oneconsult®

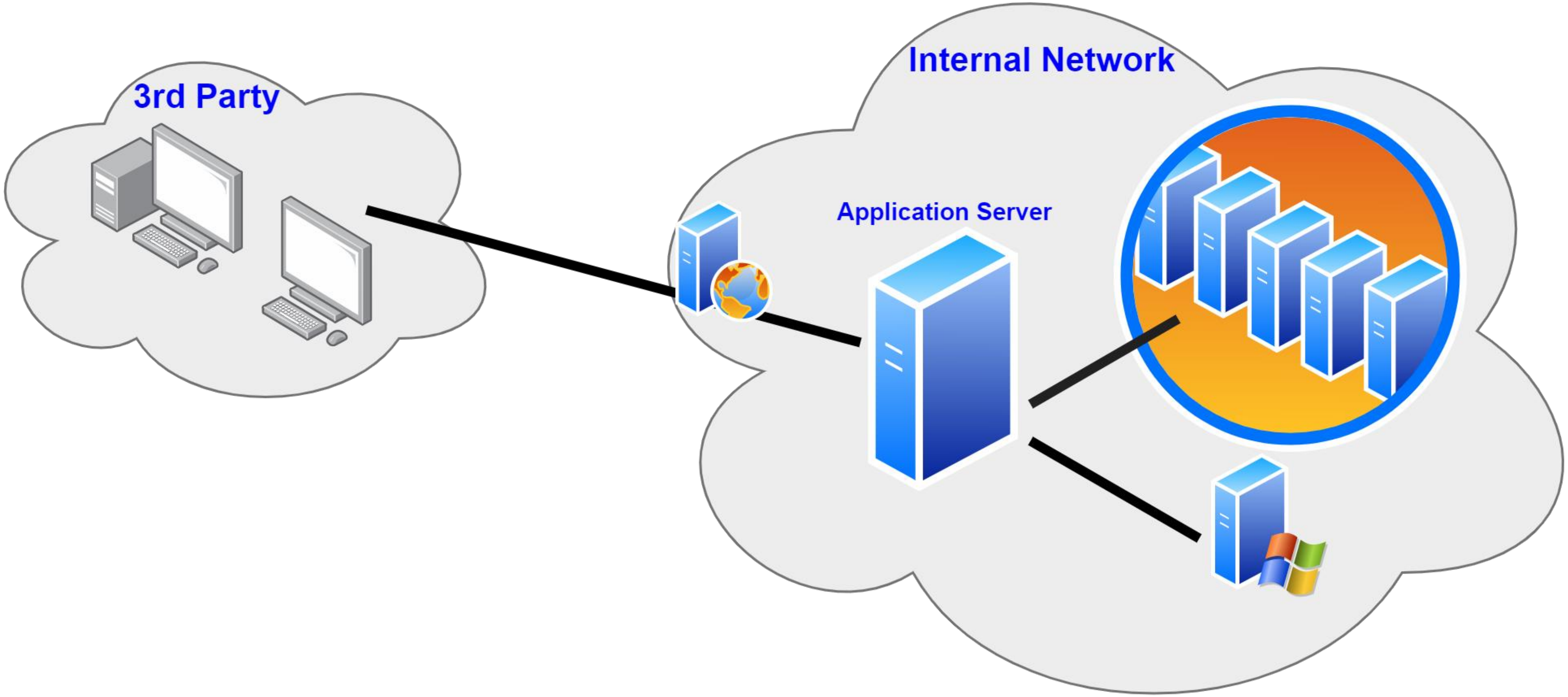
Assessing and Securing Third-Party Maintenance Access

Fabian Gonzalez

12 October 2021

CYBER ATTACKS AND DEFENSE
SWISS CYBER STORM
WWW.SWISSCYBERSTORM.COM

High-level Scenario

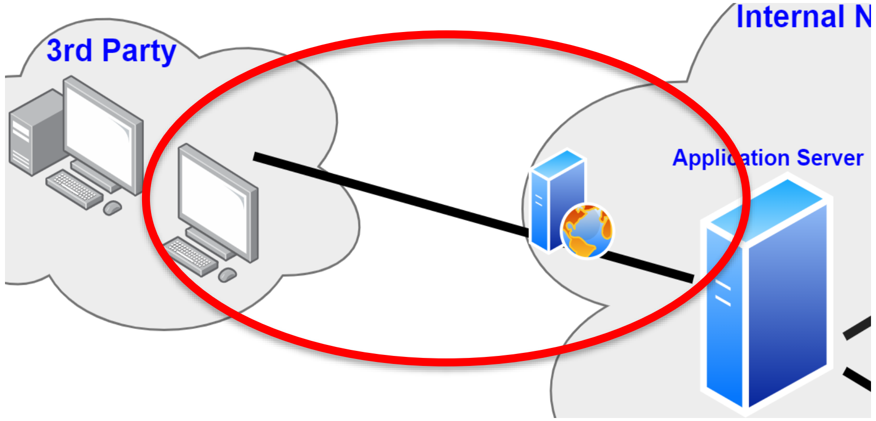


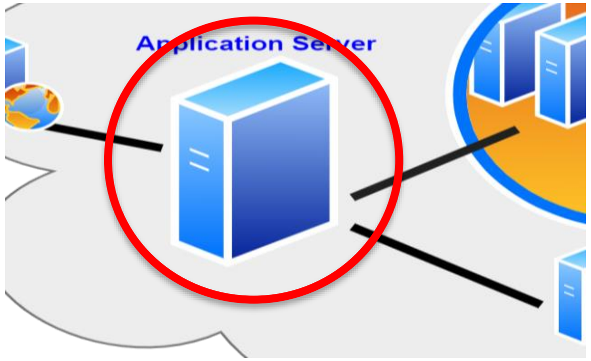
Access

- Restrict external access
  - Time
  - Location
  - Employees

- Restrict privileges
  - Least privileges

- Further restrictions
  - Use multifactor (2FA)
  - Proctored access





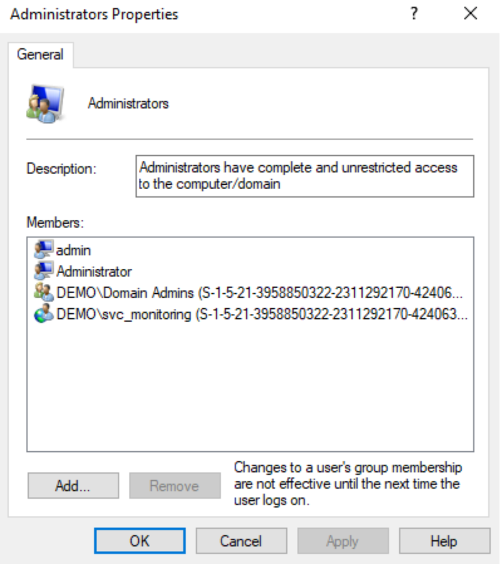
Server

- → General hardening

CIS Benchmarks™

Securing Microsoft Windows Server
An objective, consensus-driven security guideline for the Microsoft Windows Server Operating Systems.

- → Local admin rights



Administrators Properties

Administrators

Description: Administrators have complete and unrestricted access to the computer/domain

Members:

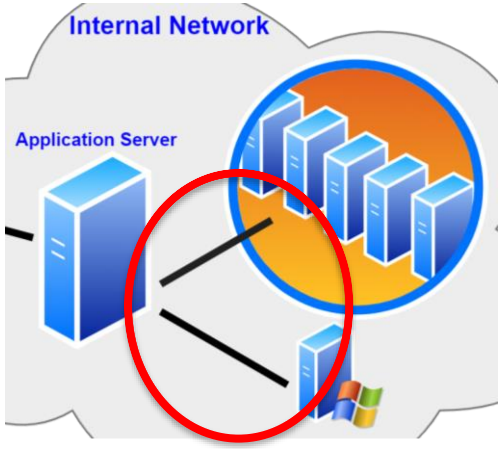
admin
Administrator
DEMO\Domain Admins (S-1-5-21-3958850322-2311292170-42406...
DEMO\svc_monitoring (S-1-5-21-3958850322-2311292170-424063...

