

파이널 프로젝트 기획서



IaC(코드형 인프라)를 활용한 인프라 및
보안 아키텍처 구축

TEAM S-Core.

2025.07.30.

Blue

Purple

Red



목차

파이널 프로젝트 기획서	
1. 프로젝트 개요	3
가) 프로젝트 소개	3
나) 프로젝트 일정	4
다) 개념도	5
라) 기획 시나리오	6
2. 네트워크 구성	7
가) 논리 구성도	7
나) 네트워크 제원	7
다) 네트워크 기술리스트	8
3. 서버 구성	10
가) 서비스 흐름도	10
나) 서버 구성도	11
다) 서버 기술리스트	12
라) 서버 제원	14
(i) 운영체제 정보	14
(ii) 서비스 패키지 정보	14
4. 보안 정책	15
가) 보안 기술리스트	15
나) 주요정보통신 취약점 점검	16
다) 취약점 개선 흐름	17
라) SOAR 흐름	18
5. 모의 해킹	19
가) 해킹시나리오	19
나) 모의해킹 기술리스트	20
다) 침투테스트 절차	21
** 부 록 **	24



1. 프로젝트 개요

가) 프로젝트 소개

항목	내용	
프로젝트명	IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축	
프로젝트 기간	2025.07.28. ~ 2025.08.08	
프로젝트 목표	Blue	<ul style="list-style-type: none">- 다양한 라우팅 프로토콜을 이용한 네트워크 망 구성- 리눅스 서버에서 MRTG 서비스를 통한 네트워크 트래픽 모니터링- 백업 및 로그 서버를 구축하여 주요 파일과 설정등을 백업- 네트워크 장비와 서버의 이중화 구축을 통해 비상시 복구 대책 마련- Snort 정책을 사용한 네트워크 보안탐지 체계 구축- Ansible을 이용한 서비스 설치 및 설정 자동화
	Red	<ul style="list-style-type: none">- 조직 내 보안 체계의 실효성 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
	Purple	<ul style="list-style-type: none">- 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	<ul style="list-style-type: none">- 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	



