How to List Domain Admins Using PowerShell

Task. List Domain Admins using PowerShell.

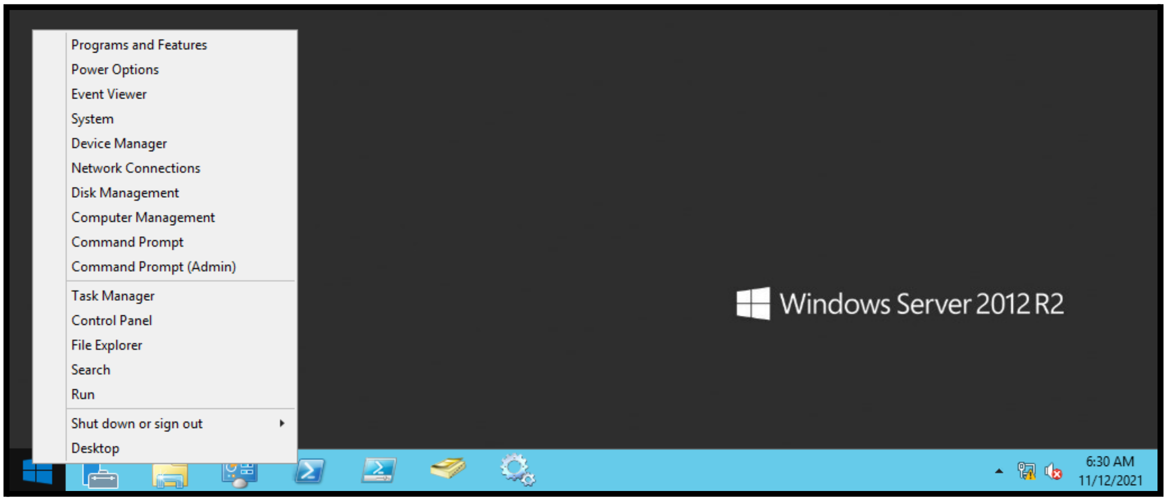
Purpose. The Domain Admins group must be monitored for unauthorized changes. Domain Admins have full control over all servers and workstations within the domain. Adversaries may seek to obtain and abuse these credentials as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion.

Conditions. You have domain administrator privileges, access to Windows PowerShell, and access to either a domain controller or a workstation with Remote Server Administration Tools (RSAT) installed.

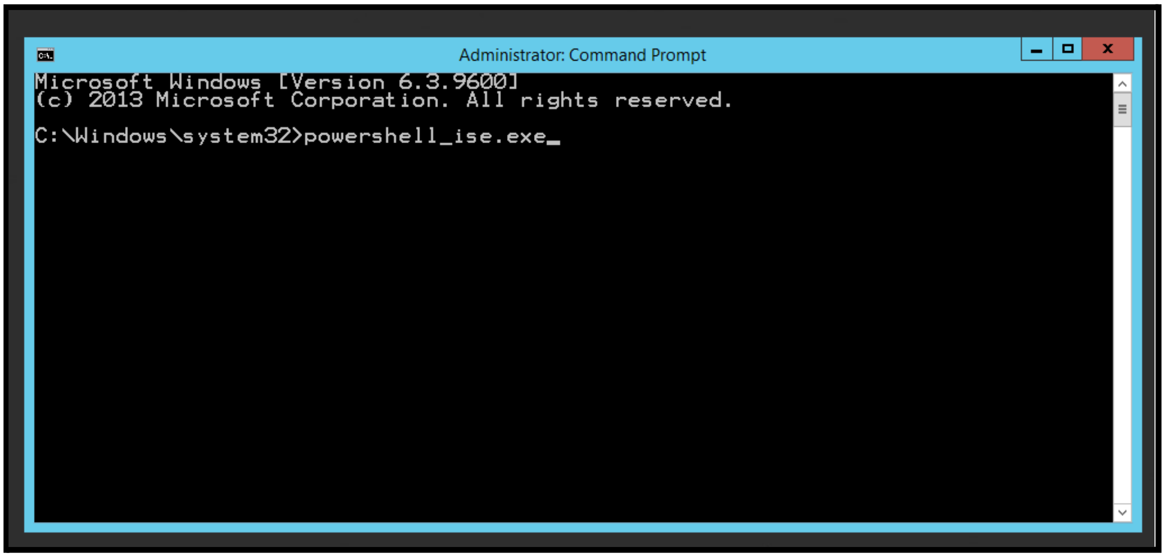
Standard. You were able to list the members of the Domain Admins group using PowerShell.

