클라우드 취약점 진단 자동화 도구

팀 명 : 정보는 역시 심정보

지 도 교 수 : 양환석 교수님

팀 장 : 한 제민

팀 원 : 유 태균

배 준호

양 윤석

심 정보

전 보경

2023. 10. 30

중부대학교 정보보호학과

목차

1. 서 론

1.1 연구 배경

세계적으로 수많은 기업과 개인 모두가 클라우드 컴퓨팅을 이용하여 데이터 저장, 애플리케이션 실행, 백업 등을 수행하고 있다. 이로 인해 클라우드 인프라스트럭처는 기업의 핵심 자산이 되고 있다. 클라우드 환경에서 데이터의 기밀성, 무결성, 가용성을 보호하기 위한 보안이 매우 중요하다. 클라우드 서비스 제공 업체들은 이러한 보안 문제에 대한 책임을 공유하지만 악의적인 공격자들은 계속해서 공격 기술을 진화시키고, 새로운 공격 벡터를 발견하고 활용한다. 이로 인해 클라우드 보안을 강화하고 취약점을 탐지하는 연구의 필요성이 점점 커지고 있다. 이러한 문제점을 고려하여 KISA(한국인터넷진흥원)에서 제공하는 취약점 진단 가이드를 참고하여 취약점 진단 프로그램을 제작하였다.

1.2 연구 필요성

클라우드 환경은 매우 복잡하고 다양한 구성 요소로 이루어져 있으며, 이로 인해 취약점이 발생하기 쉽다. 수동 취약점 진단은 시간과 노력이 많이 필요하지만 자동화된 프로그램은 보안 전문가의 시간과 노력을 절약하고 리소스를 효율적으로 활용할 수 있다. CI/CD 프로세스를 통해 애플리케이션이 지속적으로 업데이트되므로, 클라우드 환경에서 취약점을 신속하게 탐지하고 수정해야 한다. 자동화 도구는 CI/CD 환경에 적합한 방법으로 취약점 진단을 수행할 수 있다. 또한 자동화된 취약점 진단은 일관된 방식으로 취약점을 검사하므로 신뢰성을 높이고 인간의 실수를 줄일 수 있습니다.

1.3 연구 목적 및 주제 선정

이번 연구는 KISA(한국인터넷진흥원)에서 제공하는 2020 '클라우드 취약점 점검 가이드'를 기반으로 Script를 작성하여 Python GUI에서 SSH 접속을 통해 시스템 보안 취약점을 점검하고 보고서에 점검 결과와 조치 방법을 작성하여 취약한 부분을 보안할 수 있게 하도록 주제를 선정해 보았다.

2. 관련 연구

2.1 Python

파이썬(Python)은 간결하고 읽기 쉬운 문법을 가진 고수준 프로그래밍 언어로, 1991년에 Guido van Rossum에 의해 개발되었다. 파이썬(Python)은 다양한 운영 체제에서 사용할 수 있으며, 데이터 분석, 웹 개발, 인공 지능, 과학 계산, 자동화, 게임 개발 및 여러 다른 영역에서 널리 사용된다.

2.2 Pandas

판다스(Pandas)는 파이썬 프로그래밍 언어를 위한 데이터 조작과 분석을 위한 라이브러리로, 데이터 과학 및 데이터 분석 작업을 수행하는 데 널리 사용된다. 판다스(Pandas)는 데이터 프레임(DataFrame) 및 시리즈(Series)라는 두 가지 주요 데이터 구조를 제공하여 데이터를 구조화하고 조작할 수 있게 해준다. 판다스(Pandas)는 데이터 과학자, 데이터 분석가, 연구자 및 엔지니어들이 다양한 데이터 소스로부터 정보를 추출하고 데이터를 다루는 데 매우 유용한 도구로 자리 잡고 있으며, 파이썬 생태계에서 핵심 역할을 한다.

2.3 Linux

리눅스(Linux)는 오픈 소스 운영 체제로 다양한 컴퓨터 시스템 및 장치에서 사용할 수 있는 운영 체제 커널을 제공한다. 리눅스(Linux)는 서버 운영 체제로 널리 사용되며, 오픈 소스 소프트웨어 및 도구를 통해 웹 서버, 데이터베이스 서버, 클라우드 컴퓨팅, 스마트폰 운영 체제, IoT 장치, 임베디드 시스템 및 개발 환경에서 다양한 용도로 활용된다.

