Connected-Car Service 대상

모의해킹 프로젝트

IT보안 **2**기 **_ 1**팀

김선혁, 정진섭, 최지훈, 황태영

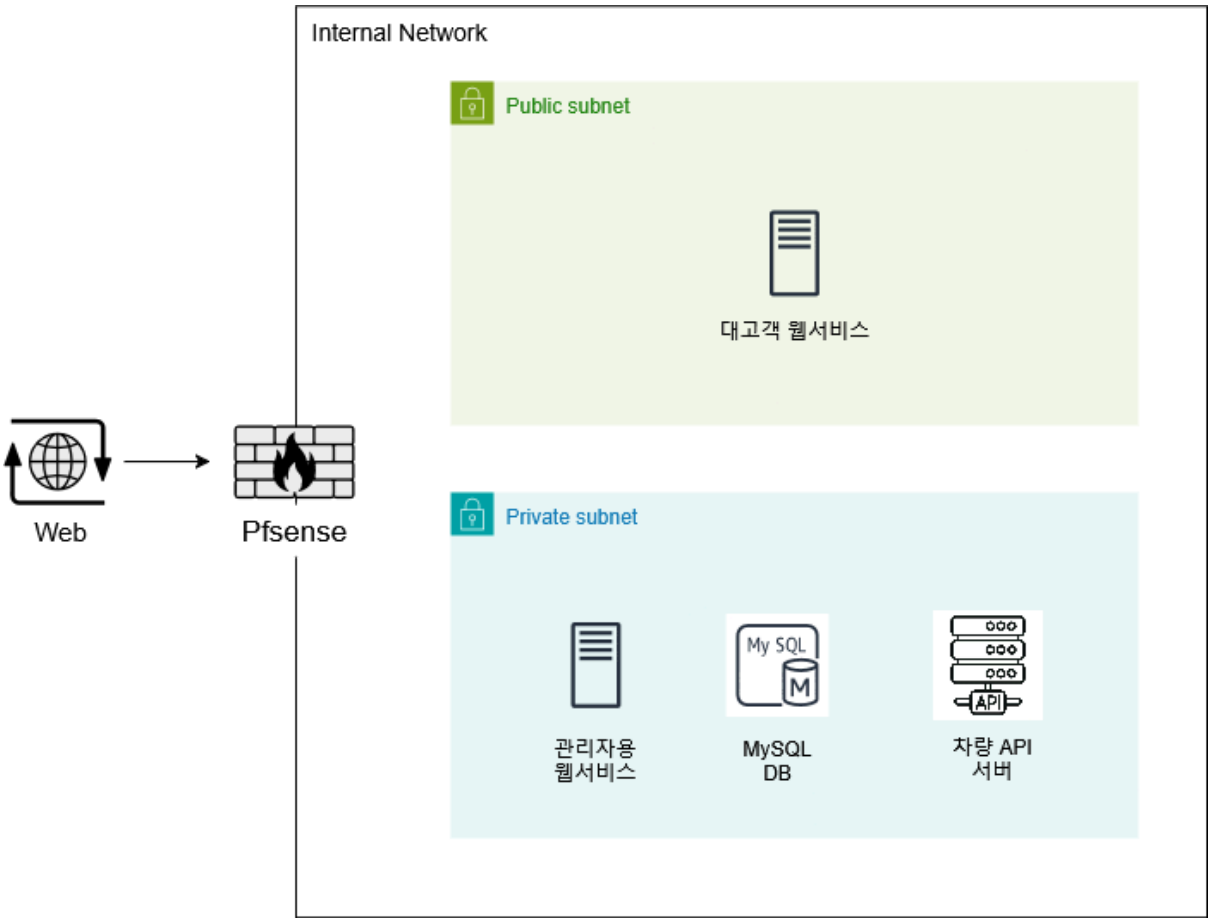
프로젝트 개요

자동차 기업의 커넥티드카 서비스와 유사한 웹 플랫폼을 구축하고, 실제 기업 환경과 유사한 네트워크 보안 아키텍처를 구성 후 모의해킹을 수행하는 프로젝트

프로젝트 목표

1. 실무 환경과 유사한 커넥티드카 웹서비스 개발
2. 차량 데이터 조회, 제어 등 Connected-Car Service의 주요 기능을 구현하고, 이를 대상으로 취약점 점검 수행
3. 발견한 취약점을 대상으로 공격 시나리오 구성 및 모의해킹 수행
4. 수행된 모의해킹 시나리오 분석 및 피해 규모, 대응방안 도출

시스템 아키텍처



네트워크 구성 **(6**개 서브넷**)**

- pfSense 방화벽: WAN 서브넷
- ExterServers: 대고객 웹서비스용 서브넷
- InterServers: 내부 시스템 (관리자용 웹서버, 내부망 PC)용 서브넷
- DBServers: 내부 DB용 서브넷
- APIServers: 내부 API용 서브넷

VM 구성 **(**총 **6**개**)**

- pfSense VM: 방화벽/라우터
- 웹서버 VM: 커넥티드카 고객 서비스 (Flask + 바닐라JS)
- DB서버 VM: 사용자/차량 데이터 저장 (MySQL)
- 관리서버 VM: 관리자 모니터링 시스템
- 차량API VM: 차량 제어 핵심 시스템

기술스택

- BackEnd: Python Flask
- FrontEnd: HTML/CSS/Vanilla JavaScript
- DB: MySQL
- Network: pfSense, VMware Workstation
- 모의해킹: Kali Linux

수행 방법

1. 환경 구축
    - 웹 서비스 개발
    - 네트워크 토폴로지 및 서버 환경 구축
2. 취약점 점검
    - KISA 주요정보통신기반시설 기술적 취약점 분석 평가 상세 가이드
3. 모의해킹 수행
    - 발견된 취약점에 대해 공격 시나리오 설계 및 모의해킹 실행
4. 결과 보고 및 발표
    - 취약점 목록, 위험도 및 영향, 공격 실행 결과 등 정리

주요 기능

1. 고객용 웹 서비스

1-1. 사용자 인증 및 차량 등록

1-2. 차량 제어

- 원격 시동/끄기, 문열림/잠김, 경적, 실내 온도 조정

1-3. 차량 상태

- 시동 상태, 도어 잠금 상태, 문열림 상태, 배터리 잔량 조회, 차량 위치 조회,

1-4. 주행 기록

- 이동 경로, 운행 통계

** 실제 구현은 Mock

- 차량 API서버에서 JSON 응답만 리턴
- 실제 차량 없이 가상 데이터로 시뮬레이션
- "시동 걸림", "문 열림" 과 같은 상태 변경만 구현

2. 관리자 시스템 **(**관리 서버 전용**)**

2-1. 전체 차량 모니터링

2-2. 사용자 계정 관리

2-3. 시스템 로그 분석

기대 효과

- 기업 환경에서의 보안 아키텍처 개선 방향 제시
- 커넥티드 카 서비스 환경에서 발생 가능한 주요 보안 위협 이해