Studienprogramm Sachbearbeiter:in Digitale Forensik
Praktikum Betriebssysteme
Dozent: Tim Wetterau
wetterau@hs-mittweida.de
Stand: 10.05.2024

HOCHSCHULE MITTWEIDA
University of Applied Sciences

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

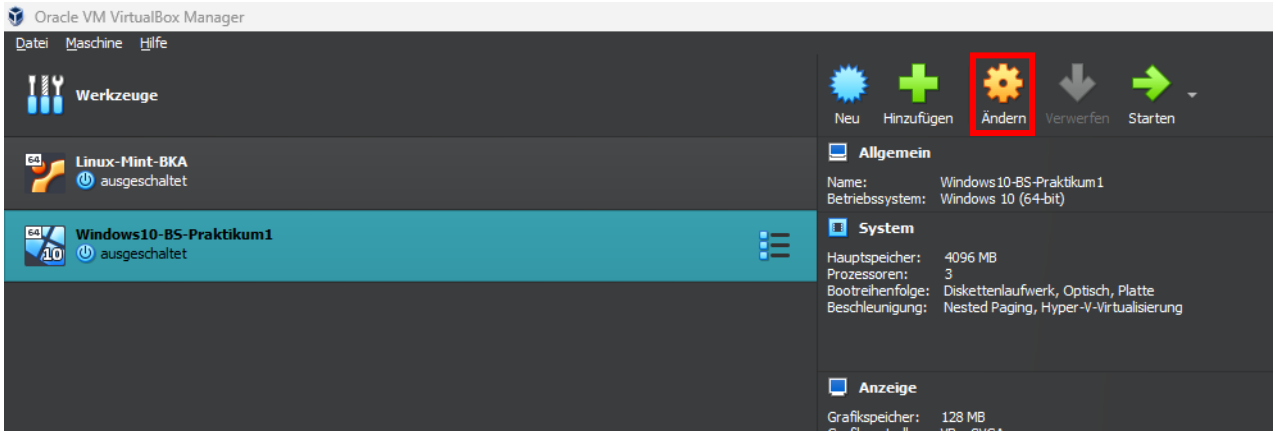
Allgemeine Hinweise

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.

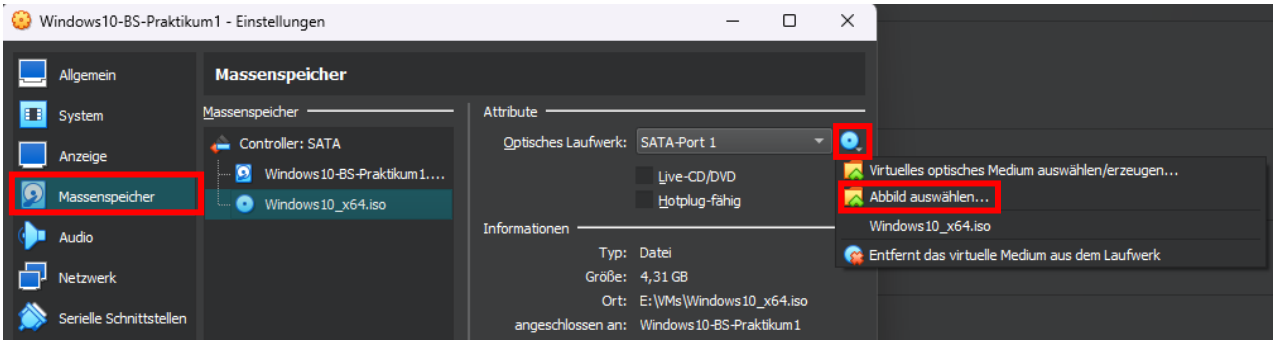
Einbinden der PR2.iso

Öffnen Sie VirtualBox.

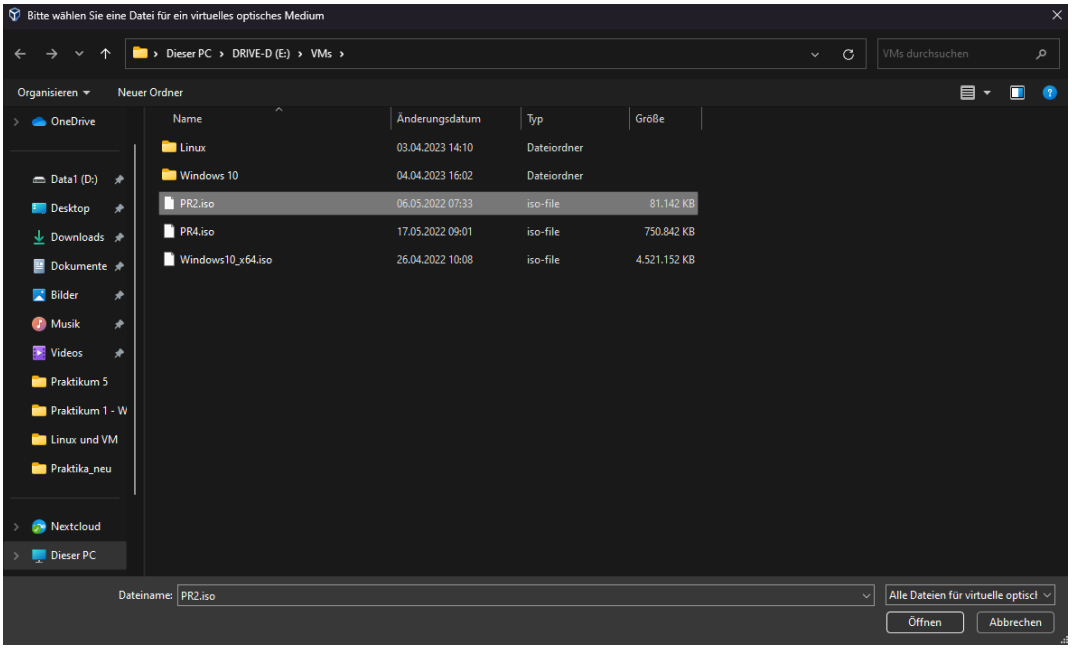
Wählen Sie die im Praktikum 1 angelegte VM aus oder importieren Sie zuerst die OVA-Datei wählen dann die VM des Praktikum 1 aus. Gehen Sie auf Ändern (nicht Doppelklicken auf die VM, das würde diese Starten).

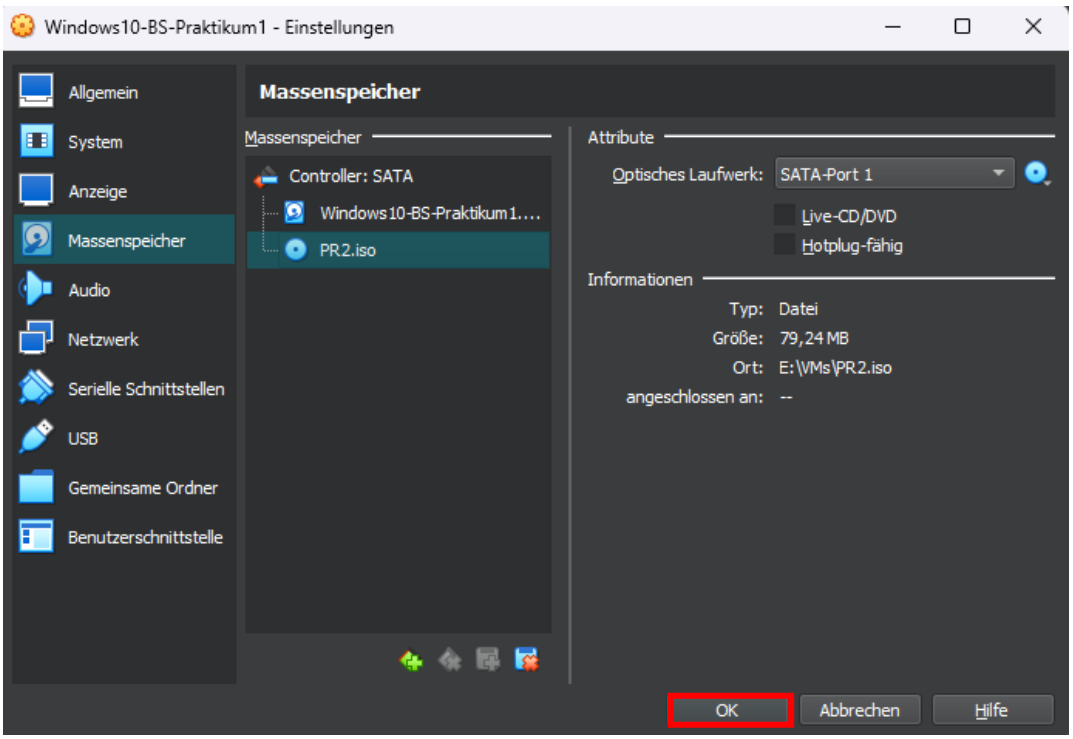


- Wählen Sie den Massenspeicher aus

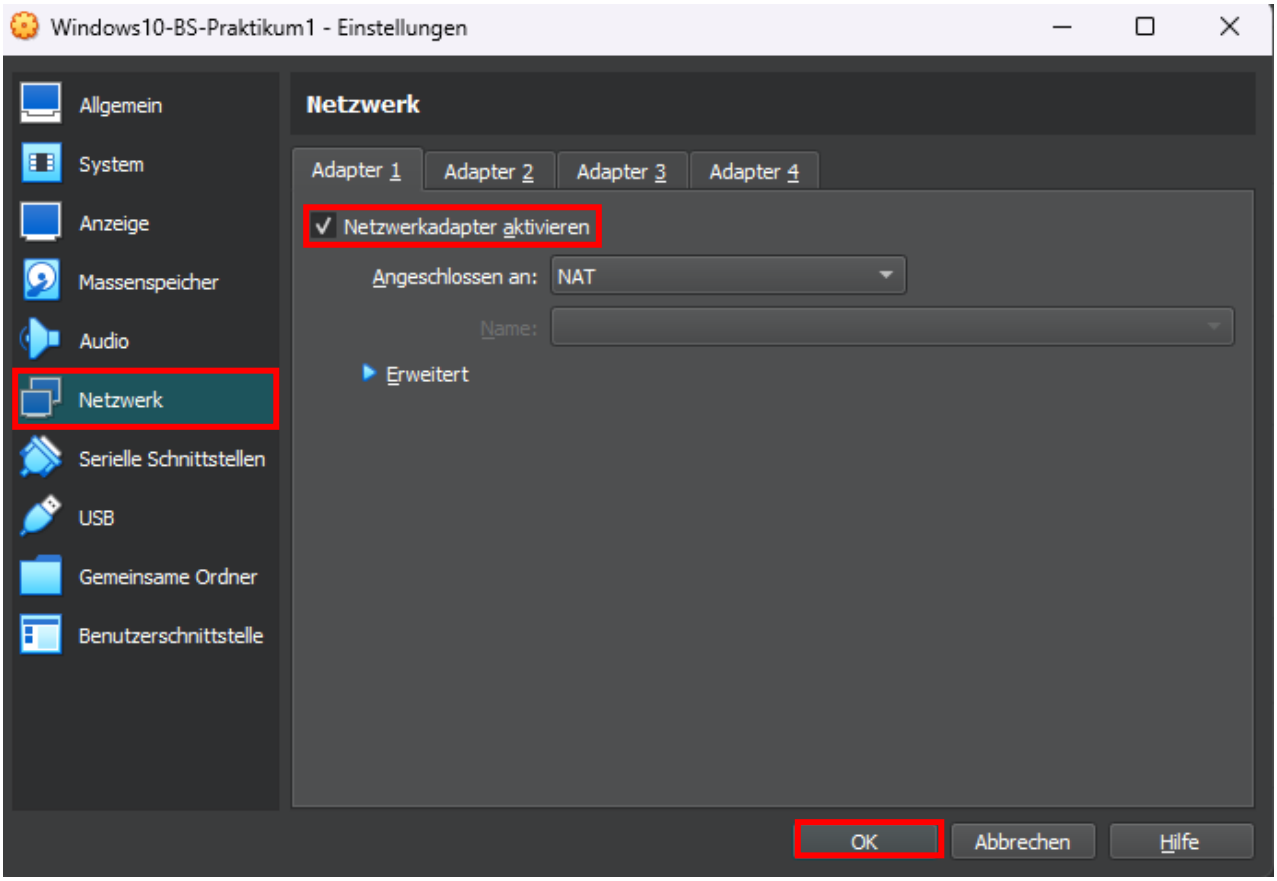


- Binden Sie bei der CD die heruntergeladene Abbilddatei **PR2.iso** ein

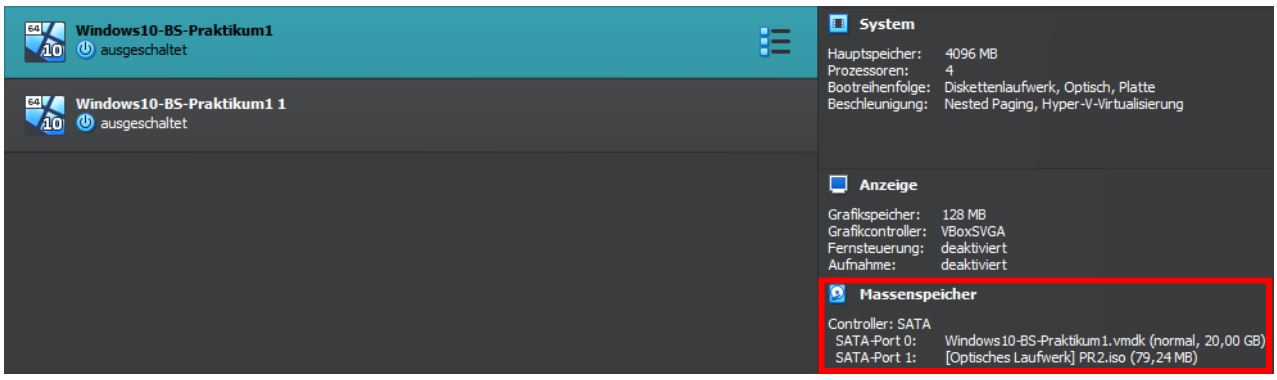




- Aktivieren Sie die Netzwerkverbindung



- Bestätigen Sie die Änderungen mit OK

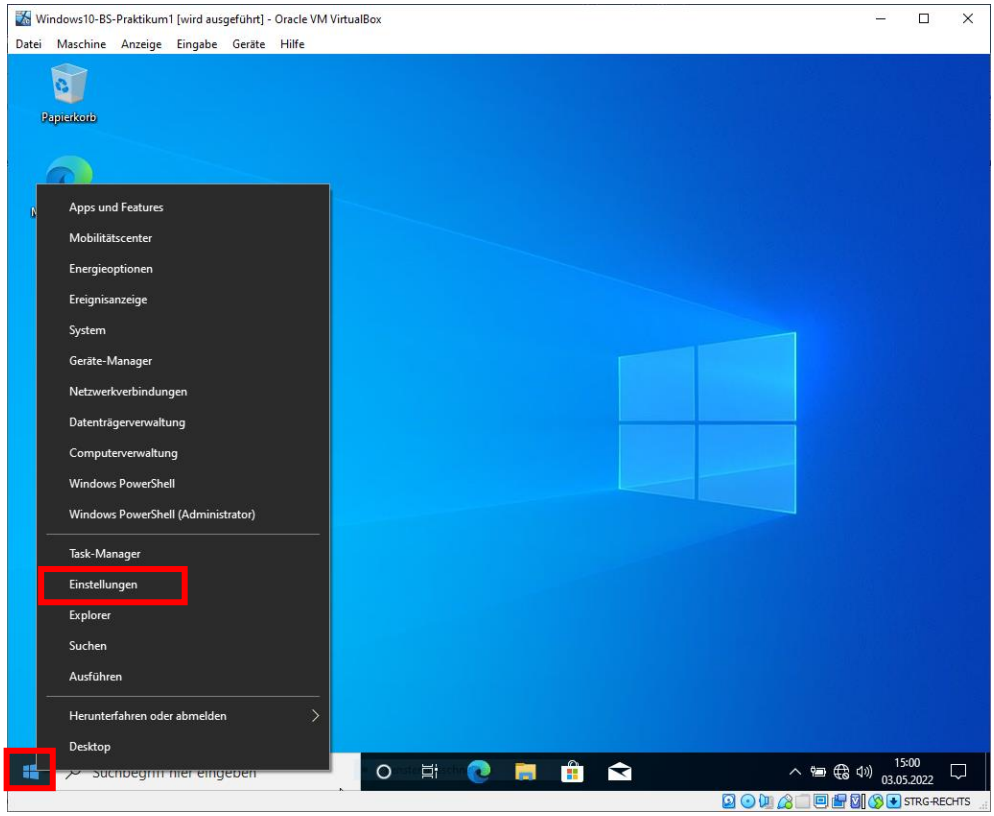


Ergebnis

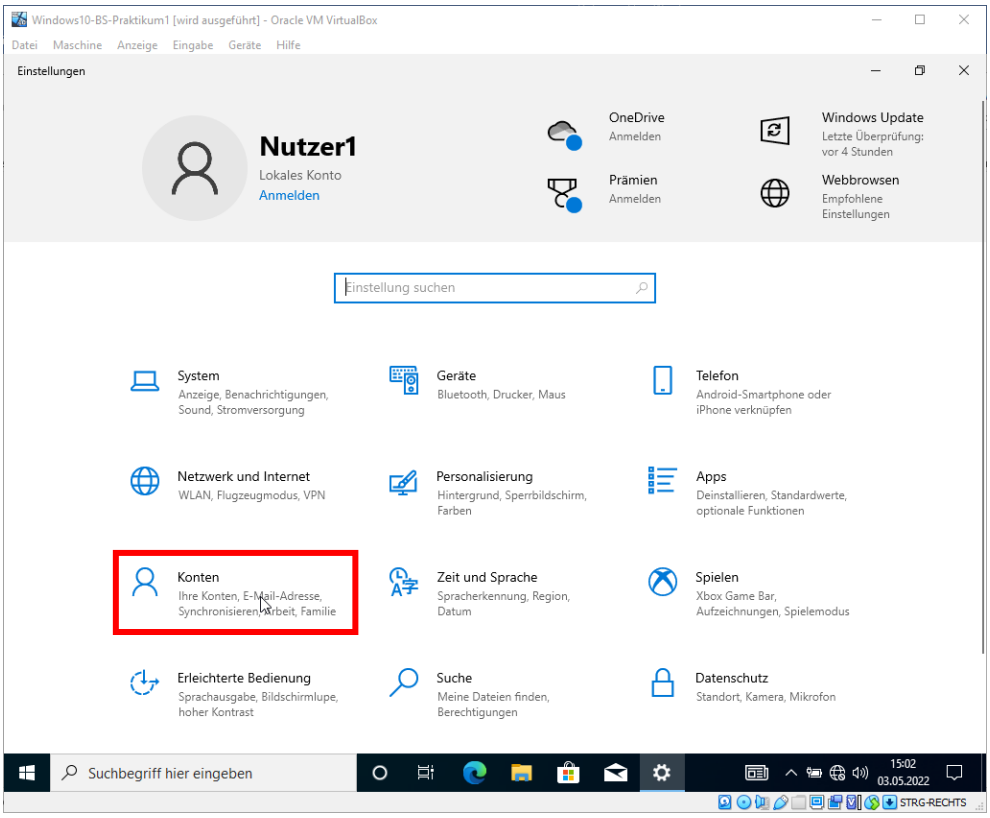
Benutzer mit Systemeinstellung anlegen und überprüfen

