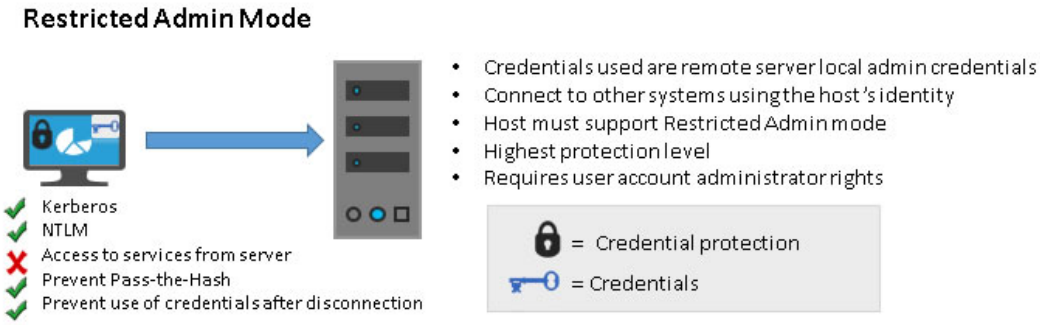
WDRCG – RDP Credential Guard

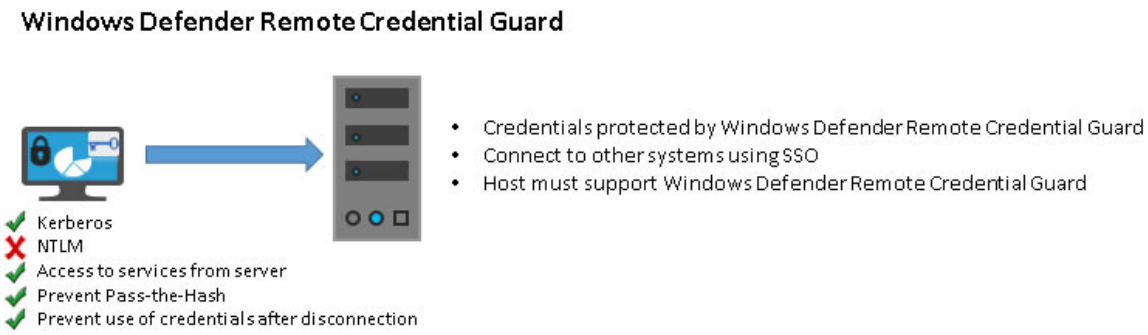
Beim Aufbau einer Remoteverbindung zu einem entfernten Host, werden die Anmeldedaten normalerweise über das Netzwerk an das Zielsystem übermittelt.

Angreifer können unter diesen Umständen mithilfe von PtH (Pass-the-Hash) die zwischengespeicherten Anmeldedaten weiterverwenden.

Das erste Bild zeigt den Restricted Admin Mode, der zur Aufgabe hat, privilegierte Anmeldedaten zu sichern. Dabei wird die Remote-Desktop-Verbindungs-Sitzung in eine lokale Admin-Sitzung umgeswitcht. Der Benutzer muss zur Nutzung von RAM der Gruppe der lokalen Administratoren, auf dem Zielsystem, angehören.



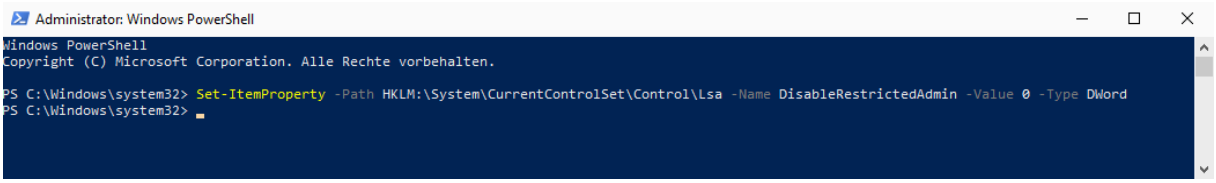
Bei der Nutzung des Windows Defender Remote Credential Guards, werden keine Anmeldedaten über das Netzwerk an das Zielsystem übermittelt. Die Anmeldung (Kerberos) erfolgt mittels Umleitung an den RDP-Client. Der Benutzer muss auf dem Zielsystem lediglich Mitglied der Gruppe Remotedesktopbenutzer sein.

