제어망의 서버,PC 등 OS로 구동되는 IT 기기의 보안 취약점 점검을 자동화 할 수 있는 기술 개발

고려대학교

인공지능사이버보안학과

4월 26일 미팅 자료

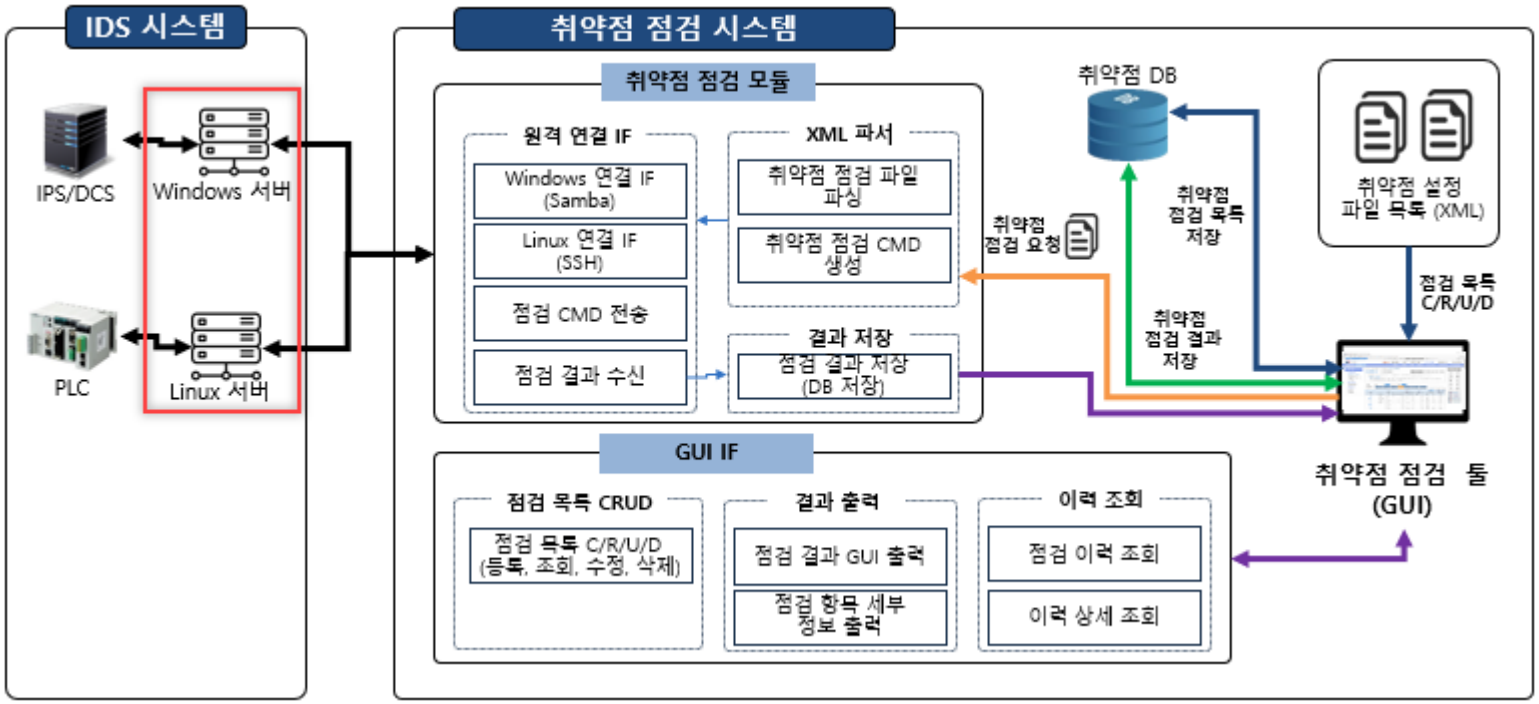
KOREA UNIVERSITY

CONTENTS

진행 상황

■ **확정된 목표**

□ L2 대상의 보안 취약점 자동 점검 기술을 개발하여, 현업에 가까운 개발을 경험 하는 것



취약점 점검 시스템 구성도

진행 상황

■ 상세 업무 분장

□ 기존의 나눴던 업무에서 실제로 어떠한 것을 맡을지 상세히 업무를 분장

```
* 규제지침을 통한 선별 및 스크립트 작성
    Windows server 취약점 규제지침 "계정 관리", "서비스 관리" , "DB 관리" 중 선별 후 스크립트 작성 및 문서화
제어시스템 규제지침 "계정관리", "서비스 관리", "패치 관리", "네트워크 접근통제" 중 선별 후 스크립트 작성 및 문서화
    -> 최정민님 담당

    Windows server 취약점 규제치짐 "패치관리", "로그 관리", "보안 관리" 중 선별 후 스크립트 작성 및 문서화
제어시스템 규제지침 "물리적 접근통제", "보안위협 탐지", "복구대응", "보안 관리" 중 선별 후 스크립트 작성 및 문서화
    -> 이도현님 담당

* 점검 모듈 구현

    3가지 함수로 작성

    점검 대상에 연결하는 함수
    -> 김연수님 담당

    xml 파일을 파싱하여 데이터를 추출하는 함수
    -> 오병윤 담당

    점검을 실행하는 함수
    -> 점검 대상에 연결
        -> 김연수님 담당
    -> 점검 실행 및 결과 DB Insert
        -> 오병윤 담당

