


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

2조 캡틴오와 선원들

목차

- 팀 소개
- 주제 개요
- 수행 일정
- 수행 내용
- 결론

팀 소개

캡틴오와 선원들



교수님

조금환 교수님



멘토님

심영복 대표님



이름 오병운

담당 자동화 모듈



이름 김연수

담당 자동화 모듈



이름 이도현

담당 점검스크립트



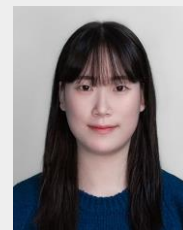
이름 최정민

담당 점검스크립트



이름 김건희

담당 UI & DB



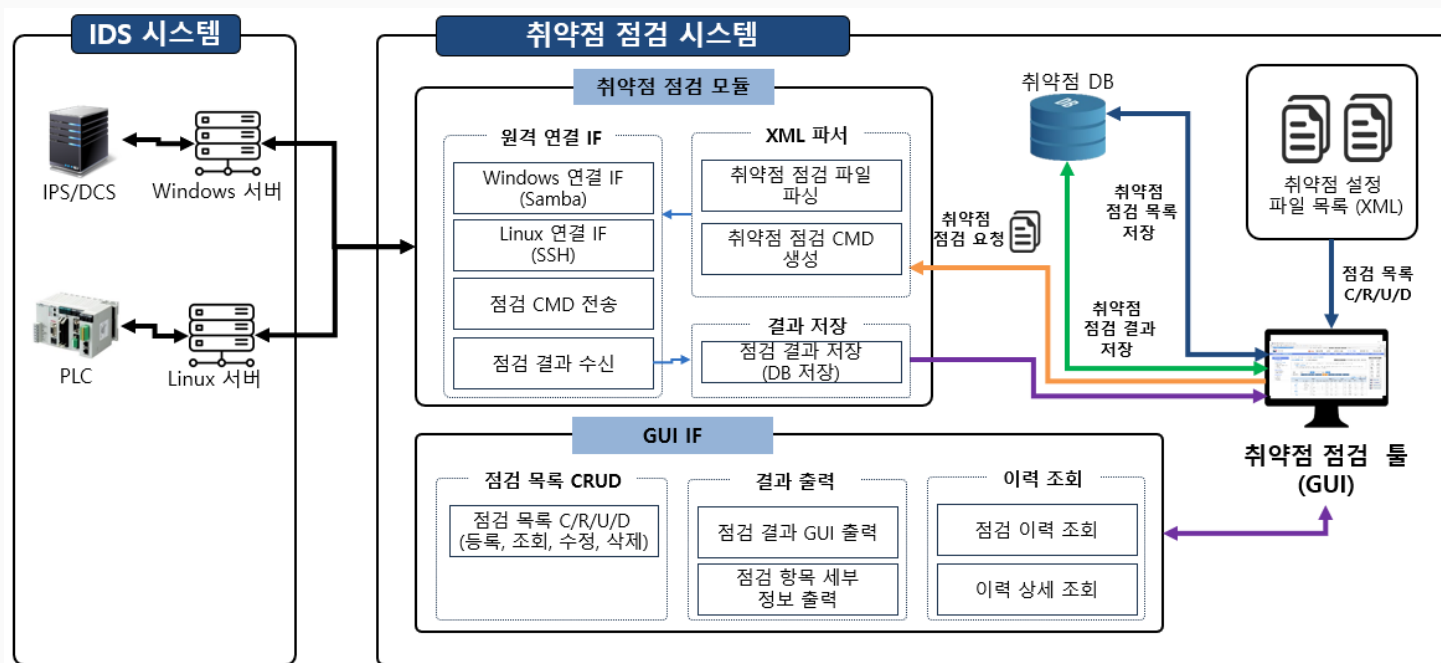
이름 조유빈

담당 UI & DB

주제 개요

Windows 서버 및 Linux 서버에 대한 가벼운 취약점 점검 시스템을 구현하기 위해 그림과 같이 시스템 구성을 설계 및 개발 진행 중

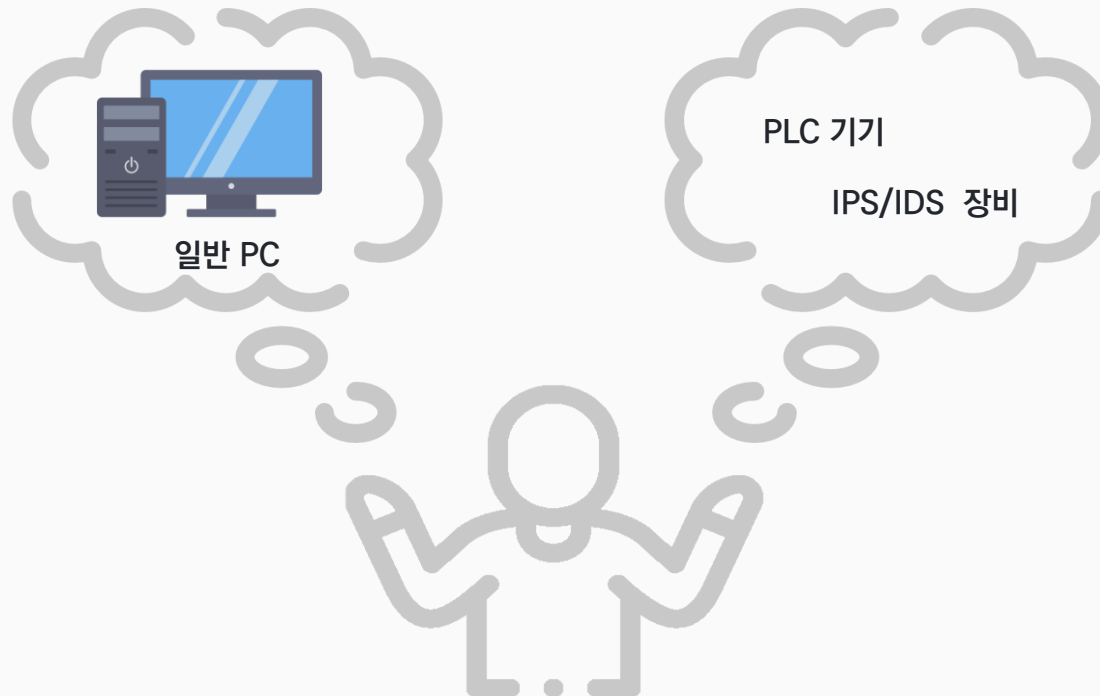
- 현업에서 보안 점검 수행 시 쉽고 간단하게 사용 가능한 시스템
- Human error를 최소화하여 점검 수행
- 가독성 있게 점검 기록 열람



