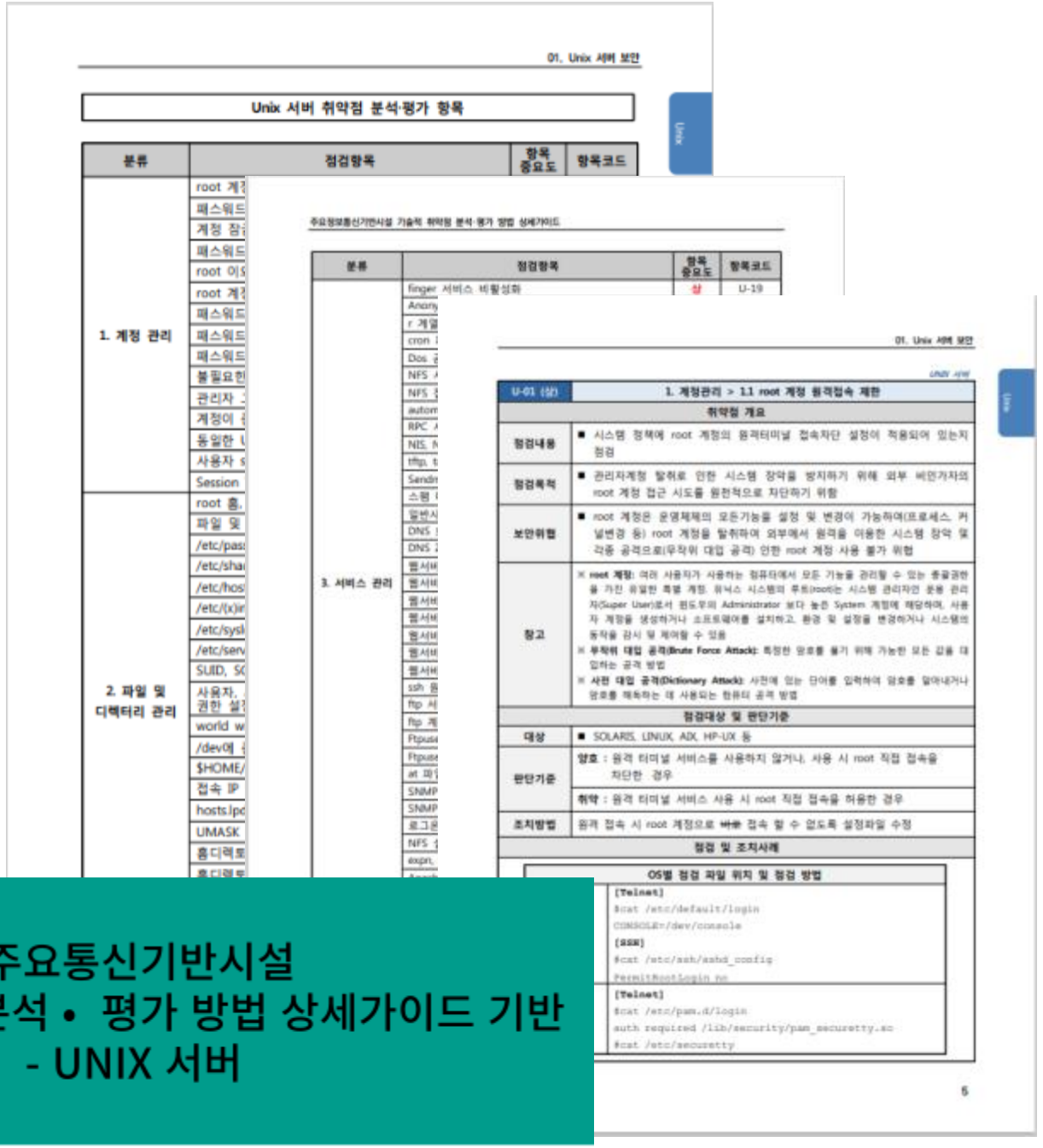
모 그 로 그

Linux 취약점 진단 및 로그 기반 이상 행위 탐지 서비스

강성현
송소연
정지수
김고운
윤지예

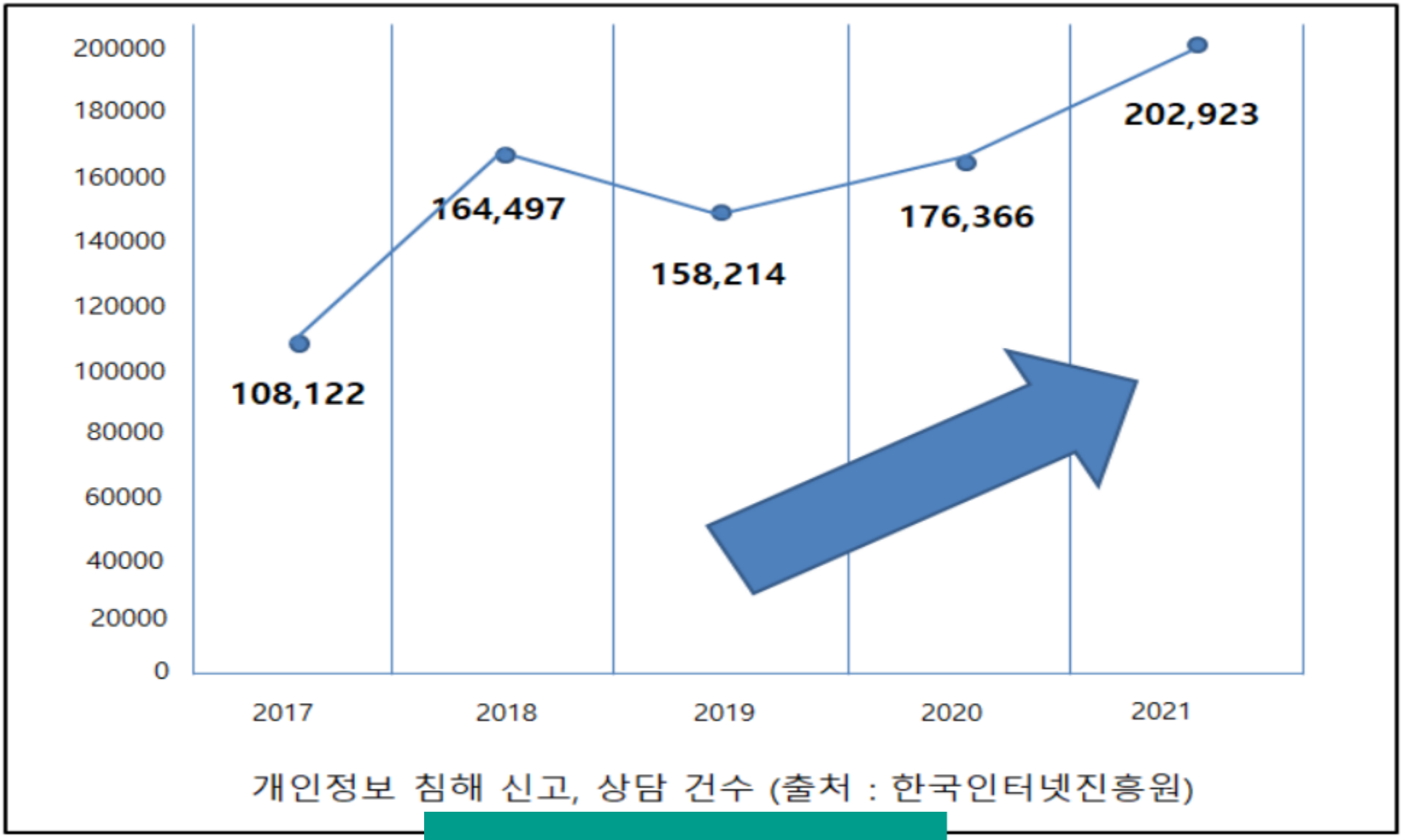
CONTENTS

Contents 01 프로젝트 소개



주요통신기반시설
기술적 취약점 분석 • 평가 방법 상세가이드 기반
- UNIX 서버

Contents 01 프로젝트 주제 선정 이유



개인정보 침해 신고, 상담 건수 (출처 : 한국인터넷진흥원)

