

# 서버 취약점 자동 진단 프로그램

4조 공포의 외인구단

지도교수: 양환석 교수님

팀장: 조재연

김세온

조영준

최송이

최유찬

# CONTENTS

---

## 1

### 프로젝트 개요

- 팀원 소개 및 역할 분담
- 프로젝트 주제 선정이유

## 2

### 프로젝트 진행

- 시스템 개발 구상도
- 개발환경

## 3

### 결론 / 기대효과

- 결론 / 기대효과



# 프로젝트 개요

팀원 소개

팀 구성원 소개

역할분담

팀원별 역할분담

주제선정이유

프로젝트 배경 및 필요성, 프로젝트 주제 및 목적



# 팀원 소개 및 역할 분담



**조재연** 팀장

- 일정 수립 및 총괄 확인
- Linux 자동진단 스크립트 개발



**최송이** 팀원

- 자동진단 프로그램 GUI 개발
- 개발 프로그램 최종 Test 진행



**김세온** 팀원

- Unix 자동진단 스크립트 개발
- Test 서버 제작



**최유찬** 팀원

- 자동진단 프로그램 GUI 개발
- 개발 프로그램 최종 Test 진행



**조영준** 팀원

- Windows 자동진단 스크립트 개발
- Test 서버 제작



# 주제 선정이유



## '모의 해킹' 해보니...기업 서버에서 보안 취약점 무더기 발견

| 과기정통부 "올해 훈련에 IoT·NFT·메타버스 관련 위협 시나리오 반영"

컴퓨팅 | 입력 :2022/01/17 12:00



김윤희 기자 | ✉ 기자 페이지 구독 📖 기자의 다른기사 보기



[이벤트] 이제 고민보다 실행할 때! 상품과 함께 데이터바우처 지원 받으세요 (교촌치킨, 로지텍 등)

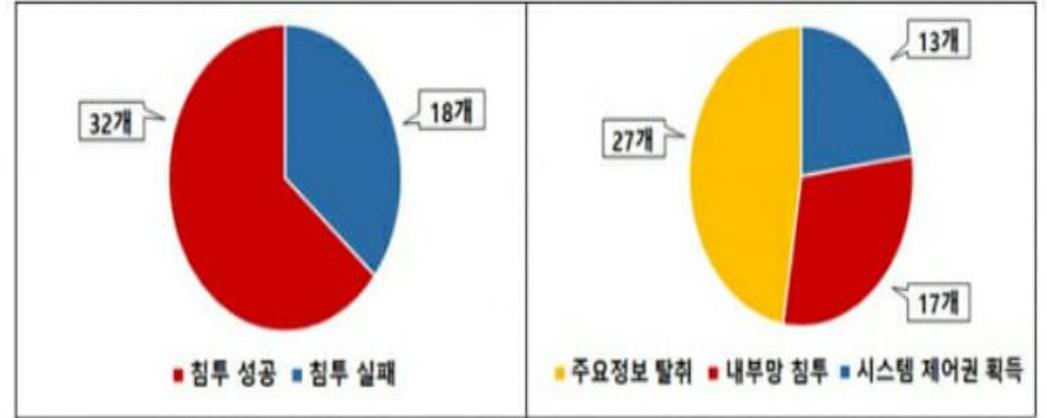
해킹 모의 훈련을 실시한 결과 기업 웹사이트와 웹서버, 업무용 서버 등에 보안 취약점이 상당수 탐지된 것으로 나타났다. 웹사이트는 45개사 중 40개사, 웹서버·업무용서버는 50개사 중 32개사가 이런 위험을 내포했던 것으로 확인됐다.

과학기술정보통신부는 한국인터넷진흥원(KISA)과 함께 실시한 지난해 하반기 사이버위기 대응 모의 훈련 결과를 17일 공개하면서 이같이 밝혔다.

지난해 하반기 모의훈련은 지난 11월1일부터 약 3주 동안 참여 기업 285개사, 임직원 9만3천257명을 대상으로 ▲해킹메일 전송 후 대응 절차 점검 ▲분산서비스거부(DDoS) 공격 및 복구 점검 ▲기업의 홈페이지와 서버 대상 모의 침투를 진행했다.



<모의침투 훈련 결과>



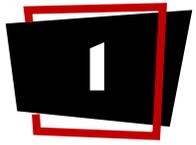
<서버 침투성공 현황>

<세부 침투성공 현황(중복)>

- ※ 주요정보 탈취(27개社) : 기업 정보 외부 전송 가능여부, 개인정보 탈취 가능여부 등 점검
- 내부망 침투(17개社) : Wi-Fi 패스워드 무력화 등을 통한 내부 네트워크 접속 여부 확인
- 시스템 제어권 획득(13개社) : 원격실행 취약점 등을 이용한 관리자 권한 획득
- ※ 일부 기업에서는 3개의 시나리오에서 2개 이상 침투가 가능한 중복 침투

모의 침투 훈련 결과

# 기업 서버 보안 위협의 심각성



# 주제 선정 이유



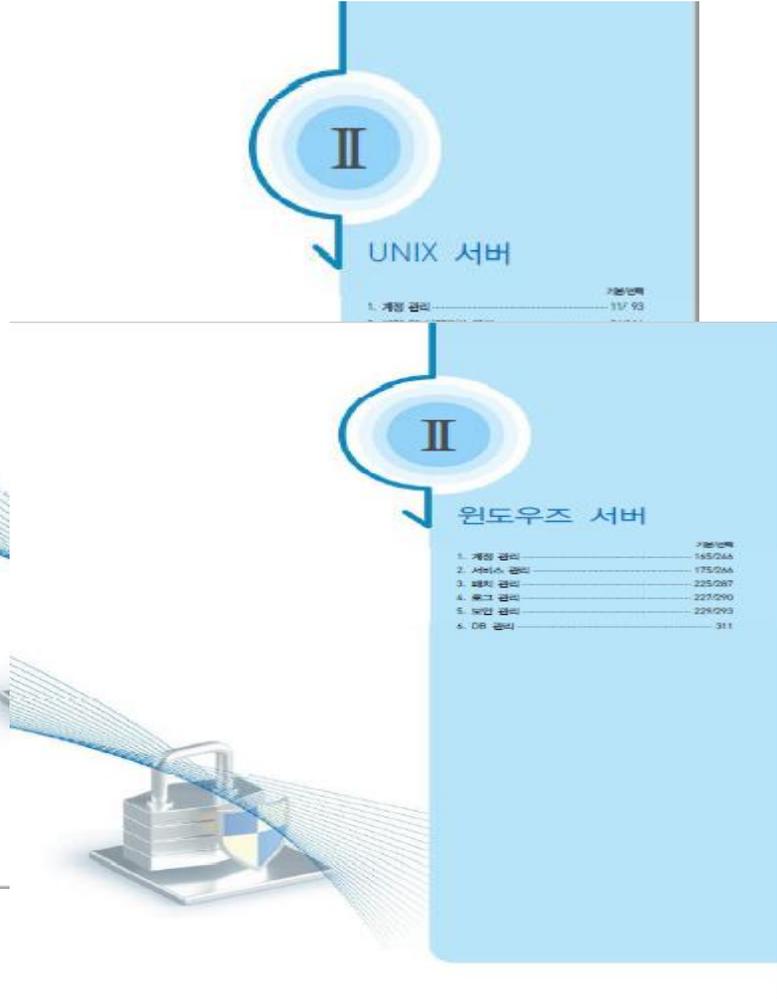
자동화 도구를 이용한 효율적인 서버 진단

“ 서버 취약점 자동 진단 도구를 이용한 취약점 진단 및 보고서 제작 ”





