```
PS C:\Users\yoojung> dsacls $OU /G "IT_Admins:CC;user" /I:S
Parameter /G was unexpected.
Displays or modifies permissions (ACLS) of an Active Directory Domain Services (AD DS)
Object

DSACLS object [/I:TSP] [/N] [/P:YN] [/G <group/user>:<perms> [...]]
              [/R <group/user> [...]] [/D <group/user>:<perms> [...]]
              [/S] [/T] [/A] [/resetDefaultDACL] [/resetDefaultSACL]
              [/takeOwnership] [/user:<userName>] [/passwd:<passwd> | *]
              [/simple]

   object           Path to the AD DS object for which to display or
                    manipulate the ACLs

   Path is the RFC 1779 format of the name, as in

       CN=John Doe,OU=Software,OU=Engineering,DC=Widget,DC=com

   A specific AD DS can be denoted by prepending \\server[:port]\
   to the object, as in

        \\ADSERVER\CN=John Doe,OU=Software,OU=Engineering,DC=Widget,DC=US

   no options       displays the security on the object.

   /I               Inheritance flags:
                        T: This object and sub objects
                        S: Sub objects only
                        P: Propagate inheritable permissions one level only.

   /N               Replaces the current access on the object, instead of
                    editing it.

   /P               Mark the object as protected
                       Y:Yes
                       N:No
```

Select Windows PowerShell

```
                  maintained.

 /G  <group/user>:<perms>
                  Grant specified group (or user) specified permissions.
                  See below for format of <group/user> and <perms>

 /D  <group/user>:<perms>
                  Deny specified group (or user) specified permissions.
                  See below for format of <group/user> and <perms>

 /R  <group/user> Remove all permissions for the specified group (or user).
                  See below for format of <group/user>

 /S               Restore the security on the object to the default for
                  that object class as defined in AD DS Schema. This option
                  works when dsacls is bound to NTDS. To restore default
                  ACL of an object in AD LDS use /resetDefaultDACL and
                  /resetDefaultSACL options.

 /T               Restore the security on the tree of objects to the
                  default for the object class.
                  This switch is valid only with the /S option.

 /A               When displaying the security on an AD DS
                  object, display the auditing information as well as
                  the permissions and ownership information.

/resetDefaultDACL Restore the DACL on the object to the default for
                  that object class as defined in AD DS Schema.

/resetDefaultSACL Restore the SACL on the object to the default for
                  that object class as defined in AD DS Schema.

/takeOwnership    Take ownership of the object.

/domain:<domainName> Connect to ldap server using this domain account
                     of the user.
```

Select Windows PowerShell

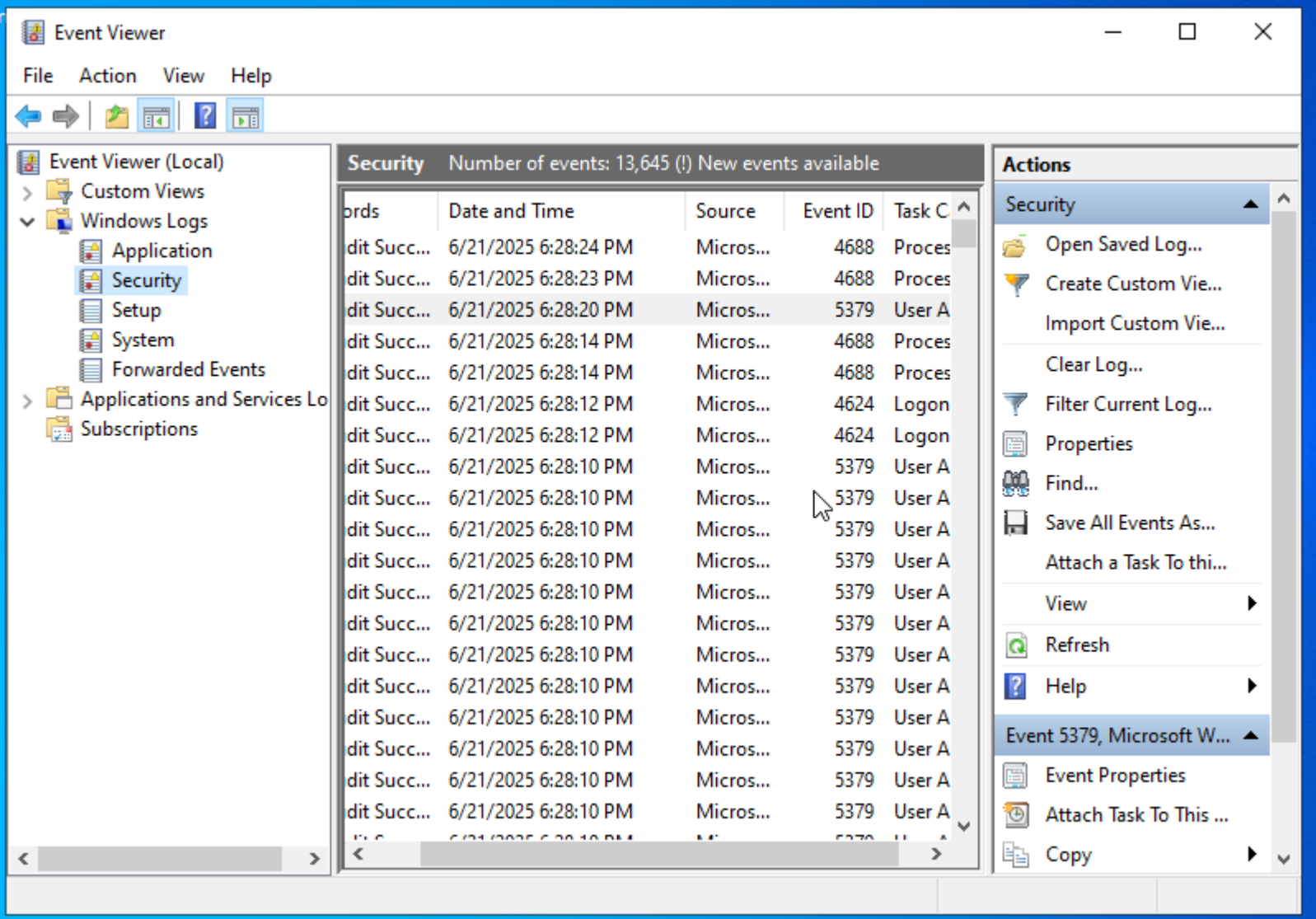
```
                option is not used dsacls will bind as the currently
                logged on user, using SSPI.

/passwd:<passwd> | * Passwd for the user account.

/simple         Bind to server using ldap simple bind. Note that the
                clear text password will be sent over the wire.

 <user/group> should be in the following forms:
              group@domain or domain\group
              user@domain or domain\user
              FQDN of the user or group
              A string SID

 <perms> should be in the following form:

      [Permission bits];[Object/Property];[Inherited Object Type]

      Permission bits can have the following values concatenated together:

      Generic Permissions
          GR      Generic Read
          GE      Generic Execute
          GW      Generic Write
          GA      Generic All

     Specific Permissions
          SD      Delete
          DT      Delete an object and all of it's children
          RC      Read security information
          WD      Change security information
          WO      Change owner information
          LC      List the children of an object

          CC      Create child object
          DC      Delete a child object
                  For these two permissions, if [Object/Property] is
                  not specified to define a specific child object type,
```