파이널 프로젝트

문서 번호

FN-008

수정일

2025-08-01

페이지

4 / 25

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												

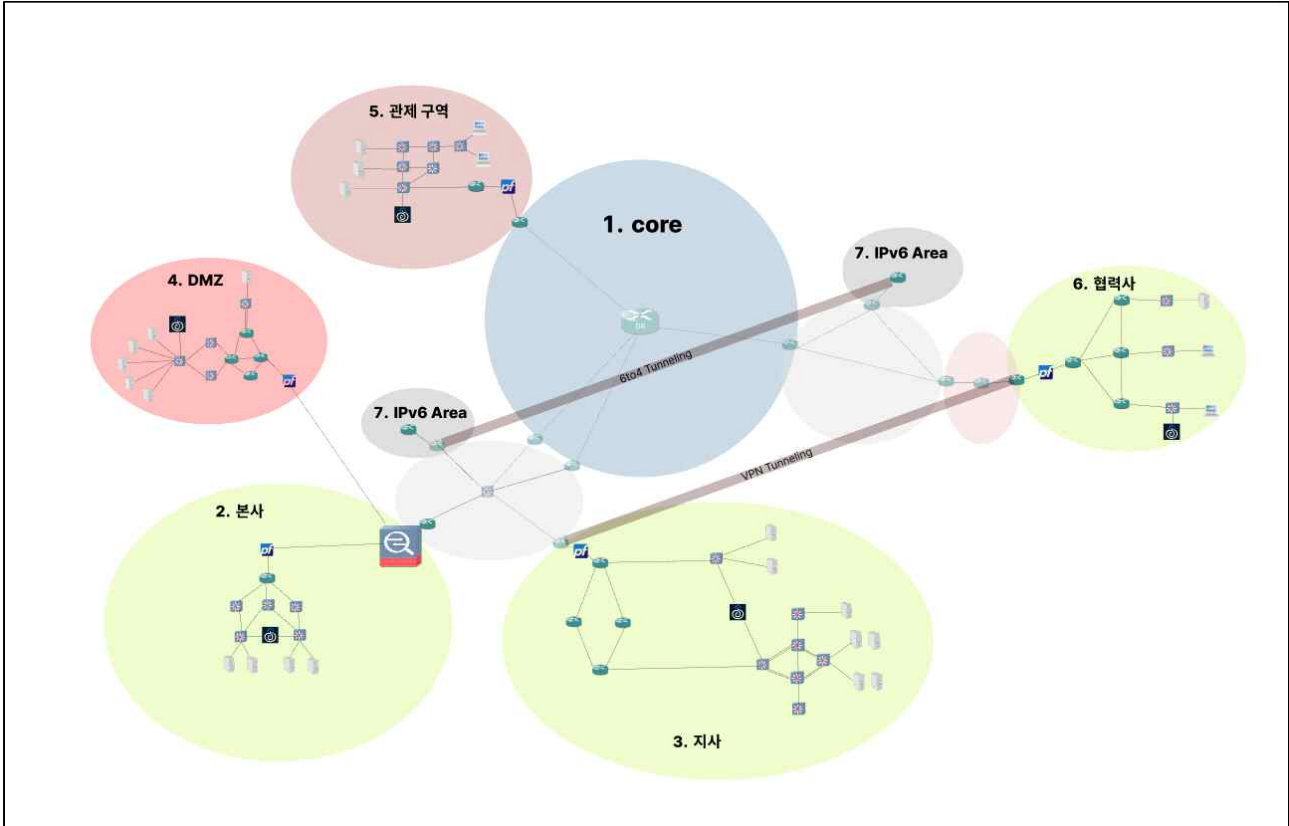
<주의>

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) 개념도



구역	별칭	구역별 설명
① 코어망	CO	- 네트워크의 중심이 되는 코어망
② 본사	HQ	- 내부 인트라넷 구조의 인프라 구축
③ 지사	BR	- 협력사와의 VPN 통신 인프라 구축
④ DMZ	DM	- 외부와의 통신이 필요한 서버팜 구축
⑤ 관제 구역	MN	- 네트워크 트래픽 및 서버 모니터링 통합 시스템 구축
⑥ 협력사	PT	- VPN을 활용한 지사 인트라넷 접속이 가능한 인프라 구축
⑦ IPv6 Area	IP6	- IPv6 사용을 위한 네트워크 구축



라) 기획 시나리오

구역	기획 시나리오
코어망	<ul style="list-style-type: none">- 백본 및 네트워크망 확장을 통한 대규모 네트워크망 구축
본사	<ul style="list-style-type: none">- 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	<ul style="list-style-type: none">- 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	<ul style="list-style-type: none">- 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	<ul style="list-style-type: none">- 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	<ul style="list-style-type: none">- 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	<ul style="list-style-type: none">- 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



파이널 프로젝트

문서 번호

FN-008

수정일

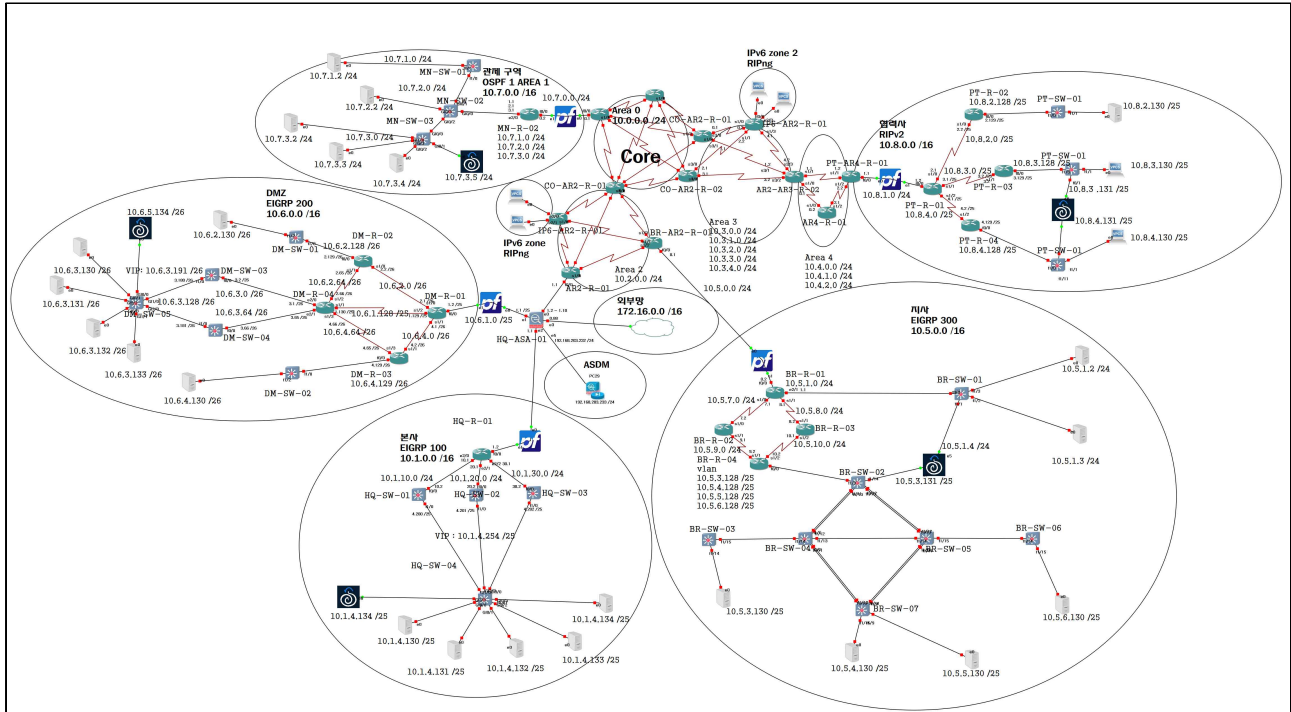
2025-08-01

페이지

7 / 25

2. 네트워크

가) 논리 구성도




나) 네트워크 자원

장비명	별칭	모델명	수량
Router	R	Cisco C7200	28대
Switch	S	Cisco C3745	24대
		Cisco IOSvL2 15.2	4대
방화벽	ASA	Cisco ASA 9.2	1대
IPS	PF	pfSense-CE-2.7.2-RELEASE	5대
IDS	SO	securityonion-16.04.7.3	5대