주제 개요

- After Kick-Off 발표

Q. PLC 또는 IPS/IDS 장비에 대한 보안 취약점 점검을 수행해야
일반 PC에 대한 점검과는 **차별점**이 생기지 않을까?



주제 개요

– After Kick-Off 발표

1. 제어시스템 점검 추가?

주요정보통신기반시설 기술적 취약점 분석 평가 상세 가이드에 ‘제어시스템’ 항목 존재
하지만 해당 항목들은 명령어 실행보다 정책 쪽에 집중되어 있어서
유의미한 제어시스템에 대한 보안 취약점 점검 자동화를 진행한다 보기 힘들

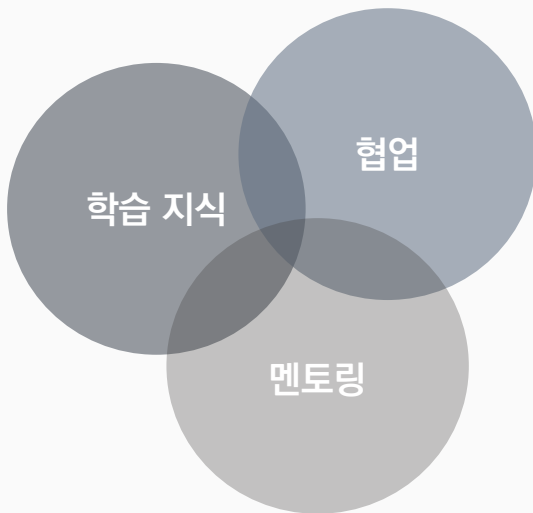
2. PLC 기기에 대한 보안 취약점 점검 추가?

- 무료로 PLC 기기를 대여할 수 없었고, 구매하기에는 너무 가격이 비쌌
- PLC 기기는 다양한 제조업체와 모델이 있어 호환성 문제가 발생할 수 있음

3. IPS 장비에 대한 보안 취약점 점검 추가?

- IPS 장비를 구하거나 가상 IPS를 기간 안에 세팅하기가 어려움
- 제어시스템에서 사용하는 IPS의 특성을 정확히 파악하지 못해 오탐지 및 오작동이 발생할 수 있음

주제 개요



취약점 점검 자동화 시스템 구현

- ✓ 본 프로젝트의 수행 시 지금까지 배웠던 것들을 통해 문제 해결
- ✓ 실제 협업에서 도움이 될 수 있는 실무적인 프로젝트 진행
- ✓ 본 프로젝트와 같은 방식을 통해 다른 시스템에서도 충분히 보안 취약점 점검 자동화가 가능하다는 것을 제시

수행 일정

- 수행 절차

요구사항 확인 및 취약점 리스트화

개발 환경 설정

요구사항 목록화

SW 상세 설계서 작성

점검할 취약점 리스트화

취약점 별 결과 판별 정의

점검 자동화 프로그램 구현

UI 화면 설계

DB 설계

점검 모듈 개발

UI, DB 개발

점검 모듈, UI 연결

프로그램 테스트 및 마무리

프로그램 동작 테스트

코드 리팩토링

프로그램 사용 매뉴얼 작성

최종 보고서 작성

수행 일정

- 수행 절차


	3월	4월	5월	6월
프로젝트 착수	프로젝트 착수			마무리
스크립트 작성	<ul style="list-style-type: none">✓ 팀 빌딩✓ 프로젝트 개요 파악✓ 요구 사항 확인✓ 업무 분장✓ 킥오프 발표	Windows 규제 지침 파악	규제 지침 파악	
점검 모듈 개발		Windows 점검 항목 스크립트 작성	Windows, Linux 점검 항목 스크립트 작성	
UI, DB 개발		점속 모듈 개발		
보 고		XML 파싱 모듈 개발		
	점검 모듈 설계		점검 모듈 개발	점검 모듈 테스트 및 최적화
	DB, UI 설계	일부 화면 구현	UI 화면 구현 및 점검 모듈 연동	UI 테스트
		점검 모듈 연동		
	주간 프로젝트 일정표 업데이트 / 캡스톤디자인 정기 레포트			
	수시로 진행된 사항, 기술에 대한 Zoom 미팅 진행			





수행 내용


- 프로젝트 관리



- Git으로 업무별로 폴더를 나눠 프로젝트를 관리
- 각 업무별 진행된 내용을 바로 관리
- 멘토님 / 교수님 또한 진행 상황을 바로 확인 가능

 **Control-Network-IT-Device-Security-Automation** Public

 Pin  Unwatch 1

 main  1 Branch  0 Tags   Code 

 **CodeByO** 프로젝트 진행 상황 표 링크 업데이트 b7ff9c5 · yesterday  119 Commits

 document	미팅 일부 반영	yesterday
 interface	InspectionResults 테이블 추가	2 days ago
 module	action 결과 방식의 점검 여부 작성	2 days ago
 script	script 수정	2 days ago
 README.md	프로젝트 진행 상황 표 링크 업데이트	yesterday

