8

1 / ADCS 0

ADCS justin ADCS med-factory

```
1  PROD     jason          ASREPRoasting       jason

2  MED-FACTORY      jason               med-factory\jason

3 med-factory\jason   justin            justin

4   ADCS    med-factory
```

2 Kerberoasting ASREPRoasting

3 **delegexec:Passw0rddeleg** Dc03

4 Impacket RBCD

5 S4U2Self rubeus Dc02$ **Asn1 Editor** (TGS https://github.com/PKISolutions/Asn1Editor.WPF) Dc02$ TGT

6 .NET SQL xp_cmdshell ( )

7 SqlRecon xp_dirtree

8 PowerUpSQL xp_cmdshell

9 .NET DLL Hex CLR RCE

10 Srv01 Srv02 OLE

11 Srv01 Srv02 CLR

12 Srv01 2 Web02 RCE

13 ADCS

14 GPO

15 Cheatsheet

DACL			
WriteDacl			
GenericAll			
GenericWrite		SPN Kerberoasting ASREPRoasting	
ForceChangePassword			
WriteOwner			
AllExtendedRights			

16 **CVE-2021-42278 PowerMad PowerView Rubeus** ( )

Revision #3
Created 10 September 2022 16:40:21 by
Updated 2 May 2023 20:57:03 by