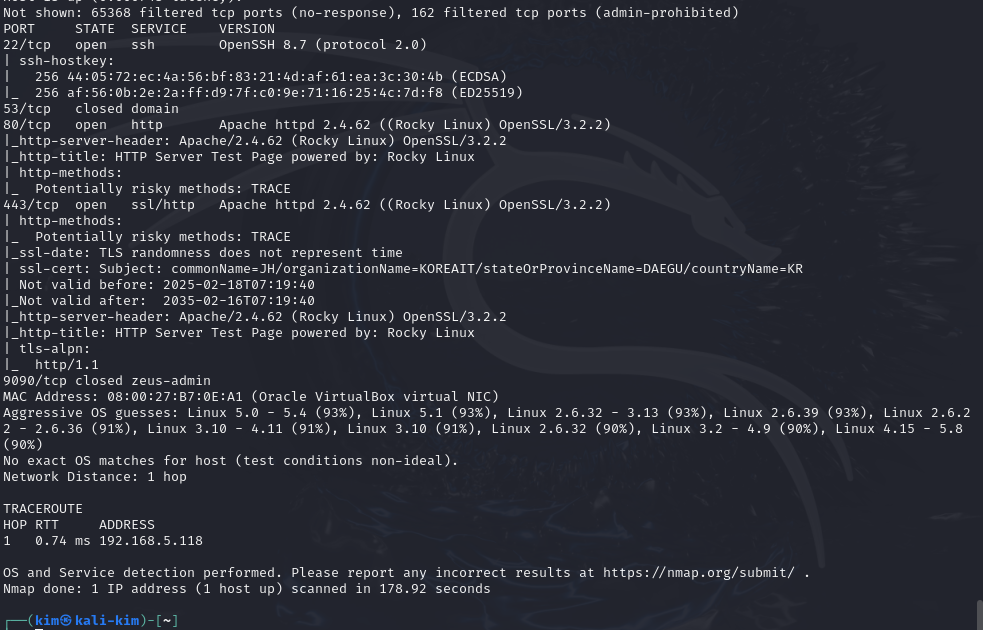
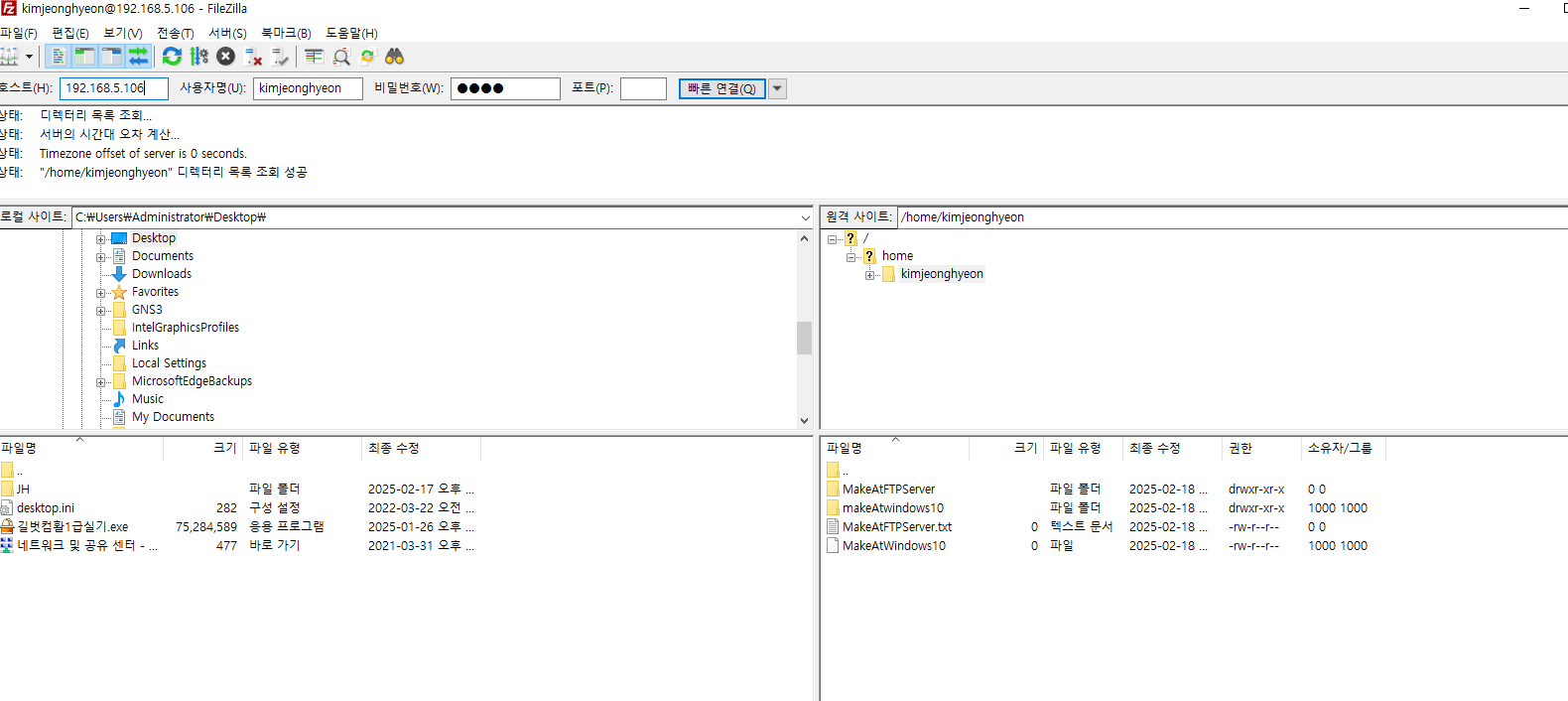
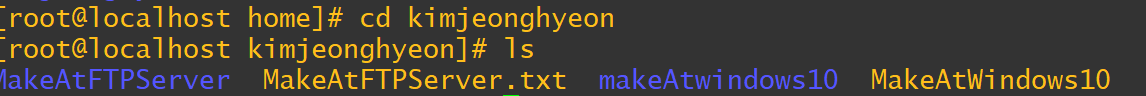
**1.1 Attaker(kali) -> Victim(wordpress) 로의 스캐닝을 통해 취약점을 확인하시오.  
**