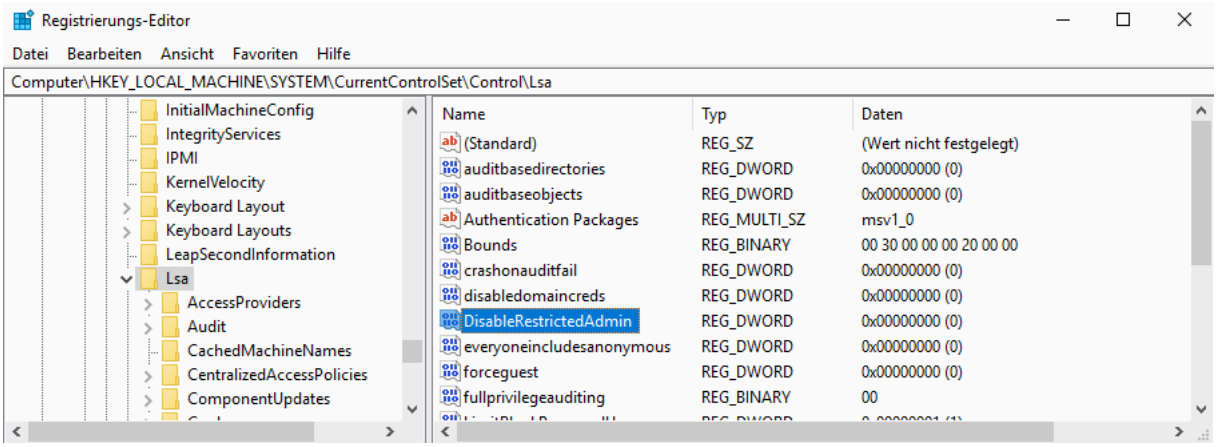


WDRCG – RDP Credential Guard

Damit WDRCG genutzt werden kann muss auf dem Zielsystem folgender Registry-Eintrag gesetzt werden.

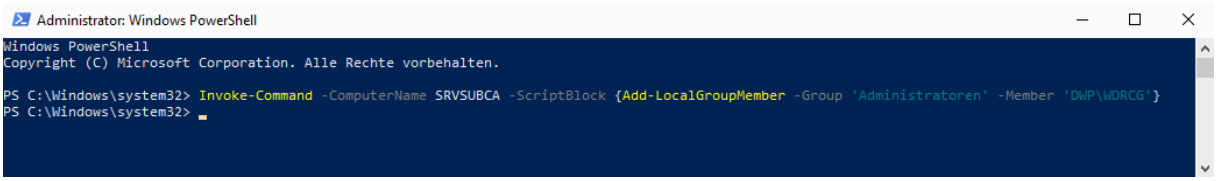
Set-ItemProperty –Path HKLM:\System\CurrentControlSet\Control\Lsa –Name DisableRestrictedAdmin -Value 0 –Type DWORD

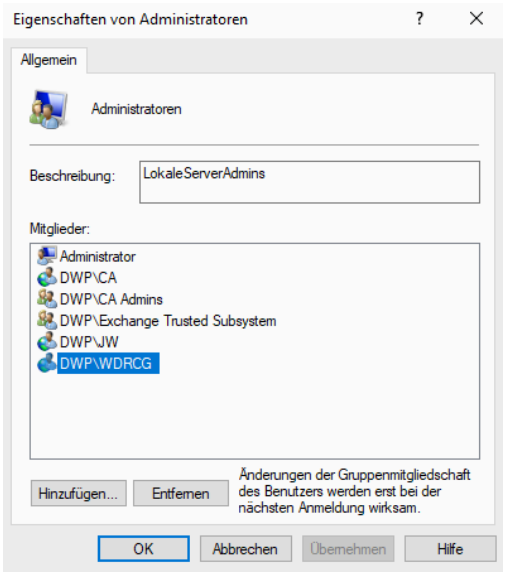




Als nächstes wird der Domänenbenutzer „WDRCG" auf dem Zielsystem SRVSUBCA entweder Mitglied der lokalen Administratorengruppe oder der Remotedesktopbenutzer.