- 프로젝트 일정표

- 프로젝트 일정표(구글 드라이브) 공유
- 매주 업데이트 진행
- 미진한 부분을 확인하여 팀원 전체가 문제 해결에 참여

프로젝트 진행 현황

.XLSX

☆

🔍

📄

📁

📑

🔗

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

🔧

- 멘토링

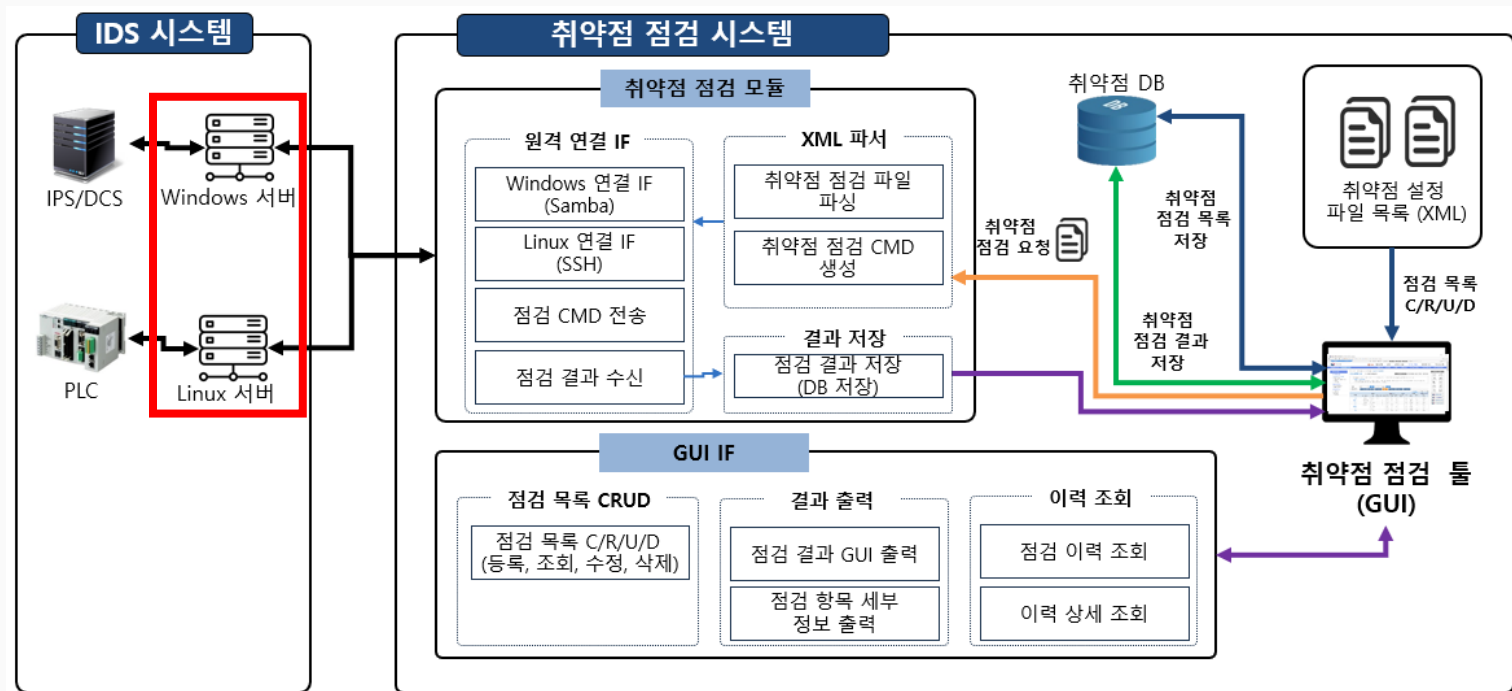
- 격주로 멘토님 / 교수님과 멘토링 진행
- 개별 문제 해결을 위해 팀원별 멘토님 / 교수님과 멘토링 진행
- 다른 업무와의 협업을 위해 수시로 Zoom 미팅 진행

[illegible]

수행 내용

- 프로젝트 요구사항 분석

- 기능 및 UI 파악
- 필요한 함수 및 기능 설계
- UI 와이어프레임 및 DB 관계도 설계 및 피드백



수행 내용

- 상세 설계

〈점검 스크립트 설계〉

- 취약점 점검 문서 분석을 통해 “취약점 유형” 상세 분류
- 스크립트 파일 작성을 위한 XML 태그 설계

Unix 서버 취약점 분석·평가 항목			
분류	점검항목	항목 중요도	항목코드
1. 계정 관리	root 계정 원격 접속 제한	상	U-01
	패스워드 복잡성 설정	상	U-02
	계정 잠금 임계값 설정	상	U-03
	패스워드 파일 보호	상	U-04
	root 이외의 UID가 '0'금지	중	U-44
	root 계정 su 제한	하	U-45
	패스워드 최소 길이 설정	중	U-46
	패스워드 최대 사용기간 설정	중	U-47
	패스워드 최소 사용기간 설정	중	U-48
	불필요한 계정 제거	하	U-49
	관리자 그룹에 최소한의 계정 포함	하	U-50
	계정이 존재하지 않는 GID 금지	하	U-51
	동일한 UID 금지	중	U-52
	사용자 shell 점검	하	U-53
2. 파일 및 디렉터리 관리	Session Timeout 설정	하	U-54
	root 홈, 패스 디렉터리 권한 및 패스 설정	상	U-05
	파일 및 디렉터리 소유자 설정	상	U-06
	/etc/passwd 파일 소유자 및 권한 설정	상	U-07
	/etc/shadow 파일 소유자 및 권한 설정	상	U-08
	/etc/hosts 파일 소유자 및 권한 설정	상	U-09
	/etc/xinetd.conf 파일 소유자 및 권한 설정	상	U-10
	/etc/syslog.conf 파일 소유자 및 권한 설정	상	U-11
	/etc/services 파일 소유자 및 권한 설정	상	U-12
	SUID, SGID, Sticky bit 설정 파일 점검	상	U-13
	사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정	상	U-14
	world writable 파일 점검	상	U-15
	/dev에 존재하지 않는 device 파일 점검	상	U-16
	\$HOME/.rhosts, hosts.equiv 사용 금지	상	U-17
	접속 IP 및 포트 제한	상	U-18
	hosts.lpd 파일 소유자 및 권한 설정	하	U-55
	UMASK 설정 관리	중	U-56
	홈디렉토리 소유자 및 권한 설정	중	U-57
	홈디렉토리로 지정한 디렉토리의 존재 관리	중	U-58
	숨겨진 파일 및 디렉터리 검색 및 제거	하	U-59

