보고서



2023년 9월 12일

김유석, 박하림, 박현철, 이재훈, 정재민, 하성현

| **목차**   1. **시나리오 및 설계 주안점**    1. 시나리오    2. 주안점    3. 사용기술 2. **초기 망 구성**    1. 업무망    2. D.M.Z Server Zone    3. 내부 서버망    4. 외부 연결 3. **체크리스트** 4. **취약점 진단**    1. Linux Server 4.4. 네트워크 장비    2. PC 사용자 4.5. WEB    3. DBMS 5. **모의 해킹**    1. 해킹 취약점 확인 5.4. 시나리오 2    2. 모의해킹 시나리오 설정 5.5. 시나리오 3    3. 시나리오 1 6. **보안 솔루션을 추가한 보안망 구축**    1. 전체 구성 6.5. Firewall    2. UTM 6.6. ESM    3. WAF 6.7. 기타    4. IDS |
| --- |

**1. 시나리오 및 설계 주안점**

# **1.1 시나리오**

인디 게임 기업 KM에서 게임 패키지 유출 등 의 해킹 피해가 의심되나 원인을 찾을 수 없어 보안 컨설팅을 요청하였다. 이에 현재 KM의 네트워크 구성 취약점을 진단하고 보안 솔루션을 제공한다.

# 

# **1.2 주안점**

* 네트워크 구성 취약점을 체크리스트에 기반하여 진단
* 해킹 피해를 유추하기 위해 시나리오 기반 모의해킹 실시
* 서버 가용성 보장
* 안전한 재택 근무 환경 조성
* 내부 관리자가 피해 발생 위험을 탐지 할 수 있도록 로그 통합 관리 기능을 제공

# 

# **1.3 사용기술**

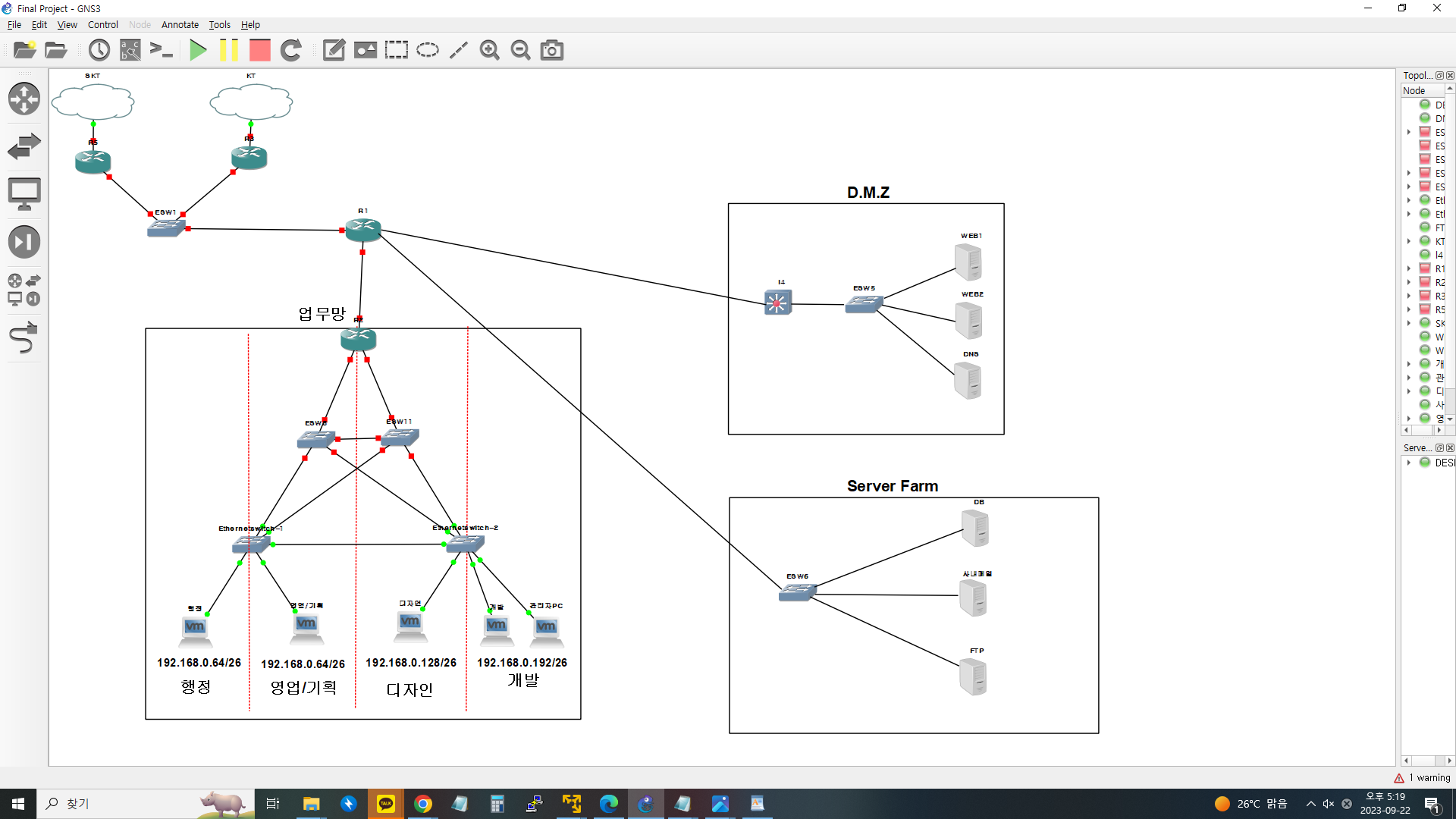
# 가) 개발 환경

| **가상화** | GNS3(Router, Switch, UDP tunnel), VMware, Oracle virtual box |
| --- | --- |
| **운영체제** | Window 7, CentOS 7, Rocky 9, Kali Linux |
| **DBMS** | MySQL, MariaDB, redis |
| **분석 툴** | Wireshark, Burp Suite |

# 나) 사용기술

| **보안 솔루션** | sophos UTM, WAF(Wapples), VPN(UTM - IPsec), ESM(elasticsearch, logstash, filebeat, kibana), IDS(snort), Firewall(linux - iptables) |
| --- | --- |
| **네트워크 장비설정** | NAT(static, NAT-PAT), Spanning Tree, Vrrp, LVS(Alteon L4 switch), Vlan |
| **서버** | Session, Backup, Web(APM 구조), Ftp, Mail, DNS, DB |
| **해킹 기법** | Sql Injection (인증 우회, non-blind), Session Hijacking, Port Scanning(nmap), XSS, DNS zone transfer, Backdoor, Webshell, DOS |
| **기타** | VScode, php, html, apache |