# 주제 선정 이유



II. 보안기타도움\_윈도우즈 서버 161

윈도우즈 서버 취약점 분석·평가 항목

II. 보안기타도움\_UNIX 서버 9

Unix 서버 취약점 분석·평가 항목

분류	점검항목	정확 상도	항목코드
1. 계정 관리	1. 계정관리		
	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	
Session Timeout 설정	하	U-54	
2. 서비스 관리	2. 파일 및 디렉터리 관리		
	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/oinetd.conf 파일 소유자 및 권한 설정	상	U-10
	/etc/xdm.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.pd 파일 소유자 및 권한 설정	하	U-55
NIS 서비스 비활성화	중	U-56	
UMASK 설정 관리	중	U-57	
폴디렉터리 소유자 및 권한 설정	중	U-58	
폴디렉터리로 지정된 디렉터리의 존재 관리	중	U-59	
숨겨진 파일 및 디렉터리 검색 및 제거	하	U-60	

주요정보통신기반시설 취약점 점검 가이드



2

# 프로젝트 진행

시스템 구상도

시스템 개발 구상도

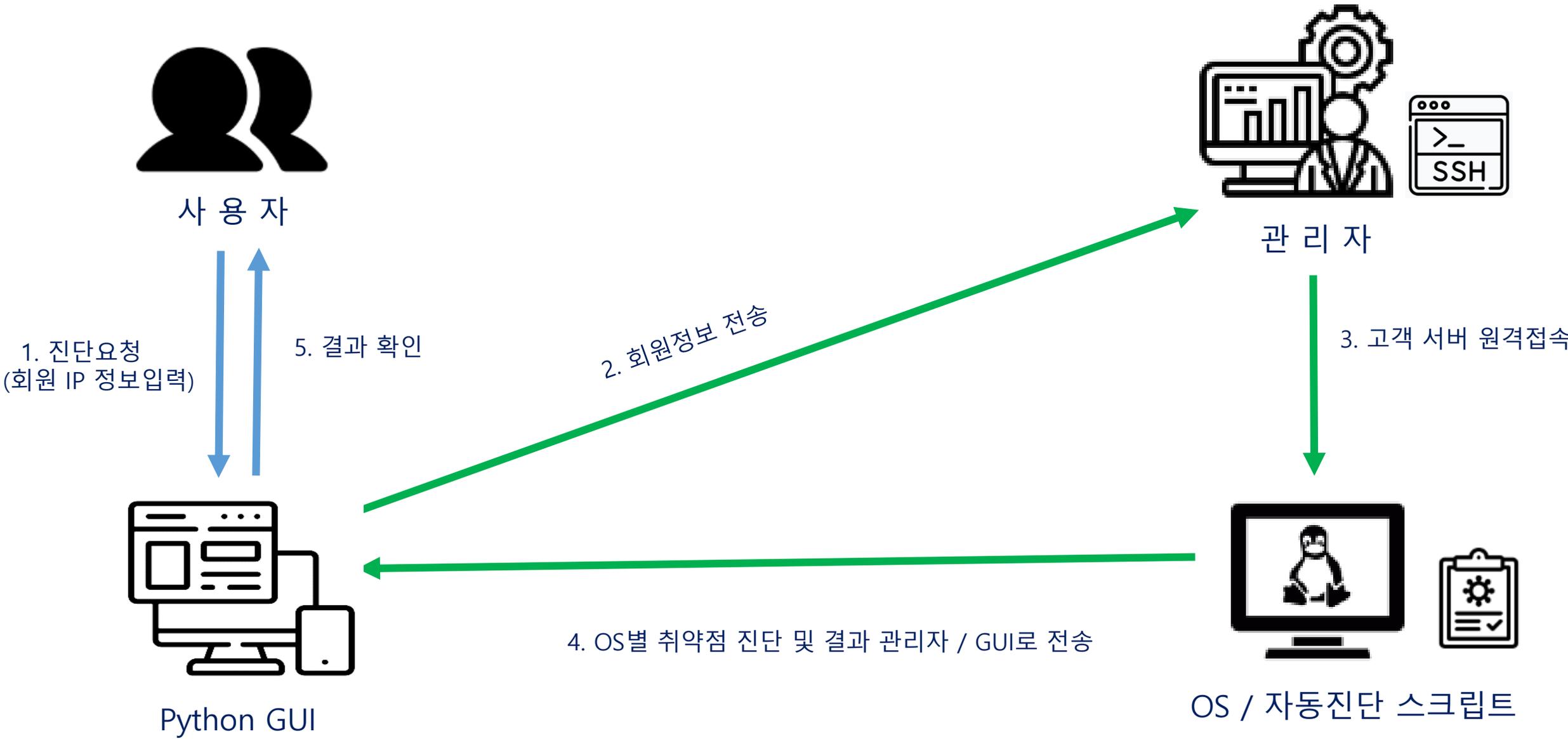
개발 환경

프로젝트 시스템 구축환경

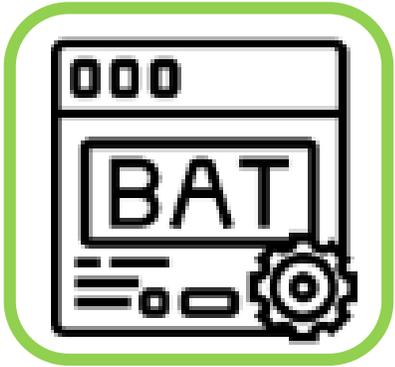
개발 내용

프로그램 구성

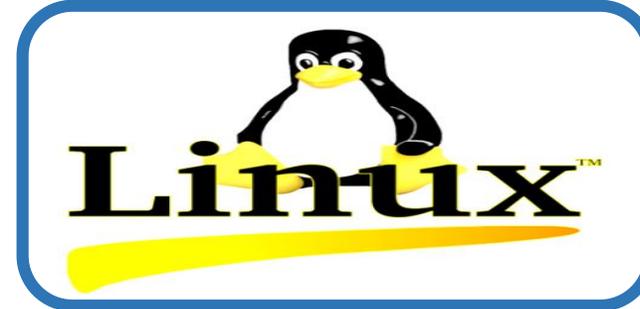
# 2 시스템 구상도



진단 스크립트



진단 환경



GUI



원격접속





```

1 @echo off
2 echo -----원도우서버 취약점 점검-----
3 echo [W-01] ~ [W-82]까지의 항목을 점검합니다.
4 echo.
5 echo Windows Server 2012 R2를 기준으로 제작된 코드입니다.이하 버전에 대해서는 점검이 정상진행 되지 않을 수 있습니다.
6 echo bad항목에서 번호 뒤에 $가 붙는 항목은 담당자의 상의하여 직접 점검하여야 하는 항목입니다.
7 echo bad항목에서 번호 뒤에 $$가 붙으면 Windows Server 2012 이하 버전에서만 해당하기에 직접 점검해야 하는 항목입니다.
8
9 mkdir C:\check\w1-82
10
11 ren *****
12 echo [W-01] Administrator 계정 이름 변경
13 echo.>> C:\check\w1-82\log.txt
14 echo '#*#*#*#[W-01] Administrator 계정 이름 변경'#*#*#*#>> C:\check\w1-82\log.txt
15
16 net user > account.txt
17 net user >> C:\check\w1-82\log.txt
18
19 type account.txt | find /I "Administrator" > NUL
20 if %errorlevel% EQU 0 (
21 echo A![W-01] Administrator 계정이 존재함 - [취약] >> C:\check\w1-82\inspect.txt
22 echo.>> C:\check\w1-82\Action.txt
23 echo [조치사항] >> C:\check\w1-82\Action.txt
24 echo [W-01] 시작: 프로그램- 제어판- 관리도구- 로컬 보안 정책 - 로컬 정책 - 보안옵션 >> C:\check\w1-82\Action.txt
25 echo [W-01] 계정: Administrator 계정 이름 바꾸기를 유추하기 어려운 계정 이름으로 변경 >> C:\check\w1-82\Action.txt
26 ) else (
27 echo A![W-01] Administrator 계정이 존재하지 않음 - [양호] >> C:\check\w1-82\inspect.txt
28 )
29
30 del account.txt

```

