1.1

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

```
Nmap scan report for 192.168.5.112
Host is up (0.00097s latency).
Not shown: 65351 filtered tcp ports (no-response), 180 filtered tcp ports (ad
min-prohibited)
PORT     STATE  SERVICE    VERSION
22/tcp   open   ssh        OpenSSH 8.7 (protocol 2.0)
| ssh-hostkey:
|   256 e6:f9:19:a5:e5:5d:fd:6a:07:70:4d:c1:3b:87:5b:af (ECDSA)
|_  256 a3:dc:29:be:5f:e4:4f:78:ee:80:4d:e1:f9:98:52:47 (ED25519)
80/tcp   open   http       Apache httpd 2.4.62 ((Rocky Linux) OpenSSL/3.2.2)
|_http-server-header: Apache/2.4.62 (Rocky Linux) OpenSSL/3.2.2
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
443/tcp  open   ssl/http   Apache httpd 2.4.62 ((Rocky Linux) OpenSSL/3.2.2)
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=jo/organizationName=Security/stateOrProvinceN
ame=Daegu/countryName=Kr
| Not valid before: 2025-02-18T06:30:00
|_Not valid after:  2035-02-16T06:30:00
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.62 (Rocky Linux) OpenSSL/3.2.2
| tls-alpn:
|_  http/1.1
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
9090/tcp closed zeus-admin
```

스캐닝을 통한 취약점 확인

1.2 ~ 1.4

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

```
[root@localhost ~]# systemctl status named
● named.service - Berkeley Internet Name Domain (DNS)
     Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; preset: di>
     Active: active (running) since Tue 2025-02-18 16:01:09 KST; 14min ago
    Process: 24839 ExecStartPre=/bin/bash -c if [ ! "$DISABLE_ZONE_CHECKING" ==>
    Process: 24841 ExecStart=/usr/sbin/named -u named -c ${NAMEDCONF} $OPTIONS >
   Main PID: 24842 (named)
      Tasks: 6 (limit: 11084)
     Memory: 31.8M
        CPU: 685ms
     CGroup: /system.slice/named.service
             └─24842 /usr/sbin/named -u named -c /etc/named.conf
```

Name Server 구축

```
[root@localhost ssl]# systemctl status httpd
● httpd.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: di>
     Active: active (running) since Tue 2025-02-18 15:31:59 KST; 45min ago
       Docs: man:httpd.service(8)
   Main PID: 24550 (httpd)
     Status: "Total requests: 8; Idle/Busy workers 100/0;Requests/sec: 0.00295;>
      Tasks: 230 (limit: 11084)
     Memory: 29.2M
        CPU: 2.170s
     CGroup: /system.slice/httpd.service
             ├─24550 /usr/sbin/httpd -DFOREGROUND
             ├─24552 /usr/sbin/httpd -DFOREGROUND
             ├─24553 /usr/sbin/httpd -DFOREGROUND
             ├─24554 /usr/sbin/httpd -DFOREGROUND
             ├─24555 /usr/sbin/httpd -DFOREGROUND
             └─24773 /usr/sbin/httpd -DFOREGROUND
```

HTTP Server 구축

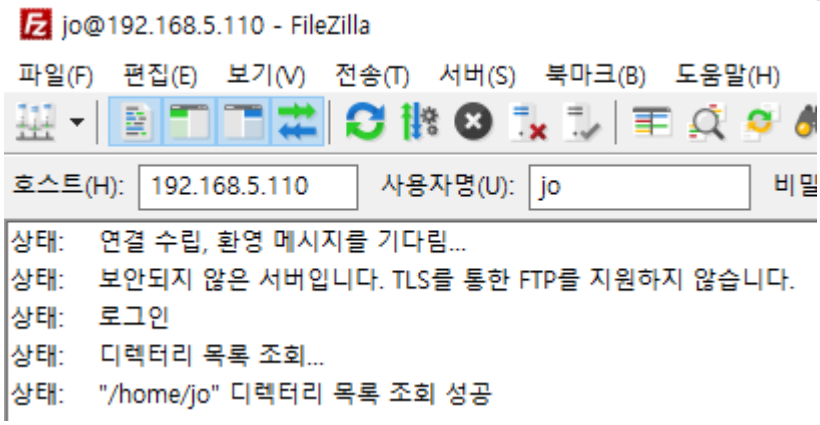
```
[root@localhost ~]# systemctl status vsftpd
● vsftpd.service - Vsftpd ftp daemon
     Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled; preset: d>
     Active: active (running) since Tue 2025-02-18 14:19:26 KST; 17s ago
   Main PID: 24258 (vsftpd)
      Tasks: 1 (limit: 11084)
     Memory: 736.0K
        CPU: 2ms
     CGroup: /system.slice/vsftpd.service
             └─24258 /usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf

Feb 18 14:19:26 localhost.localdomain systemd[1]: Starting Vsftpd ftp daemon...
Feb 18 14:19:26 localhost.localdomain systemd[1]: Started Vsftpd ftp daemon.
lines 1-12/12 (END)
```

