론**

**분반 : 1분반**

**교수명 :조성제**

**학 과 : 소프트웨어학과**

**학 번 : 32162566**

**이 름 : 안찬웅**

**2022년 5월 23일**

EMB0000356c3453

<목 차>

I. Pen test : 소프트웨어 취약점을 이용한 권한상승

A. LSE 스크립트를 통해 확인한 취약한 software 정보 캡쳐본 3

B. ‘3.2 과제설명’ – ‘사용자 정의 함수에 명령어 추가하여 실행’ 부분에서 등장하는 [table]그림 4

C. ‘3.2 과제설명’ – ‘생성한 rootbash 실행을 통한 root 권한 획득’을 수행했을 때, id 명령어 4

D. 전체 pen testing 과정의 원리 및 pen testing 방법 설명의 체계성 5

**A.**

텍스트, 모니터, 스크린샷, 화면이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

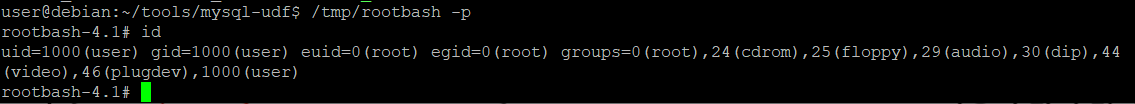
자동 생성된 설명

**B.**

텍스트이(가) 표시된 사진

자동 생성된 설명

**C.**



**D. 전체pen testing 과정의 원리 및pen testing 방법 설명의 체계성**

Pen testing은 윤리적 해킹의 한 형태로 방어와 공격의 중요성과, 공격자가 사이버 보안 방어 기법을 성공적으로 손상시키는 정교함의 레벨을 측정하고, 효과적으로 공격을 탐지 및 대응할 수 있는지를 확인 가능하다. Pen testing framework는 4단계로 이루어져 있는데, 첫번째 Planning이다. 기대효과, 목표, 법적 영향력을 논의한다. 두번째 Discovery이다 테스트하고 취약점을 분석한다. 테스트 단계에서는 시스템 정보 수집 및 시스템을 스캔하기 위해 초기 프로세스를 수행하고, 취약점 분석은 CVE database 및 searching을 통해 scanning 을 수행하고, 호스트 서비스, 어플, os정보를 수집한다. 세번째 공격단계에서는 엑세스 권한을 획득하고 다양한 도구와 기술을 통해 침입한다. 그리고 권한상승에서 시스템에서 권한을 상승시켜 시스템을 장악한다. 그리고 시스템을 자세하게 살펴보고 그리고 추가 도구를 설치한다. 마지막 reporting 단계에서는 취약점과 위험등급과 개선사항을 포함해 pen testing 수행내용을 reporting한다. raptor\_udf2.c코드는 system 함수로 인자로 들어온 명령을 수행하는데, MySQL에서 서브프로세스로 실행할 때 MYSQL이 루트 권한이면 거기서 system으로 호출되는 명령도 루트 권한으로 실행된다.