DevSecOps 시스템 보안 과제

평가자 체크 리스트 B

작성자: 정재호

작성일: 2024.10.04

# 목차

[목차 2](#_Toc178956295)

[1. Victim(wordpress) 스캐닝 결과 4](#_Toc178956296)

[1.1. nmap 4](#_Toc178956297)

[1.2. nikto 4](#_Toc178956298)

[1.3. dirb 5](#_Toc178956299)

[1.4. wordpress 버전 확인 5](#_Toc178956300)

[1.5. wpscan 6](#_Toc178956301)

[1.6. WP-admin 접속 6](#_Toc178956302)

[1.7. zap tool: proxy 설정 7](#_Toc178956303)

[1.8. hydra: 브루트 포스 공격 7](#_Toc178956304)

[1.9. 관리자 계정 접속 8](#_Toc178956305)

[2. Linux Web/Log 서버 구축 8](#_Toc178956306)

[2.1. Linux Web/Log 서버 구축 8](#_Toc178956307)

[2.2. root 계정 ssh 로그인 거부 설정 11](#_Toc178956308)

[2.3. Https 설정 12](#_Toc178956309)

[3. DDoS 공격 실습 13](#_Toc178956310)

[3.1. Kali DDoS Attack 명령어 13](#_Toc178956311)

[3.2. Wireshack 13](#_Toc178956312)

[4. Sticky Bit 설정 14](#_Toc178956313)

[4.1. Sticky Bit 설정 14](#_Toc178956314)

[4.2. root 외 계정으로 삭제 시도 14](#_Toc178956315)

[5. 패스워드 복잡성 설정 14](#_Toc178956316)

[5.1. 패스워드 복잡성 설정 15](#_Toc178956317)

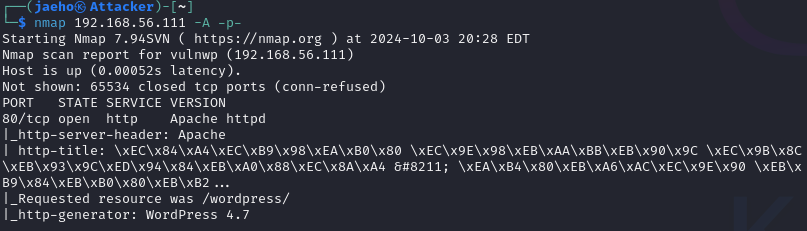
[5.2. 패스워드 만료일 설정 15](#_Toc178956318)

[6. 로그 관리 16](#_Toc178956319)

[6.1. 로그인 성공 기록 확인 16](#_Toc178956320)