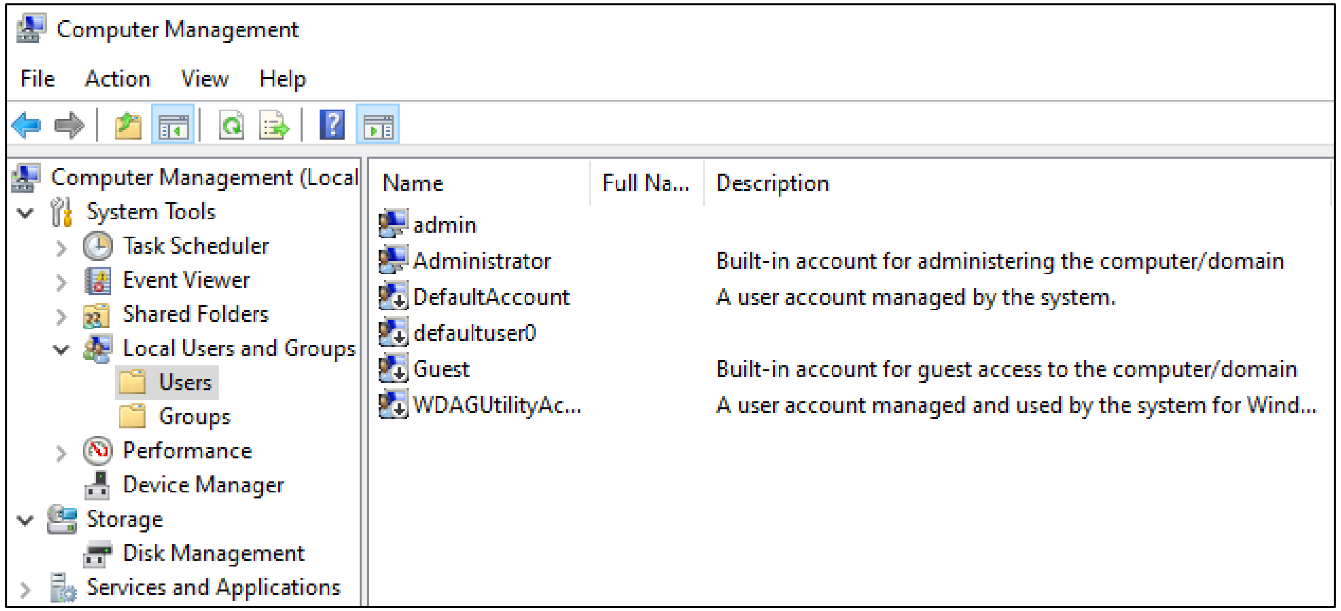
Changes to a user's group membership are not effective until the next time the user logs on.

THEY NEED LOCAL ADMIN RIGHTS

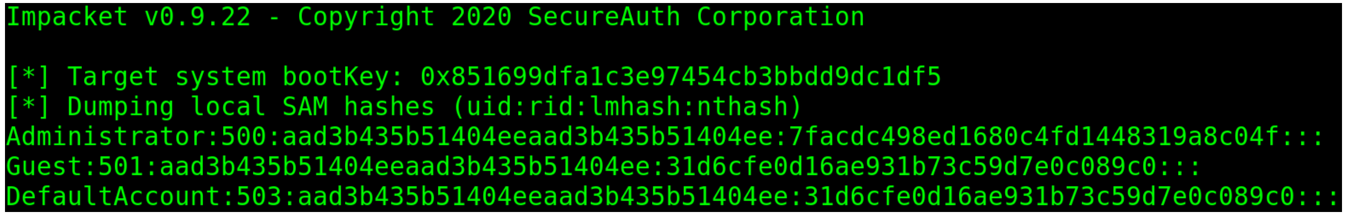
Local Users

→ Password reusing





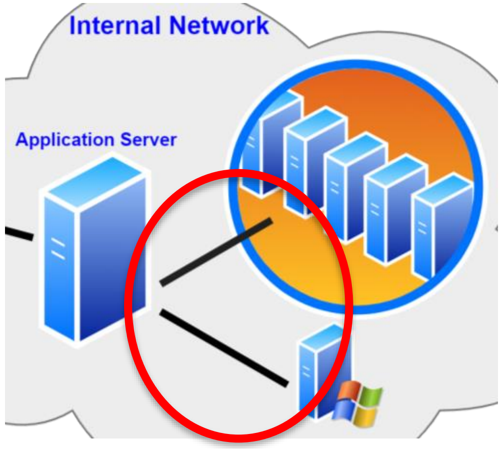
Name	Full Na...	Description
admin		
Administrator		Built-in account for administering the computer/domain
DefaultAccount		A user account managed by the system.
defaultuser0		
Guest		Built-in account for guest access to the computer/domain
WDAGUtilityAc...		A user account managed and used by the system for Wind...

