

**2차 합동 프로젝트**

**기획서(초안)**

2025.12.

**Blue, Purple, Red and Gray**

목차

1. 프로젝트 개요 (Project Overview) 4

1.1. 프로젝트명 4

1.2. 프로젝트 배경 및 목적 (Purpose &Background) 4

1.3. 프로젝트 목표 (Goals): 4

1.4. 기대효과 (Expected Results): 4

5

2. 프로젝트 일정 및 역할 (Schedule &Roles) 5

2.1. 전체 일정 (Timeline) 5

2.2. 역할 및 책임 (Roles &Responsibilities) 5

5

3. 네트워크 6

3.1 네트워크 제원 6

3.2 네트워크 기술리스트 6

3.3. 네트워크 논리 구성도 7

3.4. 네트워크 물리 구성도 8

4. 서버 9

4.1 서버 제원 9

4.2 서버 흐름도 10

4.3 서버 구성도 11

4.4 서비스 목적 12

4.5 네트워크 장비 도메인 목록 12

5. 파일 공유 시스템(iSCSI/NFS/SAMBA) 14

5.1 시스템 구성도 14

5.2 SMB 계정 목록 14

5.3 연결 프로토콜 14

6. Python 자동화 코드 관리 15

6.1 네트워크 장비\_자동화 코드 15

6.2 서버\_자동화 코드 16

7. 로그분석 17

7.1 네트워크 로그 분석 17

7.2 서버 로그 분석 17

7.3 로그분석 시나리오 19

8. 테스트 및 검증계획 20

8.1 테스트 시나리오 20

**1. 프로젝트 개요**

**1.1. 프로젝트명**

**기관 인프라 구축 및 모의해킹을 통한 취약점 진단**

**1.2. 프로젝트 배경 및 목적**

- 본 프로젝트는 보안에 대한 명확한 개념 이해를 바탕으로 네트워크 및 서버 단의 보안 취약 요소를 식별·제거하고, 안전한 시스템 운영 환경을 구축하는 것을 목적으로 한다.  
- 이를 위해 모의해킹을 통해 구성된 서버의 취약점을 분석하고, 분석 결과를 보안 정책에 반영하여 통합 보안 시스템을 구축한다.  
- 지속적인 점검과 보완 활동을 통해 보안 취약성으로 인한 위험도를 실현 가능한 수준으로 저감하고, 안정적인 보안 운영 체계를 확립하고자 한다.

**1.3. 프로젝트 목표**

|  |  |  |
| --- | --- | --- |
| **분야** | **내용** | |
| **네트워크** | 구축 | - 고가용성을 위한 회선 이중화 및 Gateway 이중화를 적용한 네트워크 구축  - 대규모 네트워크에서 빠른 경로 탐색, 라우팅 업데이트 최소화를 위해 EIGRP 적용  - 소규모 네트워크에서는 RIP 또는 static 라우팅 적용  - 특정 트래픽에 대한 정책 기반 라우팅 및 접근 제어 |
| 관제 | - 네트워크 상에서의 비정상 행위 탐지를 위한 MRTG와 같은 네트워크 장비 모니터링 시스템 구축  - Wireshark를 활용한 패킷 캡처 및 분석으로 비정상 트래픽 탐지 |
| 보안 | - 프로토콜별 인증 구성과 Access-List 및 Distribute- List를 활용하여 인가되지 않은 침입을 차단하는 안전한 네트워크 구축  - 외부와 통신하지 않는 사설망 설정을 위해 Port-based NAT 적용 |
| 대응 | - Python 기반의 패킷 분석 프로그램 개발  - 패킷 분석 결과를 바탕으로 Access-list 추가  - Port-security를 활용하여 MAC 주소 접근 제어 목록 추가 |
| **서버** | 구축 | - 단일 장애점 제거를 위한 서비스별 분산 구축으로 시스템 안정성 및 운영 효율성 극대화  - 독립적 백업 서버 운용을 통한 서비스 가용성 및 무결성 보장  - nginx reverse proxy + apache backend 구성을 통해 트래픽 부하 분산 및 최적화된 콘텐츠 전달속도 구현 |
| 관제 | - Cacti 기반의 웹 GUI 환경을 구축하여 서버 성능 지표(CPU, MEM, Disk)의 실시간 가시성 확보 및 위험 감지  - MRTG를 활용한 네트워크 대역폭 및 장비 상태의 시각화로 트래픽 이상 징후 조기 포착  - 서버 및 서비스별 로그 취합·분석을 통해 비정상적인 접근 시도 및 침해 사고 흔적의 실시간 탐지 및 기록 |
| 보안 | - SSL 키인증을 통한 데이터 전송 구간 암호화 및 통신 보안 강화  - Web, DB, Mail 등 각 서비스 별 보안 설정을 통해 안전한 서버 구축 |
| 대응 | - iptables 및 ufw 를 활용하여 허용된 신뢰 IP 외 모든 접근을 원천 차단  - NFS에 저장된 최신 백업본을 활용한 서비스 가용성 즉시 회복  - 저장된 로그를 분석하여 공격 경로 파악 및 재발 방지 |
| **관제** | 인프라 점검 | - 주요정보통신기반시설 기술적 취약점 분석·평가 상세 가이드의 ‘상’ 항목을 기반으로 Unix 서버, 윈도우즈 서버, 보안 장비, 네트워크장비, PC, DBMS, 웹에 대한 취약점 점검 수행  - 기밀성, 무결성, 가용성에 영향을 미치는 위협요인 파악, 사용자 및 공격자 관점에서의 위협요소 도출 및 대응 방안 제시 |
| 침투테스트 대비 | - 외부망에서 접근 가능한 서비스에 대해 공격자  관점의 접근 및 공격 테스트, 정보 유출 및 내부서버망과 내부 사용자망에 대한 침투 가능성 확인 |
| **모의해킹** | 침투테스트 | - 내/외부망에서 악의적인 목적을 가진 사용자로 가장하여 모의해킹 수행, 내부 및 외부 사용자에 의한 정보 유출 가능성 확인  - 시라니오 기반 침투 테스트 수행을 통해 보안 위협의 사전 발견 및 대응방안 제시 |

**1.4. 기대효과 (Expected Results)**

|  |  |  |
| --- | --- | --- |
| **분야** | **내용** | |
| **네트워크** | - 네트워크 분산 구축을 통한 데이터 전송 안정성과 가용성 보장 | |
| **서버** | - 서버 및 서비스 분산 구축을 통한 데이터 전송 안정성과 가용성 보장  - 주기적인 로그 분석 및 백업을 통한 데이터 손실 위협에 대한 대응 및 복구 보장 - 통합 모니터링 및 로그분석 선제적 위협 탐지 및 즉각 대응  - 화이트리스트기반 접근 제어와 SSL 암호화를 통해 내부 데이터 유출 최소화 - nginx reverse proxy + apache backend를 통한 부하 분산으로 서버자원의 병목 현상을 해결하고, 사용자에게 빠르고 쾌적한 웹 응답 속도 제공 | |
| **관제** | - 통합 모니터링 및 정책구현을 바탕으로 통합 관제의 컨트롤 타워 수행  - 탐지/대응방안 모색 및 보안정책에 반영 | |
| **모의해킹** | - 해커의 관점에서 보안취약점을 사전에 발굴하고 보완함으로서 실질적 방어력 향상  - 고객 정보 유출과 금전적 조작 등 기업 경영의 치명적 위협을 사전에 방지하여 대외 신뢰도 제고  - 사회공학적 공격시뮬레이션을 통하여 임직원의 보안의식을 고취시키고, 기업의 보안관리 체계 강화 | |

**2. 프로젝트 일정 및 역할 (Schedule &Roles)**

**2.1. 전체 일정 (Timeline)**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **WBS** | **세부 업무 (Task)** | **12월** | | | **1월** | | | | | | | | | | | | |
| **29** | **30** | **31** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** |
| **월** | **화** | **수** | **목** | **금** | **토** | **일** | **월** | **화** | **수** | **목** | **금** | **토** | **일** | **월** | **화** |
| **1. 계획** | | | | | | | | | | | | | |  |  |  |  |
| **1.1** | **목표 설정** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **1.2** | **프로젝트 요구사항 분석** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **1.3** | **프로젝트 기획안 작성** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **2. 설계** | | | | | | | | | | | | | |  |  |  |  |
| **2.1** | **네트워크 설계** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **2.2** | **서버 설계** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **2.3** | **모의해킹 시나리오 설계** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **2.4** | **보안관제/탐지 정책 설계** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **3. 구축 및 구현 테스트** | | | | | | | | | | | | | |  |  |  |  |
| **3.1** | **네트워크 구축** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **3.2** | **서버 구축** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **3.3** | **인프라 안정성 테스트** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **3.4** | **취약점 진단 및 스캐닝** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **3.5** | **모의해킹** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **3.6** | **공격 탐지 및 로그 분석** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **4. 환류** | | | | | | | | | | | | | |  |  |  |  |
| **4.1** | **보안대책 수립** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **4.2** | **시정조치 수행** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **4.3** | **시정조치 후 재검증** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **4.4** | **보고서 작성** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

**2.2. 역할 및 책임 (Roles &Responsibilities)**

|  |  |  |
| --- | --- | --- |
| **NO** | **성명** | **역할 및 책임** |
| **1** | 이명재 | 총괄 및 품질 보증활동 |
| **2** | 장혜원 | 네트워크 총괄 및 품질보증활동 |
| **3** | 정성현 | 네트워크 환경 구축, 자동화 코드 |
| **4** | 이하은 | 네트워크 세부 구성 및 구축, 자동화 코드 |
| **5** | 이현지 | 네트워크 세부구성 및 구축, 자동화 코드 총괄 |
| **6** | 김혜민 | 서버 총괄 |
| **7** | 유기원 | 서버 기획, 구축, 품질보증활동 외 |
| **8** | 김은성 | 서버구축 (smtp(mail), dns, cms(jl, wp)) |
| **9** | 유희영 | 서버구축 (snmp, bak) , 자동화코드 |
| **10** | 박희진 | 서버구축 (whd서버(pydio, owncloud, apache), web(nginx), client) |
| **11** | 장지웅 | 모의해킹 총괄 |
| **12** | 박소윤 | 모의해킹 자동화 코드 외 |
| **13** | 임지형 | 모의해킹 시나리오 기획 외 |
| **14** | 황한얼 | 모의해킹 시나리오 구현 및 테스트 |
| **15** | 한준희 | 모의해킹 수행 환경 정의 및 테스트 |
| **16** | 정영우 | 모의해킹 기술정의 및 취약점 분석 |
| **17** | 박혜림 | 보안 취약점 분석 및 품질보증활동 |
| **18** | 김윤영 | 보안관제 총괄 및 자동화 코드 총괄 |
| **19** | 김지원 | 로그 분석 및 관제 정책 수립 |
| **20** | 박신우 | 네트워크 패킷분석 및 대응 정책 수립 |
| **21** | 이원재 | 취약점 분석, 환경설정 및 품질보증활동 |
| **22** | 이은비 | 네트워크 관제 정책 수립 |

**3. 네트워크**

**3.1 네트워크 요구사항 총괄표**

|  |  |  |  |
| --- | --- | --- | --- |
| **요구사항 ID** | **요구사항명칭** | **구현 상세** | **도출 사유** |
| REP-N-core-01 | 로그 파일 전송시 빠른 경로 우선 | EIGRP offset-list 적용하여 경로 지정 | 관리자가 특정 경로 고정 |
| REP-N-core-01 |  |  |  |
| REP-N-core-01 |  |  |  |
| REP-N-core-01 |  |  |  |
| REP-N-BR-01 |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**3.2 네트워크 기술리스트**

|  |  |  |  |
| --- | --- | --- | --- |
| **구분** | **기능명** | **주요 기술 요소** | **상세 설명** |
| **네트워크** | SPAN | 포트 미러링 | 특정 포트에 지나가는 패킷을 다른 포트에 패킷 미러링 |
| PORT-SECURITY | MAC 주소 제어 | 스위치 포트에 접속 가능한 MAC 주소 제어 |
| ROUTING |  | 특정 대역에 대한 경로 선출 |
| FHRP | HSRP | Cisco 장비 기반 Gateway 이중화 프로토콜 |
| FHRP | VRRP | 표준 기반 Gateway 이중화 프로토콜 |
| FHRP | GLBP | Gateway 이중화와 트래픽 부하 분산 제공 |
| DEFAULT-ROUTING | STATIC | 목적지 경로가 라우팅 테이블에 없을 때 특정 포트로 패킷을 전달하는 기본 경로 설정 |
| RIPv2 |  | 거리벡터 기반 동적 라우팅 프로토콜. 클래스리스 기반 RIP, 멀티캐스트 사용 |
| RIPv2 | AUTO-SUMMARY | 클래스 경계 기준 자동 축약 |
| RIPv2 | MANUAL-SUMMARY | 광고할 라우팅 정보를 관리자가 직접 설정하여 네트워크 대역 축약 |
| RIPv2 | NEIGHBOR | 멀티캐스트 대신 유니캐스트로 라우팅 정보 교환 |
| RIPv2 | SPLIT-HORIZON | 라우팅 정보가 들어온 포트에 같은 정보를 전달하지 않아 루핑을 방지하는 기술 |
| EIGRP |  | Cisco에서 제공하는 거리벡터 기반의 링크 스테이트 동적 라우팅 프로토콜 |
| EIGRP | AUTO-SUMMARY | 클래스 경계 기준 자동 축약 |
| EIGRP | MANUAL-SUMMARY | 광고할 라우팅 정보를 관리자가 직접 설정하여 네트워크 대역 축약 |
| EIGRP | SPLIT-HORIZON | 라우팅 정보가 들어온 포트에 같은 정보를 전달하지 않아 루핑을 방지하는 기술 |
| EIGRP | DISTRIBUTE-LIST | 라우팅 업데이트 필터링 |
| EIGRP | OFFSET-LIST | 라우팅 메트릭을 인위적으로 조정하여 특정 대역에 대한 경로 지정 |
| EIGRP | KEY-CHAIN | 라우팅 프로토콜 인증을 위한 키 관리 |
| REDISTRIBUTE |  | 서로 다른 라우팅 프로토콜 간 경로 공유 |
| ACL | 표준 ACL | 트래픽을 조건에 따라 허용 또는 차단하는 접근 제어 기술 |
| ACL | 확장 ACL | 출발지, 목적지, IP 및 포트 기반 트래픽 제어 |
| PREFIX-LIST |  | 프리픽스 범위를 지정하여 특정 네트워크 대역을 차단하거나 허용하는 접근 제어 기술 |
| PAT |  | 여러 내부 사설 IP를 하나의 공인 IP로 변환하는 Port-based NAT |
| FRAME-RELAY |  | 패킷 교환 기반 WAN 기술로, 가상 회선(PVC)을 사용해 지점 간 데이터를 고속으로 전송하는 통신 방식 |
| MRTG | 장비 모니터링 | 네트워크 트래픽 모니터링 및 그래프화 도구 |
| CLOUD | VMWARE 연결 | GNS 환경과 VMWARE 가상 머신간의 Network Traffic Route를 연결하여 실제 os환경에서 gns topology를 테스트 |
| CLOUD | 이더넷 연결 | GNS Cloud Node를 Host PC의 물리적 Ethernet Interface에 연결하여 외부 네트워크와 통신 가능하게 설정 |
| ssh 원격제어 |  | 계정 인증을 통해 특정 장비나 서버에 접속하여 원경으로 제어 |

**3.3. 네트워크 구성도**

**3.3.1 논리구성도**

|  |
| --- |
|  |

**3.3.2 네트워크 물리 구성도**

|  |
| --- |
|  |

**[A구역 구현상세]**

|  |  |  |
| --- | --- | --- |
| **[A구역]** | 논리 구성도 | 물리 구성도 |
|  | 사진 | 사진 |
| (적용 기술) | 보고서에 목적과 같이 예쁘게  기술리스트항목을 따다가 개인포트폴리오 활용가능한 목적으로 작성 !!  어떤기능 , 구현 목적 , | |

**[B구역 구현 상세]**

|  |  |  |
| --- | --- | --- |
| **[B구역]** | 논리 구성도 | 물리 구성도 |
|  | 사진 | 사진 |
| (적용 기술) |  | |

**[C구역 구현상세]**

|  |  |  |
| --- | --- | --- |
| **[c구역]** | 논리 구성도 | 물리 구성도 |
|  | 사진 | 사진 |
| (적용 기술) |  | |

**[D구역 구현상세]**

|  |  |  |
| --- | --- | --- |
| **[D구역]** | 논리 구성도 | 물리 구성도 |
|  | 사진 | 사진 |
| (적용 기술) |  | |

**3.4 네트워크 제원**

|  |  |  |  |
| --- | --- | --- | --- |
| **장비명** | **별칭** | **모델명** | **수량** |
| **Router** | R | Cisco C7200 | 13대 |
| **Switch** | ESW | Cisco C3745 | 14대 |
| L2SW | CiscoIOSvL215.2(20200924:215240) | 5대 |
| **Frame Relay switch** | FRSW | Frame-Relay switch | 3대 |
| **자동화 프로그램 서버** | C&C | Rocky9 | 1대 |
| **장비 모니터링 서버** | MRTG | Rocky9 | 1대 |

**[네트워크 제원별 상세]**

|  |  |  |
| --- | --- | --- |
| 장비 | 설명 | 관리 IP |
| R1 | EIGRP 100, 이더넷 라우팅, Default route redistribute | 10.1.128.1/20 |
| R2 | EIGRP 100, EIGRP 200, redistribute, manual-summary | 10.1.16.1/20 |
| R3 | EIGRP 100, distribute-list로 로그 대역 업데이트 제어 | 10.1.32.1/16 |
| R4 | EIGRP 100, redistribute | 10.1.96.1/16 |
| R5 | EIGRP 200 | 20.0.0.5/24 |
| R6 | EIGRP 200 | 20.0.0.6/24 |
| R7 | EIGRP 100 | 10.1.224.2/20 |
| R8 | RIP, inter-vlan | 30.0.0.8/9 |
| R9 | RIP | 30.0.0.9/9 |
| R10 | EIGRP 100, R11과 static routing, redistribute | 10.1.64.2/20 |
| R11 | Static routing | 10.1.192.2/20 |
| R12 | EIGRP 100, RIP, neighbor 설정, split-horizon 해제, redistribute | 10.1.112.2/20 |
| R13 | EIGRP 100, PAT | 10.1.240.2/20 |
| ESW1 | VRRP | 1.1.1.2/24 |
| ESW2 | VRRP | 1.1.2.2/24 |
| ESW3 | VRRP | 1.1.3.2/24 |
| ESW4 | MHSRP | 2.1.1.2/24 |
| ESW5 | MHSRP | 2.1.2.2/24 |
| ESW6 | MHSRP | 2.1.3.2/24 |
| ESW7 | end device와 라우터 사이 연결 | 50.1.1.254/20 |
| ESW8 | end device와 라우터 사이 연결 | 192.168.80.254/24 |
| ESW9 | end device와 라우터 사이 연결 | 40.0.0.254/16 |
| ESW10 | VLAN 설정으로 여러 대역 연결 | 40.128.0.254/16 |
| ESW11 | GLBP | 3.1.1.2/24 |
| ESW12 | GLBP | 3.1.2.2/24 |
| ESW13 | end device와 라우터 사이 연결 | 192.168.50.254/24 |
| ESW14 | end device와 라우터 사이 연결 | 10.1.80.2/20 |
| L2SW1 | SPAN | 192.168.10.254/24 |
| L2SW2 | SPAN | 192.168.20.254/24 |
| L2SW3 | SPAN | 192.168.30.254/24 |
| L2SW4 | SPAN, Port-security | 192.168.70.254/24 |
| L2SW5 | SPAN | 192.168.90.254/24 |
| FRSW1 |  | X |
| FRSW2 |  | X |
| FRSW3 |  | X |
| 이더넷 클라우드 |  | X |
| C&C |  | 192.168.80.10/24 |
| MRTG |  | 10.1.80.10/20 |