FTP Server 구축

- FTP 접속 시 본인 이름의 계정으로 접속 가능하도록 설정

```
[root@localhost ~]# useradd jo
[root@localhost ~]# passwd jo
Changing password for user jo.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
```

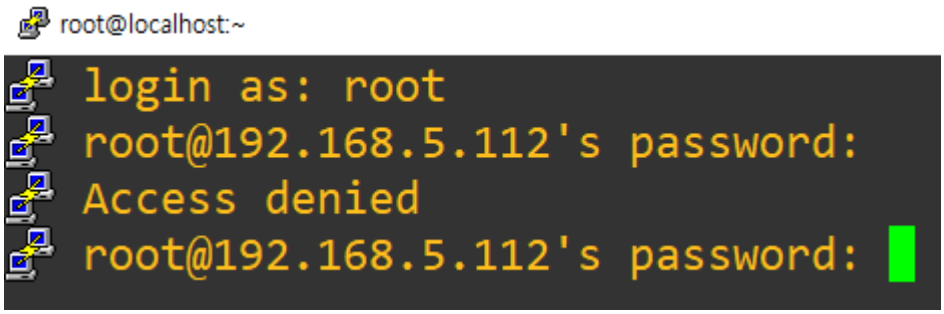


본인 이름 계정(jo)으로 접속 확인

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

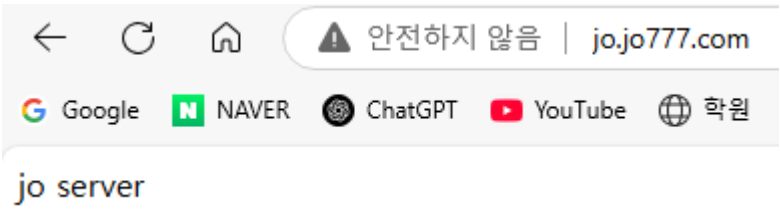
```
#LoginGraceTime 2m
PermitRootLogin no
DenyUsers root
#StrictModes yes
```