개인정보 침해 신고 계속해서 증가

Linux
Shell Script

python

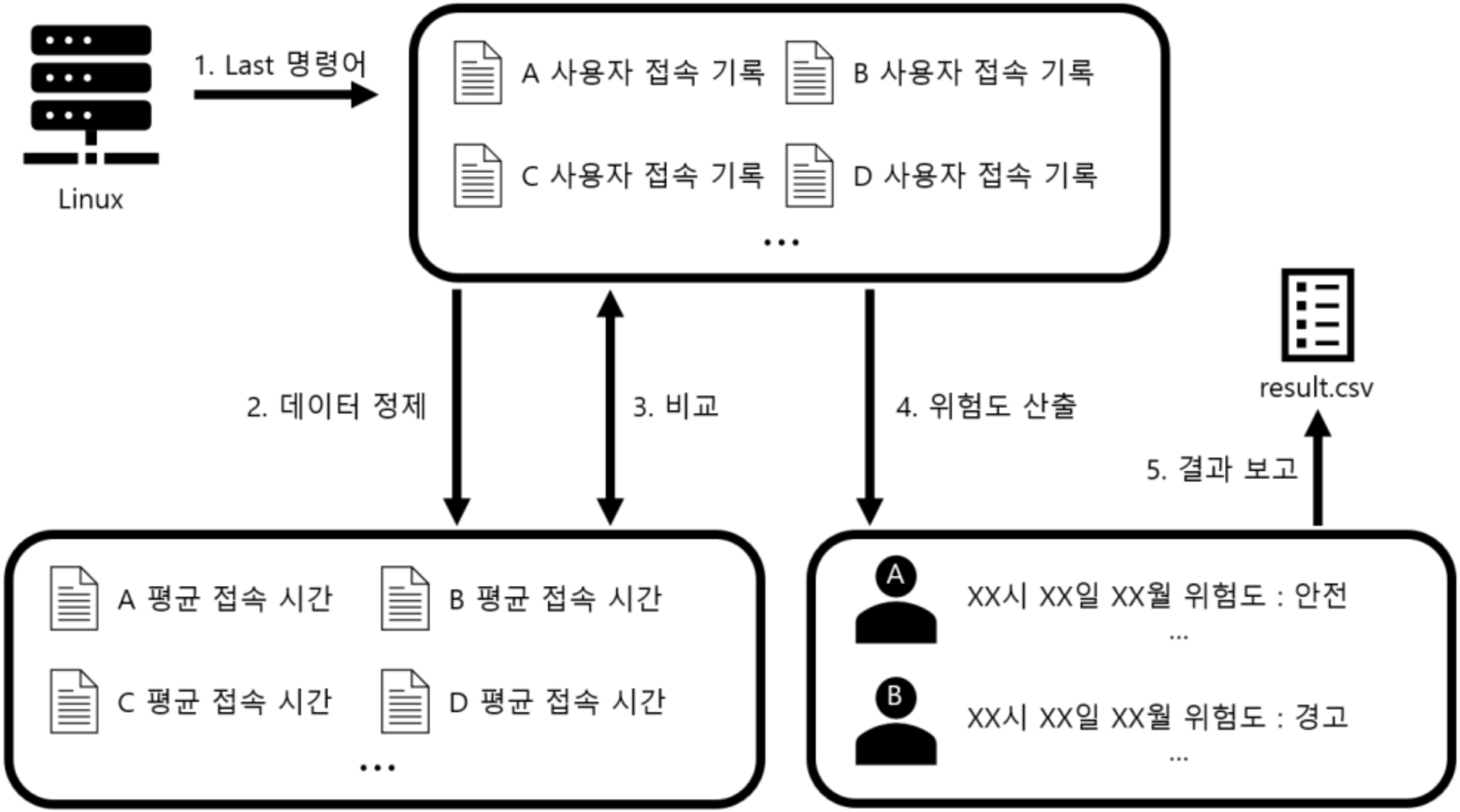
Windows®

SSH

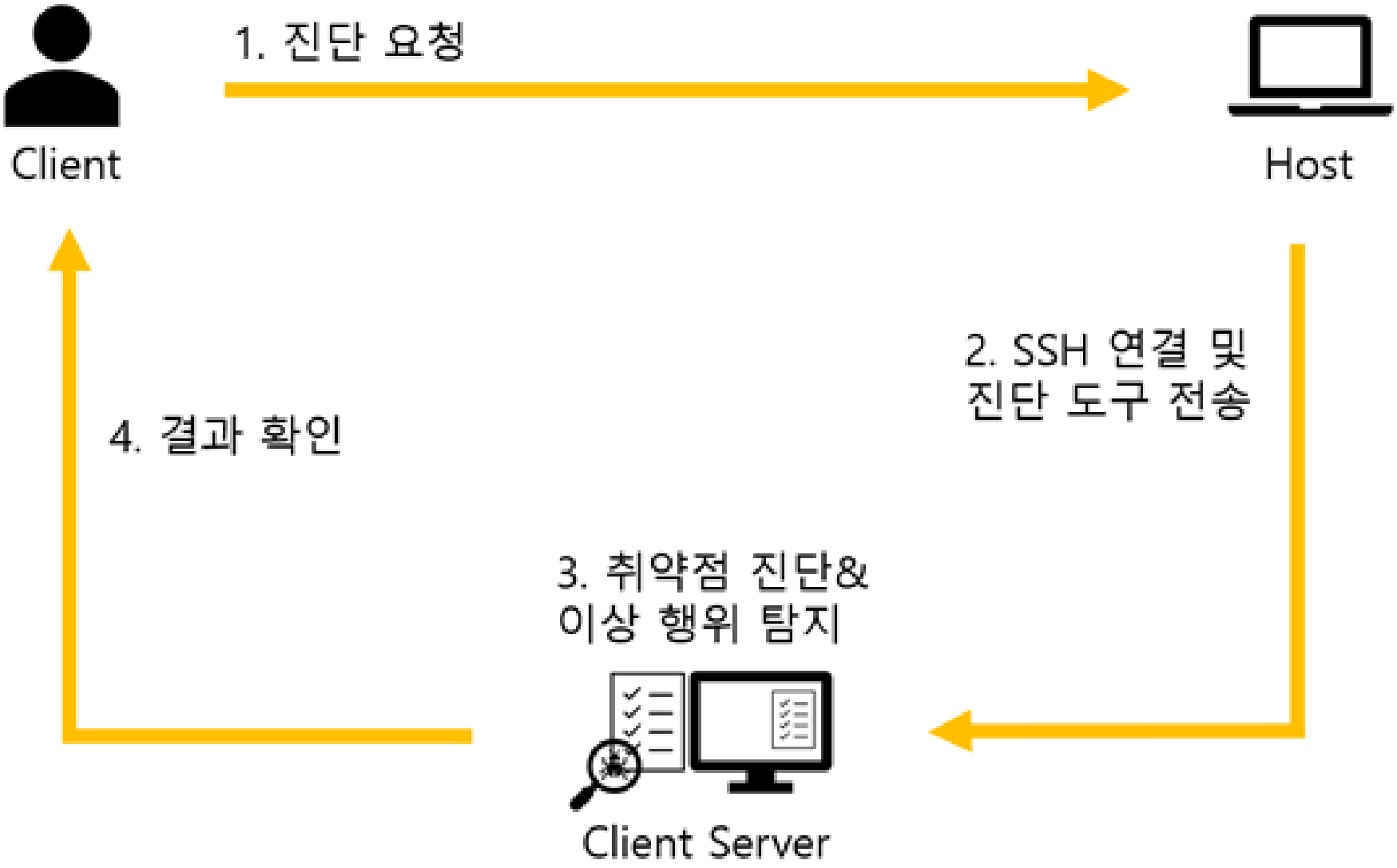
Contents 01 팀원 소개 및 역할 분담

이름	역할
강성현 (팀장)	로그 기반 이상 행위 탐지 서비스 진단 도구 개발
송소연	로그 기반 이상 행위 탐지 서비스 진단 도구 개발
정지수	linux 취약점 진단 도구 개발
김고운	linux 취약점 진단 도구 개발
윤지예	linux 취약점 진단 도구 개발
공통	GUI 개발

Contents 02 프로젝트 구상도 (로그 기반 이상 행위 탐지)



Contents 02 프로젝트 구상도 (Total)



```
#echo "항목 코드 U-01"

SECURETTY=/etc/securetty
SECURE=$(cat $SECURETTY | grep -i "pts" | wc -l)
SSH=/etc/ssh/sshd_config


if [ -e $SECURETTY ] && [ -e $SSH ]; then
        SSHD=$(cat $SSH | grep -E "PermitRootLogin yes|PermitRootLogin no" | awk '{print $2}')
        if [ $SECURE != 0 ] && [[ $SSHD == "yes" ]] ; then
                echo "U-01 취약 상" >> result.csv
        elif [ $SECURE -eq 0 ] && [[ $SSHD == "yes" ]] ; then
                echo "U-01 취약 상" >> result.csv
        else
                echo "U-01 양호 상" >> result.csv
        fi
else
        echo "U-01 점검 상" >> result.csv
fi

#echo "항목 코드 U-02"

PW=/etc/security
PWD=/etc/security/pwquality.conf
MIN=$(cat $PWD | grep "minlen" | awk '{print $4}')

if [ -e $PW ]; then
        if [[ ${MIN} -ge 8 ]]; then
                echo "U-02 양호 상" >> result.csv
        else
                echo "U-02 취약 상" >> result.csv
        fi
else
        echo "U-02 점검 상" >> result.csv
fi

#echo "항목 코드 U-03"
```

linux 취약점 진단 스크립트 작성
(1. 계정관리 항목)

```
#echo "항목 코드 U-05"

PH=$(echo $PATH | egrep "\.:|::|:.:")

if [ -z $PH ]; then
        echo "U-05 양호 상" >> result.csv
else
        echo "U-05 취약 상" >> result.csv
fi

#echo "항목 코드 U-06"