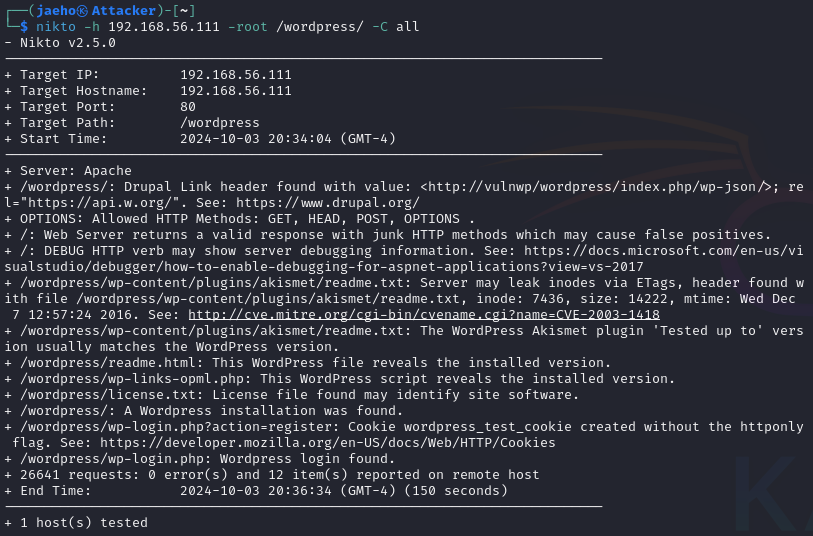
# 1. Victim(wordpress) 스캐닝 결과

## 1.1. nmap



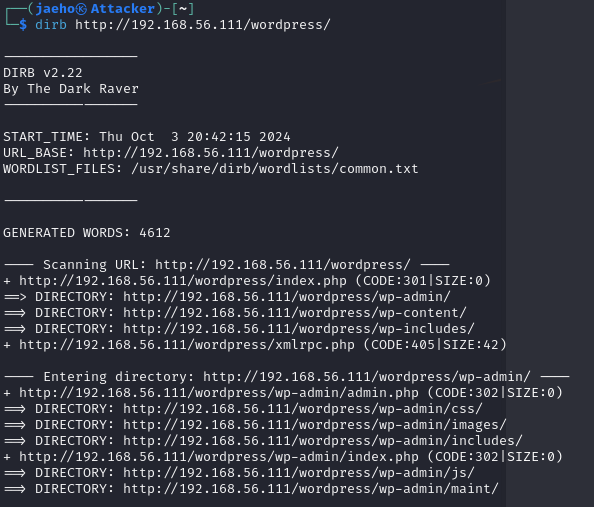
- victim 머신 nmap 스캐닝 결과 > wordpress로 구현된 서버 확인

## 1.2. nikto



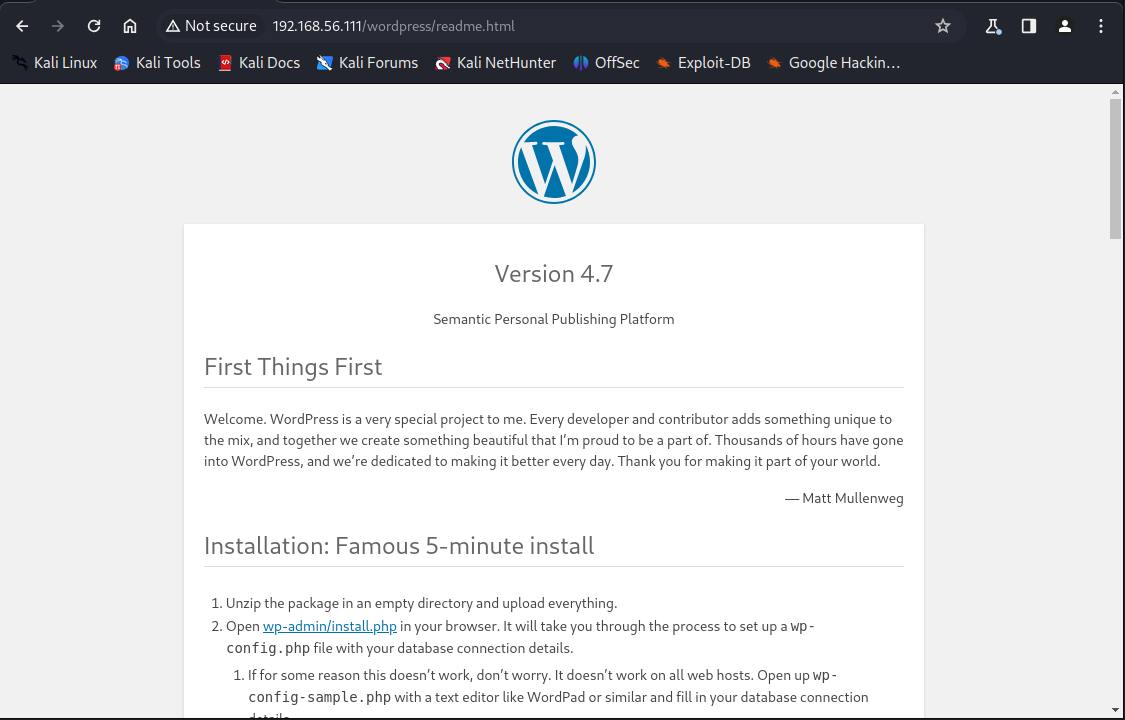
- nmap 스캐닝 결과로 알아낸 `/wordpress/`디렉터리의 취약점 탐색 > CVE-2003-1418 확인