2.4 Apache

아파치(Apache)는 웹 서버 소프트웨어로, 전 세계적으로 널리 사용되는 오픈 소스 소프트웨어이다. 아파치 웹 서버는 클라이언트(웹 브라우저)와 웹 서버 간의 통신을 처리하고 웹 페이지 및 다른 웹 기반 콘텐츠를 클라이언트에 제공하는 역할을 한다.

2.5 Docker

도커(Docker)는 컨테이너 기술을 사용하여 애플리케이션을 개발, 배포 및 실행하는 오픈 소스 플랫폼이다. 도커 컨테이너는 애플리케이션과 그 애플리케이션을 실행하는 환경을 격리시키고 효율적으로 패키징한다.

2.6 MySQL

MySQL는 오픈 소스 관계형 데이터베이스 관리 시스템(RDBMS)으로, 데이터베이스를 생성, 관리, 및 쿼리하는 데 사용되는 소프트웨어이다. 웹 애플리케이션, 엔터프라이즈 소프트웨어, 모바일 애플리케이션, 데이터 웨어하우스 및 다른 다양한 응용 분야에서 데이터 저장 및 관리를 위해 널리 사용되는 데이터베이스 시스템이다.

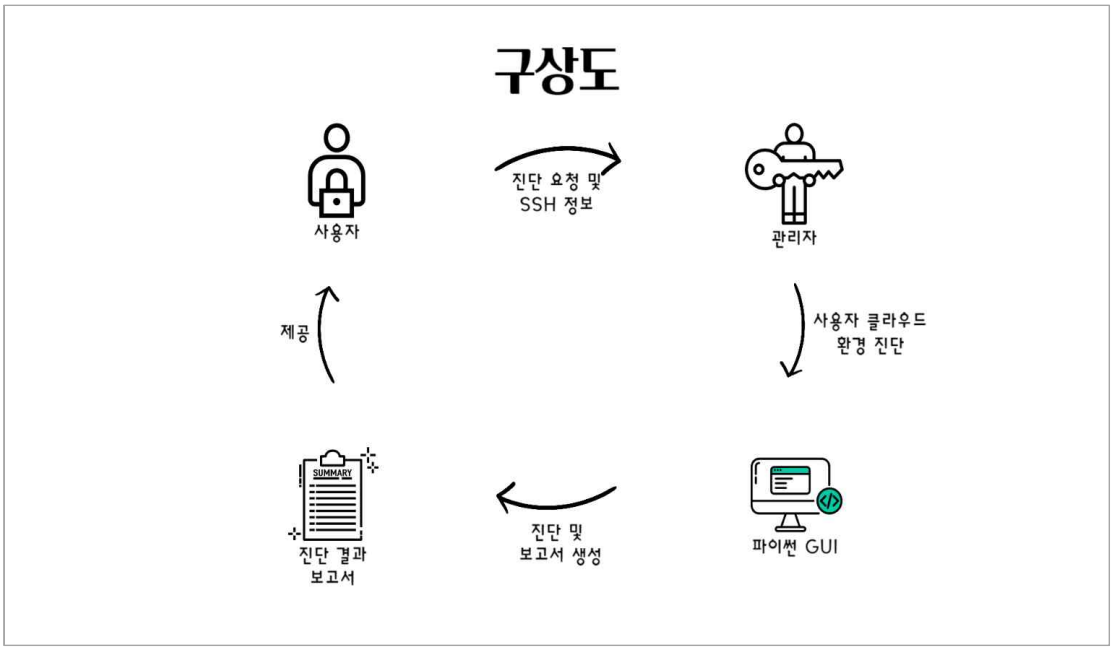
2.7 OpenStack

오픈스택(OpenStack)은 오픈 소스 클라우드 컴퓨팅 플랫폼으로, 데이터 센터에서 인프라스트럭처 및 서비스를 구축, 관리 및 배포하기 위한 솔루션을 제공하는 프로젝트와 생태계의 집합. 오픈스택은 클라우드 환경에서 인프라스트럭처를 구축하고 관리하는 데 사용되며, 퍼블릭 클라우드, 프라이빗 클라우드, 하이브리드 클라우드 등 다양한 클라우드 환경에서 활용된다. 기업과 조직이 데이터 센터 자동화, 스케일링 및 클라우드 서비스 제공을 위한 솔루션을 쉽게 구현하고 관리할 수 있도록 도와준다.

