취약점 진단 자동화 시스템

2018. 11. 7

지 도 교 수 : 유승재 교수님

T E A M : G2TG

(Group.2 Think Great)

(손현수 이경수 이문호 유승하 이혜빈 한규범 유재명)

목 차

1. 조원 편성
2. 주제 선정
3. 프로젝트 구상도
4. 추진 경과
5. 개발환경 및 시스템 개발
6. 개발 결과 및 시스템 운영
7. 결론 및 기대효과

조원 편성

손현수(조장)

- Windows08, 12 Reporting System
- Windows Reporting Program(GUI)

공통 : Research, Show attack scenarios

이경수

- Kali Linux Reporting System
- Linux Reporting Program(GUI)

이문호

- Solaris Reporting System
- Automation Reporting Program(GUI)

유승하

- Windows10, 12 Reporting System
- Automation Reporting Program(GUI)

이혜빈

- CentOS Reporting System
- CentOS Reporting Program(GUI)

한규범

- Solaris Reporting System
- Solaris Reporting Program(GUI)

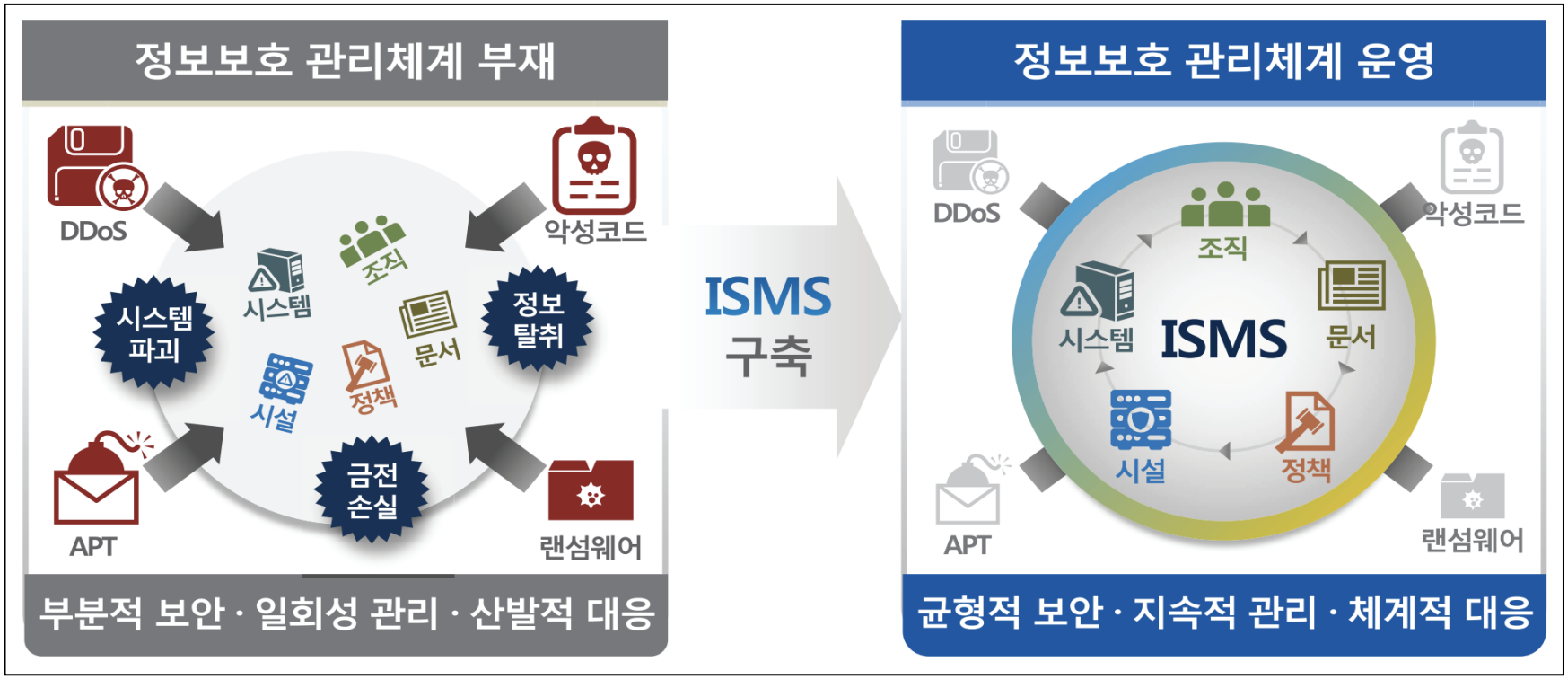
유재명

- Windows08, 12 Reporting System
- Windows Reporting Program(GUI)

주제 선정 (1/2)

❍ 정보보호 관리체계 및 운영실태 부실

- 정보보호 조직 전반의 체계적인 위험관리 체계 부재 ⇨ 일회성 보안관리 및 산발적 대응



ISMS(Information Security Management System) : 기업이 주요 정보자산을 보호하기 위해 수립·관리·운영하는 정보보호 관리체계가 인증기준에 적합한지를 심사하여 인증을 부여하는 제도

주제 선정 (2/2)

