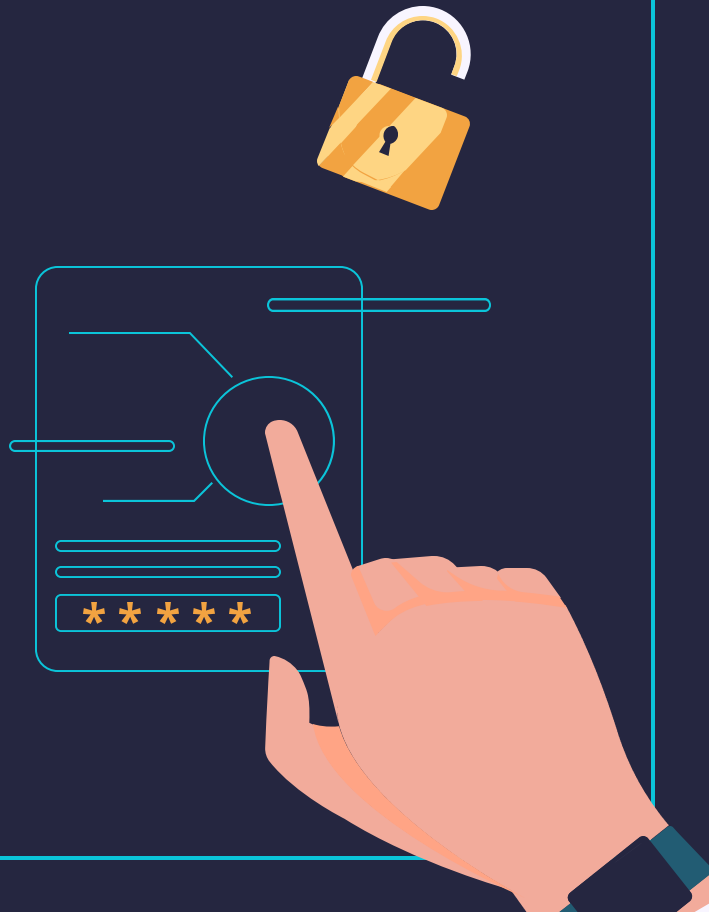
푸드파이터
밥세권

정보 보호 컨설팅 기반 네트워크 웹 보안 사업

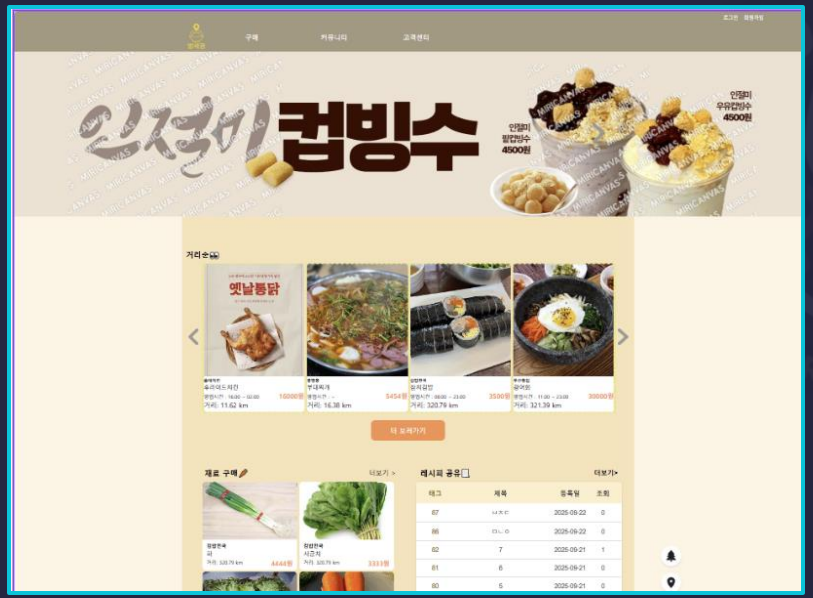


목차

01

프로젝트 배경

고객사 설명 (본사)

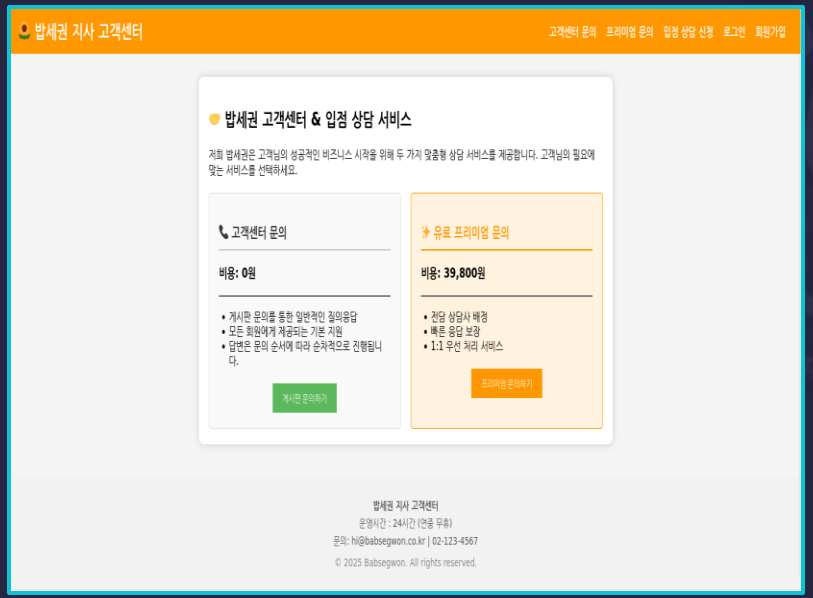


판매자 잉여 재고 판매 저렴한 가격에 구매 가능

재고 최적화로 외식비 절감과 환경 개선 실현

밥세권 www.babsegwon.com

고객사 설명 (지사)



고객 문의 게시판

판매자 입점 신청

지사 고객센터 운영

밥세권

www.babhelp.com

추진 배경


사회

‘가짜 비요르카’ 체포에 대한 보복성 해킹…경찰 34만 명 신상 유출

By Haninpost Indonesia - October 9, 2025

FREE

341K Indonesian National Police Personnel Database

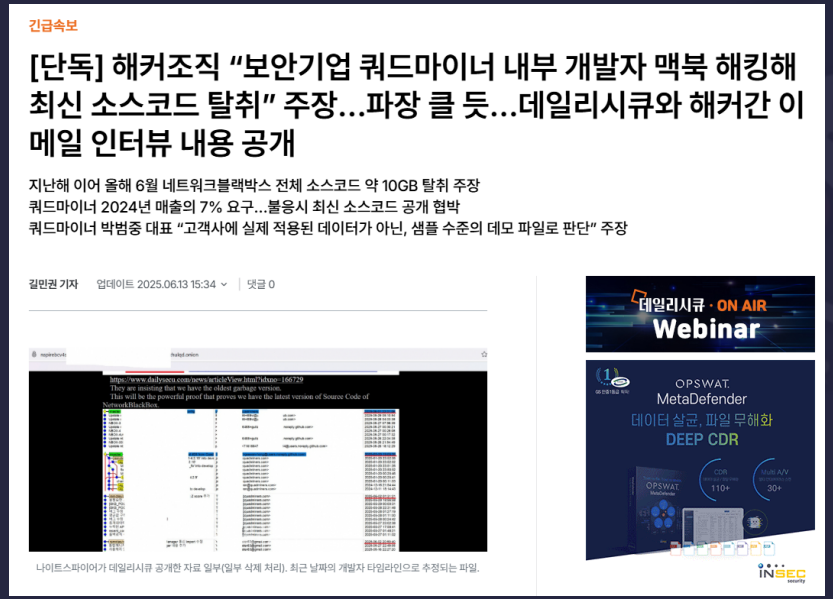
Bjorka • Sat Oct 04 2025 • #Indonesia

KEPOLISIAN NEGARA
REPUBLIK INDONESIA

‘가짜 비요르카’ 체포에 대한
보복성 해킹…경찰 34만 명 신상 유출

비요르카를 사칭한
남성을 체포한 지 하루 만에 발생한 것으로,
사실상 **보복성 공격**

추진 배경


긴급속보

[단독] 해커조직 “보안기업 쿼드마이너 내부 개발자 맥북 해킹해 최신 소스코드 탈취” 주장…파장 클 듯…데일리시큐와 해커간 이메일 인터뷰 내용 공개

지난해 이어 올해 6월 네트워크블랙박스 전체 소스코드 약 10GB 탈취 주장
쿼드마이너 2024년 매출의 7% 요구…불응시 최신 소스코드 공개 협박
쿼드마이너 박범중 대표 “고객사에 실제 적용된 데이터가 아닌, 샘플 수준의 데모 파일로 판단” 주장

김민권 기자 업데이트 2025.06.13 15:34 | 댓글 0

나이트스파이어가 데일리시큐 공개한 자료 일부(일부 삭제 처리). 최근 날짜의 개발자 타임라인으로 추정되는 파일.

“쿼드마이너, 과거 공격 무시…
이번엔 끝까지 간다”

나이트스파이어는 지난 2024년 11월과 2025년 6월, **두 차례에 걸쳐 쿼드마이너를 해킹했다**고 밝혔다.

이에 대해 나이트스파이어는
“이번에는 작년처럼 끝내지 않겠다”
며 **보복성 공격**임을 간접적으로 시사했다.

시나리오 요약

Namhyux Tovalds

고객의 분노 표출

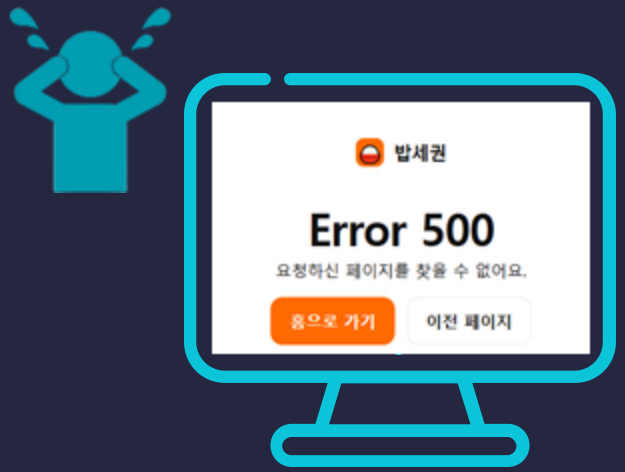
시나리오 요약

모든 네트워크
보안 설정 비활성화

밥세권 보안팀의
미흡한 초기 대응

데이터 베이스 삭제

시나리오 요약



밥세권 서비스 마비

“푸드 파이터” 에게 보안 요청

사업 목표

(C)onfidentiality

- 서비스의 취약점 선별 및 보완
- 주요 기능의 보안 강화

(I)ntegrity

- 데이터 변조 및 위조 차단
- 회원 정보. 결제 정보 등 데이터 암호화 및 접근 통제 강화

(A)VAILABILITY

- 서비스 중단 위험 최소화
- 트래픽 증가에도 서비스 유지

(O)PERATIONS

- 보안 점검 체계 정립
- 보안정책 문서화 및 내재화 완료

사용 툴

사용 도구

GNS 1.5.3

Putty 0.83

VMWare 17.6.2

Packet tracer 8.2.2

Wireshark 4.4.9

문서 도구

Word

PPT

Excel

한글

협업 도구

Notion

Discord

Google Drive

Kakao Talk

NAS

사용 툴

사용 장비

Windows Server 2016
Windows 10

Rocky Linux 8.1

Sophos 9

kail 2024.4-amd64

PHP Server 7.2.24

Apache Tomcat 9.0

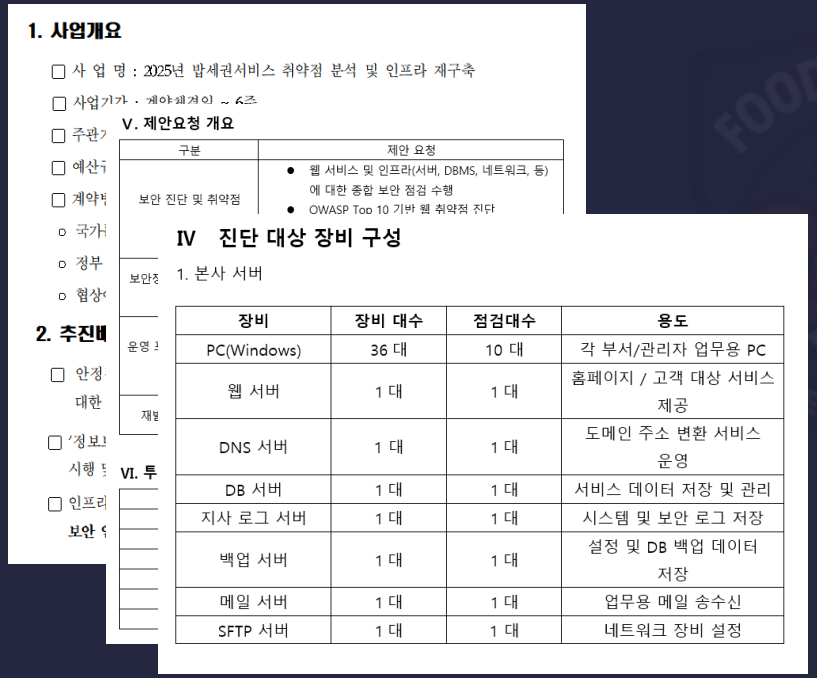
Cisco Router : Cisco 3660 Series 12.4(15)T9
Cisco L3 SW : Cisco 3745 Router 12.4(11)T