다) 네트워크 기술리스트

분류	기술		사용 목적 및 구현 방법
Switch	VLAN		지사 스위치에 vlan을 이용하여 서버의 네트워크 대역을 논리적으로 분리하여 사용(vlan10 : vlan20)
	PVST		지사 의 vlan10 ,vlan 20으로 향하는 네트워크 트래픽을 분산 및 이중화
	Frame-Relay		ospf의 코어망을 Frame-Relay를 사용하여 회선비용 절감과 여러 개의 라우팅 경로를 이용(Full Mesh)
	FHRP		게이트웨이 이중화 기술인 GLBP를 이용 DMZ, 서버팜, 본사, 지사 내의 Main서버들 기준의 게이트웨이 로드 밸런싱인 GLBP를 이용(스위치 3대 사용)
	Port-security		MAC 주소 기반 보안 기술 백업존의 관리자의 pc 개수를 제한하여 필요이상의 관리자가 내부로 들어와서 사용할수 없게 함
	SPAN		스위치에 port-mirroring을 사용해 게이트웨이 이중화로 나가는 구역을 source포트로 지정하여 네트워크 대역의 트래픽 탐지
Routing	IPv6		기숙사 및 지사 사무실에 많은 호스트 관리 DHCP RIPng를 이용하여 라우팅 관리
	static		ASAv 방화벽에서 WAN으로 향하는 기본경로를 outside방향으로 지정
	RIPv2		사무실 ASBR에서 수동 축약 사무실 내부 SMB 서버를 오프셋 리스트로 홉카운트 최대치 부여 OSPF방향으로 광고하지 않음.
	EIGRP		매우 빠른 장애 복구 능력, 효율적인 자원 사용 수많은 서버가 유기적으로 연결되어 높은 가용성과 성능 기대
	OSPF	Virtual Link	Backbone(Area 0)과 Area5 를 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	백본 망과 이어지는 인터페이스의 이웃 neighbor별 적용
		area 인증	Trransit Area로 지정한 Area4에서 area인증을 적용하여 LSA를 전달하는 모든 라우터에서 인증을 적용
	재분배		다른 동적 라우팅 프로토콜 정보를 교환함으로 내부 구간에서 모든 통신이 가능하게 함

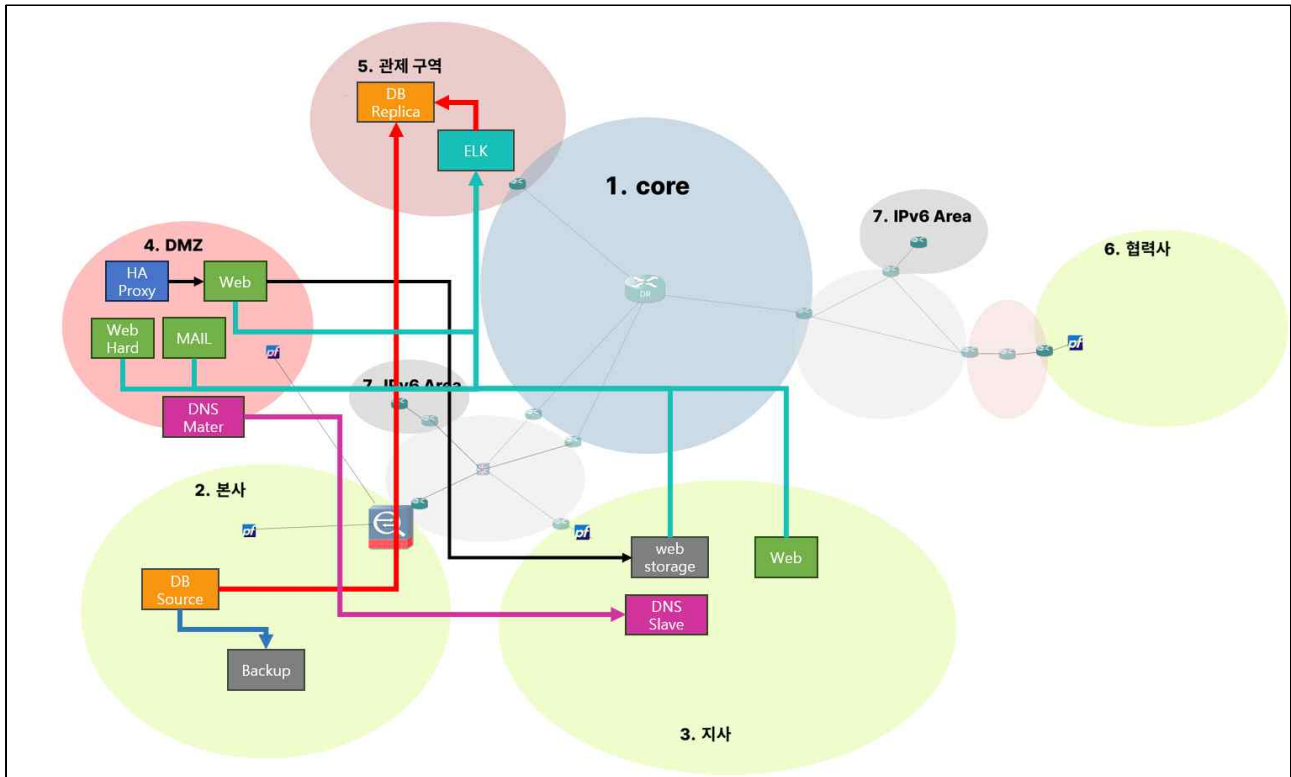
	파이널 프로젝트	문서 번호	FN-008
		수정일	2025-08-01
		페이지	9 / 25

다) 네트워크 기술리스트

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	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 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
기타	Diffie-Hellman 2		1024-bit key length 사용, 키 교환에 사용됨.
	SSH		라우터, 스위치 장비의 설정값을 자동으로 수집해서 파이썬을 통해 텍스트 파일로 백업
	DHCP		내부의 IP 주소 관리 자동화
	NAT		내부망 인터넷 접근과 보안 강화 방안