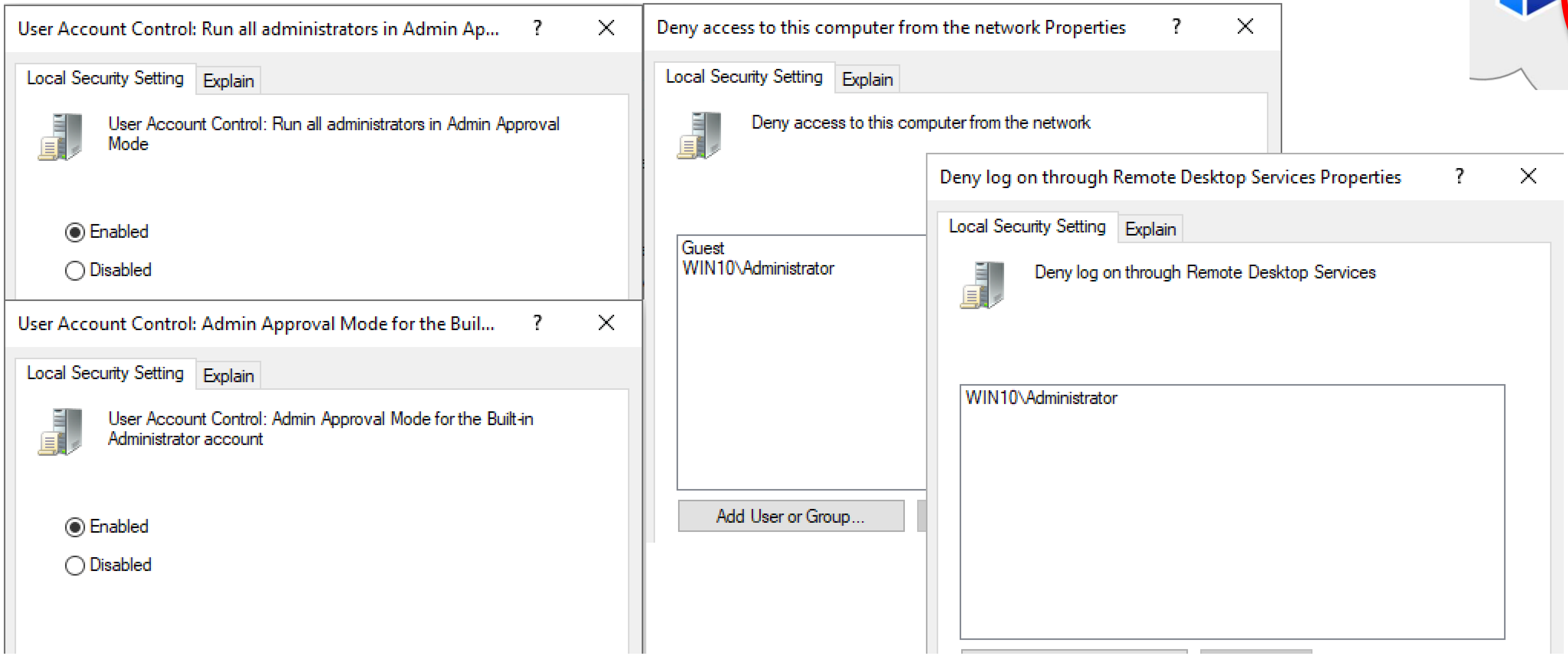


```
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Target system bootKey: 0x851699dfa1c3e97454cb3bbdd9dc1df5
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:7facdc498ed1680c4fd1448319a8c04f:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Local Users

- → Unique passwords
- → Group policy settings





User Account Control: Run all administrators in Admin Ap... ? ×

Local Security Setting | Explain

User Account Control: Run all administrators in Admin Approval Mode

● Enabled
○ Disabled

User Account Control: Admin Approval Mode for the Buil... ? ×

Local Security Setting | Explain

User Account Control: Admin Approval Mode for the Built-in Administrator account

● Enabled
○ Disabled

Deny access to this computer from the network Properties ? ×

Local Security Setting | Explain

Deny access to this computer from the network

Guest
WIN10\Administrator

Add User or Group...

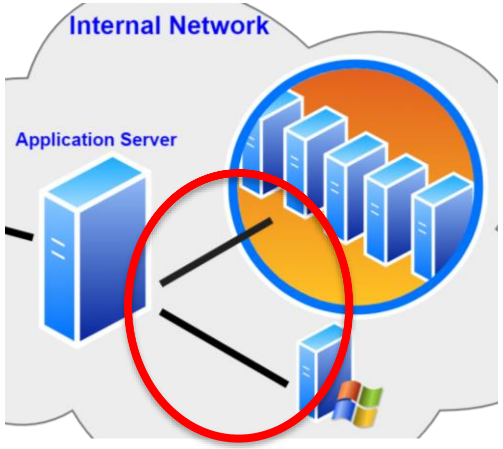
Deny log on through Remote Desktop Services Properties ? ×

Local Security Setting | Explain

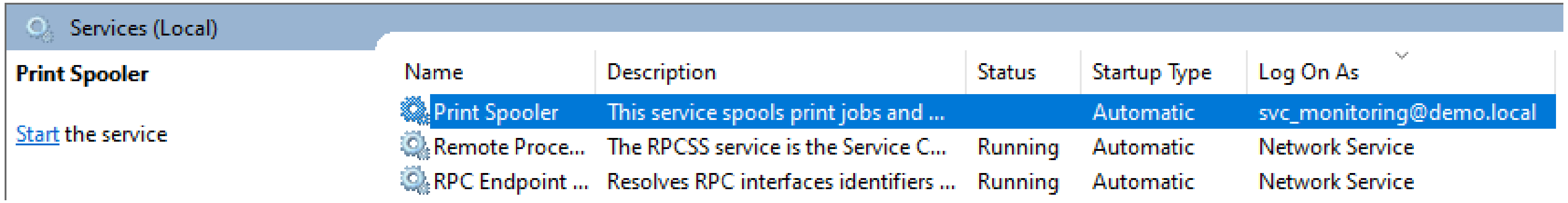
Deny log on through Remote Desktop Services

WIN10\Administrator

Service Accounts



- → Service accounts credentials

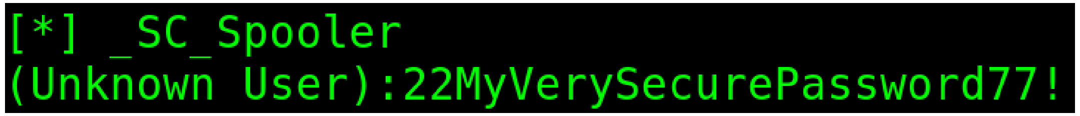


Services (Local)

Print Spooler

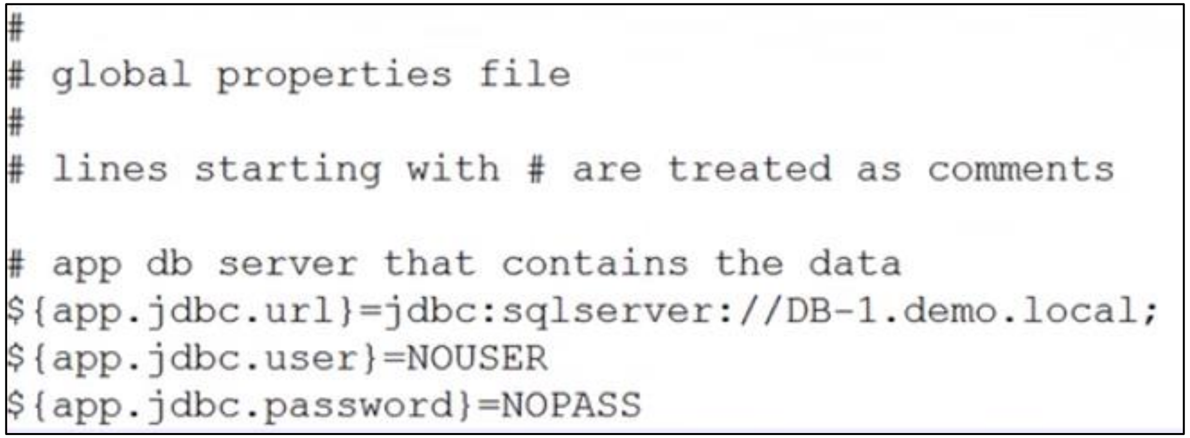
Start the service

Name	Description	Status	Startup Type	Log On As
Print Spooler	This service spools print jobs and ...		Automatic	svc_monitoring@demo.local
Remote Proce...	The RPCSS service is the Service C...	Running	Automatic	Network Service
RPC Endpoint ...	Resolves RPC interfaces identifiers ...	Running	Automatic	Network Service



```
[*] _SC_Spooler
(Unknown User):22MyVerySecurePassword77!
```

- → Configuration files



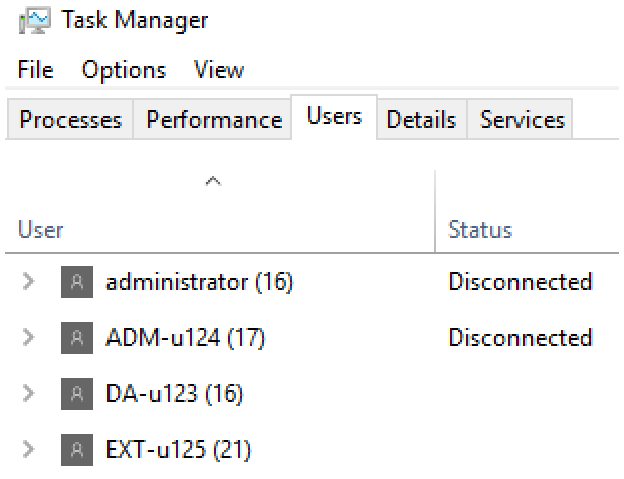
```
#
# global properties file
#
# lines starting with # are treated as comments