CentOS 7

수행 일정

구조	Task	1w	2w	3w	4w	5w	6w
프로젝트 관리	제안서 작성	3일					
	킥 오프 미팅	1일					
	일정 수립	2일					
취약점 분석 및 평가	취약점 점검 대상 식별 및 분류	2일					
	취약점 본 점검(분석/평가)		5일				
	취약점 위험 분석/평가 수행			3일			
보안 정책 수립 및 조치 지원	취약점 개선 방안 도출			2일			
	취약점 조치 지원(보안설정)				7일		
	취약점 이행점검 수행					2일	
모의 해킹	모의해킹					3일	
문서화 및 보고	정보보안 지침 및 규정					3일	
	단기, 중기 보호대책 수립					2일	
	최종 보고						1일

사업 목적



1. 사업개요

□ 사 업 명 : 2025년 밥세권서비스 취약점 분석 및 인프라 재구축

□ 사업기간 : 계약체결일 ~ 6주

□ 주관기

□ 예산규

□ 계약방

○ 국가계

○ 정부

○ 협상에

2. 추진배

□ 안정

대한

□ 정보시

시행 등

□ 인프라

보안 우

V. 제안요청 개요

구분	제안 요청
보안 진단 및 취약점	● 웹 서비스 및 인프라(서버, DBMS, 네트워크, 등)에 대한 종합 보안 점검 수행 ● OWASP Top 10 기반 웹 취약점 진단
보안정	
운영	
재발	

VI. 투

Ⅳ 진단 대상 장비 구성

1. 본사 서버

장비	장비 대수	점검대수	용도
PC(Windows)	36 대	10 대	각 부서/관리자 업무용 PC
웹 서버	1 대	1 대	홈페이지 / 고객 대상 서비스 제공
DNS 서버	1 대	1 대	도메인 주소 변환 서비스 운영
DB 서버	1 대	1 대	서비스 데이터 저장 및 관리
지사 로그 서버	1 대	1 대	시스템 및 보안 로그 저장
백업 서버	1 대	1 대	설정 및 DB 백업 데이터 저장
메일 서버	1 대	1 대	업무용 메일 송수신
SFTP 서버	1 대	1 대	네트워크 장비 설정

- **제안서에 따른 내용**으로 수행
- **자산 식별** 및 분류
- 보안 구성 및 **정책 분석**
- **취약점 점검** 및 **위험도 평가**
- 개선조치 방안 수립
- 보고서 작성 및 전달

02

분석 및 점검

자산 범위

분류	역할	본사	지사	합계
PC(Windows)	부서별 PC	36 대	30 대	66 대
Window Server	DNS, DHCP	2 대	2 대	4 대
Linux Server	SFTP, Mail, Log, DB, Backup, Web	6 대	6 대	12 대
L2 Switch	스위치, VLAN 세팅	4 대	3 대	7 대
L3 Switch	백본, 스위치, 라우팅	4 대	4 대	8 대
L4 Switch	로드 밸런싱	2 대	0 대	2 대
Security Device	UTM, WAF, 방화벽	3 대	2 대	5 대
합 계		58 대	46 대	104 대