**4. 서버**

**4.1 서버 요구사항 총괄표**

|  |  |  |  |
| --- | --- | --- | --- |
| 요구사항 ID | 분류 | 요구사항 명칭 | 구현 상세 |
| **REQI-NF-01** | 인프라 | **계층형 웹 서비스 아키텍처 구축** | C&C(Command & cuntrol) 서버로 내부 서버를 구축 및 제어 하고 DNS, DBMS, Back 서버로 내부 도메인과 데이터베이스, 백업을 관리하여 내부정보와 외부에 보여지는 웹 서비스를 분리하여 계층적 구조를 형성함. |
| **REQ-INF-02** | 인프라 | **리버스 프록시 기반 부하 분산** | Nginx 리버스 프록시를 통해 유입되는 트래픽을 백엔드 서버로 효율적으로 전달하여 서버 부하를 방지함. |
| **REQ-AVA-01** | 가용성 | **데이터 정기 백업 시스템** | 웹 소스코드, 설정 파일, 데이터베이스 등 주요 자산에 대한 정기적인 백업 스케줄을 생성하여 데이터 유실에 대비함. |
| **REQ-AVA-02** | 가용성 | **독립형 백업 서버 운영** | 메인 서버와 물리적/논리적으로 분리된 별도의 백업 저장소를 운영하여 하드웨어 장애 시 복구 불가능한 상황을 방지함. |
| **REQ-MAN-01** | 관리 | **확장 가능한 인프라 구조** | 향후 법인 규모 확대 및 직원 증가에 대비하여 새로운 서버(Node) 추가가 용이한 유연한 구조로 설계함. |
| **REQ-MAN-02** | 관리 | **SNMP기반 서버 자원 성능 모니터링 (Cacti)** | Cacti를 통해 각 서버(C&C, DNS, DBMS 등)의 CPU, 메모리, 디스크 사용률 등 하드웨어 자원 상태를 그래프 형태로 기록 및 모니터링 |
| **REQ-MAN-03** | 관리 | **SNMP 기반 실시간 네트워크 관제 (MRTG)** | SNMP 프로토콜을 활용하여 네트워크 인터페이스의 트래픽 유입/유출량을 실시간으로 모니터링하고 시각화하여 네트워크 병목 현상을 사전에 파악함. |
| **REQ-SEC-01** | 보안 | **DNS 서버를 통한 IP 보호** | 실제 웹 서버의 공인 IP 노출을 최소화하고, 도메인 기반의 접속 환경을 구축하여 직접적인 서버 공격 위협을 감소시킴. |
| **REQ-SEC-02** | 보안 | **서비스 망 분리 및 접근 제어** | 서버별 역할을 분리(분산 구축)하여 특정 서버 침해 시 전체 시스템으로 위협이 확산되는 것을 방지함. |
| **REQ-SEC-3** | 보안 | **SSH 인증키 기반 접속** | 내부 서버 SSH 접근 시 인증키만을 사용하여 접속할 수 있도록 제어 |
| **REQ-SEC-4** | 보안 | **FTP 포트 비활성화 및 SFTP 활성화** | 보안성이 적절치 못한 FTP 포트를 차단하고 SFTP 구축 |
| **REQ-SEC-5** | 보안 | **방화벽 활성화** | 화이트리스트 기반으로 방화벽을 적용하여 내부 관리 서버에 대한 외부 접근을 차단 |
| **REQ-SEC-6** | 보안 | **로그분석 자동화** | 내부 서버에 대한 로그파일을 분석 및 침해에 대한 키워드 추출, 자동화 코드 구축 |

**4.2 서버 제원**

**4.2.1 서버 기술 리스트**

|  |  |  |  |
| --- | --- | --- | --- |
| **구분** | **기술명** | | **상세 설명** |
| **Network** | DNS | | 도메인으로 버추얼호스팅 기술 |
| **Web** | Nginx | | 높은 성능의 웹 서버, 리버스 프록시, 로드 밸런서 역할을 수행하는 소프트웨어 |
| Apache | | 전 세계적으로 가장 널리 사용되는 웹 서버 소프트웨어 |
| Redirect | | 요청에 쓰인 웹 사이트 주소를 다른 주소로 넘겨주는 기술 |
| Rervers Proxy | | 웹 서버에서 다양한 서비스를 앞단에서 보호하고 요청을 효율적으로 분배하는 기술 |
| wordpress | | PHP 기반으로 웹사이트나 블로그를 쉽게 만들고 관리할 수 있다. |
| Joomla | | PHP 기반으로 복잡한 구조의 웹사이트를 만드는 도구 |
| Pydio | | 사용자의 파일을 안전하게 공유 및 동기화할 수 있는 웹 기반 플랫폼 (클라우드 스토리지 솔루션). |
| Owncloud | | 서버에 직접 설치해서 사용하는 오픈소스 공유 플랫폼 |
| **DBMS** | MariaDB | | MySQL에서 파생된 오픈 소스 관계형 데이터베이스 관리 시스템 (RDBMS |
| phpMyAdmin | | 웹 브라우저를 통해 MariaDB/MySQL과 같은 데이터베이스를 GUI로 쉽게 관리할 수 있게 해주는 도구. |
| **Storage** | NFS | | 네트워크를 통해 파일을 공유할 수 있게 해주는 분산 파일 시스템 프로토콜. |
| **Monitoring** | SNMP | MRTG | 네트워크 장비의 트래픽 사용량 등을 실시간으로 수집하여 그래프로 보여주는 모니터링 도구. |
| Cacti | 네트워크 성능 데이터를 수집, 저장, 그래프화하는 강력한 웹 기반 모니터링 솔루션. |
| **Mail** | postpix | | 메일을 전송(발송)하는 역할을 수행하는 가장 널리 사용되는 메일 전송 에이전트 (MTA). |
| dovecot | | 메일을 수신(받음)하고 클라이언트에게 제공하는 IMAP/POP3 서버 소프트웨어. |
| Roundcube | | 웹 관리 패널을 통해 메일을 이용할 수 있습니다. |
| **Security** | SSH 키인증 | | 원격 시스템에 안전하게 접속하여 명령을 실행하기 위한 암호화된 통신 프로토콜 및 인증 절차. |
| IPtables | | 네트워크 트래픽을 제어하는 시스템 방화벽 도구 |
| UFW | | 사용이 간편한 iptables 기반의 리눅스 방화벽 설정 도구. |
| Firewalld | | RHEL 계열에서 주로 사용되며, 동적 방화벽 정책 관리를 제공하는 서비스. |

**4.2.2 서버 제원**

|  |  |  |
| --- | --- | --- |
| **OS** | **ISO** | **수량** |
| **Rocky9** | Rocky-9.4-x86\_64-dvd.iso | 7 |
| **Ubuntu** | ubuntu-24.04-desktop-amd64.iso | 7 |
| **VMWorkStation** | VMware-workstation-full-17.6.1-24319023 | 1 |
| **Security Onion** | Security Onion-16.04.7.3.iso | 5 |
| **Kali Linux 25** | kali-linux-2025.3-installer-amd64.iso | 3 |

**4.2.3 버전 정보**

|  |  |  |
| --- | --- | --- |
| **서비스명** | **버전** | **비고** |
| **Apache** | Apach/2.4.58 | apach2 -v |
| **Nginx** | nginx/1.24.0 (ubuntu) | nginx -v |
| **dns** | 9.11.36 | bind9 -v |
| **nfs** | rocky: nfs-utils-2.5.4-38.el9.x86\_64  ubuntu : 1:2.6.4-3ubuntu5.1 | rocky : rpm -q nfs-utils  dpkg -l | grep nfs-common |
| **phpmyadmin** | 5.2.3 | grep "version" /usr/share/phpMyAdmin/package.json |
| **Mariadb** | mariadb Ver 15.1 Distrib 1.5.27-MariaDB | mariadb -V |
| **Joomla** | 6.0.1 |  |
| **wordpress** | 6.9 | rpm -qa | grep wordpress |
| **ftp** | vsftpd: version 3.0.5 | vsftpd -v |
| **ssh** | rocky : OpenSSH\_8.7p1  ubuntu : OpenSSH\_9.6P1 | sshd -v |
| **Mrtg** |  |  |
| **Cacti** | cacti-1.2.30-2.el9.noarch | rpm -qa | grep cacti |
| **Pydio** | 4.4.16 | /home/pydio/cells version |
| **Owncloud** | array(10,16,0,0) | cat /home/own/version.php |
| **dvwa** | v1.9 | grep -i “v” CHANGELOG.md | head -n 5(dvwa 설치 경로에서) |
| **snmp** | 5.9.1 |  |

**4.2.4 DB 컬럼 정보**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **서비스명** | **버전** | | | **비고** |
| **서버명** | **계정명** | **권한** | **DB명** |  |
| DBMS | dbms | dbms | bs\_dbms |  |
| bs | dvwa | bs\_dvwa |  |
| mails | bs\_mails |  |
| cacti | bs\_cacti |  |
| own | bs\_own |  |
| pydio | bs\_pydio |  |
| wp | bs\_wp |  |
| ,jl | bs\_jl |  |
| admin | admin | admin |  |
| CMS | cms | cms | bs\_wp |  |
| bs\_jl |  |
| CMS | whd | whd | bs\_pydio |  |
| bs\_own |
| WHD | web | web | bs\_dvwa |  |
| MAIL | snmp | snmp | bs\_mails |  |
| SNMP | snmp | snmp | bs\_cacti |  |

**4.2.5 DNS 관리**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **서비스명** | **버전** | | | **비고** |
| **서버명** | **ZONE 파일명** | **SOA** | **레코드타입** | **IN** |
| Pydio | bs.com.zone | pydio.bs.com | A | ns |
| DNS | bs.com.zone | dns.bs.com | A | ns |
| DBSM | bs.com.zone | dbsm.bs.com | A | ns |
| Wordpress | bs.com.zone | wp.bs.com | A | ns |
| Joomla | bs.com.zone | jl.bs.com | A | ns |
| Nginx | bs.com.zone | web.bs.com | A | ns |
| C&C(Server) | bs.com.zone | cnc.bs.com | A | ns |
| Mail | bs.com.zone | mails.bs.com | A | ns |
| Roundcube | bs.com.zone | cube.bs.com | A | ns |
| Cacti | bs.com.zone | cacti.bs.com | A | ns |
| DVWA | bs.com.zone | dvwa.bs.com | A | ns |
| Backup | bs.com.zone | back.bs.com | A | ns |
| OwnCloud | bs.com.zone | own.bs.com | A | ns |
| WebHard | bs.com.zone | whd.bs.com | A | ns |
| WAS | bs.com.zone | cms.bs.com | A | ns |
| client1 | bs.com.zone | cl.bs.com | A | ns |
| client2 | bs.com.zone | cl2.bs.com | A | ns |
| client3 | bs.com.zone | cl3.bs.com | A | ns |
| snmp | bn.com.zone | snmp.bn.com | A | ns |
| C&C(Network) | bn.com.zone | cnc.bn.com | A | ns |
| Kali1 | rd.com.zone | k1.rd.com | A | ns |
| Kali2 | rd.com.zone | k2.rd.com | A | ns |
| Kali3 | rd.com.zone | k3.rd.com | A | ns |
| 라우터1 | kwz.com.zone | R1.kwz.com | A | ns |
| 라우터2 | kwz.com.zone | R2.kwz.com | A | ns |
| 라우터3 | kwz.com.zone | R3.kwz.com | A | ns |
| 라우터4 | kwz.com.zone | R4.kwz.com | A | ns |
| 라우터5 | kwz.com.zone | R5.kwz.com | A | ns |
| 라우터6 | kwz.com.zone | R6.kwz.com | A | ns |
| 라우터7 | kwz.com.zone | R7.kwz.com | A | ns |
| L3스위치1 | kwz.com.zone | L3SW1.kwz.com | A | ns |
| L3스위치2 | kwz.com.zone | L3SW2.kwz.com | A | ns |
| L3스위치3 | kwz.com.zone | L3SW3.kwz.com | A | ns |
| L3스위치4 | kwz.com.zone | L3SW4.kwz.com | A | ns |
| L3스위치5 | kwz.com.zone | L3SW5.kwz.com | A | ns |
| L3스위치6 | kwz.com.zone | L3SW6.kwz.com | A | ns |
| L3스위치7 | kwz.com.zone | L3SW7.kwz.com | A | ns |
| L3스위치8 | kwz.com.zone | L3SW8.kwz.com | A | ns |
| L3스위치9 | kwz.com.zone | L3SW9.kwz.com | A | ns |
| L3스위치10 | kwz.com.zone | L3SW10.kwz.com | A | ns |
| L3스위치13 | kwz.com.zone | L3SW13.kwz.com | A | ns |
| L3스위치14 | kwz.com.zone | L3SW14.kwz.com | A | ns |
| L3스위치15 | kwz.com.zone | L3SW15.kwz.com | A | ns |
| SPSW1 | kwz.com.zone | SPSW1.kwz.com | A | ns |
| SPSW2 | kwz.com.zone | SPSW2.kwz.com | A | ns |
| PSW | kwz.com.zone | PSW.kwz.com | A | ns |
| Securityonion1 | pp.com.zone | ono1.pp.com | A | ns |
| Securityonion2 | pp.com.zone | ono2.pp.com | A | ns |
| Securityonion3 | pp.com.zone | ono3.pp.com | A | ns |
| Securityonion4 | pp.com.zone | ono4.pp.com | A | ns |
| Securityonion5 | pp.com.zone | ono5.pp.com | A | ns |
| C&C(Purple) | pp.com.zone | cnc.pp.com | A | ns |
| Wordpress | tj.com.zone | wp.tj.com | A | ns |
| Joomla | tj.com.zone | jl.tj.com | A | ns |
| pydio | tj.com.zone | pydio.tj.com | A | ns |
| owncloud | tj.com.zone | own.tj.com | A | ns |
| roundcube | tj.com.zone | cube.tj.com | A | ns |
| FTP | tj.com.zone | ftp.tj.com | A | ns |
| VN(취약서버) | tj.com.zone | vn.tj.com | A | ns |
| admin | tj.com.zone | admin.tj.com | A | ns |

**4.3 서버 흐름도**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **서버** | **역할 및 목적** | **주요 연결 대상** |
| **C&C**  **(통합관리)** | 쥬피터 및 SSH를 사용하여 원격으로 서버 제어 | 전체 서버 |
| **Back** | 서비스별 설정파일, 로그 기록 등을 별도의 공간에 저장하여 데이터 보호 및 보안 위협 대응 |  |
| **DNS** | IP대신 도메인을 사용하여 유연한 서버관리, 편의성 제공 | 전체 서버 및 서비스 |
| **DBMS** | 분산구축되어 있는 각 서비스별 데이터 저장 및 관리 | CMS, WHD,MAIL,SNMP |
| **SNMP**  **(모니터링)** | 서버의 상태를 그래프화 하여 데이터 수집 및 상태 모니터링 | 전체 서버 |
| **MAIL** | 메일 전송 및 수신 서버 |  |
| **WHD** | Pydio와 owncloud를 사용하여 파일 공유 및 스토리지 서비스 제공 |  |
| **CMS** | 쉽게 웹사이트를 만들고 디지털 콘텐츠를 발행 및 관리 |  |
| **Kali** | 서비스의 취약점을 분석하여 공격 | 공격 서버 |
| **client** |  |  |
| **onion** | 침임 탑지 시스템 IDS를 사용, 보안 룰 적용 | IDS |

**4.4 서버 구성도**

|  |
| --- |
|  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **구분** | **os** | **도메인** | **적용 기술** | **비고** |
| C&C | Rocky 9.5 | cnc.bs.com | 주피터를 사용하여 코드 실행 및 컨트롤 | 192.168.80.20/24 |
| C&C2 | Rocky 9.5 | cnc.bn.com | 192.168.80.10/24 |
| C&C3 | Ubuntu 24.04.2 | cnc.pp.com | 주피터를 사용하여 원격으로 코드 실행, 코드 결과 DB에 저장 | 192.168.50.10/24 |
| DNS | Rocky 9.5 | dns.bs.com | BIND9 | 192.168.10.10/24 |
| DBMS | Rocky 9.5 | dbms.bs.com | mariadb, phpmyadmin | 192.168.30.10/24 |
| Back | Rocky 9.5 | back.bs.com | nfs로 연결된 폴더를 통해 백업 데이터 저장 | 192.168.40.10/24 |
| Mail | Ubuntu 24.04.2 | post.bs.com | postpix, roundcube, | 192.168.40.10/24 |
| CMS | Ubuntu 24.04.2 | cms.bs.com | wordpress, joomla | 192.168.90.10/24 |
| WHD | Ubuntu 24.04.2 | whd.bs.com | pydio, owncloud | 192.168.20.10/24 |
| Web | Ubuntu 24.04.2 | web.bs.com | nginx reverse proxy apache2 backend | 192.168.90.20/24 |
| SNMP-C | Ubuntu 24.04.2 | snmp.bs.com | cacti | 40.0.0.10/16 |
| SNMP-M | Rocky 9.5  Rocky 9.5 | snmp.bn.com | mrtg | 10.1.80.10/20 |
| Client 1 | Ubuntu 24.04.2 | cl1.bs.com |  | 192.168.70.10/24 |
| Client 2 | Ubuntu 24.04.2 | cl2.bs.com |  | 192.168.60.20/24 |
| Client 3 | Ubuntu 18 | cl3.bs.com |  | 192.168.60.30/24 |
| Onion | Security Onion 16.04.7.3 | ono1.pp.com | 스노트를 사용하여 비정상 트래픽 탐지 및 스구일을 통한 탐지결과 시각화 | 192.168.10.20/24 |
| Onion 2 | Security Onion 16.04.7.3 | ono2.pp.com | 192.168.20.20/24 |
| Onion 3 | Security Onion 16.04.7.3 | ono3.pp.com | 192.168.10.30/24 |
| Onion 4 | Security Onion 16.04.7.3 | ono4.pp.com | 192.168.70.20/24 |
| Onion 5 | Security Onion 16.04.7.3 | ono5.pp.com | 192.168.90.20/24 |
| kali 1 | Kali Linux 25 | kali1.rd.com |  | 192.168.70.30/24 |
| kali 2 | Kali Linux 25 | kali2.rd.com |  | 50.1.1.10/24 |
| kali 3 | Kali Linux 25 | kali3.rd.com |  | 50.1.1.20/24 |
| MSF2 | Ubuntu 8.04 LTS | mf1.rd.com |  | 192.168.90.30/24 |

