

A Hintergrund und Ziele der Übung Secure File Transfer

Nachdem wir in der letzten Übung gelernt haben, wie man sich *remote* über *SSH* über das Netzwerk auf einem anderen Rechner anmeldet, werden wir uns in dieser Übung damit beschäftigen, wie Dateien zwischen unterschiedlichen Systemen sicher ausgetauscht werden können.

B Auto-Login mit Schlüsselpaar

- (1) SSH-Zugang ohne Passwort: Statt Passwörtern kann *ssh* auch ein Schlüsselpaar (*public + private key pair*) verwenden: Am Server wird der *public-key* eines Benutzers hinterlegt. Jede/r der den passenden *private-key* besitzt, darf sich einloggen.
 - a. Erzeugen Sie auf Ihrem Host-Rechner¹ mit *ssh-keygen* ein Schlüsselpaar (ohne *Passphrase*) für *junioradmin*.
 - Welche Dateien werden erzeugt – wie lautet deren absoluter Pfad?
 - Welche zusätzliche Informationen werden angezeigt?
 - b. Kopieren Sie den *public-key* **vom Host in** die Linux-VM:
 - Je nachdem, welches Host-System Sie verwenden, benutzen Sie dafür folgendes Kommando:
Windows-Host:

```
type %env:USERPROFILE\.ssh\id_rsa.pub | ssh user@IP-Adresse "cat >> .ssh/authorized_keys"
```


Linux-Host: *ssh-copy-id user@IP-Adresse*
 - Welche Daten werden kopiert (Quelle – Ziel)?
 - Warum darf der *private-key* die eigene Maschine **NIEMALS** verlassen?
 - c. Was passiert jetzt beim Verbinden mit *ssh user@IP-Adresse*? Wird nach einem Passwort gefragt?
 - d. Warum gilt die Authentifizierung mittels Schlüsselpaar als sicherer² als ein Login mittels herkömmlicher Passwörter?

C SSH-Client Konfiguration

Möchte man sich auf der Kommandozeile mit einem anderen Server verbinden, muss man den Rechnernamen, Benutzerkennung und evtl. auch die Portnummer bekanntgeben. Diese Voreinstellungen können (auch unter Windows) in der Datei namens *config* (im Unterordner *.ssh* Ihres Benutzerverzeichnisses) hinterlegt werden. Damit kann der Anmeldevorgang deutlich vereinfacht werden. Falls der Ordner *.ssh* bzw. die Datei *config* nicht existieren, müssen Sie diese anlegen.

- (2) Wie lautet der absolute Pfad der *ssh*-Konfigurationsdatei?
- (3) Beschreiben Sie in der folgenden Beispieldatei (auf Ihrem Host – IP-Adresse anpassen), was die jeweilige Zeile bewirkt, indem Sie Kommentare hinzufügen:

```
# ssh (secure shell) configuration file
Host linuxrechner
  Hostname 10.11.12.13
  User junioradmin
```

¹Mittlerweile funktioniert das auch unter Windows.

²vorausgesetzt man passt gut auf den geheimen *private-key* auf!

```
Host webserver
  HostName www.mysuperdomain.at
  Port 55550
  User kipferl
  IdentityFile ~/.ssh/private_ssh_key_rsa
```

- (4) Was passiert mit dieser Konfigurationsdatei nach Eingabe von `ssh linuxserver` oder `ssh webserver`? Ist das eventuell problematisch?
- (5) Erstellen Sie auf Ihrem Host-System (kann auch Windows sein) eine SSH-Client-Konfigurationsdatei³, die es Ihnen ermöglicht, sich mittels `ssh kali` als `junioradmin` in Ihrer Linux-VM anzumelden! Fügen Sie die Konfigurationsdatei im Protokoll ein!

Achtung: unter Windows zum Testen `ssh` in der `powershell` verwenden.

Konfig hier einfügen

D SSH – Dateien kopieren

Nun geht's an das Kopieren der Datei – wir wollen auf sichere Weise die Datei `xx_nwconf_25.txt` aus der letzten Übung⁴ (`xx` ist wieder IhrFamiliennamen) von der Linux-VM sowohl zur Windows-VM kopieren als auch zu einem anderen Linux-Rechner:

- (6) Öffnen Sie im Windows ein `cmd`- oder `powershell`-Fenster und legen Sie ein Verzeichnis `C:\TEMP` an.
- (7) Nachdem Sie `xx_nwconf_25.txt` auf der Linux VM im dortigem Heimatverzeichnis abgespeichert haben, verwenden Sie zum Kopieren dieser Datei auf die Windows-Maschine nun den Befehl `scp`⁵. – Schema:

Kopierbefehl Remote-User@Remote-Computer:Remote-Path Ziel

Bei uns wäre das also etwa (vollständiger Befehl und dessen Ausgabe ins Protokoll!):

```
scp                junioradmin@IP-Adresse:xx_nwconf_25.txt    C:\TEMP
```

- (8) Die Datei sollte sich jetzt auf `C:\TEMP` befinden – betrachten Sie die Datei mit `notepad`!
- (9) Jetzt kopieren Sie noch analog die selbe Datei zum Desktop Ihres Hosts (also von der virtuellen Maschine heraus). Wie lautet Ihre verwendete Kommandozeile? Testen Sie auch hier, ob Sie die kopierte Datei öffnen und lesen können!

