



# Betriebssysteme

## Praktikum 2

In diesem Praktikum lernen Sie die Benutzerverwaltung des Windowsbetriebssystems und die verschiedenen Möglichkeiten darauf Zugriff zu nehmen, kennen.

### Inhalte des Praktikums:

- Anlegen von Benutzern (ver. Methoden)
- Einsicht in die SAM-Registry Datenbank

# LÖSUNG

### Vorbereitung

Nutzen Sie bitte für die weitere Bearbeitung die in PR1 erstellte Windows VM. Eine installierbare VM vom PR1 finden Sie alternativ als OVA-Datei im Download unter:

<https://download.hs-mittweida.de/intranet/R:/CB/Bodach/BKA%20Studiengang/Betriebssysteme/Praktikum/Windows/Windows10-BS-Praktikum1.ova>

Zusätzlich finden Sie hier die für das Praktikum 2 zu nutzende ISO Datei **PR2.iso**:

<https://download.hs-mittweida.de/intranet/R:/CB/Bodach/BKA%20Studiengang/Betriebssysteme/Praktikum/Windows/PR2.iso>

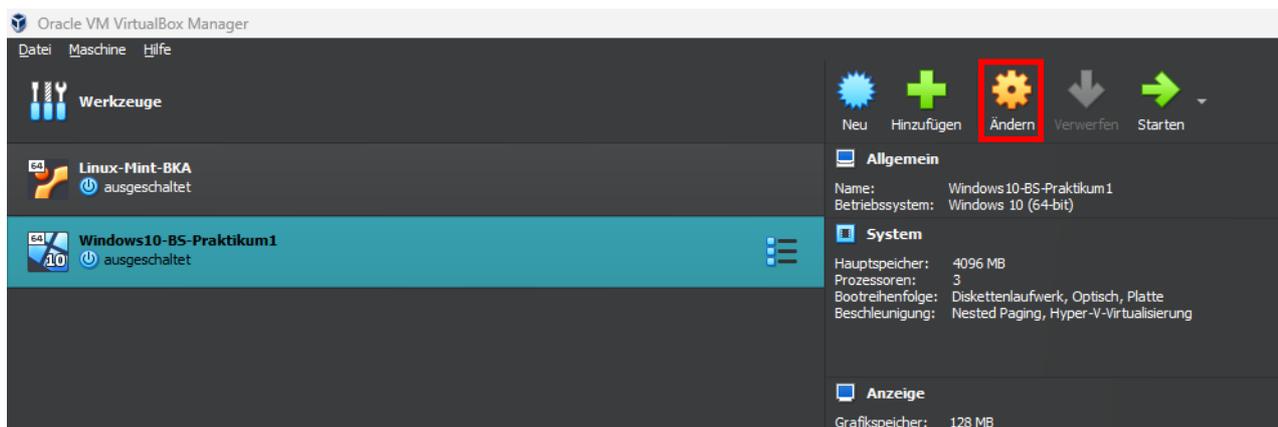
### Allgemeine Hinweise

Kopieren Sie bitte die ISO Datei PR2.iso (75MB) auf Ihre lokale Festplatte in ein separates Verzeichnis, auf das Sie Zugriff haben, bestenfalls in das VM-Verzeichnis von Praktikum 1.

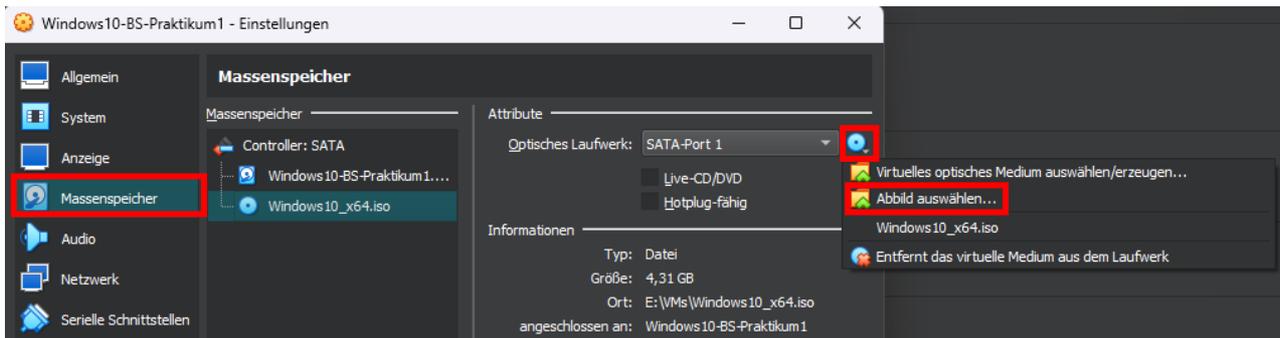
### Einbinden der PR2.iso

Öffnen Sie VirtualBox.

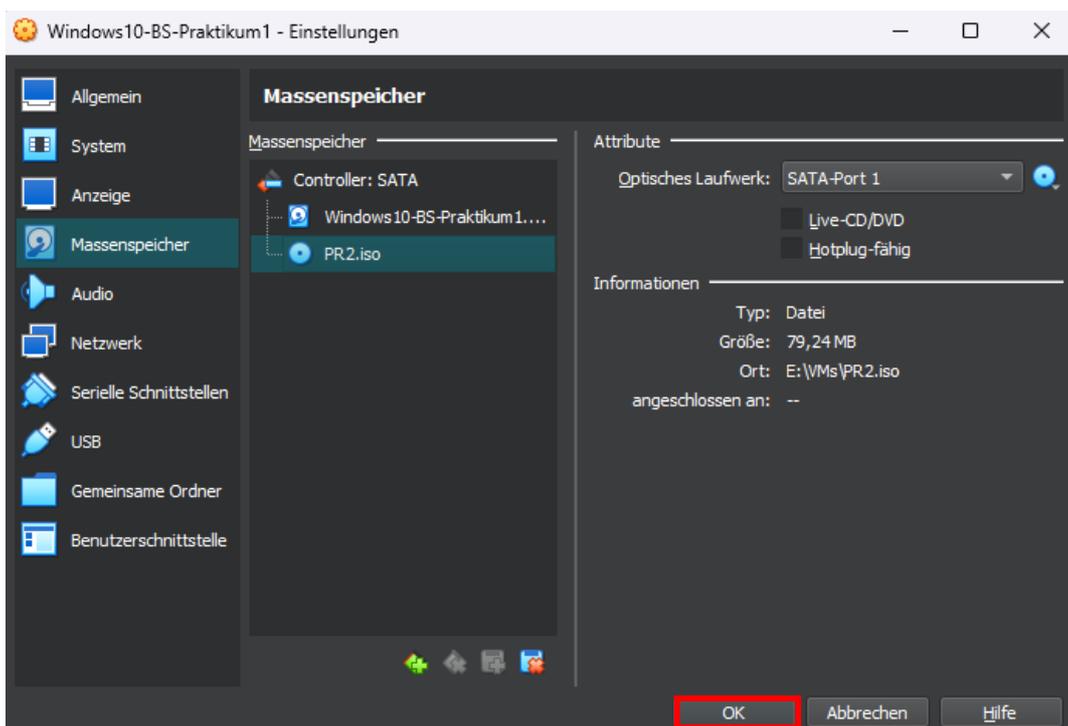
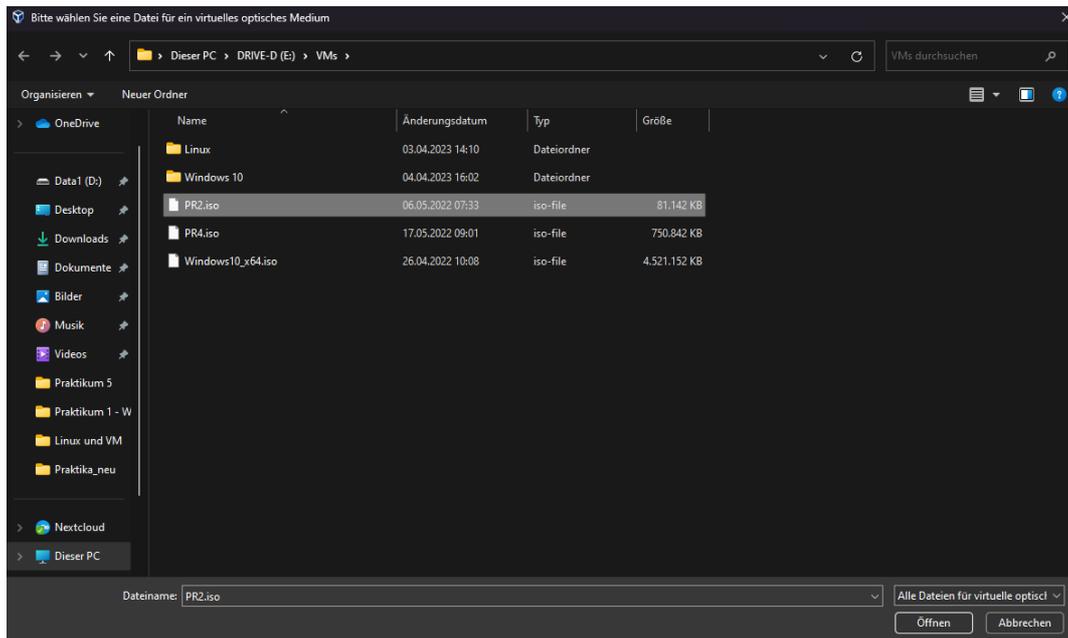
Wählen Sie die im Praktikum 1 angelegte VM aus oder importieren Sie zuerst die OVA-Datei wählen dann die VM des Praktikums 1 aus. Gehen Sie auf Ändern (nicht Doppelklicken auf die VM, das würde diese starten).



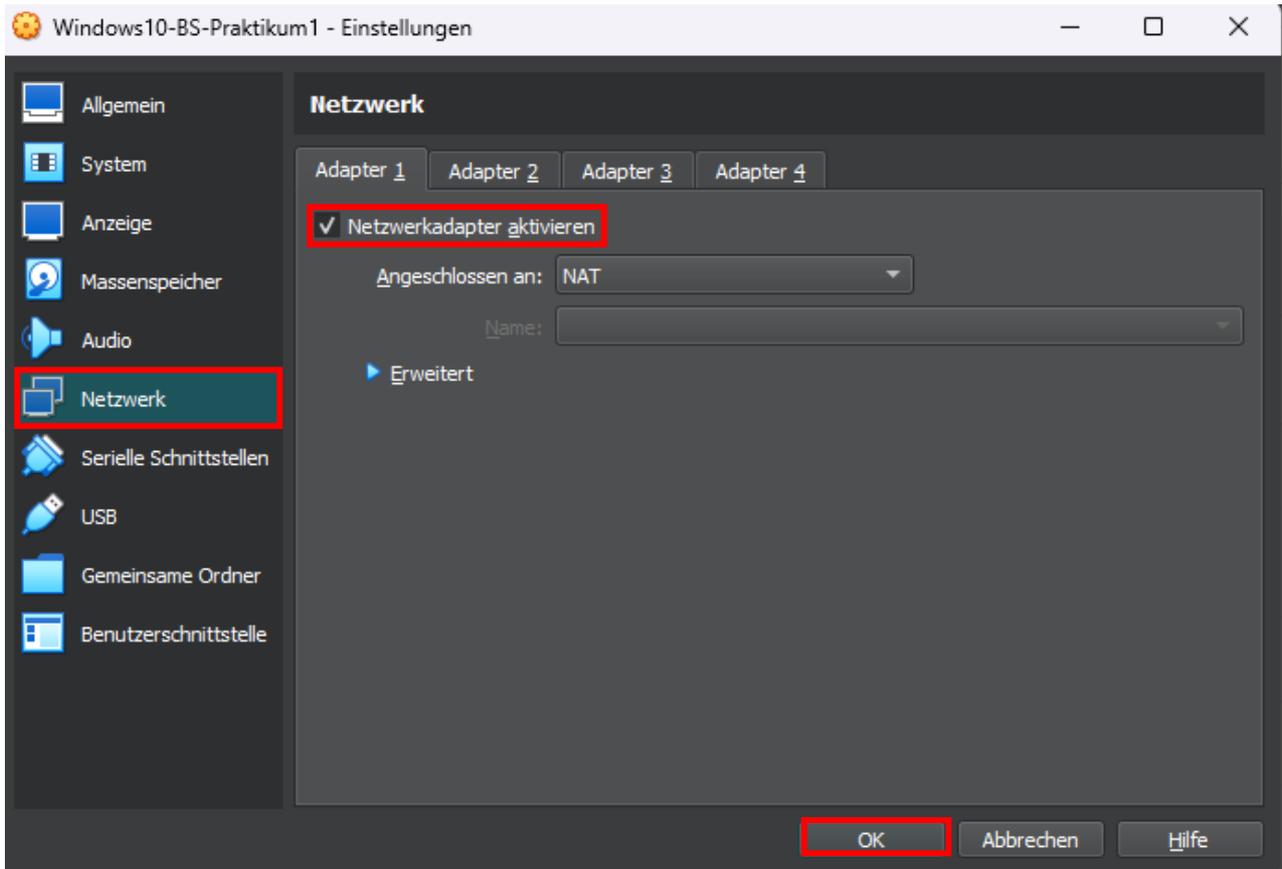
➤ Wählen Sie den Massenspeicher aus



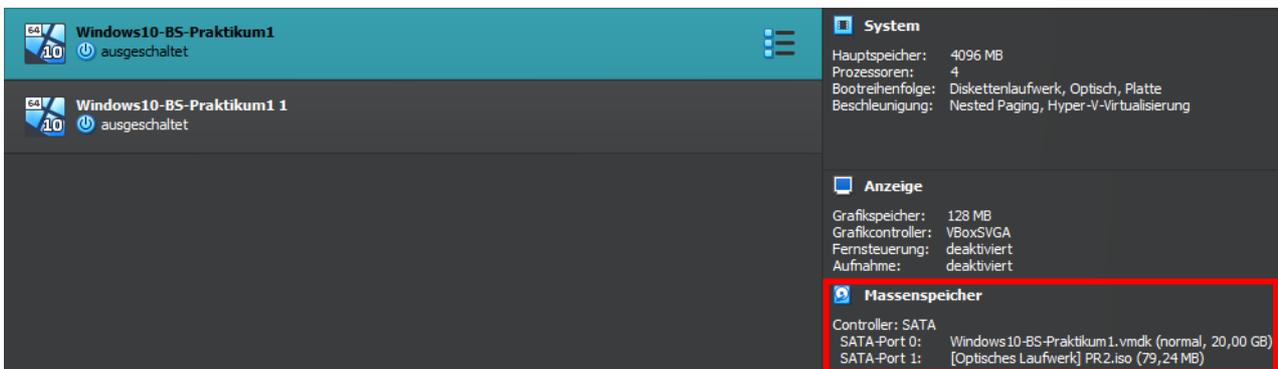
➤ Binden Sie bei der CD die heruntergeladene Abbilddatei **PR2.iso** ein



- Aktivieren Sie die Netzwerkverbindung



- Bestätigen Sie die Änderungen mit OK

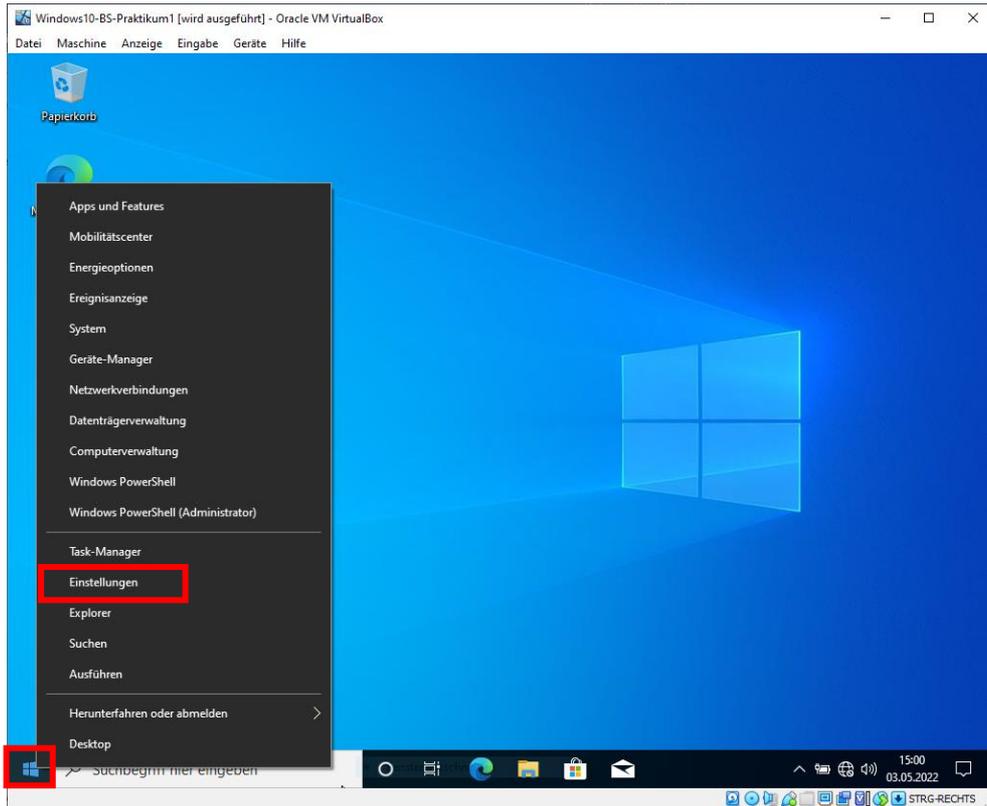


**Ergebnis**

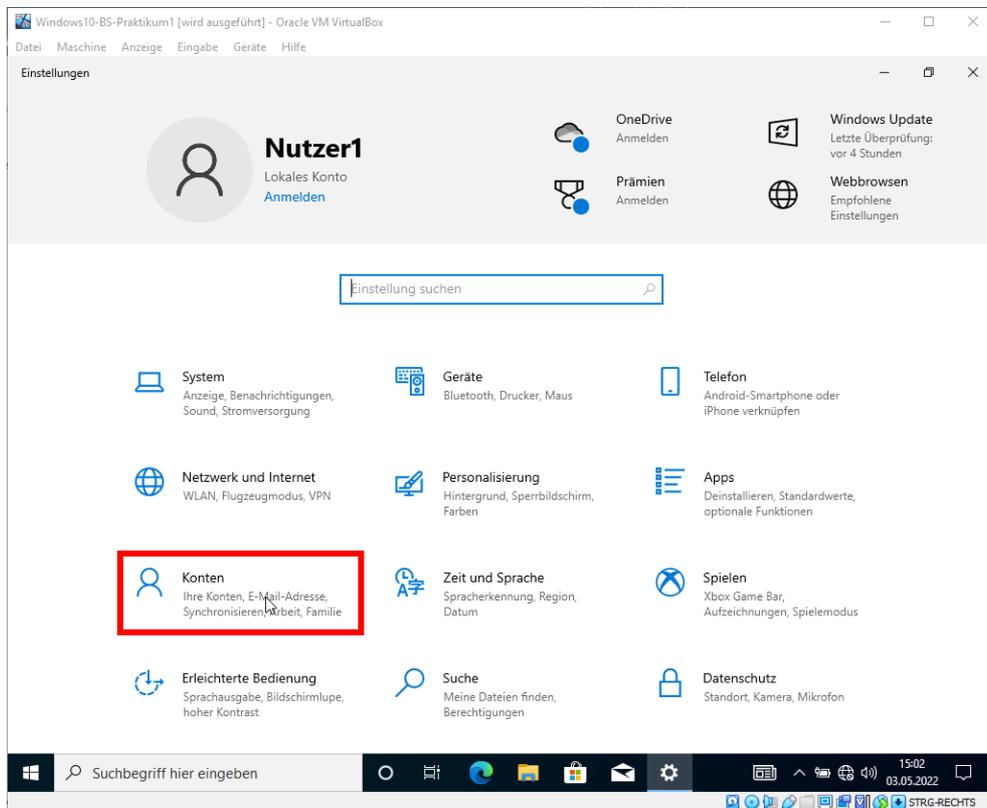
## Benutzer mit Systemeinstellung anlegen und überprüfen

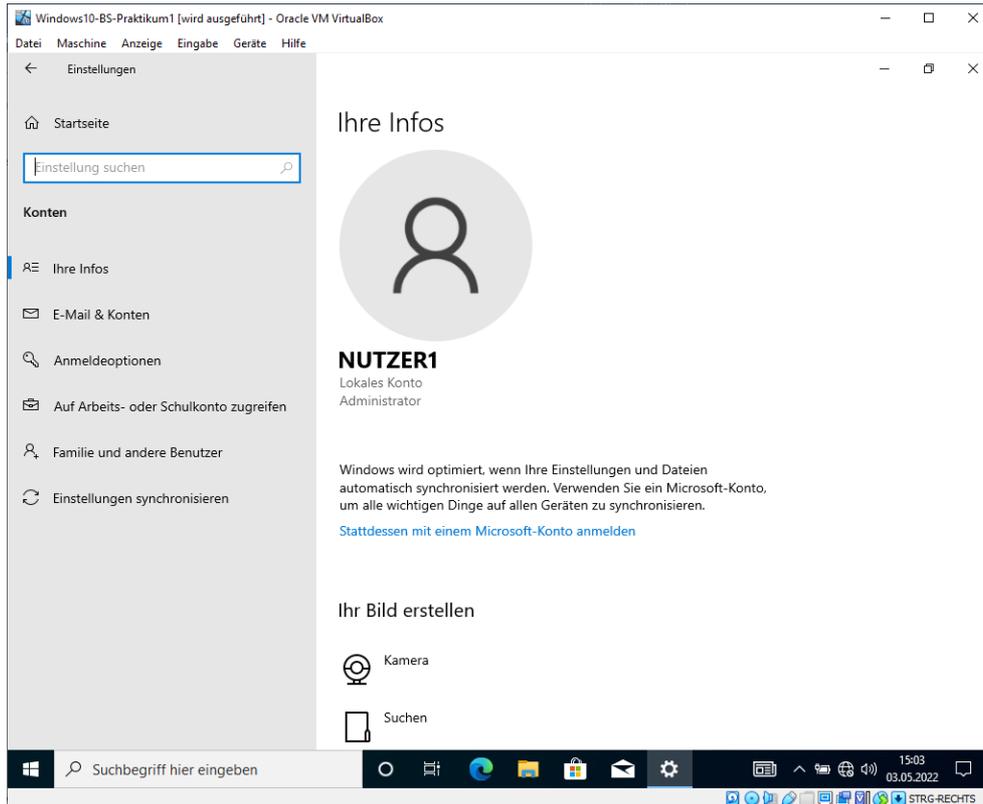
**Starten** Sie jetzt die VM und loggen sich als **Nutzer1** mit **Kennwort1** ein.

- Starten Sie Einstellungen mit rechts Klick auf den Windows Start Button

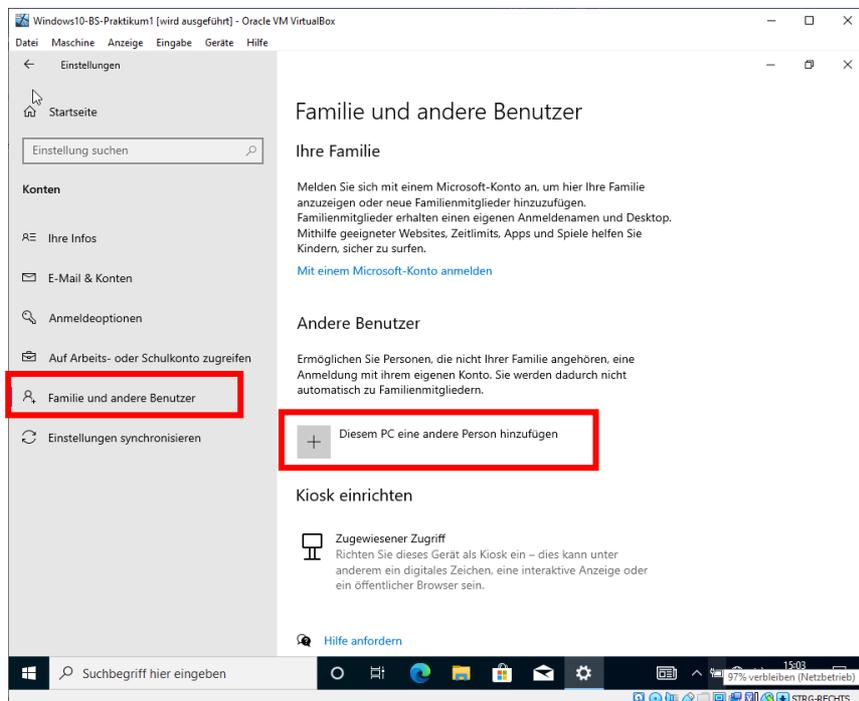


➤ Gehen Sie auf Konten





- Wählen Sie Familie und andere Benutzer und fügen eine Person hinzu
  - wählen Sie ggf.: „Ich kenne die Anmeldeoptionen für diese Person nicht“ aus
  - anschließend noch „Benutzer ohne Microsoft-Konto hinzufügen“



- Fügen Sie **Nutzer2** mit **Kennwort2** hinzu

Microsoft-Konto

### Benutzer für diesen PC erstellen

Wenn Sie ein Kennwort verwenden möchten, dann wählen Sie ein Kennwort aus, das leicht zu merken, aber von anderen schwer zu erraten ist.

Von wem wird dieser PC genutzt?

Nutzer2

Achten Sie auf Sicherheit.

.....

.....

Falls Sie Ihr Kennwort vergessen

Wie hieß Ihr erstes Haustier?

Haustier2

Weiter

Ergebnis: - **lokales Standardkonto.**

➤ Wechseln Sie den Kontotyp in **Administrator**

Windows10-BS-Praktikum1 [wird ausgeführt] - Oracle VM VirtualBox

Einstellungen

## Familie und andere Benutzer

### Ihre Familie

Melden Sie sich mit einem Microsoft-Konto an, um hier Ihre Familie anzuzeigen oder neue Familienmitglieder hinzuzufügen. Familienmitglieder erhalten einen eigenen Anmeldenamen und Desktop. Mithilfe geeigneter Websites, Zeitlimits, Apps und Spiele helfen Sie Kindern, sicher zu surfen.

[Mit einem Microsoft-Konto anmelden](#)

### Andere Benutzer

Ermöglichen Sie Personen, die nicht Ihrer Familie angehören, eine Anmeldung mit ihrem eigenen Konto. Sie werden dadurch nicht automatisch zu Familienmitgliedern.

+ Diesem PC eine andere Person hinzufügen

Nutzer2  
Lokales Konto

Kontotyp ändern Entfernen

### Kiosk einrichten

Zugewiesener Zugriff

Suchbegriff hier eingeben

15:06  
03.05.2022

STRG-RECHTS

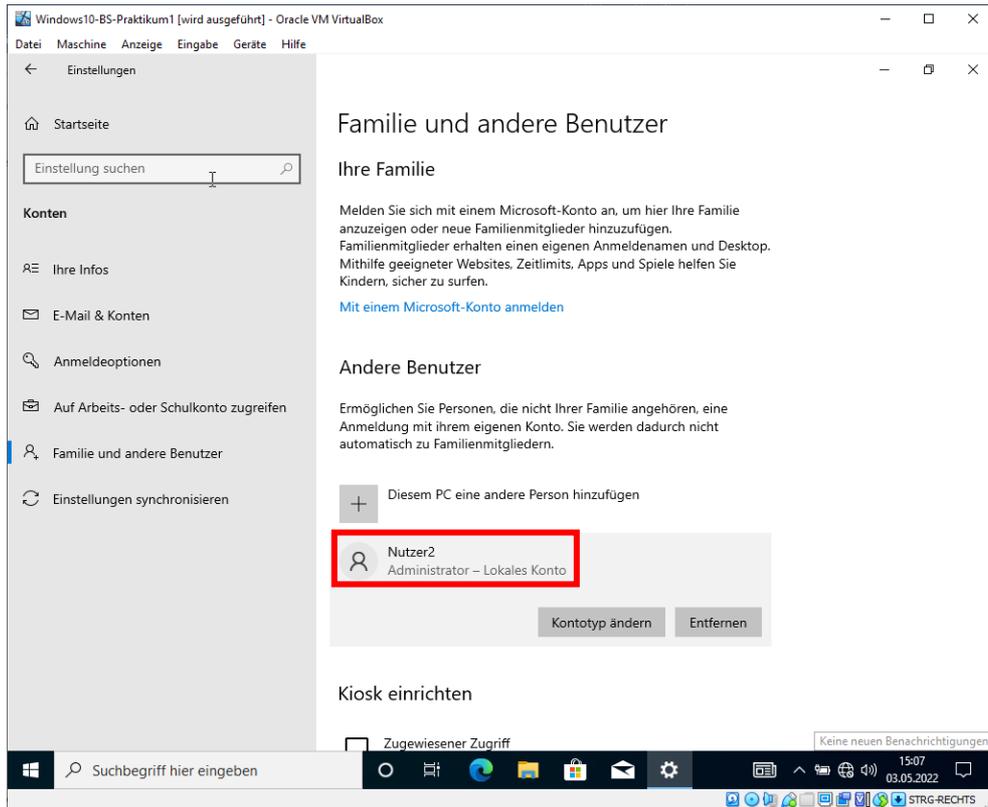
Kontotyp ändern

Nutzer2  
Lokales Konto

Administrator  
Standardbenutzer

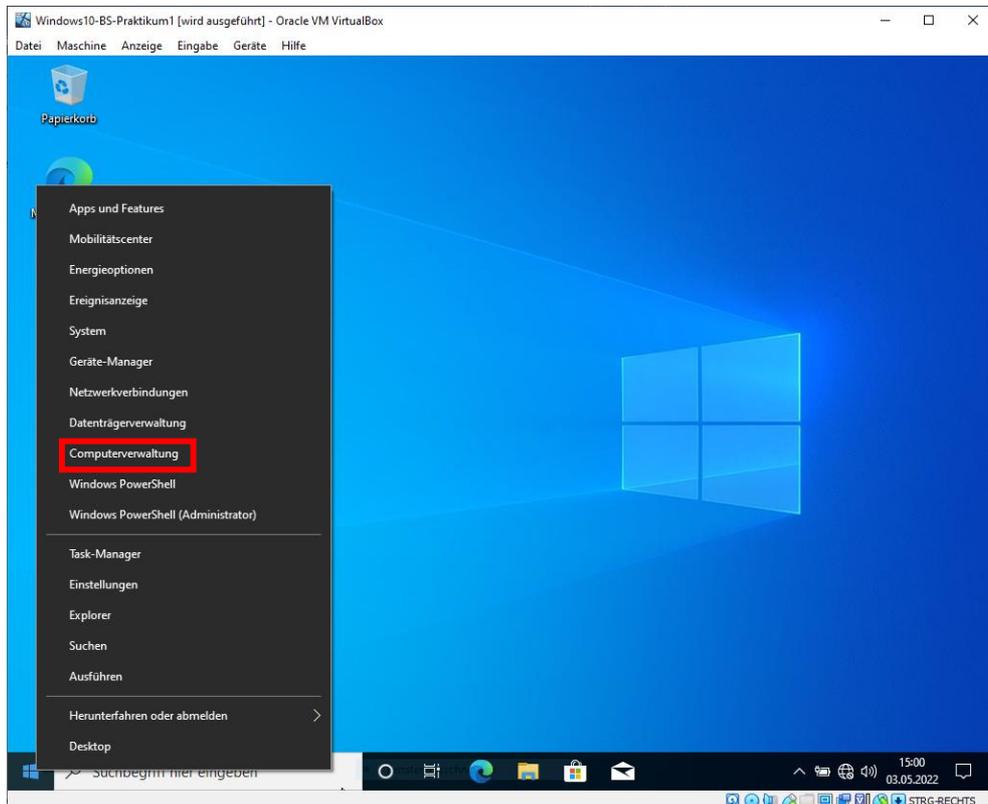
OK Abbrechen

Ergebnis: - **lokales Administrator Konto.**

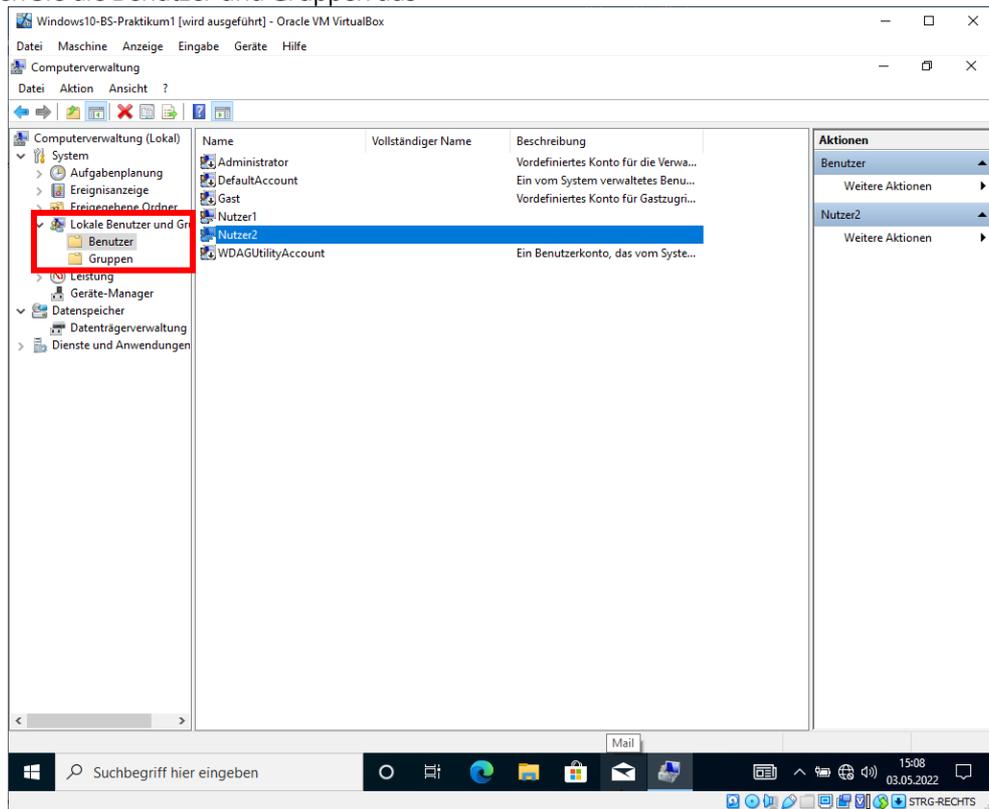


## Benutzer mit MMC anlegen und überprüfen

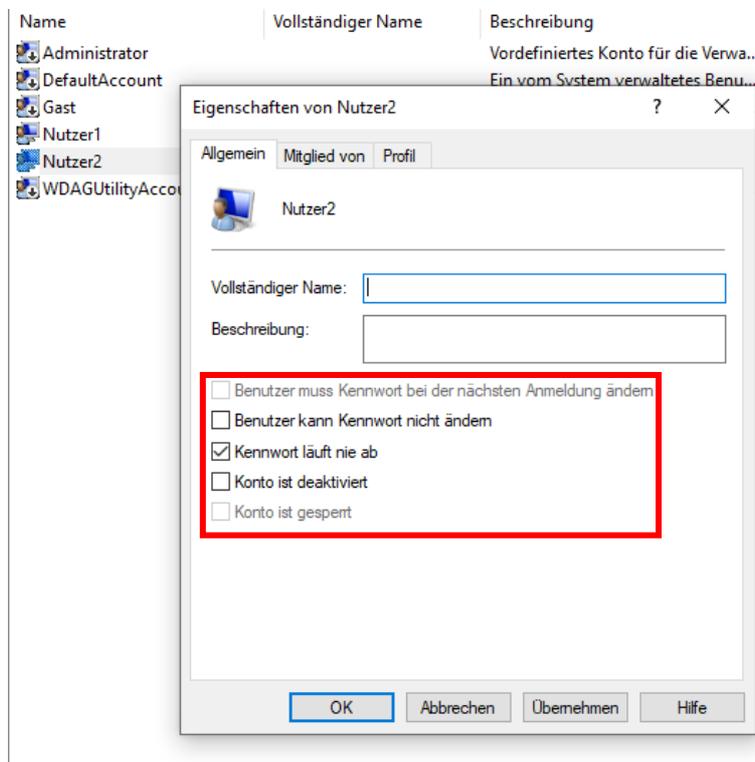
Öffnen Sie die Computerverwaltung (rechter Klick Windows Button) oder die MMC mit der Übersicht von PR1.



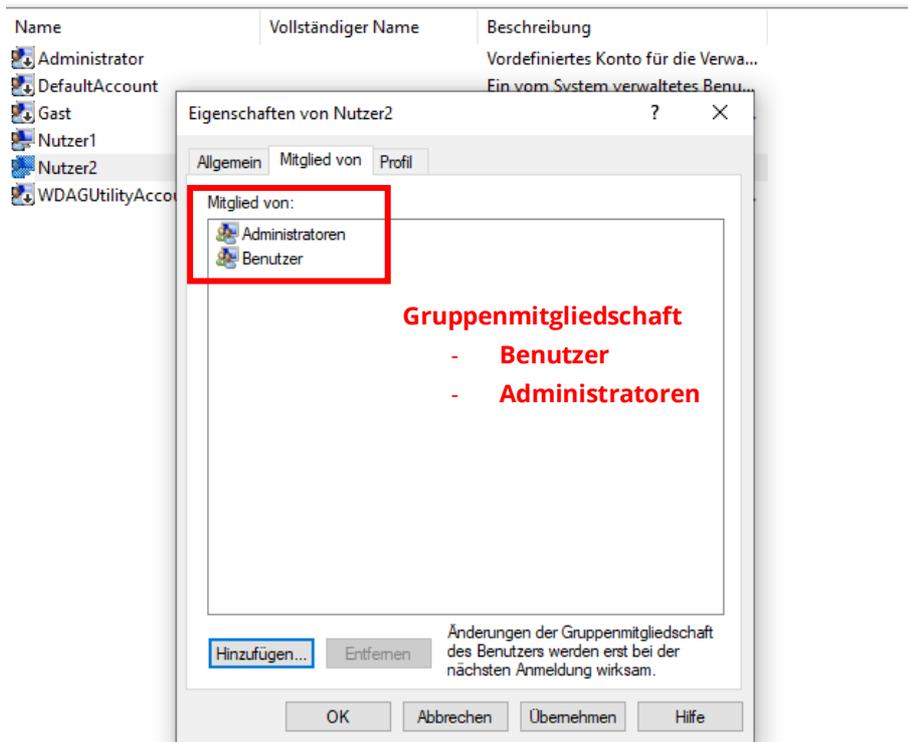
➤ Wählen Sie die Benutzer und Gruppen aus



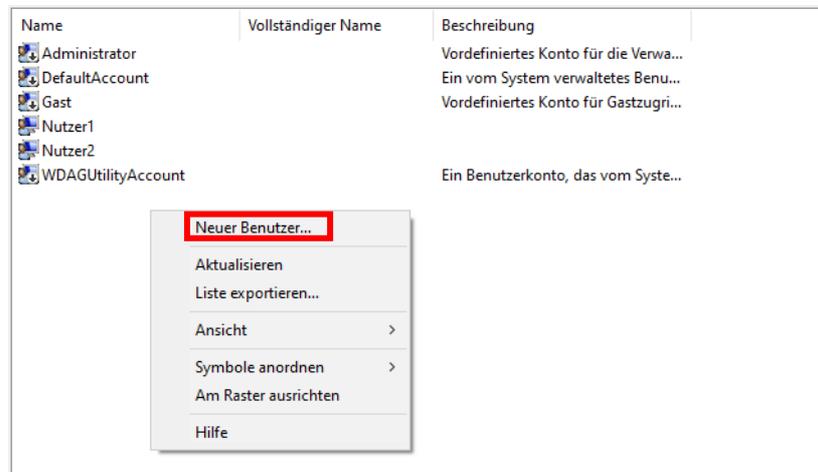
➤ Lassen Sie sich von **Nutzer2** die Einstellungen Anzeigen

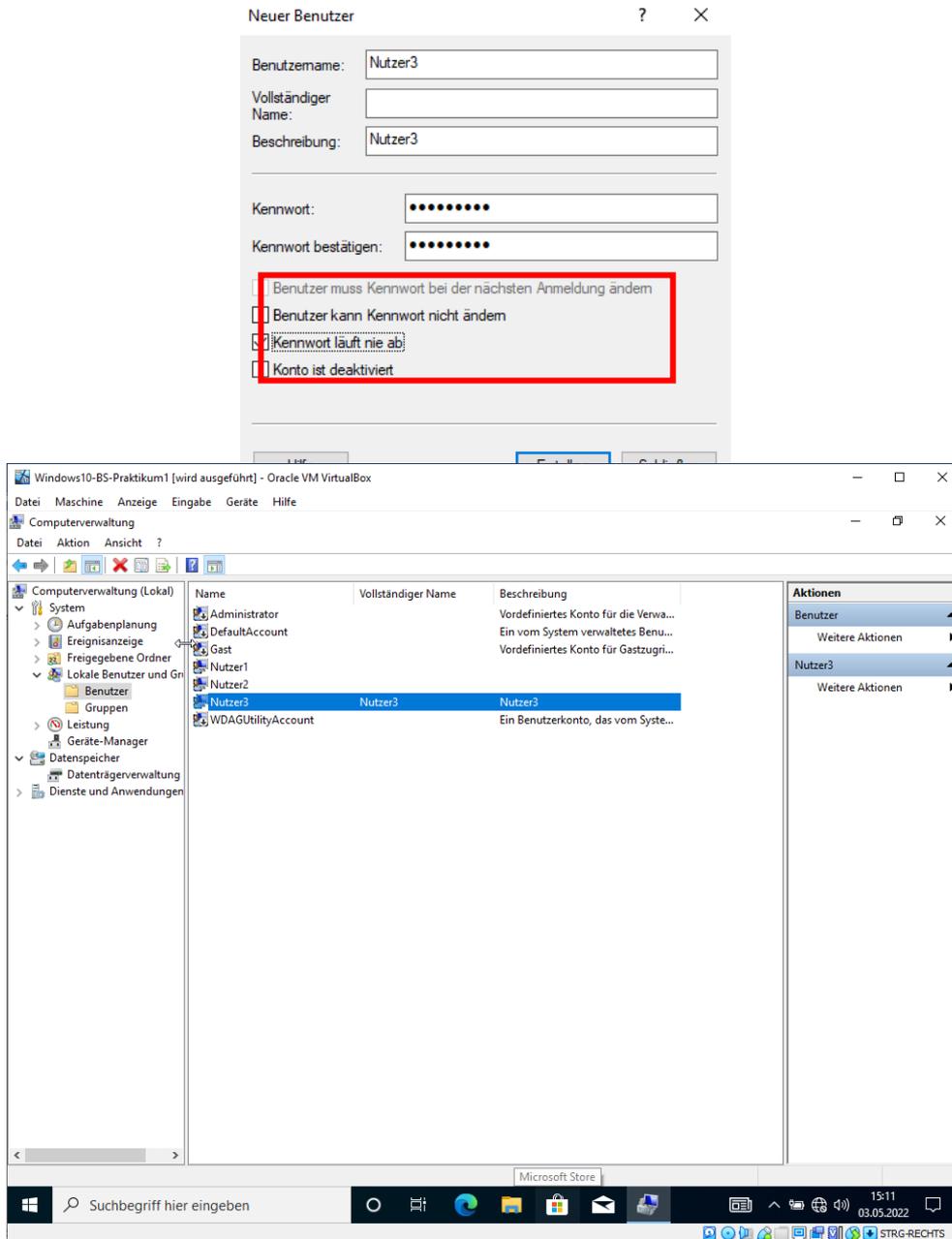


Standard wenn Benutzer aktiv

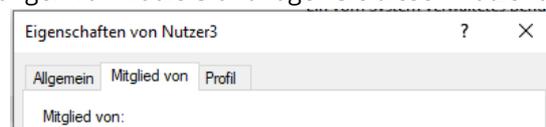


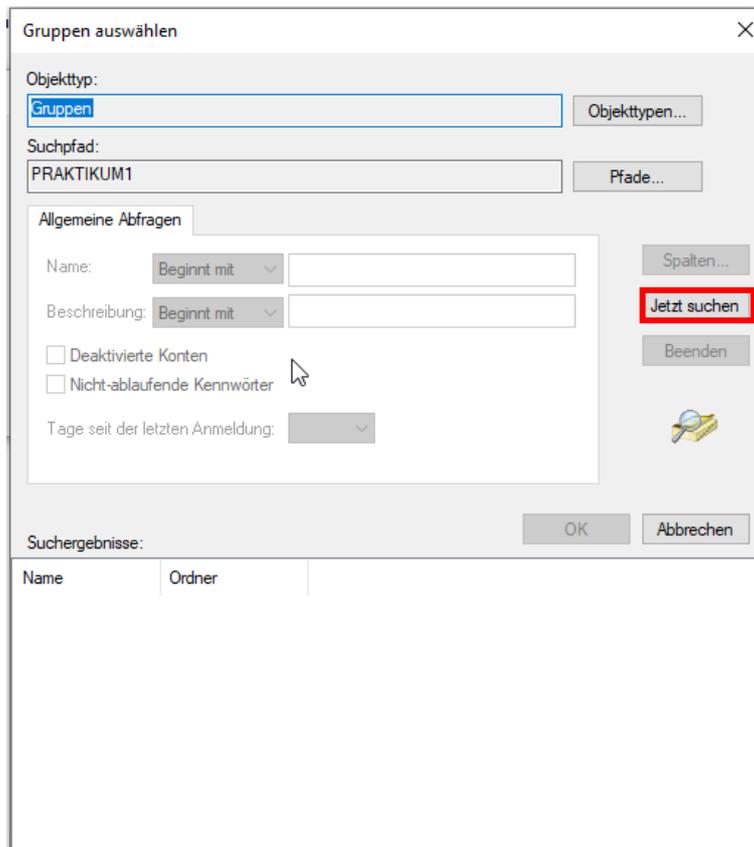
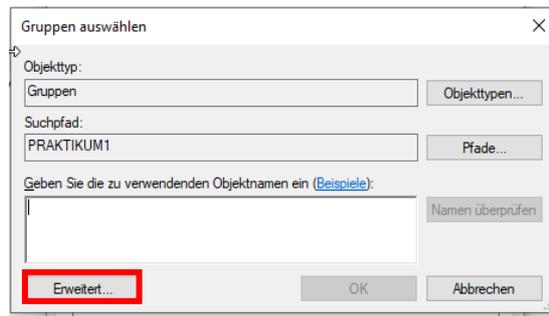
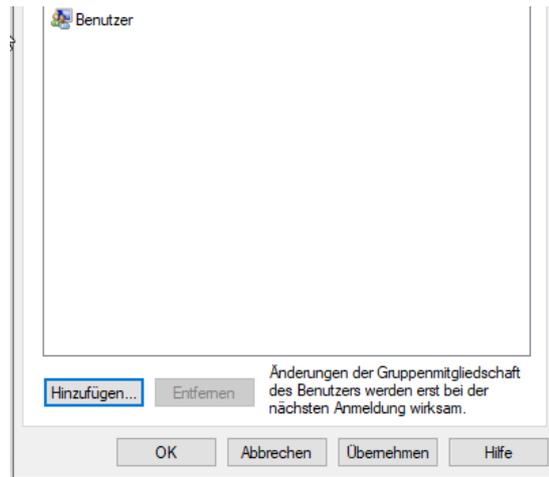
- Legen Sie einen neuen Benutzer **Nutzer3** mit **Kennwort3** an, sodass dessen Kennwort nicht neu gesetzt werden muss und nie abläuft





➤ Editieren Sie die Einstellungen von Nutzer3 und fügen Sie diesen Nutzer der Gruppe der Administratoren zu





Gruppen auswählen

Objekttyp: Gruppen Objekttypen...

Suchpfad: PRAKTIKUM1 Pfade...

Allgemeine Abfragen

Name: Beginnt mit

Beschreibung: Beginnt mit

Deaktivierte Konten

Nicht-ablaufende Kennwörter

Tage seit der letzten Anmeldung:

Spalten...

Jetzt suchen

Beenden

Suchergebnisse: OK Abbrechen

Name	Ordner
Administratoren	PRAKTIKUM1
Benutzer	PRAKTIKUM1
Distributed C...	PRAKTIKUM1
Ereignisprotok...	PRAKTIKUM1
Gäste	PRAKTIKUM1
Gerätebesitzer	PRAKTIKUM1
Hauptbenutzer	PRAKTIKUM1
Hyper-V-Admi...	PRAKTIKUM1
IIS_IUSRS	PRAKTIKUM1
Kryptografie-O...	PRAKTIKUM1

Gruppen auswählen

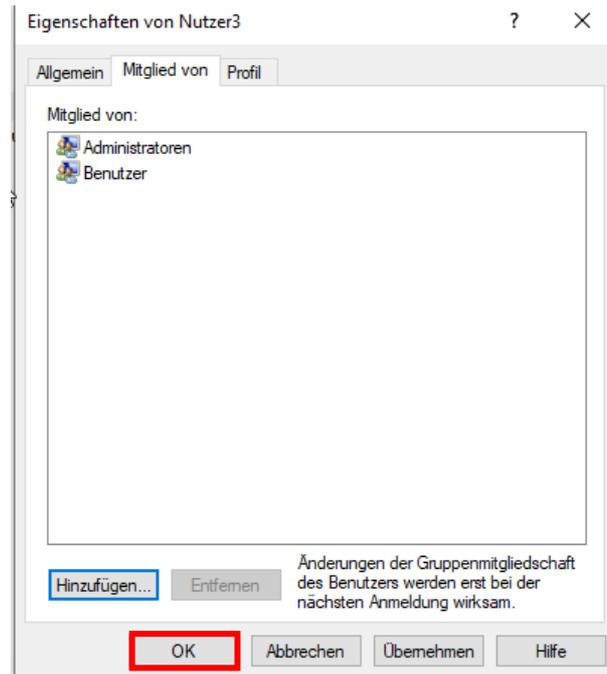
Objekttyp: Gruppen Objekttypen...

Suchpfad: PRAKTIKUM1 Pfade...

Geben Sie die zu verwendenden Objektnamen ein ([Beispiele](#)):

PRAKTIKUM1\Administratoren Namen überprüfen

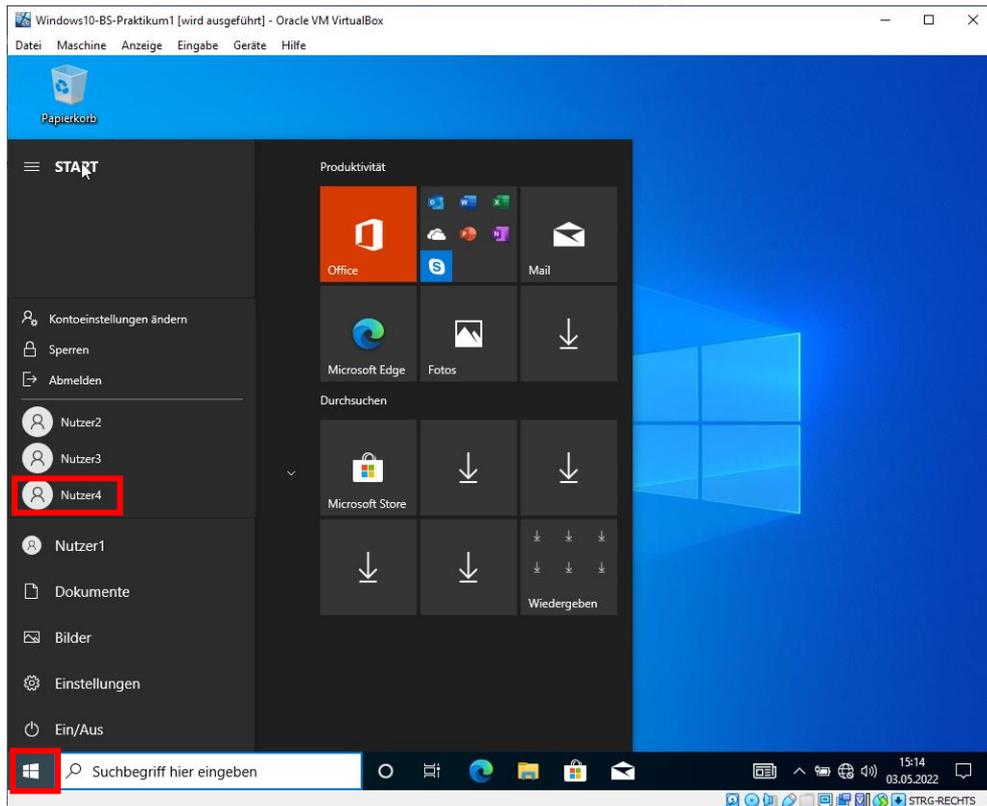
Erweitert... OK Abbrechen



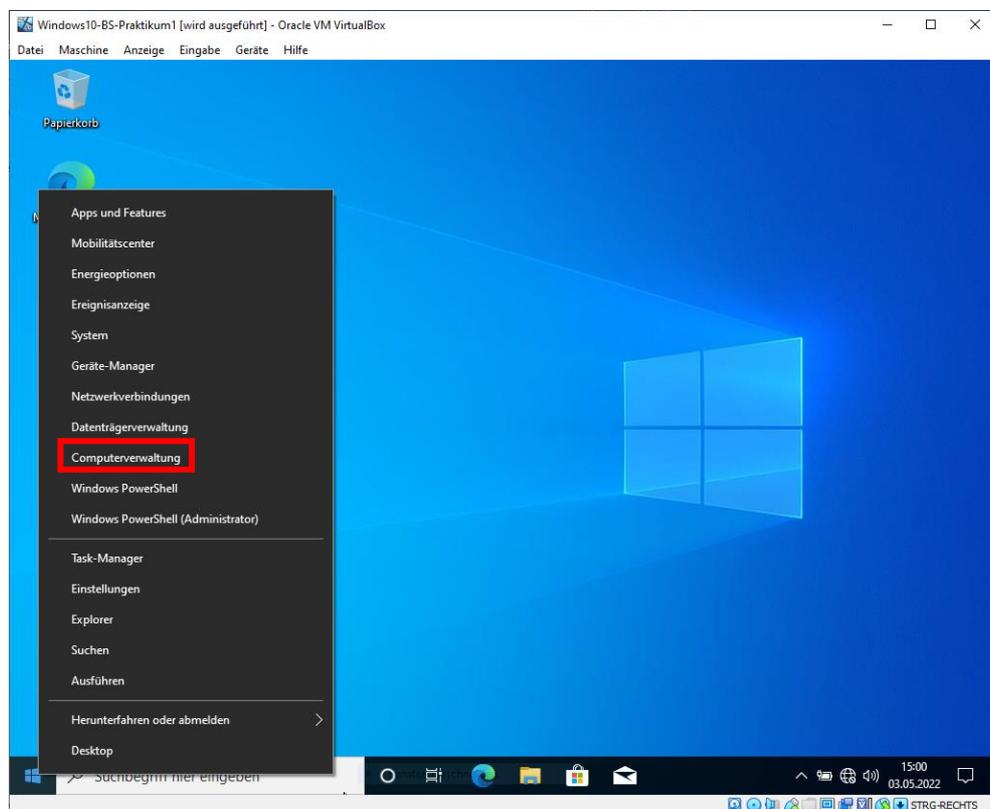
- Fügen Sie nach gleichem Schema selbständig **Nutzer4** mit **Kennwort4** hinzu aber **ohne Administratorrechte**

## Nutzer An-, Um- und Abmeldungen

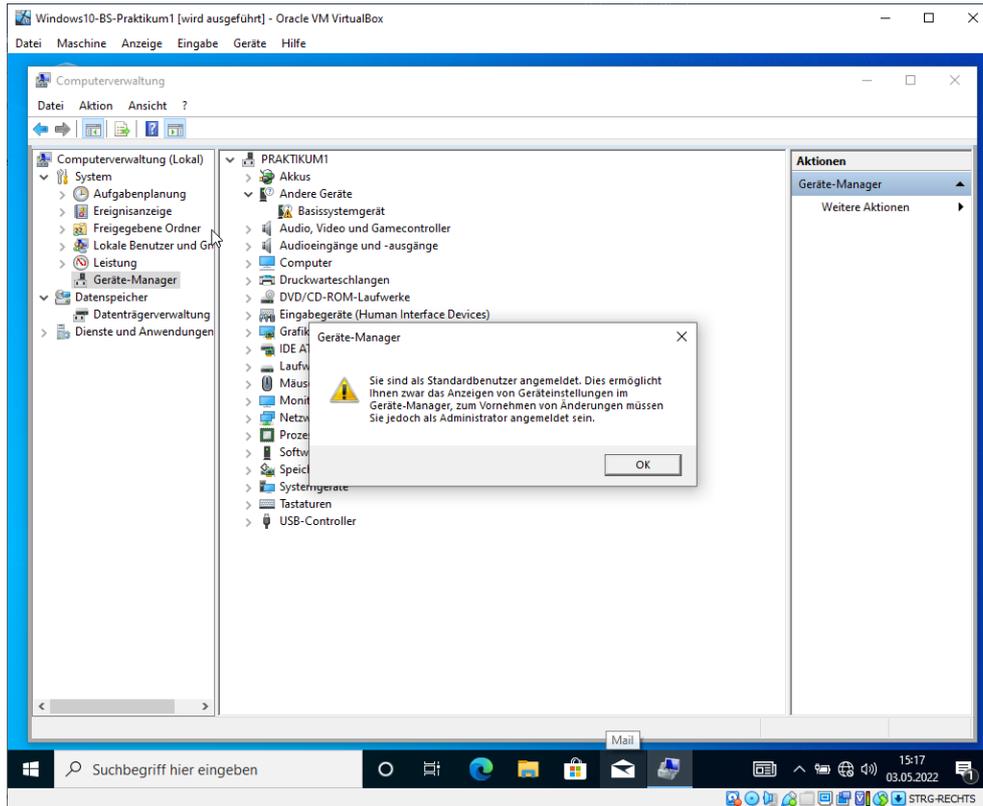
Melden Sie sich als Nutzer 4 zusätzlich am System an.