**=>>kali에서 웹서버(.118) 스캐닝 출력화면**

**1.2 ~ 1.4**

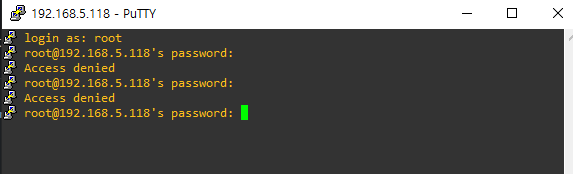
**리눅스 시스템에 DNS / WEB(HTTP) / FTP 서버를 구축하시오,**

**FTP 접속 시 본인 이름의 계정으로 접속 가능하도록 설정**

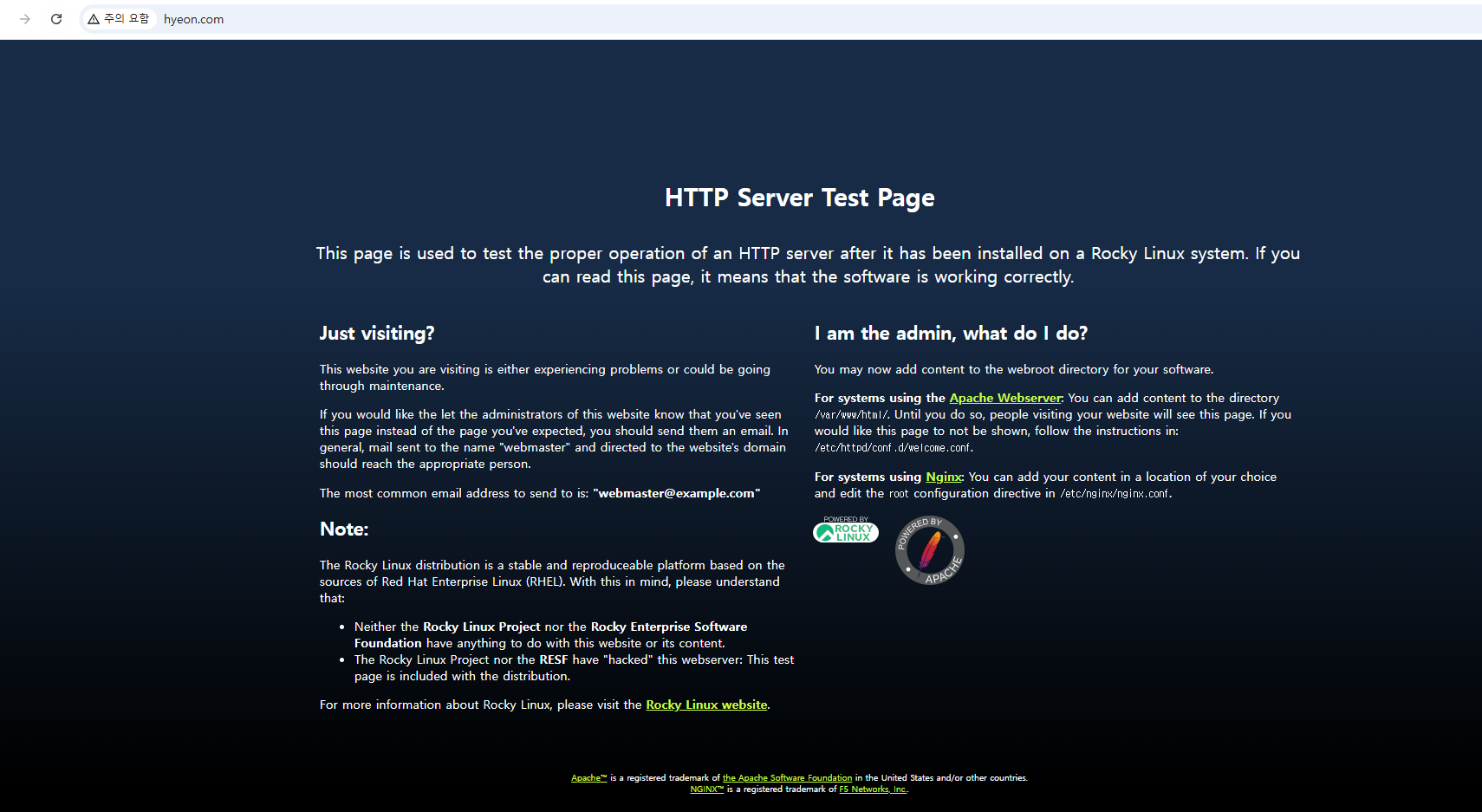
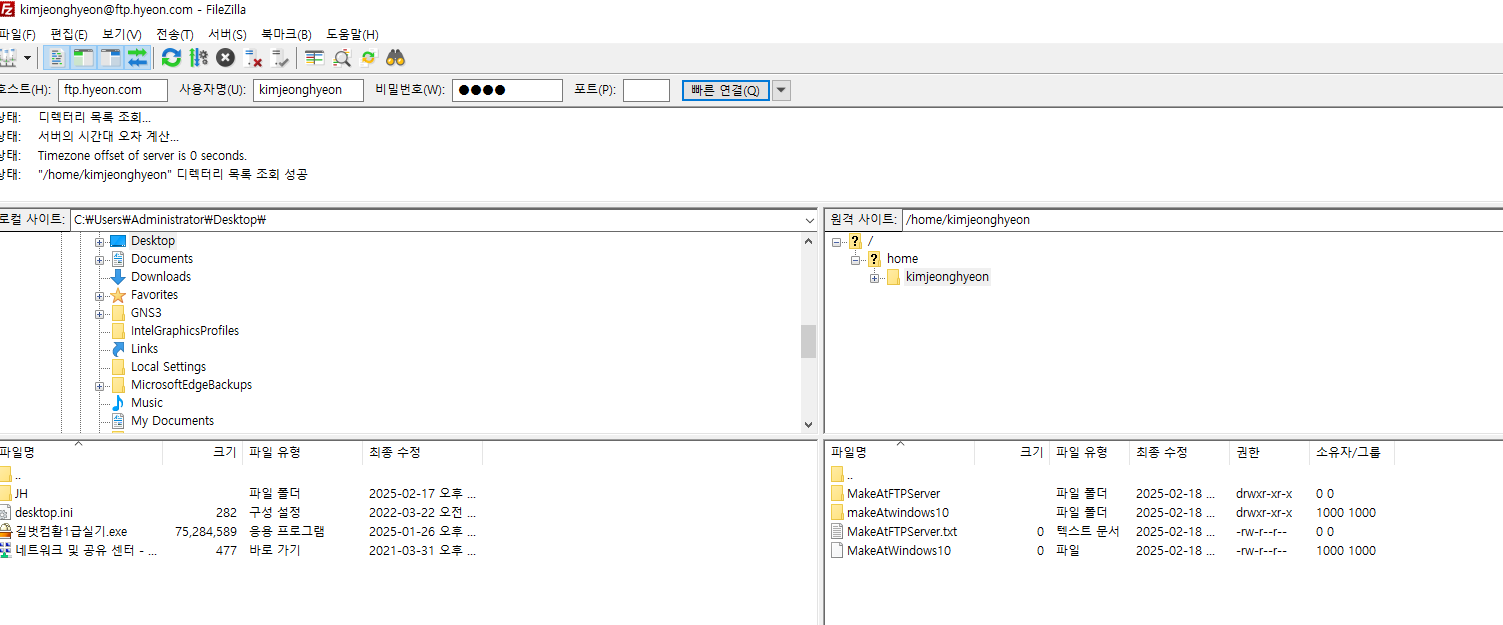
**  
=> 파일질라를 통한 FTP본인이름계정(kimjeonghyeon)으로 접속**