3. 서버 구성

가) 서비스 흐름도



서비스명	내용
DB	<ul style="list-style-type: none"> - IDS, IPS RuleSet 생성에 필요한 정보를 DB 저장 - Master - Slave 구조의 동기식 운영을 통해 DB 분산처리 진행
DNS	<ul style="list-style-type: none"> - DNS Master - Slave 구조로고가용성 확보
ELK	<ul style="list-style-type: none"> - 서버 Health 모니터링 및 침입 탐지 및 차단 로그 수집 - 중앙화된 로그를 통해 SOAR 솔루션 구현
HA Proxy	<ul style="list-style-type: none"> - 웹서버를 2개로 분산 구축하여 RoundRobin 방식으로 운영 - 웹 스토리지는 별도 구축하여 NFS를 통해 관리
Backup	<ul style="list-style-type: none"> - DB 및 주요 서비스 설정값 백업을 통한 안정성 확보

구역	별칭	OS	도메인
본사	HQ-DNS	Ubuntu	ns.s-hq.it
	HQ-DB	Ubuntu	hq-db.s-hq.it
	HQ-iSCSI	Ubuntu	hq-iscsi.s-hq.it
	HQ-Mail	Rocky	hq-mail.s-hq.it
지사	BR-DNS	Rocky	ns.s-core.it
	BR-NFS	Ubuntu	br-nfs.s-core.it
	BR-iSCSI	Windows Server 2022	br-iscsi.s-core.it
	BR-Web	msf	br-web.s-core.it
	BR-DB	msf	br-db.s-core.it
	BR-search	msf	br-search.s-core.it
DMZ	DM-DNS	Ubuntu	ns.core.it
	DM-HAproxy	Rocky	www.core.it
	DM-WebHard	Ubuntu	dm-webhard.core.it
	DM-Web1	Ubuntu	dm-web1.core.it
	DM-Web2	Rocky	dm-web2.core.it
관제	MN-ELK	Rocky	mn-elk.s-core.it
	MN-Monitorix	Rocky	mn-monitorix.s-core.it
	MN-MRTG	Rocky	mn-mrtg.s-core.it
	MN-Cacti	Rocky	mn-cacti.s-core.it
	MN-SOAR	Rocky	mn-soar.s-core.it
	MN-DB	Ubuntu	mn-db.s-core.it
협력사	PT-NFS	Rocky	pt-nfs.s-core.it

	파이널 프로젝트	문서 번호	FN-008
		수정일	2025-08-01
		페이지	12 / 25


다) 서버 기술리스트

분류	기술	사용 목적 및 구현 방법
Network	DNS	Master / Slave 구조로 고가용성 확보
Web	NginX	주정통 점검 결과 페이지 구축
	Apache	DMZ WAS 구축 CMS 폴더는 내부 FTP 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
DBMS	MariaDB	Source 서버 / Replica 서버 구성으로 고가용성 확보 고가용성 적용 DB: 로그 분석 DB / RuleSet DB / SOAR DB
		주정통 DB : 취약점 점검 시 외부 클라우드(Xen server)에서 주정통DB를 참조
	phpMyAdmin	데이터베이스 관리 및 최적화, GUI 제공
Storage	NFS	협력사와 지사 간 파일 공유 서비스
		회사 홈페이지 Master 폴더 공유
	iSCSI	iSCSI를 활용한 안전한 스토리지 공유 시스템 구축



다) 서버 기술리스트

분류	기술		사용 목적 및 구현 방법
Monitoring	Monitorix		모든 서버 리소스 모니터링 진행
	SNMP	MRTG	SNMP와 연동해서 사용하는 네트워크 트래픽 모니터링 도구
		Cacti	
	ELK	Elastic search	Elasticsearch를 이용해 로그의 중앙화 구현
		Logstash	로그 및 데이터를 수집해 필요한 형식으로 가공 후 Elasticsearch에 전달
		Kibana	Elasticsearch에 저장된 데이터를 시각적으로 표현
		Packetbeat	네트워크 인터페이스에서 캡처한 패킷을 분석
		Filebeat	시스템로그 및 애플리케이션 로그 파일을 모니터링 모니터링 한 내용을 수집하여 Logstash에 전송
		Heartbeat	실행되고 있는 웹 서비스나 ip, 포트 등의 상태 모니터링
Mail	postfix		SMTP 프로토콜을 사용하는 메일 발신 서버
	dovecot		IMAP 프로토콜을 사용하는 메일 수신 서버
	Roundcube		웹메일 기반 이메일 클라이언트
Security	UFW		서비스에 필요한 포트만 허용하는 화이트리스트 기반의 allow 정책 사용
	Firewalld		
Backup	Rsync		서버 설정 파일 Backup
	Rsyslog		로그 데이터 수집 및 백업 서버로 로그 중앙화

	파이널 프로젝트	문서 번호	FN-008
		수정일	2025-08-01
		페이지	14 / 25

라) 서버 자원

(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
pfsense	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		-
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	