❍ 사이버위협의 증가와 ISMS인증의 의무화에 따른 인증률의 점진적 증가

ISMS 인증 의무대상

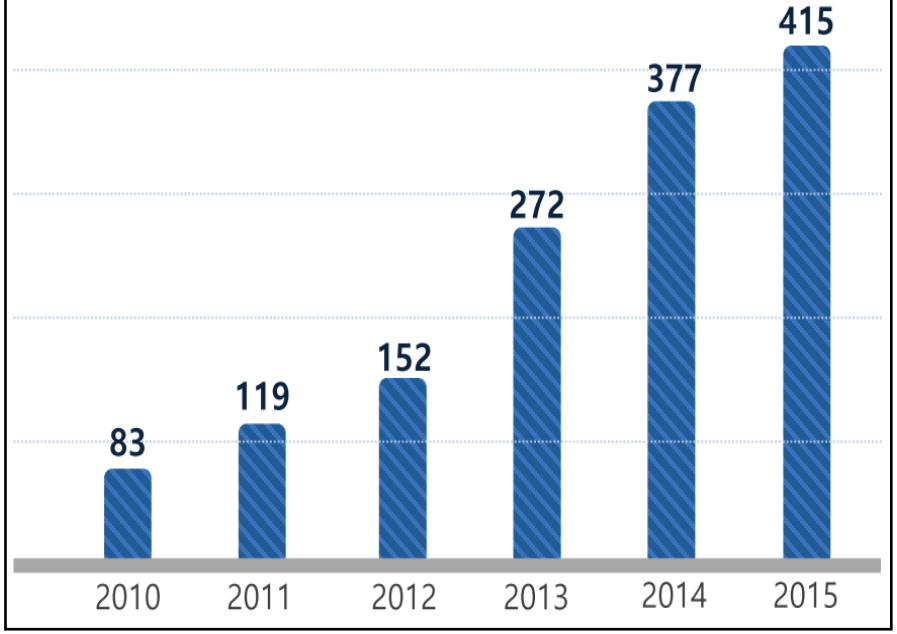
대상자 기준	세부분류 (정보통신서비스제공자)	비고
(ISP)전기통신사업법의 전기통신 사업자로 전국적으로 정보통신망 서비스를 제공하는 사업자	인터넷접속서비스, 인터넷전화서비스 등	서울 및 모든 광역시에서 정보통신망 서비스제공 (SKT,SK브로드 밴드,KT,LGU+등)
(IDC)타인의 정보통신서비스 제공을 위하여 집적된 정보통신시설을 운영·관리하는 사업자	서버호스팅, 코로케이션 서비스 등	정보통신서비스부문 전년도 매출액 100억 이하인 영세 VIDC 제외
(매출액 및 이용자기준)연간 매출액 또는 세입 등이 1,500억원 이상이거나 정보통신서비스 매출액 100억 또는 이용자수 100만명 이상인 사업자	인터넷쇼핑몰, 포털, 게임, 예약, Cable-SO 등	정보통신서비스 부문 전년도 매출액 100억이상 또는 전년도말 기준 직전 3개월간 일일평균 이용자수 100만명 이상
	상급종합병원 대학교	직전연도12월31일기준으로 재학생 수가 1만명 이상인 고등교육법 제2조에 따른 학교

출처 : KISA ISMS제도 소개

의무대상자 미인증시 3,000만원 이하의 과태료 (정보통신망법 제 76조 근거)