점검 범위

WINDOW SERVER 4대 / 4대
WINDOW PC 16대 / 66대

리눅스 서버 12대 / 12대

DBMS 2대 / 2대

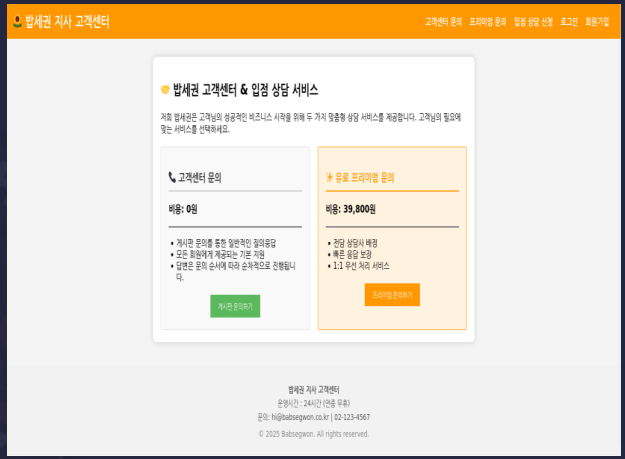
L3 스위치 8대 / 8대

UTM 2대 / 2대

점검 44 대 / 총 104 대

점검 범위

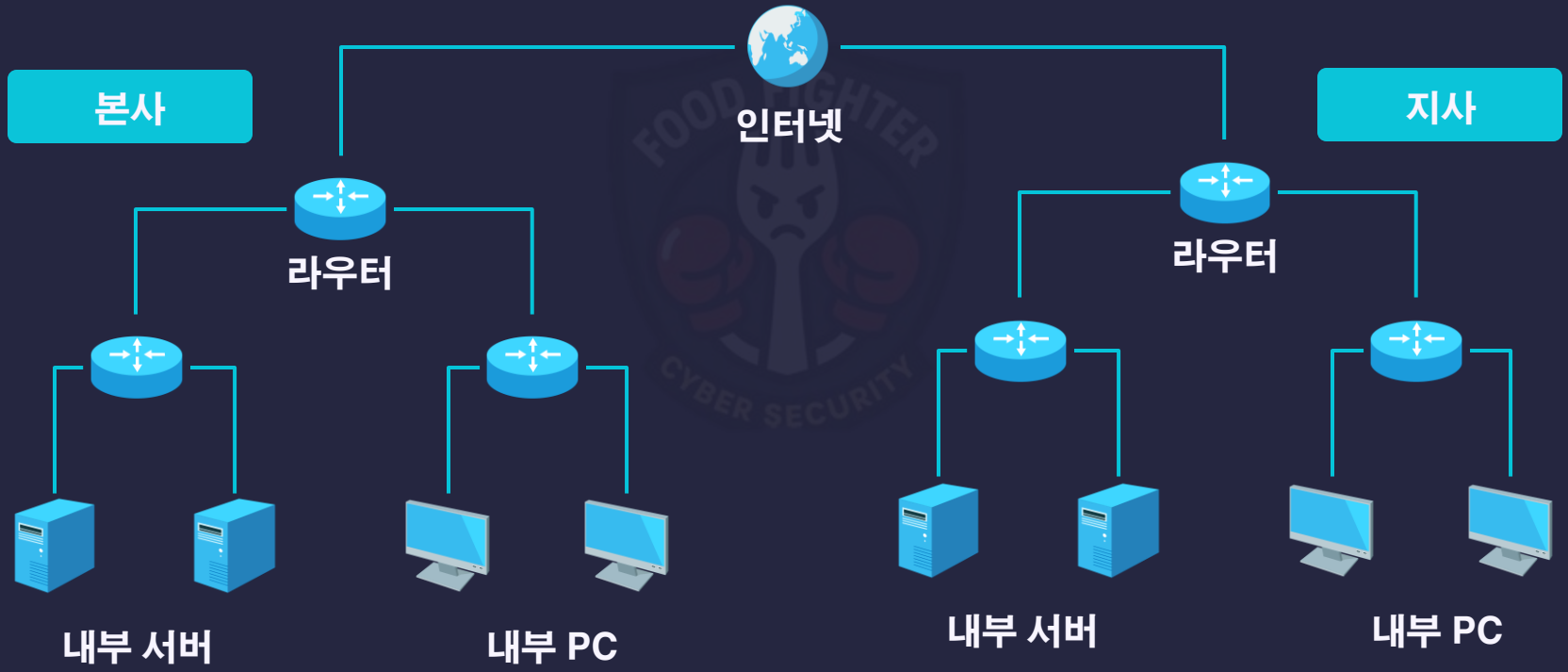
지사 웹 페이지



점검 18 페이지 / 총 18 페이지

인프라 구성

기존 인프라



기존 인프라 문제점

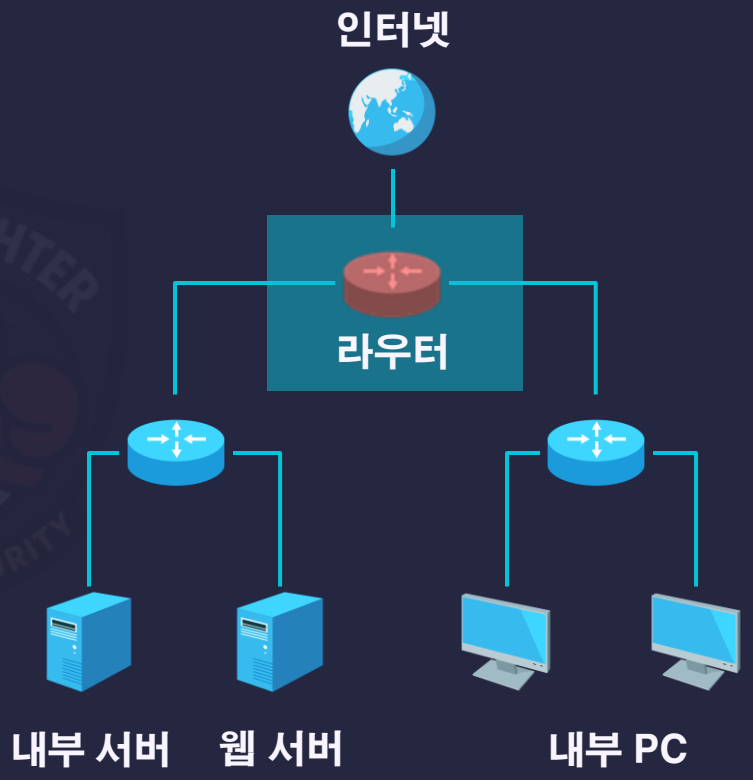
● **장비 이중화 미비**
단일 장비 장애 시 전체 서비스 마비

● **보안 장비 없음**
DDOS, 웹 해킹 등 외부 공격에 취약

● **DMZ 내부망 구분 없음**
내부망 직접 노출 및 침투 용이

● **ACL 권한 체계 미흡**
불필요한 접근 허용 상태 유지

● **백업 서버 없음**
데이터 손실 시 복구 불가



기존 인프라 문제점

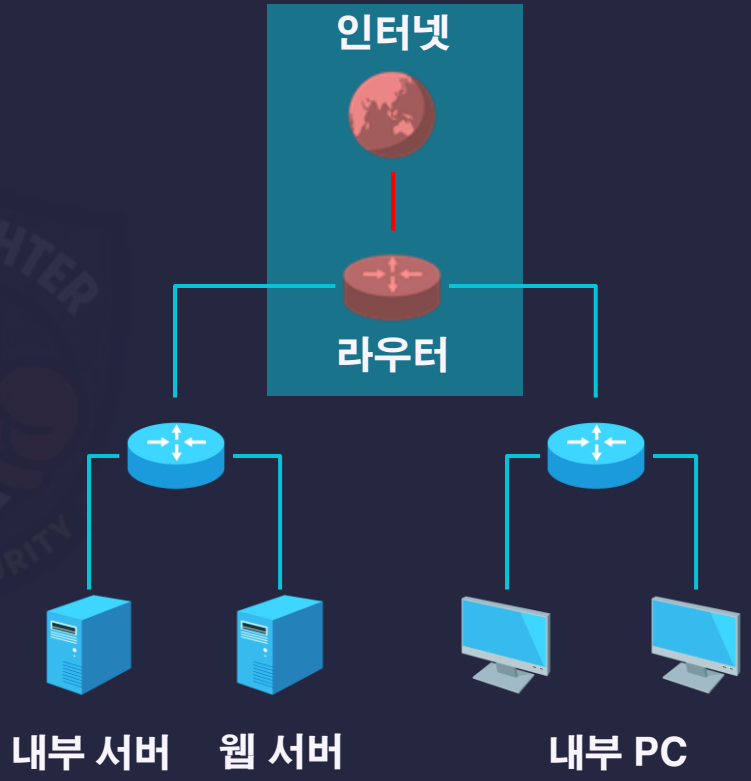
● 장비 이중화 미비
단일 장비 장애 시 전체 서비스 마비

● 보안 장비 없음
DDOS, 웹 해킹 등 외부 공격에 취약

● DMZ 내부망 구분 없음
내부망 직접 노출 및 침투 용이

● ACL 권한 체계 미흡
불필요한 접근 허용 상태 유지

● 백업 서버 없음
데이터 손실 시 복구 불가



기존 인프라 문제점

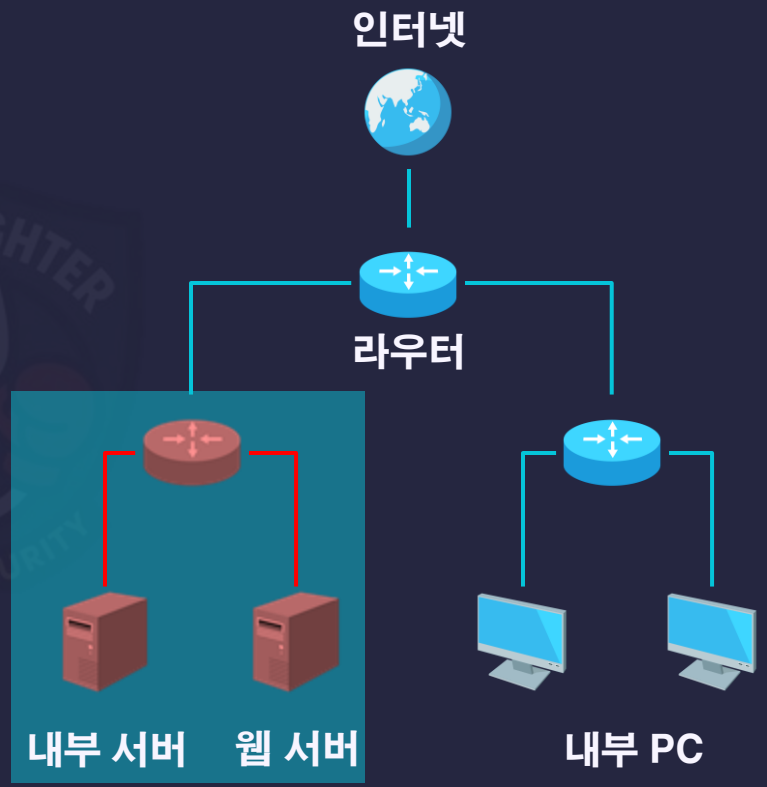
- **장비 이중화 미비**
  단일 장비 장애 시 전체 서비스 마비

- **보안 장비 없음**
  DDOS, 웹 해킹 등 외부 공격에 취약

- **DMZ 내부망 구분 없음**
  내부망 직접 노출 및 침투 용이

- **ACL 권한 체계 미흡**
  불필요한 접근 허용 상태 유지

- **백업 서버 없음**
  데이터 손실 시 복구 불가



기존 인프라 문제점

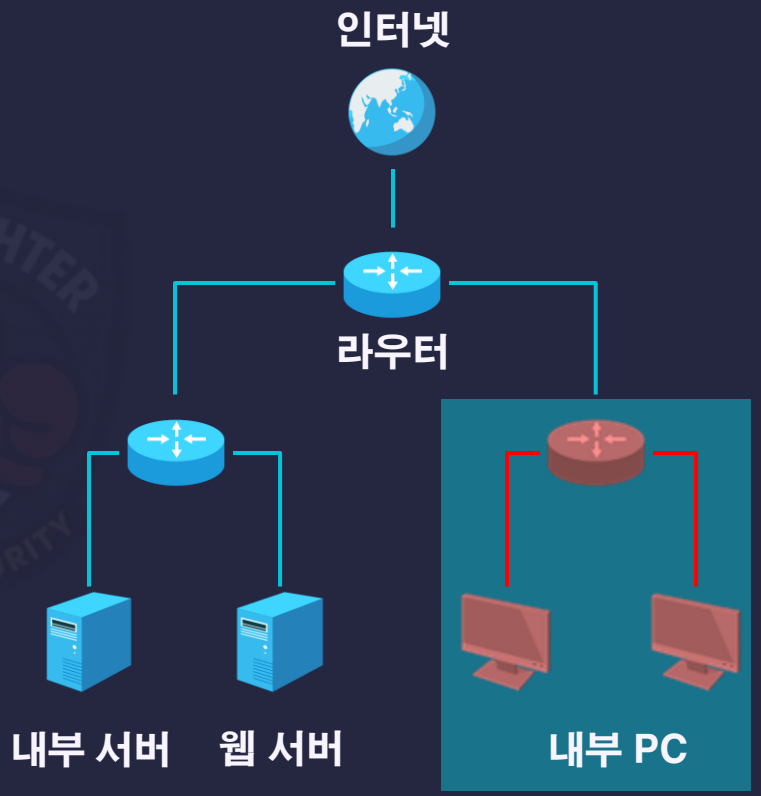
● 장비 이중화 미비
단일 장비 장애 시 전체 서비스 마비

● 보안 장비 없음
DDOS, 웹 해킹 등 외부 공격에 취약

● DMZ 내부망 구분 없음
내부망 직접 노출 및 침투 용이

● ACL 권한 체계 미흡
불필요한 접근 허용 상태 유지

● 백업 서버 없음
데이터 손실 시 복구 불가



기존 인프라 문제점

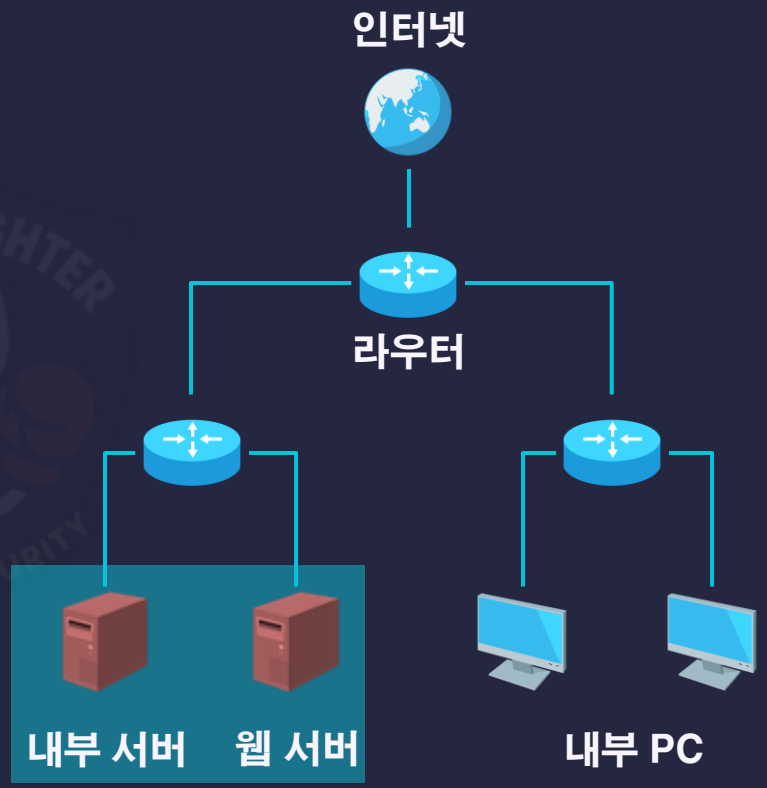
● 장비 이중화 미비
단일 장비 장애 시 전체 서비스 마비

● 보안 장비 없음
DDOS, 웹 해킹 등 외부 공격에 취약

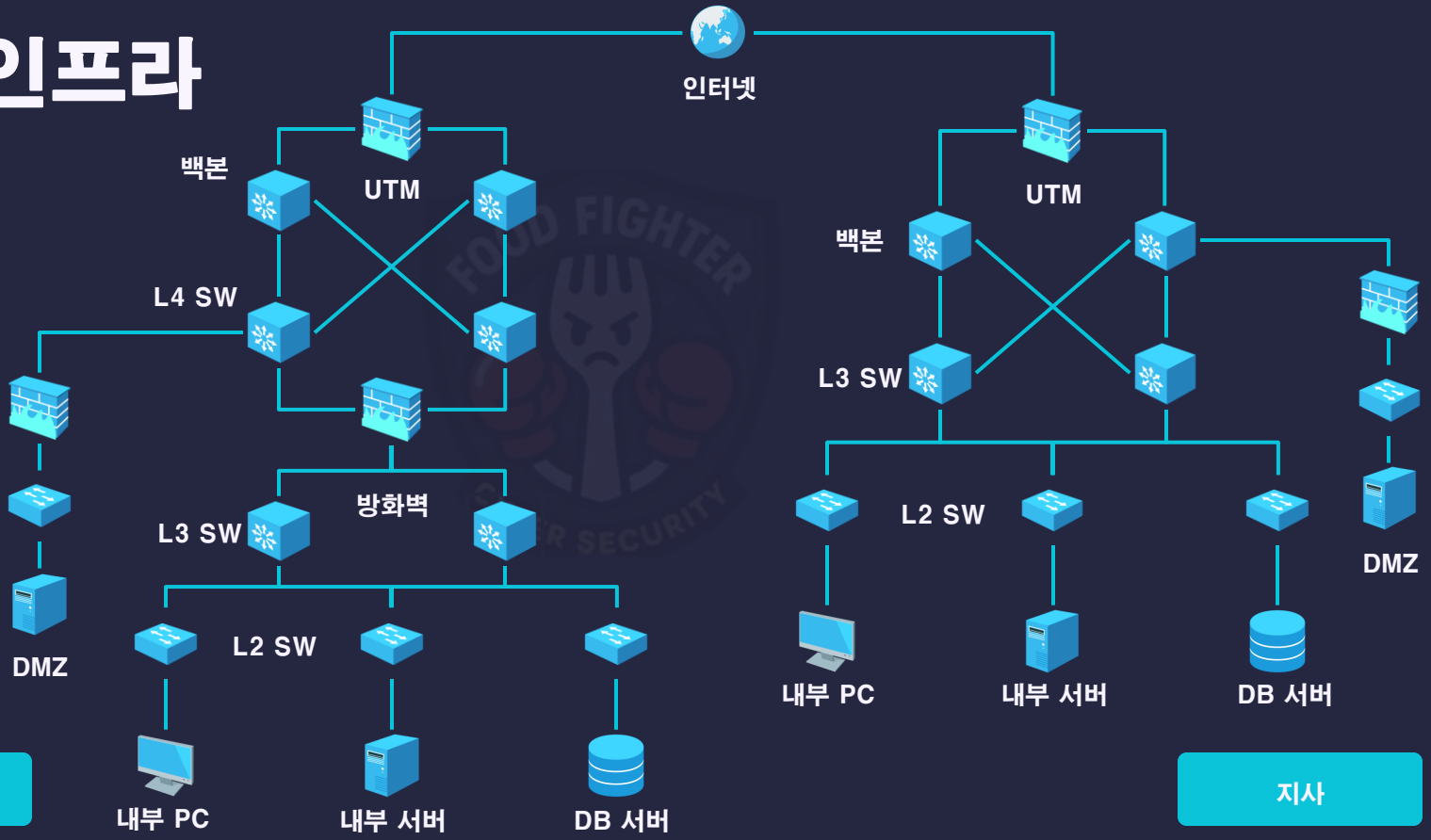
● DMZ 내부망 구분 없음
내부망 직접 노출 및 침투 용이

● ACL 권한 체계 미흡
불필요한 접근 허용 상태 유지

● 백업 서버 없음
데이터 손실 시 복구 불가



개선 인프라


인터넷
백본
UTM
L4 SW
방화벽
L3 SW
L2 SW
DMZ
내부 PC
내부 서버
DB 서버
본사
UTM
백본
L3 SW
L2 SW
DMZ
내부 PC
내부 서버
DB 서버
지사

