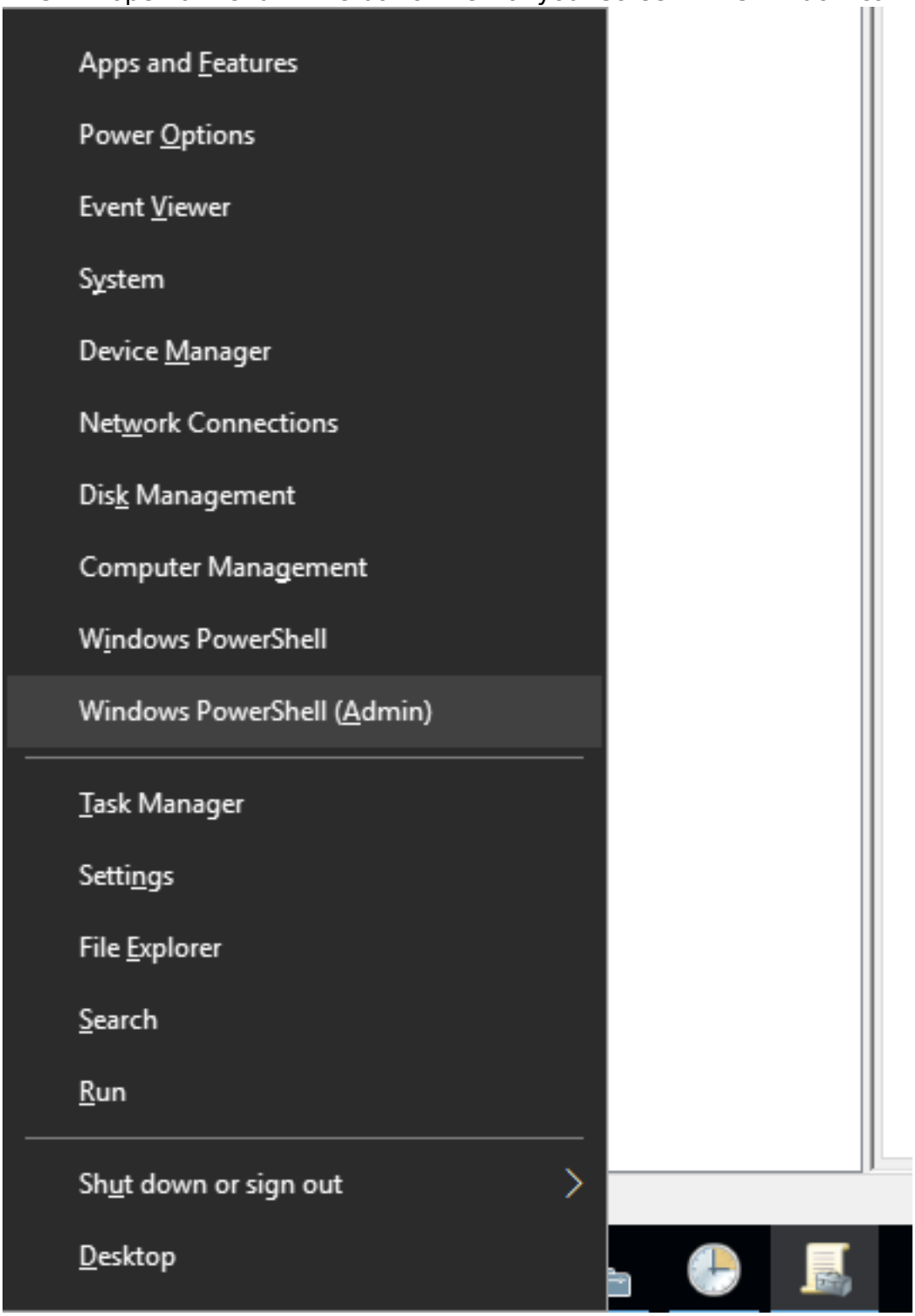
Installer.ps1 Demo

Open PowerShell with Administrative Privilege
Use the key Combo Ctrl + X
This will open a menu in the bottom left of your screen. This window can be seen pictured below



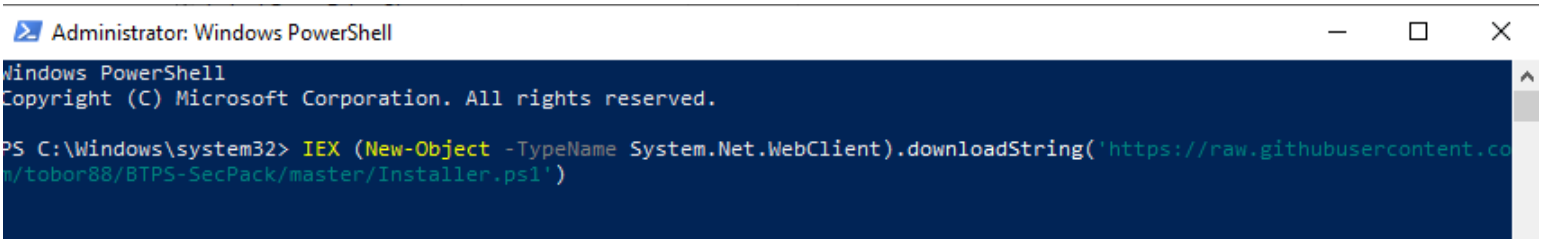
Then press A. As you can see in the above window the A is underlined where the option Windows PowerShell (Admin) is. A selects that option.

If you are prompted by User Access Control (UAC) hit YES

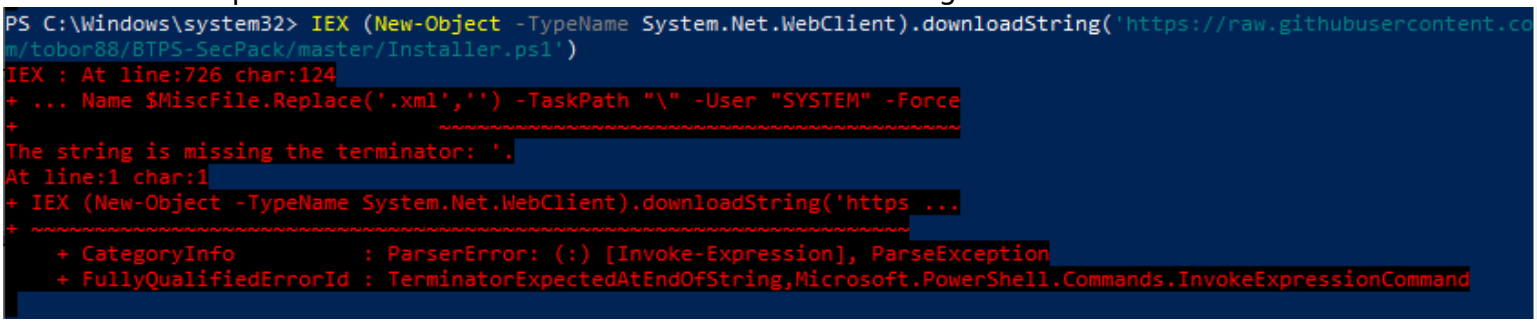
Inside the opened PowerShell window copy and paste the below command

IEX (New-Object -TypeName System.Net.WebClient).downloadString('https://raw.githubusercontent.com/tobor88/BTPS-SecPack/master/Installer.ps1')

SCREENSHOT IMAGE OF ABOVE COMMAND



NOTE: If you experience any issues see https://btps-secpack.com/installer-ps1-usage for another way to do the same thing
Next Generation Anti-Virus can prevent scripts from being executed in this manner. Also encoding translation can prevent execution as is seen in this error message



The other method that can be used will require you to copy and paste these 3 commands

Set-ExecutionPolicy RemoteSigned -Force

Invoke-WebRequest -Uri "https://raw.githubusercontent.com/tobor88/BTPS-SecPack/master/Installer.ps1" -OutFile "$env:USERPROFILE\Downloads\Installer.ps1"

."$env:USERPROFILE\Downlods\Installer.ps1"

SCREENSHOT IMAGE OF ABOVE COMMANDS

```
PS C:\Windows\system32> Set-ExecutionPolicy RemoteSigned -Force
PS C:\Windows\system32> Invoke-WebRequest -Uri "https://raw.githubusercontent.com/tobor88/BTPS-SecPack/master/Installer.
ps1" -OutFile "$env:USERPROFILE\Downloads\Installer.ps1"
PS C:\Windows\system32> ."$env:USERPROFILE\Downlods\Installer.ps1"
```