**4.4.1 ㅇㅇ구역 구성**

|  |
| --- |
|  |
| **기술, 구현목적** |

**4.4.2 ㅇㅇ구역 구성**

|  |
| --- |
|  |
|  |

**4.4.3 ㅇㅇ구역 구성**

|  |
| --- |
|  |
|  |

**4.4.4 ㅇㅇ구역 구성**

|  |
| --- |
|  |
|  |

**4.5 서비스 목적**

**4.5.1 기본 구축**

|  |  |
| --- | --- |
| **서비스명** | **주요 목적 ( 기본값으로 설정할 내용 )** |
| **snmp** | 관리서버가 각 서버에 설치된 snmp 에이전트로부터 시스템 상태 정보를 주기적으로 수집할 수 있도록함.  snmp로 수집된 시스템 정보는 cacti에서 그래프 형태로 시각화되어, 각 서버의 자원 사용 현황을 직관적으로 확인할 수 있음. |
| **cacti** | SNMP와 Cacti 모니터링 도구를 활용하여 여러 서비스 서버의 상태를 통합적으로 감시하는 것을 주요 목적으로 함.  CPU 사용률, 메모리 사용량, 디스크 사용량, 네트워크 트래픽등 각 서비스 서버의 자원 사용 추이를 그래프로 확인함으로 과부하 발생 여부 및 성능 저하 시점을 사전에 파악할 수 있다. 각 서버들을 도메인별로 관리한다. |
| **Apache** | Cacti는 웹 기반 모니터링 도구로, 관리자가 브라우저를 통해 서버 상태를 확인할 수 있도록 웹 인터페이스 환경이 필요함.  이에 따라 Apache 웹 서버와 PHP를 구성하여 Cacti의 웹 UI를 제공하고, 수집된 SNMP 데이터를 그래프 형태로 시각화하여 관리자가 직관적으로 서버 상태를 확인할 수 있도록 하였다 |
| **PHP84** | Cacti 동적 페이지 및 그래프 처리 |
| **NFS** | 각 서버에서 생성되는 로그 파일을 백업 서버로 주기적으로 전송 및 저장함으로써, 중앙 집중식 로그 관리 및 백업 환경을 구축하는 것을 목적으로 한다.  이를 통해 서버 장애 발생 시 로그 데이터 보존, 로그 위·변조 방지, 장애 원인 분석 및 이력 관리가 가능하도록 하였다. |
| **Crontab** | Crontab을 이용하여 매일 00:00시에 수집하며, NFS로 마운트된 백업 서버의 지정된 디렉터리에 규칙에 따라 저장한다. |
| **DNS** | **도메인 공급 및 관리** |
| **WordPress/Joomla** | CMS 서비스 서버 구성 |
| **Roundcube** | 메일 서버 Gui 환경 관리 |
| **apache2** | CMS, 메일 서버 버추얼 호스트 지원 |
| **postfix** | SMTP기반 메일 전송 에이전트 (MTA) |
| **dovecot** | IMAP기반 메일 수신 및 보관 에이전트 (MDA) |

**4.5.2 취약 구축**

|  |  |
| --- | --- |
| **서비스명** | **주요 목적 ( 취약한 보안 설정할 내용 )** |
| **snmp** | 기존에 환경 파일을 rocommunity public 로 설정했기 때문에  모든 호스트에서 snmp로 접근이 가능하다. |
| **cacti** | HTTPS 미적용, 로그인 정보 평문 전송 가능  따라서 패킷 스니핑을 통한 계정 정보가 노출될 위험이 있음.  또한 세션 탈취 위험이 있음. |
| **NFS** | no\_root\_squash로 root 권한 그대로 유지됨  비인가 접근 및 권한 상승 위험이 존재함.  로그 무결성 검증 미구현됨.  로그 파일에 대한 해시 검증이나 변경 감지를 미설정함. |
| **dovecot** | ssl 로그인 해제 |
| **roundcube** | 브루트포스 공격 허용 (로그인 제한 횟수 해제) |
| **mariadb** | 분산구축에 사용되는 bs계정을 허용 ip대역을 ‘%’로 설정하여 모든 ip대역에서 접근가능하도록 설정 |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**4.5.3 보안 구축 (레드팀 공격에 대비하여 어떤 보안적인 구축을 할 것인지 계획)**

|  |  |
| --- | --- |
| **서비스명** | **주요 목적 ( 화이트리스트 기반 보안 설정할 내용 )** |
| **snmp** | rocommunity public <IP>로 설정해서 접근 ip를 제한한다. |
| **cacti** | 기본 admin 계정 비활성화, 역할 기반 사용자 계정 생성  HTTPS 적용, 기본 admin 계정 비활성화 |
| **NFS** | no\_root\_squash 비활성화  이로써 클라이언트 root 권한 제한, 권한 상승 공격 방지  또 back서버의 nfs 서버의 백업 디렉토리 권한을 최소화함.  내부 관리망에서만 nfs 통신 |
| **mariadb** | 각 서비스별 계정을 생성하여 데이터베이스와 매칭을 통해 서비스 관리자만 접근할 수 있도록 별도의 허용 ip를 지정함. |
| **ssh** | 비밀번호 기반 접속을 차단하고 공개키와 개인키를 생성하여 키 인증을 통한 접속 통제 |
| **iptables** | 허용되지 않은 모든 비인가 접속을 차단하고, 특정 관리자 IP 및 필수 서비스 포트만을 개방 |
| **ufw** | ssh, 웹서비스(80, 443) 허용, 특정 ip대역 허용 등 보안 정책 룰 적용 |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**5. 모의해킹**

**5.1 모의해킹 시나리오**

|  |  |
| --- | --- |
|  | 시나리오 1 |
| “퇴사자의 원한: 전산망을 마비시켜 복수하자!!!”  퇴사자 A씨와 고용된 해커는 이전 직장 근처 카페에서 공용 와이파이 및 네트워크 패킷 분석을 통해 내부망에 침투하고 시스템을 파괴하고자 한다. |
| 시나리오 2 |
| “대형 사이트의 개인정보를 가져와서 큰 돈을 벌어보자!!!”  kali씨는 특정 사이트의 고객들의 개인정보를 가져다가 중국에 팔아버리는 방법으로 큰 돈을 벌어보고자 한다. |
| 시나리오 3 |
| “클릭 한번의 참사 : 족보 파일 클릭 한 번에 웹 서버 비자금 통로가 된 대학생”  시험 기간 족보를 탐내던 대학생 R군이 실행한 스크립트 하나가 해커에게 통로를 열어주며, 단순한 개인 정보 유출을 넘어 기업 서버의 DB를 조작해 비자금을 조성하는 거대한 금융 범죄의 시발점이 되는 과정을 재현해 보고자 한다. |

**5.2 적용 기술리스트**

|  |  |  |  |
| --- | --- | --- | --- |
| **분류** | | **기술** | **사용 목적** |
| **Web** | | | |
| 정보수집 | Active | dig | DNS 레코드 조회(A, MX, NS), DNS zone 확인 |
| dnsenum | 서브도메인 / 이메일 / 네임서버 자동 수집 |
| whatweb | apache2나 nginx의 사이트의 정보 수집 |
| 취약점분석 | WebApp | Burp Suite | 요청/응답 가로채기, CSRF/XSS/SQL 테스트 |
| file Inclusion | 사용자가 서버에 파일을 업로드 할 수 있는 기능에서 발생할 수 있는 취약점 확인 |
| File Upload | 웹 애플리케이션이 외부 시스템 명령어를 실행하는 기능에서 발생하는 취약점 확인 |
| OS command Injection | 자바스크립트 코드 실행을 통해 웹 애플리케이션에서 악성 행위를 할 수 있는 취약점 확인 |
| SQL Injection | 공격자가 웹 애플리케이션의 데이터베이스 쿼리에 악성 SQL 코드를 주입할 수 있는지 취약점 확인 |
| XSS | 인코딩이나 정리 없이 브라우저에 랜더링되는 입력으로 html/script 태그를 허용하는 취약점/결함 |
| CSRF | 로그인된 사용자의 권한으로 사용자가 의도하지 않은 요청이 실행 될 수 있는지 검증 |
| SSRF | 서버가 신뢰해서는 안되는 내부 외부 자원으로 요청을 보내도록 조작될 수 있는지 검증 |
| Exploitation | Auth | Hydra | SSH/ FTP / HTTP 로그인시 비번 cracking 및 크리덴셜 brute-force공격 자동화에 사용 |
| 자동화 | request | Python의 Request는 다양한 WEB http요청을 쉽게 다룰 수 있도록 도와주는 모듈 |
| exploit | MITM | Ettercap | MITM공격(ARPSpoofing) / 세션가로채기 |
| Control | Netcat | 포트 스캔, 리버스 / 바인드 쉘, 네트워크 연결 테스트 |
| **network** | | | |
| 탐지 | | Nmap | 포트 스캐닝, OS 식별, 서비스 버전 확인, 네트워크 자산 조사 |
| 분석 | | Wireshark | 패킷분석, 트래픽 조사, 프로토콜 분석 |
| 네크워크 공격 및 포로토콜 조작 | | scapy | 킷생성, 스니핑, 분석, 스푸핑 가능한 python기반 프레임워크 |
| **DB** | | | |
| 정보수집 / 배너 파악 | | netcat/  telnet | TCP/UDP 원시(Raw) 연결  DB 서비스가 실제로 살아있는지 확인하고, 연결 시 출력되는 배너 정보(버전 등)를 획득 |
| SQL Injection /  취약점 분석 | | Burp Suite | 수동 SQL injection  자동보다 수동으로 정교한 공격시 사용 |
| DB 계정 크랙 | | Hydra | 사전 대입 자동화 공격시 사용  SQL/Postgres/MSSQL 계정 크랙 |

**5.3 모의해킹 구현 상세**

|  |  |  |
| --- | --- | --- |
| **시나리오 1 구현 상세** | | |
| **환경** | | |
|  | | |
| **시스템 구성** | | |
| 장비 | 운영체제 | 패키지 |
| 관리자 PC | Ubuntu(GUI) | ftp, ssh |
| 해커 PC | Kali | 기본구성 |
| DNS 서버 | Rocky | bind, bind-utils |
| 주요서버(FTP, WEB) | Ubuntu | vsftpd, nginx, mariadb, netcat-traditional |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **사용도구 및 기술** | | | | |
| Ettercap | ARP Spoofing | | | |
| WireShark | 해커가 패킷을 분석하는 용도로 사용 | | | |
| dig | DNS서버의 zone 파일 탈취를 위해 사용 | | | |
| SQL injection | 주요 서버의 관리자 페이지의 로그인 우회를 위해 사용 | | | |
| Command Injection  (python) | 주요 서버에 웹쉘 파일을 삽입하기 위해 사용 | | | |
| netcat | 주요 서버 리버스 쉘방식으로 원격 조종하기 위해 사용 | | | |

|  |  |  |
| --- | --- | --- |
| **시나리오 2 구현 상세** | | |
| **환경** | | |
|  | | |
| **시스템 구성** | | |
| 장비 | 운영체제 | 패키지 |
| 외부 웹 메인 서버 | Rocky9 | httpd |
| 공격자 PC | Kali | 기본구성 |
| 외부 웹 취약서버 | MSF2 | Apache, PHP,  DVWA(웹) |
| 메일서버 | UbuntuGUI) | Roundcube |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **사용도구 및 기술** | | | | |
| dnsenum | 외부 노출 자산 식별 | | | |
| nmap / NSE | 서비스 및 버전 확인 | | | |
| Burp suite | 인증공격 자동화(Intruder) | | | |
| requests  (pythone) | 인증 우회 후 웹 컨트롤 | | | |

|  |  |  |
| --- | --- | --- |
| **시나리오 3 구현 상세** | | |
| **환경** | | |
|  | | |
| **시스템 구성** | | |
| 장비 | 운영체제 | 패키지 |
| 피해자 PC (학생 R) | UbuntuGUI) 18.4.06 | 기본 구성 |
| 공격자 PC | Kali | 기본 구성 |
| 웹서버(Web) | Ubuntu | nginx, wordpress, netcat-traditonal |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **사용도구 및 기술** | | | | |
| 사회공학기법 | 사람의 심리를 이용해 비밀번호나 정보 등을 속여서 얻는 기법 | | | |
| Brupsuite(proxy) | 웹 트래픽을 가로채서 요청/응답을 분석·조작하는 도구 | | | |
| CSRF | 사용자가 모르게 악의적인 요청을 보내게 만드는 웹 취약점 | | | |
| LFI(Local File Inclusion) | 서버의 로컬 파일을 강제로 불러와 정보 유출을 일으키는 취약점 | | | |
| netcat | 네트워크 연결을 통해 데이터 전송, 포트 확인, 쉘 연결 등에 쓰이는 도구 | | | |
| File Uplaod | 파일 업로드 기능의 취약점을 이용해 악성 파일을 올리는 공격 | | | |
| Webshell | 웹 서버에 업로드해 원격으로 서버를 제어할 수 있는 스크립트 | | | |

**5.4 취약점 분석 체크리스트**

|  |  |  |
| --- | --- | --- |
| **1. 네트워크 보안** | | |
| 점검 항목 | 점검 내용 및 목적 | 비고 |
| ARP 스푸핑 방어 | 동일 서브넷 내에서 MAC 주소 변조를 통한 패킷 가로채기(Sniffing)가 가능한가? | 시나리오 1 |
| DNS Zone Transfer 제한 | dig axfr, dnsenum 등을 통해 내부망 전체 리스트 및 IP 정보가 유출되는가? | 시나리오 1, 2 |
| 인바운드 접근 통제 | 외부에서 SSH(22), FTP(21), DB(3306) 등 관리 포트로 직접 접근이 가능한가? | 시나리오 1 |
| 프록시 설정 통제 | 시스템/브라우저 프록시 설정이 변조되어 트래픽이 외부로 유출될 수 있는가? | 시나리오 3 |
| 전송 데이터 암호화 | HTTP, FTP 등 평문 프로토콜을 사용해 패킷 분석 시 계정 정보가 노출되는가? | 시나리오 1 |
| **2. 서버 및 시스템 보안** | | |
| 점검 항목 | 점검 내용 및 목적 | 비고 |
| 서비스 배너 관리 | 웹 서버(Nginx, Apache), PHP 등의 버전 정보가 노출되어 취약점 공격의 타겟이 되는가? | 시나리오 1, 2 |
| 계정 보안 정책 | Hydra 등 도구를 이용한 무차별 대입(Brute Force) 공격에 견딜 수 있는 복잡한 암호를 사용하는가? | 시나리오 1, 2 |
| 불필요한 서비스 제거 | netcat(nc), telnet 등 공격에 악용될 수 있는 도구가 서버 내에 설치되어 있는가? | 시나리오 1, 3 |
| 로그 무결성 보호 | 공격자가 history -c, echo "" > [로그이름] 등을 통해 접속 로그(Access/Error log)를 삭제할 수 있는가? | 시나리오 1 |
| 리버스 쉘(Reverse Shell) 차단 | 내부 서버에서 외부(공격자)로의 비정상적인 아웃바운드 연결이 허용되는가? | 시나리오 1, 3 |
| **3. 웹 어플리케이션 보안** | | |
| 점검 항목 | 점검 내용 및 목적 | 비고 |
| SQL Injection (인증 우회) | 로그인 폼에 특수문자(' or 1=1#)를 주입하여 인증을 우회할 수 있는가? | 시나리오 1 |
| XSS (Cross-Site Scripting) | URL 파라미터나 게시판에 악성 스크립트를 삽입하여 사용자의 쿠키를 탈취할 수 있는가? | 시나리오 2 |
| CSRF (Cross-Site Request Forgery) | 사용자 모르게 비밀번호 변경 등 악의적인 요청을 강제로 수행하게 할 수 있는가? | 시나리오 3 |
| LFI (Local File Inclusion) | 파라미터 조작(../../etc/passwd)을 통해 서버 내부 파일에 접근 가능한가? | 시나리오 3 |
| OS Command Injection | 시스템 명령어 실행 기능(Ping 등)을 통해 임의 명령어를 실행할 수 있는가? | 시나리오 1 |
| 파일 업로드 취약점 | .php, .jsp 등 실행 권한이 있는 웹쉘(Webshell) 파일을 업로드할 수 있는가? | 시나리오 3 |
| 세션/쿠키 보안 | 쿠키에 HttpOnly, Secure 속성이 없어 스크립트로 세션 ID 탈취가 가능한가? | 시나리오 2, 3 |
| **4. 데이터 베이스 보안** | | |
| 점검 항목 | 점검 내용 및 목적 | 관련 시나리오 |
| SQL Injection  (데이터 유출) | 취약점을 통해 DB 내 고객 정보(이름, 이메일, PW 등) 테이블 전체를 조회할 수 있는가? | 시나리오 2 |
| 데이터 무결성 관리 | 급여 정보, 포인트 등 금전적 가치가 있는 데이터의 미세한 조작(살라미 어택)이 가능한가? | 시나리오 3 |
| DB 접근 권한 분리 | 웹 애플리케이션 계정이 DB의 시스템 설정 파일이나 관리자 권한에 접근 가능한가? | 시나리오 3 |
| 설정 파일 노출 방지 | db설정파일이나 관리자 문서가 웹 경로상에 노출되어 계정 정보가 유출되는가? | 시나리오 3 |
| **5. 사회공학 및 관리적 보안** | | |
| 점검 항목 | 점검 내용 및 목적 | 관련 시나리오 |
| 피싱 대응 체계 | '꿀 족보', '새해 선물' 등 사용자 클릭을 유도하는 피싱 메일/파일에 대한 대응 역량이 있는가? | 시나리오 2, 3 |
| 악성 스크립트 실행 방지 | 사용자가 출처가 불분명한 .sh, .exe 파일을 실행하지 않도록 단말 보안(EDR)이 설정되어 있는가? | 시나리오 3 |

**6. 관제 및 대응**

**6.1 운용 정책**

|  |  |  |
| --- | --- | --- |
| **구분** | **기준** | **수행방안** |
| **기본 운용** | 2026년 주요정보통신  기반시설 수행가이드 | - 자동화 코드로 점검  - 부서별 취합 검검 |
| **시나리오 기반 운용** | 패킷분석(정상/비정상패킷)  로그분석(로그발생 이벤트) | - 이벤트 발생시 정책 보완 적용 |