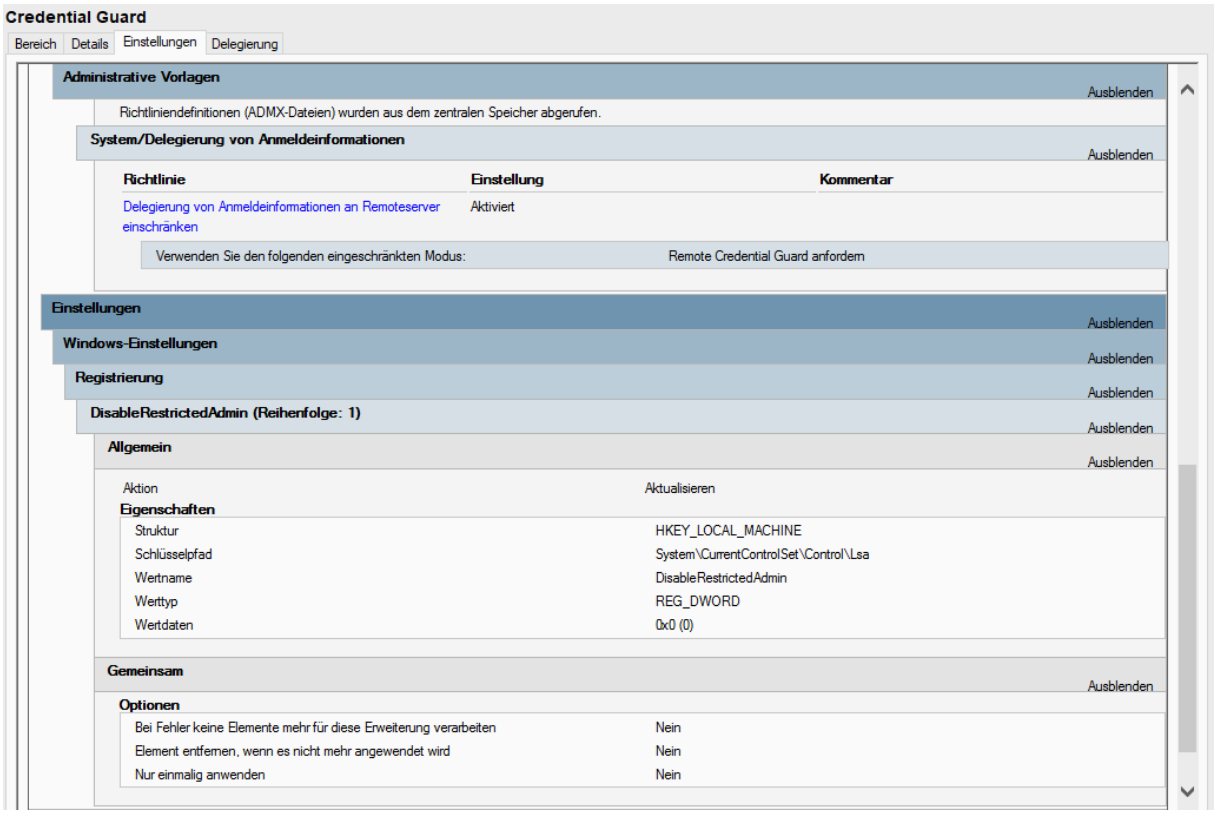
Invoke-Command –ComputerName SRVSUBCA –ScriptBlock {Add-LocalGroupMember –Group 'Remotedesktopbenutzer' –Member 'DWP\WDRCG'}