**2. 초기 망 구성**

****

# **2.1 업무망**

# Vlan 적용

| **switch 1,2,3,4** |
| --- |
|  |
| 네트워크를 4개의 망으로 분리하기 위해 Vlan 10, 20, 30, 40 번을 구성 |

| **switch 3** |
| --- |
|  |
| 행정 팀과 연결된 1/14 번 port에 vlan 10번 switchport access 설정  영업 기획 팀과 연결된 1/15번 port에 vlan 20번 switchport access 설정 |

| **switch 4** |
| --- |
|  |
| 디자인 팀과 연결된 1/7번 port에 vlan 30번 switchport access 설정  개발 팀과 연결된 1/14, 1/15번 port에 vlan 40번 switchport access 설정  외부 통신과 관련된 1/0 , 1/1번 port trunk로 설정 |

| **switch 1,2** |
| --- |
|  |
| 1,2번 스위치의 활성화된 port를 전부 trunk 설정 |

| **Router** |
| --- |
|  |
| sub interface를 구성  Vlan을 통해 192.168.0.0/24 대역을 행정/영업기획/디자인/개발 부서에 각각 CIDR /26 대역 4개로 분리하여 논리적으로 망을 분리함 |

# 

# Spanning tree 적용

| **switch 1** |
| --- |
|  |
| switch 1을 vlan 10, 20번의 root primary로 설정, vlan 30, 40번의 root secondary로 설정하여 vlan 10, 20번의 통신에서 우선 사용하도록 구성 |

| **switch 2** |
| --- |
|  |
| switch 2를 vlan 10, 20번의 root secondary로 설정, vlan 30, 40번의 root primary로 설정하여 vlan 30, 40번의 통신에서 우선 사용하도록 구성 |

구성 결과 확인

| **ping from 192.168.0.85 (영업 기획 팀) to 192.168.0.126 (디자인 팀)** |
| --- |
|  |

| **switch 1** |
| --- |
|  |

| **switch 2** |
| --- |
|  |

| **switch 3** |
| --- |
|  |
| ping 패킷이 Router까지 전달 된 후, vlan routing 되어 전달 되는 것으로 vlan 망 분리가 정상적으로 동작하는 것을 확인  Spanning tree 동작을 통해 switch 2가 아닌 switch 1을 통해 패킷이 전달되는 것을 확인 |

**2.2 D.M.Z Server Zone**

# 

# 

# WEB 구성 특이사항

| **php 파일(일부)** |
| --- |
|  |
| 웹에서 계정정보를 저장할 때 개인정보를 hex(aes\_encrypt()) 구조로 ‘customer’라는 키로 양방향 암호화 하여 16진수로 저장도록 설정하고, 가져올 때 해당 키로 복호화 하도록 작성  각 웹 page별 php에서는 해당 동작에 필요한 권한만을 보유한 계정으로 mysql에 접근하도록 구성  계정 정보는 이후 내부망의 DB 구성에서 설명 |

# 

# L4 switch LVS

| **interface 설정** |
| --- |
|  |
| interface 1을 외부로 연결되는 라우터와 통신하기 위한 172.16.1.0/24 대역의 ip로 임의 설정  interface 2를 DMZ 서버들의 gateway ip로 설정 |

| **real ip 등록** |
| --- |
|  |
| real server ip로 WEB 1, 2 의 ip 등록 |

| **Group 구성** |
| --- |
|  |
| real 서버를 2개 그룹에 구성 |

| **Virtual Server 설정** |
| --- |
|  |
| virtual Server ip로 172.16.0.10 등록 후, Group 을 통해 LVS 동작하도록 80, 443 번 port service 설정 |

# 

# **2.3 내부 서버망**

# 

# 

# 

# Ftp 접근권한 제어

| **vsftpd.conf 설정** |
| --- |
|  |
| chroot 설정 활성화 |

| **ftp service 용 계정 등록** |
| --- |
|  |
| 계정의 기본 home 디렉터리를 /home/km 으로 설정하여 ftp 접근시 동일한 디렉터리로 접근하도록 구성 |

| **ftp service 용 디렉터리 구성** |
| --- |
|  |
| ftp service의 기본 경로에 개별 폴더 및 공용 폴더를 생성하여 용도에 맞는 소유권을 부여 |

| **계정 그룹 설정** |
| --- |
|  |

* 구성 확인

| dev 계정만 chroot.list에 등록후 확인  root 계정 접속 시도 |
| --- |
|  |
| root 계정으로 접속 시도 시 권한 거부설정이 된 것을 확인 가능 |

| **행정팀(adm1) 계정으로 접근 시도** |
| --- |
|  |
| 디렉터리의 권한제어를 통해 디렉터리 접근 권한이 부분적으로 허용된 것을 확인 가능 |

# 

# DBMS 구성

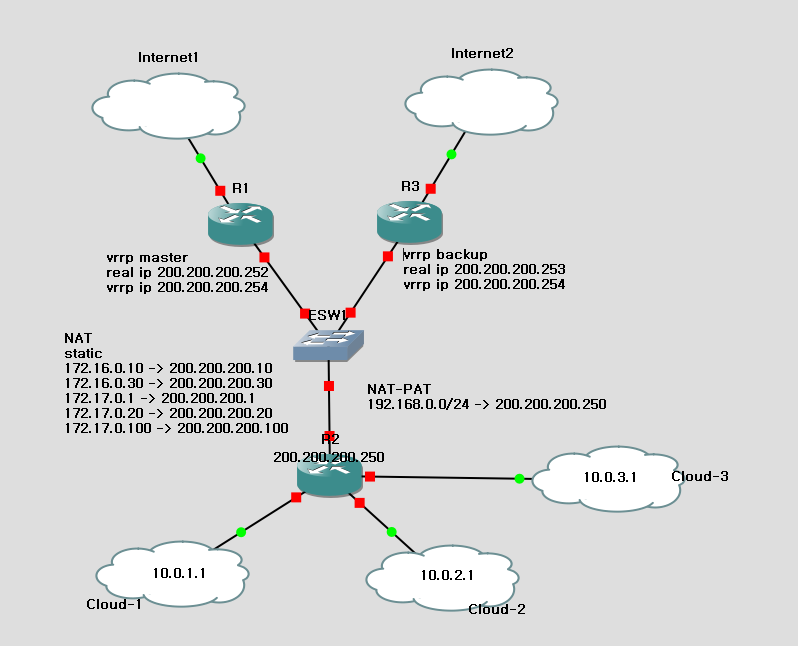
| **KHmanager.customer 테이블** |
| --- |
|  |

| **KHmanager.board 테이블** |
| --- |
|  |

| **game.game 테이블** |
| --- |
|  |
| 테이블 구성은 각각 식별하기 쉬운 컬럼명을 보유하도록 구성하고,  컬럼의 글자수 제한은 웹에서 전달된 일반 데이터와 암호화 된 데이터가 누락되지 않도록 길이를 고려하여 설정 |

| **계정권한 설정** |
| --- |
|  |
| DMZ 서버망에서만 접근이 가능하도록 host 설정한 계정을 생성하고  web에서 동작에 필요한 계정을 각각의 기능에 맞춰 한정적으로 부여 |

# **2.4 외부 연결**



# 

# 게이트웨이 이중화(vrrp)

| **R1** |
| --- |
|  |
| R1을 200.200.200.254(GW ip)에 대한 vrrp Master로 구성하기 위해 priority를 기본값(100)보다 높은 120으로 설정하고 track을 통해 외부 통신상태를 확인하도록 설정 |

| **R3** |
| --- |
|  |
| R3를 vrrp backup 으로 구성 |

# 

# 동작 확인

| **R1** |
| --- |
|  |
| **R3** |
|  |
| track 으로 탐지중인 internet 1을 삭제  track 상태가 down 으로 변경 되자 track의 decrement옵션이 정상적으로 동작하여 priority 기본값(100)인 R3가 Master로 변경된 것을 확인 할 수 있다 |