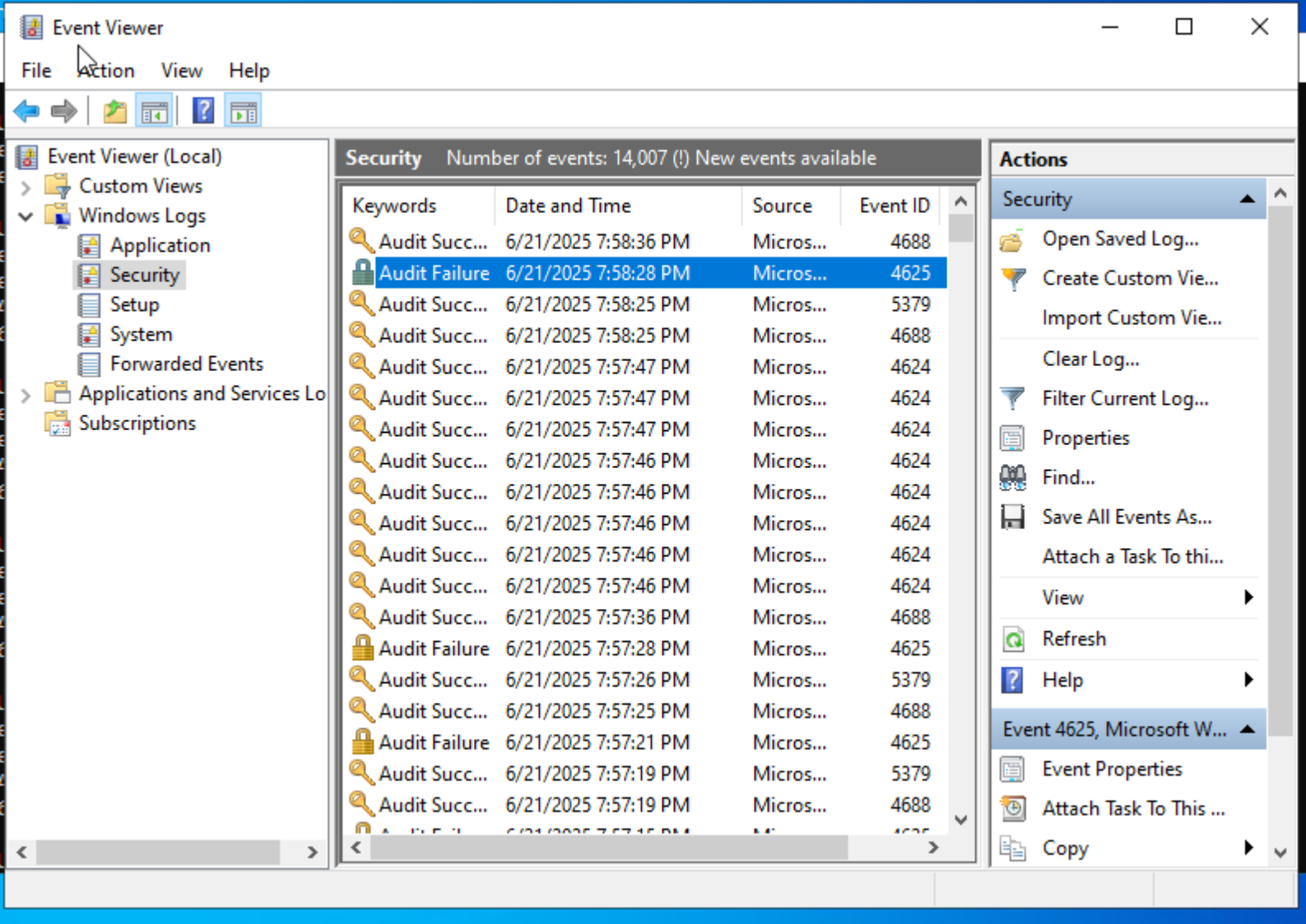
Select Windows PowerShell

```
        CC      Create child object
        DC      Delete a child object
                For these two permissions, if [Object/Property] is
                not specified to define a specific child object type,
                they apply all types of child objects otherwise they
                apply to that specific child object type.

        WS      Write To Self (also known as Validated Write). There
                are 3 kinds of validated writes:
                   Self-Membership (bf9679c0-0de6-11d0-a285-00aa003049e2)
                   applied to Group object. It allows updating membership
                   of a group in terms of adding/removing to its own account.
                Example: (WS; bf9679c0-0de6-11d0-a285-00aa003049e2; AU)
                applied to group X, allows an Authenticated User to
                add/remove oneself to/from group X, but not anybody else.
                   Validated-DNS-Host-Name (72e39547-7b18-11d1-adef-00c04fd8d5cd)
                   applied to computer object. It allows updating the
                   DNS host name attribute that is compliant with the
                   computer name & domain name.
                   Validated-SPN (f3a64788-5306-11d1-a9c5-0000f80367c1)
                   applied to computer object: It allows updating the SPN
                   attribute that is compliant to the DNS host name of the
                   computer.
        WP      Write property
        RP      Read property
                For these two permissions, if [Object/Property] is not
                specified to define a specific property, they apply to
                all properties of the object otherwise they apply to that
                specific property of the object.

        CA      Control access right
                For this permission, if [Object/Property] is not specified
                to define the specific "extended right" for control access,
                it applies to all control accesses meaningful on the
                object, otherwise it applies to the specific extended right
                for that object.
```

Select Windows PowerShell

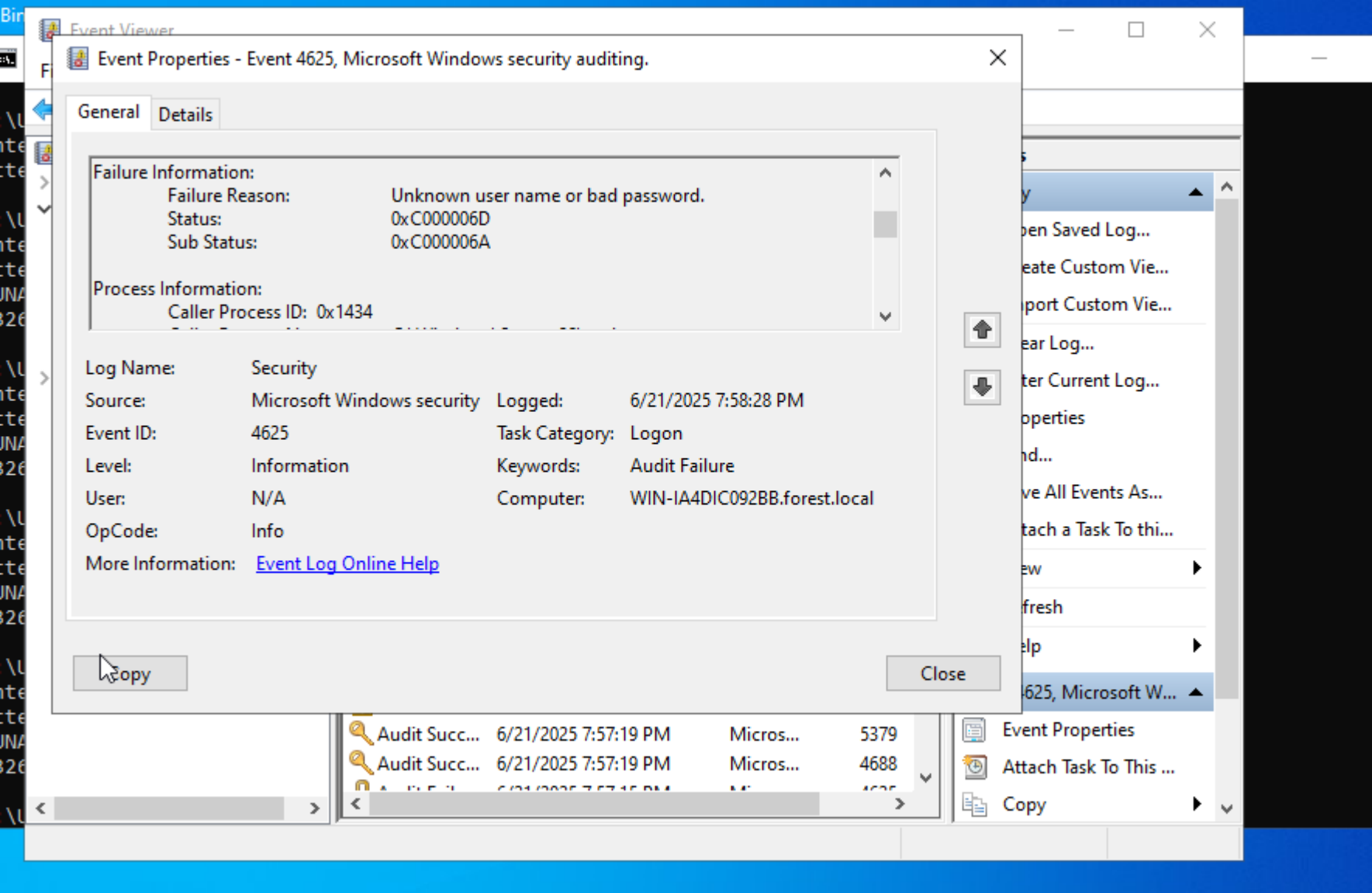
```
                this permission.

        [Object/Property]
        must be the display name of the object type or the property.
        for example "user" is the display name for user objects and
        "telephone number" is the display name for telephone number property.

        [Inherited Object Type]
        must be the display name of the object type that the permissions
        are expected to be inherited to. The permissions MUST be Inherit Only.

        NOTE: This must only be used when defining object specific permissions
        that override the default permissions defined in the AD DS schema for that
        object type.  USE THIS WITH CAUTION and ONLY IF YOU UNDERSTAND object
        specific permissions.


        Examples of a valid <perms> would be:

        SDRCWDWO;;user
        means:
        Delete, Read security information, Change security information and
        Change ownership permissions on objects of type "user".


        CCDC;group;
        means:
        Create child and Delete child permissions to create/delete objects
        of type group.

        RPWP;telephonenumber;
        means:
        read property and write property permissions on telephone number
        property

You can specify more than one user in a command.
The command completed successfully
PS C:\Users\yoojung> NEW-ADUSER -Name "TestUser" -Path $OU `  -AccountPassword (CONVERTTO-SECURESTRING "Pass123!" -ASPLAI
```