3. 본 론

3.1 시스템 구성

시스템은 다음과 같이 진행된다.



I. 사용자 진단 요청 및 SSH정보를 받는다.
II. 관리자가 진단 GUI를 통해 자동 진단을 실시한다.
III. 진단된 결과를 보고서화하여 추출한다.
IV. 진단 결과 보고서를 사용자에게 제공한다.

3.2 프로그램 구성

3.2.1 진단 스크립트

서버 취약점 진단 자동화 프로그램의 진단 스크립트는 중요한 보안 도구로서 다양한 서버 및 클라우드 환경에서 취약점을 식별하는 기능을 제공합니다. 진단 항목은 Openstack, Linux, Apache, Docker, MySQL로 총 다섯가지의 기술을 진단합니다.

해당 스크립트는 KISA(한국인터넷진흥원)의 클라우드 웹 취약점 진단 가이드와 주요 정보통신 기반 시설의 기술적 취약점 분석평가 방법 상세가이드에 기반하여 개발되었습니다. 이것은 업계에서 인정받는 보안 가이드라인을 준수하며 취약점 진단에 신뢰성을 부여합니다.

3.2.2 취약점 보고서화

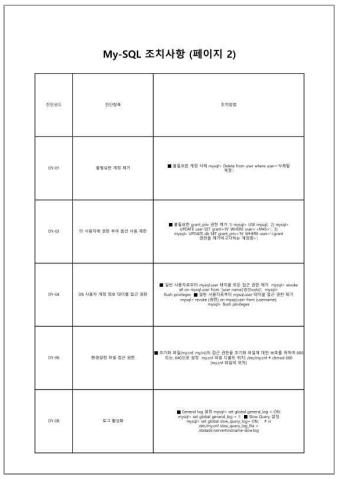
진단 스크립트로 생성된 결과 파일을 평가하고 취약점을 문서화하는 과정은 중요한 보안 관리 단계 중 하나로, 이를 효과적으로 수행하기 위해 파이썬 도구인 판다스를 활용합니다.

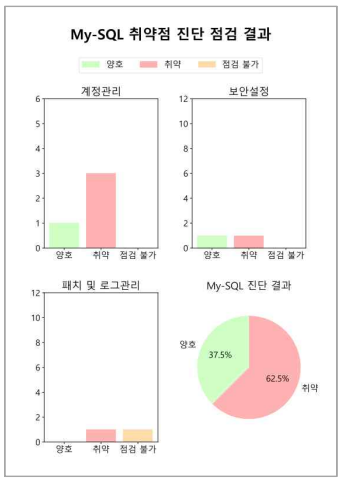
취약점 평가 결과를 기반으로 취약점 보고서를 작성합니다. 이 보고서는 진단된 기술에 대한 결과 및 발견된 취약점의 유형과 심각성을 보여줍니다. 또한 발견된 취약점에 대한 조치사항을 명확하게 제시하며 취약점의 분포나 심각성을 빠르게 파악할 수 있도록 진단 결과를 시각화하는 간단하고 명료한 그래프 파일도 포함됩니다.

해당 보고서는 개선 작업을 추적하는 데 도움이 됩니다. 보고서를 기반으로 보안 전문가나 시스템 관리자는 신속하게 취약점을 해결하고 개선 작업의 진행 상황을 추적할 수 있습니다.


My-SQL 진단결과 (페이지 1)

구분	진단코드	진단항목	취약도	점검결과
계정관리	DY-01	불필요한 계정 제거	중	취약
계정관리	DY-02	취약한 패스워드 사용제한	상	양호
계정관리	DY-03	타사용자에 권한 부여 옵션 사용제한	중	취약
계정관리	DY-04	DB 사용자 계정 정보 테이블 접근 권한	중	취약
보안설정	DY-05	root 권한으로 서버 구동 제한	상	양호
보안설정	DY-06	환경설정 파일 접근 권한	중	취약
보안 설정	DY-07	안전한 암호화 알고리즘 사용	상	양호
패치 및 로그관리	DY-08	로그 활성화	상	취약
패치 및 로그관리	DY-09	최신 패치 적용	상	N/A


My-SQL 조치사항 (페이지 2)



3.2.3 진단 GUI

진단 GUI는 자동으로 진단 도구를 쉽게 이용할 수 있는 환경을 제공합니다. 복잡한 명령어를 기억하거나 입력할 필요 없이 GUI를 통해 간편하게 프로그램을 시작하고 설정할 수 있습니다. 이는 편의성을 크게 향상시키며, 보안 취약점 진단을 보다 쉽게 수행할 수 있도록 돕습니다.