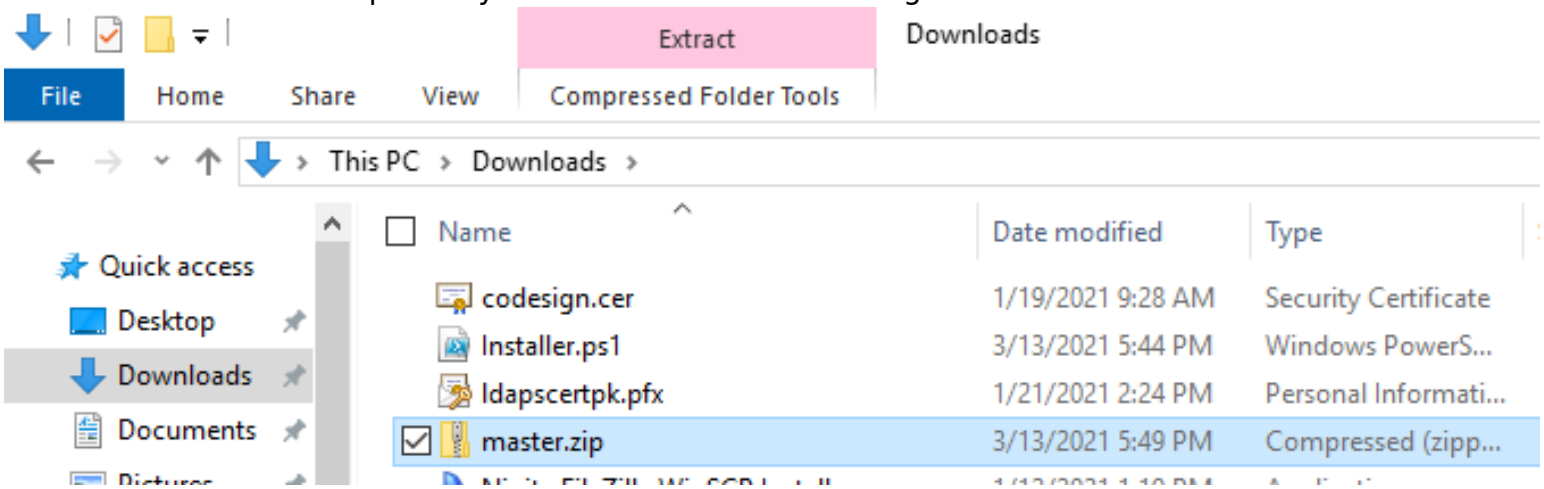
SCRIPT EXECUTION BEGINS

```
PS C:\Windows\system32> ."C:\Users\rosborne\Downloads\Installer.ps1"
[*] Ensuring install script is executing with administator privileges
================================================================================================================================
|                                                    OsbornePro                                                                |
|                                            The B.T.P.S. Security Package                                                     |
|                        https://www.btps-secpack.com Beginning the installation of the B.T.P.S Security Package               |
================================================================================================================================
[i] Suggestions and feedback are always appreciated
Define the directory location you downloaded the BTPS-SecPack Git repository too. If you leave this blank it will be downloaded for
you and placed in C:\Users\rosborne\Downloads\master.zip and Extracted to C:\Windows\System32\WindowsPowerShell\v1.0\BTPS-SecPack-ma
ster:
```

The first value we are asked for is where you downloaded the BTPS Security Package too.
If you have not downloaded the repository yet I suggest leaving the value blank and hitting ENTER
This will start the download. If you do define a value, that is where master.zip will be extracted too.

```
Administrator: Windows PowerShell
Writing web request
   Writing request stream... (Number of bytes written: 1045617)

[*] Ensuring install script is executing with administator privileges
================================================================================================================================
|                                                    OsbornePro                                                                |
|                                            The B.T.P.S. Security Package                                                     |
|                        https://www.btps-secpack.com Beginning the installation of the B.T.P.S Security Package               |
================================================================================================================================
[i] Suggestions and feedback are always appreciated
Define the directory location you downloaded the BTPS-SecPack Git repository too. If you leave this blank it will be downloaded for
you and placed in C:\Users\rosborne\Downloads\master.zip and Extracted to C:\Windows\System32\WindowsPowerShell\v1.0\BTPS-SecPack-ma
ster:
[*] Ensuring PowerShell uses TLSv1.2 for downloads
[*] Downoading the B.T.P.S Security Package.
```

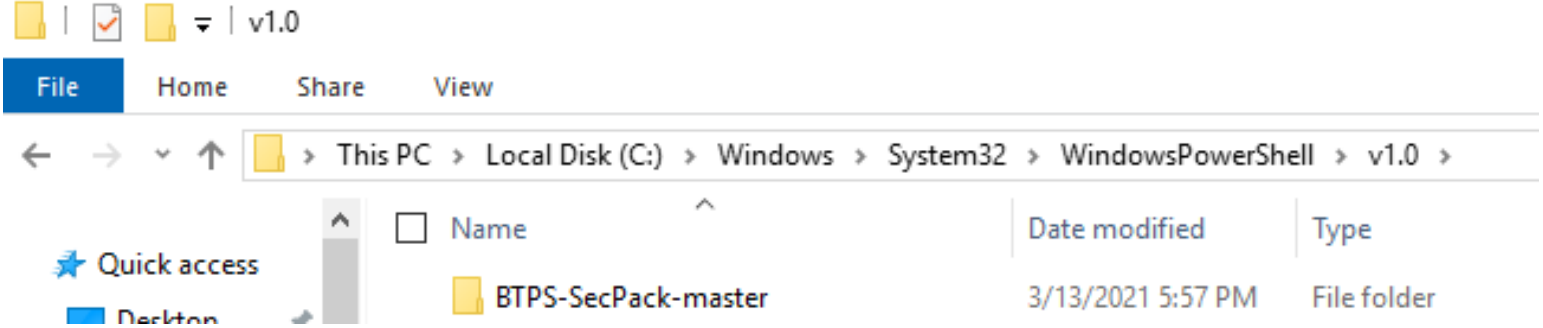
The above download will save a file called **master.zip** to your **Downloads** directory
Feel free to delete this zip file if you wish after it is done being extracted



Master.zip is then extracted to the path location you were first prompted for.

```
Expand-Archive
   The archive file 'C:\Users\rosborne\Downloads\master.zip' expansion is in progress...
   [ooooooooooooooooooooooooooooo                                                    ]

|                    https://www.btps-secpack.com Beginning the installation of the B.T.P.S Security Package                |
================================================================================================================================
[i] Suggestions and feedback are always appreciated
Define the directory location you downloaded the BTPS-SecPack Git repository too. If you leave this blank it will be downloaded for
you and placed in C:\Users\rosborne\Downloads\master.zip and Extracted to C:\Windows\System32\WindowsPowerShell\v1.0\BTPS-SecPack-ma
ster:
[*] Ensuring PowerShell uses TLSv1.2 for downloads
[*] Downoading the B.T.P.S Security Package.
```

If you left the value blank as I did, that location is **C:\Windows\System32\WindowsPowerShell\v1.0\BTPS-SecPack-master**



EMAIL CONFIGURATION CREDENTIALS

Once that is completed we will be asked to set up the SMTP server credentials we wish to use for alerts
We are presented with choosing options 1, 2, or 3
I choose option 3 to use SMTP2GO as I believe this to be the best option

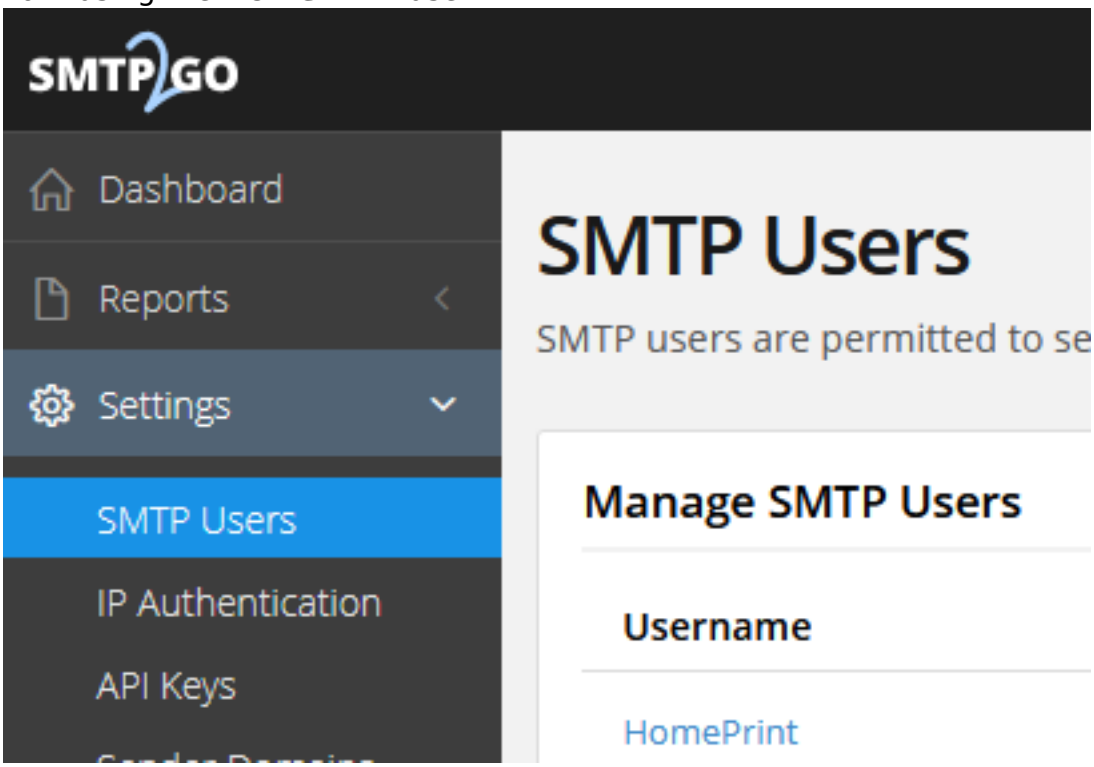
```
======================== EMAIL SENDING ========================
[!] IMPORTANT: In order to send emails you need to authenticate to an SMTP server. This can be done using different ways.

        1 : Use a Credential File (if an attacker were to compromise the computer they can view the credentials). If you choose thi
s option the Credential file will be saved too C:\Users\Administrator\AppData\Local\PackageManagement\btpssecpack.xml and permission
s will be set.

        2 : IP Authentication (If you are using Office365 you can configure a Connector to allow emails sent from your Public IP ad
dress to be good enough for authentication to your Exchange SMTP server)

        3 : BEST OPTION : Free SMTP2GO account (This can enable IP address authentication or use credentials that do not authentica
te to anywhere else in your environment. This is the best option in my opinion
Select one of the above methods [1/2/3]: 3
```