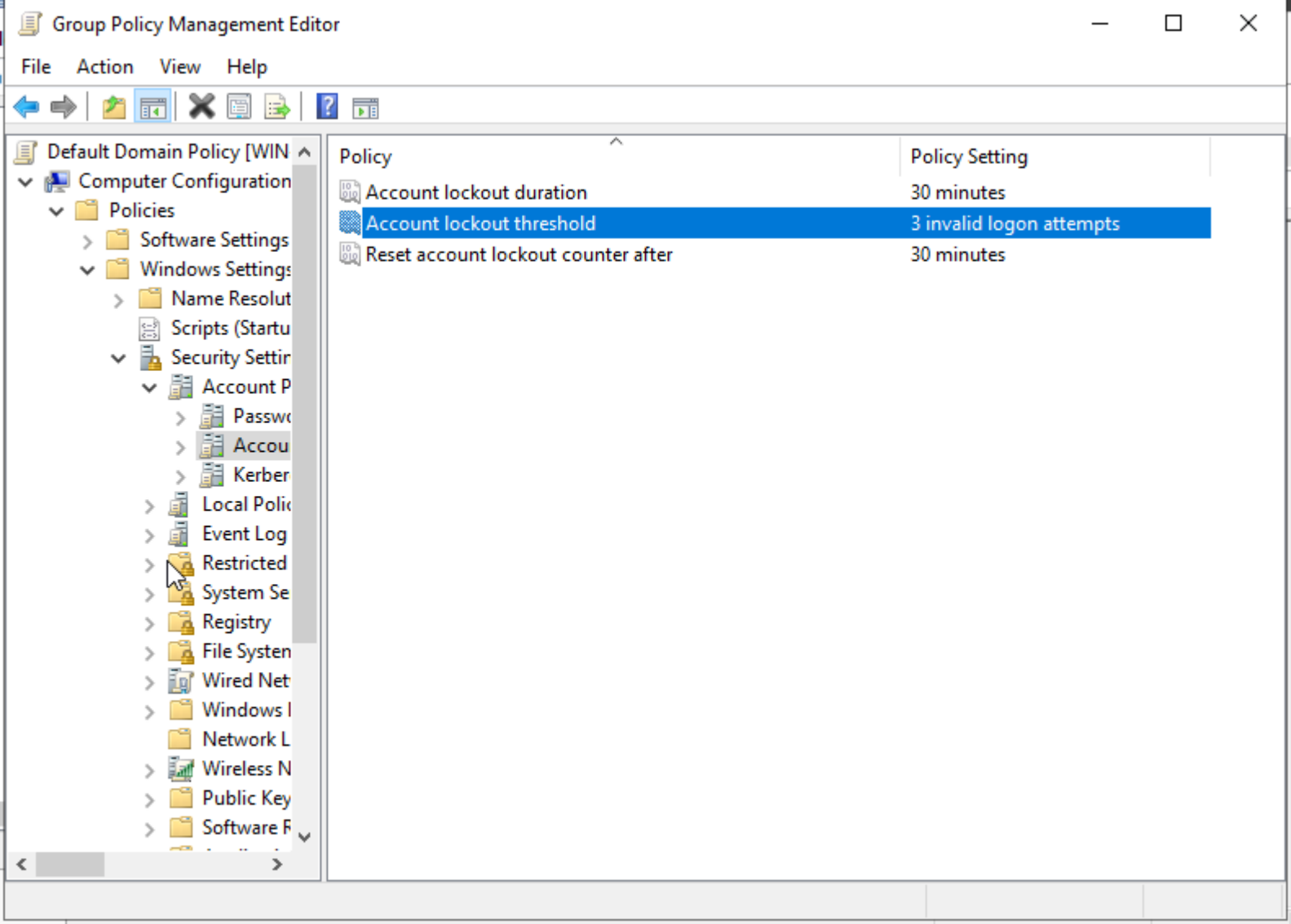

Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Lo
Subscriptions
Security Number of events: 13,645 (!) New events available
ords Date and Time Source Event ID Task C
dit Succ... 6/21/2025 6:28:24 PM Micros... 4688 Proces
dit Succ... 6/21/2025 6:28:23 PM Micros... 4688 Proces
dit Succ... 6/21/2025 6:28:20 PM Micros... 5379 User A
dit Succ... 6/21/2025 6:28:14 PM Micros... 4688 Proces
dit Succ... 6/21/2025 6:28:14 PM Micros... 4688 Proces
dit Succ... 6/21/2025 6:28:12 PM Micros... 4624 Logon
dit Succ... 6/21/2025 6:28:12 PM Micros... 4624 Logon
dit Succ... 6/21/2025 6:28:10 PM Micros... 5379 User A
dit Succ... 6/21/2025 6:28:10 PM Micros... 5379 User A
dit Succ... 6/21/2025 6:28:10 PM Micros... 5379 User A
dit Succ... 6/21/2025 6:28:10 PM Micros... 5379 User A
dit Succ... 6/21/2025 6:28:10 PM Micros... 5379 User A
dit Succ... 6/21/2025 6:28:10 PM Micros... 5379 User A
dit Succ... 6/21/2025 6:28:10 PM Micros... 5379 User A
dit Succ... 6/21/2025 6:28:10 PM Micros... 5379 User A
dit Succ... 6/21/2025 6:28:10 PM Micros... 5379 User A
dit Succ... 6/21/2025 6:28:10 PM Micros... 5379 User A
dit Succ... 6/21/2025 6:28:10 PM Micros... 5379 User A
Actions
Security
Open Saved Log...
Create Custom Vie...
Import Custom Vie...
Clear Log...
Filter Current Log...
Properties
Find...
Save All Events As...
Attach a Task To thi...
View
Refresh
Help
Event 5379, Microsoft W...
Event Properties
Attach Task To This ...
Copy