**=>FTP서버에서 공유가 되는 것을 확인**

**SSH 접속 시 root 사용자 원격 접속 허용 안되게 설정(web)  
  
  
=> 루트계정 SSH Deny 설정**

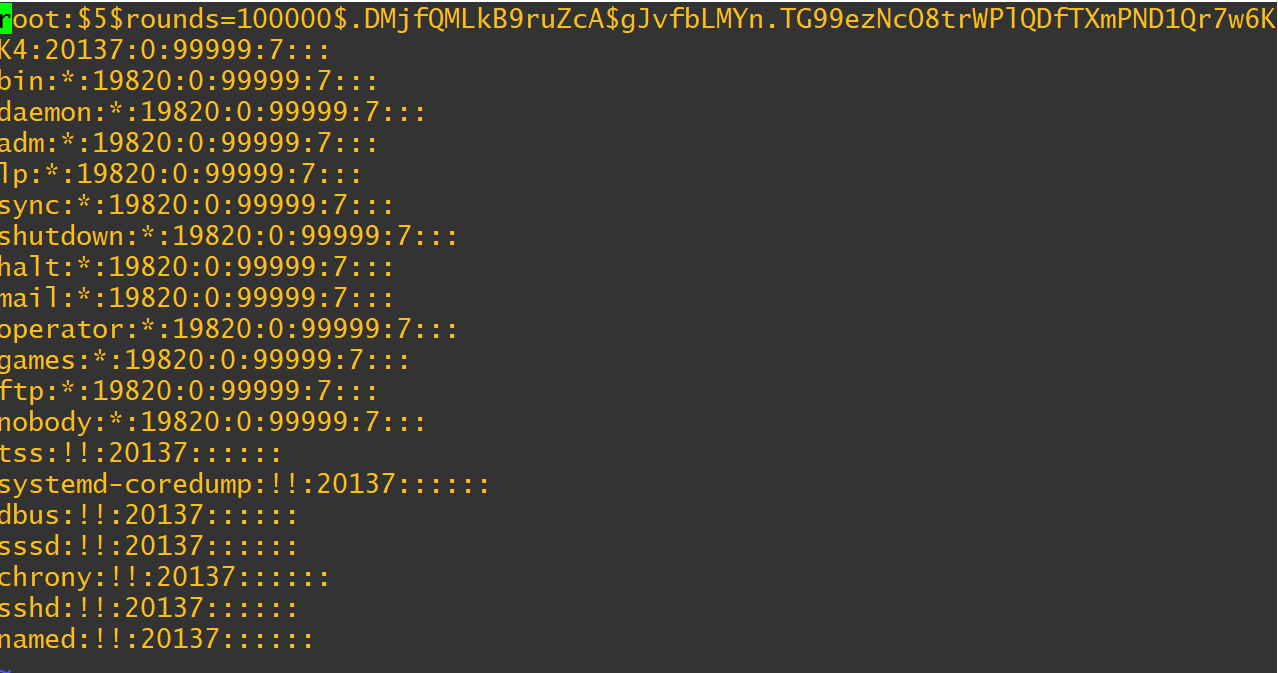
**  
=> root로 계정접속이 거부당하는 것을 확인**

**도메인으로 서버(WEB/FTP) 접속 가능하게 설정**

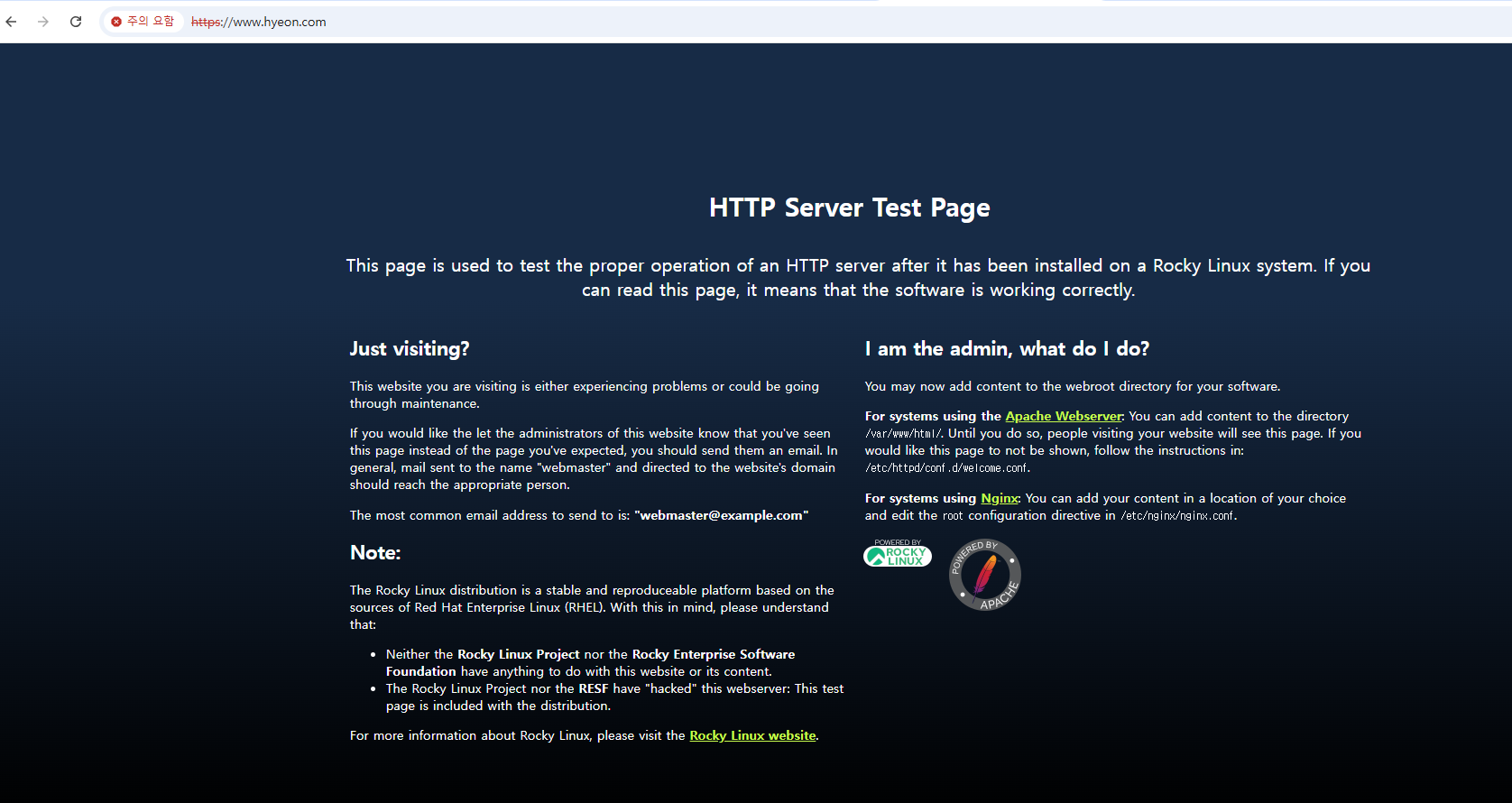