**3. 체크리스트 작성**

**KM 보안 점검 체크리스트**

| **Linux Server 취약점 분석·평가 항목** |
| --- |

| **분류** | **NO** | **점검항목** | **항목 중요도** | **비고** |
| --- | --- | --- | --- | --- |
| **1. 계정관리** | 1 | 패스워드 파일 보호 | 상 |  |
| 2 | 패스워드 최소 사용기간 설정 | 중 |  |
| 3 | 패스워드 최대 사용기간 설정 | 중 |  |
| 4 | 불필요한 계정 제거 | 하 |  |
| 5 | 관리자 그룹에 최소한의 계정 포함 | 하 |  |
| 6 | 동일한 UID 금지 | 중 |  |
| **2. 파일 및**  **디렉터리 관리** | 1 | 파일 및 디렉터리 소유자 설정 | 상 |  |
| 2 | /etc/passwd 파일 소유자 및 권한 설정 | 상 |  |
| 3 | /etc/shadow 파일 소유자 및 권한 설정 | 상 |  |
| 4 | /etc/(xinetd.conf 파일 소유자 및 권한 설정 | 상 |  |
| 5 | /etc/service 파일 소유자 및 권한 설정 | 상 |  |
| 6 | 사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정 | 상 |  |
| 7 | 접속 IP 및 포트 제한 | 상 |  |
| **3. 서비스 관리** | 1 | Anonymous FTP 비활성화 | 상 |  |
| 2 | cron 파일 소유자 및 권한 설정 | 상 |  |
| 3 | Dos 공격에 취약한 서비스 비활성화 | 상 |  |
| 4 | DNS 보안 버전 패치 | 상 |  |
| 5 | DNS Zone Transfer 설정 | 상 |  |
| 6 | 웹서비스 디렉토리 리스팅 제거 | 상 |  |
| 7 | 웹서비스 웹 프로세스 권한 제한 | 상 |  |
| 8 | 웹서비스 상위 디렉토리 접근 금지 | 상 |  |
| 9 | 웹서비스 불필요한 파일 제거 | 상 |  |
| 10 | 웹서비스 링크 사용 금지 | 상 |  |
| 11 | 웹서비스 영역의 분리 | 상 |  |
| 12 | ssh 원격접속 허용 | 중 |  |
| 13 | ftp 서비스 확인 | 하 |  |
| 14 | Ftpusers 파일 소유자 및 권한 설정 | 하 |  |
| 15 | Ftpusers 파일 설정 | 중 |  |
| 16 | at 파일 소유자 및 권한 설정 | 중 |  |
| 17 | NFS 설정파일 접근 제한 | 중 |  |
| 18 | Apache 웹 서비스 정보 숨김 | 중 |  |

| **PC 취약점 분석·평가 항목** |
| --- |

| 분류 | NO | 점검항목 | 항목 중요도 | 비고 |
| --- | --- | --- | --- | --- |
| **1.계정관리** | 1 | 패스워드의 주기적 변경 | 상 |  |
| 2 | 패스워드 정책이 해당 기관의 보안 정책에 적합하게 설정 | 상 |  |
| 3 | Administrator 계정 이름 변경 또는 보안성 강화 | 상 |  |
| 4 | Guest 계정 비활성화 | 상 |  |
| 5 | 불필요한 계정 제거 | 상 |  |
| 6 | 관리자 그룹에 최소한의 사용자 포함 | 상 |  |
| 7 | 패스워드 복잡성 설정 | 중 |  |
| 8 | 로컬 로그온 허용 | 중 |  |
| **2. 서비스 관리** | 1 | 공유 권한 및 사용자 그룹 설정 | 상 |  |
| **3. 보안 관리** | 1 | OS에서 제공하는 침입차단 기능 활성화 | 상 |  |
| 2 | 화면보호기 대기 시간 설정 및 재시작 시 암호 보호 설정 | 상 |  |
| 3 | 로그온 하지 않고 시스템 종료 허용 해제 | 상 |  |
| 4 | 원격 시스템에서 강제로 시스템 종료 | 상 |  |

| **DBMS 취약점 분석·평가 항목** |
| --- |

| **분류** | **NO** | **점검항목** | **항목 중요도** | **비고** |
| --- | --- | --- | --- | --- |
| **1. 계정관리** | 1 | 기본 계정의 패스워드, 권한 등을 변경하여 사용 | 상 |  |
| 2 | 데이터베이스의 불필요 계정을 제거하거나, 잠금설정 후 사용 | 상 |  |
| 3 | 데이터 베이스 관리자 권한을 꼭 필요한 계정 및 그룹에 허용 | 상 |  |
| 4 | DB 사용자 계정을 개별적으로 부여하여 사용 | 중 |  |
| **2. 접근 관리** | 1 | 원격에서 DB 서버로의 접속 제한 | 상 |  |
| 2 | DBA 이외의 인가되지 않은 사용자 시스템 테이블에 접근할 수 없도록 설정 | 상 |  |
| 3 | 데이터베이스의 주요 설정파일, 패스워드 파일 등과 같은 주요 파일들의 접근 권한이 적절하게 설정 | 중 |  |
| **3. 옵션 관리** | 1 | 인가되지 않은 GRANT OPTION 사용 제한 | 중 |  |

| **네트워크 장비 취약점 분석·평가 항목** |
| --- |

| **분류** | **NO** | **점검항목** | **항목 중요도** | **비고** |
| --- | --- | --- | --- | --- |
| **1. 계정관리** | 1 | 패스워드 설정 | 상 |  |
| 2 | 패스워드 복잡성 설정 | 상 |  |
| 3 | 암호화된 패스워드 사용 | 상 |  |
| 4 | 사용자-명령어별 권한 수준 설정 | 중 |  |
| **2. 접근 관리** | 1 | Session Timeout 설정 | 상 |  |
| 2 | 불필요한 보조 입,출력 포트 사용 금지 | 중 |  |
| 3 | 로그인 시 경고 메시지 설정 | 중 |  |
| **패치 관리** | 1 | 최신 보안 패치 및 벤더 권고사항 적용 | 상 |  |
| **로그 관리** | 1 | 로깅 버퍼 크기 설정 | 중 |  |
| **기능 관리** | 1 | Finger 서비스 차단 | 중 |  |
| 2 | 웹 서비스 차단 | 중 |  |
| 3 | CDP 서비스 차단 | 중 |  |
| 4 | Directed-broadcast 차단 | 중 |  |
| 5 | Source 라우팅 차단 | 중 |  |
| 6 | Proxy ARP 차단 | 중 |  |
| 7 | ICMP unreachable, Redirect 차단 | 중 |  |
| 8 | identd 서비스 차단 | 중 |  |
| 9 | Domain lookup 차단 | 중 |  |
| 10 | SNMP 서비스 확인 | 상 |  |
| 11 | SNMP community string 복잡성 설정 | 상 |  |
| 12 | 사용하지 않는 인터페이스의 Shutdown 설정 | 상 |  |