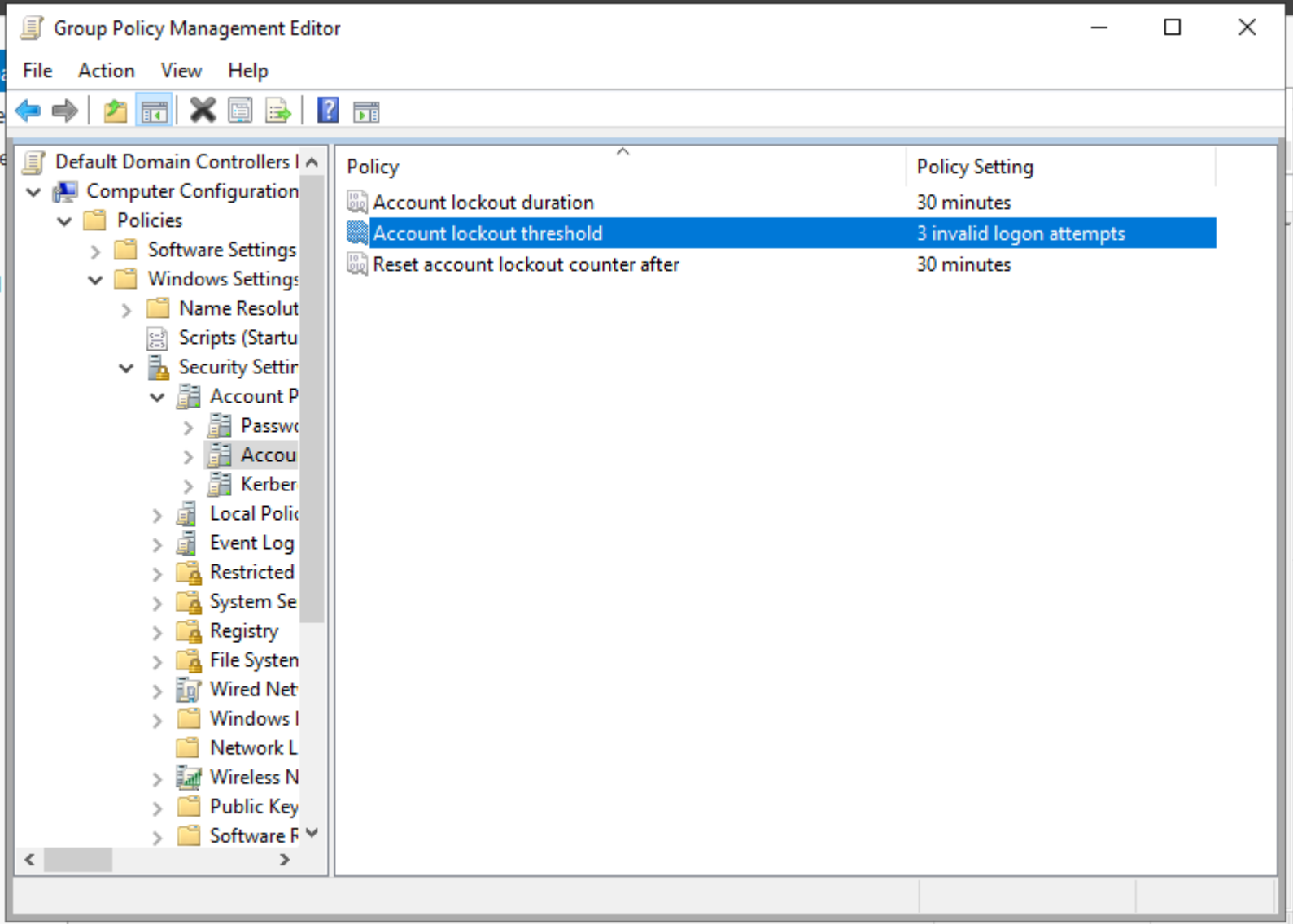

Event Viewer
File
Action
View
Help
Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Lo
Subscriptions
Security
Number of events: 14,007 (!) New events available
Keywords
Date and Time
Source
Event ID
Audit Succ... 6/21/2025 7:58:36 PM Micros... 4688
Audit Failure 6/21/2025 7:58:28 PM Micros... 4625
Audit Succ... 6/21/2025 7:58:25 PM Micros... 5379
Audit Succ... 6/21/2025 7:58:25 PM Micros... 4688
Audit Succ... 6/21/2025 7:57:47 PM Micros... 4624
Audit Succ... 6/21/2025 7:57:47 PM Micros... 4624
Audit Succ... 6/21/2025 7:57:47 PM Micros... 4624
Audit Succ... 6/21/2025 7:57:46 PM Micros... 4624
Audit Succ... 6/21/2025 7:57:46 PM Micros... 4624
Audit Succ... 6/21/2025 7:57:46 PM Micros... 4624
Audit Succ... 6/21/2025 7:57:46 PM Micros... 4624
Audit Succ... 6/21/2025 7:57:46 PM Micros... 4624
Audit Succ... 6/21/2025 7:57:36 PM Micros... 4688
Audit Failure 6/21/2025 7:57:28 PM Micros... 4625
Audit Succ... 6/21/2025 7:57:26 PM Micros... 5379
Audit Succ... 6/21/2025 7:57:25 PM Micros... 4688
Audit Failure 6/21/2025 7:57:21 PM Micros... 4625
Audit Succ... 6/21/2025 7:57:19 PM Micros... 5379
Audit Succ... 6/21/2025 7:57:19 PM Micros... 4688
Actions
Security
Open Saved Log...
Create Custom Vie...
Import Custom Vie...
Clear Log...
Filter Current Log...
Properties
Find...
Save All Events As...
Attach a Task To thi...
View
Refresh
Help
Event 4625, Microsoft W...
Event Properties
Attach Task To This ...
Copy

Administrator: Command Prompt

```
C:\Users\Administrator> runas /user:FOREST\adrien cmd
Enter the password for FOREST\adrien:
Attempting to start cmd as user "FOREST\adrien" ...

C:\Users\Administrator> runas /user:FOREST\adrien cmd
Enter the password for FOREST\adrien:
Attempting to start cmd as user "FOREST\adrien" ...
RUNAS ERROR: Unable to run - cmd
1326: The user name or password is incorrect.

C:\Users\Administrator> runas /user:FOREST\adrien cmd
Enter the password for FOREST\adrien:
Attempting to start cmd as user "FOREST\adrien" ...
RUNAS ERROR: Unable to run - cmd
1326: The user name or password is incorrect.

C:\Users\Administrator> runas /user:FOREST\adrien cmd
Enter the password for FOREST\adrien:
Attempting to start cmd as user "FOREST\adrien" ...
RUNAS ERROR: Unable to run - cmd
1326: The user name or password is incorrect.

C:\Users\Administrator> runas /user:FOREST\adrien cmd
Enter the password for FOREST\adrien:
Attempting to start cmd as user "FOREST\adrien" ...
RUNAS ERROR: Unable to run - cmd
1326: The user name or password is incorrect.

C:\Users\Administrator>
```