Unix 서버 취약점 분석, 평가 항목 일부

윈도уз 서버 취약점 분석·평가 항목			
분류	점검항목	항목 중요도	항목코드
1. 계정 관리	Administrator 계정 이름 변경 또는 보안성 강화	상	W-01
	Guest 계정 비활성화	상	W-02
	불필요한 계정 제거	상	W-03
	계정 잠금 임계값 설정	상	W-04
	해독 가능한 암호화를 사용하여 암호 저장 해제	상	W-05
	관리자 그룹에 최소한의 사용자 포함	상	W-06
	Everyone 사용권한을 익명 사용자에게 적용 해제	중	W-46
	계정 잠금 기간 설정	중	W-47
	패스워드 복잡성 설정	중	W-48
	패스워드 최소 암호 길이	중	W-49
	패스워드는 최대 사용 기간	중	W-50
	패스워드 최소 사용 기간	중	W-51
	마지막 사용자 이름 표시 안함	중	W-52
	로컬 로그인 허용	중	W-53
2. 서비스 관리	익명 SID/이름 변환 허용 해제	중	W-54
	최근 암호 기억	중	W-55
	콘솔 로그인 시 로컬 계정에서 빈 암호 사용 제한	중	W-56
	원격터미널 접속 가능한 사용자 그룹 제한	중	W-57
	공유 권한 및 사용자 그룹 설정	상	W-07
	하드디스크 기본 공유 제거	상	W-08
	불필요한 서비스 제거	상	W-09
	IIS 서비스 구동 점검	상	W-10
	IIS 디렉토리 리스팅 제거	상	W-11
	IIS CGI 실행 제한	상	W-12
	IIS 상위 디렉터리 접근 금지	상	W-13
	IIS 불필요한 파일 제거	상	W-14
	IIS 웹프로세스 권한 제한	상	W-15
	IIS 링크 사용 금지	상	W-16
	IIS 파일 업로드 및 다운로드 제한	상	W-17
	IIS DB 연결 취약점 점검	상	W-18
	IIS 가상 디렉토리 삭제	상	W-19
	IIS 데이터파일 ACL 적용	상	W-20
	IIS 미사용 스크립트 매핑 제거	상	W-21
	IIS Exec 명령어 쉘 호출 진단	상	W-22
	IIS WebDAV 비활성화	상	W-23

Windows 서버 취약점 분석, 평가 항목 일부

수행 내용

- 상세 설계

〈점검 모듈 설계〉

- 요구사항에 따라 어떠한 함수들이 필요할지 생각
- **점검 대상에 연결, XML 스크립트에서 필요한 데이터 정리, 점검을 수행하고 결과를 정리하는** 3개의 함수가 필요하다 판단 후 구현

모듈명↵	설명↵	비고↵
시스템 연결 모듈↵	점검 대상 시스템에 원격 접속 하는 모듈 ↵	ssh, samba↵
XML 스크립트 파싱 모듈↵	XML 스크립트를 자동 점검하기 위해 정보를 정리하는 ↵ 모듈↵	↵
자동 점검 모듈↵	파싱한 정보와 연결된 세션을 가지고 점검을 수행하고 ↵ 결과를 정리하여 데이터 베이스에 업로드 하는 모듈↵	↵

점검 모듈 함수 설계

수행 내용

- 상세 설계

< UI 설계 >

“>” 버튼 클릭 시

취약점
점검

점검 이력
조회

대상 OS 선택 ▼

접속 방식 선택 ▼

시스템 IP 주소

포트 번호

ID

Password

>

점검 대상 정보
입력 화면



<

+

선택	점검 항목	점검 내용	실행 방식	결과 방식	삭제
<input type="checkbox"/>	백신 프로그램 업데이트	Windows Defender 백신 프로그램을 업데이트 합니다.	Powershell	action	<div>삭제</div>
<input type="checkbox"/>	계정 잠금 임계값 변경	계정 잠금 임계값을 5로 설정	Powershell	action	<div>삭제</div>
<input type="checkbox"/>	Administrator 계정 이름 변경	Administrator 계정 이름을 유추하기 어려운 계정으로 변경	Powershell	action	<div>삭제</div>
<input type="checkbox"/>	Guest 계정 사용 안 함 설정	Guest 계정을 비활성화하여 사용하지 않도록 설정	Powershell	action	<div>삭제</div>
<input type="checkbox"/>	컴퓨터 계정 암호 최대 사용 기간 여부 점검	컴퓨터 계정 암호 최대 사용 기간을 설정하기 위한	Powershell	action	<div>삭제</div>

원격 레지스트리 서비스를 비활성화 하여 레지스트리에 대

점검 실행

규제 지침 목록 및 선택 화면

“+” 버튼 클릭 시



PluginName:

TargetOS :

▼

Result_Type :

▼

Info :

Description :

CommandCount :

1

CommandName :

CommandType:

▼

CommandString:

저장

규제 지침 등록 화면



“점검 실행” 버튼 클릭 시

점검 진행률 45/100

점검 항목	점검 내용	결과 방식	점검 결과	
1	백신 프로그램 업데이트	Windows Defender 백신 프로그램을 업데이트 합니다.	action	안전
2	계정 잠금 임계값 변경	계정 잠금 임계값을 5로 설정	action	안전
3	Administrator 계정 이름 변경	Administrator 계정 이름을 유추하기 어려운 계정으로 변경	action	안전
4	Guest 계정 사용 안 함 설정	Guest 계정을 비활성화하여 사용하지 않도록 설정	action	안전
5	컴퓨터 계정 암호 최대 사용 기간 여부 점검	컴퓨터 계정 암호 최대 사용 기간을 설정하기 위한	action	취약

원격 레지스트리 서비스를 비활성화 하여 레지스트리에 대

<

취소

점검 진행 현황 및 결과 화면

수행 내용

- 상세 설계

< UI 설계 >

점검 이력 조회 탭 클릭 시

취약점
점검

점검 이력
조회

필터링 ▼

검색

	날짜	대상 OS	IP 주소	상세 결과
1	20XX-XX-XX	Windows	192.168.0.1	상세 결과
2				
3				
4				
5				
6				
7				

점검 이력 조회 화면

“ 상세 결과 ” 버튼 클릭 시

20XX-XX-XX | Windows | 192.168.0.1

점검 상세 결과

	점검 항목	점검 내용	결과 방식	점검 결과	세부 내용
1	백신 프로그램 업데이트	Windows Defender 백신 프로그램을 업데이트 합니다.	action	안전	세부 내용
2	계정 잠금 임계값 변경	계정 잠금 임계값을 5로 설정	action	안전	세부 내용
3	Administrator 계정 이름 변경	Administrator 계정 이름을 유지하기 어려운 계정 이름으로 변경	action	안전	세부 내용
4	Guest 계정 사용 안 함 설정	Guest 계정을 비활성화하여 사용하지 않도록 설정	action	안전	세부 내용
5	컴퓨터 계정 암호 최대 사용 기간 여부 점검	컴퓨터 계정 암호 최대 사용 기간을 설정하기 위함	action	위약	세부 내용
6	원격으로 액세스 할 수 있는 레지스트리 경로	원격 레지스트리 서비스를 비활성화 하여 레지스트리에 대한 원격 접근을 차단하기 위함	action	위약	세부 내용
7	원격에서 이벤트 로그 파일 접근 차단	원격에서 로그 파일을 접근하는 것을 차단하여 로그 파일이 훼손 및 변조를 차단하기 위함	action	위약	세부 내용

점검 이력 상세 결과 화면

“ 세부 내용 ” 버튼 클릭 시

점검 항목 :
계정 잠금 임계값 변경

점검 내용 :
계정 잠금 임계값을 5로 설정

결과 방식 :
action

CommandName :
Change_Account_Lockout_Threshold

CommandType:
Powershell

CommandString:
Start-Process PowerShell "Command net accounts /lockoutthreshold:5" -Verb RunAs

출력 메시지 :
없음

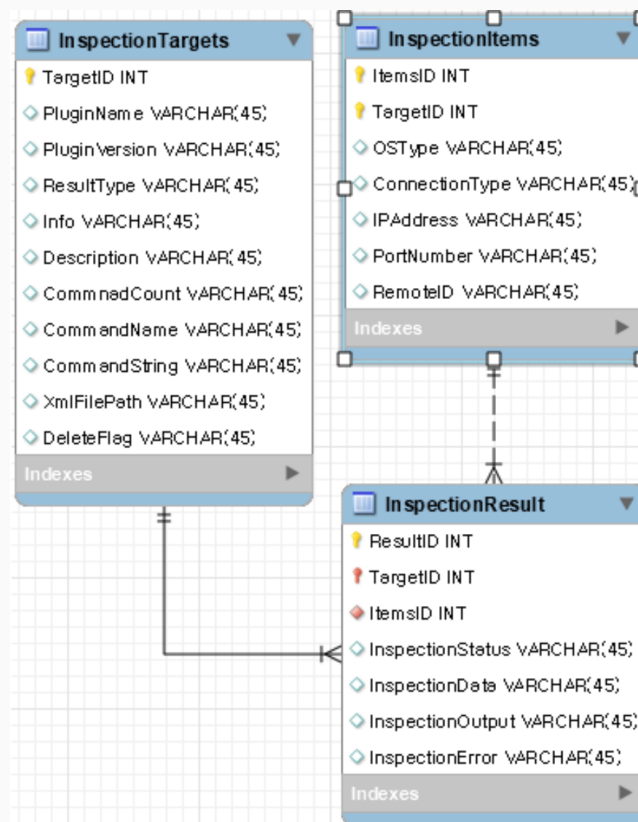
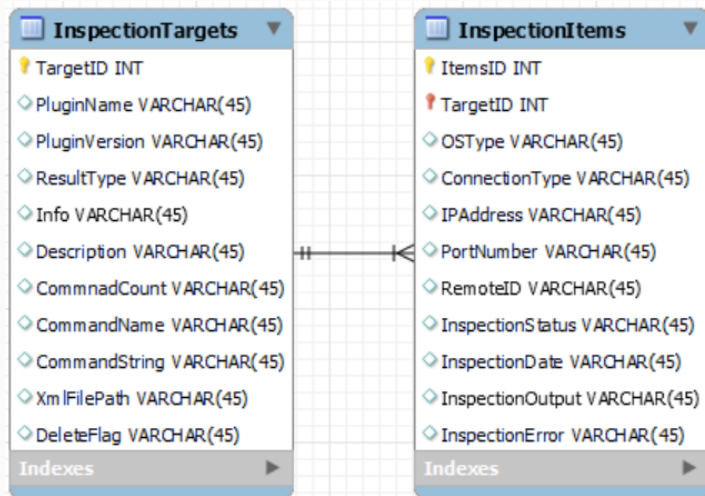
점검 결과 :
안전