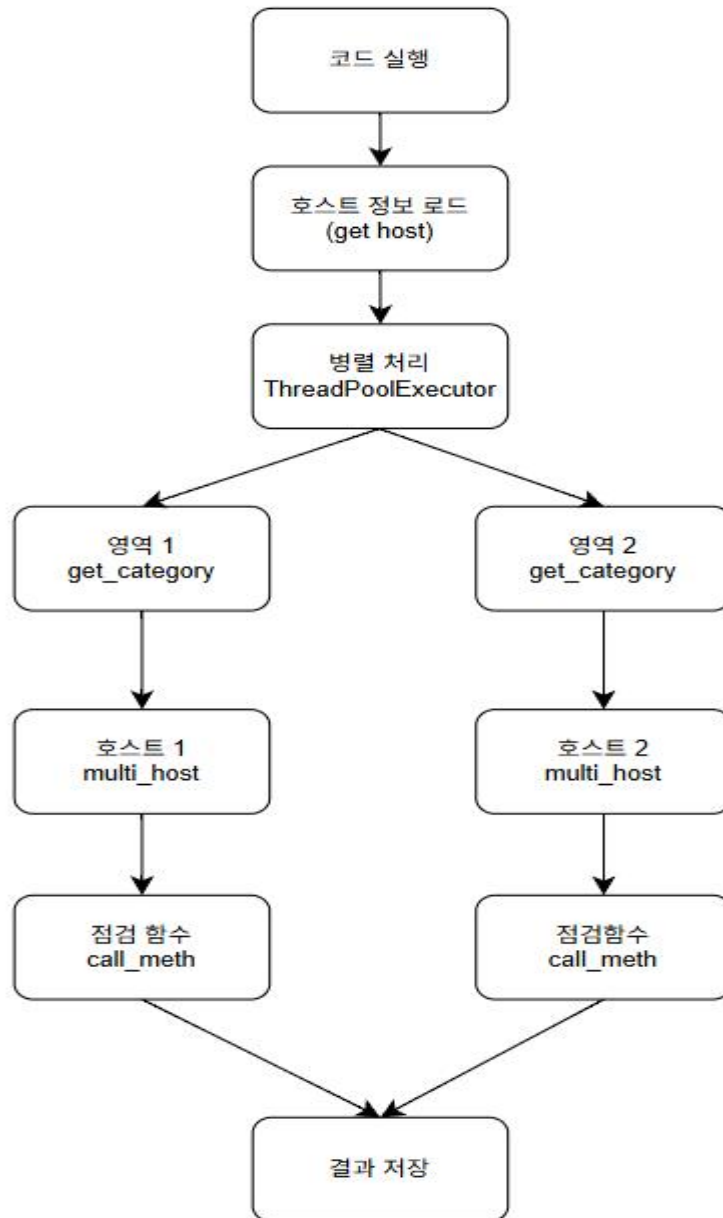
4. 보안 정책

가) 보안 기술리스트

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	IDS와 IPS에서 사용하며, 비정상 패킷 탐지 및 차단
	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