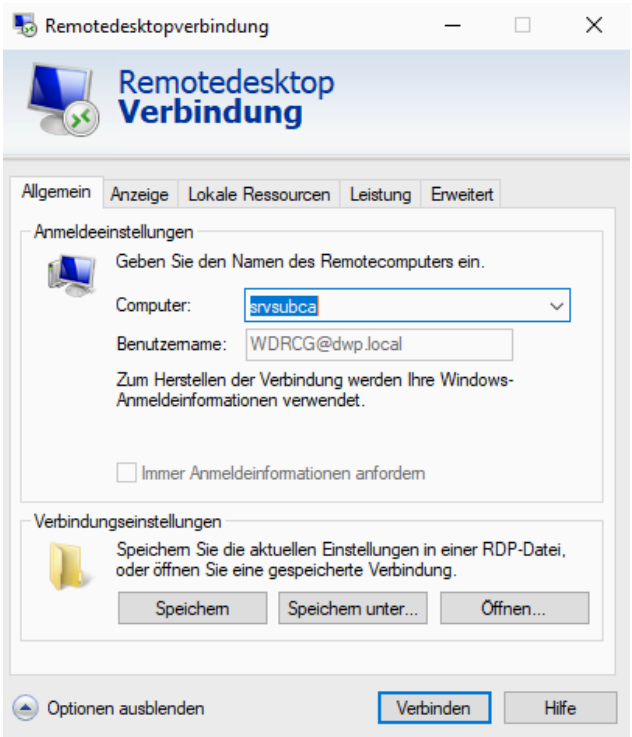


Erstellt von Jörn Walter **05.06.2021**

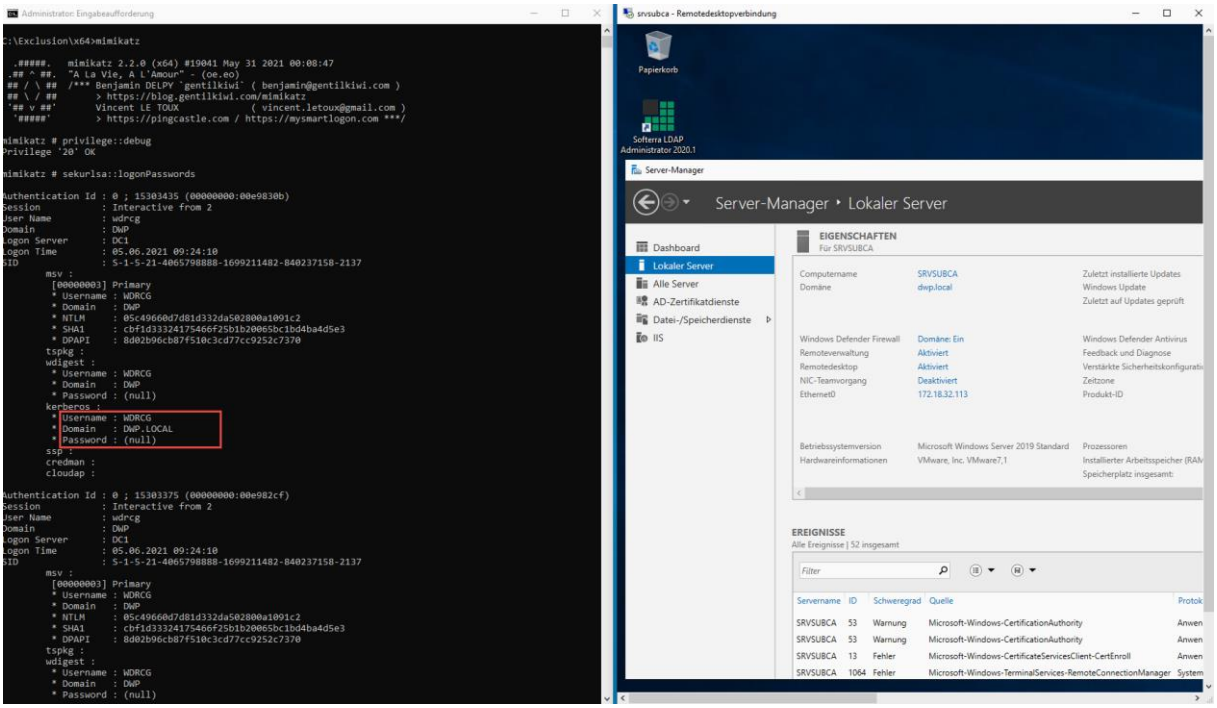
Alternative; Erstellen und verlinken das neue Gruppenrichtlinienobjekt mit folgenden Einstellungen auf die gesamte Domäne. WDRCG kann auch, ist aber nicht zu empfehlen, mit dem Aufruf mstsc /remoteguard und dem oben erwähnten Registry-Eintrag initiiert werden.