* UI, DB 설계 및 개발
    DB설계, SW 상세설계서 작성, DB 구현, 입력 화면, 규제 지침 선택 화면, 진행 & 결과 화면 구현
    -> 김건희님 담당

     UI 설계, SW 상세설계서 작성, 취약점 점검/ 점검이력 조회 선택 탭, 이력 조회, 규제 지침파일 입력 화면 구현
    -> 조유빈님 담당
```

상세 업무 분장

진행 상황

■ 진행 상황 TODO List

□ 작성된 일부 점검 스크립트를 기반으로 점검 모듈 및 UI, DB 일부 구현

```
팀 TODO List

[TODO]

    중간 발표 준비
        -> 중간 발표 자료 작성


[DOING]

    점검 모듈 개발
        -> action 타입의 결과 성공/실패 여부 체크
        -> 점검 스크립트 테스트
        -> 결과 정리하여 InspectionItems 테이블에 데이터 Insert

    SW 상세설계서 작성

[DONE]

    스크립트 작성
        -> 일부 윈도우 스크립트 작성

    점검 모듈 개발
        -> ssh, samba 연결 코드 작성, 예외처리, 동작 테스트
        -> 선택된 규제 지침 XML 파일에서 필요한 데이터 파싱

    UI, DB
        -> DB 테이블 및 컬럼 설계 및 SQLite3로 구현
        -> 입력 화면, 규제지침 선택 화면 구현
            -> 입력값에 대한 정규표현식 적용
            -> DB에 입력된 값을 기반으로 알맞는 규제 지침 선택 테이블 생성
            -> 입력된 값과 선택된 규제 지침을 점검 모듈에 전달

[ISSUE]

   없습니다.
```

팀 전체 TODO List

진행 상황

■ 점검 스크립트 설계

□ 참고한 스크립트를 기반으로 점검 스크립트 태그 설계

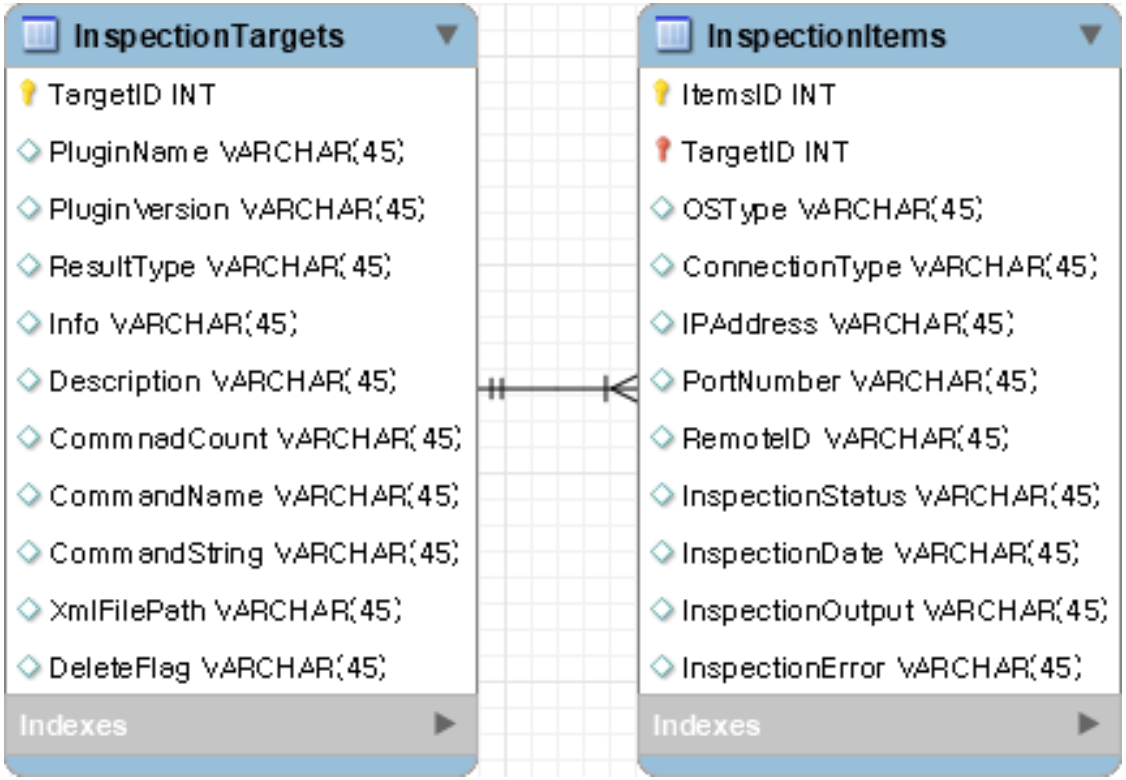
```
Result_Type - action, info, registry
CommandType - Powershell, cmd, Bash
PluginVersion - 1
PluginName - 플러그인 이름
TargetOS - Windows, Linux
CommandCount - 명령어의 개수 지정
CommandString - 명령어
Info - 해당 플러그인 간단 설명
Description - 해당 플러그인 세부 사항
```