DIR=$(find / \( -nouser -o -nogroup \) -print 2>/dev/null)

if [ -z $DIR ]; then
        echo "U-06 양호 상" >> result.csv
else
        echo "U-06 취약 상" >> result.csv
fi

#echo "항목 코드 U-07"

PWD=$(ls -l /etc/passwd | awk '{print $3}')
PSWD=$(stat -c "%a" /etc/passwd)

if [ "$PWD" == "root" ]; then
        if [ $PSWD -le 644 ]; then
                echo "U-07 양호 상" >> result.csv
        else
                echo "U-07 취약 상" >> result.csv
        fi
else
        echo "U-07 취약 상" >> result.csv
fi
```

linux 취약점 진단 스크립트 작성
(2. 파일 및 디렉터리 관리)

```
#!/bin/bash

#echo "항목코드 U-19"

ls -lL /etc/xinetd.d |grep finger > /dev/null 2>&1

if [ $? -eq 0 ]; then
        echo "U-19취약 상" >> result.csv
else
        echo "U-19 양호 상" >> result.csv
fi

#echo "항목코드 U-20"

if [ -f /etc/vsftpd/vsftpd.conf ]; then
        if grep -q "ftp" /etc/vsftpd/vsftpd.conf; then
                echo "U-20 양호 상" >> result.csv
        else
                echo "U-20 취약 상" >> result.csv
        fi
else
        echo "U-20 점검 상" >> result.csv
fi

#echo "항목코드 U-21"

files=$(ls -alL /etc/xinetd.d/* /dev/null 2>&1 | egrep "rsh|rlogin|rexec" | egrep -v "grep|klogin|kshell|kexec")

if [ -n "$files" ]; then
        echo "U-21 취약 상" >> result.csv
else
        echo "U-21 양호 상" >> result.csv
fi

#echo "항목코드 U-22"

cron_file="/etc/crontab"
cron_owner=$(stat -c %U "$cron_file")
cron_permissions=$(stat -c %a "$cron file")
```

linux 취약점 진단 스크립트 작성
(3. 서비스 관리)

```
#!/bin/bash

#echo "항목 코드 U-42"
echo "U-42 취약 상 ">> result.csv

#echo "항목 코드 U-43"
echo "U-43 점검 상" >> result.csv

#echo "항목 코드 U-72"
echo "U-72 점검 하" >> result.csv
```

linux 취약점 진단 스크립트 작성
(4. 패치 관리 & 5.로그 관리)