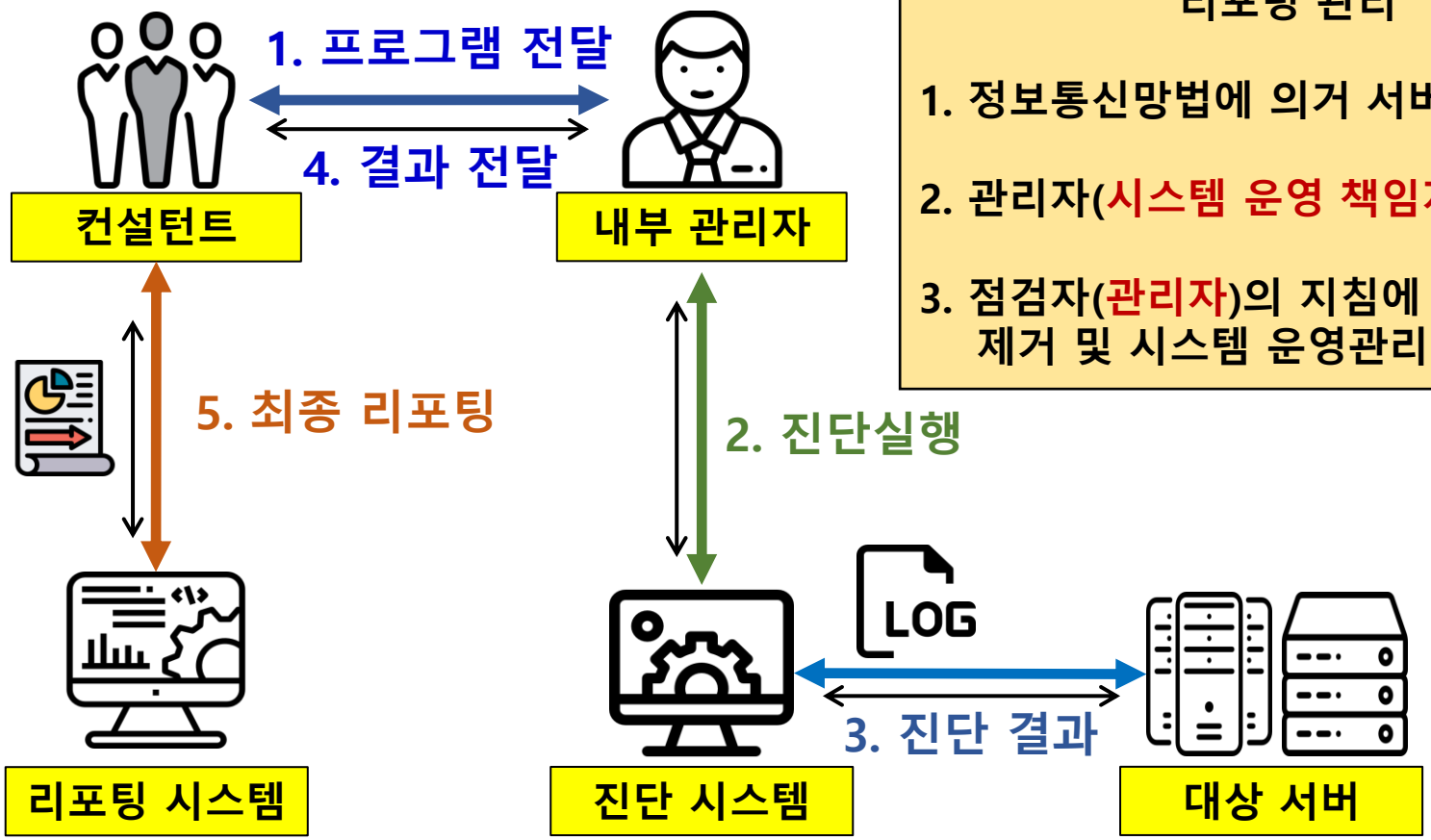
ISMS 인증 추이

출처 : KISA ISMS인증제도 안내PDF



❍ 이에 따라 인증 솔루션 개발의 전 단계로 취약점 점검 자동화 시스템 개발

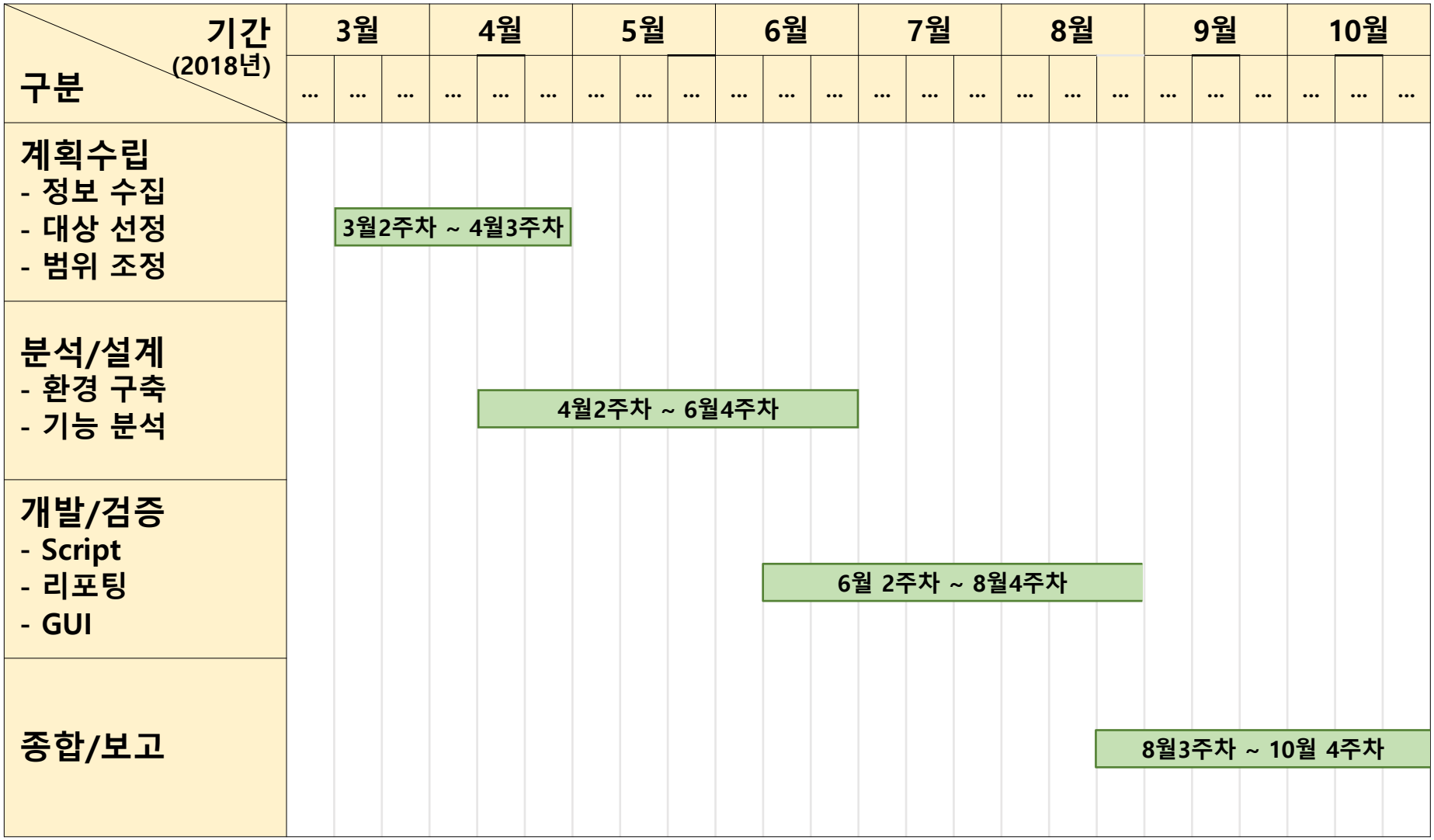
프로젝트 구상도



리포팅 관리

1. 정보통신망법에 의거 서버 취약점 점검
2. 관리자(시스템 운영 책임자) 보고
3. 점검자(관리자)의 지침에 의거 취약점 제거 및 시스템 운영관리 조정

추진 경과


기간
(2018년)
구분
3월
4월
5월
6월
7월
8월
9월
10월
계획수립
- 정보 수집
- 대상 선정
- 범위 조정
3월2주차 ~ 4월3주차
분석/설계
- 환경 구축
- 기능 분석
4월2주차 ~ 6월4주차
개발/검증
- Script
- 리포팅
- GUI
6월 2주차 ~ 8월4주차
종합/보고
8월3주차 ~ 10월 4주차

개발환경 및 시스템 개발(1/8)

개발 환경

대상
- Windows 08,10,12,16
- Linux System
- Unix System

Language
- Python
- C/C++

참고자료
- 주요정보통신 기반시설
- KISA 인증신청 가이드라인
- 금융보안원 인증기준 항목

Script
- Shell Script
- Windows Batch Script

개발환경 및 시스템 개발(2/8)

취약점 점검 항목

- 윈도우 82항목, 리눅스,유닉스 73항목

1. 계정관리	2. 파일시스템	3. 네트워크 서비스
- Default 계정 삭제 - Root 권한관리 - Password 권한	- 사용자 설정 - Inetd, xinetd 설정 - Crontab, profile, hosts, issue 설정	- RPC, NFS, NIS 제한 - Automountd 제거 - r' commands 제거
4. 로그 관리	**5. 주요 응용 설정**	**6. 보안 패치**
- System log setting - 로그 저장주기	- FTP 사용자 - SNMP, SMTP 설정 - DNS, SWAT 설정	- 보안패치 적용

*선정 기준 — KISA 주요정보통신기반시설 기술취약점 점검 리스트 참고

개발환경 및 시스템 개발(3/8)

시스템 개발

- Windows Script 제작

서비스관리 W-30

```
19 sc query W3SVC | findstr /I "state 상태" | f
20 IF NOT ERRORLEVEL 1 set IIS_STATUS="running"