## 1.3. dirb



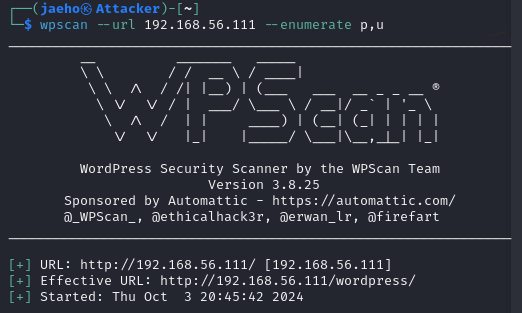
- wordpress 디렉터리에 접속 가능한 웹 디렉터리/파일 탐색> /WP-admin/ 확인

## 1.4. wordpress 버전 확인



* 워드프레스 버전 확인

## 1.5. wpscan

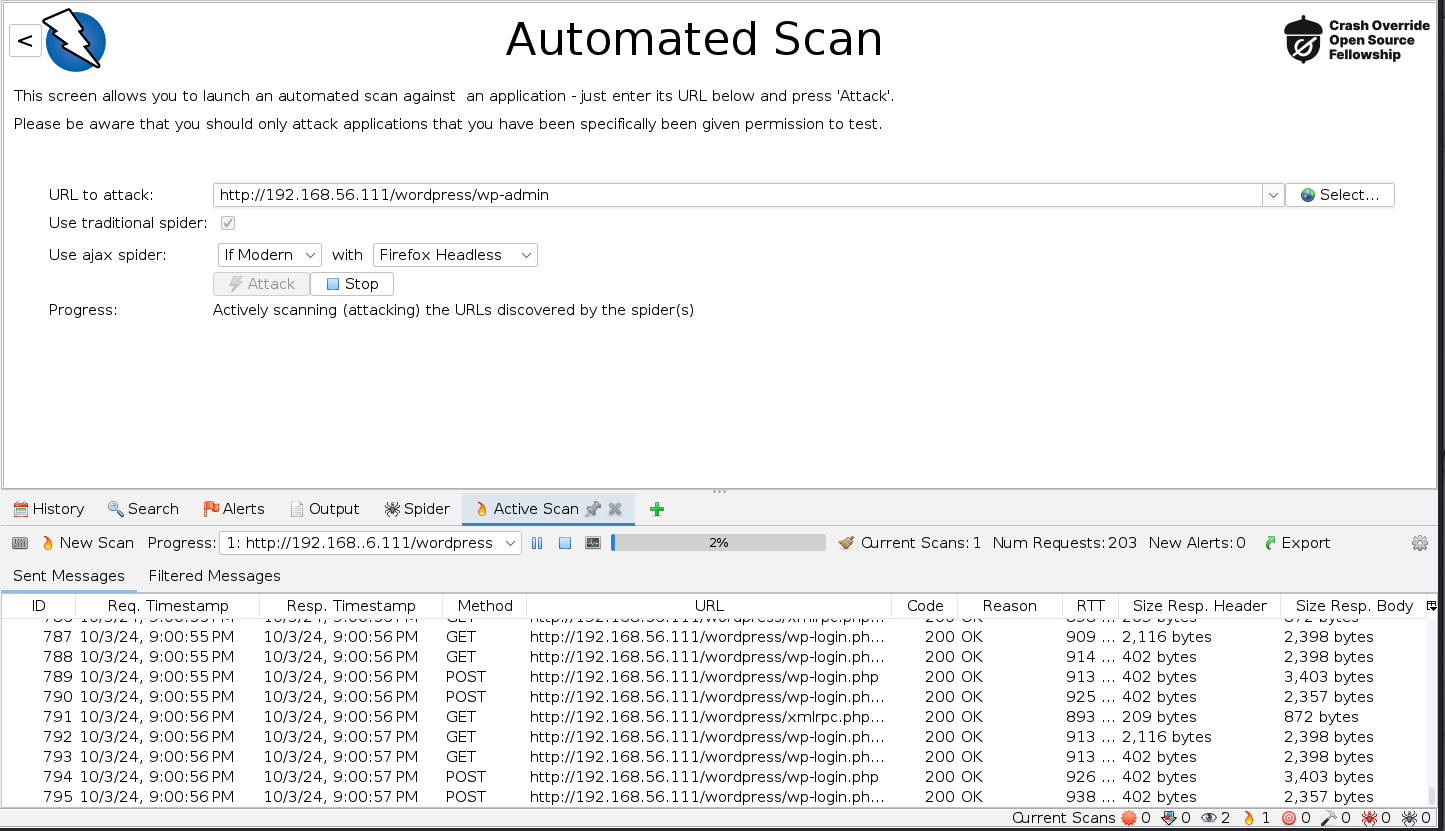


## 1.6. WP-admin 접속

|  |  |
| --- | --- |
|  |  |
| wordpress:wordpress  유효하지 않는 사용자명 | admin:admin  admin에 대한 비밀번호가 틀립니다. |