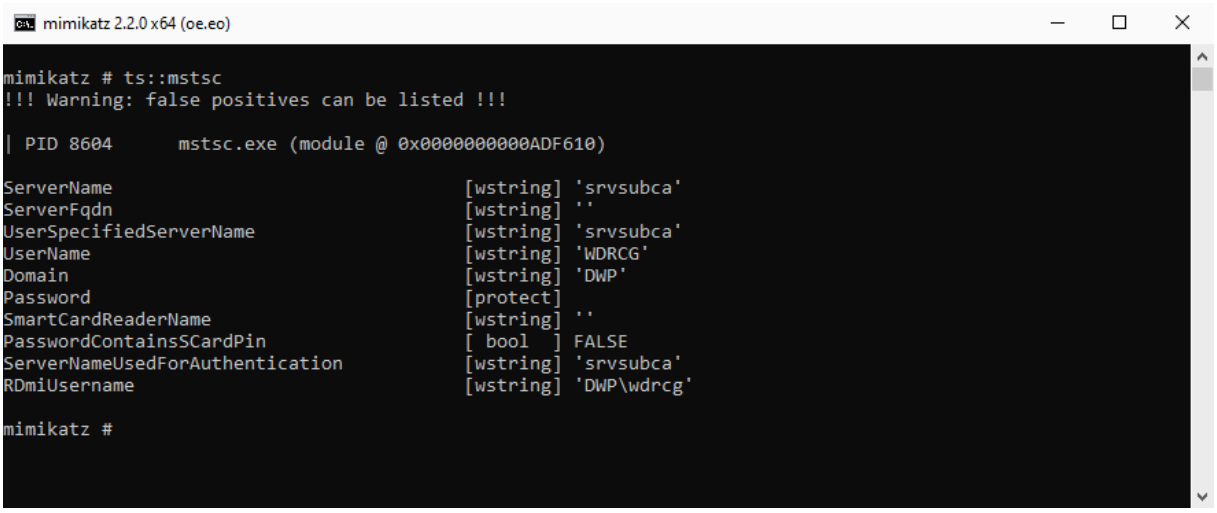
Der Windows Desktop Remote Credential Guard ist fertig konfiguriert und einsatzbereit. Sobald wir eine RDP Sitzung aufbauen, wird zunächst der UPN festgesetzt,



und kein Kennwort zwischengespeichert oder übertragen, siehe linken Bildausschnitt.