21 IF ERRORLEVEL 1 set IIS_STATUS="stopped"
22 if !IIS_STATUS!=="stopped" (
23     set IIS_VERSION="null"
24 )
25 if !IIS_STATUS!=="running" (
26     if not exist "%systemroot%\system32\inetsrv\appcmd.exe"
27         echo debug: IIS6 시작
28         set IIS_VERSION="iis6_under"
29         echo debug: !IIS_VERSION!
30     ) else (
31         echo debug: IIS7 시작
32         set IIS_VERSION="iis7_over"
33         echo debug: !IIS_VERSION!
34     )
35 )
36 echo debug: %IIS_STATUS%
37 echo debug: %IIS_VERSION%
```

IIS 진단 전 버전 체크

개발환경 및 시스템 개발(4/8)

시스템 개발

- Windows Script 제작

서비스관리 W-30

```
 85 echo debug: %IIS_STATUS%
 86 if %IIS_STATUS%=="stopped" (
 87     echo debug: iis disable
 88     echo IIS 서비스가 비활성화 됨 >> %RESULT%
 89 )
 90 if %IIS_STATUS%=="running" (
 91     echo ## .asa 매핑 정보 확인 ## >> %RESULT%
 92     if %IIS_VERSION%=="iis6_under" (
 93         echo debug: IIS7 시작
 94         type %RESOURCE_1% | findstr /I "[/ ScriptMaps .asa"
 95         echo. >> %RESULT%
 96     )
 97     if %IIS_VERSION%=="iis7_over" (
 98         echo debug: IIS7 시작
 99         type %RESOURCE_4% | findstr /I "디렉토리 .asa" | fir
100         echo. >> %RESULT%
101     )
102 )
103 type %RESOURCE_4% | findstr /I "디렉토
```

해당 버전에 맞는 진단

개발환경 및 시스템 개발(5/8)