Step 1. Login to your domain administrator account on either a domain controller or a workstation with RSAT installed.

Step 2. Right-click on the Windows icon in the bottom-left corner and select “Command Prompt (Admin)” to start an elevated Command Prompt session.



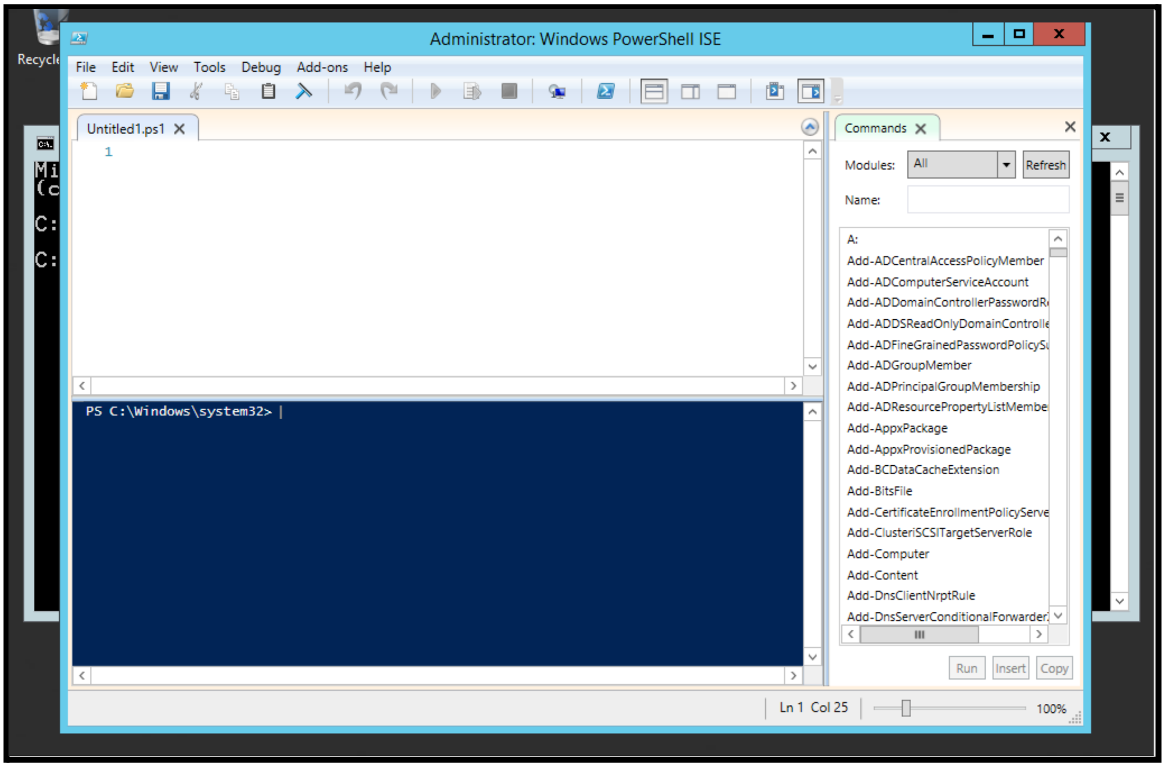
Step 3. Type “powershell_ise.exe” to invoke Windows PowerShell ISE.