나) 주요정보통신 취약점 점검

주정통 취약점 분석 흐름도

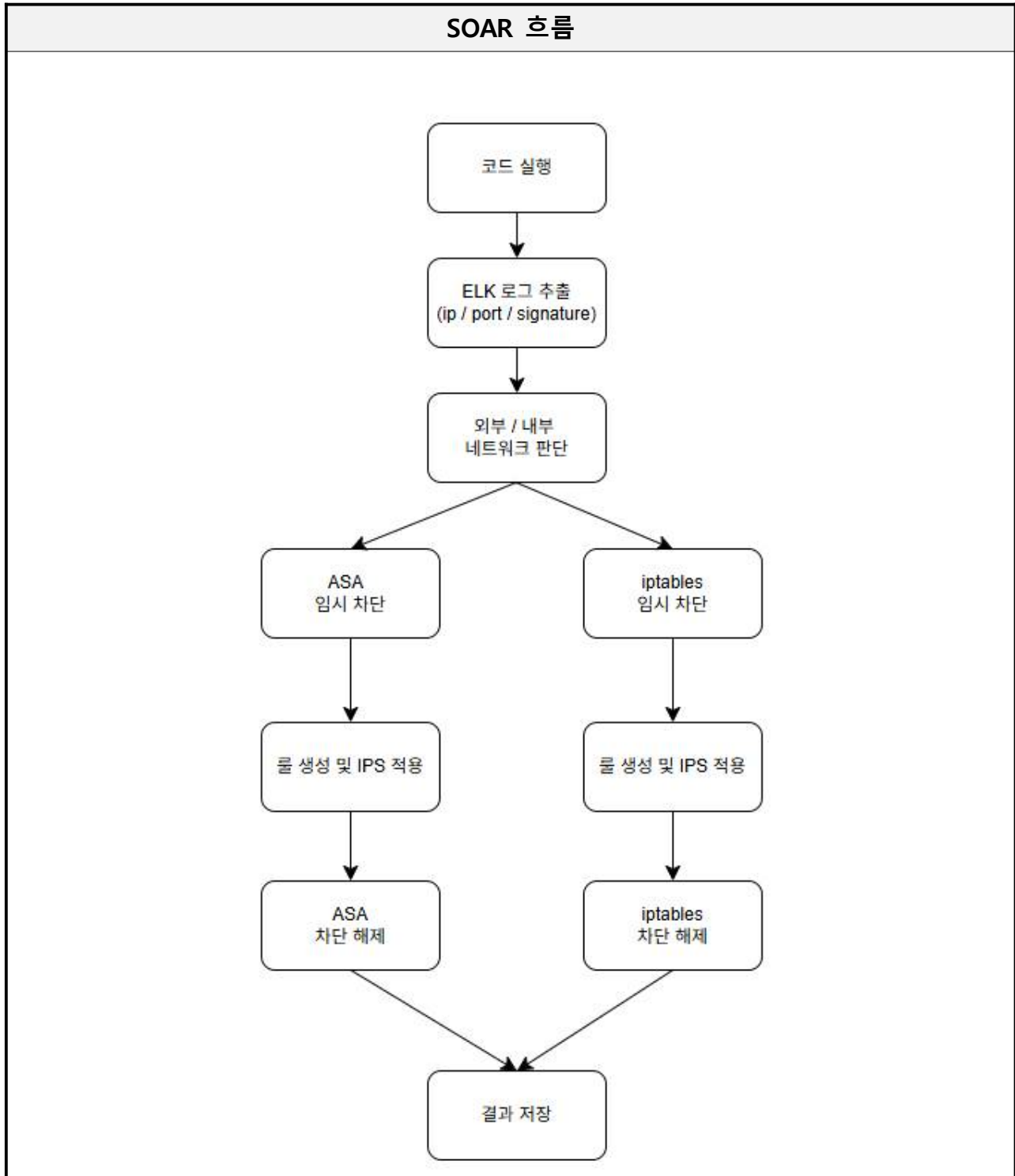


다) 취약점 개선 흐름도

취약점 개선 코드



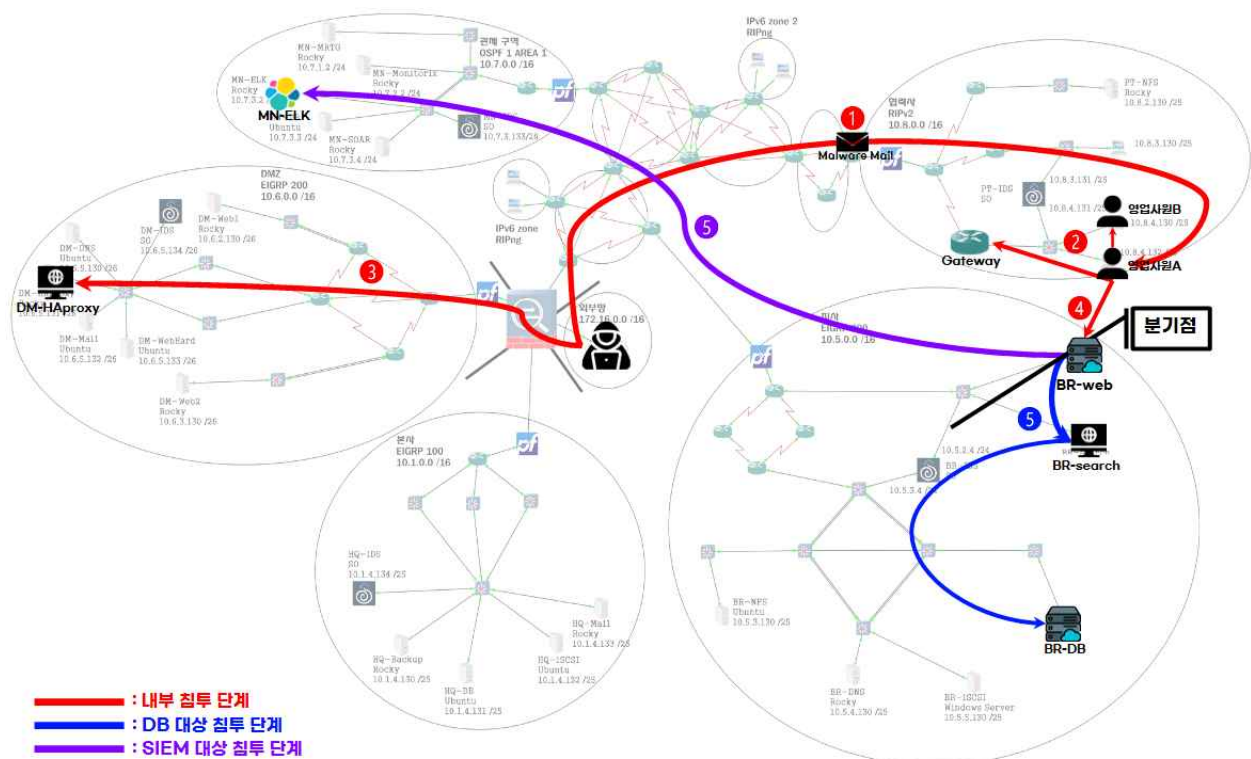
라) SOAR 흐름



5. 모의해킹

가) 모의해킹 시나리오

모의해킹 시나리오



시나리오 기반 기업의 내부 / 외부로 나누어 웹 서버, Database, SIEM을 대상으로 침투 테스트 진행



나) 기술리스트

분류	기술	상세 기술	적용 내용
침투 테스트	Information Gather	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
	Scanning	nmap	회사 내/외 네트워크 호스트 스캔 및 WAS, DB, SSH 포트 스캐닝
		nessus	회사 내/외 네트워크 호스트 스캐닝
		ffuf	내부 인트라넷 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 인트라넷 WAS 및 참조 DB의 SQL Injection 공격 취약점 진단
	Exploitation	hping3	내부 인트라넷 침투 단계에서 DMZ의 외부 WAS에 DoS 공격을 통한 시선 분산
		msfvenom	좀비 PC로 감염시키기 위한 악성 Payload 생성
		umbrella	사회공학 메일에 적재할 악성 다운로드 파일(PDF)을 생성
		metasploit	meterpreter로 좀비 PC의 리버스 셸 환경 제어 및 추가 공격
		x11vnc	영업사원 PC(좀비 PC)에서 역방향으로 원격 데스크탑 제어를 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 악성 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	백업/로그 서버(SIEM) 구역 PC의 SSH 서비스 사용자 계정 로그인 시도
		privilege escalation	일반 사용자로 시스템에 접근한 뒤에 race condition 공격을 위한 C 코드를 작성 후 권한 상승
		로그 위변조 및 무력화	백업/로그 서버(SIEM) 구역 서버의 관리자 권한으로 filebeat/logstash 설정 파일 조작 등의 로그 위변조