시스템 개발

- CentOS Script 제작

파일시스템 U-16

```
#!/bin/sh
F_NAME="$(dirname $0)/result_$(basename $0 | sed 's/.sh//' ).
echo "[LCv7-2.11]" > ${F_NAME}
echo "PATH 환경변수 설정 (중)" >> ${F_NAME}
##### 점검 현황 출력 #####
echo "[점검 현황]" >> ${F_NAME}
echo "1. PATH 환경변수 현황 "  >> ${F_NAME}
echo $PATH >> ${F_NAME}
##### 상태 출력 ######
echo "[상태]" >> ${F_NAME}
RESULT="양호"
ENV_PATH=$(echo $PATH)
if [[ "$ENV_PATH" =~ "." ]]
then
    RESULT="취약"
fi
echo $RESULT >> ${F_NAME}
```

PATH 환경변수 점검

개발환경 및 시스템 개발(6/8)

시스템 개발

- Solaris Script 제작

계정관리 U-02

```
#!/bin/sh
CURRENT_PATH=`dirname $0`
NAME=`basename $0`
RESULT="$CURRENT_PATH/result_$NAME.txt"
echo "[U-06]" >> ${RESULT}
echo "패스워드 최소길이 설정" >> ${RESULT}
echo "[점검 현황]" >> ${RESULT}
cat /etc/default/passwd | egrep "PASSLENGTH" >> ${RESULT}
echo "" >> ${RESULT}
#### 상태
echo "[상태]" >> ${RESULT}
if [ `cat /etc/default/passwd | egrep "PASSLENGTH" | cut -d"=
    echo "양호" >> ${RESULT}
else
    echo "취약" >> ${RESULT}
fi
```

패스워드 사용규칙 점검

개발환경 및 시스템 개발(7/8)

시스템 개발

- GUI 개발

```
117 function first_menu()
118 {
119
120
    {ACC
    }"
121
122
123
124
125
126
127
128
129 }
130 func
131 {
132
133
134 }
135 func
136 {
137
138
    "점 검
139
140
```

점검 프로그램

Vulnerability Check system

[Profile]
- Name : Hye Been Lee
- Team : G2TG
- Univ : Joonbu University
- Major : Information Security
- Birth : 1996.01.11
- Blog : itlearner.tistory.com
- E-mail : v_v111222@nate.com

If you have any question, contact me.

< OK >

Main GUI 개발

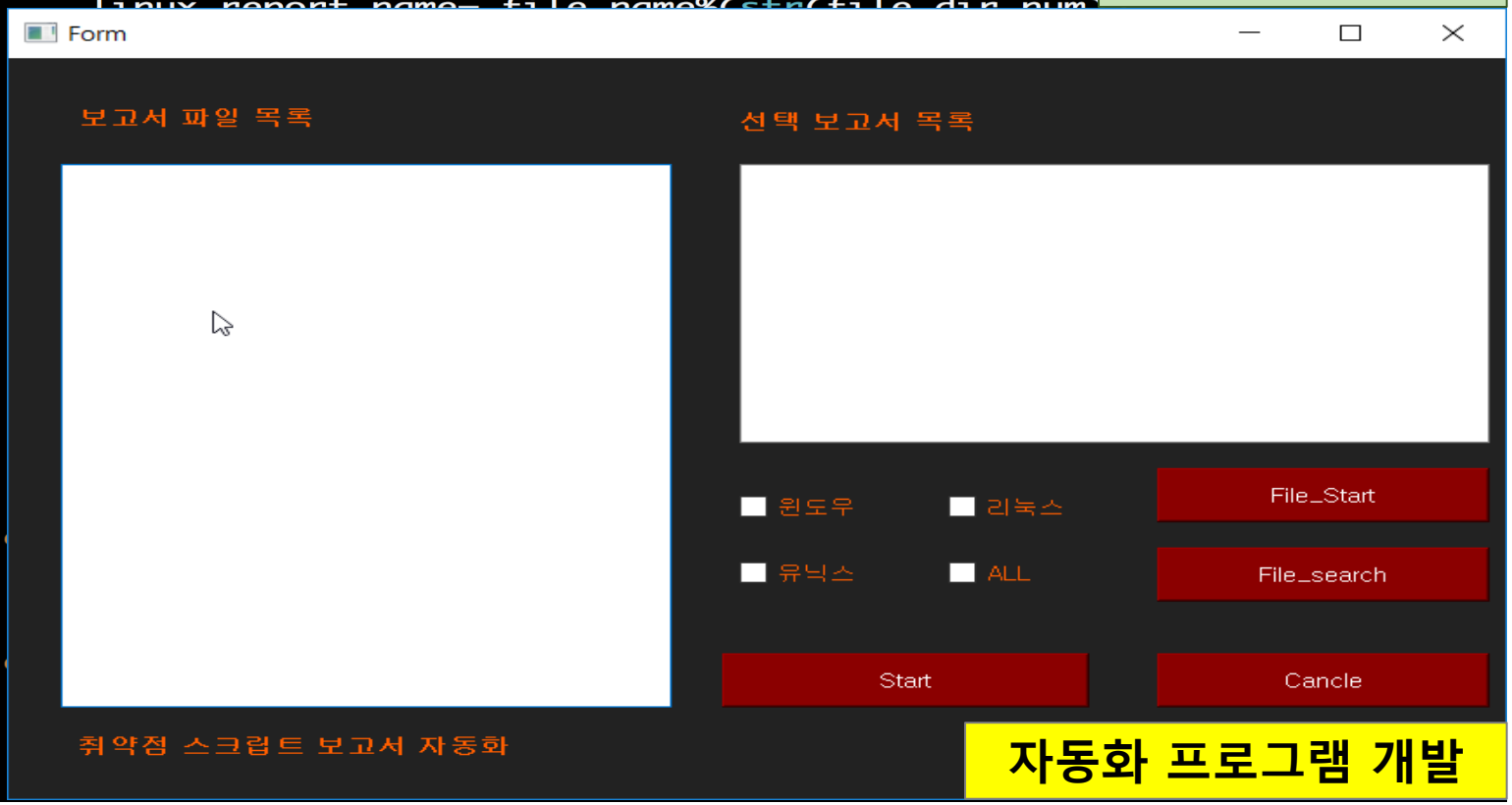
개발환경 및 시스템 개발(8/8)