# app db server that contains the data
${app.jdbc.url}=jdbc:sqlserver://DB-1.demo.local;
${app.jdbc.user}=NOUSER
${app.jdbc.password}=NOPASS
```

WINDOWS MEMORY

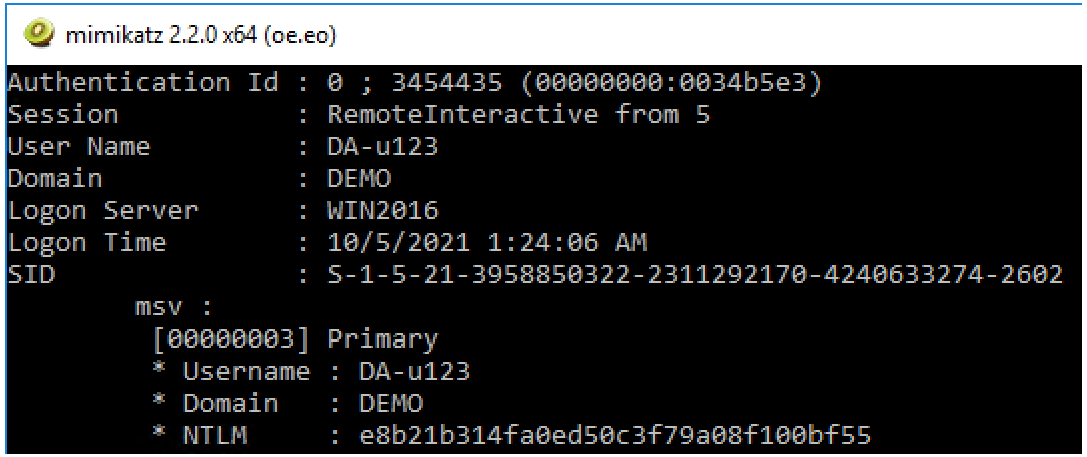
CREDENTIALS EVERYWHERE

Credentials

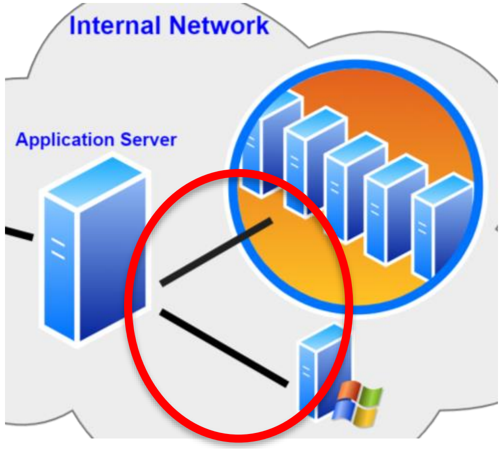
→ In memory credentials



User	Status
administrator (16)	Disconnected
ADM-u124 (17)	Disconnected
DA-u123 (16)	
EXT-u125 (21)	

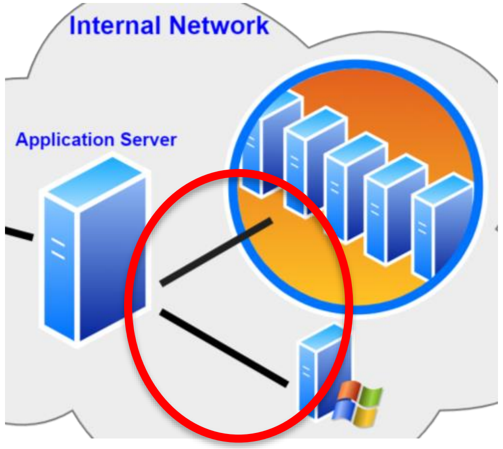

mimikatz 2.2.0 x64 (oe.eo)

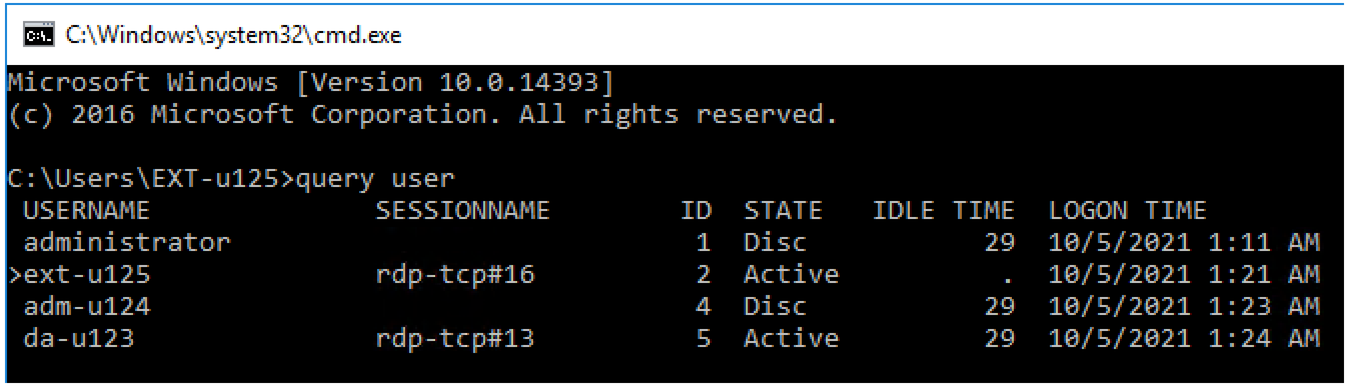
```
Authentication Id : 0 ; 3454435 (00000000:0034b5e3)
Session           : RemoteInteractive from 5
User Name         : DA-u123
Domain            : DEMO
Logon Server      : WIN2016
Logon Time        : 10/5/2021 1:24:06 AM
SID               : S-1-5-21-3958850322-2311292170-4240633274-2602
        msv :
         [00000003] Primary
         * Username : DA-u123
         * Domain   : DEMO
         * NTLM     : e8b21b314fa0ed50c3f79a08f100bf55
```



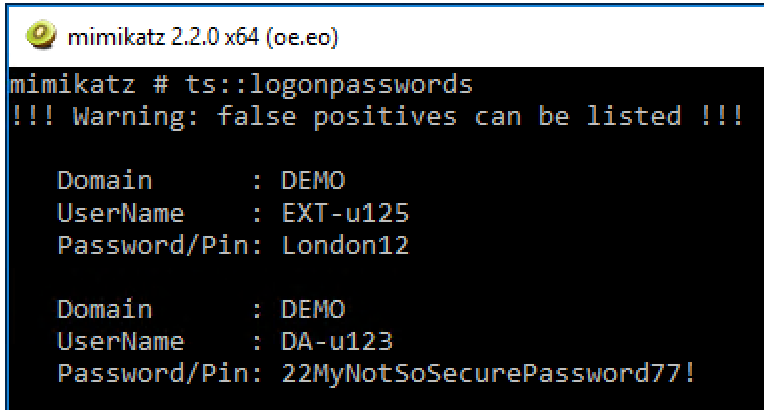
Credentials

→ In memory credentials




C:\Windows\system32\cmd.exe

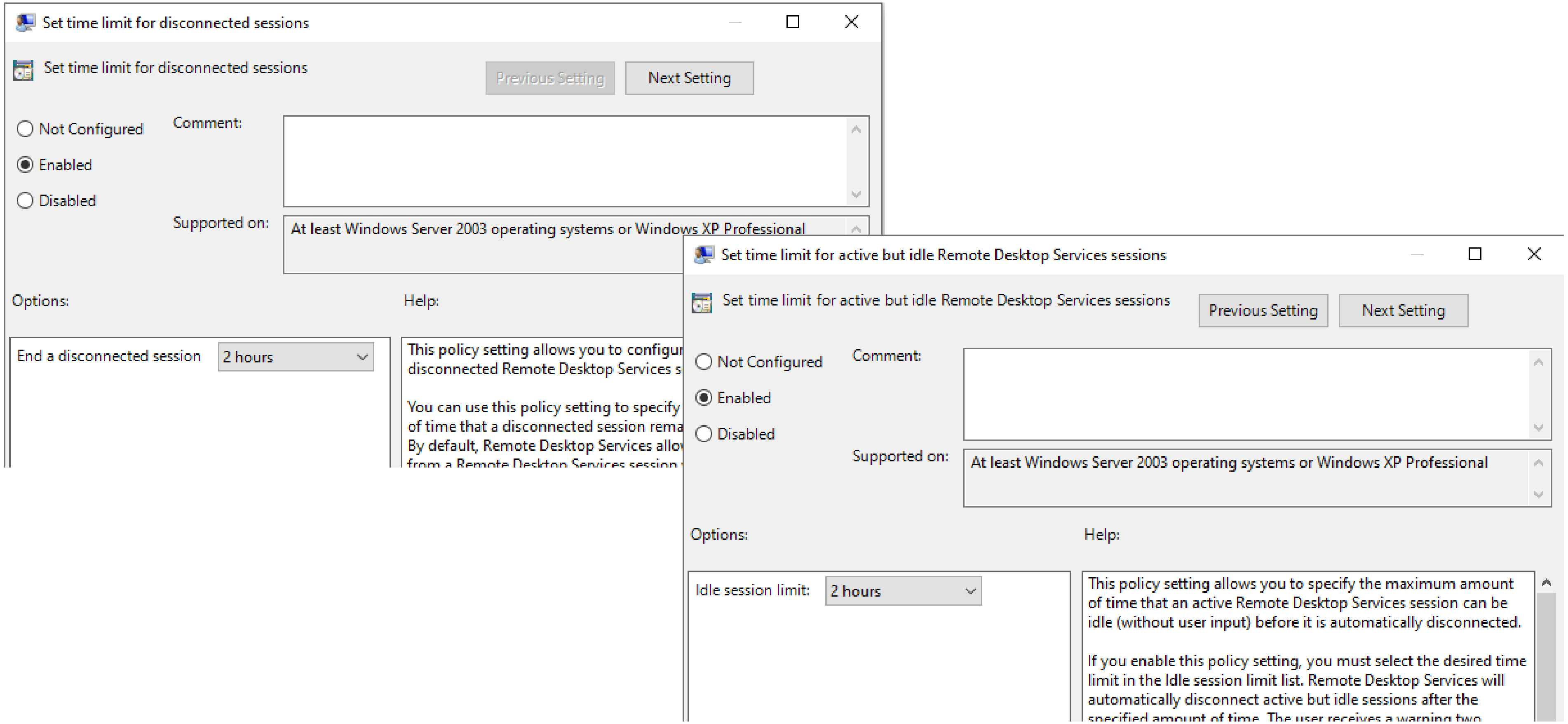
```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\EXT-u125>query user
 USERNAME              SESSIONNAME        ID  STATE   IDLE TIME  LOGON TIME
 administrator                             1  Disc           29  10/5/2021 1:11 AM
>ext-u125              rdp-tcp#16          2  Active          .  10/5/2021 1:21 AM
 adm-u124                                  4  Disc           29  10/5/2021 1:23 AM
 da-u123               rdp-tcp#13          5  Active         29  10/5/2021 1:24 AM
```


mimikatz 2.2.0 x64 (oe.eo)