파이널 프로젝트

문서 번호

FN-008

수정일

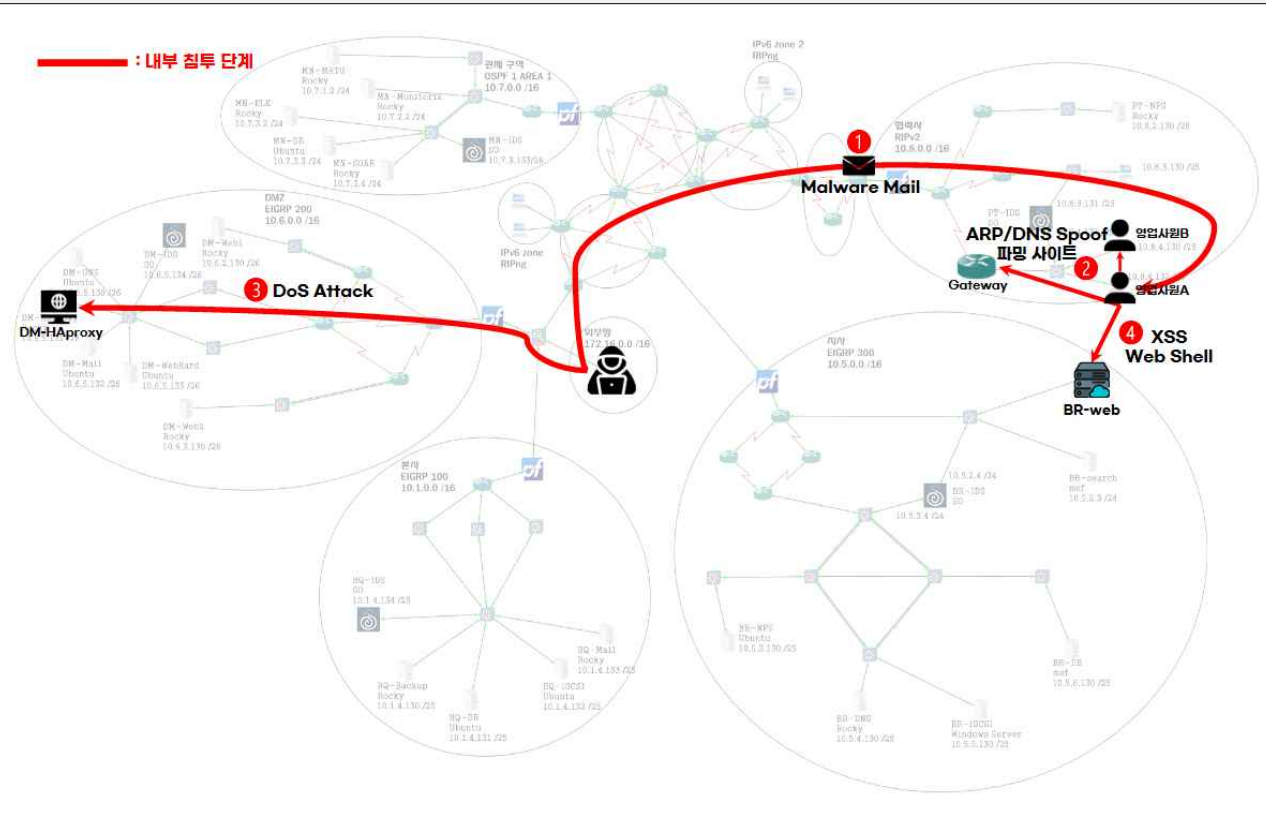
2025-08-01

페이지

21 / 25

다) 침투테스트 절차

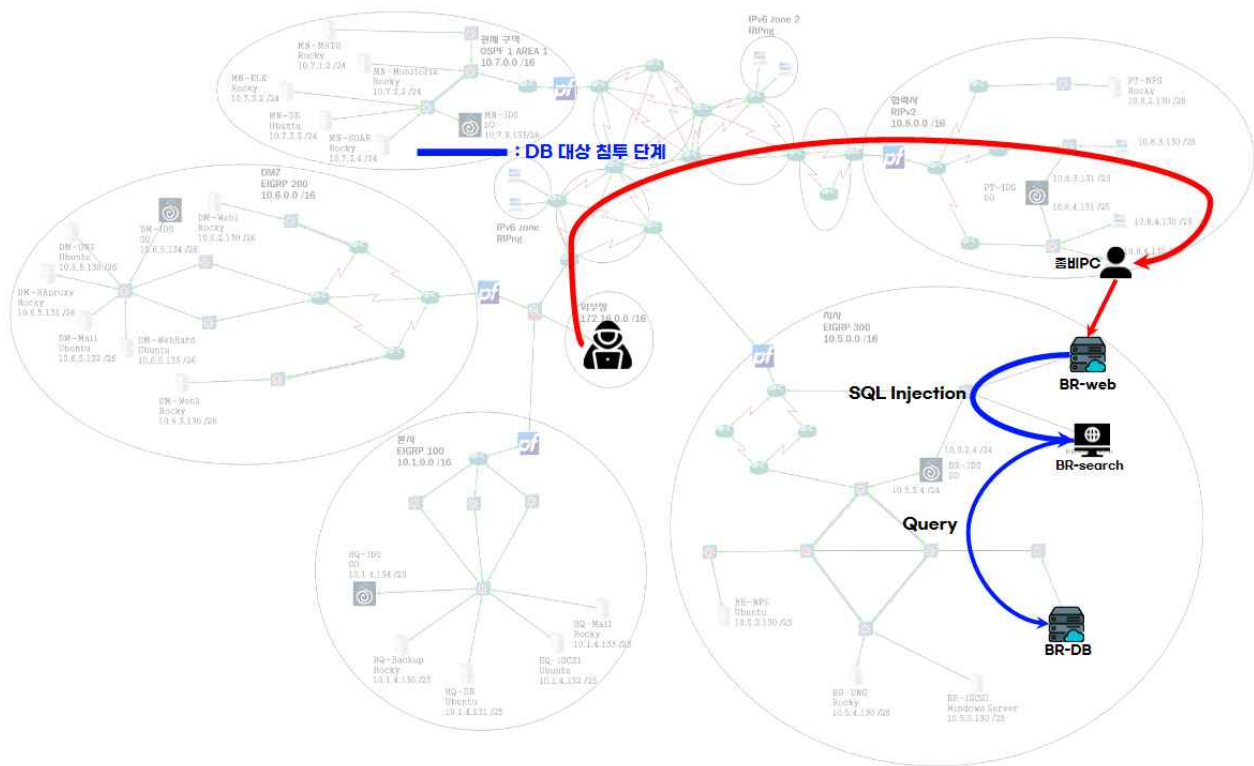
초기 침투, DMZ 구역의 웹 서버, DNS 서버를 통해 정보 수집, 영업사원 A의 메일 주소 확보 후 사회공학으로 좀비 PC 감염, 좀비 PC를 통한 내부 인프라 탐색 후 관리자 페이지 취약점으로 웹 셸 업로드 후 내부 리버스 셸 획득(내부 WAS 장악)하는 시점에 시선 분산 용도의 DoS 공격 수행





다) 침투테스트 절차