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>powershell_ise.exe_
```

Once your point-of-view looks like the screenshot below, click-on the “Maximize” button in the top-right corner of the Windows PowerShell ISE window. Then, close the “Command” pane on the right.


Recycle
Administrator: Windows PowerShell ISE
File
Edit
View
Tools
Debug
Add-ons
Help
Untitled1.ps1
1
Commands
Modules:
All
Refresh
Name:
A:
Add-ADCentralAccessPolicyMember
Add-ADComputerServiceAccount
Add-ADDomainControllerPasswordR
Add-ADDSReadOnlyDomainControlle
Add-ADFineGrainedPasswordPolicyS
Add-ADGroupMember
Add-ADPrincipalGroupMembership
Add-ADResourcePropertyListMembe
Add-AppxPackage
Add-AppxProvisionedPackage
Add-BCDataCacheExtension
Add-BitsFile
Add-CertificateEnrollmentPolicyServe
Add-ClusteriSCSITargetServerRole
Add-Computer
Add-Content
Add-DnsClientNrptRule
Add-DnsServerConditionalForwarder
Run
Insert
Copy
Ln 1 Col 25
100%

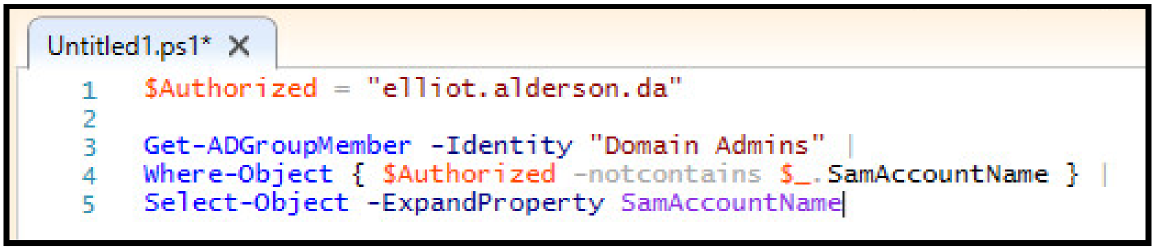
```
PS C:\Windows\system32> |
```

Step 5. Type the command sentences below in the Script pane of Windows PowerShell ISE. The first sentence services to specify which accounts are authorized to be a member of the Domain Administrators group. The remaining sentences query the Domain Controller and filter out the authorized accounts you declared with the first sentence. If you want to whitelist another account, add their SAM account name to the “Authorized” variable.

```
$Authorized = "elliot.alderson.da"