```
mimikatz # ts::logonpasswords
!!! Warning: false positives can be listed !!!

   Domain       : DEMO
   UserName     : EXT-u125
   Password/Pin: London12

   Domain       : DEMO
   UserName     : DA-u123
   Password/Pin: 22MyNotSoSecurePassword77!
```

Credentials

→ RDP force logoff



Set time limit for disconnected sessions

Set time limit for disconnected sessions

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Server 2003 operating systems or Windows XP Professional

Options:

End a disconnected session: 2 hours

Help:

This policy setting allows you to configur
disconnected Remote Desktop Services s

You can use this policy setting to specify
of time that a disconnected session rema
By default, Remote Desktop Services allo
from a Remote Desktop Services session

Set time limit for active but idle Remote Desktop Services sessions

Set time limit for active but idle Remote Desktop Services sessions

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Server 2003 operating systems or Windows XP Professional

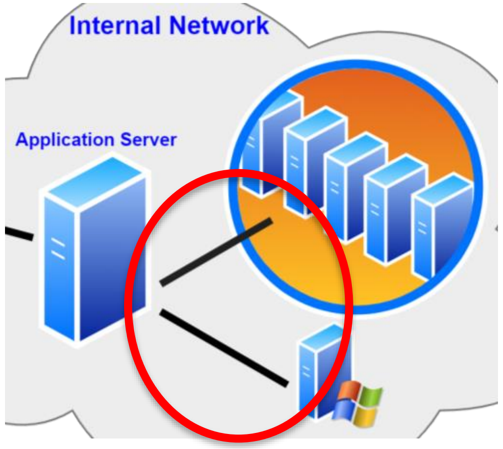
Options:

Idle session limit: 2 hours

Help:

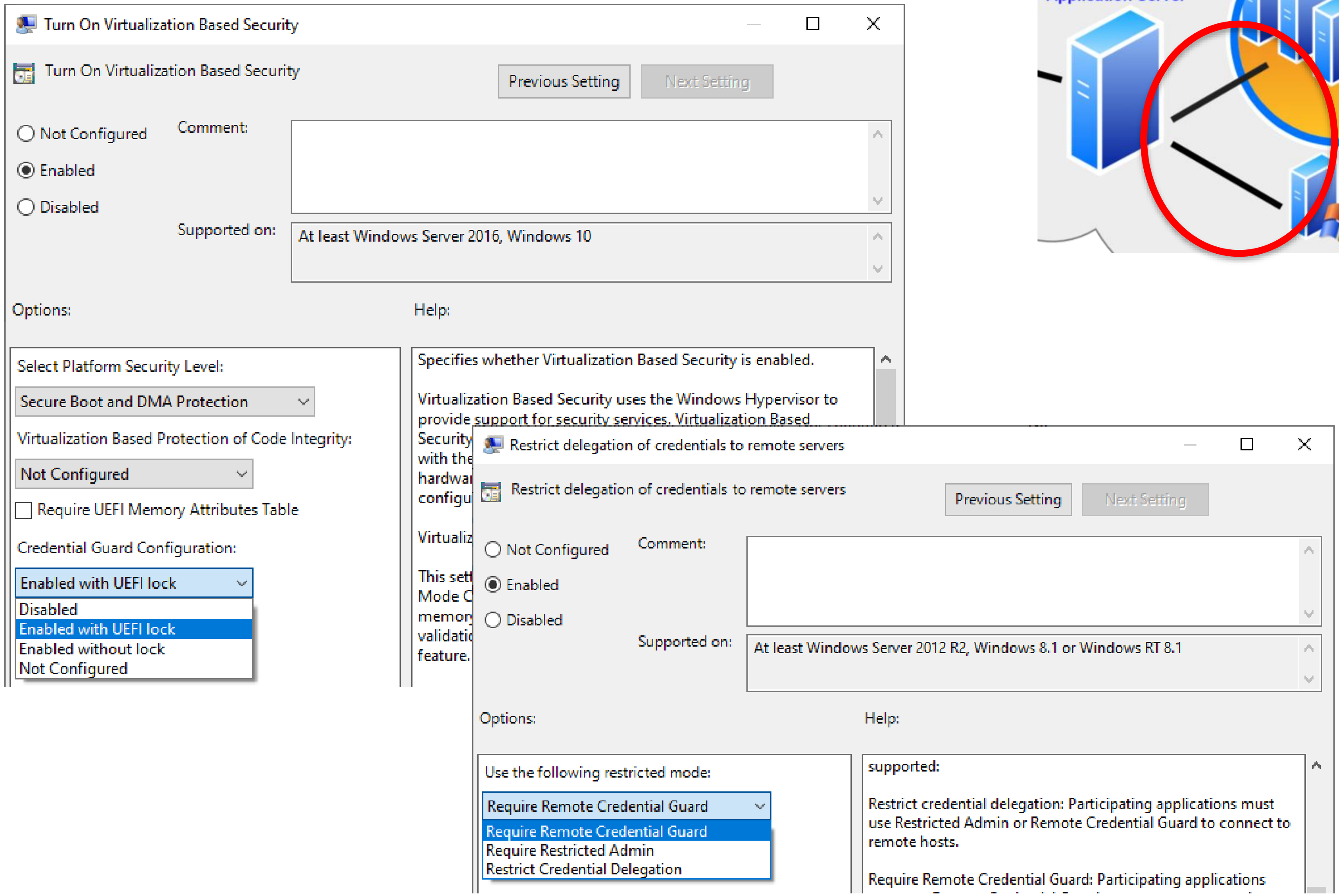
This policy setting allows you to specify the maximum amount of time that an active Remote Desktop Services session can be idle (without user input) before it is automatically disconnected.

If you enable this policy setting, you must select the desired time limit in the Idle session limit list. Remote Desktop Services will automatically disconnect active but idle sessions after the specified amount of time. The user receives a warning two



Credentials

- → Credential Guard
- → Restricted Admin
- → Remote Credential Guard



Turn On Virtualization Based Security

Turn On Virtualization Based Security

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Server 2016, Windows 10

Options:

Select Platform Security Level: Secure Boot and DMA Protection

Virtualization Based Protection of Code Integrity: Not Configured

