

Remote Computing:

SSH:

Secure Shell ist ein Netzwerkprotokoll, das Benutzern, insbesondere Systemadministratoren, eine sichere Möglichkeit bietet, über ein ungesichertes Netzwerk auf einen Computer zuzugreifen.

TelNet:

Telecommunication Network bezeichnet ein Protokoll aus der TCP/IP-Welt, mit dem sich textbasierte Kommandos auf entfernten Rechnern ausführen lassen.

Funktion:

Beide Protokolle ermöglichen das virtuelle Zugreifen auf einen entfernten Computer, der sich im gleichen Netzwerk befindet. Es werden textbasierte Kommandos vom Client auf den Server geschickt und deren Ausgabe werden auf dem Client angezeigt. SSH stellt dabei eine gesicherte Verbindung her.

Transportprotokoll: TCP

Teile der Kommandos oder Ausgaben könnten fatale Fehler hervorrufen und müssen deswegen sichergestellt übertragen werden.

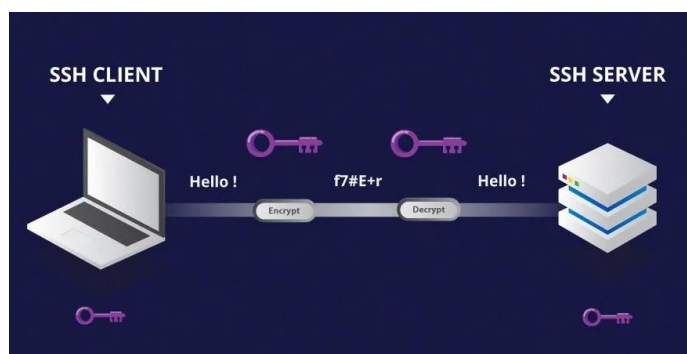
Port Nummern:

SSH: 22 auf Client und Server

TelNet: 23 auf Client und Server

Ablauf:

SSH:



1. Authentifizierung

1. Durch ein Zertifikat und einem Public Key kann sich der Client authentifizieren

2. Session-Key

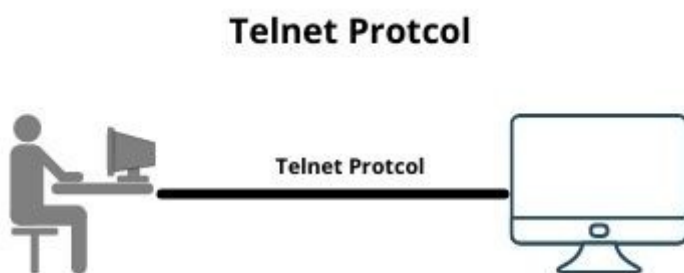
1. Nach der Authentifizierung wird ein Session-Key ausgehandelt mit dem die Kommunikation verschlüsselt wird. Dieser Session-Key kann während einer Session mehrfach neu ausgehandelt werden.

3. Verbindung

1. Zuerst wird über den Port 22 eine TCP Verbindung aufgebaut. Danach schickt zuerst der Server und dann der Client seine Protokoll Version und die unterstützten Algorithmen sowie Protokolle. Der Client sucht sich zuletzt eine Protokoll Version aus und fragt nach dem Public-Key des Servers. Damit verschlüsselt er seinen Session-Key. Mit dem Private-Key kann der Server den Session-Key wieder entschlüsseln

TelNet:

TelNet stellt eine ungesicherte TCP Verbindung standardmäßig über den Port 23 her. Eine Authentifizierung per Klartextpasswort kann statt finden. Es kann auch über andere Ports eine Verbindung aufgebaut werden.



Vor- und Nachteile:

SSH:

Vorteile:

- Gesicherte Verbindung
- Über öffentliches Internet zugreifbar
- Version2 kann mehr als nur textbasierte Verbindung
 - Tunneln von ganzen Anwendungen über SSH-2

Nachteile:

- Benutzerunfreundlicher
- SSH-1 funktioniert nur auf Terminal-Ebene

TelNet:

Vorteile:

- Benutzerfreundlich
- Simple
- Plattformübergreifend

Nachteile:

- Nur auf Terminal-Ebene
- Unverschlüsselte Verbindung
- Funktion muss ab Windows 7 vor Benutzung zuerst aktiviert werden

SSH eignet sich für eine regelmäßige Arbeit in öffentlichen Netzen mit wichtigen Daten. TelNet ist die simplere und einfachere Möglichkeit für den normalen User, der mit unwichtigen Daten arbeitet oder in physisch abgetrennten oder gesicherten Netzen arbeitet.