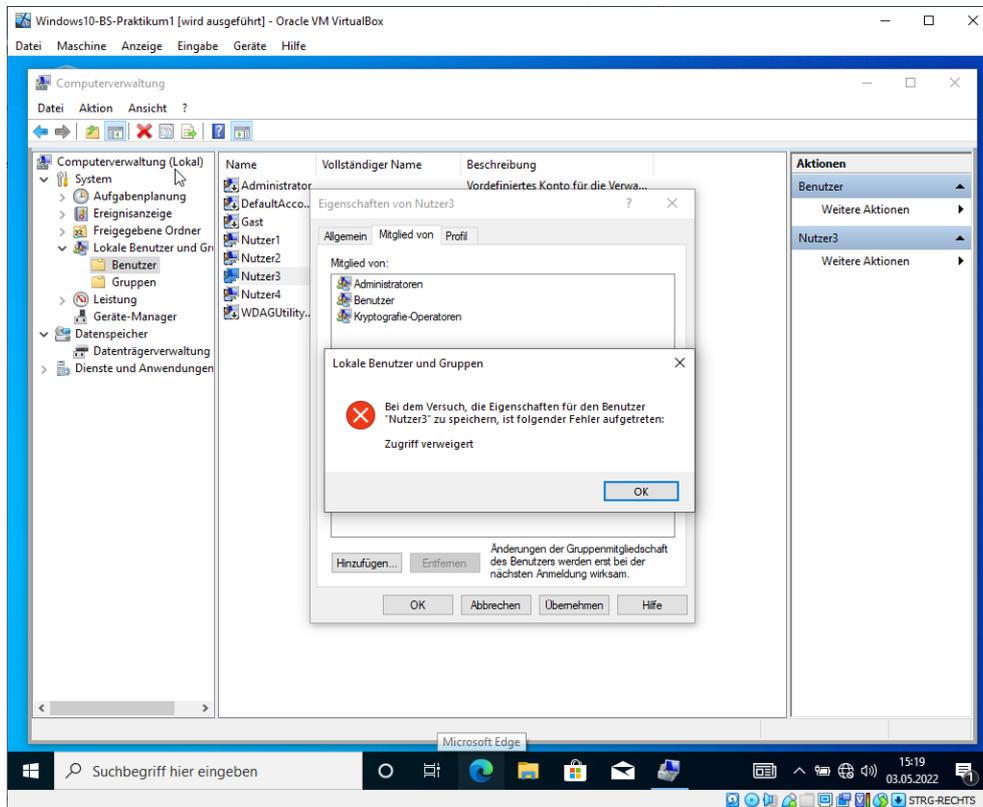
- Starten Sie die Computerverwaltung



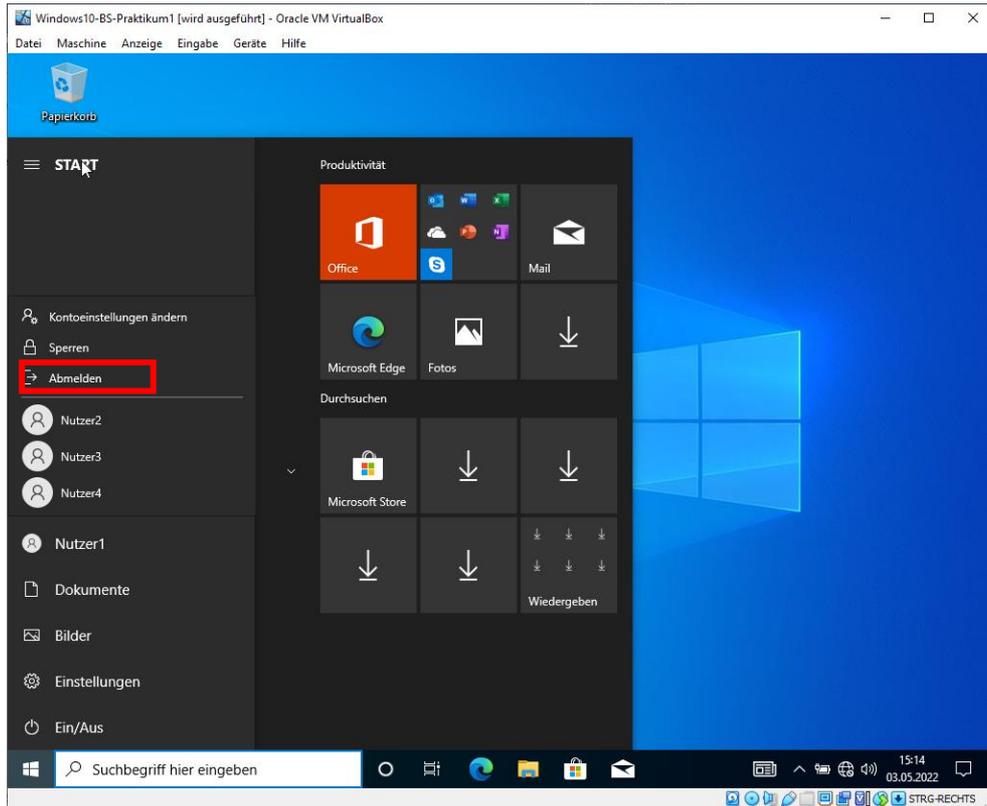
- Überprüfen Sie, ob Sie den Gerätemanager öffnen können



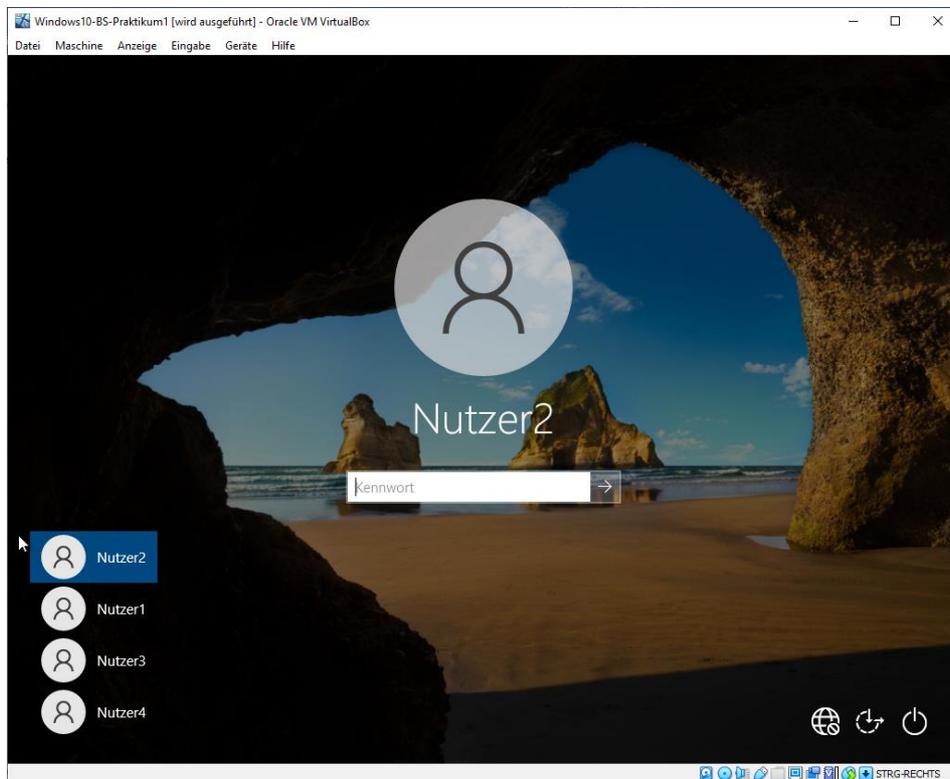
- Überprüfen Sie, ob Sie von Nutzer3 die Gruppenzugehörigkeiten erweitern können



Melden Sie Nutzer4 ab.

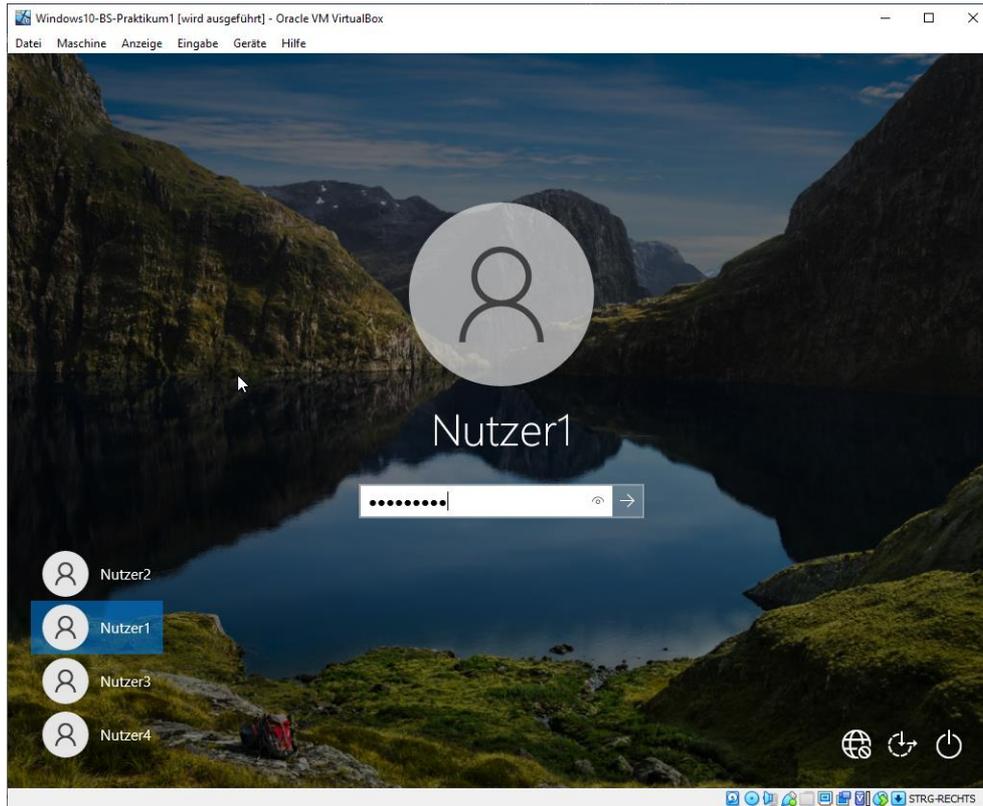


Melden Sie sich als Nutzer2 an.

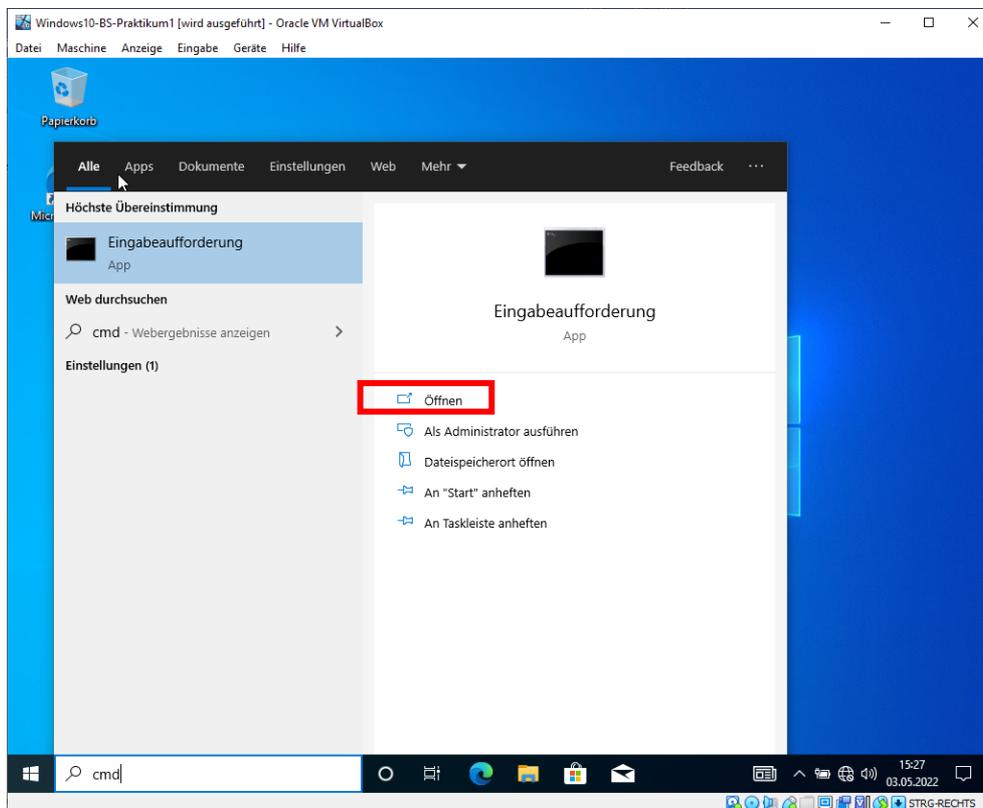


Melden Sie sich als Nutzer2 ab.

Melden Sie sich als Nutzer1 wieder an.



- Öffnen Sie eine **Kommandozeile** durch Eingabe von **CMD** nach dem Klick auf den Windows Start Button



- Geben Sie den Befehl **net user** im Kommandozeilen Fenster ein, um eine Übersicht der Benutzeraccounts zu erhalten

```

Windows10-BS-Praktikum1 [wird ausgeführt] - Oracle VM VirtualBox
Datei Maschine Anzeige Eingabe Geräte Hilfe

C:\Users\Nutzer1>net user

Benutzerkonten für \\PRAKTIKUM1
-----
Administrator          DefaultAccount          Gast
Nutzer1                 Nutzer2                 Nutzer3
Nutzer4                 WDAGUtilityAccount
Der Befehl wurde erfolgreich ausgeführt.

```

- Geben Sie den Befehl **net user administrator** im Kommandozeilen Fenster ein, um eine Übersicht der Informationen zum Administrator Account zu erhalten

```

C:\Users\Nutzer1>net user administrator
Benutzername           Administrator
Vollständiger Name
Beschreibung           Vordefiniertes Konto für die Verwaltung des Computers bzw. der Domäne
Benutzerbeschreibung
Länder-/Regionscode   000 (Standardsystemvorgabe)
Konto aktiv            Nein
Konto abgelaufen      Nie
Letztes Setzen des Kennworts 03.05.2022 15:28:21
Kennwort läuft ab     Nie
Kennwort änderbar     03.05.2022 15:28:21
Kennwort erforderlich Ja
Benutzer kann Kennwort ändern Ja
Erlaubte Arbeitsstationen Alle
Anmeldeskript
Benutzerprofil
Basisverzeichnis
Letzte Anmeldung      Nie
Erlaubte Anmeldezeiten Alle
Lokale Gruppenmitgliedschaften *Administratoren
Globale Gruppenmitgliedschaften *Kein
Der Befehl wurde erfolgreich ausgeführt.