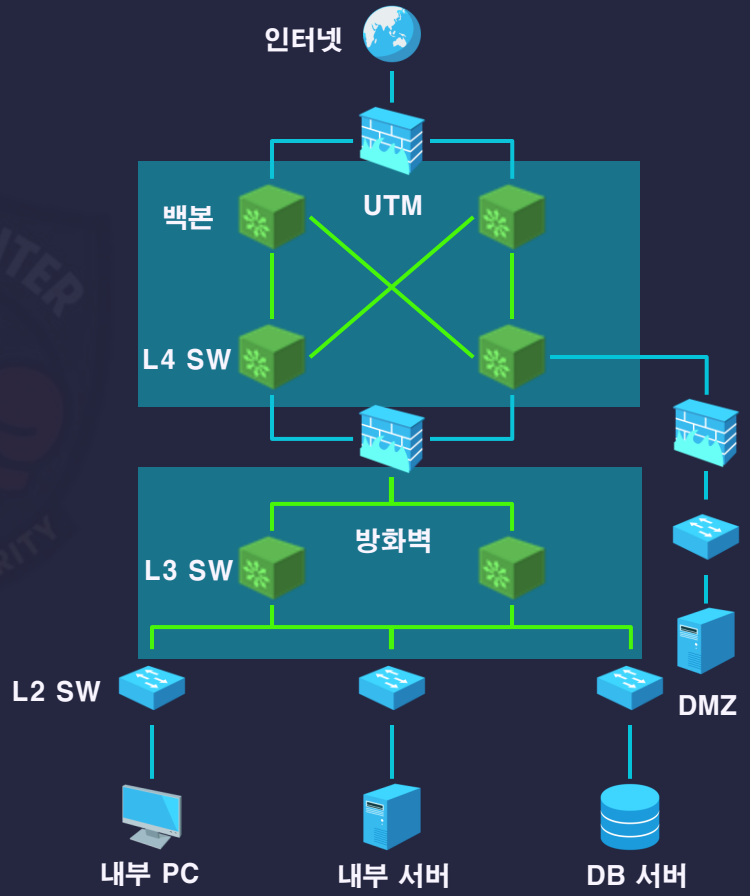
개선된 인프라

● **네트워크 장비 이중화**
장애 시 자동 전환, 무중단 운영 가능

● **UTM 장비 도입**
DDOS 방어, IPS/IDS 기능

● **망 분리**
서비스 망 / 업무망 논리적 분리

● **로그 및 파일 백업 서버 구성**
파일 손실시 대응 체계 마련



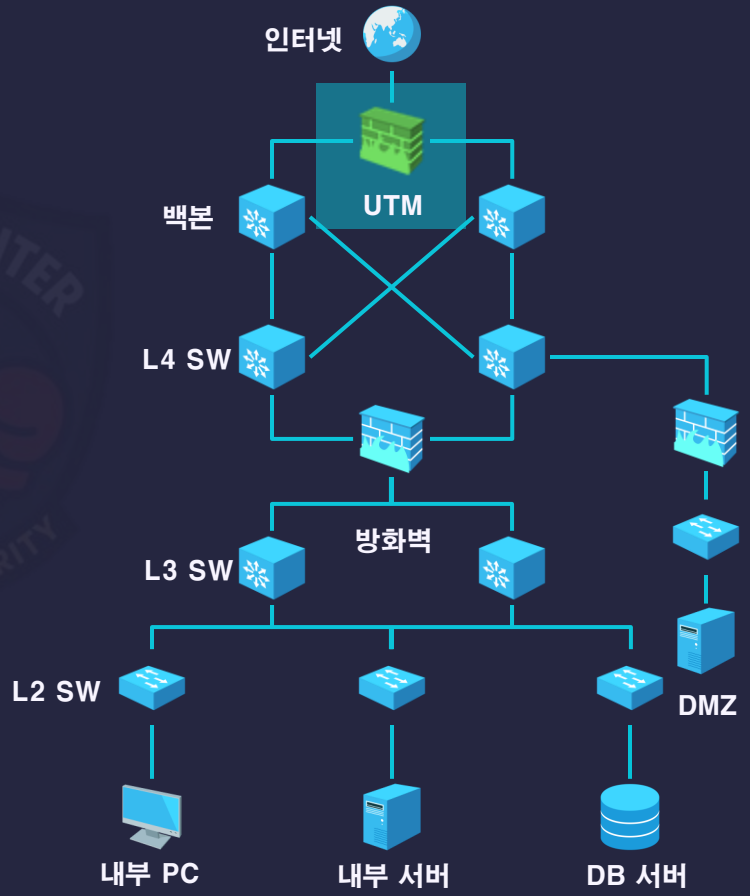
개선된 인프라

● **네트워크 장비 이중화**
장애 시 자동 전환, 무중단 운영 가능

● **UTM 장비 도입**
DDOS 방어, IPS/IDS 기능

● **망 분리**
서비스 망 / 업무망 논리적 분리

● **로그 및 파일 백업 서버 구성**
파일 손실시 대응 체계 마련



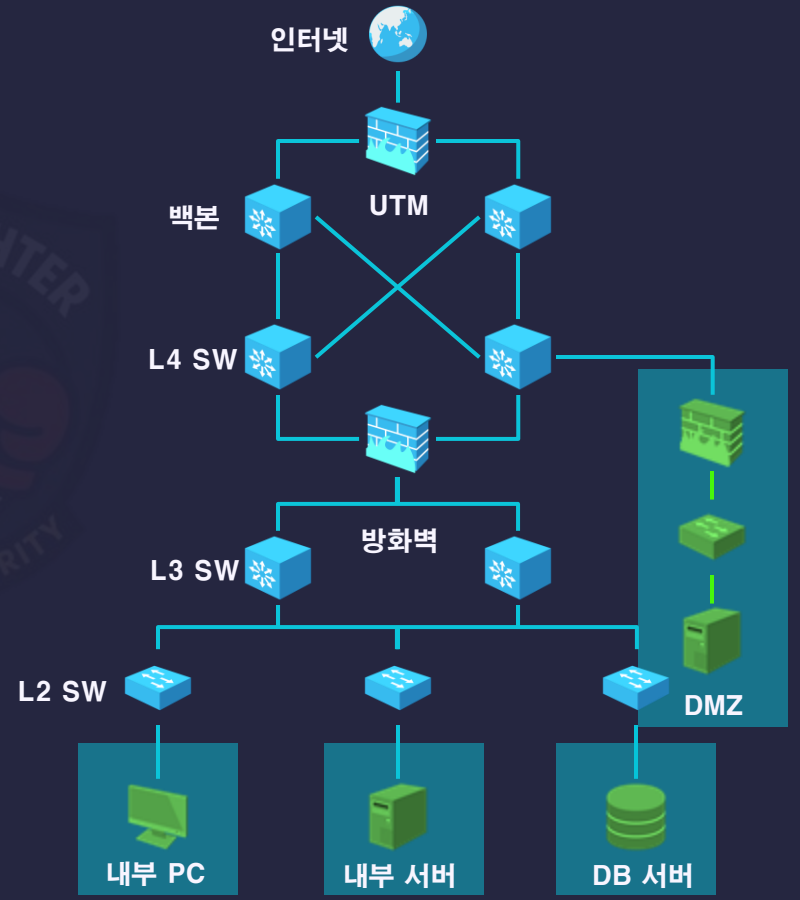
개선된 인프라

● **네트워크 장비 이중화**
장애 시 자동 전환, 무중단 운영 가능

● **UTM 장비 도입**
DDOS 방어, IPS/IDS 기능

● **망 분리**
서비스 망 / 업무망 논리적 분리

● **로그 및 파일 백업 서버 구성**
파일 손실시 대응 체계 마련



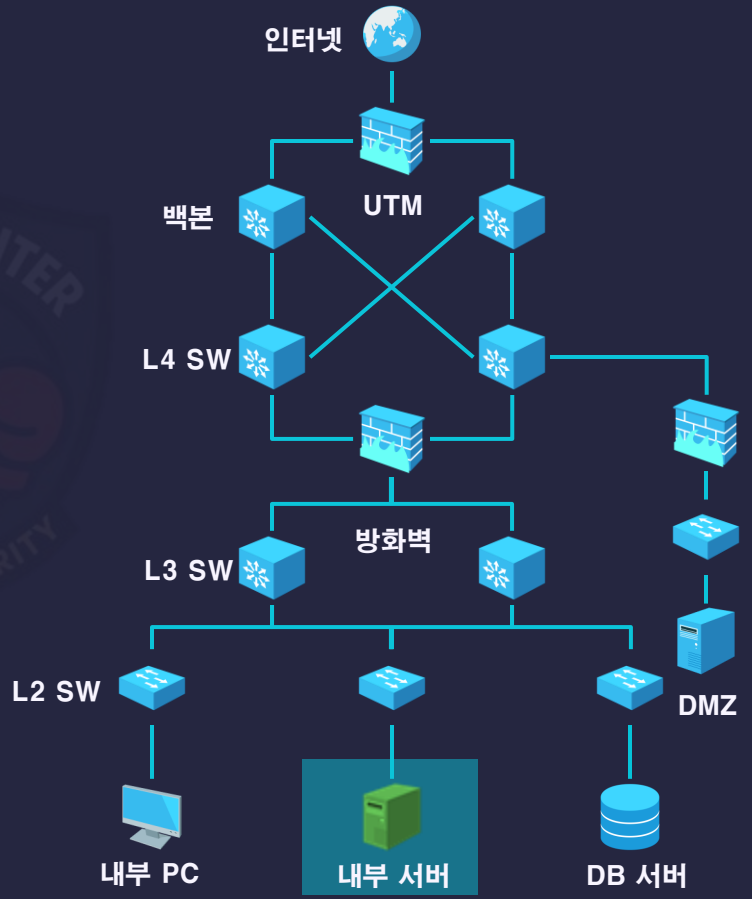
개선된 인프라

● **네트워크 장비 이중화**
장애 시 자동 전환, 무중단 운영 가능

● **UTM 장비 도입**
DDOS 방어, IPS/IDS 기능

● **망 분리**
서비스 망 / 업무망 논리적 분리

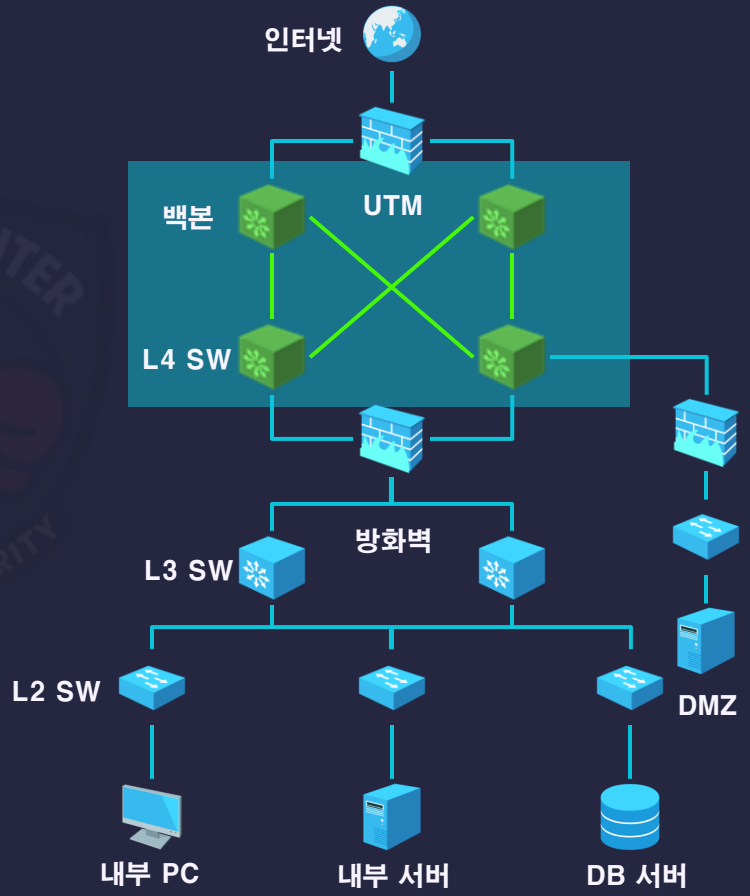
● **로그 및 파일 백업 서버 구성**
파일 손실시 대응 체계 마련



개선된 인프라

● **ACL 및 접근 제어 강화**
민감 자산에 대한 접근 최소화

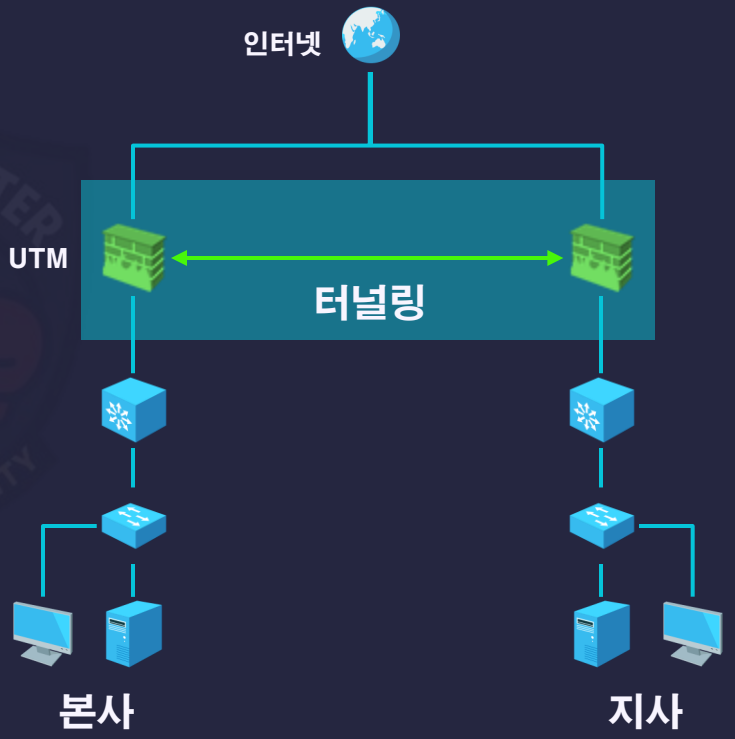
● **GRE+IPsec 구성**
본사 · 지사 간 안전한 통신 보장



개선된 인프라

● ACL 및 접근 제어 강화
민감 자산에 대한 접근 최소화

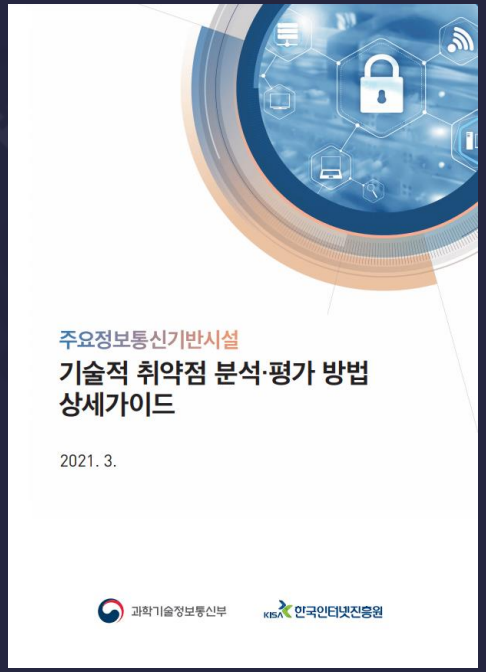
● GRE+IPsec 구성
본사 · 지사 간 안전한 통신 보장



취약점 리스트

평가 기준

주요 정보 통신 기반 시설 과
전자 금융 기반 시설 취약점
평가 방법 기준으로 취약점 파악
및 **점검 실행**



UNIX

주통 기반	금융 기반	위험도	점검 항목
U-02	SRV-075	상	패스워드 복잡성 설정
U-03	SRV-127	상	계정 잠금 임계값 설정
U-04	SRV-012	상	패스워드 파일 보호
U-05	SRV-121	상	root 홈, 패스 디렉터리 권한 및 패스 설정
U-06	SRV-096	상	파일 및 디렉터리 소유자 설정
U-07	SRV-096	상	/etc/passwd 파일 소유자 및 권한 설정
U-13	SRV-091	상	SUID, SGID, Sticky bit 설정 파일 점검
U-14	SRV-095	상	사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정
U-37	SRV-042	상	웹 서비스 상위 디렉토리 접근 금지
U-46	SRV-069	중	패스워드 최소 길이 설정

WINDOWS

주통 기반	금융 기반	위험도	점검 항목
W-01	SRV-072	상	Administrator 계정 이름 변경 또는 보안성 강화
W-02	SRV-078	상	Guest 계정 비활성화
W-06	SRV-073	상	관리자 그룹에 최소한의 사용자 포함
W-07	SRV-020	상	공유 권한 및 사용자 그룹 설정
W-08	SRV-018	상	하드디스크 기본 공유 제거
W-29	SRV-066	상	DNS Zone Transfer 설정
W-30	SRV-034	상	RDS(Remonte Data Services) 제거
W-34	SRV-115	상	로그의 정기적 검토 및 보고
W-63	SRV-173	중	DNS 서비스 구동 점검
W-71	SRV-062	중	원격에서 이벤트 로그파일 접근 차단