Get-AdGroupMember -Identity "Domain Admins" |
Where-Object { $Authorized -notcontains $_.SamAccountName } |
Select-Object -ExpandProperty SamAccountName
```

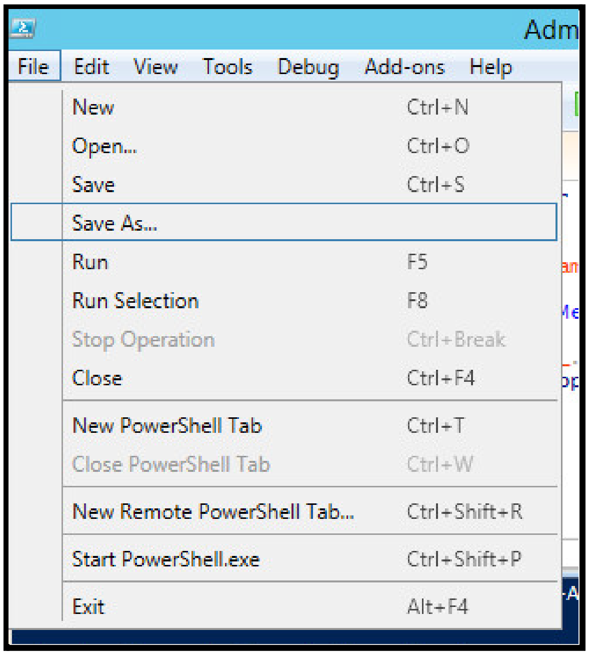
Your point-of-view should look like the screenshot below.



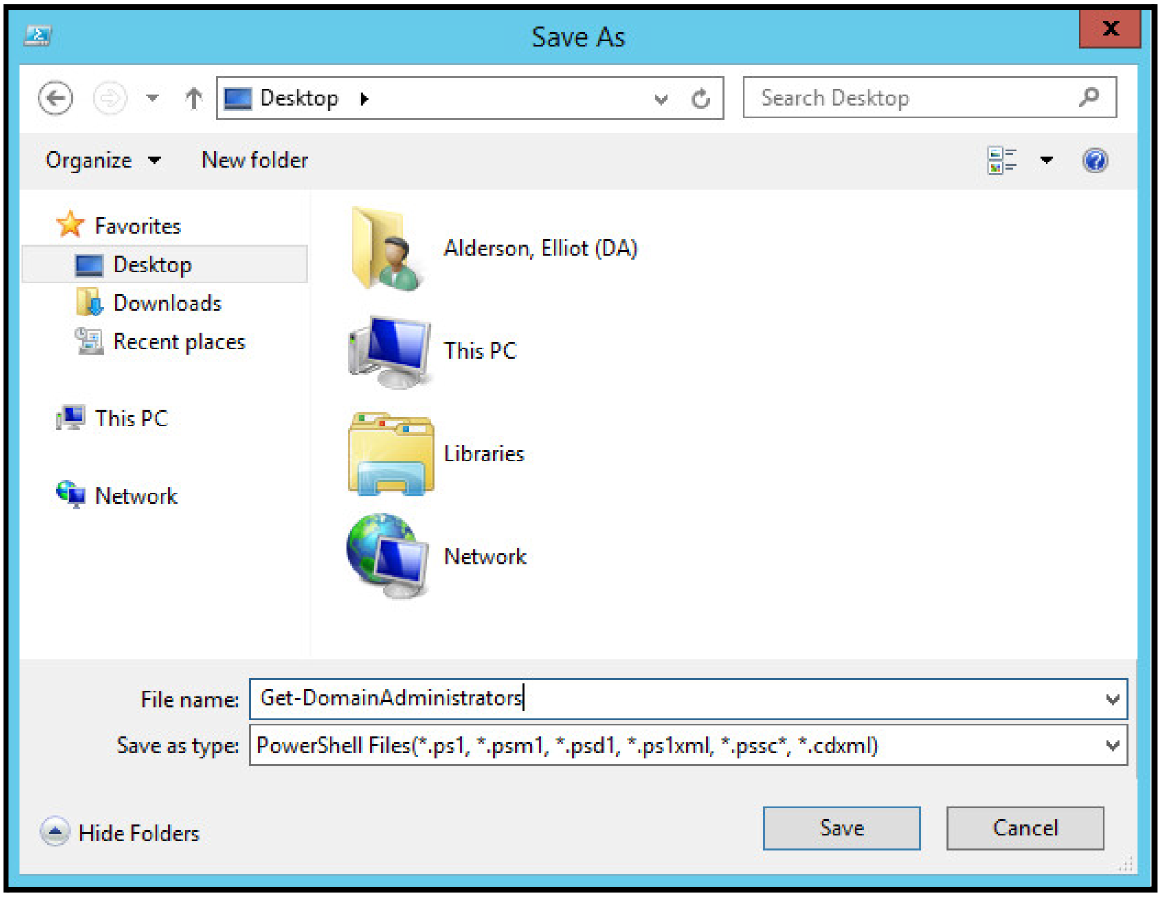
```
$Authorized = "elliot.alderson.da"