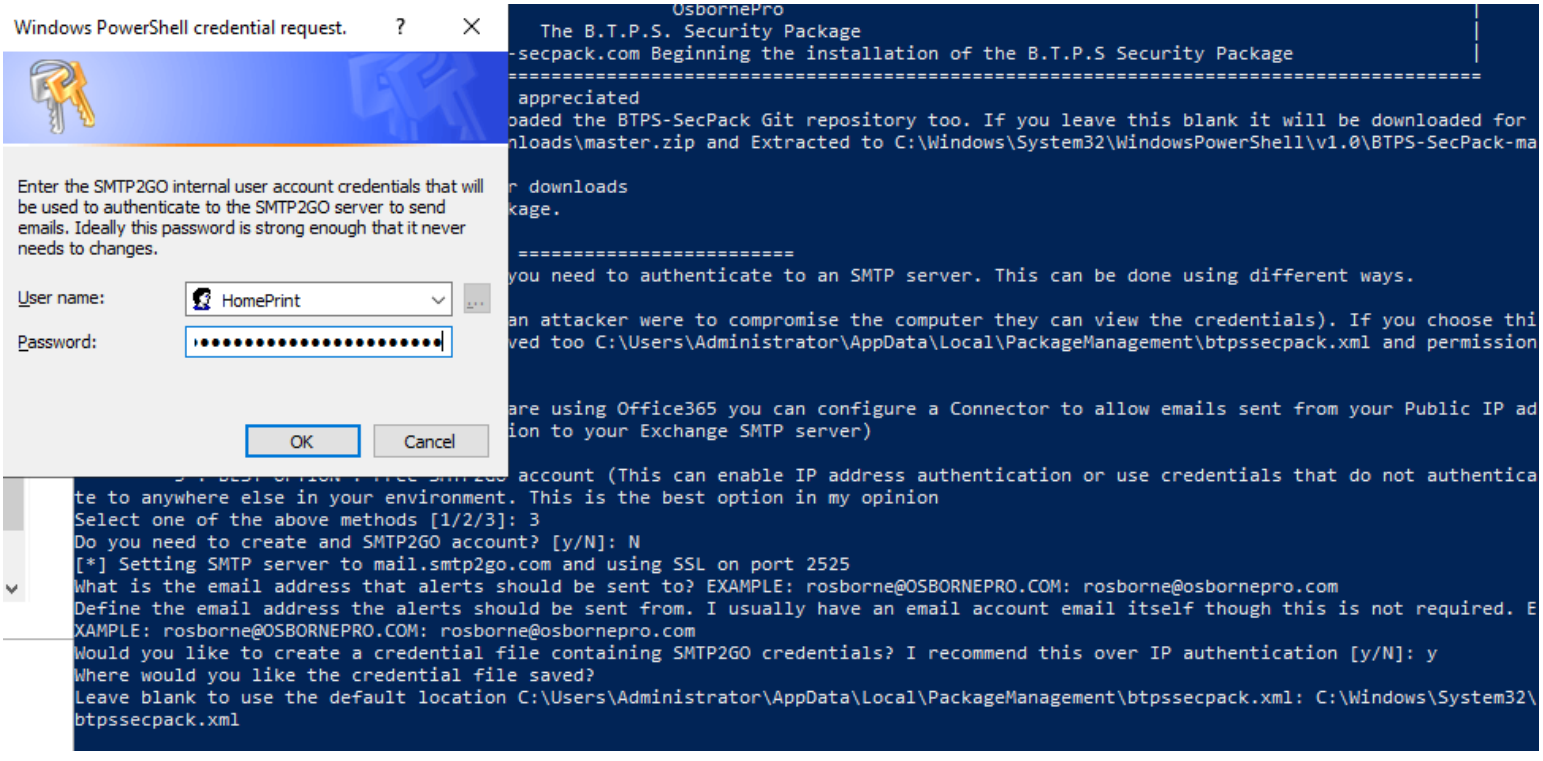
I do not need to create and SMTP2GO account. If you do not have one and select YES it will open their site for you to create a **free** account with them

I define a FROM and TO email address for alerts to be sent between
I also specify I want to use a credential file for sending emails which allows TLS to be used.
All of my alert scripts are configured to send using TLS so I suggest saying Yes when asked
Next we choose a location to save the SMTP2GO credential file. I am going to set mine to **C:\Windows\System32\btpssecpack.xml**

```
Select one of the above methods [1/2/3]: 3
Do you need to create and SMTP2GO account? [y/N]: N
[*] Setting SMTP server to mail.smtp2go.com and using SSL on port 2525
What is the email address that alerts should be sent to? EXAMPLE: rosborne@OSBORNEPRO.COM: rosborne@osbornepro.com
Define the email address the alerts should be sent from. I usually have an email account email itself though this is not required. E
XAMPLE: rosborne@OSBORNEPRO.COM: rosborne@osbornepro.com
Would you like to create a credential file containing SMTP2GO credentials? I recommend this over IP authentication [y/N]: y
Where would you like the credential file saved?
Leave blank to use the default location C:\Users\Administrator\AppData\Local\PackageManagement\btpssecpack.xml:
```

I am then prompted for the credentials that will be stored in the credential file that authenticate to SMTP2GO
The user account and password for that I am using can be accessed in your SMTP2GO area here https://app.smtp2go.com/settings/users/
I am using the **HomePrint** user

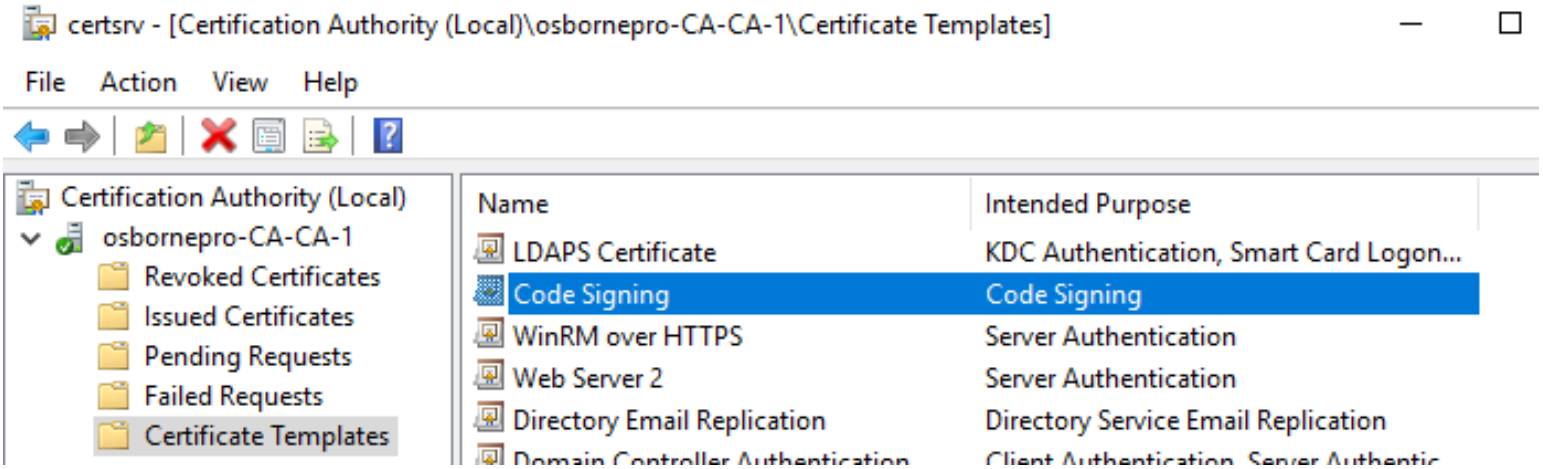




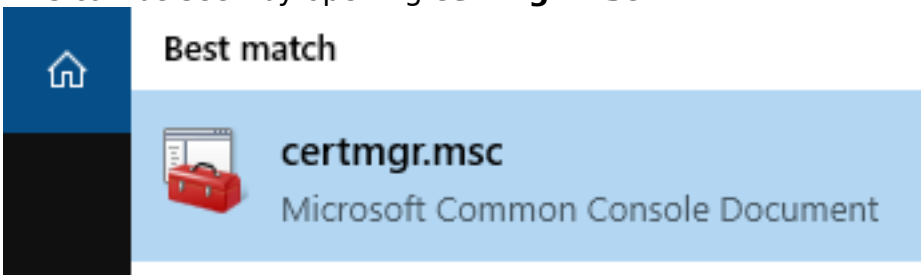
You will next receive a lot of output. This is because all of the alert scripts are being updated to use the credential file and email settings we just defined
Evidence of this can be seen in the terminal window output on the **Send-MailMessage** command in the image below