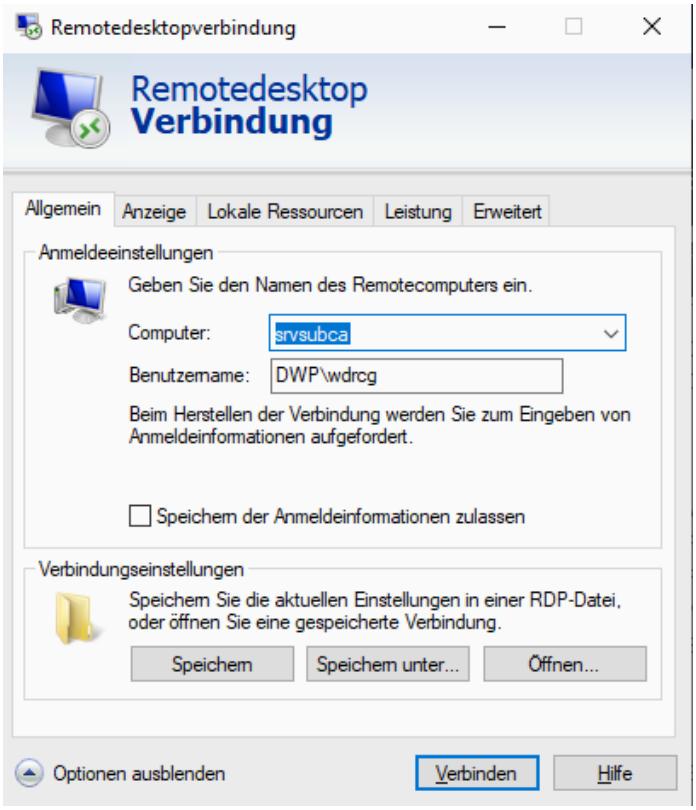


Hier noch einmal im Detail.

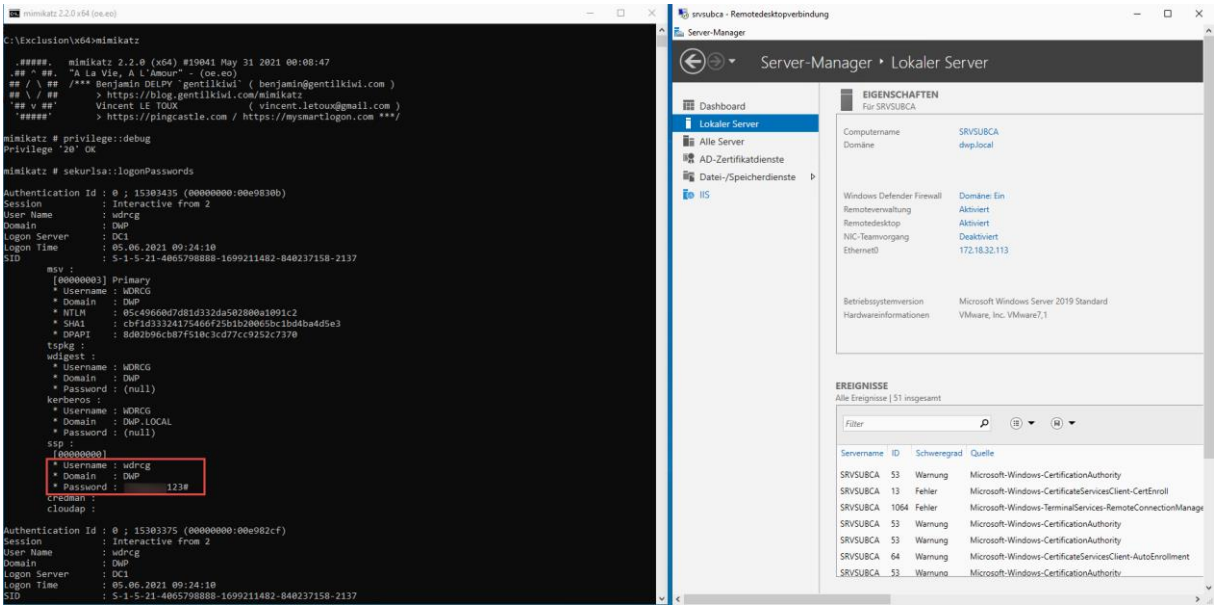


WDRCG – RDP Credential Guard

Ohne Windows Desktop Remote Credential Guard werden die Anmeldedaten übertragen und zwischengespeichert (LSA Store).