batch File

```

1 #!/bin/bash
2
3 mkdir -p /check/U1-73/
4 mkdir -p /check/U1-73/log /check/U1-73/action /check/U1-73/bad /check/U1-73/good
5
6 #####[U-01]root 계정 원격 접속 제한#####
7
8 CF1=/etc/security
9 CF2=/etc/pam.d/login
10 pts=$(grep 'pts' $CF1 | grep -v '#')
11 pan=$(grep "/lib/security/pam_security.so" $CF2 | grep 'required' | awk '{print $1}')
12 #사용할 변수 선언
13
14 echo -e "#####[U-01]root 계정 원격 접속 제한#####\n[root] 원격접속 차단 여부)" >> /check/U1-73/log/[U-01]log.txt
15 grep 'pts' $CF1 >> /check/U1-73/log/[U-01]log.txt
16 echo -e "\n[원격 터미널 서비스 사용 여부]" >> /check/U1-73/log/[U-01]log.txt
17 grep '/lib/security/pam_security.so' $CF2 | grep 'required' | grep 'auth' >> /check/U1-73/log/[U-01]log.txt
18 #로그파일의 용량에 대한 체크를 진행하여 길어져 보기 편하게 출력
19 cat /check/U1-73/log/[U-01]log.txt >> /check/U1-73/log.txt
20
21 if [[ $pan == 'auth' ]] || [[ -z $pts ]]; then
22 echo -e "A![U-01] 원격 터미널 서비스 사용 시 root 직접 접속이 허용되어 있음 - [취약]" >> /check/U1-73/good
23 cat /check/U1-73/good/[U-01]good.txt >> /check/U1-73/inspect.txt
24 else
25 echo -e "A![U-01] 원격 터미널 서비스 사용 시 root 직접 접속이 제한되어 있음 - [취약]" >> /check/U1-73/bad/[U-01]bad.txt
26 cat /check/U1-73/bad/[U-01]bad.txt >> /check/U1-73/inspect.txt
27 echo -e "[U-01] vi 편집기를 사용하여 /etc/security 파일들 열어 pts/* 설정이 존재하는 경우 제거 또는 조석치리\n[원격접속 시]
28 sed -e 's/[U-01] /\\n\\([U-01]조치사항\\)/n/g' /check/U1-73/action/[U-01]action.txt >> /check/U1-73/Action.txt

```

Shell Script

C:\Windows\system32\cmd.exe

-----원도우서버 취약점 점검-----

[W-01] ~ [W-82]까지의 항목을 점검합니다.

Windows Server 2012 R2를 기준으로 제작된 코드입니다.이하 버전에 대해서는 점검이 정상진행 되지 않을 수 있습니다.  
bad항목에서 번호 뒤에 \$가 붙는 항목은 담당자와 상의하여 직접 점검해야 하는 항목입니다.

bad항목에서 번호 뒤에 \$\$가 붙으면 Windows Server 2012 이하 버전에서만 해당하기에 직접 점검해야 하는 항목입니다.

[W-01] Administrator 계정 이름 변경  
[W-02] Guest 계정 상태  
[W-03] 불필요한 계정 제거  
[W-04] 계정 잠금 임계값 설정  
[W-05] 해독 가능한 암호화를 사용하여 암호 저장 해제

파일 탐색기: w1-82

이름	수정된 날짜	유형
Action.txt	2023-09-19 오후 1..	텍스트 문서
inspect.txt	2023-09-19 오후 1..	텍스트 문서
log.txt	2023-09-19 오후 1..	텍스트 문서

