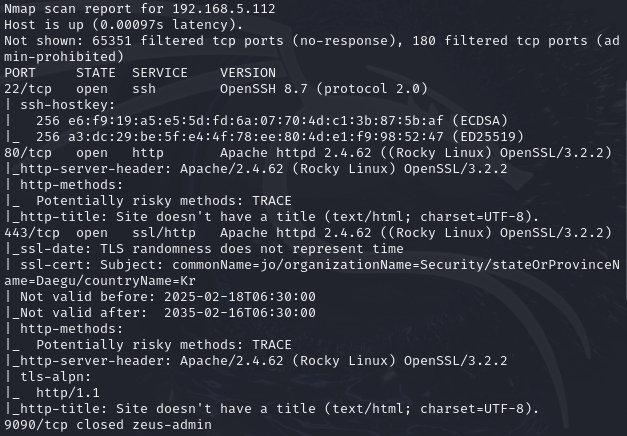
**1.1**

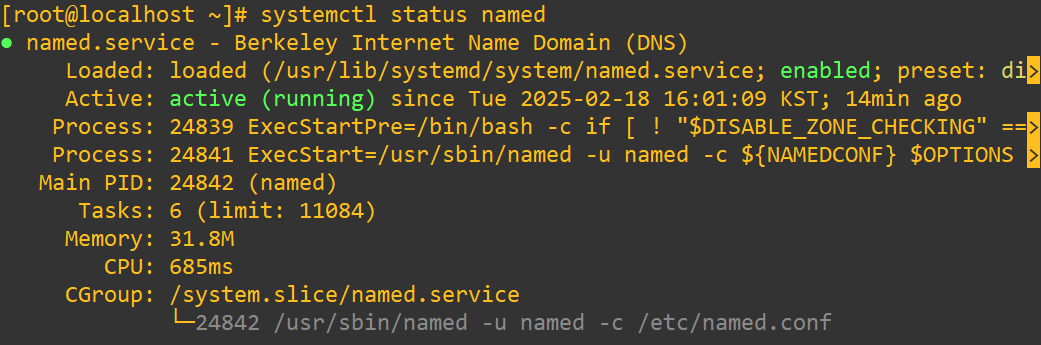
**Attaker(kali) -> Victim(wordpress) (web server) 로의 스캐닝을 통해 취약점을 확인하시오.**