DB 대상 공격, 내부 웹 서버가 참조하는 DB 서버 특정 및 취약점 분석, DB 정보 탈취를 목적으로 SQL Injection 수행





파이널 프로젝트

문서 번호

FN-008

수정일

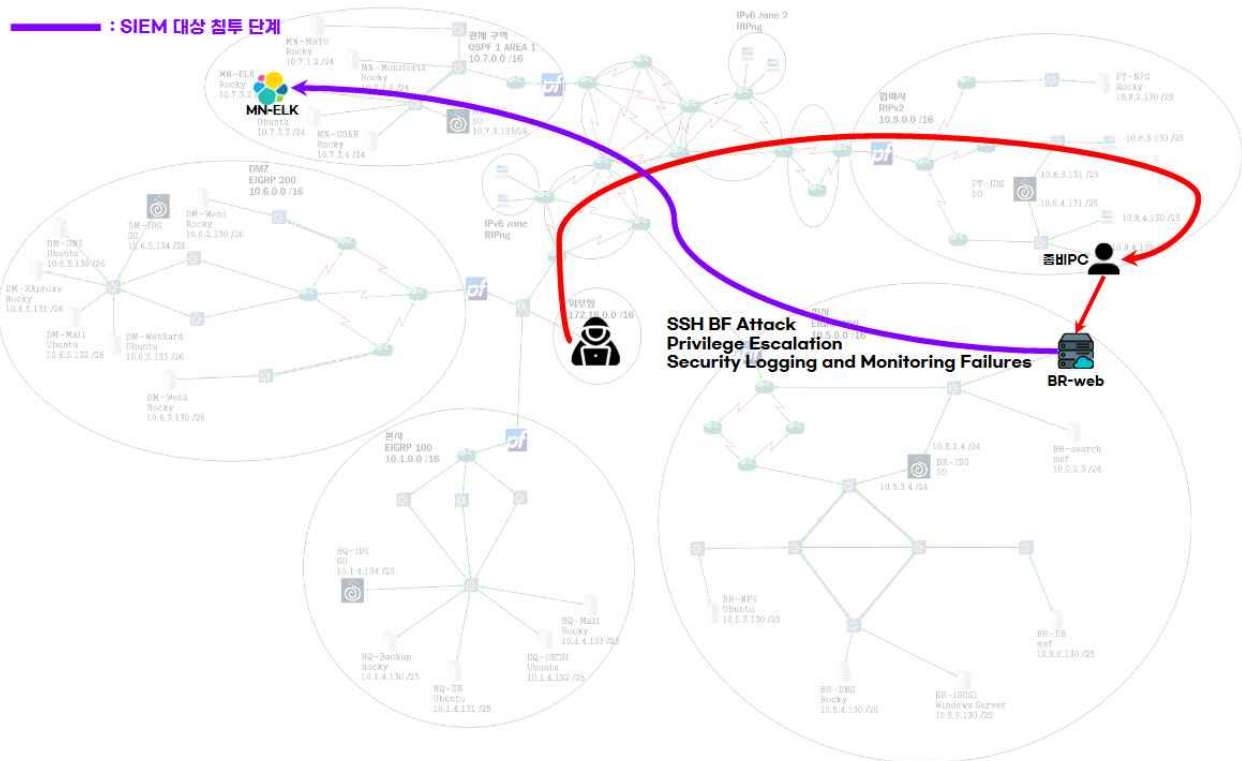
2025-08-01

페이지

23 / 25

다) 침투테스트 절차

SIEM 대상 공격, 내부 웹 서버의 로그를 수집하는 SIEM(ELK)으로 SSH BruteForce 및 권한 상승으로 시스템 장악 이후 로그 위변조 시도



**** 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