□ Require UEFI Memory Attributes Table

Credential Guard Configuration: Enabled with UEFI lock

- Disabled
- Enabled with UEFI lock
- Enabled without lock
- Not Configured

Help:

Specifies whether Virtualization Based Security is enabled.

Virtualization Based Security uses the Windows Hypervisor to provide support for security services. Virtualization Based
Security
with the
hardwar
configu

Virtualiz

This sett
Mode C
memory
validatio
feature.

Restrict delegation of credentials to remote servers

Restrict delegation of credentials to remote servers

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Server 2012 R2, Windows 8.1 or Windows RT 8.1

Options:

Use the following restricted mode: Require Remote Credential Guard

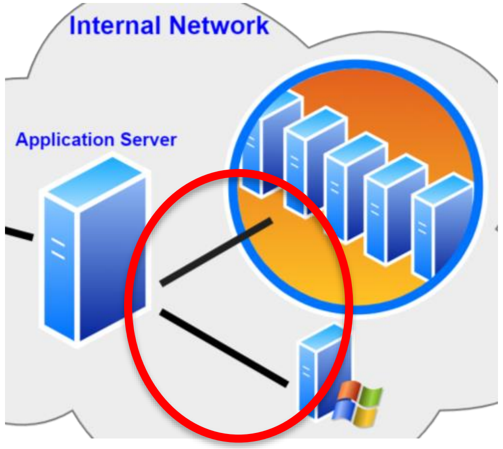
- Require Remote Credential Guard
- Require Restricted Admin
- Restrict Credential Delegation

Help:

supported:

Restrict credential delegation: Participating applications must use Restricted Admin or Remote Credential Guard to connect to remote hosts.

Require Remote Credential Guard: Participating applications

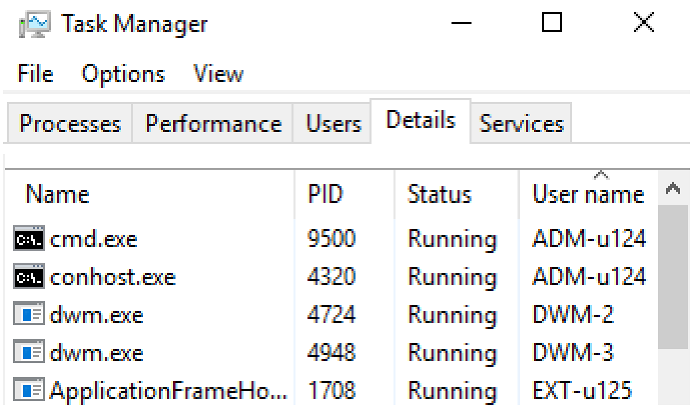


ATTACK USERS

USING WINDOWS BUILT-IN TOOLS

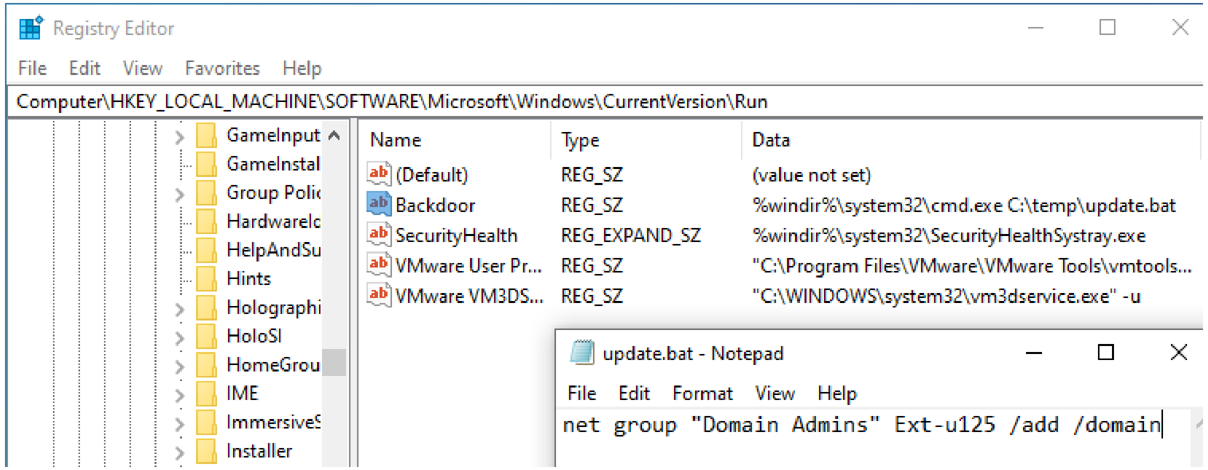
Server

- → Process injection



Name	PID	Status	User name
cmd.exe	9500	Running	ADM-u124
conhost.exe	4320	Running	ADM-u124
dwm.exe	4724	Running	DWM-2
dwm.exe	4948	Running	DWM-3
ApplicationFrameHo...	1708	Running	EXT-u125

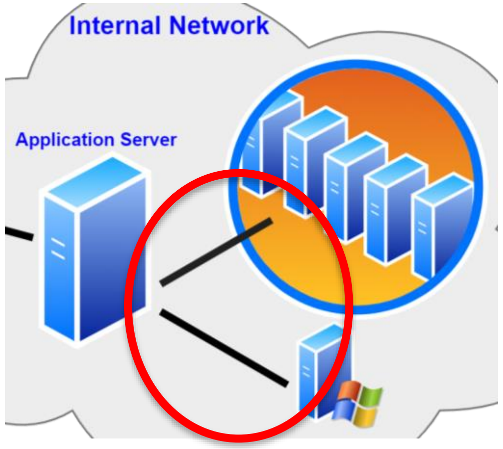
- → Backdoor
  - ○ Autorun entry
  - ○ Replace binary



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

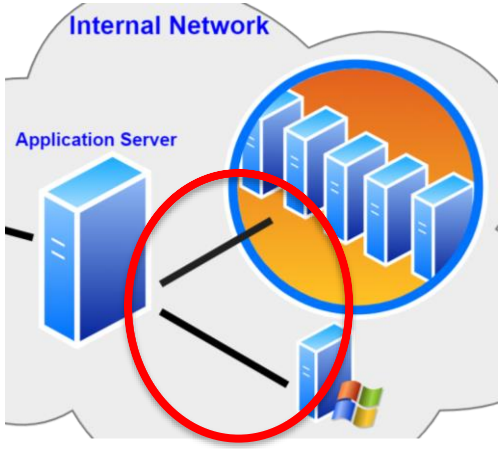
Name	Type	Data
(Default)	REG_SZ	(value not set)
Backdoor	REG_SZ	%windir%\system32\cmd.exe C:\temp\update.bat
SecurityHealth	REG_EXPAND_SZ	%windir%\system32\SecurityHealthSystray.exe
VMware User Pr...	REG_SZ	"C:\Program Files\VMware\VMware Tools\vmtools...
VMware VM3DS...	REG_SZ	"C:\WINDOWS\system32\vm3dservice.exe" -u