시스템 개발

- 리포팅 프로그램 개발

```
177     def linux_unix(self,wb,ws,stack_cell_row,stack_arry
178         view_list_name = []
179         linux_report_name= file_name%(str(file_dir_num)
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
```

Reporting 종합

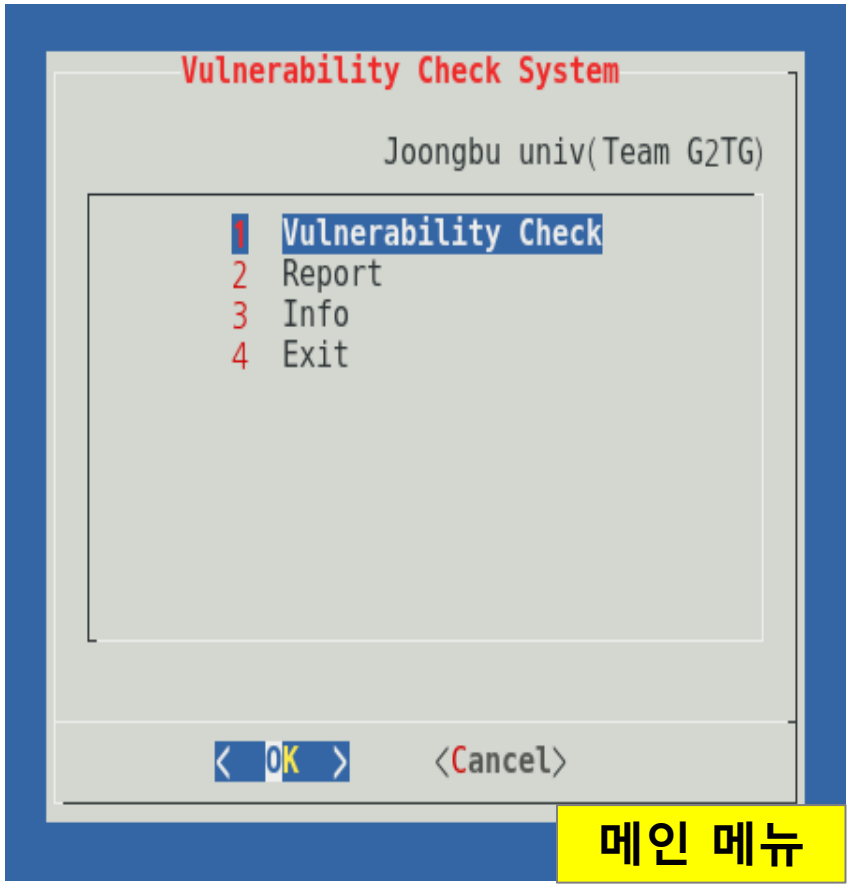


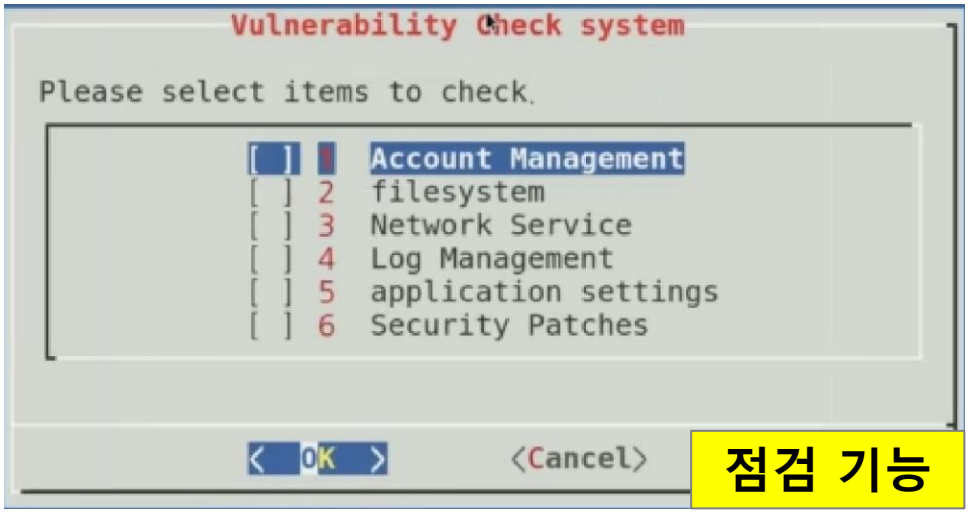
자동화 프로그램 개발

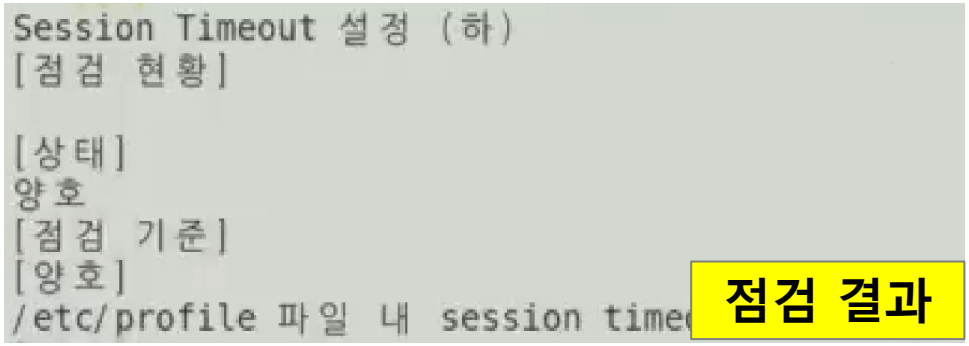
개발 결과 및 시스템 운영(1/4)

Main GUI

- GUI 기능설명

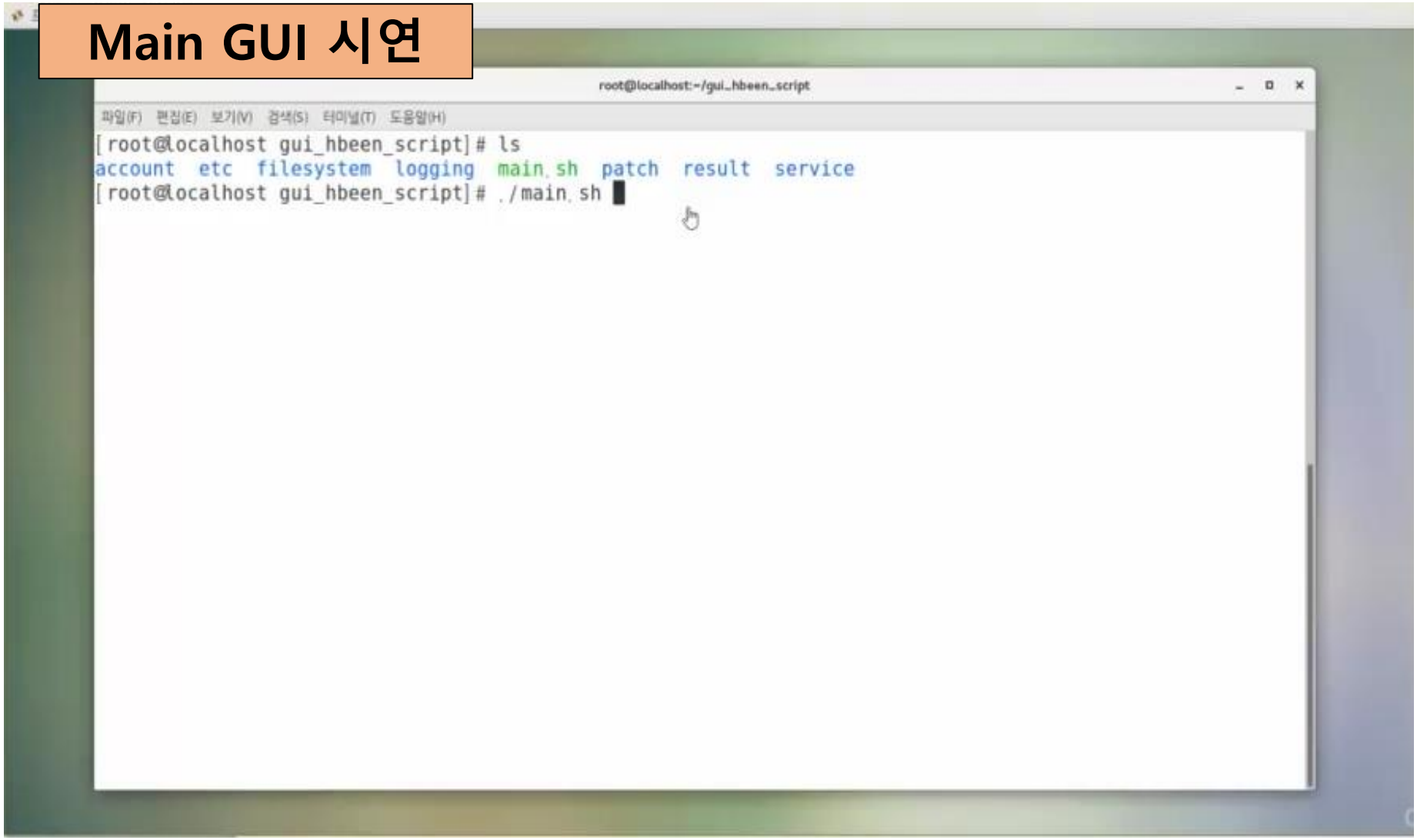






개발 결과 및 시스템 운영(2/4)