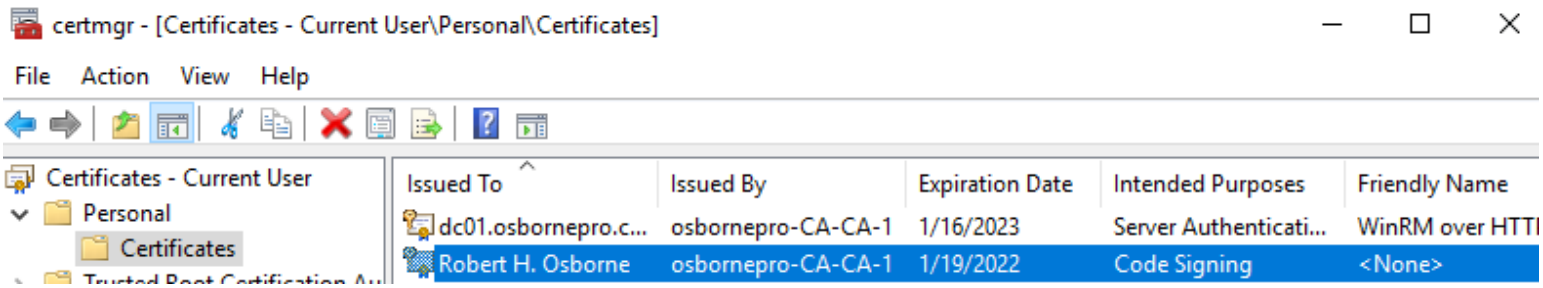
```
</style>
"@ # End CSS
    $PreContent = "<Title>Suspicous Events</Title>"
    $NoteLine = "This Message was Sent on $(Get-Date -Format 'MM/dd/yyyy HH:mm:ss')"
    $PostContent = "<br><p><font size='2'><i>$NoteLine</i></font>"
    $MailBody = $FinalResults | ConvertTo-Html -Head $Css -PostContent $PostContent -PreContent $PreContent -Body "<br>The below tab
le contains suspicous events that were triggered<br><br><hr><br><br>" | Out-String

    Send-MailMessage -From rosborne@osbornepro.com -To rosborne@osbornepro.com -Subject "SUSPICIOUS EVENT TRIGGERED" -BodyAsHtml -Bo
dy "$MailBody" -SmtpServer mail.smtp2go.com -Credential $Credential -UseSSL -Port 2525
```

If you do not already have one assigned to yourself, assign yourself a Code Signing Certificate
On your environments Certificate Authority the Template is called **Code Signing**



This can be seen by opening **certmgr.msc**





Once you have a Code Signing certificate assigned press ENTER in the PowerShell window to continue Script execution

```
WARNING: I am not able to sign alert scripts for you because we just changed the files to include your email information.
[!] We are about to move the Alert scripts to other devices in your network. These should be Code Signed for Security Reasons.
[*] If you do not have a Code Signing Certificate for rosborne please get one now
Press Enter to continue...:
```

Pressing ENTER will display all the alert scripts that were just signed

```
[!] Below is a list of the alert scripts that are about to be signed with your Code Signing Certificate.

Begining an infinite loop that will not continue Script Execution until this command returns as True : (Get-ChildItem -Path Cert:\
rrentUser\My -CodeSigningCertificate)[0]
[*] Using Code Signing Certifciate to sign your alert scripts


    Directory: C:\Windows\System32\WindowsPowerShell\v1.0\BTPS-SecPack-master\WEF Application


SignerCertificate                         Status                                    Path
-----------------                         ------                                    ----
6B510746706B428EA6F2F15379746BB9ADC35608  Valid                                     SQL-Query-Suspicous-Events.ps1


    Directory: C:\Windows\System32\WindowsPowerShell\v1.0\BTPS-SecPack-master\Local Port Scan Monitor


SignerCertificate                         Status                                    Path
-----------------                         ------                                    ----
6B510746706B428EA6F2F15379746BB9ADC35608  Valid                                     ListenPortMonitor.ps1
6B510746706B428EA6F2F15379746BB9ADC35608  Valid                                     Watch-PortScan.ps1


    Directory: C:\Windows\System32\WindowsPowerShell\v1.0\BTPS-SecPack-master\Hardening Cmdlets


SignerCertificate                         Status                                    Path
-----------------                         ------                                    ----
6B510746706B428EA6F2F15379746BB9ADC35608  Valid                                     Reset-KerberosKeys.ps1


    Directory: C:\Windows\System32\WindowsPowerShell\v1.0\BTPS-SecPack-master\Event Alerts


SignerCertificate                         Status                                    Path
-----------------                         ------                                    ----
6B510746706B428EA6F2F15379746BB9ADC35608  Valid                                     DNSZoneTransferAlert.ps1
6B510746706B428EA6F2F15379746BB9ADC35608  Valid                                     Get-NewlyInstalledService.ps1
6B510746706B428EA6F2F15379746BB9ADC35608  Valid                                     NewComputerAlert.ps1
6B510746706B428EA6F2F15379746BB9ADC35608  Valid                                     Query-InsecureLDAPBinds.ps1
6B510746706B428EA6F2F15379746BB9ADC35608  Valid                                     ReviewForwardingRulesOffice.ps1
6B510746706B428EA6F2F15379746BB9ADC35608  Valid                                     UnusualUserSignInAlert.ps1
```

At the end of the output you will see whether or not you have LDAP over SSL configured
If you do not you will be provided with a link to a video I did where I cover how to configure that safely
It is not required however I highly recommend doing it
LINK: https://youtu.be/8rlk2xDkgLw

```
SignerCertificate                         Status                                    Path
-----------------                         ------                                    ----
6B510746706B428EA6F2F15379746BB9ADC35608  Valid                                     AccountsExpiringCheck.ps1
6B510746706B428EA6F2F15379746BB9ADC35608  Valid                                     AttemptedPasswordChange.ps1
6B510746706B428EA6F2F15379746BB9ADC35608  Valid                                     AttemptedPasswordReset.ps1
6B510746706B428EA6F2F15379746BB9ADC35608  Valid                                     Failed.Username.and.Password.ps1
6B510746706B428EA6F2F15379746BB9ADC35608  Valid                                     MonitorAdminEscalation.ps1
6B510746706B428EA6F2F15379746BB9ADC35608  Valid                                     PasswordExpiryAlert.ps1
6B510746706B428EA6F2F15379746BB9ADC35608  Valid                                     User.Account.Created.ps1
6B510746706B428EA6F2F15379746BB9ADC35608  Valid                                     User.Account.Locked.ps1
6B510746706B428EA6F2F15379746BB9ADC35608  Valid                                     User.Account.Unlocked.ps1
[*] Determining whether or not LDAP over SSL is available
[*] Excellent work! LDAPS connection test was passed!
```

A task is then created that will send you an email whenever an insecure LDAP bind occurs
An insecure LDAP bind is when credentials are sent in clear text
Below is output showing the task was created

```
Actions             : {MSFT_TaskExecAction}
Author              : tobor
Date                : 2020-07-29T13:04:53.262781
Description         : Alerts IT of any LDAP Bind connections that did not use TLS
Documentation       :
Principal           : MSFT_TaskPrincipal2
SecurityDescriptor  :
Settings            : MSFT_TaskSettings3
Source              :
State               : Ready
TaskName            : Insecure LDAP Bind Discovery
TaskPath            : \
Triggers            : {MSFT_TaskDailyTrigger}
URI                 : \Insecure LDAP Bind Discovery
Version             :
PSComputerName      :

[*] LDAP over SSL alert task is set to inform you who performs and whenever an insecure LDAP bind is performed
WARNING: WinRM over SSL does not appear to be configured on DC01.osbornepro.com
I highly recommend using this. If you wish to set this up I suggest following my instructions at the below links.
https://btps-secpack.com/winrm-over-https
https://youtu.be/UcU2Iu9AXpM
This script will pause to give you time to set this up
Press Enter to continue...:
```

You will notice the yellow warning message above. I have **WinRM over HTTPS** configured
I defined the subnets that are allowed to make WinRM calls. I left out 127.0.0.1 and 127.0.1.1 from my definitions
I did this because if an attacker obtains credentials they can not elevate privilege by using the **Enter-PSSession** Command

Using a Domain Controller cmdlet I build a list next of active domain computer and servers

```
Press Enter to continue...:
[*] Obtaining computer and server list based on enabled computers that have been signed into in the last 60 days: 01/12/2021 18:17:1
7
```

SYSMON SETUP

We now start the Sysmon configuration
Enter y to have the Malicious IP Checker and Process Hash Validator setup

```
================== SYSMON ======================
With your approval, this will create a network share in C:\Sysmon which will be used to install sysmon in your environment and enabl
e the logging of blacklisted IP addresses. Is this ok to do [y/N]: y
```

Sysmon will have a network share defined at C:\Sysmon and create a blank GPO policy for you to add definitions too manually later

```
Creating Sysmon share at C:\Sysmon
Making C:\Sysmon a Network Share for use with group policy
```