DBMS

주통 기반	금융 기반	위험도	점검 항목
D-01	DBMS-001	상	기본 계정의 패스워드, 권한 등을 변경하여 사용
D-02	DBMS-003	상	데이터베이스의 불필요 계정을 제거하거나, 잠금설정 후 사용
D-03	DBMS-007	상	패스워드의 사용기간 및 복잡도를 기관 정책에 맞도록 설정
D-04	DBMS-004	상	데이터베이스 관리자 권한을 꼭 필요한 계정 및 그룹에 허용
D-05	DBMS-013	상	원격에서 DB 서버로의 접속 제한
D-06	DBMS-004	상	DBA 이외의 인가되지 않은 사용자 시스템 테이블에 접근할 수 없도록 설정
D-10	DBMS-016	상	데이터베이스에 대해 최신 보안패치와 밴더 권고사항을 모두 적용
D-13	DBMS-020	중	DB 사용자 계정을 개별적으로 부여하여 사용
D-17	DBMS-022	중	데이터베이스의 주요 설정 파일, 패스워드 파일 등과 같은 파일들의 접근 권한 설정
D-21	DBMS-024	중	인가되지 않은 GRANT OPTION 사용 제한

보안 장비

주통 기반	금융 기반	위험도	점검 항목
S-01	ISS-017	상	보안장비 Default 계정 변경
S-02	ISS-018	상	보안장비 Default 패스워드 변경
S-03	ISS-020	상	보안장비 계정별 권한 설정
S-04	ISS-019	상	보안장비 계정 관리
S-05	ISS-021	상	보안장비 원격 관리 접근 통제
S-06	ISS-016	상	보안장비 보안 접속
S-07	ISS-024	상	Session timeout 설정
S-08	ISS-005	상	벤더에서 제공하는 최신 업데이트 적용
S-09	ISS-001	상	정책 관리
S-10	ISS-004	상	NAT 설정

네트워크 장비

주통 기반	금융 기반	위험도	점검 항목
N-01	NET-56	상	패스워드 설정
N-02	NET-12	상	패스워드 복잡도 설정
N-03	NET-11	상	암호화된 패스워드 사용
N-14	NET-52	상	사용하지 않는 인터페이스의 Shutdown 설정
N-05	NET-14	상	Session Timeout 설정
N-06	NET-48	상	최신 보안 패치 및 벤더 권고사항 적용
N-12	NET-40	상	Spoofing 방지 필터링 적용 또는 보안장비 사용
N-13	NET-47	상	DDoS 공격 방어 설정 또는 DDoS 장비 사용
N-29	NET-30	중	CDP 서비스 차단
N-32	NET-26	중	Proxy ARP 차단

웹

주통 기반	금융 기반	위험도	점검 항목
FU	SER-002	상	악성파일 업로드
FD	SER-010	상	파일 다운로드
AE	SER-039	상	관리자 페이지 노출 여부
IN	SER-003	상	부적절한 이용자 인가 여부
SC	SER-033	상	불충분한 세션종료 처리
XS	SER-041	상	크로스사이트 스크립팅 (XSS)
CF	SER-028	상	크로스사이트 요청변조 (CSRF)
DI	SER-029	상	디렉토리 목록 노출
IL	SER-020	상	화면 내 중요정보 평문노출 여부
SI	SER-001	상	SQL Injection

03

수행 결과

팀원 소개

김기수 / PM

전체 총괄,
네트워크 구축, 보안 장비,
PHP 웹서버 구축, 모의해킹

최장현 / PL

지사 리눅스 서버 구축,
MariaDB 구축, 모의해킹

이남혁 / 수행원

본사 리눅스 서버 구축,
PHP 웹서버 구축,
MariaDB 구축, 모의해킹

팀원 소개

강버들 / 수행원

본사 네트워크 구축,
보안장비, 모의해킹

이태호 / 수행원

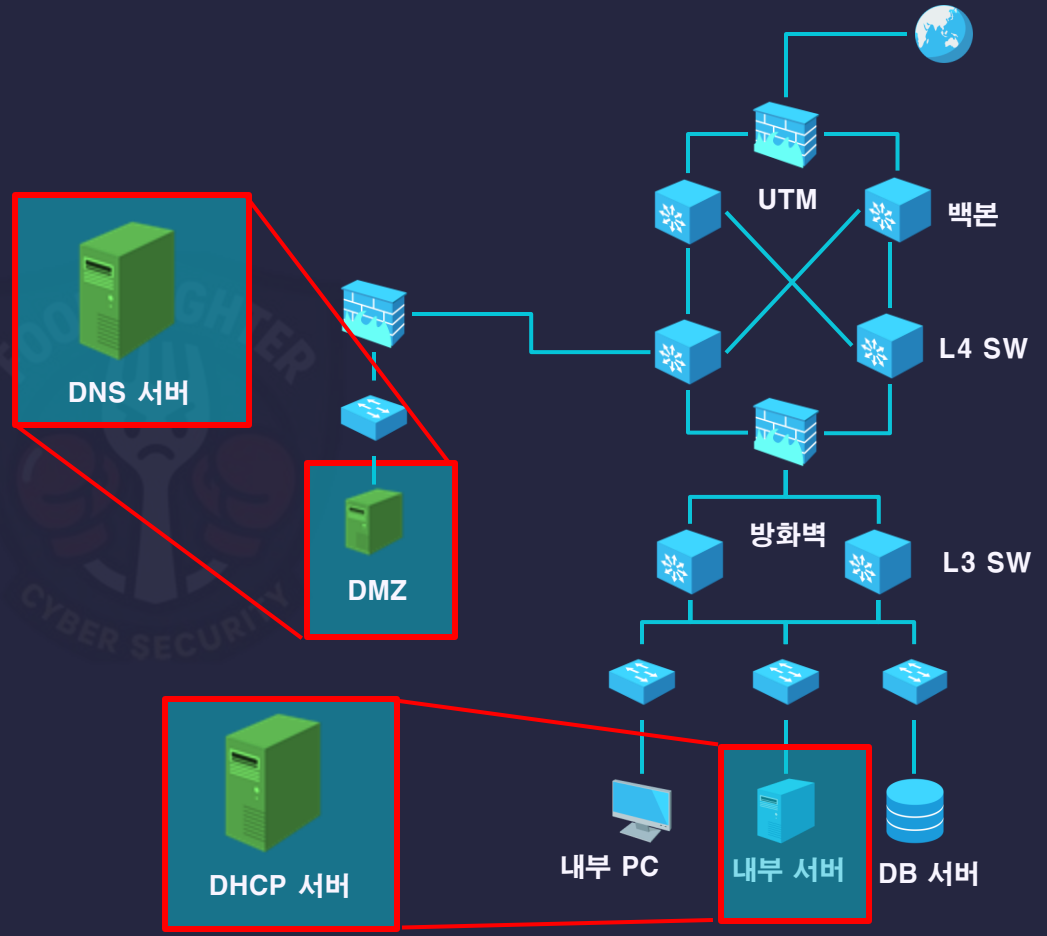
지사 네트워크 구축,
PHP웹서버 구축,
보안 장비, 모의해킹

이서진 / 수행원

윈도우 서버 구축,
모의해킹

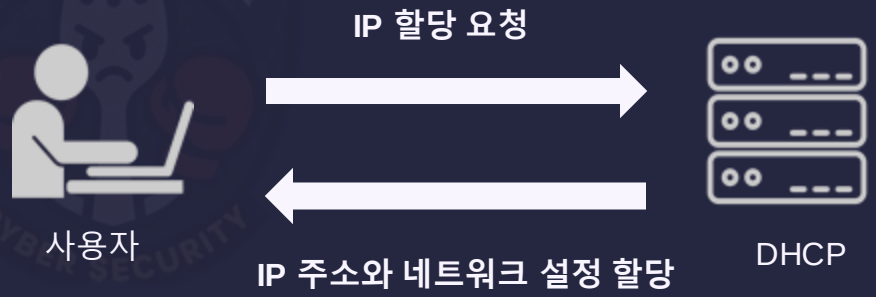
이서진

- 본사, 지사 윈도우 서버
- DNS, DHCP 서버
  구축 및 보안 설정
- 윈도우 와 Rocky SSH 연결
- 모의해킹 보고서
- 모의해킹 (파일 업로드)



DHCP 란?