진단 GUI는 진단 항목을 선택할 수 있는 기능을 제공합니다. 이를 통해 특정 기술 스택 또는 서버 구성에 대한 진단을 선택하고 원하는 범위로 진행할 수 있습니다. 또한 스크립트나 보고서 업로드의 진행 상황을 시각적으로 제공합니다. 파일 업로드가 진행 중인지, 완료되었는지, 또는 어떠한 문제가 발생했는지 쉽게 확인할 수 있습니다.

해당 GUI를 이용하여 편리한 환경에서 진단 작업을 수행하고, 선택적으로 조절할 수 있으며, 결과를 손쉽게 문서화하고 공유할 수 있습니다. 이는 시스템 보안을 강화하고 취약점 관리를 효율적으로 수행하는 데 중요한 역할을 합니다.

4. 분 석

4.1 활용 결과 및 성능

GUI 기반 서버 취약점 진단 도구는 사용자가 쉽게 취약점을 식별하고 대응 조치를 취할 수 있도록 설계되었다. 이 도구를 실제로 활용함으로써 다음과 같은 활용 결과를 얻을 수 있다. 사용자는 GUI를 통해 서버 IP 주소, 포트 번호, 사용자 이름 및 SSH 비밀번호를 입력하고, 진단 항목을 선택함으로써 간편하게 취약점 진단을 실행할 수 있다. MySQL의 경우 비밀번호를 추가로 입력하여 진행할 수 있다. 취약점 진단 결과는 구분, 진단 코드, 진단 항목, 취약도 및 점검 결과로 나타난다. 결과가 취약으로 표시되면 해당 진단 항목에 대한 조치사항 페이지가 생성되며, 조치 방법을 제시해준다. 취약점 진단과 대응 프로세스의 자동화와 효율성에 영향을 준다.

4.2 추후 보완사항

기능 추가 및 확장: 추가적인 기능 개발을 통해 도구의 기능성을 향상시킬 수 있으며, 사용자 경험을 개선할 수 있다.

UI/UX 개선: 사용자 친화성을 강화하기 위해 사용자 인터페이스와 사용자 경험을 개선할 수 있다.

새로운 취약점 유형 대응: 새로운 보안 취약점 유형에 대한 대응 방법을 연구하고 구현할 수 있으며, 시스템을 더욱 안전하게 만들 수 있다.

지속적인 업데이트 및 지원: 지속적인 업데이트와 지원을 제공하여 보안 업데이트와 사용자 피드백을 토대로 도구를 개선할 계획이다.

5. 결 론

5.1 결 론

서버 취약점 분석·평가를 희망하는 사용자가 GUI를 통해 IP주소, 포트 번호, 사용자 이름, SSH 비밀번호를 입력하여 SSH 정보를 입력한 뒤 원하는 진단 항목을 선택하여 취약점 진단을 실행하면 된다. MySQL의 경우 MySQL 비밀번호를 추가로 입력하여 진행해야 한다. 사용자의 진달 결과로 구분, 진단 코드, 진단 항목, 취약도, 점검 결과 순으로 나타나며 점검 결과는 양호, 취약, N/A 중 하나로 나타난다. 또한, 점검 결과가 취약일 경우 단순 점검으로 끝나는 것이 아닌 취약으로 뜬 진단 항목에 대한 조치사항 페이지가 작성되며 조치 방법을 제시해준다. 또한 본 프로젝트를 통해서 취약점에 대한 효과적인 대응을 실현하고, 관련 정보를 간편하게 확인할 수 있었다.