**6.2 운용 흐름**

|  |
| --- |
|  |

|  |  |  |  |
| --- | --- | --- | --- |
| **단계** | **구분** | **주요 활동 내용** | **목표** |
| 1단계 | 정책 수립 및 자동화 설계 | • 2026년 주정통 가이드 기반 표준 보안 항목 선정  • 기술 진단 항목의 분배 및 자동화 점검 | 점검 표준 가이드라인,  자동 진단 코드 (Code) |
| 2단계 | 위협 분석 및 대응 전략 | • 레드팀 침투 시뮬레이션을 통한 잠재 공격 경로 식별  • 시나리오별 맞춤형 탐지/차단 시그니처 도출  • 침투 테스트 결과 공유 및 부서별 보안 정책 문서화 | 침투 테스트 결과 보고서,  부서별 대응 전략서 |
| 3단계 | 계층별 보안 정책 이행 | [서버] 호스트 기반 차단(iptables) 및 로그 발생 경로 최적화  [네트워크] 토폴로지 분석을 통한 최적 위치 ACL 적용  [시나리오 기반] 정상/비정상 패킷 식별 기준 실무 적용 | 인프라 보안 설정 강화,  패킷/로그 분석 증적 |
| 4단계 | 방어 유효성 검증 | • 적용된 보안 정책 기반의 공격 재연을 통한 탐지 성능 확인  • 서버·네트워크 접점에서의 실질 차단 여부 로그 검증  • 방어 유효성 평가를 통한 최종 보안 표준 수립 | 방어 유효성 검증 결과,  최종 방어 기준점 정의 |
| 5단계 | 지속적 방어 체계 자산화 | • 검증된 탐지 규칙을 상시 관제 정책으로 전환  • 로그 경로, 패킷 식별 정보 등 대응 지식베이스 구축  • 정기 점검 및 사고 대응을 위한 보안 데이터 내재화 | 상시 관제 탐지 룰 (Rule),  보안 위협 지식베이스 DB |

**6.3 보안 기술리스트**

|  |  |  |  |
| --- | --- | --- | --- |
| **구분** | **기능** | **주요 기술 요소** | **상세 설명** |
| **관제** | 통합 보안 관제 | Security Onion | IDS, 로그 관리, 트래픽 분석 기능이 통합된 보안 관제 플랫폼 |
| 침입 탐지 | Snort | 네트워크 패킷 분석 및 공격 패턴 매칭을 통한 실시간 침입 탐지 |
| 이벤트 분석 | Sguil | 탐지된 보안 이벤트의 가시성 확보 및 정밀 분석용 인터페이스 |
| 패킷 분석 | Wireshark | 네트워크 트래픽 상세 분석을 통한 공격 증거 및 통신 경로 검증 |
| **자동화** | 대응 자동화 | Rule 정책 | 공격 시나리오별 탐지를 위한 룰 규칙 자동화 코드 구현 |

**6.4 기술 활용 계획**

|  |  |  |
| --- | --- | --- |
| no. | 사용도구 | 내용 |
| 1 | Security Onion | - Security Onion을 활용한 실시간 통합 관제 체계 수립 및 시각화  - 트래픽 미러링 프로브 및 중앙 로그 수집 서버의 고가용성(HA) 구성 방안 |
| 2 | Snort | Snort 기반의 지능형 침입 탐지 룰셋(Rule-set) 설계 및 튜닝 |
| Sguil | Sguil 연동을 통한 실시간 위협 가시화 및 심층 분석 프로세스 수립 |
| 3 | Wireshark | - Deep Packet Inspection(DPI) 기반의 위협 트래픽 심층 분석 방안  -공격 단계별 네트워크 증적 추출 및 시각화 |
| 4 | python | - 공격 시나리오별 맞춤형 탐지 규칙(Rule-set) 자동화 구현  - 탐지-대응 시퀀스 최적화를 통한 오탐(False Positive) 최소화 |

**6.5 운용상세**

**6.5.1 로그분석 설계**

|  |  |  |  |
| --- | --- | --- | --- |
| 구분 | 분석 항목 | 주요 설계 및  프로세스 내용 | 활용 방안 |
| **공격 자산 및**  **도구 식별** | **행위 로그 추출** | • Kali, Hydra, SQLmap 등 공격 도구 실행 시 발생하는 자체 로그 분석  • 도구별 고유한 공격 패턴 식별 (User-Agent, 리퀘스트 간격 등) | 탐지 시그니처 및 블랙리스트 기반 마련 |
| **추적 데이터 정의** | • 공격자 IP/Port 정보 및 세션 유지 시간 기록 프로세스 수립  • HTTP Request 파라미터(SQLi, LFI 등) 내 특수문자 및 구문 기록 | 공격 근거 확보 및 공격자 프로파일링 |
| **타겟 시스템 별 핵심 로그** | **인프라 로그** | • [Linux/Win] 시나리오 1(SSH Brute Force) 대응을 위한 auth.log,  Security Event Log 집중 수집 | 계정 탈취 및 비인가 접근 탐지 |
| **서비스 로그** | • [Web/DB] 시나리오 2, 3(XSS, CSRF, LFI) 분석을 위한  Access/ Error log 및 DB Audit log 확보 | 웹 취약점 공격 및 데이터 변조 감시 |

**6.5.2 패킷분석**

- Snort & Sguil: 발생된 경보(Alert)와 실제 패킷 데이터 간의 상관관계 분석

- Wireshark: 시나리오 1(ARP Spoofing) 및 시나리오 3(Reverse Shell)의 L7 페이로드 내 공격 구문 심층 식별

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **공격** **단계** | **공격 기법** | **필터 (Wireshark)** | **정상 패킷 패턴** | **비정상(공격)**  **패킷 패턴** | **정상/비정상**  **식별 기준** |
| **정보 수집** | dnsenum | dns.flags.opcode == 5 | 특정 도메인에 대한 단일 질의 | Standard query AXFR 요청 패킷 발생 | 응답 패킷 내 모든 존(Zone) 레코드 포함 여부 |
| **정보 수집** | dig | dns.flags.response == 0 | 일반적인 도메인 이름 해석 요청 | 특정 도메인 반복 쿼리 및 버전 정보 요청 | 동일 도메인 반복 질의 빈도 및 DNS 버전 정보 수집 패턴 |
| **정보 수집** | Nmap | tcp.flags.syn == 1 | 서비스 제공 포트로의 단일 접속 | 수천 개의 포트로 SYN 패킷 대량 전송 | 단시간 내 다수 포트(Multi-port) 접속 시도 |
| **정보수집** | Nmap 스캔 | tcp.flags.syn == 1 | 특정 포트 단일 접속 | 수천 개의 포트로 SYN 전송 | 단시간 내 다수 포트 접속 시도 |
| **망 확장** | DNS Zone Transfer | dns.flags.opcode == 5 | 특정 도메인 단일 질의 | Standard query AXFR 요청 | 응답 내 모든 레코드 포함 여부 |
| **권한 탈취** | SSH Brute Force | tcp.port == 22 | 간헐적 원격 접속 | 초당 수십 회 TCP 연결/해제 | 동일 IP의 인증 시도 횟수 폭증 |
| **초기 침투** | ARP 스푸핑 | arp | IP-MAC 주소 1:1 매칭 | ARP Reply 대량 발생 | 동일 IP에 MAC 주소 지속 변조 |
| **초기 침투** | FTP 패킷 스니핑 | ftp | 암호화된 전송 (식별불가) | ID/PW 평문 노출 | Payload 내 계정 정보 노출 여부 |
| **초기 침투** | WhatWeb | http.user\_agent | 브라우저 기반 요청 | UA 내 'WhatWeb' 포함 | 헤더 내 스캐너 명시 |
| **관리자 획득** | SQL Injection | http.request.uri | 일반적인 파라미터 요청 | SELECT, cat, ; 등 포함 | 요청 데이터 내 DB 예약어 포함 |
| **시스템 파괴** | Cmd Injection | http.request.uri | 정상 URI 경로 호출 | ; , cat , passwd 포함 | 메타문자 기반 OS 명령어 시도 |
| **시스템 파괴** | Reverse Shell | tcp.flags.syn == 1 | 인바운드 서비스 접속 | 비정상 아웃바운드 접속 | 외부 연결 및 쉘 명령어 |
| **최종 파괴** | DoS 공격 | icmp / tcp.flags.syn | 안정적 트래픽 유지 | SYN/ICMP 과다 유입 | PPS가 정상 임계치를 초과 |
| **세션 탈취** | Reflected XSS | http.request.uri | 일반 검색 파라미터 | <script>, cookie | URI 내 인코딩된 스크립트 포함 |
| **계정 침투** | Mail Brute Force | http.request.method=="POST" | 1회성 로그인 요청 | 로그인 POST 집중 | 대량의 401 에러 후 200 발생 |
| **정보 탈취** | Blind Injection | http.request.uri | 일반적인 웹 페이지 파라미터 요청 | union, select 등 예약어 포함 | 특정 IP의 요청 빈도 폭증 및 응답 크기 변화 |
| **미끼 투척** | 악성 쉘 실행 | tcp (외부 IP) | 목적지 직접 통신 | 해커 IP(Proxy) 경유 | 게이트웨이가 비인가 IP로 변경 |
| **권한 오용** | CSRF 공격 | http.referer | 내부 도메인발 호출 | 외부/비어있는 Referer | 외부 주소발 중요 기능 호출 |
| **서버 침투** | LFI 공격 | http.request.uri | 정상 파일 경로 호출 | ../ , /etc/passwd | 상위 디렉토리 접근 패턴 존재 |
|  | File Upload | http.request.method=="POST" | 이미지 데이터 전송 | 파일 내 <?php 포함 | 이미지 시그니처 내 스크립트 포함 |
| **서버 장악** | Reverse Shell | tcp.flags.syn==1 | 외부 접속(Inbound) | 서버발 아웃바운드 | 서버가 비인가 IP로 먼저 연결 |
| **금전 이득** | Salami Attack | mysql / tcp.port==3306 | 정상 트랜잭션 쿼리 | 소액 UPDATE 반복 | 미세 금액 조작 쿼리 임계치 초과 |
| **미끼 투척** | 악성 쉘 실행 | tcp  (외부 IP) | 목적지 직접 통신 | 해커 IP(Proxy) 경유 | 게이트웨이가 비인가 IP로 변경 |
| **권한 오용** | CSRF 공격 | http.referer | 내부 도메인발 호출 | 외부/비어있는 Referer | 외부 주소발 중요 기능 호출 |
| **서버 침투** | LFI 공격 | http.request.uri | 정상 파일 경로 호출 | ../ , /etc/passwd | 상위 디렉토리 접근 패턴 존재 |
| File Upload | http.request.method=="POST" | 이미지 데이터 전송 | 파일 내 <?php 포함 | 이미지 시그니처 내 스크립트 포함 |
| **서버 장악** | Reverse Shell | tcp.flags.syn==1 | 외부 접속(Inbound) | 서버발 아웃바운드 | 서버가 비인가 IP로 먼저 연결 |
| **금전 이득** | Salami Attack | mysql / tcp.port==3306 | 정상 트랜잭션 쿼리 | 소액 UPDATE 반복 | 미세 금액 조작 쿼리 임계치 초과 |

**6.5.3 Snort 탐지 정책 설계 및 자동화 전략**

1) 탐지 정책 식별 체계 (SID 명명 규칙) 수립

- 룰 번호만으로 공격 유형(정찰, DoS, 웹 등)을 즉시 식별하여 관제 요원의 직관적인 대응 지원

- 임의의 번호가 아닌, 내부 표준 아키텍처를 기반으로 룰을 계층화하여 관리 효율성 극대화

- SID 구조 : 2 + XX + YY + ZZ (고유 식별자 + 대분류 + 중분류 + 순번)

2) 공격 유형별 탐지 범위 및 분류 체계

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **대분류(XX)** | **공격 유형** | **중분류(YY)** | **탐지 목표 및 내용** | **공격 기술 (룰)** |
| **1** | 정보 수집 (염탐/정찰) | 01 스텔스/ 특수 스캔 | Nmap 등 도구의 특수 옵션을 사용하여 방화벽을 우회하거나 몰래 스캔하는 행위 식별 | Null Scan,  Xmas Scan |
| 02 일반/스크립트 스캔 | 핑(Ping)을 무시하거나 스크립트 엔진(NSE)을 사용하여 서버 정보를 수집하는 행위 탐지 | -Pn 스캔,  NSE 스크립트 스캔, DNS Zone Transfer |
| **2** | 서비스 마비  (DoS 공격) | 01 ICMP 과부하 | 패킷 크기를 비정상적으로 키우거나(Large Packet) 대량의 핑을 쏘아 가용성을 저해하는 행위 식별 | ICMP Flood,  Large Packet(-s) |
| 02 트래픽 폭탄 | TCP/UDP 연결을 무한대로 요청하여 시스템 자원을 고갈시키는 공격 탐지 | (TCP·UDP Flood/향후 확장 예정) |
| **3** | 웹 해킹 (사이트 공격) | 01 입력값 변조 | 로그인 창 등에 악성 쿼리나 스크립트를 주입하여 정보를 탈취하거나 인증을 우회하는 행위 식별 | SQL Injection,  XSS  (Cross Site Scripting) |
| 02 명령어 주입 | 웹 서비스를 통해 서버 컴퓨터의 시스템 명령어를 몰래 실행하려는 시도 탐지 | Command Injection,  Reverse Shell Connection |
| 03 경로 탐색 | 허용되지 않은 상위 폴더(../)로 이동하여 시스템 주요 파일을 열람하거나 탈취하려는 행위 식별 | Directory Traversal (../) |
| **4** | 패스워드 공격 (무차별 대입) | 01 SSH 접속 시도 | 관리자 포트(22번) 등 특정 서비스 포트에 패스워드를 반복적으로 대입하여 탈취하려는 행위 탐지 | Hydra  Brute Force Attack |

3) Snort 룰 자동화 프로세스

- 관리자로부터 공격 유형 및 침입 지표 (IP, Port, 패턴 등)를 입력받아 Snort의 local.rules

파일을 실시간으로 업데이트하는 자동화 코드를 설계함

**7. 자동화 코드 관리**

**7.1 코드 흐름도**

**7.1.1 네트워크 코드 흐름도**

|  |
| --- |
|  |

**7.1.2 서버 코드 흐름도**

|  |
| --- |
|  |

**7.1.3 모의해킹 코드 흐름도**

|  |
| --- |
|  |

**7.1.4 관제 및 대응 코드 흐름도**

|  |
| --- |
|  |

**7.1.5 주요정보통신시설 기반 코드 흐름도**

|  |
| --- |
|  |

**7.2 함수정의서**

**7.2.1 네트워크 함수정의서**

|  |  |
| --- | --- |
| **목적** | **G-03 목표(Python 스크립트로 L3 라우팅/L2 VLAN 자동화) 달성** |
| **특징** | **SSH 원격 접속, 인터랙티브 메뉴, 오류 처리, 설정 저장 지원** |
| **사용 환경** | **Management & Backup Zone (JUPYTER 서버)** |

|  |  |  |
| --- | --- | --- |
| **분류** | **함수명** | **기술 설명** |
| **기본함수** | **get\_all\_device()** | 장비 관리파일에 등록된 장비별 list를 생성하여 전체 장비리스트(이중리스트 형태)를 반환하는 함수  -device\_file : 장비관리파일  -device\_all : 전체 장비리스트 |
| **gen\_dir()** | 트리구조로 폴더를 생성하는 함수  -name : 하위에 생성하는 폴더의 이름리스트  -group : 상위폴더 이름  -path : 상위폴더가 위치할 절대경로 |
| **Ping 점검** | **extractiplist()** | 모든 IP정보 및 접속 정보를 가져오는 함수  -files : 전체 장비 목록을 저장하는 파일  -iplist : 전체 장비의 ip리스트 |
| **PingTest(iplist)** | 핑을 보내는 함수  -iplist : 각 장치의 ip, id, pwd 정보 리스트  -errmachines : 핑 결과가 에러나는 장비리스트 |
| **sshrun(user, pwd, ip, cmd)** | ssh 연결 및 명령어 전달 함수 |
| **errorReport(errmachines)** | 수집된 에러가 있는 장치들을 출력하는 함수  -errmachines : ping 통신이 되지 않는 장치들 목록 |
| **ping()** | 전체적인 ping 점검 및 에러있는 ip리스트 반환  위의 세부함수들을 호출하여 실행 함수 |
| **각 장치 설정 정보 출력 프로그램** | **popErrMachines(errmachines, sshinfo)** | ssh정보 리스트에서 에러난 장치를 제외시키는 함수 |
| **sshrun(user, pwd, ip, cmd)** | ssh로 명령어를 실행하는 함수  -user : 사용자 계정  -pwd : 비밀번호  -ip : 접속 IP 번호  -cmd : 실행할 명령어 |
| **extractsshinfo(machine)** | 특정 장치 (라우터, 스위치)의 모든 ssh접속에 필요한 정보 목록을 반환하는 함수  -machine : 장치 구분을 위한 플래그 값 (ex R or SW)  -sshinfo : 장비별 ssh접속정보(ip,id,pwd)를 담은 이중리스트 |
| **showconfigs(sshinfo, flag, machine)** | 모든 장치의 원하는 설정 값을 보여주는 함수  -options : 서비스별 명령어를 매칭시킨 딕셔너리  -sshinfo : ssh 접속을 위한 변수  -flag : 선택한 명령어를 담는 변수(options의 key값)  -machine : 어떤 장치인지를 알려주는 변수 |
| **showMenu(menu)** | 선택한 장비별 메뉴를 출력하는 함수  -menu : 라우터, 스위치 등 네트워크 장비 리스트 |
| **netControl()** | 위의 세부함수들을 호출하여 제어 함수  -errmachines : ping함수 실행 중 에러 발생한 ip주소  -sshinfo : 장비별 ssh 접속정보 담은 리스트  -flag\_menu : 선택한 장비에 대한 제공서비스 리스트  -choose2 : flag\_menu 중 선택한 항목 |

**7.2.2 서버 함수정의서**

- 본 프로젝트에서 Jupyter Notebook과 Paramiko 라이브러리를 활용한 Python 스크립트를 개발하여 서버(LAMP/DNS/DHCP 등)의 설치/설정을 자동화합니다.

|  |  |
| --- | --- |
| **목적** | G-04 목표(본사 서비스 NFS/SMB/FTP/VNC/XRDP 설정 및 동작 테스트) + G-03(Python 자동화) 달성 |
| **특징** | SSH 원격 실행, Expect 자동화(비번 입력), 메뉴 기반 선택 설치, 상태 확인/재시작 |
| **사용 환경** | Management & Backup Zone (JUPYTER 서버) |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **NO** | **스크립트/함수 그룹** | **대상 서버/OS** | **주요 기능 (기획서 연계)** | **입력 예시 (IP/옵션)** | **출력/결과** |
| 1 | init\_ssh + menu | Ubuntu/Rocky9 (Core) | DHCP/Apache/VirtualHost/PHP/phpMyAdmin/FTP/MariaDB 선택/전체 설치 | IP:172.16.16.122, [1-3] | 서비스 활성 + index.html |
| 2 | apa\_in()  apa\_ch\_dir\_in() | Rocky9 (Web EN/KR) | Apache + VirtualHost (team1.com) + DocRoot 변경 | /home/team1 | httpd.conf 수정 + 재시작 |
| 3 | smb\_install()  go() | Rocky9 (Storage) | Samba 설치/공유[/share/smb]/user(smb) 생성 | PW:asd123!@ | smbd/nmbd active |
| 4 | install\_and\_configure()  main() | Ubuntu (MB) | VNC(TigerVNC) + GNOME + xstartup(GNOME-session) | PW:asd123!@, :5901 | vncserver@:1 active |
| 5 | nfs\_install()  main() | Rocky9 (Storage) | NFS utils + /mnt/nfs\_share 공유 + 마운트 | NFS IP:172.16.16.100 | exportfs -v 확인 |
| 6 | download()  main() | Rocky9 (MB-Monitorix) | Monitorix + Perl deps 설치/재시작 | - | systemctl status monitorix |
| 7 | install\_gnome()  main() | Rocky9 (MB) | XRDP + GNOME GUI + user(team1) + 그룹 추가 | user:team1, PW:asd123!@ | xrdp active (RDP:3389) |
| 8 | install()  mod\_zone() | Rocky9 (DNS Server) | BIND + team1.com zone + 동적 A 레코드 편집 | dns\_data.txt 입력 | nslookup team1.com 성공 |
| 9 | format\_partition()  main() | Ubuntu (ST-R5/10) | Partition/FMT/ext4 + fstab + Disk Quota(team1) | /dev/sda1, /jupyter | repquota 제한 확인 |
| 10 | cc(cmd) | 모든 서버 | SSH 명령 실행 + 출력 파싱/오류 처리 | 임의 cmd | stdout/stderr 실시간 출력 |

