

SSH-Server-Konfiguration

ITS-Net-Lin

Sebastian Meisel

11. Dezember 2024

1 Einführung

Der SSH-Server wird in der Datei `/etc/ssh/sshd_config` konfiguriert. Dies ist eine einfache Textdatei. Zeilen die mit einer Raute (#) beginnen sind auskommentiert, d. h. sie werden nicht eingelesen. Hier stelle ich eine einfache Konfiguration vor, die einen sicheren SSH-Server konfiguriert:

1.1 Weitere Einstellungen in `/etc/ssh/sshd_config.d/` erlauben

Mit dieser Zeilen wird erreicht, dass Dateien im Unterverzeichnis `/etc/ssh/sshd_config.d/` liegen und auf `.conf` enden, weitere Einstellung enthalten dürfen. So kann man die Konfiguration aufteilen und übersichtlicher gestalten:

```
1 Include /etc/ssh/sshd_config.d/*.conf
```

1.2 Port ändern

SSH lauscht normalerweise auf Port 22, dies kann man ändern. Allerdings ist der Gewinn an Sicherheit dadurch sehr gering.

```
1 Port 2222
```

Wenn man diese Einstellung vornimmt muss zudem die Datei `~/.ssh/config` auf dem Client angepasst werden:

```
Host Debian debian deb
    HostName      debian
    Port          2222          # Neue Zeile!
    UserName      <benutzername>
    IdentityFile   ~/.ssh/config
```

2 Authentifizierung

Es gibt eine Reihe von Optionen, die bestimmen, wie Benutzer sich auf einem SSH-Server anmelden können. Die Authentifizierung durch einen öffentlichen Schlüssel (public key) ist sicher. Darum sollte man diese Erlauben und die durch Passwort-Eingabe verbieten.

```
1 PubkeyAuthentication yes
2 PasswordAuthentication yes
3 PermitEmptyPasswords no
```

Zudem sollte die interaktive Anmeldung per Tastatur verboten werden:

```
1 KbdInteractiveAuthentication no
```

Auf Linux-Systemen sollte immer Standard-Anmeldemechanismus PAM genutzt werden.

```
1 UsePAM yes
```

2.1 Weitere sinnvolle Einstellungen

Sie sollten erlauben, dass die Spracheinstellungen des Clients durch Umgebungsvariablen an den Server übermittelt werden:

```
1 AcceptEnv LANG LC_*
```

Außerdem sollte das sftp-Subsystem aktiviert werden, sodass man z. B. scp nutzen kann:

```
1 Subsystem      sftp      /usr/lib/openssh/sftp-server
```

3 Hashing und Verschlüsselungsalgorithmen

SSH unterstützt verschiedene Verschlüsselungsalgorithmen, nicht alle sind gleich sicher. Die folgende Konfiguration erlaubt nur die stärksten Algorithmen:

```
1 # KEX-(Key Exchange)-Algorithmen zum Schlüsselaustausch
2 KexAlgorithms curve25519-sha256@libssh.org,ecdh-sha2-nistp521,ecdh-sha2-nistp384,
   ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256
3
4 # Verschlüsselungsalgorithmen
5 Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-gcm@openssh.
   com,aes256-ctr,aes192-ctr,aes128-ctr
6
7 # MAC-(message authentication code)-Algorithmen
8 MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,umac-128-
   etm@openssh.com,hmac-sha2-512,hmac-sha2-256,umac-128@openssh.com
```