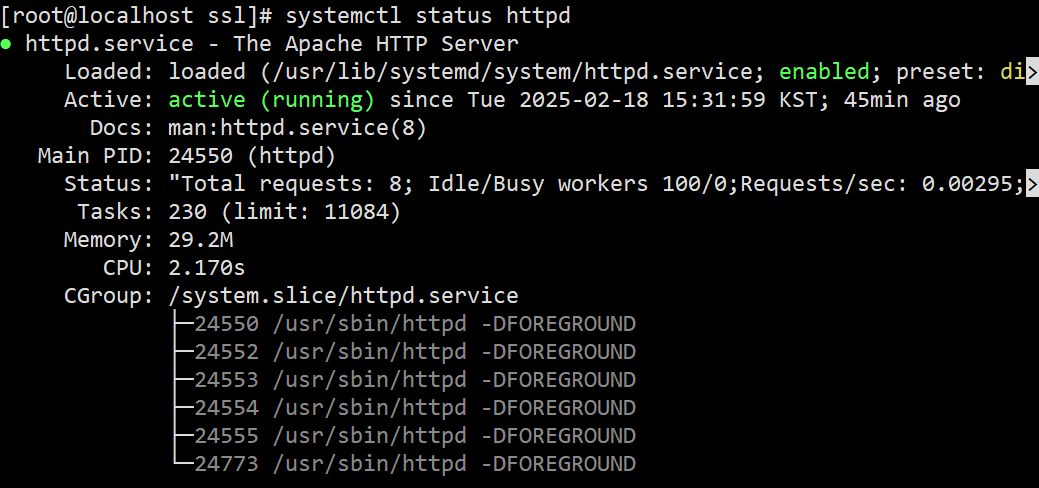
스캐닝을 통한 취약점 확인

**1.2 ~ 1.4**

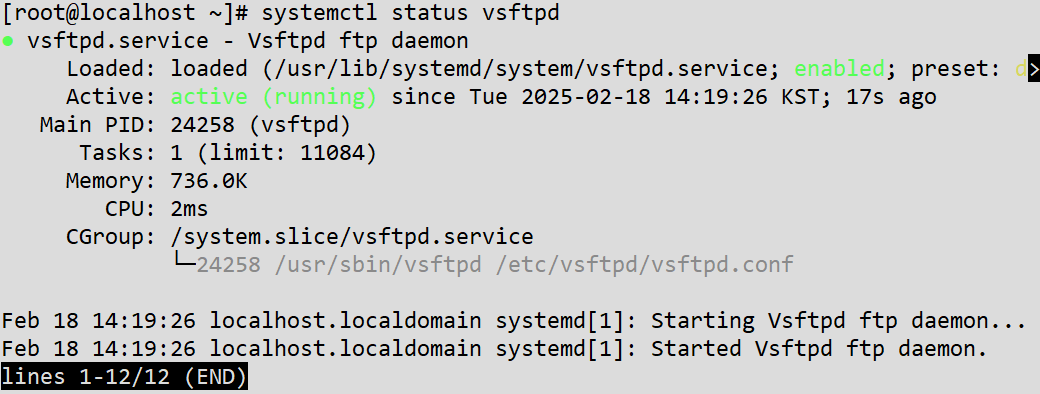
**- 리눅스 시스템에 DNS / WEB(HTTP) / FTP 서버를 구축하시오,**



Name Server 구축

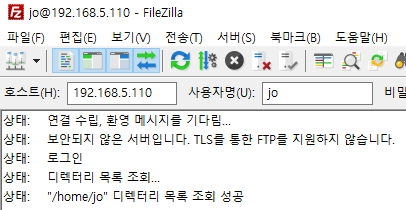
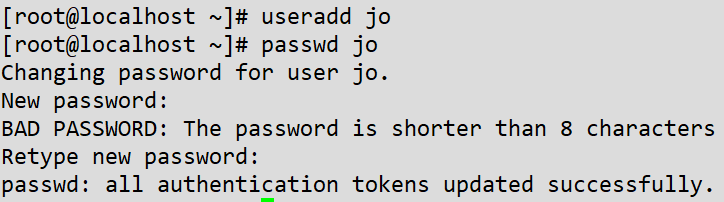


HTTP Server 구축

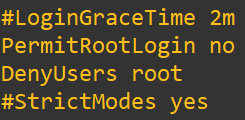


FTP Server 구축

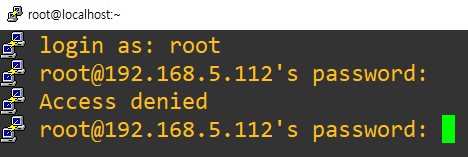
**- FTP 접속 시 본인 이름의 계정으로 접속 가능하도록 설정**



본인 이름 계정(jo)으로 접속 확인

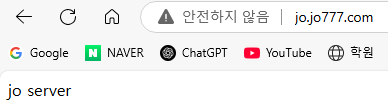
**- SSH 접속 시 root 사용자 원격 접속 허용 안되게 설정(web)  
**