**7.2.3 모의해킹 함수정의서**

|  |  |
| --- | --- |
| **목적** | 자동화 공격을 통한 효율적인 취약점 분석 |
| **특징** | SSH 원격 실행, 공격자동화, 메뉴기반의 선택적 사용 |
| **사용 환경** | Kali Linux |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **NO** | **그룹** | **함수명** | **주요 기능 (기획서 연계)** | **입력 값 (IP/옵션)** | **출력/결과** |
| 1 | Main | menu()  menu\_q() | kali에서 사용할 기능들 선택 항목 출력 및 선택 | 진행 항목 번호 | 진행할 항목의 기능들 출력 |
| gatheringInfo()  vulnerabilityAnalysis()  attack() | 정보수집/취약점분석/공격의 각 기능들 출력 및 선택 | 사용할 기능 번호 | 선택한 기능의 .ipynb 실행 |
| 2 | nmap | nmap\_start() | nmap main 실행부  nmap 실행 | 원격서버 실행 여부 | nmap 실행 결과 |
| collect\_target\_and\_port()  parse\_targets()  parse\_ports() | 타겟/포트 파싱 | (raw\_target)  (raw\_port)  ip/범위/파일명/포트 | 타겟 정보 |
| select\_nmap\_options()  print\_nmap\_menu() | nmap 옵션 출력 | (menu)  옵션 선택 | 선택된 옵션 |
| build\_final\_command() | command 명령어 조립 | (flags, target\_kind, target\_value, port\_token) | 최종 명령어 |
| 3 | SQL Injection | main()  \_\_init\_\_() | main 실행부  진행할 서비스 목록 출력  생성자 메서드 | 서비스 번호 | 서비스 목록 출력 및 기능실행 |
| getDBs()  getTables()  getColumns()  getDatas() | SQLInjection 기능들  - DB목록 탈취  - 특정 DB의 table목록 탈취  - 특정 table의 열 목록, 데이터 값 탈취 | 공격url 및 쿠키  (dbName) | 탈취한 데이터 |
| decryption() | 데이터 복호화 메서드 | 복호화 할 파일 경로 | 복호화한 데이터 |
| preprocess() | url, param, cookie를 초기화 | 타겟 url, 쿠키값 | 쿠키 초기화 |
| checkInjection() | Injection 취약 여부 사이트인지 확인 | 타겟 url, 쿠키값 | 취약점 존재 여부 |
| basicSQL() | Blind Injection을 제외한 나머지 SQL Injection 기법으로 데이터를 추출 | (sql)  requestGET() | 탈취한 데이터 |
| requestGET() | GET 요청 메서드 | 타겟 url, 쿠키값 | reply |
| printInformation()  saveData() | 탈취한 정보 값을 화면에 출력 및 저장 | (info, typ)  (data)  저장 여부 | 탈취한 데이터 |
| 4 | Command  Injection | main()  \_\_init\_\_() | main 실행부  필수 속성들 선언 및 초기화 | 취약점분석/공격 선택 | 서비스 목록 출력 및 기능실행 |
| gatherInfo()  injection() | ping 테스트 및 명령 실행 가능 여부 등 확인  command injection 공격 실행 | requestData()  요청 결과 | 탈취한 데이터 |
| preprocess() | url 및 cookie 값 초기화 | 타겟 url, 쿠키값, 공격 코드 파일 위치 | 쿠키 초기화 |
| requestData() | POST 요청 및 응답 값 반환 | (insertData) | 요청 결과 |
| saveInfo() | 탈취한 정보를 파일로 저장 | (flag, data) | 데이터 저장 결과 |
| 5 | hydra | \_\_init\_\_() | 결과 저장 리스트 및 파일 정의 | None | None |
| start\_attack() | hydra 전체적인 메인 함수  공격 실행 | 타겟 ip, 이용방식 | 결과 데이터 |  |
| 6 | requests | requests\_get() | request GET 방식 | url, 쿠키, 키워드 | url 및 상태 |
| requests\_post() | request POST 방식 | url, id/pw, 쿠키 | url,상태 및 전송 데이터 |  |

**7.2.4 관제 및 대응부분 함수정의서**

- 입력받은 snort rule 옵션을 바탕으로 snort rule을 자동으로 작성하고, snort rule을 구분하기 위한 값인 sid값을 자동으로 배분한다. 룰을 작성한 이후 문법을 검증한다.

|  |  |
| --- | --- |
| **목적** | 간편한 snort rule 작성 및 모든 Security Onion 내 snort rule 동기화 |
| **특징** | 사용자 입력을 통한 snort rule 생성, IDS서버에 snort rule 추가, IDS 서버 내부 명령어를 통한 snort rule 문법 검증 |
| **사용 환경** | Security Onion |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **NO** | **클래스** | **함수명** | **주요 기능 (기획서 연계)** | **입력 예시** | **출력/결과** |
| 1 | Server | init() | 인자값으로 클래스의 변수를 초기화한다. | 서버 ip, ssh id, ssh pw | N/A(해당없음) |
| 2 | ssh() | ssh 접속하여 인자로 받은 명령 실행 | 실행할 명령어 | 실행한 명령어의 결과 반환 |
| 3 | SnortManager | init() | 인자값으로 시작 SID 번호를 설정한다. | 시작 SID 번호 | N/A(해당없음) |
| 4 | create\_rule() | 사용자로부터 입력받아 snort rule 문자열을 생성한다. | 프로토콜, src ip, src port, dst ip, dst port, 탐지 메세지 등 | 생성한 snort rule 문자열 반환 |
| 5 | deploy\_to\_so() | create\_rule()을 통해 만든 문자열을 local.rules 파일 내에 추가하고 문법을 검증한다. | N/A(해당없음) | 문법 적용 결과(적용 성공 or 실패) 출력 |

**7.2.5 주요정보통신시설 기반 함수정의서**

- 서버 목록(Inventory) DB를 기반으로 주정통 항목을 자동 점검하고, 결과를 DB/웹으로 가시화할 수 있도록 점검·저장·확장 구조를 정의한다(현재는 CSV 저장까지 구현)

|  |  |
| --- | --- |
| **목적** | 주정통 취약점 진단 항목(U/W/WEB/S/N) 자동 점검 및 결과 리포팅을 통해 운영 효율과 보안 설정 준수 확인을 달성한다. |
| **특징** | 0/1/2 자동 판정, 증거(detail) 로그 수집, host+code 기준 최신 결과 유지(upsert), host\_memo(서버 역할) 기록으로 DB 적재/웹 가시화 연동을 용이하게 한다. |
| **사용 환경** | 진단 대상: Linux/Unix/Windows, WEB/WAS 및 보안/네트워크 장비(세션 01~05). 실행 환경: 관리자() 서버에서 Jupyter 또는 CLI로 실행. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **NO** | **스크립트/함수 그룹** | **대상 서버/OS** | **주요 기능 (기획서 연계)** | **입력 예시 (IP/옵션)** | **출력/결과** |
| 1 | \_index/items.json (+ items.csv) / INDEX.md | 모든 대상 서버 | 주정통 전체 항목 인덱스(코드/영역/분류/중요도/페이지)를 기준 데이터로 제공(마스터/CSV 실행 시 참조) | items.json(코드 목록), items.csv(엑셀 공유용), INDEX.md(경로 인덱스) | 항목 메타데이터 로드 및 세션별 필터링 기반 제공 |
| 2 | Server.connect()/close() + \_\_enter\_\_/\_\_exit\_\_ | 모든 대상 서버 | SSH 세션 수립/종료를 표준화하고 with 문으로 안전하게 자원 정리(점검 연속 실행 시 연결 관리) | with Server(host, '', user, pw, port=22, timeout=10) as server: ... | 연결/해제 자동 처리(예외 발생 시에도 close 보장) |
| 3 | Server.ssh\_str() / Server.ssh() | 모든 대상 서버 | 원격 명령 실행 및 출력 수집. ssh()는 2025 스타일 호환(stdout 객체), ssh\_str()는 문자열 반환(utf-8 decode, strip). | server.ssh\_str('id') / server.ssh('cat /etc/os-release') | stdout 문자열/파일 객체 반환(증거(detail)로 저장 가능) |
| 4 | Server.detect\_os() | Linux/Unix 서버 | os-release 기반 OS 식별(ID=)로 점검 분기/메타 기록에 활용(미탐 시 unknown) | /etc/os-release | server.os='ubuntu'|'rocky'|'unknown' 등 |
| 5 | MASTER 템플릿: find\_root() + sys.path 보정 | Jupyter Notebook | 실행 위치가 달라도 server.py/\_index/items.json를 찾도록 루트 탐색 후 import 경로 자동 보정 | Jupyter 실행 위치(2026 주정통 코드 정리 내부/하위) | ROOT 자동 결정 + 모듈 import 안정화 |
| 6 | MASTER 템플릿: importlib.reload(\_tools.run\_checks\_csv) | Jupyter Notebook | 노트북 재실행 시 모듈 캐시로 인한 함수 시그니처 불일치(예: host\_memo) 방지 목적의 강제 reload | import importlib; import \_tools.run\_checks\_csv as m; importlib.reload(m) | 최신 코드 기준으로 실행(캐시로 인한 TypeError 예방) |
| 7 | MASTER\_01~05 + parse\_selection() | Jupyter Notebook | 세션별 항목 리스트 표시 및 다중 선택(all/1,2/범위/코드), host\_memo 입력 | 선택: all 또는 U-01,U-02 / memo: '웹서버' | 선택 항목 순차 점검 실행 + results.csv 갱신 |
| 8 | MASTER 입력: host\_memo(서버 용도/역할 태깅) | 모든 세션(01~05) 공통 | 웹서버/DNS/DB/보안장비/관제 등 서버 용도를 메모로 기록하여 결과(행 단위)에 함께 저장 | host memo: '웹서버', 'DNS', 'Security Onion' 등 | results.csv 컬럼 host\_memo에 저장(추후 DB/웹 가시화 필터링에 활용) |
| 9 | \_tools/run\_checks\_csv.py::CSV\_FIELDS + RESULT\_LABEL | CLI/Jupyter | 결과 스키마(컬럼)와 0/1/2 라벨 매핑을 표준화하여 CSV/DB 적재 시 스키마 일관성 유지 | CSV\_FIELDS=[host,host\_memo,code,result,...], RESULT\_LABEL={0:'양호',...} | 결과 테이블(또는 CSV) 컬럼/라벨 표준 확정 |
| 10 | \_tools/run\_checks\_csv.py::\_load\_index() | CLI/Jupyter | items.json을 code→meta 맵으로 로드하여 결과에 domain/section/category/title/importance를 함께 기록 | \_index/items.json | index[code] 메타데이터 제공(결과 row enrichment) |
| 11 | \_tools/run\_checks\_csv.py::\_dedupe\_keep\_order() | CLI/Jupyter | 사용자 선택 순서를 유지하면서 중복 코드를 제거(동일 항목 중복 점검 방지) | ['U-01','U-01','U-02'] | ['U-01','U-02'] |
| 12 | \_tools/run\_checks\_csv.py::run\_checks\_to\_csv() | CLI/Jupyter | 선택 코드 순차 점검, 0/1/2 판정, detail(증거) 수집, host+code 최신 덮어쓰기(upsert), updated\_at 기록 | --host 192.168.0.10 --host-memo '웹' --codes U-01,U-02 | \_results/results.csv 생성/갱신(추후 MariaDB 적재/웹 가시화 연동 용이) |
| 13 | \_tools/run\_checks\_csv.py::\_parse\_codes() | CLI/Jupyter | 콤마 목록(--codes) 또는 파일(--codes-file) 기반으로 점검 코드 리스트 구성(중복 제거, 대문자 통일) | --codes U-01,U-02 또는 --codes-file my\_codes.txt | codes=[...] 확정(선택한 항목만 연속 점검) |
| 14 | \_tools/run\_checks\_csv.py::\_host\_id() | CLI/Jupyter | upsert 키(호스트 식별자) 생성: 22면 host, 아니면 host:port | host=192.168.0.10, port=22 / port=2222 | host\_id='192.168.0.10' 또는 '192.168.0.10:2222' |
| 15 | \_tools/run\_checks\_csv.py::\_read\_existing\_csv() + \_write\_csv() | CLI/Jupyter | 기존 결과를 읽고(host+code) 최신 결과로 덮어써서 저장(최신만 유지). 스키마: host\_memo 포함 | \_results/results.csv | CSV upsert 저장(중복 누적 없이 최신 결과만 남김) |
| 16 | \_tools/run\_checks\_csv.py::detail 캡처(redirect\_stdout) + \_escape\_one\_line() | CLI/Jupyter | 각 항목 점검 중 출력(print)을 증거(detail)로 캡처하고, 줄바꿈을 \n으로 이스케이프하여 1행=1결과 유지 | checks 모듈의 print 출력 | CSV detail 컬럼에 증거 저장(MariaDB LOAD DATA 적재 친화) |
| 17 | \_tools/run\_checks\_csv.py::\_run\_one() (U/W/WEB/S/N 라우팅) | CLI/Jupyter | 코드 prefix별 checks 모듈로 분기하여 해당 run(code, server)를 호출 | U-01 / W-01 / WEB-01 / S-01 / N-01 | 각 도메인 점검 로직 실행 및 0/1/2 반환 |
| 18 | checks.<domain>.run() 공통 패턴 + CHECKS 레지스트리 | 세션 01~05 공통(U/W/WEB/S/N) | 코드→함수 맵(CHECKS)에서 함수 선택 후 실행, 미구현/예외는 2로 처리하여 배치 점검을 중단하지 않음 | run('U-01', server) / CHECKS['U-01'](server) | 0/1/2 반환 + verbose 시 원인/가이드 출력 |
| 19 | checks.unix 공통 유틸(\_cmd/\_read/\_exists/\_config\_value/권한 파싱) | Linux/Unix | 원격 명령 실행 래퍼, 파일 존재/읽기, 설정값 추출, stat/ls 기반 권한·소유자 판별, 서비스/포트/프로세스 확인 등 재사용 유틸 제공 | /etc/ssh/sshd\_config, stat/ls, systemctl, ss/netstat 등 | 점검 함수의 공통 판정 근거/증거 출력 표준화 |
| 20 | checks.unix.run() + CHECKS(U-xx) | Linux/Unix 서버(Ubuntu/Rocky 등) | 계정/파일권한/서비스/패치/로그 등 U-xx 자동 점검(증거 출력 + 0/1/2 반환) | /etc/ssh/sshd\_config, /etc/passwd 등(원격 명령 기반) | 0=양호 / 1=취약 / 2=수동확인·점검실패 |
| 21 | checks.windows 공통 유틸(\_ps\_json/\_secpol\_values/\_reg\_get/\_resolve\_sids) | Windows Server(OpenSSH) | PowerShell EncodedCommand 실행, JSON 추출/파싱, 로컬 보안정책(secedit export) 캐시, 레지스트리 조회, SID→계정명 변환 등 재사용 유틸 제공 | secedit /export, HKLM 레지스트리 경로, SID 목록 등 | 정책/계정/감사 설정값을 안정적으로 수집(점검 함수에서 재사용) |
| 22 | checks.windows.\_ps(EncodedCommand) + run() + CHECKS(W-xx) | Windows Server(OpenSSH) | PowerShell(EncodedCommand) 기반 정책/레지스트리/서비스 자동 점검(증거 출력 + 0/1/2 반환) | secedit export, registry query, service status 등 | 0/1/2 + 증거(detail) 출력 |
| 23 | checks.web 공통 유틸(\_nginx\_dirs/\_grep/\_curl\_head/\_header\_value/권한 파싱) | WEB/WAS 서버 | 웹서버 설정 디렉터리 탐색, grep 기반 설정 검색, curl -I 헤더 수집 및 보안 헤더 추출, 파일 권한 판별 등 재사용 유틸 제공 | /etc/nginx,/etc/apache2,/etc/httpd, curl -I http://127.0.0.1 등 | 웹 설정/헤더 기반 자동판정 근거 제공(다중 웹서버 공존 시 결과 합산) |
| 24 | checks.web.run() + CHECKS(WEB-xx) | WEB/WAS 서버(nginx/apache/tomcat 등) | 웹 서비스 설정/헤더/SSL/로그권한 등 자동 점검(가능한 항목은 자동판정, 불가 항목은 수동확인) | curl -I http://127.0.0.1, /etc/nginx/\*, /etc/httpd/\* 등 | 0/1/2 + 증거 출력 |
| 25 | checks.security.\_manual() (수동확인 템플릿) | 보안 장비 | 장비별 상이한 UI/CLI를 고려해 '확인 포인트'를 표준 포맷으로 출력(현재는 2 반환, 추후 자동화 확장 지점) | 정책/로그/펌웨어/계정 설정 화면 또는 CLI 출력 | 수동 점검 체크리스트 출력 + 2 반환 |
| 26 | checks.security.run() + CHECKS(S-xx) | 보안 장비(방화벽/VPN/IPS/WAF 등) | 장비 계정/접근통제/로그/정책 항목 점검(현재 수동 확인 템플릿 기반) | 장비 설정 메뉴/CLI/관제 로그 기준으로 확인 | 2(수동확인) + 체크리스트 출력(자동판정 확장 예정) |
| 27 | checks.network.\_manual() (수동확인 템플릿) | 네트워크 장비 | 벤더/OS별 명령 차이를 고려해 '확인 포인트/예시 명령'을 표준 포맷으로 출력(현재는 2 반환) | show running-config / line vty / snmp 설정 등 | 수동 점검 체크리스트 출력 + 2 반환 |
| 28 | checks.network.run() + CHECKS(N-xx) | 네트워크 장비(라우터/스위치 등) | VTY/ACL/SNMP/불필요 서비스 차단 등 설정 점검(현재 수동 확인 템플릿 기반) | show running-config / line vty / snmp 설정 등 | 2(수동확인) + 체크리스트 출력(자동판정 확장 예정) |