```
net group "Domain Admins" Ext-u125 /add /domain
```



Server

- → No full prevention
- → RDP sessions force logoff
- → Deny domain admin users
- → Restricted RDP
- → Privileged Access Management (PAM) solutions

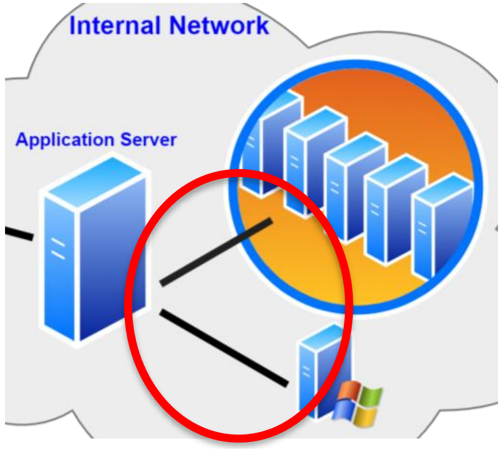


LOCAL ADMIN PERMISSIONS

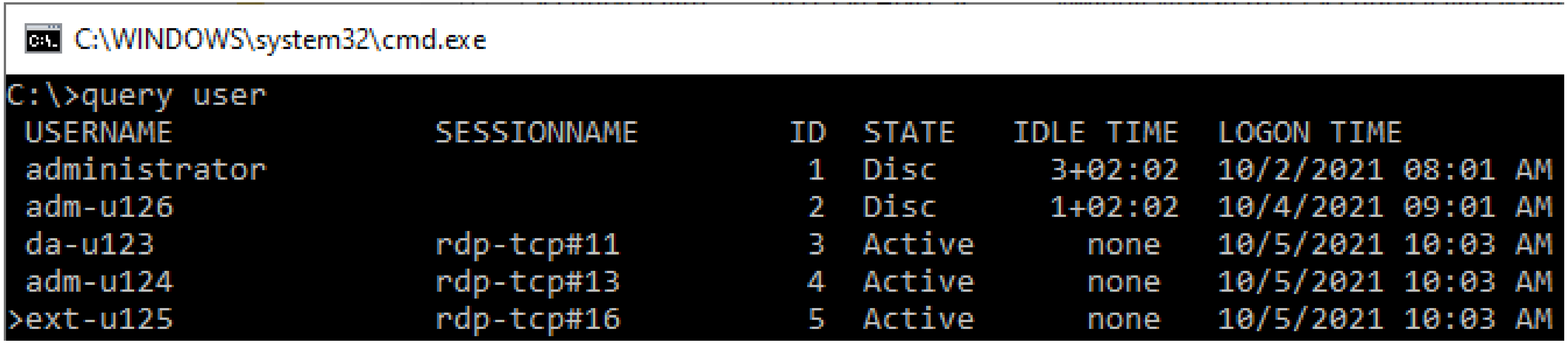
LET’S SECURE IT

Further Possibilities

- Separate active directory / forest
- Non domain joined server
- Network based isolation
- Jump host



Recap

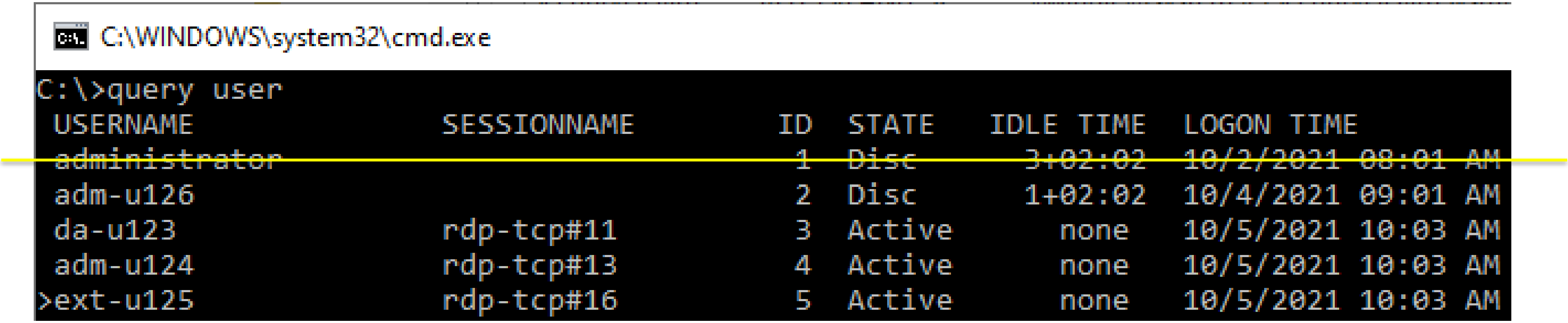

C:\WINDOWS\system32\cmd.exe

