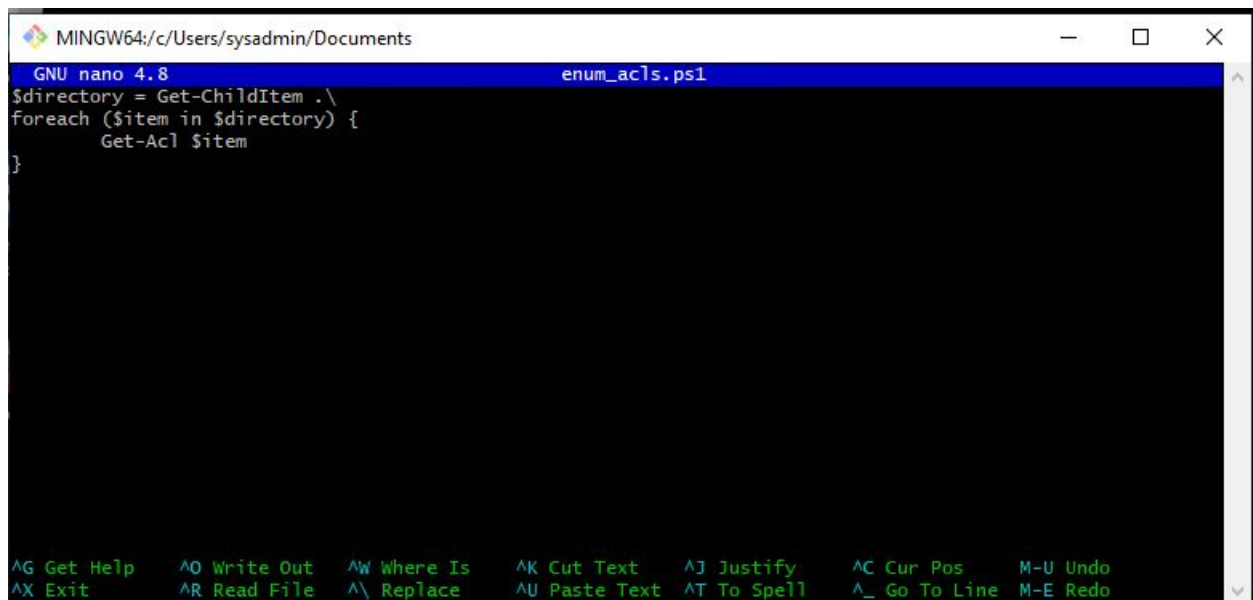


## Task 4: Create a Script: Enumerate Access Control Lists

Solution:

Log into the nested Windows 10, open **git bash**, and navigate to the path: **C:\Users\sysadmin\Documents**, and run **nano enum\_acls.ps1** to open the nano editor.

Enter the foreach loop script shown below, and save.



The screenshot shows a terminal window titled "MINGW64:/c/Users/sysadmin/Documents". Inside, the nano 4.8 editor is open with a file named "enum\_acls.ps1". The script content is as follows:

```
$directory = Get-ChildItem .\  
foreach ($item in $directory) {  
    Get-Acl $item  
}
```

The bottom of the window displays nano editor shortcuts: ^G Get Help, ^O Write Out, ^W Where Is, ^K Cut Text, ^J Justify, ^C Cur Pos, M-U Undo, ^X Exit, ^R Read File, ^\ Replace, ^U Paste Text, ^T To Spell, ^\_ Go To Line, M-E Redo.