**8. 테스트 및 검증계획**

**8.1 네트워크 테스트**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **분야** | **테스트 ID** | **테스트 케이스** | | **확인 방법** | **수행결과** |
| **네트워크** | **NT-01-a** | 로드밸런싱, Summary routing | | ping test |  |
|  |  | |  |  |
| **NT-01-b** | Static/Default Route traceroute | | wire shake 활용하여 로드밸런싱 양측 옆 지대를 비교 확인 |  |
| **NT-01-c** | Frame-Relay - R2,R3,R4를 Multi Point로 설정 | | ping test |  |
| **NT-01-d** | PAT | | 사설망 → 외부망 접속 가능 증적  외부망 → 사설망 접속 불가 증적 |  |
| **NT-02-a** | VLAN10~50 구분 (PC 11대) | | 같은 VLAN ping 통신 |  |
| **NT-02-b** | PVST+ 로드 밸런싱 구현 | | VLAN40, VLAN50 트래픽 다른 경로로 이동하여 PVST+ 기반 로드밸런싱 성공 |  |
| **NT-02-c** | inter-VLAN (PC 7대) | | VLAN10~30 ping 통신 |  |
| **NT-02-d** | 스위치 S10~12 VTP 활용 | | Server 기준으로 VLAN 정보 자동 동기화 (S11(Transparent) 제외) |  |

**8.2 서버 구축 테스트**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **분야** | **테스트 ID** | **테스트 케이스** | | **확인** | **수행결과** |
| **서버** | **bs-web-01** | ssh서비스 동작 확인(active) | | systemctl status ssh |  |
| **bs-web-02** | root 로그인 허용 여부(허용) | | vim /etc/ssh/sshd\_config  PermitRootLogin yes |  |
| **bs-web-03** | 방화벽 활성화 : 비활성화 | | ufw status |  |
| **bs-web-04** | dns 확인 | | cat /etc/resolv.conf |  |
| **bs-web-05** | vsftpd 서비스 동작 확인(active) | | systemctl status vsftpd |  |
| **bs-web-06** | ftp 설정 파일 수정 | | vim /etc/vsftpd.conf  anonymous\_enable=yes # 익명 ftp 접속 허용  local\_enable=YES # 시스템에 존재하는 로컬 사용자 계정 로그인 허용  write\_enable=YES # 파일 업로드, 삭제, 수정 허용  local\_umask=022 # ftp로 생성되는 파일/디렉터리 기본 권한 설정(755)  xferlog\_enable=YES # 파일 전송 로그 기록 활성화  connect\_from\_port\_20=YES # active ftp 모드 사용(서버가 20포트로 데이터 연결)  xferlog\_std\_format=YES # ftp 로그를 표준 형식으로 기록  chroot\_local\_user=NO # 로컬 사용자를 홈 디렉터리에 가두지 않음(상위 접근 가능)  userlist\_enable=NO # 모든 로컬 사용자 로그인 가능 |  |
| **bs-web-07** | db 클라이언트 설치 확인 | | mariadb --version |  |
| **bs-web-08** | nginx 동작 확인 | | systemctl status nginx |  |
| **bs-web-09** | nginx 설정 파일 수정 | | vim /etc/nginx/conf.d/vhost.conf  확인항목  dvwa , admin (사이트)  wp, jl, pydio,owncloud,roundcube( 프록시 설정) |  |
| **bs-web-10** | nfs 동작 확인 | | systemctl status nfs-server |  |
| **bs-web-11** | nfs 마운트 확인 | | df  vim /etc/fstab |  |
| **bs-web-13** | php 동작 확인 | | php -v |  |
| **bs-web-14** | db 동작 확인 | | mariadb --version |  |
| **bs-web-15** | db 연결 확인 | | vim /home/dvwa/config/config.inc.php |  |
| **bs-web-16** | dvwa 페이지 접속 확인 | | 터미널에서 확인  curl <http://dvwa.tj.com>  브라우저에서 확인  http://dvwa.tj.com |  |
| **bs-web-17** | snmp 설치 확인 | | systemctl status snmpd |  |
| **bs-whd-01** | ssh 서비스 동작 확인 | | systemctl status ssh |  |
| **bs-whd-02** | root 로그인 허용 여부(허용) | | vim /etc/ssh/sshd\_config  PermitRootLogin yes |  |
| **bs-whd-03** | 방화벽 활성화 여부(비활성화) | | ufw status |  |
| **bs-whd-04** | db 클라이언트 설치 확인 | | mariadb --version |  |
| **bs-whd-05** | apache 동작 확인 | | systemctl status apache2 |  |
| **bs-whd-06** | apache 설정 파일 수정 | | vim /etc/apache2/sites-available/vhost.conf  pydio (리다이렉트)  owncloud |  |
| **bs-whd-07** | apache 동작 확인 | | systemctl status apache2 |  |
| **bs-whd-08** | pydio 동작 확인 | | systemctl status pydio |  |
| **bs-whd-09** | [pydio 포트 및 TLS 확인 | | cd /home/pydio  ./cells configure sites |  |
| **bs-whd-10** | pydio 접속 확인 | | 터미널에서 확인  curl http:/pydio.bs.com  브라우저에서 확인  http://pydio.bs.com |  |
| **bs-whd-11** | php 모듈 확인 | | php7.4 -m | grep -E "mysqli|mysqlnd|gd|curl|zip|mbstring|intl“ |  |
| **bs-whd-12** | owncloud 접속 확인 | | 터미널에서 확인  curl -k <http://own.tj.com>  브라우저에서 확인  http://own.tj.com |  |
| **bs-whd-13** | nfs 동작 확인 | | systemctl status nfs-server |  |
| **bs-whd-14** | nfs 마운트 확인 | | df  vim /etc/fstab |  |
| **bs-whd-15** | snmp 설치 확인 | | systemctl status snmpd |  |
| **bs-cl-01** | x 서버 프로세스 확인 | | ps -e | grep -E "X|gdm|lightdm|sddm"  (아무것도 안나오면 CLI 환경) |  |
| **bs-cl-02** | 설치된 데스크톱 환경 확인 | | dpkg -l | grep ubuntu-desktop |  |
| **bs-cl-03** | 한글 패치 확인 | | dpkg -l | grep language-pack-ko |  |
| **bs-snmp-01** | 초기 설정 SSH 설정 확인 | | /etc/ssh/sshd\_config  40번 : PermitRootLogin yes  65번 : PasswordAuthentication yes |  |
| **bs-snmp-02** | 초기 설정 방화벽 설정 확인 | | /etc/selinux/config  22번 : SELINUX=disabled |  |
| **bs-snmp-03** | db 클라이언트 설치 확인 | | systemctl status mariadb |  |
| **bs-snmp-04** | snmp 서비스 상태 확인 | | systemctl status snmpd |  |
| **bs-snmp-05** | snmp 설정파일 확인 | | /etc/snmp/snmpd.conf  41 #com2sec notConfigUser default public  42 rocommunity public  (41번이 주석처리 되어있고 42번 확인)  74 com2sec local localhost kong  75 com2sec mynetwork 172.16.0.0/16 tj  (원하는 community 와 대역인지 확인하세요.)  78 group MyRWGroup any local  79 group MyROGroup any mynetwork  (주석 풀려있는지 확인)  85 view all included .1 80  (주석 풀려있는지 확인)  93 access MyROGroup "" any noauth 0 all none none  94 access MyRWGroup "" any noauth 0 all all all  (주석 풀려있는지 확인) |  |
| **bs-snmp-06** | cacti 설정파일 확인 | | /etc/my.cnf.d/mariadb-server.cnf  /etc/my.cnf  /etc/cacti/db.php  /etc/httpd/conf.d/cacti.conf  /etc/cron.d/cacti 주석제거 |  |
| **bs-snmp-07** | cacti 브라우저 확인 | | snmp.bs.com/cacti 들어가지는지 확인  php ,db time zone 문제 없이 next로 진행되는지 확인 |  |
| **bs-back-01** | 초기 설정 SSH 설정 확인 | | /etc/ssh/sshd\_config  40번 : PermitRootLogin yes  65번 : PasswordAuthentication yes |  |
| **bs-back-02** | 초기 설정 방화벽 설정 확인 | | /etc/selinux/config  22번 : SELINUX=disabled |  |
| **bs-back-03** | nfs서비스 상태 확인 | | systemctl status nfs-server |  |
| **bs-back-04** | nfs exprot 설정 파일 확인 | | /etc/exports |  |
| **bs-dns-01** | dns 설치,서비스 확인 | | systemctl status named |  |
| **bs-dns-02** | dns zone 설정 확인 | | grep -r "zone" /etc/named\* 2>/dev/null |  |
| **bs-dns-03** | dns 전용 포트 확인 | | netstat -tulpn | grep :53 |  |
| **bs-dns-04** | dns 문법 검사 | | named-checkconf |  |
| **bs-cms-01** | 웹서버 설치,서비스 확인 | | systemctl status apache2 |  |
| **bs-cms-02** | 웹서버 전용 포트 확인 | | netstat -tulpn | grep apache2 |  |
| **bs-cms-03** | 버추얼 호스트 확인 | | cat /etc/apache2/sites-available/000-default.conf |  |
| **bs-cms-04** | wp 설정 파일 확인 | | ls /home/\*/wp-config.php |  |
| **bs-cms-05** | 줌라 설정 파일 확인 | | ls /home/\*/configuration.php |  |
| **bs-cms-06** | 도메인 테스트(wp) | | curl -I http://wp.bs.com |  |
| **bs-cms-07** | 도메인 테스트(jl) | | curl -I http://jl.bs.com |  |
| **bs-mail-01** | postfix 서비스 확인 | | systemctl status postfix |  |
| **bs-mail-02** | dovecot 서비스 확인 | | systemctl status dovecot |  |
| **bs-mail-03** | SMTP 포트 확인 | | netstat -tuln | grep :25 |  |
| **bs-mail-04** | IMAP 포트 확인 | | netstat -tuln | grep :143 |  |
| **bs-mail-05** | postfix 설정 확인 | | cat /etc/postfix/main.cf |  |
| **bs-mail-06** | dovecot 설정 확인 1 | | cat /etc/dovecot/conf.d/10-mail.conf |  |
| **bs-mail-07** | dovecot 설정 확인 2 | | cat /etc/dovecot/conf.d/10-auth.conf |  |
| **bs-mail-08** | dovecot 설정 확인 3 | | cat /etc/dovecot/conf.d/10-ssl.conf |  |
| **bs-mail-09** | roundcube 설치 확인 | | ls -la /etc/roundcube |  |
| **bs-mail-10** | 도메인 테스트(cube) | | curl -I http://cube.bs.com |  |
| **bs-mail-11** | 메일 관리자 권한 확인 | | ls -lR /home/mails |  |
| **bs-mail-12** | 메일 사용자 권한 확인 | | ls -lR /home/client |  |
| **bs-mail-13** |  | |  |  |
| **bs-mail-14** |  | |  |  |
|  |  | |  |  |

**8.3 모의해킹 구현테스트**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **분야** | **테스트 ID** | **테스트 케이스** | **확인 방법** | **수행결과** |
|  | **RD-01-a** | host Scan, target ip 지정 | ettercap을 이용하여 호스트 스캔 후 arp poisoning 실행 |  |
| **RD-01-b** | FTP 패킷 식별 | wireshark 로 패킷 분석 |  |
| **RD-01-c** | 식별된 장치에서 열린 포트 스캔 및 서비스와 운영체제 유형 확인 | nmap의 -sV 옵션을 사용하여 열린 포트 목록, 서비스, 운영체제를 식별 |  |
| **RD-01-d** | 관리자 계정의 접근 정보 획득 가능 여부 확인 | hydra를 이용하여 brute force 실행 |  |
| **RD-01-e** | 도메인 및 서비스 목록 확보를 통한 관리용 페이지 존재 여부 확인 | dig의 axfr 옵션으로 zone파일 탈취 가능 여부 확인, 도메인 정보 확인 후 whatweb으로 관리자 페이지 탐색 |  |
| **RD-01-f** | 관리자 페이지 로그인 접근 가능 여부 확인 | 브라우저를 사용해서 로그인 페이지 접근 가능 여부 확인 |  |
| **RD-01-g** | 관리자 로그인 인증 우회 가능 여부 확인 | [‘, ’ or 1=1 #] 등을 입력하여 SQL Injection 취약점 식별 및 로그인 인증 우회 여부 확인 |  |
| **RD-01-h** | 관리자 Ping 테스트 페이지 취약점 여부 확인 | 입력창에 [IP] && ls -al, ; pwd 등 의 입력 값으로 Ping 테스트 이외의 작업 처리 여부 확인 |  |
| **RD-01-i** | 취약점 점검 프로그램을 활용해서 웹쉘 파일 생성 여부 확인 | Python의 CommandInjection 프로그램 실행 및 검사 결과 확인  - 웹쉘 코드 파일 생성 여부 확인  - /etc/passwd와 같은 주요 정보 유출 확인 |  |
| **RD-01-j** | URL 경로 조작을 통한 특정 파일 실행 가능 여부 확인 | URL 경로를 삽입한 웹쉘 코드 파일로 지정하여 실행 여부 확인 |  |
| **RD-01-k** | 공격자 시스템과 서버 간 지속적인 제어 채널 형성 가능 여부 확인 | 웹쉘을 기반으로 netcat을 활용한 reverse shell 연결 가능 여부 확인 |  |
| **RD-01-l** | 부적절한 권한 할당으로 인한 주요 정보 접근 가능성 여부 확인 및 로그 삭제 가능여부 확인 | ls -al로 주요 정보에 할당된 권한 적합성 확인 및 history, access.log 등 주요 로그 파일에 대한 접근 및 흔적 제거 가능 여부 확인 |  |
| **RD-01-m** | 내부 네트워크 자원에 과부하를 유발하여 시스템 및 서비스 중단 가능 여부 확인 | 대량 트래픽 발생 시 서비스 가용성 저하 및 DoS 영향 여부 확인 |  |
| **RD-02-a** | 외부 공개 도메인 기반 네트워크 정보 노출 여부 | dnsenum을 통한 특정 외부 공개 도메인을 기준으로 검색. 나온 결과로 타겟으로 정할 네트워크 범위 확인 |  |
| **RD-02-b** | 웹 서버 및 서버 측 정보 노출 여부 | 특정 네트워크 범위내에서 nmap(-sS -sV)를 사용하여 각 웹 서버 측 버전 정보 확인 |  |
| **RD-02-c** | 보안 관리 미흡 가능 사이트 식별 및 공격 대상 선정 | Apache 버전이 낮은 서버 중 PHP 정보도 확인하여 구버전 사용 여부 판단 |  |
| **RD-02-d** | 입력값 검증 여부 확인 | DVWA XSS 페이지를 통해 XSS 취약점 발생 가능성 확인 |  |
| **RD-02-e** | 외부 정보 전송 링크 생성 가능 여부 | 스크립트 입력을 통해 사용자 클릭 시 쿠키 정보가 외부로 전송되는 URL 생성 여부 확인 |  |
| **RD-02-f** | 수집 이메일 기반 관리자 계정 접근 가능 여부 | BurpSuite의 Proxy·Intruder·Repeater를 활용하여 메일 시스템 로그인 시도 |  |
| **RD-02-g** | 사회공학 기반 관리자 쿠키 탈취 시도 | 사회공학 기법을 활용하여 다른 관리자에게 쿠키 탈취용 악성 스크립트 링크를 전달 |  |
| **RD-02-h** | 사용자 정보 조회 기능 취약 여부 | 탈취한 세션 쿠키를 Python requests 모듈을 통해 전송하여 로그인 상태 유지 및 권한 접근 가능 여부 검증 |  |
| **RD-02-i** | SQL Injection 취약 여부 | Python requests 모듈을 이용하여 SQL Injection 페이로드를 자동 전송하고,  인증 우회·데이터 조회 등 비정상적인 SQL 실행 여부 확인 |  |
| **RD-03-a** | 학습 자료로 위장한 파일을 통해 사용자 실행 유도 가능 여부 확인 | WordPress 게시물에 첨부된 파일을 사용자가 다운로드 및 실행하는지 여부 확인 |  |
| **RD-03-b** | 사용자 PC의 네트워크 통신 경로를 공격자 시스템을 거치도록 변경 | Burp Suite 기반 사용자 트래픽 경유 여부 확인 |  |
| **RD-03-c** | 사용자 웹 트래픽을 경유시켜 로그인 인증 정보 노출 여부 확인 | Burp Suite 프록시를 통한 로그인 트래픽 확인 |  |
| **RD-03-d** | 인증 정보를 이용한 계정 권한 변경 가능 여부 확인 | Burp Suite에서 인증된 요청(Request) 조작 가능 여부 확인 |  |
| **RD-03-e** | 로그인 후 시스템 페이지 구조 및 입력값 처리 방식 확인 | Burp Suite 프록시를 통해 페이지 요청 및 입력값 흐름 확인 |  |
| **RD-03-f** | URL 입력값을 통해 서버 내부 파일 접근 가능 여부 확인 | requests를 이용해 URL 파라미터 전달 시 내부 파일 참조 가능 여부 확인 |  |
| **RD-03-g** | 서버 제어용 파일 업로드 가능 여부 | netcat(nc)을 활용한 서버 제어용 파일 업로드 및 동작 여부 확인 |  |
| **RD-03-i** | 업로드 파일 실행을 통한 제어 채널 형성 여부 | netcat 기반 서버 제어 가능 여부 확인 및 파일 탐색 |
| **RD-03-j** | 서버 설정·DB 정보 접근 가능 여부 | netcat 기반 파일 탐색 후 관리자 id로 mail 접속 |  |
| **RD-03-k** | 관리자 메일을 이용한 사용자 대상 메시지 발송 가능 여부 확인 | netcat으로 서버 제어 후 mail 명령을 이용한 공지·이벤트 메시지 발송 여부 확인 |  |
| **RD-03-l** | 공격자 웹서버에 개인정보 수집 여부 확인 | 관리자 메일로 보낸 공지·이벤트 개인정보 수집 여부 확인 |  |
| **RD-03-m** | 위장 페이지를 통한 개인정보 수집 가능 여부 확인 | netcat으로 계정 탐지 후 mariadb 접속 확인 후 DB 저장 여부 확인 |  |
| **RD-03-n** | DB 직접 접근을 통한 금전 정보 변조 가능 여부 확인 | 금전 데이터 변경 여부 확인 |  |