Main GUI 시연



개발 결과 및 시스템 운영(3/4)

Reporting 종합

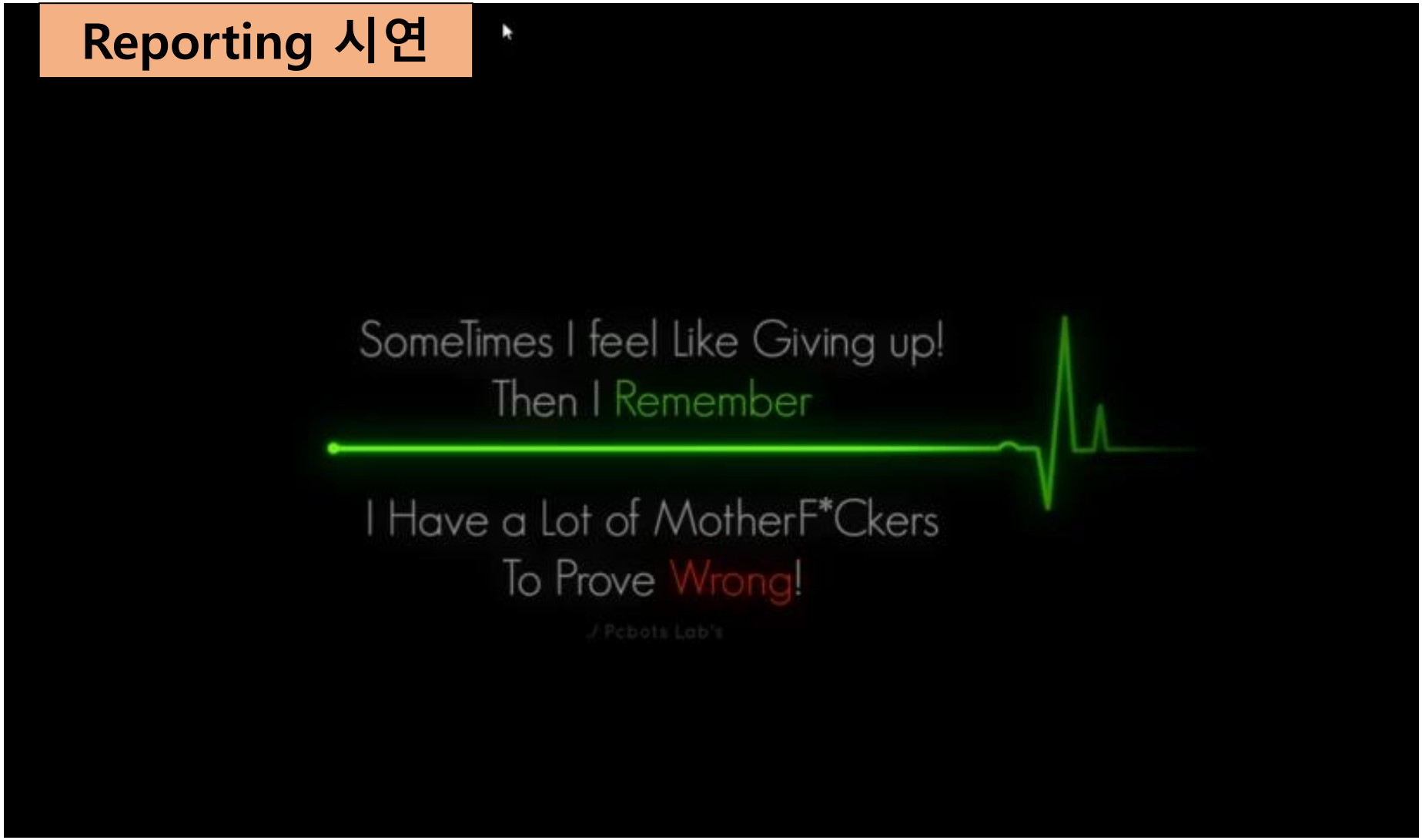
- 최종 결과 산출 프로그램

no.	점검항목	점검현황	상태
[W08-01-04]	계정 잠금 임계값 설정 (상)	## 계정 잠금 임계값 설정 ## Lockout threshold: 6 Lockout duration (minutes): 30	"취약"
[W08-01-04]	계정 잠금 임계값 설정 (상)	## 계정 잠금 임계값 설정 ## Lockout threshold: 6 Lockout duration (minutes): 30	"취약"

프로그램 결과

개발 결과 및 시스템 운영(4/4)

Reporting 시연



결론 및 기대효과

❖ 취약점 진단 자동화 시스템 개발 성과

- 개발 시스템은 취약점 진단 결과를 실시간 획득, 신속한 점검 및 대응이 가능하도록 지원하고 실무자의 편의성을 보장

- 또한 시스템의 모듈화 개발로 유지보수 및 관리가 용이

❖ 기대 효과

- 모든 조원들이 임무를 분담하여 맡은 부분의 프로그래밍을 완성함에 따라 프로그래밍 능력을 향상시키는 계기

- 취약점 진단 요소 하나 하나를 이해하고 실무 프로그램으로 구현하는 과정에서 취약점 진단 업무의 실무까지 익히는 부수적인 성과

Q & A

감사합니다