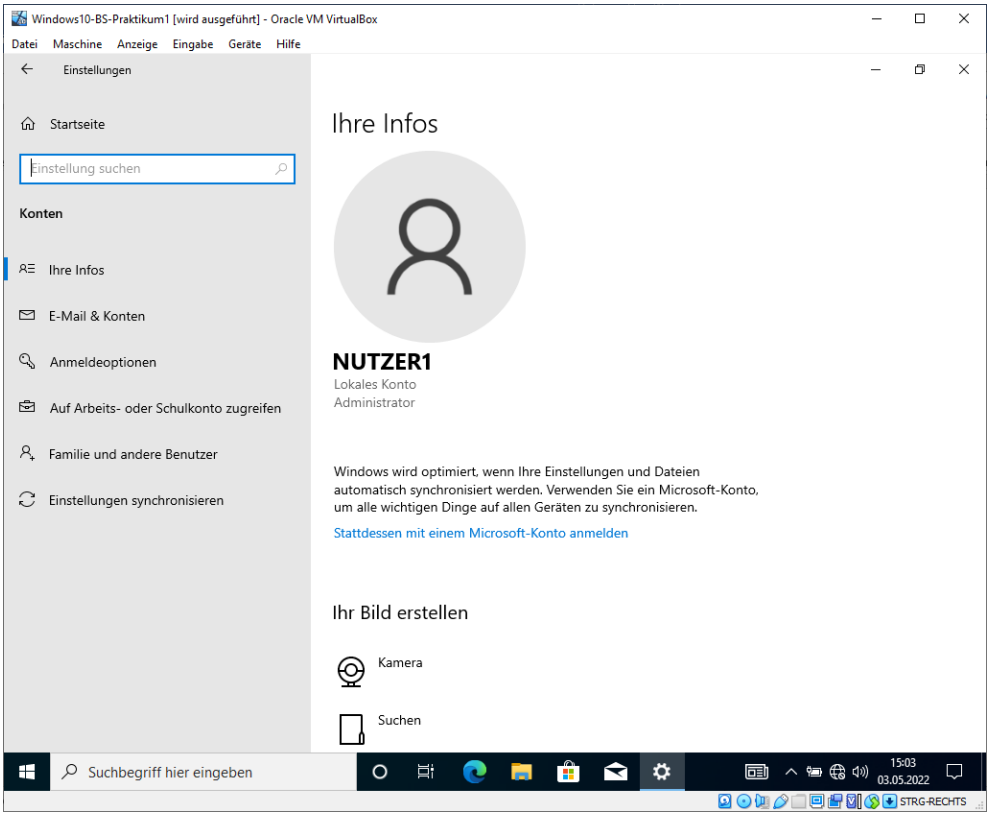
Starten Sie jetzt die VM und loggen sich als **Nutzer1** mit **Kennwort1** ein.

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

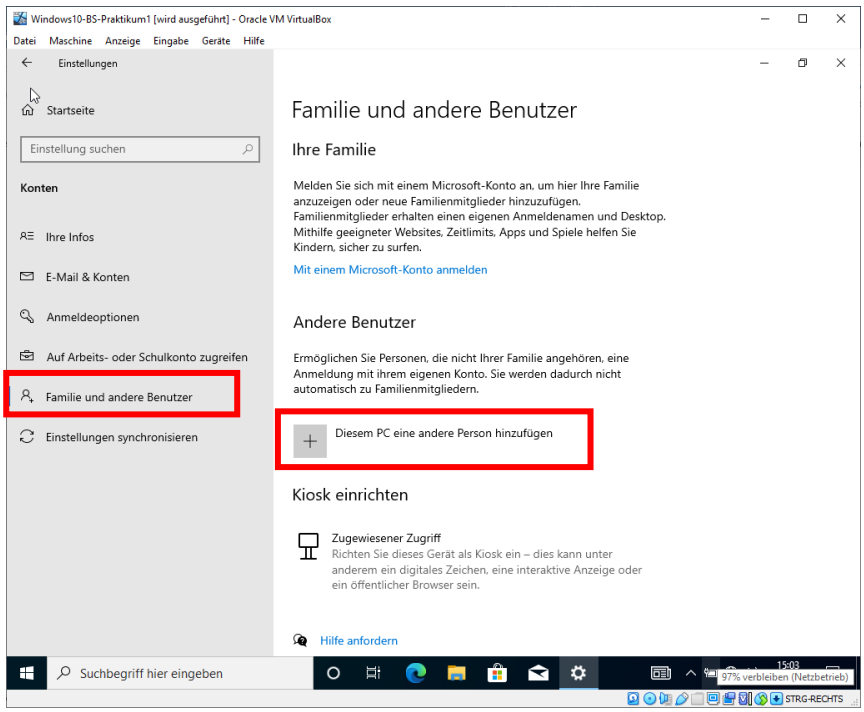


➢ Gehen Sie auf Konten

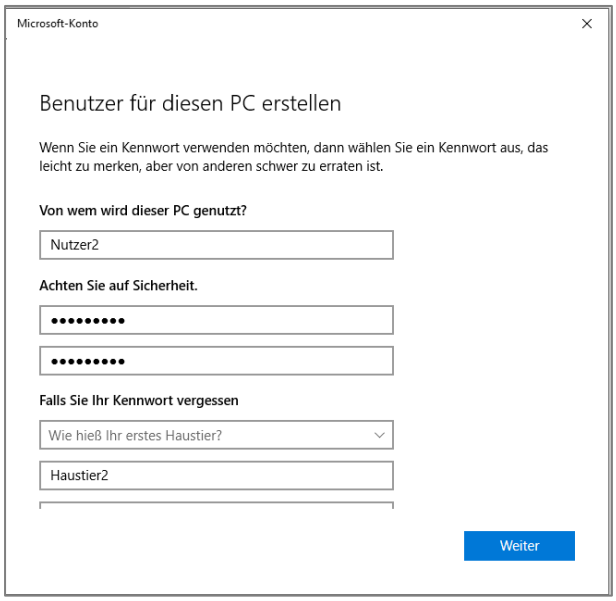




- Wählen Sie Familie und andere Benutzer und fügen eine Person hinzu
  - wählen Sie ggf.: „Ich kenne die Anmeldeoptionen für diese Person nicht“ aus
  - anschließend noch „Benutzer ohne Microsoft-Konto hinzufügen“