I then disable SMBv1 for security reasons and ensure SMBv2 and SMBv3 are enabled
Sysmon files are then copied over to the network share location

```
[*] Disabling SMB version 1
[*] Enabling SMBv2 and SMBv3
[*] Copying the needed files from the BTPS Sec Pack into C:\Sysmon

------------------------------------------------------------------------------
   ROBOCOPY     ::     Robust File Copy for Windows
------------------------------------------------------------------------------

  Started : Saturday, March 13, 2021 6:19:11 PM
   Source : C:\Windows\System32\WindowsPowerShell\v1.0\BTPS-SecPack-master\Sysmon\
     Dest : C:\Sysmon\

    Files : *

  Options : /DCOPY:DA /COPY:DAT /R:1000000 /W:30

------------------------------------------------------------------------------

                           12    C:\Windows\System32\WindowsPowerShell\v1.0\BTPS-SecPack-master\Sysmon\
100%        Newer                  7415        Eula.txt
100%        Newer                 11513        HashValidator.ps1
100%        Newer                  1983        HashValidator.xml
100%        Newer                 10647        Install-SysmonBTPSSecPack.ps1
100%        Newer                 19679        MaliciousIPChecker.ps1
100%        Newer                  2137        MaliciousIPChecker.xml
100%        Newer                  8871        README.md
100%        Newer                   484        sysmon.bat
100%        Newer                 4.6 m        Sysmon.exe
100%        Newer                 95618        sysmon.xml
100%        Newer                 1.8 m        Sysmon.zip
100%        Newer                 2.4 m        Sysmon64.exe

------------------------------------------------------------------------------

               Total    Copied   Skipped  Mismatch    FAILED    Extras
    Dirs :         1         0         1         0         0         0
   Files :        12        12         0         0         0         0
   Bytes :    9.06 m    9.06 m         0         0         0         0
   Times :   0:00:00   0:00:00                       0:00:00   0:00:00


   Speed :           206660521 Bytes/sec.
   Speed :           11825.209 MegaBytes/min.
   Ended : Saturday, March 13, 2021 6:19:11 PM

[*] Creating Malicious IP Checker task on DC01. This task will still need to be pushed out to your environment using group policy. I
nstructions on that can be found HERE https://btps-secpack.com/sysmon-setup
```

The Malicious IP Checker task will then be created

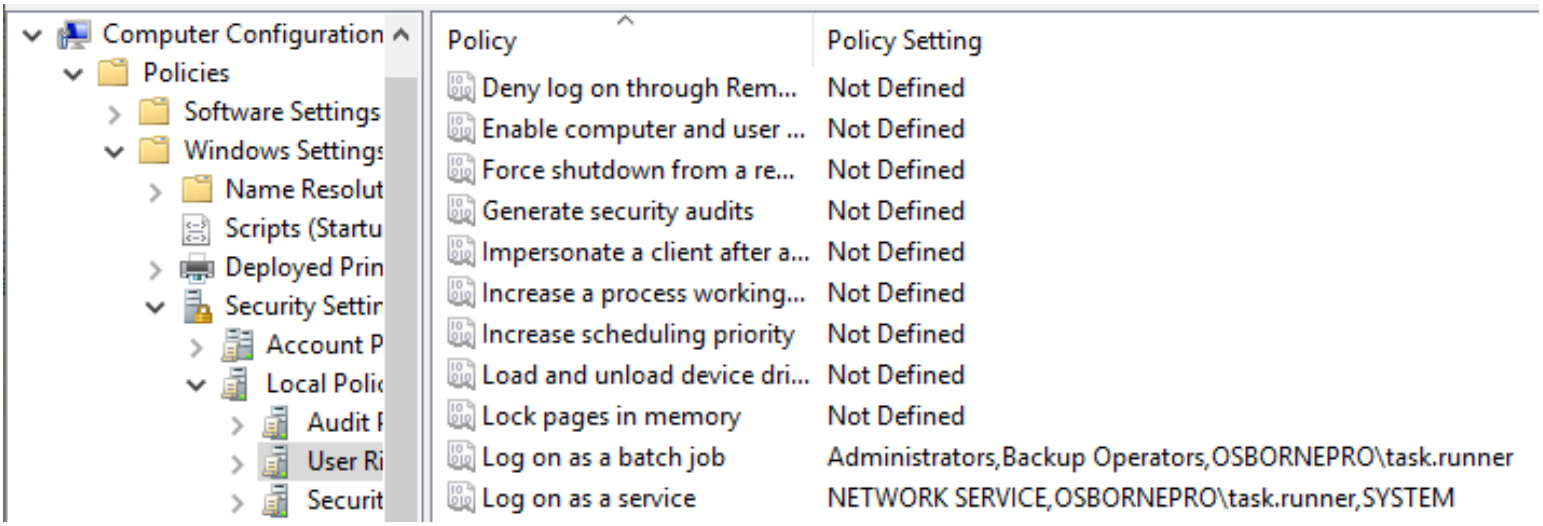
```
[*] Creating Malicious IP Checker task on DC01. This task will still need to be pushed out to
nstructions on that can be found HERE https://btps-secpack.com/sysmon-setup

Actions             : {MSFT_TaskExecAction}
Author              : tobor
Date                : 2020-10-02T10:54:58.1970414
Description         : Creates a log entry whenever a connection to a malicious IP address or yo
Documentation       :
Principal           : MSFT_TaskPrincipal2
SecurityDescriptor  :
Settings            : MSFT_TaskSettings3
Source              :
State               : Ready
TaskName            : Malicious IP Checker
TaskPath            : \
Triggers            : {MSFT_TaskTimeTrigger, MSFT_TaskBootTrigger, MSFT_TaskIdleTrigger}
URI                 : \Malicious IP Checker
Version             :
PSComputerName      :

Do you have a Virus Total API Key? [y/N]:
```

Next you will be prompted to enter your Virus Total API key.
If you answer NO to the question you will be taken to their site to create an account and generate one

to use here

Run as batch job and Run as service permissions are required for some tasks to run.
Enter an account that has those permissions

```
Do you have a Virus Total API Key? [y/N]: y
Paste your Virus Total API Key here: : be0ee5ce0585164
Enter the username this task should run as. This user
EXAMPLE: CONTOSO\TaskSchedUser: OSBORNEPRO\task.runner
```



You will then be asked to securely enter that users password and the tasks will be created

```
Enter the username this task should run as. This user will need 'Run as batch job' permissions
EXAMPLE: CONTOSO\TaskSchedUser: OSBORNEPRO\task.runner
Enter the password for the user this task is going to run as. This info will be deleted from events and history later: **********
*****
[*] Creating Hash Validation Checker task on DC01. This task will still need to be pushed out to your environment using group policy
. Instructions on that can be found HERE https://btps-secpack.com/sysmon-setup

Actions             : {MSFT_TaskExecAction}
Author              : tobor
Date                : 2021-03-13T13:46:53.8983089
Description         : Validates process hashes in Sysmon logs to check for any possibly malicious hashes
Documentation       :
Principal           : MSFT_TaskPrincipal2
SecurityDescriptor  :
Settings            : MSFT_TaskSettings3
Source              :
State               : Ready
TaskName            : Hash Validator
TaskPath            : \
Triggers            : {MSFT_TaskTimeTrigger}
URI                 : \Hash Validator
Version             :
PSComputerName      :
```

Next you will need to follow the steps I outline manually on **page 6** of the **Sysmon Setup.pdf https://btps-secpack.com/sysmon-setup**

```
Follow the setup instructions at https://btps-secpack.com/sysmon-setup Page 6 to create the group policy that gets this on all the d
evices in your environment
This creates a new log in the event viewer that providers more detailed logging and allows you to use a task that monitors connectio
ns to your devices providing an alert whenver a blacklisted IP has been connected too
Press Enter to continue...:
```

The PDF covers how to get files pushed out to domain devices and how to create the needed schedueld task to put out via group policy
I have included images of those settings below

Scheduled Task (At least Windows 7) (Name: Hash Validation Task)

Hash Validation Task (Order: 2)

General

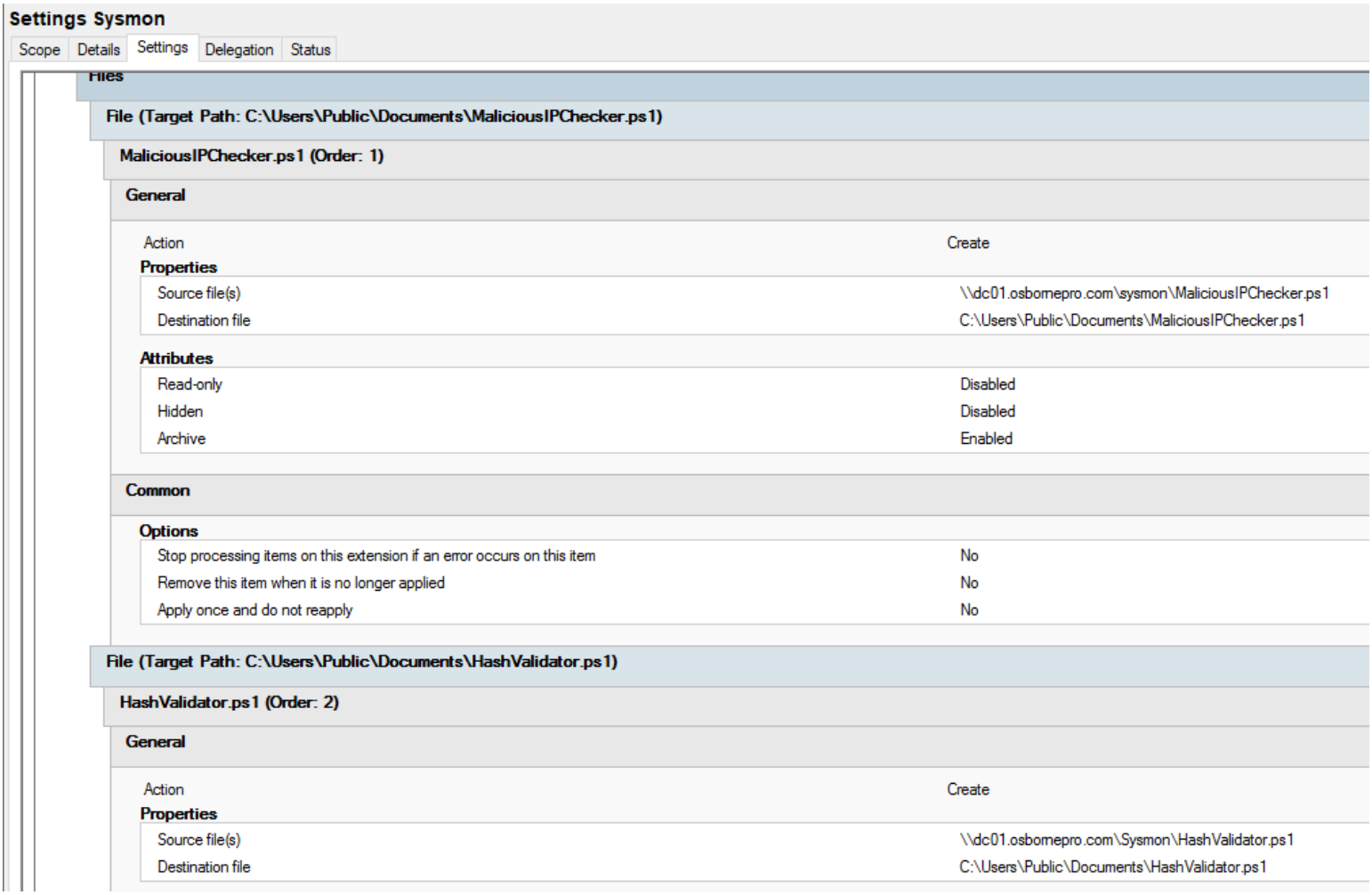
Action		Create
Task		
	Name	Hash Validation Task
	Author	OSBORNEPRO\rosborne
	Description	Runs a check on process hashes to discover and log possibly malicious processes
	Run only when user is logged on	S4U
	UserId	NT AUTHORITY\Network Service
	Run with highest privileges	HighestAvailable
	Hidden	No
	Configure for	1.2
	Enabled	Yes