5.2 기대효과

본 프로젝트를 통해 개발한 GUI 기반 서버 취약점 진단 도구는 사용자들이 쉽게 취약점을 식별하고 대응 조치를 취할 수 있게 하였다. 서버 취약점을 신속하게 진단하고, 취약점을 해결하는 데 필요한 조치를 할 수 있는 방안을 제공하여 조직 및 시스템의 보안 강화에 기여하고 이를 통해 데이터 유출, 해킹 및 다른 보안 위협으로부터 보호 수준이 향상될 것으로 기대된다. GUI 도구를 사용함으로써 취약점 진단 및 대응 프로세스가 자동화되어 작업 효율성이 향상된다. GUI를 사용하여 복잡한 작업을 수행할 수 있도록 함으로써 사용자 친화성이 개선되며 기술적 지식이 부족한 사용자도 도구를 사용하여 서버 보안을 관리할 수 있어 보안 관리에 쉽게 보완할 수 있다.

6. 별 첨

6.1 소스 코드

https://github.com/hjmxodzm/Project

6.2 발표 자료

01. 프로젝트 개요

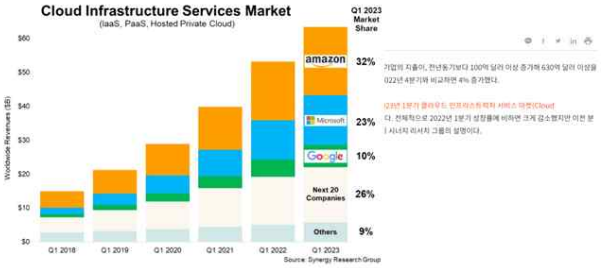
- 프로젝트 배경 및 목적
- 팀원 소개 및 역할

01. 프로젝트 배경 및 목적

1) 클라우드 사용 기업의 증가

다양한 기업들이 클라우드 서비스를 사용하며 특히, IaaS, PaaS 서비스를 많이 이용하며 Amazon,MS 등의 수익 중 높은 비율을 차지함.

"1분기 클라우드 시장 20% 성장···빅3가 65% 점유"



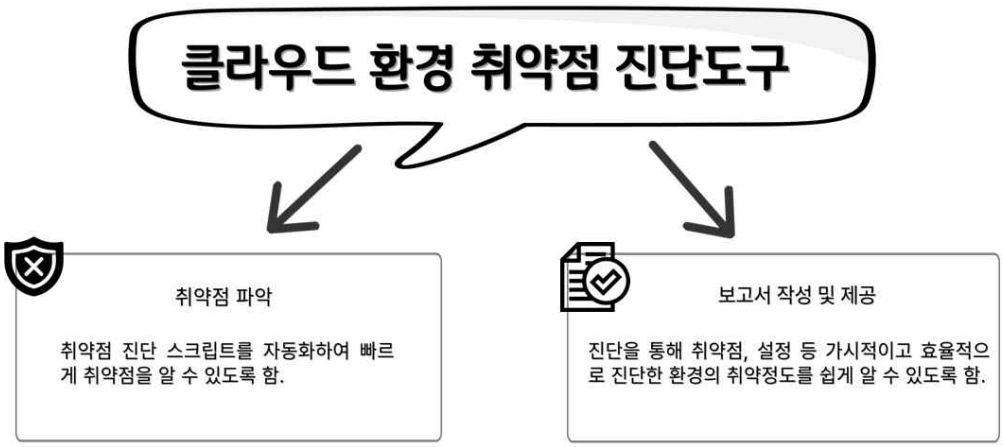
2) 클라우드 환경 보안

기업들의 사용량이 늘어날 수록 클라우드 보안에 더욱 유의해야 하며, 클라우드 설정과 환경의 취약점을 알고 보완해야함.

1억 명 피해자 낳은 캐피탈원 침해 사고, 클라우드 보안 인식 바꿔

4/16

01. 프로젝트 배경 및 목적



5/16

01. 팀원 소개 및 역할

이름	역할
한제민	GUI 개발, 스크립트 작성
유태균	클라우드 구축, 스크립트 작성
배준호	클라우드 구축, 스크립트 작성
심정보	클라우드 구축, 스크립트 작성
양윤석	GUI 개발, 스크립트 작성
전보경	클라우드 구축, 스크립트 작성