| **Web 취약점 분석·평가 항목** |
| --- |

| **분류** | **NO** | **점검항목** | **항목 중요도** | **비고** |
| --- | --- | --- | --- | --- |
| **1. WEB** | 1 | 버퍼 오버플로우 | 상 |  |
| 2 | 포맷스트링 | 상 |  |
| 3 | LDAP 인젝션 | 상 |  |
| 4 | 운영체제 명령 실행 | 상 |  |
| 5 | SQL 인젝션 | 상 |  |
| 6 | SSI 인젝션 | 상 |  |
| 7 | XPath 인젝션 | 상 |  |
| 8 | 디렉터리 인덱싱 | 상 |  |
| 9 | 정보 누출 | 상 |  |
| 11 | 크로스사이트 스크립팅 | 상 |  |
| 15 | 크로스사이트 리퀘스트 변조(CSRF) | 상 |  |
| 19 | 세션 고정 | 상 |  |
| 20 | 자동화 공격 | 상 |  |
| 22 | 파일 업로드 | 상 |  |
| 23 | 파일 다운로드 | 상 |  |
| 25 | 경로 추적-보류 | 상 |  |
| 26 | 위치 공개-보류 | 상 |  |
| 27 | 데이터 평문 전송 | 상 |  |

# 

**4. 취약점 진단**

# **4.1 Linux Server 취약점 분석· 평가 항목**

| **2. 파일 및 디렉터리 관리** | 접속 IP 및 포트 제한 | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 2.7 (상) | |  | | | 허용할 호스트에 대한 접속 IP 주소 제한 및 포트 제한 설정 여부 확인 후  접속을 허용할 특정 호스트에 대한 IP 주소 및 포트 제한을 설정하지 않 음 | | |
| 진단 결과 | 취약 |
| 권장 설정 | | 접속을 허용할 특정 호스트에 대한 IP 주소 및 포트 제한을 설정한다. | | | | | |

# 

| **3. 서비스 관리** | cron 파일 소유자 및 권한 설정 | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 3.2 (상) | |  | | | Cron 관련 파일의 권한 적절성 점검 후 crontab 명령어 일반사용자 사용가능하거나, crond 관련 파일 640 이상이었음 | | |
| 진단 결과 | 취약 |
| 권장 설정 | | crontab 명령어 일반사용자 금지 및 cron 관련 파일 640 이하로 설정 | | | | | |

# 

| **3. 서비스 관리** | DNS Zone Transfer 설정 | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 3.5 (상) | |  | | | Secondary Name Server로만 Zone 정보 전송 제한 여부 점검 후 DNS 서비스를 사용하며 Zone Transfer를 모든 사용자에게 허용함 | | |
| 진단 결과 | 취약 |
| 권장 설정 | | DNS 서비스 미사용 또는, Zone Transfer를 허가된 사용자에게만 허용함 | | | | | |

# 

| **3. 서비스 관리** | 웹 서비스 웹 프로세스 권한 제한 | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 3.18 (상) | |  | | | Apache 데몬을 root 권한으로 구동하지 않고 별도의 권한으로 구동 함으로 써 침해사고 발생 시 피해범위 확산 방지를 목적으로 Apache 데몬이 root 권한으로 구동됨 | | |
| 진단 결과 | 취약 |
| 권장 설정 | | Apache 데몬이 root 권한으로 구동되지 않게함 | | | | | |

# 

| **3. 서비스 관리** | ssh 원격접속 허용 | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 3.12 (중) | |  | | | 원격 접속 시 SSH 프로토콜을 사용하는지 점검 후 원격 접속 시 Telnet, FTP 등 안전하지 않은 프로토콜을 사용하는 경우 확인함 | | |
| 진단 결과 | 취약 |
| 권장 설정 | | 원격 접속 시 SSH 프로토콜을 사용함 | | | | | |

# 

| **3. 서비스 관리** | ftpusers 파일 소유자 및 권한 설정 | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 3.14 (하) | |  | | | FTP 접근제어 설정파일에 관리자 외 비인가자들이 수정 제한 여부 점검 후 ftpusers 파일의 소유자가 root가 아니거나, 권한이 640 이하가 아님 | | |
| 진단 결과 | 취약 |
| 권장 설정 | | ftpusers 파일의 소유자가 root이고, 권한이 640 이하로 설정 | | | | | |

# 

# 

| **3. 서비스 관리** | ftpusers 파일 설정 | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 3.28 (중) | |  | | | root의 FTP 직접 접속을 방지하여 root 패스워드 정보를 노출되지 않도록 하기 위해 FTP 서비스가 활성화 되어 있고, root 계정 접속을 허용 됨 | | |
| 진단 결과 | 취약 |
| 권장 설정 | | FTP 서비스가 비활성화 되어 있거나, 활성화 시 root 계정 접속을 차단 한다. | | | | | |

# 

| **3. 서비스 관리** | at 파일 소유자 및 권한 설정 | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 3.29 (중) | |  | | | 관리자외 at 서비스를 사용할 수 없도록 설정하고 있는지 점검하는 것을 목적으로 at 명령어 일반사용자 사용가능하거나, at 관련 파일 640 이상인 경우 | | |
| 진단 결과 | 취약 |
| 권장 설정 | | at 명령어 일반사용자 금지 및 at 관련 파일 640 이하로 설정한다. | | | | | |

# 

| **3. 서비스 관리** | Apache 웹 서비스 정보 숨김 | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 3.32 (중) | |  | | | HTTP 헤더, 에러페이지에서 웹 서버 버전 및 종류, OS 정보 등 웹 서버와 관련된 불필요한 정보가 노출되지 않도록 하기 위해 ServerTokens Prod, ServerSignature Off로 설정되어있지 않음 | | |
| 진단 결과 | 취약 |
| 권장 설정 | | ServerTokens Prod, ServerSignature Off로 설정한다. | | | | | |

# **4.2 PC 취약점 분석· 평가 항목**

| **1. 파일 및 디렉터리 관리** | Administrator 계정 이름 변경 또는 보안성 강화 | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1.3 (상) | |  | | | 계정 이름을 변경하지 않거나 단순한 비밀번호 적용되어 있음 | | |
| 진단 결과 | 취약 |
| 권장 설정 | |  | | | | | |

# 

| **1. 파일 및 디렉터리 관리** | 로컬 로그온 허용 | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1.8 (중) | |  | | | Administrators, IUSR 외 다른 계정 및 그룹이 존재함 | | |
| 진단 결과 | 취약 |
| 권장 설정 | |  | | | | | |

# 

# 

| **2. 서비스 관리** | 공유 권한 및 사용자 그룹 설정 | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 2.1 (상) | |  | | | 일반 공유 디렉토리의 접근 권한에  Everyone 권한이 있었음 | | |
| 진단 결과 | 취약 |
| 권장 설정 | |  | | | | | |

# 

| **3. 보안관리** | 로그온 하지 않고 시스템 종료 허용 해제 | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 3.3 (상) | |  | | | “로그온 하지 않고 시스템 종료 허용”이 “사용”으로 설정되어 있음 | | |
| 진단 결과 | 취약 |
| 권장 설정 | |  | | | | | |