```
C:\>query user
 USERNAME              SESSIONNAME        ID  STATE   IDLE TIME  LOGON TIME
 administrator                             1  Disc      3+02:02  10/2/2021 08:01 AM
 adm-u126                                  2  Disc      1+02:02  10/4/2021 09:01 AM
 da-u123               rdp-tcp#11          3  Active       none  10/5/2021 10:03 AM
 adm-u124              rdp-tcp#13          4  Active       none  10/5/2021 10:03 AM
>ext-u125              rdp-tcp#16          5  Active       none  10/5/2021 10:03 AM
```

OPEN SESSIONS ON SERVER

WHAT COULD GO WRONG?

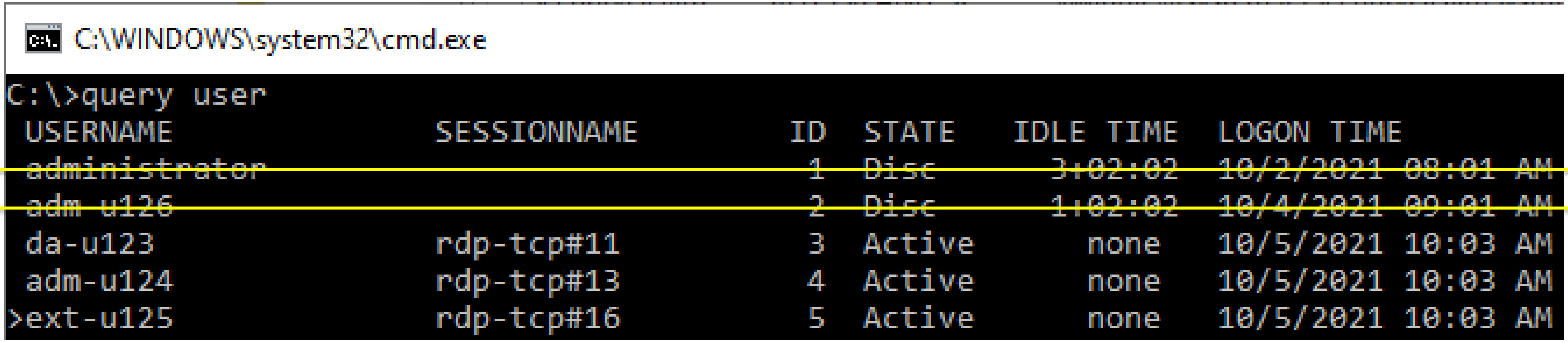
Recap



C:\WINDOWS\system32\cmd.exe

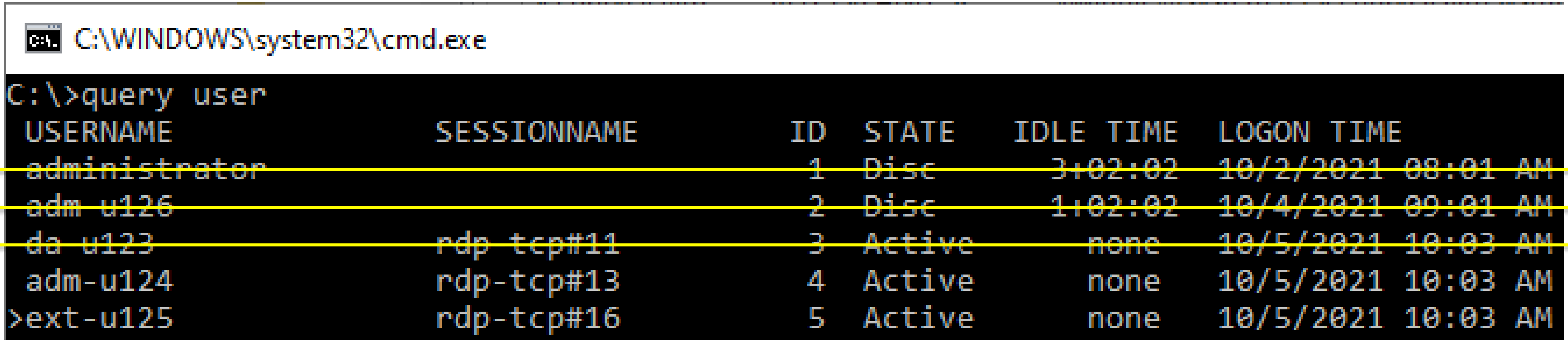
```
C:\>query user
 USERNAME              SESSIONNAME        ID  STATE   IDLE TIME  LOGON TIME
~~ administrator                             1  Disc      3+02:02  10/2/2021 08:01 AM~~
 adm-u126                                  2  Disc      1+02:02  10/4/2021 09:01 AM
 da-u123               rdp-tcp#11          3  Active       none  10/5/2021 10:03 AM
 adm-u124              rdp-tcp#13          4  Active       none  10/5/2021 10:03 AM
>ext-u125              rdp-tcp#16          5  Active       none  10/5/2021 10:03 AM
```

Recap



```
C:\>query user
 USERNAME              SESSIONNAME        ID  STATE   IDLE TIME  LOGON TIME
~~ administrator                            1  Disc       3:02:02  10/2/2021 08:01 AM~~
~~ adm-u126                                 2  Disc       1:02:02  10/4/2021 09:01 AM~~
 da-u123               rdp-tcp#11          3  Active      none    10/5/2021 10:03 AM
 adm-u124              rdp-tcp#13          4  Active      none    10/5/2021 10:03 AM
>ext-u125              rdp-tcp#16          5  Active      none    10/5/2021 10:03 AM
```

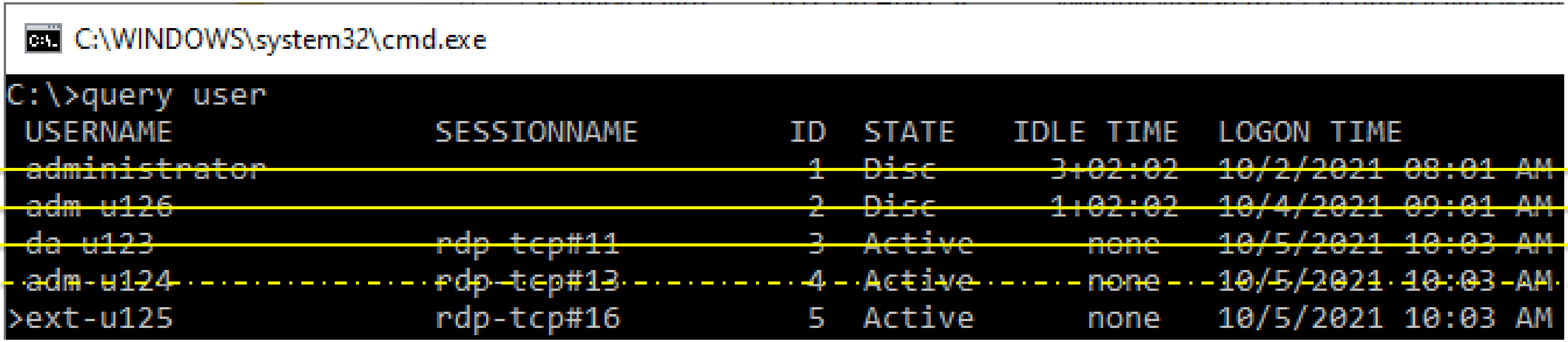
Recap



C:\WINDOWS\system32\cmd.exe

```
C:\>query user
 USERNAME              SESSIONNAME        ID  STATE   IDLE TIME  LOGON TIME
~~ administrator                             1  Disc      3:02:02  10/2/2021 08:01 AM~~
~~ adm-u126                                  2  Disc      1:02:02  10/4/2021 09:01 AM~~
~~ da-u123               rdp-tcp#11          3  Active      none   10/5/2021 10:03 AM~~
 adm-u124              rdp-tcp#13          4  Active      none   10/5/2021 10:03 AM
>ext-u125              rdp-tcp#16          5  Active      none   10/5/2021 10:03 AM
```

Recap



C:\WINDOWS\system32\cmd.exe

```
C:\>query user
 USERNAME              SESSIONNAME        ID  STATE   IDLE TIME  LOGON TIME
~~ administrator                            1  Disc       3:02:02  10/2/2021 08:01 AM~~
~~ adm-u126                                 2  Disc       1:02:02  10/4/2021 09:01 AM~~
~~ da-u123               rdp-tcp#11         3  Active        none  10/5/2021 10:03 AM~~
~~ adm-u124              rdp-tcp#13         4  Active        none  10/5/2021 10:03 AM~~
>ext-u125              rdp-tcp#16         5  Active        none  10/5/2021 10:03 AM
```

CYBER ATTACKS AND DEFENSE

SWISS CYBER STORM

WWW.SWISSCYBERSTORM.COM

Oneconsult AG

40+ security enthusiasts, no contractors

Certified **security experts**

OCINT-**CSIRT** (as a service)

Large **red team**
(ethical hacker / penetration tester)

Security **research department**

Member of **FIRST, ISECOM, ISSS, OWASP, Swiss Cyber Experts**

ASSESS
Penetration Test & Red Teaming
ISO 27001 / 27002 Security Audit
IT Forensics

PREVENT & MITIGATE
Information Security Consulting
Security Training & Awareness
Incident Response

MANAGE & SUPPORT
Security Officer Services
Incident Response & Forensics Agreement (IRFA)
Cyber Attack & Response Platform (CYARP)