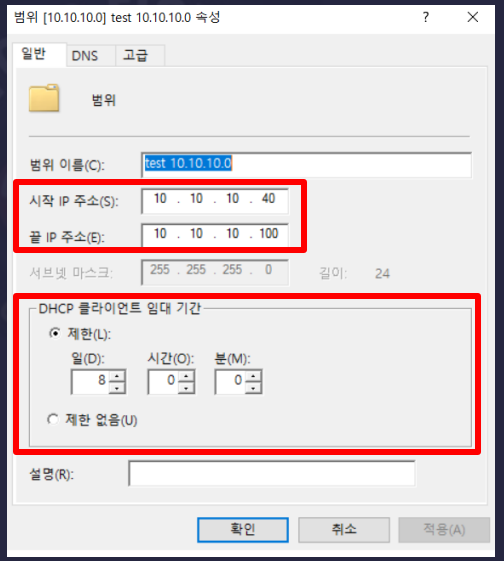
- DHCP란 네트워크에 접속한 **단말에 IP 주소와 네트워크 설정을 자동으로 할당**하는 서비스
- IP 주소, 서브넷 마스크, 게이트웨이, DNS 정보 자동 제공
- 네트워크 접속의 출발점 역할 수행



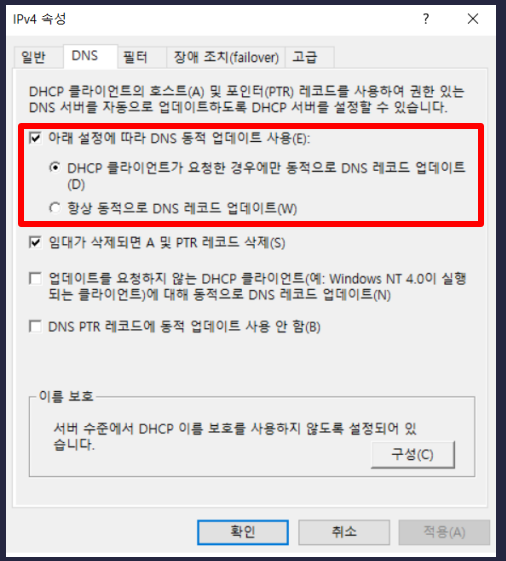
윈도우 DHCP 구축

- 내부망 전용 DHCP Scope 구성
- IP 풀 범위 및 임대 시간 설정
- DNS 동적 업데이트 설정
- DHCP 감사 로그 설정

주소 범위 & 임대기간



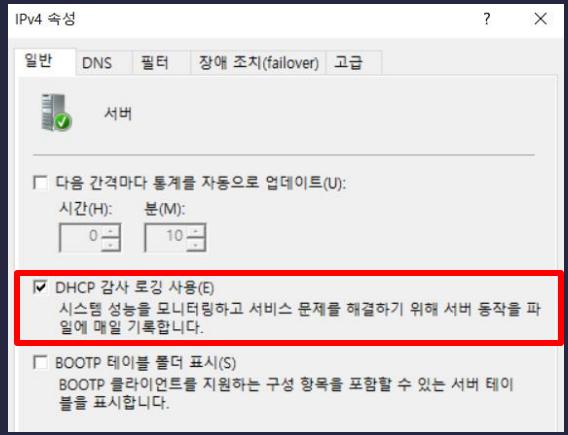
동적 업데이트 설정



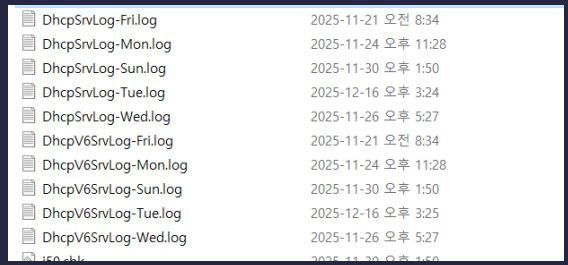
윈도우 DHCP 구축

- 내부망 전용 DHCP Scope 구성
- IP 풀 범위 및 임대 시간 설정
- DNS 동적 업데이트 설정
- **DHCP 감사 로그 설정**

DHCP 감사 로그 설정



DHCP 감사 로그
C:\Windows\System32\dhcp



윈도우 DHCP 보안 설정

- 윈도우 DHCP 보안 설정은 **주요 정보 통신 기반 시설의 윈도우 취약점 보안 기준**에 맞춰 진행

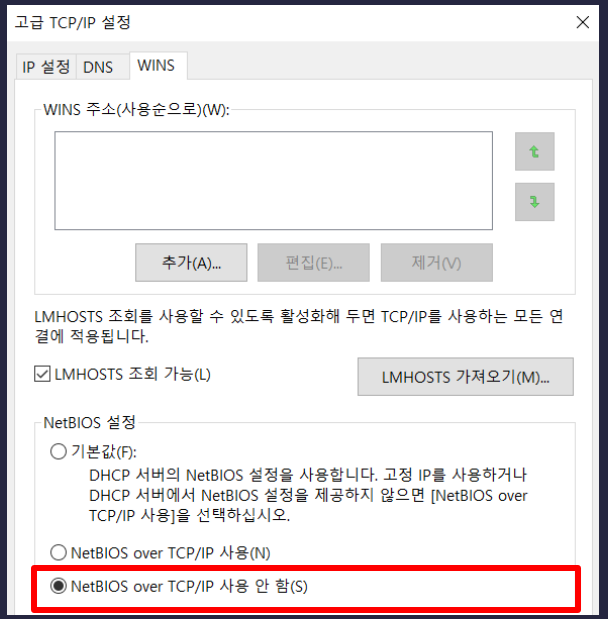
분류	점검 항목	위험도	항목코드
서비스 관리	NetBIOS 바인딩 서비스 구동 점검	상	W-24
패치 관리	정책에 따른 시스템 로깅 설정	중	W-69
보안 관리	DoS 공격 방어 레지스트리 설정	중	W-72

윈도우 DHCP 보안 설정

- NetBIOS : 파일 · 프린터 공유를 제공하는 Windows 네트워크 통신 방식
- DHCP로 IP를 할당받은 단말이 NetBIOS를 통해 **내부 공유 자원에 접근 위험 존재**
- 비인가 단말의 내부 자원 접근 경로가 될 위험 존재
- 불필요한 NetBIOS 통신을 차단하여 **내부 정보 노출을 방지**

Windows	서비스 관리	NetBIOS 바인딩 서비스 구동 점검	상	W-24

주요 인터넷의 NetBIOS 설정

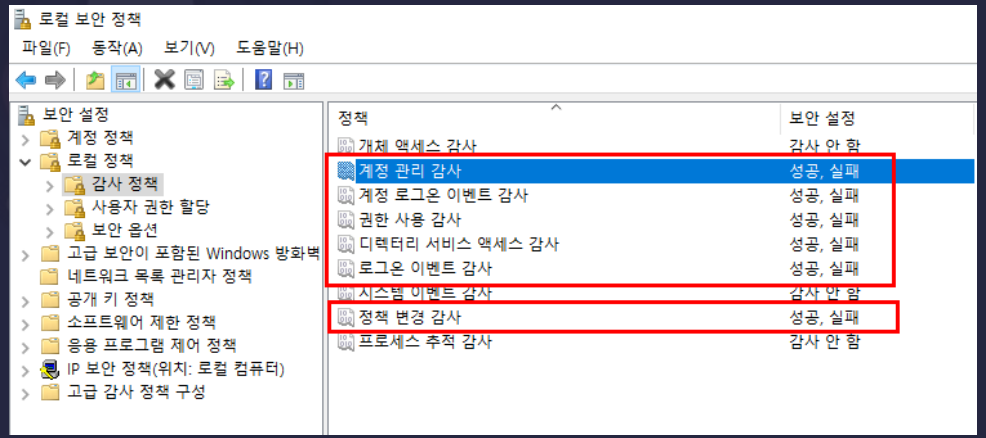


윈도우 DHCP 보안 설정

- 시스템 로깅 : 보안 사고 발생 시 **원인 분석과 책임 추적을 위한 핵심 기록**
- **보안 사고 발생 시 증거 확보 가능**
- 필수 감사 항목만 선별적으로 기록 보안 사고 분석 및 책임 추적 가능

Windows	패치 관리	정책에 따른 시스템 로깅 설정	중	W-69

정방향 babhelp.com



윈도우 DHCP 보안 설정

- DHCP는 **네트워크 접속의 출발점**으로, DoS 공격 시 IP 할당 및 서비스 제공이 중단 위험 존재
- TCP/IP 스택이 약할 경우 DHCP 서비스 가용성이 직접적으로 영향을 받음
- **DoS 공격 방어 레지스트리 설정**
- DoS공격에 대한 시스템 안정성 확보 DHCP 서비스 가용성 유지

Windows	보안 관리	DoS 공격 방어 레지스트리 설정	중	W-72

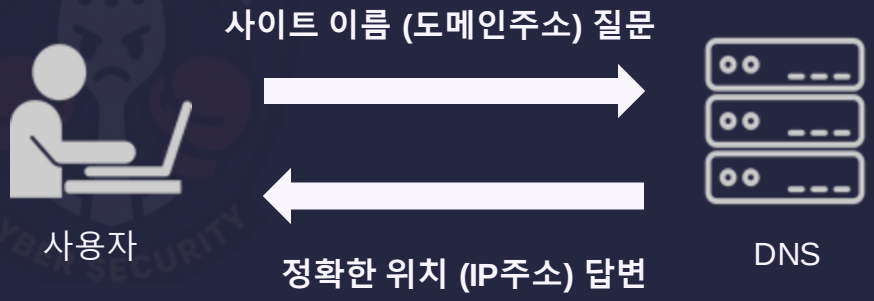
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\

도움말(H)

이름	종류	데이터
(기본값)	REG_SZ	(값 설정 안 됨)
DataBasePath	REG_EXPAND_SZ	%SystemRoot%₩System32₩drivers₩etc
DeadGWDetectDefault	REG_DWORD	0x00000001 (1)
Domain	REG_SZ	
DontAddDefaultGatewayDefault	REG_DWORD	0x00000000 (0)
EnableDeadGWDetect	REG_DWORD	0x00000000 (0)
EnableICMPRedirect	REG_DWORD	0x00000001 (1)
ForwardBroadcasts	REG_DWORD	0x00000000 (0)
Hostname	REG_SZ	BR_DNS_sec
ICSDomain	REG_SZ	mshome.net
IPEnableRouter	REG_DWORD	0x00000000 (0)
KeepAliveTime	REG_DWORD	0x000493e0 (300000)
NameServer	REG_SZ	
NV Hostname	REG_SZ	BR_DNS_sec
SearchList	REG_SZ	
SynAttackProtect	REG_DWORD	0x00000001 (1)
SyncDomainWithMembership	REG_DWORD	0x00000001 (1)
UseDomainNameDevolution	REG_DWORD	0x00000001 (1)

DNS 란?