# 

# **4.3 DBMS 취약점 분석· 평가 항목**

| **1. 계정관리** | 기본 계정의 패스워드, 권한 등을 변경하여 사용 | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1.1 (상) | |  | | | 기본 root 계정을 사용하고 알려진 초기 비밀번호 사용중 | | |
| 진단 결과 | 취약 |
| 권장 설정 | | root 계정을 삭제하거나, 안전한 비밀번호로 변경 | | | | | |

# 

| **2. 접근관리** | 원격에서 DB 서버로의 접속 제한 | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1.1 (상) | |  | | | % ( 모든 호스트 ) 대상으로 접근이 허용된 계정이 있음 | | |
| 진단 결과 | 취약 |
| 권장 설정 | | % (모든 호스트) 대상 접속 가능한 계정 삭제 | | | | | |

# **4.4 네트워크 장비 취약점 분석·평가 항목**

| **1. 계정관리** | 패스워드 설정 | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1.1 (상) | |  | | | 기본 패스워드를 변경하지 않거나 패스워드를 설정하지 않은 경우 | | |
| 진단 결과 | 취약 |
| 권장 설정 | |  | | | | | |

# 

| **1. 계정관리** | 패스워드 복잡성 설정 | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1.2 (상) | |  | | | 기관 정책에 맞지 않는 패스워드를 설정하여 사용하는 경우 | | |
| 진단 결과 | 취약 |
| 권장 설정 | |  | | | | | |

# 

| **1. 계정관리** | 암호화된 패스워드 사용 | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1.3 (상) | |  | | | 패스워드 암호화 설정을 적용하지 않은 경우 | | |
| 진단 결과 | 취약 |
| 권장 설정 | |  | | | | | |

# 

| **1. 계정관리** | 사용자-명령어별 권한 수준 설정 | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1.4 (중) | |  | | | 업무에 맞게 계정의 권한이 차등 부여 되어있지 않을 경우 | | |
| 진단 결과 | 취약 |
| 권장 설정 | |  | | | | | |

# 

| **2. 로그관리** | Session Timeout 설정 | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 2.1 (상) | |  | | | Session Timeout 시간을 기관 정책에 맞게 설정하지 않은 경우 | | |
| 진단 결과 | 취약 |
| 권장 설정 | |  | | | | | |

# 

| **2. 로그관리** | 로그인 시 경고 메시지 설정 | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 2.3 (중) | |  | | | 로그온 시 접근에 대한 경고 메시지를 설정하지 않거나 시스템 관련 정보가 노출되는 경우 | | |
| 진단 결과 | 취약 |
| 권장 설정 | |  | | | | | |

# 

| **4. 로그관리** | 로깅 버퍼 크기 설정 | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1.1 (중) | |  | | | 저장되는 로그 데이터보다 버퍼 용량이 작은 경우 | | |
| 진단 결과 | 취약 |
| 권장 설정 | |  | | | | | |

# 

| **5. 기능관리** | Finger 서비스 차단 | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1.1 (중) | |  | | | Finger 서비스를 차단하지 않는 경우 | | |
| 진단 결과 | 취약 |
| 권장 설정 | |  | | | | | |

# 

| **5. 기능관리** | Direct-broadcast 차단 | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1.4 (중) | |  | | | Directed Broadcasts를 차단하지 않는 경우 | | |
| 진단 결과 | 취약 |
| 권장 설정 | |  | | | | | |

# 

| **5. 기능관리** | Source 라우팅 차단 | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1.5 (중) | |  | | | ip source route를 차단하지 않는 경우 | | |
| 진단 결과 | 취약 |
| 권장 설정 | |  | | | | | |

# 

| **5. 기능관리** | Proxy ARP 차단 | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1.6 (중) | |  | | | Proxy ARP를 차단하지 않는 경우 | | |
| 진단 결과 | 취약 |
| 권장 설정 | |  | | | | | |

# 

| **5. 기능관리** | identd 서비스 차단 | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1.8 (중) | |  | | | identd 서비스를 차단하지 않는 경우 | | |
| 진단 결과 | 취약 |
| 권장 설정 | |  | | | | | |

# 

| **5. 기능관리** | SNMP 서비스 확인 | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1.10 (상) | |  | | | 사용하지 않는 SNMP 서비스를 비활성화하지 않은 경우 | | |
| 진단 결과 | 취약 |
| 권장 설정 | |  | | | | | |

# 

| **5. 기능관리** | SNMP community string 복잡성 설정 | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1.11 (상) | |  | | | SNMP 커뮤니티 스트링을 디폴트 또는 유추하기 쉽게 설정한 경우 | | |
| 진단 결과 | 취약 |
| 권장 설정 | |  | | | | | |

# 

# **4.5 WEB 취약점 분석·평가 항목**

| **분류** | **NO** | **점검항목** | **항목 중요도** | **비고** |
| --- | --- | --- | --- | --- |
| **1. WEB** | 1 | 버퍼 오버플로우 | 상 |  |
| 2 | 포맷스트링 | 상 |  |
| 3 | LDAP 인젝션 | 상 |  |
| 4 | 운영체제 명령 실행 | 상 |  |
| 5 | SQL 인젝션 | 상 |  |
| 6 | SSI 인젝션 | 상 |  |
| 7 | XPath 인젝션 | 상 |  |
| 8 | 디렉터리 인덱싱 | 상 |  |
| 9 | 정보 누출 | 상 |  |
| 11 | 크로스사이트 스크립팅 | 상 |  |
| 15 | 크로스사이트 리퀘스트 변조(CSRF) | 상 |  |
| 19 | 세션 고정 | 상 |  |
| 20 | 자동화 공격 | 상 |  |
| 22 | 파일 업로드 | 상 |  |
| 23 | 파일 다운로드 | 상 |  |
| 25 | 경로 추적-보류 | 상 |  |
| 26 | 위치 공개-보류 | 상 |  |
| 27 | 데이터 평문 전송 | 상 |  |

※WEB은 WAF 적용 예정이며 모의해킹과 중복되는 부분이 많아 체크리스트 확인 결과로 대체 일부 특이 취약점만 표로 기록

# 

| **1. WEB** | 크로스사이트 스크립팅 | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1.10(상) | |  | | | Cross Site scripting 항목이 “탐지 안 함” 으로 설정되어 있는 경우 | | |
| 진단 결과 | 취약 |
| 권장 설정 | |  | | | | | |

# 

**5. 모의 해킹**

# 5.1 해킹 취약점 확인

| **DNS zone transfer** |
| --- |
|  |
| dig 명령어를 이용해 [www.km.com](http://www.km.com) 의 nameserver 를 확인하여 zone 정보 요청 시도  시도가 성공하여 zone 정보를 획득 |

| **sql injection(non-blind)\_1** |
| --- |
|  |
| order by 문을 사용해 sql injection 가능여부 확인 후 컬럼 수 (5개) 확인  공격방법 : 주소/board\_view.php?no=(존재하는게시글번호)에 order by 문을 사용한 요청 후 결과 변화 확인 |

| **sql injection(non-blind)\_2** |
| --- |
|  |
| 공격을 통해 DB 정보 확인  공격 방법 : 주소/board\_view.php?no= 값을 -1로 설정후 union 문을 이용하여 요청 |

| **sql injection 인증 우회** |
| --- |
|  |
| sql injection 인증우회를 통해 admin(관리자) 계정으로 접속  접속 후 관리자용 권한에 접근  공격방법 : login\_proc.php 동작에 ‘ or 1=1 # 을 값으로 전달 |

| **XSS** |
| --- |
| XSS 스크립트 동작을 통해 세션값 호출이 가능한 것을 확인  공격방법 : <script>alert(document.cookie)</script> |

| **port scanning** |
| --- |
|  |
| nmap을 사용해 TCP Full-Connect Scanning 후 open port 확인 |

