Aufgabe 2: Ports von SSH, HTTP und HTTPS

Ein Port ist eine numerische Adresse in einem Computersystem, die zur Identifizierung eines bestimmten Dienstes oder einer Anwendung verwendet wird. Ports sind Teil des TCP/IP-Netzwerkprotokolls und ermöglichen es, Daten an den richtigen Ort auf einem Computer oder Server zu leiten.

- SSH (Secure Shell):
  SSH verwendet standardmäßig Port 22. SSH ist ein sicheres Protokoll zur Fernverwaltung von Computern über eine verschlüsselte Verbindung.

- HTTP (Hypertext Transfer Protocol):
  HTTP verwendet standardmäßig Port 80. HTTP ist das Protokoll, das für die Übertragung von Webseiten und anderen Ressourcen im World Wide Web verwendet wird.

- HTTPS (Hypertext Transfer Protocol Secure):
  HTTPS verwendet standardmäßig Port 443. HTTPS ist die sichere Version von HTTP und wird zur verschlüsselten Übertragung von Webseiten und sensiblen Daten wie Anmeldedaten und Kreditkarteninformationen verwendet.
  Der zusätzliche Buchstabe "S" steht für "sicher", und die Verschlüsselung erfolgt normalerweise mithilfe von SSL/TLS.

Aufgabe 3: Prinzip von einer Verbindung mit öffentlichen/privaten Schlüsseln (SSH)

Eine SSH-Verbindung mit öffentlichen/privaten Schlüsseln basiert auf der asymmetrischen Verschlüsselung.

- Ein SSH-Schlüsselpaar besteht aus einem öffentlichen Schlüssel und einem privaten Schlüssel.

- Der öffentliche Schlüssel wird auf dem Server hinterlegt, zu dem du dich verbinden möchtest.

- Der private Schlüssel bleibt auf deinem Client.

- Bei der Verbindungsherstellung sendet der Client (der SSH-Client) seinen öffentlichen Schlüssel an den Server.

- Der Server überprüft, ob dieser öffentliche Schlüssel im System hinterlegt ist.

- Wenn der Server den öffentlichen Schlüssel erkennt, fordert er den Client auf, eine Signatur mit dem privaten Schlüssel zu erstellen und zu senden.

- Der Server überprüft dann die Signatur mit dem gespeicherten öffentlichen Schlüssel.

- Wenn die Überprüfung erfolgreich ist, wird die Verbindung hergestellt, und du bist authentifiziert, ohne ein Passwort eingeben zu müssen.

Erstellen eines SSH-Schlüsselpaars:

1. Öffne ein Terminal auf deinem Client-Computer.

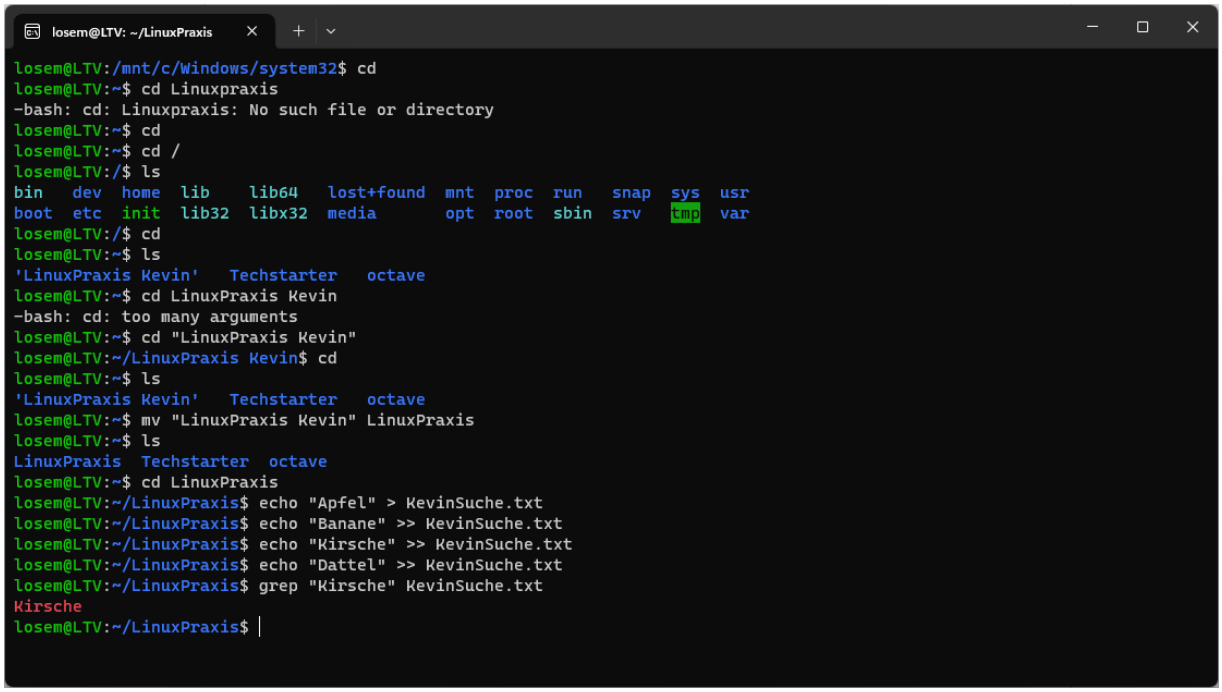
2. Verwende den Befehl `ssh-keygen` zum Generieren eines Schlüsselpaares. Standardmäßig wird ein RSA-Schlüssel erstellt.