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

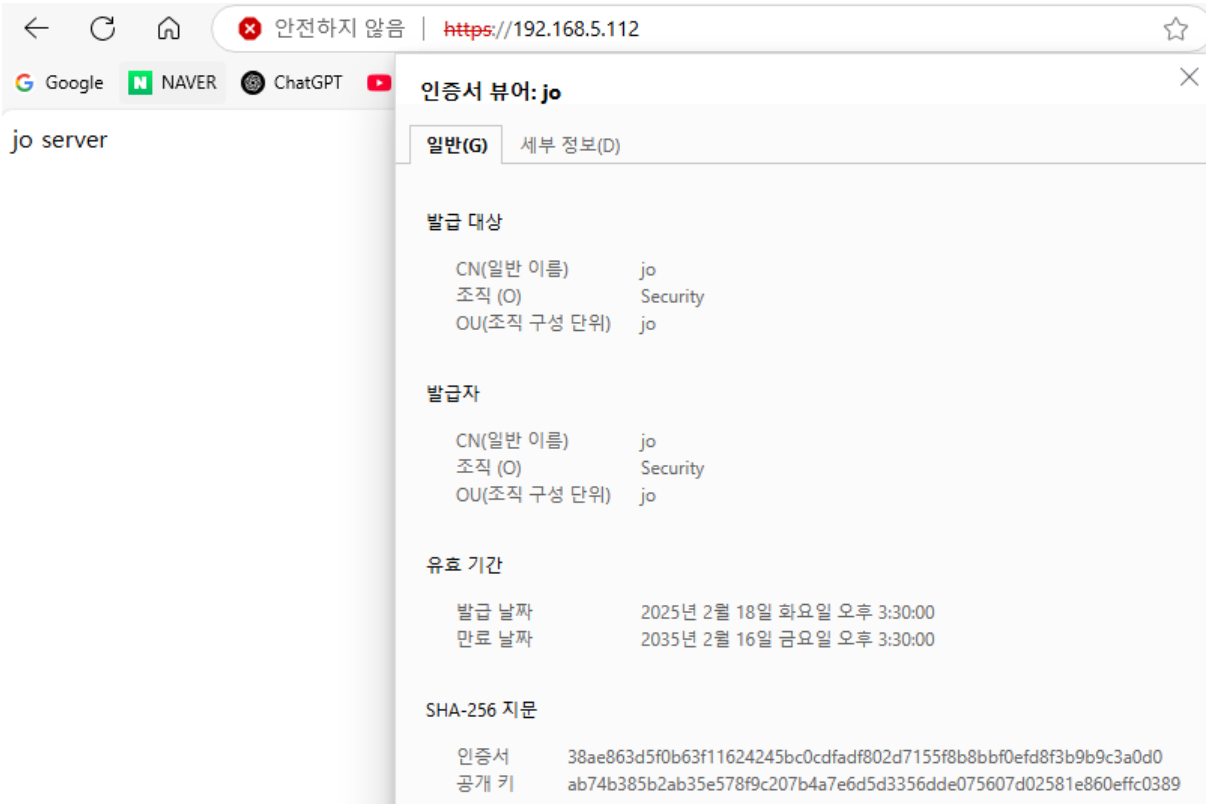
- /etc/shadow 파일에서의 Salt 에 대해 서술하고 암호화 알고리즘을 SHA256 으로 변경하시오.

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

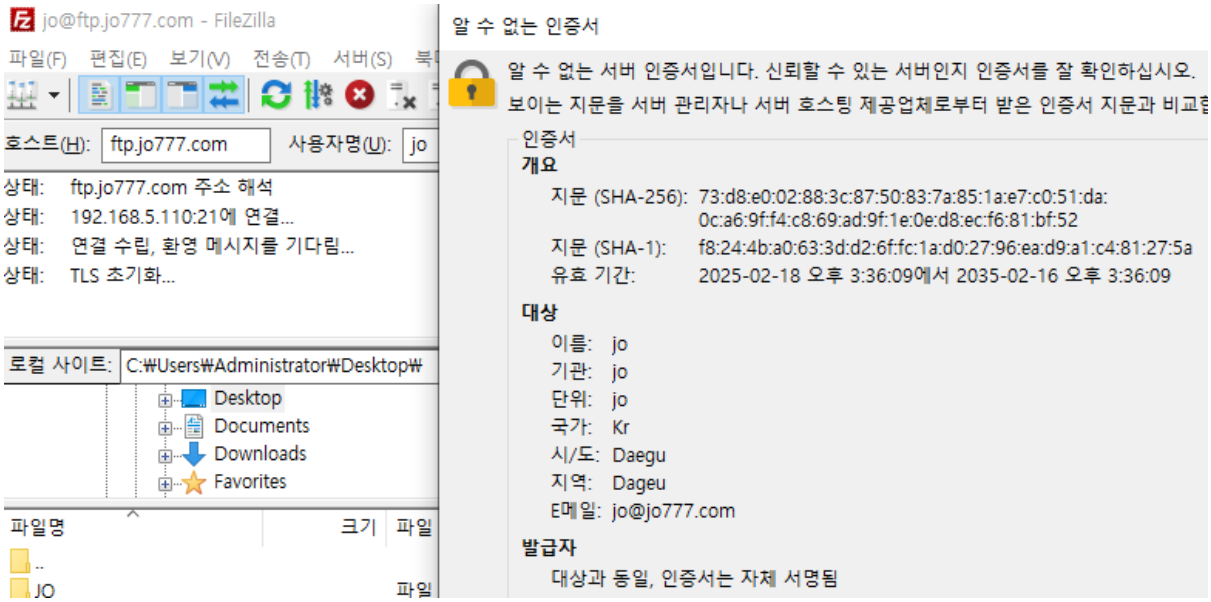
```
root:$5$rounds=100000$Y4h/6H.3ffiLkca8$HIJxINeqSKE7L3z75VCHF8dgqdfTJ1jK681KiaYjWc1:20137:0:99999:7:::
```

root 계정 암호화를 SHA512(기본)에서 SHA256 으로 수정하였음

- HTTPs 및 FTPs 설정을 하여 테스트하시오.