```

- Jetzt versuchen Sie Benutzer5 mit Kennwort5 per Kommandozeilen Befehl **net user Nutzer5 Kennwort5 /add** hinzuzufügen

```

Windows10-BS-Praktikum1 [wird ausgeführt] - Oracle VM VirtualBox
Datei Maschine Anzeige Eingabe Geräte Hilfe

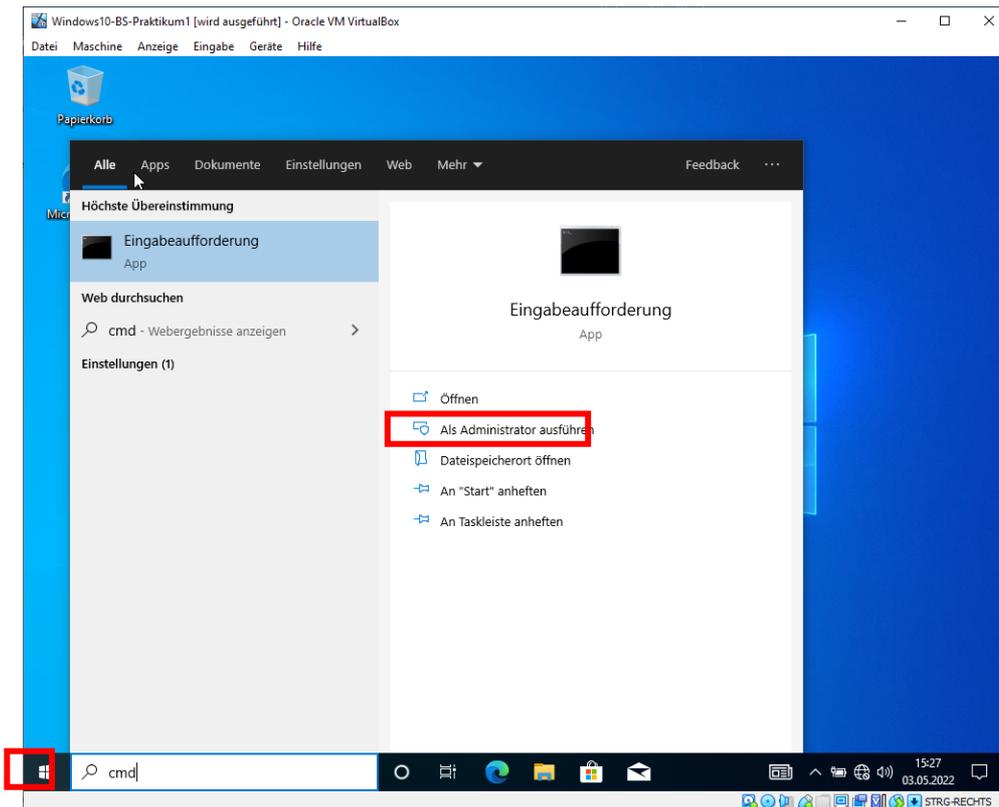
C:\Users\Nutzer1>net user Nutzer5 Kennwort5 /add
Systemfehler 5 aufgetreten.
Zugriff verweigert

C:\Users\Nutzer1>

```

- Dies scheitert wegen fehlender Administratorenrechte in der Kommandozeile!

Öffnen Sie eine **Kommandozeile** durch Eingabe von **CMD** nach dem Klick auf den Windows Start Button mit Administratorenrechten.



- Jetzt versuchen Sie Benutzer5 mit Kennwort5 per Kommandozeilen Befehl **net user Nutzer5 Kennwort5 /add** hinzuzufügen

```

Administrator: Eingabeaufforderung
Microsoft Windows [Version 10.0.19044.1288]
(c) Microsoft Corporation. Alle Rechte vorbehalten.

C:\Windows\system32>net user Nutzer5 Kennwort5 /add
Der Befehl wurde erfolgreich ausgeführt.
  
```

- Lassen Sie sich von Benutzer5 die Informationen anzeigen mit dem Kommandozeilen Befehl **net user Nutzer5**

```

C:\Windows\system32>net user Nutzer5
Benutzername                Nutzer5
Vollständiger Name
Beschreibung
Benutzerbeschreibung
Länder-/Regionscode        000 (Standardsystemvorgabe)
Konto aktiv                 Ja
Konto abgelaufen           Nie

Letztes Setzen des Kennworts 03.05.2022 15:30:14
Kennwort läuft ab          14.06.2022 15:30:14
Kennwort änderbar         03.05.2022 15:30:14
Kennwort erforderlich      Ja
Benutzer kann Kennwort ändern Ja

Erlaubte Arbeitsstationen   Alle
Anmeldeskript
Benutzerprofil
Basisverzeichnis
Letzte Anmeldung           Nie
Erlaubte Anmeldezeiten     Alle

lokale Gruppenmitgliedschaften *Benutzer
globale Gruppenmitgliedschaften *Kein
Der Befehl wurde erfolgreich ausgeführt.
  
```

- Der Nutzer ist derzeit nur normaler Benutzer

- Nehmen Sie den Nutzer5 in die Gruppe der Administratoren mit dem Kommandozeilen Befehl **net localgroup Administratoren Nutzer5 /add** auf

```

Windows10-BS-Praktikum1 [wird ausgeführt] - Oracle VM VirtualBox
Datei Maschine Anzeige Eingabe Geräte Hilfe
Administrator: Eingabeaufforderung
C:\Windows\system32>net localgroup Administratoren Nutzer5 /add
Der Befehl wurde erfolgreich ausgeführt.

```

- Lassen Sie sich von Benutzer5 die Informationen erneut anzeigen mit dem Kommandozeilen Befehl **net user Nutzer5** und überprüfen Sie die Gruppenänderung

```

C:\Windows\system32>net user Nutzer5
Benutzername                Nutzer5
Vollständiger Name
Beschreibung
Benutzerbeschreibung
Länder-/Regionscode         000 (Standardsystemvorgabe)
Konto aktiv                  Ja
Konto abgelaufen            Nie

Letztes Setzen des Kennworts 03.05.2022 15:30:14
Kennwort läuft ab           14.06.2022 15:30:14
Kennwort änderbar           03.05.2022 15:30:14
Kennwort erforderlich        Ja
Benutzer kann Kennwort ändern Ja

Erlaubte Arbeitsstationen    Alle
Anmeldeskript
Benutzerprofil
Basisverzeichnis
Letzte Anmeldung            Nie

Erlaubte Anmeldezeiten       Alle

Lokale Gruppenmitgliedschaften *Administratoren
                               *Benutzer
Globale Gruppenmitgliedschaften *Kein
Der Befehl wurde erfolgreich ausgeführt.

```

- Lassen Sie sich alle Benutzer der Gruppe **Administratoren** mit dem Kommandozeilen Befehl **net localgroup Administratoren** Anzeigen

```

Windows10-BS-Praktikum1 [wird ausgeführt] - Oracle VM VirtualBox
Datei Maschine Anzeige Eingabe Geräte Hilfe
Administrator: Eingabeaufforderung
C:\Windows\system32>net localgroup Administratoren
Aliasname      Administratoren
Beschreibung   Administratoren haben uneingeschränkten Vollzugriff auf den Computer bzw. die Domäne.

Mitglieder
-----
Administrator
Nutzer1
Nutzer2
Nutzer3
Nutzer5
Der Befehl wurde erfolgreich ausgeführt.

C:\Windows\system32>

```

## Benutzeraccount innerhalb eines anderen Accounts nutzen

Öffnen Sie im Nutzer1 eine Kommandozeile mit administrativen Berechtigungen.

- Geben Sie den Kommandozeilen Befehl **runas /user:Nutzer3 „C:\windows\system32\cmd.exe“** ein

```

Windows10-BS-Praktikum1 [wird ausgeführt] - Oracle VM VirtualBox
Datei Maschine Anzeige Eingabe Geräte Hilfe
Administrator: Eingabeaufforderung
C:\Windows\system32>runas /user:Nutzer3 "C:\windows\system32\cmd.exe"
Geben Sie das Kennwort für "Nutzer3" ein:
Es wird versucht, C:\windows\system32\cmd.exe als Benutzer "PRAKTIKUM1\Nutzer3" zu starten...

C:\Windows\system32>_

```

- Nach Eingabe des Kennworts erhalten Sie ein Kommandozeilenfenster von Nutzer3
- Überprüfen Sie mit dem Kommandozeilen Befehl **whoami** ob dies eine Kommandozeile von **Nutzer3** ist

```

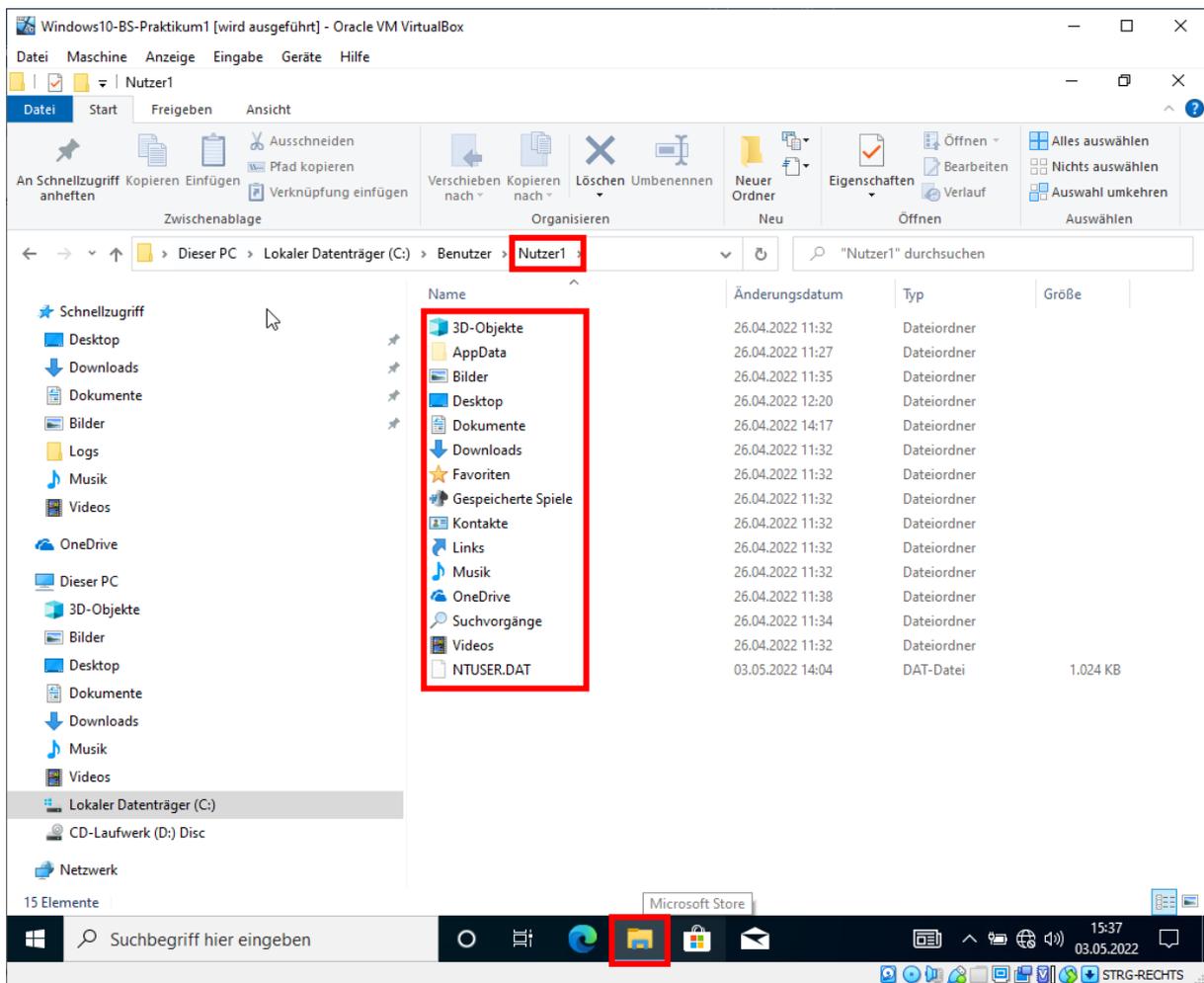
C:\Windows\system32\cmd.exe (wird als PRAKTIKUM1\Nutzer3 ausgeführt)
Microsoft Windows [Version 10.0.19044.1288]
(c) Microsoft Corporation. Alle Rechte vorbehalten.

C:\Windows\system32>whoami
praktikum1\nutzer3

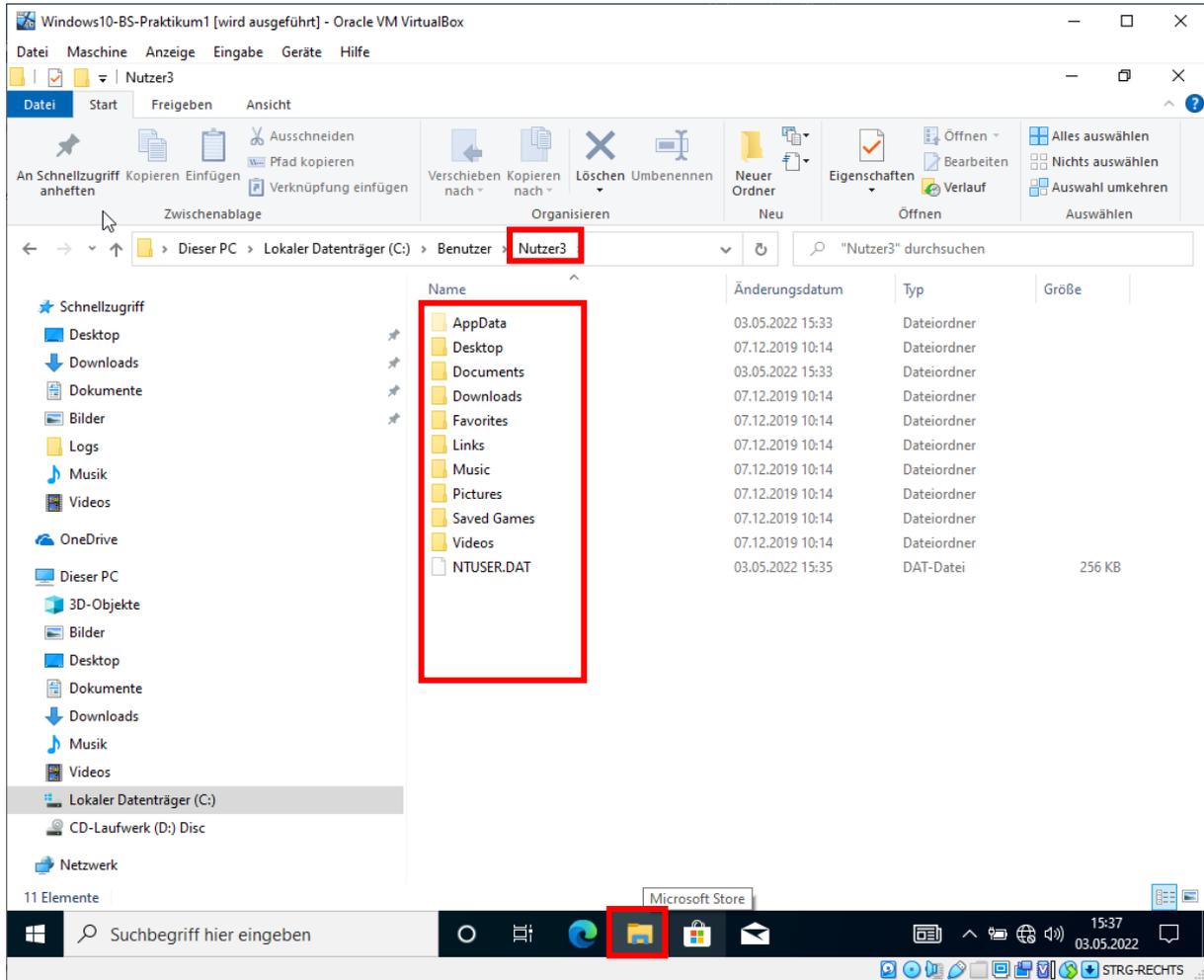
C:\Windows\system32>

```

Jetzt überprüfen Sie die Benutzerverzeichnisse von Nutzer1 und Nutzer3 im Windows Explorer (möglicherweise müssen Sie hier einige Berechtigungsfenster bestätigen).