**  
=>도메인 설정 후 hyeon.com으로 접속  
  
  
=>도메인 설정 후 ftp 접속(host:** [**ftp.hyeon.com**](ftp://ftp.hyeon.com)**)**

**2.1 ~ 2.3**

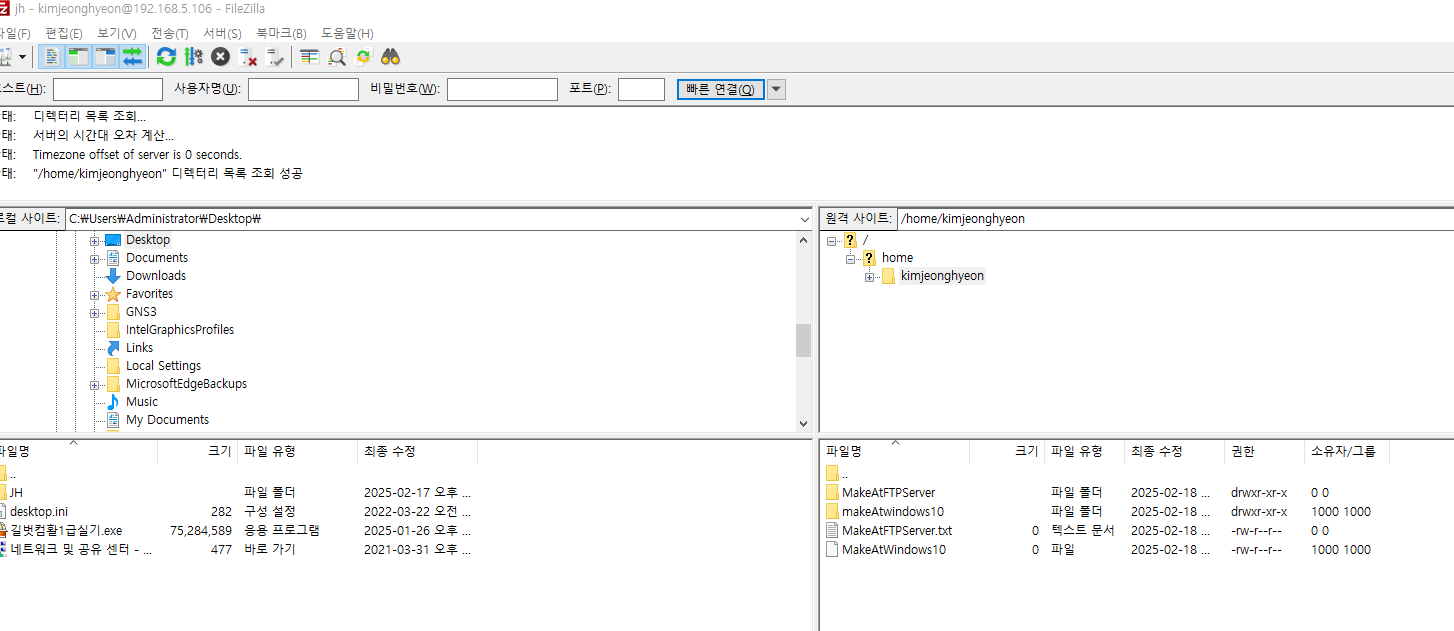