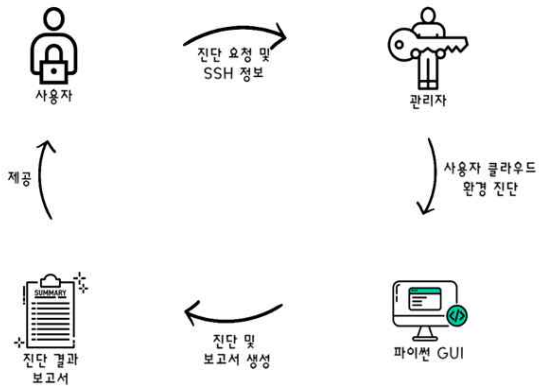
6/16

02. 프로젝트 진행

- 프로젝트 구상도
- 스크립트 제작
- 파이썬 GUI 제작
- 보고서 제작

02. 프로젝트 구상도

구상도



8/16

02. 스크립트 제작

1) IaaS 형식의 클라우드 컴퓨팅 서비스를 제공하는 오픈스택 클라우드 환경 구축

2) KISA의 클라우드 취약점 점검 가이드에 따른 스크립트 제작

9/16

02. 파이썬 GUI 제작

GUI 작동 시나리오

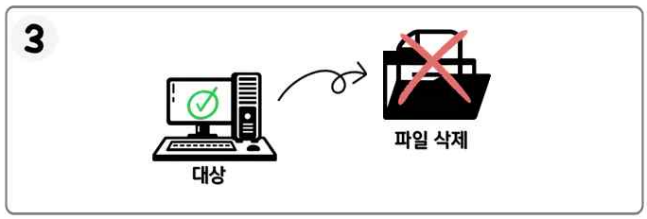
진단 대상의 정보 기입 → 진단을 요하는 프로그램 체크 및 진단 → 취약점 결과 보고서 제작