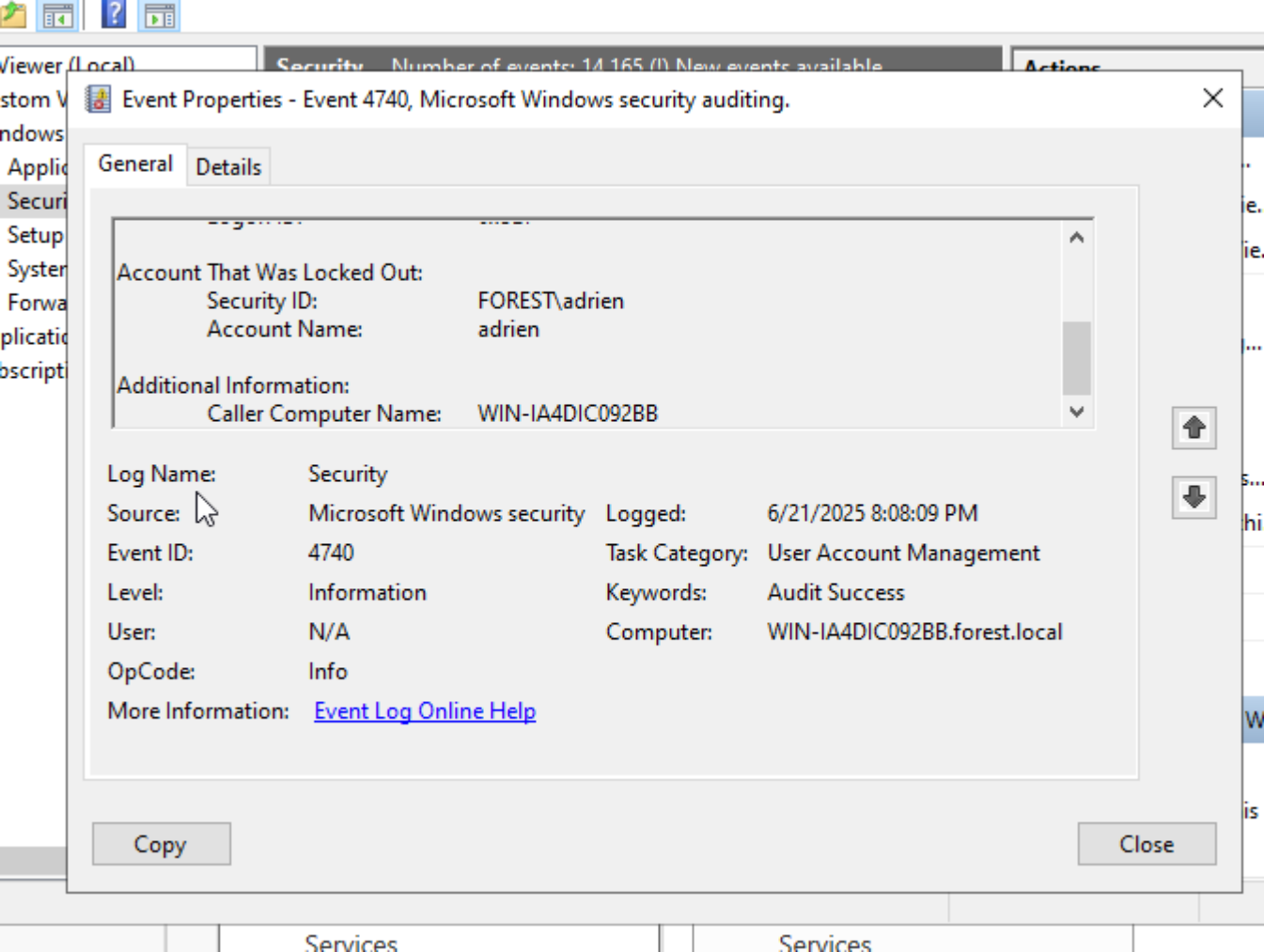

Event Viewer
Event Properties - Event 4625, Microsoft Windows security auditing.
General
Details
Failure Information:
Failure Reason: Unknown user name or bad password.
Status: 0xC000006D
Sub Status: 0xC000006A
Process Information:
Caller Process ID: 0x1434
Log Name: Security
Source: Microsoft Windows security
Logged: 6/21/2025 7:58:28 PM
Event ID: 4625
Task Category: Logon
Level: Information
Keywords: Audit Failure
User: N/A
Computer: WIN-IA4DIC092BB.forest.local
OpCode: Info
More Information: Event Log Online Help
Copy
Close
Audit Succ... 6/21/2025 7:57:19 PM Micros... 5379
Audit Succ... 6/21/2025 7:57:19 PM Micros... 4688
Event Properties
Attach Task To This ...
Copy

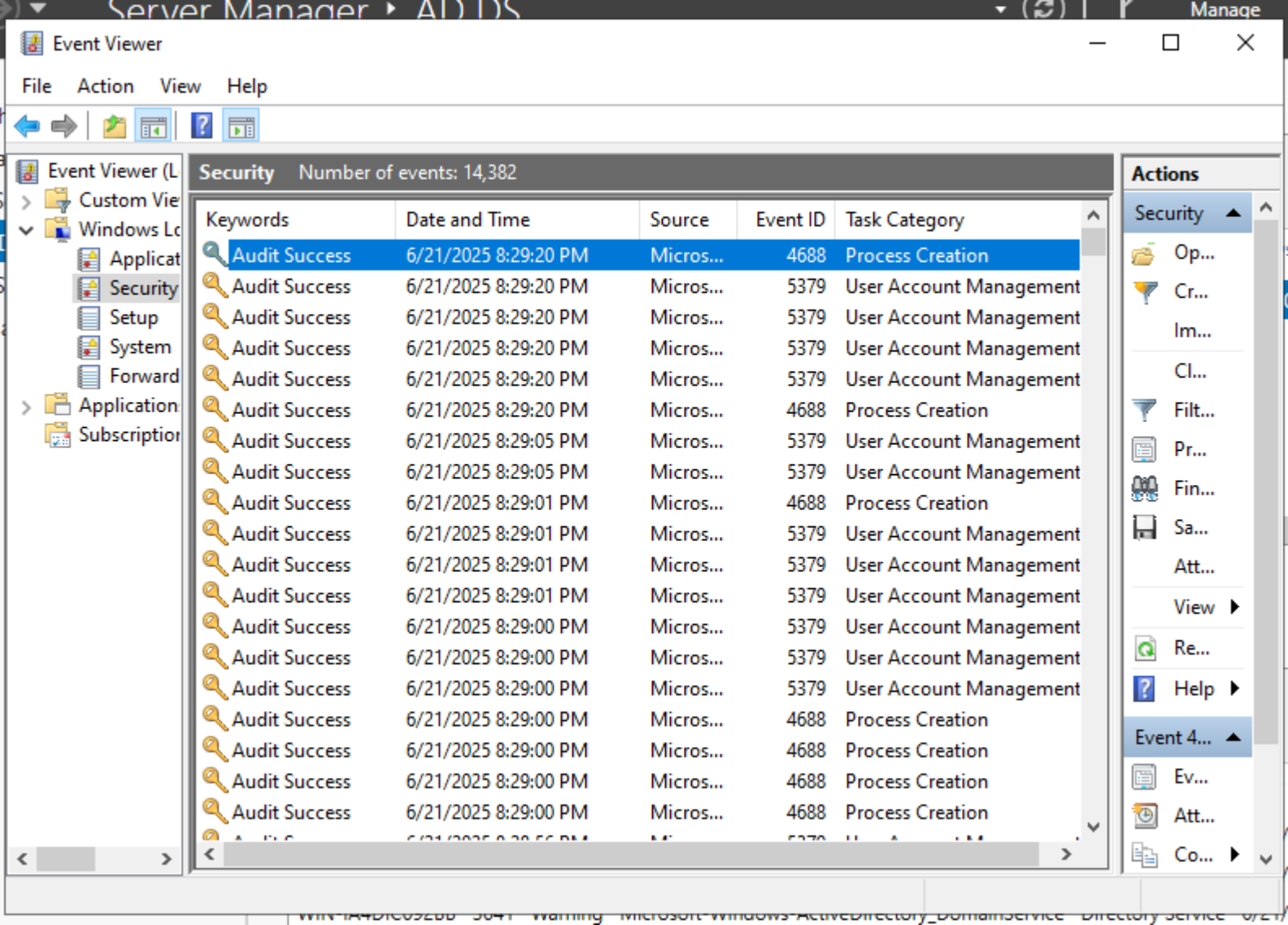

Group Policy Management Editor
File
Action
View
Help
Default Domain Policy [WIN
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolut
Scripts (Startu
Security Settir
Account P
Passwo
Accou
Kerber
Local Polic
Event Log
Restricted
System Se
Registry
File Systen
Wired Net
Windows I
Network L
Wireless N
Public Key
Software F
Policy
Policy Setting
Account lockout duration
30 minutes
Account lockout threshold
3 invalid logon attempts
Reset account lockout counter after
30 minutes

