Studienprogramm Sachbearbeiter:in Digitale Forensik
Praktikum Betriebssysteme
Dozent: Leander Hossfeld
hossfeld@hs-mittweida.de
Stand: 13.04.2023

HOCHSCHULE MITTWEIDA
University of Applied Sciences

Betriebssysteme

Praktikum 3

In diesem Praktikum lernen Sie die Ereignisanzeige des Windows Betriebssystems und die Möglichkeiten Events zu filtern, kennen. Zudem sollen Sie das EFS-Verschlüsselungssystem näher beleuchten.

Inhalte des Praktikums:

- Umgang mit EFS-Verschlüsselung
- Event-Log Untersuchung

LÖSUNG

Vorbereitung

Nutzen Sie bitte für die weitere Bearbeitung die in PR1 erstellte Windows VM oder die OVA aus PR2. Sie benötigen zudem erneut die ISO-Datei aus PR2: **PR2.iso**.

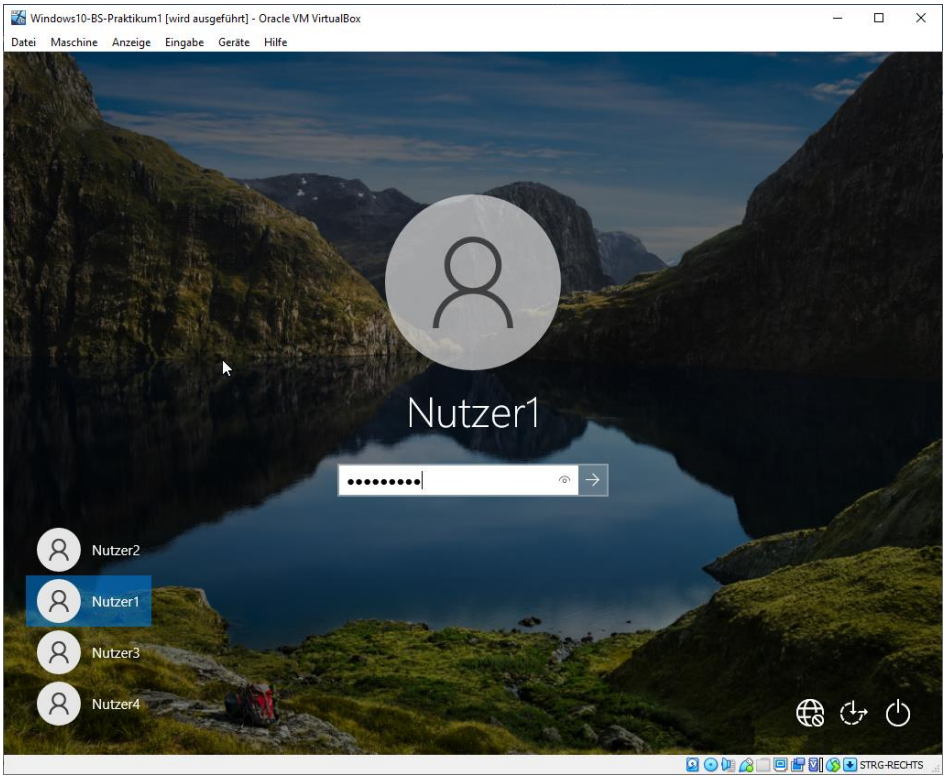
Allgemeine Hinweise

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.

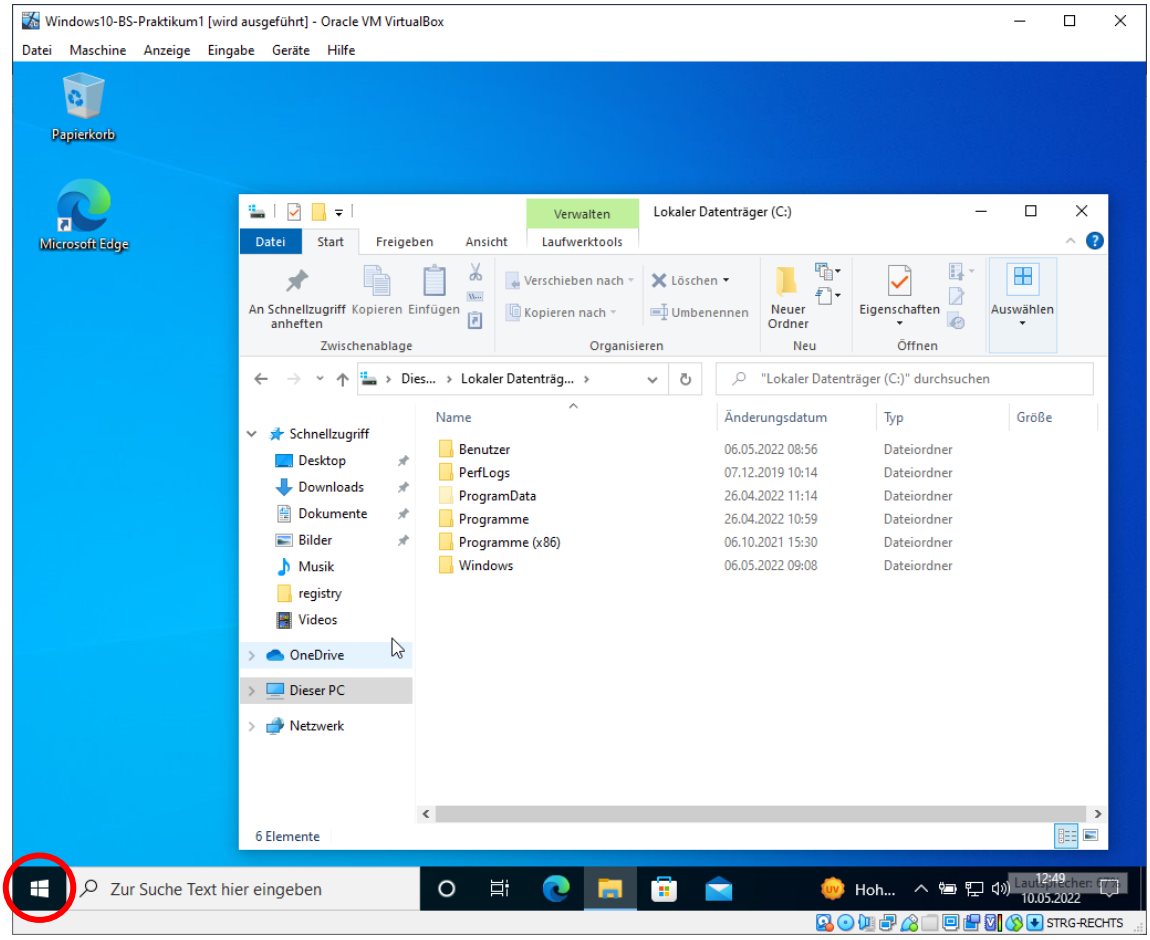
EFS-Verschlüsselung anlegen

Öffnen Sie Virtualbox und starten Sie die VM.

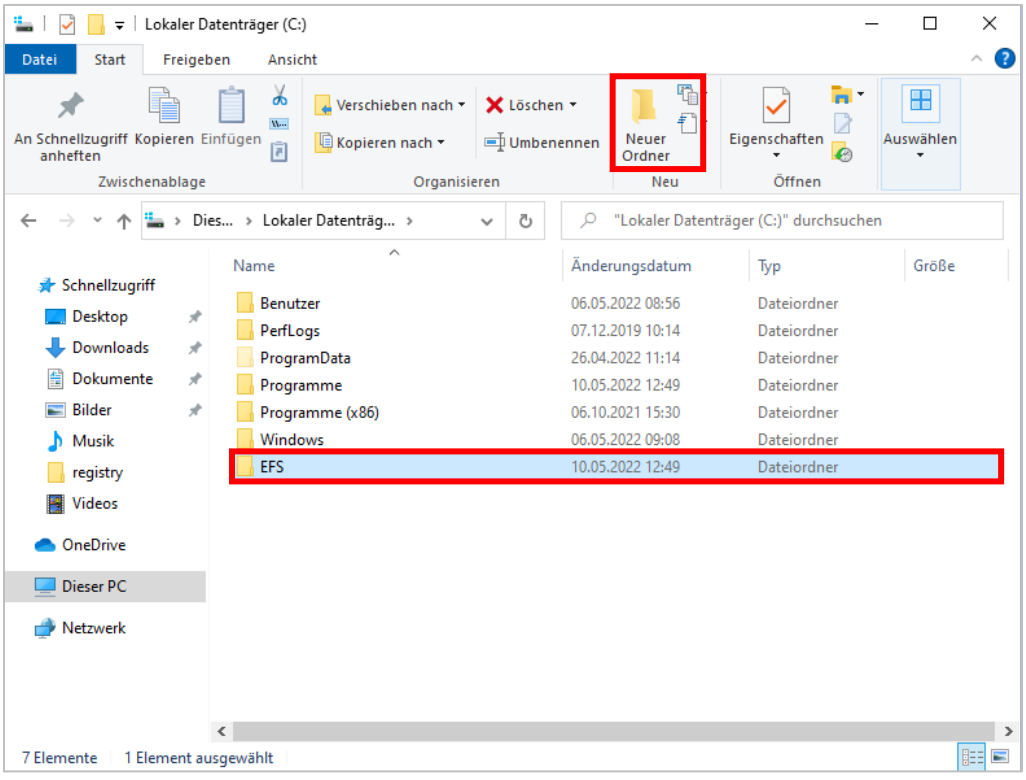
- Loggen Sie sich als **Nutzer1** mit **Kennwort1** ein



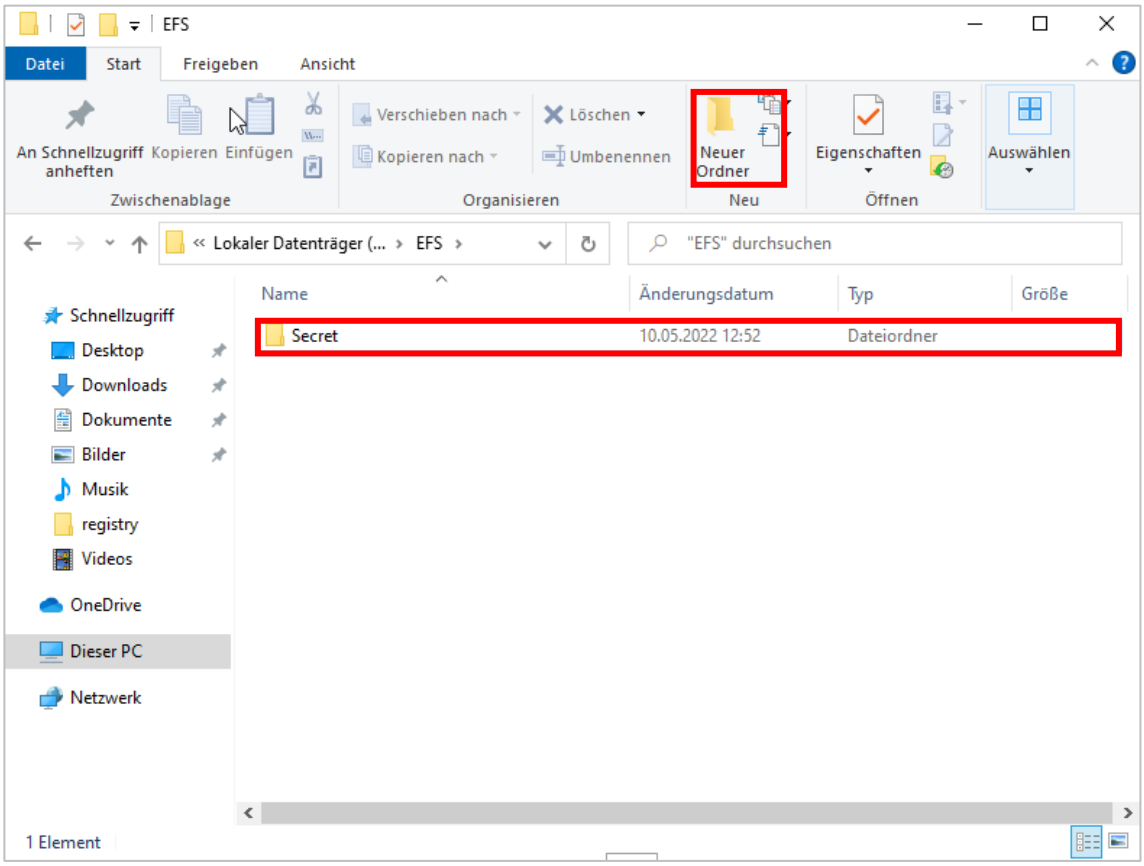
- **Öffnen** Sie im Schritt 2 den **Windows Explorer** und gehen Sie auf **Laufwerk C:**



- **Erstellen** Sie ein **Verzeichnis „EFS“** unter Nutzung von Start „Neuer Ordner“ direkt im Laufwerk C:\

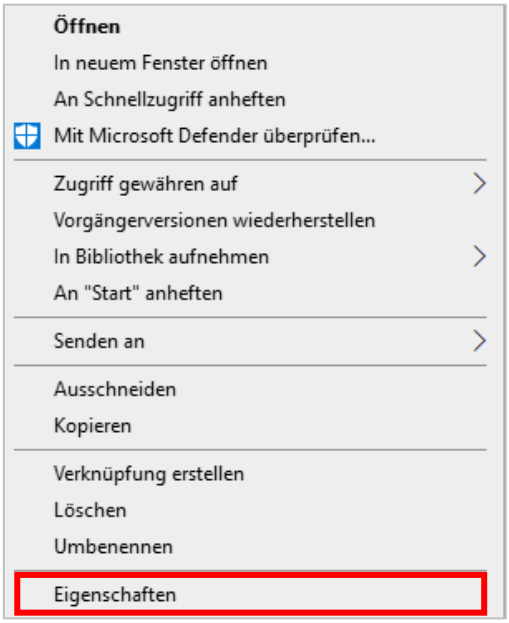


- **Erstellen** Sie innerhalb des Verzeichnis EFS ein weiteres **Unterverzeichnis „Secret“** auf gleichem Weg

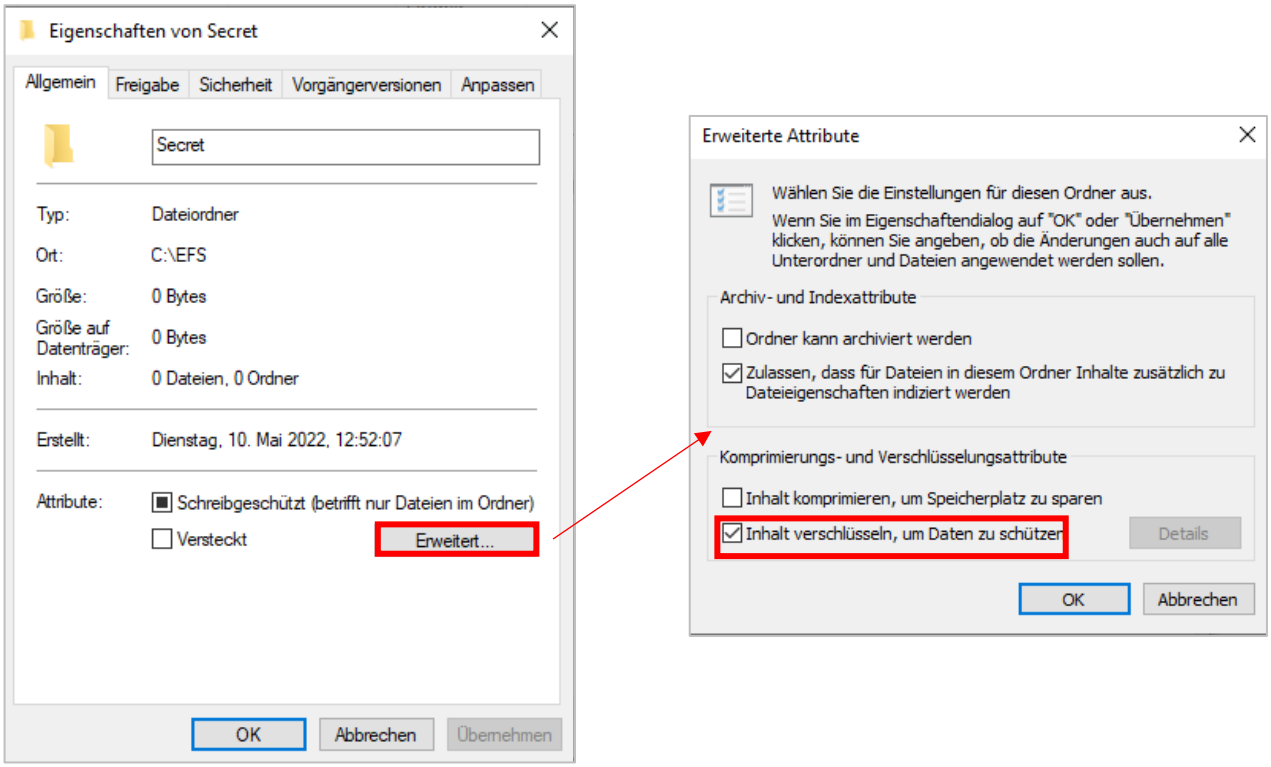


Verzeichnis bearbeiten:

- Wählen Sie die Eigenschaften (Rechtsklick) vom Verzeichnis „Secret“ und Öffnen Sie diese



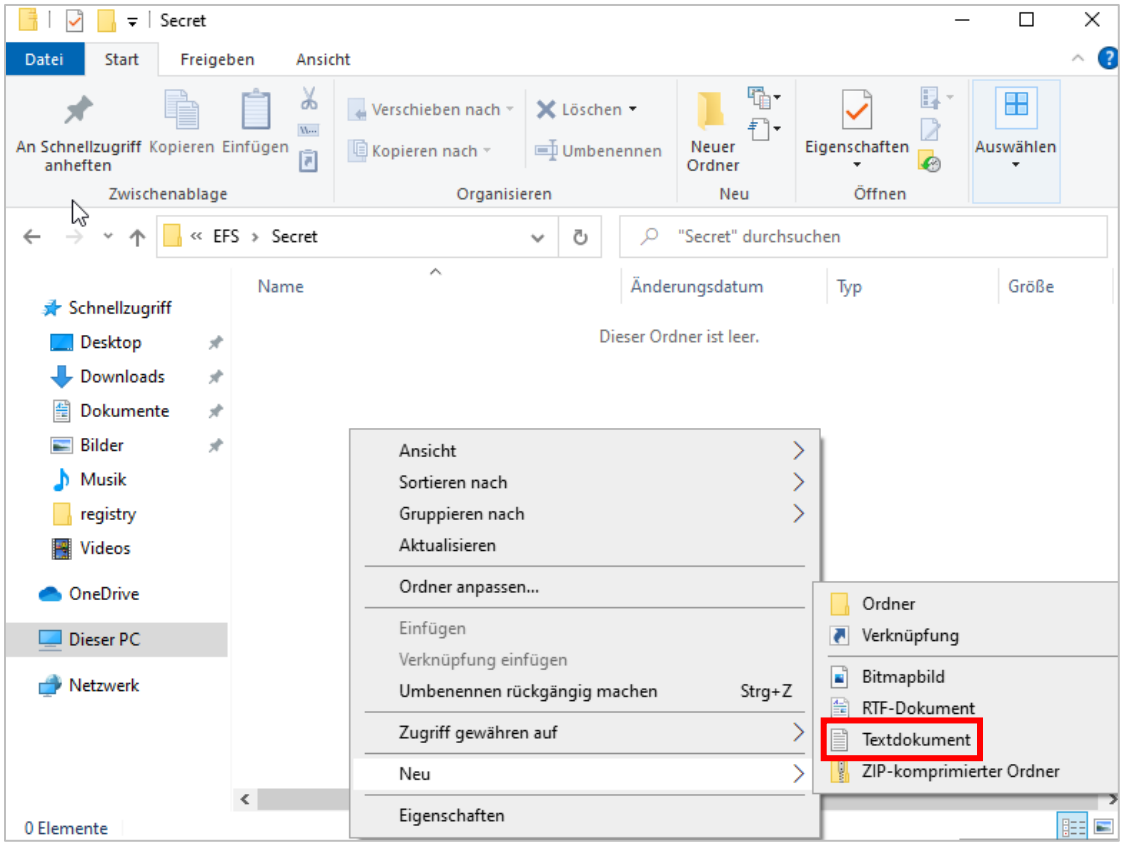
- Wählen Sie „Erweitert“ aus und aktivieren Sie „Inhalt verschlüsseln, um Daten zu schützen“



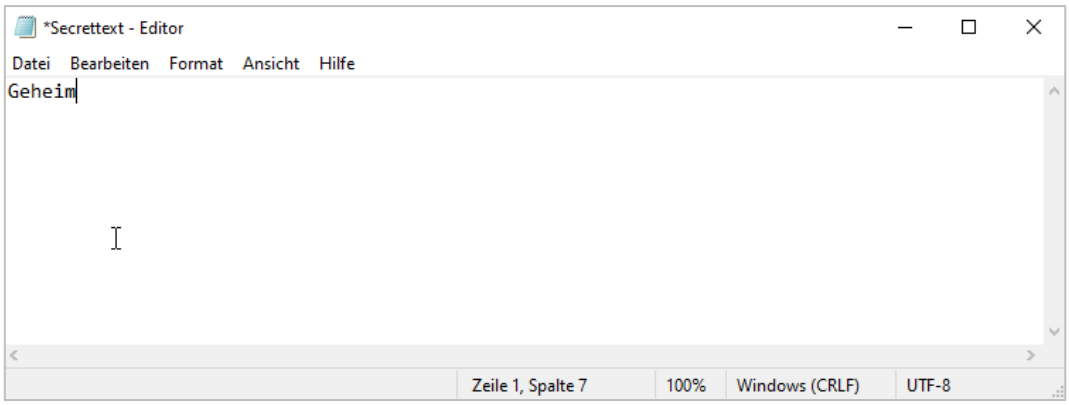
- Bestätigen Sie jeden Dialog mit OK

Verschlüsselte Datei erstellen:

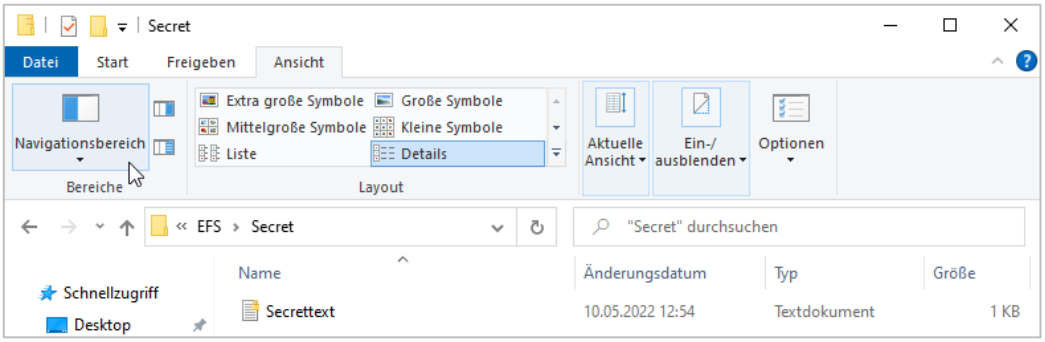
- Erstellen Sie im Verzeichnis „Secret“ eine Textdatei (Rechtsklick > Neu >Textdokument) und Benennen Sie es „Secrettext“



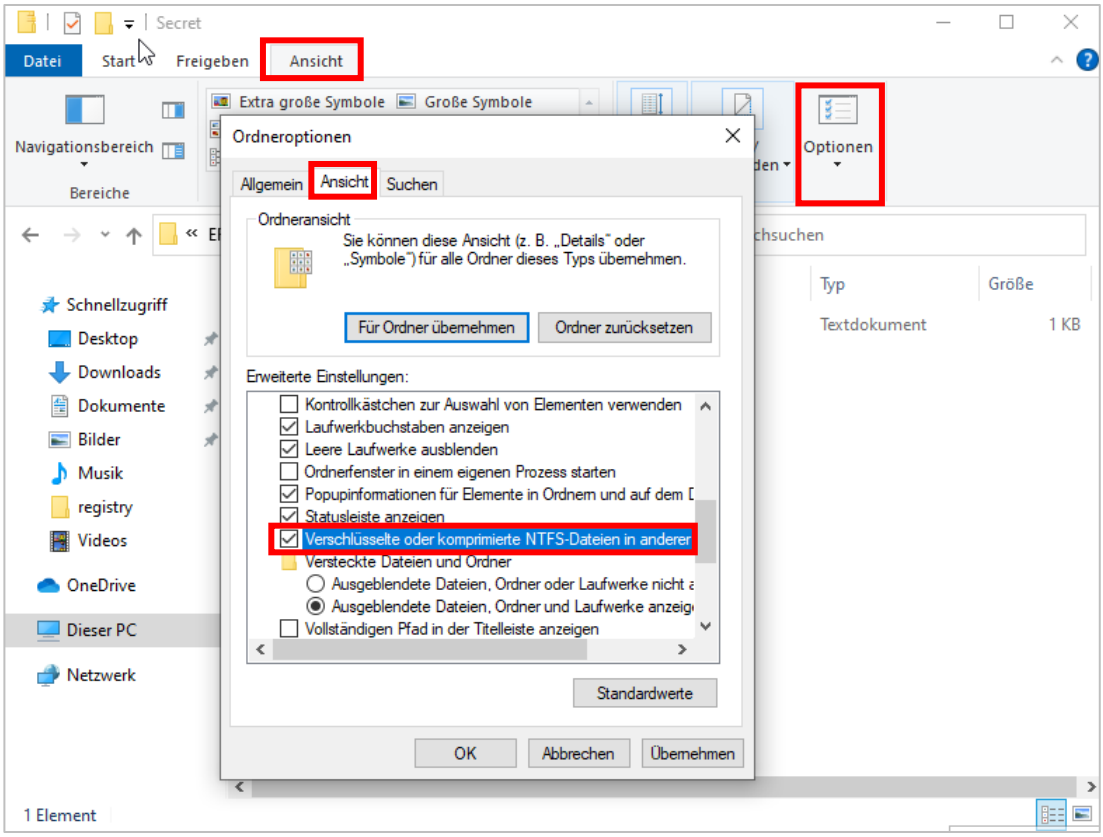
- Tragen Sie in diese Datei einen Geheimen Text hinein und Speichern Sie das Dokument ab



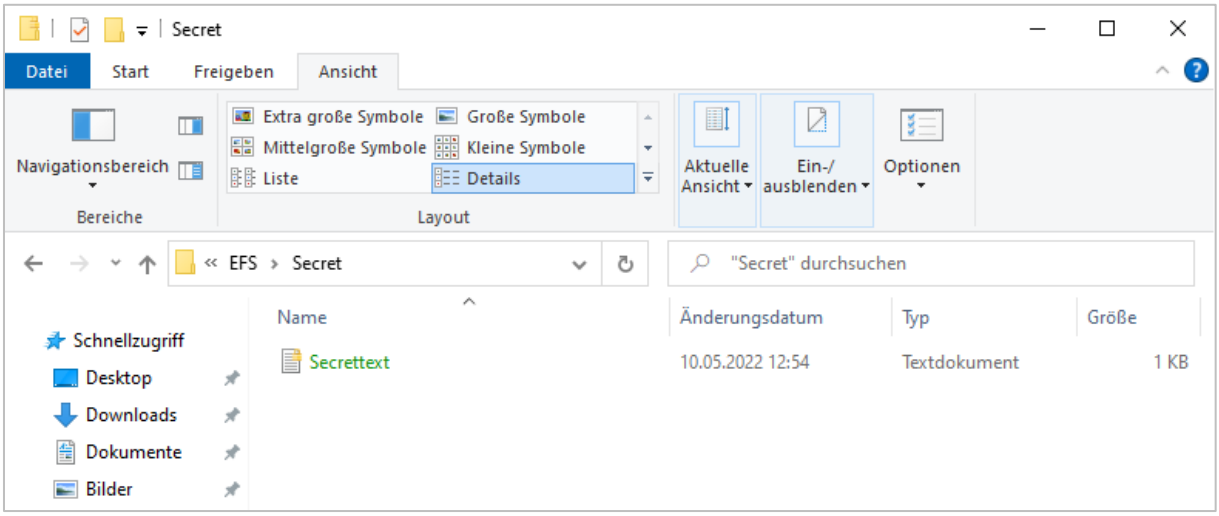
Ansicht anpassen:



- Gehen Sie auf Ansicht > Optionen und Wählen Sie unter Ansicht in der Auflistung „Verschlüsselte oder komprimierte NTFS-Dateien in anderer Farbe einfärben“ aus und markieren es

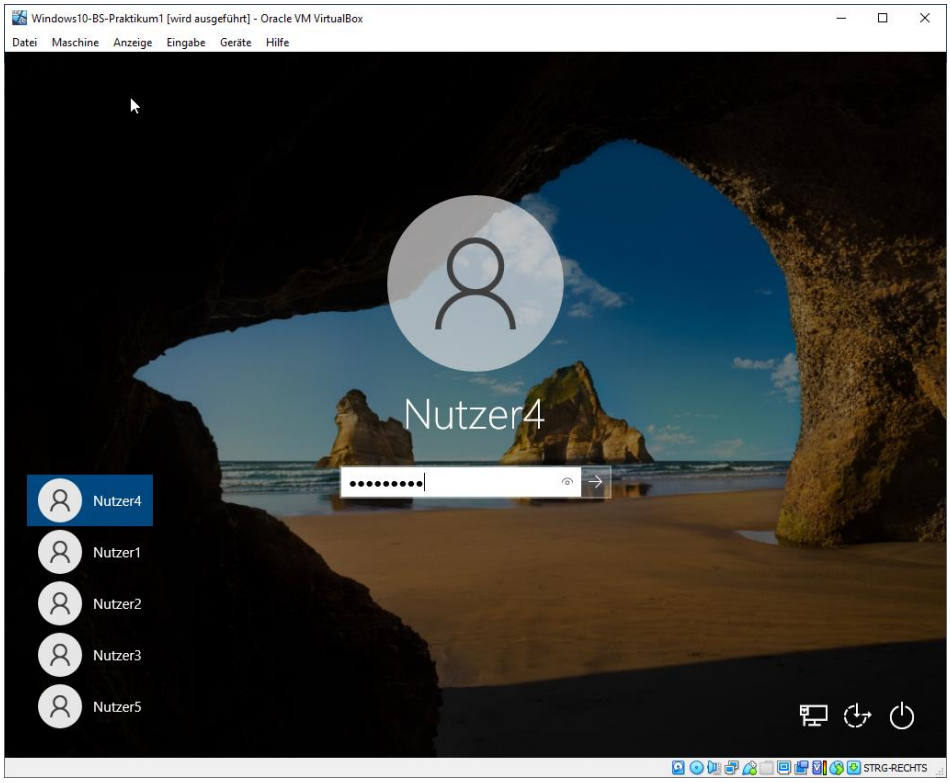


- Wie sieht die Ansicht jetzt aus?



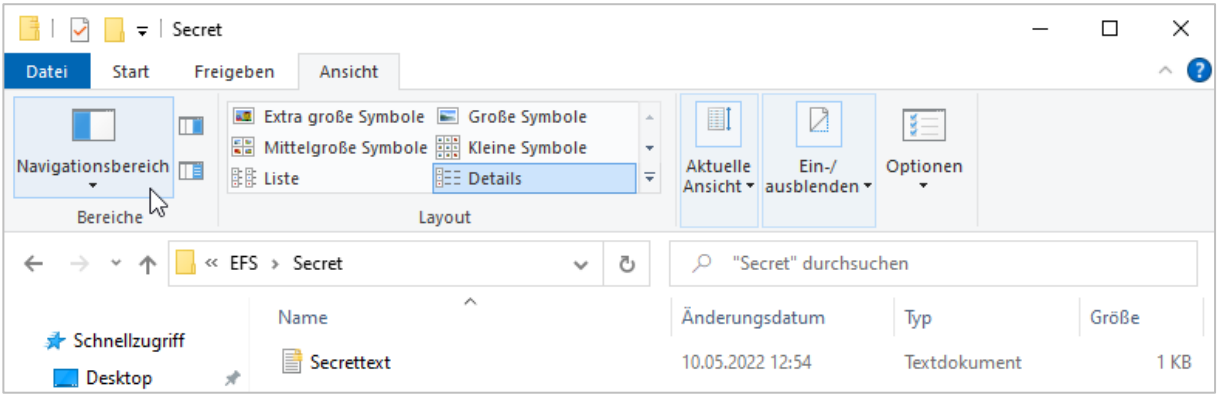
EFS-Verschlüsselung auf anderen Nutzer übertragen

Melden Sie sich von Nutzer1 aus, als Nutzer4 an.

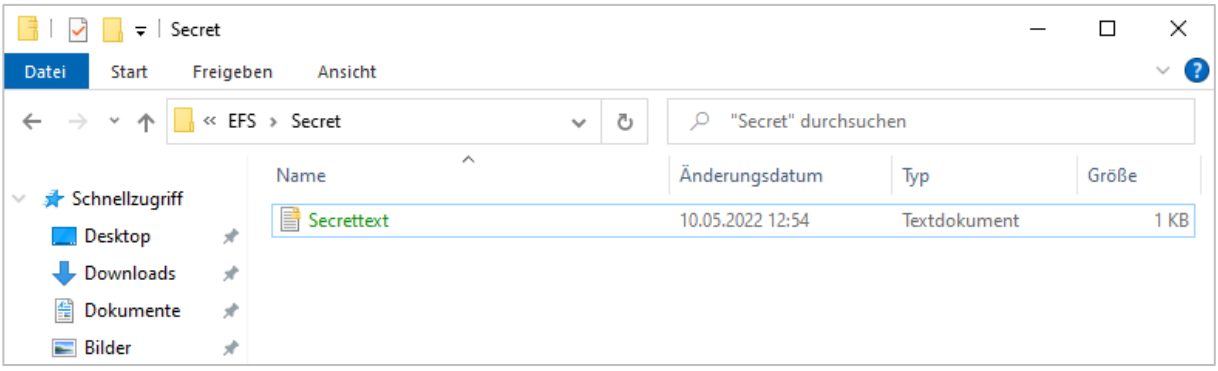


Verschlüsselte Datei von Aufgabe 1.1 Öffnen:

- Öffnen Sie den Windows Explorer und Wechseln Sie in das Verzeichnis „C:\EFS\Secret“

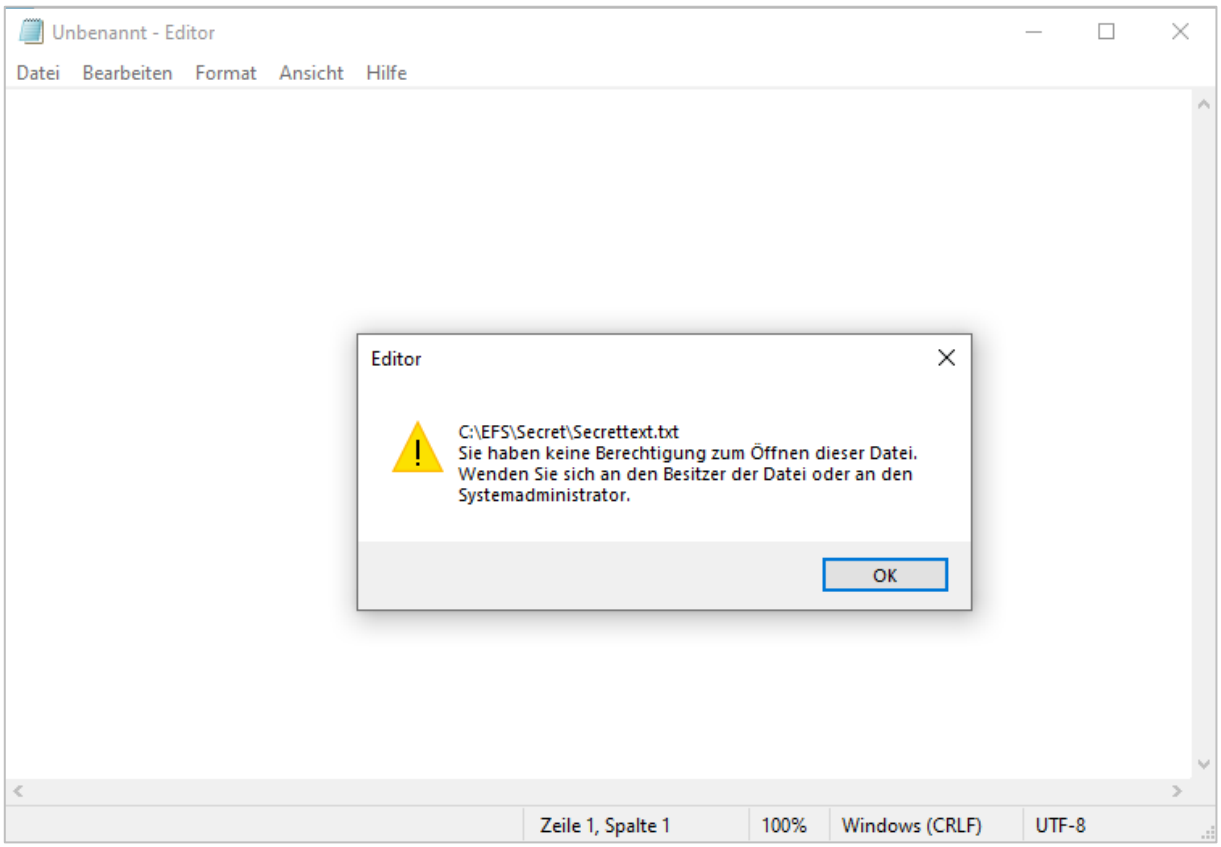


➢ Stellen Sie auch hier die Ansicht um auf „EINFÄRBEN“



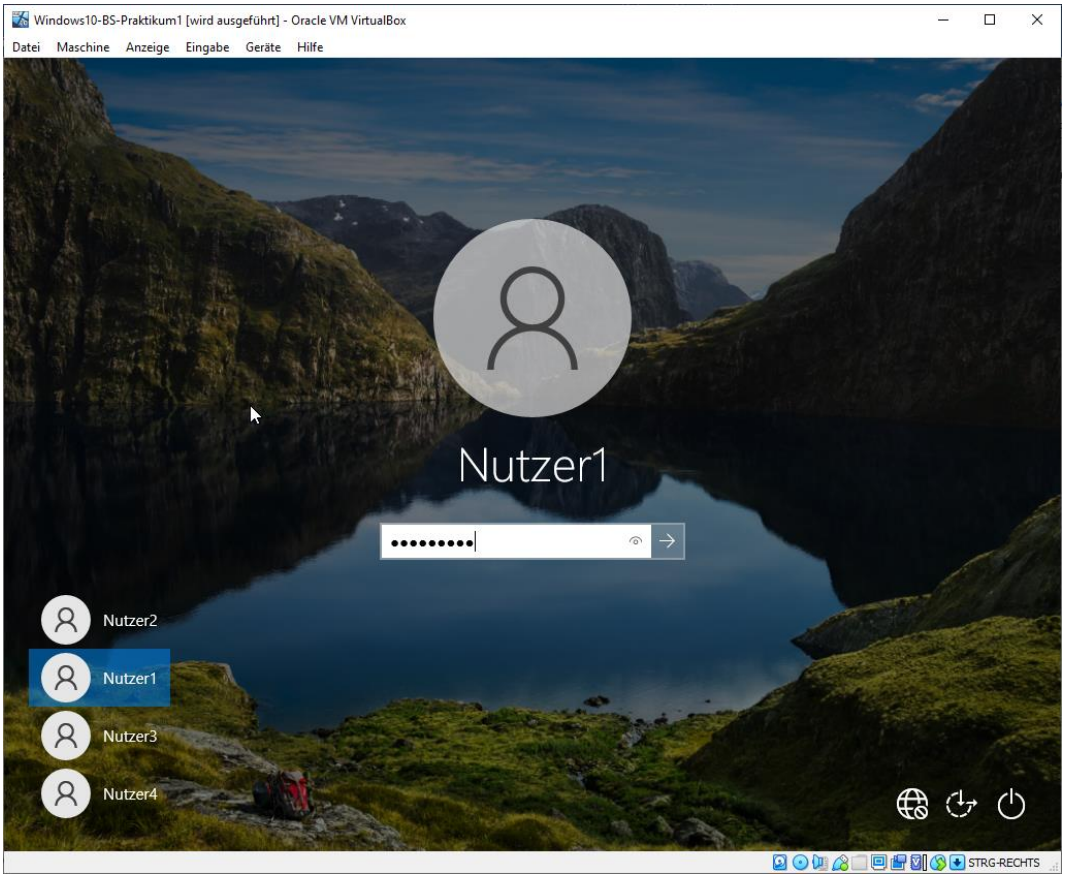
➢ Öffnen Sie die Datei Secrettext

➢ Hat dies funktioniert?

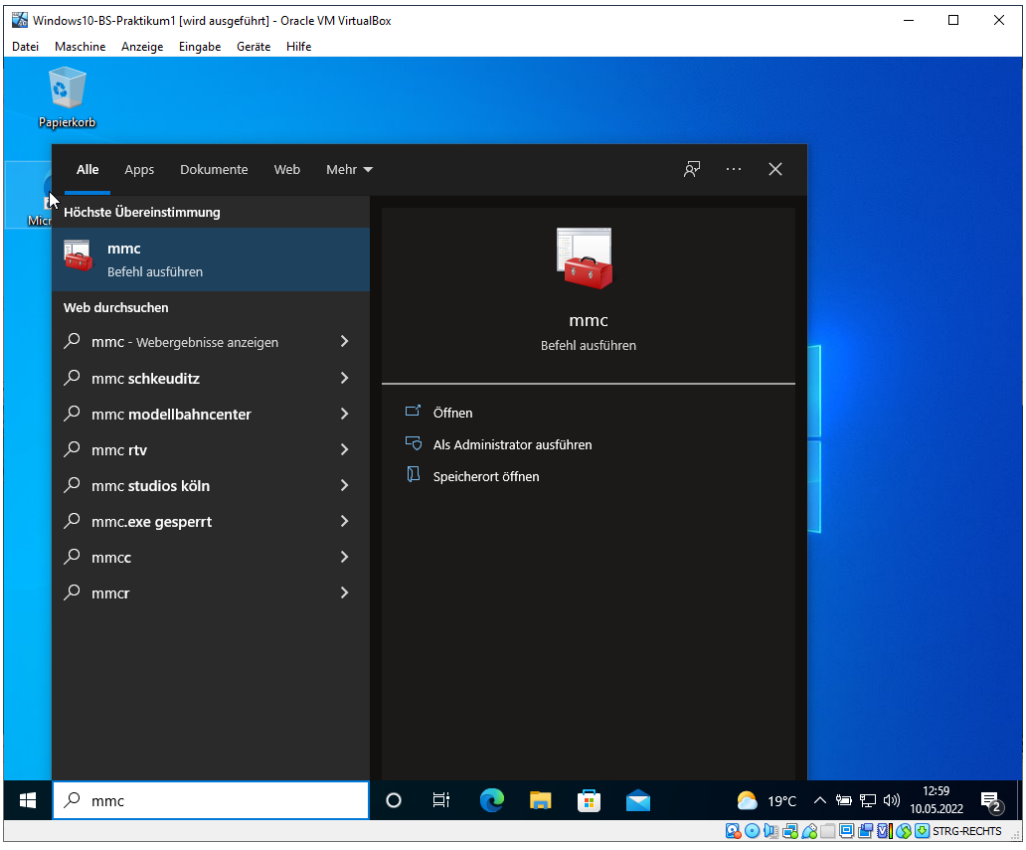


Datei lesbar machen in fremden Nutzerkontext:

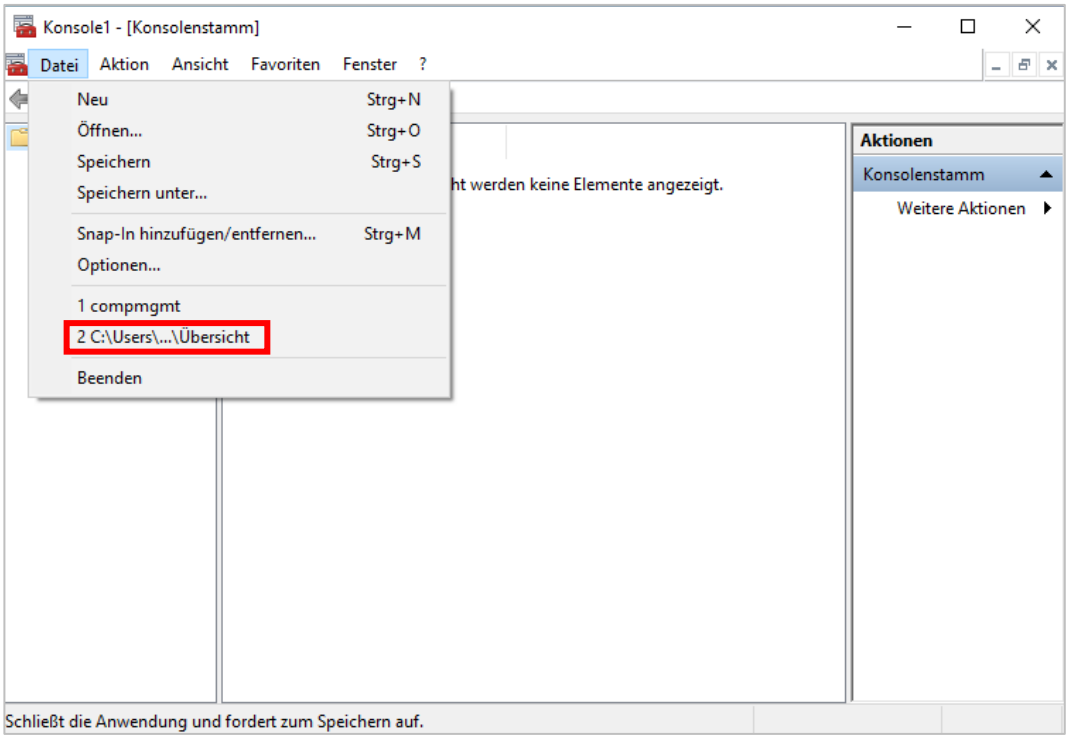
- Melden Sie sich wieder als Nutzer 1 an



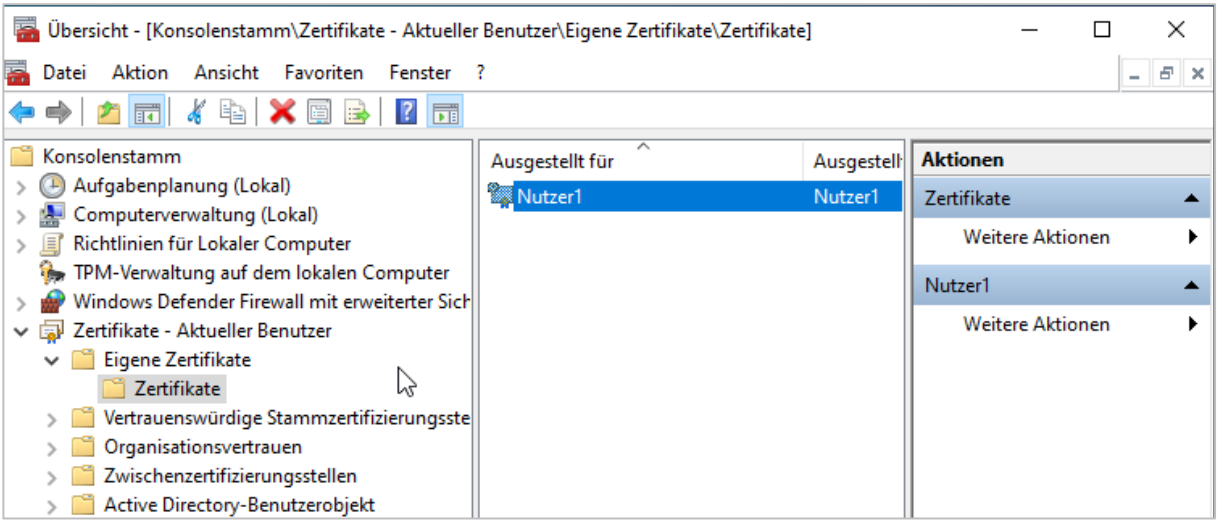
- Öffnen Sie die MMC über den Windows Start Button (MMC)



- Öffnen Sie die Übersicht aus Praktikum 1 oder fügen Sie das Snap-In „Zertifikate“ hinzu

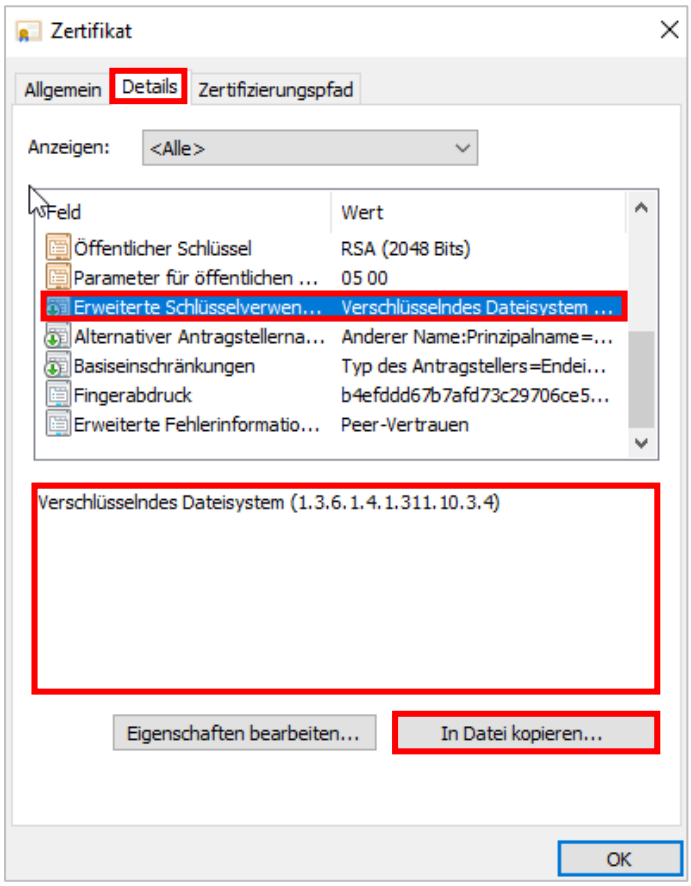


- Wählen Sie unter Zertifikate „Eigene Zertifikate“ aus

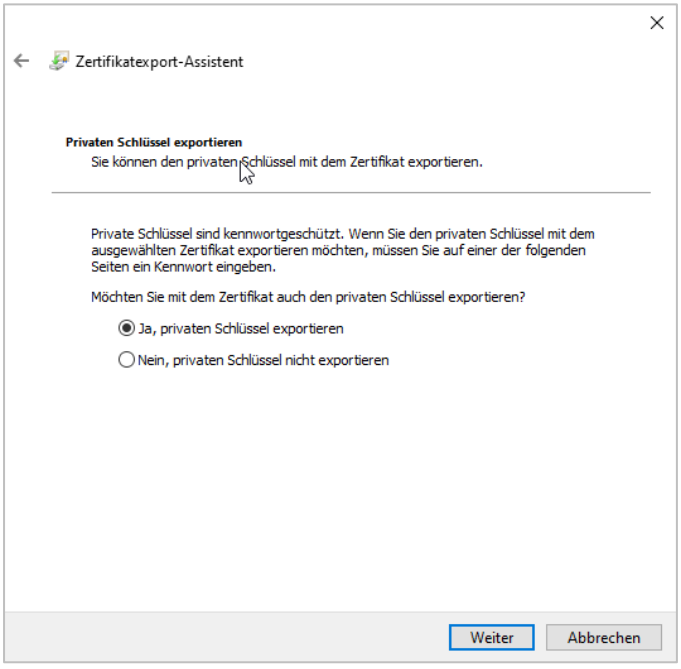


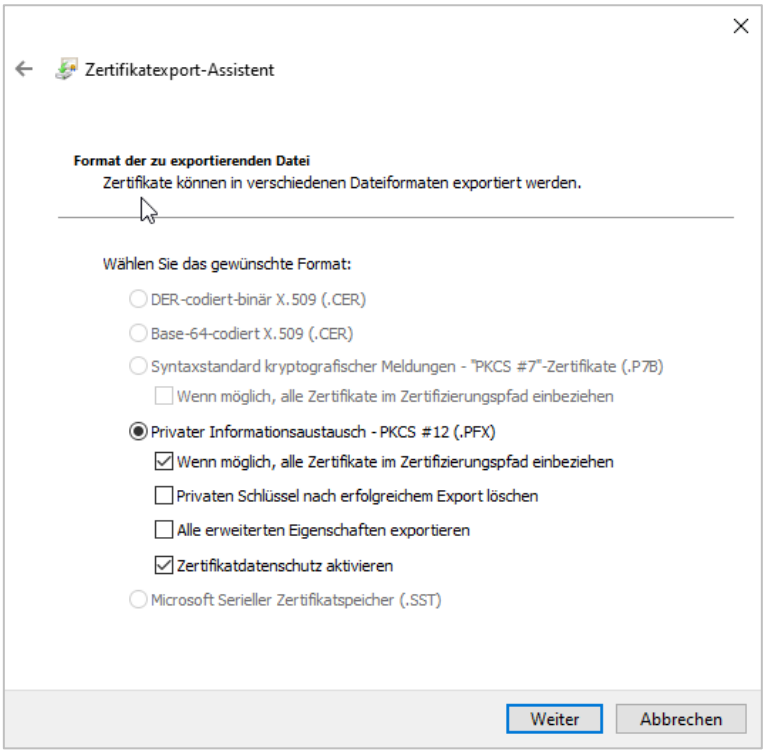
Zertifikat exportieren:

- Dort finden Sie von Nutzer1 ein Zertifikat, welches Sie sich unter Eigenschaften anzeigen lassen können
- Schauen Sie unter Details nach. Finden Sie die Erweiterte Schlüsselverwendung?
- Speichern Sie das Zertifikat ab (In Datei kopieren)!

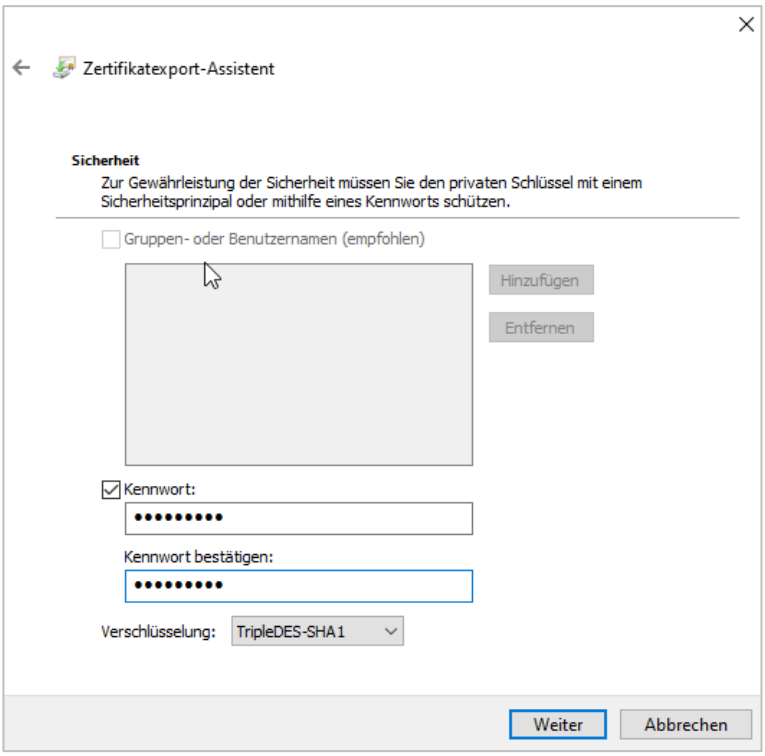


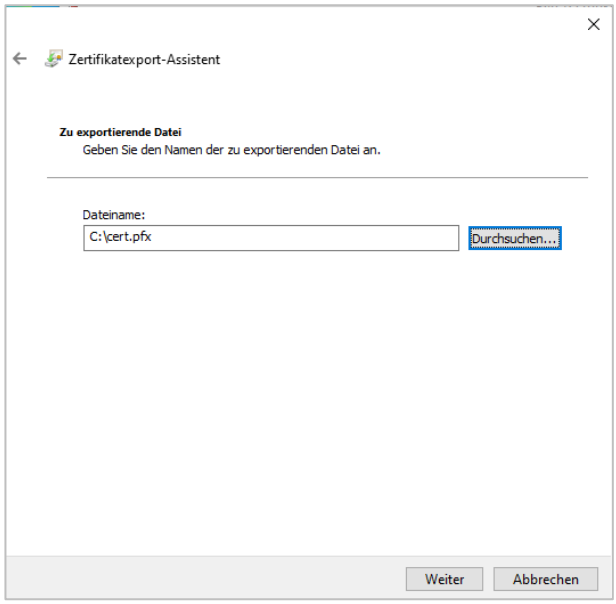
- Exportieren Sie das Zertifikat mit privatem Schlüssel!





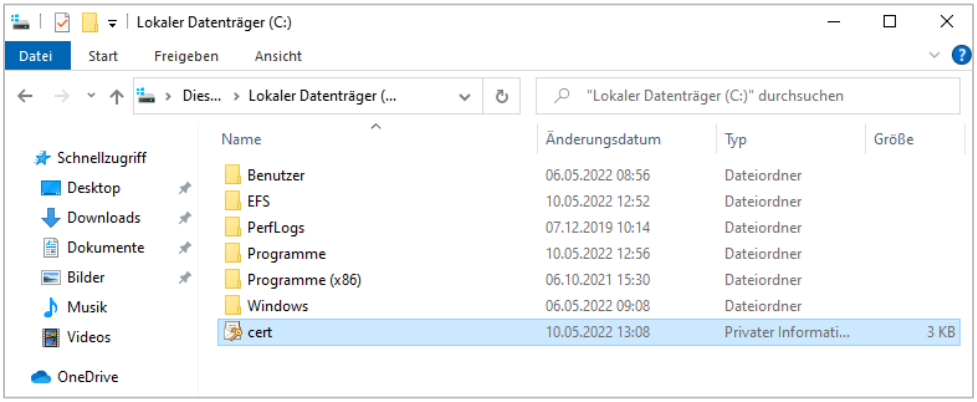
- Vergeben Sie ein Kennwort (Kennwort1) und speichern sie das Zertifikat als Cert.pfx auf Laufwerk C:\



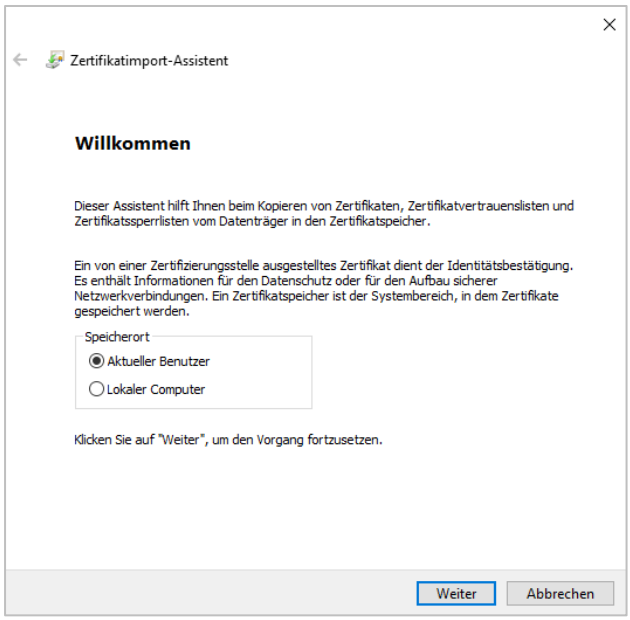


Zertifikat importieren:

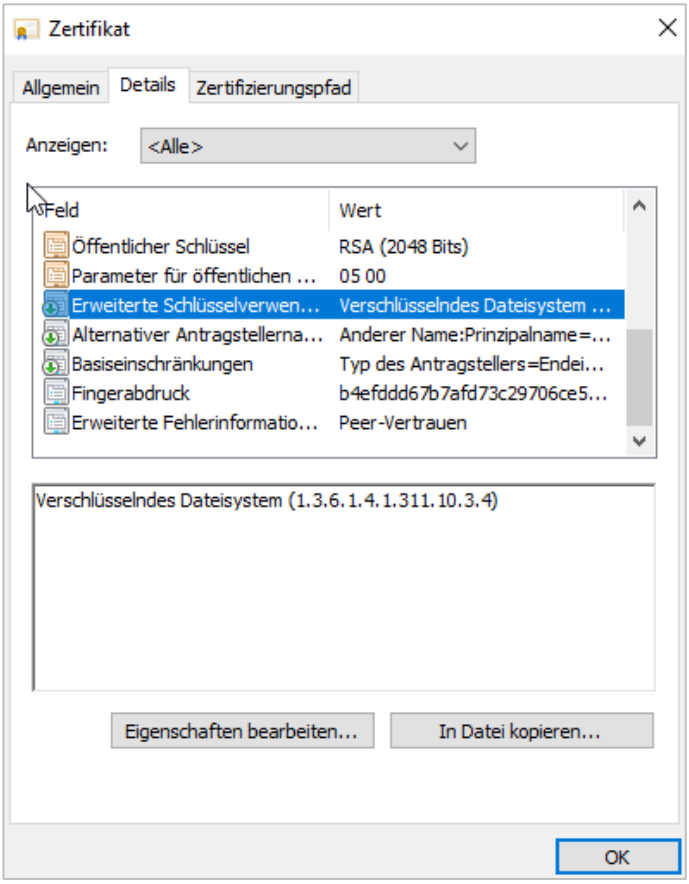
- Nach dem Speichern des Zertifikats melden Sie sich bitte als Nutzer 1 ab und als Nutzer 4 wieder an
- Öffnen Sie den Windows Explorer auf Laufwerk C:\ und Öffnen Sie die Datei Cert.pfx



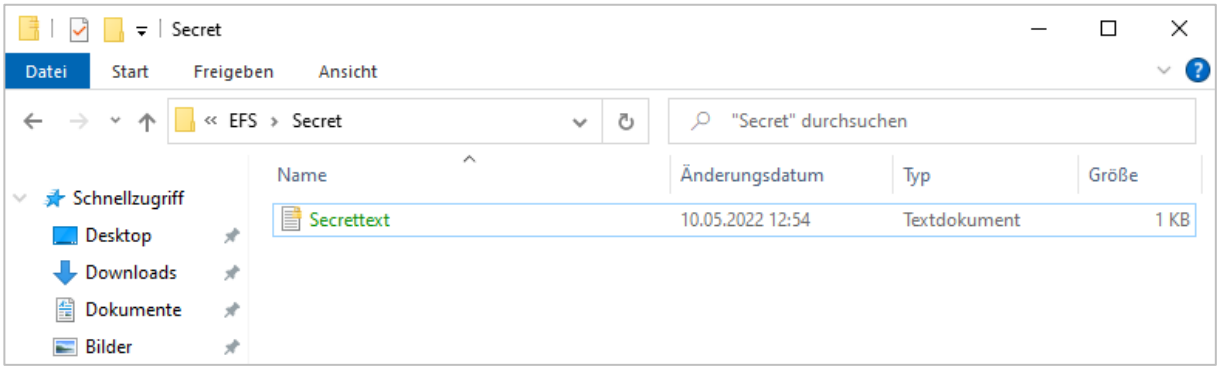
- Importieren Sie das Zertifikat für den aktuellen Benutzer



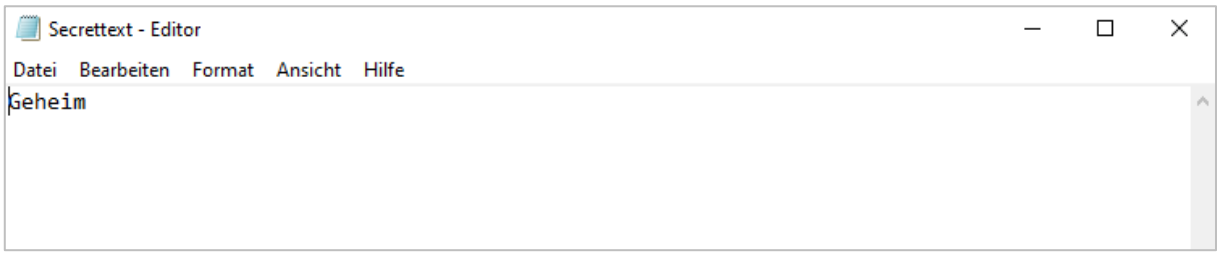
- Überprüfen Sie beim Import die Erweiterte Schlüsselverwendung und Bestätigen Sie alle folgenden Dialoge mit OK



Wechseln Sie in das Verzeichnis „C:\EFS\Secret“ und Öffnen Sie die Datei „Secrettext“.



- Hat dies funktioniert?

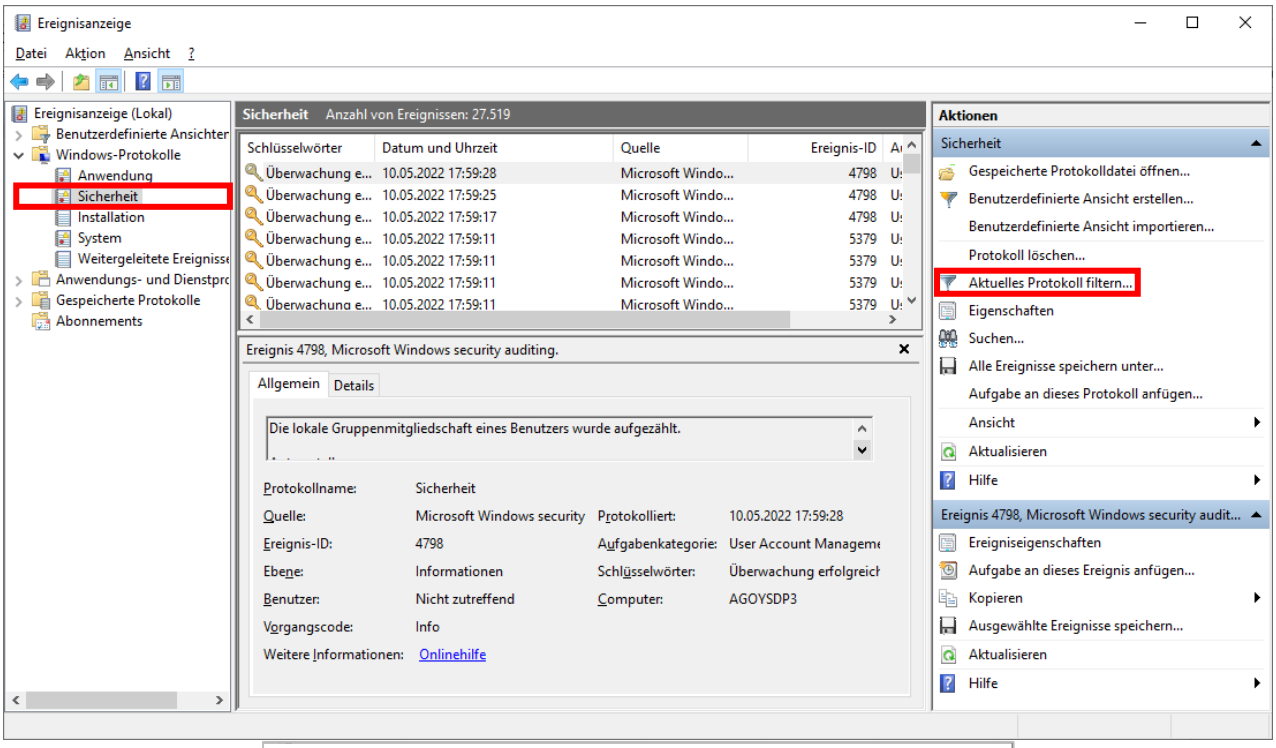


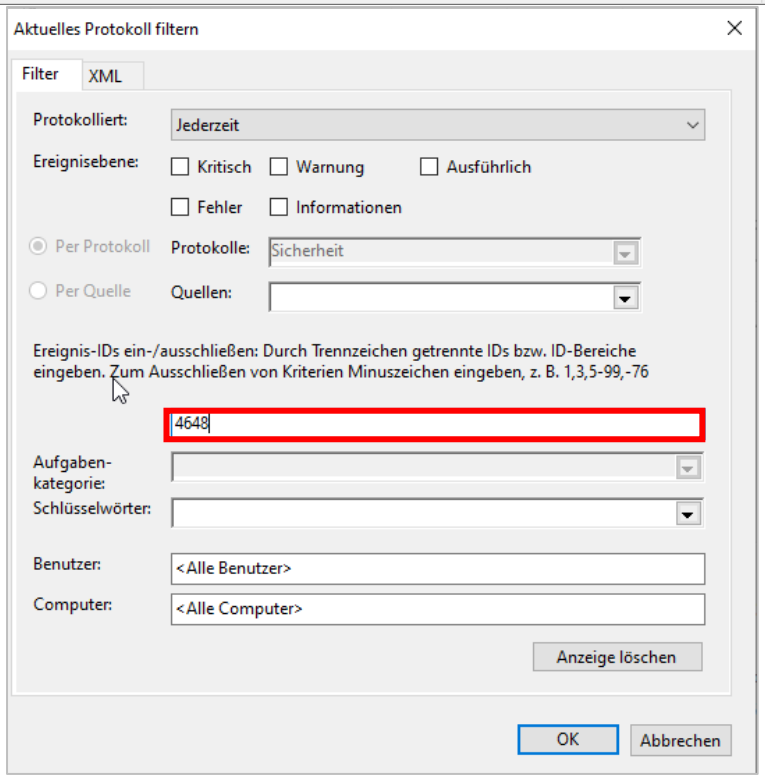
Eventlog auf Anmeldungen überprüfen

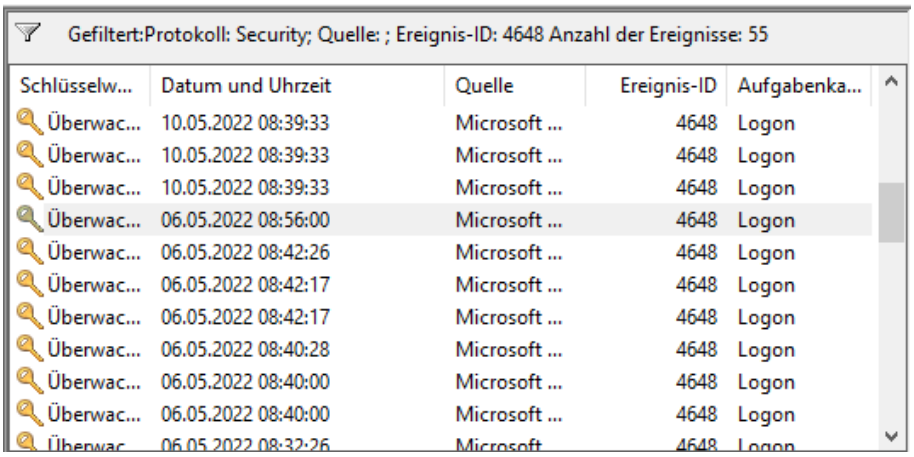
Unter der Nutzerkennung von Nutzer1 starten Sie bitte die MMC mit Übersicht aus PR1(Ereignisanzeige) oder die Ereignisanzeige über den Windows Start Button.

Run As Event-ID 4648

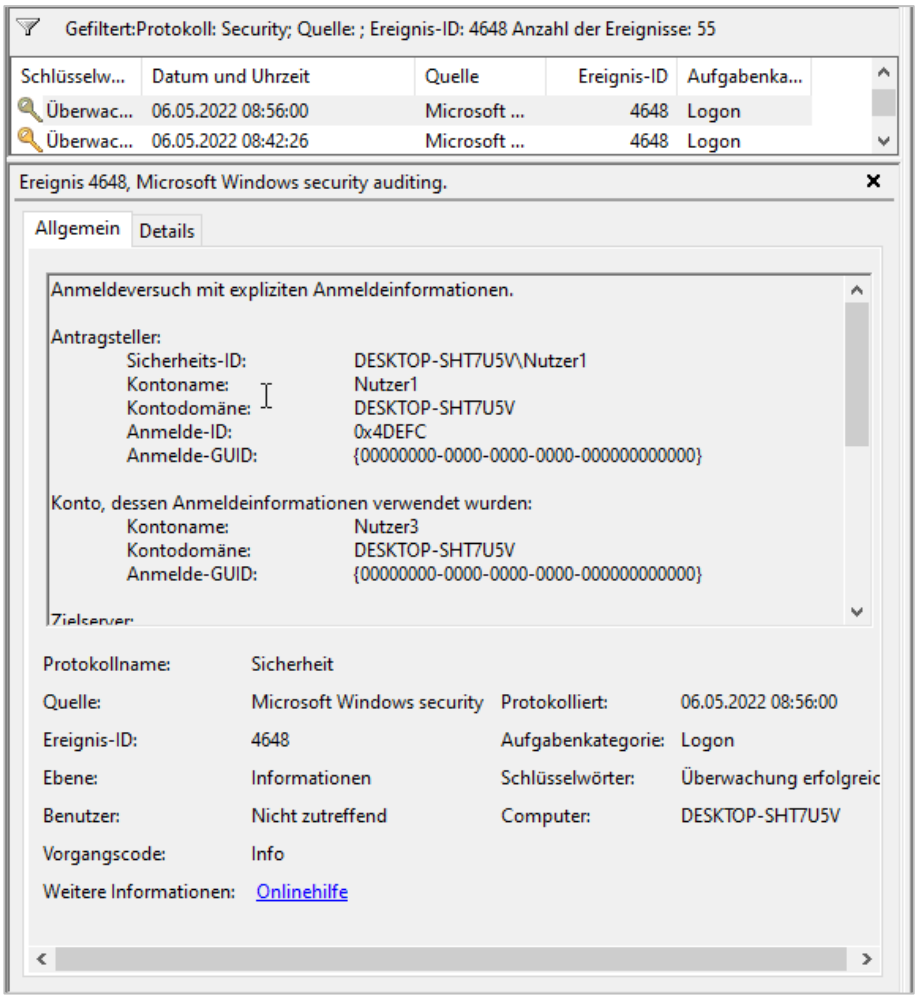
Filtern Sie nach der Event ID 4648.



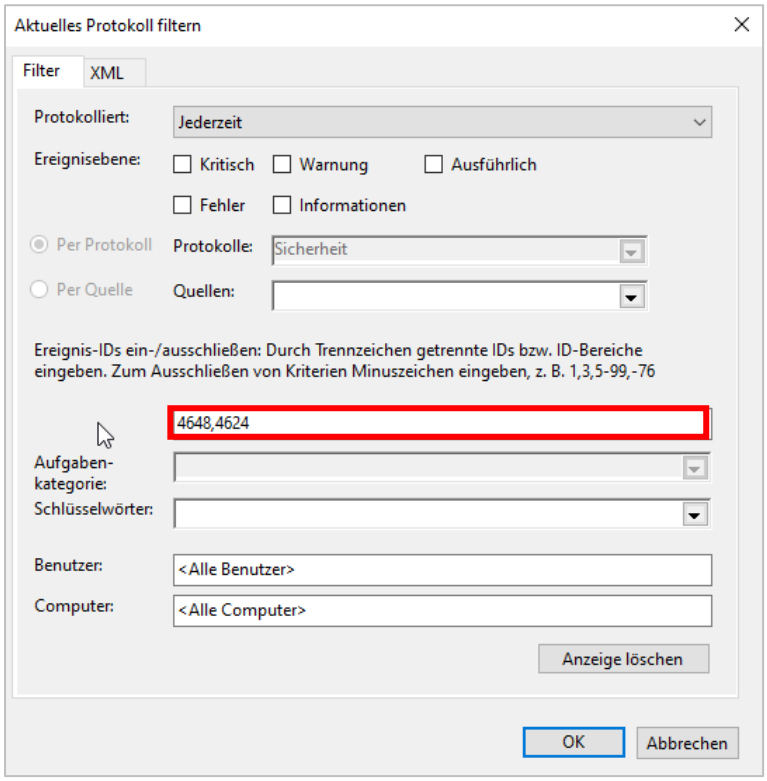




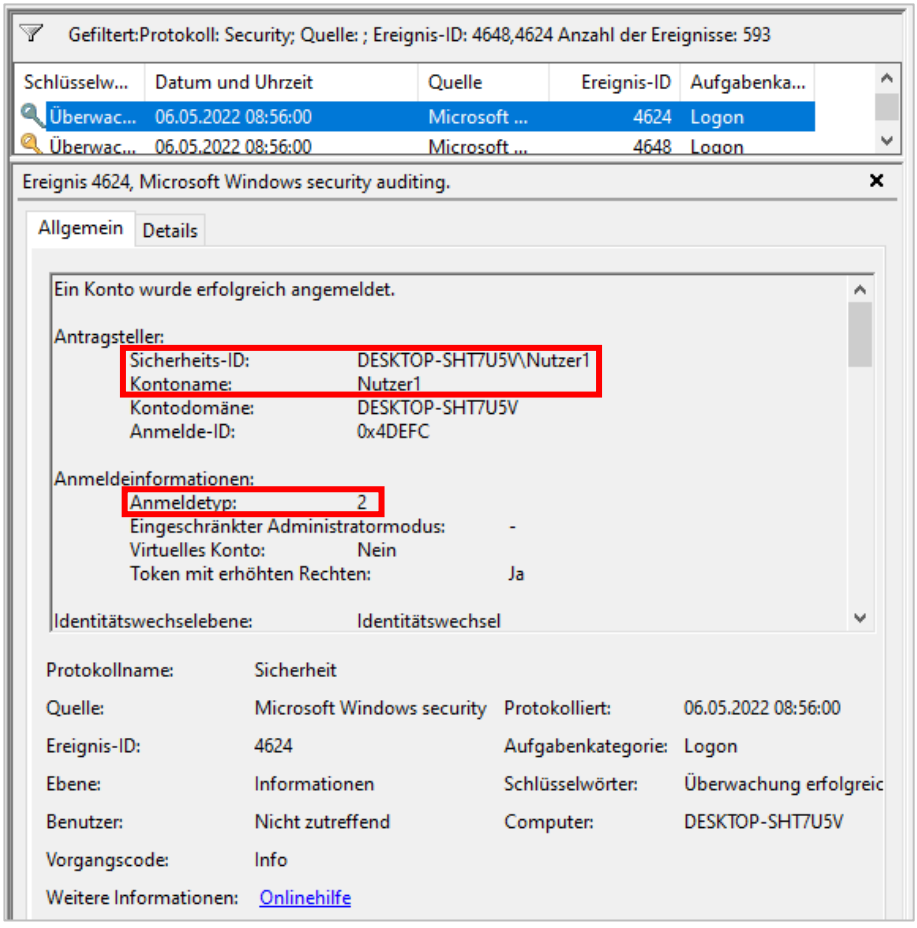
Finden Sie das **Event „Run As“** von **Praktikum1** als die **CMD.exe** durch **Nutzer1** mit **Nutzer3** Anmeldung gestartet wurde.



Schauen Sie sich die Anmeldungen im Umfeld dieser Account Nutzung an, in dem Sie die Event ID 4624 mit in den Filter aufnehmen.



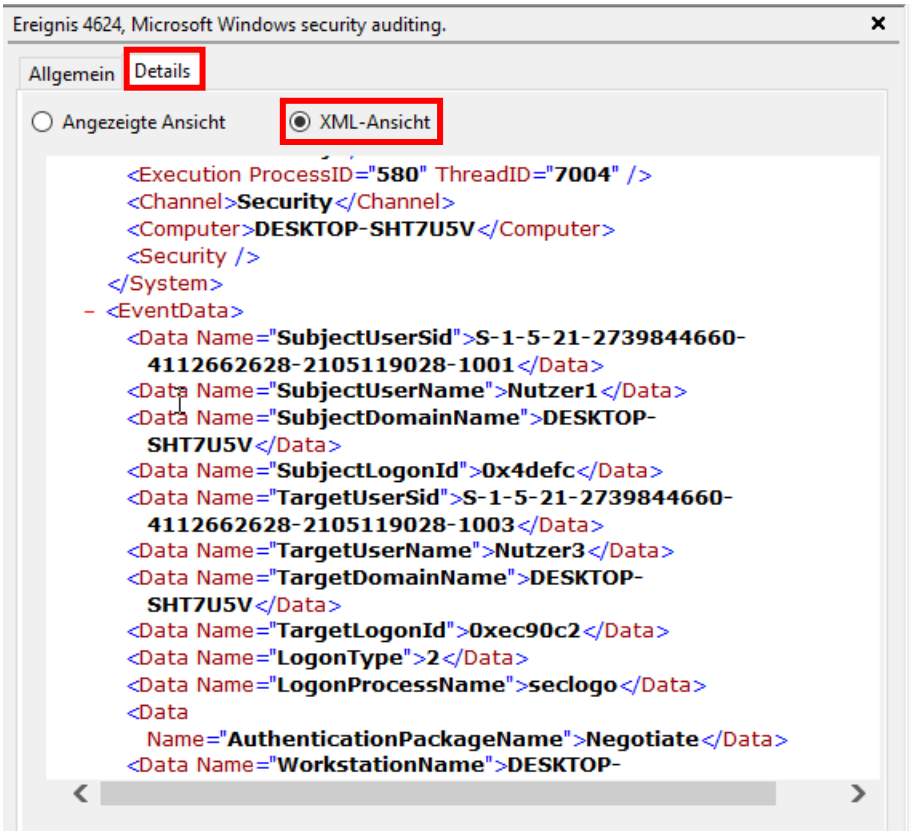
Finden Sie das dazugehörige Anmeldeereignis und Überprüfen Sie den **Anmeldetyp**.



Logon Typen - Interpretation

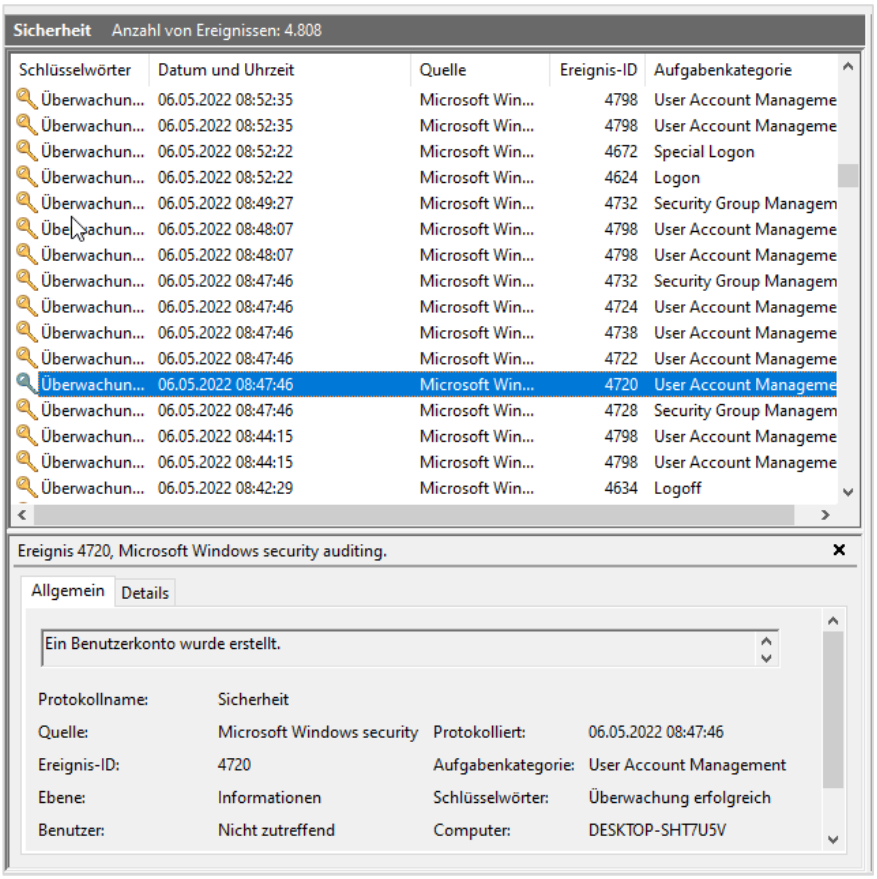
- 2 Logon via console
- 3 Network Logon
- 4 Batch Logon
- 5 Windows Service Logon
- 7 Credentials used to unlock screen
- 8 Network logon sending credentials (cleartext)
- 9 Different credentials used than logged on user
- 10 Remote interactive logon (RDP)
- 11 Cached credentials used to logon
- 12 Cached remote interactive (similar

Prüfen Sie hierbei auch einmal die XML-Ansicht.

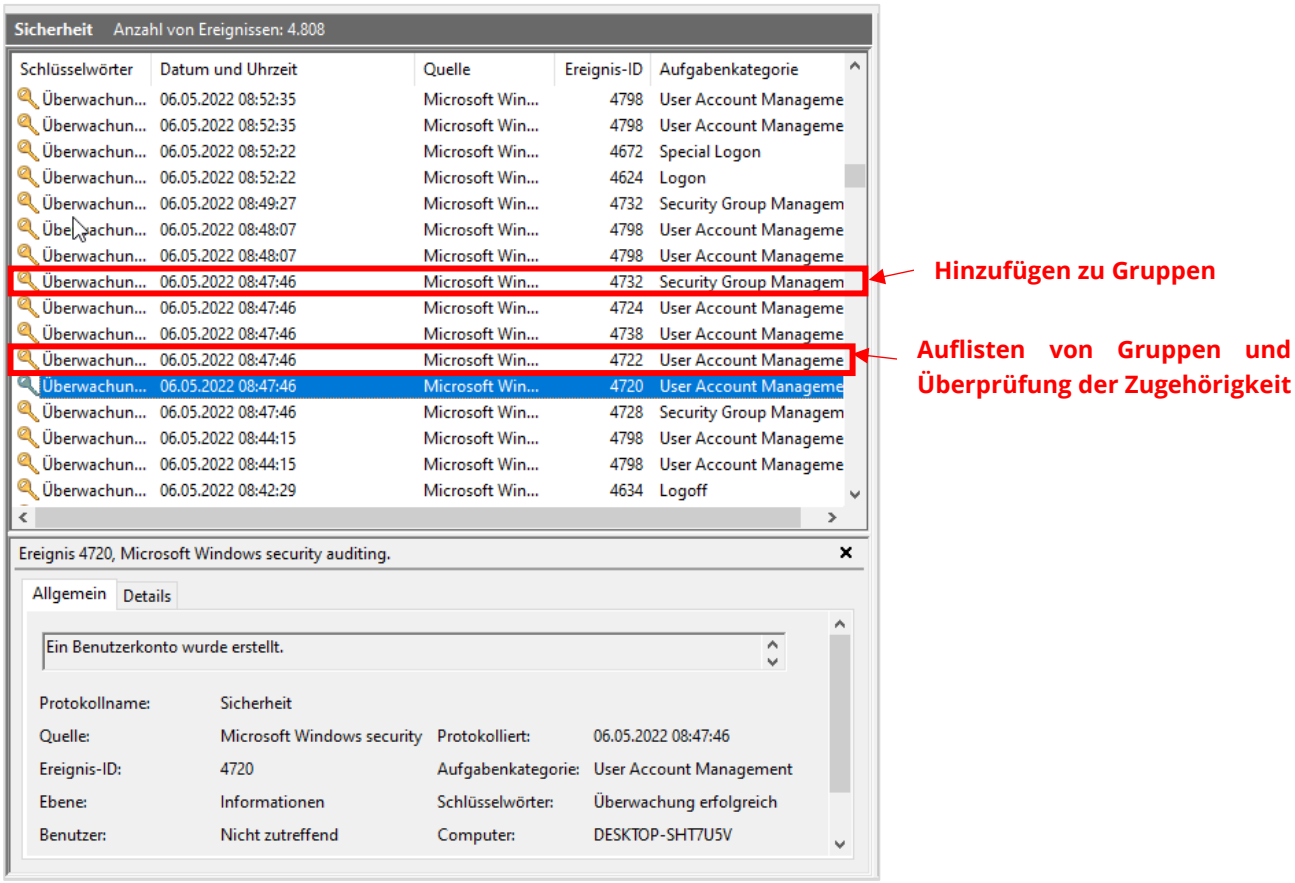


Account Creation Event-ID 4720

Schauen Sie, wann Nutzer 5 hinzugefügt wurde.



Welche Events erfolgten danach?

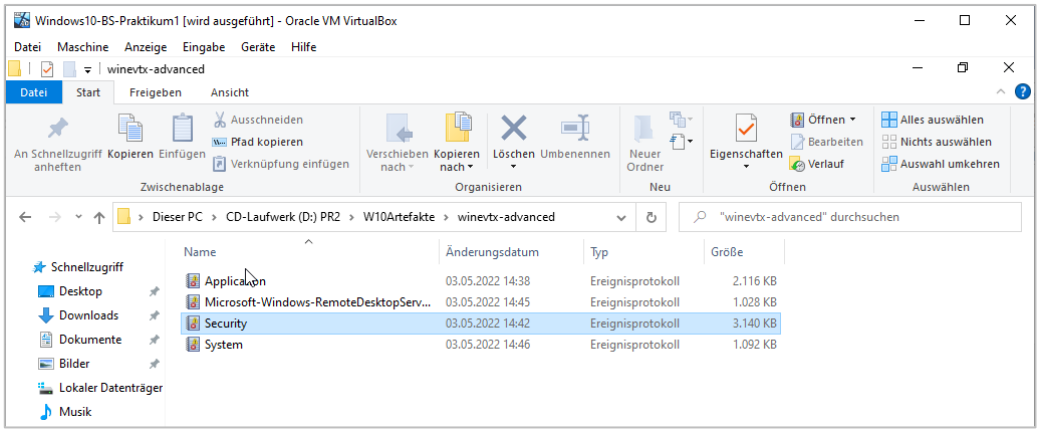


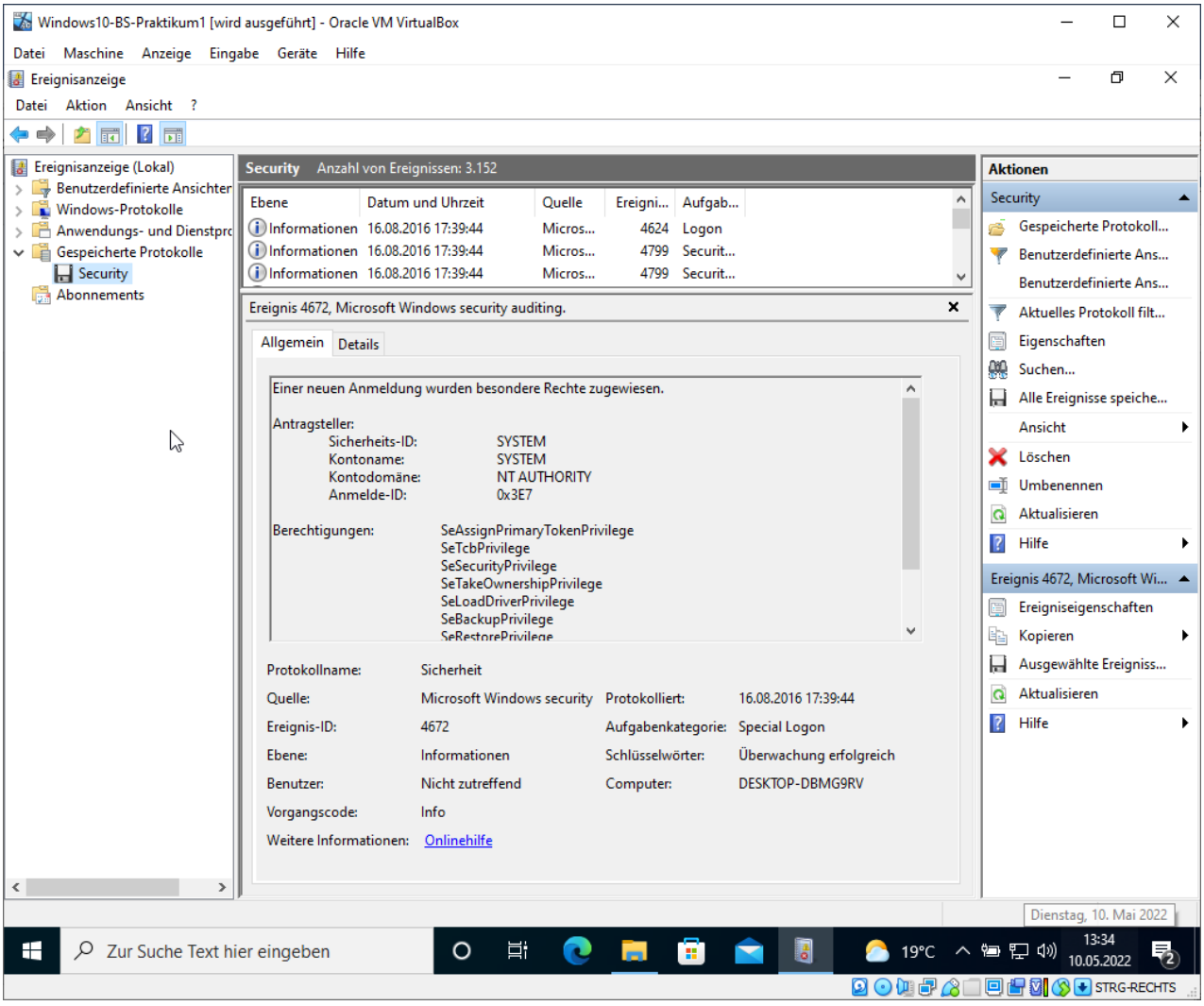
RDP-Login aus PR2.iso

Event-ID 4778, 4779 RDP-Nutzung

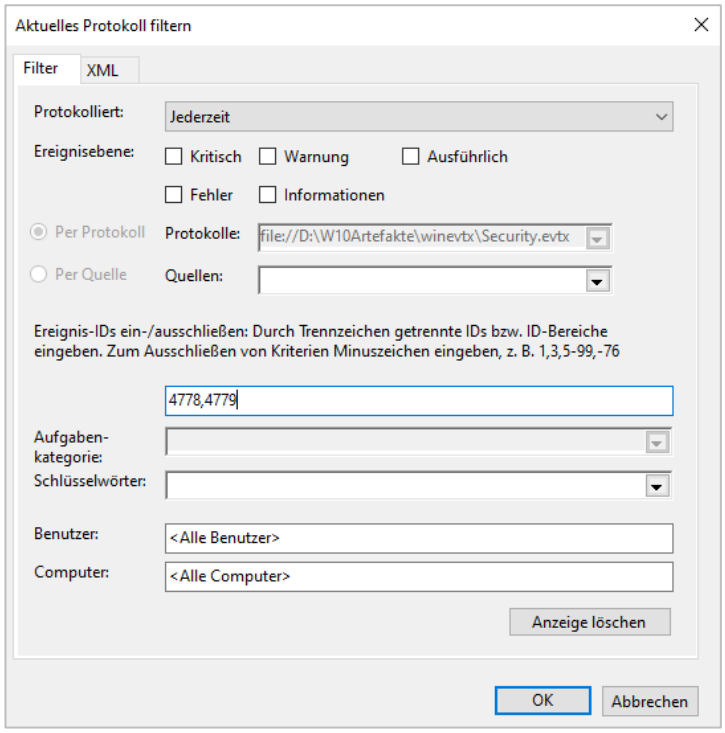
Öffnen Sie das **Security** Log aus dem Verzeichnis **CD-Laufwerk:\W10Artefakte\winevtx-advanced.**

Dieses Log beinhaltet eine aufgezeichnete RDP-Session auf ein lokales System.





Filtern Sie die Event-ID 4778 und 4779 heraus.

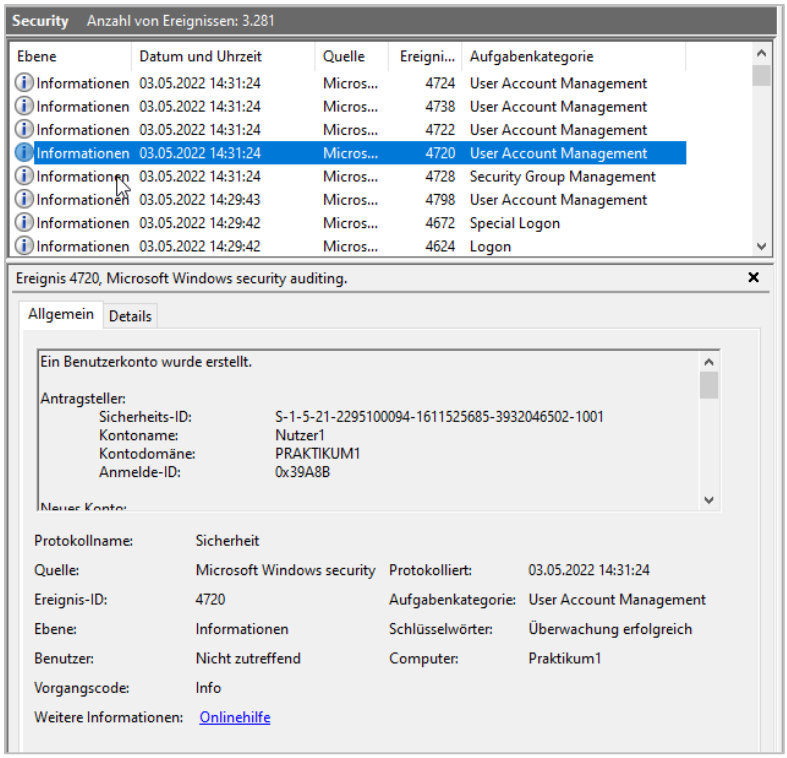


- Finden Sie hier Events mit der Eintragung 4778 oder 4779, wenn nicht recherchieren Sie im Internet was diese Event ID auszeichnen?

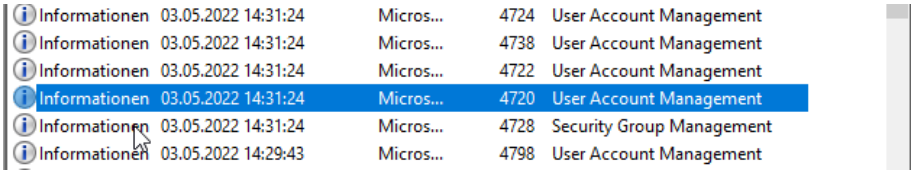
Warum fehlen diese Events: Die Event-ID 4778 und 4779 werden nur auf Terminal/RDP Server aufgezeichnet, nicht jedoch auf lokalen Systemen wo RDP aktiviert wurde.

Nutzer1 Anmeldung per RDP und Anlegen eines Nutzers – Event-ID 4720

Filtern Sie die Event-ID 4720 heraus oder Suchen Sie den einzelnen Events heraus.

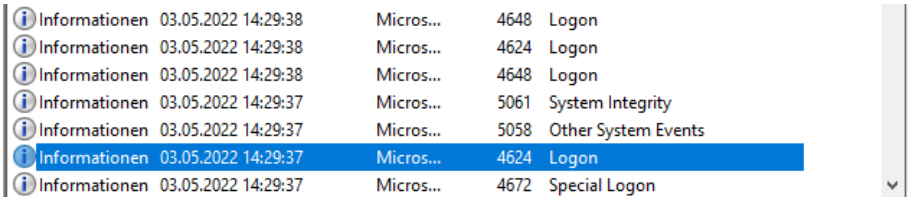


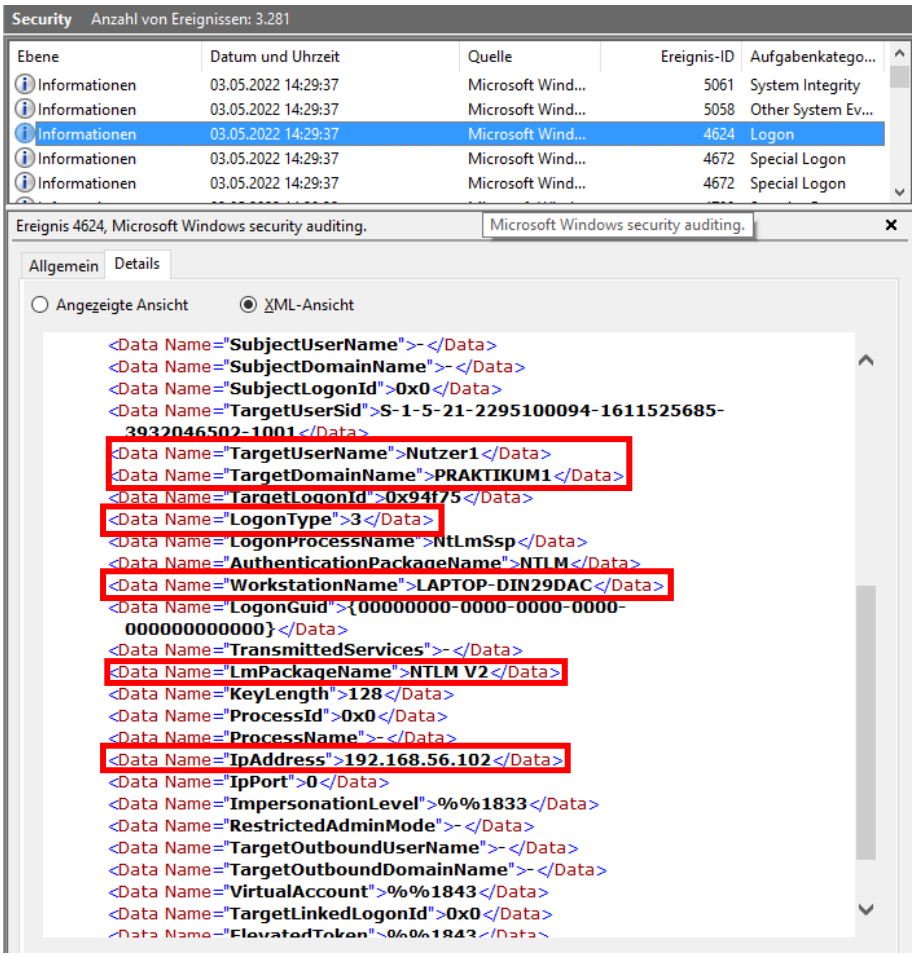
Welche Events erfolgten im Zusammenhang mit dieser Account Erstellung?



Antwort: Gruppen-Änderungen und Gruppenzugehörigkeit Auflisten/Überprüfen.

Welche Netzwerkinformationen für das RDP-Login können Sie ermitteln?





Logon Typen - Interpretation

- 2 Logon via console
- 3 Network Logon
- 4 Batch Logon
- 5 Windows Service Logon
- 7 Credentials used to unlock screen
- 8 Network logon sending credentials (cleartext)
- 9 Different credentials used than logged on user
- 10 Remote interactive logon (RDP)
- 11 Cached credentials used to logon
- 12 Cached remote interactive (similar

- Warum finden Sie einen Logon Typ 3 statt RDP Logon Typ 10 vor?

Recherchieren Sie im Internet, warum dieser Logon Typ 3 statt 10 ist.

Antwort: „Most RDP sessions show up as logon type 3 due to the default configuration of making use of NLA (Network Layer Authentication) as the authentication type since it will try and pre-authenticate you prior to giving you RDP access. RDP authentication and encryption levels need to be specifically configured to log type10 events, and its worth doing as it provides better log forensic information and it allows noise reduction of ascertaining the difference between all the other network logon type 3 events for activities such as network printing, fileshare access, access to exchange etc. “

"Die meisten RDP-Sitzungen werden als Anmeldetyp 3 angezeigt, da in der Standardkonfiguration NLA (Network Layer Authentication) als Authentifizierungstyp verwendet wird, der versucht, Sie vor dem RDP-Zugriff zu authentifizieren. Die RDP-Authentifizierungs- und Verschlüsselungsebenen müssen speziell für die Protokollierung von Ereignissen des Typs 10 konfiguriert werden. Es lohnt sich, dies zu tun, da es bessere forensische Informationen liefert und eine Rauschunterdrückung ermöglicht, um den Unterschied zwischen allen anderen Netzwerkanmeldungsereignissen des Typs 3 für Aktivitäten wie Netzwerkdruck, Dateifreigabezugriff, Zugriff auf Exchange usw. festzustellen."