스크립트 태그 및 설명

진행 상황

■ DB 설계

□ 취약점 점검 시스템 구성도에 따른 DB 테이블 및 컬럼 설계

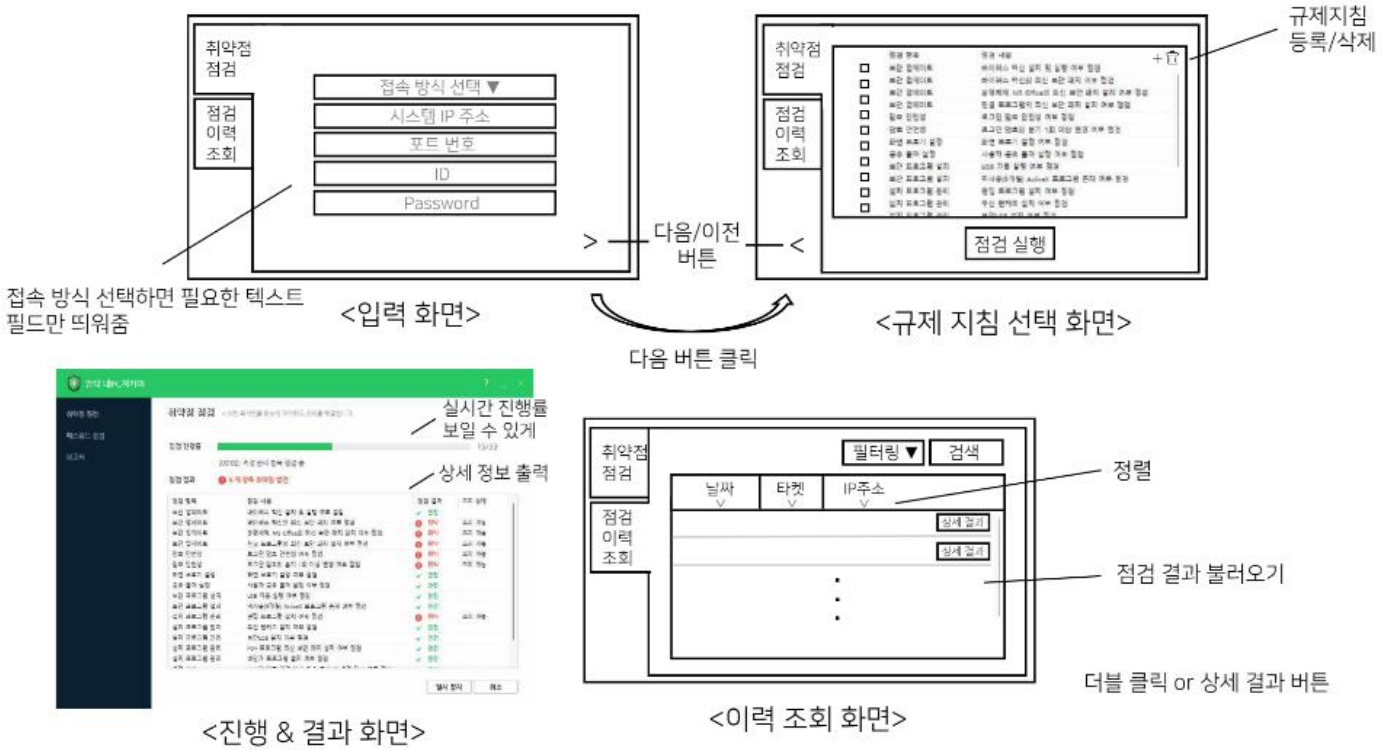


데이터베이스 관계도

진행 상황

■ UI 설계

□ 취약점 점검 시스템 구성도에 따른 UI 설계

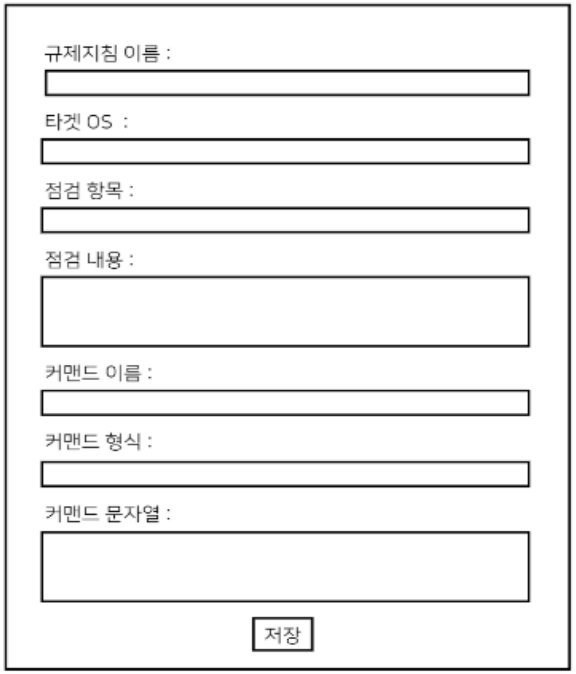


UI 설계 1

진행 상황

■ UI 설계

□ 취약점 점검 시스템 구성도에 따른 UI 설계



<규제 지침 등록 화면>

입력 시 xml 파일 생성

< 점검 이력 상세 결과 화면>

UI 설계 1

중간 발표 대비

■ 논의 사항

□ 목표의 타당성 제시

- 왜 Windows 서버와 Linux 서버에 대한 취약점 분석만 진행해도 되는지 명확한 이유가 필요
- 현업에 가까운 개발을 캡스톤 디자인에서 진행해야하는지에 대한 명확한 이유가 필요
- 실제 운영하는 제어망을 구성하고 있는 문서 및 근거 자료가 필요

□ 현업에 가까운 개발은 어떻게 진행하고 있는지에 대한 논의

- SW 상세 설계서는 현재 작성 중
- 개발 방법론(ex, 폭포수, 에자일)을 명시하여 적용해야 할지
- ~ 하게 진행하고 있어 현업과 최대한 비슷하게 진행하고 있다는 근거가 필요

□ 예상 결과물 논의

- 기존에는 자동 점검 프로그램, 사용 매뉴얼, 최종 보고서 3개가 예상되는 결과물
- SW 상세 설계서 또한 포함해야 하는지

Thank you

KOREA
UNIVERSITY