스크립트 실행

inspect.txt - 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

A![W-01] Administrator 계정이 존재함 - [취약]  
A![W-02] Guest 계정이 비활성화되어 있음 - [양호]  
A![W-03] 불필요한 계정이 존재하는 경우(관리자 직접점검) - [취약]  
A![W-04] 임계값이 6 이상으로 설정되어 있음 - [취약]  
A![W-05] '사용 안 함'으로 설정되어 있음 - [양호]  
A![W-06] Administrators 그룹에 불필요한 관리자 계정이 존재하는 경우(관리자 직접점검) - [취약]  
B![W-07] 일반 공유 디렉토리의 접근 권한에 Everyone 권한이 있는 경우(관리자 직접점검) - [취약]  
B![W-08] 하드디스크 기본 공유 제거 안 됨 - [취약]  
B![W-08] 하드디스크 기본 공유 레지스트리 값 0 이남 - [취약]  
B![W-09] 일반적으로 불필요한 서비스(아래 목록 참고)가 구동 중인 경우(관리자 직접점검) - [취약]  
B![W-10] IIS서비스가 필요하지 않아 이용하지 않는 경우 - [양호]  
B![W-11] 디렉토리 검색이 사용으로 설정되어 있음 - [취약]  
B![W-12-1] scripts 파일이 존재하지 않음 - [양호]  
B![W-12-2] 해당 디렉토리 Everyone에 모든 권한, 수정 권한, 쓰기 권한이 부여되지 않은 경우 - [취약]  
B![W-13] 상위 디렉토리 접근 기능을 제거하지 않은 경우 - [취약]  
B![W-14] 해당 웹 사이트에 IIS Samples, IIS Help 가상디렉토리가 존재하는 경우(관리자 직접점검)  
B![W-15] 웹 프로세스가 관리자 권한이 부여된 계정으로 구동되고 있는 경우(관리자 직접점검) - [취약]  
B![W-16] 심볼릭 링크, aliases, 바로가기 등의 사용을 허용하지 않음 - [양호]  
B![W-17] 웹 프로세스의 서버 자원을 관리하지 않는 경우 (업로드 및 다운로드 용량 미 제한) - [취약]  
B![W-18] 서버 "처리기매핑"의 사용 항목에 asa, asax가 등록되어 있지 않습니다. - [양호]  
B![W-18] 서버 "요청 필터링"의 asa, asax 확장자가 false로 설정되어 있습니다. - [양호]  
B![W-18] 사이트 "처리기매핑"의 사용 항목에 asa, asax가 등록되어 있지 않습니다. - [양호]  
B![W-18] 사이트 "요청 필터링"의 asa, asax 확장자가 false로 설정되어 있습니다. - [양호]  
B![W-19] 해당 웹 사이트에 IIS Admin, IIS Adminpwd 가상 디렉토리가 존재하는 경우 - [취약]  
B![W-20] 홈 디렉토리 내에 있는 하위 파일들에 대해 Everyone 권한이 존재하지 않음 - [양호]  
B![W-21] htr IDC stn shtml printer htw ida ida가 존재하지 않음 - [양호]  
B![W-22] 레지스트리값이 존재하지 않거나 IIS 6.0버전인 경우 - [양호]

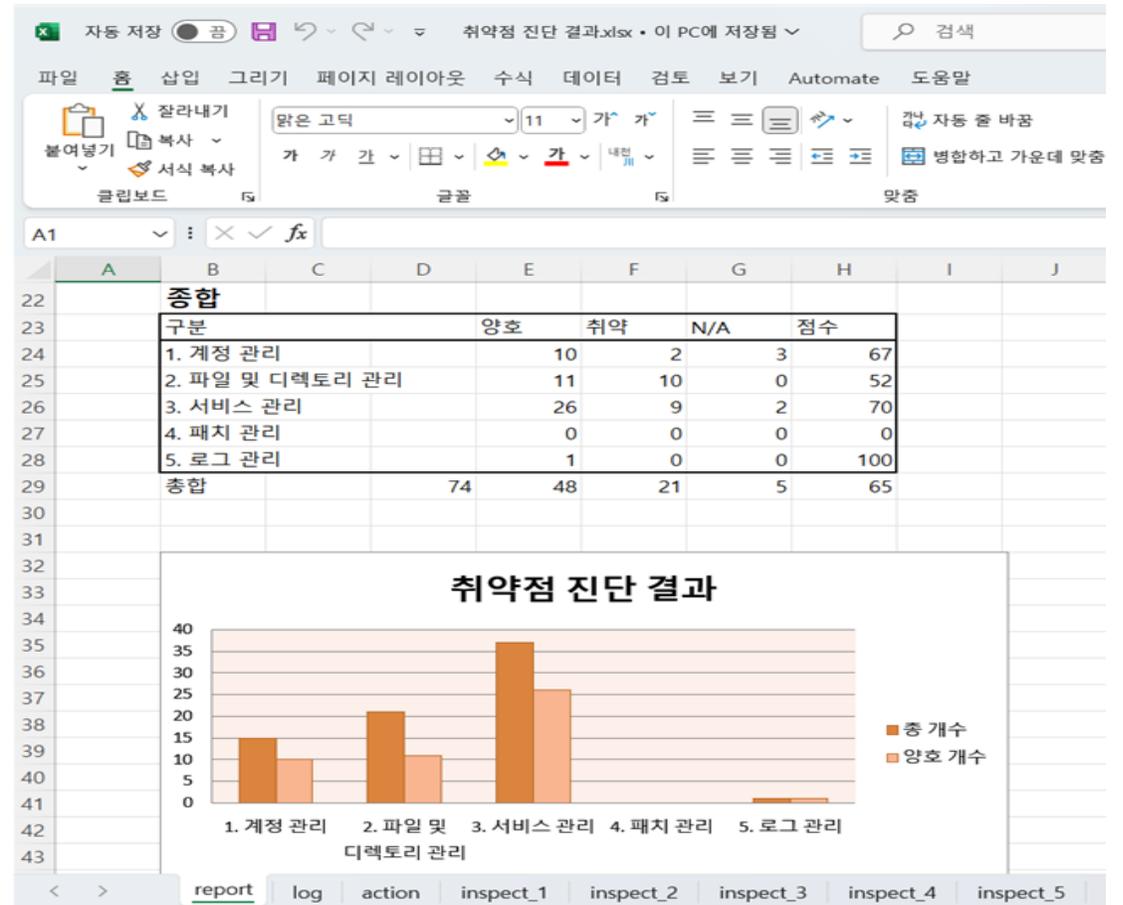
진단 결과(.TXT)

# 서버 취약점 자동진단 스크립트

```

36 wb.save(new_filename)
37 # 여기까지 엑셀파일 생성 후 저장
38 #####
39
40 wb = load_workbook(new_filename) # new_file(위에서 만든 엑셀) 불러오기
41 # 엑셀파일 불러오는 경우 new_filename대신 엑셀파일 이름 넣기
42 # wb.save(new_filename)의 경우도 마찬가지로
43 ws = wb.active
44
45 ###시트지정
46 sh_list = wb.sheetnames # 시트들을 리스트로 구분
47 w1 = wb[sh_list[0]] # 첫번째 시트(report)를 w1로 지정
48 w2 = wb[sh_list[1]] # 두번째 시트(log)를 w2로 지정
49 w3 = wb[sh_list[2]] # 세번째 시트(action)를 w3으로 지정
50 w4 = wb[sh_list[3]] # 네번째 시트(1. 계정관리)를 w4로 지정
51 w5 = wb[sh_list[4]] # 다섯번째 시트(2. 파일 및 디렉토리 관리)를 w5로 지정
52 w6 = wb[sh_list[5]] # 여섯번째 시트(3. 서비스 관리)를 w5로 지정
53 w7 = wb[sh_list[6]] # 일곱번째 시트(4. 패치 관리)를 w6로 지정
54 w8 = wb[sh_list[7]] # 여덟번째 시트(5. 로그 관리)를 w7로 지정
55
56 ###계산
57 # ws["A6"] = "=SUM(A4:A5)"
58
59 left = Border(left=Side(style="thin"))
60 right = Border(right=Side(style="thin"))
61 top = Border(top=Side(style="thin"))
62 bottom = Border(bottom=Side(style="thin"))
63
64 ##report 시트 항목 별 테두리
65 for i in range(4, 21, 4):