Scheduled Task (At least Windows 7) (Name: Malcious IP Checker Task)

Malcious IP Checker Task (Order: 1)

General

Action		Create
Task		
	Name	Malcious IP Checker Task
	Author	OSBORNEPRO\rosborne
	Description	Runs a check on domains and IP addresses this deivce connects to in order to log IP's that are possibly malicious
	Run only when user is logged on	S4U
	UserId	NT AUTHORITY\System
	Run with highest privileges	HighestAvailable
	Hidden	No
	Configure for	1.2
	Enabled	Yes



AUTORUNS

Next we install AutoRuns to keep track of registry values and changes
Answer Y to set this up

```
=================== AUTORUNS ====================
Would you like to collect Autoruns information daily on  This is for investigating fileless malware compromises [y/N]: y

Actions            : {MSFT_TaskExecAction}
Author             :
Date               :
Description        :
Documentation      :
Principal          : MSFT_TaskPrincipal2
SecurityDescriptor :
Settings           : MSFT_TaskSettings3
Source             :
State              : Ready
TaskName           : AutorunsToWinEventLog
TaskPath           : \
Triggers           : {MSFT_TaskDailyTrigger}
URI                : \AutorunsToWinEventLog
Version            :
PSComputerName     :


Actions            : {MSFT_TaskExecAction}
Author             :
Date               :
Description        :
Documentation      :
Principal          : MSFT_TaskPrincipal2
SecurityDescriptor :
Settings           : MSFT_TaskSettings3
Source             :
State              : Ready
TaskName           : AutorunsToWinEventLog
TaskPath           : \
Triggers           : {MSFT_TaskDailyTrigger}
URI                : \AutorunsToWinEventLog
Version            :
PSComputerName     :
```

DEVICE DISCOVERY

Device discovery requires Log on as batch and log on as service permissions to run the task successfully.
This will alert you whenever a new device joins your network.
It is recommended for organizations with 1000 machines or less I would estimate

```
================ DEVICE DISCOVERY ================
Would you like to set up new device discovery alerts on  This is for environments with less thatn 1000 computers. It will send you a
n alert whenever a never before seen device joins your network [y/N]: y
Enter the username this task should run as. This user will need 'Run as batch job' permissions as well as DHCP admin permissions
EXAMPLE: CONTOSO\TaskSchedUser: OSBORNEPRO\task.runner

------------------------------------------------------------------------------
   ROBOCOPY     ::     Robust File Copy for Windows
------------------------------------------------------------------------------

  Started : Saturday, March 13, 2021 6:30:12 PM
   Source : C:\Windows\System32\WindowsPowerShell\v1.0\BTPS-SecPack-master\Device Discovery\
     Dest : \\ca.osbornepro.com\C$\Users\Public\Documents\

    Files : *

  Options : /DCOPY:DA /COPY:DAT /R:1000000 /W:30
```

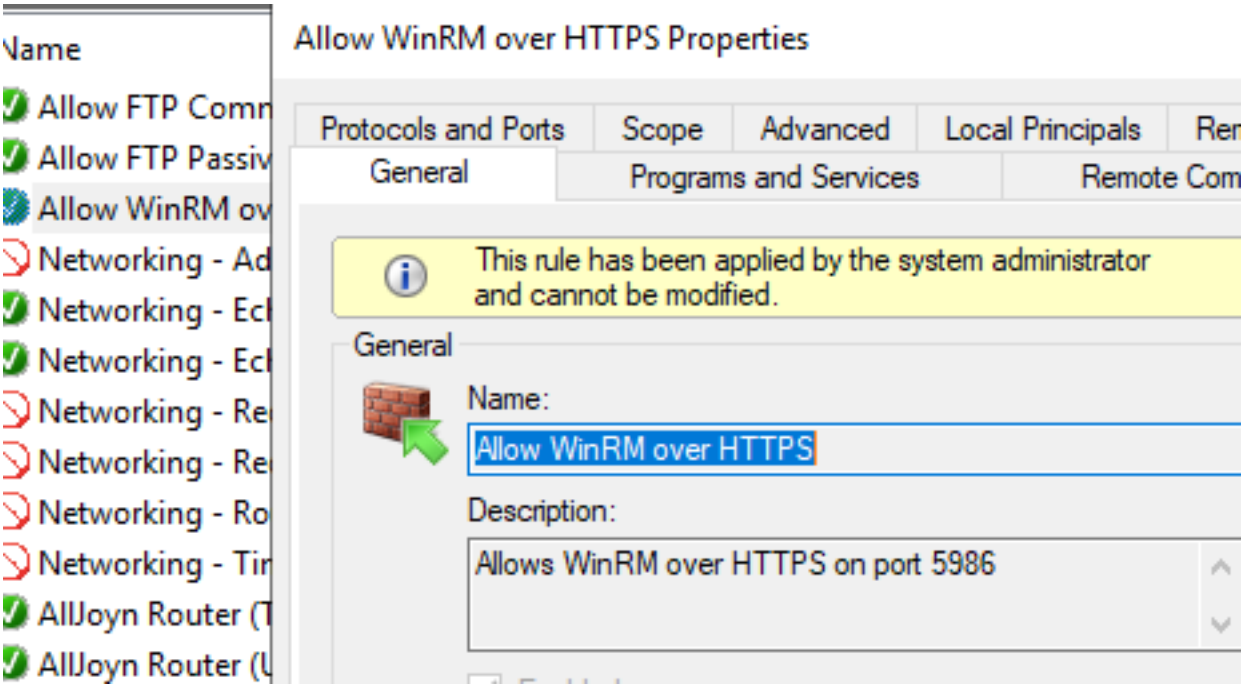
A value I generate does not work 100% of the time. If you see this error message before the PORT MONITORING SECTION

```
   Ended : Saturday, March 13, 2021 6:30:13 PM

[ca.osbornepro.com] Connecting to remote server ca.osbornepro.com failed with the following error message : WinRM cannot complete
the operation. Verify that the specified computer name is valid, that the computer is accessible over the network, and that a
firewall exception for the WinRM service is enabled and allows access from this computer. By default, the WinRM firewall exception
for public profiles limits access to remote computers within the same local subnet. For more information, see the
about_Remote_Troubleshooting Help topic.
    + CategoryInfo          : OpenError: (ca.osbornepro.com:String) [], PSRemotingTransportException
    + FullyQualifiedErrorId : WinRMOperationTimeout,PSSessionStateBroken
============== PORT MONITORING ====================
Would you like to set up port scan monitoring? This keeps record of all connections made to a server and provides email alerts if a
port scan is detected.
NOTE: If you have created an email credetial file, this is the section that copies the credential file onto all available servers. I
f you did not make a credential file it will not be copied onto your servers. This was done to save time for you.
ANSWER [y/N]:
```

This is the kind of thing that drives me nuts. There is **NO** reason for the failure other than Windows is buggy
We can see the WinRM service is running and configured

```
PS C:\Windows\system32> winrm qc -q
WinRM service is already running on this machine.
WinRM is already set up for remote management on this computer.
PS C:\Windows\system32> Get-Service winrm

Status   Name               DisplayName
------   ----               -----------
Running  winrm              Windows Remote Management (WS-Manag...


PS C:\Windows\system32> hostname
CA
```

```
 C:\Windows\system32> winrm e winrm/config/listener
stener [Source="GPO"]
  Address = *
  Transport = HTTP
  Port = 5985
  Hostname
  Enabled = true
  URLPrefix = wsman
  CertificateThumbprint
  ListeningOn = 127.0.0.1, 192.168.137.140

stener
  Address = *
  Transport = HTTPS
  Port = 5986
  Hostname = ca.osbornepro.com
  Enabled = true
  URLPrefix = wsman
  CertificateThumbprint = 21b8a21f066e6f9462b25d27856f167fff29c63d
  ListeningOn = 127.0.0.1, 192.168.137.140
```