**- /etc/shadow 파일에서의 Salt에 대해 서술하고 암호화 알고리즘을 SHA256으로 변경하시오.**

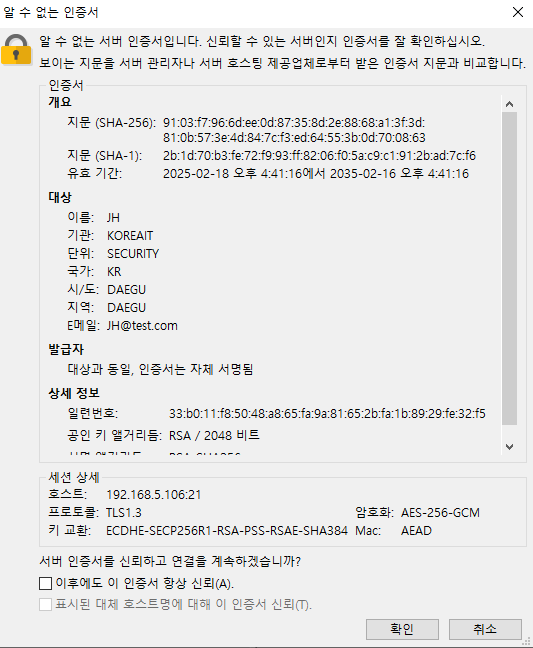
**=> Salt**는 해시화된 비밀번호의 **보안성을 강화**하기 위해 추가되는 **랜덤 값**입니다. 동일한 비밀번호라도 **Salt**가 다르면 암호화된 값이 달라지기 때문에, **다른 사용자의 비밀번호가 동일하더라도 암호화된 값이 다르게 생성됩니다.**  
  