Hinweis: Auf einem Linux-Host (oder neuerdings auch in der Powershell unter Windows) machen Sie das vom Shell-Prompt aus mit dem (zur PuTTY-Version `pscp` äquivalenten) Befehl `scp` (ohne das “p”).

- (10) *Bonus – Falls Sie die Übung auf dem Rechner in der Schule machen* –: Erzeugen Sie unter Linux eine Datei mit einem netten Textinhalt und kopieren Sie diese den Schreibtisch des Benutzers `junioradmin` auf dem (virtualisierten) Rechner Ihre/r/s Nachbar/i/n.

Welchen Befehl benutzen Sie dazu?

Was könnte man noch Interessantes auf dem Nachbarrechner machen?⁶

³Achtung: Windows-Notepad fügt standardmäßig die Erweiterung `.txt` am Dateinamen an!

⁴Ggf. müssen Sie die Datei nochmals neu erzeugen - sie beinhaltet die Ausgabe des Befehls `ip a`

⁵`scp` gibt es erst seit relativ kurzer Zeit auf Windows-Systemen. Davor konnte man `pscp.exe` aus dem Putty-Paket verwenden.

⁶Beachte aber die Gesetzeslage laut Strafgesetzbuch – StGB § 126c.: <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296> ... Störung der Funktionsfähigkeit eines Computersystems ... ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

Wie könnte sich der/die Nachbar/in davor schützen?

E SFTP

Manchmal hat man lokal eine graphische Oberfläche, aber nur SSH-Zugang zum entfernten Rechner. Um dennoch mit einem graphischen Dateibrowser auf dem *remote* System zu arbeiten, kann man eine SSH-Erweiterung, nämlich SFTP (*SSH File Transfer Protocol*) und einen smarten Datei-Browser verwenden.

- (11) Zunächst werden wir überprüfen, ob auf Ihrem Host-System ein geeigneter Datei-Browser vorhanden ist und diesen ggf. nachinstallieren.
- Falls Ihr Host-Rechner ein Windows-System ist, installieren Sie das sehr empfehlenswerte *WinSCP*: <http://winscp.net>.
 - Auf einem Linux-System eignen sich *Thunar* (Kali-Linux), *nemo* (am Linux Mint) bzw. *Nautilus* (am GNOME-Desktop).
- (12) Starten Sie Ihren graphischen Datei-Browser (also auf ihrem Windows-System oder auf einem zweiten Linux-System) und geben Sie als *Ort* an:
- ```
sftp://user@IP-Adresse
```
- Wichtiger Hinweis: Im *nemo*-Dateibrowser aktiviert die Tastenkombination Ctrl + L die Pfadeingabe.
- (13) Wechseln Sie jetzt (nach dem Anmelden) “mit der Maus” (im graphischen Dateibrowser) auf der VM in das Heimatverzeichnis von *junioradmin* und fügen Sie einen Screenshot Ihres grafischen Dateibrowsers ein, in dem Ihre Datei *xx\_nwconf\_25.txt* zu sehen ist!
- (14) Was passiert, wenn Sie dort die Datei *xx\_nwconf\_25.txt* durch Doppelklick öffnen? Screenshot!
- (15) Was passiert wenn man die Datei ändert und speichert? Was muss da im Hintergrund *passieren*?

## F Bonus: GUI über ssh

- (16) Bei der Verwendung von X-Windows (graphisches Subsystem unter Linux) kann auch die “graphische” Oberfläche durch eine ssh-Verbindung getunnelt werden. Verbinden Sie sich von einer zweiten Linux-VM oder Ihrem Linux-Host aus mit

```
ssh -Y user@IP-Adresse
```

in die Linux-VM. Starten Sie dort ein Programm mit grafischer Oberfläche z.B. eine Konsole mit *gnome-terminal* (oder eine Uhr mit *xclock*).

- Wo *läuft* dieses Programm?
- Wo *erscheint* das Fenster?

- (17) Was machen die Optionen *-L* und *-R* bei *ssh*?

*Viel Spaß!*