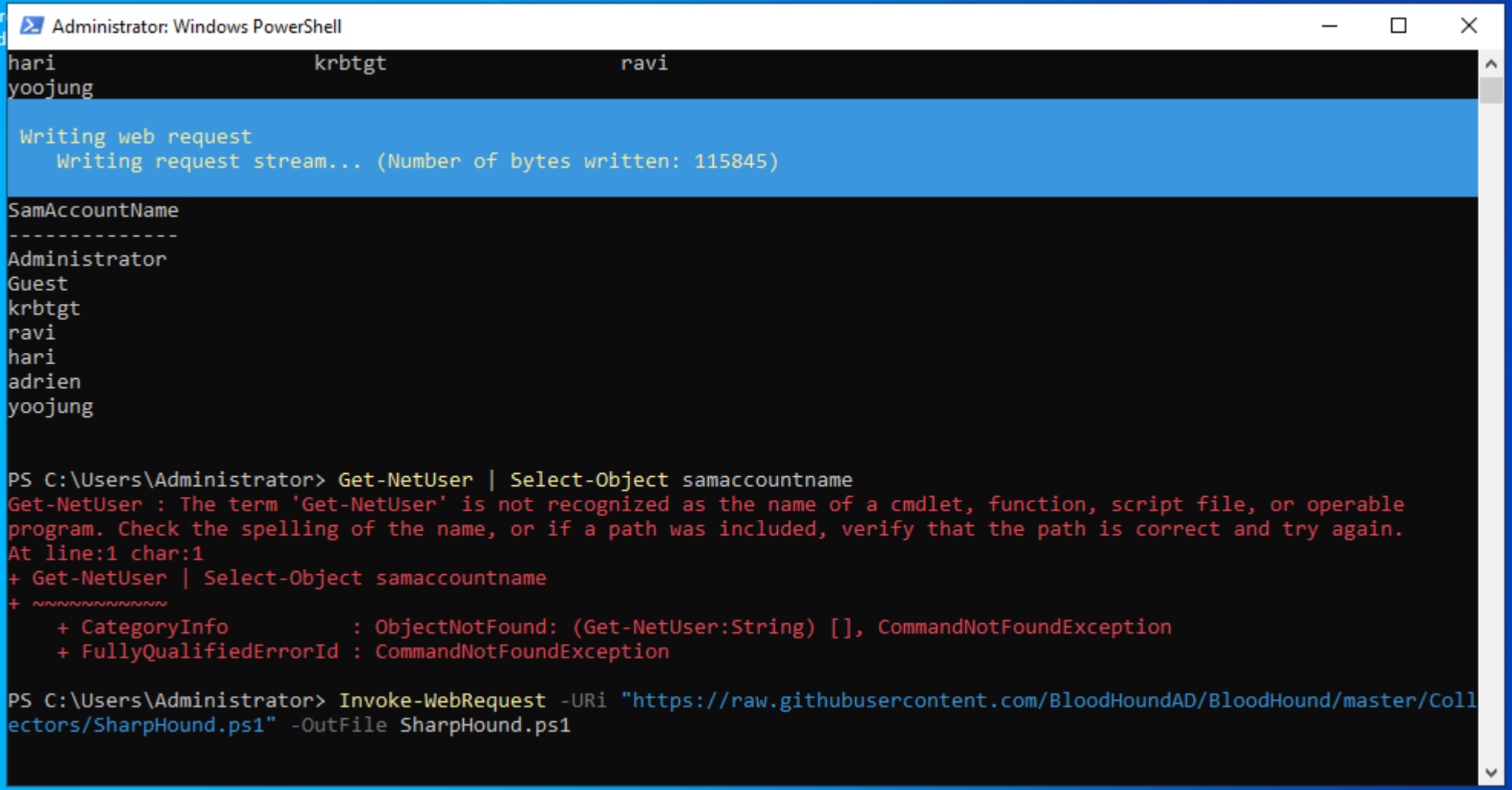

Group Policy Management Editor
File
Action
View
Help
Default Domain Controllers I
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolut
Scripts (Startu
Security Settir
Account P
Passwo
Accou
Kerber
Local Polic
Event Log
Restricted
System Se
Registry
File Systen
Wired Net
Windows I
Network L
Wireless N
Public Key
Software R
Policy
Policy Setting
Account lockout duration
30 minutes
Account lockout threshold
3 invalid logon attempts
Reset account lockout counter after
30 minutes

Administrator: Command Prompt

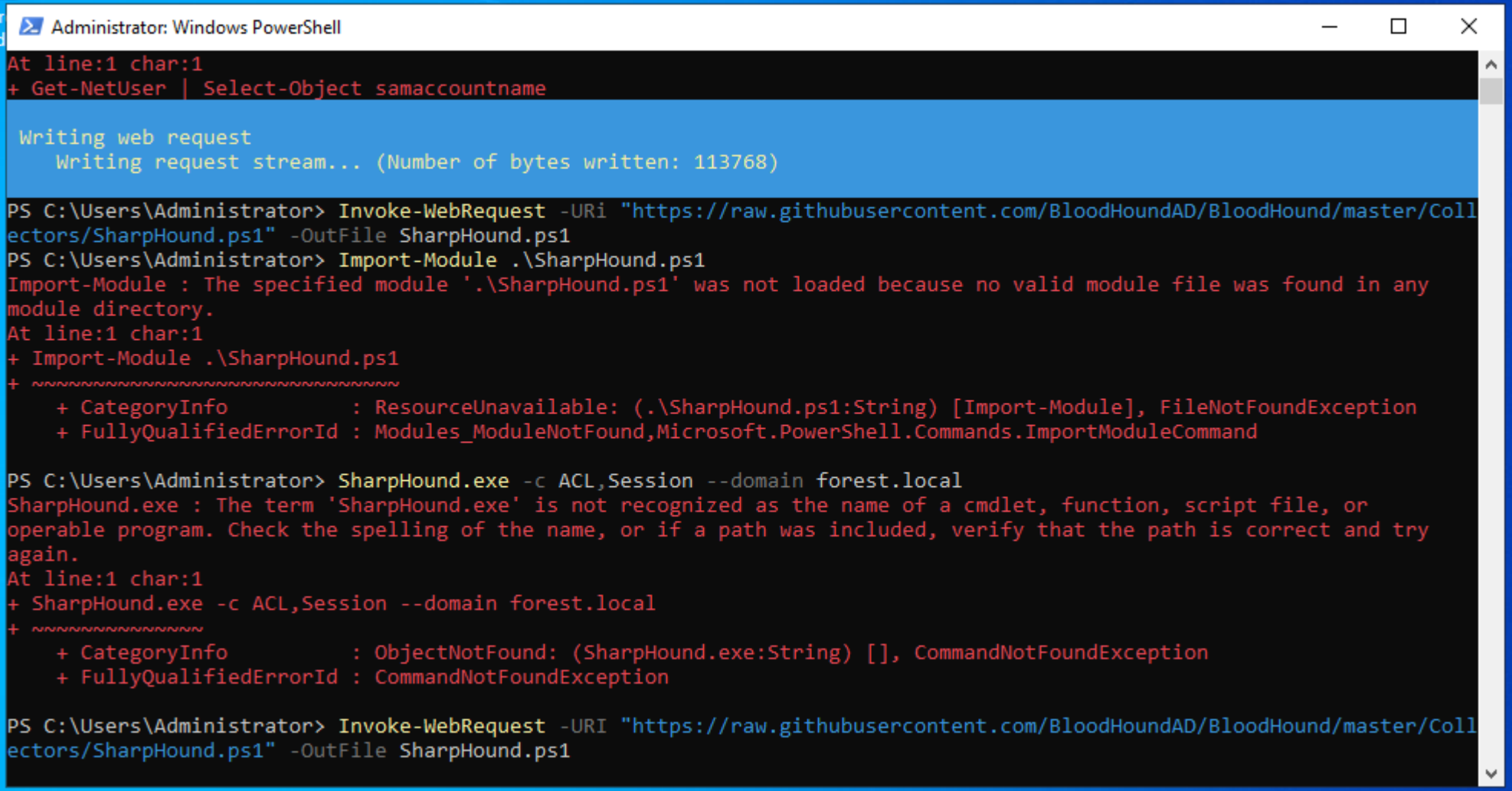
```
Enter the password for FOREST\adrien:
Attempting to start cmd as user "FOREST\adrien" ...
RUNAS ERROR: Unable to run - cmd
1326: The user name or password is incorrect.

C:\Users\Administrator> runas /user:FOREST\adrien cmd
Enter the password for FOREST\adrien:
Attempting to start cmd as user "FOREST\adrien" ...
RUNAS ERROR: Unable to run - cmd
1326: The user name or password is incorrect.

C:\Users\Administrator> runas /user:FOREST\adrien cmd
Enter the password for FOREST\adrien:
Attempting to start cmd as user "FOREST\adrien" ...
RUNAS ERROR: Unable to run - cmd
1909: The referenced account is currently locked out and may not be logged on to.

C:\Users\Administrator> runas /user:FOREST\adrien cmd
Enter the password for FOREST\adrien:
Attempting to start cmd as user "FOREST\adrien" ...
RUNAS ERROR: Unable to run - cmd
1909: The referenced account is currently locked out and may not be logged on to.

C:\Users\Administrator> runas /user:FOREST\adrien cmd
Enter the password for FOREST\adrien:
Attempting to start cmd as user "FOREST\adrien" ...
RUNAS ERROR: Unable to run - cmd
1909: The referenced account is currently locked out and may not be logged on to.

C:\Users\Administrator>
```