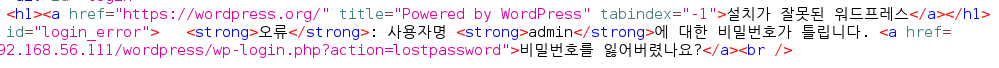
* admin 계정의 존재 확인

## 1.7. zap tool: proxy 설정

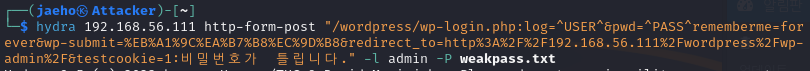


|  |  |
| --- | --- |
|  |  |
| 로그인 요청 시 보내는 post 값 | 결과로 응답하는 html 코드 |

## 1.8. hydra: 브루트 포스 공격

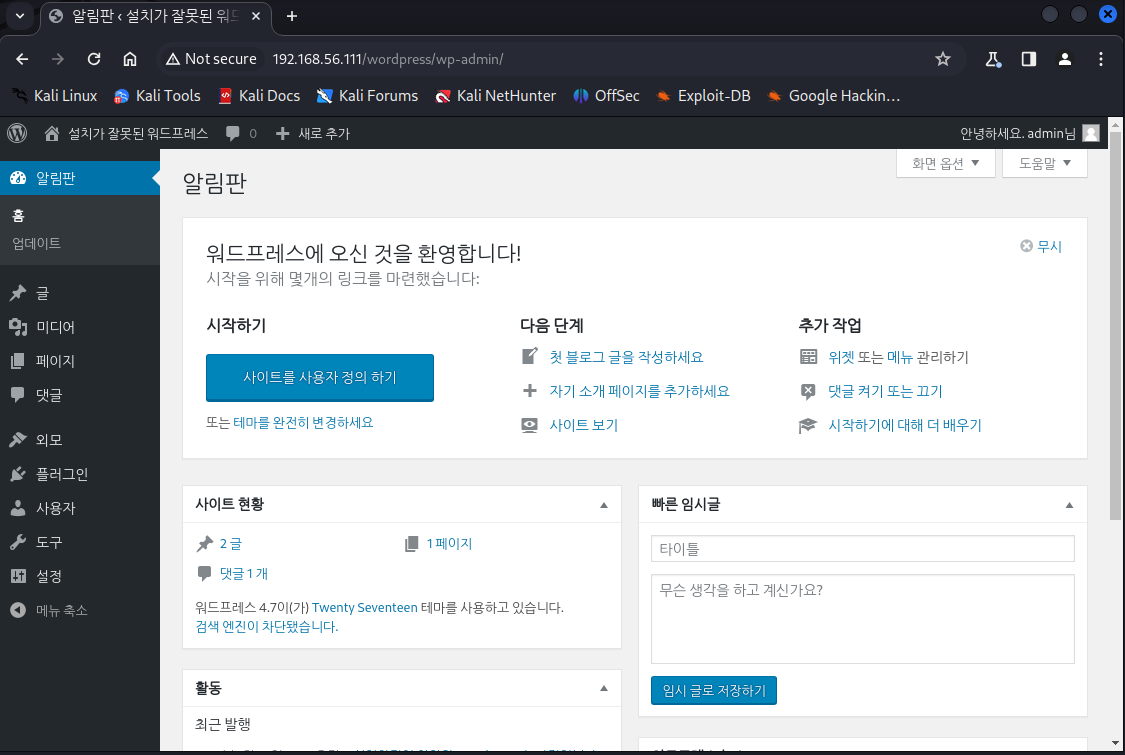


* 유효한 사용자 이름으로 로그인 시 반환하는 결과 값을 이용한 브루트 포스 공격