10/16

02. 파이썬 GUI 제작

파일 전송 및 삭제

1 진단 대상의 정보 기입



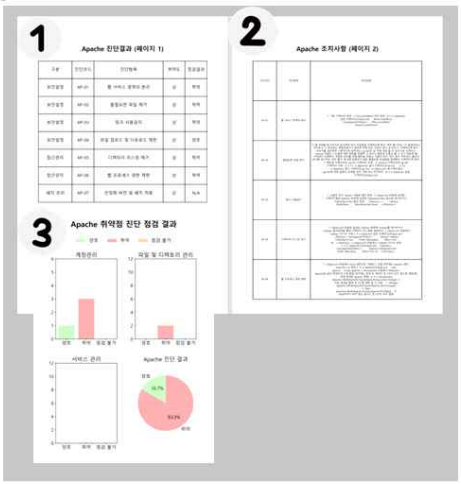
11/16

03. 프로젝트 결과

- 시연 및 영상
- 결론 및 기대효과

02. 보고서 제작

Pandas를 이용한 보고서 제작 및 시각화



목적 - 결과를 쉽고 알아 볼 수 있게 시각화

Python 사용 모듈 - Pandas,matplolib

1.스크립트 항목에 대한 진단 후, 양호와 취약으로 나타냄

2.취약 항목만 모아 대처방안을 제시

3.취약점 진단 결과를 그래프화 하여 시각화

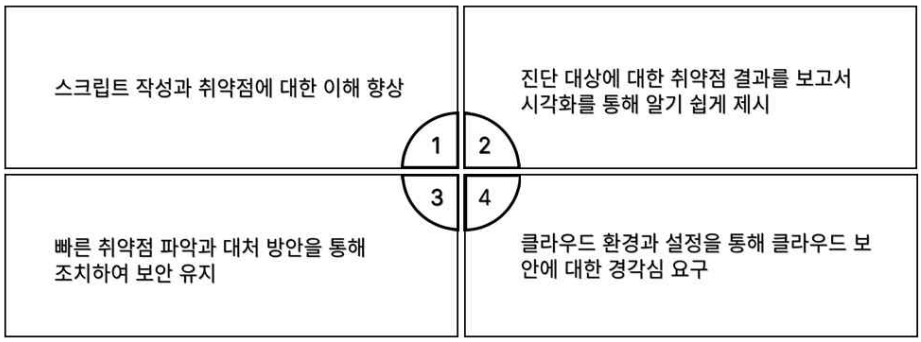
13/16

02. 시연 및 영상

14/16

02. 결과 및 기대효과

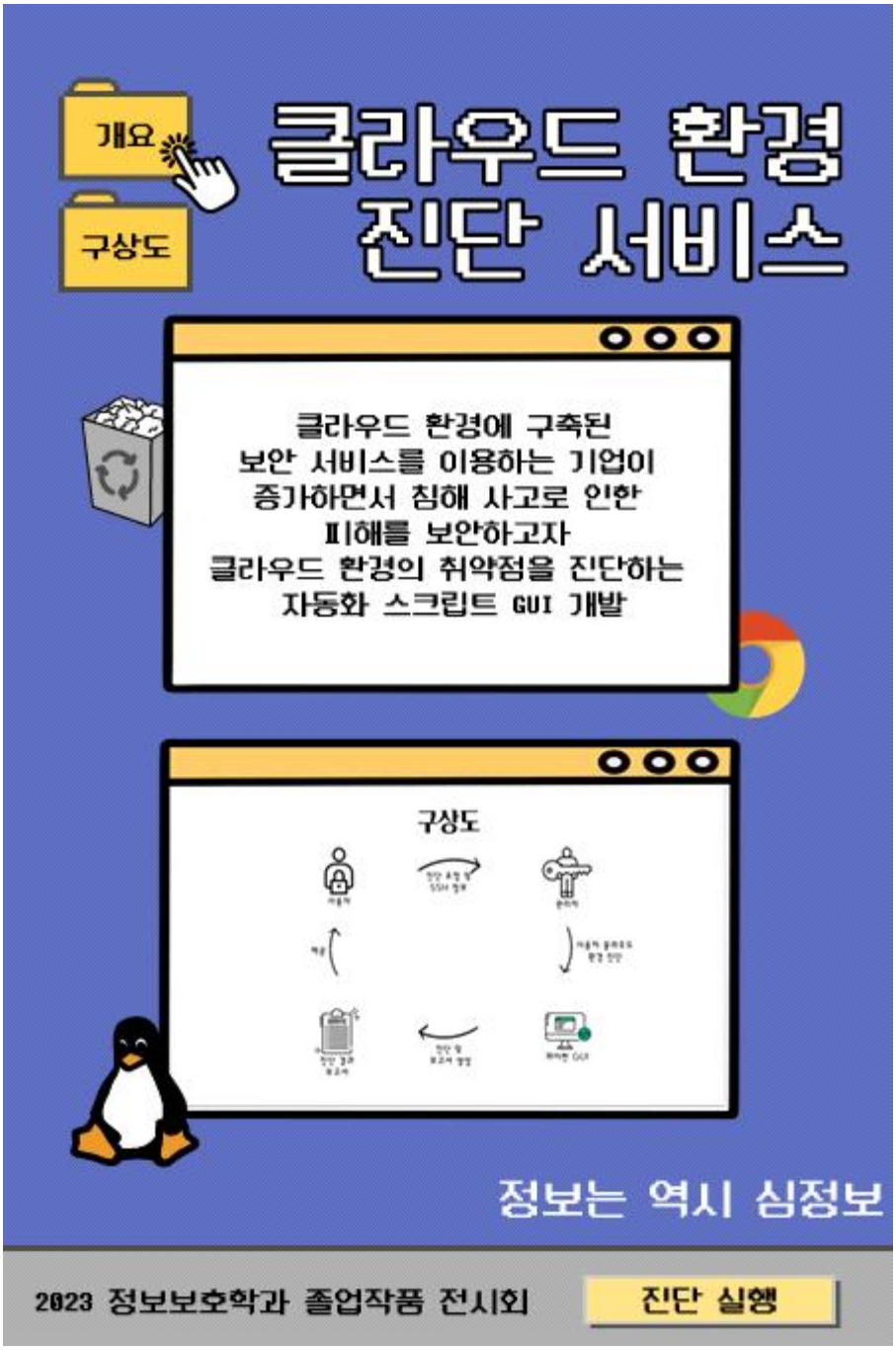