# 5.2 모의해킹 시나리오 설정

| **주요 취약점 정리** |
| --- |
| DNS Zone transfer 가능  Port Scanning 가능  ssh 원격 접속 가능  웹 서비스 정보 노출  DBMS 기본 계정 사용 및 원격 접속 가능  웹 운영체제 명령 실행  웹 SQL 인젝션  웹 XSS  웹 파일 업로드 취약점 |

| **모의해킹 시나리오 설정** | |
| --- | --- |
| 시나리오 1 | Zone file 정보와 port Scanning을 이용해 DB에 접근하여 정보 탈취 시도 |
| 시나리오 2 | Zone file 정보와 port Scanning을 이용하여 tcp 22번 port접속이 가능한 DNS 서버에 원격 접속 후, Backdoor를 작성하여 root 권한 탈취 후 DNS 정보 변조 |
| 시나리오 3 | XSS 공격을 통해 웹 관리자의 세션 정보를 획득하여 관리자 권한 탈취 후 이를 이용해 웹쉘을 설치 및 실행하여 서버 파일을 변조 |

# 

# 5.3 해킹 시나리오 1

| **1. DNS Zone Transfer** |
| --- |
|  |
| Dig 툴을 이용해 DNS zone 정보를 획득하여 접근 대상 ip 확인 |

| **2. Port Scanning** |
| --- |
|  |
| nmap을 사용해 TCP Full-Connect Scanning 시도 후 22번(ssh) port open 상태 확인 |

| **3. ssh 접근** |
| --- |
|  |
| 대상 ip 대역으로 spoof 하여 ssh 접근에 성공 |

| **4. DB 접근 시도** |
| --- |
|  |
| 알려진 초기 비밀번호 (P@ssw0rd)로 root 계정 접근 시도 성공 |

| **5. DB 내부 정보 조회** |
| --- |
|  |
| root 계정의 권한을 통해 DB 구조를 조회하고 계정정보 및 개인정보 탈취를 시도했으나 암호화 되어있어 정보 획득에는 실패 |

# 5.4 해킹 시나리오 2

| **1. DNS Zone Transfer** |
| --- |
|  |
| DNS Zone 정보를 통해 DNS서버의 주소 확인 |

| **2. Port Scanning** |
| --- |
|  |
| nmap 의 TCP Full-Connect Scanning 을 통해 dns 서버의 22번 port가 open 상태임을 확인 |

| **3. ssh로 직접 접근 시도** |
| --- |
|  |
| root 계정으로 접근 성공 |

| **4. 백도어 설치** |
| --- |
|  |
| root 계정의 권한을 통해 해당 사진과 같이 작성하여 ping 명령어를 root 권한 탈취 백도어로 한정적 동작이 가능하게 설치 |

| **5. test 계정 접근** |
| --- |
|  |
| root 계정의 접근기록이 추가 생성되지 않고, 이후에 root 계정사용이 불가능한 상황을 가정하여 일반 사용자 계정으로 접근 |

| **6. 사용자 계정으로 DNS Zone 파일 접근** |
| --- |
|  |
| 권한이 없어 zone 파일 확인 및 수정이 불가능 함을 확인 |

| **7. 설치해둔 backdoor ‘ping’ 명령어를 사용** |
| --- |
|  |
| backdoor를 이용해 root 권한으로 zone file 수정 명령 동작 |

| **8. Zone file 내용을 변경** |
| --- |
|  |
| zone file의 [www.km.com](http://www.km.com) 에 대한 레코드를 50.50.50.50 ( 해커가 사전 준비한 웹사이트 ) 로 DNS 정보 조작 |

| **9. DNS 변조 결과 확인** |
| --- |
|  |
| [www.km.com](http://www.km.com) 으로 접근을 요청하였을 때, 해커가 준비한 다른 사이트로 사용자 유도 성공 |

# 

# 5.5 해킹 시나리오 3

| **1. 웹 XSS 스크립트 작성** |
| --- |
|  |
| 웹 게시판에 XSS 공격을 통해 해커에 세션 쿠키값을 전달하는 스크립트 작성 |

| **2. 게시글 작성 확인** |
| --- |
|  |
| 게시글이 정상적으로 등록되는 것을 확인 후 관리자의 접근을 기다림 |

| **3. 관리자의 게시글 접근** |
| --- |
|  |
| 게시글 접근 시 cookie값을 포함하여 요청을 발송 하나 비정상적인 요청으로 요청완료가 되지 않음 |

| **4. 해커의 웹 access log 확인** |
| --- |
|  |
| 해커의 웹 access log에 요청값이 그대로 전달되어 쿠키값을 확인 할 수 있음 |

| **5. Session Hijacking** |
| --- |
|  |
| burp suite를 이용해 해당 세션 값으로 웹사이트에 접근 |

| **6. 관리자 권한 확인** |
| --- |
|  |
| 관리자 세션 하이재킹에 성공하여 관리자 전용 권한(업로드) 확인 |

| **7. 웹 쉘 업로드** |
| --- |
|  |
| 관리자용 업로드 기능을 이용해 웹 쉘(php 파일)을 업로드 |

| **8. 웹 쉘 요청** |
| --- |
|  |
| 웹 쉘 경로를 직접 요청하여 웹 쉘 동작 |

| **9. 웹 쉘 동작 확인** |
| --- |
|  |
| 웹 쉘을 통해 서버의 계정 정보 확인 및 변조를 시도하여 최고 관리자 권한을 가지고 있음을 확인 |

| **10. 웹 서버에 삽입 할 코드 작성** |
| --- |
|  |
| 웹 서버에서 파일 다운로드 동작을 담당하는 down\_file.php 문서를 취약한 코드로 새로작성 |

| **11. 웹 서버에 코드 삽입** |
| --- |
|  |
| 작성한 코드를 웹쉘을 통해 서버에 업로드하여 서버에서 다운로드 기능을 결제 검증 없이 이용할 수 있는 취약한 코드로 동작하게 구성 |