## 1.9. 관리자 계정 접속



- 획득한 관리자 계정과 비밀번호를 활용해 관리 페이지에 접속

# 2. Linux Web/Log 서버 구축

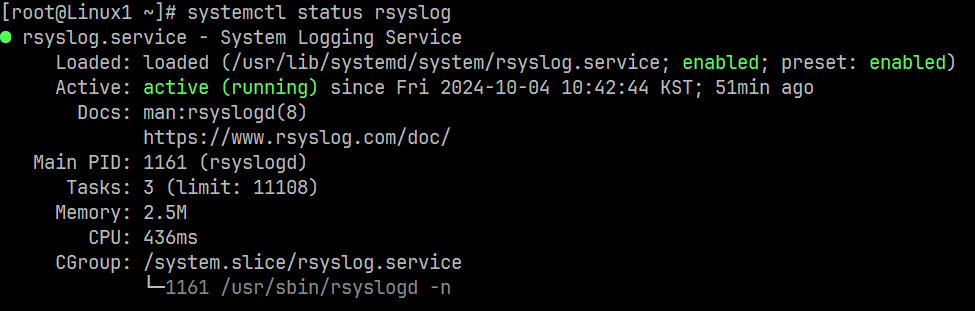
## 2.1. Linux Web/Log 서버 구축

### 1) 패키지 설치

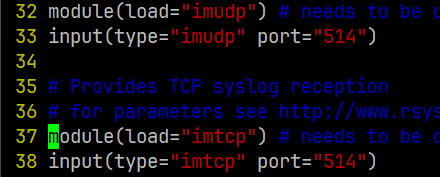
`dnf update -y && dnf install -y rsyslog rsyslog-doc`

### 2) 서비스 활성화

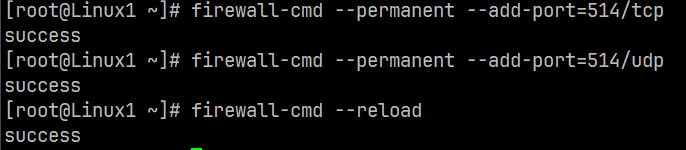
`systemctl start rsyslog && systemctl enable rsyslog`