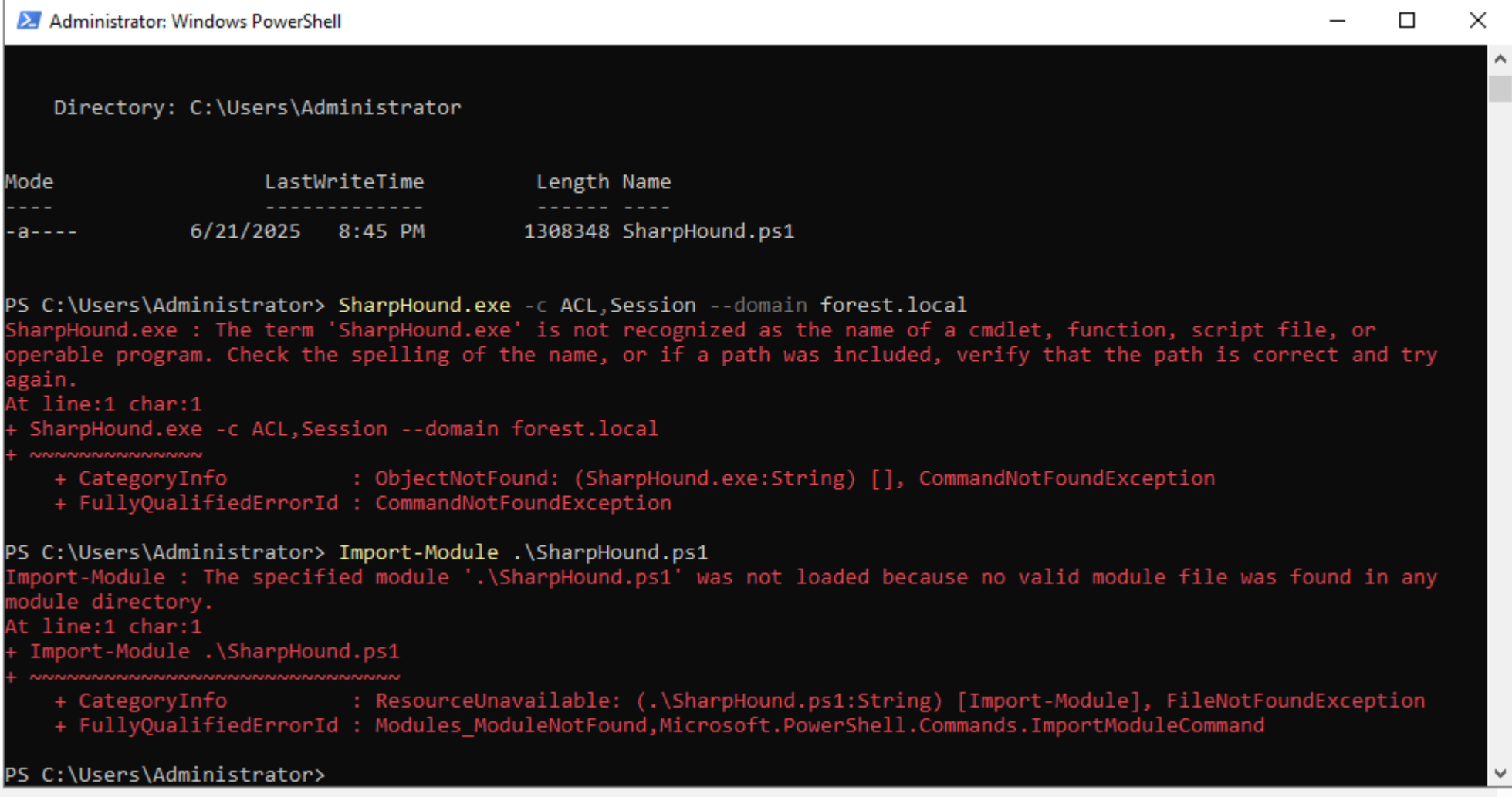

Event Properties - Event 4740, Microsoft Windows security auditing.
General
Details
Account That Was Locked Out:
Security ID: FOREST\adrien
Account Name: adrien
Additional Information:
Caller Computer Name: WIN-IA4DIC092BB
Log Name: Security
Source: Microsoft Windows security
Logged: 6/21/2025 8:08:09 PM
Event ID: 4740
Task Category: User Account Management
Level: Information
Keywords: Audit Success
User: N/A
Computer: WIN-IA4DIC092BB.forest.local
OpCode: Info
More Information: Event Log Online Help
Copy
Close


Server Manager ▸ AD DS
Manage
Event Viewer
File Action View Help
Event Viewer (L
Custom Vie
Windows Lo
Applicat
Security
Setup
System
Forward
Application
Subscriptio
Security Number of events: 14,382
Keywords Date and Time Source Event ID Task Category
Audit Success 6/21/2025 8:29:20 PM Micros... 4688 Process Creation
Audit Success 6/21/2025 8:29:20 PM Micros... 5379 User Account Management
Audit Success 6/21/2025 8:29:20 PM Micros... 5379 User Account Management
Audit Success 6/21/2025 8:29:20 PM Micros... 5379 User Account Management
Audit Success 6/21/2025 8:29:20 PM Micros... 5379 User Account Management
Audit Success 6/21/2025 8:29:20 PM Micros... 4688 Process Creation
Audit Success 6/21/2025 8:29:05 PM Micros... 5379 User Account Management
Audit Success 6/21/2025 8:29:05 PM Micros... 5379 User Account Management
Audit Success 6/21/2025 8:29:01 PM Micros... 4688 Process Creation
Audit Success 6/21/2025 8:29:01 PM Micros... 5379 User Account Management
Audit Success 6/21/2025 8:29:01 PM Micros... 5379 User Account Management
Audit Success 6/21/2025 8:29:01 PM Micros... 5379 User Account Management
Audit Success 6/21/2025 8:29:00 PM Micros... 5379 User Account Management
Audit Success 6/21/2025 8:29:00 PM Micros... 5379 User Account Management
Audit Success 6/21/2025 8:29:00 PM Micros... 5379 User Account Management
Audit Success 6/21/2025 8:29:00 PM Micros... 4688 Process Creation
Audit Success 6/21/2025 8:29:00 PM Micros... 4688 Process Creation
Audit Success 6/21/2025 8:29:00 PM Micros... 4688 Process Creation
Audit Success 6/21/2025 8:29:00 PM Micros... 4688 Process Creation
Actions
Security
Op...
Cr...
Im...
Cl...
Filt...
Pr...
Fin...
Sa...
Att...
View
Re...
Help
Event 4...
Ev...
Att...
Co...