**8.4 관제 및 대응 구현테스트 및 침투테스트**

**8.4.1 관제 및 대응 구현테스트**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **분야** | **테스트 ID** | **테스트 케이스** | **확인 방법** | **수행 결과** |
| 웹 해킹 | PP- WEB-01 | SQL Injection을 통한 관리자 계정 탈취 시도(예: sqlmap, 대상: nginx reverse proxy + apache backend) | WAF/IPS 차단 로그 또는 웹 접근 로그(access.log)에서 공격 패턴 기록 및 경고/차단 여부, SIEM 알람 확인 |  |
| PP- WEB-02 | 파일 업로드 취약점을 이용한 웹셸(Web Shell) 업로드 시도(대상: 업로드 기능/디렉터리) | 웹 서버 error.log/접근 로그에 업로드 시도 기록, 보안관제(Security Onion/Snort) 이벤트 발생 여부 확인 |  |
| PP - WEB-03 | 디렉터리 트래버설(Traversal)로 민감 파일 접근 시도(예: /etc/passwd, 설정 파일) | 웹 접근 로그에서 비정상 URI 패턴 확인, 차단 정책 적용 여부 및 경고(관제/알람) 확인 |  |
| 시스템 해킹 | PP-PT-01 | SSH 서비스 식별 및 접근 시도(Nmap 스캔으로 포트/버전 수집) | auth.log/secure 및 방화벽 로그에서 스캔 패턴 확인, 관제(Security Onion)에서 스캔 탐지 이벤트 확인 |  |
| PP-PT-02 | 무작위 대입(Brute Force)으로 SSH 접속 시도(hydra 등) | 로그인 실패 패턴(auth.log/secure) 누적 확인, 임계치 초과 시 iptables/ufw 차단 적용 여부 확인, 차단 후 재시도 시도 실패 확인 |  |
| PP-PT-03 | root 원격 로그인 시도(정책: PermitRootLogin 제한 및 직접 로그인 차단) | sshd\_config 정책 적용 여부 및 접속 차단 확인, 로그인 실패 로그 및 경고 메시지 기록 확인 |  |
| 네트워크 해킹 | PP-NET-01 | ARP Spoofing으로 내부 구간 MITM 시도(동일 IP에 MAC 주소 지속 변조) | ARP 테이블 변조/게이트웨이 MAC 변경 징후 확인(호스트/스위치), IDS/Snort 경고 및 관제 이벤트 발생 여부 확인 |  |
| PP-NET-02 | FTP 패킷 스니핑으로 계정 정보 노출 여부 확인(평문 전송) | Wireshark 필터(tcp.port==21)로 Payload 내 계정 정보 노출 확인, 정책상 FTP 미사용/대체(SFTP/FTPS) 적용 여부 확인 |  |
| DNS 공격 | PP-DNS-01 | DNS 정보 탈취 시도(예: Zone Transfer(AXFR) 요청, dig) | DNS 서버 로그에서 AXFR/비정상 요청 기록 확인, 접근 통제/차단 여부 확인, 관제 이벤트 발생 여부 확인 |  |
| PP-DNS-01 | DNS 서버 설정 상태 점검 및 정보 노출 여부 확인(재귀/권한 없는 질의 허용 등) | named.conf 등 설정 검토 결과를 증거로 남기고, 보안 정책 기준 충족 여부(양호/취약) 판정 |  |
| DDoS | PP-DOS-01 | SYN Flood/대량 연결 시도(hping3 등)로 서비스 가용성 저하 유발 | 트래픽 모니터링(MRTG 등)에서 급증 탐지, 방화벽/iptables rate-limit 또는 차단 정책 적용 여부 확인, 서비스 영향도 기록 |  |
| PP-DOS-01 | HTTP Flood 또는 Slow 공격(slowloris 등)으로 웹 서비스 자원 고갈 시도 | nginx/apache 접속 로그 및 에러 로그에서 비정상 세션 패턴 확인, 차단/제한(연결수/타임아웃) 정책 적용 여부 확인 |  |
| APT 시나리오 | PP-APT-01 | 내부망 침투 및 시스템 파괴 시나리오(권한 획득 → 내부 이동 → 중요 파일 변경/삭제 시도) | 서버/시스템 로그에서 권한 상승·명령 실행 흔적 확인, 관제(Security Onion/SIEM)에서 이상행위 알람 발생 여부 확인 |  |
| PP-APT-01 | C2 통신/Beaconing 패턴 시뮬레이션(주기적 외부 통신/비정상 도메인 질의 등) | DNS/네트워크 로그에서 주기적 패턴 확인, IDS(Snort) 탐지 룰 매칭 또는 경고 발생 여부 확인 |  |

**9. 주요정보통신기반시설에 근거한 기본관리**

**[점검항목 - 체크리스트]**

**1. Unix 서버 (U-01 ~ U-67)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 항목  코드 | 항목중요도 | 점검항목 | 점검  결과 | 비고 |
| U-01 | 상 | root 계정 원격 접속 제한 |  |  |
| U-02 | 상 | 비밀번호 관리정책 설정 |  |  |
| U-03 | 상 | 계정 잠금 임계값 설정 |  |  |
| U-04 | 상 | 비밀번호 파일 보호 |  |  |
| U-05 | 상 | root 이외의 UID가 '0' 금지 |  |  |
| U-06 | 상 | 사용자 계정 su 기능 제한 |  |  |
| U-07 | 하 | 불필요한 계정 제거 |  |  |
| U-08 | 중 | 관리자 그룹에 최소한의 계정 포함 |  |  |
| U-09 | 하 | 계정이 존재하지 않는 GID 금지 |  |  |
| U-10 | 중 | 동일한 UID 금지 |  |  |
| U-11 | 하 | 사용자 Shell 점검 |  |  |
| U-12 | 하 | 세션 종료 시간 설정 |  |  |
| U-13 | 중 | 안전한 비밀번호 암호화 알고리즘 사용 |  |  |
| U-14 | 상 | root 홈, 패스 디렉터리 권한 및 패스 설정 |  |  |
| U-15 | 상 | 파일 및 디렉터리 소유자 설정 |  |  |
| U-16 | 상 | /etc/passwd 파일 소유자 및 권한 설정 |  |  |
| U-17 | 상 | 시스템 시작 스크립트 권한 설정 |  |  |
| U-18 | 상 | /etc/shadow 파일 소유자 및 권한 설정 |  |  |
| U-19 | 상 | /etc/hosts 파일 소유자 및 권한 설정 |  |  |
| U-20 | 상 | /etc/(x)inetd.conf 파일 소유자 및 권한 설정 |  |  |
| U-21 | 상 | /etc/(r)syslog.conf 파일 소유자 및 권한 설정 |  |  |
| U-22 | 상 | /etc/services 파일 소유자 및 권한 설정 |  |  |
| U-23 | 상 | SUID, SGID, Sticky bit 설정 파일 점검 |  |  |
| U-24 | 상 | 사용자, 시스템 환경변수 파일 소유자 및 권한 설정 |  |  |
| U-25 | 상 | world writable 파일 점검 |  |  |
| U-26 | 상 | /dev에 존재하지 않는 device 파일 점검 |  |  |
| U-27 | 상 | $HOME/.rhosts, hosts.equiv 사용 금지 |  |  |
| U-28 | 상 | 접속 IP 및 포트 제한 |  |  |
| U-29 | 하 | hosts.lpd 파일 소유자 및 권한 설정 |  |  |
| U-30 | 중 | UMASK 설정 관리 |  |  |
| U-31 | 중 | 홈 디렉토리 소유자 및 권한 설정 |  |  |
| U-32 | 중 | 홈 디렉토리로 지정한 디렉토리의 존재 관리 |  |  |
| U-33 | 하 | 숨겨진 파일 및 디렉토리 검색 및 제거 |  |  |
| U-34 | 상 | Finger 서비스 비활성화 |  |  |
| U-35 | 상 | 공유 서비스에 대한 익명 접근 제한 설정 |  |  |
| U-36 | 상 | r 계열 서비스 비활성화 |  |  |
| U-37 | 상 | crontab 설정파일 권한 설정 미흡 |  |  |
| U-38 | 상 | DoS 공격에 취약한 서비스 비활성화 |  |  |
| U-39 | 상 | 불필요한 NFS 서비스 비활성화 |  |  |
| U-40 | 상 | NFS 접근 통제 |  |  |
| U-41 | 상 | 불필요한 automountd 제거 |  |  |
| U-42 | 상 | 불필요한 RPC 서비스 비활성화 |  |  |
| U-43 | 상 | NIS, NIS+ 점검 |  |  |
| U-44 | 상 | tftp, talk 서비스 비활성화 |  |  |
| U-45 | 상 | 메일 서비스 버전 점검 |  |  |
| U-46 | 상 | 일반 사용자의 메일 서비스 실행 방지 |  |  |
| U-47 | 상 | 스팸 메일 릴레이 제한 |  |  |
| U-48 | 중 | expn, vrfy 명령어 제한 |  |  |
| U-49 | 상 | DNS 보안 버전 패치 |  |  |
| U-50 | 상 | DNS Zone Transfer 설정 |  |  |
| U-51 | 중 | DNS 서비스의 취약한 동적 업데이트 설정 금지 |  |  |
| U-52 | 중 | Telnet 서비스 비활성화 |  |  |
| U-53 | 하 | FTP 서비스 정보 노출 제한 |  |  |
| U-54 | 중 | 암호화되지 않는 FTP 서비스 비활성화 |  |  |
| U-55 | 중 | FTP 계정 Shell 제한 |  |  |
| U-56 | 하 | FTP 서비스 접근 제어 설정 |  |  |
| U-57 | 중 | Ftpusers 파일 설정 |  |  |
| U-58 | 중 | 불필요한 SNMP 서비스 구동 점검 |  |  |
| U-59 | 상 | 안전한 SNMP 버전 사용 |  |  |
| U-60 | 중 | SNMP Community String 복잡성 설정 |  |  |
| U-61 | 상 | SNMP Access Control 설정 |  |  |
| U-62 | 하 | 로그인 시 경고 메시지 설정 |  |  |
| U-63 | 중 | sudo 명령어 접근 관리 |  |  |
| U-64 | 상 | 주기적 보안 패치 및 벤더 권고사항 적용 |  |  |
| U-65 | 중 | NTP 및 시각 동기화 설정 |  |  |
| U-66 | 중 | 정책에 따른 시스템 로깅 설정 |  |  |
| U-67 | 중 | 로그 디렉터리 소유자 및 권한 설정 |  |  |

**2. Windows 서버 (W-01 ~ W-64)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 항목  코드 | 항목중요도 | 점검항목 | 점검  결과 | 비고 |
| W-01 | 상 | Administrator 계정 이름 변경 등 보안성 강화 |  |  |
| W-02 | 상 | Guest 계정 비활성화 |  |  |
| W-03 | 상 | 불필요한 계정 제거 |  |  |
| W-04 | 상 | 계정 잠금 임계값 설정 |  |  |
| W-05 | 상 | 해독 가능한 암호화를 사용하여 암호 저장 해제 |  |  |
| W-06 | 상 | 관리자 그룹에 최소한의 사용자 포함 |  |  |
| W-07 | 중 | Everyone 사용 권한을 익명 사용자에게 적용 |  |  |
| W-08 | 중 | 계정 잠금 기간 설정 |  |  |
| W-09 | 상 | 비밀번호 관리정책 설정 |  |  |
| W-10 | 중 | 마지막 사용자 이름 표시 안 함 |  |  |
| W-11 | 중 | 로컬 로그온 허용 |  |  |
| W-12 | 중 | 익명 SID/이름 변환 허용 해제 |  |  |
| W-13 | 중 | 콘솔 로그온 시 로컬 계정에서 빈 암호 사용 제한 |  |  |
| W-14 | 중 | 원격터미널 접속 가능한 사용자 그룹 제한 |  |  |
| W-15 | 상 | 사용자 개인키 사용 시 암호 입력 |  |  |
| W-16 | 상 | 공유 권한 및 사용자 그룹 설정 |  |  |
| W-17 | 상 | 하드디스크 기본 공유 제거 |  |  |
| W-18 | 상 | 불필요한 서비스 제거 |  |  |
| W-19 | 상 | 불필요한 IIS 서비스 구동 점검 |  |  |
| W-20 | 상 | NetBIOS 바인딩 서비스 구동 점검 |  |  |
| W-21 | 상 | 암호화되지 않는 FTP 서비스 비활성화 |  |  |
| W-22 | 상 | FTP 디렉토리 접근권한 설정 |  |  |
| W-23 | 상 | 공유 서비스에 대한 익명 접근 제한 설정 |  |  |
| W-24 | 상 | FTP 접근 제어 설정 |  |  |
| W-25 | 상 | DNS Zone Transfer 설정 |  |  |
| W-26 | 상 | RDS(Remote Data Services) 제거 |  |  |
| W-27 | 상 | 최신 Windows OS Build 버전 적용 |  |  |
| W-28 | 중 | 터미널 서비스 암호화 수준 설정 |  |  |
| W-29 | 중 | 불필요한 SNMP 서비스 구동 점검 |  |  |
| W-30 | 중 | SNMP Community String 복잡성 설정 |  |  |
| W-31 | 중 | SNMP Access control 설정 |  |  |
| W-32 | 중 | DNS 서비스 구동 점검 |  |  |
| W-33 | 하 | HTTP/FTP/SMTP 배너 차단 |  |  |
| W-34 | 중 | Telnet 서비스 비활성화 |  |  |
| W-35 | 중 | 불필요한 ODBC/OLE-DB 데이터 소스와 드라이브 제거 |  |  |
| W-36 | 중 | 원격터미널 접속 타임아웃 설정 |  |  |
| W-37 | 중 | 예약된 작업에 의심스러운 명령이 등록되어 있는지 점검 |  |  |
| W-38 | 상 | 주기적 보안 패치 및 벤더 권고사항 적용 |  |  |
| W-39 | 상 | 백신 프로그램 업데이트 |  |  |
| W-40 | 중 | 정책에 따른 시스템 로깅 설정 |  |  |
| W-41 | 중 | NTP 및 시각 동기화 설정 |  |  |
| W-42 | 하 | 이벤트 로그 관리 설정 |  |  |
| W-43 | 중 | 이벤트 로그 파일 접근 통제 설정 |  |  |
| W-44 | 상 | 원격으로 액세스할 수 있는 레지스트리 경로 |  |  |
| W-45 | 상 | 백신 프로그램 설치 |  |  |
| W-46 | 상 | SAM 파일 접근 통제 설정 |  |  |
| W-47 | 상 | 화면보호기 설정 |  |  |
| W-48 | 상 | 로그온하지 않고 시스템 종료 허용 |  |  |
| W-49 | 상 | 원격 시스템에서 강제로 시스템 종료 |  |  |
| W-50 | 상 | 보안 감사를 로그할 수 없는 경우 즉시 시스템 종료 |  |  |
| W-51 | 상 | SAM 계정과 공유의 익명 열거 허용 안 함 |  |  |
| W-52 | 상 | Autologon 기능 제어 |  |  |
| W-53 | 상 | 이동식 미디어 포맷 및 꺼내기 허용 |  |  |
| W-54 | 중 | Dos공격 방어 레지스트리 설정 |  |  |
| W-55 | 중 | 사용자가 프린터 드라이버를 설치할 수 없게 함 |  |  |
| W-56 | 중 | SMB 세션 중단 관리 설정 |  |  |
| W-57 | 하 | 로그온 시 경고 메시지 설정 |  |  |
| W-58 | 중 | 사용자별 홈 디렉터리 권한 설정 |  |  |
| W-59 | 중 | LAN Manager 인증 수준 |  |  |
| W-60 | 중 | 보안 채널 데이터 디지털 암호화 또는 서명 |  |  |
| W-61 | 중 | 파일 및 디렉토리 보호 |  |  |
| W-62 | 중 | 시작프로그램 목록 분석 |  |  |
| W-63 | 중 | 도메인 컨트롤러-사용자의 시간 동기화 |  |  |
| W-64 | 중 | 윈도우 방화벽 설정 |  |  |

**3. 웹 서비스 (WEB-01 ~ WEB-26)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 항목코드 | 항목중요도 | 점검항목 | 점검  결과 | 비고 |
| WEB-01 | 상 | Default 관리자 계정명 변경 |  |  |
| WEB-02 | 상 | 취약한 비밀번호 사용 제한 |  |  |
| WEB-03 | 상 | 비밀번호 파일 권한 관리 |  |  |
| WEB-04 | 상 | 웹 서비스 디렉터리 리스팅 방지 설정 |  |  |
| WEB-05 | 상 | 지정하지 않은 CGI/ISAPI 실행 제한 |  |  |
| WEB-06 | 상 | 웹 서비스 상위 디렉터리 접근 제한 설정 |  |  |
| WEB-07 | 중 | 웹 서비스 경로 내 불필요한 파일 제거 |  |  |
| WEB-08 | 하 | 웹 서비스 파일 업로드 및 다운로드 용량 제한 |  |  |
| WEB-09 | 상 | 웹 서비스 프로세스 권한 제한 |  |  |
| WEB-10 | 상 | 불필요한 프록시 설정 제한 |  |  |
| WEB-11 | 중 | 웹 서비스 경로 설정 |  |  |
| WEB-12 | 중 | 웹 서비스 링크 사용 금지 |  |  |
| WEB-13 | 상 | 웹 서비스 설정 파일 노출 제한 |  |  |
| WEB-14 | 상 | 웹 서비스 경로 내 파일의 접근 통제 |  |  |
| WEB-15 | 상 | 웹 서비스의 불필요한 스크립트 매핑 제거 |  |  |
| WEB-16 | 중 | 웹 서비스 헤더 정보 노출 제한 |  |  |
| WEB-17 | 중 | 웹 서비스 가상 디렉토리 삭제 |  |  |
| WEB-18 | 상 | 웹 서비스 WebDAV 비활성화 |  |  |
| WEB-19 | 중 | 웹 서비스 SSI(Server Side Includes) 사용 제한 |  |  |
| WEB-20 | 상 | SSL/TLS 활성화 |  |  |
| WEB-21 | 중 | HTTP 리디렉션 |  |  |
| WEB-22 | 하 | 에러 페이지 관리 |  |  |
| WEB-23 | 중 | LDAP 알고리즘 적절하게 구성 |  |  |
| WEB-24 | 중 | 별도의 업로드 경로 사용 및 권한 설정 |  |  |
| WEB-25 | 상 | 주기적 보안 패치 및 벤더 권고사항 적용 |  |  |
| WEB-26 | 중 | 로그 디렉터리 및 파일 권한 설정 |  |  |

**4. 보안 장비 (S-01 ~ S-23)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 항목  코드 | 항목중요도 | 점검항목 | 점검  결과 | 비고 |
| S-01 | 상 | 보안 장비 Default 계정 변경 |  |  |
| S-02 | 상 | 비밀번호 관리정책 설정 |  |  |
| S-03 | 상 | 보안 장비 계정별 권한 설정 |  |  |
| S-04 | 상 | 보안 장비 계정 관리 |  |  |
| S-05 | 상 | 계정 잠금 임계값 설정 |  |  |
| S-06 | 상 | 보안장비 원격 관리 접근 통제 |  |  |
| S-07 | 상 | 보안장비 보안 접속 |  |  |
| S-08 | 상 | 세션 종료 시간 설정 |  |  |
| S-09 | 상 | 주기적 보안 패치 및 벤더 권고사항 적용 |  |  |
| S-10 | 중 | 보안장비 로그 설정 |  |  |
| S-11 | 중 | 보안장비 로그 보관 |  |  |
| S-12 | 중 | 보안장비 정책 백업 설정 |  |  |
| S-13 | 중 | 원격 로그 서버 사용 |  |  |
| S-14 | 중 | NTP 및 시각 동기화 설정 |  |  |
| S-15 | 상 | 정책 관리 |  |  |
| S-16 | 상 | NAT 설정 |  |  |
| S-17 | 상 | DMZ 설정 |  |  |
| S-18 | 상 | 최소한의 서비스만 제공 |  |  |
| S-19 | 상 | 이상징후 탐지 모니터링 수행 |  |  |
| S-20 | 상 | 장비 사용량 검토 |  |  |
| S-21 | 상 | SNMP 서비스 확인 |  |  |
| S-22 | 상 | SNMP Community String 복잡성 설정 |  |  |
| S-23 | 중 | 유해 트래픽 탐지/차단 정책 설정 |  |  |