**6. 보안 솔루션 적용**

# **6.1 전체 구성**

# 

# 

# **6.2 UTM**

# 가) UTM 기본 설정

| **Interface 구성** |
| --- |
|  |
| 관리자용 인터페이스 ‘작업용’ , 외부망 인터페이스 ‘External’, 내부망 인터페이스 ‘Internal’ 구성  ‘External’에 GW로 외부 라우터 ip ( 200.200.200.254 ) 설정 |

| **마스커레이딩** |
| --- |
|  |
| 내부 서버망을 제외한 업무망, DMZ 서버존에서의 외부통신을 허용하고, VPN 을 통해 접근하는 재택 근무자가 내부망 ip로 접근 할 수 있도록 설정 |

| **OSPF** |
| --- |
| [ 사진 ] |
| OSPF 설정을 통해 내부망의 라우팅 정보 공유 및 학습 |

| **DNAT** |
| --- |
|  |
| DNAT 설정을 통해 DMZ 서버망의 WEB, DNS 에 대한 직접 접근이 가능하도록 설정 |

| **유해 트래픽 방지** |
| --- |
|  |
| Port Scanning 방지 및 flooding 형태의 DOS 유형 공격 방지 옵션 활성화 |

| **방화벽 정책** |
| --- |
|  |
| 1,2 번 - DNAT 설정의 자동 방화벽 규칙  3 번 - DNS 서버의 DNS 프로토콜 모든 IP 대상으로 허용  4 번 - WEB 서버의 http 관련 프로토콜 4종 모든 IP 대상으로 허용  5번 - 업무망의 트래픽 일반적으로 모두 허용  6번 - DMZ 서버망의 트래픽 일반적으로 모두 허용  7번 - VPN 을 통해 접근한 재택 근무자의 업무망 접속 허용 |

| **적용 전** | **적용 후** |
| --- | --- |
|  |  |
| UTM 장비 설정 이후 외부에서 내부망으로 Port Scanning 기능이 차단 된 것을 확인 | |

# 나) VPN 구성

| **VPN 사용자 등록** |
| --- |
|  |
| 재택근무자를 위한 VPN(ipsec) 사용자 등록 |

| **IPsec 설정** |
| --- |
|  |
| 사전 공유키를 설정하여 키 기반의 ipsec VPN 설정 |

| **클라이언트 VPN 설치** |
| --- |
|  |
| IPsec 사용자 계정 정보 등록 후 IPsec VPN 활성화 |

| **VPN 접속 정보 확인** |
| --- |
|  |
| VPN 활성화 이후 접근 계정 정보 확인 |

| **재택 근무 활성화 확인** |
| --- |
|  |
| VPN 활성화 이후 routing table이 변경되어 내부 업무망에 접근 가능한 것을 확인 |

# 

# **6.3 WAF (Wapples)**

| **WAF interface 설정** |
| --- |
|  |
| DMZ 서버망 내부 스위치에 proxy 구조로 연결하여 내부에서 관리하기 위해 2개 인터페이스를 172.16.0.0/24 대역의 여유 ip로 설정 |

| **내부 정책 설정** |
| --- |
|  |
| 고급 보안 정책을 기반으로 서버에 대한 새 정책을 설정함 |

| **적용 전** | **적용 후** |
| --- | --- |
|  |  |
| WAF 적용 이전 XSS 공격에 취약하였으나, 정책 적용 이후 동일한 공격 시도 시 설정한 에러코드 405번이 호출되는 것을 확인 | |

**6.4 IDS (snort)**

| **ruletype 추가** |
| --- |
|  |
| 3가지 유형의 log를 별도로 기록하기 위해서 ruletype을 추가하여 출력 과정의 facility를 local 1, local 2, local 3으로 분리하되 alert 로그의 기본 형태를 사용하여 로그를 출력하도록 설정  local 1, 2, 3 이 별도의 로그파일로 저장하도록 rsyslog.config 수정 |

| **세부 정책 (alert 1)** |
| --- |
|  |
| alert1 정상 송수신 패킷을 기록하여 통신량 기록  1. 업무망에서 FTP Server에 접근하는 패킷 탐지  2. WEB Server와 DB의 통신 패킷 탐지  3. WEB Server와 Session Server의 통신 패킷 탐지 |

| **세부 정책 (alert 2)** |
| --- |
|  |
| alert2 주의 단계의 패킷 특이사항 기록  1~4. 업무망에서 FTP를 사용시 각 부서에 인가되지 않은 접근 시도 탐지  5. 관리자pc 이외의 자리에서 실행파일 접근 탐지 |

| **세부 정책 (alert 3)** |
| --- |
|  |
| alert3 공격 의심/위험 패킷을 log로 기록  1~5. 관리자pc 이외의 위치에서 내부 서버망에 원격접속(ssh) 시도 탐지  6. X-MAS Scanning 탐지  7. TCP NULL Scanning 탐지  8. DOS (Ping of death 유형) 탐지  9. DBMS root 계정 접속 탐지 |

| **TEST - alert 1** |
| --- |
|  |

# 

| **FTP 정상 접근** | **로그 기록** |
| --- | --- |
|  | **텍스트, 전자제품, 스크린샷, 디스플레이이(가) 표시된 사진  자동 생성된 설명** |

# 

# 

| **TEST - alert 2** |
| --- |
|  |

# 

| **FTP 비인가접근** | **로그 기록** |
| --- | --- |
|  | 텍스트, 전자제품, 스크린샷, 디스플레이이(가) 표시된 사진  자동 생성된 설명 |

# 

# 

| **TEST - alert 3** |
| --- |
|  |

# 

# 

| **X-MAS Scan 공격** | **로그 기록** |
| --- | --- |
|  | 텍스트, 스크린샷, 평행, 폰트이(가) 표시된 사진  자동 생성된 설명 |

# 

**6.5 Firewall (linux)**

| **Routing 설정** |
| --- |
|  |
| zebra와 ospfd를 이용해 linux에서 동적 라우팅 프로토콜 (ospf)동작을 활성화 |

| **iptables 설정** |
| --- |
|  |
| iptables를 통해 ssh 연결시도 (tcp 22번 port 접근시도) 를 관리자 pc이외에 전부 DROP 하도록 설정 |

| **ssh 접근 시도** |
| --- |
|  |
| 좌) 비 관리자 pc 에서 ssh 접근 거부  우) 관리자 pc에서 ssh 접근 성공  관리자만 ssh 연결을 통해 내부 서버망의 local 작업이 가능하도록 구성되었음을 확인 |

**6.6 ESM**

| **WEB Server** |
| --- |
|  |
| WEB에서 iptables를 통해 log 기록 후 logstash와 filebeat를 이용하여 ESM server로 전달 |

| **IDS Device (linux)** |
| --- |
|  |
| filebeat로 ids의 로그 3종을 전부 수집하여 grok 필터를 통해 logstash로 원하는 index를 포함하여 ESM Server로 전달 |

| **Grok pattern 적용 결과 조회** |
| --- |
|  |
| Kibana에서 index document를 조회해 전달값이 정상적으로 전달되는 것을 확인 |

| **ESM Server - Kibana index 리매핑** |
| --- |
|  |
| kibana에 전달된 ids 인덱스 중, ip에 대한 정보가 field type keyword 로 매핑되어, ip 형태로 사용하기 위해 매핑 정보를 수정해야하나 불가능 하여 새 query를 통해 원하는 매핑 형태의 인덱스를 생성  1. 기존 매핑정보 확인 및 복사  2. 복사한 기본 매핑정보 중 source\_ip와 desination\_ip의 type을 ip로 수정하여 새 인덱스 생성  3. reindex를 통해 기존 데이터를 새 인덱스로 이동 |

| **ESM Server - Dashboard** |
| --- |
|  |
| Dashboard 구성  1. 1시간 당 웹 트래픽을 서버의 처리능력을 고려하여 %로 표시  2. 웹에 접속한 대상을 ip 기준으로 분류하여 막대그래프로 표시  3. IDS의 alert 로그 ID를 기준으로 위험도를 분류하여 단계 표시  4. 웹의 시간당 트래픽 사용량과 접속자 수를 숫자로 표시  5. 내부 서버망 트래픽 사용량을 도넛형태의 pie 그래프로 표시  6. 업무 부서별로 내부 서버망에 접근하는 횟수를 막대그래프로 표시  7. IDS의 로그 메시지를 tag cloud 형태로 표시  ※좌상단부터 우하단 기준 |