- DNS란 **도메인 이름을 IP 주소로 바꿔주는** 인터넷의 주소 변환 시스템
- **사이트 이름 (도메인 주소)로 서비스 접근 가능**
- **www.babhelp.com**



윈도우 DNS 구축

- Zone(영역): DNS가 책임지고 관리하는 도메인 또는 IP 주소 범위의 데이터 저장 영역
- 정방향 영역으로 babhelp.com 생성
- A레코드 www. - 20.0.0.81
- 역방향 영역으로 20.0.0.x 생성

정방향 babhelp.com

이름	종류	데이터
(상위 폴더와 같음)	SOA(권한 시작)	[9], br_dns_sec., hostmast...
(상위 폴더와 같음)	NS(이름 서버)	br_dns_sec.
db	호스트(A)	20.0.0.65
root	호스트(A)	20.0.0.81
root	MX(메일 교환기)	[10] www.babhelp.com.
www	호스트(A)	20.0.0.81

역방향 20.0.0.x

이름	종류	데이터
(상위 폴더와 같음)	SOA(권한 시작)	[2], br_dns_sec., hostmast...
(상위 폴더와 같음)	NS(이름 서버)	br_dns_sec.
20.0.0.81	PTR(포인터)	babhelp.com.

윈도우 DNS 보안 설정

- 윈도우 DNS 보안 설정은 **주요 정보 통신 기반 시설의 윈도우 취약점 보안 기준**에 맞춰 진행

분류	점검 항목	위험도	항목코드
서비스 관리	DNS Zone Transfer 설정	상	W-29
서비스 관리	DNS 서비스 구동 점검	중	W-63
로그 관리	로그의 정기적 검토 및 보고	상	W-34

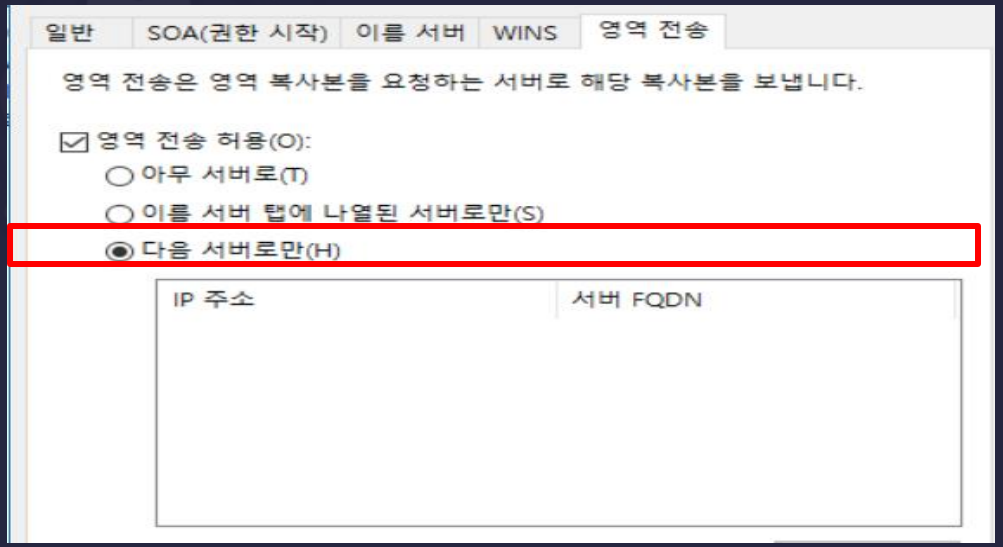
윈도우 DNS 보안 설정

- 영역 전송 : 도메인 구조를 다른 서버에 전달하는 기능
- 지정된 서버만 영역 전송 허용
- 데이터 불법 외부 유출 방지 DNS Recon 공격 차단

※ DNS Recon : DNS를 조사해 서버 구조, 서브도메인, 레코드 정보를 대량 수집하여 이후 공격을 준비하는 정보 수집 정찰 과정

Windows	서비스 관리	DNS Zone Transfer 설정	상	W-29

정방향 babhelp.com



윈도우 DNS 보안 설정

- **동적 업데이트 제거**
- **신뢰할 수 없는 데이터 업데이트 방지**
- **DNS 스푸핑 · 하이재킹 방지**

※ DNS 스푸핑 : DNS 서버로 보내는 질문을 가로채서 변조된 결과를 보내주는 것

※ DNS 하이젝킹 : DNS 설정을 공격자가 빼앗아서 사용자가 입력한 도메인을 원래랑 다른 IP로 계속 돌려버리는 공격

Windows	서비스 관리	DNS 서비스 구동 점검	중	W-63

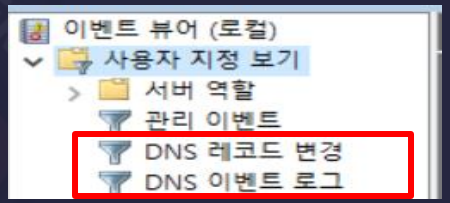
정방향 babhelp.com

윈도우 DNS 보안 설정

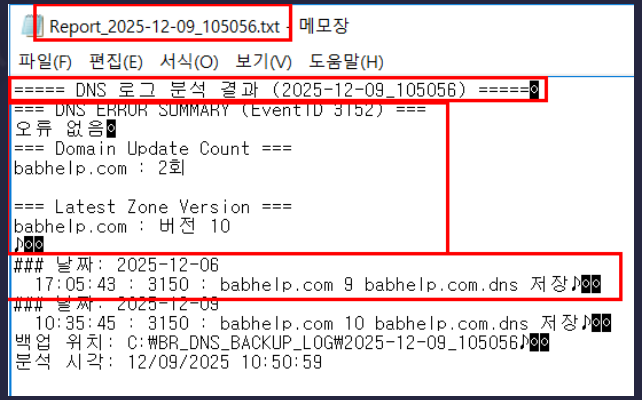
- 공격 식별과 추가조치 필요
- DNS **로그 사용자 지정 보기** 구성
- **매주 로그 분석 보고서** 작성
- 문제 발생 시 **즉시 원인을 추적**할 수 있는 구조로 개선
- 안정적인 시스템 상태 유지

Windows	로그관리	로그의 정기적 검토 및 보고	상	W-34

사용자 지정보기



로그 분석 보고서

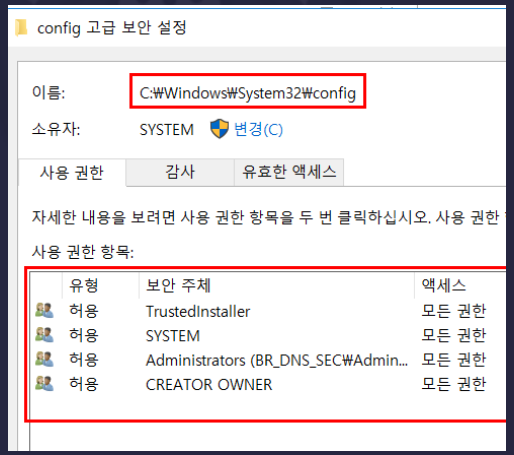


윈도우 DNS 보안 설정

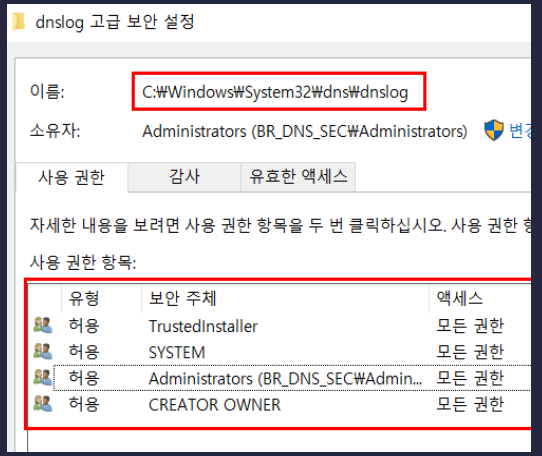
- 로그는 **보안 사고 원인 파악의 핵심** 파일
- **최소 권한 원칙 적용**으로 내부 위협 감소
- 시스템 로그 파일과 DNS로그 **파일의 원격에서 접근 차단**
- DNS 서비스 안전성 강화

Windows	로그관리	원격에서 이벤트 로그파일 접근 차단	중	W-71

시스템 로그



dns 로그



DNSSEC 대체 추가 보안 설정

- 강한 캐시 설정
- TTL 과다 설정 시 캐시 포이즈닝 발생 시 영향 시간 증가 위험 존재
- 보안성과 가용성을 동시에 고려한 Negative TTL 5분 적용
- 문제 발생 시 영향 범위를 시간적으로 최소화

TTL 설정값

```
PS C:¥Users¥Administrator> Restart-Service DNS
PS C:¥Users¥Administrator> Get-DnsServerCache


MaxTTL                          : 1.00:00:00
MaxNegativeTTL                  : 00:05:00
MaxKBSize                       : 0
EnablePollutionProtection       : True
LockingPercent                  : 100
StoreEmptyAuthenticationResponse : True
IgnorePolicies                  : False
```

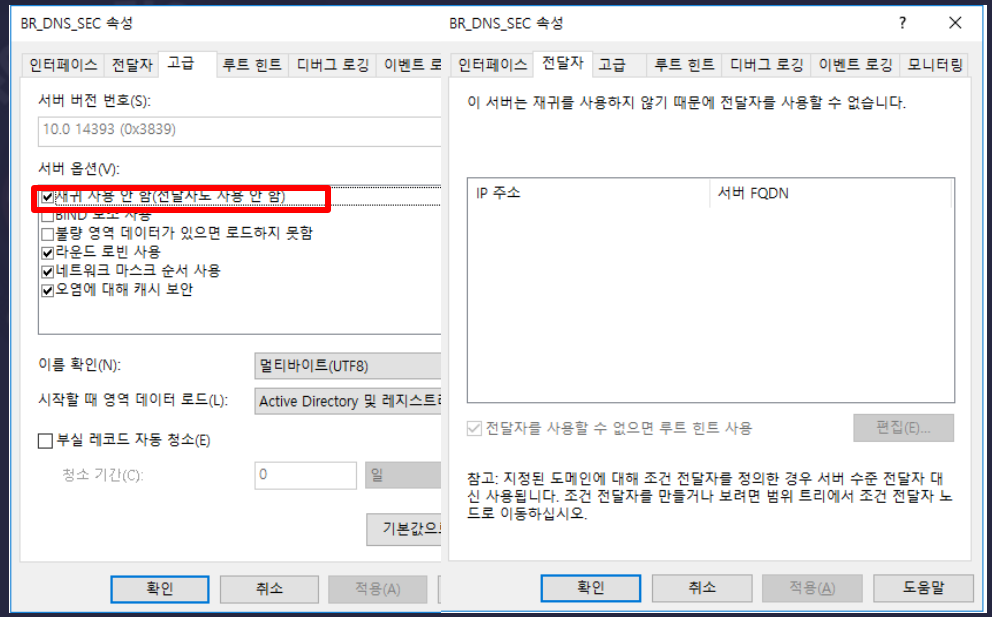
DNSSEC 대체 추가 보안 설정

- 오픈 리졸버 악용 위험
- DNS 캐시 포이즈닝 공격 가능성 증가 위험

- **DNS 재귀 요청 차단**
- **전달자 사용 제한**

- 캐시 포이즈닝 공격 시도 차단
- 오픈 리졸버 악용 차단
- DNSSEC 없이도 DNS 공격 표면 크게 감소

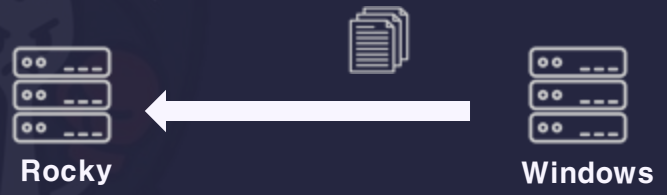
재귀 사용 제한



전달자 사용 제한

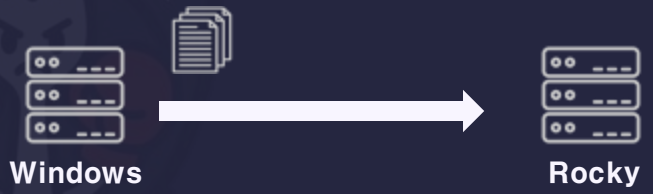
윈도우 와 Rocky SSH 연결

- 로키 PULL 방식 연결
- 사용 기능
  Windows Server : OpenSSH
  Rocky Linux : rsync + cron
- 인증 방식 : SSH 키 기반 인증
- Rocky 서버가 정해진 시간에 Windows 서버의 로그/파일을 rsync로 가져오는 방식
- Windows는 요청을 받기만 하고 능동적으로 접속하지 않음