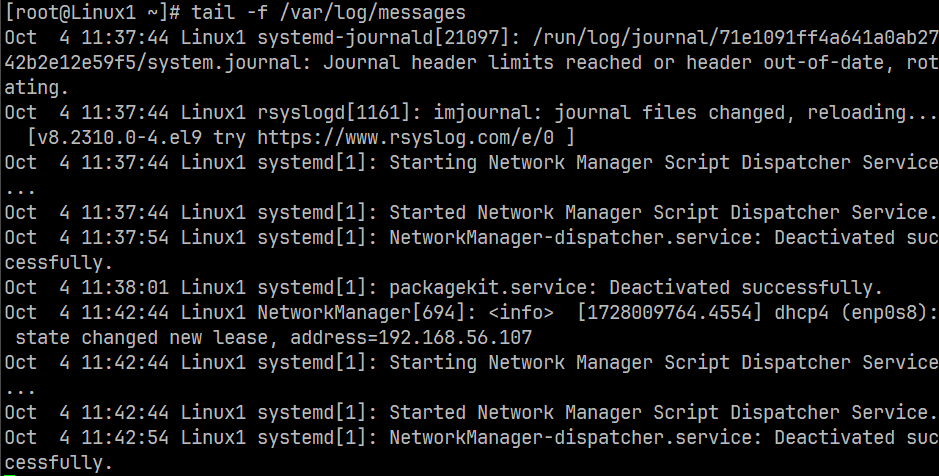
### 3) vi /etc/rsyslog.conf 수정



### 4) 방화벽 설정



### 5) log 출력 상태 확인



### 6) Log DB 구축: mariadb 설치 및 시스템 활성화

`dnf install -y mariadb\* rsyslog-mysql && systemctl start mariadb && systemctl enable mariadb`

### 7) mariadb 설정

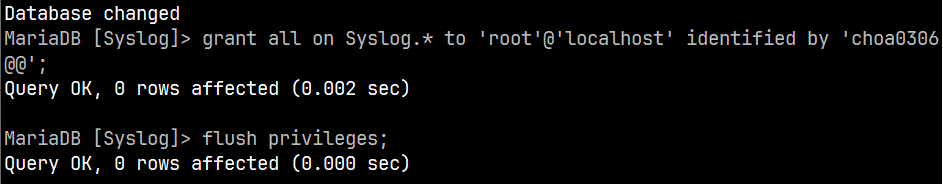
` mysql\_secure\_installation`

### 8) DB 생성

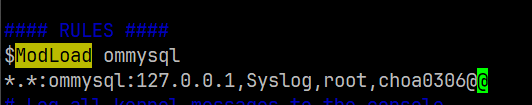
`mysql -u root -p < /usr/share/doc/rsyslog/mysql-createDB.sql`

|  |  |
| --- | --- |
|  |  |
| 생성 후 DB 상태 | Syslog DB 테이블 상태 |

### 9) DB 사용 권한 설정



### 10) rsyslog.conf 수정



11) Loganalyzer 설치

```

wget <http://download.adiscon.com/loganalyzer/loganalyzer-4.1.10.tar.gz>

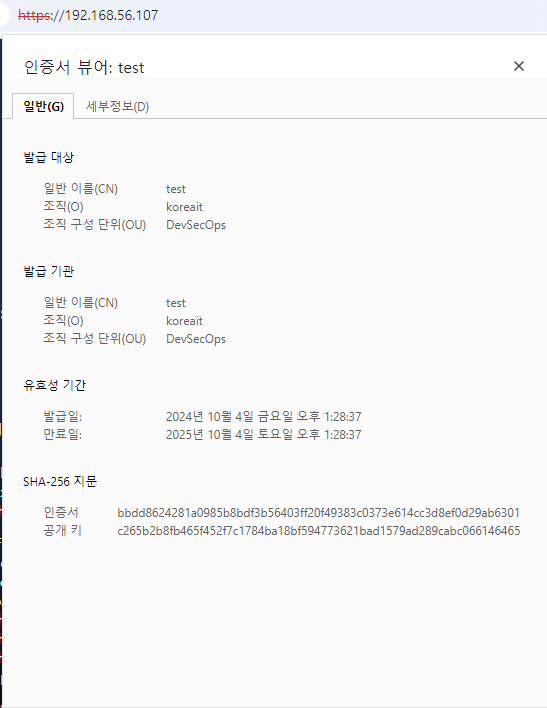
설치 과정에서 에러가 발생했습니다.