Contents 02 프로젝트 진행 방법 및 개발 내용

```
#!/bin/bash

if grep -qF "01" error.txt; then
        echo "U-01 조치 방법 안내" >> finish.csv
        echo "root 계정 원격접속 제한" >> finish.csv
        echo -e "[Telnet 서비스 사용시]\n 1. '/etc/securetty' 파일에서 pts/x 설정 제거 또는, 주석 처리\n 2. '/etc/pam.d/login' 파일 수정 또는, 신규 삽입\n (수정 전) #auth r
rity/pam_securetty.so\n (수정 후) auth required /lib/security/pam_securetty.so" >> finish.csv
        echo -e "[SSH 서비스 사용시]\n 1. vi편집기를 이용하여 '/etc/ssh/sshd_config' 파일 열기\n 2. 아래와 같이 주석 제거 또는, 신규 삽입\n (수정 전) #PermitRootLogin Yes\n
RootLogin No" >> finish.csv
        echo "" >> finish.csv
fi

if grep -qF "02" error.txt; then
        echo "U-02 조치 방법 안내" >> finish.csv
        echo "패스워드 복잡성 설정" >> finish.csv
        echo -e "1. 패스워드 복잡성 설정 파일 확인\n #/etc/security/pwquality.conf 파일 수정\n 2. 패스워드 정책을 설정함\n password requisite pam_cracklib.so try_first_pass
 lcredit=-1 ucredit=-1 dcredit=-1 ocredit=-1" >> finish.csv
        echo "" >> finish.csv
fi

if grep -qF "03" error.txt; then
        echo "U-03 조치 방법 안내" >> finish.csv
        echo "계정 잠금 임계값 설정" >> finish.csv
        echo -e "1. vi 편집기를 이용하여 '/etc/pam.d/system-auth' 파일 열기\n 2. 아래와 같이 수정 또는, 신규 삽입\n auth reqired /lib/security/pam_tally.so deny=5 unlock_ti
oot\n account required /lib/security/pam_tally.so no_magic_root reset" >> finish.csv
        echo "" >> finish.csv
fi

if grep -qF "04" error.txt; then
        echo " U-04 조치 방법 안내" >> finish.csv
        echo "패스워드 파일 보호" >> finish.csv
        echo -e "1. #pwconv ---> 쉐도우 패스워드 정책 적용 방법\n 2. #pwunconv ---> 일반 패스워드 정책 적용 방법" >> finish.csv
        echo "" >> finish.csv
fi

if grep -qF "05" error.txt; then
        echo "U-05 조치 방법 안내" >> finish.csv
        echo "root홈, 패스 디렉터리 권한 및 패스 설정" >> finish.csv
        echo -e "1. vi 편집기를 이용하여 root 계정의 설정 파일(~/.profile 과 /etc/profile) 열기\n 2. 아래와 같이 수정\n                                                  H=$P
>> finish.csv
```

vi error.sh

```
#!/bin/bash

while true :
        do
                ./moglog/moglog/result.sh # 취약점 진단 쉘 파일
                ./moglog/moglog/nds.sh # 이상행위 진단 쉘 파일
                break
        done
~
```

vi moglog.sh

```
#!/bin/bash

while true :
        do
                echo "ACCOUNT START"
                ./moglog/moglog/account.sh
                echo "ACCOUNT END"
                echo ""

                echo "FILE START"
                ./moglog/moglog/file.sh
                echo "FILE END"
                echo ""

                echo "SERVICE START"
                ./moglog/moglog/service.sh
                echo "SERVICE END"
                echo ""

                echo "LOG START"
                ./moglog/moglog/log.sh
                echo "LOG END"
                break
        done


grep "양호" result.csv >> result.txt


count=0
count1=0
count2=0

while read -r line
do
    if echo "$line" | grep -q "상"; then
        count=$(($count+3))
    elif echo "$line" | grep -q "중"; then
        count1=$(($count1+2))
    else
```

vi result.sh

```
users=$(grep /bin/bash /etc/passwd | cut -f1 -d:)
echo "사용자,로그인 날짜(월),로그인 날짜(일),로그인 시각(시),위험도" >> result.csv
sed -i '1s/^/\n/' result.csv
rm userstime.txt
for user in $users; do
  last "$user" | awk '{if($1=="'$user'") {print $4, $5, $6, $7, $8, $9}}' | awk '!/crash/ && !/still/ && !/logged/ {print}' > "${user}.txt"
  if [ -s "${user}.txt" ]; then
    echo "${user}.txt save to file completely"
  else
    echo "${user}.txt save to file False"
  fi
  file="${user}.txt"
  login_times=($(awk '{split($4, a, ":"); print a[1]}' "$file"))
  login_months=($(awk '{print $2}' "$file"))
  login_dates=($(awk '{print $3}' "$file"))
  logout_times=($(awk '{split($6, a, ":"); print a[1]}' "$file"))
  total_login=0
  total_logout=0
  for time in "${login_times[@]}"; do
    ((total_login+=time))
  done
  for time in "${logout_times[@]}"; do
    ((total_logout+=time))
  done
  if [ "${#login_times[@]}" -gt 0 ]; then
    avg_login=$((total_login / ${#login_times[@]}))
  else
    avg_login=0
  fi
  if [ "${#logout_times[@]}" -gt 0 ]; then
    avg_logout=$((total_logout / ${#logout_times[@]}))
  else
    avg_logout=0
  fi
  echo "사용자: $user" >> userstime.txt
  echo "로그인 평균 시간: $avg_login" >> userstime.txt
  echo "로그아웃 평균 시간: $avg_logout" >> userstime.txt
  for ((i=0; i<${#login_times[@]}; i++)); do
```

로그기반 이상행위탐지 스크립트 작성

```
#!/usr/bin/python3

import tkinter as tk
from tkinter import *
from tkinter import ttk
import paramiko
import subprocess
import os
import tkinter.messagebox as messagebox
import shutil

import requests
from io import BytesIO
from PIL import Image, ImageTk
import tkinter.font

# MOGLOG v1.0 GUI 창 생성
window = tk.Tk()
window.title("MOGLOG v1.0")
window.geometry("1100x650")  # 창 크기 설정

# SSH 연결 정보 (미리 초기화)
ip_address = 클라이언트 ip 주소 입력
username = 클라이언트 i d 입력
password = 클라이언트비밀번호 입력
ssh_client =
result_output = ""

# 배경 캔버스 생성
bg_canvas = tk.Canvas(window, bg="white",width=1800, height=600)
bg_canvas.pack()

# "소개" 프레임 생성
intro_frame = tk.Frame(bg_canvas)
intro_frame.pack(side="left",padx=8, pady=10)  # 왼쪽 상단에 붙이기

# "소개" 레이블 생성
intro_label = tk.Label(intro_frame, text="소개", bg="gray", width=50, height=2)
intro_label.config(font=("Helvetica", 10, "bold"))
intro_label.pack()
```

gui 스크립트 작성

Contents 02 프로젝트 진행 방법 및 개발 내용

MOGLOG v1.0

소개

MogLog v1.0은 Linux 시스템의 취약점을 진단하고 로그 기반 사용자 이상행위를 탐지하는 프로그램입니다.