점검 항목 세부 내용 화면

수행 내용

- 상세 설계

< DB 설계 >



→ 규제 지침, 점검 대상 정보, 점검 결과 테이블로 분할

초기에는 점검 대상 정보를 나타내는 컬럼과 점검 결과를 나타내는 컬럼을 같은 테이블에 구성했으나, 멘토님께서 주신 피드백을 통해 점검 대상 정보와 결과 컬럼을 각각 테이블로 분리하여 효율적으로 관리하도록 함

수행 내용

- 구현 및 테스트

XML 스크립트의 장단점

장점

- 일반화가 가능한 점검 항목을 작성, 등록 시 점검 시간 절약
- Human error 최소화
- 점검 결과 요약 정리 및 현황 도출 용이

단점

- 스크립트 작성을 위한 시간과 노력이 필요

[tag]

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

점검 스크립트 태그 설명

```
<?xml version="1.0"?>
<Plugin name="Local_Account_Password_lifetime">
  <PluginVersion>1</PluginVersion>
  <PluginName>local-account-password-lifetime.xml</PluginName>
  <TargetOS>Windows</TargetOS>
  <Result_Type>action</Result_Type>
  <Info>컴퓨터 계정 암호 최대 사용 기간 설정 여부 점검</Info>
  <Description>컴퓨터 계정 암호 최대 사용 기간을 설정하기 위함</Description>
  <Commands>
    <CommandCount>1</CommandCount>
    <Command>
      <CommandName>Local_Account-Password_Lifetime</CommandName>
      <CommandType>Powershell</CommandType>
      <CommandString>powershell.exe -Command "$MaxPasswordAge=90;$SecPolFile=\\\"$env:temp\SecPol.cfg\\\";
secedit /export /cfg $SecPolFile;
(Get-Content $SecPolFile -Raw) -replace \"MaximumPasswordAge = \\d+\\\", \"MaximumPasswordAge = $MaxPasswordAge\\\" | Set-Content $SecPolFile;
secedit /configure /db secedit.sdb /cfg $SecPolFile /areas SECURITYPOLICY;Start-Sleep -Seconds 2;
$Result = if((Get-Content $SecPolFile -Raw) -match \"MaximumPasswordAge = (\\d+)\\\")
{if($Matches[1] -eq $MaxPasswordAge) {'True\\'} else {'False\\'}};Remove-Item $SecPolFile;Write-Output $Result\"</CommandString>
    </Command>
  </Commands>
</Plugin>
```

점검 스크립트 실제 내용

수행 내용

- 구현 및 테스트

- 점검 모듈 작성 시 함수의 이름과 설명, 해야 할 일 등을 주석으로 명시
- 다른 팀원이 원활히 사용할 수 있도록 인자에 대한 설명과 반환 값에 대한 설명 추가
- 핵심 코드만 먼저 작성 후 UI와 협업하여 수정 예정

```
# [Func] InspectionAutomation
# [DESC] 정리된 스크립트를 이용하여 보안 취약점 점검
# [TODO] result 타입에 따라 실행 구분 및 action 타입에 점검 항목이 정상적으로 동작하는지 파악
# [ISSUE] None
def InspectionAutomation(target_os:str, ip:str, port:str, connection_type:str, username:str, password:str, plugin_dict:dict):
    """
    점검 실행
    :param target_os:
        접속하고자 하는 운영체제 (Windows or Linux)
    :param ip:
        접속하고자 하는 대상 PC 주소
    :param port:
        접속하고자 하는 포트 번호
    :param connection_type:
        접속 프로토콜 지정 (ssh or samba)
    :param username:
        접속을 위한 계정 이름
    :param password:
        접속을 위한 비밀번호
    :param plugin_list:
        선택한 규제 항목의 TargetID와 PluginName 딕셔너리 (ex, {1 : 'Anti_Virus_Update', 2: 'Change_Account_Lockout_Threshold'})
    :return:
        0(성공), 1(대상 접속 실패), 2(점검 실패), 3(데이터베이스 접속 에러) - 미확정
    """
```

점검 모듈 함수 코드 일부

수행 내용

- 구현 및 테스트

점검 모듈을 설계 및 개발할 때 발생했던 문제점 및 해결 방안

- 스크립트 업무에서 작성한 스크립트는 파이썬 라이브러리에서 바로 사용
- 스크립트에 따라 정상, 에러 시 출력되는 방식이 달라 일관적으로 처리가 힘들

```
for _ in range(command_count):
    if connection_type == "ssh":
        stdin, stdout, stderr = session.exec_command(command_string)
    elif connection_type == "samba":
        try:
            pass
        except OperationFailure:
            pass
inspection_date = datetime.now().strftime("%Y-%m-%d %H:%M:%S")
stdout = stdout.read().decode('euc-kr').strip()
stderr = stderr.read().dedcode('euc-kr').strip()
inspection_status = 0
if result_type == "action":
    if 'True' in stdout:
        inspection_status = 1
    else:
        inspection_status = 0
```

수행 내용

- 구현 및 테스트

점검 모듈을 설계 및 개발할 때 발생했던 문제점 및 해결 방안

- 어떤 스크립트로 실행해야 정상적으로 동작하는지 파악
- 어떻게 결과를 내서 점검 여부를 결정할지 멘토님과 상의
- 스크립트 업무 팀원에게 해당 내용 공유 후 앞으로 작성될 다른 결과 타입에 대해서도 해당 부분이 반영 될 수 있도록 업무 지원

```
<CommandString>  
    Start-Process PowerShell "-Command net accounts /lockoutthreshold:5" -Verb RunAs  
</CommandString>
```



```
<CommandString>powershell.exe -Command "net accounts /lockoutthreshold:5;  
$TempFile = New-TemporaryFile;secdit /export /cfg $TempFile /areas SECURITYPOLICY;  
$Content = Get-Content $TempFile;Remove-Item $TempFile;  
$Threshold = ($Content | Select-String "LockoutBadCount").ToString().Split(\'=\')[1].Trim();  
if ($Threshold -eq 5) {Write-Output \'True\'} else {Write-Output \'False\'}"</CommandString>
```

수행 내용

- 구현 및 테스트

실제 구현 화면

The screenshot shows the '취약점 점검 시스템' (Vulnerability Check System) window. On the left, there are two sections: '취약점 점검' (Vulnerability Check) and '점검 이력 조회' (Check History Search). The main area contains input fields for '대상 OS 선택' (Select Target OS), '접속 방식 선택' (Select Connection Method), '시스템 IP 주소' (System IP Address), '포트 번호' (Port Number), 'ID', and 'Password'. A '>' button is at the bottom right.