```



엑셀 파일 자동 생성

진단 결과 보고서 자동 작성 프로그램

```

48 def makepdf(self):
49     filenames = os.listdir("C:\\jgy\\")
50     if "취약점 진단 결과.xlsx" in filenames:
51         print('PDF생성이 가능합니다.')
52         QMessageBox.information(self, title: 'Message', text: 'PDF 생성이 가능합니다',
53
54         excel = win32com.client.Dispatch("Excel.Application")
55         excel.Visible = False
56         wb = excel.Workbooks.Open("C:\\jgy\\취약점 진단 결과.xlsx")
57         ws_report = wb.Worksheets("report")
58         ws_report.Select()
59         pdf = "C:\\jgy\\취약점 진단 결과.pdf"
60         wb.ActiveSheet.ExportAsFixedFormat(0, pdf)
61         wb.Close(False)
62         excel.Quit()
63     else:
64         QMessageBox.information(self, title: 'Message', text: 'xlsx파일이 존재하지 않음')
65
66     1개의 사용 위치
67     def openpdf(self): # 실행 코드
68         filenames = os.listdir("C:\\jgy\\")
69         if '취약점 진단 결과.pdf' in filenames:
70             os.startfile("C:\\jgy\\취약점 진단 결과.pdf")
71         else:
72             QMessageBox.information(self, title: 'Message', text: 'pdf파일이 존재하지 않음')

```

취약점 진단 결과.pdf

파일 | C:/jgy/취약점%20진단%20결과.pdf

그리기 | 소리내어 읽기 | Bing AI에 요청

1 | 11 | 11

1. 계정 관리

총 개수	양호	취약	N/A	점수
15	10	2	3	67

2. 파일 및 디렉토리 관리 Oct-12-23

총 개수	양호	취약	N/A	점수
21	11	10	0	52

3. 서비스 관리

총 개수	양호	취약	N/A	점수
37	26	9	2	70

4. 패치 관리

총 개수	양호	취약	N/A	점수
0	0	0	0	0

5. 로그 관리

총 개수	양호	취약	N/A	점수
1	1	0	0	100

종합

구분	양호	취약	N/A	점수	
1. 계정 관리		10	2	3	67
2. 파일 및 디렉토리 관리		11	10	0	52
3. 서비스 관리		26	9	2	70
4. 패치 관리		0	0	0	0
5. 로그 관리		1	0	0	100
총합	74	48	21	5	65