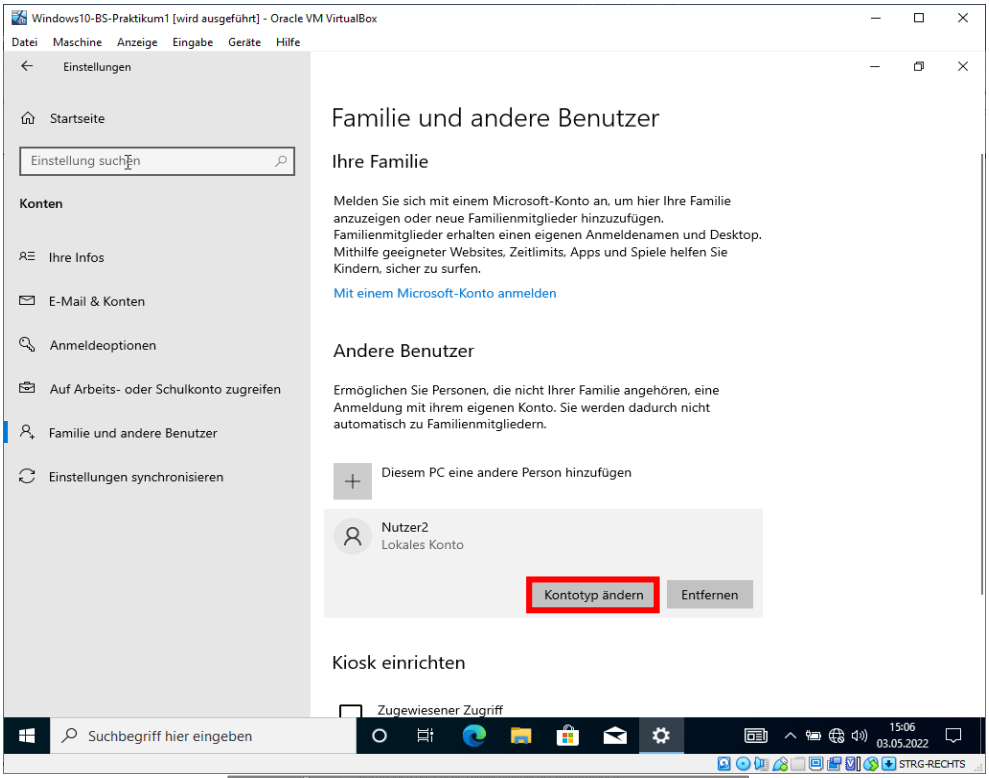


- Fügen Sie **Nutzer2** mit **Kennwort2** hinzu

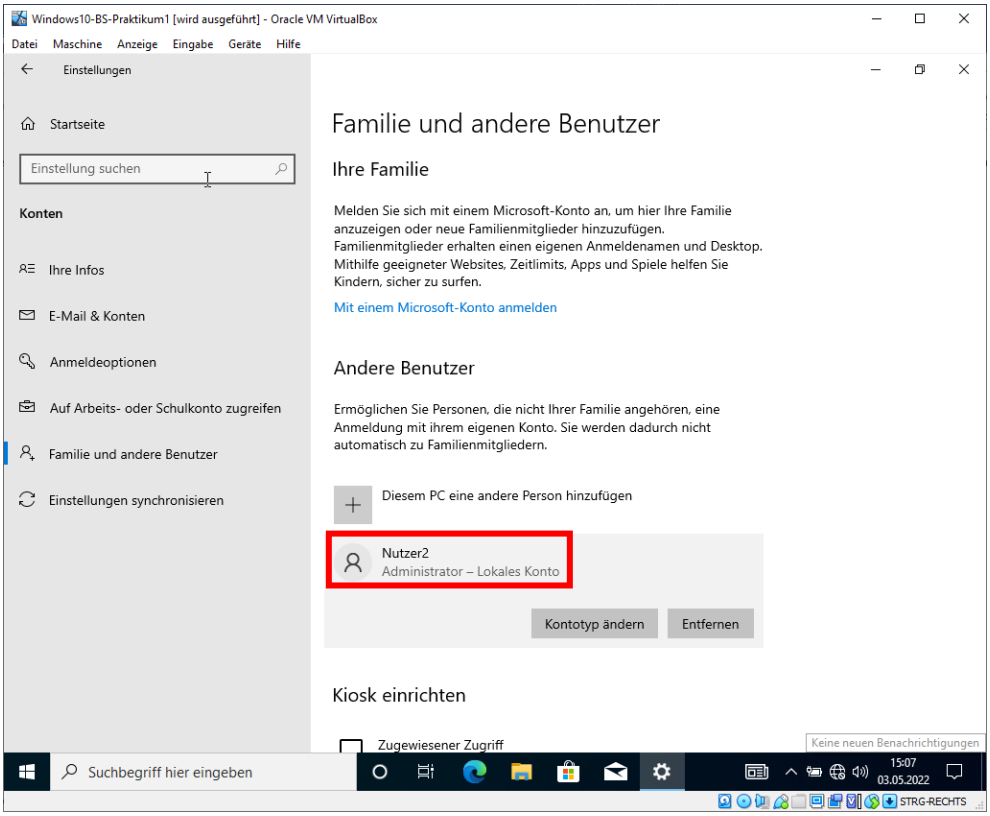


Ergebnis: - **lokales Standardkonto.**

➢ Wechseln Sie den Kontotyp in **Administrator**

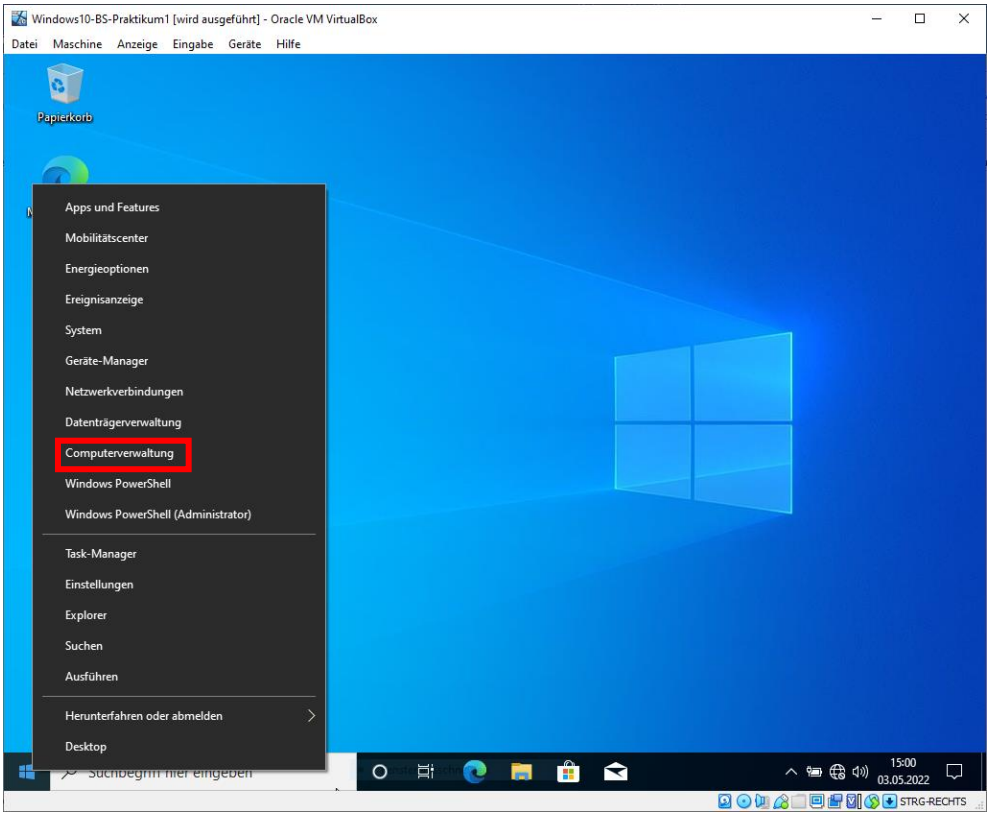


Ergebnis: – **lokales Administrator Konto.**

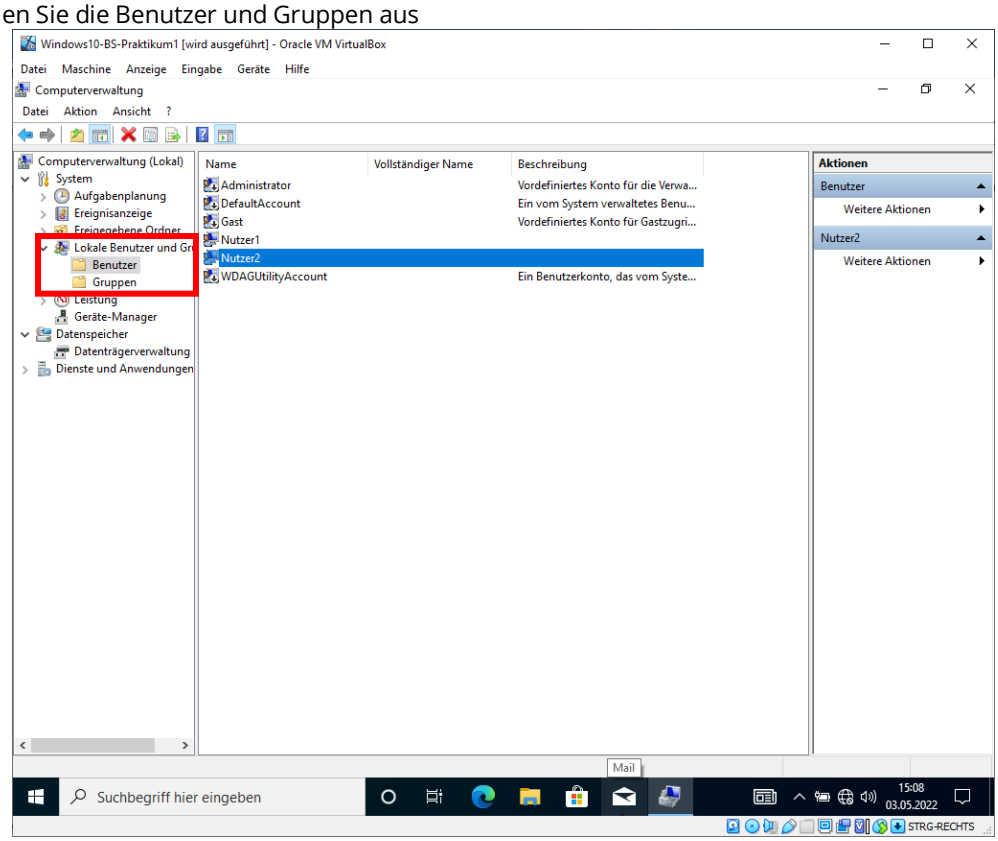


Benutzer mit MMC anlegen und überprüfen

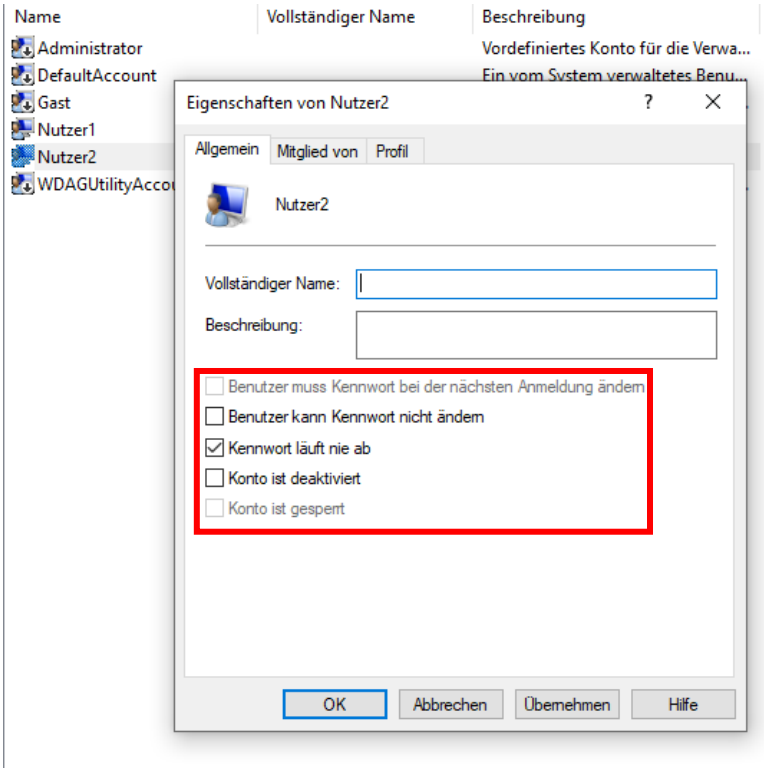
Öffnen Sie die Computerverwaltung (rechter Klick Windows Button) oder die MMC mit der Übersicht von PR1.



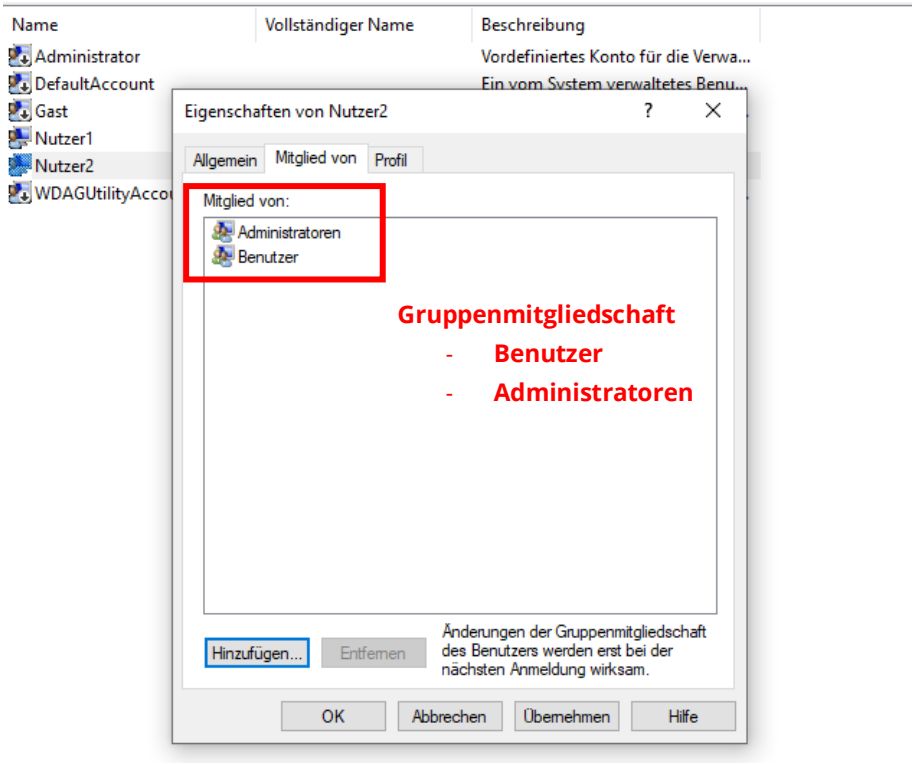
➢ Wählen Sie die Benutzer und Gruppen aus



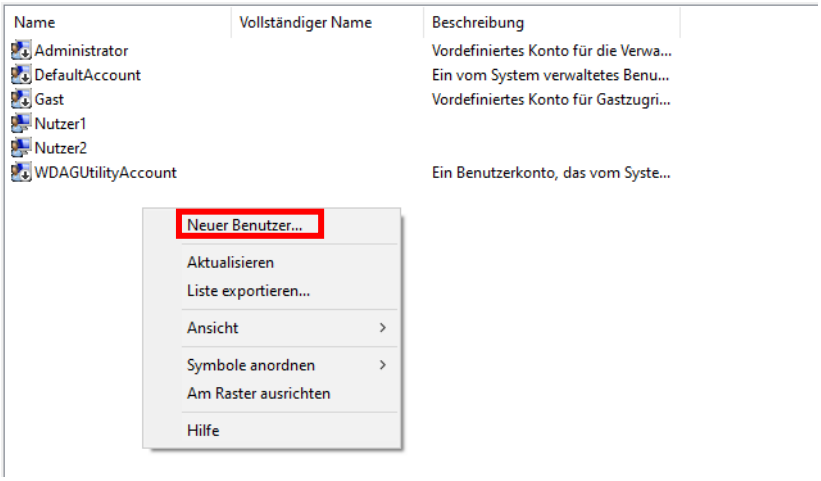
➢ Lassen Sie sich von **Nutzer2** die Einstellungen Anzeigen

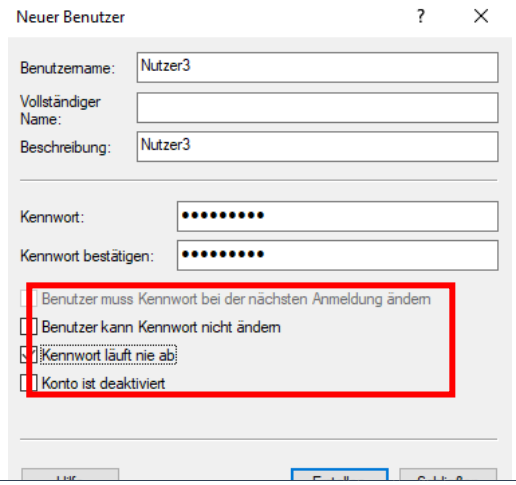


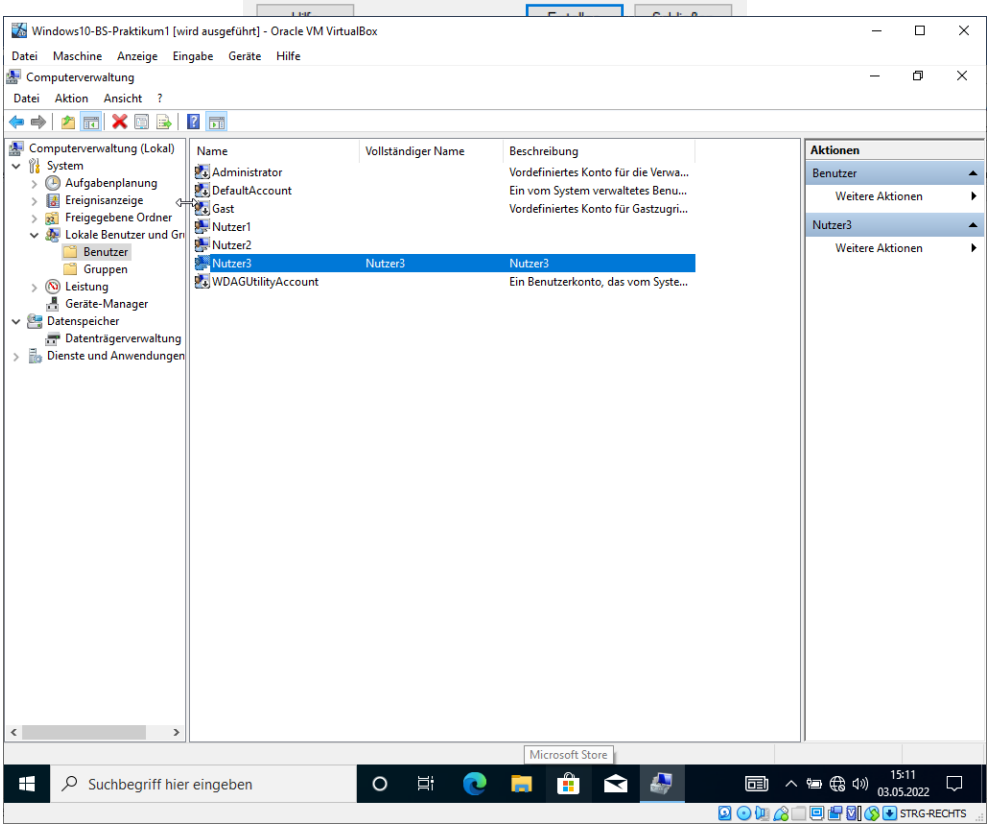
Standard wenn Benutzer aktiv



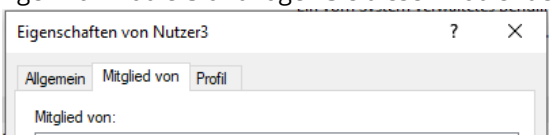
- Legen Sie einen neuen Benutzer **Nutzer3** mit **Kennwort3** an, sodass dessen Kennwort nicht neu gesetzt werden muss und nie abläuft

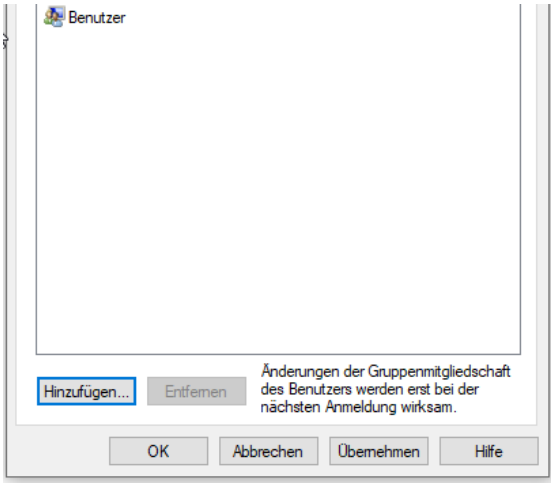


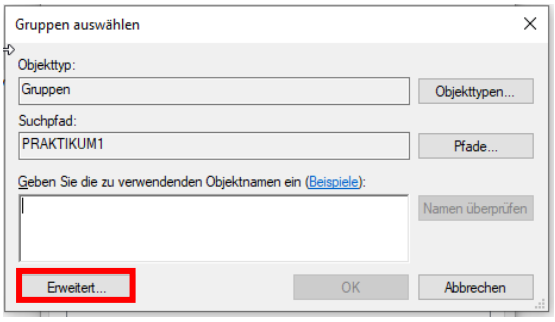


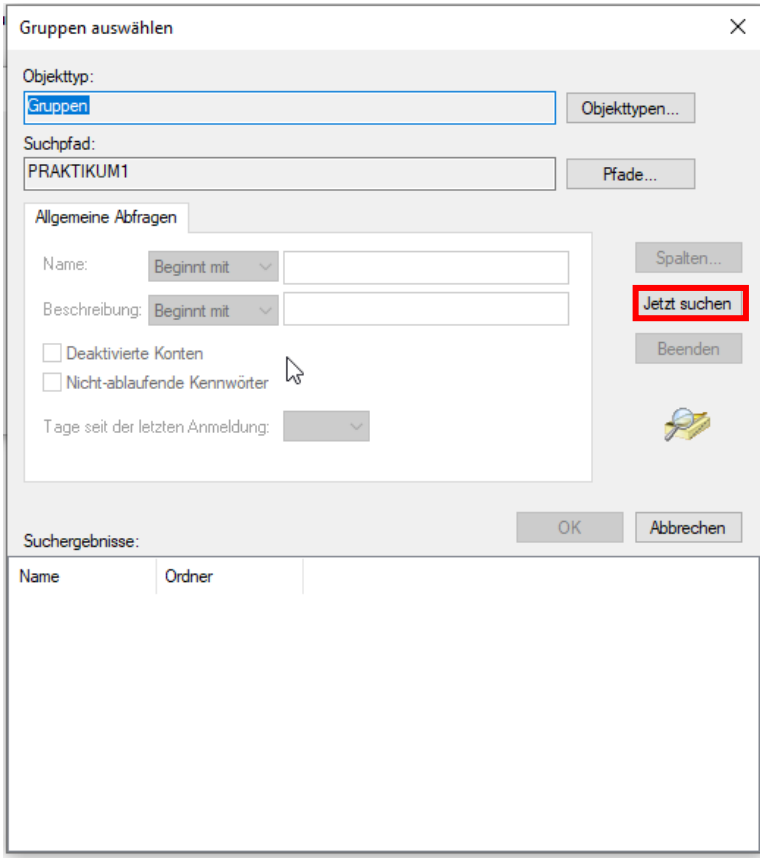


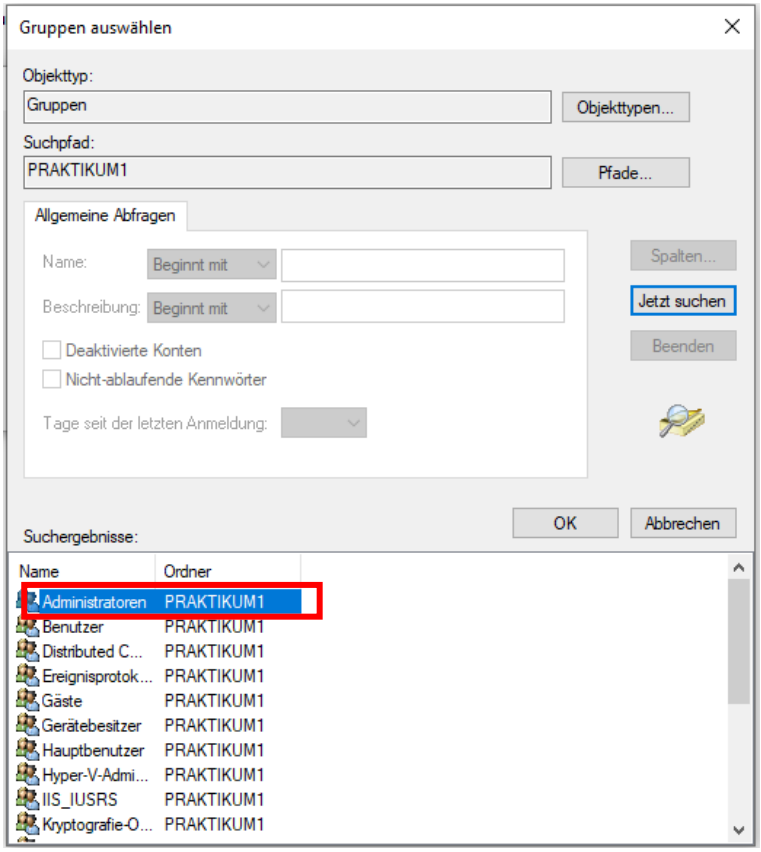
➢ Editieren Sie die Einstellungen von Nutzer3 und fügen Sie diesen Nutzer der Gruppe der Administratoren zu

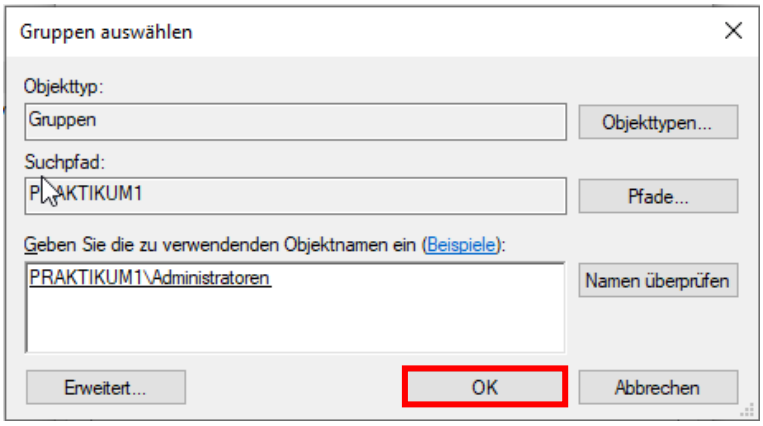


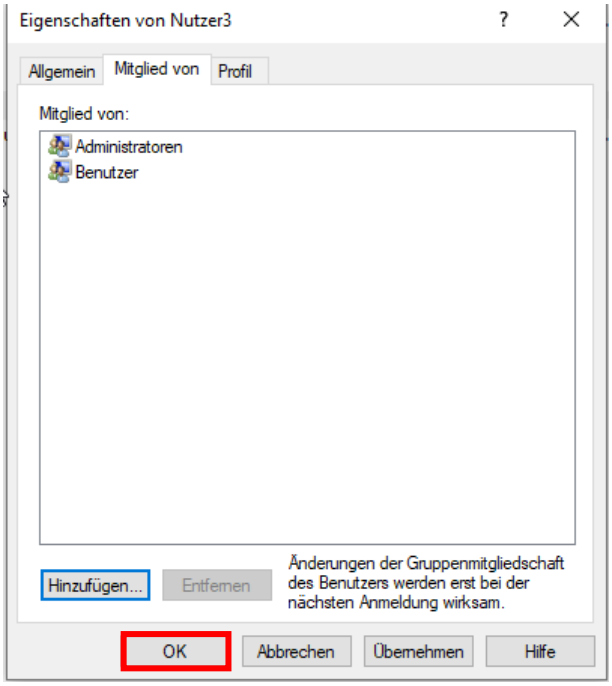

Benutzer
Hinzufügen...
Entfernen
Änderungen der Gruppenmitgliedschaft des Benutzers werden erst bei der nächsten Anmeldung wirksam.
OK
Abbrechen
Übernehmen
Hilfe


Gruppen auswählen
Objekttyp:
Gruppen
Objekttypen...
Suchpfad:
PRAKTIKUM1
Pfade...
Geben Sie die zu verwendenden Objektnamen ein (Beispiele):
Namen überprüfen
Erweitert...
OK
Abbrechen


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
OK
Abbrechen
Suchergebnisse:
Name
Ordner


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
OK
Abbrechen
Suchergebnisse:
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

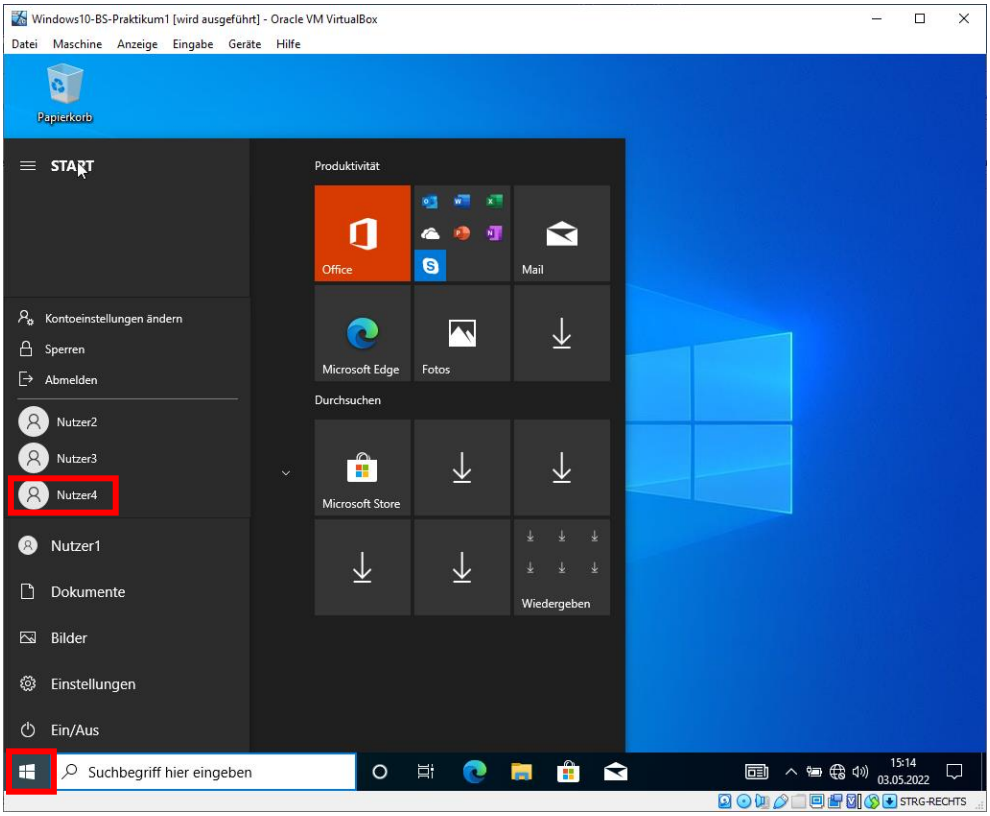

Gruppen auswählen
Objekttyp:
Gruppen
Objekttypen...
Suchpfad:
PRAKTIKUM1
Pfade...
Geben Sie die zu verwendenden Objektnamen ein (Beispiele):
PRAKTIKUM1\Administratoren
Namen überprüfen
Erweitert...
OK
Abbrechen



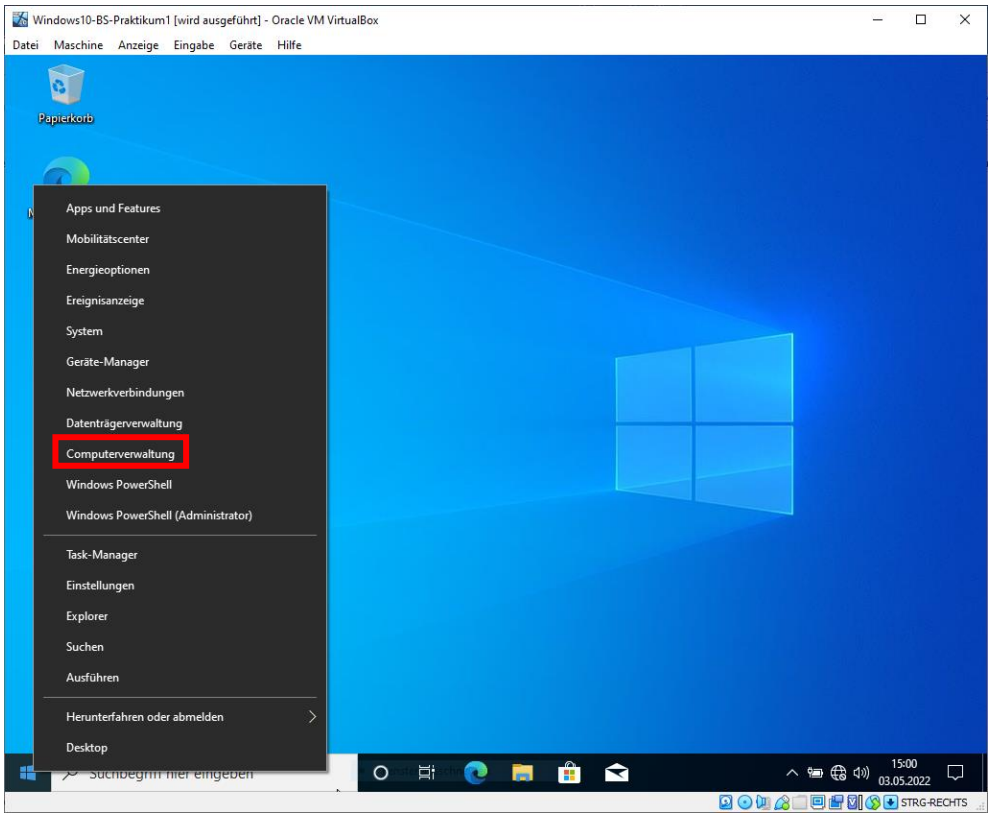
- Fügen Sie nach gleichem Schema selbständig **Nutzer4** mit **Kennwort4** hinzu aber **ohne Administratorrechte**

Nutzer An-, Um- und Abmeldungen

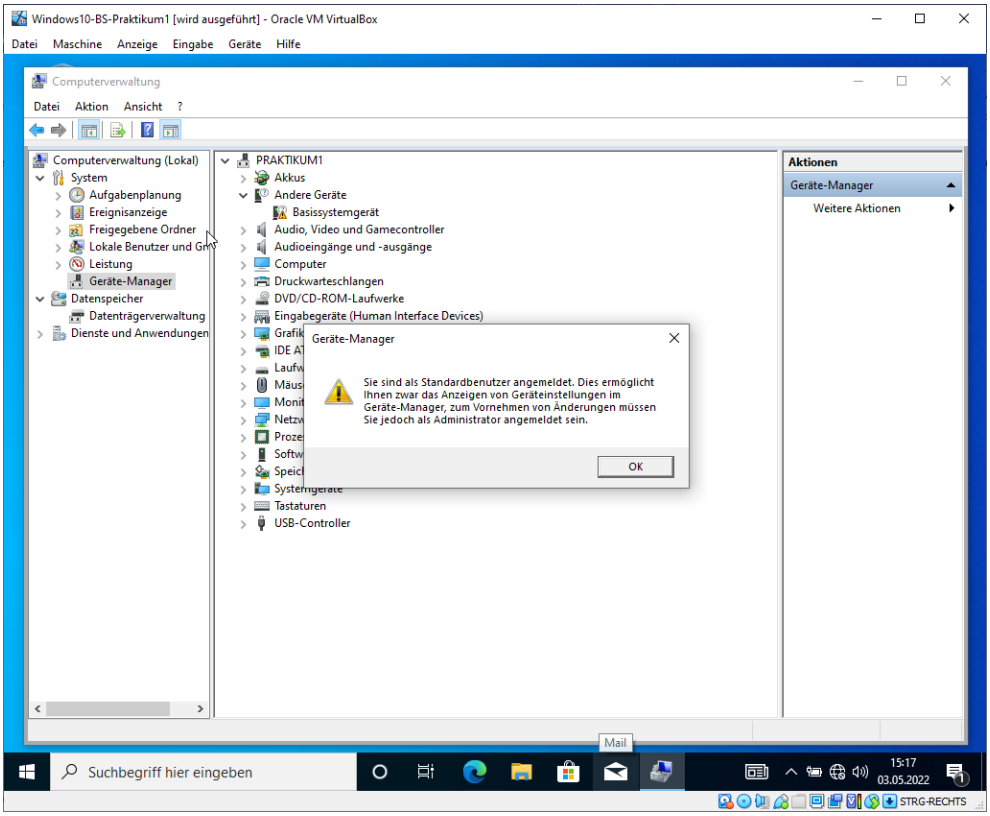
Melden Sie sich als Nutzer 4 zusätzlich am System an.



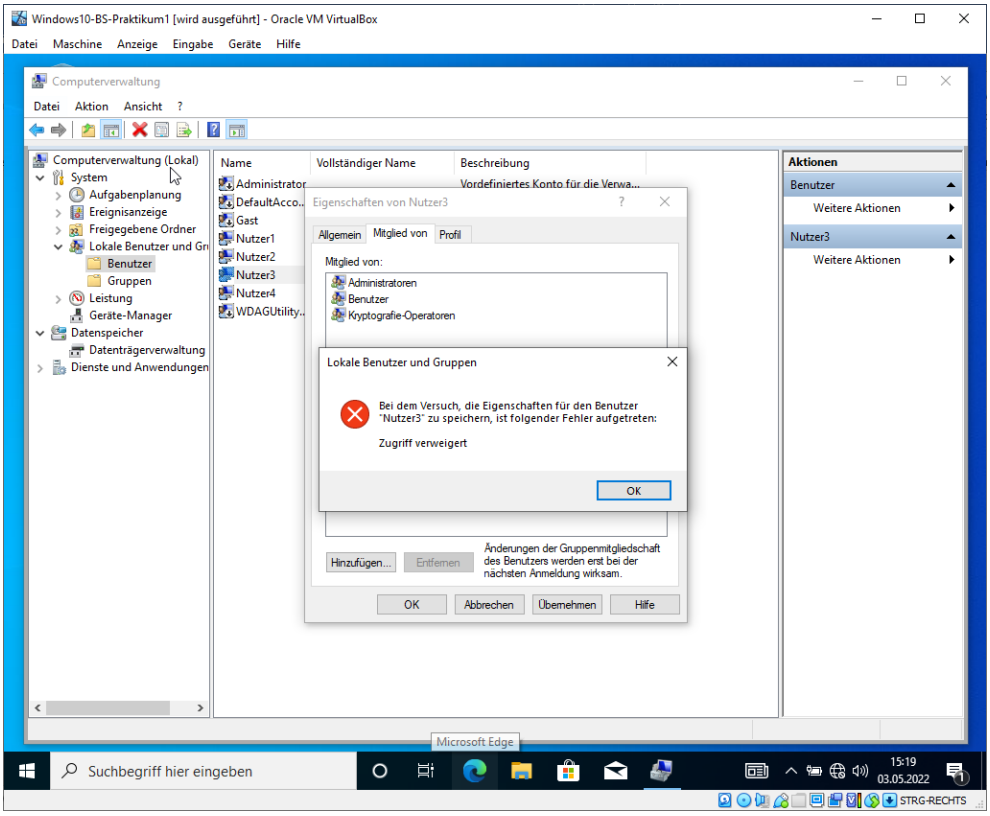
- Starten Sie die Computerverwaltung



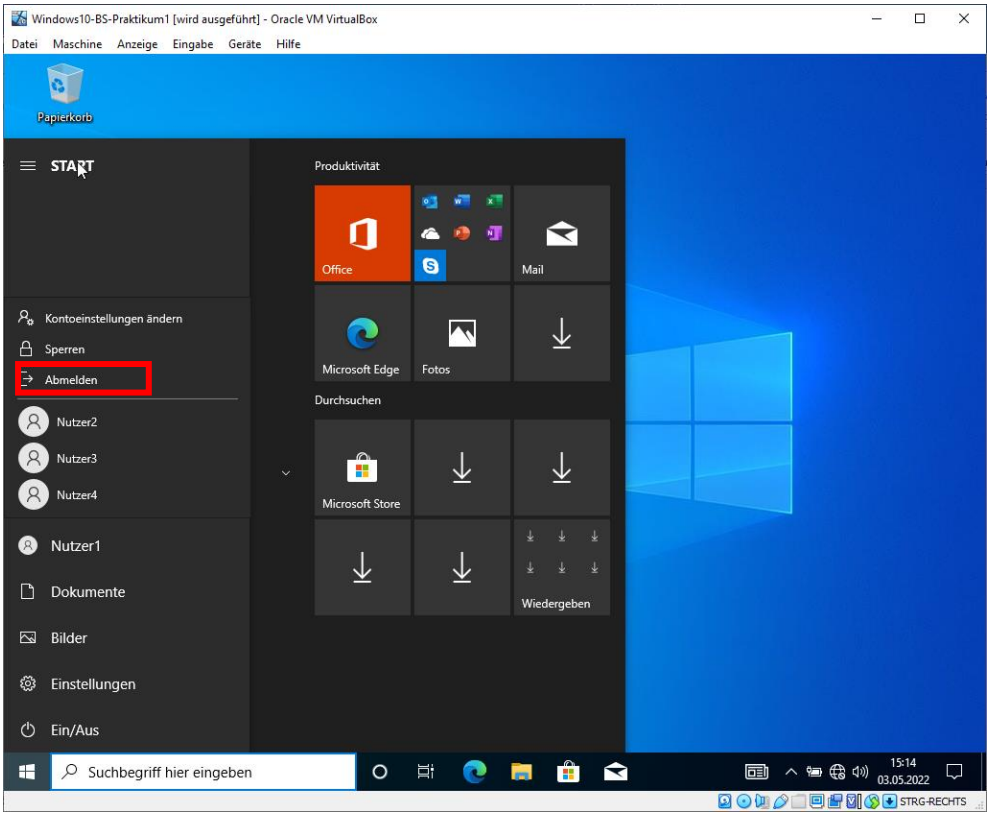
- Überprüfen Sie, ob Sie den Gerätemanager öffnen können



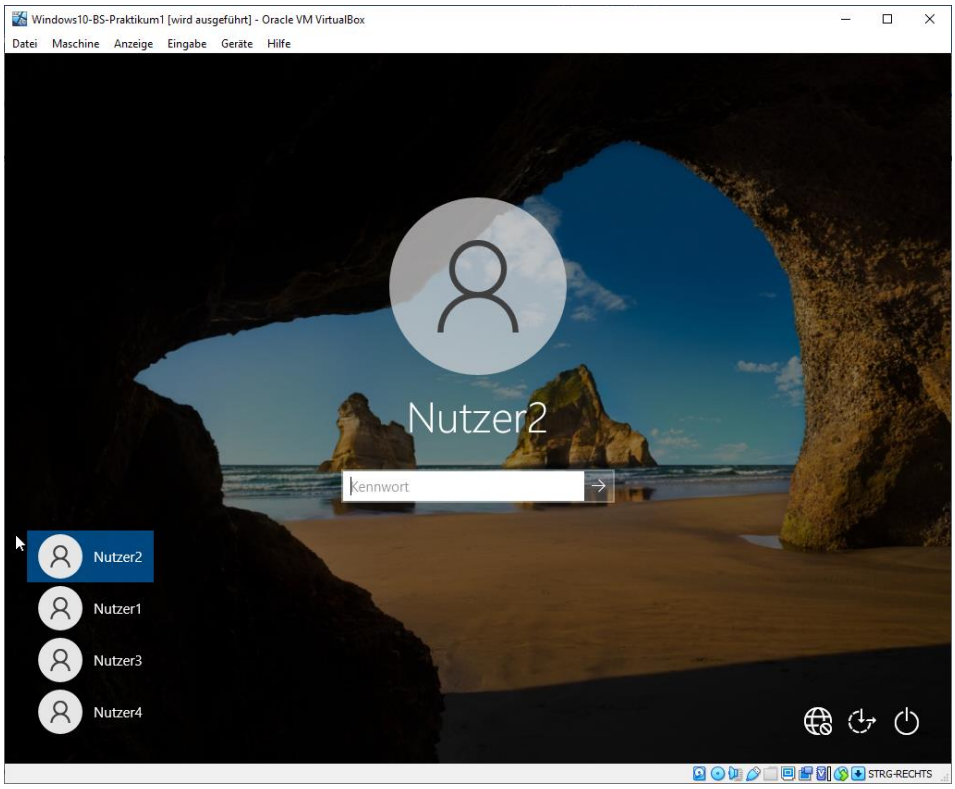
- Überprüfen Sie, ob Sie von Nutzer3 die Gruppenzugehörigkeiten erweitern können



Melden Sie Nutzer4 ab.

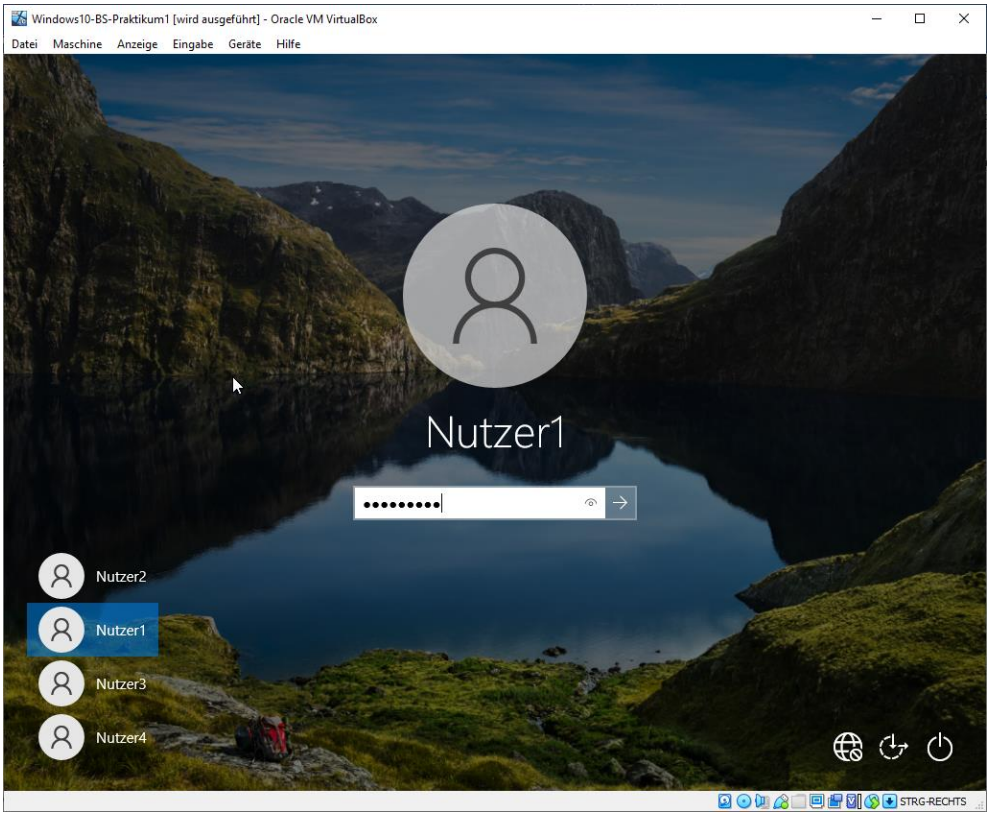


Melden Sie sich als Nutzer2 an.

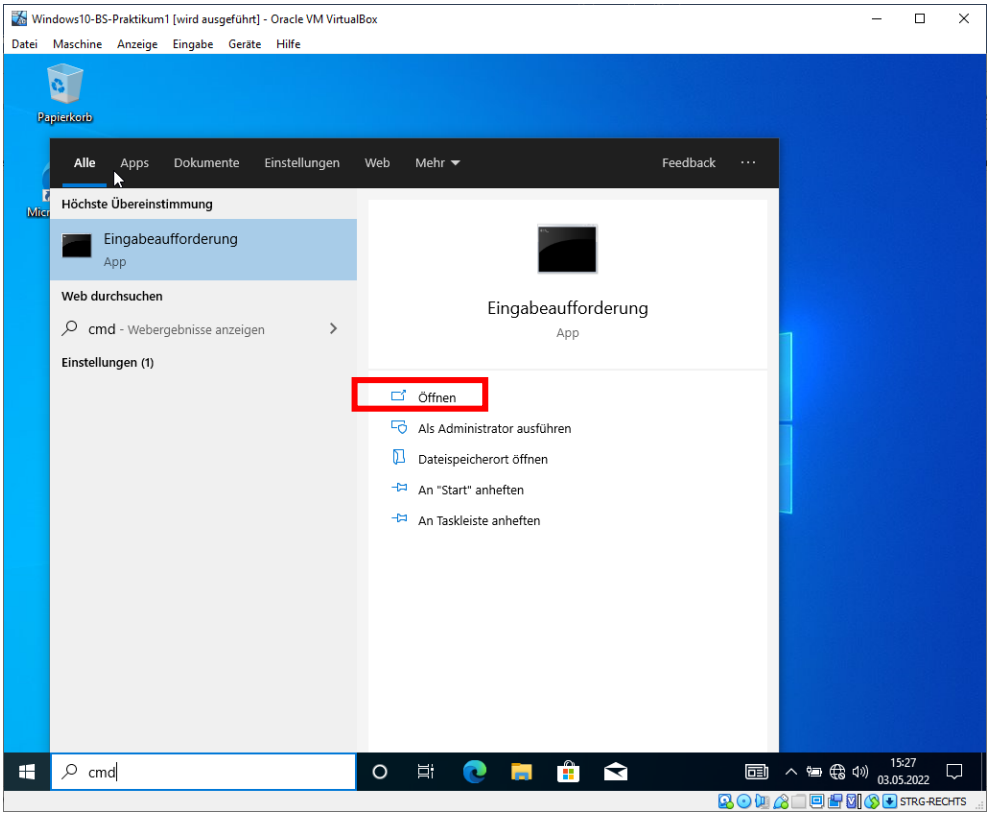


Melden Sie sich als Nutzer2 ab.

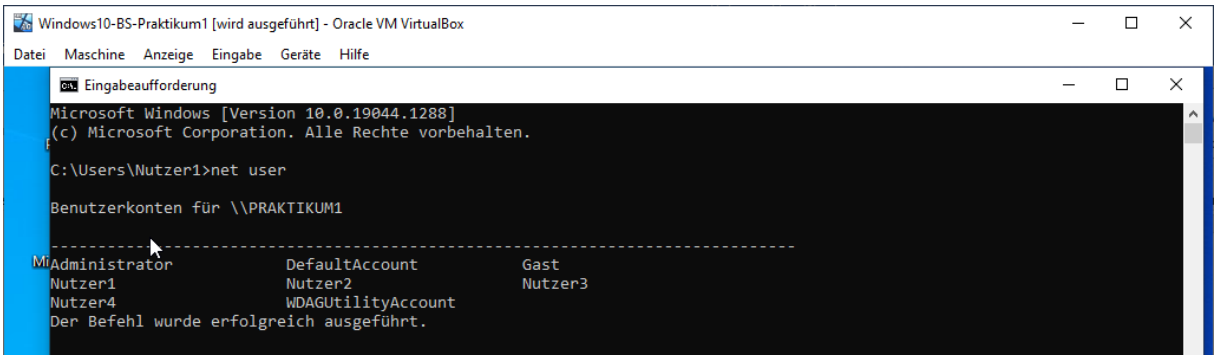
Melden Sie sich als Nutzer1 wieder an.



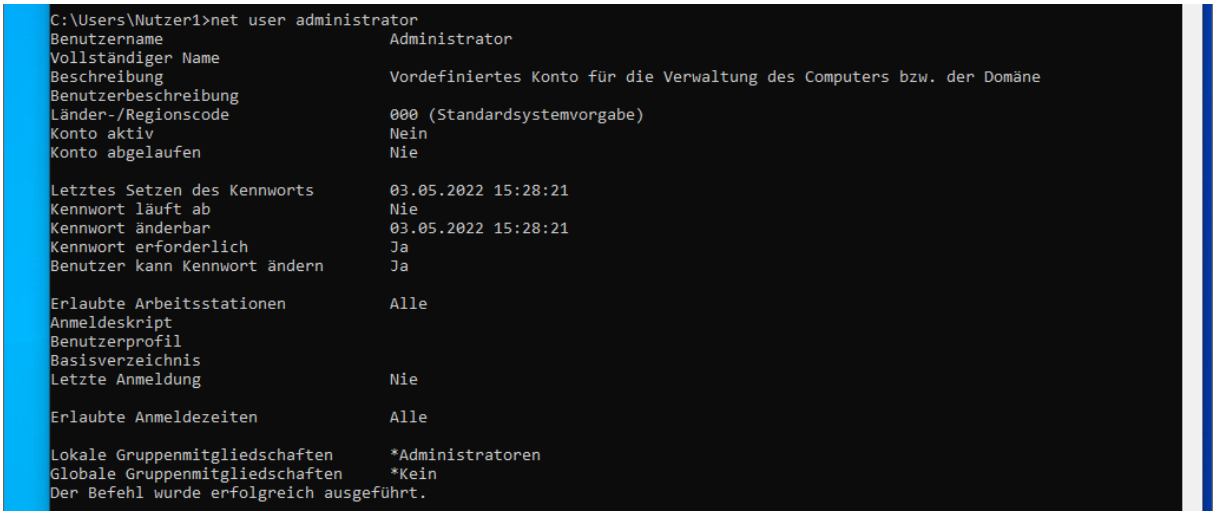
➢ Öffnen Sie eine **Kommandozeile** durch Eingabe von **CMD** nach dem Klick auf den Windows Start Button



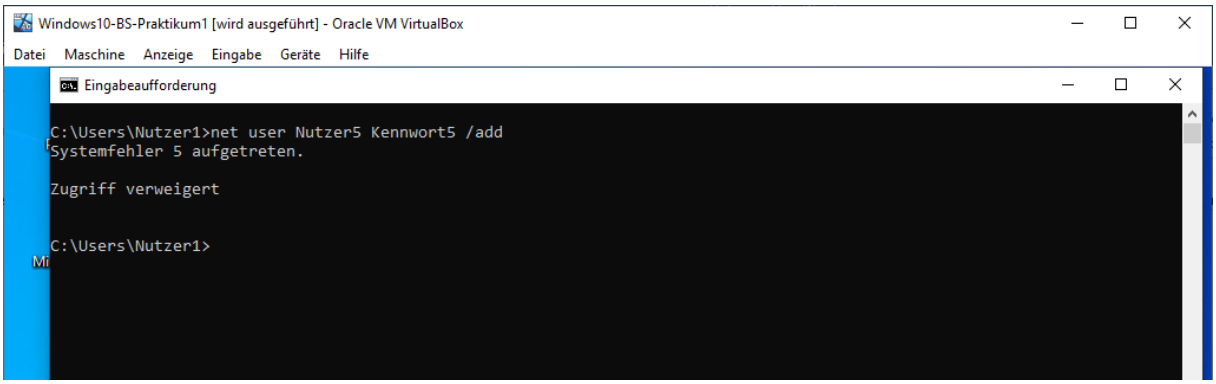
- Geben Sie den Befehl **net user** im Kommandozeilen Fenster ein, um eine Übersicht der Benutzeraccounts zu erhalten



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

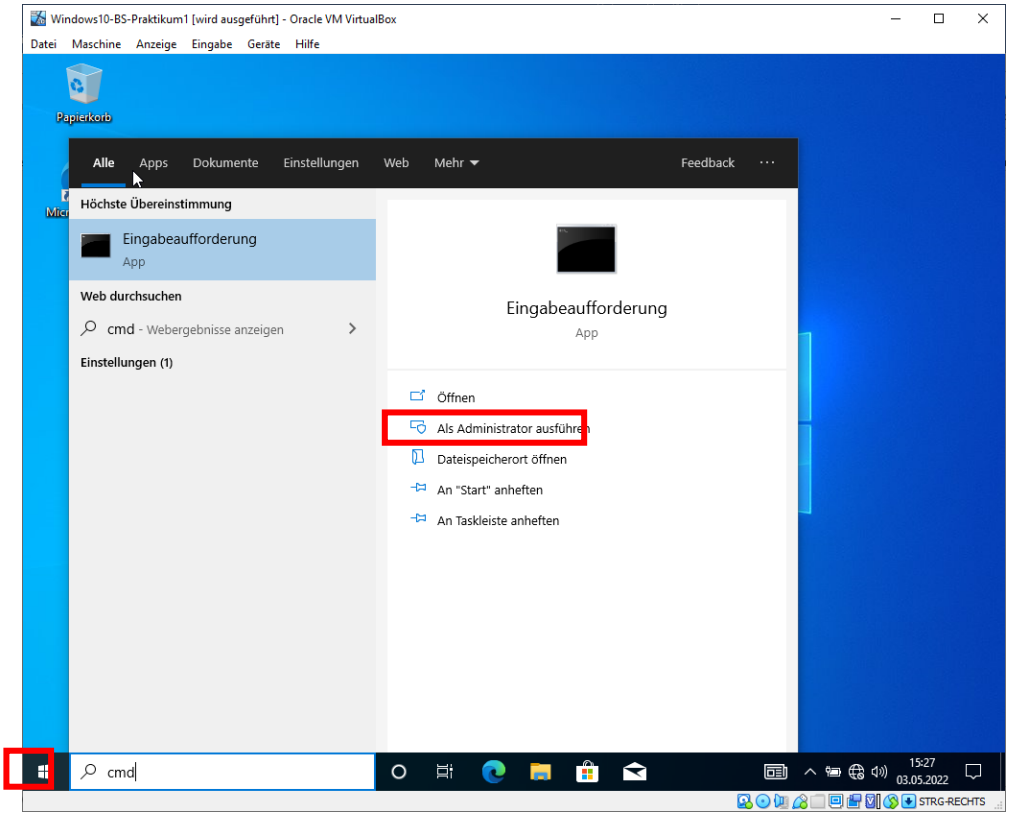


- Jetzt versuchen Sie Benutzer5 mit Kennwort5 per Kommandozeilen Befehl **net user Nutzer5 Kennwort5 /add** hinzuzufügen



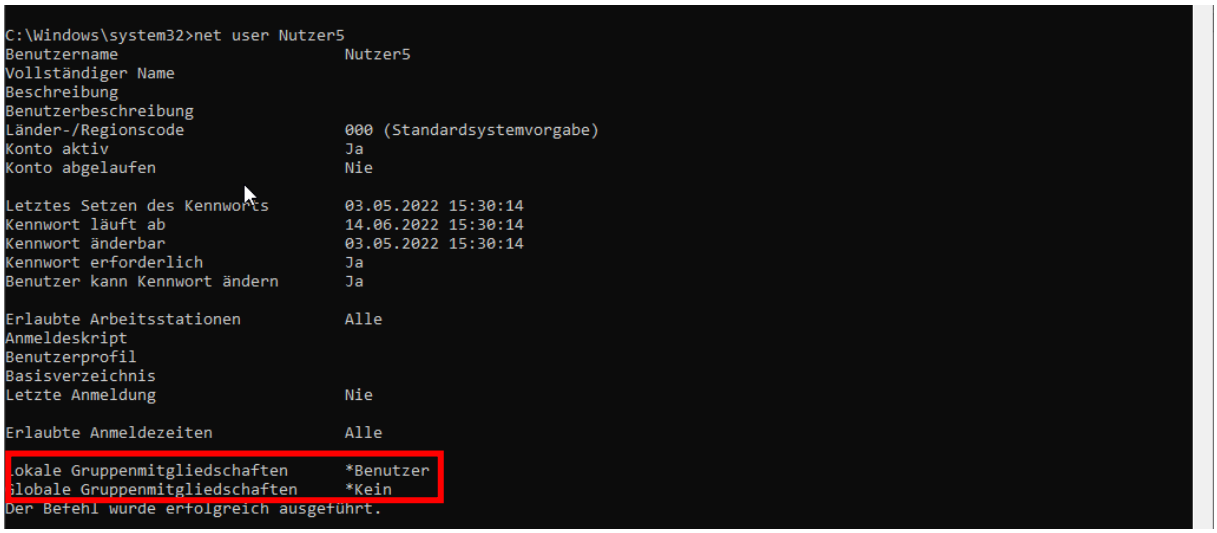
- Dies scheitert wegen fehlender Administratorenrechte in der Kommandozeile!

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



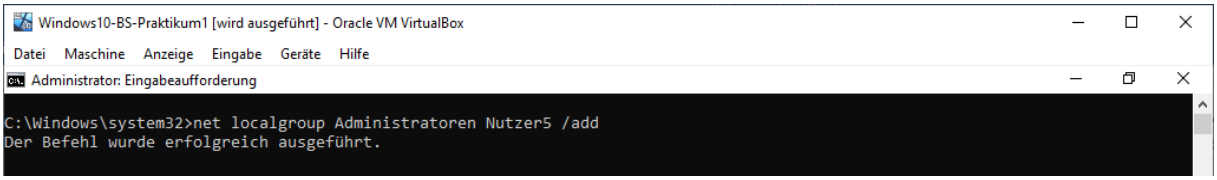
- Jetzt versuchen Sie Benutzer5 mit Kennwort5 per Kommandozeilen Befehl **net user Nutzer5 Kennwort5 /add** hinzuzufügen

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

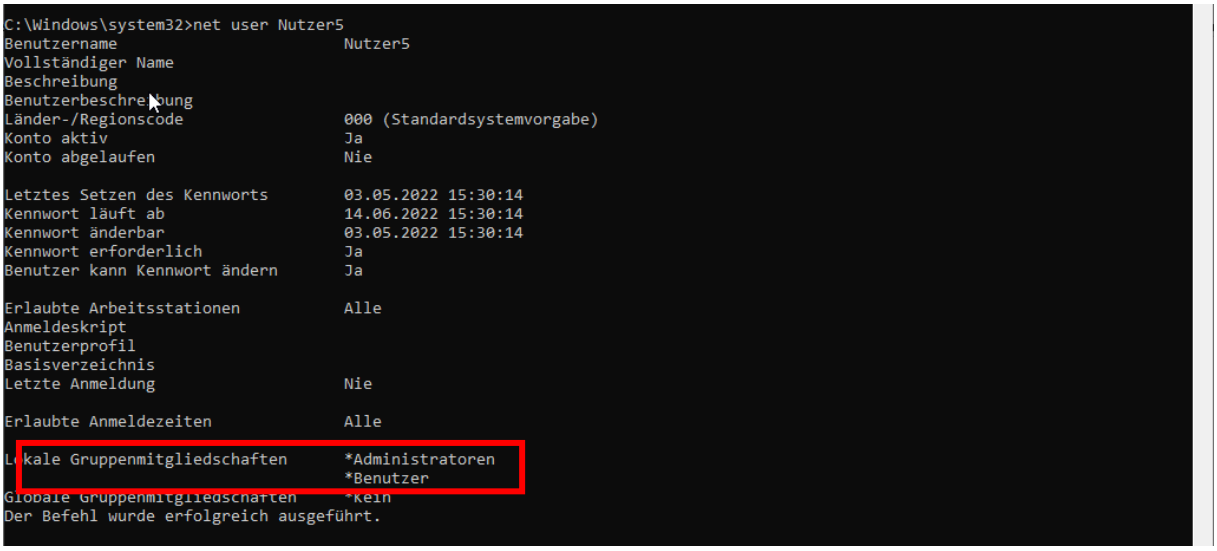


- Der Nutzer ist derzeit nur normaler Benutzer

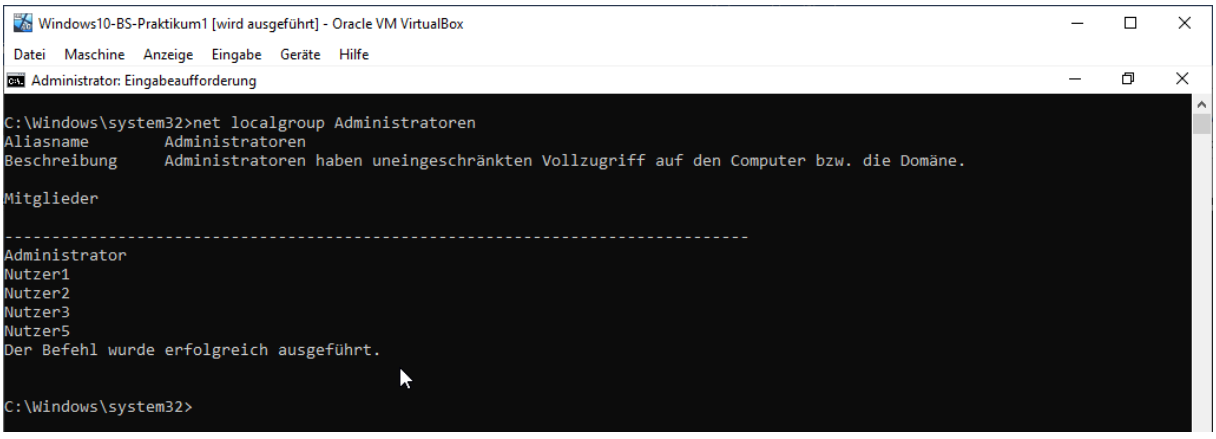
- Nehmen Sie den Nutzer5 in die Gruppe der Administratoren mit dem Kommandozeilen Befehl **net localgroup Administratoren Nutzer5 /add** auf



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



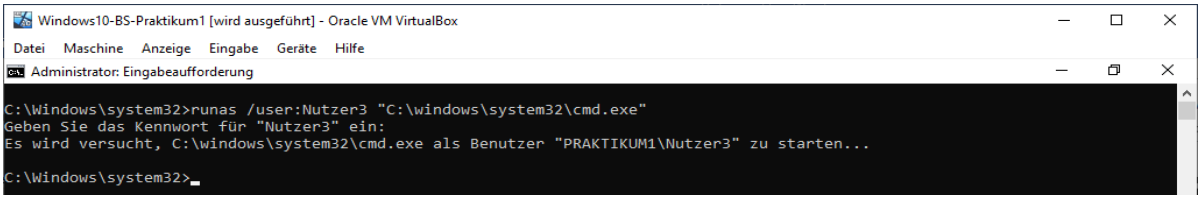
- Lassen Sie sich alle Benutzer der Gruppe **Administratoren** mit dem Kommandozeilen Befehl **net localgroup Administratoren** Anzeigen



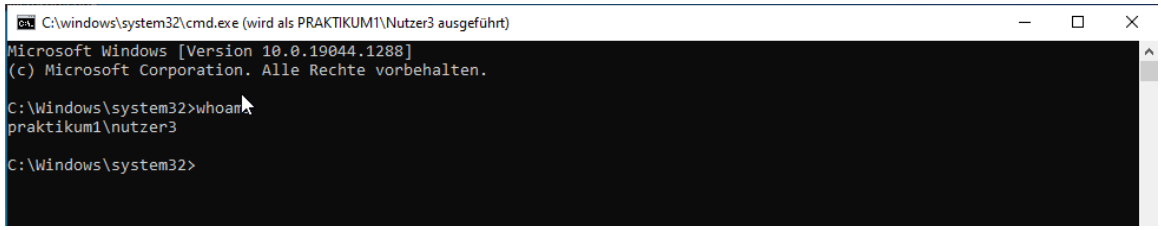
Benutzeraccount innerhalb eines anderen Accounts nutzen

Öffnen Sie im Nutzer1 eine Kommandozeile mit administrativen Berechtigungen.

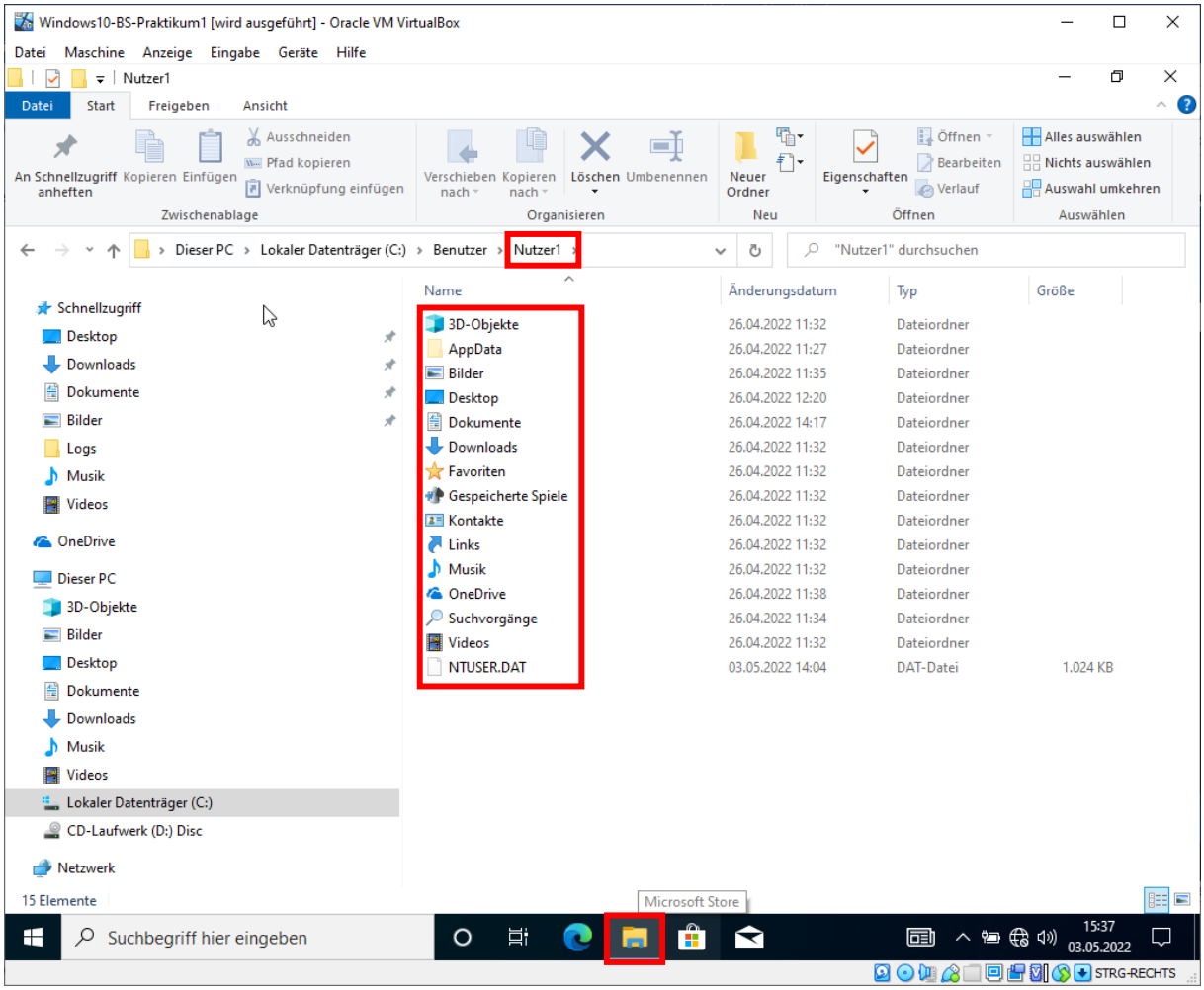
- Geben Sie den Kommandozeilen Befehl **runas /user:Nutzer3 „C:\windows\system32\cmd.exe“** ein



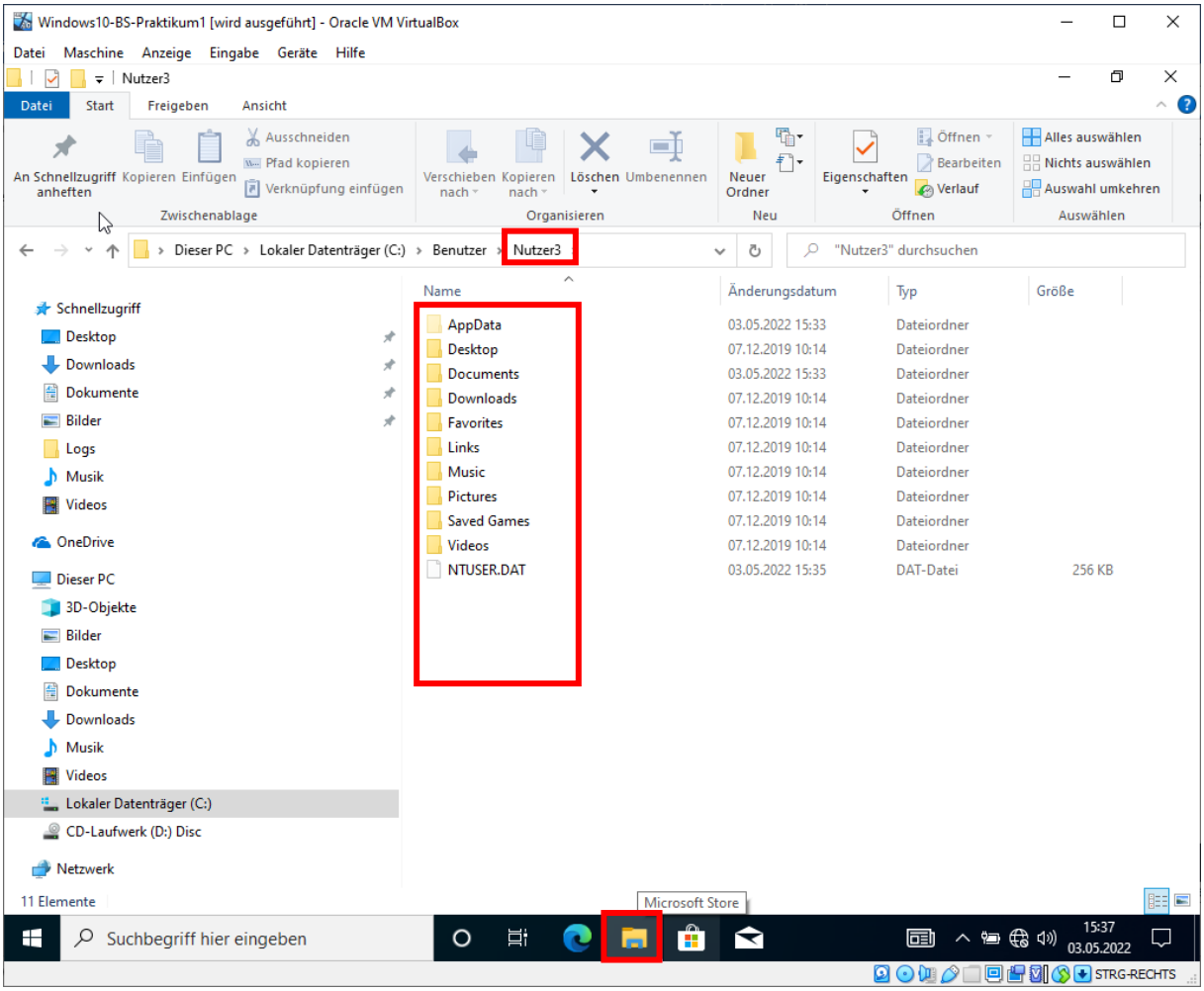
- Nach Eingabe des Kennworts erhalten Sie ein Kommandozeilenfenster von Nutzer3
- Überprüfen sie mit dem Kommandozeilen Befehl **whoami** ob dies eine Kommandozeile von **Nutzer3** ist



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

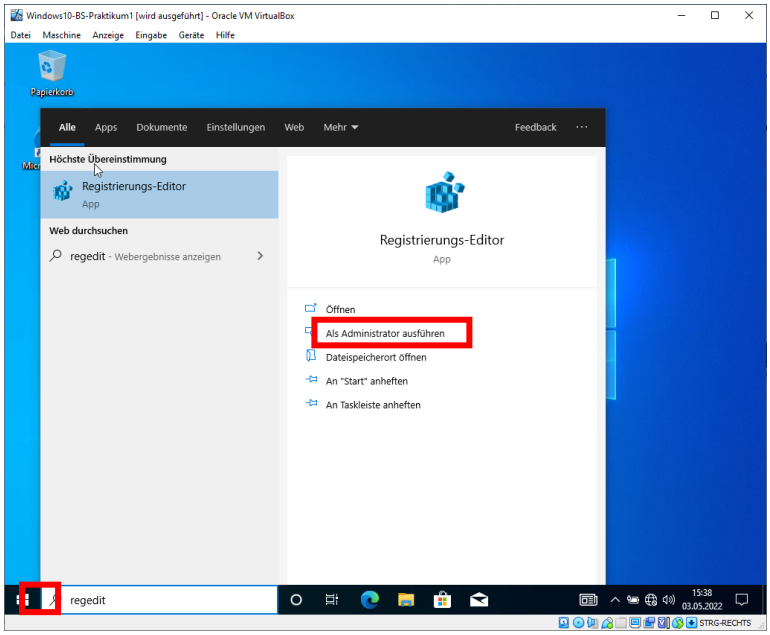


- Fällt Ihnen der Unterschied auf?

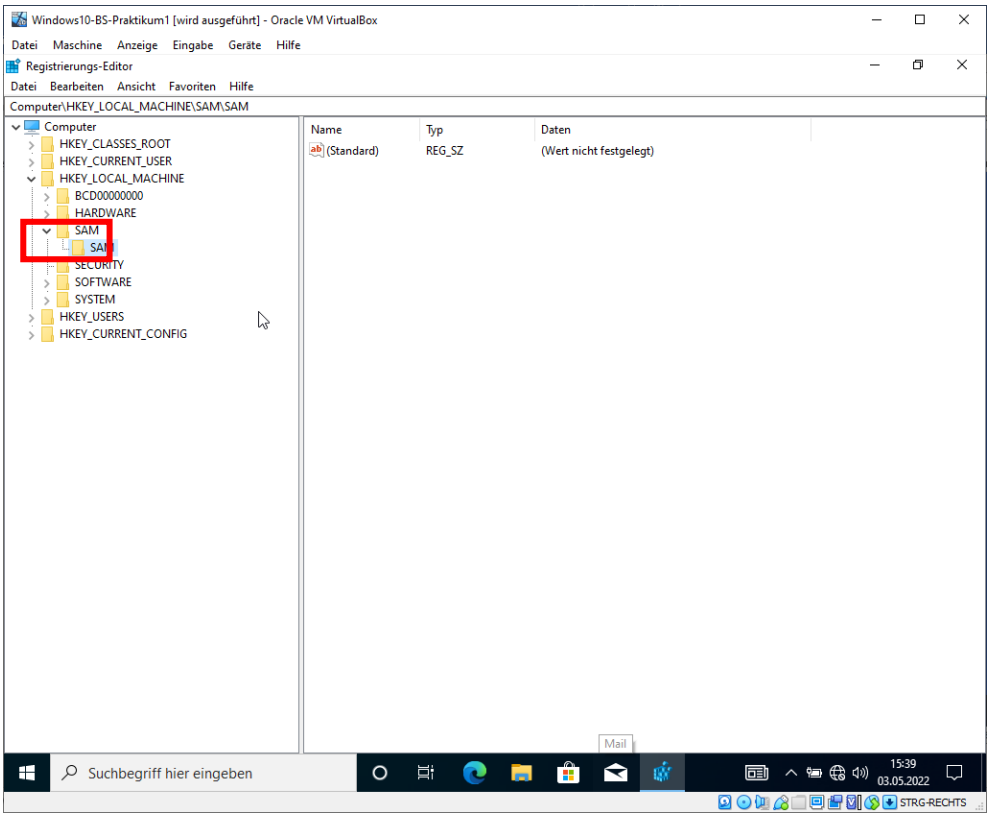


Überprüfung von Account Informationen in der Registry

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

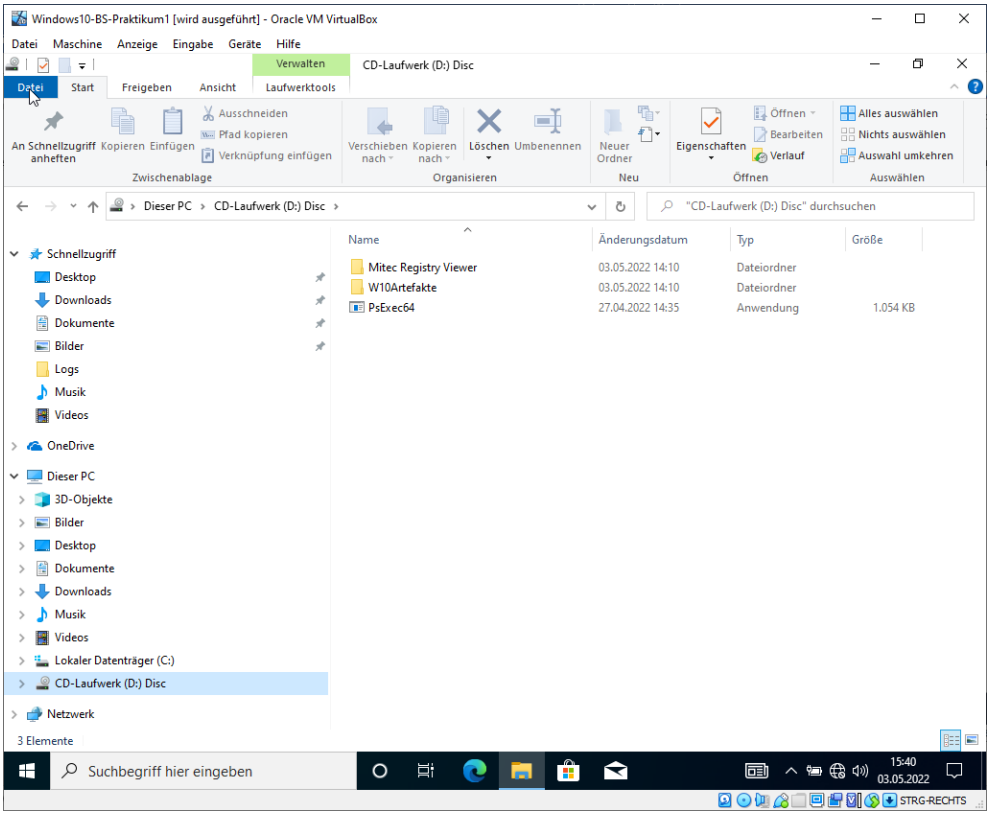


➢ Können Sie den Schlüssel der SAM-Datei öffnen?

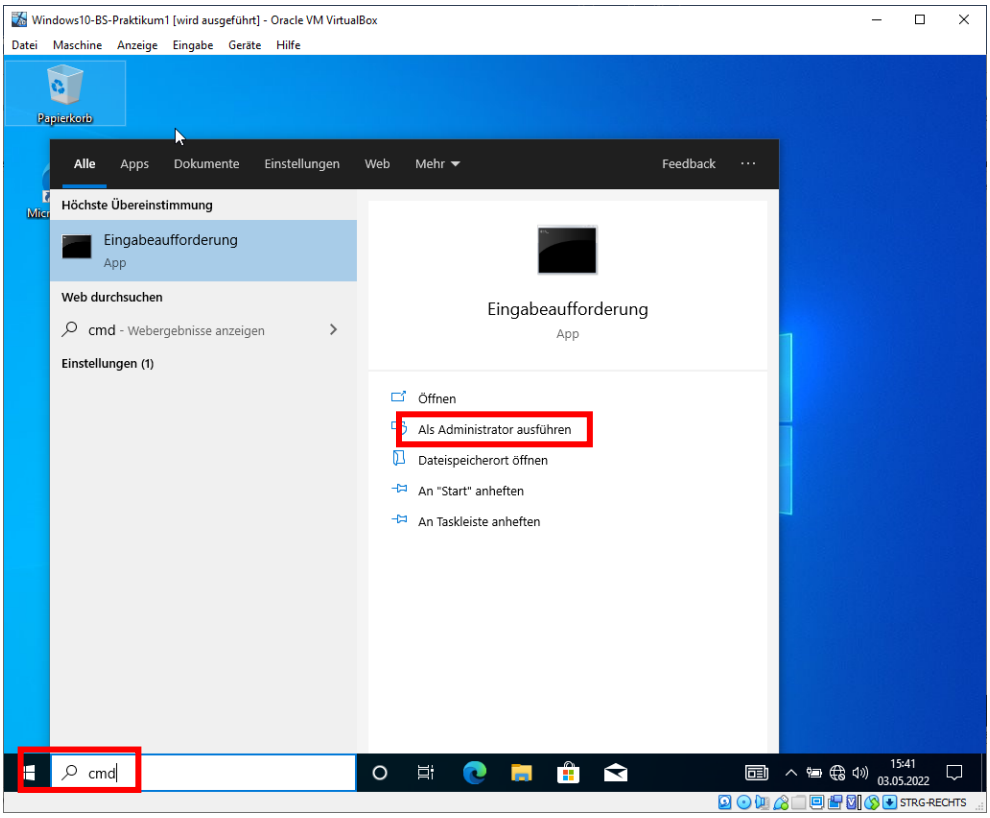


Nein, Ihnen fehlen Zugriffsrechte trotz Administrator!

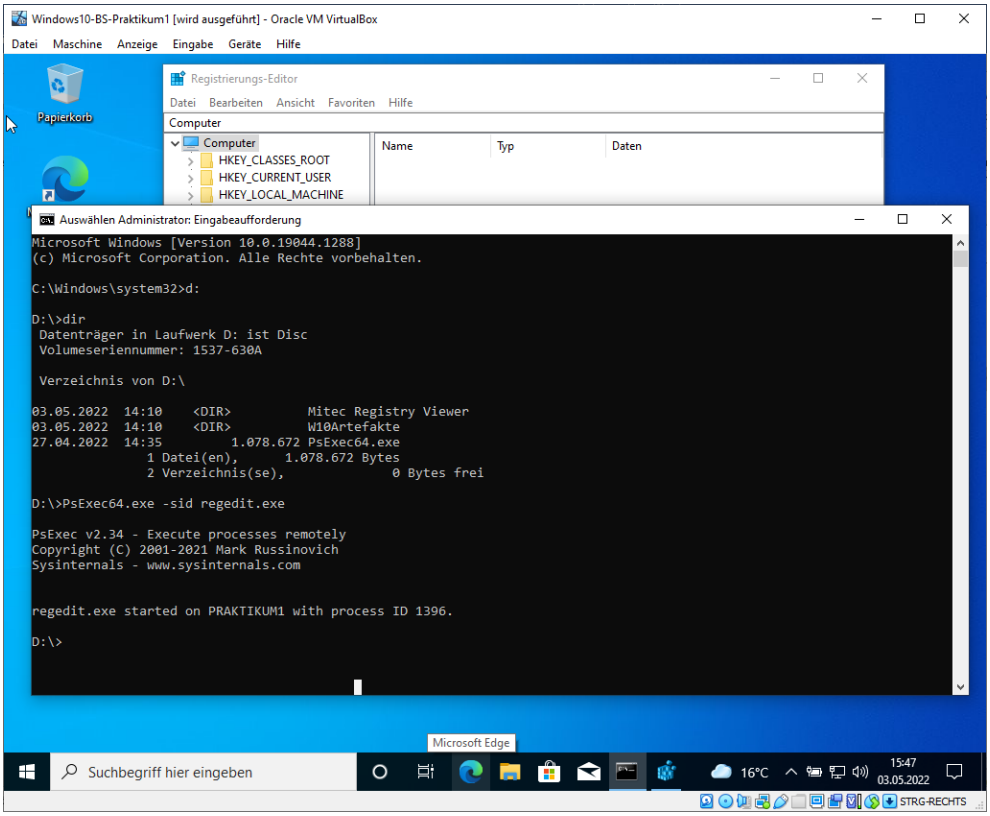
Überprüfen Sie ob die PR2.iso korrekt eingebunden ist und öffnen Sie diese im Windows Explorer.



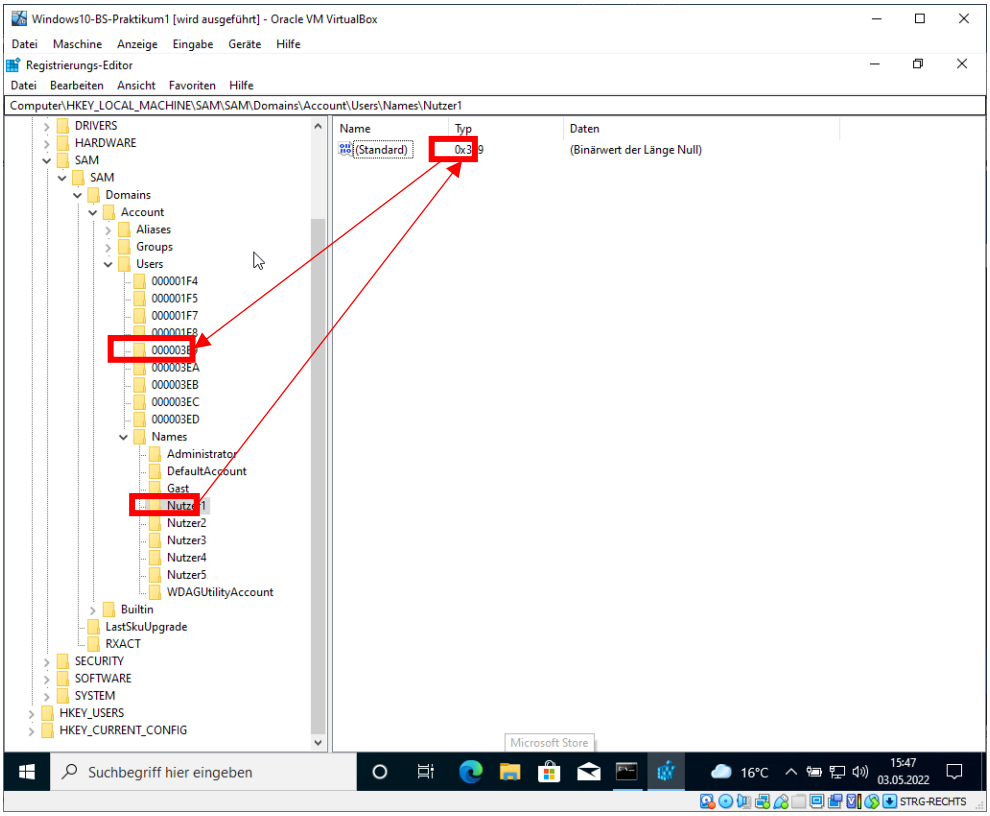
- Starten Sie ein Kommandozeilenfenster mit Administrativen Berechtigungen



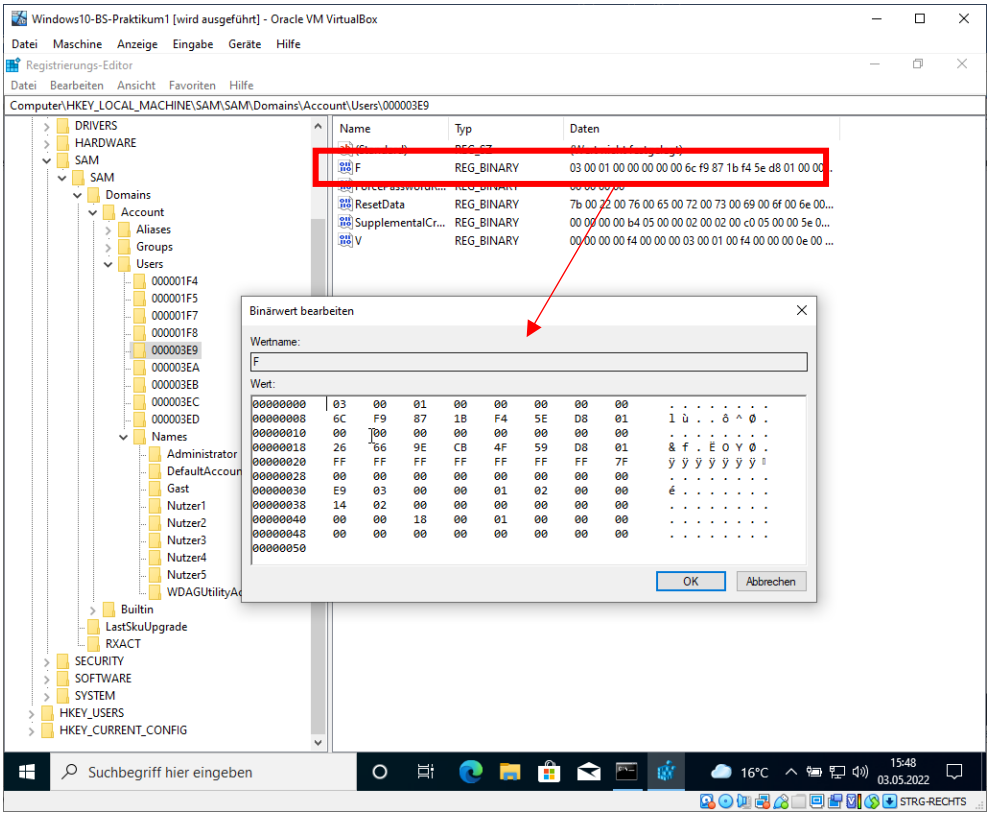
- Wechseln Sie im Kommandozeilenfenster auf den CD-Laufwerksbuchstaben (D:\)
- Schauen Sie ob die Dateien vorhanden sind mit dem **dir** Befehl
- Starten Sie den Registrierungseditor mit SYSTEM Rechten durch Aufruf von **PSEXEC64.exe –sid regedit.exe**
  (hierfür benötigt die von Sysinternals stammende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



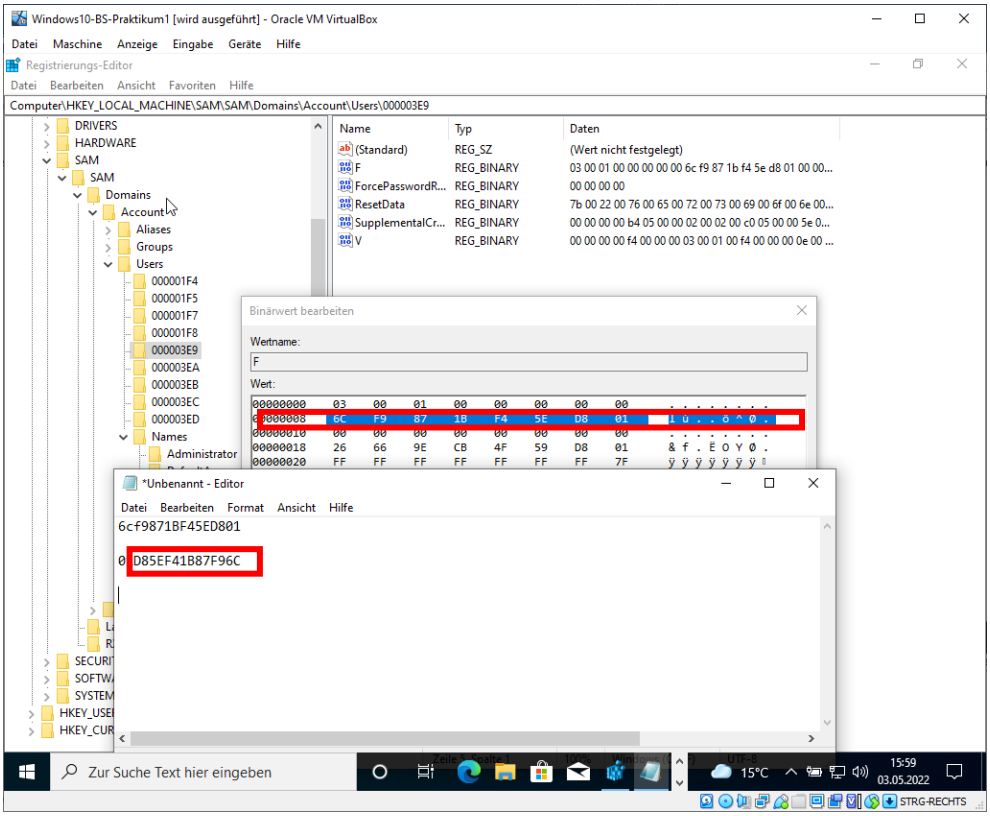
Als Ergebnis sehen Sie jetzt im Registrierungseditor die SAM-Eintragungen.



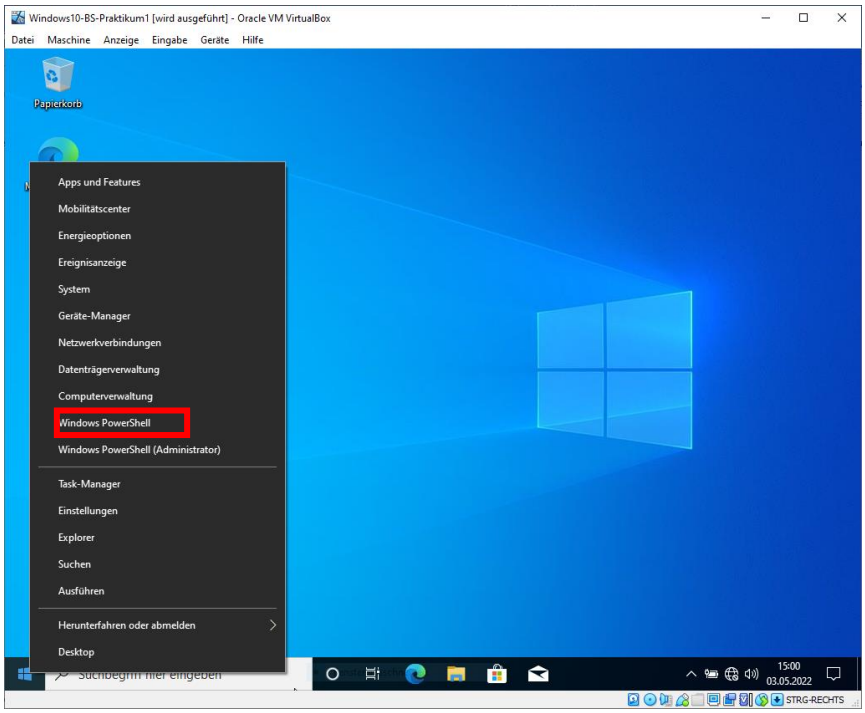
➢ Öffnen Sie im Schlüssel **00003E9** den Wert **F**



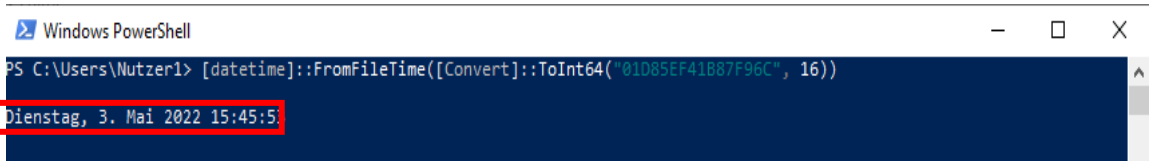
- Öffnen Sie sich den Editor (Notepad) und notieren Sie sich das Byte 0x08 – 0x0F in umgekehrter Reihenfolge (Little Endian!), dieser Wert repräsentiert den Zeitpunkt der letzten Anmeldung als 64Bit Filetime ab 01.01.1601 in ns



Öffnen Sie die Power Shell über den Windows Start Button mit Rechts Klick.



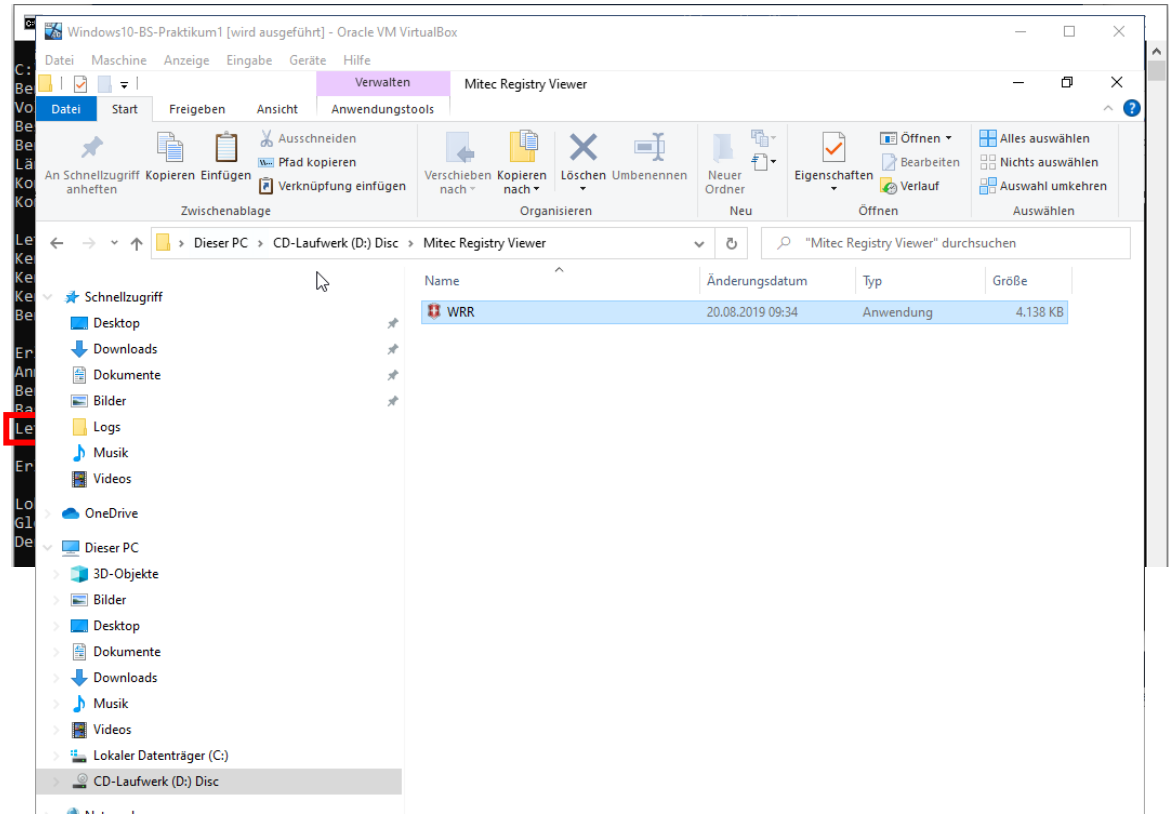
- Geben Sie im Powershell Fenster folgenden Befehl mit Ihrem Zeitstempel ein **[datetime]::FromFileTime([Convert]::ToInt64("01D85EF41B87F96C", 16))**



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

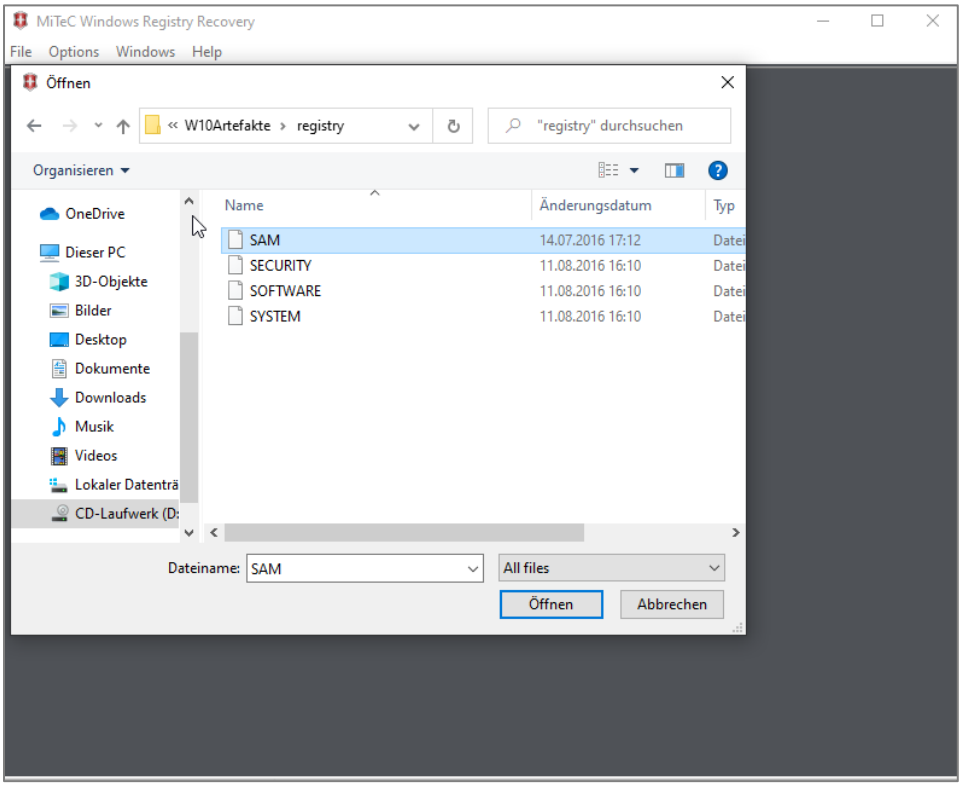
Nutzung externer Tools zur Registry Analyse der SAM

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

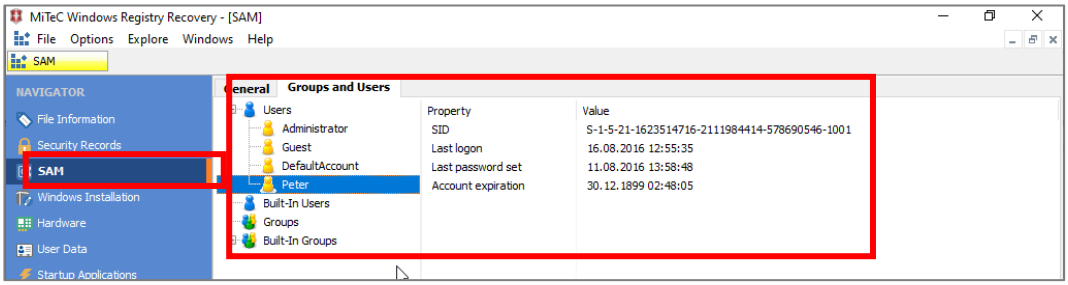


Hier haben Sie die Möglichkeit Registrierungsdatenbankdateien zu öffnen. Die lokale Registry kann auf Grund des laufenden Systemzustandes nicht geöffnet werden!

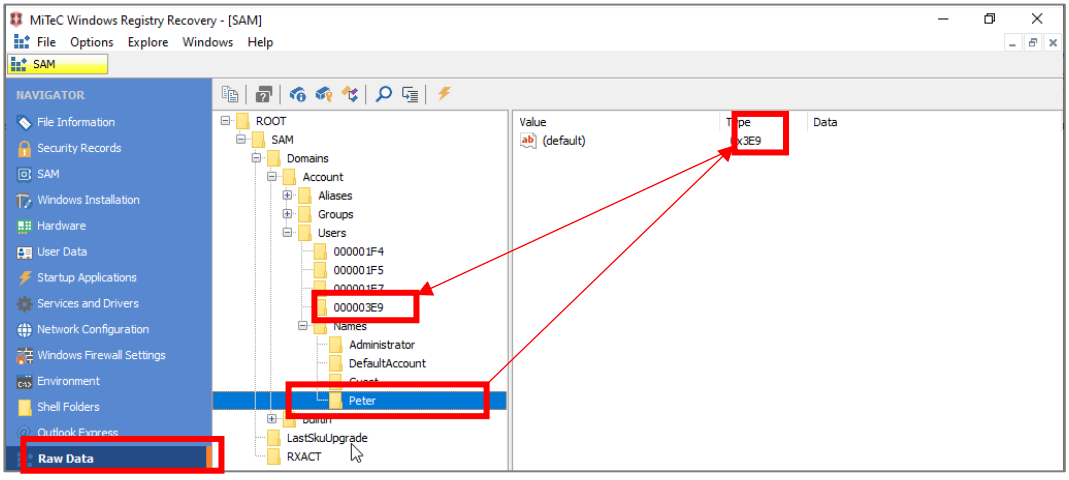
- Öffnen Sie die auf der CD befindliche **SAM**-Datenbank im Verzeichnis **\W10Artefakte\registry**

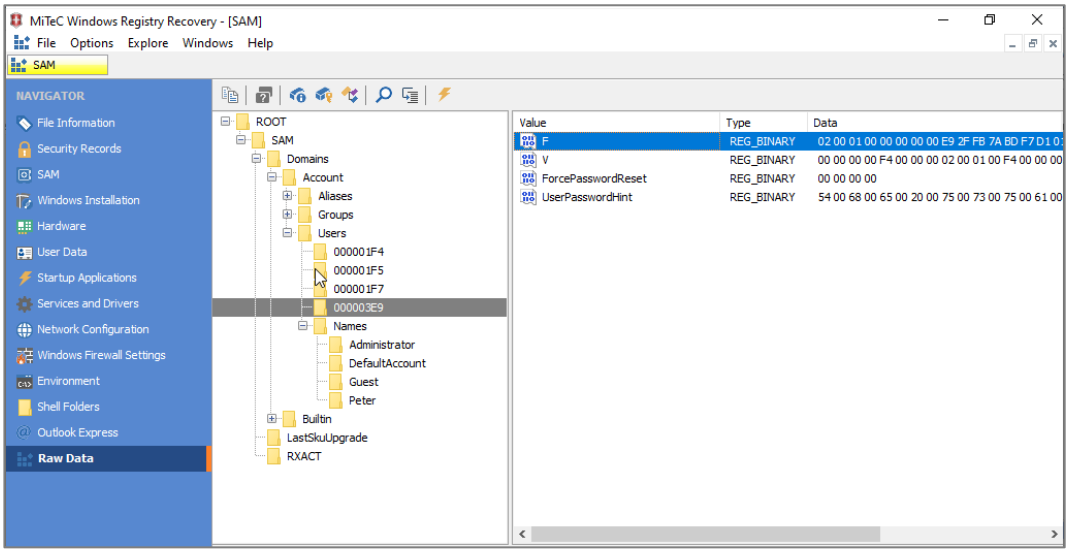


- Über den Punkt SAM können die Informationen aufbereitet eingesehen werden



- 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