점검 대상 정보 입력 화면

The screenshot shows the '취약점 점검 시스템' (Vulnerability Check System) window displaying a table of rules. The table has columns: 선택 (Select), 이름 (Name), 설명 (Description), 실행 방식 (Execution Method), 결과 방식 (Result Method), and 삭제 (Delete). Below the table is a '<' button and a '점검 실행' (Execute Check) button.

	선택	이름	설명	실행 방식	결과 방식	삭제
1	<input checked="" type="checkbox"/>	백신 프로그램 ...	Windows Defender ...	Powershell	action	삭제
2	<input checked="" type="checkbox"/>	계정 잠금 임계값 변경	계정 잠금 임계값을 ...	Powershell	action	삭제
3	<input type="checkbox"/>	Administrator 계정 ...	Administrator 계정 ...	Powershell	action	삭제
4	<input type="checkbox"/>	Guest 계정 사용 안...	Guest 계정을 ...	Powershell	action	삭제
5	<input type="checkbox"/>	컴퓨터 계정 암호 최...	컴퓨터 계정 암호 최...	Powershell	action	삭제
6	<input type="checkbox"/>	원격으로 액세스 할 ...	원격 레지스트리 ...	Powershell	action	삭제
7	<input type="checkbox"/>	원격에서 이벤트 ...	원격에서 로그 파일...	Powershell	action	삭제
8	<input type="checkbox"/>	DB 로그인 시 ...	적절한 Windows 인...	Powershell	action	삭제

규제 지침 목록 및 선택 화면

→ PyQt를 사용하면서 UI를 보다 더 사용자 친화적으로 만들 수 있도록 하는 방법 모색 중

수행 내용

- 구현 및 테스트

UI & DB를 설계 및 개발할 때 발생했던 문제점 및 해결 방안

1. 담당 팀원이 DB를 다뤄본 경험이 적어 설계, 구현하는데 어려움이 있었음

→ DB 사용에 익숙한 다른 팀원과의 멘토링을 통해 도움을 받아 구현할 수 있었음

수행 내용

- 구현 및 테스트

UI & DB를 설계 및 개발할 때 발생했던 문제점 및 해결 방안

2. 점검 모듈과 UI를 연결하는 과정에서 코드 해석에 대한 문제가 발생

→ 점검 모듈 팀원과의 협업을 통해 해결할 수 있었음

```
self.tableWidget.setItem(rowPosition, 6, QTableWidgetItem(plugin))
self.tableWidget.setColumnHidden(6, True)
self.tableWidget.setItem(rowPosition, 7, QTableWidgetItem(str(TargetID)))
self.tableWidget.setColumnHidden(7, True)
```

```
# [Func] executeInspection
# [DESC] 점검 실행 버튼 클릭 이벤트 핸들러
# [TODO] None
# [ISSUE] None
def executeInspection(self):
    plugin_dict = {}
    for row in range(self.tableWidget.rowCount()):
        chkBoxWidget = self.tableWidget.cellWidget(row, 0)
        chkBox = chkBoxWidget.findChild(QCheckBox)
        if chkBox.isChecked():
            plugin_dict[self.tableWidget.item(row, 6).text()] = int(self.tableWidget.item(row, 7).text())
    result = InspectionAutomation(self.os_type, self.ip, self.port, self.connection_type, self.id, self.password, plugin_dict)
    print(result)
```

수행 내용

- 구현 및 테스트

module > test.py > ...

```
10
11 con = sqlite3.connect(path_database)
12
13 cursor = con.cursor()
14 try:
15     # cursor.execute("DELETE FROM InspectionItems")
16     # cursor.execute("UPDATE SQLITE_SEQUENCE SET seq = 0 WHERE name = 'InspectionItems';")
17
18     cursor.execute("SELECT * FROM InspectionItems")
19 except (sqlite3.OperationalError, sqlite3.ProgrammingError):
20     pass
21
22 inspection_tagets = cursor.fetchall()
23 try:
24     # cursor.execute("DELETE FROM InspectionResults")
25     # cursor.execute("UPDATE SQLITE_SEQUENCE SET seq = 0 WHERE name = 'InspectionResults';")
26
27     cursor.execute("SELECT * FROM InspectionResults")
28 except (sqlite3.OperationalError, sqlite3.ProgrammingError):
29     pass
30
```

출력 문제 디버그 콘솔 터미널 포트 GITLENS

+ Python

PS C:\Users\codeb\Documents\GitHub\Control-Network-IT-Device-Security-Automation>