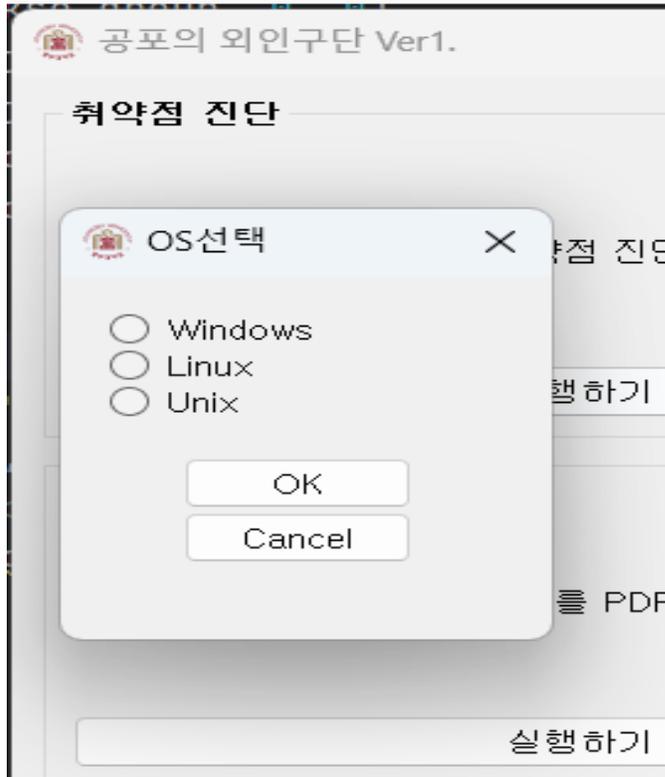
PDF 파일 자동 생성

진단 결과 보고서 자동 작성 프로그램

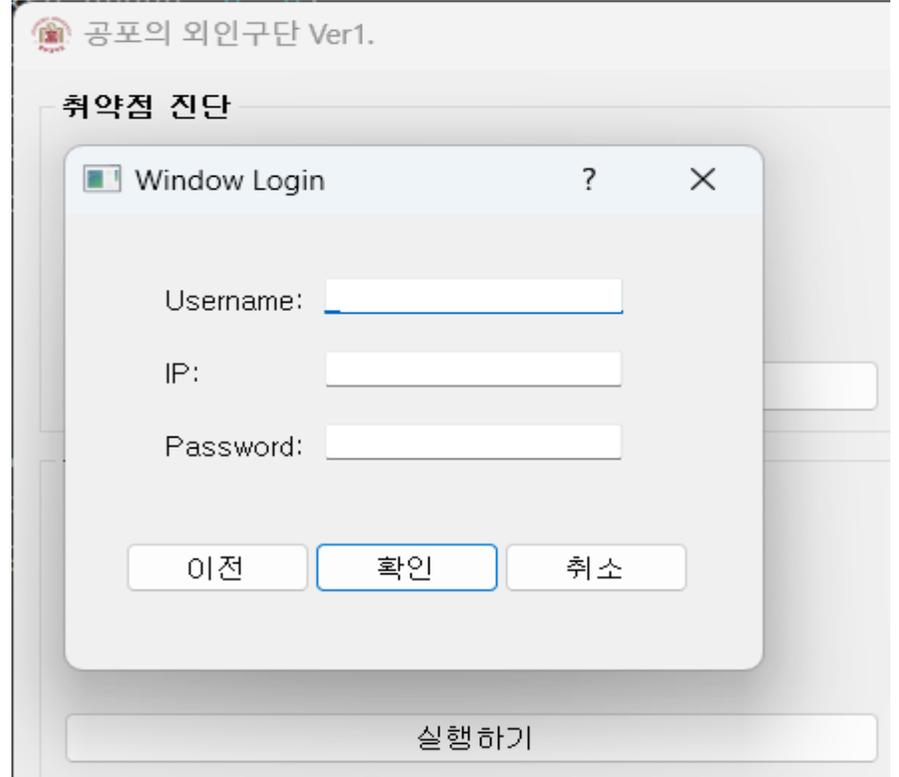
## GUI 구성



GUI 구성 모습



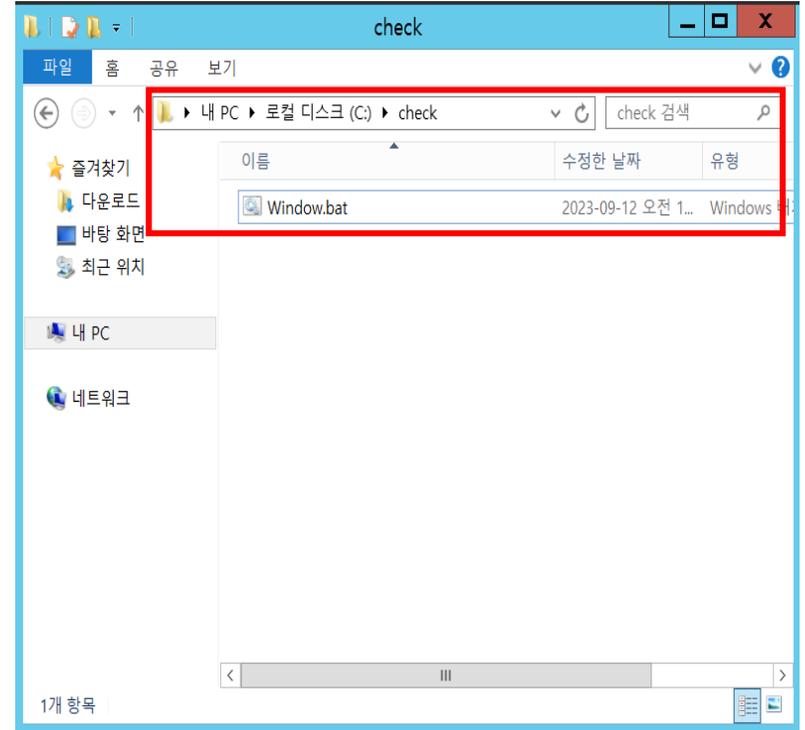
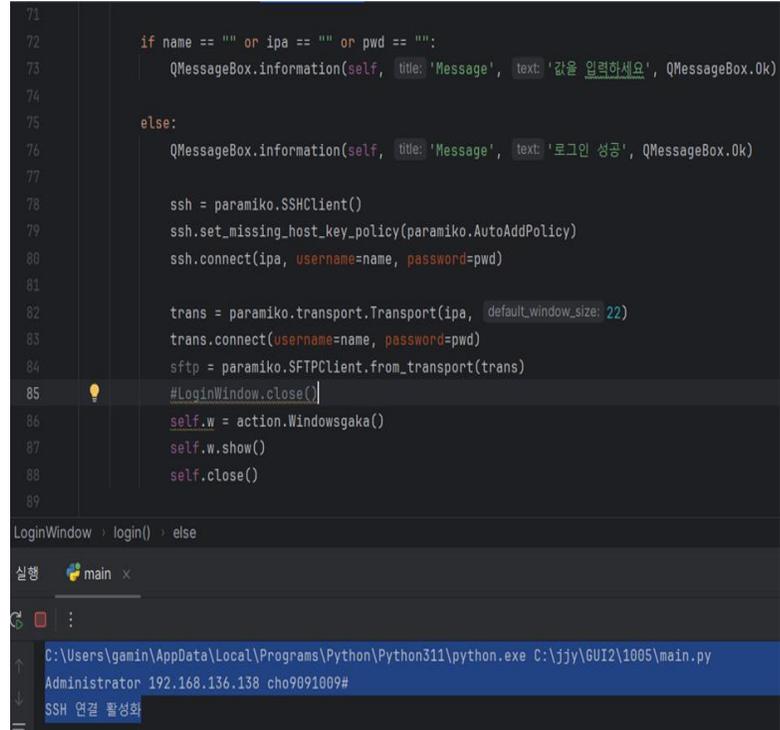
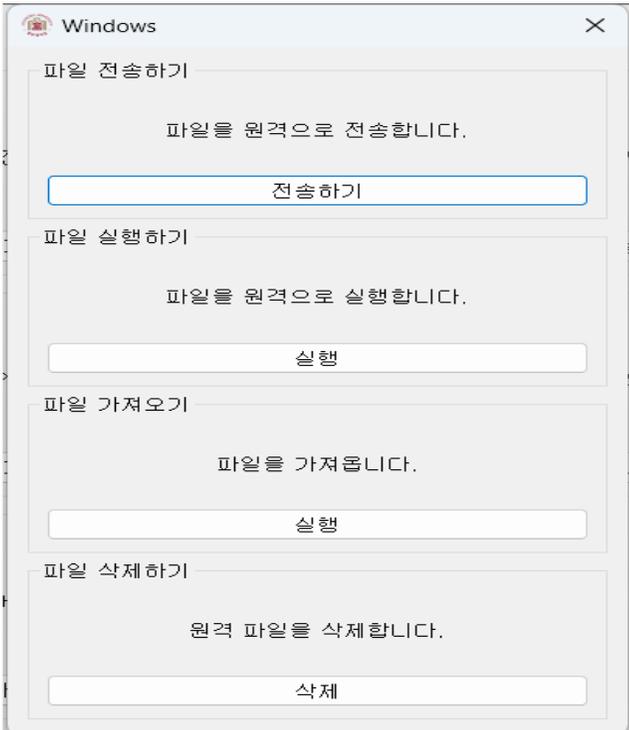
서버 OS 선택