명령어 입력

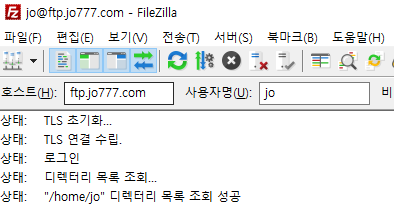
****

Root 계정 SSH 접속 불가 확인

**- 도메인으로 서버(WEB/FTP) 접속 가능하게 설정**



웹서버 도메인으로 접속 가능

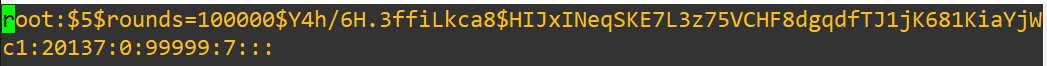


FTP 도메인으로 접속 가능

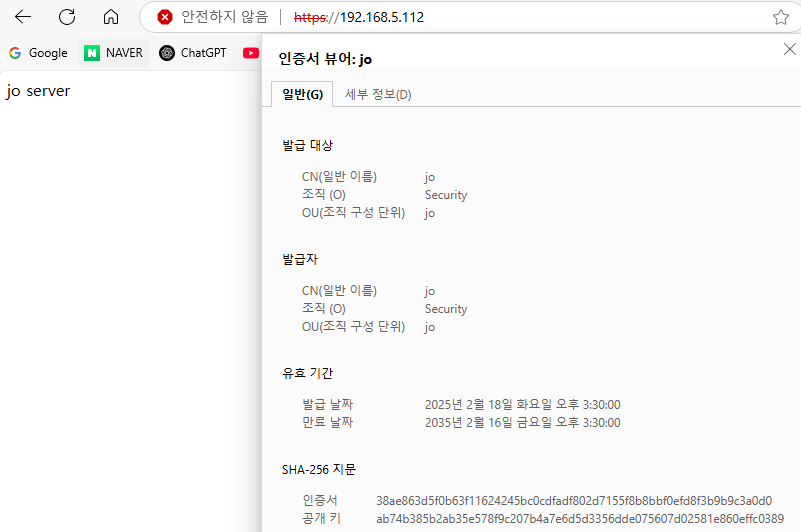
**2.1 ~ 2.3**

**- /etc/shadow 파일에서의 Salt에 대해 서술하고 암호화 알고리즘을 SHA256으로 변경하시오.**

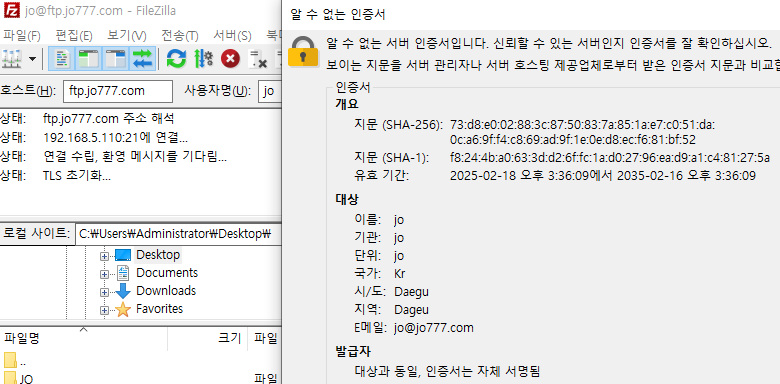
Salt란 암호화 된 패스워드를 생성할 때 사용되는 무작위 데이터로 기본 패스워드를 암호화 하면 동일한 결과가 나와 보안에 취약하지만 Salt를 추가하면 무작위로 암호화된 값이 생성되어 보안성이 크게 향상된다.

  
  
root 계정 암호화를 SHA512(기본)에서 SHA256으로 수정하였음

**- HTTPs 및 FTPs 설정을 하여 테스트하시오.**

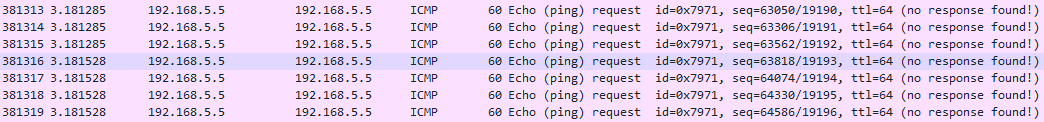


HTTPs 설정 후 테스트 화면



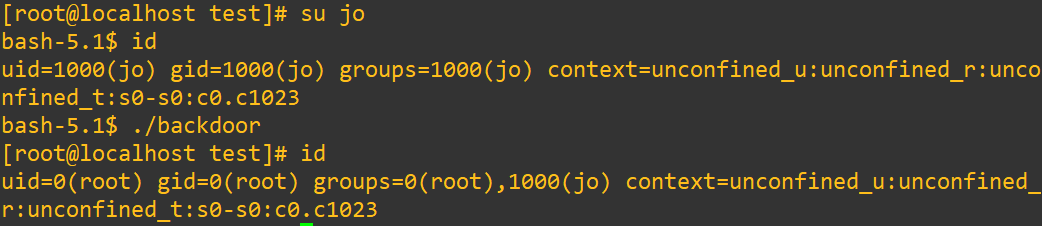
FTPs 설정 후 테스트 화면

**- DDoS(Land Attack) 공격을 실행하고 TCPDump 또는 Wireshark를 통해 패킷을 캡처하시오.**

****

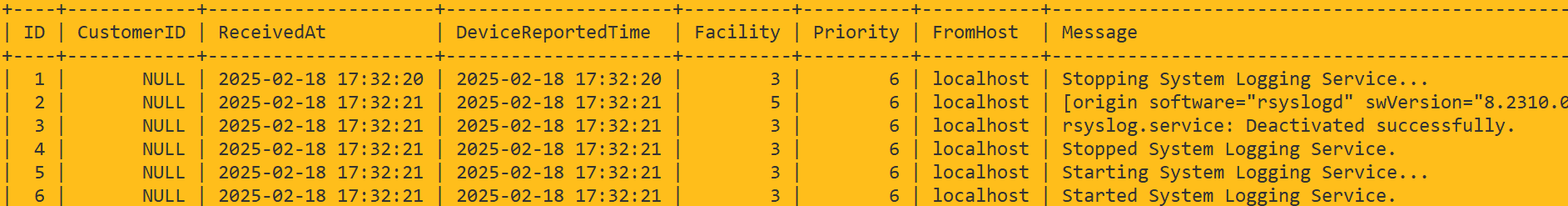
Land Attack에 의해 본인의 아이피로 공격이 온 걸 확인

**- SetUID를 활용한 권한 상승(root) 설정**

****

backdoor를 실행 한 후 권한이 상승된 것을 볼 수 있다

**- Log Server를 구축하여 FTP 서버의 Log를 실시간 확인하고 DB에 저장이 되도록 설정하시오.**



Log Server에 FTP서버의 로그를 받아와 DB에 저장되었다 (Client에서 systemctl restart rsyslog를 한 결과 로그 일부)