```

## 2.2. root 계정 ssh 로그인 거부 설정

|  |  |
| --- | --- |
|  |  |
| /etc/sshd/sshd\_config 설정 | 적용 결과 확인 |

## 2.3. Https 설정

# 3. DDoS 공격 실습

## 3.1. Kali DDoS Attack 명령어



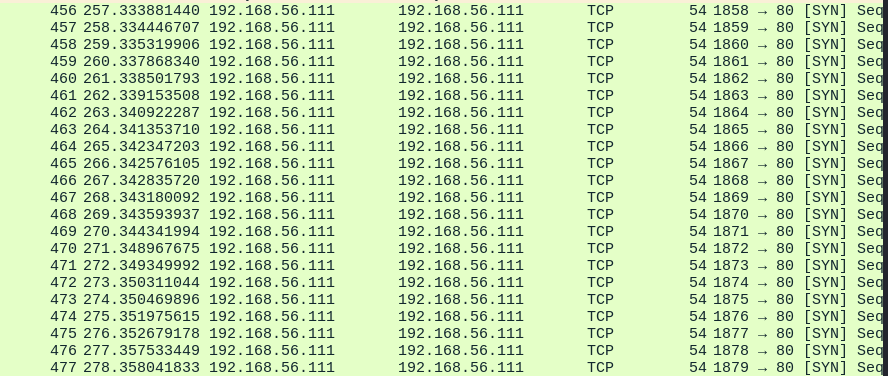
- hping3 tool을 활용

- 192.168.56.111(wordpress) 웹 서버를 대상으로 DDoS 공격 시도

- `-S`: SYN 플래그 설정

- `-a`: 소스 IP를 변조, 타겟 IP와 동일한 IP로 변경해 Land(Smurf)공격 시도

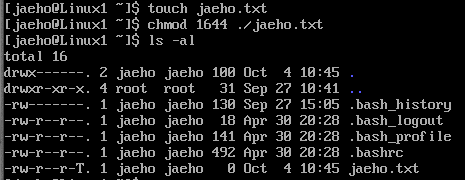
## 3.2. Wireshack



- Wireshack tool로 SYN 플래그 값의 DDoS 공격 형태 확인

# 4. Sticky Bit 설정

## 4.1. Sticky Bit 설정



- /home/jaeho/jaeho.txt 파일 생성 후 sticky bit 설정

## 4.2. root 외 계정으로 삭제 시도

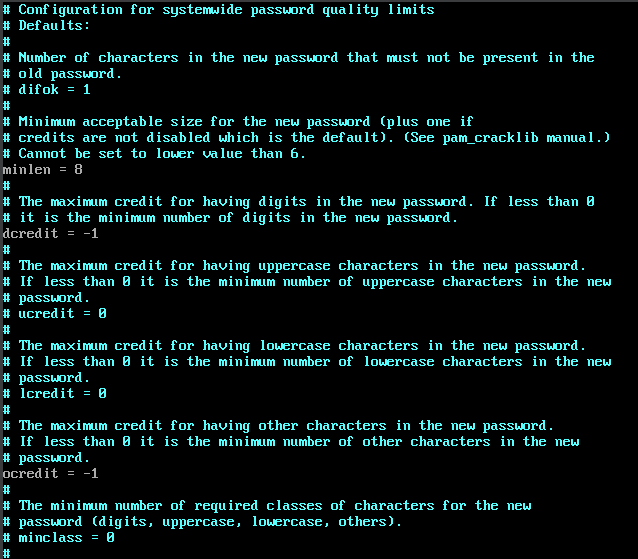


- sticky bit 설정이 정상적으로 적용된 것을 확인

# 5. 패스워드 복잡성 설정

- 조건: 특수문자, 숫자 최소 1개 이상, 최소 8글자 이상, 패스워드 만료일 60일

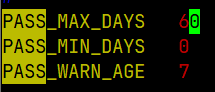
## 5.1. 패스워드 복잡성 설정



(minlen = 8, dcredit = -1, ocredit = -1)

## 5.2. 패스워드 만료일 설정

### 1) vi /etc/login.defs



### 2) chage -d 60 <사용자계정>



- chage -d 명령어로 패스워드 만료일 설정

# 6. 로그 관리

## 6.1. 로그인 성공 기록 확인

|  |  |
| --- | --- |
|  |  |
| last | last -f /var/log/wtmp |

### 6.2. 로그인 실패 기록 확인

|  |  |
| --- | --- |
|  |  |
| lastb | last -f /var/log/btmp |