* 취약점 진단은 2021년 '주요정보통신기반시설 기술적 취약점 분석 평가 방법 상세 가이드'를 기반으로 하였습니다.

- 계정 관리 : 불필요한 계정 제거 외 14개 항목
- 파일 및 디렉터리 관리 : UMASK 설정 관리 외 18개 항목
- 서비스 관리 : ftp 서비스 확인 외 34개 항목
- 패치 관리 : 최신 보안패치 및 벤더 권고사항 적용
- 로그 관리 : 로그의 정기적 검토 및 보고 외 1개 항목

* 이상 행위 탐지는 접속 로그를 추출하여 통계 분석을 통해 평균 이외의 접속 기록을 이상 행위로 판단 후 로그 기록을 하였습니다.

- Step1. Linux 시스템은 사용자의 접속 기록을 월/일/시간 형태로 저장할 수 있으며 이상행위탐지는 이 접속 기록을 사용합니다.
- Step2. 각 접속 기록을 모아 사용자별 평균 접속 시간을 계산하여 비교합니다.
- Step3. 비교 결과에 따라 평균 접속 기록에서 벗어나면 오차범위 1시간 단위로 안전/경고/위험 단계로 분류됩니다.

취약점 진단

Connect — 진단 대상 시스템과의 연결을 합니다.

스크립트 실행 — 시스템 취약점 진단 및 이상행위 탐지를 실행합니다.

결과 확인 — 취약점 진단 결과와 이상행위 탐지에 대한 결과를 Excel로 확인합니다.

Exit — 진단 시스템과 연결을 끊고 프로그램을 종료합니다.