However one command does not work and the other does
WinRM connects just fine using another command

```
[ca.osbornepro.com] Connecting to remote server ca.osbornepro.com failed with the following error messag
cannot complete the operation. Verify that the specified computer name is valid, that the computer is ac
the network, and that a firewall exception for the WinRM service is enabled and allows access from this
default, the WinRM firewall exception for public profiles limits access to remote computers within the s
subnet. For more information, see the about_Remote_Troubleshooting Help topic.
    + CategoryInfo          : OpenError: (ca.osbornepro.com:String) [], PSRemotingTransportException
    + FullyQualifiedErrorId : WinRMOperationTimeout,PSSessionStateBroken
PS C:\Windows\system32> Invoke-Command -HideComputerName $DHCPServer -UseSSL -ScriptBlock {whoami }
osbornepro\rosborne
PS C:\Windows\system32>
```

If this happens to you, remote (RDP) into your DHCP Server

Open Admin PowerShell session (Windows Key + X, Then Press A)
Copy and paste all of the below text into your powershell window and press ENTER to execute it

```
$ScheduledTaskUser = Read-Host -Prompt "Enter the username this task should run as. This user will need 'Run as batch job' permissions as well as DHCP admin permissions `nEXAMPLE: CONTOSO\TaskSchedUser"

Write-Output "[*] Creating New Device Check task on $env:COMPUTERNAME."
New-Item -ItemType Directory -Path "C:\Users\Public\Documents\PSGetHelp" -Force -ErrorAction SilentlyContinue | Out-Null
Move-Item -Path 'C:\Users\Public\Documents\MAC.Vendor.List.csv' -Destination 'C:\Users\Public\Documents\PSGetHelp\MAC.Vendor.List.csv' -Force

$SecurePassword = Read-Host -Prompt "Enter the password for the user this task is going to run as. This info will be deleted from events and history later" -AsSecureString
$BSTR = [System.Runtime.InteropServices.Marshal]::SecureStringToBSTR($SecurePassword)
$Password = [System.Runtime.InteropServices.Marshal]::PtrToStringAuto($BSTR)

Register-ScheduledTask -Xml (Get-Content -Path "C:\Users\Public\Documents\Find-
```

NewDevices.xml"| Out-String) -TaskName "New Device Discovery" -TaskPath "\" -User $ScheduledTaskUser -Password $Password –Force
Write-Output "[*] The 'New Device Discovery' Task is now set up on your DHCP server"

If the command completes successfully you should see this

```
Enter the password for the user this task is going to run as. This info will be deleted
**********

TaskPath                                    TaskName                       State
--------                                    --------                       -----
\                                           New Device Discovery           Ready
[*] The 'New Device Discovery' Task is now set up on your DHCP server


PS C:\Windows\system32>
```

PORT MONITORING

Answer YES To enable Port Monitoring on your devices. This keeps a log of all connections to a device and alerts for port scans
Define a user who has Log on as batch job and Log on as Service permissions to run the task as

```
============== PORT MONITORING ====================
Would you like to set up port scan monitoring? This keeps record of all connections made to a server and provides email alerts if a
port scan is detected.
NOTE: If you have created an email credetial file, this is the section that copies the credential file onto all available servers. I
f you did not make a credential file it will not be copied onto your servers. This was done to save time for you.
ANSWER [y/N]: y
Enter the username this task should run as. This user will need 'Run as batch job' permissions as well as DHCP admin permissions
EXAMPLE: CONTOSO\TaskSchedUser: OSBORNEPRO\task.runner

------------------------------------------------------------------------------
   ROBOCOPY     ::     Robust File Copy for Windows
------------------------------------------------------------------------------

  Started : Saturday, March 13, 2021 6:55:09 PM
   Source : C:\Windows\System32\
     Dest : C:\DC01.osbornepro.com\C$\Windows\System32\

    Files : btpssecpack.xml

  Options : /DCOPY:DA /COPY:DAT /R:1000000 /W:30
```

ACCOUNTS AND PASSWORDS

Answer YES to recieve alerts when new users are created and passwords are changed as well as other account related alerts

```
============= ACCOUNTS AND PASSWORDS ==============
With you permission, this will create tasks on DC01 that alert on password and account changes. This also creates an alert that info
rms users who have a password expiring soon [y/N]: y

------------------------------------------------------------------------------
   ROBOCOPY     ::     Robust File Copy for Windows
------------------------------------------------------------------------------

  Started : Saturday, March 13, 2021 6:57:28 PM
   Source : C:\Windows\System32\WindowsPowerShell\v1.0\BTPS-SecPack-master\Account and Password Alerts" C:\Users\Public\Documents At
temptedPasswordChange.xml\
     Dest -

    Files : *.*

  Options : *.* /DCOPY:DA /COPY:DAT /R:1000000 /W:30

------------------------------------------------------------------------------

ERROR : No Destination Directory Specified.

       Simple Usage :: ROBOCOPY source destination /MIR

            source :: Source Directory (drive:\path or \\server\share\path).
         destination :: Destination Dir  (drive:\path or \\server\share\path).
               /MIR :: Mirror a complete directory tree.

    For more usage information run ROBOCOPY /?
```

MISC ALERTS (DNS and Unusual Sign In)

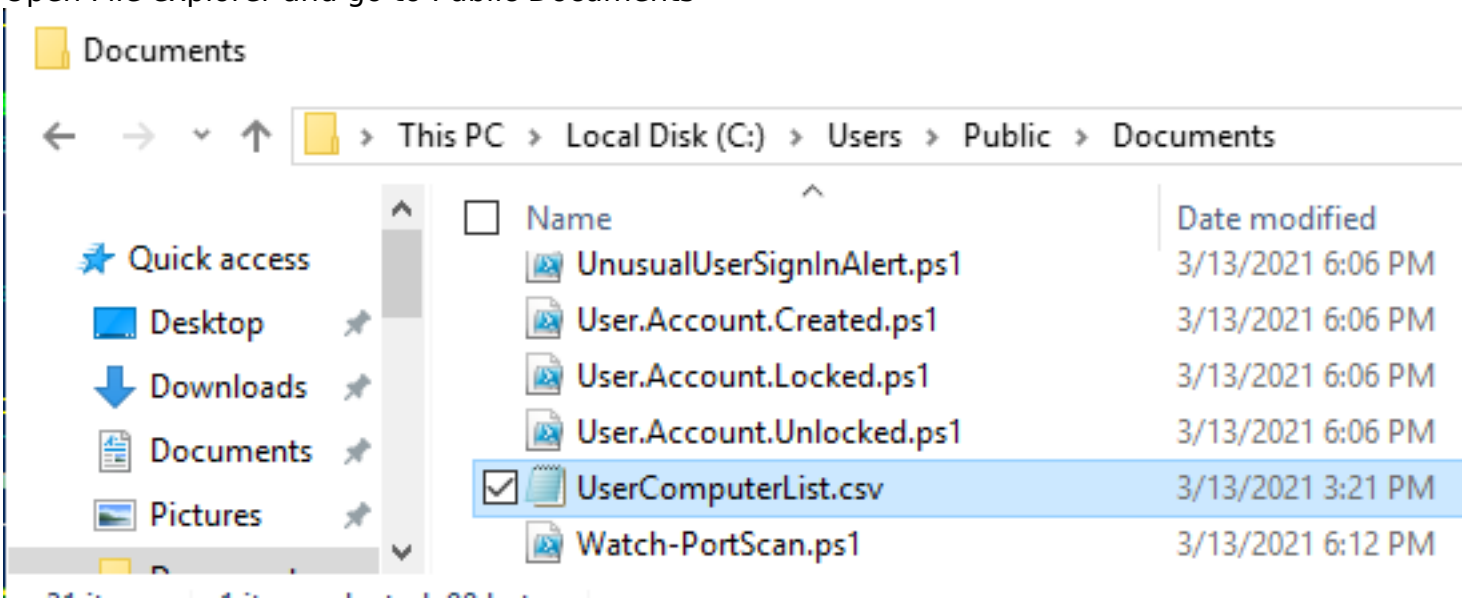
Answer yes to enable Unusual sign in alerts and DNS over HTTPS

```
[*] The UserAccountUnlocked.xml task should now set up on DC01
============= MISC ALERTS FOR DC ===============
With your permission, tasks wil be created that alert when a DNS zone transfer occurs and when an Unusual Sign In Occurs [y/N]: y

------------------------------------------------------------------------------
   ROBOCOPY     ::     Robust File Copy for Windows
------------------------------------------------------------------------------

  Started : Saturday, March 13, 2021 6:58:17 PM
   Source : C:\Windows\System32\WindowsPowerShell\v1.0\BTPS-SecPack-master\Event Alerts" C:\Users\Public\Documents DNSZoneTransferAl
ert.xml\
     Dest -

    Files : *.*

  Options : *.* /DCOPY:DA /COPY:DAT /R:1000000 /W:30

------------------------------------------------------------------------------

ERROR : No Destination Directory Specified.

       Simple Usage :: ROBOCOPY source destination /MIR
```