윈도우 와 Rocky SSH 연결

- **윈도우 PUSH 방식 연결**
- 사용 기능 Windows Server
  : OpenSSH Client, PuTTY (키 생성 및 관리, 연결 주체)
- 인증 방식
  : SSH 키 기반 인증, IP 기반 접근 제어
- Windows 서버가 로그 생성 후 Rocky Linux 서버로 직접 전송(Push)



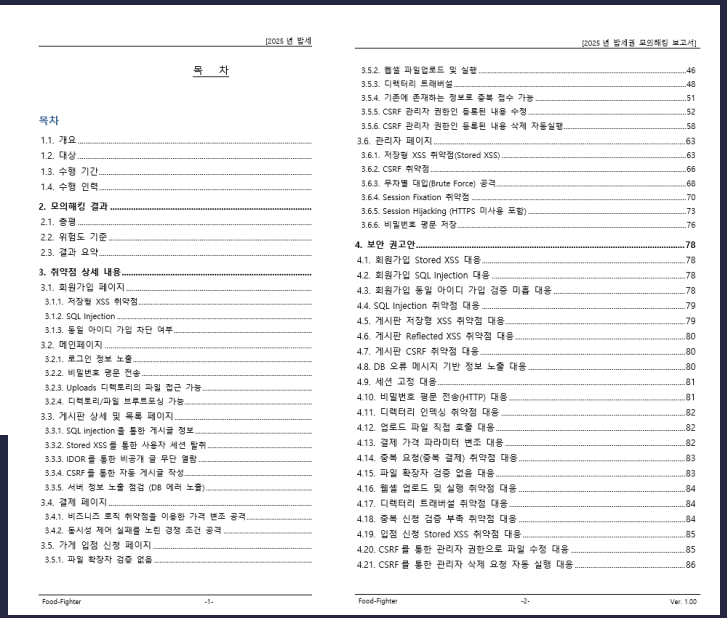
모의해킹 보고서 작성

- 취약한 상태의 **밥세권 고객센터 웹 페이지 모의해킹** 진행
- 웹 서비스 보안 취약점 식별
- 실제 공격 **시나리오 기반** 위험도 검증
- 보안 **조치 방향 제시**

2025 년 밥세권 모의해킹 보고서

모의해킹 결과 보고서 v1.00

Food-Fighter



[2025 년 밥세

목 차

목차

Food-Fighter -1-

[2025 년 밥세권 모의해킹 보고서]

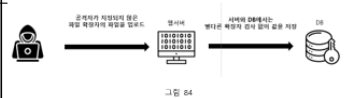
Food-Fighter -2- Ver. 1.00

모의해킹 보고서 작성

- 페이지별 취약점 식별
- 공격 시나리오 기반 검증
- 보안 권고안 제시

3.5. 가게 입점 신청 페이지

3.5.1. 파일 확장자 검증 없음

구분	설명
대상	가게 입점 신청완료 페이지 http://www.babhelp.com/php/partner_proc.php 가게 입점 신청 페이지 http://www.babhelp.com/php/partner.php 업로드한 파일 미리보기 페이지 http://www.babhelp.com/php/uploads/
취약점	파일 업로드 검증 미흡(FU)
위험도	상
시나리오	 그림 84
취약점 개요	사용자가 업로드하는 파일에 대해 확장자, MIME 타입, 파일 헤더 검사 등이 전혀 이루어지지 않는다. 따라서 HTML JS 공격 스크립트 등 어떠한 파일도 서버에 업로드할 수 있으며, 업로드된 파일은 /uploads/ 폴더에서 웹 경로로 직접 실행된다.

1. 페이지에 적힌 pdf, 이미지 파일이 아닌 html 파일을 첨부하여 신청 진행함

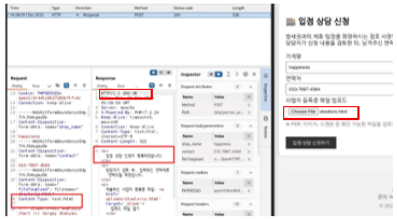


그림 85

4. 보안 권고안

4.1. 회원가입 Stored XSS 대응

취약점 항목	XS – 저장형 XSS
취약점 개요	회원가입 시 입력된 아이디 값이 필터링 없이 DB에 저장되며, 로그인 시 해당 스크립트가 그대로 실행된다. 이를 통해 공격자는 세션 탈취 또는 악성 스크립트 실행이 가능하다.

보안 조치 방법

- 모든 출력값에 HTML Escape(특수문자 변환) 적용
- 회원가입 입력값에서 스크립트·DOM 이벤트 제거
- 로그인 페이지 CSP 정책 적용
- HttpOnly·Secure 쿠키 적용
- 사용자 입력 필드에 화이트리스트 기반 검증 적용

4.2. 회원가입 SQL Injection 대응

취약점 항목	SI – SQL Injection
취약점 개요	회원가입 요청에서 입력값 검증 없이 SQL 쿼리에 직접 삽입되는 구조로 인해 SQL Injection 공격이 가능하다. 이를 통해 DB 오류 기반 구조 노출 및 데이터 변조 가능성이 확인되었다.

보안 조치 방법

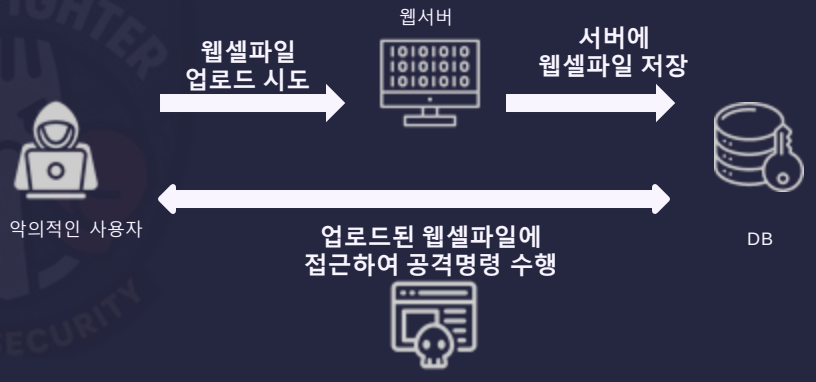
- Prepared Statement / Parameterized Query 적용
- 입력값 화이트리스트 검증
- 오류 메시지 사용자에게 미노출(커스텀 에러 페이지)
- DB 계정 최소 권한 적용
- 비밀번호는 bcrypt/Argon2 기반 해시 저장

4.3. 회원가입 동일 아이디 가입 검증 미흡 대응

취약점 항목	PV – 프로세스 검증 누락
취약점 개요	회원가입 시 기존 아이디에 대한 중복 검증이 이루어지지 않아 동일 아이디로 여러 계정을 생성할 수 있다. 이는 사용자 식별 체계 붕괴 및 내부 데이터 무결성을 크게 해친다.

모의 해킹 (파일 업로드)

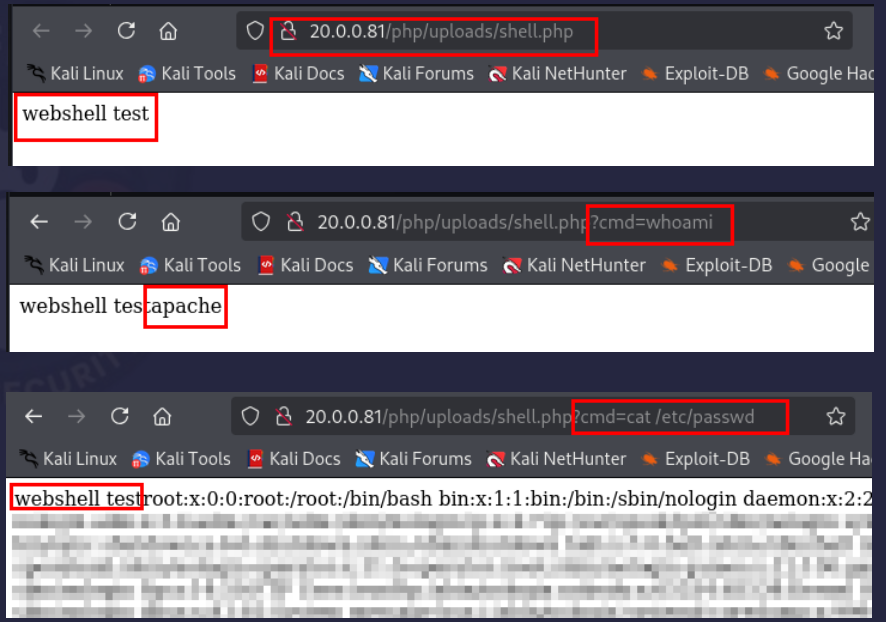
- 파일 업로드시 **확장자, MIME 검증 부족**한 취약점이 발견
- 공격자가 **백도어가 포함 된 파일을 업로드** 후 파일을 실행하여 apache 권한으로 웹서버를 실행 가능
- 실제 테스트에서 apache 계정으로 파일 접근, 디렉토리 생성 과 같은 **OS 명령 실행 과 RCE가 발생**함이 확인




```
[root@BR_PHP_SEC uploads]# cat shell.php
<?php echo "webshell test"; system($_GET['cmd']); ?>
```

모의 해킹 (파일 업로드)

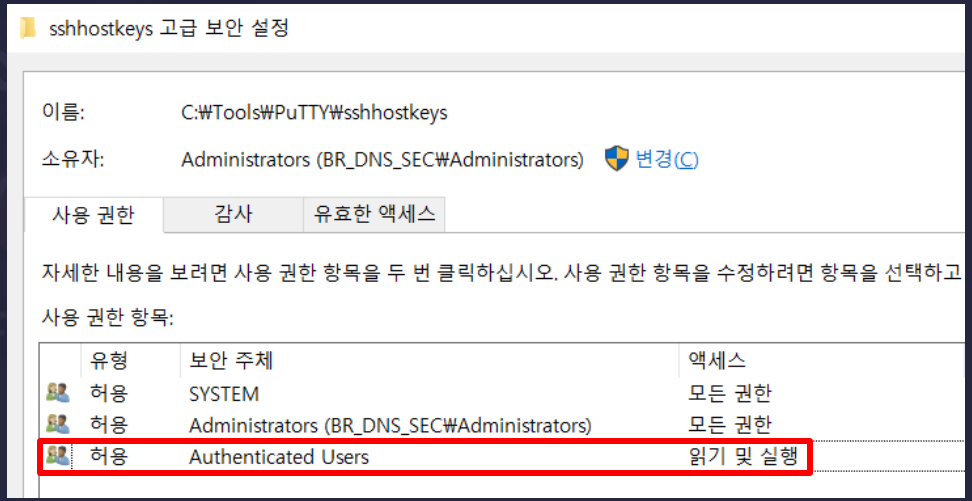
- 파일 업로드시 **확장자, MIME 검증 부족**한 취약점이 발견
- 공격자가 **백도어가 포함 된 파일을 업로드** 후 파일을 실행하여 apache 권한으로 웹서버를 실행 가능
- 실제 테스트에서 apache 계정으로 파일 접근, 디렉토리 생성 과 같은 **OS 명령 실행 과 RCE가 발생**함이 확인



Trouble Shooting

트러블 슈팅 (윈도우 와 Rocky SSH 접속)

- 키 파일이 권한에 Users가 포함되어 **최소 권한 원칙 위배**
- Rocky의 ssh가 보안 위험으로 판단 하여 **접속 거부**
- 공개키 파일 권한에 **상속과 Users를 제거하여 해결**



느낀점

- 보안 설정과 로그 필터링을 구성하면서 운영 단계에서 **문제를 발견하고 대응하는 능력**이 구축 과정만큼 중요하다는 사실을 느낄 수 있었다.
- 아울러 권한 관리와 보안 정책의 세부 요소가 시스템 전반에 큰 영향을 미친다는 점을 경험하며, **보안은 무엇보다 사전 예방이 핵심**임을 다시 한 번 확인하게 되었다.

Q&A

감사합니다