사용자 정보 입력

서버 OS 선택 / 사용자 정보입력

## GUI 구성



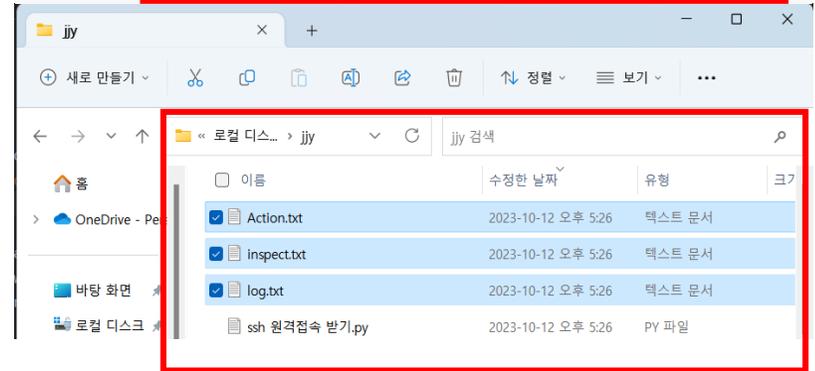
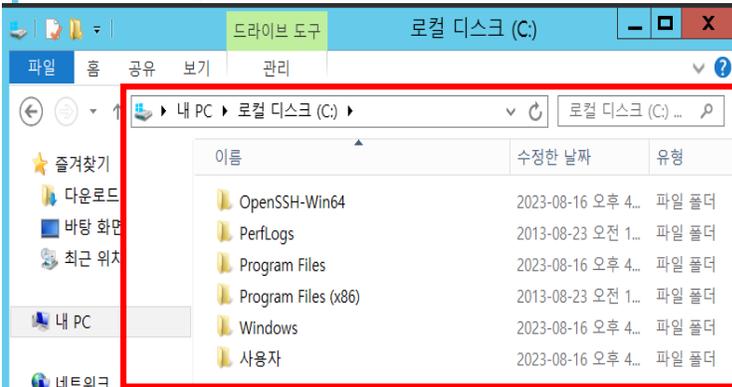
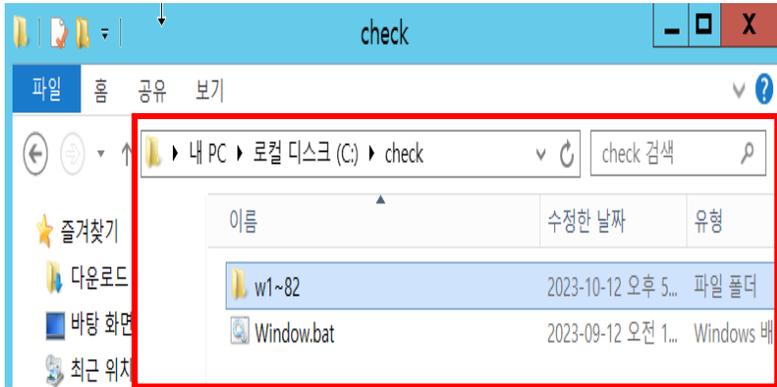
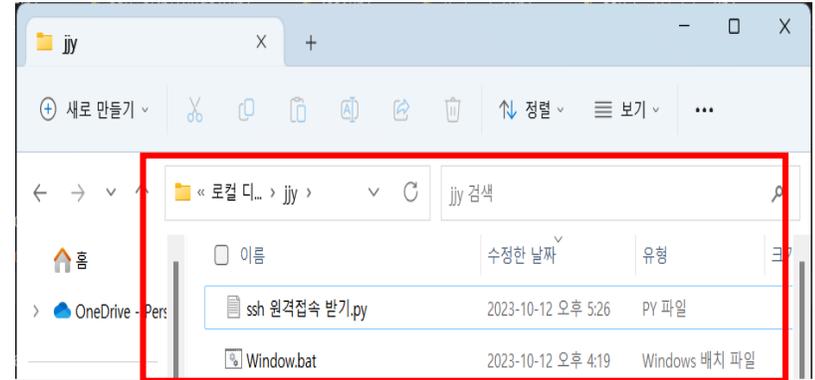
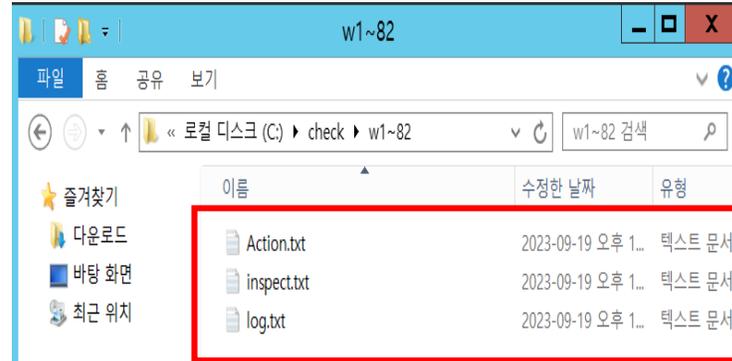
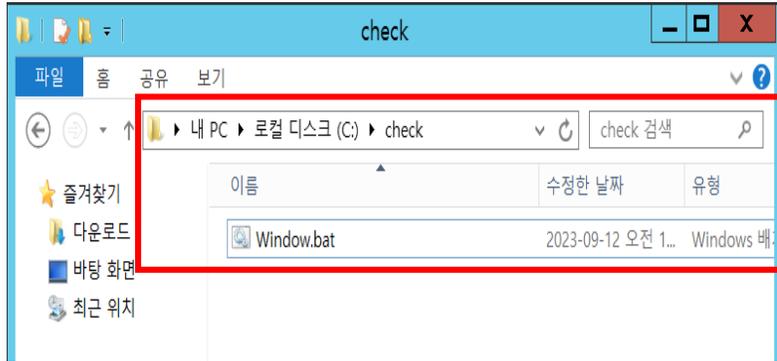
원격 접속 후 실행 화면

파일 전송 코드

사용자 서버 파일 전송 완료

원격접속 / 진단 스크립트 파일 전송

## GUI 구성

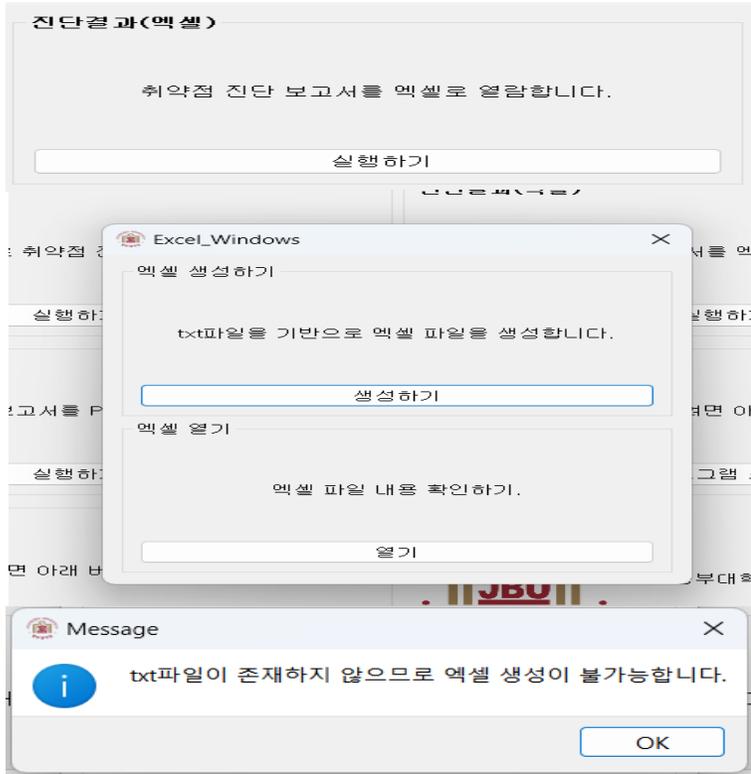


실행 후 화면(사용자 서버)