Get-ADGroupMember -Identity "Domain Admins" |
Where-Object { $Authorized -notcontains $_.SamAccountName } |
Select-Object -ExpandProperty SamAccountName
```

Step 7. Click-on “File > Save As…”


Adm
File
Edit
View
Tools
Debug
Add-ons
Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Run F5
Run Selection F8
Stop Operation Ctrl+Break
Close Ctrl+F4
New PowerShell Tab Ctrl+T
Close PowerShell Tab Ctrl+W
New Remote PowerShell Tab... Ctrl+Shift+R
Start PowerShell.exe Ctrl+Shift+P
Exit Alt+F4

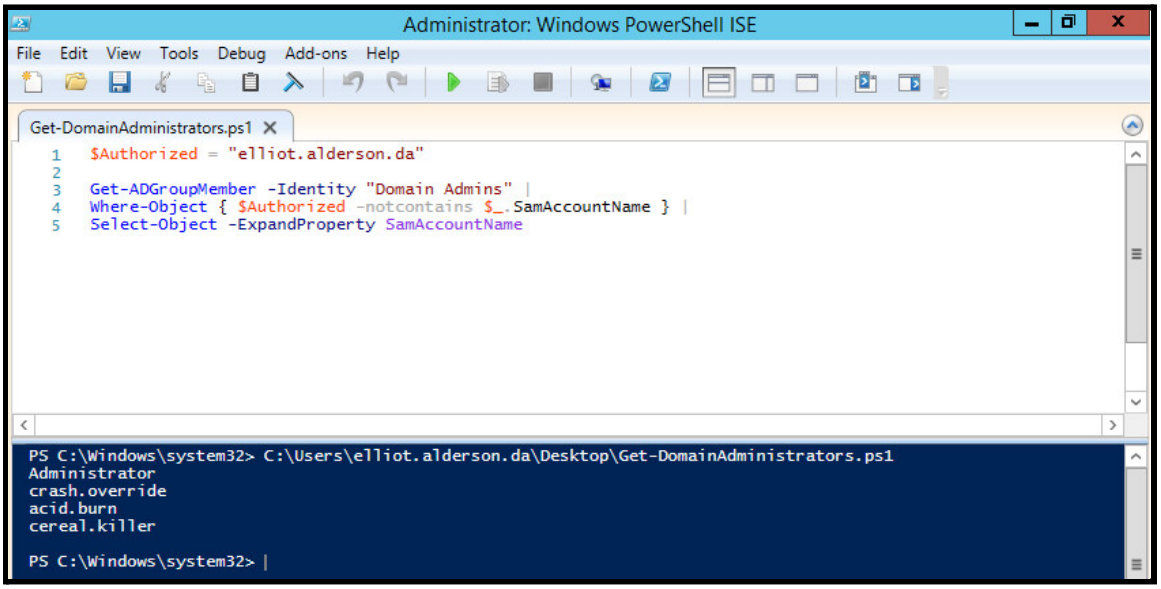
When prompted, save the file to the “Desktop” and call it “Get-DomainAdministrators.”



File name: Get-DomainAdministrators

Save as type: PowerShell Files(*.ps1, *.psm1, *.psd1, *.ps1xml, *.pssc*, *.cdxml)

Step 7. Click-on the “Run Script” button (it looks like a green “play” symbol). The resulting output represents who is currently an unauthorized member of the Domain Admins group.


Administrator: Windows PowerShell ISE
File
Edit
View
Tools
Debug
Add-ons
Help
Get-DomainAdministrators.ps1

```powershell
$Authorized = "elliot.alderson.da"

Get-ADGroupMember -Identity "Domain Admins" |
Where-Object { $Authorized -notcontains $_.SamAccountName } |
Select-Object -ExpandProperty SamAccountName
```

```
PS C:\Windows\system32> C:\Users\elliot.alderson.da\Desktop\Get-DomainAdministrators.ps1
Administrator
crash.override
acid.burn
cereal.killer

PS C:\Windows\system32> |
```