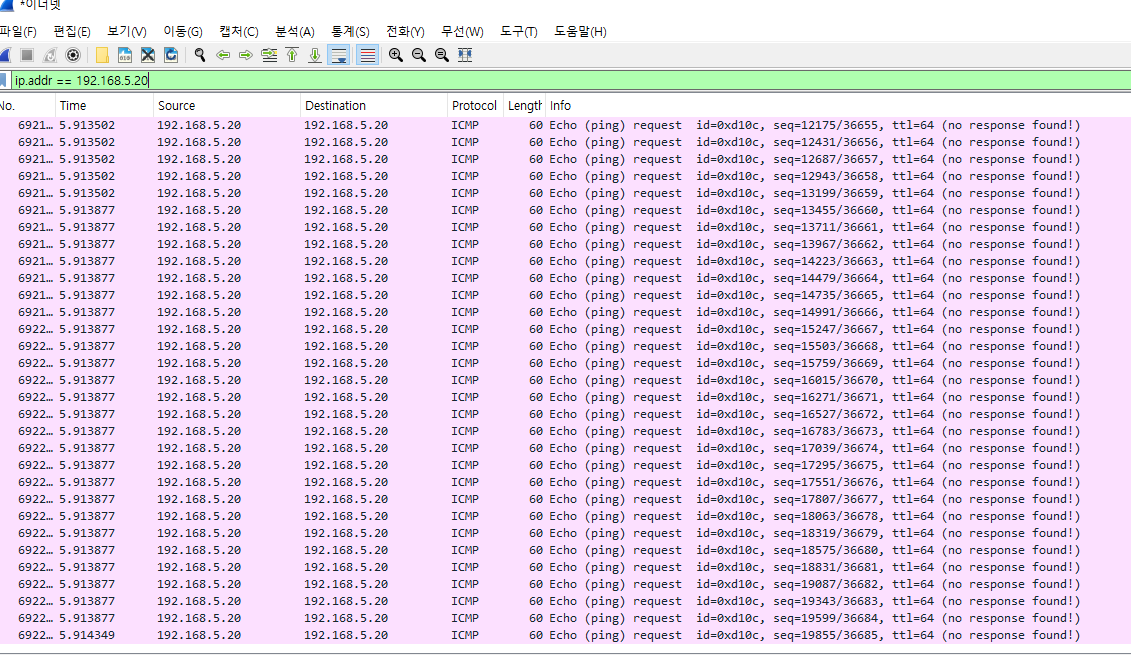
=>root계정암호화를 SHA512에서SHA256으로변경($5:$로 변경 되어 있는 걸 볼 수 있음)

**- HTTPs 및 FTPs 설정을 하여 테스트하시오.  
  
  
=>HTTPS 설정 후 웹화면**

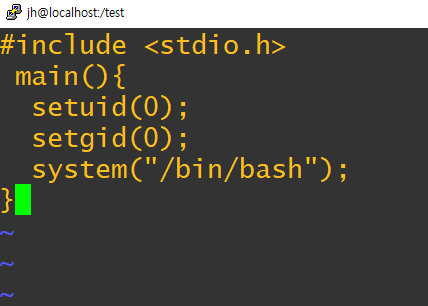
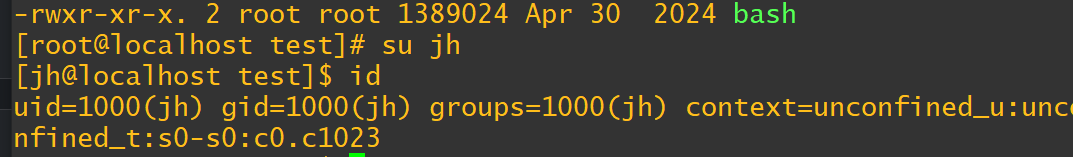
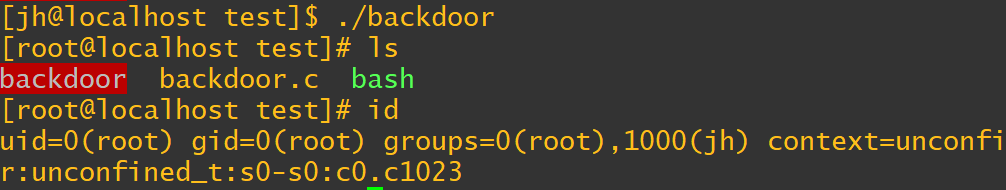
**  
=> 인증서 화면**