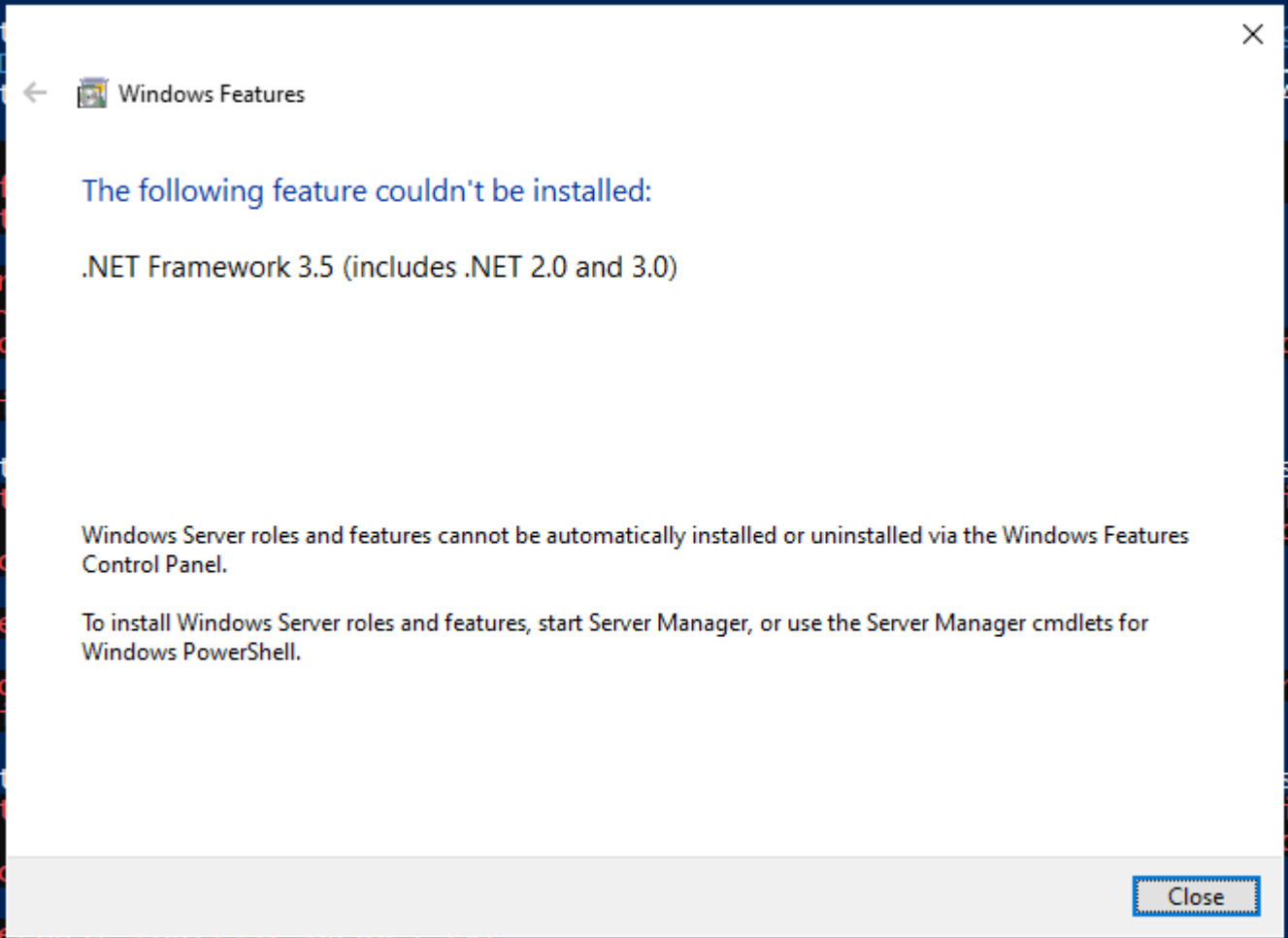

Administrator: Windows PowerShell
hari krbtgt ravi
yoojung
Writing web request
Writing request stream... (Number of bytes written: 115845)
SamAccountName
Administrator
Guest
krbtgt
ravi
hari
adrien
yoojung
PS C:\Users\Administrator> Get-NetUser | Select-Object samaccountname
Get-NetUser : The term 'Get-NetUser' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:1
+ Get-NetUser | Select-Object samaccountname
+ ~~~~~~~~~~~
+ CategoryInfo : ObjectNotFound: (Get-NetUser:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException
PS C:\Users\Administrator> Invoke-WebRequest -URi "https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/Collectors/SharpHound.ps1" -OutFile SharpHound.ps1

```
PS C:\Users\Administrator> Invoke-WebRequest -URi "https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/Collectors/SharpHound.ps1" -OutFile SharpHound.ps1
PS C:\Users\Administrator> Import-Module .\SharpHound.ps1
Import-Module : The specified module '.\SharpHound.ps1' was not loaded because no valid module file was found in any
module directory.
At line:1 char:1
+ Import-Module .\SharpHound.ps1
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ResourceUnavailable: (.\SharpHound.ps1:String) [Import-Module], FileNotFoundException
    + FullyQualifiedErrorId : Modules_ModuleNotFound,Microsoft.PowerShell.Commands.ImportModuleCommand
```


Administrator: Windows PowerShell
At line:1 char:1
+ Get-NetUser | Select-Object samaccountname
Writing web request
Writing request stream... (Number of bytes written: 113768)
PS C:\Users\Administrator> Invoke-WebRequest -URi "https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/Collectors/SharpHound.ps1" -OutFile SharpHound.ps1
PS C:\Users\Administrator> Import-Module .\SharpHound.ps1
Import-Module : The specified module '.\SharpHound.ps1' was not loaded because no valid module file was found in any module directory.
At line:1 char:1
+ Import-Module .\SharpHound.ps1
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
+ CategoryInfo : ResourceUnavailable: (.\SharpHound.ps1:String) [Import-Module], FileNotFoundException
+ FullyQualifiedErrorId : Modules_ModuleNotFound,Microsoft.PowerShell.Commands.ImportModuleCommand
PS C:\Users\Administrator> SharpHound.exe -c ACL,Session --domain forest.local
SharpHound.exe : The term 'SharpHound.exe' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:1
+ SharpHound.exe -c ACL,Session --domain forest.local
+ ~~~~~~~~~~~~~~~
+ CategoryInfo : ObjectNotFound: (SharpHound.exe:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException
PS C:\Users\Administrator> Invoke-WebRequest -URI "https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/Collectors/SharpHound.ps1" -OutFile SharpHound.ps1


Administrator: Windows PowerShell
Directory: C:\Users\Administrator
Mode LastWriteTime Length Name
---- ------------- ------ ----
-a---- 6/21/2025 8:45 PM 1308348 SharpHound.ps1
PS C:\Users\Administrator> SharpHound.exe -c ACL,Session --domain forest.local
SharpHound.exe : The term 'SharpHound.exe' is not recognized as the name of a cmdlet, function, script file, or
operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try
again.
At line:1 char:1
+ SharpHound.exe -c ACL,Session --domain forest.local
+ ~~~~~~~~~~~~~~~
+ CategoryInfo : ObjectNotFound: (SharpHound.exe:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException
PS C:\Users\Administrator> Import-Module .\SharpHound.ps1
Import-Module : The specified module '.\SharpHound.ps1' was not loaded because no valid module file was found in any
module directory.
At line:1 char:1
+ Import-Module .\SharpHound.ps1
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
+ CategoryInfo : ResourceUnavailable: (.\SharpHound.ps1:String) [Import-Module], FileNotFoundException
+ FullyQualifiedErrorId : Modules_ModuleNotFound,Microsoft.PowerShell.Commands.ImportModuleCommand
PS C:\Users\Administrator>

```
PS C:\Users\Administrator> . .\SharpHound.ps1
PS C:\Users\Administrator> Invoke-BloodHound -CollectionMethod ACL,Session -Domain forest.local
Exception calling "Load" with "1" argument(s): "Could not load file or assembly '1046528 bytes loaded from Anonymously
Hosted DynamicMethods Assembly, Version=0.0.0.0, Culture=neutral, PublicKeyToken=null' or one of its dependencies. An
attempt was made to load a program with an incorrect format."
At C:\Users\Administrator\SharpHound.ps1:413 char:2
+     $Assembly = [Reflection.Assembly]::Load($UncompressedFileBytes)
+     ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [], MethodInvocationException
    + FullyQualifiedErrorId : BadImageFormatException

You cannot call a method on a null-valued expression.
At C:\Users\Administrator\SharpHound.ps1:416 char:2
+     $Assembly.GetType("Costura.AssemblyLoader", $false).GetMethod("At ...
+     ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (:) [], RuntimeException
    + FullyQualifiedErrorId : InvokeMethodOnNull

You cannot call a method on a null-valued expression.
At C:\Users\Administrator\SharpHound.ps1:417 char:2
+     $Assembly.GetType("Sharphound.Program").GetMethod("InvokeSharpHou ...
+     ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (:) [], RuntimeException
    + FullyQualifiedErrorId : InvokeMethodOnNull
```


Windows Features
The following feature couldn't be installed:
.NET Framework 3.5 (includes .NET 2.0 and 3.0)
Windows Server roles and features cannot be automatically installed or uninstalled via the Windows Features Control Panel.
To install Windows Server roles and features, start Server Manager, or use the Server Manager cmdlets for Windows PowerShell.
Close