HTTPs 설정 후 테스트 화면



FTPs 설정 후 테스트 화면

- DDoS(Land Attack) 공격을 실행하고 TCPDump 또는 Wireshark 를 통해 패킷을 캡처하시오.

```
381313 3.181285    192.168.5.5    192.168.5.5    ICMP    60 Echo (ping) request  id=0x7971, seq=63050/19190, ttl=64 (no response found!)
381314 3.181285    192.168.5.5    192.168.5.5    ICMP    60 Echo (ping) request  id=0x7971, seq=63306/19191, ttl=64 (no response found!)
381315 3.181285    192.168.5.5    192.168.5.5    ICMP    60 Echo (ping) request  id=0x7971, seq=63562/19192, ttl=64 (no response found!)
381316 3.181528    192.168.5.5    192.168.5.5    ICMP    60 Echo (ping) request  id=0x7971, seq=63818/19193, ttl=64 (no response found!)
381317 3.181528    192.168.5.5    192.168.5.5    ICMP    60 Echo (ping) request  id=0x7971, seq=64074/19194, ttl=64 (no response found!)
381318 3.181528    192.168.5.5    192.168.5.5    ICMP    60 Echo (ping) request  id=0x7971, seq=64330/19195, ttl=64 (no response found!)
381319 3.181528    192.168.5.5    192.168.5.5    ICMP    60 Echo (ping) request  id=0x7971, seq=64586/19196, ttl=64 (no response found!)
```

Land Attack 에 의해 본인의 아이피로 공격이 온 걸 확인

- SetUID 를 활용한 권한 상승(root) 설정

```
[root@localhost test]# su jo
bash-5.1$ id
uid=1000(jo) gid=1000(jo) groups=1000(jo) context=unconfined_u:unconfined_r:unco
nfined_t:s0-s0:c0.c1023
bash-5.1$ ./backdoor
[root@localhost test]# id
uid=0(root) gid=0(root) groups=0(root),1000(jo) context=unconfined_u:unconfined_
r:unconfined_t:s0-s0:c0.c1023
```

backdoor 를 실행 한 후 권한이 상승된 것을 볼 수 있다

- Log Server 를 구축하여 FTP 서버의 Log 를 실시간 확인하고 DB 에 저장이 되도록 설정하시오.

```
+----+------------+---------------------+---------------------+----------+----------+----------+-----------------------------------------------
| ID | CustomerID | ReceivedAt          | DeviceReportedTime  | Facility | Priority | FromHost | Message
+----+------------+---------------------+---------------------+----------+----------+----------+-----------------------------------------------
|  1 |       NULL | 2025-02-18 17:32:20 | 2025-02-18 17:32:20 |        3 |        6 | localhost | Stopping System Logging Service...
|  2 |       NULL | 2025-02-18 17:32:21 | 2025-02-18 17:32:21 |        5 |        6 | localhost | [origin software="rsyslogd" swVersion="8.2310.0
|  3 |       NULL | 2025-02-18 17:32:21 | 2025-02-18 17:32:21 |        3 |        6 | localhost | rsyslog.service: Deactivated successfully.
|  4 |       NULL | 2025-02-18 17:32:21 | 2025-02-18 17:32:21 |        3 |        6 | localhost | Stopped System Logging Service.
|  5 |       NULL | 2025-02-18 17:32:21 | 2025-02-18 17:32:21 |        3 |        6 | localhost | Starting System Logging Service...
|  6 |       NULL | 2025-02-18 17:32:21 | 2025-02-18 17:32:21 |        3 |        6 | localhost | Started System Logging Service.
```

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