JOONGBU UNIVERSITY JBU 중부대학교

제작자

이름 : 강성현 (팀장)
학과 : 정보보호학전공
역할 : 이상 행위 탐지 도구 개발

이름 : 송소연
학과 : 정보보호학전공
역할 : 이상 행위 탐지 도구 개발

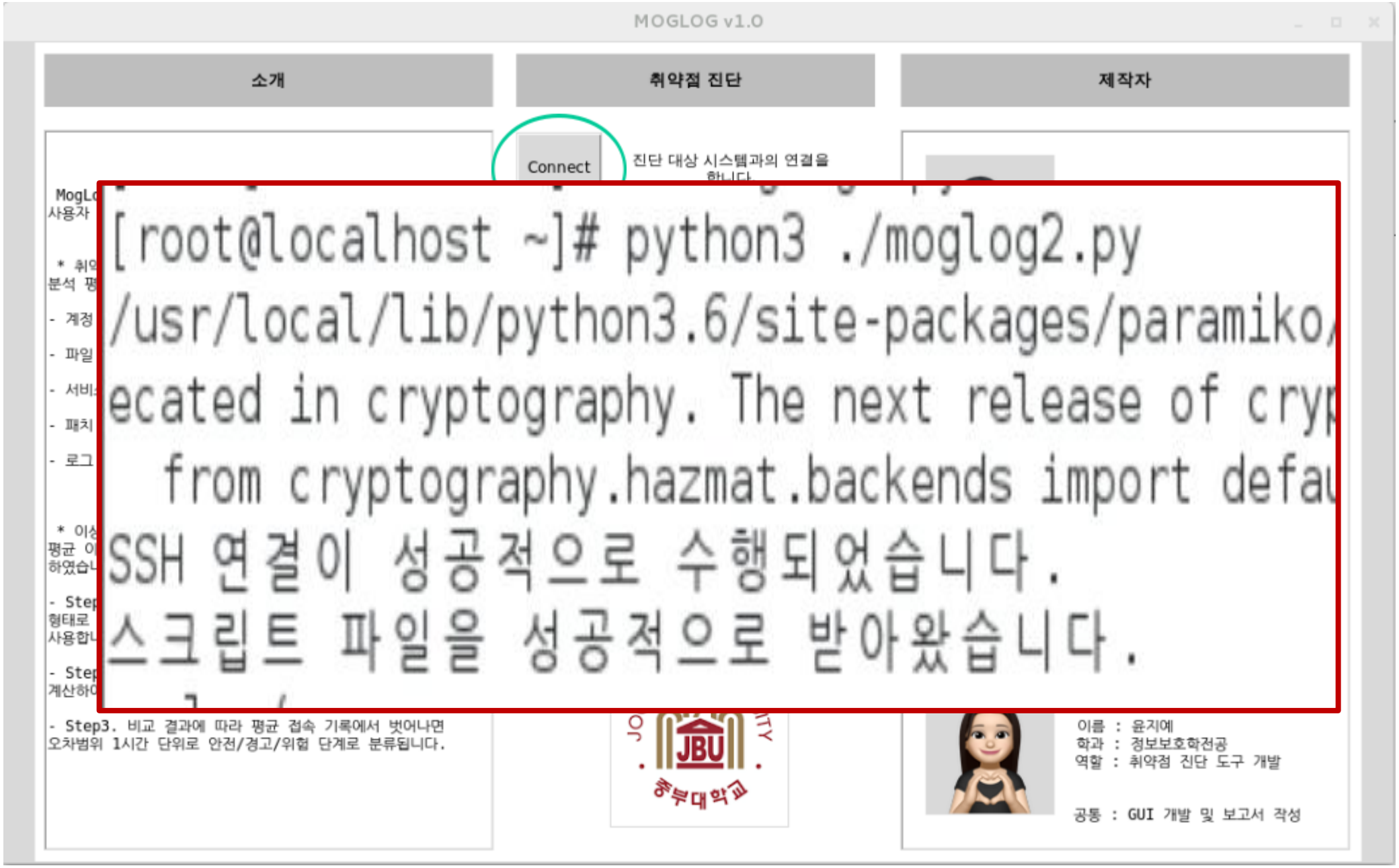
이름 : 정지수
학과 : 정보보호학전공
역할 : 취약점 진단 도구 개발

이름 : 김고운
학과 : 정보보호학전공
역할 : 취약점 진단 도구 개발

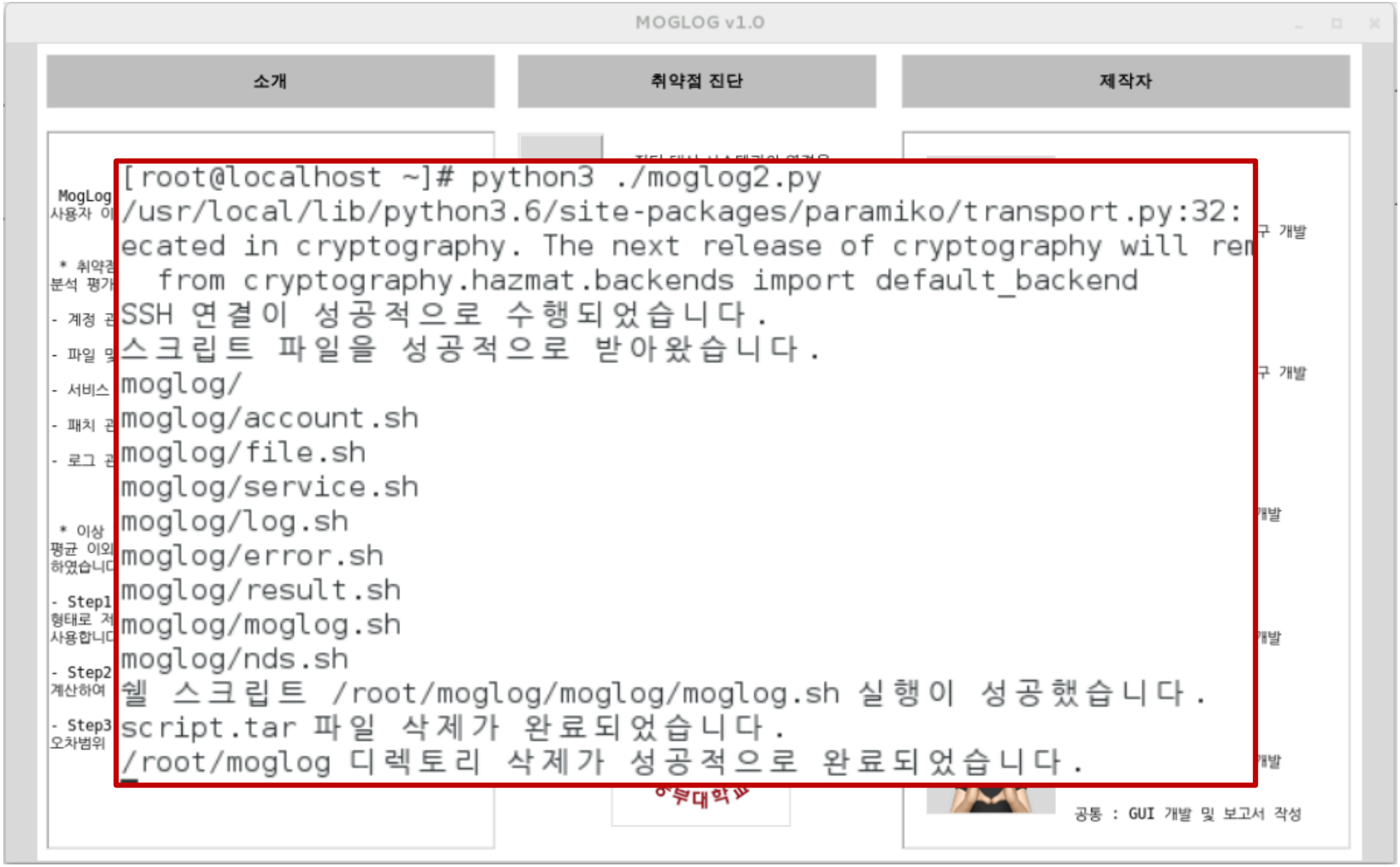
이름 : 윤지예
학과 : 정보보호학전공
역할 : 취약점 진단 도구 개발

공통 : GUI 개발 및 보고서 작성

Contents 02 프로젝트 진행 방법 및 개발 내용



Contents 02 프로젝트 진행 방법 및 개발 내용



Contents 02 프로젝트 진행 방법 및 개발 내용

MOGLOG v1.0

소개

MogLog v1.0은 Linux 시스템의 취약점을 진단하고 로그 기반 사용자 이상행위를 탐지하는 프로그램입니다.

* 취약점 진단은 2021년 '주요정보통신기반시설 기술적 취약점 분석 평가 방법 상세 가이드'를 기반으로 하였습니다.

- 계정 관리 : 불필요한 계정 제거 외 14개 항목
- 파일 및 디렉터리 관리 : UMASK 설정 관리 외 18개 항목
- 서비스 관리 : ftp 서비스 확인 외 34개 항목
- 패치 관리 : 최신 보안패치 및 벤더 권고사항 적용
- 로그 관리 : 로그의 정기적 검토 및 보고 외 1개 항목

* 이상 행위 탐지는 접속 로그를 추출하여 통계 분석을 통해 평균 이외의 접속 기록을 이상 행위로 판단 후 로그 기록을 하였습니다.

- Step1. Linux 시스템은 사용자의 접속 기록을 월/일/시간 형태로 저장할 수 있으며 이상행위탐지는 이 접속 기록을 사용합니다.
- Step2. 각 접속 기록을 모아 사용자별 평균 접속 시간을 계산하여 비교합니다.
- Step3. 비교 결과에 따라 평균 접속 기록에서 벗어나면 오차범위 1시간 단위로 안전/경고/위험 단계로 분류됩니다.

취약점 진단

Connect — 진단 대상 시스템과의 연결을 합니다.

스크립트 실행 — 시스템 취약점 진단 및 이상행위 탐지를 실행합니다.

결과 확인 — 취약점 진단 결과와 이상행위 탐지에 대한 결과를 Excel로 확인합니다.

Exit — 진단 시스템과 연결을 끊고 프로그램을 종료합니다.