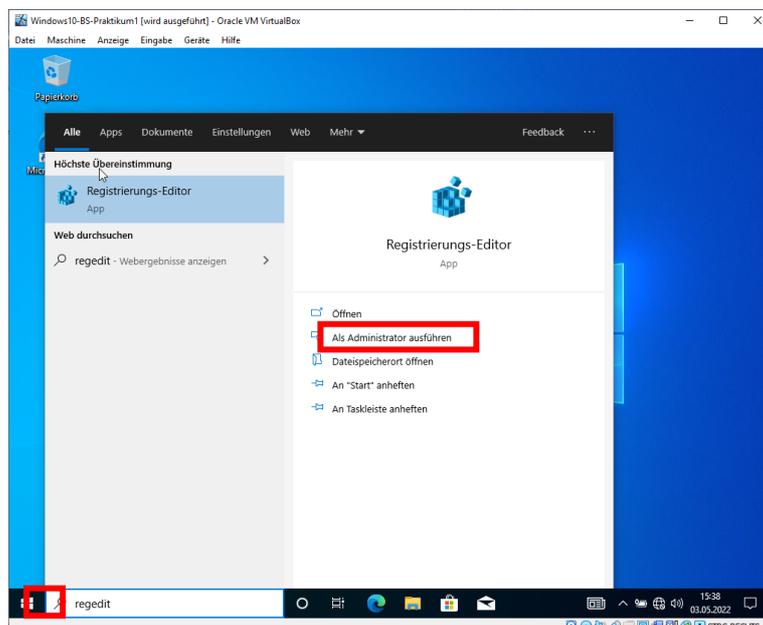


- Fällt Ihnen der Unterschied auf?

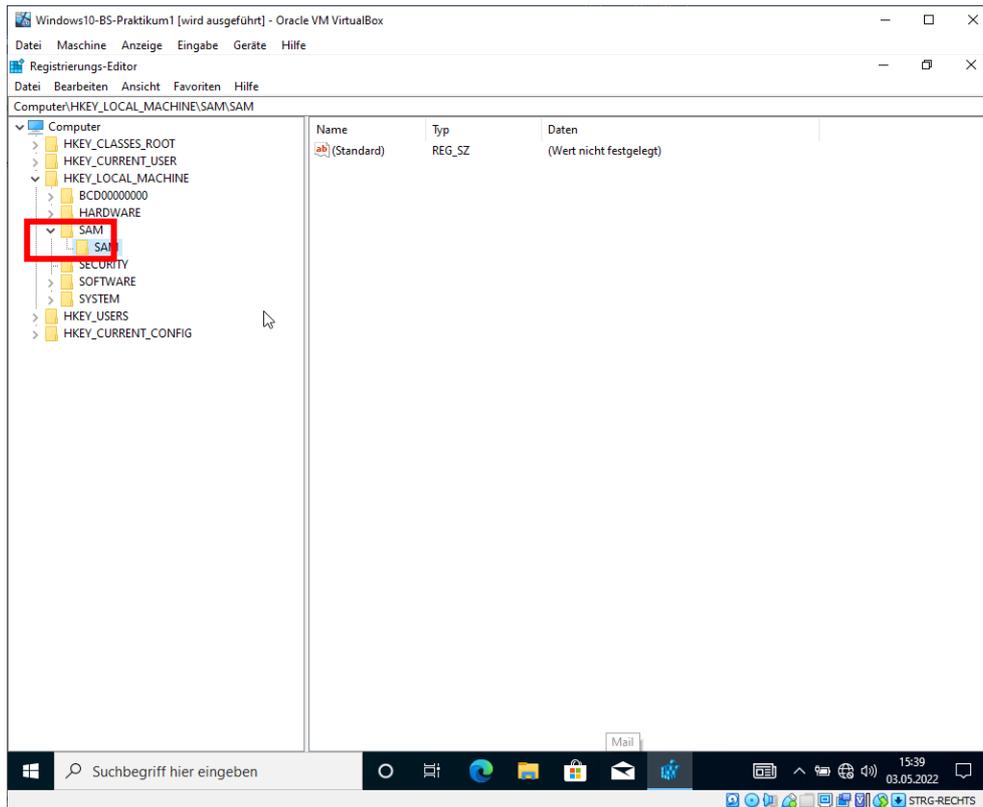


## Überprüfung von Account Informationen in der Registry

Starten Sie den Registrierungseditor **Regedit** über den Windows Start Button und die Eingabe von **Regedit als Administrator**.

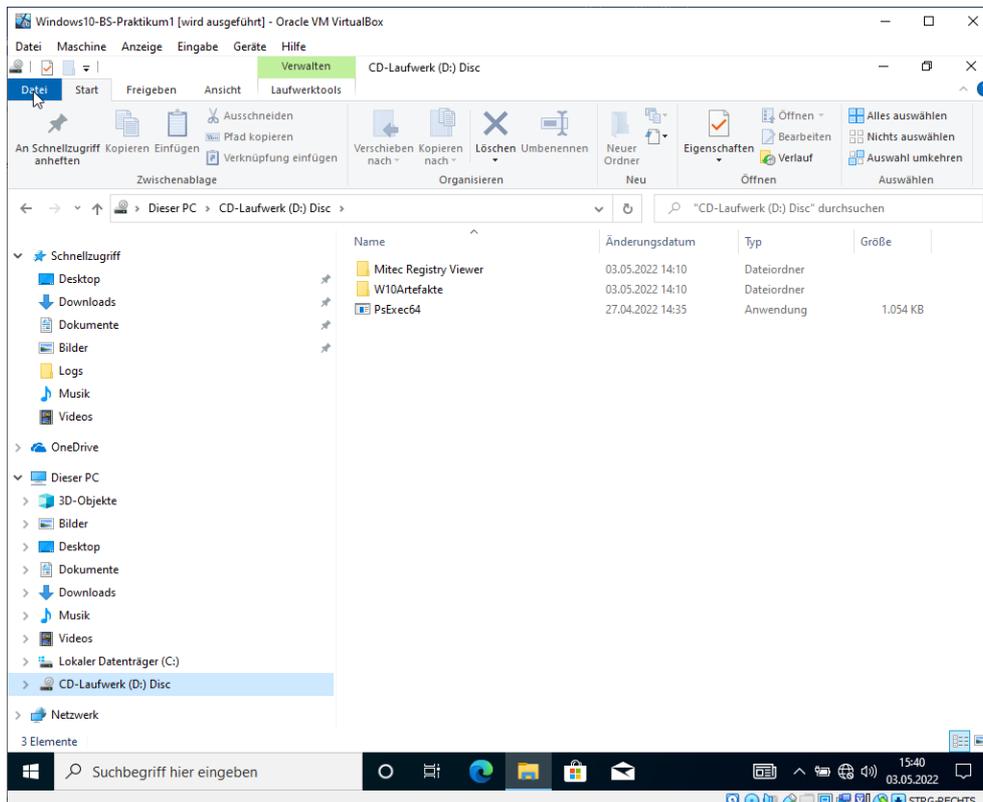


➤ Können Sie den Schlüssel der SAM-Datei öffnen?

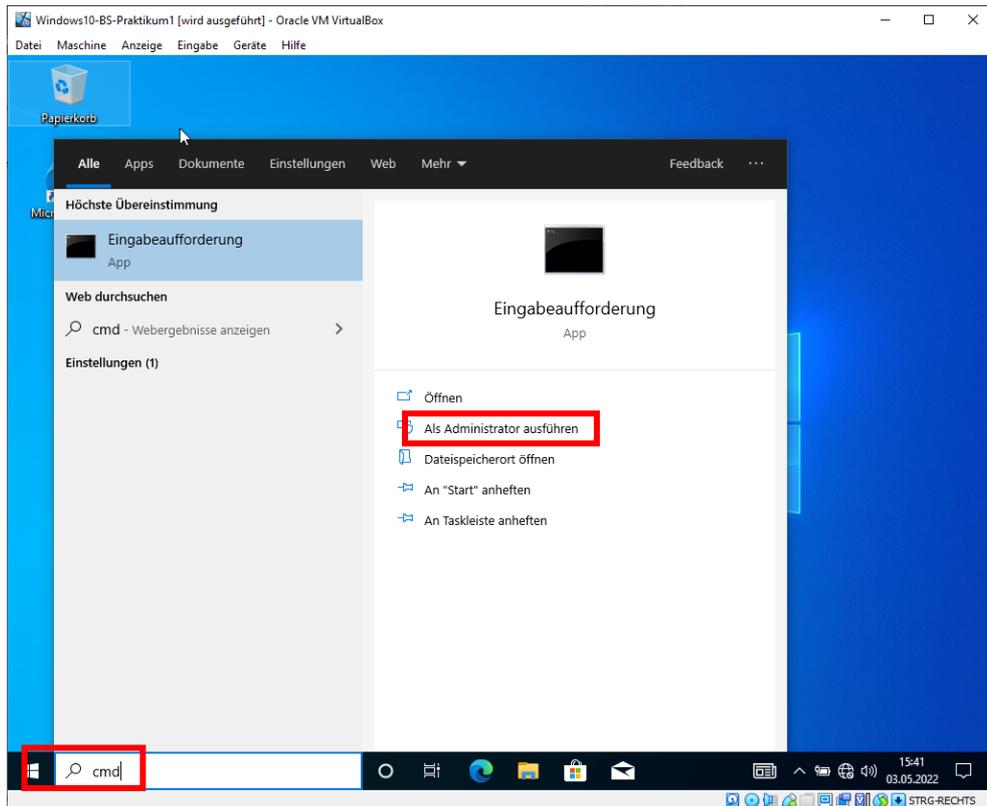


Nein, Ihnen fehlen Zugriffsrechte trotz Administrator!

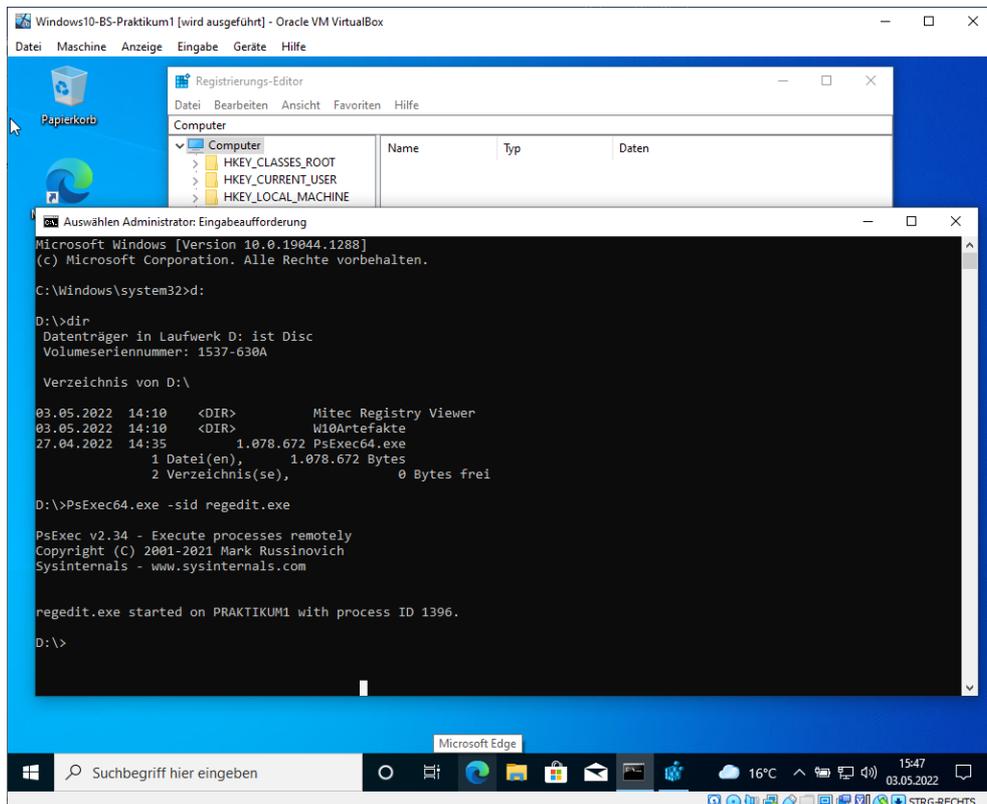
Überprüfen Sie ob die PR2.iso korrekt eingebunden ist und öffnen Sie diese im Windows Explorer.