**  
=>FTPs 설정 후 연결시도**

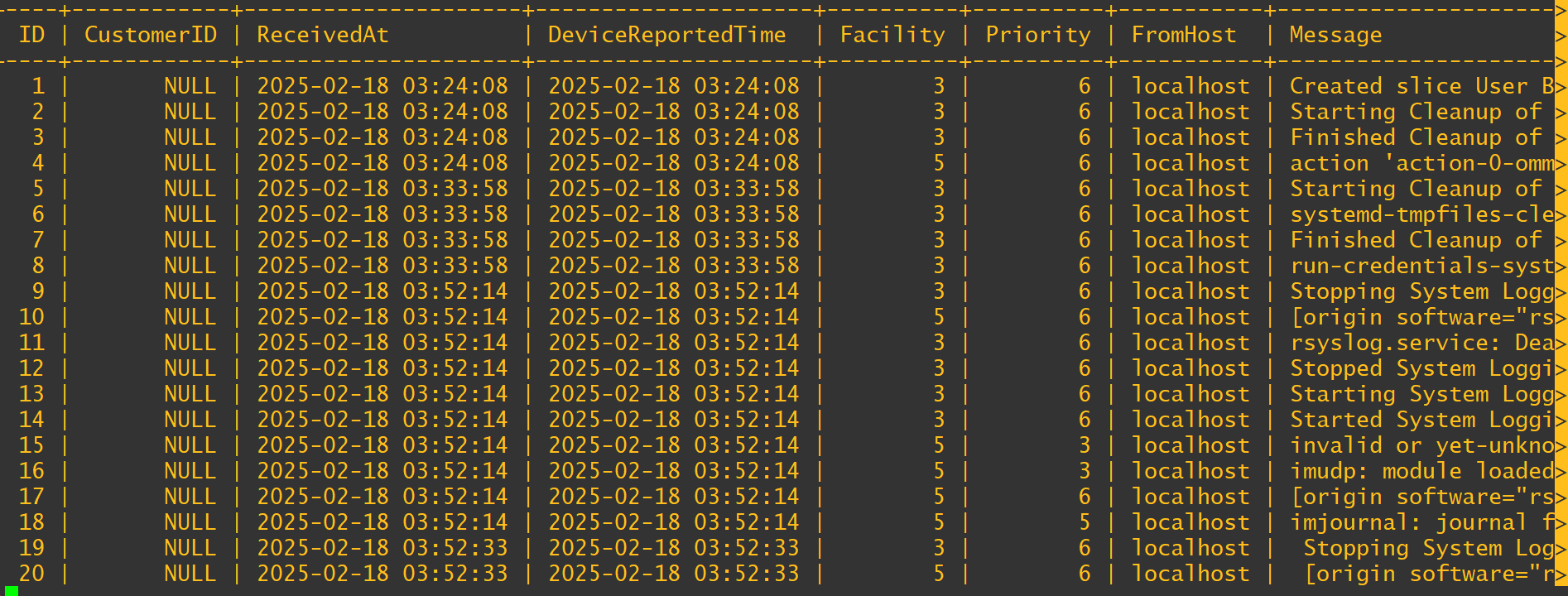
**  
=>FTPs 최초접속시 인증서 화면**

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

**=> kali리눅스에서 DDos공격(Land Attack) 와이어샤크로 감지**

**- SetUID를 활용한 권한 상승(root) 설정** **=>>백도어를위한 스크립트 작성** **=>>uid 및 gid jh(사용자계정) 으로 확인** **=>>backdoor파일 실행 후 root권한이 생긴 것을 확인 할 수 있음**

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

****  
**=>>FTP 서버로부터 Log데이터를 LogServer 디비에 적재**