Testing the script:

Launch **PowerShell**, navigate to **Documents** directory and run the **enum\_acls.ps1** script

```
Administrator: Windows PowerShell

PS C:\Windows> cd C:\Users\sysadmin\Documents\
PS C:\Users\sysadmin\Documents> ls

Directory: C:\Users\sysadmin\Documents

Mode                LastWriteTime         Length Name
----                -
d-----          9/27/2020   11:56 PM             20200927
d-----          9/28/2020   12:56 AM             20200928
-a----          9/28/2020    1:06 AM             79 enum_acls.ps1
-a----          2/20/2020    1:35 AM            1651 microsoftbloat.csv

PS C:\Users\sysadmin\Documents> .\enum_acls.ps1

Directory: C:\Users\sysadmin\Documents

Path                Owner                Access
----                -
20200927             BUILTIN\Administrators NT AUTHORITY\SYSTEM Allow FullControl...
20200928             BUILTIN\Administrators NT AUTHORITY\SYSTEM Allow FullControl...
enum_acls.ps1        DESKTOP-U3FCUKI\sysadmin NT AUTHORITY\SYSTEM Allow FullControl...
microsoftbloat.csv   BUILTIN\Administrators NT AUTHORITY\SYSTEM Allow FullControl...

PS C:\Users\sysadmin\Documents> █
```

Move to another directory path, **C:\Windows** and run the **enum\_acls.ps1** script by running it with the full path and the file name (**C:\Users\sysadmin\Documents\enum\_acls.ps1**).

## Administrator: Windows PowerShell

```
-----
20200927      BUILTIN\Administrators  NT AUTHORITY\SYSTEM Allow  FullControl...
20200928      BUILTIN\Administrators  NT AUTHORITY\SYSTEM Allow  FullControl...
enum_acls.ps1  DESKTOP-U3FCUKI\sysadmin NT AUTHORITY\SYSTEM Allow  FullControl...
microsoftbloat.csv BUILTIN\Administrators  NT AUTHORITY\SYSTEM Allow  FullControl...

PS C:\Users\sysadmin\Documents> cd C:\Windows\
PS C:\Windows> C:\Users\sysadmin\Documents\enum_acls.ps1

Directory: C:\Windows

Path                Owner                Access
-----
addins              NT SERVICE\TrustedInstaller  CREATOR OWNER Allow  268435456...
appcompat           NT AUTHORITY\SYSTEM          NT SERVICE\TrustedInstaller Allow  FullControl...
apppatch            NT SERVICE\TrustedInstaller  CREATOR OWNER Allow  268435456...
AppReadiness        NT AUTHORITY\SYSTEM          NT AUTHORITY\Authenticated Users Allow  Read, Synchroniz...
assembly            BUILTIN\Administrators      BUILTIN\Administrators Allow  FullControl...
bcastdvr            NT SERVICE\TrustedInstaller  CREATOR OWNER Allow  268435456...
Boot                NT SERVICE\TrustedInstaller  NT AUTHORITY\SYSTEM Allow  -1610612736...
Branding             NT SERVICE\TrustedInstaller  CREATOR OWNER Allow  268435456...
CbsTemp             BUILTIN\Administrators      BUILTIN\Administrators Allow  FullControl...
Containers          NT AUTHORITY\SYSTEM          NT SERVICE\TrustedInstaller Allow  FullControl...
CSC                 NT AUTHORITY\SYSTEM          NT AUTHORITY\SYSTEM Allow  FullControl
Cursors             NT SERVICE\TrustedInstaller  CREATOR OWNER Allow  268435456...
debug               NT AUTHORITY\SYSTEM          APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES D...
diagnostics          NT SERVICE\TrustedInstaller  NT AUTHORITY\SYSTEM Allow  -1610612736...
DiagTrack           NT SERVICE\TrustedInstaller  CREATOR OWNER Allow  268435456...
DigitalLocker       NT AUTHORITY\SYSTEM          NT SERVICE\TrustedInstaller Allow  FullControl...
Downloaded Program Files NT SERVICE\TrustedInstaller  CREATOR OWNER Allow  268435456...
en-US               NT SERVICE\TrustedInstaller  CREATOR OWNER Allow  268435456...
Fonts               NT SERVICE\TrustedInstaller  CREATOR OWNER Allow  268435456...
GameBarPresenceWriter NT SERVICE\TrustedInstaller  CREATOR OWNER Allow  268435456...
Globalization       NT SERVICE\TrustedInstaller  CREATOR OWNER Allow  268435456...
```