

1.1

Attacker(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 (admin-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/stateOrProvinceName=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: disabled)
   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: disabled)
   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

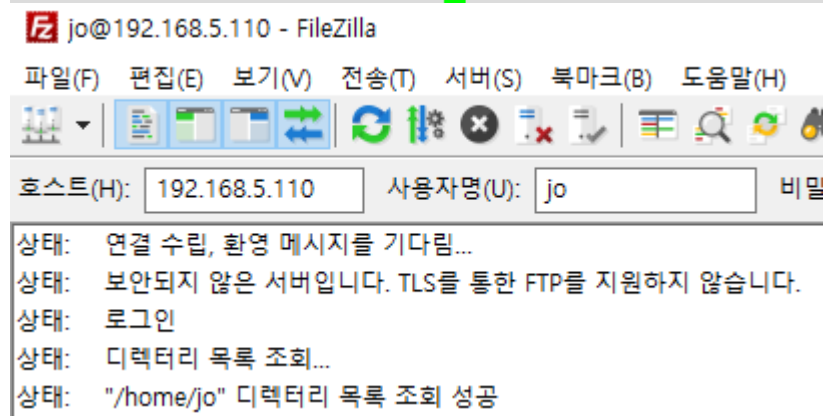
```
[root@localhost ~]# systemctl status vsftpd
● vsftpd.service - Vsftpd ftp daemon
   Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled; preset: disabled)
   Active: active (running) since Tue 2025-02-18 14:19:26 KST; 17s ago
    Main PID: 24258 (vsftpd)
       Tasks: 1 (limit: 11084)
      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.
```

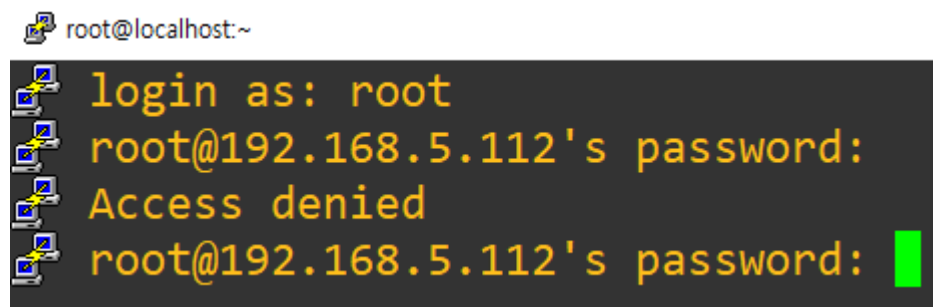


본인 이름 계정(jo)으로 접속 확인

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

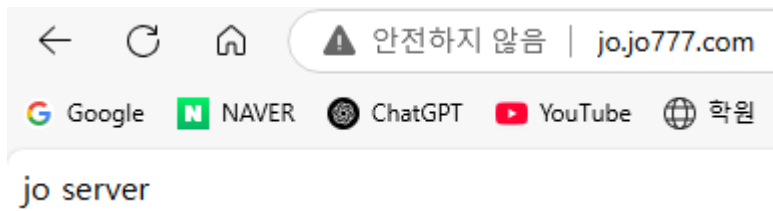
```
#LoginGraceTime 2m
PermitRootLogin no
DenyUsers root
#StrictModes yes
```

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=10000$Y4h/6H.3ffiLkca8$HIJxINeqSKE7L3z75VCHF8dgqdfTJ1jK681KiaYjWc1:20137:0:99999:7:::
```

root 계정 암호화를 SHA512(기본)에서 SHA256 으로 수정하였음

- HTTPS 및 FTPs 설정을 하여 테스트하시오.

The screenshot shows a web browser window with the address bar displaying <https://192.168.5.112>. The page title is "인증서 뷰어: jo". The main content area displays the details of a certificate for "jo server".

일반(G)		세부 정보(D)
발급 대상		
CN(일반 이름)	jo	
조직 (O)	Security	
OU(조직 구성 단위)	jo	
발급자		
CN(일반 이름)	jo	
조직 (O)	Security	
OU(조직 구성 단위)	jo	
유효 기간		
발급 날짜	2025년 2월 18일 화요일 오후 3:30:00	
만료 날짜	2035년 2월 16일 금요일 오후 3:30:00	
SHA-256 지문		
인증서	38ae863d5f0b63f11624245bc0cdfadf802d7155f8b8bbf0efd8f3b9b9c3a0d0	
공개 키	ab74b385b2ab35e578f9c207b4a7e6d5d3356dde075607d02581e860effc0389	

HTTPS 설정 후 테스트 화면

jo@ftp.jo777.com - FileZilla

파일(F) 편집(E) 보기(V) 전송(T) 서버(S) 북

호스트(H): ftp.jo777.com

사용자명(U): jo

상태: ftp.jo777.com 주소 해석

상태: 192.168.5.110:21에 연결...

상태: 연결 수립, 환영 메시지를 기다림...

상태: TLS 초기화...

로컬 사이트: C:\Users\Administrator\Desktop\W

Desktop
Documents
Downloads
Favorites

파일명

크기

파일

..

JO

알 수 없는 인증서

알 수 없는 서버 인증서입니다. 신뢰할 수 있는 서버인지 인증서를 잘 확인하십시오.

보이는 지문을 서버 관리자나 서버 호스팅 제공업체로부터 받은 인증서 지문과 비교하십시오.

인증서

개요

지문 (SHA-256): 73:d8:e0:02:88:3c:87:50:83:7a:85:1a:e7:c0:51:da:0c:a6:9f:f4:c8:69:ad:9f:1e:0e:d8:ec:f6:81:bf:52

지문 (SHA-1): f8:24:4b:a0:63:3d:d2:6f:fc:1a:d0:27:96:ea:d9:a1:c4:81:27:5a

유효 기간: 2025-02-18 오후 3:36:09에서 2035-02-16 오후 3:36:09

대상

이름: jo

기관: jo

단위: jo

국가: Kr

시/도: Daegu

지역: Dageu

E메일: jo@jo777.com

발급자

대상과 동일, 인증서는 자체 서명됨

FTPs 설정 후 테스트 화면

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

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:unconfined_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 저장되도록 설정하십시오.

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)