# 

# **6.7 기타 사항**

# 가) Backup 서버 구축

| **mysql 전체 백업** |
| --- |
|  |
| DB 서버에서 현재 DB 내용을 mysqldump 명령어를 통해 전체 백업 |

| **백업 데이터 전송** |
| --- |
|  |
| 백업 서버에서 rsync 명령어를 통해 백업된 자료 획득 |

| **cron 예약작업 - DB Server** |
| --- |
|  |
| DB server에서 cron을 통해 매 달 DB 전체 백업 작업 예약 |

| **cron 예약작업 - Backup Server** |
| --- |
|  |
| Backup Server에서 cron을 통해 매 달 rsync 동작을 통해 백업된 자료 동기화 작업 예약 |

# 

# 나) Session 서버 구축

| **Session Server** |
| --- |
|  |
| 외부에서 redis 접근 허용 |

| **Web Server** |
| --- |
|  |
| Web 서버의 php.ini 파일에서 php 동작 시 세션 정보를 redis를 통해 Session 서버에 전송하도록 설정 |

# 

| **redis monitoring** |
| --- |
|  |
| 웹 이용 시 redis를 이용해 session 정보 사용을 확인 |

# 

# 

# 다) DBMS 계정 관리

# 

| **적용 전** | **적용 사항** |
| --- | --- |
|  |  |
| 기본 계정의 비밀번호를 유추하기 어려운 비밀번호로 변경 | |

# 

| **적용 전** | **적용 사항** |
| --- | --- |
|  |  |
| 모든 host 대상으로 허용된 계정 삭제 | |

# 

# 

# 라) **DNS 보안 설정**

# 

| **적용 전** | **적용 후** |
| --- | --- |
|  |  |
| DNS zone transfer 취약점에 대한 조치사항으로 transfer 및 update는 로컬에서만 허용하도록 보안 설정 | |

# 

| **적용 전** | **적용 후** |
| --- | --- |
|  |  |
| 불필요한 정보가 노출될 가능성을 없애기 위해 ftp 와 db 레코드를 삭제처리 | |

# 

**7. 메뉴얼 작성**

| **사용자 메뉴얼** | | |
| --- | --- | --- |
| **No.** | **항목** | **내용** |
| 1 | FTP | 인가된 부서 계정으로만 접근 (사용자 PC) |
| 2 | FTP | 계정 필요시 관리자에게 요청 (사용자 PC) |
| 3 | PC | 화면 보호기 5분으로 설정 후 사용 (사용자 PC) |
| 4 | PC | 계정 비밀번호 8자리 이상으로 사용 (사용자 PC) |
| 5 | PC | 관리자 PC 사용시 반드시 명부 작성 및 관리내용 기록 (관리 PC) |
| 6 | PC | Windows 방화벽 활성화 상태로 유지 (사용자 PC 및 관리 PC ) |
| 7 | 재택  근무 | VPN 을 통해서 접근 ( 허가받은 이동식 PC 유형 ) |
| 8 | VPN 접속 | 1. sophos IPsec client 를 실행 2. 할당 받은 계정 정보 입력 3. 로그인 후 connection 버튼 활성화 확인   \* ( 허가받은 이동식 PC 유형 ) |

| **관리자 메뉴얼** | | |
| --- | --- | --- |
| **No.** | **항목** | **내용** |
| 1 | FTP | 계정 추가 방법   1. 행정팀    1. adm[번호] 형태로 ID 발급    2. 발급한 ID의 홈 디렉터리를 /home/km 으로 변경    3. 발급한 ID를 Group adm1, adm1\_plansail, dev\_adm1\_design 에 추가 2. 영업/기획    1. plan\_sail[번호] 형태로 ID 발급    2. 발급한 ID의 홈 디렉터리를 /home/km 으로 변경    3. 발급한 ID를 Group plan\_sail, adm1\_plansail,   dev\_plansail 에 추가   1. 디자인    1. design[번호] 형태로 ID 발급    2. 발급한 ID의 홈 디렉터리를 /home/km 으로 변경    3. 발급한 ID를 Group design, dev\_adm1\_design에   추가   1. 개발    1. dev[번호] 형태로 ID 발급    2. 발급한 ID의 홈 디렉터리를 /home/km 으로 변경    3. 발급한 ID를 Group dev, dev\_plansail,   dev\_adm1\_design 에 추가 |
| 2 | 내부  서버망 | 지정된 관리자 PC를 통해서 ssh 원격접근 |
| 3 | UTM | UTM 장비에 PC를 연결하여 접근 |
| 4 | UTM | 내부 서버망의 외부 연결 요청 시, Mascurading 규칙 ‘n’번을 일시적으로 활성화  \* 사용 후 반드시 비활성화 상태로 복구해야함 |
| 5 | UTM | VPN 계정 생성 방법   1. 사용자 계정 생성      1. IPsec 원격 액세스에 계정 추가      1. 재택근무자 PC에 사전 공유키 등록   \* 사전 공유 키가 알려지지 않도록 반드시 관리자가 직접 PC에 등록해주어야 함 |
| 6 | WAF | DMZ Server zone 스위치에 PC를 연결하여 접근 |
| 7 | DBMS | 관리자 계정 이외의 기존 계정 삭제 및 수정 금지  \* 부득이하게 수정해야 할 경우 WEB php code 의 ‘mysql\_connect’ 함수의 인자값 수정 필요 |
| 8 | ESM | 웹 트래픽이 70% 이상일 경우 웹 서비스에 문제가 생길 수 있음 |
| 9 | ESM | 위험 단계 1단계 -> 정상적인 상태  위험 단계 2단계 -> 비정상적인 접근 가능성이 있으므로 로그 메세지 확인 후 실제 업무내용을 비교하여 공격 가능성 확인 요망  위험 단계 3단계 -> 내부 서버가 공격당했을 가능성이 높으므로 서버 점검 요망 |
| 10 | ESM | ids indices 삭제 금지  \* 삭제 시 ip 기반 visualize 동작 불가 |
| 11 | IDS | snort log type   * alert1 : 정상 사용 트래픽 분류 * alert2 : 잘못된 접근 분류 * alert3 : 공격 탐지 분류 |
| 12 | IDS | log type 추가 방법   1. rule 파일 설정 추가   alert[숫자], LOG\_LOCAL[숫자] 형태로 구성 추천   1. rsyslog.conf log 기록 설정   위의 형태로 로그파일 기록 추가  \* 일반 alert log 사용은 권장하지 않음 |

참고 자료 :

kisa - 주요정보통신기반시설\_기술적\_취약점\_분석\_평가\_방법\_상세가이드 ( 2021.03.31 )

Elastic 가이드 북 ‘https://esbook.kimjmin.net/’ ( 2023 - 09 - 22 )

KT - 웹 방화벽(WAF) User Guide