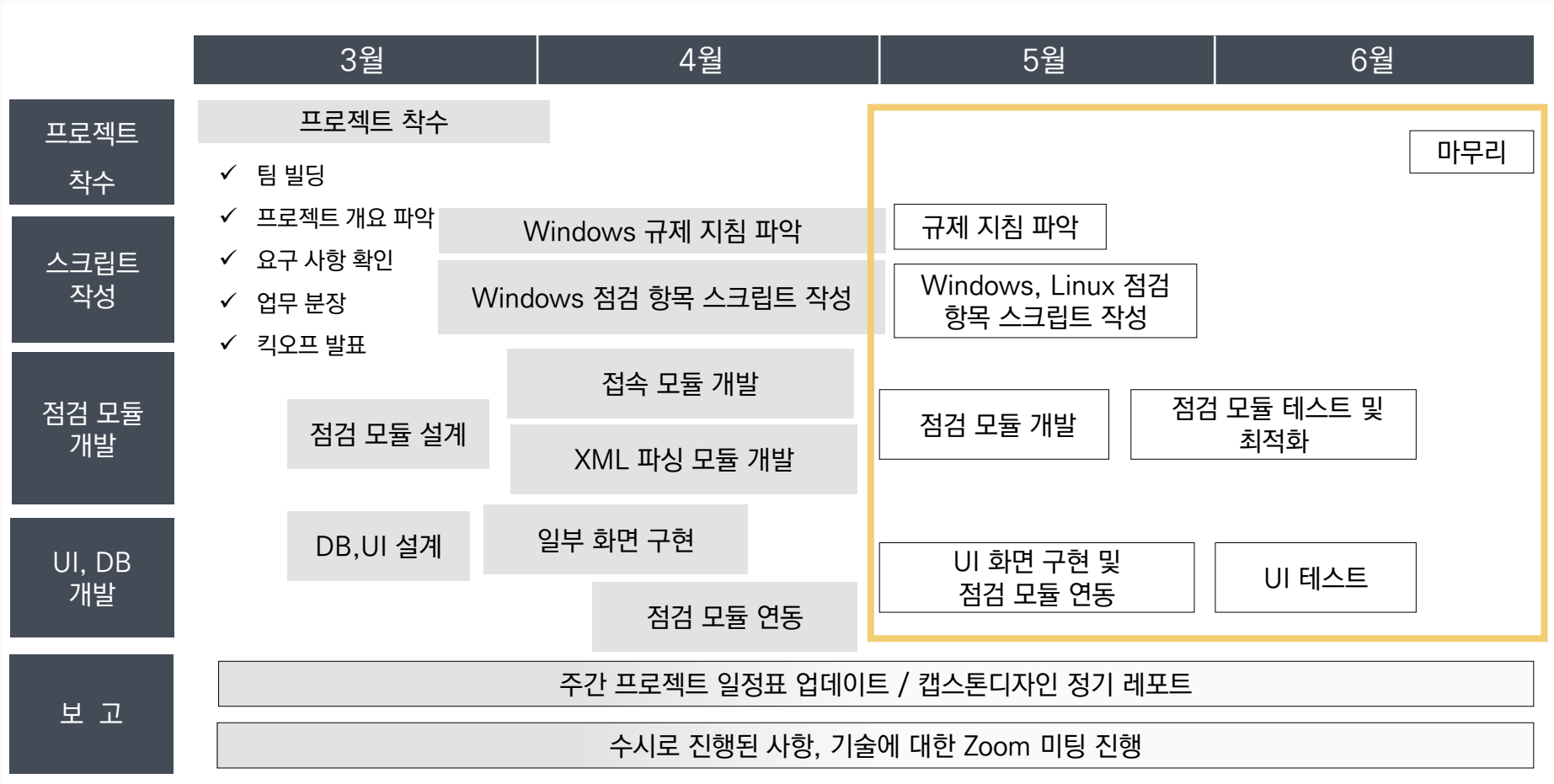
결론

- 이제까지 배운 것을 가지고 서로 긴밀하게 **협업**하여 **현업에서 도움이 될 수 있는 방향으로 프로젝트를 진행**
- 앞으로도 진행된 부분에 대해 계속 **피드백**을 받고 서로 도와가며 진행할 예정



결론

- 앞으로의 수행 일정

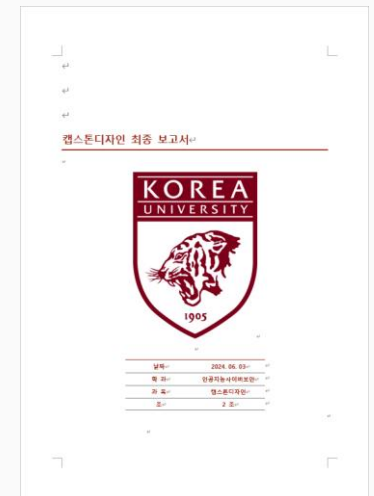
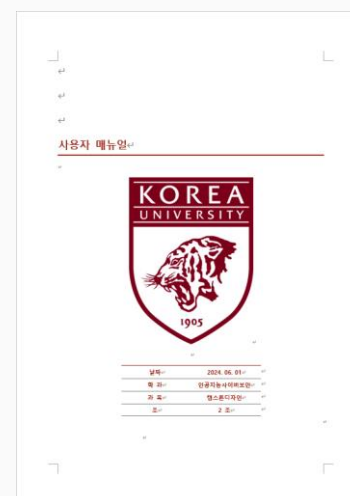
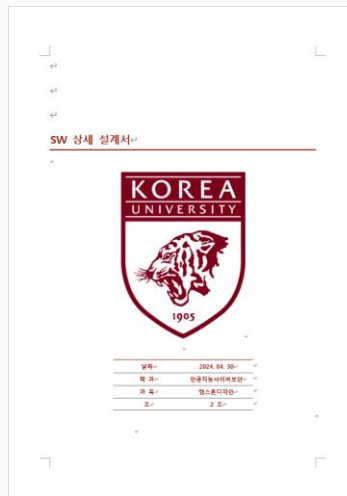


결론

- 최종 산출물

- 자동화 점검 프로그램
- SW 상세 설계서
- 사용자 매뉴얼
- 최종 보고서

```
C:.\n  AutoInspection.db\n  자동점검 도구.exe\n\ndocument\n  자동점검 도구_사용자매뉴얼.docx\n\nscript\n  anti-virus-update.xml\n  Change_Account_Lockout_Threshold.xml\n  Change_Administrator_Account_Name.xml\n  Change_Linux_Account_Lockout_Threshold.xml\n  Disable_Guest_Account.xml\n  Document\n  local-account-password-lifetime.xml\n  README.md\n  remote-access-registry.xml\n  remote-event-log-access-block.xml\n  windows-verify-mode.xml
```



감사합니다