프로젝트 결과

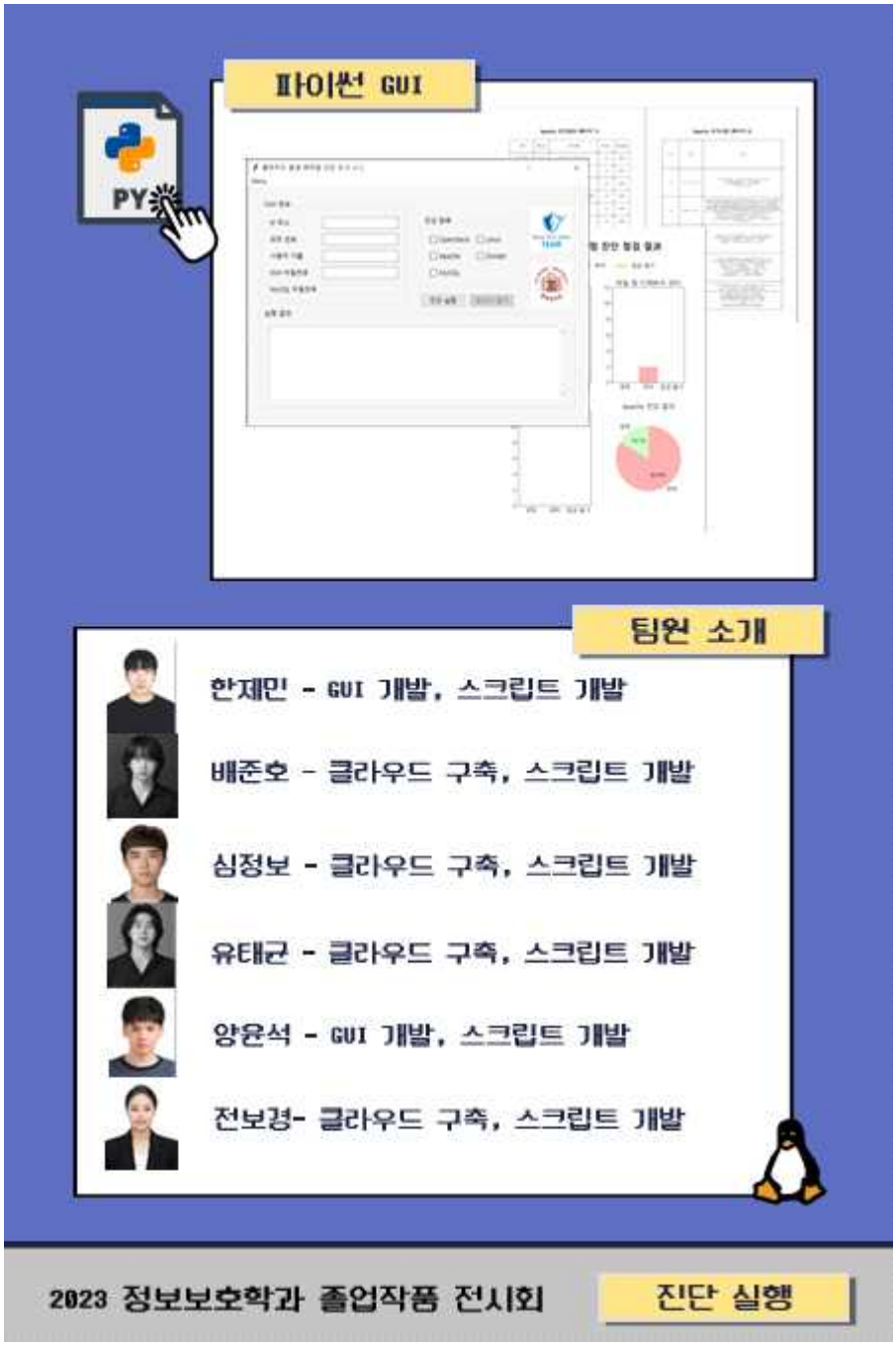


15/16

감사합니다

6.3 폼보드 소개문


개요
구상도
클라우드 환경
진단 서비스
클라우드 환경에 구축된
보안 서비스를 이용하는 기업이
증가하면서 침해 사고로 인한
피해를 보안하고자
클라우드 환경의 취약점을 진단하는
자동화 스크립트 GUI 개발
구상도
정보는 역시 심정보
2023 정보보호학과 졸업작품 전시회
진단 실행


파이썬 GUI
PY
팀원 소개
한제민 - GUI 개발, 스크립트 개발
배준호 - 클라우드 구축, 스크립트 개발
심정보 - 클라우드 구축, 스크립트 개발
유태균 - 클라우드 구축, 스크립트 개발
양윤석 - GUI 개발, 스크립트 개발
전보경- 클라우드 구축, 스크립트 개발
2023 정보보호학과 졸업작품 전시회
진단 실행