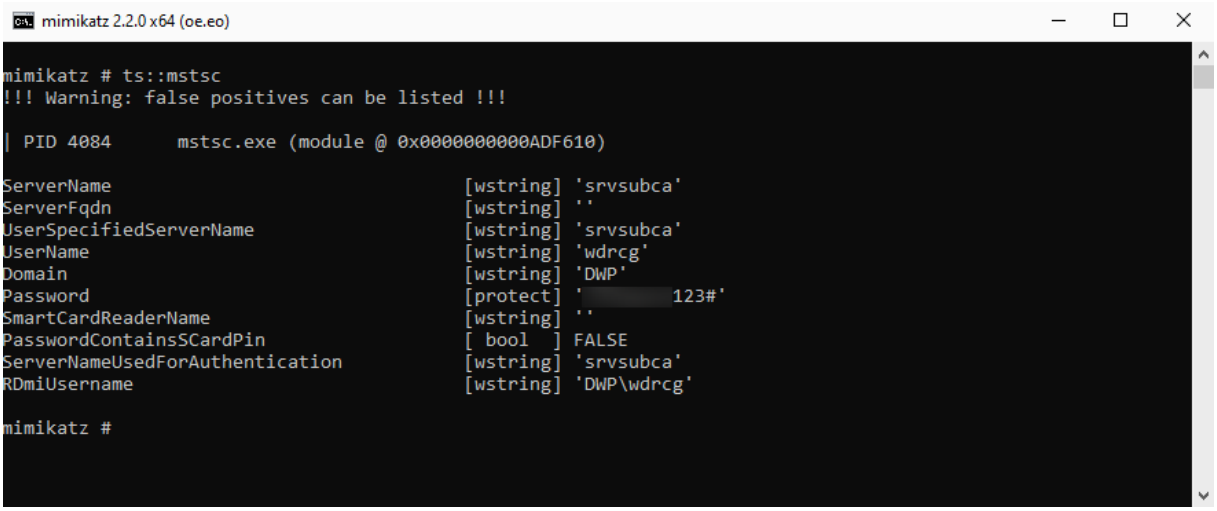


Hier sehen wir das zwischengespeicherte Kennwort.



WDRCG – RDP Credential Guard

Hier noch einmal im Detail.



Credential Guard:

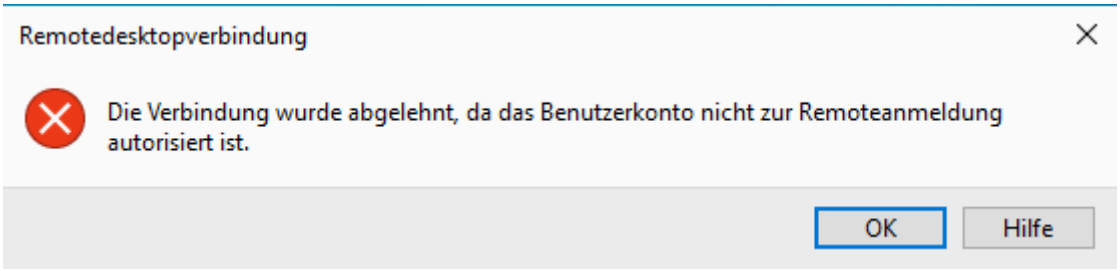
Der CG funktioniert nur mit dem RDP-Protokoll und authentifiziert ausschließlich über Kerberos (blockt NTLM). Der Credential Guard benutzt zur Anmeldung an das Zielsystem die lokalen Anmeldedaten (mit den Daten mit denen du dich an deinen Client angemeldet hast), es können keine alternativen Credentials verwendet werden.

Troubleshooting:

Wenn der Registry-Eintrag Name DisableRestrictedAdmin -Value 0 –Type DWORD auf dem Zielsystem nicht vorhanden ist, aber die Gruppenrichtlinie den Credential Guard anfordert, dann erscheint folgende Meldung:

WDRCG – RDP Credential Guard

Wenn der Benutzer, der sich an einem Remotesystem anmelden möchte, nicht in der Gruppe der Remotedesktopbenutzer ist, dann erscheint folgende Fehlermeldung:



Optional:

Mimikatz-Download:

```
New-Item -ItemType Directory -Path 'C:\Skripte' -Force

[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType

Invoke-WebRequest -Uri
https://github.com/gentilkiwi/mimikatz/releases/download/2.2.0-
20210531/mimikatz_trunk.zip -Outfile C:\Skripte\mimikatz_trunk.zip

Expand-Archive –Path C:\Skripte\mimikatz_trunk.zip -DestinationPath C:\Skripte -Force
```

Releases · gentilkiwi/mimikatz · GitHub

Mimikatz-Befehle:

```
Mimikatz
privilege::debug
sekurlsa::logonPasswords
exit
```

WDRCG – RDP Credential Guard

Die unterschiedlichen Funktionen im Detail:

Feature	Remotedesktop	Windows Defender Remote Credential Guard	Eingeschränkter Admin-Modus
Schutzvorteile	Anmeldeinformationen auf dem Server sind nicht vor Pass-the-Hash-Angriffen geschützt.	Benutzeranmeldeinformationen verbleiben auf dem Client. Ein Angreifer kann *nur* während der Sitzung im Namen des Benutzers handeln	Der Benutzer meldet sich als lokaler Administrator am Server an, sodass ein Angreifer nicht im Namen des „Domänenbenutzers" handeln kann. Jeder Angriff erfolgt lokal auf dem Server
Versionsunterstützung	Auf dem Remote-Computer kann jedes Windows-Betriebssystem ausgeführt werden	Sowohl auf dem Client als auch auf dem Remotecomputer muss **mindestens Windows 10, Version 1607 oder Windows Server 2016 ausgeführt werden**.	Auf dem Remotecomputer muss **mindestens das gepatchte Windows 7 oder das gepatchte Windows Server 2008 R2 ausgeführt werden** . Weitere Informationen zu Patches (Softwareupdates) im Zusammenhang mit dem eingeschränkten Administratormodus finden Sie in der Microsoft-Sicherheitsempfehlung 2871997 .
Hilft zu verhindern	N / A	• Pass-the-Hash • Verwendung eines Berechtigungsnachweises nach der Trennung	• Pass-the-Hash • Verwendung der Domänenidentität während der Verbindung
Vom Remote-Desktop-Clientgerät unterstützte Anmeldeinformationen	• **Angemeldete** Anmeldeinformationen • **Mitgelieferte** Anmeldeinformationen • **Gespeicherte** Zugangsdaten	• **Auf der Unterzeichnung** nur Anmeldeinformationen	• **Angemeldete** Anmeldeinformationen • **Mitgelieferte** Anmeldeinformationen • **Gespeicherte** Zugangsdaten
Zugriff	**Benutzer erlaubt**, **dh** Mitglieder der Gruppe	**Benutzer erlaubt**, **dh** Mitglieder von	**Nur Administratoren**, dh nur Mitglieder der Administratorengruppe des Remote-Hosts.

WDRCG – RDP Credential Guard

Feature	Remotedesktop	Windows Defender Remote Credential Guard	Eingeschränkter Admin-Modus
	Remotedesktopbenutzer des Remotehosts.	Remotedesktopbenutzern des Remotehosts.	
Netzwerkidentität	Die Remotedesktopsitzung **stellt als angemeldeter Benutzer eine Verbindung zu anderen Ressourcen her**.	Die Remotedesktopsitzung **stellt als angemeldeter Benutzer eine Verbindung zu anderen Ressourcen her**.	Die Remotedesktopsitzung **stellt als Identität des** Remotehosts eine **Verbindung zu anderen Ressourcen her**.
Multi-Hop	Vom Remotedesktop **aus können Sie über** Remotedesktop eine **Verbindung zu einem anderen Computer herstellen**	Vom Remotedesktop aus **können** Sie **über** Remotedesktop eine **Verbindung zu einem anderen Computer herstellen**.	Für Benutzer nicht zulässig, da die Sitzung als lokales Hostkonto ausgeführt wird
Unterstützte Authentifizierung	Jedes verhandelbare Protokoll.	Nur Kerberos.	Jedes verhandelbare Protokoll