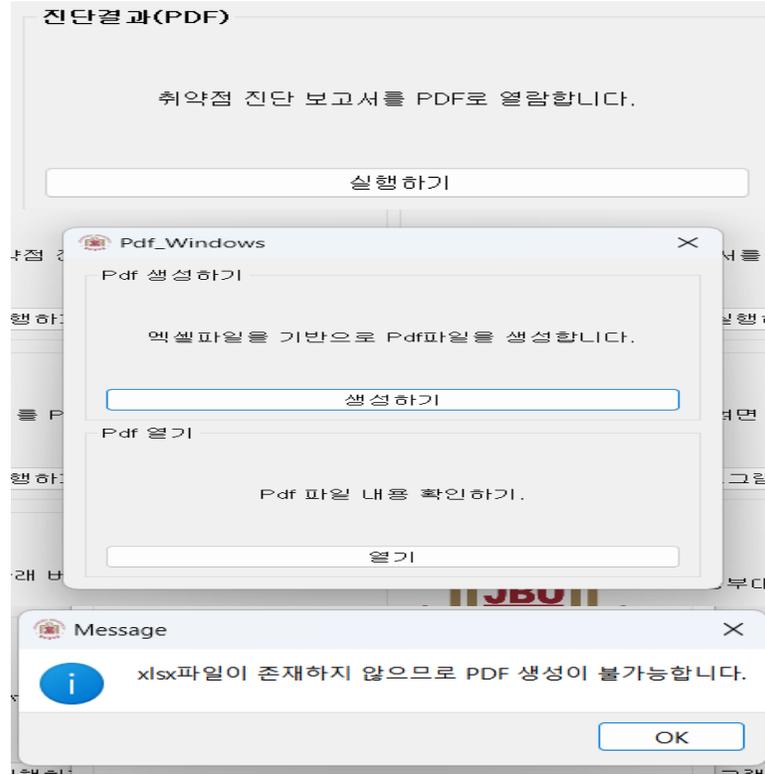
파일 추출 후 화면(관리자 서버)

진단 스크립트 파일 실행 / 결과 가져오기 / 진단 파일 삭제

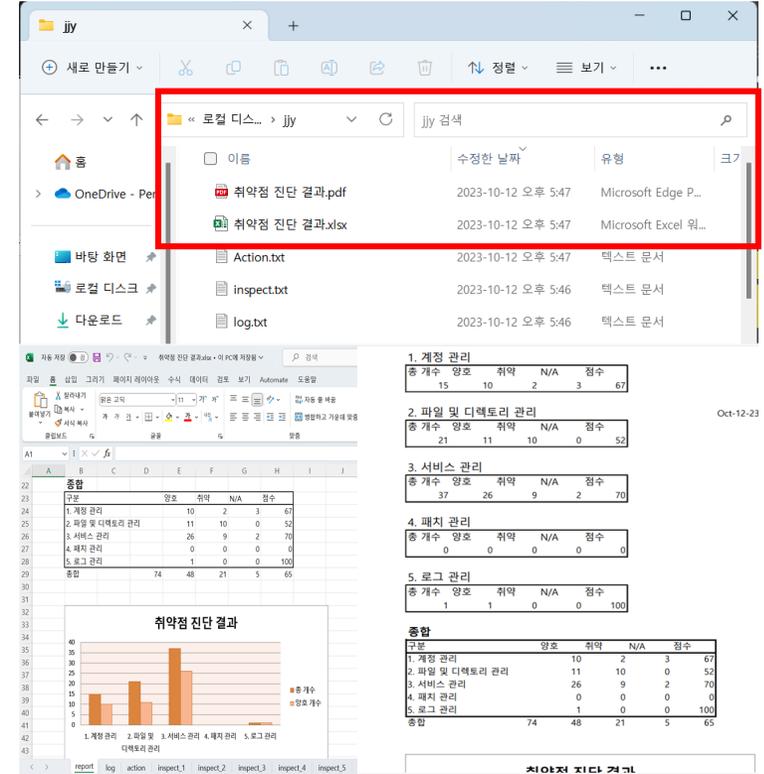
## GUI 구성



엑셀 파일 생성



PDF 파일 생성



파일 생성 결과

진단 결과 엑셀 파일 및 PDF 파일 생성 / 실행(출력)

The image displays a development environment with two main windows:

- Left Window (Python IDE):** Shows a Python script named `main.py` defining a `ProgWindow(QWidget)` class. The `__init__` method calls `super().__init__()` and `self.initUI()`. The `initUI` method sets a `QLabel` with a large text block: `self.label = QLabel('\n' + '본 프로그램은 2023년 중부대학교 공포의 외인부대 팀이 풀' + 'Windows, Linux, Unix 서버에 대한 취약점을 자동으로' + '각 서버에 대한 취약점 진단 항목은 아래와 같습니다.' + '1. Windows 서버(총 82항목)' + '- 계정관리 18항목, 서비스관리 36항목, 패치관리 3항목' + '2. Linux 서버(총 73개 항목)' + '- 계정관리 15항목, 파일 및 디렉터리관리 28항목, 서비스' + '3. Unix 서버(총 73개 항목)')`. The terminal below shows the command `C:\Users\gamin\AppData\Local\Programs\Python\Python311\python.exe C:\jfy\GUI2\10` and the output `종료 코드 0(으)로 완료된 프로세스`.
- Right Window (Windows Server 2012 VM):** Shows a file explorer window for `로컬 디스크 (C:)` with a search for `jjy`. The search results show a `Window.bat` file and three text files: `XXXXActionXXXX.txt`, `XXXXInspectXXXX.txt`, and `XXXXlogXXXX.txt`.

자동진단 프로그램 시연 영상



3

# 결론

---

기대효과

프로젝트 기대효과



## 프로젝트 기대효과



## 취약점 점검 효율성 증대

자동 진단도구 활용으로  
취약점 진단 시간 단축



## 최신 취약점 유형 연구

식별된 취약점을 통해  
주요정보통신기반  
취약 유형 연구



## 빠른 취약점 위치 식별

잠재적 취약점 발생 요소  
파악 및 대처



## 보안 역량 강화

진단 결과 보고서 및 조치  
가이드 기반 취약점 보완으로  
담당자 보안 역량 강화

Thank You