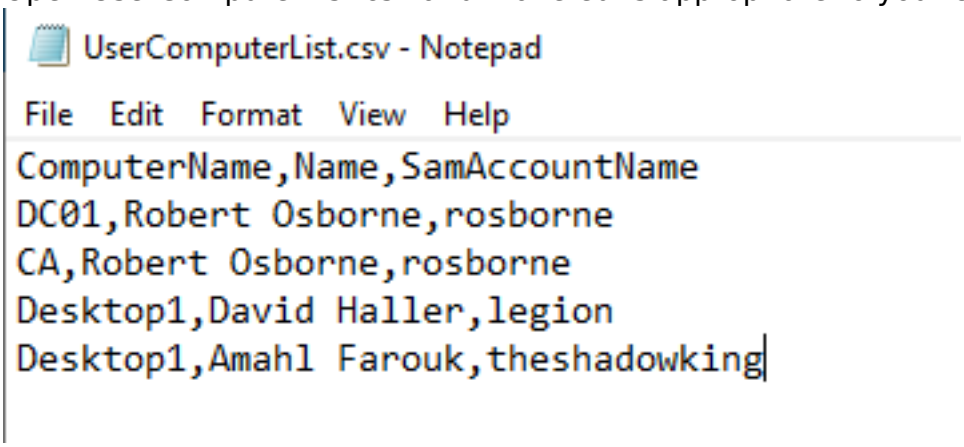
We next need to edit our UserComputerList.csv file for our Unusual Sign In Alert.
This is to define what users we expect to sign into what computers

```
Actions            : {MSFT_TaskExecAction}
Author             : tobor
Date               : 2020-03-05T09:52:14.5713289
Description        : Alerts IT when a DNS zone transfer occurs
Documentation      :
Principal          : MSFT_TaskPrincipal2
SecurityDescriptor :
Settings           : MSFT_TaskSettings3
Source             :
State              : Ready
TaskName           : DNSZoneTransferAlert
TaskPath           : \
Triggers           : {MSFT_TaskEventTrigger}
URI                : \DNSZoneTransferAlert
Version            :
PSComputerName     :

[*] The DNSZoneTransferAlert.xml task should now set up on DC01
[*] The Unusual Sign In Alert will not work until you add entries to the C:\Users\Public\Documents\UserComputerList.csv file.
[*] Pausing execution to allow you time to do this
Press Enter to continue...:
```

Open File explorer and go to Public Documents



Open UserComputerList.csv and make edits appropriate to your environment



Then press ENTER to continue

```
[*] The DNSZoneTransferAlert.xml task should now set up on DC01
[*] The Unusual Sign In Alert will not work until you add entries to the C:\Users\Public\Documents\UserComputerList.csv file.
[*] Pausing execution to allow you time to do this
Press Enter to continue...:
```

More tasks are now created every time you press ENTER

```
Actions             : {MSFT_TaskExecAction}
Author              : Administrator
Date                : 2020-11-03T08:54:11.3205392
Description         : Alerts IT when a new computer has been added to the domain
Documentation       :
```

```
Actions             : {MSFT_TaskExecAction}
Author              : tobor
Date                : 2019-08-28T16:10:38.1606495
Description         : Checks the logs from the last 24 hours for any suspicous logins and emails them to IT
Documentation       :
```

WEF APPLICATION

For more info on how to set this app up see https://btps-secpack.com/wef-application.

HARDENING CMDLETS

Next Powershell version 2 is disabled if you specify it on Computers and Servers

```
============== Remove PowerShell v2 ==============
WINRM over SSL REQUIRERED FOR THIS : Would you like to remove the legacy version of PowerShell from the servers in your environment
[y/N]: y
WINRM over SSL REQUIRERED FOR THIS : Would you like to remove the legacy version of PowerShell from client computers? [y/N]: y
[!] DC01 is vulnerable to a PowerShell downgrade attack
[*] Removing PowerShell Version 2 to remediate PowerShell Downgrade Attack vulnerability
[*] SAFE: PowerShell version 2 is not installed on DC01
[*] SAFE: PowerShell version 2 is not installed on CA
[!] DC01 is vulnerable to a PowerShell downgrade attack
[*] Removing PowerShell Version 2 to remediate PowerShell Downgrade Attack vulnerability
[*] SAFE: PowerShell version 2 is not installed on DC01
[!] DESKTOP1 is vulnerable to a PowerShell downgrade attack
[*] Removing PowerShell Version 2 to remediate PowerShell Downgrade Attack vulnerability

Path   :
Online : True

[!] DC01 is vulnerable to a PowerShell downgrade attack
[*] Removing PowerShell Version 2 to remediate PowerShell Downgrade Attack vulnerability
[*] SAFE: PowerShell version 2 is not installed on DC01
```

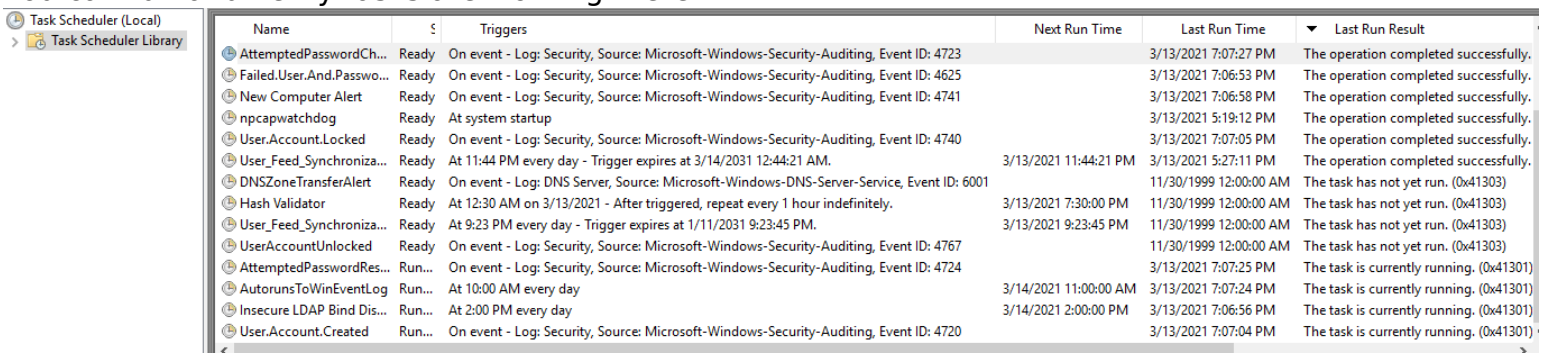
Next DNS over HTTPS Is Enabled on Servers and Computers if you specify it

```
============= ENABLE DNS OVER HTTPS ==============
WINRM over SSL REQUIRERED FOR THIS : Would you like to enabled DNS over HTTPS on the servers in your environment [y/N]: y
WINRM over SSL REQUIRERED FOR THIS : Would you like to enable DNS over HTTPS on the client computers in your environment? [y/N]: y

EnableAutoDOH : 2
PSPath        : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters
PSParentPath  : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache
PSChildName   : Parameters
PSDrive       : HKLM
PSProvider    : Microsoft.PowerShell.Core\Registry


EnableAutoDOH : 2
PSPath        : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters
PSParentPath  : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache
PSChildName   : Parameters
PSDrive       : HKLM
PSProvider    : Microsoft.PowerShell.Core\Registry
RunspaceId    : 81953903-c245-4fc6-b96d-4880787ebf6a


EnableAutoDOH : 2
PSPath        : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters
PSParentPath  : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache
PSChildName   : Parameters
PSDrive       : HKLM
PSProvider    : Microsoft.PowerShell.Core\Registry
RunspaceId    : 23d45463-a7c3-4c91-aed7-1aa589ac9c41
```

And that is it. You can open Task Scheduler on your devices by enter the command into powershell taskschd.msc

```
PS C:\Windows\System32\WindowsPowerShell\v1.0\BTPS-SecPack-master\AutoRunsToWinEvent> taskschd.msc
```

You can run and verify tasks are working there



The **UnusualUserSignInAlert.ps1** file in **C:\Users\Public\Documents** experiences encoding errors

sometimes as well
This can be seen by the aE looking characters by LDAP and RootDSE.

```
PS C:\Windows\system32> .'C:\Users\Public\Documents\UnusualUserSignInAlert.ps1'
At C:\Users\Public\Documents\UnusualUserSignInAlert.ps1:21 char:15
+ $PDC = ([ADSI]â€¢LDAP://RootDSEâ€¢).dnshostname
+               ~~~~~~~~~~~~~~~~~~~~
Unexpected token 'â€¢LDAP://RootDSEâ€¢' in expression or statement.
At C:\Users\Public\Documents\UnusualUserSignInAlert.ps1:21 char:15
+ $PDC = ([ADSI]â€¢LDAP://RootDSEâ€¢).dnshostname
+               ~
Missing closing ')' in expression.
At C:\Users\Public\Documents\UnusualUserSignInAlert.ps1:21 char:35
+ $PDC = ([ADSI]â€¢LDAP://RootDSEâ€¢).dnshostname
+                                   ~
Unexpected token ')' in expression or statement.
    + CategoryInfo          : ParserError: (:) [], ParseException
    + FullyQualifiedErrorId : UnexpectedToken
```

To fix this, open the file by issuing the powershell command
notepad C:\Users\Public\Documents\UnusualUserSignInAlert.ps1

```
PS C:\Windows\system32> notepad C:\Users\Public\Documents\UnusualUserSignInAlert.ps1
PS C:\Windows\system32>
```

Notice the single quote looks highly defined

```
# Regex used for filtering event log
[regex]$Ipv4Regex = ‘\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b’
```

Replace it with a single quote and save the file

```
# Regex used for filtering event log
[regex]$Ipv4Regex = '\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b'
```