JOONGBU UNIVERSITY JBU 중부대학교

제작자

이름 : 강성현 (팀장)
학과 : 정보보호학전공
역할 : 이상 행위 탐지 도구 개발

이름 : 송소연
학과 : 정보보호학전공
역할 : 이상 행위 탐지 도구 개발

이름 : 정지수
학과 : 정보보호학전공
역할 : 취약점 진단 도구 개발

이름 : 김고운
학과 : 정보보호학전공
역할 : 취약점 진단 도구 개발

이름 : 윤지예
학과 : 정보보호학전공
역할 : 취약점 진단 도구 개발

공동 : GUI 개발 및 보고서 작성

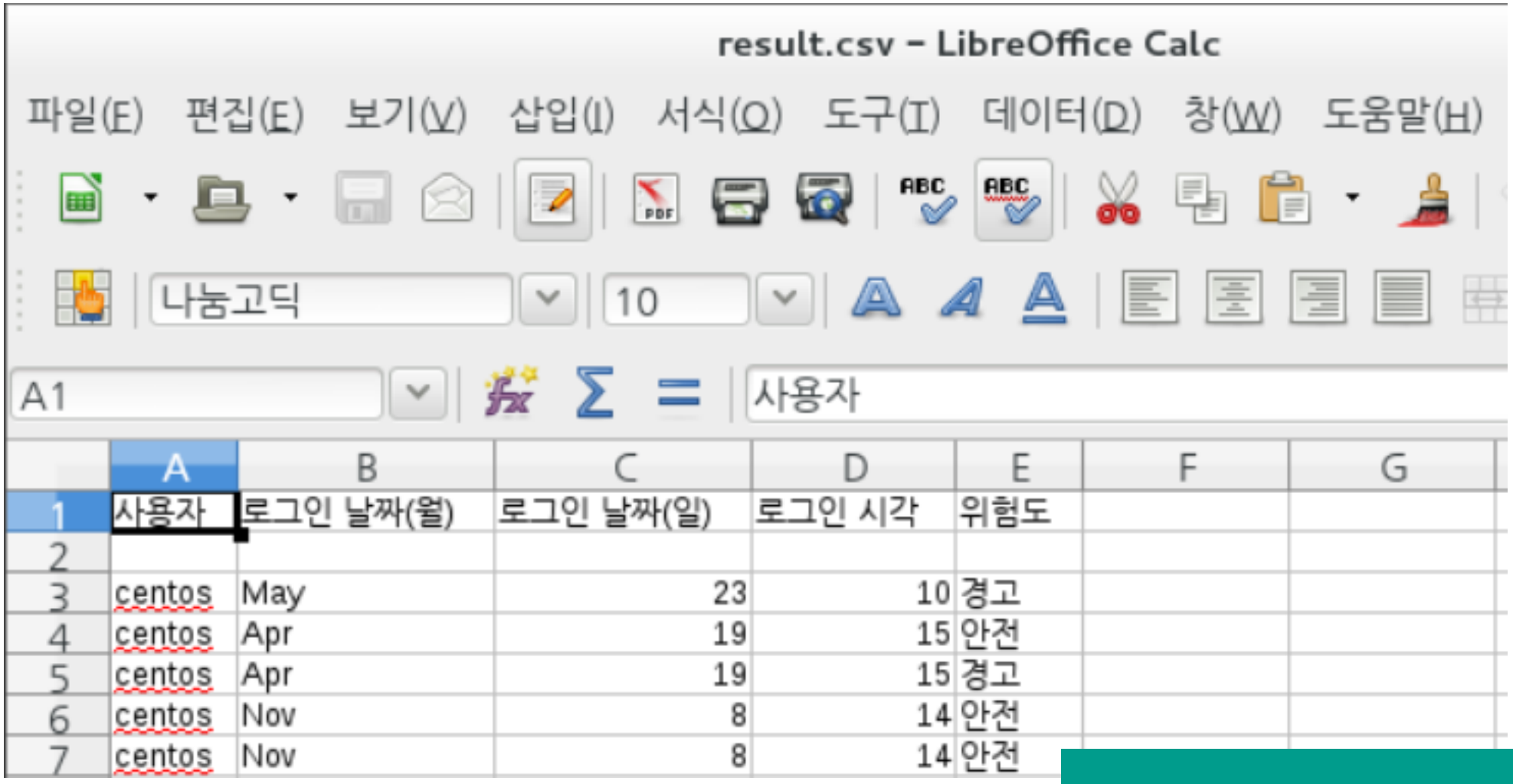
Contents 02 프로젝트 진행 방법 및 개발 내용

A1

	A	B	C
1			
2			
3	U-01 취약 상		
4	U-02 양호 상		
5	U-03 양호 상		
6	U-04 양호 상		
7	U-44 취약 중		
8	U-45 취약 하		
9	U-46 취약 중		
10	U-47 취약 중		
11	U-48 취약 중		
12	U-49 취약 하		
13	U-50 양호 하		
14	U-51 취약 하		
15	U-52 양호 중		
16	U-53 양호 하		
17	U-54 점검 하		
18	U-05 양호 상		
19	U-06 양호 상		
20	U-07 양호 상		
21	U-08 양호 상		
22	U-09 취약 상		
23	U-10 취약 상		
24	U-11 취약 상		
25	U-12 양호 상		
26	U-13 취약 상		
27	U-14 점검 상		
28	U-15 점검 상		
29	U-16 점검 상		
30	U-17 취약 상		
31	U-18 취약 상		

	A
43	U-26 취약 상
44	U-27 점검 상
45	U-28 양호 상
46	U-29 점검 상
47	U-30 점검 상
48	U-31 양호 상
49	U-32 양호 상
50	U-33 취약 상
51	U-34 취약 상
52	U-35 점검 상
53	U-36 점검 상
54	U-37 점검 상
55	U-38 점검 상
56	U-39 점검 상
57	U-40 점검 상
58	U-41 점검 상
59	U-60 양호 중
60	U-61 취약 하
61	U-62 취약 중
62	U-63 점검 하
63	U-64 양호 중
64	U-65 점검 중
65	U-66 취약 중
66	U-67 양호 중
67	U-68 점검 하
68	U-69 점검 중
69	U-70 양호 중
70	U-71 양호 중
71	U-42 취약 상
72	U-43 점검 상
73	U-72 점검 하

1. 결과 excel 파일
(리눅스 취약점 진단 결과)



	A	B	C	D	E	F	G
1	사용자	로그인 날짜(월)	로그인 날짜(일)	로그인 시각	위험도		
2							
3	centos	May	23	10	경고		
4	centos	Apr	19	15	안전		
5	centos	Apr	19	15	경고		
6	centos	Nov	8	14	안전		
7	centos	Nov	8	14	안전		

1. 결과 excel 파일
(로그기반 이상행위 탐지 결과)

Contents 02 프로젝트 진행 방법 및 개발 내용

1	U-01 조치 방법 안내
2	root 계정 원격접속 제한
3	[Telnet 서비스 사용시]
4	1. '/etc/securetty' 파일에서 pts/x 설정 제거 또는, 주석 처리
5	2. '/etc/pam.d/login' 파일 수정 또는, 신규 삽입
6	(수정 전) #auth required /lib/security/pam_securetty.so
7	(수정 후) auth required /lib/security/pam_securetty.so
8	[SSH 서비스 사용시]
9	1. vi편집기를 이용하여 '/etc/ssh/sshd_config' 파일 열기
10	2. 아래와 같이 주석 제거 또는, 신규 삽입
11	(수정 전) #PermitRootLogin Yes
12	(수정 후) PermitRootLogin No
13	
14	U-09 조치 방법 안내
15	/etc/hosts 파일 소유자 및 권한 설정
16	'/etc/hosts' 파일의 소유자 및 권한 변경 (소유자 root, 권한 600)
17	#chown root /etc/hosts
18	#chmod 600 /etc/hosts
19	
20	U-10 조치 방법 안내
21	/etc/(x)inetd.conf 파일 소유자 및 권한 설정
22	'/etc/inetd.conf' 파일의 소유자 및 권한 변경 (소유자 root, 권한 600)
23	#chown root /etc/xinetd.conf
24	#chmod 600 /etc/xinetd.conf
25	
26	U-11 조치 방법 안내
27	/etc/syslog.conf 파일 소유자 및 권한 설정
28	[CentOS 6 이상일 경우]
29	#chown root /etc/rsyslog.conf
30	#chmod 640 /etc/rsyslog.conf
31	
32	U-13 조치 방법 안내
33	SUID, SGID, 설정 파일점검

