SSH

SSH(Secure Shell)은 원격지의 셸에 접속하기 위해 사용되는 네트워크 프로토콜로, 서버의 모든 것을 서버실 내에서 모니터와 키보드를 달아서 오프라인으로 통제할 것이 아니라면 좋든 싫든 SSH를 사용할 수밖에 없다. SSH는 서버를 원격으로 통제할 수 있는 강력한 도구인 만큼, 해커들은 해당 서버의 통제권을 얻기 위해 SSH부터 공격을 시도하는 것이 일반적이다. 따라서 SSH 보안은 리눅스 보안의 가장 기본적이며 핵심적인 부분이라고 할 수 있다.

- 포트___변경__
- root 계정___접속___차단__

?? ??

> **ssh**의 기본 포트가 **22**라는 것은 이미 널리 알려진 사실이다. ftp의 21, http/https가 각각 80/443인 것과 같이 특정한 쓰임새를 위해 IANA (Internet Assigned Numbers Authority) 에서 할당한 TCP 및 UDP 포트들을 잘 알려진 포트 **(Well-known port)** 라고 부른다. 잘 알려진 포트는 특정 서비스에 접근하기 위해 포트를 알 필요가 없다는 장점이 있지만, 해커들이 취약점을 찾기위해 가장 먼저 공격하는 포트이기도 하다. 따라서, ssh의 기본 포트를 변경하는 것 만으로도 해커들의 공격 속도를 지연시키는데 도움이 될 수 있다.

SSH ???? ?? ??

```
# vi /etc/ssh/sshd_config
```

SSH ?? ??

sshd_config 파일에서 **Port** 항목의 값을 원하는 값으로 변경한다. 최초에는 해당 항목이 주석처리 되어있을 수 있으므로, 주석처리되어 있다면 주석을 해제하고 값을 변경한다. 아래의 내용은 **ssh**의 포트를 **10022**로 설정하기 위한 예제다.

```
Port 10022
```

SSH ???

Debian ??

```
# systemctl restart ssh
```

RHEL ??

```
# systemctl restart sshd
```

root ?? ?? ??

> **!!! root** 계정 접속을 차단하기에 앞서, 해당 서버에 접속할 수 있는 별도의 수단을 미리 마련해 두는것을 권장한다

SSH ???? ?? ??

```
# vi /etc/ssh/sshd_config
```

PermitRootLogin ? ??

sshd_config 파일에서 **PermitRootLogin** 항목의 값을 **no**로 변경한다. 최초에는 해당 항목이 주석처리 되어있을 수 있으므로, 주석처리되어 있다면 주석을 해제하고 값을 변경한다.

```
PermitRootLogin no
```

SSH ???

Debian ??

```
# systemctl restart ssh
```

RHEL ??

```
# systemctl restart sshd
```