3. Folge den Anweisungen, um einen Speicherort für den Schlüssel und ein optionales Passwort festzulegen.

4. Der öffentliche Schlüssel wird normalerweise in der Datei `~/.ssh/id_rsa.pub` gespeichert.

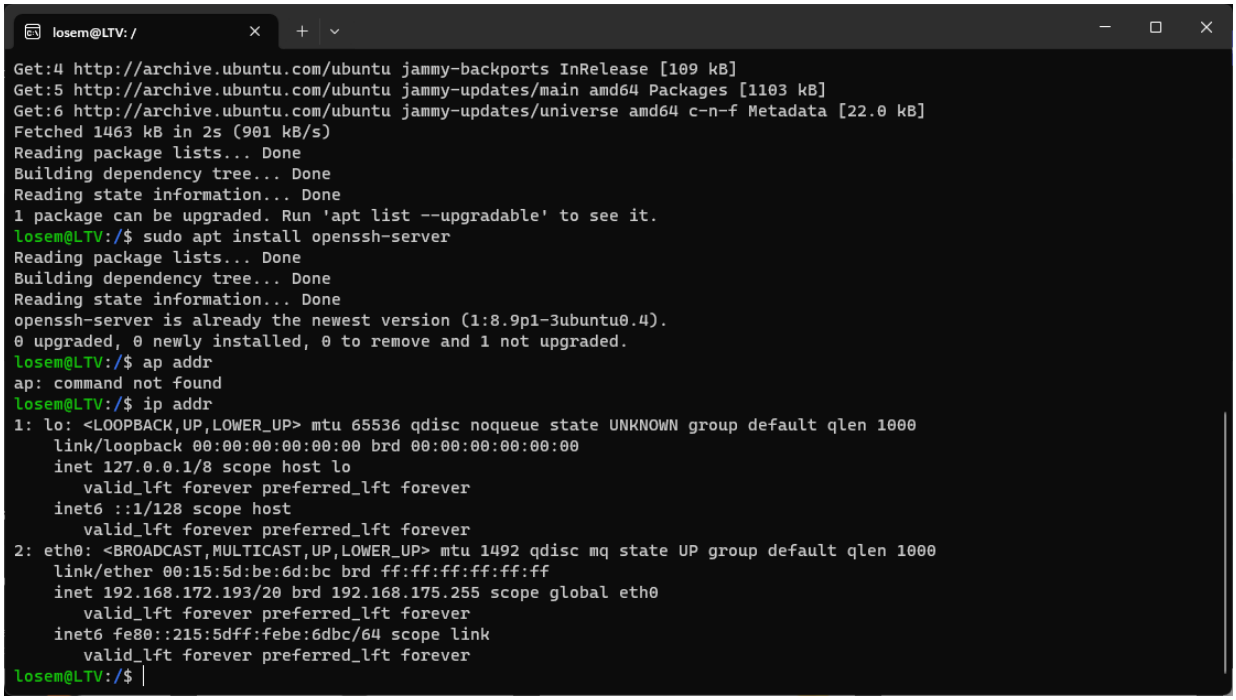
5. Du kannst den Inhalt des öffentlichen Schlüssels kopieren und auf den Server hochladen, zu dem du dich verbinden möchtest, damit dieser deinen öffentlichen Schlüssel erkennt.

Aufgabe 4: Research



Aufgabe 5: Zusatzaufgabe

Setup SSH-Server



SSH Connection über PuTTY: