

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**.

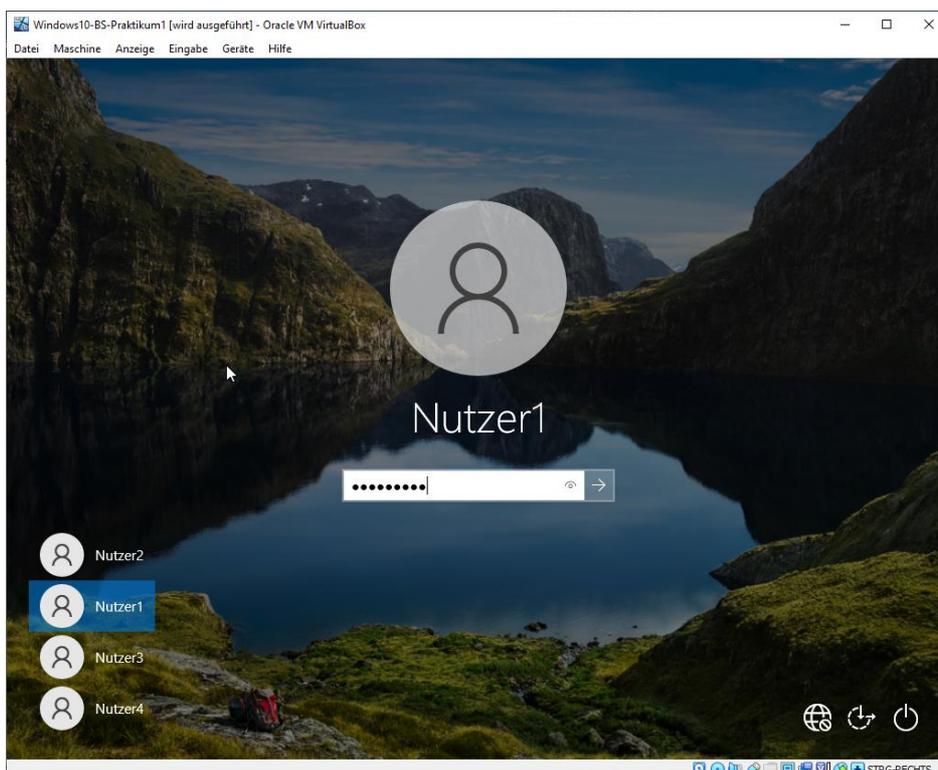
Allgemeine Hinweise

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.

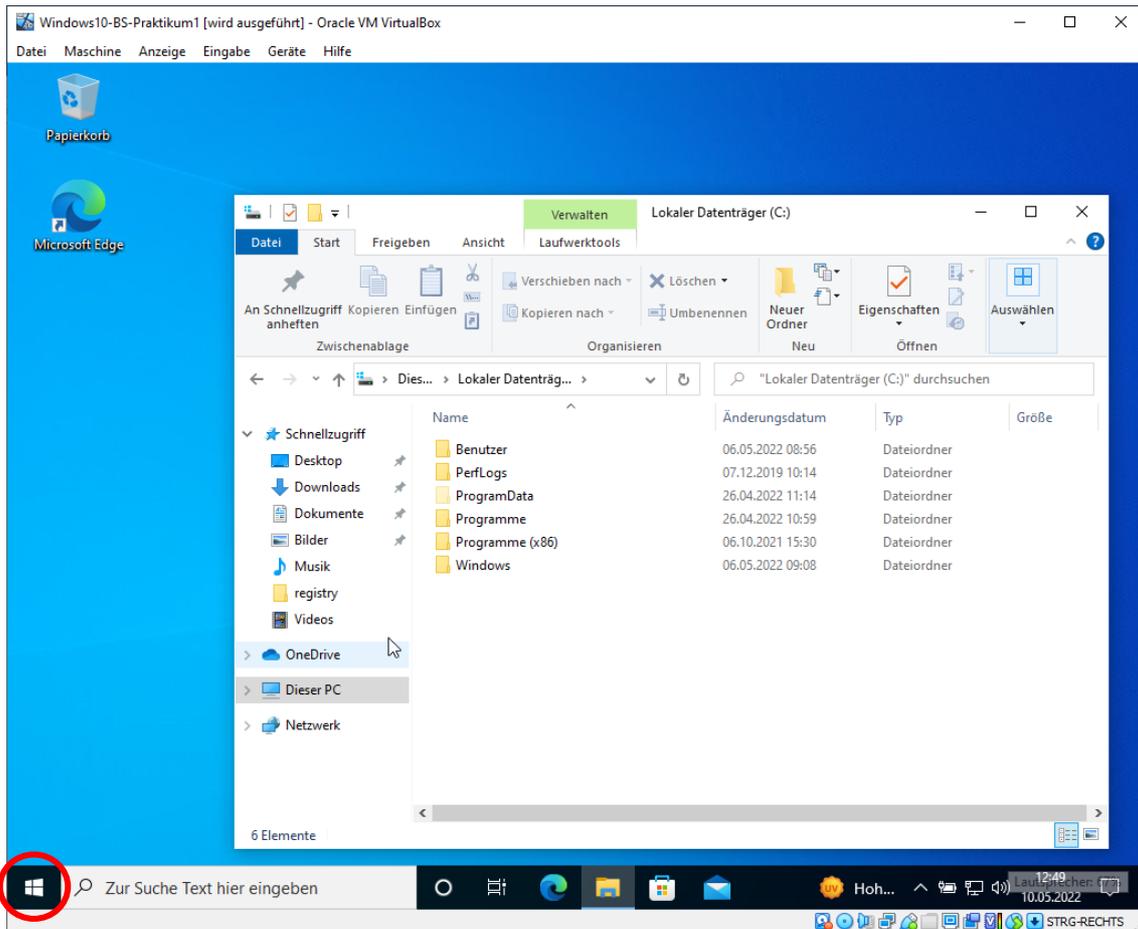
EFS-Verschlüsselung anlegen

Öffnen Sie Virtualbox und starten Sie die VM.

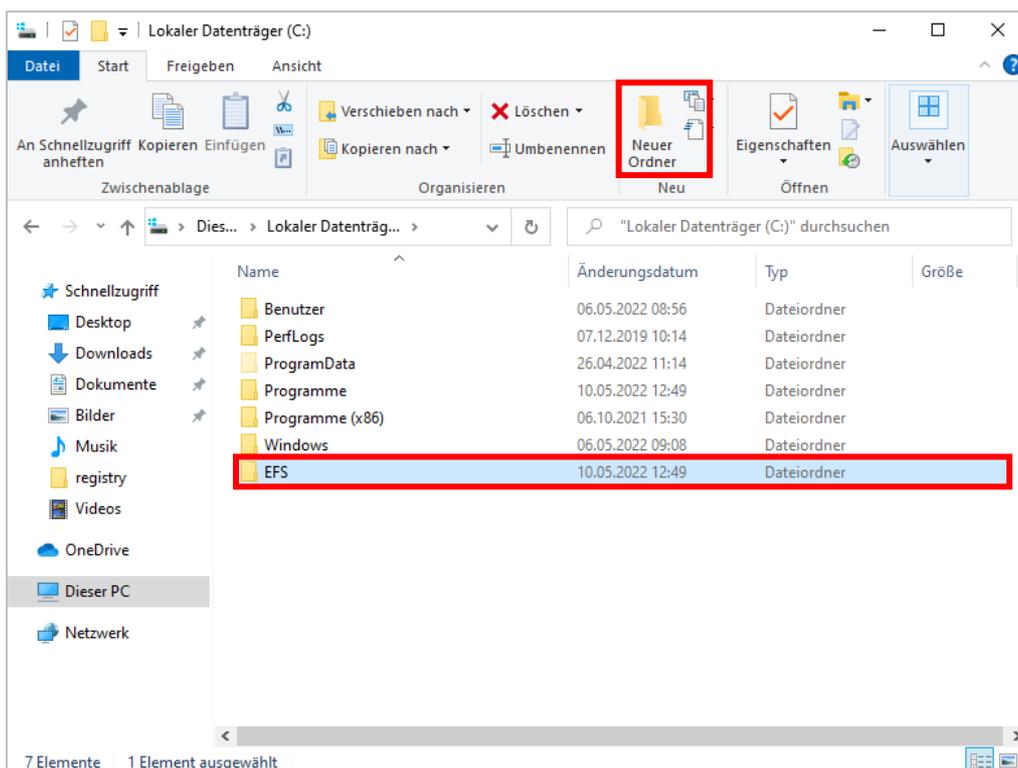
- Loggen Sie sich als **Nutzer1** mit **Kennwort1** ein



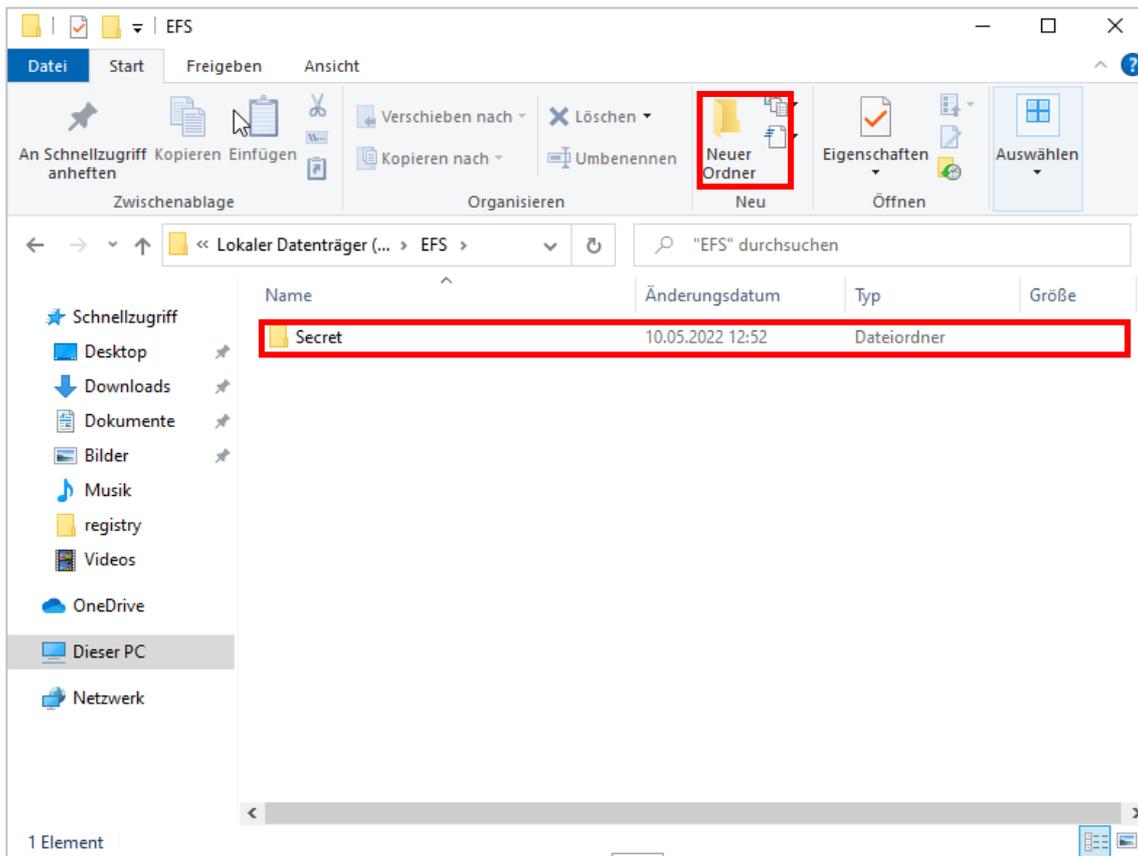
- **Öffnen** Sie im Schritt 2 den **Windows Explorer** und gehen Sie auf **Laufwerk C:**



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

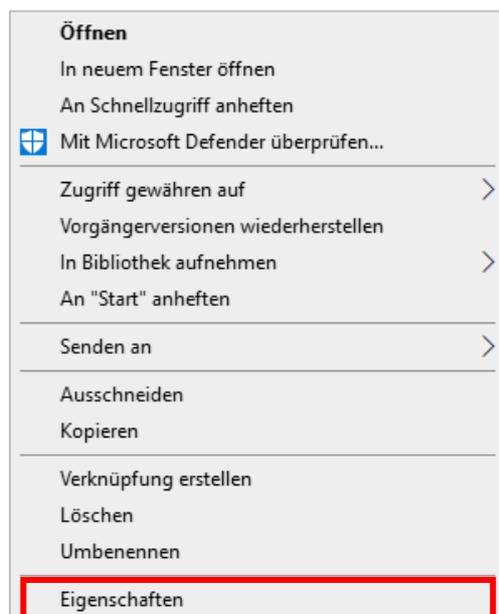


- **Erstellen** Sie innerhalb des Verzeichnis EFS ein weiteres **Unterverzeichnis „Secret“** auf gleichem Weg

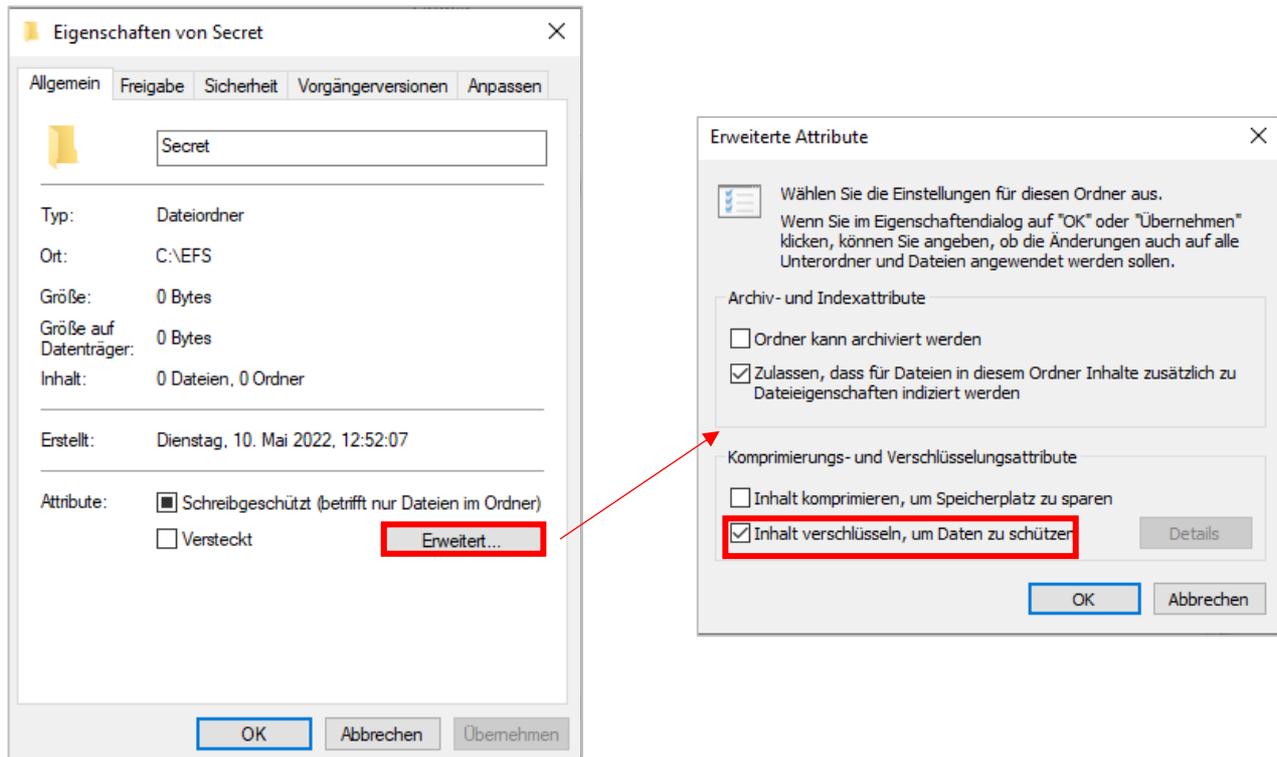


Verzeichnis bearbeiten:

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



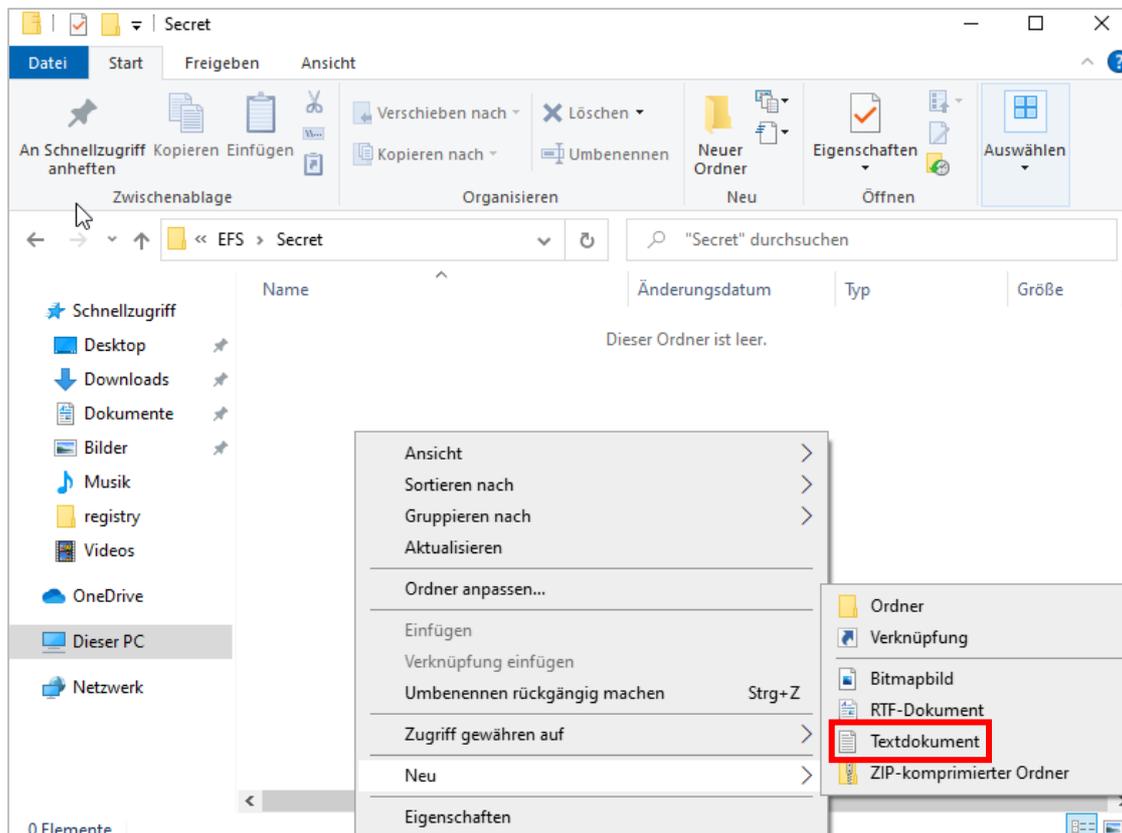
- Wählen Sie „Erweitert“ aus und aktivieren Sie „Inhalt verschlüsseln, um Daten zu schützen“



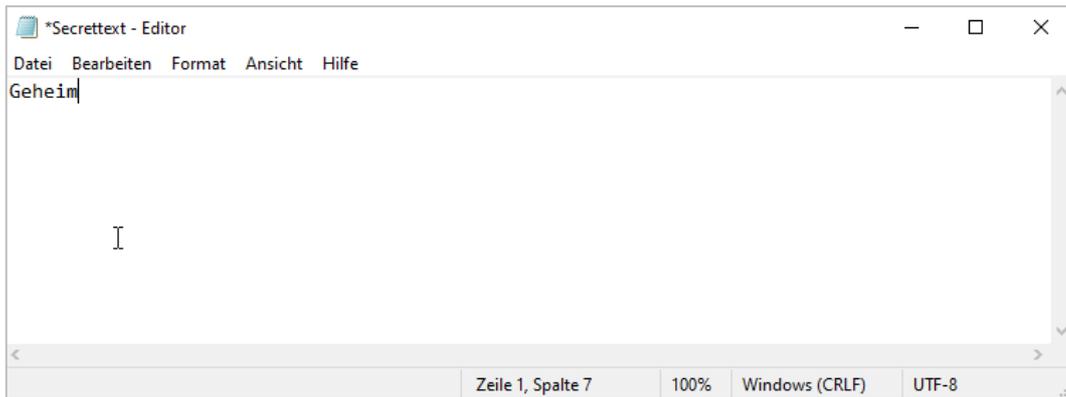
- Bestätigen Sie jeden Dialog mit OK

Verschlüsselte Datei erstellen:

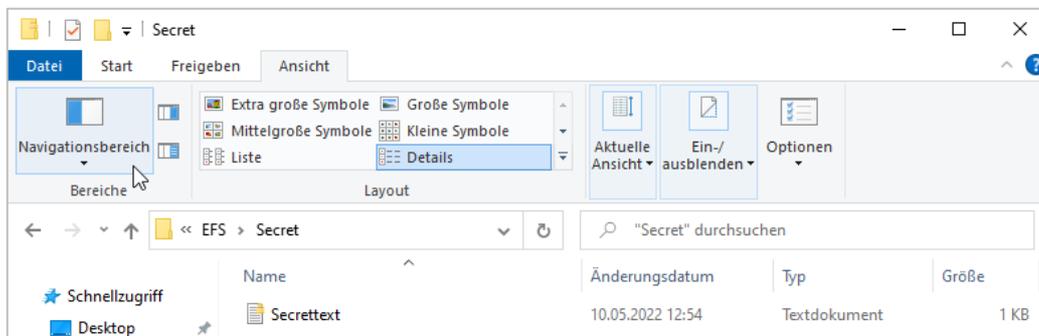
- Erstellen Sie im Verzeichnis „Secret“ eine Textdatei (Rechtsklick > Neu > Textdokument) und Benennen Sie es „Secrettext“



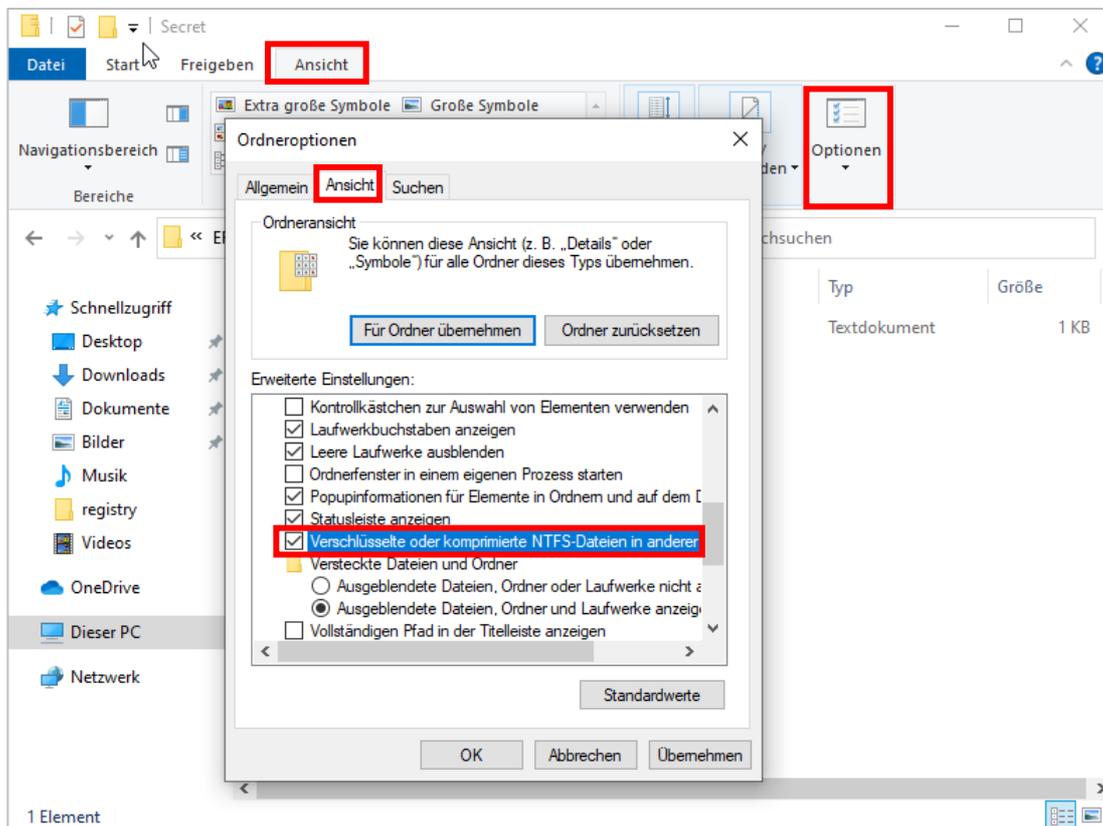
- Tragen Sie in diese Datei einen Geheimen Text hinein und Speichern Sie das Dokument ab



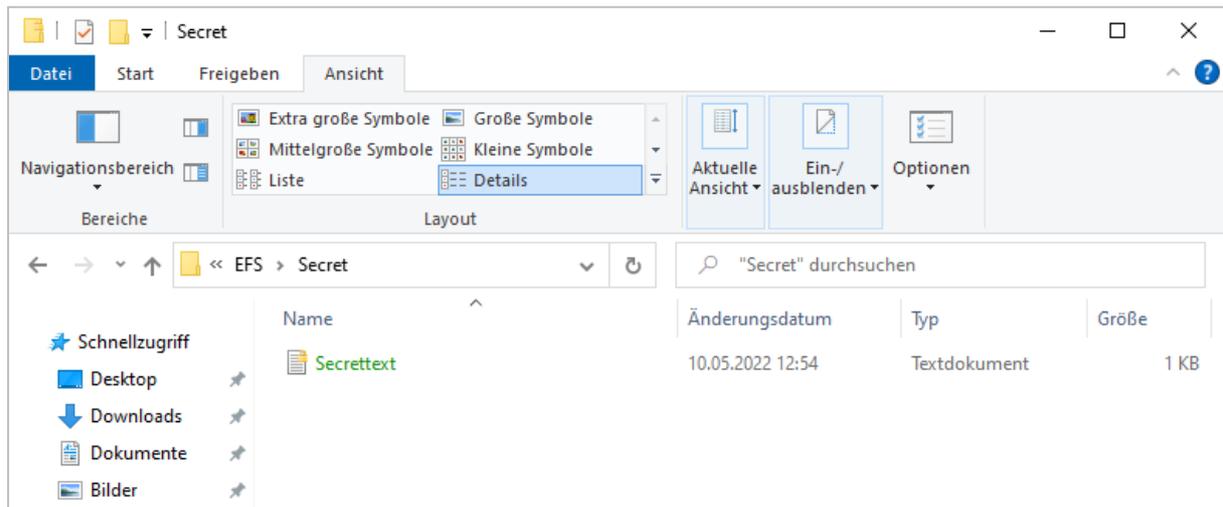
Ansicht anpassen:



- 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

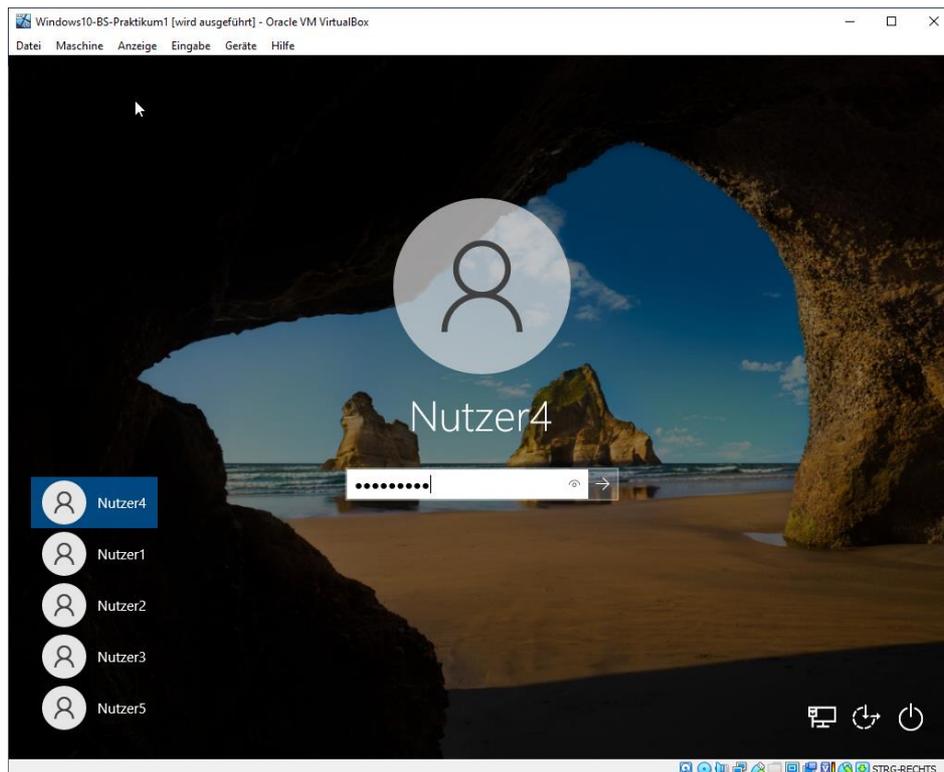


➤ Wie sieht die Ansicht jetzt aus?



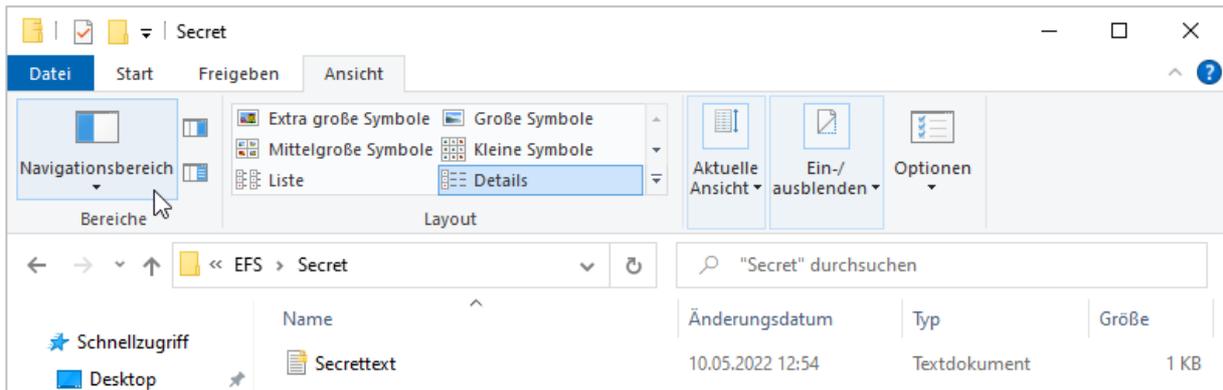
EFS-Verschlüsselung auf anderen Nutzer übertragen

Melden Sie sich von Nutzer1 aus, als Nutzer4 an.

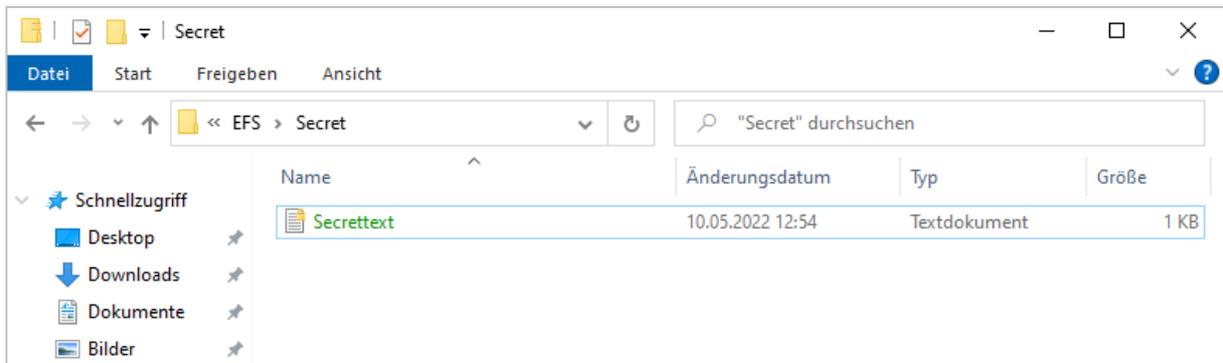


Verschlüsselte Datei von Aufgabe 1.1 Öffnen:

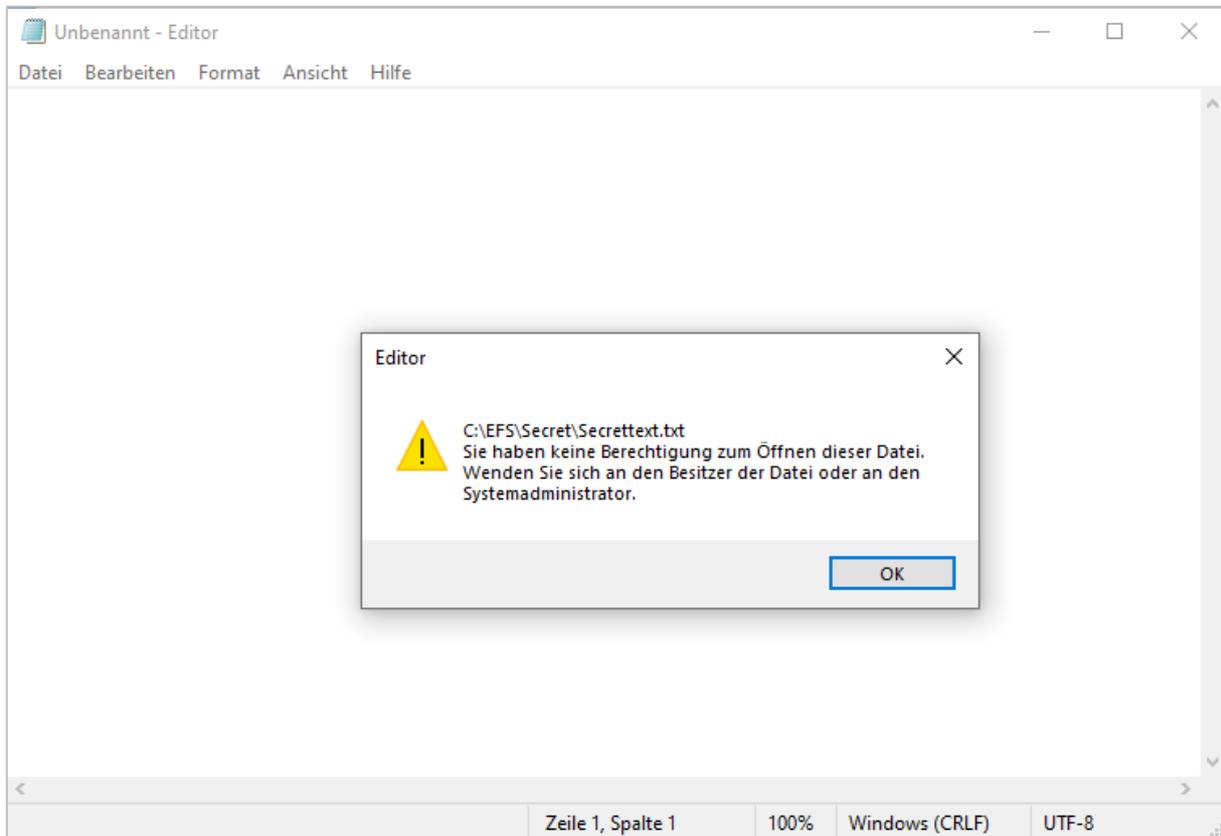
➤ Öffnen Sie den Windows Explorer und Wechseln Sie in das Verzeichnis „C:\EFS\Secret“



- Stellen Sie auch hier die Ansicht um auf „EINFÄRBE“

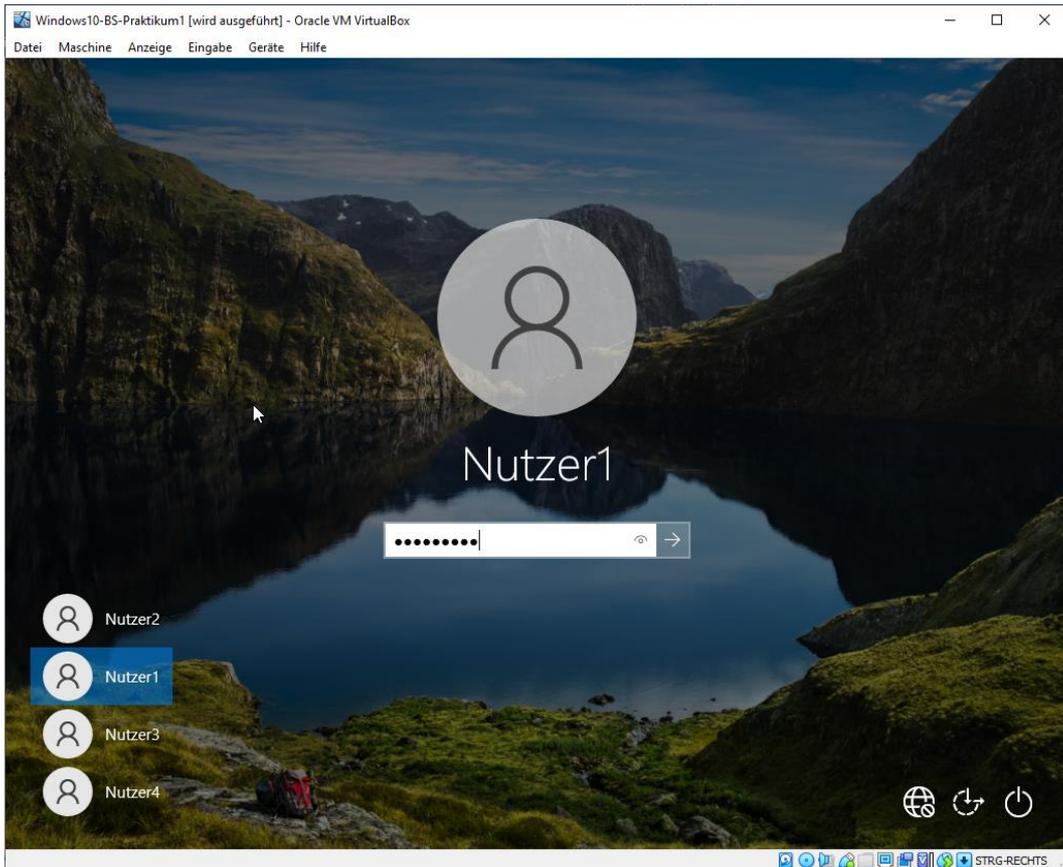


- Öffnen Sie die Datei Secrettext
- Hat dies funktioniert?

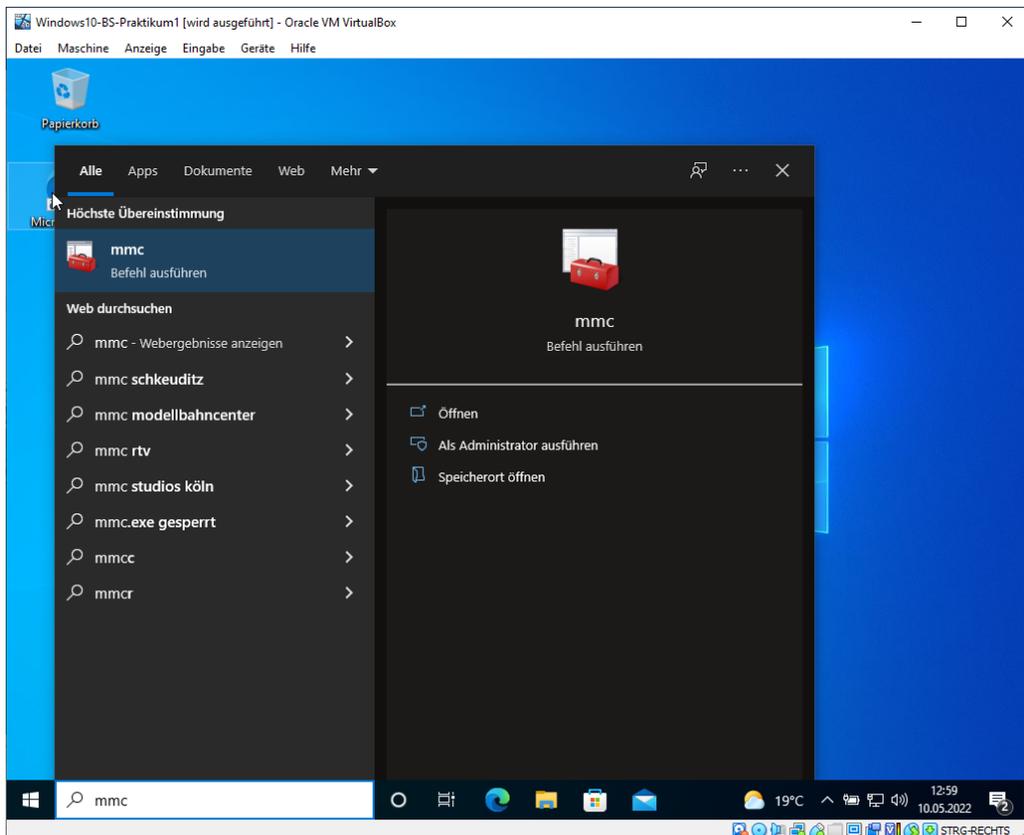


Datei lesbar machen in fremden Nutzerkontext:

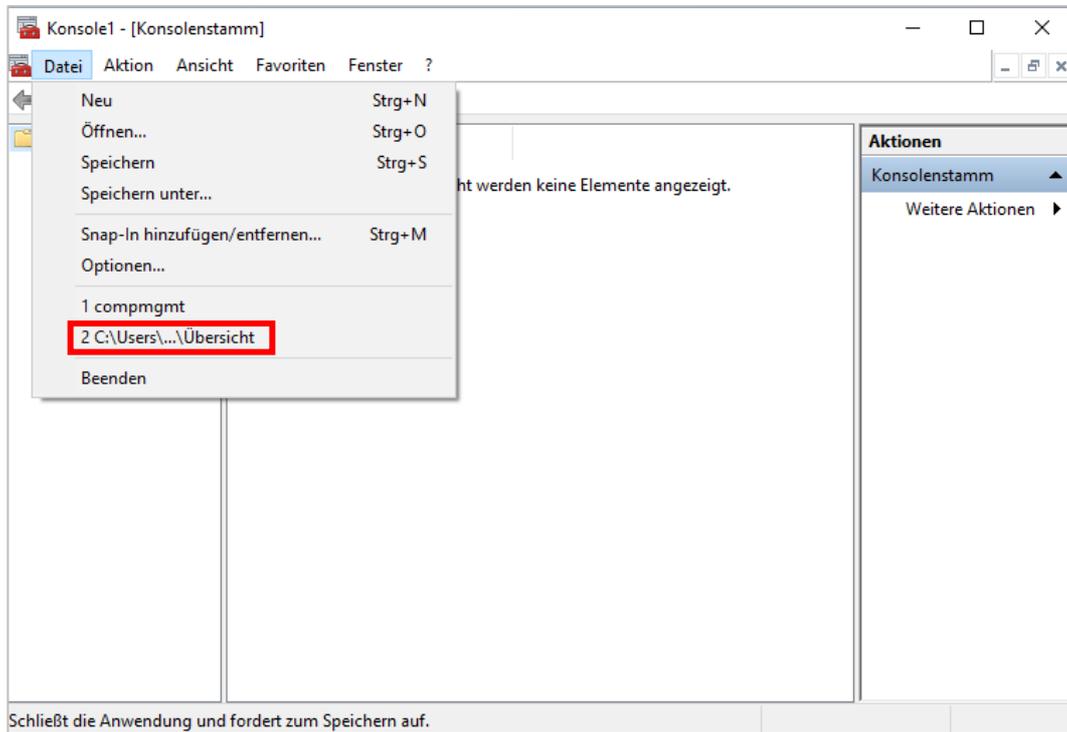
- Melden Sie sich wieder als Nutzer 1 an



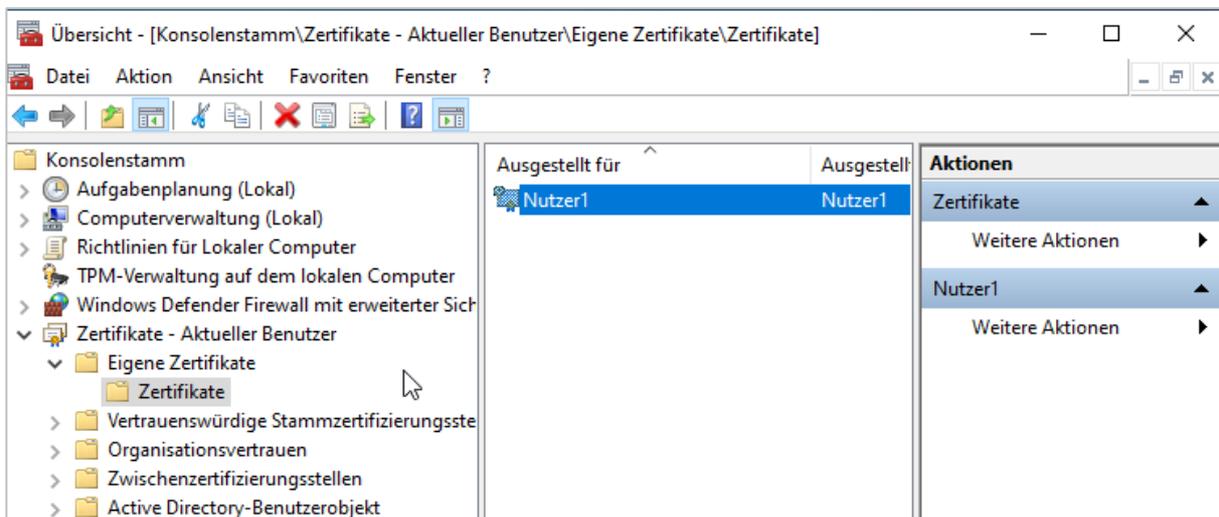
- Öffnen Sie die MMC über den Windows Start Button (MMC)



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

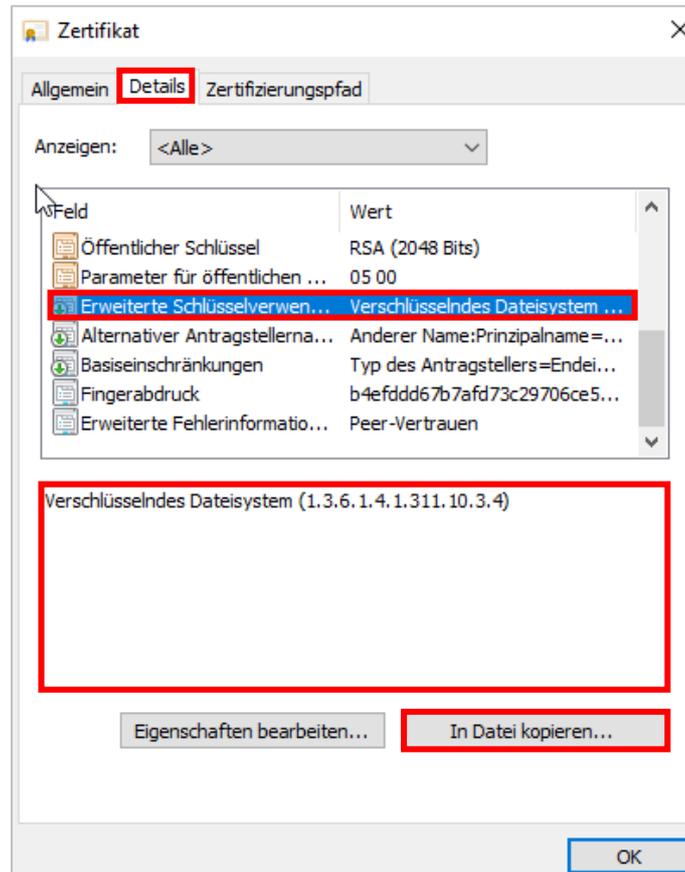


- Wählen Sie unter Zertifikate „Eigene Zertifikate“ aus

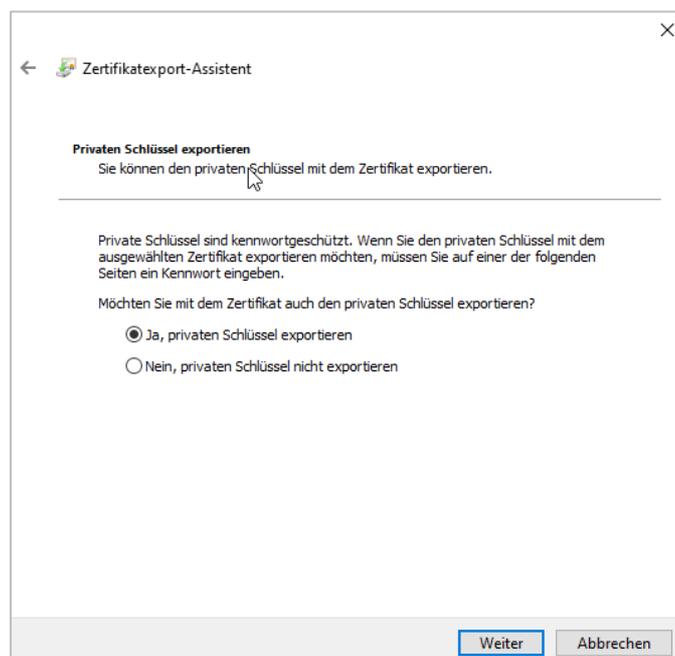


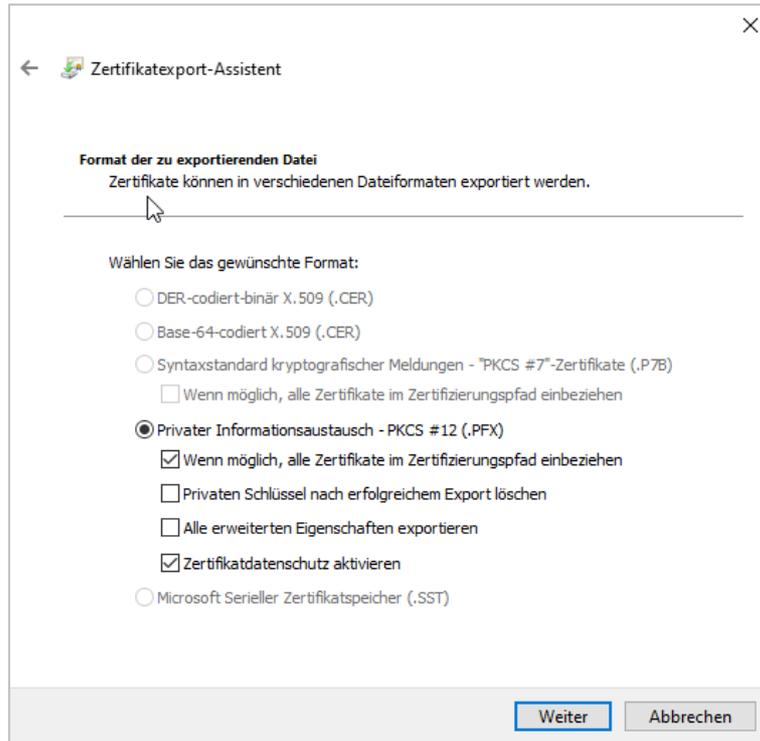
Zertifikat exportieren:

- 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)!

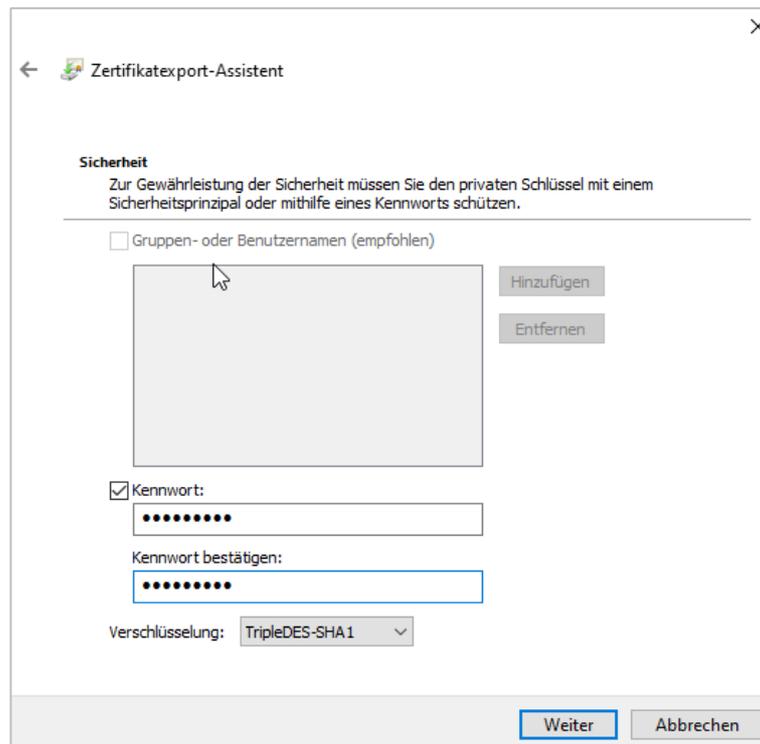


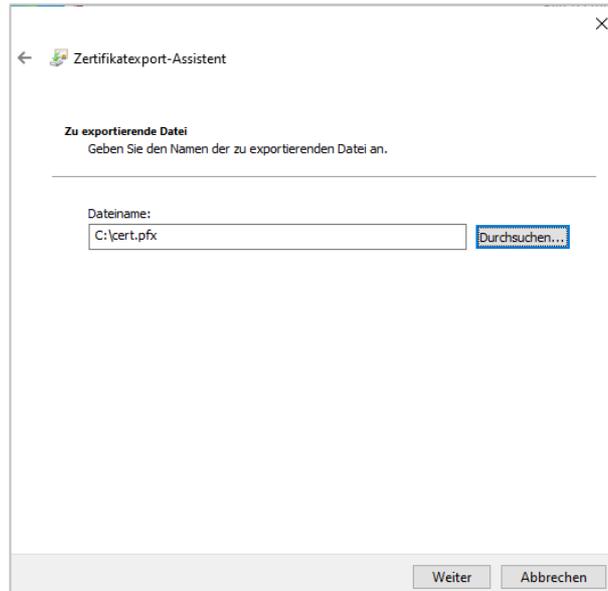
- Exportieren Sie das Zertifikat mit privatem Schlüssel!





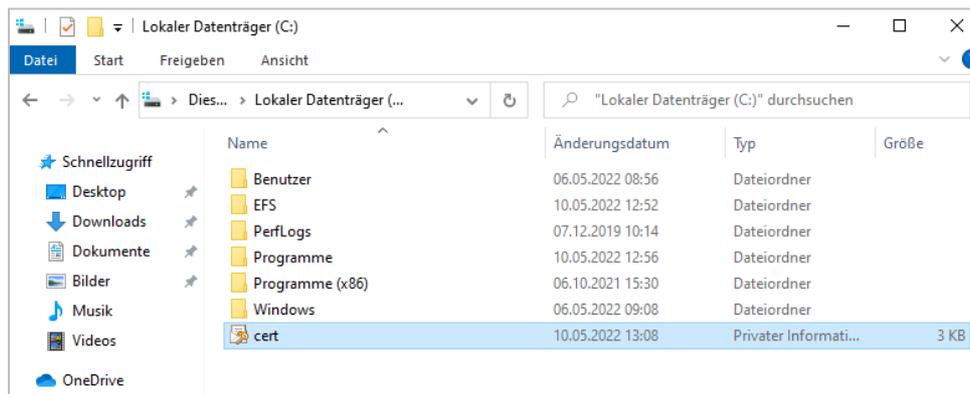
- Vergeben Sie ein Kennwort (Kennwort1) und speichern sie das Zertifikat als Cert.pfx auf Laufwerk C:\



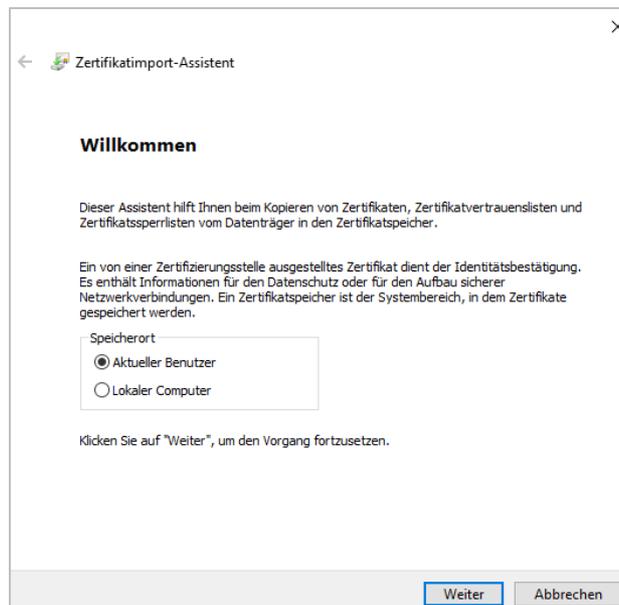


Zertifikat importieren:

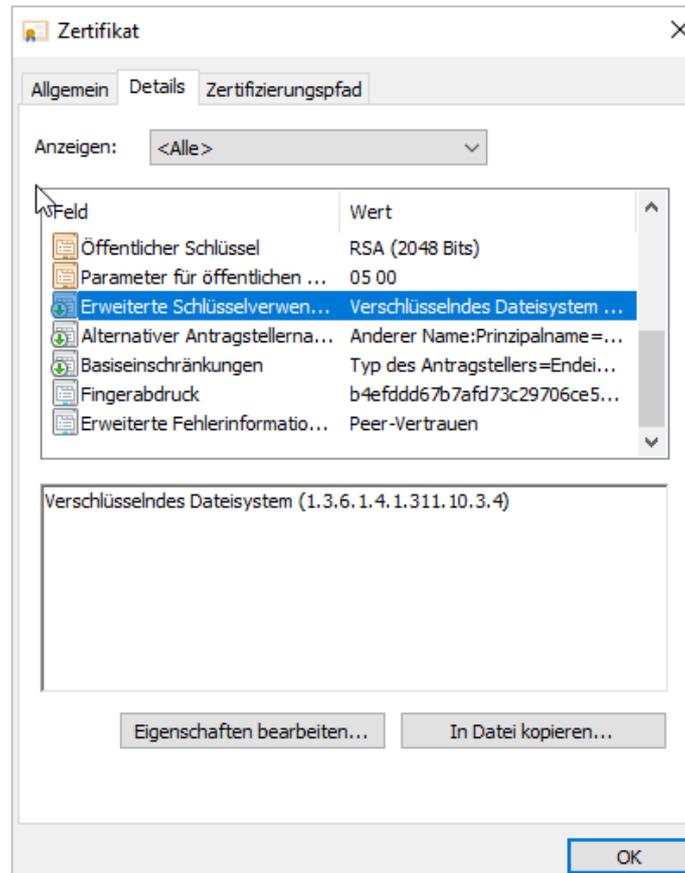
- Nach dem Speichern des Zertifikats melden Sie sich bitte als Nutzer 1 ab und als Nutzer 4 wieder an
- Öffnen Sie den Windows Explorer auf Laufwerk C:\ und Öffnen Sie die Datei Cert.pfx



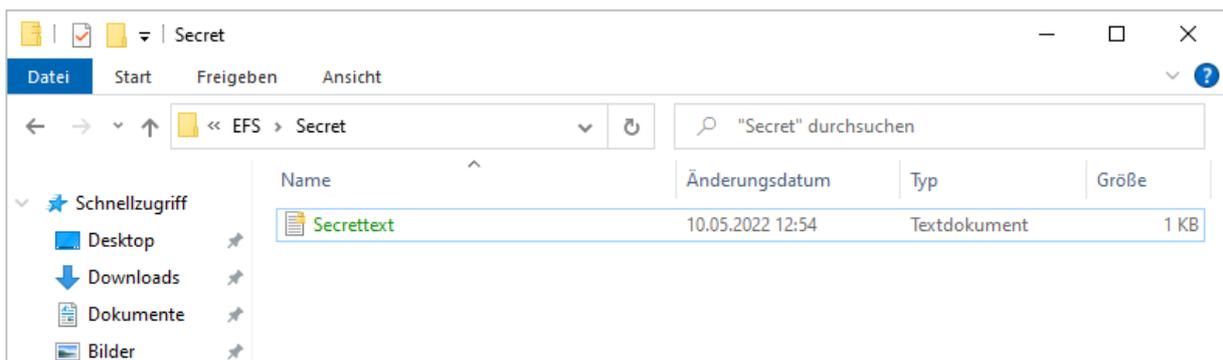
- Importieren Sie das Zertifikat für den aktuellen Benutzer



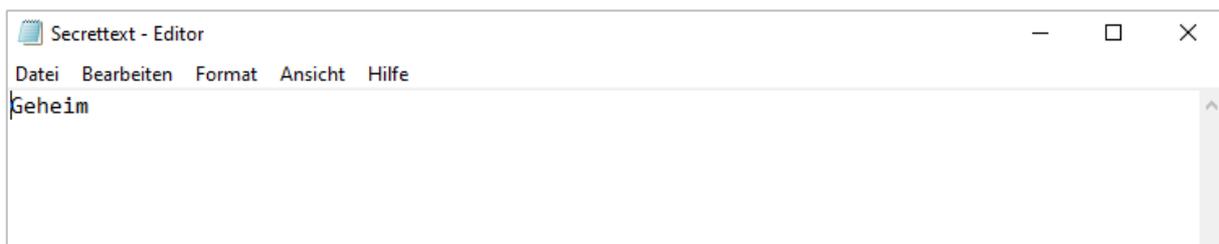
- Überprüfen Sie beim Import die Erweiterte Schlüsselverwendung und Bestätigen Sie alle folgenden Dialoge mit OK



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



- Hat dies funktioniert?

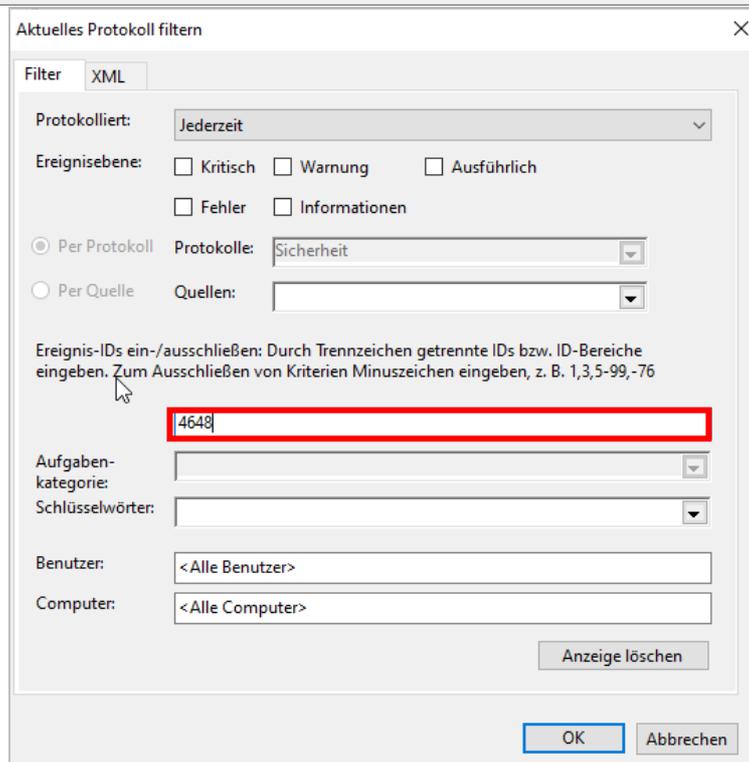
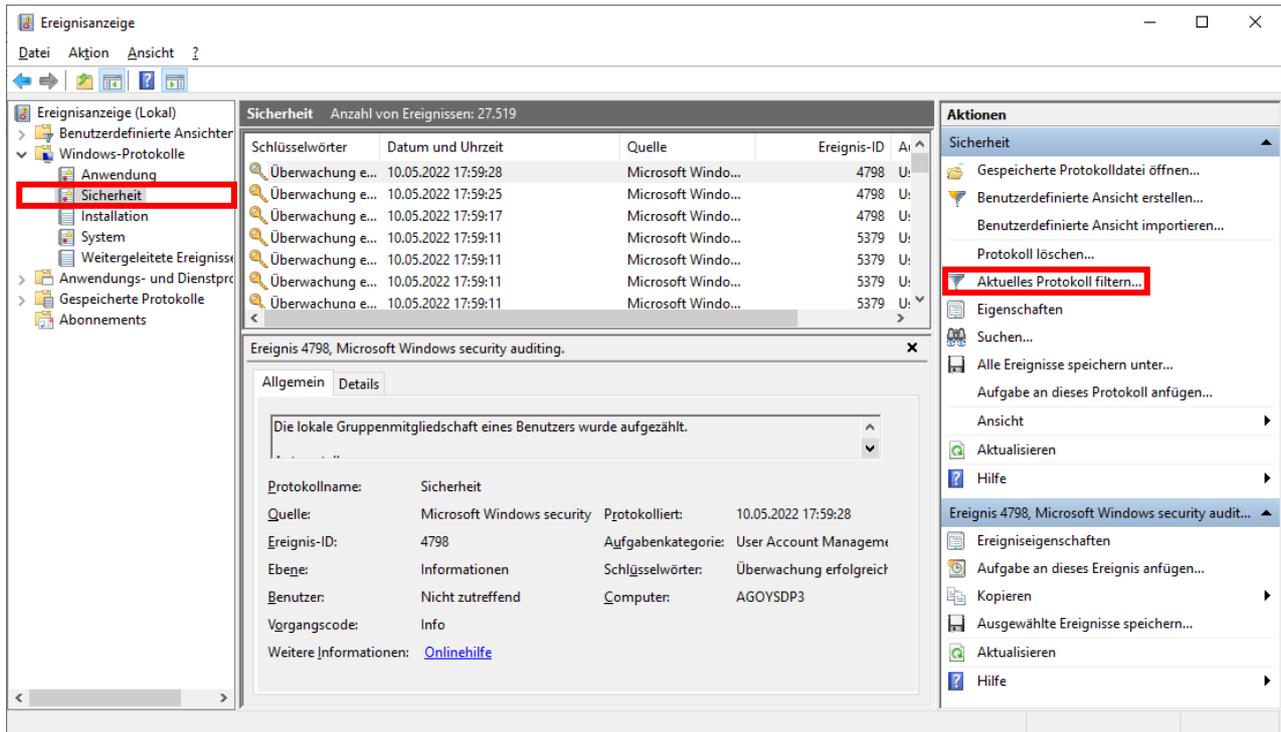


Eventlog auf Anmeldungen überprüfen

Unter der Nutzererkennung 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.



Schlüsselw...	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenka...
Überwac...	10.05.2022 08:39:33	Microsoft ...	4648	Logon
Überwac...	10.05.2022 08:39:33	Microsoft ...	4648	Logon
Überwac...	10.05.2022 08:39:33	Microsoft ...	4648	Logon
Überwac...	06.05.2022 08:56:00	Microsoft ...	4648	Logon
Überwac...	06.05.2022 08:42:26	Microsoft ...	4648	Logon
Überwac...	06.05.2022 08:42:17	Microsoft ...	4648	Logon
Überwac...	06.05.2022 08:42:17	Microsoft ...	4648	Logon
Überwac...	06.05.2022 08:40:28	Microsoft ...	4648	Logon
Überwac...	06.05.2022 08:40:00	Microsoft ...	4648	Logon
Überwac...	06.05.2022 08:40:00	Microsoft ...	4648	Logon
Überwac...	06.05.2022 08:32:26	Microsoft ...	4648	Logon

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

Schlüsselw...	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenka...
Überwac...	06.05.2022 08:56:00	Microsoft ...	4648	Logon
Überwac...	06.05.2022 08:42:26	Microsoft ...	4648	Logon

Ereignis 4648, Microsoft Windows security auditing.

Allgemein Details

Anmeldeversuch mit expliziten Anmeldeinformationen.

Antragsteller:

Sicherheits-ID:	DESKTOP-SHT7U5V\Nutzer1
Kontoname:	Nutzer1
Kontodomäne:	DESKTOP-SHT7U5V
Anmelde-ID:	0x4DEFC
Anmelde-GUID:	{00000000-0000-0000-0000-000000000000}

Konto, dessen Anmeldeinformationen verwendet wurden:

Kontoname:	Nutzer3
Kontodomäne:	DESKTOP-SHT7U5V
Anmelde-GUID:	{00000000-0000-0000-0000-000000000000}

Zielserver:

Protokollname:	Sicherheit		
Quelle:	Microsoft Windows security	Protokolliert:	06.05.2022 08:56:00
Ereignis-ID:	4648	Aufgabenkategorie:	Logon
Ebene:	Informationen	Schlüsselwörter:	Überwachung erfolgreich
Benutzer:	Nicht zutreffend	Computer:	DESKTOP-SHT7U5V
Vorgangscod:	Info		
Weitere Informationen:	Onlinehilfe		

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

Aktuelles Protokoll filtern

Filter XML

Protokolliert: Jederzeit

Ereignisebene: Kritisch Warnung Ausführlich
 Fehler Informationen

Per Protokoll Protokolle: Sicherheit

Per Quelle Quellen:

Ereignis-IDs ein-/ausschließen: Durch Trennzeichen getrennte IDs bzw. ID-Bereiche eingeben. Zum Ausschließen von Kriterien Minuszeichen eingeben, z. B. 1,3,5-99,-76

4648,4624

Aufgabenkategorie:

Schlüsselwörter:

Benutzer: <Alle Benutzer>

Computer: <Alle Computer>

Anzeige löschen

OK Abbrechen

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

Gefiltert: Protokoll: Security; Quelle: ; Ereignis-ID: 4648,4624 Anzahl der Ereignisse: 593

Schlüsselw...	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenka...
Überwac...	06.05.2022 08:56:00	Microsoft ...	4624	Logon
Überwac...	06.05.2022 08:56:00	Microsoft ...	4648	Logon

Ereignis 4624, Microsoft Windows security auditing.

Allgemein Details

Ein Konto wurde erfolgreich angemeldet.

Antragsteller:

Sicherheits-ID: DESKTOP-SHT7U5V\Nutzer1
Kontoname: Nutzer1
Kontodomäne: DESKTOP-SHT7U5V
Anmelde-ID: 0x4DEFC

Anmeldeinformationen:

Anmeldetyp: 2
Eingeschränkter Administratormodus: -
Virtuelles Konto: Nein
Token mit erhöhten Rechten: Ja

Identitätswechselebene: Identitätswechsel

Protokollname: Sicherheit
Quelle: Microsoft Windows security
Ereignis-ID: 4624
Ebene: Informationen
Benutzer: Nicht zutreffend
Vorgangscod: Info
Weitere Informationen: [Onlinehilfe](#)

Protokolliert: 06.05.2022 08:56:00
Aufgabenkategorie: Logon
Schlüsselwörter: Überwachung erfolgreich
Computer: DESKTOP-SHT7U5V

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)

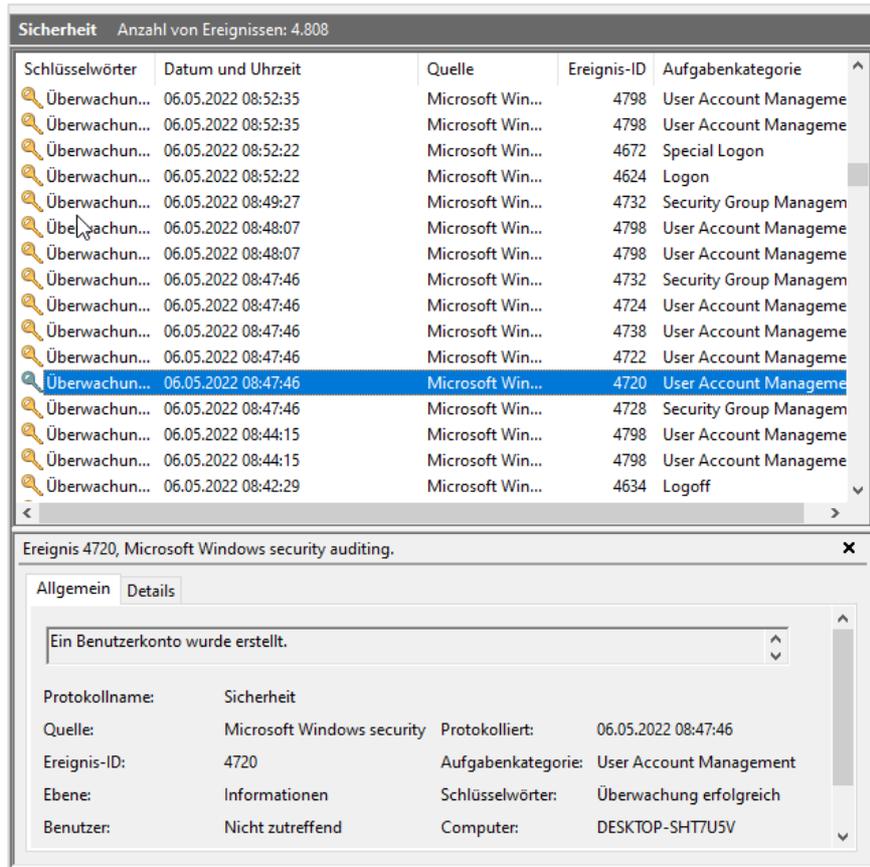
Prüfen Sie hierbei auch einmal die XML-Ansicht.

```

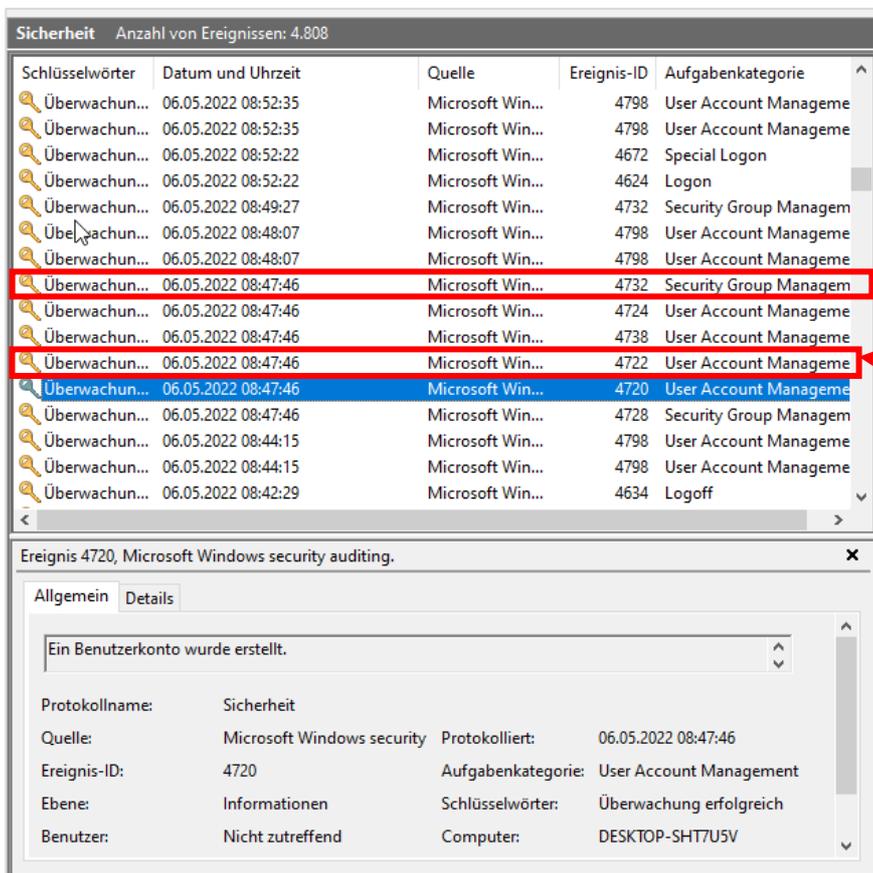
<Execution ProcessID="580" ThreadID="7004" />
<Channel>Security</Channel>
<Computer>DESKTOP-SHT7U5V</Computer>
<Security />
</System>
- <EventData>
  <Data Name="SubjectUserSid">S-1-5-21-2739844660-4112662628-2105119028-1001</Data>
  <Data Name="SubjectUserName">Nutzer1</Data>
  <Data Name="SubjectDomainName">DESKTOP-SHT7U5V</Data>
  <Data Name="SubjectLogonId">0x4defc</Data>
  <Data Name="TargetUserSid">S-1-5-21-2739844660-4112662628-2105119028-1003</Data>
  <Data Name="TargetUserName">Nutzer3</Data>
  <Data Name="TargetDomainName">DESKTOP-SHT7U5V</Data>
  <Data Name="TargetLogonId">0xec90c2</Data>
  <Data Name="LogonType">2</Data>
  <Data Name="LogonProcessName">seclogo</Data>
  <Data Name="AuthenticationPackageName">Negotiate</Data>
  <Data Name="WorkstationName">DESKTOP-
  
```

Account Creation Event-ID 4720

Schauen Sie, wann Nutzer 5 hinzugefügt wurde.



Welche Events erfolgten danach?



Hinzufügen zu Gruppen

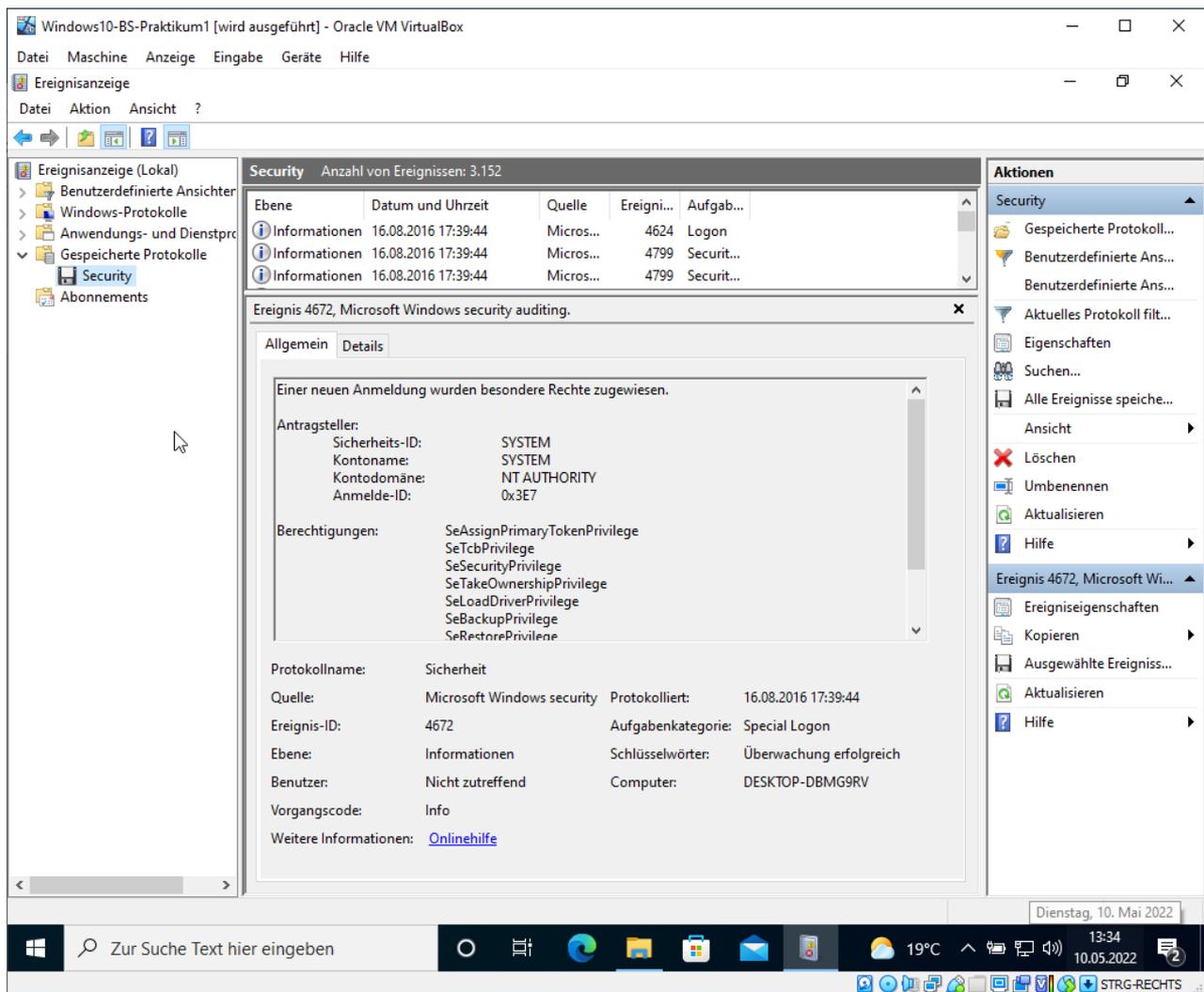
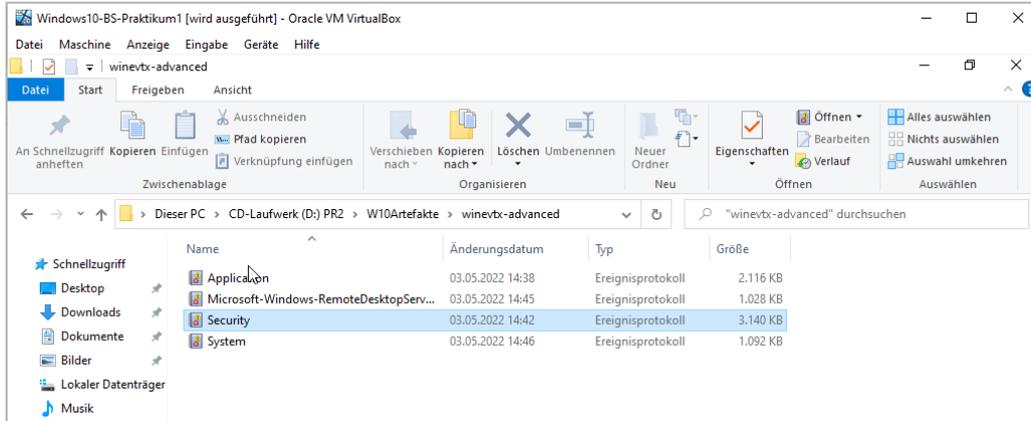
Auflisten von Gruppen und Überprüfung der Zugehörigkeit

RDP-Login aus PR2.iso

Event-ID 4778, 4779 RDP-Nutzung

Öffnen Sie das **Security** Log aus dem Verzeichnis **CD-Laufwerk (D:) PR2 > W10Artefakte\winevtx-advanced**.

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



Filtern Sie die Event-ID 4778 und 4779 heraus.

Aktuelles Protokoll filtern

Filter XML

Protokolliert: Jederzeit

Ereignisebene: Kritisch Warnung Ausführlich
 Fehler Informationen

Per Protokoll Protokolle: file://D:\W10Artefakte\winevt\Security.evtx
 Per Quelle Quellen:

Ereignis-IDs ein-/ausschließen: Durch Trennzeichen getrennte IDs bzw. ID-Bereiche eingeben. Zum Ausschließen von Kriterien Minuszeichen eingeben, z. B. 1,3,5-99,-76

4778,4779

Aufgabenkategorie:
Schlüsselwörter:

Benutzer: <Alle Benutzer>
Computer: <Alle Computer>

Anzeige löschen

OK Abbrechen

- 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.

Security Anzahl von Ereignissen: 3.281

Ebene	Datum und Uhrzeit	Quelle	Ereigni...	Aufgabenkategorie
Informationen	03.05.2022 14:31:24	Micros...	4724	User Account Management
Informationen	03.05.2022 14:31:24	Micros...	4738	User Account Management
Informationen	03.05.2022 14:31:24	Micros...	4722	User Account Management
Informationen	03.05.2022 14:31:24	Micros...	4720	User Account Management
Informationen	03.05.2022 14:31:24	Micros...	4728	Security Group Management
Informationen	03.05.2022 14:29:43	Micros...	4798	User Account Management
Informationen	03.05.2022 14:29:42	Micros...	4672	Special Logon
Informationen	03.05.2022 14:29:42	Micros...	4624	Logon

Ereignis 4720, Microsoft Windows security auditing.

Allgemein Details

Ein Benutzerkonto wurde erstellt.

Antragsteller:
Sicherheits-ID: S-1-5-21-2295100094-1611525685-3932046502-1001
Kontoname: Nutzer1
Kontodomäne: PRAKTIKUM1
Anmelde-ID: 0x39A8B

Neuer Konto:

Protokollname: Sicherheit
Quelle: Microsoft Windows security Protokolliert: 03.05.2022 14:31:24
Ereignis-ID: 4720 Aufgabenkategorie: User Account Management
Ebene: Informationen Schlüsselwörter: Überwachung erfolgreich
Benutzer: Nicht zutreffend Computer: Praktikum1
Vorgangscod: Info
Weitere Informationen: [Onlinehilfe](#)

Welche Events erfolgten im Zusammenhang mit dieser Account Erstellung?

Informationen	03.05.2022 14:31:24	Micros...	4724	User Account Management
Informationen	03.05.2022 14:31:24	Micros...	4738	User Account Management
Informationen	03.05.2022 14:31:24	Micros...	4722	User Account Management
Informationen	03.05.2022 14:31:24	Micros...	4720	User Account Management
Informationen	03.05.2022 14:31:24	Micros...	4728	Security Group Management
Informationen	03.05.2022 14:29:43	Micros...	4798	User Account Management

Antwort: Gruppen-Änderungen und Gruppenzugehörigkeit Auflisten/Überprüfen.

Welche Netzwerkinformationen für das RDP-Login können Sie ermitteln?

Informationen	03.05.2022 14:29:38	Micros...	4648	Logon
Informationen	03.05.2022 14:29:38	Micros...	4624	Logon
Informationen	03.05.2022 14:29:38	Micros...	4648	Logon
Informationen	03.05.2022 14:29:37	Micros...	5061	System Integrity
Informationen	03.05.2022 14:29:37	Micros...	5058	Other System Events
Informationen	03.05.2022 14:29:37	Micros...	4624	Logon
Informationen	03.05.2022 14:29:37	Micros...	4672	Special Logon

Ebene	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkatego...
Informationen	03.05.2022 14:29:37	Microsoft Wind...	5061	System Integrity
Informationen	03.05.2022 14:29:37	Microsoft Wind...	5058	Other System Ev...
Informationen	03.05.2022 14:29:37	Microsoft Wind...	4624	Logon
Informationen	03.05.2022 14:29:37	Microsoft Wind...	4672	Special Logon
Informationen	03.05.2022 14:29:37	Microsoft Wind...	4672	Special Logon

Security Anzahl von Ereignissen: 3.281

Ereignis 4624, Microsoft Windows security auditing.

Microsoft Windows security auditing.

Allgemein Details

Angezeigte Ansicht XML-Ansicht

```

<Data Name="SubjectUserName">-</Data>
<Data Name="SubjectDomainName">-</Data>
<Data Name="SubjectLogonId">0x0</Data>
<Data Name="TargetUserSid">S-1-5-21-2295100094-1611525685-3932046502-1001</Data>
<Data Name="TargetUserName">Nutzer1</Data>
<Data Name="TargetDomainName">PRAKTIKUM1</Data>
<Data Name="TargetLogonId">0x94f75</Data>
<Data Name="LogonType">3</Data>
<Data Name="LogonProcessName">NtLmSsp</Data>
<Data Name="AuthenticationPackageName">NTLM</Data>
<Data Name="WorkstationName">LAPTOP-DIN29DAC</Data>
<Data Name="LogonGuid">{00000000-0000-0000-0000-000000000000}</Data>
<Data Name="TransmittedServices">-</Data>
<Data Name="LmPackageName">NTLM V2</Data>
<Data Name="KeyLength">128</Data>
<Data Name="ProcessId">0x0</Data>
<Data Name="ProcessName">-</Data>
<Data Name="IpAddress">192.168.56.102</Data>
<Data Name="IpPort">0</Data>
<Data Name="ImpersonationLevel">%%1833</Data>
<Data Name="RestrictedAdminMode">-</Data>
<Data Name="TargetOutboundUserName">-</Data>
<Data Name="TargetOutboundDomainName">-</Data>
<Data Name="VirtualAccount">%%1843</Data>
<Data Name="TargetLinkedLogonId">0x0</Data>
<Data Name="ElevatedToken">%%1843</Data>
    
```

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."