**5. 네트워크 장비 (N-01 ~ N-38)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 항목  코드 | 항목중요도 | 점검항목 | 점검  결과 | 비고 |
| N-01 | 상 | 비밀번호 설정 |  |  |
| N-02 | 상 | 비밀번호 복잡성 설정 |  |  |
| N-03 | 상 | 암호화된 비밀번호 가용 |  |  |
| N-04 | 상 | 계정 잠금 임계값 설정 |  |  |
| N-05 | 중 | 사용자, 명령어별 권한 수준 설정 |  |  |
| N-06 | 상 | VTY 접근(ACL) 설정 |  |  |
| N-07 | 상 | 세션 종료 시간 설정 |  |  |
| N-08 | 중 | VTY 접속 시 안전한 프로토콜 사용 |  |  |
| N-09 | 중 | 불필요한 보조 입출력 포트 사용 금지 |  |  |
| N-10 | 중 | 로그온 시 경고 메시지 설정 |  |  |
| N-11 | 중 | 원격 로그서버 사용 |  |  |
| N-12 | 상 | 주기적 보안 패치 및 벤더 권고사항 적용 |  |  |
| N-13 | 중 | 로깅 버퍼 크기 설정 |  |  |
| N-14 | 중 | 정책에 따른 로깅 설정 |  |  |
| N-15 | 중 | NTP 및 시각 동기화 설정 |  |  |
| N-16 | 하 | Timestamp 로그 설정 |  |  |
| N-17 | 상 | SNMP 서비스 확인 |  |  |
| N-18 | 상 | SNMP Community String 복잡성 설정 |  |  |
| N-19 | 상 | SNMP ACL 설정 |  |  |
| N-20 | 상 | SNMP Community 권한 설정 |  |  |
| N-21 | 상 | TFTP 서비스 차단 |  |  |
| N-22 | 상 | Spoofing 방지 필터링 적용 |  |  |
| N-23 | 상 | DDoS 공격 방어 설정 또는 DDoS 장비 사용 |  |  |
| N-24 | 상 | 사용하지 않는 인터페이스 비활성화 |  |  |
| N-25 | 중 | TCP Keepalive 서비스 설정 |  |  |
| N-26 | 중 | Finger 서비스 차단 |  |  |
| N-27 | 중 | 웹 서비스 차단 |  |  |
| N-28 | 중 | TCP/UDP small 서비스 차단 |  |  |
| N-29 | 중 | Bootp 서비스 차단 |  |  |
| N-30 | 중 | CDP 서비스 차단 |  |  |
| N-31 | 중 | Directed-broadcast 차단 |  |  |
| N-32 | 중 | Source 라우팅 차단 |  |  |
| N-33 | 중 | Proxy ARP 차단 |  |  |
| N-34 | 중 | ICMP unreachable, Redirect 차단 |  |  |
| N-35 | 중 | identd 서비스 차단 |  |  |
| N-36 | 중 | Domain Lookup 차단 |  |  |
| N-37 | 중 | pad 차단 |  |  |
| N-38 | 중 | mask-reply 차단 |  |  |

**6. 제어시스템 (C-01 ~ C-51)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 항목  코드 | 항목중요도 | 점검항목 | 점검  결과 | 비고 |
| C-01 | 상 | 계정 기능이 있는 구성요소 계정 안전 설정 |  |  |
| C-02 | 상 | 계정의 로그인/로그아웃, 사용 기록 저장 |  |  |
| C-03 | 상 | 계정입력 시 마스킹 및 에러정보 제한 |  |  |
| C-04 | 중 | 계정 용도별 분리 운용 |  |  |
| C-05 | 중 | 계정에 대해 용도별 최소 권한 부여 |  |  |
| C-06 | 중 | 운전원별 유일 계정 부여 또는 기록 유지 |  |  |
| C-07 | 상 | 구성요소에 대한 시간 동기화 수행 |  |  |
| C-08 | 상 | 불필요/취약한 서비스 제거 또는 보완대책 |  |  |
| C-09 | 중 | 관리자 페이지 접근통제(사전인가 접근) |  |  |
| C-10 | 중 | 파일/디렉터리 접근 권한 및 신뢰 관계 부여 |  |  |
| C-11 | 중 | 제어 무관 불필요 프로그램 삭제 |  |  |
| C-12 | 중 | 운영 정보, 제어 명령 위변조 및 replay 공격 방지 |  |  |
| C-13 | 하 | 제어 명령 및 파라미터 정상 범위 식별 관리 |  |  |
| C-14 | 하 | 사용자 통신 세션 타임아웃 적용 |  |  |
| C-15 | 하 | 시각 동기화 교란 공격 대비 보안 조치 |  |  |
| C-16 | 상 | 최신 업데이트/보안패치 절차 수립 |  |  |
| C-17 | 상 | 반입 패치파일 무결성 및 악성코드 검사 |  |  |
| C-18 | 상 | 알려진 취약점에 대해 보안패치/대응책 적용 |  |  |
| C-19 | 중 | 안정된 최신 SW 사용 및 기술지원 종료 제품 미사용 |  |  |
| C-20 | 하 | 변경 전 안전성 테스트를 위한 시험환경 구축 |  |  |
| C-21 | 상 | 업무망/인터넷 등 외부망과 물리적 분리 |  |  |
| C-22 | 상 | 외부 자료전달 시 물리적 일방향 자료전달 환경 구축 |  |  |
| C-23 | 상 | 무선인터넷, 테더링 등 외부망 연결 제한 |  |  |
| C-24 | 상 | 비인가된 시스템/기기에 대한 연결 차단 |  |  |
| C-25 | 상 | 물리적 일방향 자료전달 환경의 주기적 점검 |  |  |
| C-26 | 하 | 용도에 따른 세분화 및 접근제어 수행 |  |  |
| C-27 | 상 | 미사용 네트워크/USB 포트 물리적/논리적 차단 |  |  |
| C-28 | 중 | 구성요소를 물리적으로 보호할 수 있는 조치 |  |  |
| C-29 | 상 | 백신 프로그램 설치 |  |  |
| C-30 | 하 | 침입탐지시스템 구축 및 보안 이벤트 모니터링 |  |  |
| C-31 | 상 | 사이버 위기대응 매뉴얼 수립 |  |  |
| C-32 | 상 | 사이버 위기대응 훈련 정기 시행 |  |  |
| C-33 | 상 | 설정, 중요 데이터 등 정기 백업 및 관리 |  |  |
| C-34 | 중 | 장애, 테러 등에 대한 비상계획 수립 |  |  |
| C-35 | 중 | 비상계획 훈련 정기 시행 |  |  |
| C-36 | 중 | 수작업 운전 매뉴얼 작성 및 교육 훈련 |  |  |
| C-37 | 하 | 각종 이벤트에 대한 중앙집중식 로그 관리 |  |  |
| C-38 | 하 | 구성요소 기준 형상 설정 및 형상관리 수행 |  |  |
| C-39 | 하 | 주요 장비 및 제어 네트워크 장비 이중화 |  |  |
| C-40 | 하 | 화재탐지 설비 및 화재 진압설비 구비 |  |  |
| C-41 | 하 | 누수탐지 설비 및 침수 대응 장비 구비 |  |  |
| C-42 | 하 | 사이버 위험 시나리오 식별 및 완화방안 수립 |  |  |
| C-43 | 상 | 구성요소 자산정보 항상 최신으로 유지관리 |  |  |
| C-44 | 상 | 중요 구성요소 설치 장소를 보호구역으로 설정 |  |  |
| C-45 | 상 | USB 등 이동형 저장 매체 사용 통제 정책 준수 |  |  |
| C-46 | 상 | 외부 기기 반‧출입 시 클린존 통과 및 관리 |  |  |
| C-47 | 중 | 특성 반영 정보보안 정책, 지침 수립 |  |  |
| C-48 | 중 | 운영 업무에 대해 표준업무 절차서 작성 적용 |  |  |
| C-49 | 하 | 유지보수를 위한 전용 장비 마련 및 정책 시행 |  |  |
| C-50 | 상 | 허가에 의한 로직 변경 정책 수립 |  |  |
| C-51 | 하 | 직무별 직무교육 정기 실시 |  |  |

**7. PC (PC-01 ~ PC-18)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 항목코드 | 항목중요도 | 점검항목 | 점검  결과 | 비고 |
| PC-01 | 상 | 비밀번호의 주기적 변경 |  |  |
| PC-02 | 상 | 비밀번호 관리정책 설정 |  |  |
| PC-03 | 중 | 복구 콘솔에서 자동 로그온 금지 |  |  |
| PC-04 | 상 | 공유 폴더 제거 |  |  |
| PC-05 | 상 | 항목의 불필요한 서비스 제거 |  |  |
| PC-06 | 상 | 비인가 상용 메신저 사용 금지 |  |  |
| PC-07 | 중 | 파일 시스템이 NTFS 포맷으로 설정 |  |  |
| PC-08 | 중 | 다른 OS로 멀티 부팅 불가 설정 |  |  |
| PC-09 | 하 | 브라우저 종료 시 임시 인터넷 파일 삭제 설정 |  |  |
| PC-10 | 상 | 주기적 보안 패치 및 벤더 권고사항 적용 |  |  |
| PC-11 | 상 | 지원 종료되지 않은 Windows OS Build 적용 |  |  |
| PC-12 | 중 | Windows 자동 로그인 점검 |  |  |
| PC-13 | 상 | 바이러스 백신 프로그램 설치 및 업데이트 |  |  |
| PC-14 | 상 | 백신 프로그램 실시간 감시 기능 활성화 |  |  |
| PC-15 | 상 | OS 제공 침입차단 기능 활성화 |  |  |
| PC-16 | 상 | 화면보호기 설정 및 암호 보호 |  |  |
| PC-17 | 상 | 미디어 자동실행 방지 등 보안대책 수립 |  |  |
| PC-18 | 중 | 원격 지원 금지 정책 설정 |  |  |

**8. DBMS (D-01 ~ D-26)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 항목코드 | 항목중요도 | 점검항목 | 점검결과 | 비고 |
| D-01 | 상 | 기본 계정의 비밀번호, 정책 변경 |  |  |
| D-02 | 상 | 불필요 계정 제거 또는 잠금 설정 |  |  |
| D-03 | 상 | 비밀번호 사용기간 및 복잡도 설정 |  |  |
| D-04 | 상 | 관리자 권한을 꼭 필요한 계정/그룹만 허용 |  |  |
| D-05 | 중 | 비밀번호 재사용에 대한 제약 설정 |  |  |
| D-06 | 중 | DB 사용자 계정 개별 부여 |  |  |
| D-07 | 중 | root 권한으로 서비스 구동 제한 |  |  |
| D-08 | 상 | 안전한 암호화 알고리즘 사용 |  |  |
| D-09 | 중 | 일정 횟수 로그인 실패 시 잠금 정책 |  |  |
| D-10 | 상 | 원격에서 DB 서버로의 접속 제한 |  |  |
| D-11 | 상 | 시스템 테이블 접근 제한 설정 |  |  |
| D-12 | 상 | 안전한 리스너 비밀번호 설정 및 사용 |  |  |
| D-13 | 중 | 불필요한 ODBC/OLE-DB 데이터 소스 제거 |  |  |
| D-14 | 중 | 주요 설정 파일들의 접근 권한 적절 설정 |  |  |
| D-15 | 하 | 리스너 로그 및 trace 파일 변경 제한 |  |  |
| D-16 | 하 | Windows 인증 모드 사용 |  |  |
| D-17 | 하 | Audit Table 접근 제한 |  |  |
| D-18 | 상 | Role이 Public으로 설정되지 않도록 조정 |  |  |
| D-19 | 상 | OS\_ROLES 등 인증 관련 설정 FALSE 유지 |  |  |
| D-20 | 하 | 인가되지 않은 Object owner 제한 |  |  |
| D-21 | 중 | 인가되지 않은 GRANT OPTION 사용 제한 |  |  |
| D-22 | 하 | 자원 제한 기능 TRUE로 설정 |  |  |
| D-23 | 상 | xp\_cmdshell 사용 제한 |  |  |
| D-24 | 상 | Registry Procedure 권한 제한 |  |  |
| D-25 | 상 | 주기적 보안 패치 및 벤더 권고 사항 적용 |  |  |
| D-26 | 상 | 감사 기록 정책 수립 및 설정 |  |  |

**9. 이동통신 (M-01 ~ M-04)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 항목코드 | 항목중요도 | 점검항목 | 점검결과 | 비고 |
| M-01 | 상 | 엣지 네트워크 운영 시 보안기술 적용 |  | 미수행 |
| M-02 | 상 | 가상화 기술 적용 시 보안 설정 적용 |  | 미수행 |
| M-03 | 상 | 제조사 등과 보안 정책 마련 운영 |  | 미수행 |
| M-04 | 상 | 장비 구축 시 보안 내재화 수행 |  | 미수행 |

**10. Web Application (웹) (CI~WM)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 항목코드 | 항목중요도 | 점검항목 | 점검결과 | 비고 |
| CI | 상 | 코드 인젝션 (Code Injection) |  |  |
| SI | 상 | SQL 인젝션 (SQL Injection) |  |  |
| DI | 상 | 디렉터리 인덱싱 |  |  |
| EP | 상 | 에러 페이지 적용 미흡 |  |  |
| IL | 상 | 정보 누출 |  |  |
| XS | 상 | 크로스사이트 스크립트 |  |  |
| CF | 상 | 크로스사이트 요청 위조(CSRF) |  |  |
| SF | 상 | 서버사이드 요청 위조(SSRF) |  |  |
| BF | 상 | 약한 비밀번호 정책 |  |  |
| IA | 상 | 불충분한 인증 절차 |  |  |
| IN | 상 | 불충분한 권한 검증 |  |  |
| PR | 상 | 취약한 비밀번호 복구 절차 |  |  |
| PV | 상 | 프로세스 검증 누락 |  |  |
| FU | 상 | 악성 파일 업로드 |  |  |
| FD | 상 | 파일 다운로드 |  |  |
| IS | 상 | 불충분한 세션 관리 |  |  |
| SN | 상 | 데이터 평문 전송 |  |  |
| CC | 상 | 쿠키 변조 |  |  |
| AE | 상 | 관리자 페이지 노출 |  |  |
| AU | 상 | 자동화 공격 |  |  |
| WM | 상 | 불필요한 Method 악용 |  |  |

**11. 가상화 장비 (HV-01 ~ HV-25)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 항목코드 | 항목중요도 | 점검항목 | 점검결과 | 비고 |
| HV-01 | 상 | 계정 로그오프/세션 관리 |  |  |
| HV-02 | 상 | 가상화 장비 외부접속 차단 |  |  |
| HV-03 | 상 | 가상화 장비 루트계정 관리 |  |  |
| HV-04 | 상 | 가상화 장비 계정 권한 관리 |  |  |
| HV-05 | 상 | 가상화 장비 사용자 인증 강화 |  |  |
| HV-06 | 상 | 비밀번호 관리정책 설정 |  |  |
| HV-07 | 상 | 계정 잠금 임계값 설정 |  |  |
| HV-08 | 중 | 시스템 사용 주의사항 출력 설정 |  |  |
| HV-09 | 중 | NTP 및 시각 동기화 설정 |  |  |
| HV-10 | 중 | SNMP Community String 복잡성 적용 |  |  |
| HV-11 | 상 | MOB 서비스 비활성화 |  |  |
| HV-12 | 상 | ESXi Shell 비활성화 |  |  |
| HV-13 | 상 | ESXi Shell 세션 종료 시간 설정 |  |  |
| HV-14 | 중 | 원격 로그 서버 이용 |  |  |
| HV-15 | 상 | 시스템 주요 이벤트 로그 설정 |  |  |
| HV-16 | 상 | 비휘발성 경로 내 로그 파일 저장 |  |  |
| HV-17 | 상 | 코어덤프 수집 기능 활성화 |  |  |
| HV-18 | 상 | 가상 머신의 장치 변경 제한 설정 |  |  |
| HV-19 | 상 | 가상 머신의 불필요한 장치 제거 |  |  |
| HV-20 | 상 | 콘솔 클립보드 복사&붙여넣기 비활성화 |  |  |
| HV-21 | 상 | 콘솔 드래그 앤 드롭 기능 비활성화 |  |  |
| HV-22 | 상 | 가상 스위치 MAC 주소 변경 정책 비활성화 |  |  |
| HV-23 | 상 | 가상 스위치 무차별 모드 정책 비활성화 |  |  |
| HV-24 | 상 | 가상 스위치 위조전송 모드 정책 비활성화 |  |  |
| HV-25 | 상 | 주기적 보안 패치 및 벤더 권고사항 적용 |  |  |

**12. 클라우드 (CA-01 ~ CA-19)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 항목코드 | 항목중요도 | 점검항목 | 점검결과 | 비고 |
| CA-01 | 상 | 사용자 계정 관리 |  | 3차에 반영 |
| CA-02 | 중 | 사용자 정책 관리 |  | 3차에 반영 |
| CA-03 | 상 | MFA 설정 |  | 3차에 반영 |
| CA-04 | 중 | 클라우드 계정 비밀번호 정책 관리 |  | 3차에 반영 |
| CA-05 | 상 | 인스턴스 서비스 정책 관리 |  | 3차에 반영 |
| CA-06 | 상 | 네트워크 서비스 정책 관리 |  | 3차에 반영 |
| CA-07 | 상 | VPC 네트워크 서브넷 관리 |  | 3차에 반영 |
| CA-08 | 중 | 가상 네트워크 리소스 관리 |  | 3차에 반영 |
| CA-09 | 상 | 접근 제어 설정 관리 |  | 3차에 반영 |
| CA-10 | 중 | 스토리지 리소스 퍼블릭 접근 관리 |  | 3차에 반영 |
| CA-11 | 중 | 관계형 데이터베이스 암호화 설정 |  | 3차에 반영 |
| CA-12 | 중 | 통신 구간 암호화 설정 |  | 3차에 반영 |
| CA-13 | 상 | 클라우드 서비스 사용자 계정 로깅 설정 |  | 3차에 반영 |
| CA-14 | 중 | 인스턴스 로깅 설정 |  | 3차에 반영 |
| CA-15 | 중 | 관계형 데이터베이스 로깅 설정 |  | 3차에 반영 |
| CA-16 | 중 | 오브젝트 스토리지 버킷 로깅 설정 |  | 3차에 반영 |
| CA-17 | 중 | 로그 보관 기간 설정 |  | 3차에 반영 |
| CA-18 | 중 | 백업 사용 여부 |  | 3차에 반영 |
| CA-19 | 중 | 가상 리소스 이상징후 알림 설정 |  | 3차에 반영 |