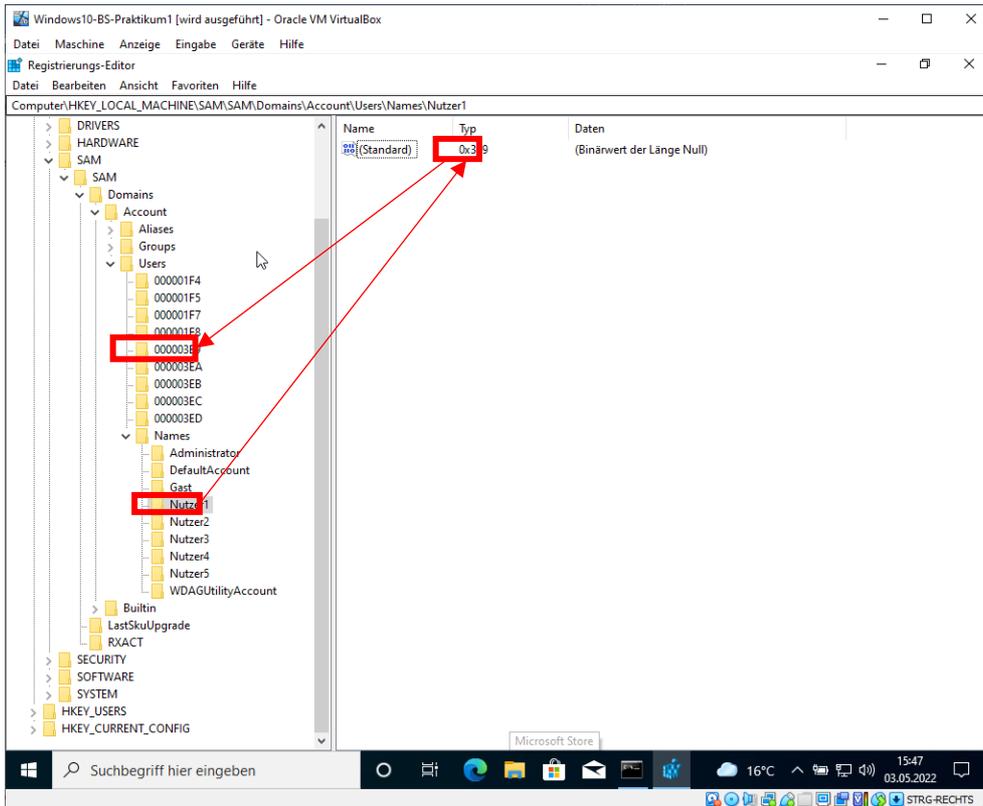
- Starten Sie ein Kommandozeilenfenster mit Administrativen Berechtigungen



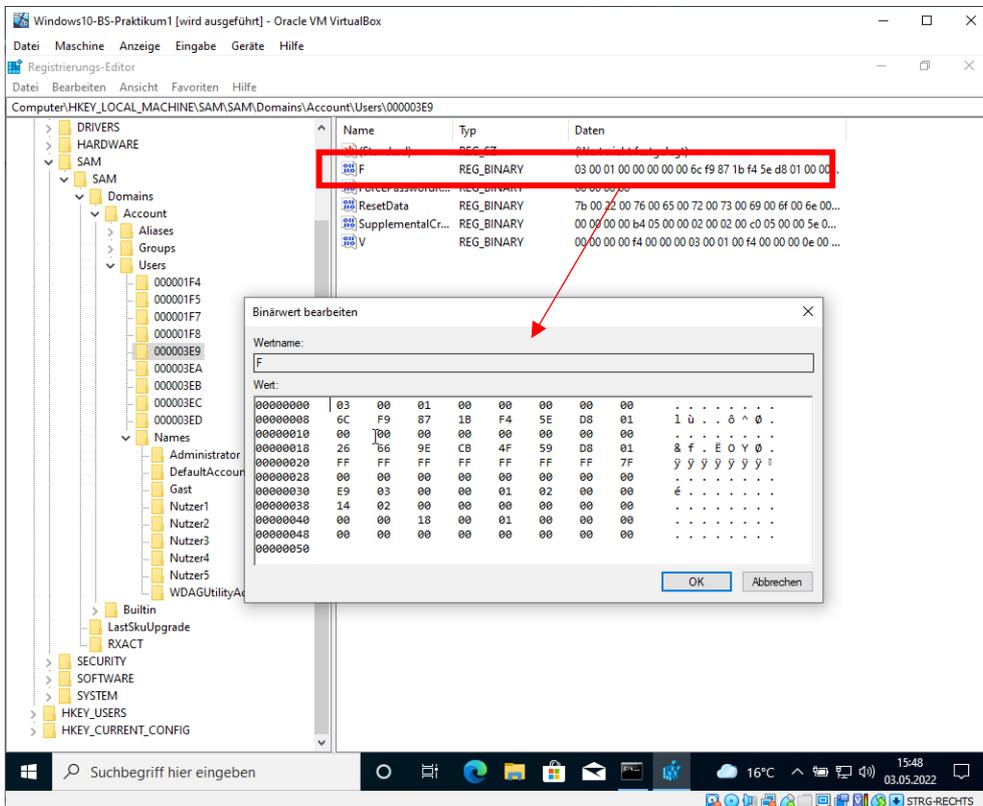
- Wechseln Sie im Kommandozeilenfenster auf den CD-Laufwerksbuchstaben (D:\)
- Schauen Sie ob die Dateien vorhanden sind mit dem **dir** Befehl
- Starten Sie den Registrierungseditor mit SYSTEM Rechten durch Aufruf von **PSEXEC64.exe -sid regedit.exe** (hierfür benötigt die von Sysinternals stammende Softwareinternetzugriff für die Lizenzprüfung!)



Als Ergebnis sehen Sie jetzt im Registrierungseditor die SAM-Einträgen.



➤ Öffnen Sie im Schlüssel **00003E9** den Wert **F**



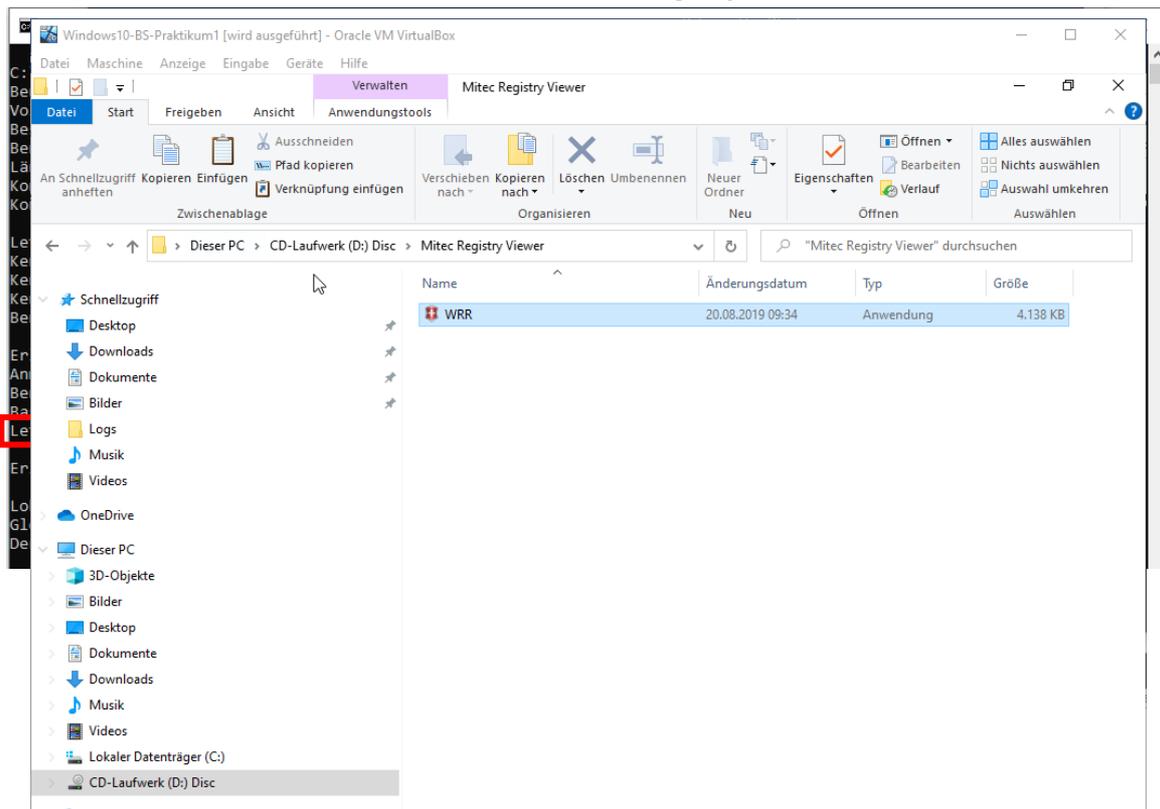


```
Windows PowerShell
PS C:\Users\Nutzer1> [datetime]::FromFileTime([Convert]::ToInt64("01D85EF41887F96C", 16))
Dienstag, 3. Mai 2022 15:45:5
```

➤ Prüfen Sie mit Eingabe des Kommandozeilen Befehls **net user Nutzer1** gegen

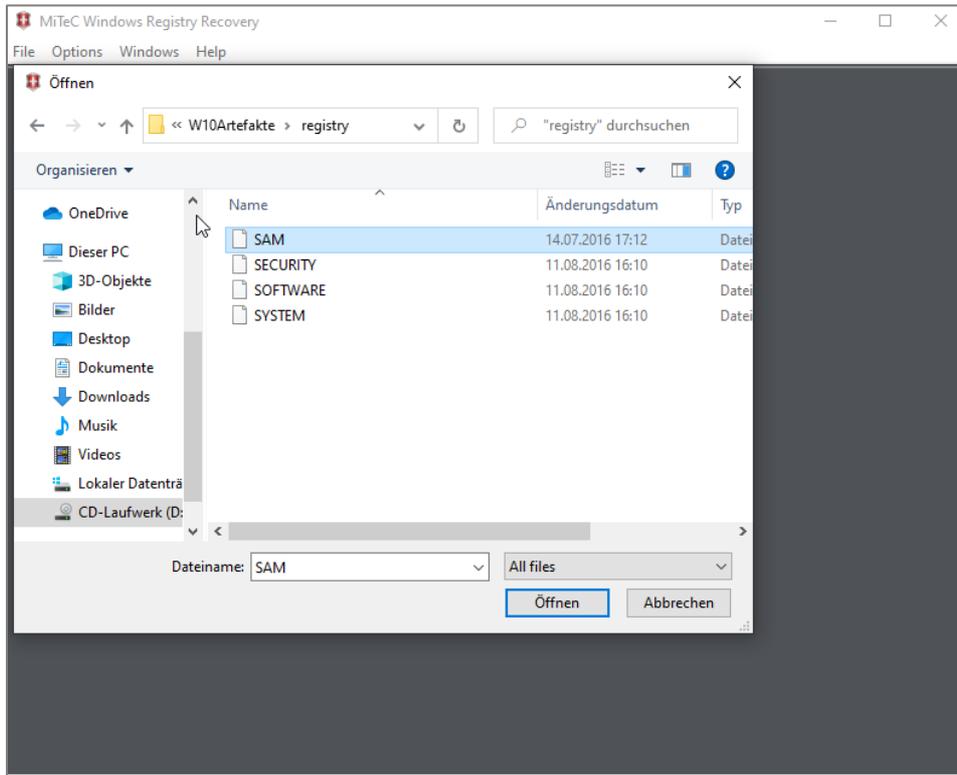
## Nutzung externer Tools zur Registry Analyse der SAM

Öffnen Sie die Software **WRR.exe** aus dem Verzeichnis **Mitec Registry Viewer** des CD-Laufwerks.

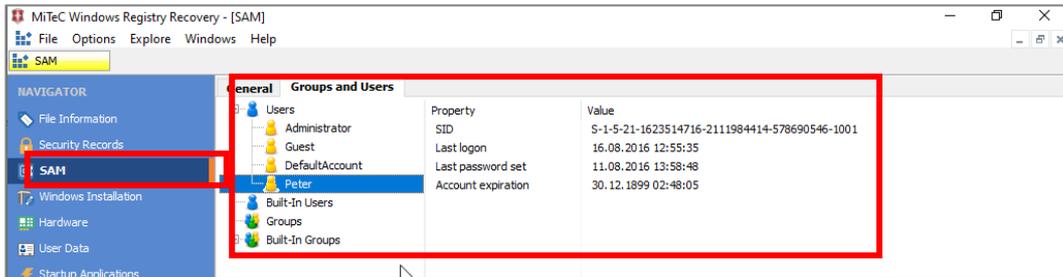


Hier haben Sie die Möglichkeit Registrierungsdatenbankdateien zu öffnen. Die lokale Registry kann auf Grund des laufenden Systemzustandes nicht geöffnet werden!

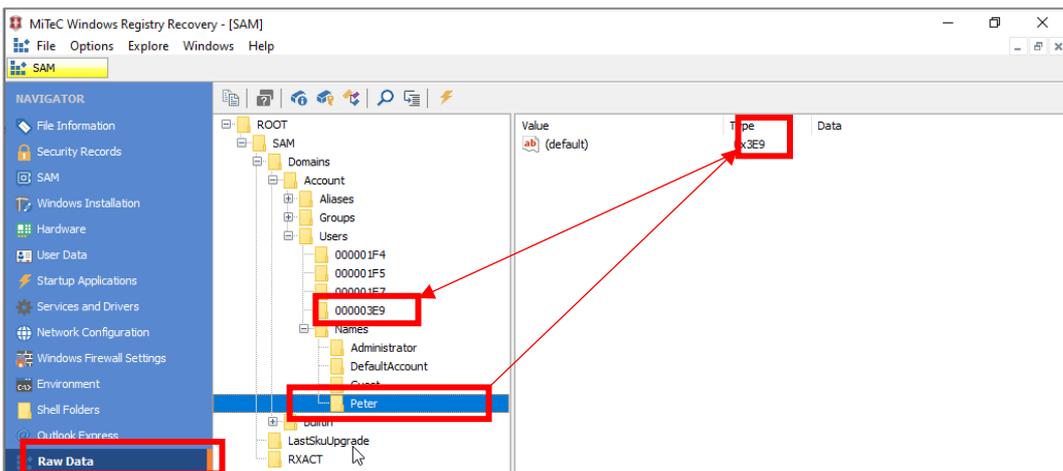
- Öffnen Sie die auf der CD befindliche **SAM**-Datenbank im Verzeichnis **W10Artefakte\registry**

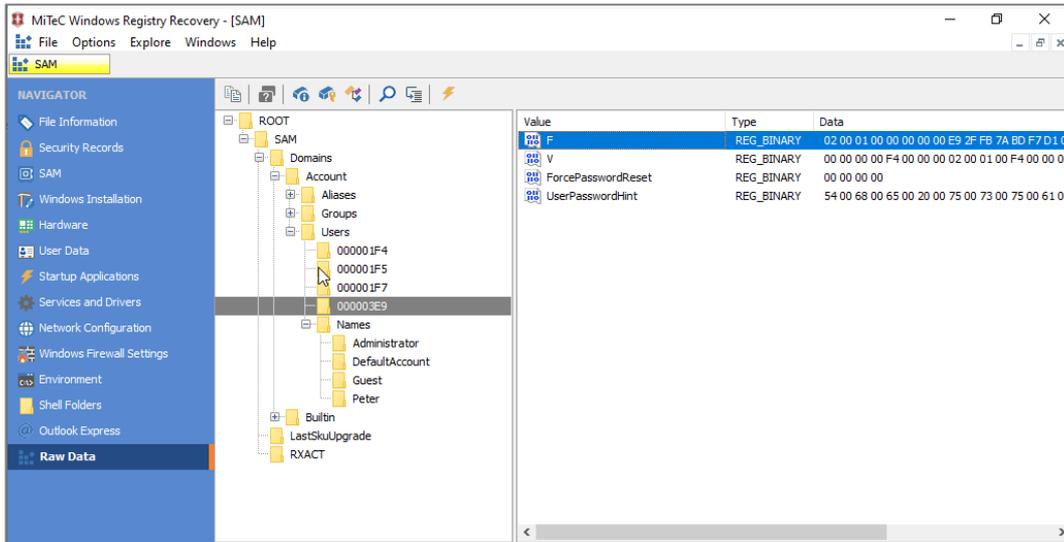


- Über den Punkt SAM können die Informationen aufbereitet eingesehen werden



- Über RAW Data hat man Zugriff auch auf die reinen Registry Daten





➤ Hier lassen sich im Editor sogar die Zeitstempel direkt innerhalb der Byte Werte interpretieren