26	U-11 조치 방법 안내
27	/etc/syslog.conf 파일 소유자 및 권한 설정
28	[CentOS 6 이상일 경우]
29	#chown root /etc/rsyslog.conf
30	#chmod 640 /etc/rsyslog.conf
31	
32	U-13 조치 방법 안내
33	SUID, SGID, 설정 파일점검
34	1. 제거 방법
35	#chmod -s <file_name>
36	2. 주기적인 감사 방법
37	#find / -user root -type f \(-perm -04000 -o -perm -02000 \) -xdev -exec ls -al {} \;
38	3. 반드시 사용이 필요한 경우 특정 그룹에만 사용하도록 제한하는 방법
39	일반 사용자의 Setuid 사용을 제한함 (임의의 그룹만 가능)
40	#/usr/bin/chgrp <group_name> <setuid_file_name>
41	#/usr/bin/chmod 4750 <setuid_file_name>
42	
43	U-14 조치방법 안내
44	1. 소유자를 변경하세요.
45	• #chown <user_name> <file_name>
46	2. 일반 사용자 쓰기 권한을 제거하세요.
47	• #chmod o-w <file_name>
48	
49	U-15 조치방법 안내
50	1. 일반 사용자 쓰기 권한을 제거하세요.
51	• #chmod o-w <file_name>
52	2. 파일을 삭제하세요.
53	• #rm –rf <world-writable 파일명>
54	
55	U-16 조치방법 안내
56	1. /dev 디렉터리 파일을 점검하세요.
57	• #find /dev –type f –exec ls –l {} |;
58	2. major, minor, number을 가지지 않는 device일 경우 삭제하세요.

2. 점검, 위험 항목에 대한
조치 방법 excel 파일

Contents 02 프로젝트 진행 방법 및 개발 내용

MOGLOG v1.0

소개

MogLog v1.0은 Linux 시스템의 취약점을 진단하고 로그 기반 사용자 이상행위를 탐지하는 프로그램입니다.

* 취약점 진단은 2021년 '주요정보통신기반시설 기술적 취약점 분석 평가 방법 상세 가이드'를 기반으로 하였습니다.

- 계정 관리 : 불필요한 계정 제거 외 14개 항목
- 파일 및 디렉터리 관리 : UMASK 설정 관리 외 18개 항목
- 서비스 관리 : ftp 서비스 확인 외 34개 항목
- 패치 관리 : 최신 보안패치 및 벤더 권고사항 적용
- 로그 관리 : 로그의 정기적 검토 및 보고 외 1개 항목

* 이상 행위 탐지는 접속 로그를 추출하여 통계 분석을 통해 평균 이외의 접속 기록을 이상 행위로 판단 후 로그 기록을 하였습니다.

- Step1. Linux 시스템은 사용자의 접속 기록을 월/일/시간 형태로 저장할 수 있으며 이상행위탐지는 이 접속 기록을 사용합니다.
- Step2. 각 접속 기록을 모아 사용자별 평균 접속 시간을 계산하여 비교합니다.
- Step3. 비교 결과에 따라 평균 접속 기록에서 벗어나면 오차범위 1시간 단위로 안전/경고/위험 단계로 분류됩니다.

취약점 진단

Connect — 진단 대상 시스템과의 연결을 합니다.

스크립트 실행 — 시스템 취약점 진단 및 이상행위 탐지를 실행합니다.

결과 확인 — 취약점 진단 결과와 이상행위 탐지에 대한 결과를 Excel로 확인합니다.

Exit — 진단 시스템과 연결을 끊고 프로그램을 종료합니다.

프로그램 종료

프로그램이 성공적으로 종료되었습니다.

OK

JBU 전북대학교

제작자

이름 : 강성현 (팀장)
학과 : 정보보호학전공
역할 : 이상 행위 탐지 도구 개발

이름 : 송소연
학과 : 정보보호학전공
역할 : 이상 행위 탐지 도구 개발

이름 : 정지수
학과 : 정보보호학전공
역할 : 취약점 진단 도구 개발

이름 : 김고운
학과 : 정보보호학전공
역할 : 취약점 진단 도구 개발

이름 : 윤지예
학과 : 정보보호학전공
역할 : 취약점 진단 도구 개발

공통 : GUI 개발 및 보고서 작성

Contents 03 프로젝트 시연

root@localhost:~

File Edit View Search Terminal Help

```
[root@localhost ~]# vi moglog2.py
[root@localhost ~]# python3 ./moglog2.py
/usr/local/lib/python3.6/site-packages/paramiko/transport.py:32: CryptographyDeprecationWarning: Python 3.6 is no longer supported by the Python core team. Therefore, support for it is depr
ecated in cryptography. The next release of cryptography will remove support for Python 3.6.
  from cryptography.hazmat.backends import default_backend
[root@localhost ~]# vi moglog2.py
[root@localhost ~]# python3 ./moglog2.py
/usr/local/lib/python3.6/site-packages/paramiko/transport.py:32: CryptographyDeprecationWarning: Python 3.6 is no longer supported by the Python core team. Therefore, support for it is depr
ecated in cryptography. The next release of cryptography will remove support for Python 3.6.
  from cryptography.hazmat.backends import default_backend
SSH 연결이 성공적으로 수행되었습니다.
스크립트 파일을 성공적으로 받아왔습니다.
moglog/
moglog/account.sh
moglog/file.sh
moglog/service.sh
moglog/log.sh
moglog/error.sh
moglog/result.sh
moglog/moglog.sh
moglog/nds.sh
쉘 스크립트 /root/moglog/moglog/moglog.sh 실행이 성공했습니다.
script.tar 파일 삭제가 완료되었습니다.
/root/moglog 디렉토리 삭제가 성공적으로 완료되었습니다.
```

- 결론

이번 Linux 시스템의 취약점 진단 도구 개발 및 이상 행위 탐지 도구 개발 연구를 통해 Linux 운영체제와 각 진단 항목에 대한 이해도를 높였으며 Linux 시스템의 명령어 및 스크립트 개발에 대한 숙련도가 증가하였고, 계정 관리 및 권한 설정의 중요성을 깊게 탐구하는 계기가 되었다. 또한 취약점 진단을 통한 공격 피해를 예방할 수 있게 되었다.

- 기대 효과

현대 사회에서 보안 문제는 점점 더 중요해지고 있다.
사이버 공격, 데이터 유출, 악성 코드 등으로부터의 보호가 필요한 기업 및 개인이 늘어나고 이에 따라 시스템 취약점 진단과 접속 로그 기반 이상행위 탐지 솔루션은 신속한 보안 대응이 가능할 것으로 보인다.

모 그 로 그

THANK YOU